فرصت بهبود در متدولوژی پیاده‌سازی سیستم مدیریت امنیت اطلاعات

حسین شیرازی، فوق دکتری کامپیوتر (سیستم‌های خبره)، دانشیار دانشگاه صنعتی مالک اشتر

هاشم حبیبی، کارشناس ارشد مهندسی کامپیوتر

رحیم معصومی، کارشناس ارشد مدیریت، مربی دانشگاه صنعتی مالک اشتر

مصطفی تمتاجی[1]

چکیده

امروزه اطلاعات به عنوان یکی از با ارزش‌ترین دارایی‌ها و منابع سازمان‌ها برای رقابت و کسب مزیت‌های رقابتی محسوب می‌شود و امنیت اطلاعات خود یک دغدغه و معضل دنیای دانایی محور شده است. لذا پرداختن به موضوع امنیت اطلاعات امری ضروری و اجتناب ناپذیر است.

کلید حل برخی مشکلات امنیت اطلاعات در دنیای صفر و یکی امروز توجه بیشتر و اعتماد به حاصل تلفیق علم، فناوری و تجربه به نام استاندارد است. این بار استاندارد ISO/IEC 27001 با نگرش جامع و کامل به مقوله امنیت، سکاندار ایجاد امنیت در سازمانها شده است. اما مساله قابل بحث این است که آیا سازمانها قادر به پیاده سازی و استقرار موفق این استاندارد و تضمین تداوم امنیت اطلاعات خود هستند؟تجربه نشان داده است که در کشور ما علیرغم الزامات ضمنی و قانونی، سازمانهای اندکی موفق به استقرار کامل و موثر سیستم مدیریت امنیت اطلاعات شده‌اند.

با بررسی موانع و مشکلات پیاده‌سازی سیستم مدیریت امنیت اطلاعات می‌توان به تاثیر متدلوژی انتخاب شده در پیاده سازی سیستم پی برد. بطور کلی متدلوژی استقرار ، رویکرد سازمان، مراحل و گام های اجرا، زمانبندی و نقاط عطف پیاده سازی، نقش ها و مسوولیت های کلیدی، جریان و توالی فعالیتها را بیان میکند.

در این مقاله پس از بررسی اجمالی مفاهیم اساسی مطرح در موضوعات سیستم مدیریت امنیت اطلاعات و استاندارد مبنا، به معرفی و بررسی متدلوژی‌های متداول در پیاده سازی سیستم مدیریت امنیت اطلاعات پرداخته و ضمن مقایسه و بیان مشکلات آنها، راهکاری برای حل برخی از موانع پیاده سازی سیستم مدیریت امنیت اطلاعات موثر و پایدار پیشنهاد خواهد شد. این راهکار بهره‌گیری از روش تکراری-افزایشی (حلزونی)، با الهام از تکنیک‌ها و تجربیات ارزشمند موجود در متدلوژی برتر RUP، در پیاده‌سازی استاندارد بجای روش متداول آبشاری است.

کلمات کلیدی: استاندارد، امنیت اطلاعات، سیستم مدیریت امنیت اطلاعات

۱. مقدمه

امروزه با به‌کارگیری گسترده از خدمات فنآوری‌اطلاعات در سازمان‌ها، می‌توان گفت که اغلب سازمان‌ها با یکی از حوادث و یا مشکلات امنیت اطلاعات نظیر آلودگی به ویروس‌ها و نرم‌افزارهای مخرب، دسترسی غیرمجاز افراد بدون صلاحیت به داده های حساس سازمان، قطعی و یا کندی شبکه‌های اطلاعاتی، عدم تطابق و صحت اطلاعات در برنامه‌های کاربردی و غیره مواجه می‌باشند.

[1] - نویسنده پاسخگو: تمتاجی، مصطفی، دانشجوی کارشناسی ارشد مهندسی IT، mostafatamtaji@yahoo.com، ۰۹۳۹۳۵۹۰۵۲۶

وابستگی به خدمات و سیستم‌های اطلاعاتی بدان معنی است که سازمان‌ها بیشتر در معرض تهدیدهای امنیتی قرار دارند. اما راهکار مقابله با این مشکلات چیست؟ امنیت اطلاعات فراتر از نصب نرم‌افزار ضدویروس و یا پیکره‌بندی یک دیوارهٔ‌آتش یا حتی نصب سیستم‌های تشخیص و پیشگیری از نفوذ می‌باشد.

مخاطرات امنیت اطلاعات همواه با عدم قطعیت همراه بوده و مدیران سازمان‌ها تا با یک حادثهٔ امنیت اطلاعات مواجه نشوند معمولاً توجهی به آن ندارند. پیچیدگی و تعداد رو به فزونی سیستم‌ها، فراهم آوردن محیط پردازش، ذخیره و انتقال امن اطلاعات را دشوار می‌سازد. مساله امنیت اطلاعات بسیار پیچیده است، معمولاً در فرآیند توسعهٔ سیستم‌ها تمایل زیادی برای نادیده گرفتن و صرفنظر کردن از مدل‌سازی‌های امنیتی دیده می‌شود. [۳]

در چند سال گذشته، با توجه به آگاهی به مخاطرات و حتی در بعضی موارد پرداخت هزینه‌هایی سنگین برای بازیابی از تهدیدات امنیت اطلاعات در شرایطی که راه‌حلهای مناسب قبل از آن اندیشیده نشده بود، جستجو برای راهکارهای مقابله و مدیریت این مخاطرات آغاز شده است. در همین راستا در سال ۱۳۸۳ شاهد انتشار بخشنامه‌ای از سوی شورای عالی امنیت فضای تبادل اطلاعات کشور بوده‌ایم که طراحی و پیاده‌سازی سیستم مدیریت امنیت اطلاعات بر مبنای استاندارد ISO/IEC 27000:2005 را به کلیهٔ سازمان‌های دولتی توصیه کرده است. [۱]

۲. امنیت اطلاعات

امنیت به معنای دور بودن یا محفوظ ماندن از خطرات می باشد. کنترل‌های مورد نیاز برای تامین امنیت اطلاعات به سه دسته امنیت فیزیکی (استفاده از قفل‌ها، نگهبان‌ها، علایم و ...)، امنیت فنی(عملیات یا برنامه های کاربردی، تمهیدات سخت افزاری و نرم افزاری و ...) و امنیت مدیریتی (محدودیت‌های مدیریتی، رویه‌های عملیاتی، رویه‌های رویدادنگاری و ...) تقسیم می‌شوند.

پیشرفت‌های بسیار سریع در زمینه کامپیوترها و شبکه‌های کامپیوتری در سال‌های اخیر سبب پیچیده‌تر شدن مقوله ایجاد امنیت شده است. در نتیجه مدیران باید امنیت را در یک مقیاس بسیار وسیع‌تر تامین و مدیریت کنند. وظیفه مدیر امنیت اطلاعات، برقراری یک برنامه امنیت است که سه نیاز محرمانگی[۲]، جامعیت[۳] و دسترس‌پذیری[۴] منابع‌اطلاعاتی سازمان را مورد توجه قرار دهد. [۴]

بطور کلی امنیت اطلاعات از شش وجه، یعنی دسترسی‌فیزیکی، نیروی انسانی، سیستـــم عامل، داده‌ها، برنامه‌های کاربردی و شبکه قابل بررسی می‌باشد. [۵]

۳. استاندارد و امنیت اطلاعات

استاندارد، مدرکی(سندی) است در برگیرنده قواعد، راهنمایی‌ها یا ویژگی‌هایی برای فعالیت‌ها یا نتایج آنها بمنظور استفاده عمومی و مکرر که از طریق اجماع ایجاد شده و مورد تصویب سازمان شناخته شده (دارای صلاحیت) قرار گرفته باشد و هدف آن دستیابی به میزان مطلوبی از نظم در یک زمینه خاص است. استاندارد باید مبتنی بر نتایج تثبیت شده علم، فناوری و تجربه بوده و به ارتقا منافع جامعه کمک کند. [۶]

---

2. Confidentiality
3. Integrity
4. Availability

توجه روزافزون به مباحث مدیریت امنیت اطلاعات از طریق برقراری قوانین و ضوابط ملی/منطقه ای/بین المللی و همچنین توجه به راهبردهای جدید به منظور پاسخگویی به انتظارات و الزامات طرف های ذینفع نسبت به اطمینان از امنیت و ایمنی شبکه ها و سیستم های اطلاعاتی، باعث پدید آمدن استانداردهایی برای ایجاد، پیاده‌سازی، حفظ و ممیزی سیستم های مدیریت امنیت اطلاعات شده است.[۷]

در سال ۱۹۹۳ اولین گروه های کاری صنایع برای انسجام بخشیدن و سیستماتیک کردن مدیریت امنیت اطلاعات تشکیل شده و استانداردهای BS-7799-1 و BS-7799-2 در سال ۱۹۹۹ منتشر شدند. در سال ۲۰۰۰ استاندارد ISO/IEC 17799 جایگزین استاندارد BS-7799-1 شد.در سال ۲۰۰۲ ویرایش جدید استاندارد BS-7799-2 منتشر شد. [۷ و ۸]

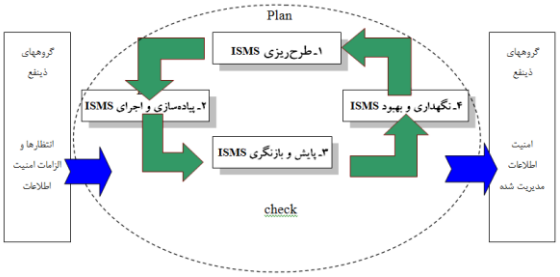
در سال ۲۰۰۵ نگرش جامع‌تری نسبت به استاندارد مدیریت امنیت اطلاعات شکل گرفت و منجر به معرفی خانواده استاندارد ۲۷۰۰۰ شد. به همین منظور استاندارد ISO/IEC 27001 جایگزین استاندارد BS-7799-2 شد. استاندارد ISO/IEC 17799 در سال ۲۰۰۷ به ISO/IEC 27002 تغییر نام داد. [۹]

۴ .معرفی استاندارد ISO/IEC27001

استاندارد ISO/IEC27001 یک مجموعه جامع از کنترل‌ها است که حاصل بهترین تجارب در مورد امنیت اطلاعات می باشد. این استاندارد بصورت بین‌المللی به رسمیت شناخته شده است و شامل ۱۱ حوزه، ۳۹ منظور مدیریتی و بیش از ۱۳۳ کنترل امنیتی به منظور اقدامات بازدارنده و نظارتی و بیش از ۵۰۰ زیر کنترل می‌باشد. حوزه‌های یازده‌گانه استاندارد عبارتند از: خط مشی امنیتی، سازمان امنیت اطلاعات، مدیریت دارائی، امنیت منابع انسانی، امنیت محیطی و فیزیکی، مدیریت عملیات و ارتباطات، کنترل دسترسی، تهیه، توسعه و نگهداری سیستم‌های اطلاعاتی، مدیریت حوادث امنیت اطلاعات، مدیریت تداوم کسب و کار، انطباق . [۸]

این استاندارد دیدگاه فرایند گرا را برای ایجاد، پیاده سازی، اجرا، پایش، بازنگری، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات انتخاب کرده است. مدل اعمال شده بر کلیهٔ فرآیندهای سیستم مدیریت امنیت اطلاعات شامل چرخه ای مستمر (شکل(۱)) و متشکل از ۴ مرحلهٔ زیر است: [۱۰ و ۸]

۱) طرح‌ریزی (ایجاد سیستم مدیریت امنیت اطلاعات): در این مرحله از چرخهٔ بهبود، باید خط‌مشی امنیتی، اهداف، مقاصد، فرآیندها و روش‌های اجرایی مرتبط با مدیریت مخاطرات و بهبود امنیت اطلاعات، به‌گونه‌ای ایجاد شوند تا نتایج مطلوبی در چارچوب اهداف و خط مشی‌های کلی سازمان به‌دست آید.



شکل (۱): استفاده از چرخه PDCA در فرایندهای سیستم مدیریت امنیت اطلاعات

۲) اجرا (پیاده سازی و اجرای سیستم مدیریت امنیت اطلاعات): در این مرحله باید خط مشی‌های امنیتی، کنترل‌ها و فرآیندهای لازم در جهت بهبود امنیت اطلاعات پیاده‌سازی و اجرا شوند.

۳) بررسی (پایش و بازنگری سیستم مدیریت امنیت اطلاعات): در این مرحله باید بر اساس خط‌مشی‌های امنیتی، اهداف و فعالیت‌های عملی انجام گرفته در جهت ایجاد امنیت اطلاعات، ارزیابی‌های لازم برای اندازه‌گیری اثربخشی فرآیندها، پیاده سازی صحیح کنترل‌ها در سیستم و چگونگی انجام گرفتن فعالیت‌ها صورت گیرد و در نهایت گزارشی از عدم انطباق‌ها برای بازنگری دوباره فرآیندهای صورت گرفته، تهیه شود.

۴) اقدام (نگهداری و بهبود سیستم مدیریت امنیت اطلاعات): در این مرحله باید فعالیت‌های پیشگیرانه و اصلاحی بر مبنای نتایج بازخورهای مناسب انجام گیرد؛ به‌عبارتی باید فرآیند بهبود مستمر سیستم مدیریت امنیت اطلاعات اجرا شود.

این استاندارد، به‌منظور حمایت از پیاده‌سازی و اجرای یکسان و یکپارچهٔ استانداردهای مدیریتی، با استانداردهای ISO 9001:2000 **و** ISO 14001:2004 هم‌راستا شده است. یک سیستم مدیریت که به‌طور مناسب طراحی شده است، می‌تواند پاسخگوی تمامی الزامات این استانداردها باشد. این استاندارد برای توانمندسازی سازمان در جهت یکپارچه‌سازی سیستم مدیریت امنیت اطلاعات با نیازمندی‌های سیستم مدیریت طراحی شده است. [۸]

۵ .متدولوژی‌های پیاده‌سازی سیستم مدیریت امنیت اطلاعات

سیستم مدیریت امنیت اطلاعات برای انطباق با استاندارد ISO/IEC27001 باید کلیه الزامات ذکر شده در استاندارد را برآورده سازند. استاندارد فوق یک استاندارد جامع و کامل است که پیاده سازی آن نیازمند برنامه ریزی و پیش بینی ساز و کارهای مورد نیاز می باشد.

یکی از عوامل کلیدی موفقیت در استقرار این استاندارد وجود یک رویکرد و چارچوب برای پیاده سازی، پایش واصلاح امنیت اطلاعات یا متدلوژی است. [۱۰]

روش های مختلفی برای پیاده سازی یا استقرار سیستم مدیریت امنیت اطلاعات بیان شده است. در این تحقیق ۱۴ متدلوژی (۴ متدلوژی پژوهشی و ۱۰ متدلوژی تجاری) مطابق جدول (۱) مورد بررسی قرار گرفته و در ادامه مقاله بدلیل محدودیت فقط ۳ متدلوژی (یک متدلوژی خارجی پژوهشی و یک متدلوژی ایرانی و خارجی تجاری) به اختصار معرفی شده‌اند.

جدول(۱): تقسیم بندی متدلوژی ها از نظر ملیت و ماهیت

	پژوهشی(تحقیقاتی)	تجاری (عملیاتی)
ایرانی	سعید قنبری رحمت الله صوفی علی پورمند محمد خالقی	دانشگاه صنعتی مالک اشتر سعید سادات و دیگران
خارجی	Vinod Kumar	شرکت DISC شرکت ATSEC شرکت Meil شرکت Alan Calder شرکت Auditing Resourse شرکت Active Agancy نرم افزار Callio

۵,۱ .متدولوژی دانشگاه صنعتی مالک اشتر – مجتمع امنیت و فناوری اطلاعات

در سند " فرآیندهای اجرا و پیاده‌سازی سیستم مدیریت امنیت اطلاعات"، مراحل زیر برای پیاده‌سازی استاندارد ISO27001 بیان شده است: [۲]

۱- شناسایی سازمان و طبقه بندی دارایی ها: شامل استخراج روالهای سازمانی، شناسایی اولیه معضلات امنیتی سازمان، شناسایی دارایی‌های سخت افزاری، شناسایی دارایی‌های نرم افزاری، شناسایی دارایی‌های شبکه‌ای، شناسایی دارایی‌های اطلاعاتی، شناسایی دارایی‌های امنیتی، شناسایی اولویتهای کلان امنیتی سازمان، تولید سند راهبردی امنیت اطلاعات سازمان، شناخت سازمان و فعالیتها و روالهای آن و طبقه بندی دارایی‌ها می‌باشد.

۲- ارزیابی مخاطرات: شامل ارزش گذاری کلیه داراییهای سازمان، شناسایی نقاط ضعف امنیتی سازمان، شناسایی تهدیدات موجود علیه هر یک از داراییها و محاسبه احتمال وقوع تهدیدات مختلف در سازمان و استخراج مخاطرات مرتبط با هر یک از داراییها و استخراج مخاطرات مرتبط با روالها و ساختار سازمانی و اولویت‌بندی مخاطرات است.

۳- مدیریت مخاطرات: شامل انتخاب کنترلهای مورد نیاز برای مقابله با هر مخاطره، تعیین هزینه مقابله با هر مخاطره، اتخاذ سیاست مواجهه با هر مخاطره از قبیل رفع، کاهش یا پذیرش هر مخاطره، تولید سند سیاست امنیتی سازمان، استقرار کنترل‌های تعیین شده در سطح شبکه و سازمان، تولید طرح امنیتی سازمان، تولید طرح مدیریت تغییرات سازمان و تولید طرح استمرار فعالیتهای سازمان است.

۴- آموزش، اطلاع رسانی و فرهنگ سازی: شامل آموزش کاربران عادی،مدیران ارشد و آموزشهای فنی مدیران و راهبران شبکه است.

۵,۲. متدولوژی Vinod Kumar

Vinod Kumar در مقاله خود گام های زیر برای پیاده سازی سیستم مدیریت امنیت اطلاعات ذکر شده است: [۱۱]

۱- تعهد مدیریت: الزام به پیاده سازی این سیستم و اخذ گواهینامه عمدتا از فشار ذینفعان بیرون سازمان مانند مشتریان نشات می گیرد. مدیریت نه تنها باید نگران این موضوع باشد، بلکه باید بودجه و منابع لازم برای این پروژه را تامین نماید.

۲- تشکیل تیم: برای هدایت و انجام فعالیت ها لازمست تیم مناسب تشکیل شود. فردی برای برقراری ارتباط بین تیم و مدیر ارشد نیاز است.این فرد همان مدیر ارشد امنیت اطلاعات[۵] است.

۳-تعریف دامنه: سیستم مدیریت امنیت اطلاعات را می توان برای یک واحد، یک طبقه از سازمان یا همه بخش های سازمان تعریف کرد. دامنه پیاده سازی سیستم بسته به اهمیت اطلاعاتی واحدها و توانمندی سازمان باید تعیین و در خط مشی امنیت اطلاعات به وضوح ذکر گردد.

۴- تهیه لیست دارایی ها: همه دارایی های اطلاعاتی دامنه پیاده سازی سیستم باید مستند شوند. دارایی های اطلاعاتی می توانند در قالب داده/اطلاعات، فناوری، افراد و خدمات باشند.

۵- ارزش گذاری دارایی ها[۶]: در این گام ارزش کمی هر دارایی با توجه به محرمانگی، جامعیت و دسترس پذیری هر دارایی مشخص می شود.

۶- مقدار دهی مخاطرات [۷]: مقدارکمی مخاطرات هر دارایی از طریق تعیین تهدیدات ممکن، نرخ وقوع و چگونگی تاثیر آنها که بر محرمانگی، جامعیت و دسترس پذیری هر دارایی تاثیر می گذارند، مشخص می شود.

۷- تحلیل تاثیر کسب و کار[۸]: این گام برای تحلیل اثرات رخدادها یا حوادث جدید که قبلا رخ نداده اند، روی سیستم انجام می شود. سناریوهای شکست مختلف و تاثیرات احتمالی آنها روی کسب و کار تجزیه و تحلیل می شود. این موارد شامل مشکلات فنی، منابع انسانی و سایر رخدادها می‌شود.

۸- تعیین احتمال رخداد[۹]: این گام برای تعیین نرخ تکرار شکست (عیب) انجام می شود. اینکار بر اساس تجربیات قبلی و همچنین توجه به پیاده سازی فعلی صورت می گیرد.

۹- طرح مدیریت مخاطرات[۱۰]: در این گام، طرح مقابله با مخاطرات تدوین می گردد. روشهای مقابله با مخاطرات می تواند شامل پذیرش[۱۱]، اجتناب[۱۲]، محدود سازی[۱۳] یا انتقال[۱۴] مخاطره باشد. تصمیم گیری برای کاهش مخاطرات با تعریف و بکارگیری کنترل‌های مناسب در این گام انجام می گیرد.

۱۰-تدوین بیانیه کاربردپذیری: بیانیه کاربردپذیری شامل همه کنترل های استاندارد است. همچنین در این بیانیه کنترل‌های مورد استفاده و توجیه علت انتخاب آنها وتوجیه علت کنترل‌های انتخاب نشده ذکر می شود.

۱۱- طرح تداوم کسب و کار[۱۵] و واکنش به حوادث[۱۶]: اجرای این گام جزو فعالیت های حیاتی است. قبل از ایجاد و تدوین این طرح، ضروری است که تاثیرات بالقوه حوادث مد نظر قرار گرفته و مخاطرات اساسی درک شوند.

---

[5] . Chief Information Security Officer-CISO
[6] .Asset Value
[7] . Risk Value
[8] . Business Impact Analysis-BIA
[9] . Probability of Occurrence
[10] . Risk Management
[11] . Risk Acceptance
[12] . Risk Avoidance
[13] . Risk Limitation
[14] . Risk Transfer
[15] . Business Continuity Plan-BCP
[16] . Disaster Recovery-DR

۱۲- برنامه آموزشی و آگاهی کاربران: آموزش های مورد نیاز باید در سطوح مختلف (مدیریت ارشد، مدیران میانی و کاربران نهایی) انجام شود.

۱۳- ممیزی: این گام شامل ممیزی اولیه، بازنگری مستندات و ممیزی داخلی و ممیزی فنی است.

۵,۳. متدولوژی شرکت Active Audit Agency

شرکت اکراینی Active Audit Agency واقع در Kyiv ارایه دهنده مجموعه کاملی از خدمات برای مدیریت امنیت اطلاعات اعم از مشاوره برای پیاده‌سازی، نرم‌افزارهای جانبی و ممیزی سیستم‌ها، برای پیاده سازی سیستم مدیریت امنیت اطلاعات در نقشه راه تدوین شده و بر اساس چرخه PDCA مراحل زیر را ارایه کرده است و مطابق گام های ذکر شده در این متدولوژی نرم‌افزارهای جانبی را برای تسریع مراحل استقرار توسعه داده است.[۱۲]

۱- تعهد مدیریت و تعیین مسوولیت ها: مدیریت ارشد سازمان باید از طریق جهت گیری واضح و تعیین مسوولیت‌ها و تخصیص منابع از پروژه پشتیبانی نماید.

۲- تعیین دامنه و محدوده سیستم: در این گام باید دامنه و محدوده سیستم برحسب ماهیت و مشخصه های کسب وکار، سازمان، موقعیت آن، دارایی ها و فناوری هایش مشخص شود.

۳- تعریف خطی مشی امنیت: برحسب مشخصه‌های سازمان و کسب و کار آن و موقعیت و دارایی و فناوری‌هایش باید خط مشی سیستم مدیریت امنیت اطلاعات مشخص گردد.

۴- مدیریت دارایی‌ها: شامل طبقه بندی دارایی‌های اطلاعاتی و تعیین مسوولیت هریک.

۵- تعیین رویکرد ارزیابی مخاطرات: متدولوژی ارزیابی مخاطرات انتخاب شده باید تضمین نماید که ارزیابی های مخاطرات انجام شده، خروجی های قابل مقایسه و تکرارپذیر تولید می کند.

۶- تعیین مخاطرات: این گام شامل تعیین دارایی‌های موجود در دامنه و مالک آنها، تعیین تهدیدات متناظر با هر دارایی، تعیین آسیب پذیری‌ها و تعیین تاثیر از دست رفتن محرمانگی، دسترس پذیری و جامعیت بر هر یک از دارایی‌ها است.

۷- تحلیل و ارزیابی مخاطرات: ارزیابی تاثیرات ناشی از شکست امنیتی بر سازمان، ارزیابی احتمال وقوع واقعی شکست های امنیتی ناشی از تهدیدات، تخمین سطوح مخاطرات و تعیین قابل پذیرش بودن یا نبودن مخاطره در این گام انجام می شود.

۸- تعیین و ارزیابی گزینه هایی برای مقابله با مخاطرات: این گام شامل اقداماتی مانند اعمال کنترل های مناسب، پذیرش آگاهانه مخاطره با درنظر گرفتن معیارهای پذیرش مخاطرات مشخص شده، اجتناب از مخاطره و انتقال مخاطره است.

۹- انتخاب اهداف کنترلی و کنترلها برای مقابله با مخاطرات: اهداف کنترلی و کنترل ها برای برآورده کردن الزامات مشخص شده بوسیله فرایند ارزیابی مخاطرات و مقابله با مخاطرات باید انتخاب و پیاده سازی شوند.

۱۰- اخذ تصویب مدیریت برای مخاطرات باقیمانده و پیاده‌سازی سیستم: در صورتی که برای مخاطره ای به هر دلیلی اقدامی طراحی و اجرا نشود، این مخاطرات باید به تایید و تصویب مدیریت برسد.همچنین مدیریت باید با توجه به فعالیت‌های انجام شده، ادامه روند پیاده سازی را تایید نماید.

۱۱- تدوین بیانیه کاربردپذیری: بیانیه کاربردپذیری خلاصه‌ای از تصمیمات مرتبط با مقابله با مخاطرات و توجیه کنار گذاشتن و استثنا شدن کنترل‌ها را بیان می کند.

۱۲- نظام مند کردن و پیاده سازی طرح مقابله با مخاطرات: این طرح مدیریت مناسب اقدامات، منابع و مسوولیت ها و همچنین اولویت بندی برای مدیریت مخاطرات امنیت اطلاعات را تعیین می‌کند.

۱۳- بازنگری منظم کارآیی سیستم: این گام می تواند از طریق ممیزی امنیت اطلاعات توسط شخص ثالث و بررسی نتایج انجام شود.

۱۴- اندازه گیری کارآیی کنترل ها: در این گام بررسی‌های لازم در مورد کارآمدی کنترل های اعمال شده و سطح امنیت ایجاد شده با بکارگیری آنها در زمینه هایی از قبیل شبکه، امنیت فیزیکی و مهندسی اجتماعی انجام می شود.

۱۵- ممیزی داخلی: سازمان باید در بازه های زمانی طرح ریزی شده ممیزی داخلی سیستم مدیریت امنیت اطلاعات را انجام دهد تا از پیاده سازی، تداوم و عملکرد مورد انتظار سیستم و همچنین تطابق اهداف کنترلی، کنترل ها، فرایندها و روش‌های اجرایی با الزامات استاندارد، قوانین و مقررات مرتبط، الزامات امنیتی مشخص شده اطمینان حاصل نماید.

۱۶- پیاده سازی بهبودهای تعیین شده در سیستم: سازمان باید اقداماتی را برای حذف علل عدم انطباق ها با الزامات بمنظور جلوگیری تکرار وقوع آنها انجام دهد.

۱۷- اقدام پیشگیرانه: سازمان باید اقدامات مورد نیاز برای حذف علت عدم انطباق های بالقوه با الزامات بمنظور جلوگیری از وقوع آنها را انجام دهد.

۵,۴ .جمع بندی و تجزیه و تحلیل یافته‌ها

در جدول (۲) و (۳) گام های ذکر شده در متدلوژی های بررسی شده در این تحقیق ذکر شده اند.

جدول(۲): متدلوژی های پیاده سازی سیستم مدیریت امنیت اطلاعات ایرانی

نام / گام	پورمند	خالقی	قنبری	سادات	صوفی	دانشگاه مالک اشتر
۱	آماده سازی اولیه	تدوین و اجرای اهداف، راهبردها و سیاست‌ها	شناخت سازمان	پیش نیاز	ایجاد ISMS	شناسایی سازمان و طبقه بندی دارایی
۲	تعریف ISMS	تدوین و اجرای طرح ارزیابی مخاطرات	شناسایی، دسته‌بندی و ارزش‌گذاری دارایی‌ها	تهیهٔ پروپزال	پیاده سازی و اجرای ISMS	ارزیابی مخاطرات
۳	ایجاد سند سیاست امنیت اطلاعات	تدوین و اجرای طرح امنیت	شناسایی آسیب‌پذیری‌ها و تهدیدات	طرحریزی	نظارت و بازنگری	مدیریت مخاطرات
۴	ارزیابی مخاطرات	تدوین و اجرای طرح پشتیبانی حوادث امنیتی	شناسایی مخاطرات	پیاده سازی و اجرا	حفظ و به سازی ISMS	آموزش واطلاع رسانی
۵	آموزش و آگاهی بخشی	تدوین و اجرای طرح تداوم عملکرد و ترمیم خرابی‌ها	میزان تاثیرگذاری آسیب‌پذیری‌ها و شدت اثر تهدیدات	مرور و پایش	مستندسازی	-
۶	آمادگی برای ممیزی	تدوین و اجرای برنامهٔ آگاهی‌رسانی، و آموزش	تعیین راه کار ارزیابی مخاطرات	نگهداری و بهبود	-	-
۷	ممیزی	ایجاد واحد راهبری و سیاست‌گذاری	محاسبهٔ میزان مخاطرات	-	-	-
۸	کنترل و بهبود مداوم	ایجاد واحد اجرایی	پیاده‌سازی	-	-	-
۹	مستندات	ایجاد واحد پشتیبانی فنی	-	-	-	-

همانطور که مشاهده می شود با وجود اینکه استاندارد مبنا دارای الزامات ثابت و مشخصی است، اما متدلوژی های ارایه شده دارای مراحل متفاوتی می باشد و در سازمان های مختلف از توالی و اولویت های متفاوتی برای پیاده سازی استفاده می کنند. از مقایسه متدلوژی های ارایه شده نکات زیر قابل توجه است:

- باوجود اینکه یکی از اهداف توسعه استاندارد ایجاد نظم و یکپارچگی است، اما متدلوژی های پیاده سازی در روش رسیدن به این نظم از چارچوب یکسانی استفاده نمی کنند و هر سازمان مشاوره دهنده برای پیاده سازی سیستم مدیریت امنیت اطلاعات از مفاهیم و اولویت بندی خاص خود بهره می گیرد و در این میان مزایا و معایب هر متدلوژی مشخص نیست.
- تعدد متدولوژی ها و گام های مختلف نشان از وجود تعابیر مختلف از بندهای استاندارد دارد. اینکه متخصصان مختلف اولویت انجام مراحل را متفاوت با یکدیگر در نظر می گیرند، نشان میدهد که تفکیک بین مراحل و اجرای گامها بصورت متوالی موضوع قابل بحث و بررسی است و مورد تایید و توافق همه صاحبنظران نیست.

نگاه سطری به جداول فوق نشان می‌دهد که توالی ثابت و مشخصی در اجرای گام‌ها و فعالیت‌ها وجود ندارد، بلکه می‌توان در هر گام بخشی از فعالیت‌های موجود در گام‌های مختلف دیگر را انجام داد که همان مفهوم موازی بودن و یا همپوشانی زمانی انجام فعالیت‌ها است.

مانند هرپروژه دیگر، پروژه های ایجاد سیستم مدیریت امنیت اطلاعات را میتوان بصورت آبشاری یا تکراری اجرا کرد که در کلیه متدلوژی های بررسی شده از روش تکراری برای انجام فعالیت ها استفاده شده است که در آن کلیه فعالیتها بصورت متوالی انجام میشود. در روش تکراری از چرخه حیات با چندین تکرار استفاده می‌شود. هر تکرار مجموعه‌ای تعریف شده از اهداف دارد و بخشی از سیستم نهایی را پیاده‌سازی می‌کند. روش آبشاری دارای معایبی است که به برخی از آنها اشاره می شود:

- سطح بلوغ هر گام سیستم مدیریت امنیت اطلاعات در سازمان ها و سطح درک الزام استاندارد متفاوت است، لذا ممکن است قبل از اتمام کامل و واقعی یک مرحله، مرحله بعدی آغاز گردد.
- اگر در گام های اولیه مدل کسب وکار، شناسایی دارایی ها و تهدیدها و آسیب پذیری ها بصورت کامل انجام نشده و شناخته نشوند، میزان و سطح مدیریت مخاطرات کاهش میابد.
- استراتژی مراحل بعدی قبل از شروع آن مرحله بصورت کامل مدنظر قرار نمیگیرد.
- کلیه اعضای تیم از ابتدا درگیر پروژه نشده و وقفه های کاری بدلیل انتظار برای دریافت نتیجه گروهی دیگر از اعضای ایجاد می شود.
- در صورت عدم اجرای درست یک مرحله، ضمن بروز مشکل در مراحل بعدی، امکان بازگشت و تکمیل مرحله قبل وجود ندارد و اصلاح و تغییر زمانبر و مشکل است.
- در بیشتر موارد مدیران در ابتدای گامهای پیاده سازی، در خواستهایی برای انجام گامهای آخر دارند که روش آبشاری پاسخگوی چنین انتظاراتی نیست.
- با توجه به انجام متوالی هرگام، توسعه دهندگان سیستم مدیریت امنیت اطلاعات مجاز به بهره گیری از یادگیریهای خود در حین پروژه برای تکمیل مراحل قبلی نیستند.

جدول (۳):متدلوژی های پیاده سازی سیستم مدیریت امنیت اطلاعات غیر ایرانی

	Active Audit Agency	VinodKumar	atsec	Auditing Resources	DISC	Alan Calder	Callio	meil
۱	تعهد مدیریت و تعیین مسوولیت‌ها	تعهد مدیریت	اخذ حمایت مدیر ارشد	اخذ حمایت مدیر ارشد	بیان و تصدیق اهمیت	شروع پروژه	آغاز پروژه	تهیه پروفایل امنیت اطلاعات
۲	تعیین دامنه و محدوده	تشکیل تیم	تعیین دامنه	تعریف دامنه	تعیین دامنه	حمایت مدیریت	برآورد مخاطرات و راه مقابله	تدوین دستورالعمل امنیت اطلاعات
۳	تعریف خطی مشی امنیت	تعیین دامنه	تعیین قوانین و مقررات قابل کاربرد	تهیه لیست دارایی	تعریف خط مشی	محدوده و قلمرو	رفع مخاطرات	تدوین طرح امنیت اطلاعات
۴	مدیریت دارایی ها	تهیه لیست دارایی	تعیین روش ارزیابی مخاطرات	ارزیابی مخاطرات	ایجاد تشکیلات امنیت	برنامه ریزی	مهیا سازی ممیزی	مراقبت امنیت اطلاعات
۵	تعیین رویکرد ارزیابی مخاطرات	ارزش گذاری دارایی	تهیه لیست دارایی	بیانیه کاربرد پذیری و طرح مقابله مخاطرات	تعیین و طبقه بندی دارایی	ارتباطات	مدیریت مستندساز ی	گواهی امنیت اطلاعات
۶	تعیین مخاطرات	مقدار دهی مخاطرات	تعیین مخاطرات	ایجاد برنامه پیاده سازی	تعیین و طبقه بندی مخاطرات	ارزیابی مخاطرات	–	–
۷	تحلیل و ارزیابی مخاطرات	تحلیل تاثیر کسب و کار	ارزیابی مخاطرات	تدوین برنامه پیاده سازی	ارزیابی گزینه های مدیریت مخاطرات	انتخاب کنترل‌ها	–	–
۸	تعیین و ارزیابی گزینه هایی برای مقابله با مخاطرات	تعیین احتمال رخداد	تعیین اهداف و کنترل	محصولات عملیاتی	استراتژی کاهش مخاطرات	مستندسا زی	–	–
۹	انتخاب اهداف کنترلی و کنترلها	طرح مدیریت مخاطرات	خط مشی و روال کنترل مخاطرات	بازنگری انطباق	تدوین بیانیه کاربردپذیری	آزمون	–	–
۱۰	اخذ تصویب مدیریت	تدوین بیانیه کاربردپذیری	تخصیص منابع و آموزش	اقدام اصلاحی	آموزش و هشیاری امنیتی	–	–	–
۱۱	تدوین بیانیه کاربردپذیری	طرح تداوم کسب و کار	پایش پیاده سازی	ارزیابی قبل از صدور گواهینامه	بازنگری و پایش	–	–	–
۱۲	نظام مند کردن و پیاده سازی طرح مقابله با مخاطرات	برنامه آموزشی و	آماده شدن برای ممیزی	ممیزی صدور گواهینامه	حفظ و بهبود	–	–	–
۱۳	بازنگری منظم کارآیی سیستم	ممیزی	–	–	–	–	–	–
۱۴	اندازه گیری کارآیی کنترل ها	–	–	–	–	–	–	–
۱۵	ممیزی داخلی	–	–	–	–	–	–	–
۱۶	پیاده سازی بهبودهای تعیین شده در سیستم	–	–	–	–	–	–	–
۱۷	اقدام پیشگیرانه	–	–	–	–	–	–	–

- پیاده سازی سیستم مدیریت امنیت اطلاعات بصورت آبشاری مستلزم دانش و تسلط کامل متخصصین بر هر گام میباشد،زیرا که برگشت به مرحله قبل و تکمیل آن در این روش پیش بینی نشده است،که بخصوص در سازمان های تازه کار چنین دانشی وجود ندارد.

در روش تکراری مراحل با یکدیگر ترکیب شده و ترکیبی از فعالیتهای مراحل مختلف بصورت گام به گام انجام میشود. به این معنی که بر خلاف روش توسعه آبشاری، در روش تکراری اساس کار بر اجرای مراحل در حالتی تقریبا موازی و بصورت وزن دهی شده با امکان تکمیل و بازگشت به مراحل قبلی است. از خطرات و آسیب‌های موجود در روش تکراری نیز می‌توان به موارد زیر اشاره کرد:

- طرح‌ریزی بیش از حد تفصیلی تا پایان کار
- عدم همگرایی پروژه
- امکان تمرکز بر خروجی اشتباه
- قرار دادن بیش از حد فعالیت‌ها در تکرار اول
- تکرارهای غیر ضروری و بیش از حد و یا همپوشان
- مدیریت نامناسب در طول پروژه

تجربه نشان می‌دهد نیازهای سازمان و انتظارات مسوولین با بکارگیری روش تکرار سریعتر براورده میشود و تمایل بیشتری برای بکارگیری این روش وجود دارد. سازمان‌ها تمایل دارند تا بدون نگرانی از عدم انجام کامل یک مرحله، سایر مراحل را دنبال کرده و از طرفی قبل از اعلام اتمام کلیه مراحل پیاده سازی از رفع کمبودها و نواقص گامهای قبلی اطمینان حاصل کنند..

از طرفی تجربه کم متخصصین و به تبع آن سازمانها و در واقع ناشناخته بودن ابعاد مختلف آن سبب می‌شود تا پرداختن به موضوع بصورت گامهای مشخص و دارای خروجی معلوم و کامل کردن یک گام بطور کامل مشکل و دور از واقعیت بنظر برسد. واقعیت آن است که سازمان تازه کار در قدمی که به سوی استقرار سیستم مدیریت امنیت اطلاعات برمی دارد، مرتبا در حال یادگیری و تسلط بیشتر بر مراحل قبلی است، در حالی‌که در روش آبشاری امکان برگشت به مرحله قبل و اصلاح آن پیش‌بینی نشده است.

۶. نتیجه گیری

در این مقاله ابتدا مفهوم امنیت و ضرورت توجه ویژه به آن به عنوان یک موضوع بین رشته ای و جامع بیان شد. با توجه به اهمیت موضوع حفظ و تداوم امنیت اطلاعات ، شکی نیست که کلیه سازمانهایی که اطلاعات در آنها جز دارایی های مهم محسوب می شوند، باید اقدام به ایجاد یک سیستم مدیریت امنیت اطلاعات نمایند.

نتایج بررسی ها و جستجوها در مقالات، کتب و نتایج تحقیق‌ها نشان میدهد که در حال حاضر جامع ترین و فراگیرترین استاندارد برای پیاده سازی سیستم مدیریت امنیت اطلاعات، خانواده ااستانداردهای ISO/IEC27000 است که ضمن پذیرش بین‌المللی، توسط مراجع قانونی و ذیصلاح کشور (از جمله دبیرخانهٔ شورای عالی امنیت فضای تبادل کشور، وابسته به مرکز فناوری‌اطلاعات‌ریاست جمهوری) صحه گذاری شده است.

لذا این استاندارد بعنوان جامع‌ترین استاندارد موجود و در برگیرنده کلیه الزامات فیزیکی، فنی و امنیتی موردنیاز برای پیاده سازی سیستم مدیریت امنیت اطلاعات معرفی شد.

در ادامه با توجه به نقش مهم روش پیاده‌سازی استاندارد مذکور در موفقیت و کارآمدی آن در سازمان و تداوم و بقای امنیت اطلاعات، ۱۴ متدلوژی متداول پیاده سازی سیستم مدیریت امنیت اطلاعات (۴ متدلوژی پژوهشی و ۱۰ متدلوژی تجاری) بطور مختصر مورد بررسی قرار گرفته و معرفی شدند. ذکر این نکته لازمست که وجود یک رویکرد و چارچوب برای پیاده سازی سیستم مدیریت امنیت اطلاعات، در استاندارد ISO/IEC 27002 بعنوان یک عامل حیاتی موفقیت آورده شده است.

تجربیات و سوابق موجود در زمینه پیاده سازی سیستم مدیریت امنیت اطلاعات در سازمانها نشان میدهد که پیاده سازی آبشاری سیستم مدیریت امنیت اطلاعات در بیشتر موارد با شکست مواجه شده است و با ساختار، انتظارات و توانمندی‌های سازمان‌های ایرانی سازگار نیست . لذا با توجه به معایب و مزایای ذکر شده برای این دو روش،لازمست چارچوبی برای پیاده سازی سیستم مدیریت امنیت اطلاعات مبتنی بر روش توسعه تکراری و افزایشی (حلزونی) ارایه گردد تا راهگشای برخی از موانع موجود در این مسیر باشد.در ارایه و تدوین این چارچوب می‌توان از تکنیک‌ها و تجربیات ارزشمند موجود در متدلوژی برتر توسعه نرم‌افزار یعنی RUP بهره گرفت.

مراجع

[۱] محمود خالقی، سند راهنمای پیاده سازی سیستم مدیریت امنیت اطلاعات،دبیرخانه شورای عالی امنیت فضای تبادل اطلاعات کشور،۱۳۸۳.

[۲] دانشگاه صنعتی مالک‌اشتر – مجتمع امنیت و فناوری اطلاعات ، فرایندهای اجرا و پیاده‌سازی سیستم مدیریت امنیت اطلاعات، ۱۳۸۷

[3] Freeman,J.W.,Neely,R.B.,&Hechard,M.A. “A Validated Security Policy Modeling Approach” Proceeding of the Loth Annual Computer Security Applications Conference, Orland,FL, 189-200,(2005)

[4] BS7799-2, Information Security Management- Specification For information Security Management Systems, (2002)

[5] Shroder W., “Firewall And Internet Security”, Prentice Hall, (2005)

[6] ISO/IEC Directives Part 2: Edition 6.0: 2011; Rules for the Structure and Drafting of International Standards.

[7] International Organization for Standardization, List of ISO technical committees, http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees.htm

[8] ISO/IEC 27001 :2005 (BS 7799-2: 2005) Information technology – Security techniques – Information security management systems – Requirements

[9] Maximus International LLC, ISMS Lead Auditor Course, Training Material, 2010

[10] ISO/IEC 27002 :2005 Information technology- Security techniques- Code of practice for information security management

[11] ISMS Implementation Guide, By Vinod Kumar Puthuseeri, 2006; http://www.infosecwriters.com/text_resources/pdf/ISMS_VKumar.pdf

[12] Active Audit Agancy, Road map for ISO 27001 implementation,

http://www.auditagency.com.ua/?r=blog_14_RoadMap