بانک مرکزی جمهوری اسلامی ایران

مدیریت کل نظارت بر بانک‌ها و مؤسسات اعتباری

«اداره مطالعات و مقررات بانکی»

اصول مدیریت ریسک در بانکداری الکترونیک

از دیدگاه کمیته نظارت بر بانکداری بال

ترجمه:

محمد روشندل–سلیم ملا احمد نالوس

شهریور ۱۳۸۷

فهرست مطالب

«بسمه تعالی»

اصول مدیریت ریسک در بانکداری الکترونیک از دیدگاه کمیته نظارت بر بانکداری بال

دیدگاه هیأت اجرایی کمیته بال

نوآوری‌های مستمر در عرصه فن‌آوری و رقابت میان بانک‌ها و متقاضیان جدید ورود به این صنعت باعث شده است که محصولات و خدمات بانکی گسترده‌تری از طریق ابزارهای توزیع الکترونیک به مشتریان خرد و کلان[1] ارائه گردد، که اصطلاحاً تحت عنوان بانکداری الکترونیک[2] شناخته شده است. به هر حال توسعه سریع ظرفیت‌ها و توانمندی‌های بانکداری الکترونیک با مزایا و مخاطراتی همراه می‌باشد.

کمیته نظارت بانکی بال انتظار دارد که این‌گونه مخاطرات شناسایی شده و از سوی بانک‌ها با شیوه‌ای احتیاطی[3] و مطابق با ویژگی‌ها و چالش‌های اساسی مربوط به بانکداری الکترونیک مدیریت شوند. این ویژگی‌ها در برگیرنده سرعت بی‌سابقه تغییرات در عرصه فن‌آوری و نوآوری‌های مربوط به ارائه‌ی خدمات به مشتریان، ماهیت منحصر به فرد و جهانی شبکه‌های الکترونیک باز، یکپارچه‌سازی برنامه‌های بانکداری الکترونیک با سیستم‌های کامپیوتری و افزایش وابستگی بانک‌ها به شرکت‌های تأمین‌کننده فن آوری اطلاعات می‌باشند. هرچندریسک‌های مرتبط با بانکداری الکترونیک به طور ذاتی ایجاد نمی‌شوند، ولی کمیته بال بر این باور است که ویژگی‌های بانکداری الکترونیک باعث افزایش و تغییر برخی از ریسک‌های متداول

1 Retail and Wholesale Customers

2 E – Banking

3 Prudent Manner

فعالیت‌های بانکی از جمله ریسک‌های عملیاتی، شهرت و قانونی شده و در مجموع ریسک کلی بانک‌ها را تحت تأثیر قرار داده است.

با توجه مباحث مورد اشاره، کمیته بال اعلام می‌دارد که علاوه بر اجرای اصول مدیریت ریسک فعلی در بانکداری الکترونیک، ضروری است این اصول با ویژگی‌های فعالیت بانکداری الکترونیک تطابق یافته و متناسب با چالش‌های مدیریت ریسک در حوزه فعالیت‌های این نوع بانکداری توسعه یابند. بر همین اساس، کمیته بال معتقد است که هیأت مدیره و مدیریت ارشد بانک‌ها باید اقداماتی جهت حصول اطمینان از تغییر و تجدیدنظر در اصول مدیریت ریسک فعلی مطابق با فعالیت‌های بانکداری الکترونیک و فرآیندهایی جهت پوشش این‌گونه فعالیت‌های جاری و آتی بانک بکارگیرند. همچنین، کمیته اعتقاد دارد که یکپارچه‌سازی برنامه‌های کاربردی بانکداری الکترونیک با سیستم‌های فعلی بانکداری در بر گیرنده‌ی رویکرد مدیریت ریسک جامع برای تمام فعالیت‌های یک بانک می‌باشد

جهت توسعه بانکداری الکترونیک، کمیته بال اصول چهارده‌گانه مدیریت ریسک بانکداری الکترونیک را تدوین نموده است که به بانک‌ها کمک می‌کند تا سیاست‌های مدیریت ریسک فعلی را توسعه داده و فرآیندهایی را جهت پوشش فعالیت‌های بانکداری الکترونیک گسترش بخشند.

این اصول تأمین کننده تمام نیازها نیست و حتی نمی توان آنها را بهترین رهنمود قلمداد کرد. کمیته بال اعتقاد دارد که تعیین ساز و کارهای تفصیلی مدیریت ریسک در حوزه بانکداری الکترونیک باید از سوی بانک‌ها به طور مداوم و به روز صورت پذیرد، زیرا این احتمال وجود دارد که سرعت تغییرات فن آوری و نوآوری‌های مربوط به خدمات مشتری، برخی از روش‌های بانکداری الکترونیک را منسوخ سازد. بنابراین، به منظور ارتقای سلامت و ثبات فعالیت‌های بانکداری الکترونیک و حفظ انعطاف‌پذیری لازم در برابر تغییرات در این حوزه، کمیته بال ترجیح می‌دهد رهنمود نظارتی را به شکل اصول مدیریت ریسک مطرح نماید. به علاوه، این کمیته معتقد است که

ریسک‌های بانکی متفاوت هستند و مدیریت ریسک باید بر مبنای فعالیت‌های عملیاتی بانکداری الکترونیک صورت پـذیرد. بـراین اسـاس، ممکـن اسـت رویکـرد واحـدی درخصوص مدیریت ریسک بانکداری الکترونیک برای همه‌ی بانک‌ها مناسب نباشد.

براساس دلایل ذکر شده، اصول مدیریت ریسک ارائه شـده از سـوی کمیتـه بال در تلاش نیست تا راهکارها یا استانداردهای فنـی مشخـصی را بـرای بانکـداری الکترونیک تدوین نماید. این راهکارها و استانداردها باید توسط سازمان‌ها و نهادهـای تدوین کننده استانداردها تدوین شوند. به هرحال این گـزارش شـامل پیوسـت‌هـایی است که در آنها نمونه‌هایی از اقدامات مؤثر جهت کاهش ریسک در حـوزه بانکـداری الکترونیک ارائه شده است.

در نتیجه، انتظار می‌رود اصول مدیریت ریسک مورد نظـر در ایـن رهنمـود از سوی نهادهای نظارت بانکی کشورها مورد اسـتفاده قـرار گیرنـد و در صـورت لـزوم براساس شرایط و ریسک‌های خاص هر کشور تطبیـق داده شـوند. در برخـی مـوارد، اصول مورد اشاره قبلاً در اصول نظارت بر بانک‌ها(منتشره از سوی کمیته بـال) مطـرح شده است. به هرحال، با توجه به ماهیت و کاربردهای منحصر به فرد شبکه اینترنـت، برخی مباحث همچون مدیریت روابط برون سـپاری، کنتـرل‌هـای امنیتـی و مـدیریت ریسک قانونی و شهرت با جزئیات بیشتری نسبت به قبل مطرح شده است.

اصول مدیریت ریسک به سه بخش تقسیم شده اسـت: نظـارت مـدیریت و هیأت مدیره، کنترل امنیتی و مدیریت ریسک قانونی و شهرت.

نظارت هیأت مدیره و مدیریت

مسئولیت توسعه راهبرد تجاری بانک و بکارگیری مدیریت مؤثر نظارت بر ریـسک‌هـا برعهده هیأت مدیره و مدیریت ارشد است و انتظار مـی‌رود آنـان تـصمیم راهبـردی روشن و مستندی در خصوص چگونگی ارائه‌ی خـدمات بانکـداری الکترونیـک اتخـاذ نمایند. تصمیم‌گیـری‌هـای اولیـه هیـأت مـدیره و مـدیریت ارشـد بایـد دربرگیرنـده

مسئولیت‌ها، سیاست‌ها و کنترل‌های مشخص در مورد مدیریت ریسک، به خصوص مواردی که متأثر از ریسک‌های برآمده از خارج از مرزها است، باشد. انتظار می‌رود که مدیریت نظارت مؤثری بر جنبه‌های کلیدی فرآیند کنترل امنیتی همچون توسعه و حفظ زیرساخت‌های کنترل امنیتی داشته باشد و به طور دقیق از سیستم‌ها و داده‌های بانکداری الکترونیک در مقابل تهدیدهای داخلی و خارجی محافظت نماید. همچنین نظارت مدیریت باید در برگیرنده فرآیندهای جامع کاهش ریسک‌های مرتبط با پیچیدگی فزاینده و افزایش وابستگی به روابط برون سپاری و اشخاص ثالث جهت انجام فرآیندهای حساس بانکداری الکترونیک باشد.

کنترل‌های امنیتی

هیأت مدیره و مدیریت ارشد مسئولیت حصول اطمینان از فرآیندهای کنترل امنیتی مناسب در بانکداری الکترونیک را برعهده دارند و اجرای این فرآیندها مستلزم مدیریت ویژه است، زیرا چالش‌های امنیتی زیادی در بانکداری الکترونیک وجود دارد. فرآیندهای امنیتی باید در برگیرنده اجازه دسترسی، معیارهای شناسایی، کنترل‌های دسترسی فیزیکی و مجازی، زیرساخت‌های امنیتی مناسب جهت حفظ محدوده دسترسی مناسب و محدودیت ها در هر دو زمینه فعالیت‌های کاربری داخلی و خارجی و اصالت داده های مبادلاتی، ثبت ها و اطلاعات باشد. علاوه بر آن، باید از وجود روش‌های حسابرسی مشخص برای مبادلات بانکداری الکترونیک اطمینان حاصل کرد و معیارهای حفظ رازداری[1] در مورد اطلاعات کلیدی بانکداری الکترونیک باید متناسب با میزان حساسیت اطلاعات باشد.

هرچند حفاظت از مشتریان و مقررات مربوط به رازداری اطلاعات مشتری از کشوری به کشور دیگر متفاوت است، اما بانک‌ها به طور کلی مسئولیت روشنی در قبال افشای

[1] Confidentiality

اطلاعات مشتریان، حفاظت از داده‌های مشتری و دسترسی آنها به خدمات الکترونیک، که هم سطح با خدمات بانکداری متداول باشد، دارند.

جهت حداقل کردن ریسک شهرت و قانونی مرتبط با فعالیت‌های بانکداری الکترونیک در هر دو بخش داخلی و بین المللی، بانک‌ها باید نسبت به افشای کافی اطلاعات در وب سایت هایشان اقدام نمایند و معیارهای مناسبی جهت حصول اطمینان از حفظ اطلاعات مشتری، متناسب با مقررات کشور مربوطه، در ارائه‌ی خدمات بانکداری الکترونیک بکار گیرند.

مدیریت ریسک قانونی و شهرت

جهت حفاظت از بانک‌ها در مقابل ریسک‌های تجاری، قانونی و شهرت، فعالیت‌های بانکداری الکترونیک باید به موقع و مطابق با انتظارات بالای مشتری صورت گرفته و قابلیت دسترسی سریع و پایدار و توانایی پاسخگویی تقاضای مبادلات در سطح گسترده را به طور بالقوه داشته باشد. بانک‌ها باید توانایی ارائه‌ی خدمات بانکداری الکترونیک را به تمام کاربران داشته باشند و بتوانند قابلیت دسترسی را در تمام شرایط حفظ کنند. وجود مکانیزم‌های عکس العمل مؤثر جهت حداقل کردن ریسک‌های عملیاتی، قانونی و شهرت، که از رخدادهای غیر منتظره همچون حملات داخلی و خارجی ناشی می‌شود و ممکن است بر نحوه ارائه سیستم‌ها و خدمات بانکداری الکترونیک اثر گذار باشد، حیاتی است. بانک‌ها باید جهت تأمین انتظارات مشتری از ظرفیت مؤثر، برنامه‌ریزی اقتضایی[1] و استمرار فعالیت تجاری برخوردار باشند. بانک‌ها باید از وجود برنامه‌های واکنش مؤثر همچون راهبردهای ارتباطی (که استمرار فعالیت تجاری را اطمینان می‌بخشند)، کنترل ریسک شهرت و محدود کردن شکاف‌های خدمات بانکداری الکترونیک مطمئن شوند.

1 Contingency Planning

۱– مقدمه

بانک‌ها ارائه‌ی خدمات الکترونیک به مشتریان و شرکت‌ها را از چند سال قبل آغاز کرده‌اند. از ویژگی‌های عمومی و جهانی بانکداری الکترونیک می‌توان به انتقال الکترونیک وجوه، شامل سیستم‌های پرداخت در سطح خرد و سیستم‌های مدیریت وجوه نقد مشترک، ماشین‌های خودپرداز برداشت وجه با قابلیت دسترسی عموم و مدیریت حساب‌های خرد اشاره کرد. به هر حال، افزایش مقبولیت اینترنت[1] در عرصه جهانی به عنوان یک شیوه انتقال خدمات و محصولات بانکی باعث ایجاد فرصت‌های تجاری جدیدی برای بانک‌ها و ایجاد منافعی برای مشتریان شده است.

تداوم نوآوری در فن‌آوری و افزایش رقابت‌پذیری باعث شده بانک‌ها خدمات و محصولات بانکداری الکترونیک[2] گسترده‌ای در سطح خرد و کلان به مشتریان ارائه نمایند. این محصولات و خدمات در برگیرنده فعالیت‌هایی همچون دسترسی به اطلاعات مالی، دریافت انواع وام‌ها، افتتاح حساب سپرده و تا حدودی ارائه محصولات و خدمات جدید همچون صدور صورتحساب الکترونیک و یکپارچه‌سازی حسابها[3] می‌باشد.

1در این گزارش، اینترنت شامل تمام فن‌آوری‌ها و شبکه های ارتباط از راه دور باز از جمله ارتباط تلفنی، شبکه جهانی اینترنت و شبکه های خصوصی مجازی است

2در این گزارش، بانکداری الکترونیک یا e-banking هم شامل ارائه خدمات و محصولات خرد و کوچک از طریق کانال‌های الکترونیک است و هم پرداخت مبالغ بالا از طریق کانالهای الکترونیک را دربر می‌گیرد.

3 یکپارچه‌سازی حسابها(Account aggregation) به مشتریان اجازه می دهد که اطلاعات حساب‌های مالی و غیرمالی خود را بصورت یکجا مشاهده کنند. مؤسسه ای که به ارائه خدمات یکپارچه نمودن حساب‌ها می پردازد در واقع کارگزار مشتری است که اطلاعات حساب‌های وی در مؤسسات مالی مختلف را جمع آوری و دراختیار وی قرار می دهد. مشتریان اجازه کاربری و رمز عبور خود را در اختیار کارگزار قرار می دهند تا بتوانند به اطلاعات حساب آنها دسترسی داشته باشد. آنها می‌توانند بدون اطلاع مشتریان و یا با عقد قرارداد با مؤسسات مختلف مالی، اطلاعات مشتری را جمع آوری کنند.

عـلاوه بـر مزایـای قابـل ملاحظـه نـوآوری‌هـای فـن‌آوری، توسـعه سـریع توانمندی‌های بانکداری الکترونیک ریسک‌هایی را نیز بـه همـراه دارد، لـذا شناسـایی این‌گونه ریسک‌ها و مدیریت آنها بر مبنای رویکرد احتیاطی از سوی بانک‌هـا ضـروری است.[۱] براساس توسعه فعالیت‌های بانکی، کمیته نظارت بانکی بال مطالعات اولیـه‌ای درخصوص مدیریت ریسک بانکداری الکترونیک و پـول الکترونیـک[۲] در سـال ۱۹۹۸ انجام داد.[۳] مطالعات اولیه این کمیتـه بیـشتر بـر حـوزه مـدیریت ریـسک بانکـداری الکترونیک متمرکز بود و براین اساس گـروه بانکـداری الکترونیـک[٤] در نـوامبر ۱۹۹۹ تشکیل شد.

کمیته بال، گزارش گروه یاد شده در مورد مباحث مدیریت ریسک و نظارت در حوزه بانکداری الکترونیک را در سال ۲۰۰۰ منتشر کرد.[٥] در این گزارش، ریسک‌هـای عمده بانکداری الکترونیک تحت عناوین ریسک راهبردی[٦]، ریسک شـهرت[۷]، ریـسک

---

۱ بدلیل تغییرات سریع در فن آوری اطلاعات، هیچ تعریف جامعی از این ریسک‌هـا نمـی توانـد وجـود داشته باشد. به هرحال، ریسک‌هایی که بانک‌ها در بانکداری الکترونیک با آن روبرو هستند، ریسک‌های جدیدی نیستند و در نشریه کمیته بال تحت عنوان« اصول نظارت مؤثر بانکی» در سپتامبر۱۹۹۷ به آنها اشاره شده است. در آن نشریه به هشت ریسک مختلف اشاره شده اسـت: ریـسک اعتبـاری، ریـسک انتقال و کشور، ریسک بازار، ریسک نرخ بهره، ریسک نقدینگی، ریـسک عملیـاتی، ریـسک قـانونی و ریسک شهرت. این اصول در وب سایت کمیته بال به آدرس www.bis.org قابل دسترسی هستند.

2 E – Money

۳ «مدیریت ریسک در بانکداری الکترونیک و فعالیت‌های پـول الکترونیـک»، مـارس۱۹۹۸، در سـایت بانک تسویه بین المللی به آدرس www.bis.org قابل دسترسی است.

4 Electronic Banking Group (EBG)

۵ «ابتکارات و گزارشات گروه بانکداری الکترونیک»، اکتبر۲۰۰۰، در سایت بانک تسویه بین المللی بـه آدرس www.bis.org قابل دسترسی است.

6 Strategic risk

7 Reputational risk

عملیاتی[1] (شامل ریسک امنیتی[2] و ریسک قانونی[3])[4]، ریسک اعتباری[5]، ریسک بازار[6] و ریسک نقدینگی[7] مورد ارزیابی قرار گرفت. گروه بانکداری الکترونیک به این نتیجه رسید که فعالیت‌های بانکداری الکترونیک برخی از ریسک‌های متداول را افزایش و تغییر می‌دهد و در مجموع بر کل ریسک بانک اثر می‌گذارد. به طور خاص، ریسک‌های راهبردی و شهرت در بانکداری الکترونیک به خاطر پیشرفت سریع فعالیت‌های بانکی در این حوزه و پیچیدگی‌های فنی فعالیت‌ها از اهمیت خاصی برخوردار هستند.

الف- چالش‌های مدیریت ریسک

گروه بانکداری الکترونیک اشاره دارد که ویژگی‌های اساسی بانکداری الکترونیک (تجارت الکترونیک[8]) چالش‌هایی برای مدیریت ریسک ایجاد کرده است.

- سرعت تغییرات فن‌آوری و نوآوری در ارائه‌ی خدمات به مشتریان در بانکداری الکترونیک بی‌سابقه است. به لحاظ تاریخی، برنامه‌های جدید بانکداری عموماً طی مدت زمان طولانی و پس از آزمون‌های بنیادی بکار گرفته شده است. اما امروزه بانک‌ها در شرایط رقابتی شدیدی قرار دارند و مجبورند برنامه‌های تجاری نوین را در چارچوب‌های زمانی کوتاه‌مدت

---

1 operational risk

2 Security risk

3 Legal risk

4 این گزارش، از تعریف کمیته بال در مورد ریسک عملیاتی استفاده می کند که شامل ریسک امنیتی و ریسک قانونی است.(نگاه کنید به نشریه کمیته بال در مورد نظارت بانکی، توافق نامه سرمایه جدید کمیته بال، آوریل۲۰۰۳، پاراگراف ۶۰۷، تحت عنوان« ریسک زیان ناشی از فرآیندها، افراد و سیستم‌های ناموفق داخلی یا رخدادهای خارجی»)

5 Credit risk

6 Market risk

7 liquidity risk

8 E-commerce

بکارگیرند. تشدید رقابت‌پذیری، چالش‌های مدیریت جهت حصول اطمینان از ارزیابی صحیح راهبرد، تجزیه و تحلیل ریسک و توجه به مسائل امنیتی را افزایش داده است. توجه به مسائل امنیتی بر اجرای برنامه‌های بانکداری الکترونیک اولویت دارد.

هرچند روش‌های الکترونیک باعث کاهش خطاهای انسانی و تقلب‌های مربوط به فرآیندهای دستی می‌گردد، اما وابستگی آنها را به طراحی و ساخت سیستم‌های دقیق، مناسب و یکپارچه الکترونیک افزایش می‌دهد.

- بانکداری الکترونیک وابستگی بانک را به فن آوری اطلاعات افزایش می‌دهد؛ بنابراین پیچیدگی فنی بسیاری از مباحث عملیاتی و امنیتی افزایش یافته و مشارکت و تأمین خدمات از دیگران (برون‌سپاری[1]) ضرورت می‌یابد. توسعه این روند منجر به ایجاد مدل‌های تجاری جدید برای بانک‌ها و سایر شرکت‌ها از قبیل تأمین‌کنندگان خدمات اینترنت و شرکت‌های ارتباطی از راه دور و سایر شرکت‌های فن‌آوری شده است.
- اینترنت ماهیتی منحصر به فرد و جهانی دارد، این شبکه از سوی افراد ناشناخته در هر نقطه از جهان قابل دسترسی می‌باشد. این وضعیت اهمیت کنترل‌های امنیتی، روش‌های تأیید اعتبار مشتری[2]، جمع‌آوری داده‌ها، دستورالعمل‌های حسابرسی و استانداردهای حفظ اسرار مشتری[3] را برجسته می‌سازد.

ب- اصول مدیریت ریسک

کمیته بال براساس اقدامات اولیه گروه بانکداری الکترونیک به این نتیجه رسید که هر چند اصول مدیریت ریسک بانکداری متداول برای فعالیت‌های بانکداری الکترونیک

1 Outsourcing

2 Customer authentication

3 Customer privacy

قابل اجرا می‌باشند، ولی ویژگی‌های پیچیده ابزار انتقال اینترنتی مستلزم بکارگیری این اصول متناسب با فعالیت‌های بانکداری الکترونیک و چالش‌های مدیریت ریسک مرتبط با آنها می باشد. در مجموع کمیته بال بر این باور است که مسئولیت بکارگیری اقداماتی جهت حصول اطمینان از تعدیل و اصلاح سیاست ها و دستورالعمل‌های مدیریت ریسک فعلی جهت تطبیق با فعالیت‌های بانکداری الکترونیک بر عهده هیأت مدیره و مدیریت ارشد بانک می‌باشد. علاوه بر آن، کمیته اعتقاد دارد همانطور که بانک‌ها باید رویکرد مدیریت ریسک یکپارچه‌ای برای تمام فعالیت‌های بانکداری بکارگیرند، ضروری است که نظارت بر مدیریت ریسک فعالیت‌های بانکداری الکترونیک بخش جدایی ناپذیری از چارچوب مدیریت ریسک کلی بانک‌ها باشد.

در همین راستا، کمیته بال از گروه بانکداری الکترونیک تقاضا دارد تا اصول کلیدی مدیریت ریسک را مورد شناسایی قرار داده و به بانک‌ها کمک کند تا سیاست ها و فرآیندهای ریسک فعلی خویش را جهت پوشش فعالیت‌های بانکداری الکترونیک و محصولات و خدمات الکترونیک توسعه دهند.

اصول مدیریت ریسک در بانکداری الکترونیک، که در این گزارش ارائه شده، نه به‌عنوان برنامه‌های کاربردی مطلق و بهترین روش‌های اجرایی، بلکه بیشتر به عنوان رهنمودی جهت ارتقای صحت و سلامت بانکداری الکترونیک مورد توجه قرار می گیرد. کمیته بال معتقد است که تعیین جزئیات مدیریت ریسک در بانکداری الکترونیک چندان مطلوب نیست و احتمالاً با سرعت فزاینده تغییرات فنی و نوآوری ها در این حوزه همخوانی ندارد. بنابراین اصول مورد اشاره در این متن بیان کننده انتظارات نظارتی جهت حصول اطمینان از صحت و سلامت سیستم مالی است، نه ارائه مقررات دقیق و جزیی در حوزه بانکداری الکترونیک.

کمیته اعتقاد دارد که اینگونه انتظارات نظارتی باید متناسب و هماهنگ با راهکارهای ارائه‌ی خدمات و محصولات الکترونیک باشد و با سایر فعالیت‌های متداول بانکداری نیز اساساً متفاوت نباشد. ضمن اینکه اصول مورد اشاره در این متن به طور کلی از

اصول قبلی نظارت بر بانک‌ها(منتشره از سوی کمیته بال) اقتباس شده است. برخی از موضوعات مورد اشاره همچون مدیریت روابط برون سپاری، کنترل‌های امنیتی و مدیریت ریسک قانونی و شهرت، ویژگی‌ها و برنامه‌های بکارگیری اینترنت ضرورت تشریح بیشتراصول را نمایان ساخته است.

کمیته اعتقاد دارد که بانک‌ها باید برای مجموعه ریسک انفرادی[1] ، ساختار عملیاتی[2] و فرهنگ حاکمیت شرکتی[3] بانک و نیز هماهنگی با الزامات مدیریت ریسک و سیاست‌های تعیین شده از سوی نظارت کنندگان بانک، فرآیندهای مناسب مدیریت ریسک را توسعه بخشند. هرچند که برنامه‌های کاربردی متعددی در زمینه مدیریت ریسک بانکداری الکترونیک در این متن ارائه شده است، اما افراد مسئول در این زمینه در بانک نباید فعالیت خویش را به این موارد محدود سازند، زیرا بسیاری از کنترل‌های امنیتی و سایر روش‌های مدیریت ریسک‌همراه با فن آور های نوین به سرعت در حال تغییر می‌باشند.

این گزارش درصدد ارائه راه حل های فنی و دقیق در خصوص ریسک‌های خاص یا مجموعه ای از استانداردهای فنی مرتبط با بانکداری الکترونیک نیست. مباحث فنی نیازمند آن هستند که به طور مستمر از سوی بانک‌ها و نهادهای تدوین استاندارد مورد بررسی و تدوین قرارگیرند.علاوه بر آن، همانطور که مباحث فنی بانکداری الکترونیک(که در برگیرنده چالش‌های امنیتی می‌باشد) مورد توجه قرار دارد، نوآوری ها در این حوزه رو به گسترش بوده و راه‌حل‌های جدید مدیریت ریسک از سوی متخصصان ارائه می‌گردد. این راه‌حل‌ها احتمالاً در برگیرنده مباحثی همچون تنوع بانک‌ها در اندازه، پیچیدگی و فرهنگ مدیریت ریسک و تفاوت در چارچوب‌های قانونی و نظارتی می‌باشد.

---

1 Individual Risk

2 Poerational Structure

3 Corporate Governance Culture

به دلایل مورد اشاره، کمیته اعتقادی به بکارگیری رویکرد واحد برای مدیریت ریسک بانکداری الکترونیک در همه‌ی بانک‌ها ندارد، بلکه آنها را تشویق می‌کند تا با جایگزینی روش‌ها و استانداردهای بهتر ابعاد ریسک کانالهای توزیعی بانکداری الکترونیک را مشخص سازند. با درنظر گرفتن این فلسفه نظارتی، انتظار می‌رود مقامات نظارتی اصول مدیریت ریسک و اقدامات عملیاتی، که در این گزارش به آنها اشاره شده است، را به عنوان ابزارهایی مورد استفاده قرار داده و آنها را با شرایط خاص کشور خود تطبیق دهند تا به افزایش سلامت و امنیت فعالیت‌ها و عملیات بانکداری الکترونیک کمک کنند.

کمیته معتقد است که ریسک‌های بانکی متفاوت بوده و هر کدام از آنها با توجه به ضوابط عملیات بانکداری الکترونیک، اهمیت بالفعل و بالقوه ریسک‌ها و توانایی بانک در مدیریت آنها مستلزم بکارگیری روش مناسب جهت کاهش ریسک می‌باشند. با توجه به این تفاوتها، اصول مدیریت ریسک مورد اشاره در این گزارش باید به گونه‌ای انعطاف‌پذیر باشند که همه‌ی بانک‌ها در تمام کشورها بتوانند آنها را بکار گیرند. مقامات نظارتی اهمیت ریسک‌های مرتبط با فعالیت‌های بانکداری را در بانک مشخص می‌کنند و لزوم و میزان بکارگیری اصول مدیریت ریسک بانکداری الکترونیک را براساس چارچوب مدیریت ریسک بانک تعیین می نمایند.

۲- اصول مدیریت ریسک در بانکداری الکترونیک

اصول مدیریت ریسک بانکداری الکترونیک در این گزارش به سه بخش تقسیم‌بندی می‌شود. به هرحال، این اصول بر اساس اهمیت یا ارجحیت مرتب نشده‌اند. در طول زمان ممکن است اهمیت یا ارجحیت تغییر کند، اما این تقسیم‌بندی بدون تغییر باقی خواهد ماند.

الف–نظارت هیأت مدیره و مدیریت ارشد[1] (اصول۱تا۳):

۱- نظارت مؤثر هیأت مدیره بر فعالیت‌های بانکداری الکترونیک

۲- برقراری فرآیند کنترل امنیتی جامع

۳- نظارت جامع و مستمر هیأت مدیره بر روابط برون سپاری و وابستگی‌ها به اشخاص ثالث

ب–کنترل‌های امنیتی

۴- اجازه کاربری به مشتریان بانکداری الکترونیک

۵- عدم انکار و مسئولیت پذیری در مبادلات بانکداری الکترونیک

۶- ضوابط مناسب برای اطمینان از تقسیم وظایف

۷- کنترل‌های مناسب در اعطای اجازه کاربری در سیستم‌ها، پایگاه داده ها و برنامه‌های کاربردی

۸- اصالت داده‌ها در اطلاعات، اسناد و مبادلات بانکداری الکترونیک

۹- برقراری حسابرسی‌های آتی برای مبادلات بانکداری الکترونیک

۱۰- محرمانه نگه داشتن اطلاعات کلیدی بانک

ج– مدیریت ریسک شهرت و قانونی

۱۱- افشای مناسب خدمات بانکداری الکترونیک

---

1 این گزارش به ساختارهای سازمانی اشاره دارد که شامل هیئت مدیره و یک مدیر ارشد هستند. کمیته هشدار می دهد که تفاوت‌های معنی داری در قوانین و چارچوب مقرراتی کشورهای مختلف در مورد وظایف و اختیارات هیأت مدیره و مدیرعامل وجود دارد. در برخی کشورها، وظیفه اصلی هیأت مدیره نظارت است و می‌تواند بر کار مدیر ارشد یا مدیر اجرایی نظارت کند. به همین دلیل گاهی اوقات به هیأت مدیره هیأت نظارت می‌گویند. در این موارد، هیأت مدیره قدرت اجرایی ندارد. در مقابل در کشورهای دیگر، هیأت مدیره اختیارات گسترده‌تری دارد و چارچوب مدیریتی بانک را تعیین می کند. به خاطر این تفاوت‌ها، در این گزارش از واژه‌های «هیأت مدیره» و «مدیریت ارشد» استفاده شده تا صرفنظر از زیرساخت‌های قانونی، هر دو مرجع تصمیم‌گیری در بانک‌ها مورد توجه قرار گیرد.

۱۲- محرمانه نگه داشتن اطلاعات مشتری

۱۳- ظرفیت تداوم ارائه‌ی خدمات و برنامه‌ریزی رخدادهای احتمالی برای اطمنیان از در دسترس بودن همیشگی سیستم‌ها و خدمات بانکداری الکترونیک

۱۴- برنامه‌ریزی واکنش و عکس‌العمل در برابر رخدادهای غیر منتظره[1]

هر یک از موارد یاد شده در ارتباط با بانکداری الکترونیک و اصول مدیریت ریسک که باید توسط بانک‌ها مورد توجه قرار گیرند در بخش‌های بعدی بیشتر توضیح داده می‌شوند. هرجا لازم باشد، اقدامات مؤثر برای مشخص کردن ریسک‌ها به صورت پیوست ارائه می شوند.

الف ـ نظارت هیأت مدیره و مدیریت ارشد(اصول ۱ تا ۳)

هیأت مدیره و مدیریت ارشد مسئول توسعه راهبرد تجاری بانک می‌باشند. در یک تصمیم راهبردی صریح و قبل از شروع ارائه محصولات و خدمات بانکداری الکترونیک باید مشخص گردد که هیأت مدیره تمایل دارد بانک این‌گونه فعالیت‌ها و خدمات را ارائه نماید یا خیر.

به طور مشخص، هیأت مدیره باید اطمینان یابد که برنامه‌های بانکداری الکترونیک به طور واضح در درون اهداف راهبردی بانک لحاظ شده‌اند، تجزیه و تحلیل ریسک در فعالیت‌های پیشنهادی بانکداری الکترونیک به کار گرفته شده است، فرآیندهای نظارت و کاهش ریسک مناسب برای ریسک‌های شناسایی شده اجرا شده‌اند و تجدید نظرهای مستمری در ارزیابی نتایج فعالیت‌های بانکداری الکترونیک نسبت به برنامه‌ها و اهداف تجاری بانک صورت پذیرفته‌اند.

علاوه بر آن، هیأت مدیره و مدیریت باید اطمینان یابند که اجزای ریسک عملیاتی و امنیتی در راهبردهای تجاری بانکداری الکترونیک به طور مناسب مورد ملاحظه و

1 Incident response planning

بررسی قرار گرفته اند. ارائه‌ی خدمات مالی از طریق شبکه اینترنت ممکن است ریسک‌های متداول بانک‌ها (همچون ریسک‌های راهبردی، شهرت، عملیاتی، اعتباری و نقدینگی) را به شدت افزایش دهد. بنابراین، بانک باید اقداماتی جهت حصول اطمینان از اینکه فرآیندهای مدیریت ریسک فعلی بانک، کنترل امنیتی و نظارت مستمر بر روابط برون‌سپاری به طور مناسب و مطابق با خدمات بانکداری الکترونیک مورد ارزیابی و تعدیل قرار گرفته اند، انجام دهد.

اصل۱- هیأت مدیره ومدیریت ارشد بانک باید نظارت مؤثری بر مدیریت بر ریسک‌های مرتبط با فعالیت‌های بانکداری الکترونیک داشته باشند که دربرگیرنده مسئولیت ها، خط‌مشی‌ها و کنترل‌های مورد نیاز جهت مدیریت این ریسک‌ها باشد.

مدیریت نظارت قوی، برای ایجاد کنترل‌های داخلی مؤثر بر فعالیت‌های بانکداری الکترونیکی ضروری است. علاوه بر آن، با توجه به ویژگی‌های خاص شبکه ارتباطی اینترنت، که در مقدمه مورد بحث قرار گرفت، جنبه‌های بانکداری الکترونیک ذیل ممکن است چالش‌های اساسی برای فرآیندهای مدیریت ریسک ایجاد کند:

- عوامل اصلی شبکه انتقال اطلاعات (اینترنت و فن آوری های مرتبط) خارج از کنترل مستقیم بانک است.
- هرچند شبکه اینترنت ارائه‌ی خدمات در سطح بین المللی را تسهیل نموده است، اما دربرگیرنده همه‌ی خدماتی نیست که در حال حاضر توسط بانک به صورت فیزیکی صورت می گیرد.
- پیچیدگی مباحث مرتبط با بانکداری الکترونیک و موارد و جنبه های فنی بالای آن در بسیاری از موارد خارج از تجارب فعلی هیأت مدیره و مدیریت ارشد است.

با وجود ویژگی‌های منحصر به فرد بانکداری الکترونیک، برنامه‌های جدید آن

ممکن است اثر قابل ملاحظه ای بر مجموعه ریسک بانک داشته باشد و راهبرد بانک باید توسط هیأت مدیره و مدیریت ارشد مورد تجدید نظر قرار گرفته و هزینه- منفعت[1] آن باید مورد تجزیه و تحلیل راهبردی قرار گیرد. بدون تجدید ارزیابی مناسب و کامل راهبردها و عملکرد مداوم برنامه‌ها، بانک‌ها با ریسک کاهش برآورد هزینه یا برآورد بیش از حد منافع حاصل از بانکداری الکترونیک مواجه می شوند.

بعلاوه، هیأت مدیره و مدیریت ارشد باید اطمینان یابند که بانک در صورت ورود به فعالیت‌های بانکداری الکترونیک جدید یا تطبیق با روش‌های نوین بانکداری الکترونیک از توانایی و شایستگی لازم جهت نظارت بر مدیریت ریسک برخوردار است. مدیریت و کارکنان اجرایی باید با توجه به ماهیت و پیچیدگی فنی برنامه‌های بانکداری الکترونیک و فن آوری های مرتبط با آنها خود را با شرایط تطبیق دهند. برخورداری از مهارت کافی، هم برای نیروهای داخلی بانک و هم برای کسانی که خارج از بانک به عنوان طرف قرارداد با سیستم‌های بانکداری الکترونیک کار می‌کنند، ضروری است. فرآیندهای نظارت مدیریت ارشد باید به شیوه فعال و به منظور مداخله کارا جهت رفع هرگونه مشکل در سیستم‌های بانکداری الکترونیک و حل مسائل امنیتی که ممکن است اتفاق بیافتند، اجرا شود. افزایش ریسک شهرت، اهمیت نظارت قوی بر فعالیت‌های عملیاتی سیستم‌ها و حصول رضایت مشتری و ارائه گزارش مناسب به هیأت مدیره و مدیریت ارشد را نمایان می‌سازد.

در نهایت، هیأت مدیره و مدیریت ارشد باید اطمینان یابند که فرآیندهای مدیریت ریسک فعالیت‌های بانکداری الکترونیک با رویکرد مدیریت ریسک کلی بانک هماهنگ و یکپارچه می‌باشد. سیاست‌ها و دستورالعمل‌های مدیریت ریسک فعلی بانک باید به گونه‌ای باشند تا اطمینان حاصل گردد ریسک‌های جدید فعالیت‌های بانکداری الکترونیک در سطح برنامه‌ریزی شده یا جاری به طور مناسب ارزیابی می‌شوند.

---

1 Cost-Benefit

اقدامات بیشتر نظارت بر مدیریت ریسک، که هیأت مدیره و مدیریت ارشد باید مورد ملاحظه قرار دهند، به شرح ذیل است:

- مشخص کردن دقیق نقاط ریسک‌پذیر سازمان در ارتباط با فعالیت‌های بانکداری الکترونیک
- مشخص کردن مسئولیت‌ها و مکانیزم‌های گزارش‌دهی، شامل دستورالعمل‌های لازم در مواقعی که بر ثبات و سلامت یا شهرت بانک اثر می‌گذارند (همچون نفوذ در شبکه، تخلفات امنیتی کارکنان و هرگونه سوءاستفاده از تجهیزات کامپیوتری)[1]
- شناسایی همه‌ی عوامل منحصر به فرد ریسک مرتبط با مسائل امنیتی، صحت، اصالت و دسترسی به خدمات و محصولات بانکداری الکترونیک که نیازمند برون سپاری سیستم‌های اصلی بانک می‌باشد
- اطمینان از اینکه قبل از ارائه‌ی خدمات و محصولات بانکداری الکترونیک، تجزیه و تحلیل دقیق ریسک صورت پذیرفته است.

اینترنت به طور قابل ملاحظه‌ای توانایی یک بانک برای توزیع کالاها و خدمات در مناطق جغرافیایی کاملا ًنامحدود را تسهیل می‌کند. اینگونه فعالیت بانکداری الکترونیک در عرصه جهانی، خصوصاً اگر بدون هرگونه حضور فیزیکی در کشور میزبان صورت پذیرد، به طور بالقوه باعث افزایش ریسک قانونی، ریسک نظارت و ریسک کشوری می شود، زیرا ممکن است بین رعایت الزامات امنیتی از سوی نهادهای قانونی کشور میزبان و الزامات حمایت از مشتری و نظارت از سوی بانک تفاوت‌های اساسی وجود داشته باشد. به خاطر اجتناب از عدم تطابق ناخواسته با قوانین و مقررات یک کشور خارجی و مدیریت عوامل ریسک کشور مربوطه، بانک‌ها باید قبل از مبادرت به

1علاوه بر الزامات گزارش‌های داخلی، گزارش رخدادهای غیرمنتظره جزء جدایی ناپذیر گزارش‌های ارائه شده به مقامات نظارتی است.

فعالیت‌های عملیاتی بانکداری الکترونیک در مورد فعالیت‌های عملیاتی و ریسک مرتبط با آن به طور کامل تحقیق و تفحص کنند.[1]

براساس دامنه و پیچیدگی فعالیت‌های بانکداری الکترونیک، دامنه و ساختار برنامه‌های مدیریت ریسک در بانک‌های مختلف، متفاوت است. منابع مورد نیاز جهت نظارت بر فعالیت‌های بانکداری الکترونیک باید با کارکرد و حساسیت سیستم‌ها، آسیب پذیری شبکه ها و حساسیت اطلاعات ارسالی متناسب باشد.

اصل ۲- هیأت مدیره و مدیریت ارشد باید جنبه های کلیدی فرآیند کنترل امنیتی بانک را مورد بررسی قرار داده و آنها را مورد تأیید قرار دهند.

هیأت مدیره و مدیریت ارشد باید بر توسعه و نگهداری مستمر زیرساخت های کنترل امنیتی، که سیستم‌های بانکداری الکترونیک و اطلاعات را از تهدیدهای داخلی و خارجی محافظت می‌کند، نظارت داشته باشند. این اقدامات باید دربرگیرنده اجازه کاربری[2]، دسترسی مجازی و فیزیکی[3] به کنترل‌ها و زیرساخت های امنیتی مناسب، جهت رعایت محدودیت‌های مشخص در مورد فعالیت‌های کاربران داخلی و خارجی باشد.

حفاظت از دارایی‌های بانک یکی از وظایف هیأت مدیره و یکی از مسئولیت-های اساسی مدیریت ارشد است. به هر حال به خاطر پیچیدگی ریسک‌های امنیتی مرتبط با فعالیت‌های عملیاتی بر روی شبکه عمومی اینترنت و استفاده از فن آوری جدید، حفاظت از دارایی‌های بانک یکی از وظایف چالشی در محیط بانکداری الکترونیک محسوب می‌گردد.

1برای جزئیات بیشتر نگاه کنید به: نشریه کمیته بال در مورد نظارت بانکی تحت عنوان« نظارت و مدیریت بر فعالیتهای بانکداری الکترونیک در خارج از مرزها»

2 **Authorisation privilege**

3 **Logical and physical access**

جهت حصول اطمینان از کنترل‌های امنیتی صحیح بر فعالیت‌های بانکداری الکترونیک، هیأت مدیره و مدیریت ارشد باید مشخص کنند که آیا بانک از یک فرآیند امنیتی جامع، شامل خط‌مشی‌ها و دستورالعمل ها، برخوردار است و می‌تواند تهدیدهای ایمنی داخلی و خارجی بالقوه را مورد شناسایی قرار داده و برای جلوگیری از وقوع آنها عکس العمل مناسبی انجام دهد یا خیر. عناصر کلیدی یک فرآیند امنیتی مؤثر بانکی شامل موارد ذیل است:

- **مشخص کردن صریح مسئولیت مدیریت و کارکنان جهت نظارت بر تعیین و حفظ خط مشی‌های امنیتی بانک.[1]**
- **کنترل‌های فیزیکی کافی جهت جلوگیری از دسترسی فیزیکی افراد غیرمسئول به محیط کامپیوتری.**
- **کنترل‌های مجازی کافی و فرآیندهای نظارت[2] مناسب جهت جلوگیری از دسترسی داخلی[3] و خارجی افراد غیرمسئول به برنامه‌های کاربردی و پایگاه اطلاعاتی بانکداری الکترونیک.**
- **بررسی و آزمایش معیارها و کنترل‌های امنیتی به طور مستمر و منظم، شامل گسترش مداوم برنامه‌های امنیتی و نصب آخرین برنامه‌های نرم افزاری مناسب و بسته های خدماتی و سایر معیارهای مورد نیاز در این زمینه.[4]**

---

1 این مسئولیت به طور معمول جزئی از شرح وظایف حسابرسی که وظیفه بررسی نحوه نظارت مؤثر بر کنترلهای امنیتی را به عهده دارد، نیست.

2 شامل حق دسترسی کنترل شده و نظارت مداوم بر تلاش‌هایی که برای ورود بدون اجازه به شبکه صورت می گیرد.

3 شامل کارکنان، پیمانکاران و کسانی که براساس قراردادهای برون سپاری به اطلاعات دسترسی دارند

4 شامل ضوابط نظارت بر فعالیت‌های شبکه، گزارش تلاش های صورت گرفته برای ورود غیر مجاز به شبکه و شکاف‌های مهم امنیتی.

پیوست شماره ۱، برخی اقدامات مؤثر در زمینه حصول اطمینان از ایمنی بانکداری الکترونیک را ارائه می کند.

اصل ۳– هیأت مدیره و مدیریت ارشد باید برنامه ریزی و نظارت مستمر و جامعی درخصوص مدیریت روابط برون سپاری و واگذاری فعالیت‌ها به سایر اشخاص خارج از بانک صورت دهد.

افزایش اتکای بانک‌ها به شرکتهای تأمین خدمات الکترونیک جهت انجام فعالیت‌های بانکداری الکترونیک باعث کاهش کنترل مستقیم مدیریت بانک می‌شود.

بر این اساس، یک فرآیند جامع برای مدیریت ریسک‌های مرتبط با واگذاری فعالیت‌ها به خارج از بانک و وابستگی ها به اشخاص ثالث ضروری است. این فرآیند فعالیت‌های مربوط به تأمین خدمات از طریق اشخاص ثالث و قراردادهای فرعی مربوط به برون سپاری بانک، که ممکن است اثر مشهودی بر فعالیت‌های بانک داشته باشد، را دربر می گیرد.

به لحاظ تاریخی، قبلاً برنامه برون سپاری عموماً به یک تأمین کننده خدمات و برای انجام فعالیت‌های خاص محدود شده بود، اما در سالهای اخیر، روابط حاکم در واگذاری فعالیت‌های بانک به خارج، از لحاظ مقیاس و پیچیدگی و به عنوان نتیجه مستقیم پیشرفت فن آوری اطلاعات و ظهور خدمات جدید بانکداری الکترونیک گسترده شده است. علاوه بر آن، پیچیدگی برنامه‌های بانکداری الکترونیک یک واقعیت است و برنامه برون سپاری می‌تواند به صورت قراردادهای فرعی با تأمین‌کنندگان داخلی یا خارجی انجام شود. با پیشرفت و رشد راهبردی محصولات و خدمات بانکداری الکترونیک، حوزه‌های عملکردی خاص آن از قبیل تعداد فروشندگان تخصصی و تأمین‌کنندگان خدمات وابسته نیز افزایش یافته است. پیشرفت‌ها در این زمینه ممکن است منجر به افزایش ریسک شوند، بنابراین نیاز به یک ارزیابی جامع و

مداوم درخصوص نحوه واگذاری فعالیت‌ها به اشخاص ثالث در خارج از بانک، که دربرگیرنده مفاهیم مرتبط با مجموعه ریسک بانک و توانایی‌های نظارت بر مدیریت ریسک باشد، مشهود می‌باشد.[1] نظارت هیأت مدیره و مدیریت ارشد بر روابط حاکم در واگذاری فعالیت‌ها و منابع به خارج و وابستگی‌ها به اشخاص ثالث باید به طور خاص بر حصول اطمینان موارد ذیل متمرکز باشد:

- **بانک کاملاً به ریسک‌های مرتبط با واگذاری منابع به خارج یا قرارداد مشارکت برای سیستم‌های بانکداری الکترونیک یا برنامه‌های کاربردی آن آگاه باشد.**
- **یک بررسی دقیق و مناسب درخصوص شایستگی و اعتبار مالی هریک از اشخاص ثالث تأمین‌کننده خدمات یا مشارکت کننده که درخصوص خدمات بانکداری الکترونیک با آنها قرارداد منعقد می‌گردد، صورت پذیرد.**
- **مسئولیت تمام مشارکت کنندگان یا اشخاص ثالثی که منابع و فعالیت‌های بانک به آنها واگذار می‌شود[2] ، در تمام جنبه های قرارداد به طور واضح تعریف شود. برای مثال، مسئولیت ارائه اطلاعات تأمین کنندگان خدمات و دریافت اطلاعات از آنها به طورمشخص تعیین شود.**
- **تمام سیستم‌ها و فعالیت‌های عملیاتی بانکداری الکترونیک، که برون سپاری شده و مشمول مدیریت ریسک، خط مشی های امنیتی و حفظ اسرار مشتری قرار می گیرد، باید با استانداردهای بانک مطابقت داشته باشد.**

---

1 این ارزیابی ها باید در مورد میزان کنترل بر اشخاص ثالث طرف قرارداد نیز صورت گیرد. در بسیاری از موارد کنترل در مورد یک شریک که در ریسک سهیم است، نسبت به یک پیمانکار ارائه دهنده خدمات باید بیشتر باشد. به هرحال، این بدان معنا نیست که کنترل یک شریک، به ویژه زمانی که خدمات و فن آوری‌های مورد نیاز برای عملیات بانک توسط یک شریک وابسته صورت می گیرد به تنهایی کافی است. به ویژه زمانی که خدمات و فن آوری‌های مورد نیاز برای عملیات توسط یک شریک وابسته صورت می گیرد

2 این مورد شامل پیمانکاران فرعی هم می شود.

- حسابرسان مستقل و داخلی به صورت دوره ای فعالیت‌های مرتبط با برون‌سپاری را مورد بررسی قرار دهند.
- برنامه‌های اقتضایی مناسبی برای برون سپاری فعالیت‌های بانکداری الکترونیک ایجاد شود.

پیوست شماره۲،برخی از اقدامات مؤثر در خصوص مدیریت برون سپاری سیستم‌های الکترونیکی و وابستگی به اشخاص ثالث را به طور تفصیلی‌تری ارائه می کند.

ب- کنترل‌های امنیتی (اصول ۴ تا ۱۰)

هیأت مدیره مسئولیت حصول اطمینان از فرآیندهای کنترل امنیتی مناسب برای فعالیت‌های بانکداری الکترونیک را بر عهده دارد و مدیریت ارشد باید توجه خاصی به این فرآیندها داشته باشد، زیرا فعالیت‌های بانکداری الکترونیک با چالش‌های امنیتی در حال افزایش مواجه می‌باشند[1]. موارد ذیل از جمله چالش‌های مربوطه می‌باشد:

- اجازه کاربری[2]
- عدم انکار[3]
- صحت داده ها و مبادلات
- تفکیک وظایف
- کنترل‌های کاربری
- انجام حسابرسی های آتی

---

1 به عنوان مثال، در جایی که هیأت مدیره در خدمات بانکداری الکترونیک به شخص ثالث ارائه دهنده خدمات تکیه می کند، باید اطمینان حاصل کند که وی به طور کافی به این چالشها توجه دارد و حداقل استانداردهای بانک را رعایت می کند.

2 authorization

3 Non-repudiation

- محرمانه نگه داشتن اطلاعات کلیدی بانک

اصل ۴- بانک‌ها باید معیارهای مناسبی جهت تعیین اعتبار، احراز هویت و اجازه کاربری[1] مشتریانی که از طریق شبکه اینترنت مبادرت به فعالیت بانکداری الکترونیک می‌نمایند، داشته باشند.

ضروری است بانک‌ها قانونی بودن مبادلات و درخواست دسترسی افراد به شبکه اینترنت را تأیید کنند. همچنین بانک‌ها باید روش‌های قابل اتکایی جهت تأیید، شناسایی و اجازه فعالیت مشتریان به مبادلات الکترونیک بکارگیرند.

تأیید اعتبار مشتری در جریان افتتاح حساب جهت کاهش ریسک سرقت، عدم بکارگیری شماره حساب تقلبی و جلوگیری از پول‌شویی ضرورت دارد. کوتاهی و ناتوانی بانک در شناسایی و احراز هویت صحیح مشتریان ممکن است موجب دسترسی افراد غیرمجاز به حساب‌های الکترونیک شود و در نهایت بانک به علت تقلب و افشای اطلاعات محرمانه با زیان سوء شهرت مواجه شده و درگیر فعالیت‌های مجرمانه افراد متقلب گردد.

بکارگیری برنامه‌هایی جهت شناسایی و احراز هویت مشتری و اجازه دسترسی به سیستم‌های بانک در یک محیط شبکه‌ای و باز الکترونیک ممکن است وظیفه دشواری باشد. اجازه کاربری مشروع می‌تواند از طریق مجموعه روش‌هایی که

---

1 تعیین اعتبار(Authentication) که در این گزارش به آن اشاره شده، عبارتست از روش‌ها و فرآیندهایی که برای تأیید هویت و اجازه کاربری یک مشتری بالقوه بکار می روند. تشخیص هویت(Identification)عبارتست از روش‌ها و فرآیندهایی که برای شناسایی یک مشتری هنگام افتتاح حساب بکار می روند. اجازه کاربری(Authorization) عبارتست از روش‌ها و فرآیندهایی که برای تعیین میزان دسترسی مشتری یا کارکنان به حساب‌های بانکی یا انجام مبادلات آن حساب به کار می‌رود

عموماً تحت عنوان حقه بازی(Spoofing)[1] نام برده می‌شود، مورد سوء استفاده قرار گیرد. هکرهای شبکه می‌توانند به روش‌های مختلف از جمله استراق سمع (Sniffer)[2] به اطلاعات محرمانه افراد مجاز دست پیدا کرده و یا به فعالیت‌های مجرمانه ای دست بزنند. همچنین فرآیندهای کنترل شناسایی و تأیید مشتریان می‌تواند از طریق تغییر در پایگاه اطلاعاتی مورد نفوذ قرار گیرند.

بنابراین، بانک‌ها باید روش‌ها و دستورالعمل هایی مدون جهت شناسایی و تأیید کامل فرد، کارگزار یا سیستم[3]داشته باشند که منحصر به فرد و کارا بوده و منجر به عدم دسترسی افراد و سیستم‌های[4] غیرمجاز به اطلاعات شبکه گردد. بانک‌ها می‌توانند جهت تأیید و شناسایی مشتری از روش‌هایی از قبیل PIN (شماره شناسایی شخصی)، رمزهای عبور، کارت های هوشمند[5]، تشخیص هویت و گواهی دیجیتالی استفاده کنند[6]. هرکدام از این روش‌ها می‌تواند یک عاملی یا چند عاملی(به عنوان

---

1 استفاده غیرمجاز یک مشتری مجاز از شماره حساب، کلمه عبور، کد شناسایی و آدرس پست الکترونیک جهت دسترسی به حساب الکترونیک

2 ابزاری است که از طریق آن می توان از شبکه های ارتباطی، کدهای محاسباتی و اطلاعات در حال انتقال استراق سمع نمود.

3 سیستم شامل وب سایت بانک هم می شود.

4 سیستمها باید اطمینان حاصل کنند که با یک فرد، کارگزار یا سیستم مجاز و یک پایگاه داده مورد تأیید در ارتباط هستند.

5 Smart cards

6 یک بانک ممکن است با استفاده از زیرساختهای عمومی کلیدی(PKI) گواهی‌های دیجیتالی برای مشتریان صادر کند تا امنیت رابطه آنها با بانک تأمین شود. گواهی‌های دیجیتال و زیرساختهای عمومی کلیدی (PKI) در اصل ۵ توضیح داده می شوند.

مثال، استفاده از هر دو عامل کلمه عبور و روش تشخیص هویت[1] جهت تأیید مشتری) باشد. معمولاً شناسایی چندعاملی اطمینان بیشتری را فراهم می‌سازد.

بانک باید روش‌هایی جهت شناسایی و تأیید مشتری بکارگیرد که مدیریت ریسک بانکداری الکترونیک و جزئیات آن لحاظ شده باشد. در تجزیه و تحلیل ریسک بانکداری الکترونیک باید توانمندی‌های مبادلاتی[2] سیستم‌های الکترونیک (به عنوان مثال انتقال وجوه، پرداخت صورتحساب، یکپارچه‌سازی حساب‌ها و غیره)، حساسیت و ارزش داده‌های ذخیره شده الکترونیک و سهولت استفاده کاربران از روش‌های احراز هویت لحاظ شوند.

فرآیندهای قوی شناسایی و احراز هویت مشتری در بانکداری الکترونیک، علی‌رغم دشواری‌های زیاد، از اهمیت خاصی برخوردار است، زیرا انجام مبادلات الکترونیک با مشتری در محدوده کشوری و بین المللی صورت می گیرد و ریسک‌های فزاینده‌ای در ارتباط با شناسایی افراد به همراه دارد. بنابراین، دشواری زیادی در کنترل‌های مؤثر مشتریان وجود دارد.

با توجه به گسترش وتکامل روش‌های شناسایی و احراز هویت مشتریان، بانک باید روش‌هایی جهت حصول اطمینان در بکارگیری موارد ذیل انجام دهد:

- پایگاه اطلاعاتی مربوط به شناسایی و احراز هویت مشتریان، که دسترسی به حساب‌های مشتری یا سیستم‌های حساس الکترونیک را مهیا می‌سازند، در دسترس افراد غیرمجاز قرار نگیرد و هرگونه مداخله غیرمسئولانه در این زمینه ردیابی شده و در حسابرسی اسناد و مدارک نشان داده شود.

---

1 تشخیص هویت یک روش خودکار شناسایی مشخصه های فیزیکی و رفتاری جهت تایید یک فرد می باشد. روش های متداول تشخیص هویت شامل اسکن فیزیکی، اسکن انگشت، اسکن صدا و غیره می باشد

2 اگرضوابط تعیین اعتبار مؤثر باشند، بانک‌ها می توانند ریسک انکار را کاهش دهند، اما مکمن است پیچیدگی بکارگیری این ضوابط از سایر روشهای احراز هویت و اعطای اجازه کاربری بیشتر باشد.

- هر گونه اضافه، حذف یا تغییر یک فرد، عامل یا سیستم از پایگاه اطلاعاتی مربوط به شناسایی و تأیید مشتریان منحصراً توسط مقامات مسئول و مجاز صورت پذیرد.[1]
- معیارهای مناسب شناسایی و تأیید مشتری، که ارتباط با سیستم بانکداری الکترونیک را کنترل می کنند، به گونه ای باشند که اشخاص ناشناخته توانایی شناسایی مشتریان شناخته شده را نداشته باشند.
- ارتباط بین فرستنده و گیرنده در زمان شناسایی طرفین و در جریان ارتباط فی مابین باید کاملاً محرمانه باقی بماند.

اصل ۵- بانک‌ها باید از روش‌های شناسایی واحراز هویتی جهت انجام مبادلات استفاده کنند که انکار در فعالیت‌های الکترونیک را کاهش داده و مسئولیت‌ها در انجام مبادلات بانکداری الکترونیک را معین سازد.

تأییدیه عدم انکار مبادلات در برگیرنده مدرکی روشن و یا اطلاعات الکترونیک است که باعث ایجاد اطمینان خاطر فرستنده در قبال انکار احتمالی گیرنده در دریافت اطلاعات ارسالی به وی می‌شود.

ریسک انکار مبادلات در حال حاضر یک بحث مربوط به مبادلات متداول الکترونیکی از قبیل کارت های اعتباری است.

به هر حال ریسک انکار مبادلات فعالیت‌های بانکداری الکترونیک بالا است، زیرا مشکلات مربوط به شناسایی و احراز هویت دو طرف یک مبادله، مشکلات مربوط به تغییر یا تقلب در مبادلات الکترونیک و مشکلات مربوط به ادعای کاربران الکترونیک مبنی بر تقلب در مبادلات در حال افزایش است.

---

1 در بعضی از موارد، منبع تعیین اعتبار ممکن است یک منبع الکترونیک باشد.

بنابراین بانک‌ها باید جهت کاهش این ریسک، براساس نوع و اهمیت مبادلات الکترونیک اقدامات مناسبی انجام دهند تا اطمینان حاصل گردد:

- **سیستم‌های بانکداری الکترونیک جهت کاهش احتمال انجام مبادلات ناخواسته کاربران مجاز طراحی شده است و مشتریان به طور کامل با ریسک‌های مرتبط با انواع مبادلاتی که انجام می دهند آشنایی دارند.**
- **تمام طرف‌ها در مبادلات به طور دقیق همدیگر را مورد شناسایی قرار داده و ابزارهای کنترلی لازم بر روی کانال‌های شناسایی و احراز هویت افراد لحاظ شده است.**
- **داده‌های مربوط به رخداد های مالی در برابر هرگونه تغییر احتمالی محافظت شده است.**

اخیراً بانک‌ها از روش‌هایی جهت احراز هویت مشتری استفاده می‌کنند که باعث افزایش رازداری و اصالت مبادلات[1] بانکداری الکترونیک می گردد، همچون گواهی دیجیتال که از زیر ساخت عمومی کلیدی (Public Key Infrastructure)[2] استفاده می‌کند. بانک ممکن است برای مشتری یا طرف قرار داد یک گواهینامه دیجیتال صادر کند و به آنها یک اجازه کاربری منحصر به فردی اعطا نماید تا ریسک انکار مبادلات بانکداری الکترونیک کاهش یابد.

---

1 Integrity of transaction

2 در زیر ساخت کلیدی اصلی هر یک از طرف های انجام مبادله دو شماره کلید عمومی و خصوصی دریافت می کنند. کلید خصوصی باید برای شخص استفاده کننده محرمانه باقی بماند، اما هر دو طرف از کلیدهای عمومی استفاده می کنند. کلید خصوصی یک امضای الکترونیک را بر روی سند ایجاد می کند. هر دو کلید عمومی و خصوصی به گونه ای طراحی شده اند که پیام رمز گذاری شده با کلید خصوصی بتواند تنها با استفاده از کلید دیگری خوانده شود.

اصل ۶ – بانک‌ها باید از وجود معیارهای مناسب جهت تفکیک مطلوب وظایف در زمینه برنامه‌ها، پایگاه‌های اطلاعاتی و سیستم‌های بانکداری الکترونیک اطمینان حاصل کنند.

تفکیک وظایف، که یکی از معیارهای اساسی کنترل داخلی محسوب می‌شود، جهت کاهش ریسک تقلب در فرآیندهای عملیاتی و سیستم‌ها و حصول اطمینان از ثبت صحیح و حفاظت از انجام مبادلات و دارایی‌های بانک توسط افراد مجاز صورت می‌گیرد. تفکیک وظایف، که برای حصول اطمینان از صحت و اصالت داده‌ها جنبه حیاتی دارد، در راستای جلوگیری از انجام تقلب توسط اشخاص صورت می‌پذیرد. اگر وظایف به درستی تفکیک شوند، تقلب تنها از طریق تبانی می‌تواند انجام شود.

خدمات بانکداری الکترونیک ممکن است باعث تغییر روش‌های تفکیک وظایف به کار گرفته شده در بانکداری متداول شود، زیرا در بانکداری الکترونیک مبادلات از طریق سیستم‌های الکترونیک انجام می‌شود که امکان هرگونه تقلب در آن وجود دارد. ضمن این که فعالیت‌های الکترونیک در بسیاری از موارد به صورت یکپارچه صورت می‌پذیرد. بنابراین، کنترل‌هایی که به طور معمول مستلزم تفکیک وظایف بوده باید مورد ارزیابی مجدد قرار گرفته تا از وجود سطح مناسب کنترل اطمینان حاصل شود. از آنجایی که دسترسی به پایگاه‌های اطلاعاتی می‌تواند از طریق شبکه‌های داخلی و خارجی صورت پذیرد، انجام روش‌های شناسایی واحراز هویت قوی، برخورداری از زیرساخت‌های مطمئن و روش‌های حسابرسی مناسب باید مورد تأیید قرار گیرند.

به کارگیری تفکیک وظایف در قلمرو بانکداری الکترونیک باید مشتمل بر موارد ذیل باشد:

- فرآیندها و سیستم‌های مبادلاتی باید به گونه‌ای طراحی شود که هیچ یک از تأمین‌کنندگان خدمات الکترونیک نتوانند به سیستم وارد شده و یا اقدام به انجام مبادله نمایند.

- باید بین مسئول ورود داده‌های اولیه (شامل مطالب مندرج در صفحه وب) و مسئول بررسی صحت داده‌ها تفکیک وظایف صورت پذیرد.
- سیستم‌های بانکداری الکترونیک باید آزمایش شوند تا اطمینان حاصل گردد وظایف موازی و متداخل وجود ندارد.
- باید سیستم‌های بانکداری الکترونیک در حال توسعه و سیستم‌های بانکداری الکترونیک درحال اجرا از یکدیگر تفکیک شوند. [1]

اصل ۷ – بانک‌ها باید از کنترل تأیید اعتبار، احراز هویت و حق دسترسی به برنامه‌ها، پایگاه‌های اطلاعاتی و سیستم‌های بانکداری الکترونیک اطمینان حاصل کنند.

به منظور حفظ تفکیک وظایف، بانک‌ها نیازمند کنترل قوی احراز هویت و دسترسی به سیستم‌های الکترونیک هستند. ناتوانی در انجام کنترل مناسب تأیید اعتبار و احراز هویت ممکن است باعث شود اشخاص غیرمجاز به سیستم‌ها، پایگاه‌های اطلاعاتی یا به محدوده‌های کاربری غیر مجاز در بانکداری الکترونیک دست پیدا کنند.

در سیستم‌های بانکداری الکترونیک، شناسایی مشتریان و حق دسترسی آنها به حساب‌های خویش می‌تواند به صورت متمرکز یا پراکنده در یک بانک انجام شده و در یک پایگاه اطلاعاتی ذخیره شود. بنابراین حفاظت پایگاه اطلاعاتی از هرگونه سوءاستفاده و یا خرابی، برای کنترل مؤثر شناسایی و احراز هویت مشتریان بسیار حیاتی است.

پیوست شماره ۳، بعضی از اقدامات مناسب را در این زمینه ارائه می‌کند.

---

1 یا از سایر کنترلهای جایگزین استفاده شود.

اصل ۸ – بانک‌ها باید از وجود معیارهای مناسب جهت حفاظت از اصالت داده‌های مبادلات الکترونیک، ثبت آنها و اطلاعات مربوطه اطمینان حاصل نمایند.

اصالت داده‌ها به این معنی است که اطلاعاتی که در حال ذخیره کردن بوده و یا ذخیره شده‌اند، بدون اجازه افراد مجاز تغییر نکرده‌اند. ناتوانی در حفاظت صحیح داده‌های مبادلاتی، ثبت آنها و اطلاعاتی که می‌تواند بانک‌ها را در معرض زیان‌های مالی قرار دهند باعث ریسک شهرت و قانونی می‌شوند. ماهیت ذاتی فرآیند فعالیت‌های الکترونیک به گونه‌ای است که ممکن است با اشتباه در برنامه‌ریزی یا فعالیت متقلبانه همراه باشد و حفاظت از داده‌ها را در هر مرحله با مشکلات جدی همراه سازد. بنابراین بانک‌ها باید فرآیندهای داده پردازی را به شیوه‌ای به کار گیرند که اصالت و صحت داده‌ها حفظ شود.

همچنانکه فعالیت‌های بانکداری الکترونیک از طریق شبکه‌های عمومی صورت می‌پذیرد، داده‌های مبادلات الکترونیک نیز در معرض انحراف، تقلب و اشتباه در ثبت قرار می‌گیرند. بر همین اساس، بانک‌ها باید از وجود معیارهای مناسب جهت حصول اطمینان از صحت، جامعیت و قابلیت اتکای مبادلات، ثبت‌ها و اطلاعات فعالیت‌های بانکداری الکترونیک، که از طریق شبکه اینترنت صورت گرفته و در پایگاه‌های اطلاعاتی داخلی بانک ذخیره شده و یا از طریق کارگزار بانک فعالیت‌های آنها صورت می‌گیرد، اطمینان حاصل نمایند.[1] اقدامات متداول مورد استفاده جهت حفاظت از اصالت داده‌ها در زمینه بانکداری الکترونیک در برگیرنده موارد ذیل است:

- **مبادلات بانکداری الکترونیک باید به شیوه‌ای انجام شود که از هرگونه سوء استفاده یا انحراف در کل فرآیندهای الکترونیک به شدت جلوگیری نماید.**

---

1 بانکها باید اطمینان حاصل کنند که سیستم نگهداری اسناد به گونه ای طراحی و پیاده سازی شده است که اسنادی که تغییر داده شده اند یا از بین رفته اند، قابل بازیابی باشد.

- اسناد بانکداری الکترونیک باید به شیوه‌ای دریافت، ذخیره و نگهداری شوند که از هرگونه رخنه و نفوذ در امان باشند.
- مبادلات الکترونیک و فرآیندهای ثبت آنها باید به شیوه‌ای طراحی شوند که از هرگونه شناسایی غیرمجاز در امان باشند.
- سیاست‌های کنترل تغییر مناسب، شامل نظارت و آزمایش دستورالعمل‌ها باید به شیوه‌ای باشند که از هرگونه تغییرات سیستم بانکداری الکترونیک، که ممکن است به طور اشتباه یا ناخواسته قابلیت اتکاء داده‌ها و کنترل‌ها را زیر سئوال می‌برد، ممانعت به عمل آورد.
- هرگونه نفوذ و رخنه در مبادلات یا ثبت‌های الکترونیک باید از طریق پردازش و نظارت بر مبادلات و ثبت کاغذی آنها مشخص شود.

اصل ۹ – بانک‌ها باید اطمینان حاصل کنند که برنامه‌های حسابرسی آتی مشخصی برای تمام مبادلات بانکداری الکترونیک وجود دارد.

ارائه‌ی خدمات مالی از طریق شبکه اینترنت مشکلات زیادی برای بانک‌ها به همراه دارد و مستلزم بکارگیری کنترل‌های داخلی و برنامه‌های حسابرسی دقیق می‌باشد. بانک‌ها با چالش حصول اطمینان از وجود کنترل داخلی مؤثر مواجه هستند، لذا کنترل‌ها و فعالیت‌های حساس بانکداری الکترونیک باید به طور مستقل حسابرسی شوند.

محیط کنترل داخلی بانک ممکن است در صورت ناتوانی در بکارگیری روش‌های حسابرسی دقیق فعالیت‌های الکترونیک ضعیف شود، زیرا ثبت فعالیت‌ها و مبادلات به شکل الکترونیک صورت می‌گیرد. در راستای به کارگیری روش‌های حسابرسی دقیق، انواع مبادلات بانکداری الکترونیک ذیل باید منظور شوند:

- ایجاد، اصلاح یا بستن یک حساب مشتری

- هرگونه انجام فعالیت‌های مالی
- هرگونه اجازه کاربری داده شده به مشتری که فراتر از محدوده تعیین شده باشد.
- هرگونه اعطاء، اصلاح یا لغو دسترسی به سیستم‌های الکترونیک.

پیوست شماره ۴، برخی از اقدامات مؤثری جهت حصول اطمینان از وجود روش‌های حسابرسی آتی برای مبادلات الکترونیکی ارائه می‌نماید.

اصل۱۰- بانک‌ها باید معیارهای مناسبی جهت حفظ رازداری اطلاعات کلیدی بانکداری الکترونیک تدوین نمایند. معیارهای تعیین شده باید متناسب با حساسیت اطلاعاتی باشد که به پایگاه اطلاعاتی انتقال یافته و یا در آنجا ذخیره می‌شوند.

رازداری به معنی اطمینان از این موضوع است که اطلاعات به طور محرمانه نزد بانک باقی می ماند و قابل رؤیت یا استفاده توسط اشخاص غیر مجاز نیست. سوءاستفاده یا افشای غیرمجاز اطلاعات، بانک را با ریسک شهرت و ریسک قانونی مواجه می‌سازد. پیدایش بانکداری الکترونیک چالش امنیتی در بانک‌ها را افزایش داده است، زیرا در بانکداری الکترونیک اطلاعات از طریق یک شبکه عمومی منتقل می‌شوند و یا در پایگاه داده‌هایی ذخیره می‌شوند که ممکن است در دسترس افراد غیر مجاز و غیر مرتبط قرار گیرد و یا به گونه‌ای مورد استفاده قرار گیرند که مطلوب مشتری نباشد. علاوه بر این استفاده از شرکت‌های خدمات پشتیبانی ممکن است اطلاعات کلیدی بانک‌ها را در اختیار دیگران قرار دهد.

برای مواجهه با این چالشها و حفظ رازداری در مورد اطلاعات کلیدی بانکداری الکترونیک، بانک‌ها باید اطمینان حاصل کنند که:

- همه‌ی داده‌ها و اسناد محرمانه بانک تنها توسط افراد ، کارگزاران و سیستم‌های مجاز و مورد تأیید قابل دسترسی است.

- همه‌ی داده‌های محرمانه بانک به روشی امن نگهداری می شوند و از دسترسی افراد غیر مجاز یا تغییر در فرآیند انتقال از طریق شبکه های داخلی، خصوصی و عمومی محفوظ می مانند.
- زمانی که(در موارد برون سپاری) اشخاص ثالث به اطلاعات دسترسی دارند، استانداردها و کنترل‌های بانک برای استفاده و حفاظت از داده ها رعایت می‌شوند
- همه‌ی دسترسی ها به اطلاعات محرمانه محدود شده و تلاش‌های مناسبی برای اطمینان از اینکه محدودیت‌های دسترسی غیرقابل نفوذ هستند، به عمل می‌آید.

ج- مدیریت ریسک قانونی و ریسک شهرت(اصول۱۱ الی۱۴)

حمایت ویژه از مشتری و قوانین و مقررات حفظ اسرار مشتری از یک کشور به کشور دیگر بسیار متفاوت است. به هرحال، بانک‌ها به طور کلی مسئولیت روشنی دارند تا آسایش خاطر مشتریان خود را در مورد افشا و حفاظت از اطلاعات و نیز دسترسی مداوم آنها به کانال‌های ارائه‌ی خدمات بانکداری الکترونیک را فراهم نمایند.

اصل ۱۱- بانک‌ها باید قبل از مبادرت به فعالیت‌های بانکداری الکترونیک اطمینان حاصل کنند که اطلاعات مورد نیاز مشتریان در مورد وضعیت و مقررات بانک در پایگاه اینترنتی بانک وجود دارد.

برای به حداقل رساندن ریسک شهرت مرتبط با فعالیت‌های بانکداری الکترونیک در داخل و خارج از کشور بانک‌ها باید اطمینان حاصل کنند که اطلاعات کافی در وب سایت آنها به مشتریان ارائه می‌شود تا آنها قبل از اینکه وارد مبادلات

بانکداری الکترونیک شوند، از وضعیت و مقررات بانک آگاه شوند.

نمونه هایی از اطلاعاتی که بانک می‌تواند در وب سایت خود ارائه دهد عبارتند از:

- نام بانک و آدرس دفتر مرکزی(و دفاترمنطقه ای در صورت وجود).
- وضعیت مقام ناظر بانکی که مسئولیت نظارت بر دفتر مرکزی را به عهده دارد.
- مشتریان در صورتی که مشکل یا شکایتی داشتند و یا در مورد سوء استفاده از حساب خود مشکوک شدند، چگونه می توانند با مرکز خدمات مشتری بانک ارتباط برقرار کنند.
- مشتریان چگونه می توانند به برنامه‌های کاربردی رسیدگی به شکایات دسترسی داشته و از آن استفاده کنند.
- مشتریان چگونه می توانند به اطلاعاتی در مورد طرح ملی جبران خسارت[1] یا پوشش بیمه سپرده و سطح حمایتی که از آنها به عمل می آید دسترسی پیدا کنند.(وب‌سایت بانک به وب‌سایتی که این اطلاعات را ارائه می دهد متصل باشد)
- سایر اطلاعاتی که توسط مقامات ذیصلاح درخواست گردد.[2]

اصل ۱۲- بانک‌ها باید معیارهای مناسبی جهت ارائه محصولات و خدمات بانکداری الکترونیک بکارگیرند که اطمینان حاصل گردد الزامات حفظ اسرار مشتریان قابلیت دفاع درمحاکم قضایی را دارد.

نگهداری اطلاعات مشتری به صورت محرمانه مسئولیت کلیدی یک بانک است. سوء استفاده یا افشای غیرمجاز اطلاعات محرمانه مشتری بانک را در معرض ریسک

---

1 National compensation

2 بعنوان مثال، بانک ممکن است بخواهد کشورهایی که در آنها خدمات بانکداری الکترونیک ارائه می‌دهد و یا برعکس کشورهایی که در آنها خدمات بانکداری الکترونیک ارائه نمی دهد را مشخص کند.

شهرت و ریسک قانونی قرار می دهد. برای مواجهه با این چالشها در ارتباط نگهداری محرمانه اطلاعات مشتری، بانک‌ها باید تلاش‌های معقولی بعمل آورند تا اطمینان حاصل کنند که:

- **استانداردها و خط‌مشی‌های حفظ اسرار مشتری در بانک با همه‌ی قوانین و مقررات مربوط به حفظ اسرار مشتری، که توسط مقامات ذیصلاح در مورد ارائه‌ی خدمات و محصولات بانکداری الکترونیک تهیه شده است، مطابقت دارد.**
- **مشتریان از سیاستهای حفظ اسرار مشتری در بانک و موارد محرمانه در استفاده از خدمات و محصولات بانکداری الکترونیک آگاه می شوند**
- **مشتری می‌تواند در خصوص استفاده از اطلاعات شخصی وی از قبیل نیازها، علایق، موقعیت مالی و فعالیت‌های بانکداری الکترونیک توسط شرکت ثالث برای اهداف بازاریابی مخالفت کند.**
- **اطلاعات مشتری جز برای مواردی که به طور مشخص مجاز هستند یا مقاصدی که خود مشتری اجازه داده است، مورد استفاده واقع نمی شوند.[1]**
- **زمانیکه اشخاص ثالث(در موارد برون‌سپاری) به اطلاعات مشتری دسترسی دارند، استانداردهای بانک برای استفاده از اطلاعات مشتری رعایت می‌شود.**

پیوست شماره ۵، برخی از اقدامات مؤثری در زمینه حفظ اطلاعات مشتری در بانکداری الکترونیک را ارائه داده است.

---

[1] **در برخی کشورها، قوانین و مقررات ممکن است بانک‌ها را متعهد به کسب اجازه از مشتری برای استفاده از اطلاعات مشتری برای مقاصد داخلی نکند. یا ممکن است بانک‌ها را متعهد کنند که مشتری بتواند به بانک اجازه ندهند اطلاعات وی را در اختیار اشخاص ثالث قرار دهند. در برخی کشورهای دیگر مشتریان ممکن است حق داشته باشند به بانک اجازه ندهند از اطلاعات آنها برای مقاصد داخلی یا خارجی استفاده کند.**

اصل ۱۳- بانک‌ها باید ازظرفیت موثر و فرآیند های برنامه‌ریزی مستمر برخوردار باشند که اطمینان حاصل گردد سیستم‌ها و خدمات بانکداری الکترونیک همیشه در دسترس می‌باشند.

برای محافظت از بانک‌ها در برابر ریسک تجاری، ریسک قانونی و ریسک شهرت، خدمات بانکداری الکترونیک باید به صورت پایدار، به موقع و براساس انتظارات مشتری ارائه شود. برای دستیابی به این هدف، بانک باید توانایی داشته باشد تا خدمات بانکداری الکترونیک را از منبع اولیه(از قبیل سیستم‌ها و برنامه‌های کاربردی داخلی) یا از منبع ثانویه(از قبیل سیستم‌ها و برنامه‌های کاربردی شرکتهای ارائه دهنده خدمات الکترونیک) به استفاده کننده نهایی تحویل دهد. در دسترس بودن همیشگی خدمات بانکداری الکترونیک بستگی به توانایی سیستم‌های پشتیبانی در تداوم خدمت رسانی و مقابله با رخدادهایی که به طور بالقوه ممکن است به کسب و کار بانک لطمه بزنند، دارد.

در دسترس بودن همیشگی برنامه‌ها و سیستم‌های کاربردی چالش مهم و بالقوه‌ای در ارتباط با تقاضاهای فراوان برای انجام مبادله به ویژه در زمانهای پرتراکم به شمار می‌رود. علاوه بر این، انتظارات زیاد مشتریان برای پردازش سریع مبادلات در زمان کوتاه و در دسترس بودن همیشگی(در تمام ایام هفته به طور شبانه روزی)، اهمیت داشتن ظرفیت مناسب، تداوم ارائه‌ی خدمات و برنامه ریزی برای رخدادهای احتمالی را افزایش داده است. برای ارائه مستمر و همیشگی خدمات بانکداری الکترونیک به مشتریان، بانک باید اطمینان حاصل کند:

- **ظرفیت فعلی و آتی سیستم بانکداری الکترونیک براساس محرک‌های کلی بازار برای تجارت الکترونیک و نرخ پیش‌بینی شده جذب مشتری برای خدمات و محصولات الکترونیک مورد تجزیه و تحلیل قرار می گیرد**
- **ظرفیت پردازش مبادلات بانکداری الکترونیک برآورد شده، مورد آزمایش**

قرار گرفته و به طور دوره ای بازبینی می‌شود.

- برنامه ریزی برای تداوم مناسب ارائه‌ی خدمات و رخدادهای احتمالی برای فرآیندهای اساسی بانکداری الکترونیک و سیستم‌های پرداخت صورت گرفته و به طور منظم مورد آزمایش قرار می گیرد.

پیوست شماره۶، برخی از اقدامات مؤثر در زمینه تداوم عملیات و برنامه ریزی برای رخدادهای غیر منتظره را ارائه می‌کند.

اصل۱۴- بانک‌ها باید برنامه‌های مناسبی برای عکس العمل در مقابل رخدادهای غیرمنتظره در جهت مدیریت و حداقل کردن مشکلات ناشی از رخدادهای احتمالی، از جمله حملات داخلی و خارجی که ارائه‌ی خدمات و سیستم‌های الکترونیک را مختل می‌سازد، بکار گرفته و آنها را توسعه بخشند.

مکانیزمهای مؤثر عکس العمل در مقابل رخدادها برای به حداقل رساندن ریسک عملیاتی، قانونی و شهرت ناشی از رخدادهای غیر منتظره شامل رخدادهای داخلی و خارجی که ممکن است سیستم‌ها و خدمات بانکداری الکترونیک را تحت تأثیر قرار دهند، بسیار مهم هستند.

بانک‌ها باید برنامه‌های واکنش و عکس العمل در مقابل رخدادهای غیر منتظره را گسترش دهند و راهبرد ارتباطی خود را بهبود بخشند تا اطمینان حاصل کنند که خدمات به طور مداوم ارائه می‌شود، ریسک شهرت کنترل می گردد و تعهدات مربوط به قطع خدمات بانکداری الکترونیک(شامل خدمات خود بانک و خدماتی که از طریق منابع خارجی ارائه می‌شود) محدود می‌شود.

برای اطمینان از واکنش مناسب در مقابل رخدادهای غیرمنتظره، بانک‌ها باید موارد زیر را گسترش دهند:

- برنامه‌های واکنش و عکس العمل در مقابل رخدادهای غیرمنتظره برای

تشخیص بهبود سیستم‌ها و خدمات بانکداری الکترونیک در سناریوها، کسب و کارها و محل‌های جغرافیایی مختلف. تجزیه و تحلیل سناریوها باید شامل توجه به وقوع ریسک‌های احتمالی و اثر آنها بر بانک باشد. سیستم‌های بانکداری الکترونیک که برون‌سپاری می‌شوند باید جزء جدائی‌ناپذیر این برنامه‌ها باشند.

- مکانیزم‌هایی برای مشخص کردن یک رخداد غیرمنتظره یا بحرانی در سریعترین زمان ممکن، مشخص کردن اهمیت آن و کنترل ریسک شهرت مربوط به قطع خدمات در صورت وجود آن رخداد.
- راهبرد ارتباطی به منظور شناسایی کامل گرایش بازارها و رسانه ها که ممکن است در اثر فقدان امنیت، حمله‌های آن لاین و قطع خدمات بانکداری الکترونیک حساس شوند.
- فرآیند روشن برای آگاه کردن به موقع مقام نظارتی در هنگام رخدادهای مهم امنیتی یا قطع خدمات در اثر رخدادهای غیر منتظره.
- گروههای عکس العمل در مقابل رخدادهای غیرمنتظره با داشتن اختیار عمل در موقعیتهای اضطراری، آموزش کافی این گروه برای تجزیه و تحلیل سیستم‌های عکس العمل در مقابل رخدادهای غیرمنتظره و تفسیر نتایج بدست آمده در اثر این رخدادها.
- سلسله مراتب فرماندهی دقیق که هم عملیات درونی و هم عملیات برون سپاری شده را در بر بگیرد،برای اطمینان از این موضوع که براساس اهمیت اتفافات غیرمنتظره عکس العمل مناسب اتخاذ می‌شود. علاوه برآن، روش‌های ارتباطات داخلی باید توسعه داده شده و در مواقع لزوم به مدیریت ارشد هشدار دهند.
- فرآیندی برای اطمنیان از اینکه همه‌ی طرف‌های خارجی شامل مشتریان بانک، همکاران و رسانه ها به موقع و از طریق روش‌های مناسب از قطع

خدمات بانکداری الکترونیک، ادامه و بهبود آن مطلع می شوند.

- **فرآیندی برای جمع آوری و نگهداری مدارک مستدل بـرای تـسهیل بررسـی رخدادهای غیر منتظره‌ای که در دوره های گذشته اتفاق افتاده و نیز کمـک در تعقیب حمله کنندگان به سیستم.**

پیوست۱: اقدامات مؤثر برای حصول اطمینان از امنیت بانکداری الکترونیک

۱- بانک باید مجموعه تدابیر امنیتی بکار گیرد و محدوده دسترسی تمام کاربران سیستم‌ها و ابزارهای بانکداری الکترونیک، از جمله مشتریان، کاربران بین بانکی و تأمین‌کنندگان خدمات خارج از بانک را مشخص سازد. کنترل‌های دسترسی مجازی باید در راستای حمایت از تفکیک صحیح وظایف طراحی شوند.

۲- داده‌ها و سیستم‌های بانکداری الکترونیک باید براساس حساسیت، اهمیت و دامنه پوشش طبقه بندی شوند. مکانیزم‌های مناسب، همچون داشتن رمز، کنترل دسترسی و برنامه‌های بازیافت داده‌ها باید جهت حفاظت از تمام سیستم‌های حساس و سیستم‌های بانکداری الکترونیک پرریسک، سرورها، پایگاه های اطلاعاتی و برنامه‌های کاربردی بکار گرفته شوند.

۳- ذخیره کردن داده‌های حساس یا داده‌های با ریسک بالا در میزکار سازمان یا سیستم‌های لب تاپ باید به حداقل ممکن برسد. این داده‌ها باید از طریق رمزنگاری، کنترل دسترسی و برنامه‌های بازیافت داده ها به طور صحیحی حفاظت شوند.

۴- باید کنترل‌های فیزیکی کافی در مکان های فعالیت صورت پذیرد تا مانع دسترسی غیرمجاز افراد به سیستم‌های حساس بانکداری الکترونیک، سرورها، پایگاه‌های اطلاعاتی و برنامه‌های کاربردی گردد.

۵- باید روش‌های مناسبی جهت کاهش تهدیدهای خارجی به سیستم‌های بانکداری الکترونیک صورت پذیرد، این روش‌ها شامل موارد زیر است:

- نصب نرم افزار ویروس یاب در تمام نقاط ورودی حساس (به عنوان مثال دسترسی از راه دور به سرورها، پست‌های الکترونیک) و هر بخش از سیستم میز کار.

- **نصب نرم افزار کشف مزاحم و سایر ابزارهای سنجش امنیت که به طور متناوب شبکه ها، سرورها و غیره را بررسی می‌کنند تا نقاط ضعف و آسیب‌پذیر سیاست‌ها و کنترل‌های امنیتی مشخص شوند.**
- **آزمایش نفوذ پذیری داخلی و خارجی به شبکه ها**

۶- **فرآیند ارزیابی امنیتی قوی باید برای تمام کارکنان و تأمین کنندگان خدمات، که به نقاط حساس دسترسی دارند، بکار گرفته شود.**

پیوست۲: اقدامات مؤثر برای مدیریت سیستم‌ها و خدمات برون سپاری بانکـداری الکترونیک

۱- بانک‌هـا بایـد فرآینـدهای مناسـبی جهـت ارزیـابی تـصمیمات مربـوط بـه برون‌سپاری سیستم‌ها و خدمات بانکداری الکترونیک بکارگیرند.

- مدیریت بانک باید به طور واضح اهداف راهبردی، مزایا و هزینه های مرتبط با برون‌سپاری خدمات و سیستم‌های بانکداری الکترونیک را شناسایی کند.
- تصمیم‌گیری درخصوص برون سپاری یک بخش یا خدمات کلیدی بانکـداری الکترونیک باید با راهبرد های تجاری بانک سـازگاری داشـته و بـر نیازهـای تجاری کاملاً مشخص استوار باشد و ریسک‌هـای خـاص مـرتبط بـا بـرون سپاری را شناسایی نماید.
- تمام حوزه های تأثیرپذیر بانک باید درخصوص اینکه چطور تامین کننـدگان خدمات، راهبرد بانکداری الکترونیـک بانـک را مـورد پـشتیبانی قـرار داده و فعالیت‌های آنها با ساختار عملیاتی بانک متناسب می‌باشد، آگاهی کسب کنند.

۲- بانک‌ها باید قبل از انتخاب تأمین کننده خدمات بانکداری الکترونیـک و حتـی پس از فعالیت آنها، تجزیه و تحلیل ریسک مناسبی انجام دهند.

- بانـک‌هـا بایـد روش‌هـای پیـشرفته‌ای بـرای بررسـی پیـشنهادهای اولیـه مشارکت‌کنندگان مورد استفاده قرارداده و معیارهایی بـرای انتخـاب از میـان پیشنهادات مختلف داشته باشند.
- پس از آنکه ارائه کننده خدمات بالقوه شناسـایی شـد، بانـک بایـد بررسـی دقیق‌تر و مناسب تری از جمله تجزیه و تحلیل ریسک درخصوص توان مـالی تأمین کننده خدمات، شهرت، سیاست ها و کنتـرل‌هـای مـدیریت ریـسک و توانایی پاسخگویی کامل به تعهدات در مورد ارائه کننـده خـدمات بـه عمـل آورد.

- پس از اتخاذ تصمیم و عقد قرارداد، بانک باید به طور منظم و دقیق بر فعالیت‌های تأمین‌کننده خدمات نظارت نماید و در طول قرارداد به طور دقیق توانایی آن در ارائه‌ی خدمات به طور کامل و پاسخگویی به تعهدات را مورد ارزیابی قرار دهد.
- بانک‌ها باید اطمینان حاصل کنند که منابع کافی جهت نظارت بر روابط برون‌سپاری، که فعالیت‌های بانکداری الکترونیک را پشتیبانی می‌کند، وجود دارد.
- مسئولیت‌ها در نظارت بر روابط برون سپاری باید به طور مشخص تعیین شوند.
- بانک باید یک راهبرد بیرونی مناسب داشته باشد تا بتواند ریسک‌ها را مدیریت نموده و در صورت لزوم روابط برون سپاری را خاتمه بخشد.

۳- بانک‌ها باید راهکارهای مناسبی اتخاذ نمایند تا اطمینان حاصل گردد قراردادهای منعقده می‌توانند به طور مناسب فعالیت‌های بانکداری الکترونیک را پوشش دهند. به عنوان مثال، قراردادهای مشتمل بر برون سپاری فعالیت‌های بانکداری الکترونیک باید موارد ذیل را مشخص سازد:

- تعهدات و مسئولیت‌های مربوط به قرارداد طرف های مربوطه جهت تصمیم‌گیری، از جمله هرگونه قراردادهای فرعی مربوط به خدمات عمده باید به طور مشخص شناسایی شوند.
- مسئولیت های ارائه اطلاعات از سوی تأمین کنندگان خدمات و دریافت اطلاعات از آنها باید به طور مشخص تعریف شوند. اطلاعاتی که تأمین کنندگان خدمات ارائه می‌کنند باید به موقع و جامع باشند تا به بانک اجازه دهد به حد کافی به سطوح خدمات و ریسک‌های مرتبط با آنها دسترسی داشته باشند. اقدامات و دستورالعمل های اساسی بکارگرفته شده باید بانک‌ها را در خصوص اختلال های خدمات الکترونیک، رخنه های امنیتی و

سایر رخدادهایی که ریسک اساسی برای بانک به همراه دارد، مطلع سازند.

- تأمین شرایط برای پوشش احتیاطی، مالکیت داده های ذخیره شده در سرورها یا پایگاه های اطلاعاتی و حقوق بانک در بازیافت داده‌ها بعد از انقضاء و خاتمه قرارداد باید به طور مشخص تعریف شوند.
- انتظارات در مورد عملکرد تأمین کنندگان خدمات در هر دو شرایط عادی و احتمالی باید مشخص شود.
- ارائه کننده خدمت شرایطی فراهم کند که برای اصلاح عملکردهای غیراستاندارد، بانک بتواند به موقع مداخله نماید.
- جهت تنظیم ترتیبات برون‌سپاری خارج از کشور باید اجرای قوانین و مقررات کشور مربوطه، از جمله موارد مرتبط با حفظ اسرار مشتری محرز شود.
- حقوق بانک جهت بررسی های مستقل یا حسابرسی برنامه‌های امنیتی، کنترل‌های داخلی و برنامه‌های تجاری باید به طور دقیق مشخص شود.

۴- بانک‌ها باید اطمینان حاصل کنند که حسابرسی های مستقل داخلی و خارجی به صورت دوره ای بر فعالیت‌های عملیاتی برون سپاری صورت می پذیرد.

- برای روابط برون سپاری مرتبط با خدمات پیچیده فنی و حساس بانکداری الکترونیک، بانک‌ها ممکن است نیازمند بررسی های دوره ای از سوی طرف‌های ثالث مستقل و برخوردار از مهارت فنی کافی باشند.

۵- بانک‌ها باید برنامه‌های اقتضایی مناسبی برای فعالیت‌های برون سپاری بانکداری الکترونیک توسعه بخشتد.

- برنامه‌های اقتضایی باید دربرگیرنده بدترین سناریوها برای ارائه‌ی خدمات مستمر بانکداری الکترونیک در صورت اختلال در فعالیت‌های عملیاتی برون سپاری باشد.
- بانک‌ها باید از یک تیم مشخصی برخوردار باشند که مسئولیت ارزیابی اثرات

مالی اختلال در خدمات برون سپاری بانکداری الکترونیک را بر عهده بگیرند.

۶- بانک‌هایی که خدمات بانکداری الکترونیک را به اشخاص ثالث واگذار می‌کنند، باید اطمینان حاصل نمایند که فعالیت‌های عملیاتی، مسئولیت ها و تعهدات آنها به اندازه کافی روشن می‌باشد، بنابراین مؤسسات دریافت کننده خدمات می‌توانند به میزان کافی بررسی های دقیق و موثر و نظارت مستمری بر روابط داشته باشند.

- **بانک‌ها باید مسئولیت ارائه‌ی خدمات همراه با ارائه اطلاعات ضروری به موسسات طرف قرارداد را برعهده بگیرند تا همه‌ی ریسک‌های مرتبط با خدمات بانکداری الکترونیک شناسایی، کنترل و نظارت شوند.**

پیوست ۳: اقدامات مؤثر برای اعطای اجازه کاربری در بانکداری الکترونیک

۱- اجازه کاربری و حق دسترسی باید به همه‌ی افراد، کارگزاران و سیستم‌هایی که با فعالیت‌های بانکداری الکترونیک مرتبط هستند، اعطا شود

۲- همه‌ی سیستم‌های بانکداری الکترونیک باید به گونه ای بنیانگذاری شوند که اطمینان حاصل شود که با یک پایگاه داده معتبر اجازه کاری در ارتباط هستند.

۳- هیچ فرد، کارگزار یا سیستمی نباید حق تغییر اجازه کاربری یا سطح دسترسی خود را داشته باشد یا به پایگاه داده اجازه کاربری دسترسی داشته باشد.

۴- ورود افراد، کارگزارن و سیستم‌های جدید یا تغییر سطح دسترسی و اجازه کاربری در یک پایگاه داده باید توسط منبع معتبری صورت گیرد که دارای اختیار کافی است و به طور مرتب و به موقع تحت بازرسی و حسابرسی قرار می گیرد.

۵- به منظور مقاوم سازی پایگاه داده مربوط به اجازه کاربری در مقابل نفوذ، باید معیارهای مناسبی در نظر گرفته شود. هر گونه نفوذ در پایگاه داده باید در فرآیند بازبینی مداوم کشف شود. باید برای مستندسازی این نفوذها، حسابرسی کافی وجود داشته باشد.

۶- هر پایگاه داده مربوط به اجازه کاربری که به آن نفوذ صورت گرفته است تا زمانی که پایگاه داده معتبر جایگزین آن نشود، نباید مورد استفاده قرار گیرد.

۷- برای جلوگیری از تغییر اجازه کاربری در جریان پردازش مبادلات بانکداری الکترونیک باید کنترل کافی وجود داشته باشد و هرگونه تلاش برای تغییر اجازه کاربری مشخص شده و به مدیریت گزارش شود.

پیوست ۴: اقدامات مؤثر در زمینه حسابرسی آتی در سیستم‌های بانکداری الکترونیک

۱- همه‌ی مبادلات بانکداری الکترونیک باید ثبت و نگهداری شوند تا زمینه برای حسابرسی های آتی و حل اختلافات فراهم شود

۲- سیستم‌های بانکداری الکترونیک باید به گونه ای طراحی و نصب شوند که بتوان مدارک و مستندات را استخراج و نگهداری کرد، آنها را کنترل نمود و از نفوذ و جمع آوری شواهد نادرست جلوگیری کرد

۳- در مواردی که سیستم‌های پردازش و حسابرسی های آتی به عهده شخص ثالثی گذاشته شده است:

- بانک باید اطمنیان حاصل کند که به مدارک حسابرسی های آتی که توسط اشخاص ثالث نگهداری می‌شود، دسترسی دارد.
- حسابرسی‌های انجام شده توسط اشخاص ثالث با استانداردهای بانک مطابقت دارد.

پیوست ۵: اقدامات مؤثر برای محرمانه نگه داشتن اطلاعات مشتری در بانکـداری الکترونیک

۱- بانک‌ها باید برای اطمینان از رازدای اطلاعات مشتری از تکنیک‌های کدگـذاری، پروتکل‌های خاص و سایر کنترل‌های امنیتی استفاده کنند.

۲- بانک‌ها باید به منظور تشخیص دوره‌ای زیرساخت‌هـا و پروتکـل‌هـای امنیتـی مشتری، کنترل‌ها و روش‌های مناسب را گسترش دهند.

۳- بانک‌ها باید اطمنیان حاصل کنند که روش‌های رازداری و حفظ اسرار اشـخاص ثالث طرف قرارداد با روش‌های بانک مطابقت دارند.

۴- بانک‌ها باید گامهای مؤثری برای آگاه سازی مشتری از رازداری و حفـظ اسـرار خود بردارند. این گامها می‌تواند شامل موارد زیر باشند:

- آگاه سازی مشتری از روش‌های حفـظ اسـرار از طریـق وب سـایت بانـک. بدیهی است استفاده از زبان واضح و مختصر برای اطمینان از اینکه مـشتری کاملاً روش‌های حفظ اسرار بانک را درک کرده، بسیار اساسی است. تفاسـیر حقوقی طولانی، هر چند دقیقتر هستند ولی احتمالاً بسیاری از مشتریان آنها را مطالعه نمی‌کنند.
- راهنمایی مشتریان برای حفظ رمز عبور و شماره تعیین هویت شخصی(PIN) و سایر اطلاعات بانکی و یا شخصی.
- ارائه اطلاعات مربوط به امنیت عمومی کامپیوترهای شخـصی بـه مـشتریان، شامل مزایای استفاده از برنامه‌هـای ضـد ویـروس، کنتـرل دسترسـی‌هـای فیزیکی و استفاده از سیستم‌های امنیتی شخصی برای دسترسی به اینترنت.

پیوست ۶: اقدامات مؤثر برای تداوم عملیات و برنامه ریزی رخدادهای غیرمنتظره

۱- همه‌ی خدمات و برنامه‌های کاربردی، شامل آنهایی که توسط اشخاص ثالث ارائه می شوند باید با شرایط بحرانی تطبیق داده شوند.

۲- ریسک برنامه‌های کاربردی و خدمات اصلی بانکداری الکترونیک اساسی شامل موارد بالقوه توقف ارائه‌ی خدمات، ریسک‌های اعتبار، بازار، نقدینگی، قانونی و شهرت مورد ارزیابی قرار گیرد.

۳- ضوابط عملیاتی برای همه‌ی برنامه‌های کاربردی و خدمات اصلی بانکداری الکترونیک و سطح خدماتی که برای رعایت این ضوابط باید رعایت شود، مشخص شود. برای اطمنیان از اینکه سیستم‌های بانکداری الکترونیک می‌توانند مبادلات با حجم پایین و بالا را پردازش کنند و ظرفیت بانک با رشد آتی بانکداری الکترونیک متناسب است، باید ارزیابی های مناسبی صورت گیرد.

۴- زمانی که سیستم‌های بانکداری الکترونیک به مرحله خاصی از ظرفیت رسیدند، باید فرآیندهای جایگزین برای مدیریت تقاضا مورد توجه قرار گیرد.

۵- برنامه‌های تداوم عملیات باید براساس میزان اعتماد به اشخاص ثالث ارائه دهنده خدمات و دسترسی به سایر منابع خارجی وابسته، تنظیم شوند.

۶- برنامه‌ریزی رخدادهای غیرمنتظره در بانکداری الکترونیک باید شامل مجموعه‌ای از فرآیندها برای بازیابی یا جایگزینی ظرفیت های پردازش بانکداری الکترونیک واطلاعات تجدید ساختار پشتیبانی مبادلات باشد. همچنین این برنامه‌ریزی‌ها باید شامل ارزیابی از میزان در دسترس بودن برنامه‌های کاربردی و خدمات اساسی بانکداری الکترونیک در شرایط توقف عملیات باشد.