مدل پیشنهادی سنجش سطح بلوغ کنترل‌های امنیتی سازمان

مصطفی تمتاجی
حسین یادگاری

تاریخ دریافت: ۹۴/۰۶/۲۳
تاریخ پذیرش: ۹۴/۰۹/۲۴

چکیده:

پیاده‌سازی کامل کنترل‌های امنیتی یکی از گام‌های اصلی در برقراری امنیت در سازمان است. این کار مستلزم صرف منابع بسیاری است که در اغلب موارد در کوتاه‌مدت امکان‌پذیر نیست. از طرفی مدیران سازمان تمایل دارند تا ضمن آگاهی از وضعیت امنیتی سازمان خود در تمام ابعاد و نقاط قوت و ضعف سازمان، از اثربخشی منابع تخصیص یافته برای پیاده‌سازی کنترل‌های امنیتی و میزان تأثیر آن در ارتقای سطح امنیتی و همچنین اولویت‌های بعدی تخصیص منابع مطلع شوند.

این مقاله، پس از بیان ضرورت، هدف، سؤالات و ادبیات تحقیق، رویکرد و نگرش فازی به‌منظور سنجش میزان و سطح پیاده‌سازی کنترل‌های امنیتی بیان کرده و براساس آن مدلی برای سنجش سطح بلوغ کنترل‌های امنیتی سازمان ارائه می‌کند.

قابلیت به‌کارگیری در تمامی سازمان‌ها صرف‌نظر از نوع، اندازه و ماهیت آن، سازگاری با استانداردهای بین‌المللی متداول و مرتبط در این حوزه، ارائه‌ی داشبورد مدیریتی امنیتی برای مدیران ارشد، قابلیت به‌کارگیری به‌عنوان سیستم تصمیم‌یار مدیران، ارائه‌ی وضعیت شفاف و دقیق وضعیت سازمان در همه ابعاد امنیتی و تعیین نقاط قوت و ضعف امنیتی سازمان از مشخصه‌ها و کاربردهای مدل پیشنهادی است.

واژگان کلیدی:
کنترل امنیتی، مدل بلوغ، سنجش سطح بلوغ

۱. مقدمه

امنیت، مطلوب همگان است و رسیدن به امنیت کامل، آرزویی دست نیافتنی است. استانداردهای متعددی تلاش کرده‌اند که راهکارهایی برای برقراری امنیت در سازمان ارائه دهند. برآورده‌سازی الزامات مندرج در استانداردها، نیازمند طرح‌ریزی دقیق و صرف منابع سازمانی فراوان است.

از سوی دیگر ایجاد امنیت در یک سطح در همان لحظه، تضمینی برای وجود امنیت در همان سطح برای ساعتی دیگر نیست. امنیت این مشخصه را از ماهیت پویای تهدیدات امنیتی عاریه گرفته است.

هر چند اساس و مبنای برقراری امنیت در یک سازمان ایجاد نظام مدیریت امنیت و به تبع آن مدیریت مخاطرات سازمان (شامل شناسایی تهدیدات امنیتی و آسیب‌پذیری‌های دارایی‌های اطلاعاتی سازمان و محاسبه‌ی سطح مخاطره و اولویت‌بندی آن و تهیه طرح مقابله با مخاطرات و پایش اثربخشی آن) است، لیکن این موضوع در این تحقیق مورد توجه قرار نگرفته است.

این تحقیق به نقطه‌ای از ایجاد امنیت می‌پردازد که کنترل‌های امنیتی که باید در سازمان پیاده‌سازی شوند، تعیین‌شده و تیم اجرایی در قالب یک پروژه، کنترل امنیتی را استقرار داده است. تمرکز تحقیق حاضر در پاسخ به این سؤال است: آیا استقرار یک کنترل امنیتی با منطق دودویی قابل ارزیابی است یا با منطق فازی؟

به‌عنوان مثال آیا ترددها به نواحی امن سازمان تحت کنترل است؟ منطق دودویی به این سؤال پاسخ آری یا خیر می‌دهد. اگر پاسخ آری باشد، یعنی تردد تحت کنترل است و هیچ فرد غیرمجازی قادر به تردد به نواحی امن سازمان را ندارد. تأکید این جمله بر هیچ است. در سازمان‌های متعددی به این سؤال پاسخ آری داده می‌شود ولی همان سازمان حضور افراد غیرمجاز را تجربه کرده است. از سویی دیگر اگر پاسخ خیر باشد، یعنی تردد تحت کنترل نیست، درحالی‌که

تـردد بـه هـر سـازمانی بـه نوعـی تحـت کنتـرل اسـت و خیـر مطلـق وجـود نـدارد.

یکـی از راهکارهـای حـل ایـن تناقـض، نگـرش فـازی بـه اسـتقرار کنترل‌هـای امنیتـی اسـت. اگـر گفتـه شـود سـازمان تـا سـطح مطلوبـی تـردد را تحـت کنتـرل دارد، در واقـع بصـورت فـازی اسـتقرار کنتـرل بیـان شـده اسـت. سـطح مطلـوب بیانگـر نگـرش پیوسـته و طیفـی بـه اسـتقرار اسـت، طیفـی پیوسـته از آری (اسـتقرار کامـل) تـا خیر(اسـتقرار نیافتـه).

ایـن تحقیـق تـلاش کـرده اسـت تـا بـا نـگاه بـه الزامـات امنیتـی و مدل‌هـای بلـوغ موجـود، شـاخص‌های اثربخشـی و کارایـی اسـتقرار کنترل‌هـای امنیتـی را اسـتخراج کـرده و در قالـب مدلـی بـرای سـنجش سـطح بلـوغ امنیتـی سـازمان ارائـه نمایـد.

۲. ضرورت، سؤال و اهداف تحقیق

آنچـه ضـرورت ارائـه مـدل سـنجش بلـوغ امنیتـی سـازمان را دو چنـدان می‌کنـد، موانـع پیاده‌سـازی نظـام مدیریـت امنیـت اطلاعـات در سـازمان است. یکـی از ایـن موانـع عدم به‌کارگیـری چارچـوب اسـتقرار متناسـب بـا سـطح بلـوغ سـازمان اسـت. تجربـه نشـان داده اسـت کـه چارچوب‌هـای متـداول اسـتقرار سیسـتم مدیریـت امنیـت اطلاعـات در سـازمان‌های ایرانـی کارآمـد نبـوده و منجـر بـه برقـراری و تـداوم یـک سیسـتم مدیریـت امنیـت اطلاعـات پایـدار و قابـل اتـکا نمی‌شـوند [۱]. بـر ایـن اسـاس، وجـود یـک مـدل بـرای تعییـن سـطح بلـوغ، بـرای ترسـیم راهبـرد و نقشـه راه سـازمان ضـروری اسـت.

از طرفـی پایـش وضعیـت امنیتـی و ایجـاد یـک داشـبورد مدیریتـی یکـی از مطالبـات همیشـگی تصمیم‌گیـران سـازمان اسـت. تعریـف شـاخص‌های قابـل اندازه‌گیـری و قضـاوت و تعییـن مراحلـی کـه بایـد بـرای رسـیدن بـه نقطه مطلـوب بایـد طـی شـود، لازمـه ایجـاد چنیـن داشـبوردی اسـت کـه در یـک مـدل سـنجش بلـوغ امنیتـی می‌توانـد لحـاظ شـود.

سـؤال اساسـی در ایـن تحقیـق ایـن اسـت کـه چگونـه می‌تـوان سـطح بلـوغ امنیتـی سـازمان را تعییـن کـرد. از اهـداف تحقیـق حاضـر تعییـن شـاخص‌های بلـوغ سـازمان در پیاده‌سـازی کنترل‌هـای امنیتـی و ارائـه یـک مـدل سـاده و کاربـردی بـرای سـنجش بلـوغ امنیتـی سـازمان اسـت.

ایجـاد ارتبـاط بیـن مدل‌هـا و رویکردهـای ارزیابـی فراینـد بـا کنترل‌هـای امنیتـی و مناسب‌سـازی سـطح بلـوغ فراینـد بـرای سـنجش عمـق پیاده‌سـازی کنترل‌هـا از نوآوری‌هـای تحقیـق حاضـر محسـوب می‌شـود.

۳. ادبیات تحقیق

در ایـن بخـش، تلاش‌شـده اسـت تـا ادبیـات تحقیـق و مفاهیـم بـه‌کار رفتـه، در قالـب معرفـی چنـد مرجـع معتبـر در زمینـه مـورد مطالعـه تشـریح شـوند.

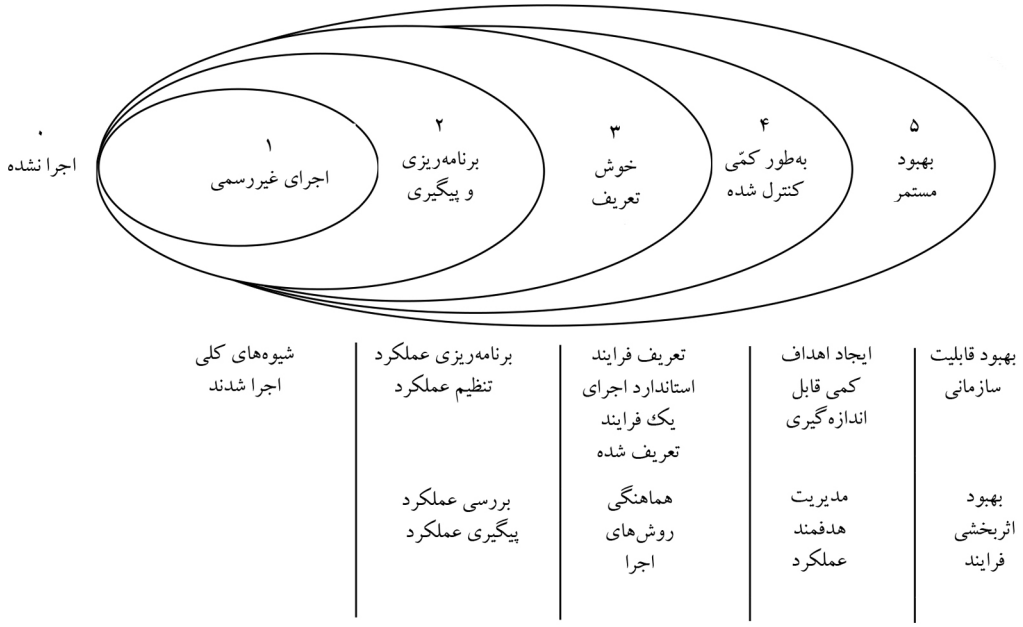
۳ـ۱) اسـتاندارد ISO/IEC 27001: 2013، نظـام مدیریـت امنیـت اطلاعـات را ارائـه داده کـه عـلاوه بـر الزامـات نظـام مدیریتـی مبتنـی بـر مدیریـت مخاطـرات، مجموعـه ۱۱۴ کنتـرل امنیتـی را در ۱۴ حـوزه کنترلـی مطرح‌کـرده اسـت. ایـن اسـتاندارد، یـک مرجـع پذیرفته‌شـده در سـطح جهانـی اسـت و پیش‌نیـاز بسـیاری از تعامـلات و معاهـدات تجـاری بیـن شـرکت‌های معتبـر لحـاظ می‌شـود. گرچـه محتـوای کنترل‌هـای امنیتـی در محـدوده و هـدف ایـن تحقیـق نیسـت، لیکـن بـه سـازمان‌ها توصیـه می‌شـود بـرای برقـراری و حفـظ امنیـت سـازمان خـود، از ایـن اسـتاندارد اسـتفاده کننـد [۲و۳]. بـرای پیاده‌سـازی اسـتاندارد مذکـور بایـد بـا توجـه بـه نتایـج مدیریـت مخاطـرات، مجموعـه کنترل‌هـای امنیتـی دارای کاربـرد در سـازمان را از پیوسـت (الـف) اسـتاندارد انتخاب‌کـرده و اسـتقرار داد. راهنمایی‌هـای پیاده‌سـازی هـر کنتـرل در اسـتاندارد ISO/IEC 27002: 2013 آمده است[۴].

۳ـ۲) اسـتاندارد ISO/IEC 21827 یـک مـدل بلـوغ قابلیـت ارائه‌کـرده اسـت. مـدل SSE-CMM[1] تلفیقـی از تجـارب برتـر مهندسـی امنیـت و مـدل مرجـع فراینـدی اسـت کـه بـر روی الزامـات پیاده‌سـازی امنیـت در یـک سـامانه یـا مجموعـه‌ای از سـامانه‌های بـه هـم مرتبـط کـه دامنـه‌ی امنیـت فنـاوری اطلاعـات هسـتند، تمرکـز دارد. SSE-CMM، مهندسـی امنیـت را در سـه حـوزه‌ی مخاطره، مهندسـی و تضمیـن تحلیـل می‌کنـد.

SSE-CMM دارای دو بعـد دامنـه و قابلیـت اسـت. ایـن بعـد شـامل تمامـی فنونـی اسـت کـه در مجمـوع مهندسـی امنیـت را تعریـف می‌کننـد. بعـد قابلیـت، نمایش‌دهنـده‌ی

1. Systems Security Engineering - Capability Maturity Model (SSE-CMM)

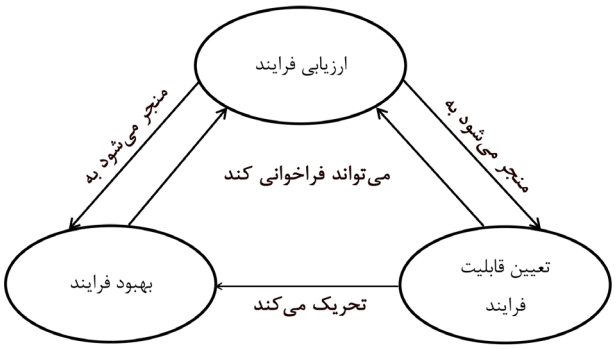
فنونی است که قابلیت مدیریت و نهادینگی فرایند را نشان می‌دهند. SSE-CMM شامل پنج سطح است که در شکل (۱) نشان داده‌شده است [۵].



شکل ۱: سطوح قابلیت

این استاندارد با ISO/IEC 15504 و به‌ویژه با ISO/IEC 15504-2 در ارتباط است زیرا هر دو بر بهبود فرایند و ارزیابی رشد قابلیت تمرکز دارند. ISO/IEC 15504 به‌طور خاص روی نرم‌افزار متمرکز است، درحالی‌که این سند بر روی امنیت تمرکز دارد.

۳ـ۳) مجموعه استاندارد خانواده ISO/IEC 15504 با موضوع ارزیابی فرایند، بیشتر بر فرایندهای توسعه نرم‌افزار تمرکز دارند. گرچه مدل و مفاهیم بیان‌شده در هر فرایندی قابل تعمیم است. در این استاندارد، هدف از ارزیابی فرایند، تعیین قابلیت فرایند و بهبود فرایند ذکرشده است. چرخه‌ی بیان‌شده در شکل (۲) هدف و دستاورد مورد انتظار از ارزیابی فرایند و نحوه‌ی اثرگذاری اجزا روی یکدیگر را نشان می‌دهد [۶].



شکل ۲: چرخه‌ی اثرگذاری ارزیابی فرایند

در تهیه‌ی این استاندارد، از استاندارد فرایند چرخه‌ی حیات نرم‌افزار (ISO/IEC 12207) و مدل‌های بلوغ مانند Boot-strap ، Trillium و مدل بلوغ قابلیت[1] استفاده‌شده است [۶].

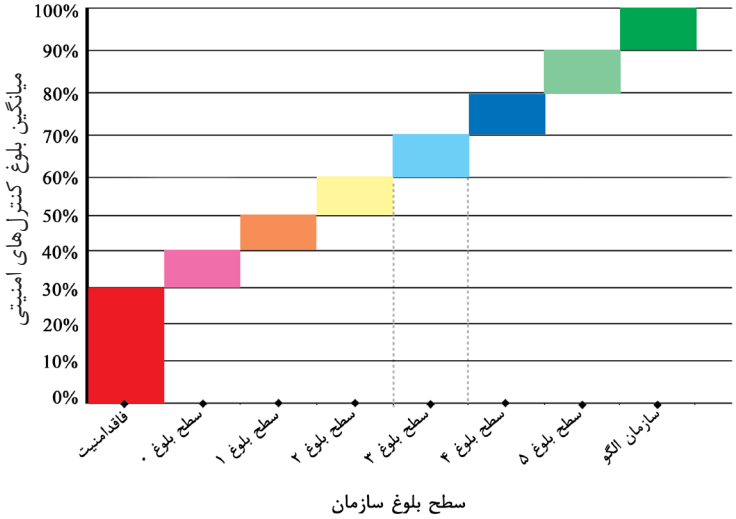
۴. مدل پیشنهادی

در ارائه مدل سنجش بلوغ امنیتی، فرض بر این است که سازمان مجموعه‌ای از کنترل‌های امنیتی را باید برای برقراری امنیت استقرار دهد. منطقی و معقول آن است که سازمان، کنترل‌های امنیتی مورد نیاز خود را از خروجی یک روش‌شناسی تکرارپذیر و قیاس‌پذیر مدیریت مخاطرات استخراج کرده باشد. با این همه مدل پیشنهادی مبتنی بر مجموعه کنترل‌های امنیتی مشخصی مثل آنچه در استاندارد ISO/IEC 27001:2013 آورده‌شده است، نیست.

۴ـ۱) کلیات مدل

به‌منظور ارزیابی سطح بلوغ کنترل‌های امنیتی از مفاهیم مدل بلوغ قابلیت و سطح بلوغ فرایند استفاده می‌شود. در مدل پیشنهادی برای هر کنترل شش سطح درنظر گرفته‌شده و امتیازی بین صفر تا پنج درنظرگرفته خواهد شد. میانگین امتیاز تمامی کنترل‌های امنیتی قابل کاربرد، سطح بلوغ امنیتی سازمان را تعیین می‌کند.

مدل پیشنهادی، هشت سطح بلوغ را برای یک سازمان درنظرگرفته که در جدول (۱) نشان داده‌شده است. سطح بلوغ امنیتی سازمان با میانگین سطح بلوغ کنترل‌های امنیتی تعیین می‌شود.



شکل ۳: مدل پیشنهادی

برای ارزیابی سطح بلوغ کنترل‌های امنیتی باید اثربخشی مشخصه‌های زیر را ارزیابی کرد. از آنجا که الگوی COBIT یک مدل فرایندی برای پاسخ‌گویی به نیازهای سازمانی در حوزه فناوری اطلاعات است و از طرفی عمده کنترل‌های امنیتی به‌طور مستقیم مربوط به فناوری اطلاعات بوده و یا ماهیتی مشابه آن دارند؛ لذا مشخصه‌های مورد ارزیابی از این مدل استخراج‌شده و تعریف هر یک در هر سطح بلوغ متناسب با موضوع امنیت مناسب‌سازی شده‌اند. مدل COBIT از نظر سطوح بلوغ تعریف‌شده، مشابهت فراوانی با مدل بلوغ امنیتی تشریح‌شده در ادبیات تحقیق دارد: [۷]

۱. خط‌مشی‌ها، برنامه‌ها و رویه‌ها،
۲. ابزارها و کنترل خودکار،
۳. مهارت‌ها و تخصص،
۴. مسئولیت و پاسخ‌گویی،
۵. تعیین اهداف و سنجش آن‌ها.

هر یک از مشخصه‌های فوق مطابق با تعاریف ذکر شده در ادامه مقاله مورد ارزیابی قرارگرفته و درنهایت کنترل مربوطه در یکی از پنج سطح قرار خواهد گرفت:

۴ـ۲) سطح صفر: عدم وجود یا ناقص

سازمان هیچ گونه برنامه‌ای برای پیاده‌سازی کنترل

1. Capability Maturity Model-CMM

مـورد نظـر نـدارد. در مـواردی کنتـرل به‌صـورت تجربـی توسـط برخـی کارکنـان انجـام می‌شـود. شـواهدی بـرای هیچ‌یـک از شـاخص‌های پنج‌گانـه‌ی مـورد نظـر وجـود نـدارد.

۴ـ۳) سـطح یـک: پیاده‌سـازی غیررسـمی (ابتدایـی، فاقـد عمومیـت)

در ایـن سـطح، نشـانه‌هایی مبنـی بـر توجـه بـه کنتـرل مـورد نظـر و نیـاز بـه آن در سـطح سـازمان مشـاهده می‌شـود. در ایـن سـطح، کنتـرل به‌صـورت اسـتاندارد اجـرا نمی‌شـود و رویکـرد مدیریتـی به‌هـم ریختـه و آشـفته اسـت. افـراد درون سـازمان تشـخیص می‌دهنـد کـه چـه اقدامـی بایـد انجـام شـود و یـک توافـق کلـی وجـود دارد کـه ایـن اقـدام در هنگامـی کـه مـورد نیـاز اسـت، انجـام شـود. کارایـی کنتـرل و اثربخشـی آن بسـتگی بـه دانـش و تلاش‌هـای فـردی دارد. واکنش‌هـا در برابـر نقـض امنیـت، غیرقابـل پیش‌بینـی اسـت.

الـف) خط‌مشـی‌ها، برنامه‌هـا و رویه‌هـا: تشـخیص نیـاز بـرای فراینـد در حـال ظهـور اسـت. رویکردهـای فاقـد عمومیـت بـرای کنتـرل، روش‌های تجربـی در پیاده‌سـازی و خط‌مشـی‌های تعریف‌نشـده قابـل مشـاهده اسـت.

ب) ابزارهـا و کنتـرل خـودکار: برخـی ابزارهـا موجـود هسـتند. هیـچ رویکـرد برنامه‌ریزی‌شده‌ای بـرای اسـتفاده از ابـزار وجـود نـدارد.

پ) مهارت‌هـا و تخصـص: مهارت‌هـای لازم بـرای اثربخش‌کـردن کنتـرل شناسـایی نشـده‌اند. برنامه‌هـای آموزشـی وجـود ندارد.

ت) مسـئولیت و پاسـخ‌گویی: تعریفـی از پاسـخ‌گویی و مسـئولیت وجـود نـدارد.

ث) تعییـن اهـداف و سـنجش آن‌هـا: اهداف شـفاف نیسـتند و اندازه‌گیـری و سـنجش انجـام نمی‌شـود.

۴ـ۴) سطح دو: تکرارپذیر ولی حسّی (انجام‌شده)

در ایـن سـطح، رویه‌هـا و فرایندهـای مشـابهی بـرای پیاده‌سـازی کنتـرل وجـود دارنـد کـه توسـط افـراد مختلـف دارای یـک وظیفـه اجـرا می‌شـود. در ایـن سـطح، هیـچ آمـوزش یـا رویه‌هـای اسـتانداردی وجـود نـدارد و مسـئولیت برعهـده‌ی خـود افـراد اسـت و اتـکای اصلـی بـه دانـش افـراد اسـت (بنابرایـن امـکان خطـا وجـود دارد). اطلاعـات و گزارش‌هـای امنیتـی تهیـه می‌شـوند؛ ولـی مـورد تحلیـل قـرار نمی‌گیرنـد.

الـف) خط‌مشـی‌ها، برنامه‌هـا و رویه‌هـا: آگاهـی از نیـاز بـرای پیاده‌سـازی کنتـرل وجـود دارد. فرایندهـای اجرایـی مشـابه و مشـترک ظهـور می‌کننـد. تعریـف شـفافی از رویه‌هـا و خـط مشـی‌ها وجـود نـدارد.

ب) ابزارهـا و کنتـرل خـودکار: رویکردهـای مشـترک بـرای اسـتفاده از ابـزار وجـود دارد (بـر مبنـای راهکارهـای ارائه‌شـده از سـوی افـراد کلیـدی) ابزارهـای مـورد نیـاز تهیـه می‌شـود، ولـی به‌درسـتی مـورد اسـتفاده قـرار نمی‌گیـرد.

پ) مهارت‌هـا و تخصـص: کمینـه نیازمندی‌هـای مهارتـی بـرای حوزه‌هـای کلیـدی شناسـایی می‌شـوند. آمـوزش بـر مبنـای نیـاز انجـام می‌شـود.

ت) مسـئولیت و پاسـخ‌گویی: افـراد، عهـده‌دار مسـئولیت می‌شـوند و به‌طورمعمـول پاسـخ‌گو هسـتند. هنـگام بـروز مشـکل، یـک نـوع آشـفتگی در رابطـه بـا مسـئولیت‌ها وجـود دارد.

ث) تعییـن اهـداف و سـنجش آن‌هـا: تـا حـدودی اهـداف و برخـی از شـاخص‌های مالـی تعییـن می‌شـوند، البتـه ایـن شـاخص‌ها فقـط بـرای مدیریـت، شناخته‌شـده هسـتند. نظـارت متناقـض در حوزه‌هـای تفکیک‌شـده مشـهود اسـت.

۴ـ۵) سطح سه: خوش تعریف (نهادینه‌شده)

رویه‌هـا، اسـتاندارد و از طریـق آمـوزش منتقل‌شـده اسـت. پیـروی از رویه‌هـا اجبـاری اسـت؛ امـا تخلفـات شناسـایی نمی‌شـود. رویه‌هـا خیلـی پیشـرفته نیسـتند؛ امـا روش‌هـای کاری موجـود را رسـمی می‌کننـد.

یـادآوری: یـک فراینـد خـوش تعریـف فراینـدی اسـت کـه همـراه بـا خط‌مشـی‌ها، اسـتانداردها، ورودی‌هـا، معیارهـا یـا معیـار ورود، اقدامـات، رویه‌هـا، نقش‌هـای مشخص‌شـده، ارزیابی‌هـا، اعتبارسـنجی، چارچوب‌هـا، خروجی‌هـا و معیارهـا یـا معیـار خـروج باشـد کـه مستندشـده و نامتناقـض و کامـل باشـد.

الـف) خط‌مشـی‌ها، برنامه‌هـا و رویه‌هـا: درک از نیـاز بـرای پیاده‌سـازی کنتـرل وجـود دارد. اسـتفاده از روش‌هـای عملـی مناسـب تحقـق می‌یابـد. فرایندهـا، خط‌مشـی‌ها

و رویه‌های لازم برای فعالیت‌های کلیدی، تعریف و مستند می‌شوند. استانداردهای هر حوزه‌ی کنترلی شناسایی‌شده‌اند و برنامه‌ی استقرار هر یک تهیه شده است.

ب) ابزارها و کنترل خودکار: برنامه‌ای برای استفاده و استانداردسازی ابزارها به‌منظور کنترل خودکار فرایند تعریف و ابزارها در راستای اهداف پایه‌ای آن‌ها مورد استفاده قرار می‌گیرند، ولی شاید استفاده از آن‌ها چندان مطابق با برنامه‌ی تعریف‌شده نباشد.

پ) مهارت‌ها و تخصص: نیازمندی‌های مهارتی برای تمامی حوزه‌ها تعریف و مستند می‌شوند. یک برنامه آموزشی رسمی تدوین می‌شود، ولی آموزش رسمی کماکان بر مبنای ابتکارات فردی است.

ت) مسئولیت و پاسخ‌گویی: مسئولیت و پاسخ‌گویی فرایند تعریف می‌شود و متصدیان فرایند شناسایی می‌شوند. متصدی فرایند از اختیار کامل برای انجام مسئولیت‌ها برخوردار نیست.

ث) تعیین اهداف و سنجش آن‌ها: تا حدودی اهداف و شاخص‌های اثربخش تعیین می‌شوند و یک ارتباط روشن با اهداف کسب و کاری وجود دارد. فرایندهای اندازه‌گیری ظهور می‌یابند؛ ولی به‌صورت با ثبات مورد استفاده قرار نمی‌گیرند. ایده‌های استفاده از کارت امتیازدهی متوازن مشاهده می‌شود.

۴ـ۶) سطح چهار: مدیریت‌شده، قابل سنجش و پیش‌بینی

مدیریت، تبعیت از رویه‌ها و سازگاری با آن‌ها را نظارت کرده و با اقدامات متناقض برخورد می‌کند. کنترل‌ها پی‌درپی بهبودیافته و نتایج خوبی ارائه می‌کنند. از خودکارسازی و ابزارها به‌صورت محدود یا جسته گریخته استفاده می‌شود.

الف) خط‌مشی‌ها، برنامه‌ها و رویه‌ها: درک کاملی نسبت به نیازمندی‌ها وجود دارد. فرایند، صحیح و کامل است؛ بهترین روش‌های عملی درونی مورد استفاده قرار می‌گیرد. تمامی ابعاد فرایند، مستند و قابل تکرار هستند. خط‌مشی‌ها از سوی مدیریت تصویب می‌شود. برای توسعه و تقویت فرایندها و رویه‌ها از استانداردها استفاده‌شده و بخش‌هایی از استانداردها پیاده‌سازی شده‌اند.

ب) ابزارها و کنترل خودکار: ابزارها بر مبنای یک برنامه استانداردشده پیاده‌سازی می‌شوند و تا حدودی با دیگر ابزارها یکپارچه می‌شوند. ابزارها در حوزه‌های اصلی برای مدیریت خودکار فرایند و نظارت بر فعالیت‌ها و ابزار کنترلی کلیدی مورد استفاده قرار می‌گیرند.

پ) مهارت‌ها و تخصص: نیازهای مهارتی برای تمامی حوزه‌ها به‌روز می‌شود. کارایی این مهارت‌ها برای تمامی حوزه‌های حیاتی تضمین می‌شود. از فنون آموزشی تکامل‌یافته بر مبنای یک برنامه آموزشی استفاده می‌شود و انگیزه به اشتراک‌گذاری دانش به‌وجود می‌آید. اثربخشی برنامه آموزشی ارزیابی می‌شود.

ت) مسئولیت و پاسخ‌گویی: مسئولیت و پاسخ‌گویی فرایند پذیرفته می‌شود و متصدی فرایند متعهد به انجام کامل تمامی مسئولیت‌های خویش است. فرهنگ پاداش‌دهی برای افزایش انگیزه‌ی کارکنان در قبال مسئولیت ایشان جاری می‌شود.

ث) تعیین اهداف و سنجش آن‌ها: کارایی و اثربخشی اندازگیری می‌شود و ارتباط آن با اهداف کسب وکاری مشخص می‌شود. کارت امتیازدهی متوازن در حوزه‌های مورد انتظار مدیریت پیاده‌سازی می‌شود و رویدادها و حوادث مورد تحلیل قرار می‌گیرند. بهبود مستمر قابل مشاهده است.

۴ـ۷) سطح پنج: بهینه‌شده (بهبود مستمر)

بر مبنای نتایج بهبودهای مستمر و الگوگیری از دیگر سازمان‌ها، اجرای کنترل‌ها به سطح عالی رسیده‌اند. بهبود مستمر، تجزیه و تحلیل اثربخشی کنترل و اصلاح مداوم نواقص به وضوح قابل مشاهده است. یکپارچگی در فعالیت‌ها و فرایندهای سازمان مورد توجه قرار گرفته است.

الف) خط‌مشی‌ها، برنامه‌ها و رویه‌ها: درک پیشرفته و رو به جلویی نسبت به نیازمندی‌ها وجود دارد. از بهترین روش‌های عملی و استانداردهای بیرونی استفاده می‌شود. مستندسازی فرایند در جهت جریان خودکارسازی تکامل می‌یابد. فرایندها، خط‌مشی‌ها و رویه‌ها برگرفته از استانداردهای موجود در حوزه‌ی

مـورد نظـر بـوده و اسـتانداردها به‌طـور کامـل اسـتقرار یافته‌انـد.

ب) ابزارهـا و کنتـرل خـودکار: مجموعـه ابـزار استانداردشـده توسـط سـازمان به‌خدمـت گرفتـه می‌شـود. تمامـی ابـزار مربـوط بـه پشـتیبانی از فرایندهـا بـا یکدیگـر یکپارچـه می‌شـوند. ابـزار بـرای پشـتیبانی از بهبـود فراینـد و کشـف خـودکار اسـتثناهای کنترلـی مـورد اسـتفاده قـرار می‌گیرنـد.

پ) مهارت‌هـا و تخصـص: سـازمان به‌صـورت رسـمی و بـر مبنـای اهـداف سـازمانی شـفاف و تعریف‌شـده، خواهـان بهبـود مسـتمر مهارت‌هاسـت. آمـوزش و پـرورش موجـب تقویـت بهتریـن روش‌هـای عملـی بیرونـی و مفاهیـم فنـون پیشـرفته می‌شـود. بـه اشـتراک‌گذاری دانـش به‌صـورت یـک فرهنـگ سـازمانی در می‌آیـد و از سیسـتم‌های دانـش بنیـان اسـتفاده می‌شـود.

ت) مسـئولیت و پاسـخ‌گویی: مالـکان فراینـد بـرای تصمیم‌گیـری و انجـام اقدامـات، صاحـب اختیـار می‌شـوند. پذیـرش مسـئولیت از سـطوح بـالا تـا سـطوح پایین‌تـر سـازمانی تحقـق می‌یابـد.

ث) تعییـن اهـداف و سـنجش آن‌هـا: یک سیسـتم سـنجش عملکـرد یکپارچـه و بـر مبنـای اسـتفاده سراسـری از کارت امتیازدهـی متـوازن یـا روش‌هـای دیگـر وجـود دارد. اسـتثناهای موجـود در سراسـر سـازمان مـورد توجـه مدیریـت قـرار می‌گیـرد و از روش‌هـای تحلیـل پیشـرفته بـرای بررسـی نتایـج اسـتفاده می‌شـود. بهبـود مسـتمر به‌عنـوان راهـکاری بـرای بقـا درنظرگرفتـه می‌شـود.

۴ـ۸) ارزیابی و اعتبارسنجی مدل پیشنهادی

گرچـه محدودیـت زمانـی تحقیـق، مانـع از ارائـه‌ی نتایـج پیاده‌سـازی مـدل و بهره‌گیـری از آن در تعییـن سـطح بلـوغ کنترل‌هـای امنیتـی چنـد سـازمان و مقایسـه بـا نتایـج سـایر روش‌هـای تعییـن سـطح بلـوغ شـده اسـت، لیکـن ایـن مـدل از سـه منظـر جامع‌بـودن، مانع‌بـودن و قابلیـت اسـتفاده در جلسـه خبرگـی مطرح‌شـده و توسـط کارشناسـان ایـن حـوزه به‌عنـوان مـدل قابـل قبـول پذیرفته‌شـده اسـت.

همچنیـن از آنجـا کـه ایـن مـدل مبتنـی بـر ادبیـات تحقیق اسـتاندارد اسـت، به‌نظـر می‌رسـد بـا آنچـه بایـد باشـد، تفـاوت چندانـی نداشـته و می‌توانـد به‌عنـوان مبنـای اولیـه مـورد اسـتفاده قـرار گیـرد و بـا نتایـج به‌دسـت آمـده مـدل را مـورد بازنگـری و اصـلاح قـرار داد.

۵. جمع‌بندی و نتیجه‌گیری

به‌عنـوان یـک قاعـده‌ی کلـی، معـروف اسـت کـه هـر چیـزی کـه قابـل سـنجش نباشـد، قابـل مدیریـت نیسـت. امنیـت نیـز از ایـن قاعـده مسـتثنی نیسـت. پیاده‌سـازی یـک نظـام مدیریـت امنیـت در سـازمان نیازمنـد ابزارهایـی اسـت کـه امنیـت را بسـنجد تـا سـازمان بتوانـد ضمـن بررسـی اثربخشـی و کارایـی منابـع هزینه‌شـده بـرای آن، گام‌هـای بعـدی حفـظ و ارتقـای سـطح امنیتـی را طرح‌ریـزی کنـد.

ایـن موضـوع در قالـب مدلـی بـرای سـنجش بلـوغ امنیتـی قابـل بررسـی و پاسـخ‌گویی اسـت. ایـن تحقیـق از مبانـی نظـری موجـود در ایـن حـوزه کـه به‌طورعمـده در حـوزه اسـتانداردها و تجربیـات برتـر بـوده، اسـتفاده کـرده و مدلـی سـاده و کاربـردی بـرای سـنجش سـطح بلـوغ امنیتـی در تمـام سـازمان‌ها (صرف‌نظـر از نـوع، انـدازه و ماهیـت سـازمان) ارائـه کـرده اسـت.

بـرای سـنجش سـطح بلـوغ یـک کنتـرل از مفهـوم اندازه‌گیـری بلـوغ فراینـد در پنـج سـطح استفاده‌شـده اسـت. پنـج شـاخص اندازه‌گیـری بلـوغ هـر فراینـد عبارتنـد از:

۱. خط مشی‌ها، برنامه‌ها و رویه‌ها،
۲. ابزارها و کنترل خودکار،
۳. مهارت‌ها و تخصص،
۴. مسئولیت و پاسخ‌گویی،
۵. تعیین اهداف و سنجش آن‌ها.

مفهـوم هـر شـاخص در سـطح بلـوغ متناظـر در بنـد۴ مقاله تعریـف شـده اسـت. ایـن شـاخص‌ها در کنـار یکدیگـر سـطح بلـوغ هـر کنتـرل را تعییـن کرده‌انـد. میانگیـن بلـوغ کنترل‌هـای امنیتـی طرح‌ریزی‌شـده بـرای سـازمان براسـاس شـکل (۳) سـطح بلـوغ امنیتـی سـازمان را در یکـی از سـطوح هشـت‌گانه تعییـن خواهـد کـرد.

مدل پیشنهادی، به سازمان کمک می‌کند تا:

• سـطح امنیتـی یـا بـه تعبیـر ایـن مقالـه میـزان بلـوغ امنیتـی خـود را تعییـن کنـد؛

• داشبورد مدیریتی امنیت سازمان را برای مدیران ارشد طراحی کند؛
• داده‌های علمی و واقعی برای سنجش اثربخشی هر کنترل فراهم کند؛
• تأثیر منابع تخصیص یافته در ارتقای سطح امنیتی سازمان را مشاهده کند؛
• نقاط قوت و ضعف امنیتی سازمان را شناسایی کند؛
• تصمیم‌های صحیح‌تر و مطمئن‌تری برای تخصیص منابع در جهت ارتقای سطح امنیتی خود اتخاذ کند.

هرچند در گام نخست، استفاده از این مدل برای تمامی سازمان‌ها توصیه می‌شود، لیکن باید توجه داشته که نگرش اقتضایی به میزان نیاز سازمان به عمق پیاده‌سازی یک کنترل و همچنین ضریب اهمیت متفاوت یک کنترل امنیتی در سازمان‌های مختلف دو متغیر مهمی هستند که باید در ارائه یک مدل دقیق‌تر مورد توجه قرار گیرند. اضافه کردن متغیرهای مذکور به مدل ضمن افزایش دقت مدل در سنجش بلوغ امنیتی سازمان، پیچیدگی آن را نیز به میزان قابل توجهی اضافه خواهد کرد و طبیعتاً ضریب نفوذ و گستردگی کاربرد آن را محدودتر خواهد کرد.

۶. مراجع

۱) مقاله "ارائه چارچوب پیاده‌سازی ISMS مبتنی بر متدلوژی RUP"، مصطفی تمتاجی و دیگران، پنجمین کنفرانس ملی فرماندهی و کنترل ایران، آذرماه ۱۳۹۰، دانشگاه تهران.

۲) بررسی و تحلیل تغییرات استاندارد ISO/IEC 27001: 2013 و ارائه مدل انتقال، مصطفی تمتاجی، طاهره رضایی ، سال چهارم، شماره ۴ و ۱، زمستان ۹۲ و بهار ۹۳. صفحات ۳۸ تا ۴۷.

3) ISO/IEC 27001: 2013; Information Technology - Security Techniques- Information Security Management System - Requirements.

4) ISO/IEC 27002: 2013; Information Technology - Security Techniques- Information Security Management System- Code of practice.

5) ISO/IEC 21827: 2008; Information Technology - Security Techniques - Systems Security Engineering - Capability Maturity Model.

6) ISO/IEC 15504-2, Information Technology - Process Assessment - Part 2: Performing an Assessment.

7) Control Objectives for Information and Related Technologies (COBIT); V4.1; by ISACA: 2007.