نقش مدیریت امنیت اطلاعات در
کاهش ریسک عملیاتی مؤسسات مالی

محمدرضا فراهانی

فعالیت بانک‌ها، و مؤسسات مالی و اعتباری در حوزه‌های مختلف فعالیت از جمله اعطای تسهیلات، سرمایه‌گذاری، صدور انواع اوراق قرضه، صدور انواع گواهی سپرده، صدور ضمانت‌نامه‌ها و گشایش انواع اعتبارات اسنادی و یا به عبارت دیگر، اقدام به ایفای نقش در بازارهای پول و سرمایه، آنها را در معرض مخاطرات و ریسک‌های خاص اینگونه فعالیت‌ها قرارداده است. از جمله ریسک‌های با اهمیت می‌توان به ریسک عملیاتی و اعتباری اشاره نمود.

نیاز روزافزون مؤسسات مالی و اعتباری به اطلاعات صحیح و به‌روز در تعاملات و رشد سریع فن‌آوری‌های نوین در عرصه اطلاعات و ارتباطات در عصر حاضر، ضرورت استقرار یک نظام مدیریت امنیت اطلاعات را در کاهش ریسک‌های احتمالی بیش از پیش نمایان می‌سازد. این نوشتار سعی دارد ضمن اشاره به برخی از ویژگی‌های این نظام مدیریتی به معرفی استانداردهای بین‌المللی موجود در این زمینه بپردازد.

مفهوم ریسک و مدیریت آن

یک سازمان ممکن است بوسیله یک یا مجموعه‌ای از اتفاقات کوچک و بزرگ دچار آسیب شود. سوانح و خطرات، شرایطی هستند که به صور گوناگون، سازمان‌ها را با قابلیت پذیرش ضرر و زیان در قبال آنها مواجه می‌سازند. این ضررها ممکن است مربوط به سلامت کارکنان، ایمنی و عملکرد ماشین‌آلات، تجهیزات یا کل تأسیسات یک کارخانه، محیط زیست، محصول، دارایی‌های مالی و یا اطلاعات باشد و نیز می‌تواند دارایی‌های غیرمشهود یک سازمان مثل لطمه زدن به اعتبار و حیثیت آن را شامل شود.

ریسک، شامل ابعاد احتمالی قرار گرفتن در معرض یک سانحه، تکرار و طول مدت سانحه است و احتمالات حادث‌شدن یک واقعه را خواسته یا ناخواسته در نظر می‌گیرد. از این‌رو ریسک را می‌توان به رویدادهای غیر منتظره که معمولاً به صورت تغییر در ارزش دارایی‌ها یا بدهی‌ها می‌باشد، تعریف کرد.

مدیریت ریسک، فرایندی است که هدف آن کاهش آثار زیان‌آور یک فعالیت از طریق اقدام آگاهانه برای پیش‌بینی حوادث ناخواسته و برنامه‌ریزی برای اجتناب از آنها می‌باشد. بایستی توجه داشت که:

- ریسک قابل حذف نیست.
- هدف از برنامه‌های مدیریت ریسک، رسانیدن ریسک به حدود قابل قبول است، نه حذف کامل ریسک.
- و از نظر عملی، ریسک صفر وجود ندارد.

انواع ریسک:

مخاطرات و ریسک‌هایی که سازمان‌ها با آن روبرو هستند به‌لحاظ نوع فعالیتی که آنها انجام می‌دهند، می‌توانند متفاوت باشند. مهمترین مخاطرات و ریسک‌هایی که مؤسسات مالی و اعتباری با آن مواجه خواهند بود، عبارتنداز:

۱- ریسک اعتباری: ریسک مربوط به زیان‌های ناشی از عدم بازپرداخت یا بازپرداخت با تأخیر اصل یا فرع وام از طرف مشتری.

۲- ریسک بازار: ریسک مربوط به زیان‌های محتمل بر دارایی‌های مؤسسه براساس تغییرات و نوسانات عوامل بازار (مانند نرخ ارز، نرخ بهره، قیمت سهام و ...)

۳- ریسک عملیاتی: عموماً ناشی از اشتباهات انسانی یا اتفاقات و خطای تکنیکی تعریف می‌شود. این ریسک شامل تقلب (موقعیتی که معامله‌گرها اطلاعات غلط می‌دهند)، اشتباهات مدیریتی و فرایندهای ناکافی یا ناصحیح داخل سازمان می‌باشد. خطای تکنیکی ممکن است ناشی از نقص در اطلاعات، پردازش معاملات، یا به طور کلی هر مشکل دیگری که در سطح سازمان روی می‌دهد، باشد. ریسک‌های عملیاتی ممکن است منجر به ریسک‌های اعتباری و بازار شوند.

٤- ریسک قانونی: زمانی مطرح می‌شود که یک معامله از نظر قانونی قابل انجام نباشد. ریسک قانونی در کل با ریسک اعتباری مرتبط است زیرا طرفین معامله در صورت زیان در یک معامله به دنبال بستر قانونی برای زیر سؤال بردن اعتبار معامله می‌گردند.

۵- ریسک کفایت سرمایه: عموماً ابعاد مختلف ریسک در شرکت‌های مالی به طور مستقیم یا غیر مستقیم تحت تأثیر هزینه سرمایه و میزان سرمایه است. سرمایه یکی از عوامل کلیدی در تعیین میزان امنیت بانک‌ها و مؤسسات مالی و اعتباری است. سرمایه کافی در شرکت‌های مالی به عنوان یک ابزار امنیتی برای سایر ابعاد ریسک در

طول دوره فعالیت تجاری بانک و مؤسسه است. سرمایه، نقاط ضعف محتمل در سایر ابعاد مالی شرکت را جذب می‌کند. لذا، سرمایه مبنایی برای حفظ تأمین‌کنندگان منابع مالی شرکت به‌حساب می‌آید.

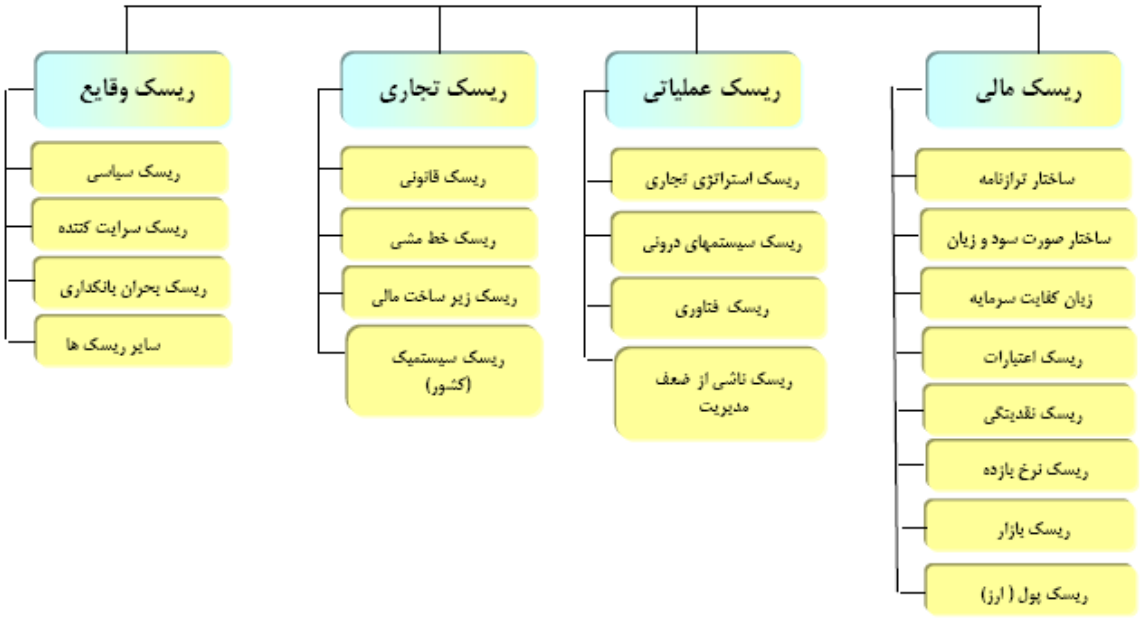
٦- ریسک نرخ بازده: ریسک نرخ بازده عبارت است از تغییری که در ارزش اوراق قرضه ناشی از تغییر در نرخ بازده آن اتفاق می‌افتد. از طرف دیگر احتمال تغییر در دریافت‌های آتی حاصل از فروش یک اوراق بهادار و همچنین عدم توان پرداخت سود در آن به ریسک بازده اشاره دارد. توان تولید شرکت، تغییر در تقاضا و شرایط رقابتی، تغییر در ریسک ملی و ساختار اقتصادی، ریسک سیاسی، همه و همه می‌تواند سود شرکت‌ها و به تبع آن توان پرداخت سود بیشتر به اوراق بهادار را تحت تأثیر قرار دهد. به نوعی که تمامی تغییرات احتمالی در وقایع بازرگانی، در نهایت تأثیر خود را در ریسک سهام به جا می‌گذارد.

۷- ریسک نقدینگی: ریسک نقدینگی دارایی، که با نام ریسک نقدینگی بازار محصول هم شناخته می‌شود، زمانی ظاهر می‌شود که معامله با قیمت پیش‌بینی‌شده قابل انجام نباشد (به دلیل تغییر وضعیت نسبت به زمان معامله عادی). این ریسک در بین گونه‌های دارایی‌ها و در زمان وابسته به شرایط بازار تغییر می‌کند. بعضی دارایی‌ها مانند ارزهای اصلی یا اوراق قرضه، بازارهای عمیقی دارند و در اغلب مواقع به راحتی با نوسان کمی در قیمت، نقد می‌شوند اما این امر در مورد همه دارایی‌ها صادق نیست. در مورد بانک‌ها، ریسک نقدینگی به دلیل کمبود و عدم اطمینان در میزان نقدینگی بانک ایجاد می‌شود. حالت دیگری که باعث افزایش ریسک نقدینگی می‌شود این است که بازارهایی که منابع بانک در آنها قرار دارد دچار کمبود نقدینگی شوند. ریسک نقدینگی با سایر ریسک‌های مالی مختلط است و به همین دلیل سنجش و کنترل آن با دشواری روبرو است.

۸- ریسک پول یا نرخ ارز: ریسک نرخ ارز عبارت است از احتمال از دست دادن اصل و فرع سرمایه به دلیل کاهش قدرت خرید پول. تورم از طرف دیگر نرخ بهره را نیز افزایش می‌دهد. این امر به‌نوبه خود موجب کاهش ارزش اوراق بهادار خواهد شد.

شکل ۱، ریسک‌هایی که بانک‌ها و مؤسسات مالی و اعتباری با آن مواجه هستند را نشان می‌دهد. همانطور که در این شکل مشاهده می‌شود، یکی از عمده مخاطرات ناشی از ریسک عملیاتی، ریسک فناوری است که در این مقاله محور اصلی بحث می‌باشد.

شکل ۱- نمودار ریسک‌های احتمالی بانک‌هاو مؤسسات مالی



مدیریت ریسک‌های عملیاتی با مدیریت ریسک‌های اعتباری و بازار متفاوت است. مؤسسات مالی و اعتباری می‌توانند برای ارزش‌گذاری ریسک عملیاتی گزینه‌هایی را انتخاب کنند و از طریق یکی از رویکردهای زیر آن را ارزیابی کنند:

- رویکرد شاخص مبنا[1] : سرمایه با استفاده از یک شاخص نماینده (مانند درآمد خالص) برای ارائه ریسک عملیاتی کلی، تخصیص داده می‌شود.
- رویکرد استانداردشده : سازمان به خطوط کاری خاص تقسیم می‌شود. هرکدام از این تقسیمات یک شاخص برای خود دارند (مثلاً متوسط سالانه دارایی‌ها، درآمد خالص یا نرخ خطا). این روش نیازمند ردیابی و ردگیری داده‌های ضررها و ارزیابی مدیریت است.
- رویکرد ارزیابی درونی[2] : در این روش از تحلیل‌های ریسک کمی استفاده می‌نماید. سازمان‌های ارائه‌دهنده خدمات مالی نیاز خواهند داشت با توجه به تأثیر سوانح تبادلات بر روی کسب و کار، آنها را دسته‌بندی نمایند. پایگاه داده‌های «ضررها» برای محاسبه احتمال و شدت خسارت مورد انتظار در هرکدام از خطوط کسب و کار مورد استفاده قرار می‌گیرد. هزینه سرمایه بر مبنای تجربه خسارت‌های عملیاتی در یک چارچوب ارزیابی شارژ می‌شوند.

[1] Basic Indicator Approach
[2] Internal Measurement Approach

فن‌آوری اطلاعات و مدیریت مخاطرات ناشی از آن:

عصر کنونی را بایستی بدون شک عصر اطلاعات و ارتباطات نامید. گسترش روزافزون فن‌آوری ارتباطات و اطلاعات[۳] و همگراشدن آنها، ظهور اینترنت و رسانه‌های مرتبط گواهی بر این مدعاست. تفاوت این عصر با سایر اعصار را بایستی در سرعت تغییرات فن‌آوری‌ها، و رشد سریع و چشمگیر علوم دانست که همه این‌ها در سایه ارتباطات وسیع و دسترسی همگانی به اطلاعات میسر گردیده‌است. فن‌آوری اطلاعات، به نحو فزاینده‌ای بر چگونگی عملکرد و نحوه کارآیی سازمان‌ها و شرکت‌ها اعم از دولتی و خصوصی اثرگذاشته است، و نقش سیستم‌های مبتنی بر فن‌آوری اطلاعات در انجام کارآمد امور اداری و تجاری انکار ناشدنی است.

در حال حاضر، اطلاعات مهمترین گنجینه برای سازمان‌ها و اشخاص به حساب می‌آید و از بین رفتن و حتی آسیب‌دیدن آن منجر به صرف زمان، هزینه و نیروی کار غیر قابل تصوری جهت دستیابی به آنها می‌شود و در برخی موارد اصول کاری و موجودیت یک سازمان را مورد تهدید قرار می‌دهد. فن‌آوری اطلاعات همانند سکه می‌تواند دو رو داشته باشد، هم فرصت و هم تهدید! اگر به همان اندازه‌ای که به فکر توسعه و فراگیری آن هستیم، به ایمن‌سازی آن توجه نکنیم، می‌تواند به سادگی تبدیل به یک تهدید و مصیبت بزرگ شود. تجسم مسائل زیر می‌تواند ما را در درک بهتر موضوع یاری رساند:

- مبالغ حساب‌ها با هک شدن اطلاعات حساب‌های بانکی، کلمات عبور کارت‌های بانکی و ... جا به جا شود.
- اطلاعات موجود در ثبت اسناد و املاک جا به جا شده، تغییر یابد و یا حذف شود.
- دانش فنی یک کارخانه که با یک فرمولاسیون خاص دارای برند خوبی است، به سرقت رود.
- تمامی اطلاعات دانشجویان یک دانشگاه دستکاری شده و یا تغییر یابد و یا امکان دستیابی در نتایج آزمون‌های ورودی به دانشگاه‌ها فراهم شود.
- و نظایر آن ...

بنابراین IT به همان اندازه که باعث رفاه و افزایش توانمندی‌های ما می‌شود، می‌تواند خطرناک باشد و سازمان و حتی کشور را فلج نماید. لذا جهت حفظ اطلاعات و مدیریت آنها و جلوگیری از هر گونه سوء استفاده می‌بایست بر اساس آخرین دستاوردهای روز دنیا و استانداردهای مربوطه نسبت به ایمن‌سازی آن اقدام کرد.

همان‌طور که سیستم‌های مبتنی بر ICT و IT امروزه به عنوان اصلی‌ترین عامل مؤثر در تعیین برنامه‌ها و تصمیم‌گیری‌های سازمان شناخته می‌شود، بهره‌گیری از فن‌آوری اطلاعات در مدیریت ریسک و به تبع آن بکارگیری تکنیک‌های مدیریت

۳Information & Communication Technology (ICT)

ریسک در فن‌آوری اطلاعات می‌تواند تأثیری شگرف بر چگونگی سر و سامان دادن به فعالیت‌های سازمان‌ها و مدیریت سیستم‌های مکانیزه داشته باشد.

اطلاعات و مدیریت امنیت آن:

اطلاعات، به‌لحاظ معنایی طیف متنوعی را از کاربرد روزمره تا محیط‌های فنی دارد. اطلاعات مجموعه‌ای از آگاهی‌هاست، اطلاعات چی، کجا، چطوری یک موضوع است و به معنای جزئیاتی است که در موضوعی به آن نیاز داریم. در علوم رایانه اطلاعات، داده‌های پردازش شده است که دارای ارزش و اعتبار می‌باشد. همان‌طور که در بخش‌های گذشته به آن اشاره شد، نیاز روزافزون به اطلاعات و استفاده از فن‌آوری‌های اطلاعات و ارتباطات در تمامی سازمان‌ها و بنگاه‌های اقتصادی و بخصوص بانک‌ها و مؤسسات مالی و اعتباری و تهدیدات ناشی از بکارگیری آن، ضرورت داشتن یک نظام مدیریت امنیت اطلاعات را بیش از پیش بر ما نمایان می‌سازد.

همانگونه که اشاره شد، ریسک‌هایی که هر سازمان با آن مواجه است، بسته به زمینه فعالیت آن متفاوت است (گرچه ریسک‌های مشترکی نیز در این میان وجود دارد). شکل ۲ میزان نسبی مخاطره‌پذیری سیستم‌های اطلاعاتی را بسته به نوع فعالیت آن سازمان نشان می‌دهد.

شکل ۲- میزان نسبی در معرض ریسک بودن یک سیستم اطلاعاتی در بخش‌های مختلف

زیاد (بالاتر)	متوسط	پایین (کم‌تر)
دولت	خودروسازی	کشاورزی
هوا - فضا و دفاع	شیمی	ساختمان‌سازی و معاملات املاک
زیست‌پزشکی	انرژی، نفت و گاز	غذا و دخانیات
الکترونیک	حمل ونقل	تجهیزات صنعتی
خدمات مالی	عمده فروشی	معادن و مواد معدنی
بهداشت و سلامت		
خدمات اطلاعات		
داروسازی		
خرده فروشی		

واضح است که عدم توجه به تأمین امنیت فضای تبادل اطلاعات و برخورد نادرست با این مقوله، مانعی بر سر راه گسترش فضای مذکور در جامعه و جلب اعتماد مدیران در بکارگیری روش‌های نوین نظارتی و اطلاع‌رسانی خواهد شد. به همین

جهت است که ضرورت ایجاد یک نظام منسجم در سطح ملی در خصوص فضای تبادل اطلاعات و ایجاد امنیت آن با در نظر گرفتن ویژگی‌های خاصی که دارد، بیش از پیش مشخص می‌شود. برخی از این ویژگی‌ها عبارتند از اینکه:

- امنیت فضای تبادل اطلاعات، مفهومی کلان و مبتنی بر حوزه‌های مختلف دانش است.
- امنیت، با توجه به هزینه و کارایی تعریف می‌شود و مقوله‌ای نسبی است.
- امنیت، متأثر از مجموعه آداب، سنن و اخلاقیات حاکم بر جامعه است.
- امنیت در فضای تبادل اطلاعات، از روند تغییرات سریع فن‌آوری‌های مرتبط تأثیرپذیر است.

امنیت اطلاعات به مفهوم حفاظت و مراقبت از اطلاعات و سیستم‌های اطلاعاتی در مقابل هرگونه مخاطره و تهدید است. مخاطرات و تهدیدهای این حوزه شامل دسترسی، کاربرد، افشاء، قطع، تغییر یا انهدام غیر مجاز اطلاعات است. استاندارد ISO 27001 ، امنیت اطلاعات را حفظ محرمانگی، جامعیت یا صحت، و در دسترس بودن اطلاعات در مقابل مخاطرات، تهدیدها و آسیب‌پذیری‌ها تعریف می‌کند. جامعیت[٤]اطلاعات به مفهوم تأمین نمودن درستی و تمامیت اطلاعات و روش‌های پردازش است به عبارت دیگر اطلاعات فقط توسط افراد مجاز قابل تغییر باشد. محرمانگی[٥]بیان می‌دارد اطلاعات فقط در دسترس افرادی است که مجاز به دسترسی به آنها هستند و در دسترس بودن[٦]به معنای دسترسی به اطلاعات توسط کاربر مجازاست، زمانی‌که نیازمند آن اطلاعات است. علاوه براین‌ها سایر ویژگی‌ها از قبیل اصالت[٧] قابلیت جوابگویی و اعتبار[٨] انکارناپذیری[٩] و قابلیت اطمینان[١٠]اطلاعات نیز می‌توانند مشمول این حفاظت باشند.

در این راستا، امنیت اطلاعات از طریق اجرای مجموعه‌ای از کنترل‌ها که شامل سیاست‌ها، عملیات، رویه‌ها، ساختارهای سازمانی و فعالیت‌های نرم‌افزاری است، حاصل می‌شود. این کنترل‌ها باید به‌منظور اطمینان از تحقق اهداف امنیتی مشخص هر سازمان برقرار شوند.

نظام مدیریت امنیت اطلاعات

بیشتر سازمان‌ها در مواجهه با تهدیدات امنیتی، سیاست خرید محصولات امنیتی مانند دیواره آتش[١١]و برنامه‌های ضد ویروس[١٢]و بکارگیری آنها در سیستم‌های رایانه‌ای را دنبال می‌کنند. اما استفاده از گران‌قیمت‌ترین محصولات امنیتی بدون

٤ Integrity
٥ Confidentiality
٦ Availability
٧ Authenticity
٨ Accountability
٩ Non- repudiation
١٠Reliability
١١Fire Wall
١٢Anti Virus

شناخت و تحلیل دقیق نیازهای امنیتی، و استفاده از رویه‌های استاندارد در بکارگیری و کنترل سیستم‌های امنیتی و به‌روزرسانی مداوم این سیستم‌ها به تنهایی کارساز نخواهند بود.

نظام مدیریت امنیت اطلاعات (ISMS)[۱۳]در مجموع یک رویکرد نظام‌مند به مدیریت اطلاعات حساس بمنظور محافظت از آنهاست. نظام مدیریتی مذکور باید شامل روش‌های ارزیابی، محافظت، مستندسازی و بازنگری باشد، که این مراحل در قالب یک چرخه بهبود مستمر (PDCA)[۱۴]تحقق‌پذیر است. (چرخه یادشده که به چرخه دمینگ نیز معروف است، نقش محوری در تشریح و تحقق استانداردهایISO دارد.)

استانداردهای BS7799 و ISO 27001 استانداردهای بین‌المللی برای استقرار و بهبود سیستم مدیریت امنیت اطلاعات در سازمان‌ها به شمار می‌آیند. تاریخچه ورود این استانداردها با BS7799 شروع شده است که در دوره خود کامل‌ترین و معروف‌ترین استاندارد در این زمینه بوده است. این استاندارد در سال ۱۹۸۷ توسط مؤسسه CCSC[۱۵]تدوین گردید، سپس با توجه به گذشت زمان و تجارب مختلف از سنجش میزان امنیت اطلاعات توسط CCSC و مرکز محاسبات بین‌المللی NCC و یک کنسرسیوم از کاربران، یک نسخه استاندارد امنیت با عنوان مستندات راهبری PD003 در انگلستان منتشر شد و نسخه بازنگری شده این استاندارد در سال ۱۹۹۵ با عنوان استاندارد ISO ثبت گردید.

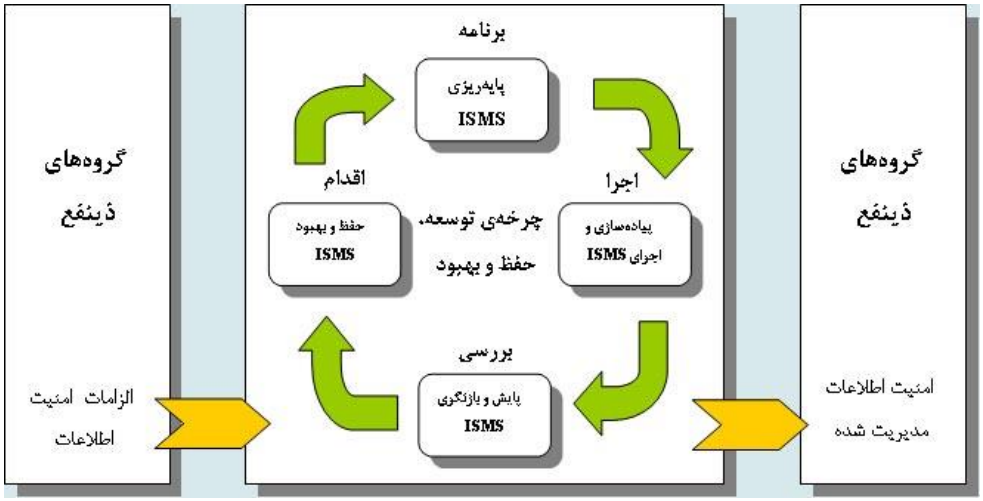
در فوریه سال ۱۹۹۸ نسخه دوم استاندارد BS7799 تحت عنوان سیستم مدیریت امنیت اطلاعات (ISMS) منتشر شد. در سال ۲۰۰۰ با افزودن الحاقیه‌ای به استاندارد BS7799 که به‌عنوان ISO ثبت شده بود این استاندارد تحت عنوان راهنمای اجرای استاندارد امنیت اطلاعات ISO/IEC17799 به ثبت رسید. استاندارد BS7799 در سال ۲۰۰۲ مجدداً مورد بازنگری قرار گرفت و در نهایت آخرین نگارش استاندارد ISMS در ۲۸ ژوئن سال ۲۰۰۵ تحت عنوان ISO/IEC FDIS (Draft BS7799-2:2005) ۲۷۰۰۱:۲۰۰۵ توسط کمیته IST/33 سازمان بین‌المللی استاندارد ISO منتشر شد.

استقرار و اجرای سیستم مدیریت امنیت اطلاعات

فعالیت‌های مربوط به پیاده‌سازی سیستم مدیریت امنیت اطلاعات بر اساس چرخه دمینگ[۱۶]به همراه گروهای ذینفع و روابط آنها با یکدیگر در شکل ۳ و جدول ذیل آن نشان داده شده‌است.

۱۳- Information Security Management System
۱۴- Plan-Do-Check-Act
۱۵- Commercial Computer Security Center
۱۶- Deming Cycle

شکل ۳- مدل سیستم مدیریت امنیت اطلاعات



فعالیت‌هایی که در هر مرحله از استقرار سیستم اجرا می‌شوند عبارتند از:

Plan (برنامه‌ریزی)	– تعریف چشم‌انداز نظام مدیریتی و سیاست‌های امنیتی سازمان. – تعیین و ارزیابی مخاطرات. – انتخاب اهداف کنترل و آنچه سازمان را در مدیریت این مخاطرات یاری می‌کند. – آماده‌سازی شرایط اجرایی.
Do (انجام)	– تدوین و اجرای یک طرح برای تقلیل مخاطرات. – اجرای طرح‌های کنترلی انتخابی برای تحقق اهداف کنترلی.
Check (ارزیابی)	– استقرار روش‌های نظارت و پایش. – هدایت بازنگری‌های ادواری به‌منظور ارزیابی اثربخشی ISMS. – بازنگری درحد قابل قبول مخاطرات. – پیشبرد و هدایت ممیزی‌های داخلی به‌منظور ارزیابی تحقق ISMS.
Act (بازانجام)	– اجرای توصیه‌های ارائه شده برای بهبود. – نظام مدیریتی مذکور. – انجام اقدامات اصلاحی و پیشگیرانه. – ارزیابی اقدامات صورت پذیرفته در راستای بهبود.

همانند نظام‌های مدیریت کیفیت، نظام مدیریت امنیت اطلاعات نیز در دو بخش فرایندها و محصولات مطرح است. بخش فرایندها بر طراحی و اجرای دستورالعمل‌های مدیریتی به‌منظور برقراری و حفظ امنیت اطلاعات استوار است و بخش محصولات، یک نظام مدیریتی است که سازمان به‌منظور بکارگیری محصولات نرم‌افزاری معتبر در زیرساخت‌های فناوری اطلاعات خود برای برقراری و حفظ امنیت اطلاعات خویش از آن بهره می‌گیرد. چیزی که این دو بخش را به هم پیوند

می‌دهد میزان انطباق با بخش‌های استاندارد است که در یکی از چهار رده حفاظت ناکافی، حفاظت حداقل، حفاظت قابل قبول و حفاظت کافی قرار می‌گیرد.

پیاده‌سازی ISMS در یک سازمان مراحل ذیل را در بر می‌گیرد:

- آماده‌سازی اولیه: حصول اطمینان از همراهی مدیریت ارشد سازمان، انتخاب و آموزش اعضای تیم راه‌انداز.
- تعریف نظام مدیریت امنیت اطلاعات: شامل تعریف چشم‌انداز و چهارچوب نظام در سازمان است.
- ایجاد سند سیاست امنیت اطلاعات: شامل مجموعه‌ای از عبارات اجرایی در جهت پیشبرد اهداف امنیتی سازمان.
- ارزیابی مخاطرات: شناسایی و ارزیابی سرمایه‌هایی که نیاز به محافظت دارند و تعیین میزان آسیب‌پذیری اطلاعات و سرمایه‌های فیزیکی مرتبط.
- آموزش و آگاهی‌بخشی: کاهش آسیب‌پذیری کارکنان مؤثر در حلقه امنیت اطلاعات از طریق آموزش.
- آمادگی برای ممیزی: آگاهی از نحوه ارزیابی چارچوب مدیریتی سازمان و فراهم نمودن آمادگی برای انجام ممیزی.
- ممیزی: شناسایی شرایط لازم برای اخذ گواهینامه در سازمان.
- کنترل و بهبود مستمر: کنترل و ارتقاء اثربخشی نظام مدیریتی پیاده‌سازی شده، مطابق مدل به‌رسمیت شناخته شده.

نتیجه‌گیری

متأسفانه مقوله امنیت در ایران چندان جدی گرفته نشده و حداکثر محدود به فروش و نصب دیواره آتش و آنتی‌ویروس است. اما در چند سال اخیر سازمان‌های معدودی اقدام به پیاده‌سازی راهکارهای امنیتی و استقرار استاندارد مدیریت امنیت اطلاعات نموده‌اند. امید است این استاندارد به کوشش سازمان‌ها و نهادهای وابسته و صاحب‌نظران حوزه فن‌آوری اطلاعات و سیستم‌های مدیریتی به شکل مؤثرتری بررسی و کاربردی شود.

هر چند بکارگیری نظام مدیریت امنیت اطلاعات و اخذ گواهینامه‌های مربوطه به‌تنهایی نشان‌دهنده برقراری امنیت کامل در یک سازمان نیست، اما استقرار این نظام مزایایی دارد.

- در سطح سازمانی، تضمینی است برای التزام به اثربخشی تلاش‌های امنیتی در همه سطوح و نمایشی از تلاش‌های مدیران و کارکنان سازمان در این زمینه است.
- در سطح قانونی، اخذ گواهینامه به اولیای امور ثابت می‌کند که سازمان تمامی قوانین و قواعد اجرایی در این زمینه را رعایت می‌کند.
- در سطح اجرایی، استقرار این نظام باعث اطلاع دقیق‌تر از سیستم‌های اطلاعاتی و ضعف و قوت آنها می‌شود. علاوه‌بر این چنین سیستمی استفاده مطمئن‌تر از سخت‌افزار و نرم‌افزار را تضمین می‌کند.

- در سطح تجاری، تلاش‌های مؤثر سازمان به منظور حفاظت از اطلاعات، اطمینان خاطر بیشتری را در شرکا و مشتریان فراهم می‌آورد.
- در سطح مالی، این اقدام باعث کاهش هزینه‌های مرتبط با مسائل امنیتی و کاهش احتمالی حق بیمه‌های مرتبط می‌شود.
- در سطح پرسنلی، افزایش آگاهی ایشان از نتایج برقراری امنیت اطلاعات و مسئولیت‌های آنها در مقابل سازمان از مزایای بکارگیری چنین نظامی است.

منابع

۱- جورج سادوسکای و دیگران، **راهنمای امنیت فناوری اطلاعات**، گروه مترجمین مهدی میردامادی، زهرا شجاعی، محمدجواد صمدی، دبیرخانه شورای عالی اطلاع‌رسانی، چاپ اول، ۱۳۸٤

۲- دشتی، افسانه، " استانداردهای امنیت، آشنایی با استاندارد BS7799"، ماهنامه شبکه، شماره ٥٤، خرداد ۱۳۸٤

۳- ذاکری، اسلامیان، "نگاهی اجمالی بر مدیریت ریسک در سیستم بانکی"، اداره آمار و برنامه‌ریزی بانک سینا، فروردین ماه ۱۳۸۸

٤- محمدی نوده، عبدالرحمن، " نقش فن‌آوری اطلاعات در مدیریت ریسک"، www.itiran.com

٥- "نظام مدیریت امنیت اطلاعات (ISMS)"، شرکت بهبود صنعت مهرگان www.behboudsanat.com

٦- شبکه اطلاع‌رسانی قاصدک، www.ghasedak.com

۷- سلیمانی، محسن، "مدیریت ریسک در مبادلات الکترونیک"، راهکار مدیریت، www.mgtsolution.com

۸- پورمند، علی، " استانداردی برای مدیریت امنیت اطلاعات"، خبرگزاری فارس

۹- نوده فراهانی، محمدرضا، "مدیریت ریسک‌های استراتژیک لیزینگ"، روزنامه سرمایه، شماره ۹۰۲، سال ۱۳۸۷

۱۰- نوده فراهانی، محمدرضا، "پیمان بین‌المللی نظارت بر امور بانکی (بازل)"، فصلنامه تخصصی داخلی ره‌آورد لیزینگ، شماره ٤، سال ۱۳۸۹