

# تحلیل مدیریت ریسک عملیاتی نظام بانکداری الکترونیک با استفاده از رویکرد خودارزیابی (جامعه مطالعه، یک بانک دولتی)

نویسندگان: دکتر سعید صفری\*<sup>۱</sup>، رضا سلیمانی<sup>۲</sup>

۱. عضو هیئت علمی دانشگاه شاهد

۲. کارشناس ارشد مدیریت بازرگانی گرایش مالی

\* Email: safari@shahed.ac.ir

## چکیده

ریسک عملیاتی از جمله مهمترین ریسک‌های شناخته شده در عرصه فعالیت‌های بانکی می‌باشد. گسترش بازارهای مالی، ظهور تکنولوژی‌های نو و جهانی شدن مؤسسات مالی بر اهمیت این ریسک افزوده است. مدیران بانک‌ها و مؤسسات مالی به منظور کنترل و کمینه کردن ریسک عملیاتی باید ضمن درنظر گرفتن عوامل مؤثر بر این نوع ریسک، سیاستها و رویه‌های کنترلی مناسبی اتخاذ کرده و در دوره‌های زمانی مشخص آن‌ها را مورد بررسی قرار دهند. در این پژوهش با درنظر گرفتن عوامل مؤثر بر ریسک عملیاتی در نظام بانکداری الکترونیک بانک‌های دولتی ایران و با استفاده از رویکرد خودارزیابی به تحلیل مدیریت ریسک عملیاتی یک بانک دولتی در زمینه فعالیت‌های بانکداری الکترونیک پرداخته شده است. روش آماری مورد استفاده در این پژوهش آزمون t تک متغیره بوده و نتایج بیانگر این بوده است که مدیریت ریسک عملیاتی در حوزه فعالیت‌های بانکداری الکترونیک در بانک مورد مطالعه از وضعیت چندان مناسبی برخوردار نمی‌باشد. در پایان راهکارهایی به منظور ارتقاء سطح مدیریت ریسک عملیاتی در بانک مذکور ارائه گردیده است.

**واژه‌های کلیدی:** ریسک عملیاتی، بانکداری الکترونیک، مدیریت ریسک، رویکرد خودارزیابی.

مختلف به صورت از راه دور ارائه می‌کنند و نقل و انتقال الکترونیکی پول، شامل پرداخت‌های کوچک و سیستم‌های مدیریت وجوه نقد، دستگاه‌های خودپرداز و سیستم‌های مدیریت خرده‌حساب‌ها ساختار جهانی پیدا کرده‌اند (۷). گسترش این نوآوری‌ها در جهان موجب شد که در دهه‌های ۱۳۶۰ و ۱۳۷۰ هجری شمسی فعالیتهای گسترده‌ای

توسعه سریع فن‌آوری اطلاعات و ارتباطات بر صنعت بانکداری تأثیر گذاشته و باعث ایجاد تغییرات ساختاری در این بخش شده است. در حقیقت بانکداری در حال حاضر به صنعت پردازش اطلاعات تبدیل شده است (۱). امروزه بانک‌ها خدمات خود را به مشتریان و کسب‌وکارهای

## دانشور

رشتار

مدیریت و پیشرفت

Management and Achievement

• دریافت مقاله: ۸۷/۶/۲۵

• پذیرش مقاله: ۸۸/۷/۱۵

Scientific-Research  
Journal of  
Shahed University  
Eighteenth Year  
No. 47-1  
Jun.Jul.2011

دوماهنامه علمی - پژوهشی  
دانشگاه شاهد  
سال هجدهم - دوره جدید  
شماره ۱-۴۷  
تیر ۱۳۹۰

## مقدمه

مواجهه‌اند. به منظور کنترل ریسک عملیاتی مدیریت بانک باید با در نظر گرفتن رویه‌ها و سیاست‌های مناسب مدیریت ریسک اقدام به شناسایی عوامل مؤثر بر ریسک عملیاتی کند و با توجه به این عوامل کارایی نظام‌های موجود در فرایند-های بانکی خود را ارزیابی کرده و یک سیستم ایمن از کنترل‌های داخلی برقرار سازد. سپس در دوره‌های زمانی مشخص چارچوب ریسک عملیاتی خود را ارزیابی کند (۷).

در این پژوهش با در نظر گرفتن عوامل مؤثر بر ریسک عملیاتی در نظام بانکداری الکترونیکی ایران، به دنبال پاسخ به این پرسش مهم هستیم که وضعیت فعلی رعایت اصول مدیریت ریسک عملیاتی بانکداری الکترونیک در حوزه هر یک از عوامل مورد بررسی در بانک دولتی مورد مطالعه به چه صورت است؟ با پاسخ به این پرسش کلیدی می‌توان رویه‌ها و سیاست‌های موجود را ارزیابی کرد و در صورت وجود نقص، آن‌ها را بهبود بخشیده و بهینه کرد.

### ضرورت و اهمیت پژوهش

توسعه تکنولوژی این امکان را برای مؤسسات مالی فراهم آورد تا اطلاعات بازار را سریع‌تر تجزیه و تحلیل کرده و از خود واکنش نشان دهند. توانایی دریافت، تلفیق، تجزیه و تحلیل و واکنش به این جریان اطلاعاتی یک مزیت رقابتی برای مؤسسات مالی فراهم می‌آورد. در چنین بازار در حال تحول سریع و پر حجم و با تکنولوژی بالا، اهمیت ریسک عملیاتی نیز افزایش می‌یابد. در چنین محیطی وجود یک مدیریت ریسک قوی و کارا برای مؤسسه بسیار حائز اهمیت است (۱۳).

اگر ریسک عملیاتی به خوبی مدیریت نشود نه فقط به زیان‌های مالی، بلکه به ورشکستگی بانک نیز منجر می‌شود. ریسک عملیاتی پدیده جدیدی نیست، اما با گسترش استفاده از فن‌آوری اطلاعات در سال‌های اخیر، اهمیت این ریسک بسیار برجسته شده است (۱). هدف از جلوگیری از زیان عملیاتی، کاهش تناوب و شدت وقایعی است که به زیان عملیاتی منجر می‌شود. این فعالیت‌ها شامل بازرسی داخلی، جرائم و پاداش‌ها و تکرار فرایندها می‌باشد که می‌تواند در برابر سوءاستفاده یا سرقت و قیمت‌گذاری نادرست یا خرابی سیستم‌ها به کار رود (۱۷).

هدف از این پژوهش، تحلیل رویه‌های جاری مورد استفاده در مدیریت ریسک عملیاتی فعالیت‌های بانکداری

برای استفاده از سیستم‌های رایانه‌ای در بانک‌های ایران انجام شود. از این رو بانک‌های تجاری و تخصصی کشور ضمن بهبود روش‌های خود و حرکت به سمت بانکداری نوین، بانکداری الکترونیک را نیز جزء برنامه‌های آتی خود قرار دادند (۱). اما حرکت از پردازش دستی به پردازش کاملاً رایانه‌ای و به همراه آن افزایش در حجم پردازش چه در تعداد و چه در منبع مهم‌ترین مسئله نگران‌کننده در این صنعت است، چرا که این امر احتمال ریسک را افزایش داده و کنترل‌هایی که بر روی این معاملات وجود داشته را کاهش داده است (۴). این پیشرفت‌ها سبب شد تا کمیته بال<sup>۱</sup> در سال ۱۹۹۸ مطالعات مقدماتی را بر روی اصول مدیریت ریسک در بانکداری الکترونیک و پول الکترونیک آغاز کند، که نتیجه آن تشکیل یک گروه کاری مرکب از سرپرستان بانک‌ها و بانک‌های مرکزی کشورهای توسعه یافته به نام گروه بانکداری الکترونیک<sup>۲</sup> بود. گزارش این گروه درباره مدیریت ریسک و مباحث سرپرستی در بانکداری الکترونیک در اکتبر سال ۲۰۰۰ به واسطه کمیته بال به تصویب رسید و عمده ریسک‌های مربوط به بانکداری الکترونیک به قرار زیر شناسایی شدند.

ریسک استراتژیک<sup>۳</sup>، ریسک اعتباری<sup>۴</sup>، ریسک عملیاتی<sup>۵</sup> شامل ریسک امنیتی<sup>۶</sup> و قانونی<sup>۷</sup>، ریسک نقدینگی<sup>۸</sup>، ریسک بازار<sup>۹</sup> و ریسک شهرت<sup>۱۰</sup> (۷).

همان‌طور که بیان شد یکی از ریسک‌های شناسایی شده در زمینه فعالیت‌های بانکداری الکترونیک ریسک عملیاتی می‌باشد. ریسک عملیاتی در هر سازمانی اعم از قانونمند و یا فاقد یک نظام مشخص، متمرکز یا غیر متمرکز، داری فن‌آوری قدیمی یا مدرن، محلی، ملی یا بین‌المللی، تک‌محصولی یا چندمحصولی، با یک کانال توزیع و یا چند کانال توزیع وجود دارد (۹).

از این رو بانک‌ها و مؤسسات مالی ایران نیز از این امر مستثنی نبوده و در فرایندهای کاری خود با این ریسک

1. Basel committee
2. Electronic Banking Group (EBG)
3. Strategic risk
4. Credit risk
5. Operational risk
6. Security risk
7. Legal risk
8. Liquidity risk
9. Market risk
10. Reputation risk

سوی دیگر، فقط به ریسک سیستمی ویا ریسک‌های مرتبط با تکنولوژی اطلاعات محدود نمی‌شود (۵).

### رویکرد خودارزیابی در تحلیل مدیریت ریسک

یکی از متداول‌ترین رویکردها در برقراری چارچوبی برای شناسایی عوامل ریسک عملیاتی، استفاده از تکنیک خودارزیابی است. خودارزیابی می‌تواند به‌طور دوره‌ای و از طریق پرسشنامه‌هایی کهبه‌وسیله مدیران ریسک (متخصصان) طراحی شده به اجرا درآید و اطلاعاتی را درباره سیستم و کیفیت کنترل داخلی و خارجی سازمان در دوره موردنظر ارائه دهد که به منظور پیش‌بینی ریسک عملیاتی استفاده می‌شود. در روش‌های پیشرفته‌تر آن، متخصصان می‌توانند با استفاده از روش‌های کیفی تناوب و شدت زیان‌ها را برای هر عامل ریسک عملیاتی ارزیابی کنند (۱۰). این رویکرد عموماً به تأیید حساب‌رسان بوده و قانونگذاران و مراجع قانونی نیز آن را به عنوان ابزاری منطبق با رویه‌های قانونی، ترویج کرده‌اند. این روش به صورت‌های مختلف به‌واسطه نهادهای مالی به کار گرفته می‌شود و عموماً در این پرسشنامه‌ها از طیف لیکرت استفاده می‌شود. مهم‌ترین مزیت این روش شناسایی حوزه‌های پرخطر و انجام فعالیت‌هایی به منظور کاهش ریسک آن حوزه‌ها می‌باشد. این روش بر اطلاعات ذهنی که به صورت دوره‌ای جمع‌آوری می‌شود مبتنی است. دوره‌ای بودن رویکرد خودارزیابی آن را در برقراری کنترل‌ها، بازنگری مدیریت عملکرد و تخصیص سرمایه با مشکل مواجه کرده‌است. با این حال رویکرد خودارزیابی مؤثرترین روش برای شناسایی ریسک‌های یک سازمان می‌باشد. به منظور ارزیابی وضعیت مدیریت ریسک عملیاتی در نظام بانکی می‌توان از پرسشنامه‌های متفاوتی استفاده کرد. برخی از این پرسشنامه‌ها به صورت استاندارد بوده و از سوی کمیته بال تحت عنوان QIS1,2,3 انتشار یافته‌است. دسته دوم پرسشنامه‌هایی هستند که بر اساس طبقات زیان شناسایی شده در حوزه فعالیت‌های بانکی طراحی می‌شوند (۱۵).

همچنین کمیته بال به این نتیجه رسید که پروفایل ریسک هر بانک متفاوت بوده و نیاز به رویکرد ریسک متناسب با توجه به دامنه فعالیت بانکداری الکترونیک خود دارد. از این‌رو یک رویکرد جامع متناسب برای مسائل مدیریت

الکترونیک در بانک مورد مطالعه می‌باشد تا بر اساس نتایج به‌دست‌آمده به شناسایی و تقویت نقاط قوت و اصلاح نقاط ضعف احتمالی اقدام شود.

### مدیریت ریسک عملیاتی و تحلیل آن

بانکداری الکترونیک عبارت است از "استفاده از وسایل الکترونیکی در عرضه محصولات و خدمات بانکی"، که خود زیرمجموعه‌ای از تأمین بودجه الکترونیکی می‌باشد (۶). در تعریف دیگری آمده‌است، بانکداری الکترونیکی عبارت است از "انجام عملیات بانکی و ارائه خدمات بانکی از طریق شبکه‌های الکترونیکی" (۱۸). اما یکی از کامل‌ترین تعاریف بانکداری الکترونیکی عبارت است از "هر نوع فعالیت بانکی مبتنی بر وسایل الکترونیکی شامل دستگاه‌های خودپرداز، مراکز تلفن خودکار، رایانه‌های شخصی، تلفن و سایر ابزارهای موجود در وب"؛ این ابزارها می‌توانند برای پرداخت صورت حساب‌ها، انتقال وجوه و دسترسی به سایر خدمات مالی استفاده‌شوند. بانک ممکن است این خدمات را خود ارائه داده و یا از طریق قراردادی به‌واسطه عرضه‌کنندگان خارجی به ارائه این خدمات پردازد (۱۲).

همان‌طور که پیش از این بیان شد، توسعه نظام بانکداری الکترونیک سبب شد تا کمیته بال مطالعات مقدماتی بر روی اصول مدیریت ریسک در بانکداری الکترونیک را با تشکیل گروه بانکداری الکترونیک آغاز کند؛ ماحصل این کار شناسایی ریسک عملیاتی به عنوان یکی از انواع ریسک‌های نظام بانکداری الکترونیک بود. ریسک عملیاتی را "ریسک زیان‌های ناشی از عدم کفایت و شکست کنترل‌های داخلی، اشتباهات نیروی انسانی، سیستم‌ها و رویدادهای خارجی" تعریف کرده‌اند (۱۹). این تعریف نه فقط برای بانک‌ها بلکه از سوی کمیته بال برای هر مؤسسه مالی، ارائه شده‌است؛ همچنین در این تعریف بر روی علل ریسک عملیاتی تمرکز شده‌است، که از فواید آن می‌توان به تسهیل اندازه‌گیری ریسک عملیاتی اشاره کرد. باید به این نکته توجه نمود که برخلاف برداشت‌های گذشته در ارتباط با ریسک عملیاتی، ریسک استراتژیک و ریسک شهرت در زمره ریسک عملیاتی طبقه‌بندی نمی‌شوند، لذا این تعریف عام که "ریسک عملیاتی شامل هرگونه ریسکی بجز ریسک‌های اعتباری و بازار است" دیگر صحیح نبوده و از

ریسک بانکداری الکترونیک وجود ندارد. در نتیجه بانکها باید این ریسک را با توجه به ویژگی‌های ساختاری و چالش‌های اصلی خدمات بانکداری الکترونیک خود در یک رویه شفاف بررسی و مدیریت کنند (۷). ریسک عملیاتی می‌تواند به طبقات مختلفی تقسیم‌بندی شود؛ سازمانها دارای ساختارهای متفاوتی هستند و طبقه بندی‌های انجام شده درباره ریسک عملیاتی قراردادی می‌باشد (۱۶).

طبقه‌بندی‌های متفاوتی از انواع زیان‌های عملیاتی در نظام بانکی ارائه شده است. در یک نوع طبقه‌بندی بر اساس عوامل انسانی، زیان‌های عملیاتی را به چهار گروه خطاهای نظارتی مدیریت، تقلب‌های مدیریتی، خطاهای فعالیت کارکنان و تقلب‌های کارکنان تقسیم‌بندی کرده‌اند. در طبقه‌بندی دیگری که بر اساس علم حسابداری انجام شده، زیان‌های عملیاتی را چهار گروه ریسک ارزشیابی، ریسک تطبیق، ریسک سازگاری و ریسک خط زمانی اسناد کرده‌اند (۱۵).

کورفس<sup>۱</sup> (۲۰۰۴) انواع ریسک عملیاتی را در سازمان‌ها به سه گروه عمده زیان‌های کلاسیک، زیان‌های مدرن و زیان‌های مبتنی بر فن‌آوری اطلاعات طبقه‌بندی کرده است. بر این اساس زیان‌های کلاسیک دربرگیرنده شایستگی‌های مدیریتی در تمام سطوح، کیفیت و مهارت‌های متخصصان و کارکنان، مسائل سازمانی از جمله عدم انطباق فعالیت‌های صفی و ستادی، ریسک اجرایی شامل مدیریت مبادلات، بدهی‌ها، اعتبارات و تاییدیه‌ها می‌باشد. زیان‌های مدرن دربرگیرنده فعالیت‌های امنی، سپرده‌گذاری از طریق کانال‌های حمایت‌شده، ریسک قانون در تمامی حوزه‌های قضایی که بانک در آن حوزه‌ها فعالیت می‌کند و انطباق با قوانین، مستند سازی، پرداخت‌ها و تسویه‌ها بوده و ریسک فن‌آوری اطلاعات نیز شامل امنیت، تقلب (درون سازمانی و برون سازمانی)، خدمات زیرساختی (مخابرات و تامین نیرو) و وضعیت حال و آتی ریسک عملیاتی در ارتباط با نوآوری‌ها و جهانی‌سازی می‌باشد (۹). مهم‌ترین زیان‌های عملیاتی در بانک‌های سرمایه‌گذاری سطح منابع نسبت به فعالیت‌ها، مجموعه مهارت‌ها و توانایی‌های مدیران و کارکنان، مسائل تکنولوژیکی، رویه‌ها منسوخ شده و

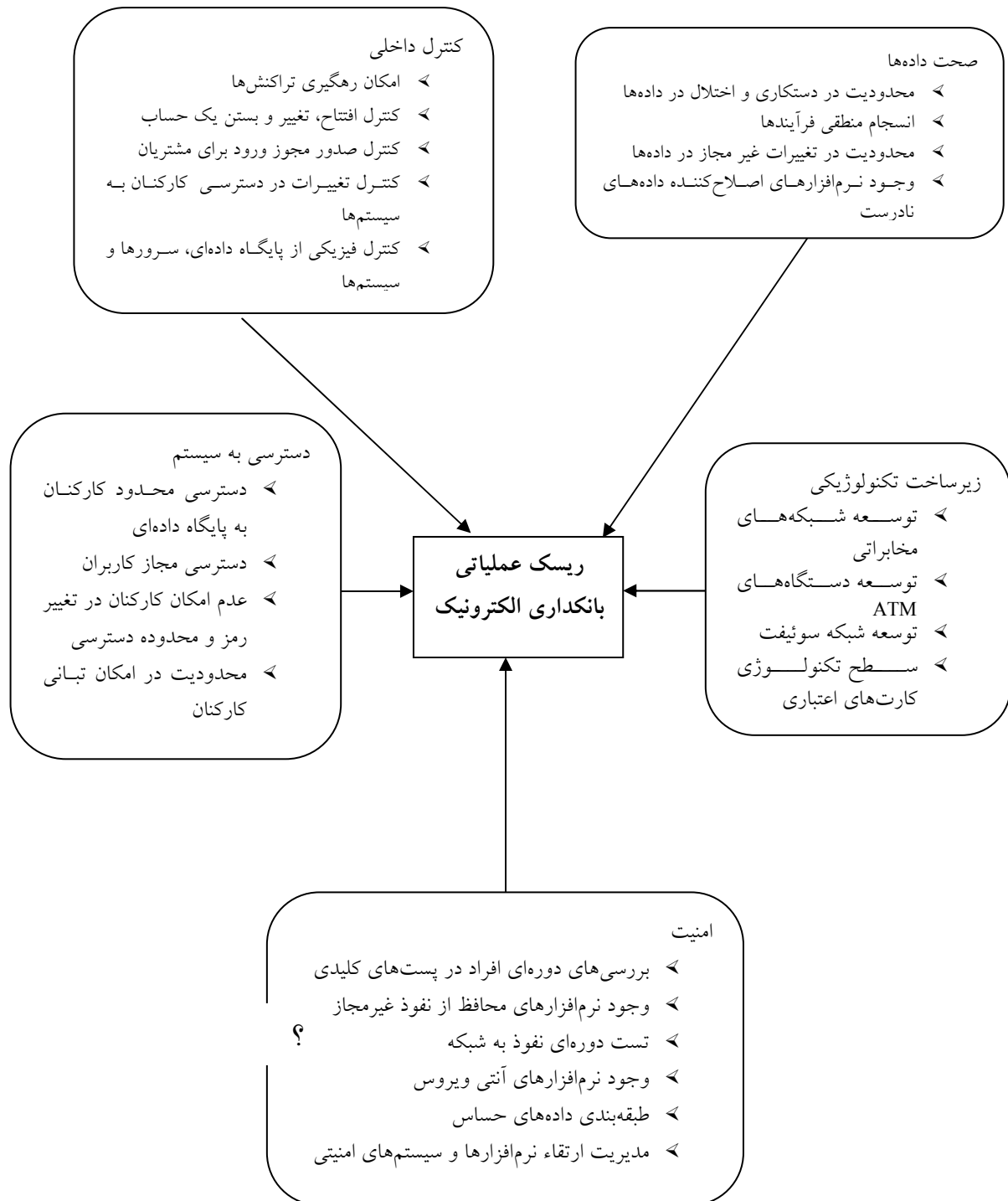
ناکارآمد، مسائل و مشکلات امور برون سازمانی شده و شرکاء تجاری، فقدان کنترل بر فرایندها، دسترسی و محیط‌کاری عنوان شده است (۱۶).

روبرت جارو (۲۰۰۸) ریسک عملیاتی در بانک‌ها را به دو گروه تقسیم‌بندی کرده است؛ دسته اول زیان‌های مرتبط با فعالیت‌ها و عملیات شرکت همچون شکست در مبادلات یا سرمایه‌گذاری‌ها و حتی خطاها در پشت باجه، محصول، فرایند و ملاحظات قانونی. دسته دوم زیان‌های ناشی از محرک‌ها شامل سوء مدیریت و اختلاس. نوع دوم این زیان‌ها نمایانگر مسئله هزینه نمایندگی و هزینه ناشی از جدایی مالکیت از مدیریت می‌باشد (۱۴).

هلبوک و واگنر (۲۰۰۵) رویه‌های گزارش ریسک عملیاتی در بانک‌ها را برای یک دوره سه ساله بررسی کرده و به این نتیجه رسیدند که در دوره مورد بررسی دامنه و محتوای افشاجری بانک‌ها درباره ریسک عملیاتی به‌طور قابل ملاحظه‌ای افزایش یافته است؛ این امر نشان‌دهنده افزایش اقدامات مدیریت ریسک در بانک‌ها بوده است. همچنین آن‌ها به این نتیجه رسیدند که دامنه و محتوای گزارشگری ریسک عملیاتی با نسبت دارایی و سودآوری بانک‌ها رابطه معکوس دارد. کامینز (۲۰۰۶) در یک مطالعه موردی به بررسی تأثیر رویدادهای ریسک عملیاتی بر ارزش بازار بانک‌های شرکت‌های بیمه در امریکا پرداخت و به این نتیجه رسید که یک رابطه آماری قوی منفی بین قیمت سهام با انتشار اخبار زیان عملیاتی در این شرکت‌ها وجود دارد. به علاوه کاهش ارزش بازار سهام این شرکت‌ها فراتر از میزان زیان عملیاتی آن‌ها بوده که بیانگر این است که چنین زیان‌هایی تأثیرات نامطلوبی بر جریان وجوه نقد آتی شرکت‌ها دارد (۱۱).

سلیمانی (۱۳۸۶) با الگوبرداری از عوامل تأثیرگذار معرفی شده از سوی کمیته بال و اصول مدیریت ریسک در نظام بانکداری الکترونیک مدل زیر را طراحی و به بررسی تأثیرگذاری پنج عامل صحت داده‌ها، کنترل‌های داخلی، زیرساخت تکنولوژیکی، دسترسی به سیستم و امنیت بر ریسک عملیاتی نظام بانکداری الکترونیک بانک‌های دولتی ایران پرداخته و به این نتیجه رسیده است که هر پنج عامل مورد بررسی با تمامی مؤلفه‌های مورد بررسی در حوزه هر عامل بر ریسک عملیاتی بانکداری الکترونیک بانک‌های ایران تأثیرگذار است (۳).

شکل ۱. مدل مفهومی تحقیق (سلیمانی ۱۳۸۶)



اعتبار و قابلیت دسترسی به سیستم‌ها، برنامه‌های کاربردی و پایگاه داده‌ای بانکداری الکترونیک (۷).

**زیرساخت تکنولوژیکی:** شامل سخت‌افزار، نرم‌افزار، پایگاه داده‌ای و ارتباطی که برای انجام وظیفه در قالب ارائه خدمات از طریق اینترنت، پشتیبانی از انتقال الکترونیکی داده‌ها و سایر اشکال پیام‌گذاری و پیام‌گیری از

در این مدل هر یک از عوامل مورد بررسی به قرار زیر تعریف شده‌اند.

**صحت داده‌ها:** مجموعه معیارهای مناسب برای حفاظت از انسجام و صحت داده‌ها در اطلاعات رکوردها و تراکنش‌های بانکداری الکترونیک.

**دسترسی به سیستم:** مجموعه اقداماتی برای کنترل

طریق اینترنت یا سایر شبکه‌ها به کار می‌رود (۲).

**امنیت:** ترکیبی از سیستم‌ها، کاربست‌ها و کنترل‌های داخلی که برای حفاظت از صحت و محرمانه‌بودن داده‌ها و فرایندهای عملیاتی به کار می‌رود.

**کنترل داخلی:** مجموعه مکانیزم‌های کنترلی مستقل برای یافتن نقایص و کاهش ریسک‌ها در ارائه خدمات بانکداری الکترونیک (۸).

در این پژوهش با توجه به مطالعه مدل اخیر در نظام بانکی کشور از آن به عنوان مدل مرجع و بومی در تحلیل مدیریت ریسک عملیاتی نظام بانکداری الکترونیک در بانک سپه استفاده شده است. در این راستا و با توجه به اهداف پژوهش و مدل مورد بررسی فرضیات زیر مطرح شده است.

**فرضیه اصلی:** سیاست‌های مدیریت ریسک عملیاتی در نظام بانکداری الکترونیک در بانک مورد مطالعه از وضعیت مطلوبی برخوردار است.

**فرضیه فرعی اول:** عامل صحت داده‌ها در نظام بانکداری الکترونیک در بانک مورد بررسی از وضعیت مطلوبی برخوردار است.

**فرضیه فرعی دوم:** عامل کنترل‌های داخلی در نظام بانکداری الکترونیک در بانک مورد بررسی از وضعیت مطلوبی برخوردار می‌باشد.

**فرضیه فرعی سوم:** عامل زیرساخت تکنولوژیکی در نظام بانکداری الکترونیک در بانک مورد بررسی از وضعیت مطلوبی برخوردار است.

**فرضیه فرعی چهارم:** عامل دسترسی به سیستم در نظام بانکداری الکترونیک در بانک مورد بررسی از وضعیت مطلوبی برخوردار می‌باشد.

**فرضیه فرعی پنجم:** عامل امنیت در نظام بانکداری الکترونیک در بانک مورد بررسی از وضعیت مطلوبی برخوردار است.

### روش شناسی تحقیق

این تحقیق از نظر هدف کاربردی و از نظر ماهیت و روش توصیفی پیمایشی می‌باشد که در آن جمع‌آوری اطلاعات عمدتاً به روش میدانی انجام شده است. ابزار گردآوری داده‌ها در این پژوهش پرسشنامه بوده و از آزمون آماری  $t$  تک متغییره برای تجزیه و تحلیل داده‌ها استفاده به عمل

آمده است. قلمرو موضوعی این پژوهش در حوزه مدیریت مالی می‌باشد و این تحقیق در فاصله زمانی بین اردیبهشت ۱۳۸۶ تا آذر ۱۳۸۶ انجام شده است. روش نمونه‌گیری از نوع نمونه‌گیری تصادفی طبقه‌بندی شده می‌باشد و با توجه به حجم جامعه مورد مطالعه ( $N=147$ ) و در سطح  $\alpha=5\%$  اندازه نمونه ۵۶ نفر تعیین شده است. در این تحقیق روایی پرسشنامه‌ها به طریق محتوایی حاصل شده و برای تعیین روایی محتوایی از نظر اساتید و کارشناسان بانکی استفاده و روایی پرسشنامه تأیید شده است. همچنین برای آزمون پایایی پرسشنامه از ضریب آلفای کرونباخ استفاده شده است و مطابق محاسبات انجام شده میزان آلفای کرونباخ به دست آمده ۰/۹۰۴ می‌باشد که نشانگر پایایی بالای پرسشنامه طراحی شده است.

### تجزیه و تحلیل داده‌ها

در این قسمت به تجزیه و تحلیل داده‌های حاصل از پرسشنامه پرداخته و با استفاده از آزمون  $t$  تک متغییره فرضیه‌های پژوهش آزموده شده است.

**فرضیه فرعی اول:** عامل صحت داده‌ها در نظام بانکداری الکترونیک بانک مورد بررسی از وضعیت مطلوبی برخوردار است.

بر اساس اطلاعات جدول شماره ۱۰ با آزمون این فرضیه نتیجه گرفته می‌شود که به اطمینان ۹۵ درصد وضعیت فعلی عامل صحت داده‌ها در نظام بانکداری الکترونیک بانک بررسی شده مطلوب است. همچنین سه مؤلفه از چهار مؤلفه مورد بررسی در حوزه این عامل نامطلوب شناخته شده‌اند (فقط محدودیت در تغییر غیرمجاز داده‌ها مطلوب شناخته شده است).

اما به دلیل اختلاف کم کران پایین مؤلفه‌های نامطلوب با میانگین ۳ در کل وضعیت عامل صحت داده‌ها مطلوب شناخته شده است. این نتایج رویکرد نامناسب این بانک را نسبت به عامل صحت داده‌ها نشان می‌دهد و انتظار می‌رود که بانک نسبت به این عامل سیاست‌های دقیق‌تر و حساس‌تری اتخاذ نماید.

**فرضیه فرعی دوم:** عامل کنترل‌های داخلی در نظام بانکداری الکترونیک بانک مورد بررسی از وضعیت مطلوبی برخوردار است.

بر اساس اطلاعات جدول شماره ۲ و با آزمون فرضیه

وضعیت نامطلوبی قرار دارند؛ لذا پیش‌بینی می‌شود که بانک از تهدیدات و زیان‌های شناخته‌شده در این حوزه در امان نبوده و همواره در معرض خطر زیان عملیاتی ناشی از این شکست‌ها قرار داشته‌باشد.

**فرضیه فرعی سوم:** عامل زیرساخت تکنولوژیکی در نظام بانکداری الکترونیک بانک مورد بررسی از وضعیت مطلوبی برخوردار است. (جدول ۳)

فرعی دوم نتیجه گرفته می‌شود که در سطح اطمینان ۹۵ درصد وضعیت فعلی کنترل‌های داخلی در نظام بانکداری الکترونیک بانک بررسی شده مطلوب بوده و نتایج نشانگر این است که مؤلفه‌های امکان رهگیری تراکنشها و کنترل فیزیکی از پایگاه داده‌ای، سرورها و سیستمها در وضعیت مطلوبی قرار دارند، اما سه مؤلفه کنترل افتتاح، تغییر و بستن یک حساب، کنترل صدور مجوز ورود برای مشتریان و کنترل تغییرات در دسترسی کارکنان به سیستمها در

جدول ۱. آزمون t تک نمونه‌ای مربوط به بررسی وضعیت فعلی صحت داده‌ها در نظام بانکداری الکترونیک بانک مورد مطالعه

نتیجه	فاصله اطمینان ۹۵ درصد		اختلاف میانگین	P مقدار	آماره t	میانگین	عامل مورد مطالعه	بررسی مؤلفه‌های صحت داده‌ها
	کران بالا	کران پایین						
مطلوب	۰/۳۷	۰/۰۶	۰/۲۲	۰/۰۰۶۴	۲/۸۳۳	۳/۲۲۲	صحت داده‌ها	
نامطلوب	/۰۹۰۳	-۰/۳۳۶۰	-۱/۲۲۸	۰/۲۵۳	-۱/۱۵۴	۲/۸۷۷۲	محدودیت در دستکاری و اختلال در داده‌ها	
نامطلوب	۰/۴۷۸۹	-۰/۰۲۲۷	۰/۲۲۸۱	۰/۰۷۴	۱/۸۲۲	۳/۲۲۸۱	انسجام منطقی فرایندها	
مطلوب	۰/۸۹۵۲	۰/۳۶۸۰	۰/۶۳۱۶	/۰۰۰۰	۴/۸۰۰	۳/۶۳۱۶	محدودیت در تغییرات غیرمجاز در داده‌ها	
نامطلوب	۰/۲۸۷۸	-۰/۱۷۲۴	۰/۰۵۷۶	۰/۶۱۷	۰/۵۰۳	۳/۰۵۷۷	وجود نرم‌افزارهای اصلاح‌کننده داده‌های نادرست	

جدول ۲. آزمون t تک نمونه‌ای مربوط به بررسی وضعیت فعلی کنترل‌های داخلی در نظام بانکداری الکترونیک بانک مورد مطالعه

نتیجه	فاصله اطمینان ۹۵ درصد		اختلاف میانگین	P مقدار	آماره t	میانگین	عامل مورد مطالعه	بررسی مؤلفه‌های کنترل‌های داخلی
	کران بالا	کران پایین						
مطلوب	۰/۵۲	۰/۱۶	۰/۳۴	۰/۰۰۰۴	۳/۷۷	۳/۳۴	کنترل‌های داخلی	
مطلوب	۰/۸۳۴۴	۰/۳۲۳۵	۰/۵۷۸۹	/۰۰۰۰	۴/۵۴۱	۳/۵۷۸۹	امکان رهگیری تراکنشها	
نامطلوب	۰/۶۱۲۳	-۰/۰۷۶۵	۰/۲۶۷۹	۰/۱۲۵	۱/۵۵۸	۳/۲۶۷۹	کنترل افتتاح، تغییر و بستن یک حساب	
نامطلوب	۰/۴۶۸۶	-۰/۰۱۲۵	۰/۲۸۱	۰/۶۳	۱/۸۹۹	۳/۲۲۸۱	کنترل صدور مجوز برای مشتریان	
نامطلوب	۰/۳۶۹۴	۰/۰۵۳۵	۰/۱۵۷۹	/۱۴۰	۱/۴۹۶	۳/۱۵۷۹	کنترل تغییرات در دسترسی به سیستمها	
مطلوب	۰/۶۶۹۳	۰/۲۴۳۰	۰/۴۵۶۱	/۰۰۰۰	۴/۲۸۷	۳/۴۵۶۱	کنترل فیزیکی از پایگاه داده‌ای، سرورها و سیستمها	

جدول ۳. آزمون t تک نمونه‌ای مربوط به بررسی وضعیت فعلی زیرساخت تکنولوژیکی در نظام بانکداری الکترونیک بانک مورد مطالعه

نتیجه	فاصله اطمینان ۹۵ درصد		اختلاف میانگین	مقدار P	آماره t	میانگین	عامل مورد مطالعه	تکنولوژیکی بررسی مؤلفه‌های زیرساخت
	کران بالا	کران پایین						
نامطلوب	۰/۰۶	-۰/۲۲	-۰/۰۸	۰/۲۴۳۵	-۱/۱۸	۲/۹۲	زیرساخت تکنولوژیکی	
نامطلوب	۰/۱۴۹۰	-۰/۳۲۴۴	-۰/۰۸۷۷	۰/۴۶۱	-۰/۷۴۲	۲/۹۱۲۳	توسعه شبکه‌های مخابراتی	
نامطلوب	۰/۱۷۹۴	-۰/۲۸۴۷	۰/۰۵۲۶	۰/۶۵۱	-۰/۴۵۴	۲/۹۷۷۴	توسعه دستگاه‌های ATM	
مطلوب	۰/۴۹۱۵	۰/۰۲۷۰	۰/۲۵۹۳	۰/۰۲۹	۲/۲۳۹	۳/۲۵۹۳	توسعه شبکه سوئیفت	
نامطلوب	۰/۲۱۹۴	-۱/۷۹۸	۰/۰۱۷۵	۰/۸۵۹	۰/۱۷۸	۳/۰۱۷۵	سطح تکنولوژی کارت‌های اعتباری	
مطلوب	-۰/۲۸۹۵	-۰/۷۲۸۰	-۰/۵۰۸۸	/۰۰۰۰	-۴/۶۴۸	۲/۴۹۱۲	کارآیی شبکه‌های اینترنتی	

کارت‌های اعتباری از وضعیت مطلوبی برخوردار نیستند. از این رو می‌توان گفت که این بانک فاقد بسیاری از زیرساخت‌های اولیه مناسب برای برقراری یک نظام بانکداری الکترونیک کارآمد است.

**فرضیه فرعی چهارم:** عامل دسترسی به سیستم در نظام بانکداری الکترونیک بانک مورد بررسی از وضعیت مطلوبی برخوردار است.

بر اساس اطلاعات جدول شماره ۳ و با آزمون فرضیه فرعی سوم نتیجه گرفته می‌شود که در سطح اطمینان ۹۵ درصد عامل زیرساخت تکنولوژیکی در نظام بانکداری الکترونیک در بانک بررسی شده وضعیت مطلوبی نداشته و در میان متغیرهای مورد بررسی در حوزه این عامل فقط دو مؤلفه توسعه شبکه سوئیفت و کارآیی شبکه‌های اینترنتی از وضعیت مطلوبی برخوردارند؛ اما توسعه شبکه‌های مخابراتی و توسعه دستگاه‌های ATM و سطح تکنولوژی

جدول ۴. آزمون t تک نمونه‌ای مربوط به بررسی وضعیت فعلی دسترسی به سیستم در نظام بانکداری الکترونیک بانک مورد مطالعه

نتیجه	فاصله اطمینان ۹۵ درصد		اختلاف میانگین	مقدار P	آماره t	میانگین	عامل مورد مطالعه	تکنولوژیکی بررسی مؤلفه‌های دسترسی به سیستم
	کران بالا	کران پایین						
مطلوب	۰/۴۳	۰/۱۴	۰/۲۸	۰/۰۰۰۳	۳/۸۵	۳/۲۸	دسترسی به سیستم	
مطلوب	۰/۵۷۴۳	۰/۰۰۷۵	۰/۲۹۰۹	/۰۴۴	۲/۰۵۸	۳/۲۹۰۹	دسترسی محدود کارکنان به پایگاه داده‌ای	
مطلوب	۰/۸۵۳۴	۰/۳۰۴۵	۰/۵۷۸۹	/۰۰۰۰	۴/۲۲۶	۳/۵۷۸۹	دسترسی مجاز کاربران	
مطلوب	۰/۶۷۹۵	۰/۰۱۱۴	۰/۳۴۵۵	/۰۴۳	۲/۰۷۴	۳/۳۴۵۵	عدم امکان کارکنان در تغییر رمز و محدوده دسترسی	
نامطلوب	۰/۱۵۳۲	-۰/۲۹۸۶	-۰/۰۷۲۷	۰/۵۲۱	-۰/۶۴۵	۲/۹۲۷۳	محدودیت در امکان تبانی کارکنان	

مؤلفه‌های مورد بررسی در وضعیت مطلوبی قرار دارند، که بیانگر سیاست‌ها و استراتژی‌های قوی‌تر مدیریت بانک در حوزه این عامل نسبت به سایر عوامل مورد بررسی است، اما مدیریت بانک باید در سطح دسترسی کارکنان بانک به پایگاه داده‌ای و سیاست تفکیک وظایف، چرخش شغلی و

با آزمون فرضیه فرعی چهارم نتیجه گرفته می‌شود که در سطح اطمینان ۹۵ درصد عامل دسترسی به سیستم در نظام بانکداری الکترونیک بانک مورد بررسی مطلوب بوده و در حوزه این عامل فقط مؤلفه محدودیت در امکان تبانی کارکنان است که دارای وضعیت نامطلوبی می‌باشد و سایر



رویه‌های کنترل پرسنلی خود تجدیدنظر کند. فرضیه فرعی پنجم: عامل امنیت در نظام بانکداری برخوردار است.

جدول ۵. آزمون t تک‌نمونه‌ای مربوط به بررسی وضعیت فعلی امنیت در نظام بانکداری الکترونیک بانک مورد مطالعه

نتیجه	فاصله اطمینان ۹۵ درصد		اختلاف میانگین	P مقدار	آماره t	میانگین	عامل مورد مطالعه	بررسی مؤلفه‌های امنیت
	کران بالا	کران پایین						
نامطلوب	۰/۱۵	-۰/۲۳	-۰/۰۴	۰/۶۹۰۷	-۰/۴۰	۲/۹۶	امنیت	
نامطلوب	۰/۰۸۰۷	-۰/۵۰۱۸	-۰/۲۱۰۵	۰/۱۵۳	-۱/۴۴۸	۲/۷۸۹۵	بررسی‌های دوره‌ای افراد در پست‌های کلیدی	
مطلوب	۰/۵۵۹۴	۰/۱۰۷۲	۰/۳۳۳۳	/۰۰۵	۲/۹۵۳	۳/۳۳۳	وجود نرم‌افزارهای محافظ از نفوذ غیرمجاز	
نامطلوب	۰/۰۰۱۸	-۰/۴۵۸۰	-۰/۲۲۸۱	۰/۰۵۲	-۱/۹۸۷	۲/۷۷۱۹	تست‌های دوره‌ای نفوذ به شبکه	
مطلوب	۰/۷۱۳۳	۰/۱۶۳۹	۰/۴۲۸۶	۰/۰۰۲	۳/۱۹۸	۳/۴۳۸۶	وجود نرم‌افزارهای آنتی-ویروس	
نامطلوب	۰/۱۱۳۲	-۰/۴۳۴۷	-۰/۱۶۰۷	۰/۲۴۵	-۱/۱۷۶	۲/۸۳۹۳	طبقه‌بندی داده‌های حساس	
مطلوب	-۰/۱۵۸۶	-۰/۶۴۸۴	۰/۴۰۳۵	۰/۰۰۲	-۳/۳۰۰	۲/۵۹۶۵	مدیریت ارتقاء نرم‌افزارها و سیستم‌های امنیتی	
نامطلوب	۰/۰۸۰۷	-۰/۵۰۱۸	-۰/۲۱۰۵	۰/۱۵۳	-۱/۴۴۸	۲/۷۸۹۵	بررسی‌های دوره‌ای افراد در پست‌های کلیدی	

۳ می‌باشد در سطح خطای ۰/۰۵ رد می‌شود؛ یعنی میانگین جامعه به‌طور معنی‌دار از عدد ۳ بزرگ‌تر است. گرچه این اختلاف چندین چشمگیر نیست، اما می‌توان گفت سیاست‌های مدیریت ریسک عملیاتی در نظام بانکداری الکترونیک بانک مورد بررسی دارای وضعیت مطلوبی می‌باشد.

جدول ۶. آزمون t تک‌نمونه‌ای بررسی سیاست‌های مدیریت ریسک عملیات در نظام بانکداری الکترونیک بانک مورد مطالعه

«سیاست‌های مدیریت ریسک عملیاتی»		
فرآوانی	میانگین	انحراف معیار
۵۶	۳/۱۴۴۶	۰/۴۵۰۳
آماره t	درجه آزادی	P - مقدار
۲/۴۲۵	۵۵	۰/۰۱۹
اختلاف میانگین‌ها	فاصله اطمینان ۹۵ درصد جهت اختلاف میانگین‌ها	
	کران پایین	کران بالا
۰/۱۴۴۶	۰/۰۲۵۱	۰/۲۶۴۱

با آزمون این فرضیه نتیجه گرفته می‌شود که در سطح اطمینان ۹۵ درصد عامل امنیت در نظام بانکداری الکترونیک این بانک وضعیت نامطلوبی دارد. همچنین در حوزه این عامل سه مؤلفه تست دوره‌ای شبکه، بررسی دوره‌ای افراد در پست‌های کلیدی و طبقه‌بندی داده‌های حساس از وضعیت نامطلوبی برخوردار بوده اما سه مؤلفه دیگر مورد بررسی در حوزه این عامل دارای وضعیت مطلوبی می‌باشند. با توجه به این که امنیت از لحاظ تأثیرگذاری دارای رتبه اول در بین سایر عوامل می‌باشد و با توجه به نامطلوب شناخته‌شدن وضعیت فعلی این عامل، موقیعت پرخطر و بحرانی بانک در حوزه این عامل کاملاً مشهود است.

فرضیه اصلی: سیاست‌های مدیریت ریسک عملیاتی در نظام بانکداری الکترونیک در بانک مورد مطالعه از وضعیت مطلوبی برخوردار است.

با توجه به مندرجات جدول نتایج، P- مقدار به‌دست‌آمده کوچک‌تر از سطح خطای  $\alpha=0/05$  می‌باشد؛ بنابراین فرض  $H_0$  مبنی بر اینکه میانگین جامعه کوچک‌تر یا مساوی عدد

## بحث و نتیجه گیری

با بررسی نتایج آزمون فرضیات پژوهش نتیجه گرفته می شود که بانک مورد مطالعه از یک مدیریت ریسک مطلوب و با قابلیت اعتماد بالایی برخوردار نیست و اختلاف بسیار ناچیز کران های بالا و پایین با میانگین ۳ بیانگر این است که سیاست های به کار گرفته شده در حوزه های مختلف عملیاتی هرچند از نظر آماری مطلوب شناخته شده است اما از قابلیت اعتبار و امنیت بالایی برخوردار است. مهم تر اینکه بانک در دو حوزه بسیار مهم و استراتژیک امنیت و زیرساخت تکنولوژیکی دارای وضعیت نامطلوب می باشد و این امر می تواند فعالیت های بانک را بشدت در معرض خطرات شناخته شده در این حوزه ها قرار دهد. از سوی دیگر در سه حوزه دیگر بررسی شده نیز بانک صرفاً در حد رعایت حداقل امتیاز لازم برای حصول درجه مطلوبیت از نظر آماری قرارداد و اختلاف ناچیز کران های بالا و پایین نسبت به میانگین ۳ نشانگر مستعد بودن این حوزه به وقوع زیان های عملیاتی است.

## پیشنهادها

- ۱- در حوزه صحت داده ها پیشنهاد می شود اداره تشکیلات و بهبود روش های بانک، ضمن مستندسازی کامل تمامی فرایندهای بانکداری الکترونیک در این بانک و بررسی فنی و مدیریتی آنها، اقدام به اصلاح و تعریف بهینه آنها کند؛ تا فرایندهای بانکداری الکترونیک بانک در یک رویه منطقی و مناسب سازماندهی شوند. در این مسیر می توان با بررسی سابقه تاریخی زیان ها و تعیین نقاط آسیب پذیر از یک سو به بهبود این نقاط و تقویت نظام های امنیتی اقدام کرد تا از نفوذ، دستکاری و اختلال در داده ها جلوگیری به عمل آید، و از سوی دیگر نیازهای بانک در فرایند مدیریت داده ها را شناسایی و بر اساس آن اقدام به طراحی و تولید نرم افزارهای اصلاح کننده داده های نادرست کارآ برای بانک کرد.
- ۲- در حوزه کنترل های داخلی پیشنهاد می شود بانک به تعریف رکوردهای کافی برای هر مرحله از فرایند انجام تراکنش های بانکداری الکترونیک خود اقدام کند. بانک با استفاده از این رکوردها می تواند تمامی تراکنش ها را رهگیری و کنترل نماید. همچنین استفاده

- هم زمان از چندین روش تأیید اعتبار به ویژه استفاده از شناسه بیومتریک برای شناسایی کاربران در زمان اتصال به سرورها و پایگاه های داده ای توصیه می شود.
- ۳- پیشنهاد می شود برای کنترل کارکنان، تمامی پرسنل بانک با توجه به پست سازمانی آنها و الزامات اطلاعاتی متناسب با آن پست طبقه بندی شوند و متناسب با هر طبقه سطح اطلاعاتی و سطح دسترسی به سیستم های بانکداری الکترونیک تعریف شده و فقط به کاربران اجازه دسترسی به آن سطوح داده شود. درباره سرورها، سیستم و پایگاه های داده ای نیز پیشنهاد می شود که به منظور جلوگیری از هرگونه اختلال و وقفه در ارائه خدمات ناشی از وقایع و حوادث طبیعی ( سیل، زلزله، طوفان و ...) و حوادث پیش بینی نشده عمدی و سهوی انسانی، بانک اقدام به تعریف یک برنامه اقتضایی کارآمد کرده و وظایف هر یک از کارکنان را در چنین شرایطی به طور دقیق مشخص کرده و به آنها آموزش های لازم را ارائه دهد. تهیه سیستم ها و بانک های اطلاعاتی پشتیبان که به صورت روزانه به روزرسانی می شوند و استقرار آنها در مکان جغرافیایی متفاوت از محل استقرار سرورها و پایگاه های داده ای اصلی از نکات حائز اهمیت در این زمینه است.
- ۴- در حوزه زیرساخت تکنولوژیکی پیشنهاد می شود بانک با عقد قرارداد همکاری با شرکت های خصوصی تولیدکننده تجهیزات مخابراتی و وزارت ارتباطات و فن آوری اطلاعات، اقدام به سرمایه گذاری در این بخش کرده و زیرساخت های مخابراتی لازم برای فعالیت های بانکداری الکترونیک خود را تقویت کند. همچنین با توجه به این که دستگاه های خودپرداز و به تناسب آن کارت های اعتباری صادره این بانک از پایین ترین سطوح تکنولوژی روز دنیا (تکنولوژی دهه ۱۹۸۰) برخوردارند، این بانک می تواند با به روزرسانی این دستگاه ها و ارتقاء سطح تکنولوژی کارت های اعتباری خود علاوه بر ارائه خدمات متنوع تر، موجب ارتقاء زیرساخت های تکنولوژیکی و کاهش زیان های ناشی از کارآبی نامناسب دستگاه های خودپرداز خود شود. سرمایه گذاری در شبکه های اینترنتی و شرکت های ارائه کننده خدمات اینترنتی، تولیدکنندگان سخت

تحت بررسی‌های دقیق امنیتی قرار گیرند. قبل از ورود به خدمت باید سوابق گذشته کارکنان به دقت بررسی شود و به محض ورود باید سیاست‌های امنیتی مورد انتظار از کارکنان با توجه به نقش آن‌ها، به هر یک آموزش داده شده و پس از انجام آزمون‌های لازم و تأیید صلاحیت، به فعالیت مشغول شوند. در طول مدت فعالیت نیز به‌طور پیوسته و در مقاطع منظم و گاهی نامنظم تمامی سیاست‌های امنیتی تدوین شده درباره کارکنان ارزیابی شود.

### منابع

۱. پژوهشکده پولی و بانکی (۱۳۸۴)؛ "خدمات بانکداری الکترونیک و معیارهای اجرایی آن"، چاپ اول. تهران: پژوهشکده پولی و بانکی.
۲. حسن‌زاده، علی. (شهریور ۱۳۸۲)؛ "مدیریت ریسک در مبادلات الکترونیک"، مجله تازه‌های اقتصاد، ش ۱۰۰، صص ۱۵-۱۸.
۳. سلیمانی، رضا (۱۳۸۶)؛ "بررسی عوامل مؤثر بر ریسک عملیاتی نظام بانکداری الکترونیک"، پایان‌نامه کارشناسی ارشد. به راهنمایی دکتر سعید صفری و مشاوره دکتر محمد توکل محمدی، گروه مدیریت دانشگاه شاهد.
۴. شیخانی، سعید (۱۳۷۸)؛ "بانکداری الکترونیک و راهبردهای آن در ایران". چاپ اول. تهران: مؤسسه تحقیقات پولی و بانکی.
۵. شربت اوغلی، احمد، عرفانیان، امیر (تابستان ۱۳۸۵)؛ "مطالعه تطبیقی و اجرای مدل‌های اندازه‌گیری ریسک عملیاتی مصوب کمیته بال در بانک صنعت و معدن"، فصلنامه شریف. سال ۲۲. ش ۳۴، صص ۱-۱۷.
۶. عباسی‌نژاد، حسین، مهرنوش، مینا (۱۳۸۵)؛ "بانکداری الکترونیک". تهران: سمت.
7. Basel committee. (2003). Risk Management for

افزار و نرم‌افزار رایانه‌ای نیز از جمله راهکارهای پیشنهادی برای افزایش کیفیت و کمیت ارائه خدمات بانکداری الکترونیک می‌باشد که علاوه بر کاهش زیان‌ها و خطرات ناشی از ناکارایی شبکه‌های اینترنتی چه در محیط داخلی بانک و چه در محیط خارجی بانک، می‌تواند برای خود بانک نیز بسیار سودآور و اقتصادی باشد.

- ۵- در حوزه دسترسی به سیستم نیز پیشنهاد می‌شود تقسیم وظایف در مراحل انجام فرایندهای بانکداری الکترونیک به دقت و با منطقی پیشگیرانه انجام شود. تمامی تغییرات در محدوده‌های دسترسی ثبت و ضبط شود و هرگونه تغییر در این محدوده‌ها باید مستلزم تأیید مدیریت ارشد بانک، واحدهای کنترلی و نظارت و بازرسی بانک باشد. همچنین فعالیت کارکنان هم به صورت محسوس و منظم و هم به صورت نامحسوس و تصادفی کنترل شود. چرخش شغلی و جابجایی کارکنان نیز از دیگر سیاست‌های کنترلی است که می‌تواند در کاهش زیان‌های عملیاتی ناشی از کارکنان مؤثر باشد؛ هر چند که مؤسسات مالی به دلیل نیاز به تخصص بالا برای احراز پست‌های مرتبط با فعالیت‌های بانکداری الکترونیک نسبت به این امر تمایلی نشان نمی‌دهند، اما می‌توان با ارائه آموزش‌های مستمر به کارکنان و برنامه‌ریزی شغلی این مشکل را برطرف کرد.
- ۶- همچنین پیشنهاد می‌شود سیاست‌های مشابه‌ای را نسبت به کاربران خارجی بانک (مشتریان) به کار گرفت، تا فقط کاربران مجاز بتوانند در محدوده تعیین و تعریف شده اقدام به انجام عملیات و تراکنش‌های مجاز نمایند. تغییر دوره‌ای رمزهای عبور و کنترل‌های نامنظم و رهگیری تصادفی تراکنش‌های بانکداری الکترونیک از ابتدا تا انتها، از جمله رویه‌های پیشنهادی برای کنترل دسترسی کاربران به سیستم‌های بانکداری الکترونیک در بانک می‌باشد.
- ۷- در حوزه امنیت پیشنهاد می‌شود بانک سیاست دقیق و قوی امنیتی درباره کارکنان فعال در واحدهای مرتبط با فعالیت‌های بانکداری الکترونیک طراحی کرده و به اجرا درآورد. بر اساس این سیاست تمامی کارکنان قبل از ورود به خدمت تا مرحله خروج از خدمت، باید

14. Jarrow, Robert A. (2008). "Operational risk". *Journal of Banking & Finance*. NO 32, PP 870-879. Electronic Banking. Basel. Switzerland: Bank for International Settlements.
15. L.King, Jack. (2001). *Operational Risk Measurement and Modeling*. USA : John Wiley & Sons Ltd.
16. Loader, David. (2007). *Managing a key component of operational risk under Basel II*. Cornwall. Britain: MPG Books Ltd.
17. Muermann, Alexander. Oktom, Ulku. (2002). "The Near-Miss Management of Operational Risk". The Wharton School, University of Pennsylvania.
18. Pennathur, Anita K. (2001). "e-Risk Management for Banks in the Age of the Internet". *Journal of Banking and Finance*. No 25, PP 2103- 2123.
19. Wahlstrom, Gunnar. (2006). "Worrying but Accepting New Measurements: the Case of Swedish Bankers and Operational Risk". *Critical Perspectives on Accounting*. NO 17, PP 493-522.
8. Basel committee. (1998). *Risk management for Electronic Banking and Electronic Money*. Basel. Switzerland: Bank for International Settlements.
9. Chorafas, Dimitris N. (2004). *Operational Risk Control with Basel II*. Oxford. Britain: Elsevier Finance.
10. Cornalba, Chiara., Giudici, Paolo. (2004). "Statical Model for Operational Risk Management". *Physica A*. No 338, PP 166- 172.
11. Cummins, David., M. Lewis, Christopher., Ran, Wei. (2006). "Market Value Impact of Operational Loss Event for US Banks and Insures". *Journal of Banking & Finance*. NO 30, PP 2605- 2634.
12. Gup, Benton. E., Kolari, James W. (2005). *Commercial Banking the Management of Risk*. Third edition. USA: John Wiley & Sons. Ins.
13. Hussain, Amanat. (2000). *Managing Operational Risk in Financial Markets*. Britain: Planta Tree Publication.