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 حملات 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