ششمین همایش ملی تجارت و اقتصاد الکترونیکی

ضرورت پیاده سازی ISMS در بانکداری الکترونیک

علیرضا دهقان، عضو هیات علمی مجتمع آموزش عالی کازرون، Dehghan.itsu@yahoo.com
پرهام ارجمند، عضو هیات علمی مجتمع آموزش عالی کازرون، Arjomand.itsu@yahoo.com
سارا عباسپور، دانشجوی مهندسی فناوری اطلاعات مجتمع آموزش عالی کازرون[1]، abbasspoor.itsu@yahoo.com

چکیده

اطلاعات به عنوان یک دارایی ارزشمند در تمام فعالیت‌ها چه به صورت فردی و چه سازمانی به شمار می آید که در فضای مجازی به واسطه اتصال به اینترنت و شبکه‌های کامپیوتری نامحدود و وجود تهدیدات امنیتی، همواره در معرض خطر جدی قرار دارد. وجود این خطرات و خسارت‌های احتمالی ناشی از آن سبب شده که سازمان‌ها و شرکت‌های فعال در عرصه تجارت الکترونیک به دنبال ارائه راه‌حل‌هایی برای کاهش این خسارت‌ها باشند. در این راستا ضرورت بکارگیری اقدامات امنیتی مؤثر مورد توجه جدی مدیران سازمان‌ها قرار گرفته است. مجموعه‌ای از استانداردها مانند سری استانداردهای ISO/IEC17799 وجود دارد که به مدیران سازمان‌ها کمک می‌کند تا علاوه بر پیاده‌سازی مناسب سیستم مدیریت امنیت اطلاعات (ISMS)[2]، به طور پیوسته امنیت اطلاعات سازمانی را بهبود بخشند. در این مقاله ضمن بیان اهمیت امنیت اطلاعات و استانداردهای مربوطه جهت اجرای اقدامات امنیتی لازم برای بانکداری الکترونیک، بکارگیری ISMS مبتنی بر استانداردهای امنیتی ISO/IEC17799 که به استمرار چرخه‌ی ایمن سازی فضای تبادل اطلاعات منجر می‌شود، مورد بررسی قرار گرفته؛ سپس ضرورت پیاده‌سازی ISMS در بانکداری الکترونیکی به وسیله تحلیل SWOT تحلیل گردیده و راهکارهایی جهت پیاده‌سازی ISMS در نظام بانکداری الکترونیکی در ایران ارائه شده است.

کلمات کلیدی: امنیت اطلاعات، بانکداری الکترونیک، سیستم مدیریت امنیت طلاعات (ISMS)، SWOT.

۱. مقدمه

اطلاعات یکی از با اهمیت‌ترین متغییرها در کسب‌وکارهای جدید بشمار می‌رود. بنابراین شرکت‌ها و سازمان‌ها باید بسیاری از خطرات امنیتی اطلاعات را رسیدگی کنند، از جمله حملات تروریستی، آتش سوزی، سیل، زلزله و حوادث دیگر که می‌تواند امکانات پردازش اطلاعات و اسناد مهم را نابود کند. سرقت اسرار تجاری و از دست رفتن اطلاعات به علت خاموش شدن ناگهانی کامپیوتر و بازنگه‌داشتن سیستم‌های اطلاعاتی می تواند باعث از بین رفتن مزایای تجاری برای صاحبان کسب‌وکار و ایجاد لطمه به موقعیت اعتباری سازمان شود از این رو حفاظت از اطلاعات یکی از اهداف اولیه برای جلوگیری از ضررهای مالی و تکرار آسیب‌ها

[1] نویسنده مسئول: سارا عباسپور. تلفن: ۰۹۱۷۶۸۷۸۳۴۸
abbasspoor.itsu@yahoo.com فارس، کازرون،خیابان طالقانی مجتمع آموزش عالی کازرون دانشکده فنی مهندسی

[2] Information Security Management System

می‌باشد. تعدادی از معیارهای امنیتی فنی و سازمانی برای حفاظت از محرمانگی، صحت، در دسترس بودن اطلاعات الزامی شده است که در بانکداری الکترونیک این موارد شامل پذیرش فرآیندهای تصدیق ایمنی برای بررسی آخرین تهدیدات می باشد[35]. برای مقابله با تهدیدات راهکارهای متعددی وجود دارد که انتخاب مطمئن‌ترین شیوه حائز اهمیت می باشد. استانداردهای امنیتی تأییدشده توسط سازمان بین المللی استاندارد (ISO)[1] یکی از این روش‌ها می باشد. از میان استانداردهای امنیتی سری استاندارد ISO/IEC27000 پیشنهادهایی مرتبط با مدیریت امنیت اطلاعات برای کسانی که وظیفه طراحی و راه اندازی، پیاده-سازی یا نگه‌داری امنیت در سازمان را بعهده دارند، ارائه می کنند. این استانداردها اصول متداولی را برای شیوه های مدیریتی امنیت دنبال می کنند و به صورت غیر مستقیم عامل بالقوه اعتماد در مبادلات هستند[29] به این دلیل مبادلات در بانکداری از راه دور برای انتقال سرویس‌های مالی به مشتریان اهمیت بیشتری پیدا کرده است و اهمیتش به این خاطر است که این سرویس‌ها با یک روش امن و راحت منتقل شده اند. بنابراین بهتر است بانک های تجاری را مبتنی بر ISO/IEC27000 پیاده سازی کنند زیرا بهترین روش برای عملکردها و فرآیندهای مهم‌شان می باشد[36]. در این تحقیق به دلیل اهمیت موضوع امنیت اطلاعات در بانکداری الکترونیکی، پس از مطالعات و تحلیل و ارزیابی نتایج حاصل از تحقیقات پیشین در زمینه‌ی ISMS و امنیت در بانکداری الکترونیکی، ضرورت پیاده‌سازی ISMS در بانکداری الکترونیکی بوسیله‌ی تحلیل SWOT بررسی شده است.

۲. تعریف بانکداری الکترونیک

بانکداری الکترونیکی نوع خاصی از بانکداری است که جهت ارائه سرویس به مشتریان از یک محیط الکترونیکی (مانند اینترنت) استفاده می کند. در واقع بانکداری الکترونیکی یک سرویس الکترونیکی[2] است که ارائه تمامی عملیات بانکی از طریق این سرویس ها به صورت الکترونیکی انجام می پذیرد و انجام تمامی این عملیات با سطوح امنیتی مناسب محافظت می شود[2]؛ یا به بیان دیگر بانکداری الکترونیکی عبارتست از بکارگیری فناوری های پیشرفته نرم افزاری و سخت افزاری مبتنی بر شبکه و مخابرات برای تبادل منابع و اطلاعات مالی به صورت الکترونیکی که می تواند باعث حذف نیاز به حضور فیزیکی مشتری در شعب بانک شود[13]؛ علاوه بر این بانکداری الکترونیک را با عنوان بانکداری مجازی ارائه می‌نماید زیرا به اعتقاد برخی صاحبنظران، خدمات بانکی توسط ابزارهای جدید، فناوری و با شیوه هایی متفاوت از ابزار بانکداری سنتی ارائه می دهند[18]. طبق گزارش کمیته بازل در نظارت بانکداری در سال1998، بانکداری الکترونیک به ارائه کارها و خدمات بانکی در مقدار کم و جزئی به واسطه کانال های الکترونیکی اشاره می کند. بدین ترتیب در یک تعریف جامع بانکداری الکترونیک موارد سپرده‌های مستقیم، خودپردازها، کارت های اعتباری و بدهی، بانکداری تلفنی، پرداخت الکترونیکی صورتحساب و بانکداری مبتنی بر وب را دربر می گیرد[28].

۳. مزایای بانکداری الکترونیک

مزایای بانکدار الکترونیک از دو دید مشتری و بانک قابل توجه می باشند که در زیر به بیان آنها می پردازیم:
مزایای بانکداری الکترونیک از دید مشتری شامل : کاهش هزینه ها در عملیات و استفاده از سرویس های الکترونیک، افزایش راحتی و صرفه جویی در زمان عملیات بانکی بدون نیاز به شعبه بانکی، سرعت و افزایش دسترسی به اطلاعات، بهبود مدیریت وصول پول، مدیریت حساب در هر زمان، امکان پرداخت قبوض، بررسی حساب با استفاده از دستگاه‌های ATM، ارائه تمامی خدمات بانکی از طریق وب سایت بانک، کاهش هزینه های رفت و آمد به شعبه بانکی[13,31,8,4].

[1] International standards for organization
[2] Electronic Service (E – Service)

همچنین مزایایی که برای بانک در بردارد شامل موارد زیر است: افزایش منافع مالی برای فروشندگان از طریق شبکه و سرویس های آن لاین، کاهش هزینه های شارژ و سرویس ها برای بانک، کامپیوتری شدن باعث افزایش کارآیی سرویس های و وظایف راکد در بهترین زمان، افزایش مزایای اقتصادی و ایجاد فرصت های جدید در فرآیند های بانکی، کاهش کاغذ بازی، بهبود ثبت و مستندات مبادلات و در نهایت می توان گفت سرویس‌های بانکداری الکترونیک بهترین شیوه در پاسخگویی به نیازهای تجارت الکترونیک می باشند[13,31,10,6,5].

۴. امنیت اطلاعات

امنیت اطلاعات در واقع فرآیند محافظت از اطلاعات در برابر طیف وسیعی از تهدیدات، دسترسی و تغییرات غیرمجاز مختلف[7] که با هدف تضمین و تأمین امنیت ادامه فعالیت‌های کاری، به حداقل رساندن ریسک‌های کاری و به حداکثر رساندن میزان بازده سرمایه‌گذاری‌ها و فرصت‌ها صورت می پذیرد[32]. امنیت اطلاعات حفظ محرمانگی، صحت، دردسترس بودن اطلاعات و همچنین سایر مواردی مانند تصدیق هویت، مسئولیت‌پذیری، عدم انکار و قابلیت اطمینان را شامل می شود[30]. امنیت اطلاعات به عنوان پیش نیاز پذیرش و توسعه‌ی فناوری اطلاعات یکی از مهم‌ترین جنبه‌هایی می‌باشد که سازمان‌ها برای توسعه و بهبود اهداف کسب-وکار و حفاظت از دارایی‌های سازمان با بکاربردن رویه‌ها، سیاست‌ها و استانداردها در جهت پیاده‌سازی اهداف سازمان بهره می-گیرند.

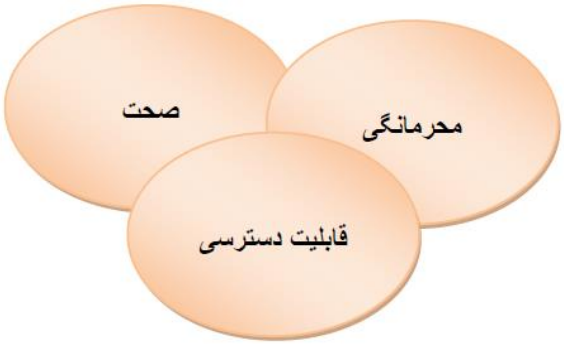
۵. استانداردهای امنیت اطلاعات

تعداد زیادی از سیستم های مدیریت امنیت اطلاعات با دستورالعمل های مربوطه در سراسر دنیا توسعه یافته اند. به عنوان مثال استانداردهای BS 7799 در انگلستان، استاندارد بین المللی و معیار متداول برای ISMS کره با نامDITSCAP و در آمریکا با نام های TCSECو DIACAP و در آلمان با نام ITSEC. بعضی از این ها مانندBS 7799 سیستم ها را توسعه داده اند و با عنوان یک آیین نامه کلی در سازمان بین المللی استاندارد با نام استانداردهای ISO/IEC 17799 به ثبت رسانده اند[16] که آخرین ویرایش آن با نام سری استانداردهای ISO/IEC 27000 شناخته شده است و برای استقرار و بهبود سیستم مدیریت امنیت اطلاعات در شرکت‌ها و سازمان‌های مرتبط با فناوری اطلاعات و تجارت الکترونیک مورد توجه قرار گرفته اند. این استانداردها از لایه‌های بالای مدیریت در یک سازمان تا مدیریت میانی و سایر بخش‌های یک سازمان را مورد بحث قرار می دهند. سری استاندارد ISO/IEC 27000 در واقع توصیفی از چارچوبی برای ISMS که به صورت بین المالللی سازماندهی شده و در سطوح بالا مورد ملاحظه قرار گرفته است و با گذشت زمان همچنان قابل قبول و انعطاف پذیر می باشد[15]. ما در این مقاله به استاندارد ISO/IEC 27001 که در کل اصول نظارت بر شخص ثالث و تعیین عملیاتی ریسک است و همچنین ISO/IEC 27002 که بستر پیاده سازی ISMS می باشد توجه داریم.

۶. امنیت اطلاعات و بانکداری الکترونیک

همان طور که بیان شد امنیت اطلاعات شامل حفاظت از اطلاعات یا سیستم های اطلاعاتی از دسترسی ها و استفاده غیر مجاز، افشا سازی، قطع، تغییرات و یا خرابی می باشد که برای ایجاد محرمانگی، صحت و در دسترس بودن اطلاعات و یا سیستم اطلاعاتی در نظر گرفته می شود[19]. شکل ۱ این سه مؤلفه اصلی امنیت را نشان می دهد و قابل ذکر است که بسته به نوع

کاربردشان ممکن است اولویت‌های متفاوتی داشته باشند. مثلاً در ارسال اطلاعات شخصی در دسترس بودن مهم نیست اما صحت و محرمانگی مهم هستند[9]. بر اساس گفته Yi-Jen Yang در مقاله ای با عنوان **" امنیت بانکداری الکترونیکی"** امنیت مبادلات را یکی از نگرانی های اولیه تمامی صنایع مبتنی بر اینترنت می داند [27] همچنین Jiaqin Yang و Kh Tanveer Ahmed نیز در مقاله ای با عنوان **" نگرش ها و توسعه های اخیر در بانکداری الکترونیک در ملت های توسعه نیافته بر اساس مطالعه تجربی"** یکی از اولین و مهم‌ترین عامل را در صنعت بانکداری الکترونیک نگرانی های امنیتی معرفی کرده اند[25]. در واقع عملکرد ناکافی امنیت در سیستم های بانکداری الکترونیک مخاطرات غیره منتظره عملیاتی سیستم ها را افزایش می دهد[34]. به طور کلی مخاطرات بانکداری الکترونیکی از کلاه‌برداری، خطای پردازش، قطعی سیستم و یا نتایج حوادث پیش بینی نشده در ناتوانی موسسات برای ارسال سرویس‌ها و محصولات، مبادلات آن لاین، انتقال وجه و ضرب پول الکترونیکی نشأت می گیرد. مخاطرات در تمامی محصولات و ارائه خدمات می توانند نفوذ یابند. این مؤسسات هستند که باید سطح مناسب کنترل های امنیتی را مبتنی بر تشخیص حساس بودن اطلاعات برای مشتری و مؤسسات و البته متناسب با سطح پذیرش مخاطرات در هنگام تأسیس مؤسسه تعیین کنند[25]. هر بانک به اقدام امنیت اطلاعاتی جداگانه ای نیاز دارد که باید به طور خاص برای تمرکز بر مدیریت امنیت اطلاعات ایجاد شود. اقدام امنیت اطلاعاتی باید متناسب با ماهیت و اندازه فعالیت‌های بانک و حجم شیوه های بکارگیری فناوری اطلاعات و کانال های انتقال الکترونیکی باشد. اقدام باید به اندازه کافی در مواردی مانند کارمندان متناسب با رتبه و سطح توانایی شان، ابزارها و تکنیک‌ها مناسب سازی شده باشد [36] بنابراین بانکداری الکترونیک مانند هر سازمان دیگر برای امنیت اطلاعات نیازمند اجرای کنترل های امنیتی است. استانداردهای امنیتی تایید شده توسط سازمان بین المللی مانند سری استانداردهای ISO/IEC27000 جهت تحقق این هدف برای حفاظت و بهبود در نظر گرفته شده اند.



شکل ۱: سه مؤلفه اصلی امنیت[9]

۷. ISMS

با توجه به تعریف سازمان بین المللی استاندارد، ISMS بعنوان یک سیستم مدیریتی شامل ساختار سازمانی، سیاست ها، برنامه ریزی فعالیت ها، مسئولیت ها، شیوه ها، مراحل، فرآیندها و منابع می باشد[36]. ISMS شیوه‌ی پیش‌گیرنده‌ای می باشد که مدیریت را در سطوح بالا و به صورت مداوم و کارآ و امنیت اطلاعات را برای افراد، ساختار و کسب و کار انجام می دهد [33]. برای مدیریت مؤثر امنیت اطلاعات در سازمان سیستم های مدیریت امنیت اطلاعات توسعه یافته اند. سیستم های مدیریت امنیت اطلاعات قادر به اجرا در مشکل های امنیتی مشابه هستند، به علاوه این سیستم ها می توانند به طور پیوسته امنیت اطلاعات در فناوری، مدیریت سخت افزار سیستم‌های اطلاعاتی و نگهداری مهم‌ترین کارکترهای ایمنی سیستم یعنی: محرمانگی، صحت و

قابلیت در دسترس بودن را مدیریت و اجرا کنند[16] . به عبارت دیگر ISMS در برگیرنده‌ی برنامه جامع امنیت اطلاعات سازمان که شامل ارتباط با قسمت های دیگر سازمان نیز می باشد و فرآیندهای ISMS برای اجرا و مستندسازی به صورت سیستماتیک و مدیریت پیوسته روندها برای بهبود ایمنی و قابلیت اطمینان دارایی‌های سازمان قابل اجرا می باشند و همچنین برای تحقق محرمانگی، صحت، در دسترس بودن اطلاعات و بهبود مستمر امنیت اطلاعات در نظرگرفته شده است[20]. ISMS با بکارگیری مدل PDCA برای پیاده سازی، نظارت و بهبود روند پیاده‌سازی ISMS در سازمان و مسائل امنیتی مورد پذیرش بسیاری از سازمان‌ها می باشد.

هدف ISMS اطمینان از تداوم کسب و کار از طریق جلوگیری و به حداقل رساندن اثرات حوادث امنیتی است. اطمینان از ذخیره امن اطلاعات و حفاظت از آن توسط یک سیستم مدیریت که موجب افزایش رقابت با سازمان های دیگر می‌گردد[7]. هدف دیگر آن پیاده سازی نوعی از کنترل‌های امنیتی است که با برقراری زیر ساخت‌های مورد نیاز، امنیت اطلاعات را تضمین نمایند و به این وسیله به مشتریان و دیگر گروه‌های ذینفع درباره‌ی امنیت اطلاعات موجود در سازمان اطمینان خاطر دهند. همچنین این سیستم رهیافت سیستماتیکی را برای اداره و مدیریت اطلاعات حساس با هدف حفاظت از آنها فراهم می‌آورد و کل کارکنان، فرآیندها و سیستم‌های اطلاعاتی یک سازمان را در بر می‌گیرد و به طور خلاصه می توان اینگونه اذعان داشت که این سیستم وظیفه پایه-گذاری، پیاده‌سازی، بهره‌برداری، نظارت، بازبینی، نگهداری و بهبود امنیت اطلاعات را دارا می‌باشد[3].

۸. مزایای ISMS

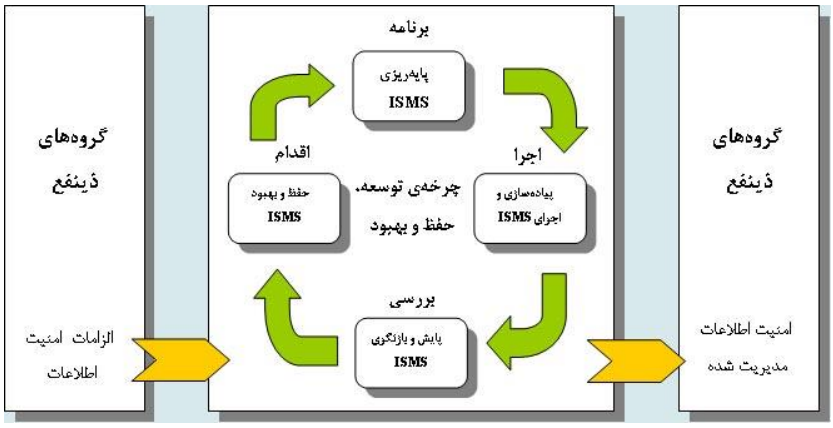
پذیرش استاندارد ISO/IEC17799 که توسط BS7799 تدوین شده و شامل اجرا، پیاده سازی، نظارت و بازرسی ISMS می باشد مزایای مهمی در بسیاری از سطوح فراهم می‌کند که موارد کلی در زیر بیان می گردد: گواهینامه BS7799 بعنوان یک اظهارنامه عمومی از توانایی‌های سازمان برای مدیریت امنیت اطلاعات بکار می رود، با استفاده از ISMS سازمان می‌تواند مطمئن باشد که فرآیند امنیت اطلاعاتش را به شیوه‌ای ساخت یافته اندازه‌گیری و مدیریت می‌کند. شرکت‌ها می‌توانند سیستم خود را به منظور رفع نیازها کنترل کنند. اگر شرکت‌ها چارچوب استاندارد ISMS را اجرا کنند می‌توانند اطمینان یابند که این چارچوب ها از تجربه‌ی دیگران حاصل شده‌اند و اینکه سیستم آزموده شده است و بهترین نتایج را منعکس خواهد کرد. ابزاری است که به مدیریت کمک می‌کند تا اطمینان یابد که امنیت منابع به طور مؤثر برای کسب و کار بکارگرفته شده است و کمیته سازمان را اطمینان می بخشد که ISMS و تداوم سیاست های امنیتی در برابر تغییرات ریسک های آشکارشده بکارگرفته و سازگار شده است. صدور گواهینامه یک علامت تمایز است که سازمان جدای از مزیت رقابتی اعتماد بیشتری به شرکا، ذینفعان و مشتریان می بخشد، نشاندهنده‌ی این که سازمان پیاده سازی مناسب امنیت اطلاعات و کنترل های مداوم کسب و کار را بکارگرفته است، نشان دهنده‌ی تعهد سازمان به حصول اطمینان از ISMS آن و سیاست های امنیتی و در نهایت، نشانه ای از اهمیت پذیرش ISO/IEC17799 که در واقع شروعی برای دعوت به مناقصه بین المللی می باشد[22,38].

۹. چرخه‌ی دمینگ یا مدل PDCA[1]

PDCA چرخه‌ای است که باید به طور مداوم در دراز مدت و با پشتوانه محکمی از مدیریت انجام شود. PDCA گاهی اوقات به عنوان چرخه سیستم مدیریت امنیت اطلاعات نیز نامیده می‌شود[1] این مدل شناخته شده می تواند برای همه‌ی مراحل ISMS به کار گرفته شود که توسط استاندارد ISO/IEC27002 نیز پذیرفته شده است، این استاندارد نیازمندی‌های ISMS

[1] Plan-Do-Check-Act (PDCA)

را فراهم و به سازمان ها برای تنظیم شیوه‌های امنیتی بر اساس مدلPDCA کمک می کند. شکل۱ چگونگی دریافت اطلاعات امنیتی مورد نیاز به صورت ورودی توسط این مدل و برآورده شدن انتظارات اشخاص ذینفع را نشان می‌دهد و از طریق اقدامات لازم و فرآیندهای تولید امنیت اطلاعات خروجی، انتظارات و نیازهای سازمان را برآورده می‌سازد[3].



شکل (۱): مدلPCDA [3]

در زیر اقداماتی که در هر مرحله انجام شده بیان می شود:

- **طراحی (Plan)**

ایجاد خط مشی ISMS، اهداف، فرآیندها و رویه‌های مناسب برای مدیریت ریسک و بهبود اطلاعات به منظور بدست آوردن نتایج بر طبق تمامی خط مشی‌ها و اهداف یک سازمان.

- **اصلاح (Do)**

انجام و اداره‌ی خط مشی‌ها، کنترل‌ها، فرآیندها و رویه‌های ISMS.

- **ارزیابی (Check)**

ارزیابی و ملاک قابل قبول، میزان کارایی فرآیند در برابر خط مشی ISMS، اهداف و تجربیات عملی و گزارش نتایج به مدیریت برای بازدید.

- **اصلاح (Act)**

اصلاح کردن و اعمال پیشگیری مبتنی بر نتایج ممیزی داخلیISMS و مدیریت نظارت یا سایر اطلاعات وابسته، برای دستیابی به بهبود و پیشرفت داخلی ISMS.

۱۰. ضرورت بکارگیری ISMS در بانکداری الکترونیک

صاحبان کسب و کارهای جدید متمایلند برای انتقال خدمات و سرویس‌ها به مشتریان از شیوه های نوین توسط سرویس های الکترونیکی استفاده کنند[14,23]. اما این روش‌ها برای سیستم های اطلاعاتی و شبکه‌های سازمان تهدیدات و آسیب های

گسترده‌ای را در پی دارد. افزایش تهدیدات موضوع مهمی در اجرای اقدامات امنیتی می باشد که دلیلی برای عملی کردن دستورالعمل‌ها در همه‌ی همکاری های جامعه اطلاعاتی است[39]. از جمله این راهنمایی هایی اقدامات مهم و کاربردی، بکارگیری استانداردهای امنیتی مانند ISO/IEC27002 می باشد که به سازمان ها کمک می کند تا شیوه‌هایشان و فرآیندهای مدیریت امنیت اطلاعات را به حد کمال برسانند. بواسطه‌ی این اقدامات و راهنمایی‌ها در ISMS علاوه برفعالیت های آگاهانه امنیتی، کارکنان بیشتر با مفهوم امنیت اطلاعات آشنا می شوند[15] زیرا یکی از انواع تهدیدات امنیت اطلاعات درون سازمانی منابع انسانی سازمان هستند که بر اساس عدم آگاهی و آموزش کافی باعث بروز مشکلات امنیتی می شوند. ISMS برای مدیریت اطلاعات مربوط به مشتریان و سازمان بوسیله‌ی دولت یا سازمان های کسب و کار پیشرو در تجارت الکترونیک، شبکه های موبایل و بانکداری اینترنتی، استفاده می شود[16]. ISMS تأثیر و تحول بسیار در بخش فناوری اطلاعات دارد و ممکن است عامل بالقوه-ای برای راه اندازی مهندسی مجدد فرآیند کسب و کار و به طور مشابه تغییرات عمیق سازمانی در سیستم هایشان باشد. به گفته‌ی لرگیس، اینگهام و کلرت در سال۲۰۰۳ سازمان ها هر ساله به طور قابل توجهی برای خرید و به روز رسانی ساختارهای سیستم های اطلاعاتی شان هزینه می‌کنند. باتوجه به گرایش و رشد تجارت، صنعت بانکداری نیز با طرح‌های فنی مختلف به جایگزینی و ارتقای سرویس‌هایشان برای دسترسی عمومی و افزایش انتقال خدمات به مشتریان از راه دور به روز شده اند[11,21] که این سیستم ها و تکنولوژی های مورد استفاده در سرویس ها خدمات بانکی را توسط انواع جدید بانکداری مانند بانکداری الکترونیک، موبایل بانک، بانکداری اینترنتی و غیره ارائه می کنند. از آنجا که بانکداری الکترونیکی یکی از جامع ترین روش‌های تجارت و تبادلات مالی است ایمنی و ایجاد اعتماد از مهمترین الزامات و جز جدانشدنی در این روش محسوب می باشد. بانک این سیستم جامع برای تحقق بانکداری الکترونیکی به استفاده از استانداردهای مدیریتی و امنیتی نیاز دارد. یکی از این مجموعه استانداردهای مدیریتی و فنی ایمن‌سازی فضای تبادل اطلاعات استانداردهای ISO/IEC27000 می باشد. هدف از تدوین این استانداردها ارائه پیشنهاداتی در زمینه مدیریت امنیت اطلاعات برای کسانی است که مسئول طراحی، پیاده سازی یا پشتیبانی مسائل امنیتی در یک سازمان می باشند. از مجموعه استانداردهای بین المللی، استاندارد ISO/IEC27000:2005 به نام ISMS شناخته شده است و با توجه به ویژگی رویکرد مبتنی بر فرآیندی ISMS پذیرش آن یک تصمیم راهبردی برای سازمان محسوب می شود و برای تحقق هدف امنیت در بانکداری الکترونیک می تواند انتخاب مناسبی باشد که به سازمان‌ها اجازه می دهد انعطاف‌پذیری عملیاتی فرآیندهای مناسب آن سازمان را دنبال کنند؛ این عملیات شامل درک نیازمندی‌های امنیت اطلاعات کسب‌وکار، ایجاد سیاست های و اهداف مناسب، پیاده‌سازی و مدیریت مناسب اصول حفاظتی (از طریق اندازه گیری معنی دار)، نظارت و بررسی عملکرد مؤثر ISMS و حصول اطمینان از اینکه سیستم به طور مدام بهبود می یابد[15,38].

استاندارد ISO/IEC27002 بطور خاص سازمان‌ها را در ایجاد برنامه های امنیتی جامع و مقرون به صرفه کمک می‌کند، همچنین تضمین کننده‌ی این که منابع امنیتی آگاهانه اجرا شده و پیشنهادات بر روی فعالیت‌هایی متمرکز شده است که ریسک‌های موجود کسب‌وکار را کاهش می دهد. سرمایه گذاری در پذیرش ISO/IEC27002 بازدهی بالا را نتیجه می دهد[12]. تحقیقات اخیر نشان می دهد که پیاده سازی ISMS بر اساس استانداردISO/IEC27000 در سازمان‌ها رشد ۳۳ درصدی در سال۲۰۰۷ نسبت به ۲۰۰۶ داشته وتعداد ۵۷۹۷ گواهی نامه اخذ شده است[24]. پیاده سازی این استاندارد سبب خواهد شد که امکان سو استفاده از اطلاعات و از بین رفتن آن و سایر خطرات به حداقل برسد. با پیاده سازی استانداردISO/IEC27000 سازمان قادر به اخذ گواهینامه ی امنیت اطلاعات می باشد.

۱۱. تحلیل ماتریس SWOT بانکداری الکترونیک بر اساس بکارگیری ISMS

در این تحقیق به منظور تدوین استراتژی‌هایی برای ارتقای سیستم امنیت در بانکداری الکترونیکی، تحلیل جامعی از وضعیت موجود براساس تحلیل SWOT صورت گرفته و بر اساس آن نقاط قوت و ضعف به عنوان عوامل داخلی، فرصت‌ها و تهدیدها به عنوان عوامل خارجی که بر پیاده‌سازی بانکداری الکترونیکی تأثیر می‌گذارند مشخص شده‌اند و بر اساس آنها استراتژی‌هایی جهت استفاده از نقاط قوت برای بهره‌گیری از فرصت‌ها، بهره‌برداری از فرصت‌ها برای بهبود بخشیدن نقاط ضعف داخل سازمان، کاهش اثرات ناشی از تهدیدات موجود در محیط خارجی با استفاده از نقاط قوت داخل سازمان و کم کردن نقاط ضعف داخلی و پرهیز از تهدیدات ناشی از محیط خارجی ارائه شده است.

جدول۲: تحلیل های داخلی ماتریس SWOT

Strengths	Weakness
❖ توجه مدیران ارشد بانکداری به موضوع توسعه بانکداری الکترونیک ❖ وجود نیروهای متخصص در طراحی نرم افزارهای بانکی ❖ تغییر در ساختار عملیات بانکی و پیرو آن در بانکداری الکترونیک جهت افزایش رضایت مشتری ❖ امکان جذب مشریان از خارج از کشور ❖ افزایش قدرت بانک در مدیریت وجوه ❖ تمرکز بر کانال های توزیع جدید ❖ ارائه خدمات اصلاح شده به مشتریان و استفاده از راهبردهای تجارت الکترونیکی در ارائه خدمات ❖ سرعت و راحتی انجام مبادلات برای کاربران ❖ کاهش اشتباهات متصدی بانک و مشتریان	❖ عدم آشنایی با معیارهای امنیتی متأثر در بانکداری الکترونیک ❖ عدم توجه به مسائل امنیتی در بانکداری الکترونیکی ❖ انجام نقل و انتقالات از طرق شبکه‌های کامپیوتری و ایجاد زمینه پیدایش شکاف‌های امنیتی در سیستم‌های بانکداری الکترونیکی ❖ عدم بکارگیری استانداردهای امنیتی تدوین شده توسط سازمان بین‌المللی استاندارد و کمیسیون بین‌المللی الکتروتکنیک (IEC)[1] در مورد بانکداری الکترونیک ❖ عدم وجود بسترهای امنیتی مثل بستر امضای دیجیتال و زیر ساخت کلید عمومی[2] (PKI) ❖ امکان سوء استفاده از حساب های بانکی ❖ مقاومت پرسنل و مدیران بانکی در بکارگیری بانکداری الکترونیکی ❖ ضعف مدیریت در بکارگیری و نگهداری متخصصان حرفه‌ای و سطح بالا در بخش IT ❖ عدم توجیه اقتصادی و ریسک‌پذیری لازم برای استفاده از سیستم‌های بانکداری الکترونیکی ❖ عدم اطمینان و قابلیت اطمینان برای کاربران ❖ ریسک تبادلات ارزی ❖ ضعف زیرساخت های امنیتی موجود ❖ هزینه بالای پیاده سازی امنیت و عدم تخصیص بودجه کافی از سوی مدیران

[1] International Electronically Commission
[2] Public Key Infrastructure

جدول۳: تحلیل های خارجی ماتریس SWOT

Opportunities	Threats
❖ اختصاص اعتبارات مختلف دولتی به فناوری اطلاعات برای بخش‌های دولتی ❖ تمایل قانون‌گذاران در تصویب قوانین مرتبط با بانکداری الکترونیک ❖ ایجاد زیر ساخت ها و شاهراه‌های اطلاعاتی پر ظرفیت	❖ عدم شناخت این نوع سیستم‌های و مزیت‌های آن توسط کاربران و مشتریان سنتی بانک‌ها ❖ نبود بستر مخابراتی مناسب شامل شبکه ها و خطوط ارتباطی پر سرعت و ایمن ❖ نبود روش های رسیدگی به شکایات و تخلفات در بانکداری الکترونیکی ❖ دسترسی افراد غیرمجاز به اطلاعات صاحبان حساب‌ها ❖ دسترسی صاحبان حساب به اطلاعاتی بیش از حد مجاز ❖ امکان سوء استفاده از حساب شخصی مشتریان در حین تبادل اطلات روی شبکه های کامپیوتری ❖ حملات ناشی از ویروس و غیره

جدول (۴): استراتژی برای بیان ضرورت پیاده سازی سیستم مدیریت امنیت اطلاعات در بانکداری الکترونیک

	S	W
O	❖ افزایش سطح قابلیت اطمینان برای سیستم‌های بانکداری الکترونیکی با استقرار ISMS ❖ پیاده‌سازی قوانین پیشنهادی از سوی مشاورین حقوقی در زمینه بانکداری الکترونیک با نظارت مدیران بانکی و مشاوران IT ❖ مدیریت مستقیم و پشتیبانی از امنیت اطلاعات با پیاده سازی ISMS ❖ اطمینان از نتیجه دادن روش های پیاده سازی ISMS در بانکداری الکترونیک برای مقابله با مشکلات امنیتی ❖ به‌روز رسانی سیاست‌ها و رویه‌های امنیتی بانکداری الکترونیک ❖ اطمینان از برقراری اهداف و طرح های امنیتی با پیاده سازی ISMS ❖ تهیه الزام های امنیتی و شرح کنترل های متناسب با سیستم بانکداری الکترونیک	❖ تدوین راهکار سیاستی برای توسعه همسان بانک‌ها در بستر بانکداری الکترونیکی ❖ شناسایی قوانین و مقررات موردنیاز و پیگیری برای تصویب آنها ❖ مدیریت ریسک از طریق استقرار ISMS در بانکداری الکترونیک ❖ برگزاری دوره آموزش شناخت سیستم‌های بانکداری الکترونیک به کارمندان و مدیران بانک‌ها ❖ استفاده از راهکارهای تأیید شده امنیتی مانند سری استاندارد های ISO/IEC27000 ❖ استقرار حوزه‌ی مدیریتی کارآمد برای اطمینان از فرآیند موفق مبادلات بانکداری الکترونیک ❖ تخصیص بودجه کافی از سوی مدیران بانک ها برای پیاده‌سازی سیستم های امنیتی در جهت افزایش عملیات بانکداری الکترونیک

T	❖ بهره‌گیری از یک سیستم جامع مدیریتی مانند ISMS جهت بهبود فرآیند مبادلات بانکداری الکترونیک ❖ کوشش در ایجاد اعتماد به مردم برای استفاده از روش های نوین بانکداری ❖ انجام پژوهش‌های آماری مورد نیاز بانکداری الکترونیکی و به روز آوری دانش در این زمینه ❖ استفاده از نیروهای متخصص جهت آموزش نیرو های بانکی با هدف کاهش مخاطرات درون سازمانی ❖ نظارت و کنترل امنیتی برای جلوگیری از صدمه به اعتبار بانک‌ها با پیاده سازی ISMS ❖ مدیریت بانکی برای تحقق خدمات بانکداری الکترونیکی ❖ توزیع زیرساخت امن مستقر شده مبتنی بر ISMS ❖ استفاده از سیاست های امنیتی، اهداف و فعالیت ها که روند کسب و کار بهبود می بخشد.	❖ ایجاد ارتباط قوی با مؤسسات ثالث شبیه بیمه برای تأمین امنیت مبادلات ❖ بکارگیری ISMS جهت هماهنگی در فرآیند مبادلات ❖ اگاهی رسانی جهت پذیرش بیشتر بانکداری الکترونیک برای کاربران ❖ بهبود خدمات ارائه شده با بکارگیری مدل PDCA پذیرفته شده در استاندارد ISO/IEC 27000 ❖ استفاده از سیستم هایی که عملکرد مدیریت امنیت اطلاعات را ارزیابی کرده و بهبود سرویس های بانکداری الکترونیک بر اساس پیشنهادات کاربران ثبت شده در سیستم.

۱۲. نتیجه گیری

با توجه به رشد سریع فناوری اطلاعات و تأثیر آن بر اقتصاد و فرآیندهای مالی بخصوص بانکداری، مزایای رقابتی بسیاری را برای بانک‌ها بوجود آمده است. از این رو توجه به امنیت در شیوه نوین بانکداری یعنی بانکداری الکترونیک بسیار مورد توجه جدی مدیران قرار گرفته است. محدودیت هایی که در بازخورد روش های امنیتی وجود دارد ما را به استفاده از شیوه های امن که نتیجه-ی مطمئن و قابل اجرا را در اختیار گذارد، ملزوم می کند. از راه‌هایی که می توان کنترل‌های امنیتی لازم را در بانکداری الکترونیک بکاربرد استقرار سیستم‌های مدیریتی مبتنی بر استانداردهای بین المللی ISO/IEC27000 می باشد. در این مقاله با در نظر گرفتن و استفاده از استانداردهای بین‌المللی امنیت اطلاعات و همچنین با توجه به ویژگی و مزیت‌های ISMS، بر ضرورت استفاده از امنیت اطلاعات در بانکداری الکترونیک و بررسی مزایای پیاده‌سازی ISMS تأکید گردید و نتایج حاصل از این مطالعه را با استفاده از تحلیل SWOT به بیان استراتژی هایی جهت بکاربردن این روش برای بهبود تهدیدات امنیت اطلاعات در بانکداری الکترونیک پرداخته شد.

منابع

- **مقاله مندرج در مجله علمی:**

[1] محمود زاده، ابراهیم؛ (رادرجبی، ، مهدی). ۱۳۸۵. "مدیریت امنیت در سیستم های اطلاعاتی". *فصلنامه علوم مدیریت ایران* . دوره اول . شماره ی ۴. ص۷۸-۱۱۲.

- **مقاله کنفرانس:**

[2]آتشک، محمد(ماهزاده، ، پریسا). ۱۳۸۷. "بررسی موانع و منابع پیاده سازی بانکداری الکترونیک در ایران". *دومین کنفرانس بانکداری الکترونیک*. تهران.

[3] بحرانی، یزدی(پیام، مهران). ۱۳۸۸. "اهمیت و لزوم سیستم مدیریت امنیت اطلاعات در دولت الکترونیک". *دومین کنفرانس بین‌المللی نظام اداری الکترونیک*. تهران.

[4] حمداله زاده، ساناز (نامی، محمد رضا).۱۳۸۷. "بانکداری الکترونیکی چالش‌ها و ضرورت‌ها"، *دومین کنفرانس بانکداری الکترونیک*. تهران.

[5]صنایعی، علی، (حسینی، امینیان جزی، میرزا حسن، ابراهیم). ۱۳۸۹. "مطالعه تطبیقی بانکداری الکترونیکی و سنتی از نظر امنیت و کاربرپذیری در بانک ملی ایران". *اولین کنفرانس سالانه مدیریت، نوآوری و کارآفرینی*. شیراز.

[6]عمل نیک، محسن صادق، (کشه فراهانی، سمیه). ۱۳۸۶."تدوین استراتژی های بانکداری الکترونیکی با استفاده از ماتریس SWOT"، *پنجمین کنفرانس بین المللی مدیریت*. تهران.

[7] قاسمی شبانکاره، کبرا (مختاری، امینی لاری، وحید، منصور). ۱۳۸۶. "امنیت و تجارت الکترونیکی". *چهارمین همایش ملی تجارت الکترونیکی*، تهران.

[8] یوسفی، مجید (اسماعیلی، جواد).۱۳۸۷. "عدم وابستگی مشتریان به شعبه ای خاص مروری بر وضعیت نظام بانکی کشور و بررسی چالش های پیاده سازی بانکداری الکترونیک". *دومین کنفرانس بانکداری الکترونیک*.تهران.

- کتاب:

[9]فتحیان، محمد (مهدوی نور، سید حاتم). ۱۳۸۷." مبانی و مدیریت فناوری اطلاعات". *دانشگاه علم و صنعت ایران*. ص۳۲۶-۳۲۷.

- پایان نامه:

[10]الهیاری فرد، محمود. ۱۳۸۲. "بررسی مقایسه‌ای خدمات بانکداری سنتی و بانکداری الکترونیک در ایران". *دانشگاه آزاد اسلامی واحد تهران مرکز، دانشکده حسابداری و اقتصاد*.کارشناسی ارشد.

- JOURNALS

[11] Chan, S., (Lu, M.) (2004). Understanding internet banking adoption and use behavior: A Hong Kong perspective. Journal of Global Information Management, 12(3), 21-43.

[12] Gossels, Mackey, (Jr. Jonathan, Richard,) 2007, ISO 2700X: A cornerstone of true security, ISSA Journal The Global Voice of Information Security: Identifying the right standards for your organization.

[13] Gurău, Catalin. (2002) E-banking in Transition Economies. The Case of Romania: Journal of Financial Services Marketing Vol. 6, No. 4, pp. 362–379.

[14] Guriting, P., & Ndubisi, O. N. 2006. "Borneo online banking: Evaluating customer perceptions and behavioural intention". *Management Research News*. Vol.29.pp 6-15.

[15] Hinson, Gary.2009. "How Much is an ISO/IEC 27000-Series Information Security Management System Actually Worth?" *ISSA Journal Preeminent Trusted Global Information Security Community*. pp 30-48.

[16] Jo, Heasuk (Kim , Won, Seungjoo, Dongho). 2011, "Advanced Information Security Management Evaluation System". *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS*. VOL. 5, NO. 6.pp1192-1213.

[17]Legris, P.(Ingham, Collerette J.P.) 2003. "Why do people use information technology? A critical review of the technology acceptance model". *Information and Management*, vol.40. no.2), pp191-204.

[18] Liao, Ziqi (Tow Cheung, Michael). 2002." Internet-Based Banking and Consumer Attitude". *Information Management*. vol.38 Issue5.pp299-306.

[19] Munir, Usman (Manarvi, Irfan). 2010." Information Security Risk Assessment for Banking Sector-A Case study of Pakistani Banks". *Global Journal of Computer Science and Technology (GJCST Classification)* . Vol. 10. Issue 10, Ver. 1.0, pp44-55.

[20] Rezakhani , Afshin (Hajebi, Mohammadi, AbdolMajid, Nasibe). 2011. "Standardization of all Information Security Management Systems". *International Journal of Computer Applications (0975 – 8887)*.Vol 18– No.8, pp4-8.

[21] Sachan, A.,(Ali, A.) 2006. "Competing in the age of information technology in a developing economy: Experiences of an Indian Bank". *Journal of Cases on Information Technology*.vol.8. no.2. pp62- 81.

[22]Saint-Germain , René . 2005. "Information Security Management Best Practice Based on ISO/IEC 17799". *The Information Management Journal*. pp60-66.

[23] Srinivasan, S. 2004. "Role of trust in e-business success". *Information Management & Computer Security* .pp 66-72.

[24]Vaish ,Abhishek (Varma ,Shirshu). 2010. "Parameter Extraction for Measurement of the Effective Information Security Management - Statistical Analysis". *International Journal of Computer and Electrical Engineering*. Vol. 2, No. 4. pp654-659.

[25] VÂRLĂNUȚĂ , FLORINA,(IOAN, MOGA, LILIANA, Viorica). 2008. "Risk management of e-banking activities". . *ANALELE Universitatii DIN-ORADEA Stiint Economic*. pp887-880.

[26]Yang ,Jiaqin, (Ahmed , Kh Tanveer). *2009* . "Recent trends and developments in e-banking in an underdeveloped nation – an empirical study". *Int. J. Electronic Finance, Vol. 3, No. 2. pp115-132.*

- **CONFERENCE**

[27]Yang ,Yi-Jen. 1997. " the security of e-banking". *20th National Information Systems Security Conference*. Maryland.

[28] Al-Jadeed, Mohammed (Molina, , Alfonso). 2005, "E-Banking value creation strategies: the case of the SAUDI investment bank", *International Association for Development of the Information Society(IADIS) International Conference on WWW/Internet.* Lisbon, Portugal.

[29] Mitrakas, Andreas(Portesi, , Silvia). 2007, "Regulating Information Security: A Matter of Principle?". *Securing Electronic Business Processes*(ISSE/SECURE 2007).

[30]Lee, Jang, Wan-Soo, Sang-Soo, 2009. "A Study on Information Security Management System Model for Small and Medium Enterprises". *Recent advances in E-activities information security and privacy*. Korea.

- **BOOK**

[31] SCN Education B.V. 2001. "BankAway! (2001) Net Banking Benefits. Sheer Acceleration. Electronic Banking: The Ultimate Guide to Business and Technology of Online Banking. *Vieweg & Sohn Verlags*gesell *Schaft mbH, Braun Schweig/Wieshaden.* 7-54.

[32]Gattiker ,Urs E. ,2004,THE INFORMATION SECURITY DICTIONARY ,KLUWER ACADEMIC PUBLISHERS, NEW YORK, BOSTON, DORDRECHT, LONDON.

- **THESIS**

[33]] Erkan, Ahmet, (Baykal, Nazife). 2006. "An automated tool for information security management" , *SCHOOL OF INFORMATICS OF THE MIDDLE EAST TECHNICAL UNIVERSITY SYSTEM* , Master of Science.Turkuy.

- **REPORTS**

[34]BANK VAN DE NEDERLANDSE ANTILLEN. 2007. "Provisions and Guidelines for Safe and Sound Electronic Banking".
[35] European Payments Council (EPC) 397-08v1.1. 2009. "Customer- to-bank security good practices guide".

[36] G.Gopalakrishna, et al. 2011**. "**Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds"**.** Report of the Working Group on Electronic Banking.]

[37] ISO/IEC 27001:2005(E), Information technology — Security techniques — Information security management systems — Requirements
[38] OECD. (2002), Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD.

[39] Pattinson, Fiona, 2007. "Certifying Information Security Management Systems", atsec information security corporation,