مدیریت ریسک در بانکداری الکترونیک

دکتر نوروز کهزادی

رئیس هیات مدیره و مدیرعامل بانک توسعه صادرات ایران

مقدمه

سرعت تحولات بازارهای مالی به ویژه طی دو دهه اخیر موجب پیچیده‌تر شدن ساختار فعالیت‌های مالی در سطوح مختلف گردیده است. از بین رفتن مرزهای سنتی بین فعالیت بانکها و مؤسسات مالی غیربانکی از یک سو، و ظهور مفاهیم و روش‌های جدید در زمینه مبادلات از سوی دیگر، اهمیت مقوله ریسک در فعالیتهای مالی و بانکی را بیش از پیش نمایان ساخته است. در این راستا بحرانهای مالی که هر از چندگاه در عرصه بین‌المللی به وقوع می‌پیوندد و کمترین اثر آن تحرکات تخریبی سرمایه است، توجه بانکداران و مقامات مالی را به خود جلب نموده و آنها را به همیاری و تلاش مشترک برای ریشه‌یابی مشکلات و نیز جستجوی راه‌حل‌های مقابله با شوکها اعم از شوکهای قیمتی، شوکهای نقدینگی، و شوکهای مربوط به ساختار مؤسسه مالی، تغییرات در چارچوب قانونی، یا تغییر عرضه و تقاضای دارائیها در شرایطی که ساختار مالی با آن تطابق نداشته است)، فرا خوانده است.

ظهور تجارت الکترونیکی و روند رو به رشد آن در سطح جهان و همچنین شکل‌گیری بانکداری الکترونیکی و توسعه روزافزون روش‌های نوین مبادلات پولی، احتمال وقوع نارسائی در سیستم بانکی یک کشور و توسعه خطرات ناشی از آن به سایر کشورها را افزایش داده که این امر می‌تواند به نوبه خود ثبات مالی در سطح بین المللی با مخاطره مواجه سازد. از اینرو موضوع ریسک و نحوه مدیریت آن در بانکداری الکترونیکی به طور ویژه‌ای مورد توجه دست‌اندرکاران قرار گرفته است. بنابراین لازم است ضمن اهتمام به فراهم ساختن زیر ساختارهای لازم برای گسترش هرچه بیشتر تجارت و بانکداری الکترونیکی، موضوع ریسک در بانکداری الکترونیکی و نحوه مدیریت آن نیز مورد توجه قرار گیرد. یکی از پیش نیازهای تحقق این امر که مقدم بر موضوع بانکداری الکترونیکی نیز می‌باشد، برقراری سیستمهای مدیریت ریسک یکپارچه در بانکهاست که به دلایل مختلف، از جمله عدم ارتباط و پیوستگی لازم سیستم مالی و بانکی کشور با سایر سیستم‌های بانکی و نیز بازارهای جهانی کمتر به آن توجه شده است.

اگرچه در سالهای اخیر ایجاد سیستم مدیریت ریسک در نظام بانکی کشور به عنوان یکی از بخش‌های عمده اصلاحات راهبردی مطرح گردیده، لیکن بنظر نمی‌رسد تاکنون فعالیت چشم‌گیری در زمینه برقراری یک سیستم یکپارچه و منسجم مدیریت ریسک صورت گرفته باشد. بدین ترتیب به منظور برقراری مدیریت ریسک بانکداری الکترونیکی قبل از هرچیز ایجاد سیستم مدیریت ریسک امری ضروری است.

در این مقاله سعی شده انواع ریسک در بانکداری الکترونیکی، وجوه تشابه و افتراق ریسک در بانکداری الکترونیکی و بانکداری سنتی و نحوه مدیریت آن تبیین گردد. در این راستا در ادامه ابتدا موضوع ریسکهای عملیات بانکی و مدیریت آن ارائه می‌شود. سپس ضمن مروری بر بانکداری الکترونیکی، نحوه پیدایش و شکل‌گیری و زیرساختهای لازم برای آن ارائه می‌شود. سپس با بیان

ریسک‌های مطرح در بانکداری الکترونیکی به نحوه مدیریت ریسک‌های مطروحه پرداخته خواهد شد.

ریسک‌های متداول عملیات بانکداری

محققان و صاحب نظران در زمینه انواع ریسک در عملیات بانکی به دلیل گستردگی و تنوع فعالیت‌های بانکی، اتفاق نظر ندارد. برخی از صاحبنظران[۱] ریسک اعتباری، ریسک نرخ بهره و ریسک نقدینگی را از جمله ریسک‌های اصلی عملیات بانکی بر می‌شمارند، در حالیکه برخی دیگر[۲] معتقدند ریسک بازار، ریسک اعتباری، ریسک نقدینگی، ریسک عملیاتی، ریسک قانونی و ریسک عوامل انسانی مهمترین ریسک‌های عملیات بانکی هستند.

اگرچه نظرات و دیدگاههای صاحب نظران در مورد انواع ریسک‌های عملیات بانکی متفاوت است، با این وجود ریسک‌های عمده عملیات بانکی را در شش گروه به ترتیب زیر می‌توان تقسیم‌بندی نمود[۳]:

۱- **ریسک اعتباری**[۴]: احتمال یا خطر عدم بازپرداخت وام توسط وام گیرنده ریسک اعتباری نام دارد. با توجه به سهم اندک سرمایه بانکها از کل ارزش دارائیهای آنها، کافی است که درصد کمی از وامها قابل وصول نباشند تا بانک با خطر ورشکستگی روبرو شود.

۱- Sinkey (1992)

۲- Crouhy (2001)

۳- Rose (1997)

۴- Credit Risk

۲- ریسک نقدینگی[۱]: خطر بروز کمبود نقدینگی برای تأمین هزینه‌های جاری و نیز تقاضای سپرده‌گذاران در بانکها ریسک نقدینگی نامیده می‌شود.

۳- ریسک بازار[۲]: تغییرات در انواع نرخ‌ها می‌تواند مدیریت پورتفولیوی دارائیهای بانک را، خصوصاً در زمینه دارائیهایی چون اوراق قرضه دولتی و سایر اوراق بهادار قابل معامله، با بحران مواجه نماید. این تغییرات می‌تواند قیمت بازار اوراق مورد نظر را دستخوش تغییر نماید. هرگونه تغییر ارزش دارائیها که در اثر تغییر نرخ بهره پدید آید به عنوان ریسک بازار شناخته می‌شود.

۴- ریسک نرخ بهره[۳]: تغییر در نرخ بهره می‌تواند در حاشیه درآمد عملیاتی بانک اثر بگذارد. به همین دلیل اثر تغییرات نرخ بهره روی حاشیه سود بانک، ریسک نرخ بهره خوانده می‌شود.

۵- ریسک درآمد[۴]: خطر هرگونه تغییر در درآمد خالص پس از کسر مالیات بانک، ریسک درآمد نامیده می‌شود.

۶- ریسک عدم کفایت در پرداخت تعهدات[۵]: خطر عدم توانائی ادامه فعالیت بانکها در بلندمدت در اثر کثرت وامهای معوق، کاهش ارزش پورتفولیوی دارائیها و افزایش ضرر وزیان، ریسک عدم کفایت در پرداخت تعهدات نامیده می‌شود.

---

۱ - Liquidity Risk

۲ - Market Risk

۳ - Interest Rate Risk

۴ - Earning Risk

۵ - Solvency Risk

ساختار مدیریت ریسک در بانک

بـر اسـاس ادبیات نظری مدیریت ریسک، مراحل فرآیند مدیریت ریسک در عملـیات بانکـی کـه بر کنترل و مدیریت چهار ریسک عمده عملیات بانکی، یعنی ***ریسـک اعتباری، ریسک نرخ بهره، ریسک نرخ ارز و ریسک نقدینگی*** متمرکز می‌باشد، به شرح ذیل است:

- اسـتاندارد سـازی: تعییـن استانداردها و الگوها جهت شناسائی و مدل سازی ریسک
- محاسـبه: تعییـن مقـدار کمـی ریسـک مورد نظر بر اساس مدل‌های تعریف شده
- محـدود سـازی دامـنه پذیرش ریسک: تعیین دامنه مورد قبول برای پذیرش ریسک در عملیات بانکی
- مدیریـت: تعیین برنامه‌های راهبردی مناسب همچنین کنترل، تقلیل و پوشش ریسک با استفاده از ابزارهای مناسب

همچنیـن بانکهـا نـیز همچون سایر مؤسسات مالی برای مدیریت ریسک باید سیاسـت‌هـای مناسـبی را بـه طـور گسترده در سطح تمام سازمان به کار بسته و متدولوژیهای مربوطه را به همراه زیر ساختارهای لازم ایجاد نمایند.

یکـی از اجـزاء اصلی فرایند مدیریت ریسک، انجام محاسبات و مدیریت همه ریسـک‌های بانک تحت شاخص‌ها و استراتژی یکسان می‌باشد. در این راستا تمام ریسـک‌هایـی کـه بانک با آن مواجه است از جمله ریسک اعتباری، ریسک بازار، ریسـک نقدینگـی و ریسک عملیاتی باید پوشش داده شود. یکپارچه‌سازی ریسک موجـب مـی‌شود که بانک با در نظر گرفتن هم‌زمان ریسکها اثرات و همپوشی هر یک بر دیگری را تحت کنترل درآورد.

بـر ایـن اسـاس مـی‌توان ارکان سیستم مدیریت ریسک در بانکها را به شرح ذیل بر شمرد:

سیاسـتگذاری: سیاسـتگذاری زمینـه‌هـای ریسـک بـازار، ریسـک اعتباری و ریسک عملیاتی را شامل می‌شود.

مـتدولوژی: در ارتباط با متدولوژی، لازم است بانک مدلهای تحلیلی در زمینه ریسـکهای بـازار، اعتـباری و عملیاتـی، و نیز روش‌های تحلیلی برای قیمت‌گذاری ایجـاد نمـاید. بانکهـا بـا توجـه بـه رابطـه بین ریسک و بازده، باید از روش‌های محاسـباتی کارا برای تعیین وضعیت خود برخوردار باشند و نهایتاً باید متدولوژی لازم را جهت محاسبه بازده سرمایه بر اساس ریسک موجود برقرار نمایند.

زیرسـاختارها[۱]: رکـن دیگـر مدیریـت ریسـک زیرساختارهاسـت. یکـی از مهمتریـن زیرسـاختارها نـیروی انسـانی می باشد. زیرا مدیریت ریسک تنها ابزار تحلیلـی صـرف نیسـت بلکـه ایـن انسانها هستند که نهایتاً بر اساس ابزار موجود تصـمیم‌گـیری و قضـاوت مـی‌نمایـند. عـامل مهـم دیگـر در زمینه زیرساختارها یکـپارچه‌سازی و هماهنگی عملیات مدیریت و فناوری است. بدین منظور استفاده از ابـزار محاسـباتی چـون رایانـه و نـرم‌افزارها و سخت‌افزارهای مربوطه موجب سـرعت و دقـت عملیات خواهد شد. عملیات اتوماسیون سیستم‌های ریسک نباید جـدا از هم باشد بلکه لازم است که ضمن حفظ یکپارچگی، از همپوشی و عملیات تکـراری و مـوازی در آنهـا خـودداری شود. همچنین برای حفظ موقعیت رقابتی سیسـتم اطلاعاتی، بانک باید توانائی استفاده از اطلاعات روزآمد خارج از سازمان را نـیز داشـته باشـد. یکـی دیگـر از زیرسـاختارهای مهم برای مدیریت ریسک سـاختار فـناوری اطلاعـات مـی‌باشد. مدیریت فعال ریسک باید بتواند اطلاعات لازم بـرای اداره و مدیریـت ریسـک و نـیز سـاختن توابع تحلیلی را ایجاد نماید. همچنین بانک باید توانائی حفظ و ایجاد اطلاعات پشتیبان را نیز داشته باشد.

۱-Infrastructures

در هسته سیستم مدیریت ریسک، مدیران مستقل تراز اول ریسک که از دانش کافی در این زمینه برخوردارند، قرار داشته و مدیریت ریسک را در زمینه‌های زیر به عهده دارند:

- تعیین ریسک‌هایی که بانک می‌تواند متقبل شود
- تحلیل ریسک
- تعیین خصوصیات سرمایه‌ای بانک
- تحلیل ریسک قیمت گذاری
- مدیریت پورتفولیو

بانکداری الکترونیکی

پیشرفت و توسعه سریع فناوری اطلاعات و ارتباطات طی دو دهه اخیر، جهان را با تحولاتی شگرف مواجه نموده است. ایجاد و خلق مفاهیم نوینی همچون تجارت الکترونیکی، اینترنت، پول الکترونیکی، بانکداری الکترونیکی، بیمه الکترونیکی، تأمین مالی الکترونیکی و حتی دولت الکترونیکی، دروازه‌های جدیدی از پیشرفت و توسعه را به روی بشریت گشوده است. روند تولید و خلق خدماتی با پسوند الکترونیکی چنان سریع و شتابان است که از تحولات مزبور به عنوان انقلاب الکترونیکی یاد می‌نمایند. در این بین تجارت الکترونیکی مکانیزم‌های جدیدی برای مبادلات تجاری داخلی و بین‌المللی کشورها ایجاد نموده که به سبب مزایایی همچون کاهش هزینه مبادلات و افزایش سرعت معاملات، به طور روزافزون مورد استقبال و توجه کشورها قرار گرفته‌اند. از سوی دیگر به سبب گریزناپذیر بودن جریان مبادلات پولی در تجارت الکترونیکی پدیده دیگری به نام سیستم‌های پرداخت الکترونیکی ایجاد شده که مکمل فرآیند تجارت الکترونیکی می‌باشد. در این میان بانکها نیز با ارائه خدمات بانکداری الکترونیکی به جایگاهی رسیده‌اند که به عقیده برخی صاحبنظران بدون آنها انجام تجارت الکترونیکی بسیار مشکل خواهد بود. با توسعه اینترنت در سطح جهان و به سبب دسترسی آسان افراد به آن، این شاهراه اطلاعاتی به عنوان

بستری برای بانکداری الکترونیکی به طور روز افزونی مورد استفاده قرار می‌گیرد.

پیشرفت‌های بیشتر در زمینهٔ خدمات بانکی الکترونیکی با همگانی شدن رایانه‌های شخصی وتوسعه تکنیک‌های جدید ارسال و دریافت اطلاعات (در شکل سوئیچینگ Packetهای حاوی اطلاعات که امکان ایجاد مکانیزمی را برای جریان اطلاعات در سطح ملی و بین المللی فراهم می‌نمود)، حاصل شد.

از همین زمان، مسالهٔ "امنیت" در شبکهٔ بانکی بلافاصله در صدر توجه قرار گرفت. در حقیقت عمدهٔ مشتریان به دلیل عدم آشنایی با تکنولوژی بکاررفته در سیستم فوق، نسبت به آن بی‌اعتماد بوده و نگران از دست رفتن منابع مالی و اعتباری خویش گردیدند.

در آغاز دههٔ ۹۰ میلادی با شکل گیری ابزار نوین الکترونیکی تحت عنوان "پول الکترونیکی"، بانکداری الکترونیکی وارد مرحلهٔ بلوغ خود گشت و امکان انجام عملیات فراگیر بانکی در سطح بین المللی از جمله معاملات ارزی، گزارش دهی از وضعیت موجودی، تامین مالی و... ، فراهم گردید.

امروزه در کنار این پیشرفت‌های فوق‌العاده و افزایش چشمگیر سرعت و دقت در عملیات بانکی تحت اینترنت، احتمال انواع اخلال‌ها و اشتباهات برگشت ناپذیر نیز افزایش یافته است و آینده بانکداری الکترونیکی را چالش بین این امکانات و مخاطرات رقم خواهد زد.

قابلیت های بانکداری الکترونیکی

طی سال های اخیر و با توسعه فناوری‌های الکترونیکی مؤسسات مالی انواع خدمات الکترونیکی را در اختیار مشتریان خود قرار داده‌اند که از جمله می‌توان به بانکداری تلفنی و شبکه های خود پرداز[۱] و سیستم اتاقهای پایای خودکار اشاره نمود. همچنین از طریق دسترسی به اینترنت امکان ارائه خدماتی که قبلاً بانکها به صورت سنتی در اختیار مشتریان قرار می‌دادند مانند گشایش حساب، انجام حوالجات، اعطای وام و... ، وجود دارد. از سوی دیگر با ظهور پدیده پول

---

۱ -Automated Teller Networks

الکترونیکی خدمات جدید نیز در این زمینه شکل گرفته و در حال توسعه می‌باشد. در ادامه برای بررسی و نظارت بر نحوه ارائه خدمات بانکی در چارچوب بانکداری الکترونیکی و نهایتاً بررسی خطرات و ریسک‌های آن، ویژگی‌های سیستم‌های پرداخت الکترونیکی مورد بررسی قرار می‌گیرند.

سیستم‌های پرداخت الکترونیکی

سیستم پرداخت در بانکداری الکترونیکی بر اساس قابلیت‌ها و فناوریهای الکترونیکی فعالیت می‌نماید. به عبارت دیگر فناوریهای موجود به منظور مبادلات بانکی و انجام سایر خدمات مربوطه بکار گرفته می‌شوند. سیستم‌های پرداخت در بانکداری الکترونیکی و سنتی هر دو از سه مرحله درخواست پرداخت[۱]، تسویه و توزیع تشکیل شده‌اند. در هر دو حالت اعتماد طرفین مبادله و محرمانه بودن در مقبولیت و بقای سیستم‌های مبادله نقش اساسی ایفا می‌نمایند

مشخصه‌های سیستم‌های پرداخت

سه زمینه عمده برای مشخصه‌های یک سیستم پرداخت الکترونیکی وجود دارند که عبارتند از اجزای سیستم[۲]، متدولوژی فرآیند[۳] و ساختار سیستم[۴]. این مشخصه‌ها در سطحی گسترده نمایانگر ریسک و خطرات موجود در سیستم پرداخت می‌باشند. البته ریسک سیستم پرداخت به طور قابل توجهی به عواملی نظیر کاربری سیستم، نظارت و کنترل طرفهای شرکت کننده در عملیات نیز بستگی دارد. در جدول (۱) مشخصه‌های مربوط به سیستم پرداخت با توجه به سه زمینه فوق‌الذکر ارائه شده است.

---

۱ -Payment Entry

۲ -System Components

۳ -Process Methodology

۴ -System Structure

جدول (۱): مشخصه‌های سیستم‌های پرداخت	
اجزای سیستم	فناوری تراشه‌های الکترونیکی در مقابل فناوری نوار مغناطیسی سیستم کارتی در مقابل سیستم‌های مبتنی بر رایانه سخت افزار(رایانه شخصی، کارت خوان، خود پرداز و...)
متدولوژی عملیات	فرآیند دسته‌ای[۱] در مقابل عملیات همزمان[۲] دسترسی به‌هنگام در مقابل دسترسی غیر به‌هنگام
ساختار سیستم	پول قانونی(رایج) در مقابل ارزش (پول) منتشره از طرف یک بنگاه خاص پول واحد و یا چندگانه سیستم‌های برپایه بدهی در مقابل سیستم‌های برپایه اعتبار سیستم‌های باز* در مقابل سیستم‌های بسته سیستم‌های قابل بارگذاری دوباره[۳] در مقابل سیستم‌های یک بار مصرف[۴] سیستم‌های کنترل شده در مقابل سیستم‌های ایمن سیستم‌های مجتمع[۵] در مقابل سیستم‌های مجزا[۶] عدم افشای نام کاربر[۷] مکانیزم پرداخت (ارتباط بین فروشنده و خریدار) نحوه تسویه پرداختها حجم مبادله (خرد و یا کلان) سطح دسترسی جغرافیائی

*سیستم‌هایی باز تلقی می‌شوند که در سطح جغرافیایی گسترده‌ای و توسط تعداد زیادی از بنگاههای تجاری و برنامه‌های مختلف مورد استفاده قرار گیرند و بالعکس سیستم‌های بسته آنهایی هستند که دارای برد جغرافیایی و کاربران محدود می‌باشند.

- در جدول فوق فقط شاخص‌های اصلی تصمیم‌گیری در مورد سیستم‌های پرداخت مورد نظر بوده و نرم افزارهای مورد استفاده در نظر گرفته نشده است هرچند نوع نرم افزارها به طور ضمنی با موارد فوق در ارتباط است. همچنین حالت‌های ذکر شده برای زمینه‌های فوق‌الذکر لزوماً گسسته نیستند بلکه حالتهای بینا بین نیز ممکن است.

مأخذ: Federal Deposit Insurance Corporation, Division of Supervision, ***Electronic Banking***, 1998, p 5.

---

۱ -Batch

۲ -Real-Time

۳ -Reloadable

۴ -Single Use

۵ -Integrated

۶ -Stand alone

۷ -User Anonymity

نقش بانکها در سیستم‌های پرداخت الکترونیکی

فعالان عمده سیستم‌های پرداخت الکترونیکی عبارتند از کاربران (مشتریان)، مؤسسات مالی، اشخاص (طرفهای ذی مدخل در عملیات) و بانکهای مرکزی. بانکها همچون سایر فعالان سیستم، وظایف مختلفی را به عهده داشته و به تبع آن با ریسکهای متفاوتی نیز مواجه می‌باشند. در ادامه ضمن اشاره به نقش بانکها در سیستم‌های پرداخت الکترونیکی، ریسکهای مربوط به هر یک از آنها نیز ارائه می‌شود.

- **مالک و سرمایه‌گذار**: بانکها می‌توانند نسبت به جذب سهام‌داران و سرمایه‌گذاران و همچنین مشارکت در سایر سرمایه‌گذاریها اقدام نمایند. بدین ترتیب بانکها با توجه به تصمیم‌گیری در زمینه‌های مربوطه با انواع ریسک‌های مالی، سیستمی، شهرت و استراتژیک مواجه می‌گردند.

- **گسترش دهنده و توسعه دهنده سیستم**: گسترش و توسعه سیستم می‌تواند به صورت درون سازمانی توسط خود بانک صورت بگیرد و یا از طریق موافقت و قرارداد با سایر افراد انجام شود. در هر صورت این امر ریسک‌هایی همچون ریسک‌های مالی، سیستمی، شهرت و استراتژیک را در پی دارد.

- صادرکننده و انتشار دهنده[۱]: در چارچوب این نقش بانک نسبت به فروش اسناد و به طور کلی ارزش ذخیره شده[۲] به سایر افراد اقدام می‌نماید. بدین ترتیب بانک با توجه به بدهی ایجاد شده با ریسک‌های مبادله و نقدینگی مواجه می‌شود. از سایر ریسک‌هایی که در این زمینه مطرح است می‌توان به

---

۱ -Issuer

۲ -Stored Value

ریسک‌های استراتژیک، پذیرش (قبولی)[۱] و ریسک شهرت اشاره نمود که با توجه به خطر تقلب و یا سوء ظن نسبت به صحت اسناد و ارزش صادر شده به وجود می‌آیند.

- **توزیع کننده و جبران کننده**[۲]: در قالب این دو نقش بانک با توزیع دوباره و مباد له ارزشی که در اختیار دیگران قرار گرفته است و نیز پشتیبانی، از سیستم مربوط به ارزش ذخیره شده حمایت می‌نماید. در این ارتباط بانک می‌تواند رأسا مسئولیت این امررا به عهده گرفته و یا از ظرفیت‌های مضاعف بدین منظور استفاده کند. در چارچوب نقش توزیع کننده، ریسک‌های انتقال، پذیرش، شهرت، اعتباری و نقدینگی متوجه بانک می‌باشد. از سوی دیگر در قالب نقش جبران کننده بانک با ریسک‌های اعتباری و انتقال مواجه می‌شود.

- **صدور مجوز و اجرا کننده عملیات**: این نقش مشابه نقش بانک‌ها در زمینه مدیریت کارت‌های اعتباری است که در آنها مجوز عملیات قبل از انجام آن صادر می‌شود. در این حالت مسئولیت بانکها عبارتست از ارائه مجوز، ارسال پول و یا ارزش، تسویه و پرداخت نهائی است. ریسک‌های موجود در این زمینه ریسک اعتباری و نقدینگی است که می‌توان با عملیات اجرائی معاملات آن را پوشش داد.

- **نگهداری آمار و اطلاعات معاملات انجام شده**: هرچند این بخش از عملیات بسیار اجرائی به نظر می‌رسد، لیکن این نقش، پیگیری بازرسان و حسابرسان و رفع مناقشات ممکن بین اجزای عمل کننده را تسهیل می‌نماید. به هرحال ایفای ناکارای این نقش موجب افزایش ریسک‌های انتقال، شهرت و ریسک پذیرش می‌گردد.

۱-Compliance

۲-Redeemer

- **تأییدکننده و پشتیبانی کننده**: در این چارچوب مؤسسه مالی به عنوان تأیید کننده مبادلات الکترونیکی ایفای نقش می‌نماید. بدین ترتیب که بانک طرفهای شرکت کننده در مبادله الکترونیکی را تأیید می‌نماید. لذا بروز هرگونه خطا در این زمینه می‌تواند به بروز تعهدات عمده برای بانک منجر شود.

- **سایر نقش‌ها**: به سبب اینکه بسیاری از سیستم‌ها به صورت اعتباری (مانند کارت اعتباری) و یا بر پایه بدهی (مانند کارتهای بدهی) طراحی شده‌اند، بانکها می‌توانند در این چارچوب وظایف سنتی خود را نیز ایفا نمایند. این امر می‌تواند به صورت ارائه خدمات اطلاعات رسانی و یا حسابهای اداره شده در راستای سفارش سایر ارائه دهندگان خدمات کارتهای اعتباری و بدهی صورت پذیرد.

ریسک‌های عملیات بانکداری الکترونیکی

صرف نظر از اینکه عملیات بانکداری الکترونیکی در چه سطحی از پیشرفتگی و تخصص انجام شود در تمام ابعاد آن به صورت ذاتی ریسک‌ها و خطراتی وجود دارد. برای مثال اطلاعات مندرج در وب سایت ممکن است توسط افراد غیر مجاز تغییر یابد. پست‌های الکترونیکی که دارای اطلاعات محرمانه و یا مربوط به اموال اشخاص باشند، به طور اشتباه توزیع شوند. همچنین ممکن است افراد غیر مجاز به سیستم‌های شبکه‌ای بانک که به سیستم یا بانک اطلاعاتی مرکزی متصل می‌باشند، دسترسی یابند. از سوی دیگر نقص و از کار افتادگی سیستم در اثر تغییرات و نوسانات برق نیز از مخاطرات بالقوه می‌باشند. علاوه بر این سیستم پرداختهای الکترونیکی نیز به طور ذاتی و بالقوه با انواع ریسک‌ها مواجه‌اند. به بیان دیگر در عملیات بانکدای الکترونیکی بانکها علاوه بر ریسکهای مربوط به عملیات بانکداری سنتی، با ریسک‌های منحصر به فرد انتقال منابع و خدمات از طریق کانالهای الکترونیکی نیز روبرو می‌باشند. این ریسک‌های منحصر به فرد عمدتاً به افزایش قابل توجه سرعت عملیات، دسترسی گسترده

از طریق شبکه در اقصی نقاط جهان، تنوع کاربران، بانکهای اطلاعاتی، و سیستمهای جانبی[۱] مربوط می‌باشند. باید توجه داشت سرعت بالای عملیات انتقال الکترونیکی در سطح شبکه‌ها موجب می‌شود ریسک‌های بانکداری سنتی همچون *ریسک اعتباری، نقدینگی و ...* ، از اثرات و تبعات سریعتری برخوردار باشد.

ریسک‌های خاص عملیات بانکداری الکترونیکی

ریسک‌های خاص عملیات بانکداری الکترونیکی را می‌توان در شش زمینه به شرح جدول (۲) که عمدتاً در اتباط با انتقال اطلاعات، سیستم‌های پرداخت الکترونیکی، و عدم قطعیت قانونی می‌باشند، مطرح نمود.

هر چند در جدول (۲) به ریسک‌های گوناگونی اشاره شده است، لیکن یکی از خطرات عمده در زمینه بانکداری الکترونیکی مربوط به اختلالات و نقایص سیستم در ارتباط با شبکه‌های به هم پیوسته رایانه‌ای می‌باشد. به همین دلیل معمولاً به این موضوع توجه بیشتری معطوف می‌گردد. علل عمده بروز نقایص و اختلالات مذکور عبارتند از سوانح و مشکلات طبیعی، حمله و نفوذ به سیستم و نقایص مربوط به افراد و اشخاص ثالث. در ادامه ریسک‌های مربوط به زمینه‌های یاد شده تشریح می‌گردد:

- **سوانح و مشکلات طبیعی**: ریسک وقوع سوانح و مشکلات طبیعی با گسترش جغرافیایی عملیات بانکداری الکترونیکی و نیز توسعه شبکه‌های رایانه‌ای افزایش می‌یابد. برای مثال با گسترش شبکه لازم است تا سرورهای[۲] مختلفی در گستره جغرافیایی استقرار یابند و ارتباطات مخابراتی لازم برای برقراری ارتباط با مشتریان و سایر افراد ایجاد گردد. بنابراین بروز مشکل در هر بخش ممکن است موجب اختلال در انجام کار سیستم شود.

---

۱ -Peripheral Systems

۲ -Servers

- **حمله و نفوذ به سیستم**: حملات داخلی و یا خارجی ممکن است به منظور جلوگیری از ارائه خدمات به دیگران و یا به منظور دسترسی به بانکهای اطلاعاتی، دستکاری در برنامه‌ها و یا تغییر در مشخصه‌ها و نتایج مالی صورت پذیرد. به جز مقاصد مالی، انگیزه‌های نفوذ به سیستم می‌تواند صرفاً به منظور غلبه بر سیستم امنیتی و جاسوسی تجاری[۱] باشد. در این ارتباط افراد نفوذگر سعی می‌نمایند به صورت مخفی به سیستم نفوذ کنند که این امر تعیین و تشخیص افراد مزبور و نیز روش بکارگرفته شده از سوی آنها را با مشکل مواجه می‌نماید.

- **نقص مربوط به افراد و اشخاص ثالث**: نقص در عملکرد افراد و اشخاص ثالث که در انجام عملیات سیستم‌های پرداخت سهیم هستند می‌تواند اثرات مالی قابل توجهی برروی تمام دست‌اندرکاران سیستم ایجاد نماید. برای مثال بر اساس قرارداد منعقده بین تمام افراد درگیر در عملیات بانکداری الکترونیکی ممکن است به این نکته تأکید شده باشد که در صورت وقوع ضرر و زیان از سوی یکی از افراد، تمام افراد در ضرر حاصله شریک باشند. لذا در بدترین حالت ممکن، زیان ناشی از نقص و مشکل مربوط به یک فرد می‌تواند به زیان بقیه نیز منجر شود. چرا که به سبب نقص یکی از اجزا و نیز با توجه به ارتباط آن با سایر افراد اعتماد و اطمینان عمومی نسبت به کل سیستم شدیداً تحت الشعاع قرار می‌گیرد. بدین ترتیب با توجه به اهمیت مخاطرات مربوط به عملیات بانکداری الکترونیکی و نیز گستردگی اثرات آن بر اعتماد مردم در نظر گرفتن تمهیدات لازم برای مدیریت ریسک‌های مزبور از اهمیت به سزایی برخوردار می‌باشد.

---

[۱]-Commercial Espionage

جدول (۲): ریسک‌های خاص عملیات بانکداری الکترونیکی

زمینه ریسک	نوع ریسک و موضوعات مربوط به آن
برنامه‌ریزی و اجرا	روند ناکافی تصمیم‌گیری عمدتاً در ارتباط با برنامه‌ریزی و کاربرد امکانات الکترونیکی تأثیرات هزینه‌های استفاده از تکنولوژی‌های موجود بر موقعیت مالی شرکت برنامه استراتژیک مربوط به انجام فعالیت‌ها در سطح کشور و یا سطح بین‌المللی طراحی سیستم ممکن است خواسته‌های مشتریان را بر آورده ننماید افزایش رقابت از سوی مؤسسات غیر مالی به سبب گسترش خدمات الکترونیکی عدم قطعیت در ارتباط با بیمه خدمات الکترونیکی
سیاست‌ها و روش‌های اجرائی	ناکافی بودن تخصص مدیریتی و تکنیکی در ارتباط با استانداردهای فعالیت‌های بانکداری الکترونیکی ناکافی بودن کنترل‌های در زمینه حفظ محرمانه بودن اطلاعات ناکافی بودن سیاست‌ها و روش‌های اجرائی با توجه به سرعت انتقال اطلاعات و گستردگی کانال‌های الکترونیکی
نظارت و بازرسی	- ناکافی بودن پیگری حسابرسان و بازرسان در زمینه سیستم‌های الکترونیکی
قوانین و مقررات	عدم قطعیت قابلیت اعمال مفاد قراردادها، موافقتنامه‌ها و امضاهای دیجیتال موضوعات مربوط به خصوصی بودن اطلاعات کاربران و مشتریان موضوع بدهی‌های مشروط[۱] ناشی از مشتریان و افراد درگیر در عملیات الکترونیکی عدم قطعیت موضوعات قانونی مربوط به مالیات، جرائم، و قوانین مدنی نحوه اجرای عملیات تجارت داخلی و بین‌المللی محیط قانونی غیر شفاف و همراه با عدم قطعیت قانونی در زمینه قوانین منطقه‌ای، ملی، بین‌المللی همچنین در زمینه فعالیت‌ها و خدمات مالی و سایر زمینه‌های مرتبط عدم قطعیت در زمینه میزان ذخایر مربوط به پول الکترونیکی عدم قطعیت در ارتباط با ثبتهای مالی، افشا و سایر الزامات مربوط به عملیات الکترونیکی عدم قطعیت در ارتباط با تهیه اسناد الکترونیکی و نحوه افشای آنها با توجه به قوانین و مقرارت مختلف
مدیریت عملیات اجرائی	اختلالات و نقایص مربوط به عملکرد نرم‌افزارها و سخت‌افزارها مخاطرات مربوط به سیستم‌های اطلاعاتی و نیز اطلاعات موجود در آنها ظرفیت ناکافی سیستم از کارافتاگی یا قدیمی بودن سیستم اجرای پروتکل‌ها و استانداردهای چندگانه حفاظت ناکافی ارتباطات الکترونیکی کنترل‌های امنیتی ناکافی سیستم
پیمانکاران و اشخاص ثالث ارائه کننده خدمات	اطمینان به اشخاص ثالث ارائه کننده خدمات در رابطه با اجرای عملیات خطیر و مهم عدم گسترش کنترل‌های داخلی به اشخاص ثالث ارائه کننده خدمات پشتیبانی ناکافی سیستم از اشخاص ثالث ارائه کننده خدمات مدیریت و نگهداری سیستم‌های چندگانه که دارای ارتباطات داخلی هستند و نیز فعالیت‌های مربوط به آنها نقص در بررسی و نظارت ارتباطات درونی در بین مؤسسات مالی، اشخاص ثالث ارائه دهنده خدمات و نیز افراد شریک در سیستم‌های پرداخت الکترونیکی

مأخذ: Federal Deposit Insurance Corporation, Division of Supervision, ***Electronic Banking***, 1998, p 8.

---

۱ -Contingent Liabilities

مدیریت ریسک در بانکداری الکترونیکی

برای کنترل بهتر ریسک‌ها در بانکداری الکترونیکی باید ساختار سنتی مدیریت ریسک با نیازهای موجود در این زمینه تطبیق یابد. در ارتباط با مبادلات و سیستم‌های پرداخت الکترونیکی، مدیریت ریسک باید تمام ابعاد و زمینه‌های مهم ریسک‌های عملیاتی، قانونی و شهرت را پوشش دهد. با توجه به سطوح مختلف فعالیت، برای مدیریت ریسک در بانکداری الکترونیکی تمهیدات زیر باید در نظر گرفته شود: (FDIC,1998)

- نظارت عمومی در زمینه‌های برنامه‌ریزی و تحلیل، سیاست‌ها و نحوه اجرا، اختیارات و مسئولیتها، تبعیت از مقررات و چارچوب قانونی، منابع انسانی و حسابرسی
- عملیات مبادله شامل: اجازه استفاده، سلامت اطلاعات، غیرقابل انکار بودن مبادلات، و محرمانه بودن اطلاعات
- نظارت سیستم در زمینه منابع مورد نیاز، امنیت سیستم، قابل اعتماد بودن سیستم و برنامه‌ریزی مشروط، ظرفیت سیستم، سیاست واگذاری کار به اشخاص ثالث، و کنترل روز آمد بودن سیستم.

بر این اساس لازم است فرایند اجرایی مدیریت ریسک در زمینه‌های مختلف از جمله برنامه‌ریزی راهبردی و تحلیل امکان‌سنجی، نظارت و سرپرستی مدیریت و کنترل‌های داخلی، سیاست‌ها وروش‌های اجرائی و عملیاتی، نظارت بر سیستم، حسابرسی و نحوه انجام آزمون‌ها، امنیت فیزیکی مبادلات و سیستم، شناسایی افراد ثالث دست‌اندرکار در انجام عملیات، آمادگی در زمینه اتخاذ پاسخ مناسب به اتفاقات، پوشش و بهبود وقایع و پدیده‌های نامطلوب، ملاحظات تجاری و برنامه‌ریزی مشروط، و بررسی مستمر پیشرفت‌های تکنولوژیکی و بهبود ظرفیت‌های موجود، متمرکز شود (ebid). در تمام ابعاد فوق‌الذکر می‌توان از تکنیک‌های مدیریت ریسک عملیات بانکداری سنتی برای تجزیه و تحلیل

ریسک مربوطه استفاده نمود. البته در برخی موارد نیاز است تا تکنیک‌های خاصی برای کنترل ریسک در بانکداری الکترونیکی استفاده نمود که عبارتند از: برنامه‌ریزی راهبردی و تحلیل امکان سنجی، واکنش مناسب در مقابل اتفاقات و آمادگی طرح‌ها برای این منظور، روش‌های اجرائی و کنترل‌های داخلی. شایان ذکر است تعداد زیادی از مؤسسات، بخشی یا تمام عملیات مربوط به سیستم پرداخت و مبادله الکترونیکی را به اشخاص ثالث واگذار می‌نمایند. لیکن نهایتاً مسئولیت تمام عملیات مربوط به بانک، کنترل نامه‌های الکترونیکی، و سایر مواردی که به اشخاص ثالث واگذار شده بر عهده هیأت مدیره بانک است.

- **برنامه‌ریزی راهبردی و تحلیل امکان‌سنجی**: برنامه‌ریزی راهبردی و تحلیل امکان‌سنجی باید به عنوان یکی از بخشهایی که مدیریت ریسک بانکداری الکترونیکی بر آن تمرکز دارد در نظر گرفته شود. البته نباید در برخورد با این موضوع و در راستای حرکت به سمت محیط الکترونیکی بیش از حد بر موضوعاتی همچون حجم سرمایه‌گذاری عمده مورد نیاز، فرصتها و ریسک‌های مربوط به توسعه توانائیهای الکترونیکی تأکید گردد. برنامه‌ریزی راهبردی یک روند مستمر است که توسط آن اهداف و مأموریت سازمان توسعه و بهبود می‌یابد. از سوی دیگر هرچند در سازمانها تحلیل امکان‌سنجی دارای فرایندی مشابه با برنامه‌ریزی راهبردی است لیکن این تحلیل بیشتر بر روی یک طرح خاص متمرکز می‌باشد. تحلیل امکان‌سنجی باید از یک نقطه به عنوان فرصت بالقوه شروع و ادامه یابد. بر این اساس هر فرصت بالقوه باید در سه مرحله مورد بررسی قرار گیرد ۱) مطالعه، که در آن موارد لازم، نیازها و اهداف مربوطه تحلیل و حالت های ممکن برای انجام عملیات مورد بررسی قرار می‌گیرد، ۲) طراحی و توسعه که در آن بهترین راه حل ممکن بر اساس مشخصات فنی تعیین و سیستم راه اندازی، سیاست‌ها، روش‌های اجرایی و اسناد مربوطه مشخص می‌گردند،۳) مرحله عملیات که طی آن سیستم شروع به کار نموده و نگهداری می‌شود.

پس از راه اندازی و شروع به کار سیستم، لازم است به طور مرتب عملکرد آن براساس راهبردها و اهداف موجود، همچنین نیازهای اجرائی و توسعه فناوری مقایسه، بررسی و هرگونه نقص و کمبودی رفع گردد.

- **آمادگی برای واکنش مناسب به اتفاقات**: یکی از اهداف اولیه مدیریت ریسک کاهش اثرات منفی ناشی از وقوع یک مشکل می‌باشد. این امر در محیط‌های الکترونیکی به علت سرعت بسیار زیاد، پیچیدگی عملیات و دسترسی تعداد زیادی از کاربران، حائز اهمیت بیشتری است. علاوه بر این از آنجا که در سیستم‌های الکترونیکی برای دسترسی به وب سایت بانک افشای هویت مشتری و یا ارتباط با آن الزامی نیست، لذا به طور بالقوه خطر دسترسی برخی افراد به طور ناشناس جهت مقاصد غیر قانونی و سوء استفاده از سیستم وجود دارد. علاوه بر این به سبب ارتباط‌های داخلی بین اجزای مختلف سیستم، بروز یک مشکل می‌تواند بر زمینه‌های مختلفی از جمله مدیریت خدمات و تولیدات، بازاریابی و خدمات مشتریان و سایر بخش‌های عملیات اثر گذار باشد. برای مثال در تبلیغات الکترونیکی که اطلاعاتی در زمینه تولیدات، خدمات، نرخ‌ها و کارمزدها در اختیار کاربران قرار می‌گیرد، در صورت وجود اشتباه در اطلاعات ممکن است موجبات نارضایتی مشتریان و ایجاد تعهدات مشروط و یا از دست دادن سود و یا موقعیت بانک را فراهم آورد. همچنین در صورت نفوذ غیرقانونی به سیستم ممکن است در محتویات و اطلاعات موجود در وب سایت تغییر ایجاد شده و این امر در معرض دید عموم قرار گیرد و یا در اثر نقص کنترل و تمهیدات امنیتی، کاربران قادر به دسترسی، افشا و یا سوء استفاده از اطلاعات محرمانه باشند. بنابراین لازم است تا گروهی برای مقابله با مشکلات و اتفاقات، تجهیز و یا برنامه‌ای برای چگونگی برخورد با اینگونه موارد ایجاد گردد. البته پیچیدگی این امر به طور مستقیم به ریسک‌های ذاتی موجود در سیستم بستگی دارد. بدین منظور باید بر اساس یک برنامه اقتضائی ضمن تعیین اهداف، برای

مقابلـه بـا بحـران‌های ناشی از اتفاقات غیر مترقبه، مدیران ارشد و کارمندانی که عملـیات کلـیدی سـازمان را بـه عهده داشته و از تخصص و آمادگی کافی برای پاسـخ سـریع و مدبـرانه بـه مشـکلات برخوردارند، در قالب یک گروه مشخص مشـغول بـه فعالیت گردند. ترکیب و نحوه استفاده از گروههای مقابله با بحران و نـیز طـرح‌هـای از قـبل تعریف شده به طور کامل به سطح پیچیدگی سیستم‌های بـانکداری الکترونیکی بستگی دارد. در ارتباط با تعیین گروههای مقابله با بحران و یـا هـر طـرح مقابله دیگر، باید هدایت تصمیم‌گیری‌ها بر اساس قضاوت مدیریت باشـد. در نقطـه شـروع نـیز بـاید ریسک‌های سیستم‌های الکترونیکی و بخش‌ها، مـنابع، فعالیـت‌هـا و مـناطق اصـلی کـه بـه طـور بالقوه از ریسک‌های مزبور اثر مـی‌پذیـرند، تعیین شده و در گام بعدی افراد به صورت رسمی و با تعیین سلسله مراتب و نیز قدرت کافی برای مقابله با بحرانهای احتمالی به کار گمارده شوند.

- **روش‌هـای اجرائـی و کنـترل‌های داخلی**: هر قطعه و بخشی از سیستم‌های رایانـه‌ای مـی‌توانـد بـه طـور طبیعی و یا غیر طبیعی با تهدیدات مختلفی مواجه شـود. بـه سـبب ایـنکه بـا گسـترش دسترسـی بـه شبکه مقدار این خطرات نیز افـزایش مـی‌یـابد لـذا این امر می‌تواند شبکه را در مقابل مشکلات مزبور آسیب پذیـر نماید. البته با اتخاذ کنترل‌هایی می‌توان از سیستم‌های عملیاتی و نیز داده‌ها محافظـت نمود. نکته حائز اهمیت این است که برنامه‌های امنیتی کارا منحصر به یـک راه حـل نیستند و لازم است محاسبات و تمهیدات جهت تشخیص، نظارت، کنـترل و همچنیـن جلوگیری از ریسکهای بالقوه به صورت ترکیبی صورت پذیرد. کاراتریـن بـرنامه‌هـای کنترلی آنهایی هستند که در طی مراحل توسعه نسبت به تطبـیق سـخت‌افـزارها، نـرم‌افزارها و نیز تهیه راهنماهای کنترلی اقدام می‌نمایند. سیسـتم‌هـای کنـترل، بخـش جدائی‌ناپذیر هر برنامه مدیریت ریسک می‌باشد. از سـوی دیگـر بـرای حصـول حداکـثر کارائـی مدیـران باید به اهمیت یادگیری و آمـوزش کاربـران بـه مـنظور تبعیـت از استانداردهای کنترلی، واقف باشند. این آموزشـها بـاید کاربـران را بـا ریسـکهایی کـه عـدم تبعیـت از استانداردها ایجاد می‌نماید، آشنا سازد.

در جـدول (۳) ریسـک‌های بالقوه عملیات بانکداری الکترونیکی و همچنین راه حل کنترلی آنها ارائه شده است.

جدول (۳): ریسک‌های بالقوه بانکداری الکترونیکی و راههای کنترل آنها

ریسک‌های بالقوه	کنترل‌های لازم جهت کاهش ریسک
دسترسی غیر مجاز به اطلاعات سیسـتم امنیتـی بـه سـبب دسترسـی نفـوذ گـرها۲ بگونـه‌ای تغییـر مـی‌یـابد که امکان رد داده‌ها هنگام انتقال و یا ضبط آنها فراهم می‌گردد.	کنترل دسترسی برقـراری کنـترل هـای فیزیکـی و همچنیـن کنترل دسترسی به سیسـتم از قبـیل تمهـیدات امنیتـی مسـتقیم، کلمات عبور برای سیسـتم، دیوارهـای آتـش۱ و مکانـیزم‌های شناسائی دسترسی افراد غیر مجاز
از بین رفتن صحت داده‌ها بـه سبب تولید غیر مجاز اطلاعات، سیستم حسابرسی و نظـارت ضعیف، فقدان تأیید فیزیکی، اشتباهات و یا سـوء اسـتفاده، دقت داده‌ها و قابلیت اعتماد به آنها از بین می‌رود.	صدور مجوز کنـترل صـدور مجـوز دسترسـی بـه مـنظور نظـارت بر صحت داده‌هـا. کنـترل مـزبور در برگـیرنده تصـدیق و تأیید وصول۳، شناسـه‌هـای رایانـه‌ای۴، امضاهای دیجیتال، کنترل تغییرات۵ و تفکیک وظایف می‌باشد.
نقص در تکمیل مبادله و ضعف در انتقال مبادلات نقـص در انـتقال اطلاعـات مبادله در حین ارسال آن، مضـاعف شدن مبادله در حین انتقال و یا عدم توانائی ارسال مبادلات	تصدیق و تأیید وصول الـزام در کنـترل تصـدیق و تأیـید وصول، پیروی از پروتکل‌ها و اسـتفاده از نـرم‌افـزارهای ضـد ویـروس، پرونده‌های پشتیبان و برنامه‌ریزی مشروط

مـأخذ: Federal Deposit Insurance Corporation,Division of Supervision, ***Electronic Banking***,1998, p 12.

- **سـایر تمهـیدات**: هرچـند حمایـت از مـنافع مشتریان و سایر فعالیت های اختصاصـی در سـایر زمینه‌های کنترلی مورد توجه قرار می‌گیرند، لیکن ضعف در ایـن زمیـنه اثـرات مهمـی بـرای شـرایط کلی بانک ایجاد می‌نماید. لذا برقراری

---

۱ -Firewalls

۲ -Hackers

۳ -Acknowledgement

۴ -Computerized Logs

۵ -Edit Checks

سیستم‌های الکترونیکی که دامنه گسترده‌ای از فعالیتهای مورد نیاز مشتریان را پوشش دهد از اهمیت زیادی برخوردار است. چرا که در غیر این صورت ممکن است شرایط نارضایتی مشتریان فراهم آید که خود تبعات خاصی بر فعالیت‌های بانک خواهد داشت.

اصول مدیریت ریسک از نظر کمیته بال

کمیته بال معتقد است که می‌توان از طریق مدیریت بانکی، امنیت و اطمینان بنگاهها را تضمین و سیاست‌های مدیریت ریسک را معرفی و ارزیابی نمود تا بتوان حوادث و اتفاقات ناشی از فعالیتهای بانکداری الکترونیکی را مرتفع نمود.

کمیته بال چهار مدل ریسک را جهت کمک به بنگاهها برای پوشش ریسکهای مربوط به فعالیتهای بانکداری الکترونیکی در نظر گرفته است. لیکن فراهم ساختن تجهیزات مدیریت ریسک در محدوده بانکداری الکترونیکی، به علت سرعت تغییرات تکنولوژیکی و نوآوری‌های به وجود آمده در ارائه خدمات به مشتریان همواره مفید فایده نخواهد بود. در واقع مدل ریسک هر بانکی از دیگری متمایز است و باید با توجه به اندازه عملیات بانکداری الکترونیکی، ریسکهای فعلی و نقاط ضعف و قوت مؤسسات بانکی، نحوه مدیریت این ریسک‌ها تعدیل شود.

برای این منظور کمیته بال اصول مدیریت ریسک را از سه دیدگاه ۱) دیدگاه مدیریتی و هیأت مدیره ۲) کنترل‌های امنیتی و ۳) مدیریت ریسک قانونی، مورد بررسی قرار داده است که در ادامه به صورت اجمالی ارائه می‌شود:

دیدگاه مدیریتی و هیأت مدیره

با توجه به آنکه هیأت مدیره و مدیریت ارشد در برابر استراتژی تجاری مؤسسات و ایجاد یک دیدگاه مدیریتی مؤثر در برابر ریسک مسئول هستند، انتظار می‌رود که تصمیمات روشن و مستدل، راجع به چگونگی مهیاسازی خدمات بانکی، ارائه دهند.

این تصمیم‌گیری‌های اولیه باید قابلیت پاسخگوئی ویژه، سیاست‌گذاری و اعمال کنترل به منظور معرفی ریسک را دارا باشد. از دیدگاه مدیریتی مؤثر انتظار می‌رود که نقد و تأیید جنبه‌های کلیدی کنترل‌های بانکی، همچنین توسعه و حفظ بنیادی کنترل‌های امنیتی (که خطر ورود و خروج اطلاعات را رفع می‌نماید) را پوشش دهد.

کنترل‌های امنیتی

برای اینکه هیأت مدیره از مراحل کنترل امنیتی مطمئن باشد باید توجهات مدیریتی ویژه‌ای به منظور بالا بردن امنیت در مقابل چالش‌هایی که در بانکداری الکترونیکی مطرح می‌شود، اعمال گردد. این امر باید بر اساس صدور مجوز و اختیارات متناسب، معیارهای قانونی، کنترل‌های فیزیکی و غیر فیزیکی، زیرساختهای امنیتی کافی به منظور حفظ محدوده فعالیتهای مشتریان و مصرف‌کنندگان داخلی و خارجی و یکپارچه کردن اطلاعات وداده‌ها باشد.

به علاوه باید از وجود حسابرسی شفاف برای همه تراکنش‌های بانکداری الکترونیکی مطمئن بوده و حفظ اطلاعات کلیدی بانکداری الکترونیکی، متناسب با حساسیت چنین اطلاعاتی، مورد سنجش قرار گیرد.

مدیریت ریسک قانونی و رایج

به منظور آماده‌سازی بانکها در قبال تجارت و محدودیت‌های ریسک خدمات بانکی الکترونیکی، این خدمات باید به موقع و هماهنگ با انتظارات بالای مشتریان با سرعت و ثبات مورد نظر باشد. به طوری که تقاضای مبادلاتی بالقوه بالای مشتریان را پوشش دهد.

بانک باید قادر باشد که خدمات بانکی الکترونیکی را برای همه استفاده‌کنندگان فراهم کرده و در برابر همه ترفندها و انحرافات، آن را حفظ نماید. به منظور پاسخ دادن به انتظارات مشتریان، بانکها باید ظرفیت مؤثر و

برنامه‌ریزی در جهت تداوم تجارت در قبال اتفاقات غیرمترقبه را مد نظر داشته باشند.

اصول مدیریت ریسک در بانکداری الکترونیکی

به لحاظ اهمیت تشخیص و مدیریت ریسک و همچنین لزوم مطالعات مبسوط در این زمینه، از سوی کمیته بال گروهی متشکل از مدیران بانک و بانک مرکزی (E BG) مسئول این امر شده‌اند. بنا بر مطالعات این گروه کمیته بال به این نتیجه رسیده است که هر چند وجود چالشهای مدیریتی ریسک از خصوصیات اساسی بانکداری الکترونیکی است لیکن می‌توان اصول مدیریت ریسک بانکداری سنتی را، به منظور اجرای بانکداری به هنگام و چالشهای مدیریتی ریسک همراه آن، با توجه به مشخصه‌های پیچیده کانال توزیعی شبکه اینترنت، تعدیل نمود. بر این اساس کمیته بال اصول مدیریت ریسک بانکداری الکترونیکی را از سه دیدگاه مذکور در قالب ۱۴ اصل مهم تقسیم‌بندی و ارائه کرده است که به طور خلاصه به شرح ذیل است:

الف - اصول اول تا سوم (نگرش مدیریت ارشد وهیأت مدیره)

۱ - نگرش اثربخش مدیریتی در فعالیتهای بانکداری الکترونیکی: هیأت مدیره و مدیریت ارشد باید نگرش مدیریتی مؤثری را جهت پوشش ریسک اجرای بانکداری الکترونیکی که شامل ایجاد قابلیت حسابرسی ویژه، خط مشی‌ها و نظارت‌های مربوط به اداره این ریسکها می‌شود، ایجاد نمایند.

۲- ثبات و انسجام در فرایند کنترل ایمنی: هیأت مدیره و مدیریت ارشد باید جنبه‌های کلیدی مربوط به فرایند کنترل امنیتی بانک را بررسی نمایند.

۳ - انسجام و جدیت فرایند نگرش مدیریت: هیأت مدیره و مدیریت ارشد باید یک فرایند نگرشی جدی و منسجم برای اداره روابط کارگزاری و یا اشخاص ثالث وابسته به بانکها، ایجاد نموده و از طریق بانکداری الکترونیکی پشتیبانی نماید.

ب - اصول چهارم الی دهم (کنترل‌های ایمنی)

۴ - تأیید مشتریان بانکداری الکترونیکی: بانکها برای ارائه خدمات اینترنتی باید معیارهای مناسبی را برای تأیید افراد و مشتریان در نظر بگیرند.

۵ - عدم انکار و پاسخگویی در قبال تراکنش‌های الکترونیکی: بانکها باید روش‌های تشخیص و تصدیق مبادلات را که در آن امکان رد و انکار وجود نداشته باشد مورد استفاده قرار دهند به طوری که این روش‌ها در مقابل معاملات بانکداری الکترونیکی پاسخگو باشند.

۶- ایجاد معیار مناسب برای حصول اطمینان از تفکیک وظایف: بانک‌ها باید اطمینان حاصل نمایند که تمهیدات مناسبی به منظور توسعه و تشویق تفکیک وظایف در سیستم بانکداری الکترونیکی، بانکهای اطلاعاتی و کاربردها صورت پذیرد.

۷ - اعمال کنترل‌های قانونی با توجه به شبکه داده‌ها، کاربردها وسیستم‌های بانکداری الکترونیکی: بانک‌ها باید مطمئن شوند که کنترل‌های لازم در زمینه اختیارات و دسترسی به امکانات خاص در سیستم‌های بانکداری الکترونیکی، بانکهای اطلاعاتی و زمینه‌های کاربردی اعمال شده است.

۸- انسجام داده‌های حاصل از تراکنش‌های الکترونیکی، ثبت‌ها و اطلاعات: بانک‌ها باید از انجام تمهیدات مناسب در زمینه حفاظت از انسجام داده‌ها و مبادلات بانکداری الکترونیکی و داده‌های ضبط شده و سایر اطلاعات، اطمینان حاصل نمایند.

۹- ایجاد مکانیزم لازم برای حسابرسی تراکنش‌های الکترونیکی: بانک‌ها باید اطمینان حاصل نمایند که روش حسابرسی شفافی برای مبادلات بانکداری الکترونیکی وجود دارد.

۱۰- محرمانه شمردن اطلاعات بانکی مهم: بانک‌ها باید تمهیدات و محاسبات لازم را برای حفظ امانت اطلاعات بانکداری الکترونیکی ایجاد نمایند.

ایـن محاسـبات باید متناسب با حساسیت اطلاعات ارسالی و یا نگهداری شده در بانک‌های اطلاعاتی باشند.

ج- اصول یازدهم تا چهاردهم (مدیریت ریسک قانونی و رایج)

۱۱- تفکـیک مناسـب خدمـات بانکداری الکترونیکی: بانک‌ها باید اطمینان حاصـل نمایـند کـه اطلاعـات کافـی در وب سایت آنها برای مشتریان بالقوه در زمیـنه موقعیت و هویت بانک و ضوابط فعالیت‌های آن قبل از ورود به عملیات و مبادلات بانکداری الکترونیکی ارائه می‌شود.

۱۲- محـرمانه تلقـی کـردن اطلاعـات مشـتری: بـانک‌هـا باید تمهیدات و محاسـبات مناسـبی را بـرای کسـب اطمیـنان از پایبـندی بـه الزامات مربوط به خصوصـی بودن اطلاعات مشتریان در محدوده قانونی که بانک‌ها در آن خدمات و تولیدات بانکداری الکترونیکی ارائه می‌شود، در نظر بگیرند.

۱۳- **بـرنامه‌ریـزی اقتضـائی، تداوم کسب وکار و مد نظر داشتن ظرفیت به مـنظور حصـول اطمیـنان از روان وآسـان بـودن جریان خدمات و سیستم‌های بـانکداری الکترونیکـی**: بانک‌ها باید از ظرفیت‌های فعال، تداوم فعالیت تجاری و بـرنامه‌ریـزی اقتضـایی بـه مـنظور کسـب اطمینان از دسترس بودن سیستم‌های بانکداری و خدمات، برخوردار باشند.

۱۴- بـرنامه‌ریـزی در جهـت پاسـخگویی سـریع: بـانک‌هـا بـاید به منظور مدیریـت و کـاهش مسـائل برخواسـته از وقـایع غیر مترقبه برنامه‌های مواجه با حـوادث را توسعه دهند. وقایع غیر مترقبه می‌تواند در برگیرنده حملات از داخل و یـا خـارج از سیسـتم باشـد و موجـب جلوگـیری از فعالیـت‌هـای آزاد سیستم بانکداری الکترونیکی و نظارت‌های مربوطه شود.

وضعیت مدیریت ریسک در بانکداری الکترونیکی در ایران

توسـعه و گسـترش بـانکداری الکترونیکـی موجـب آشکار شدن هرچه بیشتر اهمیـت مدیریت ریسک در این زمینه گردیده است و لذا موضوع نحوه مدیریت

ریسک جزء موارد نظارتی است که در کشورهای توسعه یافته مورد بررسی ناظرین و بازرسان پولی و بانکی قرار می‌گیرد. هرچند هم اکنون بانکداری الکترونیکی در ایران گستردگی لازم را نیافته و به تبع آن هنوز کنترل‌های مزبور در دستور کار بانک مرکزی جمهوری اسلامی ایران قرار ندارد، لیکن با توجه به نیاز گسترده‌ای که هم اکنون در کشور جهت ایجاد و توسعه بانکداری الکترونیکی وجود دارد، انتظار می‌رود در آینده مدیریت ریسک و نظارت بر برقراری سیستم‌های مربوطه در بانکها در دستور کار نظام بانکی کشور قرار گیرد. لذا در ادامه نحوه انجام نظارتهای مرتبط با مدیریت ریسک بانکداری الکترونیکی که بی‌شک یکی از مواردی است که به منظور بررسی سلامت مالی بانکها در کشورهای توسعه یافته در نظر گرفته می‌شود، ارائه می‌گردد.

برنامه‌ریزی قبل از بررسی وضعیت ریسک

قبل از انجام هرگونه بررسی در زمینه تعیین ریسک بانکداری الکترونیکی لازم است طی برنامه‌ریزی اولیه تمام فعالیتهای مربوط به بانکداری الکترونیکی مشخص و تعیین گردد. بررسی کنندگان باید اطلاعات بانکداری الکترونیکی قابل دسترس از طریق سیستم مربوطه و نیز وب سایت بانک را به منظور تعیین سطح پیچیدگی‌های موجود مورد بازبینی قرار دهند.

برای تعیین وضعیت ریسک بانکداری الکترونیکی لازم است بررسی‌ها در سه سطح با توجه به مقدار پیچیدگی عملیات بانکداری به ترتیب زیر در نظر گرفته شود:

- **بررسی فعالیت‌های سطح ۱: سیستم‌های صرفاً اطلاعاتی**

معمولاً سطوح فعالیت مؤسساتی که دارای عملیات ساده بانکداری الکترونیکی هستند از این سطح فراتر نمی‌رود. سیستم‌های مزبور صرفاً امکان دسترسی به اطلاعات بازاریابی چند منظوره و یا سایر اطلاعات عمومی مانند اطلاعات در

ارتباط با خدمات بانک، نرخها و کارمزدها و انتقال نامه الکترونیکی غیر حساس را در اختیار می‌گذارند. شایان ذکر است بررسی این سطح از عملیات برای تمام مؤسسات و از جمله آنهائی که دارای سطوح فعالیت پیچیده نیز می‌باشند صورت می‌پذیرد. به دلیل گستردگی و تنوع استفاده از سیستم‌های اطلاعاتی سطح ۱ در سیستم‌های بانکداری الکترونیکی، اعم از ساده و پیچیده، مقتضی است در بررسی‌ها تنوع‌های موجود در نظر گرفته شود.

- **بررسی فعالیتهای سطح ۲: سیستم‌های الکترونیکی انتقال اطلاعات**

این بررسی پس از بررسی سیستم سطح ۱ صورت می‌گیرد و برای سیستم بانکداری الکترونیکی انجام می‌شود که در آنها امکان دسترسی، انتقال داده‌ها، فایل‌ها و یا پیام‌ها وجود دارد. سیستم مزبور ممکن است توانائی پیاده سازی[۱] و یا سوار نمودن[۲] و یا مبادله پیام‌های الکترونیکی حساس و یا اطلاعات محرمانه را دارا باشد. لذا باید این سیستم‌ها از نظر حساسیت آنها به اطلاعات، مورد بررسی قرار گیرند. نمونه‌ای از این سیستم‌ها آنهائی هستند که امکان پرداختهای وام و یا سپرده‌گذاری از طریق شبکه جهانی وب را فراهم می‌سازند.

- بررسی فعالیتهای سطح۳: سیستم مخصوص مبادلات تجاری

این بررسی پس از بررسی‌های سطوح ۱ و۲ صورت می‌گیرد و مختص سیستم‌هایی است که امکان انجام مبادلات مستقیم را به استفاده کنندگان خود می‌دهند. برای این منظور لازم است موارد ذیل صورت پذیرد:

✓ ارائه تضمین یا تعهدی مشابه از طرف بانک در رابطه با سیستم دریافت و پرداخت.

---

۱ -Downloading

۲ -Uploading

- ✓ بررسی، تضمین‌های فوق توسط مشاوران قانونی بانک.
- ✓ بـه طور کلی بررسی‌های تمام سطوح فوق‌الذکر باید شامل موارد ذیل باشند:
- ✓ بررسـی وجـود رویه‌های مناسب به منظور حفظ ارتباطات و پیوستگی بیـن شـبکه‌هـای (سـایت) وب، شـامل سـایت‌هـای داخلی و خارجی (اینترانـت یـا دیگـر شـبکه‌هـای خصوصی). همچنین وضعیت کنترل مدیریـت بـه مـنظور صـحت و تناسـب مداوم معرفی شبکه، به طور مرتب شبکه‌های مرتبط با یکدیگر.
- ✓ بررسـی وجـود روش‌هایـی بـه مـنظور کنـترل و نظارت جستجوهای غیرقانونی در دست‌یابی به اطلاعات شبکه بانکی.
- ✓ تعیین وضعیت سیاست‌های بانک در گزارشات رسمی مورد نیاز.
- ✓ بررسـی همه وقایع شناخته شده و اطمینان از اینکه به مقامات مربوط گزارش داده شده باشد.
- ✓ بررسـی وجـود یـک بـرنامه مـدون و متناسـب و یـا ایجـاد یک تیم پاسـخگو بـه مـنظور حـل موقعیـت‌هـای بحران (به طوری که حدود اختـیارات مقامـات و مسـئولین ایـن تـیم از طـرف هـیأت مدیره به تصویب رسیده باشد).
- ✓ تعییـن وضـعیت سیاسـت‌هـا و روش‌هایـی به منظور معرفی چگونگی اسـتفاده بانک از پست الکترونیکی (اعم از داخلی و خارجی)، به طوری کـه ارسـال به همه گروه از کاربران، اعم از مشتریان، مقامات رسمی و کارکنان را در برگیرد.
- ✓ بررسـی وجـود قـرارداد رسمی با هر یک از فروشندگان به طوری که ایـن قـراردادها بـه تأیـید مشـاوران قانونی بانک رسیده و تناسب در موارد ذیل را شامل باشد:

- دسترسی، مالکیت و کنترل اطلاعات مشتریان و دیگر اطلاعات محرمانه
- تضمینات مستدل به منظور تداوم خدمات از طریق ایجاد پشتیبان[۱] در مواقع بروز مشکل یا بحران.
- متناسب بودن پیمانکاران فرعی و دیگر فروشندگان پشتیبان.
- کنترل‌های مستدل و به هنگام از حجم و ظرفیت فعالیت‌ها به شیوه‌ای بجا.
- فرصت‌هایی به منظور بررسی گزارشات حسابرسان مستقل.
- احتیاط‌های امنیتی بر بخش فراهم کنندگان خدمات.

✓ بررسی وضعیت همزمان بودن تاریخ انقضاء قراردادهای خدمات وابسته به یگدیگر.

✓ بررسی نیازها و تجهیزات مستدل جهت فعالیت ارائه دهندگان شامل پیمانکاران، پیمانکاران فرعی، فروشندگان پشتیبان و دیگر شرکت کنندگان در عملیات بانکداری الکترونیکی.

✓ بررسی موارد مجاز به منظور حداقل کردن ریسک افشای موارد محرمانه.

✓ بررسی امکان دسترسی به سطوح مناسبی از اطلاعات و درخواست‌ها برای مقامات رسمی، کارکنان، فروشندگان سیستم، مشتریان و دیگر کاربران. همچنین، تعیین اینکه این سطوح دسترسی برپایه‌ای منظم و مقرر متکی باشند.

✓ بررسی قانونی بودن عملیات مربوط به هر حساب مورد درخواست، دستورات و اطلاعات وارد شده.

۱-Back up

- ✓ بررسی وجود برنامه‌ای مناسب در جهت ارائه خدمات مشتریان، حمایت و آموزش مشتریان، به گونه‌ای که فعالیت‌های کنترلی و حمایتی ذیل را به دنبال داشته باشد:
  - آموزش‌های متناسب و موارد مرجع در ارتباط با سیستم امنیتی، کنترلی و تعهدی مشتریان.
  - طراحی برنامه‌ای به منظور شناسایی مشکلات احتمالی به شیوه‌ای بجا و مناسب.
- ✓ بررسی گزارشات خاص و موردی توسط مدیریت و به صورت دوره‌ای.
- ✓ بررسی وجود معیار متناسبی به منظور حمایت سیستم در برابر تخطی از موارد قید شده در قراردادها

پس از تجزیه و تحلیل‌های مربوط به بررسی‌های سطوح فوق‌الذکر باید بتوان به سؤالات زیر پاسخ داد:

۱.آیا یک برنامه یا طرح مدیریت ریسک مؤثر وجود دارد؟

۲.آیا سیاست‌ها و روش‌ها در اثربخشی و اجرا به اندازه کافی مؤثر هستند؟

۳.آیا بررسی‌ها از نظر بی‌نقص بودن، مستقل بودن و یا وابستگی متقابل، به خوبی نمایانگر وضعیت سیستم‌ها می‌باشند؟

۴.آیا عملیات بانک با موارد قانونی مورد لزوم متناسب و سازگار می‌باشد؟

۵.آیا اجرا و نظارت برنامه به خوبی اعمال می‌شود؟

۶.آیا یک برنامه نظارتی مؤثر به منظور کنترل فروشندگان و ارائه کنندگان خدمات وجود دارد؟

بررسی ریسک در زمینه‌های شش‌گانه

برای تعیین ریسک عملیات بانکداری الکترونیکی لازم است شش زمینه ذکر شده در جدول (۲)، به شرح ذیل مورد بررسی قرار گیرد.

برنامه‌ریزی و اجرا: به دلیل توسعه تسهیلات و خدمات بانکداری الکترونیکی، سطوح دسترسی به اطلاعات محرمانه و مالی افزایش یافته است. مدیریت سازمان (از جمله هیأت مدیره، مدیران ارشد، مدیران ارشد صف) باید به طور کامل در جریان ریسک‌های اجرای سیستم بانکداری الکترونیکی قرار گیرند. نقص در برنامه‌ریزی و اجرا موجب افزایش قابل توجه ریسک و همچنین عدم توانائی در پاسخگوئی به مشکلات می‌گردد. علاوه بر این از آنجا که هیأت مدیره مسئولیت اصلی را در قبال هرگونه سیستم بانکداری الکترونیکی به عهده دارد لذا لازم است تمام تصمیم‌گیری‌های راهبردی تجاری و تکنولوژیکی از جمله تحلیل ریسک، مطالعات امکان‌سنجی و برنامه‌ریزی‌های راهبردی را تأیید و تصویب نمایند. همچنین مدیران ارشد باید در جهت حصول نیازهای امنیتی در ارتباط با طرح سیستم بانکداری الکترونیکی گامهای لازم را بردارند.

سیاست‌های اجرائی و روش‌ها: تجهیزات الکترونیکی این توانائی را دارند که به طور عمده‌ای خصوصیت فعالیت تجاری بانک را تغییر داده و یا تولیدات و خدمات جدید با شیوه‌های مختلف را ارائه دهند. لذا سیاست‌ها و روش‌های اجرائی باید همگام با محیط جدید به‌روز شده و دستورالعمل‌های موجود با استانداردها هماهنگ گردند. تفکیک وظایف، یکی دیگر از عناصر اصلی اجرای بی‌نقص مدیریت ریسک و کنترل سیستم می‌باشد و عدم رعایت کاربرد آن در زمینه مدیریت امنیت اطلاعات که شامل حفظ و نگهداری اطلاعات محرمانه فردی نیز می‌باشد، می‌تواند به طور بالقوه به سلامت و یکپارچگی سیستم لطمه بزند. مدیریت ریسک بانکداری الکترونیکی باید در قالب برنامه کلی مدیریت ریسک سازمان به کار گرفته شود. تمام سیاست‌های و رویه‌های اجرائی در

زمینه مدیریت ریسک باید موضوع امنیت را در نظر داشته باشند. از سوی دیگر هرگونه برنامه امنیتی کارا ضمن لحاظ نمودن سیاست‌ها، روش‌ها، و رویه‌های بدون نقص، نیازمند حمایت هیأت مدیره و مدیران ارشد است. اندازه‌گیری ریسک، بررسی چارچوب سیاست‌ها، روش‌های اجرائی و عملیاتی، بررسی حدود اختیارات افراد، مسئولیت و تعهدات کارمندان مربوطه، و بررسی سطح آموزش و توسعه دانش کارمندان و مشتریان از مهمترین فرایندهای مدیریت برنامه‌های امنیتی می‌باشند.

نظارت و بازرسی: ساختار امنیتی و نظارت داخلی نقش اساسی در عملکرد صحیح و سالم سازمان دارد. از اینرو نیل به محیطی ایمن برای انجام عملیات، نیازمند بر خورداری از سیستم کارای کنترل برای جلوگیری، آشکار سازی هرگونه نفوذ و دسترسی غیر مجاز و اصلاح اطلاعات تغییر یافته می‌باشد. در این راستا لازم است تا نظارت و بازرسی و تفکیک وظایف در کنار یکدیگر به کار روند. سیستم‌های نظارت و بازرسی هنگامی از کارائی برخوردار هستند که همگام با فازهای توسعه سیستم به کار گرفته شوند. همچنین زمانی که نظارت بازرسی به طور مستمر با مدیریت ریسک همراه گردد امکان حفظ منافع سازمان و مشتریان آن و سایر افراد دخیل در عملیات بانکداری الکترونیکی را فراهم خواهد آورد. علاوه بر این لازم است به منظور حفظ اطلاعات و دارائیهای مالی، قابلیت اعتماد سیستم، و رفاه و آسودگی خیال مشتریان، در توسعه برنامه‌های نظارت و بازرسی ابعاد مختلف عملیات لحاظ شود.

قوانین و مقررات: توسعه تجهیزات الکترونیکی موجب می‌شود که سازمان چارچوب قانونی و مقررات مربوط به عملیات خود را بازنگری نمایند. با تعیین حداقل استانداردهای لازم برای انجام فعالیت‌ها و نیز تکمیل و تقویت اسناد

قانونی و نیز انتقالات مالی می‌توان ارزش و نیز کارائی سیستم را در محیط‌های پیچیده مورد محافظت قرار داد. ضعف بازنگری استانداردها و زیر ساختهای لازم قانونی می‌تواند به زیانهای مستقیم مالی، اقدامات حقوقی علیه سازمان و یا بدهی‌های مشروط ناشی از قوانین عمومی منجر شود. سیستم‌های بانکداری الکترونیکی، چه آنهایی که ساده و محدود به تبلیغات و اطلاع رسانی هستند و چه سیستم‌های پیچیده انتقال الکترونیکی، باید به منظور حفاظت از اطلاعات و منافع مشتریان مورد بازنگری قرار گیرند.

مدیریت عملیات اجرائی: در انجام عملیات بانکداری الکترونیکی با هر سطحی از پیچیدگی و گستردگی، بانک متعهد است که حداقل استاندارد لازم جهت انجام عملیات را رعایت نماید. بنابراین تهیه دستورالعمل‌های مربوط به سطوح دسترسی، گزارش موارد استثنائی، و حفظ و ضبط اطلاعات مربوط به انجام عملیات و نیز نظارت بر آنها باید به عنوان روال جاری سازمان درآید. زیرا هرگونه نقص و اشکالی در این امر ممکن است به عدم توانائی سیستم در انجام عملیات مورد انتظار منجر شود. همچنین با توجه به دامنه عملیات و فقدان تمهیدات امنیتی مناسب، کاربران و مشتریان نیز ممکن است در معرض ریسک قرار گیرند. یکی از عوامل مهم در زمینه کسب قبولی و رضایت مشتریان، ارائه آموزشهای لازم به افراد ذی‌ربط جهت مقابله با مشکلات و مسائل مبتلا به می‌باشد. مدیریت سازمان برای تعیین سطح توانائی سیستم در ارائه خدمات و یا نتایج مورد انتظار، به صورت دوره‌ای ظرفیت‌ها، قابلیت دسترسی و صحت و سلامت سیستم را مورد آزمایش قرار دهد. به هر صورت نقص در ارائه پشتیبانی در زمینه‌های مذکور به واسطه کاهش اعتماد و تعهد مشتریان به سیستم، می‌تواند هزینه‌های اجرائی بنگاه را به سبب افزایش خطاها افزایش داده و در ضمن ریسک شکایات و اقدامات قانونی را نیز فزونی بخشد.

همچنین در صورتی که بانک اطلاعات لازم راجع به تمهیدات امنیتی سیستم را به مشتریان ارائه ندهد ممکن است با ریسک مواجه شود.

پیمانکاران و اشخاص ثالث ارائه‌کننده خدمات: به سبب پیچیدگی و سیر تغییرات در بانکداری الکترونیکی، ممکن است لازم باشد انجام عملیات به پیمانکاران و اشخاص ثالث ارائه‌کننده خدمات واگذار شود. البته این واگذاری مسئولیت مدیریت سازمان را در تمام زمینه‌های مربوط به سیستم عملیاتی بانک کاهش نمی‌دهد. هرگونه تفویض اختیار در زمینه انجام عملیات باید همراه با شناخت طرفین از یکدیگر و نیز تعیین شرایط واگذاری باشد و شرایط، حقوق و مسئولیتها باید در قالب قراردادهای مکتوب تعیین گردد. این موضوع بسیار حائز اهمیت است چرا که در بانکداری الکترونیکی واگذاری ارائه خدمات برای کوتاه مدت، تغییرات و توسعه خدمات جدید و همچنین ارائه کنندگان ناشناس و آزمایش نشده، امری غیر معمول نیست. علاوه بر این تمام قراردادهای پیمانکاری باید طوری تنظیم شوند که امنیت، قابلیت اعتماد و سلامت سیستم را با خطر مواجه ننمایند.

نتیجه‌گیری

نوآوریهـای مداوم تکنولوژیکی و رقابتی در زمینه فناوری اطلاعات و ارتباطات موجـب گـردیده مؤسسـات مالـی و بانکی بتوانند از طریق کانالهای الکترونیکی و سیسـتم‌های بانکداری الکترونیکی خدمات نوینی را ارائه نمایند. اگرچه سرعت رو بـه رشـد قابلیـت‌های بانکداری الکترونیکی سود قابل توجهی به همراه دارد، لیکن تـوأم بـا ریسـک نـیز اسـت. سهولت استفاده از پول الکترونیکی باعث شده که با بکارگـیری سیسـتمهای مدیریـت نقدینگی و پرداختهای کوچک بتوان به خوبی از مکانـیزمهای خودکـار بـرای جـذب وجوه نقد و مدیریت حسابها استفاده نمود. از سـوی دیگـر افزایش تمایلات جهانی برای استفاده از اینترنت به عنوان یک کانال پـیام رسـانی بـرای تولـیدات و خدمات بانکی، فرصت‌های جدید تجاری را برای بانکهـا بـه مـنظور فـراهم کـردن خدمات برای مشتریان ایجاد می‌کند. ابداعات تکنولوژیکـی مسـتمر و رقابتـی بیـن سـازمانهای بانکی و بازارهای جدید ،کالاها و خدمـات وسـیع بانکـی الکترونیکـی را بـرای مشـتریان مهیا کرده است. خدماتی نظیرگرفتـن اطلاعـات مالـی و اعتـباری ،گرفتن وام و باز کردن حساب سپرده و همچنیـن خدمـات جدید در زمینه خدمات پرداختی حواله ها ، اطلاعات شخصی واطلاعات مالی وغیر مالی و مبادلات شرکت به شرکت را شامل می شود.

لیکـن همچنان که اشاره شده علی رغم فوائد نو آوریهای تکنولوژیکی ، سرعت توسـعه بـانکداری الکترونیکـی ریسکهایی را هم پیش رو خواهد داشت. ریسکهای مـزبور چـنان جـدی اسـت کـه براساس نظر کارشناسان و دست‌اندرکاران نظام بانکـی چالشـهای مدیریـت ریسـک از خصوصـیات اساسی بانکداری الکترونیکی اسـت. بـه رغـم اینکه پیدایش و توسعه و بانکداری الکترونیکی مفاهیم جدیدی را

ابـداع نمـوده و بـه تبع آن ریسک‌های جدیدی برای بانکها تعریف گردیده است لیکـن در بسـیاری از عملـیات بانکداری الکترونیکی، بانکها با ریسکهای بانکداری سـنتی همچـون ریسـک اعتـباری، نقدینگـی و بـازار و نرخ بهره روبرو هستند اما افـزایش سـرعت در عملیات بانکداری الکترونیکی سرعت اثرات این ریسک ها و شاید خطرات آنها را افزایش داده است.

بـاید توجـه نمود که مدیریت ریسک در بانکداری الکترونیکی مفهومی جدا از مدیریـت ریسـک عملـیات بانکـی نیسـت و بـرای تحقـق آن باید زیر ساختهای مدیریـت ریسـک یکپارچه در بانک پی ریزی شده و به منظور کنترل هرچه بهتر ریسـک‌های مزبور لازم است تا ساختار سنتی مدیریت ریسک با نیازهای موجود در زمیـنه بـانکداری الکترونیکـی تطبـیق یابد. در ارتباط با مبادلات و نیز سیستم پرداخـتهای الکترونیکـی، مدیریـت ریسـک بـاید تمـام ابعـاد و زمیـنه‌های مهم ریسـکهای عملیاتـی، قانونـی، شـهرت را پوشش داده و با توجه به سطوح مختلف فعالیت تمهیدات زیر در نظر گرفته شود:

- نظـارت عمومی در زمینه‌های برنامه‌ریزی و تحلیل، سیاست‌ها و نحوه اجـرا، اختـیارات و مسـئولیتها، تبعیـت از مقررات و چارچوب قانونی، منابع انسانی و حسابرسی
- عملـیات مبادله شامل: اجازه استفاده، سلامت اطلاعات، غیرقابل انکار بودن مبادلات، و محرمانه بودن اطلاعات

- نظارت سیستم در زمینه منابع مورد نیاز، امنیت سیستم، قابل اعتماد بودن سیستم و برنامه‌ریزی مشروط، ظرفیت سیستم، سیاست واگذاری کار به اشخاص ثالث، و کنترل روز آمد بودن سیستم.

همچنین لازم است تا روند اجرایی مدیریت ریسک در زمینه‌های زیر متمرکز گردد:

- برنامه‌ریزی راهبردی و تحلیل امکانپذیری
- نظارت و سرپرستی مدیریت و کنترل‌های داخلی
- سیاست‌ها وروش‌های اجرائی و عملیاتی
- نظارت بر سیستم، حسابرسی و نحوه انجام آزمون‌ها
- امنیت فیزیکی، مبادلات و سیستم
- شناسایی افراد ثالث دست‌اندرکار در انجام عملیات
- آمادگی در زمینه اتخاذ پاسخ مناسب به اتفاقات
- پوشش و بهبود وقایع و پدیده‌های نامطلوب، ملاحظات تجاری و نیز برنامه‌ریزی مشروط
- بررسی مستمر پیشرفت‌های تکنولوژیک و نیز بهبود ظرفیت‌های موجود

در تمام ابعاد فوق‌الذکر می‌توان از تکنیک‌های مدیریت ریسک عملیات بانکداری سنتی برای تجزیه و تحلیل ریسک مربوطه استفاده نمود. البته در برخی موارد نیاز است تا تکنیک‌های خاصی برای کنترل ریسک به بانکداری الکترونیکی استفاده شود که عبارتند از برنامه‌ریزی راهبردی و تحلیل امکان‌سنجی، پاسخ‌دهی در مقابل اتفاقات و آمادگی طرح‌ها برای این منظور، و روش‌های اجرائی و کنترل‌های داخلی.

منابع و مآخذ

1- Basel Committee of Banking Supervision, ***Management and Supervision of Cross-Border Electronic Banking Activities,*** October 2002.

2- Basel Committee of Banking Supervision, Risk Management for Electronic Banking and Electronic Money, March 1998.

3- Basel Committee of Banking Supervision, Risk Management Principles for Electronic Banking, May 2001.

4- Comptroller of the Currenct Administrator of National Banks, Internet Banking, October 1999.

5- Comptroller of the Currenct Administrator of National Banks, The Internet and the National Bank Charter, January 2001.

6- Crouhy,Michel, Risk Management,2000.

7- Federal Deposit Insurance Corporation,Division of Supervision, Electronic Banking Safety and Soundness Eximination Procedures, June 1998.

8- Glantz Morton, Managing Bank Risk, Academic Press, 2003.

9- NatWest Corporation Banking Services, Electronic Banking and Treasury Security, Woodhead Publishing Limited and The Association of Corporate Treasurers, 1999.

10- Rose,Peter,S., Commercial Bank Management,1999.

11- Santamero,Antonio M.,Commercial Bank Risk management, TheWharton School, University of Pennsylvania.1997.

12- Sinkey,Jr. Joseph F.,Commrcial Bank Financial Management,1992.