	RFP **طرح پژوهشی** **" پیاده‌سازی استاندارد امنیت اطلاعات ISMS** **(پیاده‌سازی سامانه مدیریت امنیت اطلاعات ISMS با رویکرد مدیریت رخدادها و حوادث غیر مترقبه)"**	**کد طرح : ۱۴۰۲۰۷** **تاریخ تنظیم :۱۴۰۲/۰۳/۳۱**

۱- مشخصات درخواست کننده طرح :

واحد تهیه‌کننده :	**اداره کل امنیت و زیرساخت**	**کارشناس تحقیقات : سامان افشار زاده** **الهام کاظمی تلفن تماس: ۸۱۵۶۳۰۴۱**
واحد بهره بردار:	**اداره کل امنیت و زیرساخت**	

۲- ماهیت طرح :

الف) مسئله محور ■ **ب) توسعه محور** ☐ **ج) استقرار فناوری جدید** ☐

۳-واژگان کلیدی :

سیستم مدیریت امنیت اطلاعات (ISMS)، محدوده (Scope)، ارزیابی ریسک (Risk Assessment)، تحلیل کاستی‌ها (GAP Analysis)، مدیریت ریسک امنیت اطلاعات (Information Security Risk Managment)

۴- ضرورت انجام طرح :

پیشرفت سریع و هر لحظه در دنیای فناوری اطلاعات و ارتباطات باعث شده است نیاز به استقرار امنیت بیشتر از هر زمانی آشکار شود. همانقدر که فناوری‌های نوینی روی کار می‌آیند، اگر به امنیت آن توجه نشود، منجر به بروز خطرات و حوادث غیر قابل جبرانی خواهد شد. سازمان‌ها باید اطمینان حاصل کنند که فرآیندهای تجاری، سیاست‌ها و رفتار نیروی انسانی این خطرات را به حداقل می‌رسانند یا کاهش می‌دهند. ISMS یک سیستم مدیریت یکپارچه است که شامل مجموعه‌ای از کنترل‌های امنیتی است که از محرمانه بودن، در دسترس بودن و یکپارچگی دارایی‌ها در برابر تهدیدها و آسیب پذیری‌ها محافظت می‌کند. سیستم مدیریت امنیت اطلاعات (ISMS) چارچوبی از سیاست‌ها و کنترل‌هایی است که امنیت و خطرات را به طور سیستماتیک و در کل امنیت اطلاعات سازمان را مدیریت می‌کند. ISMS شامل چگونگی شناسایی افراد، سیاست‌ها، کنترل‌ها، سپس رسیدگی به فرصت‌ها و تهدیدهای حول اطلاعات ارزشمند و دارایی‌های مرتبط سازمان است. چارچوب ISMS معمولاً بر ارزیابی ریسک و مدیریت ریسک متمرکز است. در واقع می توان به آن به عنوان یک رویکرد ساختاریافته برای تعادل متوازن بین کاهش ریسک و هزینه (ریسک) متحمل شده به سازمان، فکر کرد.

۵- تاریخچه و سوابق طرح :

این طرح تاریخچه و سابقه‌ای در بانک ندارد

۶- اهداف طرح :

[1] Information Security Management System

- ✓ رضایت نیازمندی‌های امنیتی مشتریان و سایر ذینفعان
- ✓ بهبود فرآیندها و فعالیت‌های سازمان
- ✓ تأمین اهداف امنیت اطلاعات سازمان
- ✓ تطابق با آیین نامه‌ها و قوانین و الزامات بالادستی
- ✓ تأمین امنیت در همه سطوح شامل امنیت فیزیکی، پرسنلی و ارتباطات
- ✓ افزایش وجهه و اعتبار سازمان
- ✓ پیاده‌سازی سیستم مدیریت امنیت پویا و مستمر

۷- مشخصات فنی و استانداردهای مورد نیاز :

- ✓ پیاده‌سازی استاندارد امنیت اطلاعات ISO27001
- ✓ شرح خدمات فنی پروژه مطابق بند ۵ الزامات استقرار سیستم مدیریت امنیت اطلاعات مرکز مدیریت راهبردی افتای ریاست جمهوری (پیوست شماره ۱)
- ✓ بهره مندی از تعاریف، متدها و یافته های روز مرتبط با طرح
- ✓ رعایت اصول طرح نویسی
- ✓ رعایت اصول گزارش دهی
- ✓ رعایت اصل امانتداری و اخلاق حرفه ای
- ✓ رعایت سایر ضوابط و دستورالعمل ها حسب اعلام بانک

۸- نتایج مورد انتظار (خروجی مورد انتظارطرح) :

- ✓ مطالعه و بررسی وضعیت فعلی بانک، احصاء نقاط قوت وضعف و ارائه گزارش شناخت
- ✓ تعیین دامنه (Scope) استقرار سیستم مدیریت امنیت اطلاعات (پیوست شماره ۲)اخذ تاییدیه از مرکز مدیریت راهبردی افتای ریاست جمهوری
- ✓ اجرای پروژه ISMS باتوجه به Scope تعیین شده و اخذ گواهینامه ISO27001

۹- مدت زمان اجرای طرح :

یک سال

۱۰- محل تأمین اعتبار طرح :

- ✓ ٪۱ هزینه های غیر عملیاتی بانک در سال ۱۴۰۲

۱۱- مستندات مرتبط با طرح :

- ✓ پیوست شماره ۱: الزامات استقرار سیستم مدیریت امنیت اطلاعات
- ✓ پیوست شماره ۲: راهنمای تعیین دامنه استقرار سیستم مدیریت امنیت اطلاعات
- ✓ رعایت کلیه استانداردها و ضوابط درون/ برون سازمانی مرتبط با طرح حسب اعلام بانک

۱۲- واحدهای مرتبط با اجرای طرح :

ر	نام واحد	نقش
۱		
۲		
۳		

جمهوری اسلامی ایران
ریاست جمهوری
مرکز مدیریت راهبردی افتا

راهنمای تعیین دامنه استقرار سیستم مدیریت امنیت اطلاعات

دی ماه ۹۸

سطح محرمانگی: عادی


بسم الله الرحمن الرحيم

فهرست مطالب

مقدمه

با توجه به چارچوب تعیین شده در استاندارد ISO ۲۷۰۰۱:۲۰۱۳، سازمان‌ها مکلف‌اند مناسب‌ترین دامنه را جهت استقرار سیستم مدیریت امنیت اطلاعات تحلیل و تعیین نمایند. در این نسخه از استاندارد توصیه شده است سازمان مطالعات لازم را بر پایه دو عامل درک سازمان و بافتار آن و شناسایی انتظارات و نیازهای طرف‌های ذی‌نفع، انجام داده و از برآیند این دو عامل و ضمن رعایت اصل اولویت‌بندی، دامنه استقرار سیستم مدیریت امنیت اطلاعات را تعیین نمایند. به عبارتی، اصل بر توجیه‌پذیری محدوده سیستم مدیریت امنیت اطلاعات بوده و نیاز است سازمان دلایل کافی برای انتخاب محدوده پیشنهادی خود گردآوری نموده باشد.

همچنین در نظر داشته باشید که در بسیاری از موارد دلیل عدم اثربخشی و توجیه ناپذیر بودن استقرار سیستم‌های مدیریتی بدلیل انتخاب محدوده نامناسب استقرار سیستم است. عدم حمایت مدیریت ارشد، مقرون به صرفه نبودن تأمین منابع جهت استمرار سیستم‌های مدیریتی و مشکلاتی از این دست عموماً بدلیل عدم توجه به نیاز واقعی کسب‌وکار به موضوع امنیت اطلاعات بدلیل عدم مطالعات صحیح در محدوده استقرار سیستم و در نتیجه انتخاب حوزه‌های فاقد اولویت به عنوان دامنه استقرار سیستم برای سال‌های متمادی رخ می‌دهد.

از این‌رو این سند با تفسیر الزامات ISO۲۷۰۰۱:۲۰۱۳ به عنوان راهنمای تعیین دامنه استقرار سیستم مدیریت امنیت اطلاعات برای سازمان‌ها تدوین شده است و لازم است کارفرمایان، پیش از شروع اجرای پروژه‌های استقرار سیستم مدیریت امنیت اطلاعات و به‌کارگیری مجریان صاحب صلاحیت و برای تعیین مناسب ترین دامنه و نیز تعیین حجم فعالیت‌های مورد نیاز توسط مجری، متناسب با سازمان خود، جداول مورد نیاز را طبق محتوای این سند تهیه نمایند.

۱-درک سازمان و بافتار آن

سازمان می‌بایست باتوجه به نیازهای درونی و ماهیت کسب و کار خود مبادرت به امکان‌سنجی استقرار سیستم مدیریت امنیت اطلاعات نماید. از آنجا که اساساً نیاز به امنیت اطلاعات و تحقق آن برای تمامی ارکان سازمان یکسان نیست، می‌بایست با تدوین یک مدل کاربردی، سازمان را به بخش‌های

کوچک‌تری تقسیم کرده و دستاورد و تأثیر مثبت امنیت اطلاعات را در هر بخش مقداردهی نمود.

برای تقسیم بندی سازمان به اجزاء کوچک‌تر مدل‌های بسیاری وجود دارد:

- می‌توان سازمان را بر اساس فرآیندهای کسب‌وکاری بخش‌بندی نمود؛ به طور مثال فرآیند تولید، فرآیند برنامه‌ریزی، فرآیند خرید، فرآیند مدیریت مالی و غیره.
- در شرایطی که سازمان الگویی حداقلی برای شناسایی و تفکیک فرآیندهای خود نداشته باشد، چارت سازمانی و یا گروه‌های مختلف کاری می‌تواند الگویی برای کوچک‌سازی سازمان باشد.
- در برخی دیگر از موارد، موقعیت‌های جغرافیایی و مکان‌های فیزیکی روشی برای بخش‌بندی سازمان است؛ این روش در مواردی که سازمان ابعاد بزرگی داشته و دارای سایت‌های متعددی است می تواند روش مناسبی باشد.

در این رابطه لازم است جدول شماره ۱ برای افراز سازمان به بخش‌های کوچک‌تر تکمیل گردد:

ردیف	عنوان فرآیند/دپارتمان/گروه	توضیح اثرگذاری بر کسب‌وکار و اهداف سازمان	ارتباط با سایر فرآیندها/دپارتمان‌ها/گروه‌ها
۱			• •
۲			• •

جدول ۱ – افراز سازمان به بخش‌های کوچک‌تر

در صورت نیاز (در سازمان‌های بزرگ و پیچیده) می‌توان افراز سازمان را در دو یا چند مرحله متوالی انجام داد؛ به این ترتیب که فرآیند/دپارتمان/گروه انتخاب شده در مرحله اول اجرای این راهنما، خود در مرحله بعد به زیر فرآیندها یا زیرمجموعه‌ها مجددا تقسیم گردد.

پس از آنکه بر اساس مدل مورد نظر، سازمان به بخش‌های کوچکتری تقسیم شد، نیاز است بافتار (زمینه) داخلی و خارجی تأثیر گذار بر سیستم مدیریت امنیت اطلاعات شناسایی شوند.

شناسایی بافتار داخلی و خارجی در زمینه امنیت اطلاعات به معنی شناسایی عواملی در محیط داخلی و خارجی است که بتواند دلیل و ضرورتی بر استقرار سیستم مدیریت امنیت اطلاعات باشد؛ در واقع محیط داخلی و خارجی است که سازمان در آن به دنبال نیل به اهداف خود است. عوامل خارجی یا محیطی، مواردی هستند که خارج از کنترل سازمان قرار دارند و عوامل داخلی مواردی هستند که تحت کنترل سازمان قرار دارند. این عوامل صرفنظر از داخلی یا خارجی بودن می‌بایست بر امنیت اطلاعات

یا نحوه مدیریت امنیت اطلاعات اثر گذار بوده و نیز به اهداف سازمان مرتبط باشند. برخی از انواع این عوامل در جدول زیر آمده است.

عوامل داخلی	عوامل خارجی یا محیطی
فرهنگ سازمان؛	اجتماعی و فرهنگی
خط‌مشی‌ها، اهداف و راهبردهای نیل به آن‌ها؛	سیاسی، حقوقی، قانونی و مقرراتی
راهبری سازمان، ساختار سازمانی، نقش‌ها و مسئولیت‌ها؛	مالی و اقتصاد کلان
استانداردها و مدل‌هایی که در سازمان پیاده‌شده است (مانند سیستم‌های مدیریتی دیگر)؛	فناوری
روابط قراردادی که بر انتخاب دامنه ISMS اثرگذار باشد؛	طبیعی
فرآیندها و رویه‌ها؛	رقابتی
توانمندی‌ها شامل منابع و دانش؛	
زیرساخت فیزیکی و محیطی؛	
سامانه‌های اطلاعاتی و جریان اطلاعات و فرآیندهای تصمیم‌گیری؛	
نتایج ممیزی‌های قبلی و یا ارزیابی مخاطرات قبلی (در صورت وجود).	

جدول ۲ – نمونه‌های عوامل داخلی و خارجی موثر بر دلیل و ضرورت استقرار ISMS

برای درک بیشتر، در ادامه مثال‌هایی از تاثیر این عوامل بر امنیت اطلاعات یا نحوه مدیریت امنیت اطلاعات و نیز به اهداف سازمان ارائه شده است:

عوامل خارجی	افزایش حملایت سایبری که می‌تواند منجر به توقف در فرآیندهای کسب‌وکار و یا آسیب به سرمایه‌های اطلاعاتی سازمان شود
	توسعه و فراگیری شبکه‌های اجتماعی و امکان افشاء اطلاعات محرمانه سازمان در این بستر
	توانمندی رقبا در بکارگیری پایدار سرویس‌های فناوری اطلاعات در پشتیبانی از محصولات و خدمات
	توسعه فناوری اطلاعات و نیاز به ارائه برخی از سرویس‌ها به مشتریان سازمان برروی بسترهای الکترونیک بدون نیاز به مراجعه حضوری
عوامل داخلی	محافظت از دانش فنی سازمان (شرکت) در برابر سوء استفاده و کپی برداری‌های غیرمجاز
	حفاظت از اطلاعات مربوط به فروش محصولات و خدمات سازمان که در صورت افشاء می‌تواند تأثیرات مخربی بر کسب و کار سازمان به‌دنبال داشته باشد
	ایجاد پایداری حداکثری برای سرویس‌ها و سامانه‌های اطلاعاتی که می توانند منجر به توقف خط تولید محصول شوند

	حفظ صحت پردازش اطلاعات در بخش‌هایی که می تواند منجر به اتخاذ تصمیمات حساس و راهبری سازمان شوند

جدول۳– نمونه‌هایی از تاثیر عوامل داخلی و خارجی

نکته بعدی در خصوص شناسایی عوامل داخلی و خارجی این است که برخی از این عوامل تأثیری بر ضرورت و دلیل استقرار سیستم مدیریت امنیت اطلاعات نداشته بلکه یک عامل تأثیر گذار بر توانایی سازمان در دستیابی به اهداف خود از استقرار سیستم مدیریت امنیت اطلاعات به شمار می‌آید. (شناسایی و تحت کنترل قرار دادن این فاکتورها در ادامه منبع مناسبی برای شناسایی ریسک‌ها و فرصت‌های سیستم مدیریت امنیت اطلاعات مشروح در بند ۶,۱,۱ استاندارد به شمار می‌رود.) مثال هایی از این دسته از عوامل عبارتند از:

عوامل داخلی	عوامل خارجی
تغییرات مداوم در لایه مدیریت ارشد سازمان (اثر منفی)	تحریم و عدم امکان تهیه برخی از تجهیزات و لایسنس‌ها (اثر منفی)
عدم آگاهی لازم و کافی مدیران ارشد نسبت به ضرورت محافظت از دارایی‌های اطلاعاتی (اثر منفی)	نواسانات نرخ ارز و اختلاف میان بودجه پیش بینی شده و هزینه روز تجهیزات امنیتی (اثر منفی)
امکانات زیر ساختی مناسب جهت برگزاری دوره‌های آموزشی و آگاهی‌رسانی به کاربران و پرسنل سازمان (اثر مثبت)	توانمندی‌های شرکت‌های داخلی در بومی‌سازی و تولید برخی تجهیزات و ادوات امنیت اطلاعات (اثر مثبت)

جدول ۴ – نمونه‌های عوامل داخلی و خارجی موثر در دستیابی به اهداف استقرار ISMS

برای ثبت مجموعه عوامل داخلی و خارجی اثرگذار بر سیستم مدیریت امنیت اطلاعات بر مبنای توضیحات فوق لازم است جدول شماره ۵ تکمیل گردد.

در این جدول میزان اهمیت یا اثر عامل می‌تواند با اعداد ۱ و ۲ (برای اثرات مثبت) و ۱- و ۲- (برای اثرات منفی) تکمیل گردد.

ردیف	توضیح عامل اثرگذار	داخلی/خارجی	ضرورت/توانایی	اثر مثبت یا منفی	میزان اهمیت یا اثر عامل
۱					
۲					

جدول ۵ – شناسایی عوامل داخلی و خارجی اثرگذار بر امنیت اطلاعات

۲- شناسایی نیازها و انتظارات ذینفعان

دراین مرحله نیاز است سازمان به تحلیل و شناسایی دقیق آنچه ذینفعان در حوزه امنیت اطلاعات از سازمان انتظار دارند، بپردازد. برای اینکار ابتدا باید تمامی ذی‌نفعان این بخش به خوبی شناسایی شوند. منظور از ذی‌نفعان، موجودیت‌های حقیقی و حقوقی پیرامونی سازمان هستند که سازمان در فضای پویای کسب‌وکار خود با ایشان در ارتباط بوده و بر امنیت اطلاعات سازمان اثرگذار و یا از آن تأثیرپذیر هستند و در نتیجه نیاز است الزامات و انتظارات ایشان بدرستی شناسایی و اجرایی شود.

ذینفعان شامل و نه محدود به موارد زیر می‌باشد:

- مشتریان
- تأمین‌کنندگان
- شرکای تجاری
- هولدینگ‌ها و مجموعه‌های بالادستی
- شرکت‌های تابعه
- مراجع قانونی و حاکمیتی
- نهادهای صنفی
- نهادهای اجتماعی و مدنی

در گام بعدی باید انتظارات و نیازهایی که هر یک از این ذی‌نفعان در حوزه امنیت اطلاعات از سازمان دارند به دقت و بصورت شفاف شناسایی شود. دقت نمایید در این بخش صرفاً باید انتظارات حوزه امنیت اطلاعات ذی‌نفعان را شناسایی شوند. در زیر مثال‌هایی از برخی ذی‌نفعان و انتظارات و نیازهای ایشان در حوزه امنیت اطلاعات ذکر شده است:

مثال‌هایی از ذی‌نفعان	مثال‌هایی از انتظارات و نیازهای آن‌ها
تأمین کنندگان	– رعایت حقوق دارایی معنوی و محافظت از حریم خصوصی اطلاعات
مشتریان	– محافظت از حریم خصوصی اطلاعات – دریافت سرویس‌های اطلاعاتی پایدار، به‌روز، ایمن و صحیح برروی پرتال اطلاع‌رسانی
مرکز مدیریت راهبردی افتای ریاست جمهوری	– استقرار سیستم مدیریت امنیت اطلاعات – دریافت خدمات حوزه افتا از شرکت‌های دارای پروانه فعالیت این بخش
سهامداران	– محافظت از تمامی دارایی‌ها و سرمایه‌های اطلاعاتی سازمان

	– محافظت از حسن شهرت سازمان (شرکت) و جلوگیری از بروز تهدیداتی که می تواند تأثیر منفی براعتماد مشتریان داشته باشد

جدول۶– احصاء نیازمندی‌ها و انتظارات ذی‌نفعان

یک روش مناسب برای مدل‌سازی این بخش امتیازدهی به ذی‌نفعان و انتخاب ضریب اهمیت برای انتظارات ایشان است. به طور مثال سازمان می‌تواند مشتریان خود را در مقایسه با تأمین‌کنندگان از امتیاز بالاتری برخوردار نماید. به طور معمول برای تعیین اهمیت ذی‌نفعان از ترکیب معیار میزان انگیزه یا علاقه‌مندی ذی‌نفع به موضوع (در اینجا امنیت اطلاعات) در کنار معیار توانایی اثرگذاری یا قدرت ذی‌نفع استفاده می‌گردد؛ به گونه‌ای که ذی‌نفعانی با بیشترین علاقه‌مندی و بیشترین توانایی اثرگذاری بالاترین اهمیت را دارا خواهند بود و کمترین اهمیت به ذی‌نفعانی با حداقل علاقه‌مندی و حداقل اثرگذاری تعلق می‌گیرد. توصیه می‌شود میزان اهمیت ذی‌نفعان از بین اعداد ۲ (اهمیت زیاد)، ۱ (اهمیت متوسط) و ۰,۵ (اهمیت کم) در جدول ۷ اختصاص داده شود؛ همچنین چنانچه انتظار یا نیازی از ذی‌نفعان با پیاده‌سازی ISMS در تناقض قرار می‌گیرد با اعداد منفی مشخص شود.

عنوان ذی‌نفع	میزان اهمیت ذی‌نفع	انتظارات و نیازهای مرتبط با امنیت اطلاعات	میزان اهمیت یا اثر انتظار/نیاز

جدول ۷– شناسایی ذی‌نفعان و انتظارات و نیازهای مرتبط با امنیت اطلاعات ایشان

۳- جمع‌بندی یافته‌ها و تعیین اولیه دامنه ISMS

با توجه به اطلاعات جمع‌آوری شده در گام‌های فوق، در این مرحله با تحلیل و نگاشت عوامل داخلی و خارجی شناسایی شده (جدول ۵) و همچنین انتظارات و نیازمندی‌های شناسایی شده ذی‌نفعان (جدول ۷) به بخش‌ها یا فرآیندهای سازمان (جدول ۱)، اولویت و امتیاز هر بخش برای قرارگیری در دامنه سیستم مدیریت امنیت اطلاعات شناسایی می‌شود.

نیاز است با یک مطالعه تطبیقی، مؤثر بودن هر یک از عوامل داخلی و خارجی با بخش‌ها یا فرآیندهایی که شناسایی شده‌اند بررسی و امتیازدهی شود. بدیهی است که فرآیندها و بخش‌هایی که با

عوامل از نوع ضرورت یا عوامل از نوع توانایی مثبت بیشتری مرتبط شوند از اولویت بالاتری برای قرارگیری در دامنه برخوردار خواهند بود.

همچنین باید انتظارات و الزامات گردآوری شده با مدل تفکیک سازمان به بخش‌های کوچک‌تر مطابقت داده شده و اثرگذاری هریک از این انتظارات و الزامات بر بخش‌های سازمان تعیین شود. پر واضح است بخش‌هایی که در تناظر با الزامات بیشتری از ذی‌نفعان قرار دارند و با نیازمندی‌های کمتری در تعارض قرار می‌گیرند از اهمیت بیشتری برای ورود به دامنه، برخوردارند.

در این بخش امتیازات مثبت و منفی شناسایی شده در جداول ۵ و ۷ در صورت ارتباط با استقرار سیستم مدیریت امنیت اطلاعات در بخش یا فرآیند مربوطه درج شده و امتیاز فرآیند یا بخش از جمع جبری اعداد فوق حاصل می‌شود.

عنوان فرآیند/دپارتمان/گروه			امتیاز	جمع امتیاز
	عوامل داخلی و خارجی			
	انتظارات و نیازمندی‌های ذی‌نفعان			
	عوامل داخلی و خارجی			
	انتظارات و نیازمندی‌های ذی‌نفعان			

جدول ۸- وزن‌دهی بخش‌های سازمانی بر اساس عوامل داخلی و خارجی مؤثر و انتظارات ذی‌نفعان

با در نظر گرفتن نتایج حاصل از گام اول و گام دوم، تمامی بخش‌های تفکیک شده سازمان را هم از منظر عوامل داخلی و خارجی و هم از منظر انتظارات ذی‌نفعان تحلیل و امتیاز دهی شده اند و کافی است بخش‌های با امتیاز بالاتر را گزینش نموده و در دامنه سیستم مدیریت امنیت اطلاعات برای شروع بگنجانید.

توجه نمایید که هدف کلی در این حوزه اولویت‌بندی در احراز بخش‌های سازمان در دامنه سیستم است. در حقیقت مقوله امنیت اطلاعات همواره برای تمامی بخش‌ها و ارکان سازمان مؤثر و مفید است

و بدلیل محدودیت در منابع، سازمان‌ها به اجبار استقرار سیستم را از بخش‌های پراهمیت تر آغاز می‌نمایند. لذا این امکان وجود دارد که در نتایج مطالعات انجام گرفته هیچ بخشی از سازمان یافت نشود که امتیازی از امنیت اطلاعات نگرفته باشد؛ بلکه هدف تعیین یک سازوکار منطقی برای تعیین اولویت‌های زمانی و منابعی جهت ارتقا امنیت اطلاعات سازمان است. رویکرد مناسب در این خصوص، تدوین یک برنامه زمانی میان مدت (به طور مثال ۵ ساله) جهت گسترش دامنه سیستم مدیریت امنیت اطلاعات از محدوده اولیه به کل ارکان سازمان است.

در نهایت جدول شماره ۹ به عنوان نتیجه و خروجی رویه فوق تکمیل خواهد شد.

بیانیه دامنه	
دامنه سازمانی	
دامنه فیزیکی	
دامنه پرسنلی	
دامنه فرآیندی	
دامنه تکنولوژی	

جدول ۹- دامنه سیستم مدیریت امنیت اطلاعات

جمهوری اسلامی ایران
ریاست جمهوری
مرکز مدیریت راهبردی افتا

الزامات استقرار سیستم مدیریت امنیت اطلاعات

خرداد ماه ۹۷

سطح محرمانگی: عادی


بسم الله الرحمن الرحيم

مشخصات سند:

عنوان سند	الزامات استقرار سیستم مدیریت امنیت اطلاعات
شناسه سند	**ISMS-howto-1.0**
ویرایش	**۱,۰**
تاریخ آخرین تغییرات	**۱۳۹۷/۰۳/۳۰**
سطح محرمانگی	سطح محرمانگی: عادی
مخاطبان	**سازمان‌ها و شرکت‌های درگیر در پروژه استقرار سیستم مدیریت امنیت اطلاعات**

تهیه کننده	تاییدکننده	تصویب کننده
مجید عسکرزاده **وحید دوست محمدی**	**مینو غریبی**	**محمود روزبهانی**

پیشگفتار:

از آنجائی که امنیت در حوزه‌ی فناوری اطلاعات همواره به عنوان یکی از مسائل روز دنیا مطرح می‌باشد، ارائه‌کنندگان خدمات افتا به منظور تامین امنیت و ممیزی آن در سازمان‌ها و زیرساخت‌های حیاتی کشور فعال شدند. در این راستا، مرکز افتا و سازمان فناوری اطلاعات به منظور ساماندهی خدمات افتا و ارتقاء کیفی ظرفیت‌های بخش خصوصی فعال در زمینه ارائه خدمات افتا نظام ارزیابی خدمات افتا را ایجاد کرده‌اند.

مرکز افتا و سازمان فناوری اطلاعات به عنوان مرجع تائید کننده براساس روال‌ها و خط‌مشی‌های موجود برای ارائه‌کنندگان خدمات افتا، پروانه صادر می‌نمایند. سند "الزامات استقرار سیستم مدیریت امنیت اطلاعات" یک تعریف مشخص از پروژه استقرار سیستم مدیریت امنیت اطلاعات را بیان می‌کند که کارفرما و مجری بر روی سطح کیفی قابل قبول ارائه این خدمت به یک ادبیات مشترک برسند. این سند با این رویکرد با همکاری متخصصان این حوزه تدوین گردیده است.

این سند با مشارکت سازمان فناوری اطلاعات و ارتباطات ایران و شرکت‌های توف نورد، داده پردازان آبشار،کمسیون امنیت نظام صنفی، و مشارکت فعال شرکت‌های پردازشگران داده آرای سپاهان، هیرساویژن، کاربرد سیستم سدید، ایده فروزان امن و راهبران انطباق نیس تهیه شده است.

شایان ذکر است که با هدف پوشش مناسب نیازهای روز کشور، این سند در بازه‌های زمانی دو ساله بازبینی و اصلاح خواهد شد. همچنین مرکز مدیریت راهبردی افتا آماده دریافت پیشنهادهای اصلاحی بهبودی برای بازنگری این سند می‌باشد.

فهرست مطالب

۱ مقدمه

هدف از تدوین این سند، معرفی روش اجرایی جهت آماده‌سازی گزارش برای ارائه به دستگاه‌های زیرساختی (حیاتی، حساس و مهم) و دستگاه‌های غیر زیرساختی است. این سند حداقل انتظارات مرکز مدیریت راهبردی افتا در پروژه سامانه مدیریت امنیت اطلاعات ا ست که در د ستگاه‌های زیر ساختی و غیر زیرساختی توسط شرکت‌های دارای گواهی پیاده‌سازی می‌شود.

۲ قلمرو این سند

همانطور که در بند قبل گفته شد این سند در تمامی پروژه‌های سامانه مدیریت امنیت اطلاعات، در تمامی سطوح، که در د ستگاه های زیر ساختی و غیر زیر ساختی اجرا می شود کاربردی خواهد بود. به عبارت بهتر شرکت‌های مجری این سامانه و سازمان‌ها و واحدهای کارفرما ملزم به رعایت تمامی بندهای این سند هستند.

۳ اصطلاحات و مفاهیم

کارفرما: سازمان‌های دولتی/غیردولتی و یا شرکت‌ها و واحدهای خصوصی که قصد پیاده‌سازی سامانه مدیریت امنیت اطلاعات را دارند.

مجری: شرکت‌های دارای گواهی "مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات" که کارفرما جهت پیاده‌سازی و یا مشاوره پروژه سامانه مدیریت امنیت اطلاعات با آن‌ها قرارداد منعقد کرده است.

قلمرو: محدوده‌ای که برای پیاده سازی سامانه مدیریت امنیت اطلاعات تو سط کارفرما انتخاب شده است.

طرح اقدامی:[۱] برنامه های کلان فناوری اطلاعات است.

روش اجرایی:[۲] شرح اینکه چه کاری توسط چه کسی و در چه زمانی باید انجام شود.

دستورالعمل:[۳] چگونگی انجام کار است.

---

[۱] Plan
[۲] Procedure
[۳] Instruction

۴ اقدامات کارفرما قبل از پیشنهاد پروژه

کارفرما قبل از پیشنهاد پروژه باید اقدامات زیر را انجام دهد:

- تعیین محدوده (قلمرو) پروژه سامانه مدیریت امنیت اطلاعات
- تعیین متولی/مسئول پروژه ISMS در سازمان: متولی پروژه در سازمان باید مشخص باشد که با تیم پیاده ساز، مشاور و ممیز در ارتباط بوده و اطلاعات مورد نیاز پروژه را در اختیار شرکت مجری قرار دهد.
- برگزاری مناقصه بین شرکت‌های دارای گواهینامه مرتبط از مرکز مدیریت راهبردی افتا
- تعیین کمیته اجرایی ISMS در سطح سازمان: در سازمان باید تیمی از کارشناسان برای همراهی با شرکت مجری تعیین شوند. این تیم با شرکت در دوره های آموزشی و فراگیری اصول سامانه مدیریت امنیت اطلاعات در کنار شرکت مجری وظیفه پیاده سازی و نگهداری از سامانه ISMS را در سازمان خواهد داشت.
- ارتباط با ذی‌نفعان: در صورتی که کارفرما جزء دستگاه‌های زیرساختی(حیاتی، حساس و مهم) باشد در پیاده سازی سامانه مدیریت امنیت اطلاعات ملزم به رعایت الزامات مرکز مدیریت راهبردی افتا خواهد بود که در قالب "طرح امن سازی زیر ساخت‌های حیاتی در قبال حملات الکترونیکی" به زیرساخت‌ها ابلاغ شده است و از این مرکز قابل استعلام است. در غیر اینصورت هر گونه الزام بالادستی که سازمان ملزم به رعایت آن است و پروژه ISMS می تواند تحت تاثیر آن باشد، باید شناسایی شده و اطلاعات آن در اختیار شرکت مجری قرار گیرد.

۵ اجزای فنی سند پیشنهاد پروژه

۵-۱ قلمرو پروژه

کارفرما باید محدوده اجرایی پروژه ISMS را به طور دقیق مشخص کند. در مورد دستگاه‌های زیرساختی، قلمرو پروژه باید با هماهنگی مرکز افتا تعریف شود و به تایید این مرکز برسد.

۵-۲ شرح خدمات فنی پروژه

در ادامه مطابق با ا ستانداردهای خانواده ISO/IEC 27000 فازهای ا صلی پروژه سامانه مدیریت امنیت اطلاعات(ISMS) و شرایط پیاده‌سازی آن‌ها آورده شده است. کارفرما و مجری ملزم به رعایت موارد مذکور هستند.

۱– بازبینی زمینه (بافتار) و ذینفعان	
توضیحات فعالیت‌ها	• زمینه (بافتار) داخلی و خارجی سازمان بازبینی گردد. • ذینفعان شناسایی شده و انتظارات ذینفعان از سیستم مدیریت امنیت اطلاعات بررسی گردد.
گستره و پوشش فعالیت	• بررسی و بازنگری موارد مربوط به مدیریت امنیت اطلاعات از اطلاعات کلی این موضوع در سازمان می‌شود • بررسی توسط مجری بر اساس اطلاعات زمینه (بافتار) و ذینفعان که توسط کارفرما پیش از آغاز پروژه تهیه شده است، انجام خواهد شد.
خروجی	• عوامل داخلی و خارجی • فهرست ذینفعان و انتظارات ایشان **توضیح:** (هر دو می‌تواند مستقلاً یا به عنوان بخشی از یک سند دیگر –مثلاً سند دامنه– ارائه شود)
سطح کیفی مورد انتظار	اطلاعات مباید دقیقاً منطبق بر سازمان و شرایط آن بوده و موارد ذکر شده در استاندارد IISO/IEC 27001 در مورد زمینه (بافتار) بیرونی و درونی را شامل شود.
مسئولیت‌های به عهده کارفرما	• مستندات زمینه (بافتار) و ذینفعان تهیه شده توسط کارفرما پیش از آغاز پروژه در اختیار مشاور قرار گیرد. • تحلیل SWOT در سطح کسب و کار و یا موارد مرتبط با برنامه‌ریزی استراتژیک در صورت وجود در اختیار مجری قرار گیرد. • زمینه (بافتار) و انتظارات ذینفعان تأیید و تصویب گردد.
۲– نهایی‌سازی دامنه	
توضیحات فعالیت‌ها	دامنه سیستم مدیریت امنیت اطلاعات باید با در نظر گرفتن زمینه (بافتار) و انتظارات ذینفعان نهایی شود.
گستره و پوشش فعالیت	دامنه تعیین شده در ابتدای پروژه با توجه به زمینه (بافتار) و انتظارات ذینفعان برر سی شده و در صورت نیاز باید بازنگری شود.
خروجی	• سند دامنه سیستم مدیریت امنیت اطلاعات (می‌تواند مستقلاً یا به عنوان بخشی از یک سند دیگر ارائه شود) – در قالب مستندات تحت کنترل • پیشنهاد تغییرات در پروژه (در صورت تغییر دامنه)
سطح کیفی مورد انتظار	• عنوان دامنه (که در گواهینامه ثبت می شود) به طور دقیق و شفاف مشخص باشد. • دامنه پرسنلی به طور دقیق مشخص باشد. • محدوده تکنولوژیکی به طور دقیق مشخص شود. در این محدوده باید ایستگاه‌های کاری، برنامه‌های کاربردی خاص/توسعه داده شده، سرورها، سازوکارهای امنیتی (نظیر فایروال، IDS/IPS و ...) و موارد دیگر به طور دقیق مشخص شود. • محدوده فرایندی به طور دقیق مشخص باشد. در این محدوده باید فرایندهای کاری و سرویس‌های فناوری اطلاعات که در محدوده قرار می‌گیرند به طور دقیق مشخص شود. • محدوده سازمانی شفاف باشد. در این محدوده باید تمامی قسمت‌هایی از سازمان (به طور مثال معاونت ها، واحدها، گروه ها و...) که در محدوده قرار می گیرند به طور دقیق مشخص شوند. • محدوده فیزیکی تعریف شود. این محدوده شامل محدوده فیزیکی دامنه نظیر سایت های فیزیکی، مراکز داده و... خواهد بود.

	• موارد خارج از دامنه با توجه به زمینه (بافتار) و انتظارات ذینفعان مشخص شود و واسطها و وابستگی‌ها با فعالیت‌های خارج از سازمان درنظر گرفته شود. **توضیح:** در مورد سازمان‌های دولتی/ غیردولتی زیرساختی و شرکت‌های خصوصی دارای زیرساخت حیاتی دامنه پروژه باید به تایید مرکز مدیریت راهبردی افتا برسد.
مسئولیت‌های به عهده کارفرما	• بازنگری حدود قرارداد مجری در صورت تغییر دامنه استقرار • تأیید اولیه دامنه سیستم مدیریت امنیت اطلاعات
۳- گردآوری اطلاعات اولیه و تهیه طرح مدیریت پروژه و به‌روزرسانی برنامه اقدام	
توضیحات فعالیت‌ها	• مجری شناخت اجمالی روی سازمان کارفرما و محدوده پروژه کسب کند. • مخاطرات پروژه تعیین شود. • مراحل تفکیکی انجام پروژه توسط مجری و با همکاری کارفرما تهیه شود. • برنامه های زمان‌بندی و مدیریت پروژه روی هر یکی از مراحل تفکیکی پروژه توسط مجری و با همکاری کارفرما تهیه شود.
گستره و پوشش فعالیت	تدوین طرح مدیریت پروژه به عهده مجری ا ست که حداقل شامل فرآیندهای مدیریت زمان، ارتباطات، کیفیت و ریسک پروژه می‌شود.
خروجی	• سند اولیه طرح مدیریت پروژه PMP • نسخه اولیه برنامه اقدام پروژه Action plan
سطح کیفی مورد انتظار	• طرح مدیریت پروژه حداقل باید شامل روال‌ها، مسئولیت‌ها و فرم‌های مورد نیاز برای فرآیندهای مربوطه باشد. این طرح توسط مجری ارائه می شود. • برنامه اقدام حداقل باید تا سطح ۳ شکست فعالیت‌ها، ترتیب و توالی فعالیت‌ها و خروجی‌ها را شامل گردد و دربرگیرنده اقدامات مورد نیاز از سمت کارفرما و مجری، به طور دقیق باشد. این برنامه توسط مجری ارائه می شود. • زمانبندی اجرای فعالیت‌ها حداقل باید تا سطح ۲ توسط مجری ارائه شود.
مسئولیت‌های به عهده کارفرما	تأیید اولیه طرح مدیریت پروژه و برنامه اقدام پروژه
۴- برگزاری جلسه افتتاحیه رسمی	
توضیحات فعالیت‌ها	• نمایندگان رسمی کارفرما و مجری باید معرفی شوند. • نحوه مدیریت پروژه (شامل نقش‌ها و مسئولیت‌های طرفین و فرآیندهای مدیریت پروژه) به طور دقیق بررسی شود. • توافق در مورد Milestone های مراحل تفکیک انجام پروژه صورت گیرد. **توضیح:** لیست افراد شرکت مجری باید در گواهینامه شرکت مجری که از طرف مرکز مدیریت راهبردی افتا صادر شده است، آورده شده باشد. در غیراینصورت فرد معرفی شده از طرف شرکت مجری مجاز به فعالیت در سازمان/شرکت کارفرما نیست.
گستره و پوشش فعالیت	• برگزاری جلسه/جلساتی در محل کارفرما • بازدید اولیه از سازمان

خروجی	• صورت‌جلسه آغاز پروژه • طرح نهایی مدیریت پروژه و برنامه نهایی اقدام پروژه • دامنه نهایی شده سیستم مدیریت امنیت اطلاعات • اصلاحات و تغییرات در قرارداد شرکت مجری در صورت تغییر دامنه نسبت به تعریف اولیه پیش از آغاز پروژه
سطح کیفی مورد انتظار	این جلسه با حضور مدیر ارشد کارفرما، مدیران ذینفع در دامنه پروژه، مدیران پروژه کارفرما و همچنین تیم پیاده‌سازی/مشاور شرکت مجری باید برگزار شود.
مسئولیت‌های به عهده کارفرما	• هماهنگی برگزاری جلسه • تصویب نهایی طرح مدیریت پروژه و برنامه اقدام پروژه • تصویب نهایی دامنه سیستم مدیریت امنیت اطلاعات • تأیید و ابلاغ تغییرات در قرارداد مجری در صورت تغییر دامنه استقرار نسبت به شرح کار اولیه
۵– تهیه/بررسی و به‌روزرسانی روش مدیریت اطلاعات مستندشده	
توضیحات فعالیت‌ها	تدوین/بررسی و به‌روزرسانی موارد زیر انجام شود: ○ ساختار اطلاعات مستند شده سازمان ○ قالب و چارچوب هر یک از انواع اطلاعات مستند شده ○ نحوه شناسایی، کدگذاری و مدیریت ویرایش‌ها ○ روال و مسئولیت‌های تهیه، تدوین، تأیید، تصویب، ابلاغ، انتشار و نگهداری مستندات ○ ساختار، سازوکار و ابزارهای مورد نیاز مدیریت و نگهداری کتابخانه مستندات و آرشیو سوابق سازمانی
گستره و پوشش فعالیت	• در صورت وجود سیستم‌های مدیریتی دیگر و یا روال‌های مدیریت اسناد و سوابق در سازمان، مجری باید روال موجود را از نظر کفایت و تناسب بررسی نموده و در صورت نیاز نظرات اصلاحی خود را به کارفرما ارائه دهد. • در صورتی که روال مدیریت اسناد و سوابق در سازمان وجود نداشته باشد، مجری باید فرآیند مربوطه و جزئیات مورد نیاز آن، مشتمل بر ساختار، قالب، مسئولیت‌های آماده‌سازی، تأیید، انتشار، مدیریت، بازنگری و به‌روزرسانی اطلاعات مستند شده را تهیه نماید. • در مورد سازوکار و ابزارهای مورد نیاز جهت مدیریت و نگهداری کتابخانه مستندات و آرشیو سوابق، پیشنهاد توسط مجری ارائه می‌گردد، لیکن اجرا و پیاده‌سازی آن به عهده شرکت مجری نیست.
خروجی	• روال بازنگری/تدوین شده مدیریت اطلاعات مستند شده • ساختار، سازوکار و ابزارهای مورد نیاز طراحی/بازنگری شده مدیریت و نگهداری کتابخانه مستندات سازمانی و آرشیو سوابق
سطح کیفی مورد انتظار	• توصیه می شود روال ارائه شده برای مدیریت اطلاعات مستند شده از راهنمایی‌های استاندارد ISO10013 تبعیت نماید و با دیگر سیستم‌های مدیریتی مستقر، یکپارچه باشد. • درباره قالب اسناد لازم است نوع مستند، هدف و دامنه، عنوان، تاریخ تصویب و انتشار، طبقه‌بندی امنیتی، کد سند، شماره ویرایش و سوابق ویرایش‌ها، مشخصات تدوین کننده، تأیید و تصویب‌کننده و همچنین مسئول بهره‌برداری و نگهداری مشخص شود. • در مورد اسناد و سوابق، الزامات قالب شامل زبان، قلم، نوع فایل و ویرایش نرم‌افزار مربوطه، نحوه مدیریت نسخ کاغذی و الکترونیک مشخص گردد.

	• فرآیند نگهداری و بازنگری شامل مدت اعتبار، مسئول بازنگری، چکانه (Trigger) بازنگری و مدیریت تغییرات در اطلاعات مستند شده می‌شود.
مسئولیت‌های به عهده کارفرما	• در صورت استقرار سیستم‌های مدیریتی دیگر و یا روال‌های مدیریت اسناد و سوابق، مستندات مرتبط در اختیار مجری قرارداده شود. • اصلاحات در روال موجود ابلاغ شده و اصلاح گردد و در صورتی که روال جدیدی تدوین شود ابلاغ گردد. • سازوکار و ابزارهای مورد نیاز مدیریت و نگهداری کتابخانه مستندات اجرا و پیاده‌سازی شود.
۶– تهیه سند خط مشی امنیت اطلاعات	
توضیحات فعالیت‌ها	خط مشی امنیت اطلاعات با در نظر گرفتن الزامات استاندارد تهیه، به تأیید مدیریت ارشد سازمان رسیده و ابلاغ گردد.
گستره و پوشش فعالیت	تهیه پیش‌نویس و ارائه راهنمایی‌های مناسب به مدیریت ارشد به عهده شرکت مجری خواهد بود.
خروجی	سند خط‌مشی امنیت اطلاعات (در قالب مستندات تحت کنترل)
سطح کیفی مورد انتظار	• پیش‌نویس تهیه شده توسط مجری باید متناسب با مشخصات سازمان/شرکت کارفرما و نوع کسب و کار، برای کارفرما خصوصی‌سازی شده و متناسب با اهداف کلان سازمان/شرکت کارفرما باشد. • این سند باید رویکرد سازمان در قبال الزامات بالادستی را مشخص نماید. **توضیح:** در صورتی که برای سایر سیستم‌های مدیریتی مستقر در سازمان خط مشی‌هایی وجود دارد، خط مشی سیستم مدیریت امنیت اطلاعات (که توسط مجری پیشنهاد می شود) باید همراستا و همسو با سایر خط مشی‌های سیستم‌های مدیریتی مستقر در سازمان/شرکت کارفرما باشد.
مسئولیت‌های به عهده کارفرما	• همکاری و مسئولیت پذیری مدیریت ارشد برای اطمینان از منعکس شدن ملاحظات و انتظارات سازمان در خط مشی • نهایی‌سازی و ابلاغ خط‌مشی به کارکنان و به فراخور نیاز ذینفعان
۷– تعیین ساختار، نقش‌ها، مسئولیت‌ها و اختیارات سیستم مدیریت امنیت اطلاعات و صلاحیت‌های مورد نیاز	
توضیحات فعالیت‌ها	• شرح وظایف و مسئولیت‌های حوزه ISMS و انطباق آن با ساختار سازمانی به طور شفاف باید مشخص شود. • صلاحیت‌های مورد نیاز هر نقش شامل دانش، مهارت و تجربه مورد نیاز باید تعیین شود.
گستره و پوشش فعالیت	• نقش‌ها، مسئولیت‌ها و اختیارات مرتبط با موارد زیر باید مشخص شود: ○ مختص ISMS، شامل نقش‌ها، مسئولیت‌ها و اختیارات مرتبط با هماهنگی، پیاده‌سازی، اجرا، نگهداری، گزارش‌دهی، مشاوره و بهبود فرآیندها و کنترل‌های امنیتی ○ مالکین دارایی و ریسک ○ مدیران، پرسنل سازمان و کاربران عمومی در رابطه با ISMS
خروجی	• شناسنامه نقش‌ها، مسئولیت‌ها، اختیارات و صلاحیت‌های مرتبط با امنیت اطلاعات (هماهنگ با قالب مورد استفاده سازمان) • شناسنامه کمیته/کمیته‌های مرتبط با سیستم مدیریت امنیت اطلاعات **توضیح:**

	- در خصوص دستگاه‌های زیرساختی در کمیته‌های امنیتی پیشنهادی در سازمان/شرکت کارفرما، نماینده‌ای از مرکز افتا نیز در ساختار این کمیته‌ها لحاظ شود.
سطح کیفی مورد انتظار	تمامی نقش‌ها، مسئولیت‌ها و صلاحیت‌ها باید توسط مجری و پس از مطالعه و شناخت سازمان/شرکت کارفرما برای کارفرما خصوصی‌سازی شده و متناسب با ساختار سازمانی وی تعریف شود. **توضیح**: - مجری موظف است نقش‌ها، مسئولیت‌ها و اختیارات مرتبط با ISMS را به کارفرما پیشنهاد دهد و طراحی ساختار سازمانی یا نقش‌ها و مسئولیت‌های کارکردی سازمان،جزء وظایف وی به حساب نمی‌آید.
مسئولیت‌های به عهده کارفرما	• ارائه مستندات نقش‌ها و مسئولیت‌ها و اختیارات و صلاحیت‌های موجود سازمانی به مجری • ادغام نقش‌ها و مسئولیت‌ها و اختیارات و صلاحیت‌های مرتبط با سیستم مدیریت امنیت اطلاعات در اسناد سازمانی مربوطه و ابلاغ آن
۸– شناسایی مخاطرات و فرصت‌های سیستم مدیریت امنیت اطلاعات	
توضیحات فعالیت‌ها	• موارد ناشی از زمینه (بافتار) درونی و بیرونی و انتظارات ذینفعان بررسی شده و مخاطرات و فرصت‌های مربوط به استقرار سیستم مدیریت امنیت اطلاعات و حصول نتایج مطلوب شناسایی شوند. • اقدامات لازم برای پرداختن به مخاطرات و فرصت‌های فوق الذکر شناسایی و اجرا گردد.
گستره و پوشش فعالیت	شامل مخاطرات و فرصت‌های پروژه استقرار ISMS و همچنین مخاطرات و فرصت‌های عملکرد ISMS و حصول نتایج مورد انتظار آن **توضیح**: موارد فوق می‌تواند در قالب مدیریت ریسک پروژه نیز پوشش داده شود.
خروجی	• شناسایی مخاطرات و فرصت‌ها و اقدامات متناسب برای پرداختن به مخاطرات و فرصت‌ها که اجرایی شده و با سیستم یکپارچه هستند. • نتایج ارزیابی اثربخشی اقدامات فوق
سطح کیفی مورد انتظار	• سازوکاری برای ارزیابی تأثیر اقدامات و پایش اثربخشی اقدامات طرح‌ریزی شده مستقر گردد؛ این سازوکار می‌تواند در قالب مدیریت مخاطرات امنیت اطلاعات ادغام شده و یا مجزا باشد. • در صورت امکان یکپارچه‌سازی شناسایی مخاطرات و فرصت‌های سیستم با روش مدیریت مخاطرات امنیت اطلاعات و شناسایی مخاطرات و فرصت‌های سایر سیستم‌های موجود در سازمان صورت پذیرد.
مسئولیت‌های به عهده کارفرما	نهایی سازی، ابلاغ، اجرا و یکپارچه‌سازی اقدامات طرح‌ریزی شده در روال‌های سازمان
۹–تدوین متدولوژی مدیریت مخاطرات امنیت اطلاعات	
توضیحات فعالیت‌ها	• روش مدیریت مخاطرات امنیت اطلاعات شامل روش شناسایی، تحلیل، ارزشیابی، معیارهای پذیرش مخاطرات باید متناسب با شرایط کسب و کار کارفرما توسط مجری خصوصی سازی شود. **توضیح:** - روش شناسایی مخاطرات می‌تواند مبتنی بر «دارایی–آسیب‌پذیری–تهدید» و یا «رویداد محور» و یا دیگر روش‌ها باشد - رویکرد تحلیل مخاطرات می‌تواند کیفی، کمی یا نیمه–کمی باشد

گستره و پوشش فعالیت	تمامی جزئیات فرآیند مدیریت مخاطرات شامل فازهای مختلف، اقدامات، راهنماها، روش گردآوری و تحلیل اطلاعات و مخاطرات، فرم‌ها و قالب‌ها و همچنین ابزارها (در صورت نیاز به ابزار) باید شناسایی و مدون گردد.
خروجی	سند متدولوژی مدیریت مخاطرات امنیت اطلاعات – در قالب مستندات تحت کنترل
سطح کیفی مورد انتظار	• رویه مدیریت مخاطرات امنیت اطلاعات با اهداف، زمینه (بافتار)، انتظارات ذینفعان و شرایط سازمان/شرکت کارفرما منطبق باشد و متناسب با آن باید خصوصی‌سازی شود. • روش مدیریت مخاطرات استفاده شده باید بتواند منجر به تولید نتایج همخوان و قابل تکرار شود. • رویه مدیریت مخاطرات پوشش دهنده انواع مختلف مخاطرات (فرآیندی، فنی، مدیریتی و ...) باشد. • رویه مدیریت مخاطرات قابلیت اجرا توسط سازمان را داشته باشد. **توضیح:** - در صورتی که در سازمان/شرکت کارفرما رویه‌ای برای مدیریت مخاطرات مستقر باشد، رویه مدیریت مخاطرات امنیت اطلاعات باید حتی الامکان همسو و یکپارچه با روش موجود باشد.
مسئولیت‌های به عهده کارفرما	تأیید و ابلاغ روال مدیریت مخاطرات
۱۰– ارزیابی مخاطرات امنیت اطلاعات	
توضیحات فعالیت‌ها	مخاطرات امنیت اطلاعات مطابق با متدولوژی مدیریت مخاطرات، شناسایی، تحلیل و ارزیابی شوند.
گستره و پوشش فعالیت	- تجمیع، دسته‌بندی، صحت‌سنجی، تحلیل اطلاعات و ارائه نتایج مربوط به مخاطرات امنیت اطلاعات - شناسایی آسیب‌پذیری‌های فنی با پویش آسیب‌پذیری در سطح سیستم، سرویس و برنامه کاربردی **توضیح:** - تجمیع، دسته‌بندی، صحت‌سنجی، تحلیل اطلاعات و ارائه نتایج مربوط به مخاطرات امنیت اطلاعات در سال اول پیاده‌سازی سامانه مدیریت امنیت اطلاعات، به عهده شرکت مجری و با همکاری و آموزش کامل کارفرما خواهد بود و از سال‌های بعدی پیاده‌سازی به عهده کارفرما و با همکاری و مشاوره شرکت مجری خواهد بود.
خروجی	• در خصوص مخاطرات امنیت اطلاعات، شناسایی موارد زیر: ○ سناریوی مخاطره ○ سطح مخاطره ○ در صورت استفاده از رویکرد مبتنی بر «دارایی–آسیب‌پذیری–تهدید»، جزئیات مربوطه ○ نتیجه مقایسه مخاطرات با معیار پذیرش و فهرست مخاطرات نیازمند اقدام کنترلی و مخاطرات ابقا شده (Retained)
سطح کیفی مورد انتظار	• میزان ریزدانگی، جزئیات و پوشش حوزه‌های مختلف در ارزیابی مخاطرات کافی و همگن باشد. • مخاطرات خاص مرتبط با صنعت و کسب و کار کارفرما توسط مجری و با همکاری کارفرما استخراج شود. • کلیه مخاطرات سیستمی و فنی شناسایی شوند. • کلیه دارایی‌های امنیت اطلاعات شناسایی شوند. **توضیح:** - در خصوص استخراج دارایی‌های امنیت اطلاعات موارد زیر باید رعایت شوند:

	○ مدل دارایی ها (ترجیحا با رویکرد سرویس گرایی) توسط شرکت مجری پیشنهاد شده و رابطه سلسله مراتبی و وابستگی بین دارایی‌ها تهیه شود. در صورتی که مدل دارایی خاصی در سازمان/شرکت کارفرما مستقر است مدل دارایی حتی الامکان منطبق و یا همسو با مدل موجود باشد. ○ دارایی‌های اصلی و پشتیبان و رابطه بین آن‌ها شناسایی شوند. ○ اطمینان حاصل شود که کلیه دارایی‌های اصلی(اولیه) شناسایی شده‌اند. ○ آموزش فرآیند گردآوری فهرست دارایی‌ها و مدل دارایی بر عهده مجری و گرد آوری دارایی‌ها بر عهده کارفرما با هدایت و نظارت شرکت مجری خواهد بود. ○ مسئولیت اطمینان از اجرای کامل فرآیند گردآوری دارایی‌ها بر عهده مجری است. ○ کارفرما موظف است تسلط لازم برای مدیریت دارایی‌ها را در طول زمان داشته باشد. ○ در خصوص دستگاه‌های زیرساختی، کارفرما باید سامانه‌های مدیریت دارایی را در سازمان/شرکت مستقر کند. - در مورد استخراج آسیب پذیری‌های فنی و غیرفنی موارد زیر رعایت شود: ○ برای استخراج آسیب‌پذیری‌ها حداقل از منابع زیر استفاده شود: ▪ آسیب پذیری‌های مرتبط با کنترل‌های پیوست الف استاندارد ۲۷۰۰۱ و توضیحات مندرج در ۲۷۰۰۲ ▪ پیوست D استاندارد ۲۷۰۰۵ ▪ نتایج پروژه‌های قبلی ارزیابی آسیب‌پذیری و تست نفوذ و سوابق رخدادها در دامنه ○ آسیب‌پذیری‌های خاص مرتبط با صنعت و کسب و کار کارفرما توسط مجری و با همکاری کارفرما استخراج شود. ○ شناسایی آسیب‌پذیری‌های فنی در دستگاه‌های غیر زیرساختی؛ از طریق پویش آسیب‌پذیری، حداقل در سطح سیستم، سرویس و برنامه کاربردی با هماهنگی با کارفرما در محیط کارفرما توسط شرکت مجری(در صورتی که این توانایی در کارفرما وجود نداشته باشد و یا کارفرما تمایل به برون سپاری این خدمت داشته باشد) انجام می شود. ○ شناسایی آسیب‌پذیری‌های فنی در دستگاه‌های زیرساختی؛ از طریق انجام آزمون نفوذپذیری در کل دامنه پیاده‌سازی، با هماهنگی با کارفرما توسط شرکت مجری (در صورتی که این توانایی در کارفرما وجود نداشته باشد و یا کارفرما تمایل به برون سپاری این خدمت داشته باشد) انجام می شود. ○ شناسایی آسیب‌پذیری‌های غیرفنی در سال اول به عهده مجری و با همکاری و آموزش کامل کارفرما و از سال‌های بعدی پیاده سازی، به عهده کارفرما و با همکاری و مشاوره شرکت مجری خواهد بود. - در محاسبه اثر ریسک معیارهای محرمانگی، یکپارچگی و دسترس پذیری دیده شوند.
مسئولیت‌های به عهده کارفرما	• گردآوری و ارائه اطلاعات پایه‌ای مورد نیاز ارزیابی مخاطرات مربوط به کارفرما (مانند دارایی‌ها، سوابق رخدادها و...) به شرکت مجری • ارائه اطلاعات آسیب‌پذیری فنی تجهیزات، ابزارها و سیستم‌ها به شرکت مجری (مگر در مواردی که انجام ارزیابی آسیب‌پذیری فنی در شرح خدمات مجری درج شده باشد)

۱۱– مقابله با مخاطرات امنیت اطلاعات

توضیحات فعالیت‌ها	• استراتژی مقابله با مخاطرات تعیین شود؛ • راهکارهای مقابله با مخاطرات تعریف و به کنترل‌های پیوست الف استاندارد ISO/IEC 27001 نگاشت شود؛ • سند بیانیه کاربردپذیری (SoA) تدوین شود؛ • طرح مقابله با مخاطرات(RTP) تدوین شده و به تأیید مالکین مخاطرات برسد.
گستره و پوشش فعالیت	• تعیین استراتژی‌های مقابله با مخاطرات و پیشنهاد کنترل‌های مقابله با مخاطرات با توجه به شناخت از سازمان/شرکت کارفرما، توسط شرکت مجری با همکاری کارفرما انجام می‌شود؛ • تجمیع، قالب‌دهی و تولید سند طرح مقابله با مخاطرات توسط مجری با همکاری کارفرما و آموزش کامل وی انجام می‌شود؛ • تجمیع اطلاعات، قالب‌دهی و تولید سند بیانیه کاربردپذیری (SoA) توسط مجری با همکاری کارفرما و آموزش کامل وی انجام می‌شود؛ • ارائه طراحی جزئی فنی، فهرست اقلام (LoM)، پیاده‌سازی و بهره‌برداری از کنترل‌های مقابله با مخاطرات در مسئولیت شرکت مجری نیست. کارفرما برای پیاده‌سازی کنترل‌های پیشنهادی باید از شرکت‌های دارای گواهینامه مرتبط از مرکز مدیریت راهبردی افتا (در صورتی که توانایی پیاده‌سازی کنترل در کارفرما وجود نداشته باشد و یا کارفرما تمایل به برون‌سپاری خدمت داشته باشد) استفاده نماید. • RFP های فنی مورد نیاز و شرح خدمات اصلی برای پروژه های مورد نیاز، به صورت کلان تهیه می‌گردد.
خروجی	• طرح مقابله با مخاطرات (RTP) • سند بیانیه کاربردپذیری (SoA)
سطح کیفی مورد انتظار	- ارتباط هر راهکار با مخاطرات مشخص و انتخاب راهکار از منظر اثربخشی و کارآمدی (بهره‌وری) قابل دفاع باشد؛ - سند SoA شامل توجیه شمول و کنارگذاری کنترل‌ها، وضعیت کنونی کنترل، راهکارهای اجرایی به‌کارگرفته شده برای هر کنترل، اسناد و سوابق مرتبط با هر کنترل و مسئولیت اجرای هر کنترل باشد؛ - RTP شامل ریسک، کنترل منتخب، راهکارهای اجرایی مربوطه، وضعیت و پیشرفت اجرای اقدامات، مالک مخاطرات، مقدار مخاطره اولیه و پیش‌بینی مخاطره باقیمانده، مسئولیت اجرا، برنامه زمانی یا زمان پایان اقدامات باشد؛ **توضیح:** - کنترل‌های پیشنهادی در یکی از چهاردسته زیر قرار می گیرد: ○ سیاست: مجری با هماهنگی و تایید کارفرما ○ روش اجرایی: مجری با هماهنگی و تایید کارفرما (مانند رویه مدیریت حوادث) ○ دستورالعمل: کارفرما با هماهنگی و هدایت مجری (مانند چگونگی تغییر کلمه عبور) ○ طرح: پیشنهاد عنوان طرح و نیازمندی‌های ریسک توسط مجری و تهیه برنامه زمانی اجرای طرح توسط کارفرما (نیاز به زیرساخت‌های نرم افزاری یا سخت افزاری) ○ آموزش و آگاهی‌رسانی
مسئولیت‌های به عهده کارفرما	• تبدیل کنترل‌ها و اقدامات مقابله با مخاطرات به برنامه‌اجرایی یا پروژه

	• ارائه برنامه زمانی اجرایی‌سازی طرح مقابله با مخاطرات • پیگیری تصویب طرح مقابله با مخاطرات توسط مالکین مخاطرات • ابلاغ طرح مقابله با مخاطرات • پیگیری اجرای طرح مقابله با مخاطرات مطابق برنامه مصوب
۱۲– تعیین اهداف امنیت اطلاعات و تدوین برنامه نیل به اهداف	
توضیحات فعالیت‌ها	• اهداف امنیت اطلاعات همراستا با خط مشی امنیت اطلاعات استخراج شود و روش و سنجه‌های اندازه‌گیری تحقق اهداف تعریف شود؛ • برنامه‌های نیل به اهداف امنیت اطلاعات طرح‌ریزی شود؛ • فرآیند پایش، هدایت و بازنگری اهداف امنیت اطلاعات تدوین گردد.
گستره و پوشش فعالیت	• تدوین اهداف و برنامه‌های نیل به اهداف • تدوین فرآیند پایش، هدایت و بازنگری اهداف
خروجی	مستند اهداف امنیت اطلاعات و برنامه‌های نیل به اهداف و فرآیند پایش، هدایت و بازنگری اهداف امنیت اطلاعات
سطح کیفی مورد انتظار	• اهداف امنیت اطلاعات باید همراستا و همسو با اهداف و برنامه‌های استراتژیک سازمان و زمینه (بافتار) و انتظارات ذینفعان باشد؛ • ارتباط اهداف با مخاطرات امنیت اطلاعات مشخص شود؛ • اهداف امنیت باید توسط یک یا چند شاخص کلیدی عملکرد (KPI) پشتیبانی شود. هر یک از شاخص‌ها باید حداقل شامل موارد زیر باشد: ○ عنوان شاخص ○ معیار و مطلوبیت ○ روش اندازه‌گیری ○ مسئول اندازه‌گیری ○ دوره اندازه‌گیری **توضیح:** - تدوین اهداف و برنامه‌های نیل به اهداف به عهده شرکت مجری است. - پیشنهاد شاخص‌های کلیدی عملکرد به عهده شرکت مجری است. - اهداف امنیت اطلاعات باید با توجه به بافتار، اهداف و برنامه‌های استراتژیک کارفرما و انتظارات ذی‌نفعان خصوصی‌سازی شود.
مسئولیت‌های به عهده کارفرما	• تصویب و ابلاغ اهداف امنیت اطلاعات • تصویب برنامه‌ها و اجرای برنامه‌های مصوب • تصویب فرآیند پایش، هدایت و بازنگری اهداف امنیت اطلاعات و اجرای آن
۱۳– تدوین سیاست‌ها، روش‌های اجرایی، دستورالعمل‌ها و طرح‌ها	

توضیحات فعالیت‌ها	• سیاست‌ها (خط‌مشی‌ها)ی امنیتی بر اساس مشخصات و الزامات سازمان، اهداف امنیت اطلاعات و نتایج مدیریت مخاطرات تدوین شود؛ • روش‌های اجرایی و دستورالعمل‌ها بر اساس روال‌های موجود عملیاتی سازمان، الزامات ناشی از سیاست‌های امنیتی، اهداف امنیت اطلاعات و نتایج مدیریت مخاطرات تدوین شود؛ • روش‌های اجرایی الزامی قید شده در استاندارد ISO/IEC27001 با توجه به مشخصات سازمان و روال‌های موجود بازنگری یا تدوین شود؛ • برای کلیه سیاست‌هایی که اجرایی‌سازی آنها منوط به تامین زیرساخت‌های نرم افزاری یا سخت افزاری است طرح متناسب تدوین شود.
گستره و پوشش فعالیت	• تعداد و تفکیک سیاست‌ها، فرآیندها و روال‌ها بسته به ابعاد سازمان، پیچیدگی فرآیندهای داخلی، سطح حساسیت امنیتی کسب‌وکار، مخاطرات شناسایی شده و میزان بلوغ امنیتی سازمان باید توسط مجری تصمیم‌گیری و با کارفرما توافق گردد و بر اساس آن مستندات مربوط به سیاست‌ها، فرآیندها و روال‌ها تدوین شود. • نگارش متن سیاست‌ها، روال‌ها و فرآیندهای امنیتی و همچنین طراحی فرم‌ها، راهنماها و مستندات تکمیلی مورد نیاز برای بهره‌برداری از روال‌ها و فرآیندها به عهده مجری و با همکاری (و آموزش کامل) کارفرما است. • کلیه مستندات باید در قالب مورد استفاده سازمان برای مدیریت اطلاعات مستند شده (مستندات و سوابق) تهیه و به کارفرما ارائه گردد. • در صورت وجود سیستم‌های مدیریتی دیگر، روال‌های الزامی و مشترک ISMS با آن‌ها تلفیق و در غیر این صورت مستقلاً تدوین خواهد شد. • در مورد طرح‌ها، پیشنهاد عنوان طرح و نیازمندی‌های ریسک توسط مجری تدوین گردد.
خروجی	مستندات سیاست‌ها، روش‌های اجرایی، دستورالعمل‌ها و طرح‌ها
سطح کیفی مورد انتظار	• کلیه سیاست‌ها، روش‌های اجرایی و دستورالعمل‌ها باید علاوه بر پوشش الزامات امنیتی، با شرایط و اختصاصات سازمانی منطبق باشد. • ارتباط سیاست‌های امنیتی با اهداف، نتایج مدیریت مخاطرات، کنترل‌های استاندارد و الزامات بالادستی، همچنین ارتباط روش‌های اجرایی و دستورالعمل‌ها با سیاست‌های امنیتی می‌بایست مشخص شود. • روش‌های اجرایی و دستورالعمل‌ها باید به صورت یکپارچه با روش‌های اجرایی و دستورالعمل‌ها و فعالیت‌های موجود و عملیاتی سازمان طراحی و تدوین شود. • نقش‌هاو مسئولیت‌های اجرای روش‌های اجرایی و دستورالعمل‌ها باید مشخص ومدون گردد. • جهت اطمینان از اجرای صحیح و کنترل‌شده روش‌های اجرایی و دستورالعمل‌ها لازم است ساختار اطلاعات (در قالب فرم و چک‌لیست)، راهنماهای اجرایی و مستندات مرجع مورد نیاز به میزان کافی تهیه شود. • پیشنهاد عنوان طرح و نیازمندی‌های ریسک و تهیه برنامه زمانی اجرای طرح **توضیح:** - تمامی سیاست‌ها، طرح‌ها، روش‌های اجرایی و دستورالعمل‌ها و به تبع آن‌ها طراحی فرم‌ها، راهنماها و مستندات تکمیلی می‌بایست توسط مجری و با همکاری کارفرما برای سازمان خصوصی‌سازی شود. در صورتی که قبلاً در سازمان فرم، مستند و یا راهنمایی تدوین شده و یا روالی برای تدوین آن‌ها وجود دارد؛ مجری موظف است

	حتی‌الامکان از روال‌های موجود برای مستندسازی، طراحی فرم‌ها و راهنماها در سازمان/شرکت کارفرما تبعیت کند. - آموزش‌های لازم در خصوص استفاده و به‌روزرسانی مستندات، فرم‌ها و راهنماها از طرف مجری به کارفرما داده شود. - در خصوص دستگاه‌های زیرساختی (حیاتی، حساس و مهم) در تدوین سیاست‌ها، روش‌های اجرایی، دستورالعمل‌ها و طرح‌ها الزامات مرکز مدیریت راهبردی افتا نیز که در قالب "طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات الکترونیکی" به آن‌ها ابلاغ شده است، باید مدنظر قرار گیرد. - هر نوع سیاست، طرح، روش اجرایی و دستورالعمل حتما باید توسط کارفرما بررسی و تایید شود. مجری موظف است تا زمانی که موارد مذکور به تایید کارفرما برسد نسبت به بازنگری و بازبینی آن‌ها اقدام کند.
مسئولیت‌های به عهده کارفرما	• قراردادن اطلاعات مورد نیاز از وضعیت فعلی روش‌های اجرایی و دستورالعمل‌ها در اختیار شرکت مجری • بررسی و تصویب سیاست‌ها، روش‌های اجرایی، دستورالعمل‌ها و طرح‌های تهیه شده توسط مجری و ابلاغ آن‌ها • تهیه برنامه زمانی اجرای طرح
۱۴– تعیین ارتباطات مورد نیاز سیستم مدیریت امنیت اطلاعات	
توضیحات فعالیت‌ها	تمامی ارتباطات مورد نیاز برای عملکرد مؤثر سیستم مدیریت امنیت اطلاعات باید شناسایی و مدون گردد.
گستره و پوشش فعالیت	برای تمامی ارتباطات مدون شده باید فرآیند مربوطه، فرد مسئول برقراری ارتباط، طرف دریافت‌کننده ارتباط، زمان و چکانه (trigger) برقراری ارتباط، کانال و نحوه ارتباط، محتوا و ضوابط ارتباط مشخص شود.
خروجی	• فهرست یا جدول ارتباطات سیستم مدیریت امنیت اطلاعات • فرایندهای ارتباطی مدون شده (با ذکر جزئیاتی نظیر کانال ارتباطی، فرد مسئول برقراری ارتباط، طرف دریافت‌کننده ارتباط، زمان و چکانه (trigger) برقراری ارتباط، کانال و نحوه ارتباط، محتوا و ضوابط) *توضیح: در قالب یک سند مستقل یا به صورت توزیع شده در روال‌ها و فرآیندهای مربوطه
سطح کیفی مورد انتظار	• در شناسایی ارتباطات باید حداقل موارد زیر لحاظ گردد: ○ خواسته‌ها و انتظارات ذینفعان ○ برنامه‌ها و نتایج مدیریت مخاطرات ○ اهداف امنیت اطلاعات و نتایج نیل به اهداف ○ رخدادها و بحران‌های امنیت اطلاعات ○ وظایف، نقش‌ها و مسئولیت‌ها ○ اطلاعات مورد نیاز برای تبادل جهت اثربخشی فرآیندهای ISMS ○ تغییرات در ISMS و فرآیندها یا کنترل‌های امنیتی ○ موارد مورد نیاز ناشی از کنترل‌ها، فرآیندها یا روال‌های امنیت اطلاعات **توضیح:** - در خصوص دستگاه‌های زیرساختی، مرکز مدیریت راهبردی افتا به عنوان نهاد هماهنگ کننده و متولی امنیت مدنظر قرار گرفته و روالی برای ارتباط دائمی و مستمر با این مرکز در سازمان/شرکت کارفرما ایجاد شود.

	همچنین نقش این مرکز به عنوان مرکز عملیات امنیت (SOC) ملی و تیم امداد رایانه‌ای ملی مد نظر قرار گیرد. - در خصوص دستگاه‌های زیرساختی الزامات مرکز افتا (طرح امن سازی مرکز افتا) در قالب انتظارات ذی‌نفعان لحاظ شود.
مسئولیت‌های به عهده کارفرما	بررسی، تصویب و اجرای ارتباطات مورد نیاز
۱۵– مشاوره و نظارت بر طرح مقابله با مخاطرات و کنترل‌های مقابله با مخاطرات	
توضیحات فعالیت‌ها	• نظارت بر اقدامات و پروژه‌های تعریف شده در سازمان/شرکت کارفرما در فرایند مدیریت مخاطرات و بررسی انطباق با نتایج مورد انتظار • بررسی اثربخشی اقدامات و پروژه‌های تعریف شده در سازمان/شرکت کارفرما در کاهش سطح مخاطرات امنیت اطلاعات
گستره و پوشش فعالیت	• کلیه اقدامات و طرح‌هایی که مطابق برنامه مقابله با مخاطرات در طی چرخه اول سیستم مدیریت امنیت اطلاعات قرار می‌گیرند باید از منظر اثربخشی در کاهش سطح مخاطره توسط مجری تحت نظارت قرار گیرند. • نظارت عملیاتی یا فنی بر اجرای برنامه و پروژه‌ها و بر عهده مجری قرار ندارد.
خروجی	• گزارش وضعیت اثربخشی کنترل‌های مقابله با مخاطرات اجرا شده
سطح کیفی مورد انتظار	• در صورتی که کنترل‌های پیشنهادی نتوانسته‌اند سطح مخاطره را به اندازه پیش‌بینی شده کاهش دهند مجری موظف است راه‌کارهای کنترلی جدید را با همکاری خود کارفرما به آن‌ها پیشنهاد دهد. **توضیح:** - در خصوص دستگاه‌های زیرساختی، مرکز مدیریت راهبردی افتا به عنوان ناظر پروژه‌های امنیتی بوده و طرح‌ها و پروژه‌های امنیتی که در راستای کاهش مخاطرات امنیت اطلاعات تعریف می‌شود باید با نظارت و تایید مرکز افتا تعریف و اجرایی شود. همچنین کارفرما برای اجرای طرح‌ها و پروژه‌های تایید شده باید از شرکت‌های دارای گواهینامه از مرکز افتا استفاده کند. - در خصوص دستگاه‌های غیرزیرساختی، کارفرما برای اجرای طرح‌ها و پروژه‌های امنیتی –که برای کاهش سطح مخاطرات امنیت اطلاعات تعریف کرده است صرفاً می‌تواند از شرکت‌های دارای گواهینامه "مرتبط" با پروژه تعریف شده از مرکز مدیریت راهبردی افتا استفاده نماید.
مسئولیت‌های به عهده کارفرما	• اجرای برنامه مقابله با مخاطرات و کنترل‌های مرتبط با آن • ارائه نتایج حاصل از اقدامات و پروژه‌ها به مجری برای انعکاس در فرایند مدیریت مخاطرات و ارزیابی اثربخشی کنترل‌ها • اعمال اصلاحات و نظرات مجری در اقدامات و پروژه‌های مقابله با مخاطرات
۱۶– مدیریت عملیات ISMS و همکاری در پیاده‌سازی روال‌ها و فرآیندها	
توضیحات فعالیت‌ها	• متولیان اجرای روش‌های اجرایی و دستورالعمل‌ها در مورد روش اجرا و الزامات سیاست‌های تدوین شده و کنترل‌های امنیتی توجیه شوند. • همراهی و راهنمایی لازم برای تولید سوابق اجرای روش‌های اجرایی و دستورالعمل‌ها صورت گیرد. • بازخوردهای ذینفعان در مورد سیاست‌ها، روش‌های اجرایی و دستورالعمل‌ها و نتایج اجرای آن‌ها اخذ و در صورت لزوم اصلاحات و تنظیمات در روش‌های اجرایی و دستورالعمل‌ها شناسایی و اعمال گردد.

گستره و پوشش فعالیت	• توجیه متولیان اجرا در جلسه/جلسات مورد نیاز توسط مجری انجام گیرد؛ • مجری موظف است بر اساس بررسی‌ها و بازخوردهای کارفرما نسبت به بازنگری و بهبود روش‌های اجرایی اقدام کند و در خصوص دستورالعمل‌ها پیشنهاداتی برای بهبود به کارفرما ارائه دهد. • شرکت مجری تنها راهنمایی و رفع اشکال را انجام داده و در زمینه اجرای روش‌های اجرایی و دستورالعمل‌ها و تولید سوابق مسئولیت عملیاتی ندارد.
خروجی	• سوابق اجرای روش‌های اجرایی و دستورالعمل‌ها • اصلاحات در روش‌های اجرایی و دستورالعمل‌ها • پیشنهاد اصلاح سیاست‌ها و کنترل‌ها جهت طرح در بازنگری مدیریت
سطح کیفی مورد انتظار	• تمام روش‌های اجرایی و دستورالعمل‌های تدوین شده باید در زمان ممیزی داخلی حداقل دوماه و یا در مورد روال‌های غیر مستمر یک دوره سوابق اجرایی داشته باشند. • تسلط کافی برای اجرای روش‌های اجرایی و دستورالعمل‌ها توسط متولیان مربوطه بدون کمک مجری حاصل شده باشد. • اصلاحات مورد نیاز در مورد جزئیات و مراحل اجرای روش‌های اجرایی و دستورالعمل‌ها، قالب ثبت سوابق و نتایج، راهنمایی‌ها و توضیحات مورد نیاز باید اعمال شود. • اصلاحاتی که نیازمند تعریف طرح یا نیازمند تغییر در سیاست‌های امنیتی است شناسایی و مدون گردد.(مجری با هماهنگی و همکاری کارفرما)
مسئولیت‌های به عهده کارفرما	• توزیع نسخ دستورالعمل‌ها و روش‌های اجرایی به مسئولین مربوطه • ابلاغ الزام اجرای سیاست‌ها، روش‌های اجرایی و دستورالعمل‌ها به متولیان مربوطه • پیگیری و نظارت مدیریتی بر اجرای روش‌های اجرایی و دستورالعمل‌ها و تولید سوابق
۱۷– تدوین سازوکارهای سنجش اثربخشی	
توضیحات فعالیت‌ها	• مواردی که باید تحت پایش و سنجش قرارداشته باشند شناسایی و تعیین شوند؛ این موارد حداقل شامل موارد زیر است: ○ اهداف امنیت اطلاعات ○ کنترل‌های امنیت اطلاعات ○ فرآیندهای امنیتی، روش‌های اجرایی و دستورالعمل‌ها • سازوکار پایش، سنجش، تحلیل و ارزیابی و فرآیندهای مربوطه تدوین شود.
گستره و پوشش فعالیت	• سنجه‌های مورد نیاز باید حداقل شامل موارد زیر تعریف گردند: ○ عنوان سنجه ○ معیار و مطلوبیت ○ روش اندازه‌گیری ○ مسئول اندازه‌گیری ○ دوره اندازه‌گیری ○ دوره تحلیل و گزارش‌دهی

	• در صورت نیاز به ابزار برای بدست آوردن و نگهداری اطلاعات سنجه‌ها، سطح ورود مجری در حد تعیین نیازمندی‌های عملکردی می‌باشد.
خروجی	• فرآیند پایش و اندازه‌گیری سنجه‌ها و تحلیل و ارزیابی نتایج • فهرست سنجه‌های مورد نیاز برای تعیین وضعیت سیستم مدیریت امنیت اطلاعات
سطح کیفی مورد انتظار	• سنجه‌ها باید بنا به نیاز شامل سنجه‌های عملکردی و سنجه‌های اثربخشی باشد. • در صورت تشخیص نیاز و وجود تعداد زیاد سنجه‌ها، لازم است سنجه‌های کلیدی با ترکیب سنجه‌های جزئی‌تر تشکیل گردد. • استخراج و پیشنهاد سنجه‌ها به عهده مجری با همکاری کارفرما می باشد.
مسئولیت‌های به عهده کارفرما	نهایی‌سازی و ابلاغ فرآیند سنجش اثر بخشی
۱۸– سنجش شاخص‌ها و اجرای روال‌های پایش	
توضیحات فعالیت‌ها	• اطلاعات شاخص‌های سنجش اثربخشی گردآوری و شاخص‌های تعریف شده اندازه‌گیری شود؛ • وضعیت شاخص‌ها تحلیل شود و پیشنهادات اصلاحی تهیه شود.
گستره و پوشش فعالیت	• تحلیل داده‌های شاخص‌های امنیت اطلاعات در چرخه اول استقرار سیستم بر عهده شرکت مجری قرار دارد. • مجری موظف است آموزش‌های لازم در خصوص تحلیل شاخص‌ها را به کارفرما ارائه دهد.
خروجی	نتیجه اندازه‌گیری شاخص‌ها و پیشنهادات اصلاحی در موارد لزوم
سطح کیفی مورد انتظار	• تحلیل شاخص‌ها شامل بررسی وضعیت، در صورت لزوم استفاده از اطلاعات جانبی یا تخمین‌ها برای تحلیل دقیق‌تر و شناسایی علت انحراف از هدف • نتایج تحلیل شاخص‌ها باید در فرایند مدیریت مخاطره و تدوین راهکارهای مقابله با مخاطره (RTP) قابل ردگیری باشد.
مسئولیت‌های به عهده کارفرما	گردآوری اطلاعات مورد نیاز برای اندازه‌گیری شاخص‌ها
۱۹– ممیزی داخلی	
توضیحات فعالیت‌ها	• ممیزی داخلی سیستم مدیریت امنیت اطلاعات مستقر شده انجام شود.
گستره و پوشش فعالیت	کلیه الزامات عمومی و تمامی کنترل‌های امنیتی انتخاب شده و پیاده‌سازی شده ممیزی شود. **توضیح:** در صورتی که سازمان/شرکت کارفرما جزء دستگاه‌های زیرساختی باشد الزامات مرکز مدیریت راهبردی افتا نیز بررسی شود.
خروجی	برنامه و گزارش ممیزی داخلی سیستم مدیریت امنیت اطلاعات
سطح کیفی مورد انتظار	• فرآیند ممیزی داخلی مطابق الزامات ISO 19011 انجام شده و اطلاعات فرآیند به صورت کامل مستند شود. **توضیح:** در صورتی که شرکت مجری خود اقدام به انجام ممیزی داخلی می‌کند، تیم ممیزی باید کاملاً مستقل از تیم پیاده ساز باشد.
مسئولیت‌های به عهده کارفرما	تأیید برنامه ممیزی و هماهنگی‌های لازم برای ممیزی
۲۰– شناسایی بهبودها	

توضیحات فعالیت‌ها	بهبودهای سیستم مدیریت امنیت اطلاعات شناسایی شود.
گستره و پوشش فعالیت	موارد ناشی از همراهی در پیاده‌سازی، پایش سنجه‌ها، ممیزی داخلی تحلیل شده و بهبودهای ممکن شناسایی شود.
خروجی	فهرست پیشنهادی بهبودهای ISMS جهت بررسی در بازنگری مدیریت
سطح کیفی مورد انتظار	• بهبودها حداقل شامل بررسی موارد زیر باشد: ○ استفاده از فناوری‌های جدید ○ تغییر در سیاست‌ها و رویکردهای امنیتی ○ تغییر در برنامه مقابله با مخاطرات ○ تغییر در فرآیندها ○ اختصاص منابع ○ افزایش توانمندی افراد مؤثر در سیستم
مسئولیت‌های به عهده کارفرما	مشارکت در تحلیل یافته‌ها و شناسایی بهبودها
۲۱- بازنگری مدیریت	
توضیحات فعالیت‌ها	بازنگری مدیریت ISMS باید در زمان‌های مشخص انجام شود.
گستره و پوشش فعالیت	• ورودی‌های بازنگری مدیریت شامل موارد زیر تهیه شود: ○ تغییرات در بافتار درونی و بیرونی ○ نتایج فرآیندهای پایش شامل ممیزی داخلی، سنجش اثربخشی و اهداف امنیت اطلاعات ○ بازخوردهای ذینفعان ○ نتایج ارزیابی مخاطرات و وضعیت اقدامات مقابله با مخاطرات ○ بهبودهای شناسایی شده • پیشنهاد برنامه میان‌مدت توسعه و بهبود ISMS (شامل گسترش دامنه استقرار سیستم)
خروجی	• تغییرات در اهداف و سیاست‌های امنیت اطلاعات • تغییر در معیارهای پذیرش و ارزیابی مخاطرات • اقدامات اصلاحی و بهبودها • تغییر در منابع و بودجه ISMS
سطح کیفی مورد انتظار	اطلاعات ورودی جلسه، مباحث و تصمیمات در قالب مناسب مستندسازی و نگهداری شود.
مسئولیت‌های به عهده کارفرما	• هماهنگی برگزاری جلسه بازنگری مدیریت • اتخاذ تصمیمات لازم
۲۲- آماده‌سازی برای ممیزی شخص ثالث	
توضیحات فعالیت‌ها	• پیگیری برنامه‌های اقدامات اصلاحی • پیگیری مصوبات بازنگری مدیریت • اطمینان از تولید سوابق مورد نیاز سیستم به شکل مناسب و کافی

گستره و پوشش فعالیت	• نظارت بر برنامه و طرح‌های اقدامات اصلاحی تعریف شده، برنامه‌های رفع عدم انطباق‌ها و تصمیمات بازنگری مدیریت به عهده مجری قرار دارد. • بررسی مجدد کفایت سوابق با درنظر گرفتن نتایج ممیزی داخلی به عهده مجری می‌باشد.
خروجی	• نتایج اقدامات اصلاحی ناشی از عدم انطباق‌ها و تصمیمات جلسه بازنگری مدیریت که زمان‌بندی آن در چرخه اول سیستم قراردارد. • وجود سوابق کافی از عملکرد سیستم
سطح کیفی مورد انتظار	• اقداماتی که برنامه زمانی بستن آن‌ها در چرخه اول سیستم قرار می‌گیرد باید انجام گرفته و اثربخشی آن سنجیده شود. • دوره وجود سوابق سیستم مطابق الزامات نهاد ممیزی‌کننده و مرکز افتا کفایت لازم را داشته باشد.(در زمان ممیزی شخص ثالث می بایست حداقل سوابق یک دوره ۴ ماهه از سوابق سامانه مدیریت امنیت اطلاعات در دسترس باشد) **توضیح:** در زمان ممیزی شخص ثالث، مخاطب تیم ممیزی کارفرما خواهد بود و مجری نباید در فرایند ممیزی دخالت کند؛ بنابراین تمامی دانش سامانه مدیریت امنیت اطلاعات باید از طرف مجری به کارفرما انتقال یابد.
مسئولیت‌های به عهده کارفرما	• اجرای اقدامات اصلاحی • پیگیری و اجرای مصوبات بازنگری مدیریت • تولید سوابق سیستم
۲۳- آموزش و آگاهی‌رسانی	
توضیحات فعالیت‌ها	• آموزش‌های مربوط به نحوه راهبری سیستم پیاده‌سازی شده در سازمان و آگاهی‌رسانی به افراد مؤثر بر سیستم انجام شود. • عناوین دوره‌های آموزشی عمومی و تخصصی ISMS و دوره‌های فنی مورد نیاز استخراج و برای اجرای آن برنامه‌ریزی شود.
گستره و پوشش فعالیت	• حداقل ۳ سمینار آگاهی‌بخشی نیم‌روزه برای پرسنل سازمان باید توسط مجری برگزار شود. • مجری موظف است جلسات توجیهی را برای آموزش نحوه اجرای فرآیندها و روش‌های اجرایی سامانه مدیریت امنیت اطلاعات به همراه جزئیات مربوط به آن‌ها به مدت کافی برای کارفرما برگزار کند. • مجری باید عناوین دوره‌های آموزشی عمومی و تخصصی مرتبط با سامانه مدیریت امنیت اطلاعات را به کارفرما ارائه دهد. • برگزاری دوره‌های آموزشی امنیت صرفاً می‌تواند توسط شرکت‌هایی انجام شود که دارای گواهی فعالیت در حوزه خدمات آموزشی (نما) باشند. • برگزاری دوره های آموزشی تخصصی نمی تواند در قالب پروژه ISMS باشد و تنها برگزاری دوره‌های آگاه‌سازی امنیتی می تواند ارائه شود.
خروجی	• فهرست دوره‌های برنامه‌ریزی شده آموزشی و سوابق اجرای آن • آموزش نحوه راهبری سیستم و اجرای فرآیندها و روال‌ها • برگزاری سمینارهای آگاهی‌بخشی

سطح کیفی مورد انتظار	• برنامه‌ریزی آموزش‌های عمومی ISMS مورد نیاز کارفرما در ابتدای پروژه استقرار صورت گیرد و آموزش‌های تکمیلی و تخصصی مرتبط با سیستم مدیریت امنیت اطلاعات بر اساس نتایج ارزیابی مخاطرات برنامه‌ریزی گردد.
مسئولیت‌های به عهده کارفرما	• پیگیری اجرای دوره‌های آموزشی پیشنهاد شده توسط شرکت مجری و عقد قراردادهای لازم یا طی روال تأمین به فراخور نیاز • تامین محل اجرا و تسهیلات لازم برای برگزاری دوره آموزشی/توجیهی

۶ الزامات کارفرما در اجرای پروژه

هر گونه قوانین داخلی و الزامات داخلی کارفرما که شـرکت مجری ملزم به رعایت آن‌ها در طول قرارداد اسـت، باید به طور دقیق مشخص شده و توسط کارفرما اطلاع رسانی گردد.