اصول مدیریت ریسک برای بانکداری الکترونیکی

میثم حجازی نیا، 8331701

چکیده

ادامه ی نو آوری در تکنولوژی و رقابت در بین سازمان های بانکداری موجود و داوطلبان جدید، اجازه ارائه آرایه گسترده تری از محصولات بانکی و سرویس ها جهت دسترسی و تحویل به مشتریان خرده فروش و عمده فروش توسط یک کانال گسترده الکترونیکی که مجموعا به یک سیستم بانکداری الکترونیکی اطلاق می شود، را داده است. بهر حال، توسعه سریع قابلیت های بانکداری الکترونیکی ریسک هایی را نیز مانند عوایدی که رائه می نماید، در برخواهد داشت. کمیته باسل که بر روی نظارت بر بانکداری فعالیت می نماید انتظار دارد این ریسک ها تشخیص داده شده، عنوان گشته و توسط نهاد های بانکداری با احتیاط و بر اساس خصوصیات اساسی و سرویس های چالش بانکداری الکترونیکی مدیریت گردند. این خصوصیات سرعت بی سابقه تغییرات مربوط به نو آوری های سرویس مشتری و تکنولوژیکی را در بر می گیرد. این موارد شامل طبیعت عمومی و همه جا حاضر شبکه الکترونیکی باز، یکپارچه سازی سیستم های بانکداری الکترونیکی با سیستم های کامپیوتری موروثی و وابستگی فزاینده بانک ها به شخص ثالثی که اطلاعات تکنولوژی ضروری را تامین می نماید، می شود. تا وقتی که ما ریسک های جدید موروثی را خلق نمی کنیم، کمیته اعلام می نماید که این خصوصیات افزوده شده و برخی از ریسک های سنتی ملحقه به فعالیت های بانکداری، در استراتژی خاص، عملیاتی، ریسک های مشهور و مجاز تغییر می یابند، در نتیجه تاثیر بر پروفایل ریسک بانکی می گذارند.
بر اساس این نتایج، کمیته به این تفکر رسیده که با توجه به آنکه اصول مدیریت ریسک قابل اعمال بر فعالیت های بانکداری الکترونیکی هستند، این اصول بایستی برای بانکداری الکترونیکی تکدوزی،تعدیل و در برخی مواردی برای عنوان ساختن برخی چالش های مدیریت ریسک که با خواص فعالیت های بانکداری الکترونیکی ایجاد شده توسعه یابند.
برای این هدف، کمیته اعتقاد دارد که ناگذیر بر اساس هیئت مدیره آن و مدیریت ارشد بانک قدم هایی را برای تضمین آنچه نهاد ها آن دارد را مورد بازنگری قرار داده تغییر دهد و سیاست های مدیریت ریسک و فرآیندهایی را برای پوشاندن فعالیت

برنامه ریزی شده بانکداری الکترونیکی تغییر دهد. این کمیته همچنین بر این اعتقاد است که ادغام برنامه های کاربردی بانکداری الکترونیکی با سیستم های موروثی راه حل مدیریت ریسک یکپارچه ای را برای تمام فعالیت های بانکداری الکترونیکی نهاد ها ایجاد می نماید.
برای مجهز سازی این توسعه های، این کمیته چهارده اصل مدیریت ریسک را برای بانکداری الکترونیکی جهت کمک به نهاد ها به جهت بهبود اشتباه نظری کنونی ریسک آنها و پردازش آن برای پوشاندن فعالیت ها بانکداری الکترونیکی آنها مشخص نماید.

1-مقدمه

سازمان های بانکداری سالهاست که سرویس های الکترونیکی را به مصرف کنندگان و کسب و کارها بصورت متحرک ارائه می کنند. انتقال الکترونیکی سرمایه های، شامل پرداخت های کوچک و سیستم های مدیریت خزانه سازمان، همچنین ماشین های اتوات شده در دسترس عموم برای کنار گذاری ارز و مدیریت حساب های خرده فروشی، که اثاث ثابت جهانی است، می باشد. هر چند افزایش مقبولیت متداول در اینترنت جهانی، به عنوان کانال توزیعی برای محصولات بانکداری و سرویس ها، فرصت های کسب و کار نو ای را برای بانک ها مانند سود سرویس ها برای مشتریان آنها فراهم می آورد. ادامه نو آوری تکنولوژیکی و رقابت بین سازمان های بانک داری موجود و ورود کسب و کارهای جدید اجازه سری وسیعی از بانکداری الکترونیکی محصولات و سرویس هایی برای مشتریان بانکداری خرده فروشی و عمده فروشی، فراهم ساخته است. این موارد شامل فعالیت های سنتی مانند دسترسی اطلاعات مالی، کسب وام ها و باز کردن حساب های سپرده همانند محصولات جدید و سرویس هایی مانند سرویس های پرداخت صورتحساب الکترونیکی، پورتال های شخصی شده مالی، تجمیع حساب ها و بازارهای تجاری-تجاری و مبادلات است. با وجود عواید مهم نو آوری تکنولوژی توسعه سریع توانمندی های بانکداری الکترونیکی ریسک هایی را همانند عوایدش بهمراه آورده و اینکه ریسک ها تشخیص داده شوند و توسط نهادهای بانکداری بروش محتاطانه ای مدیریت شوند، از اهمیت بسزایی برخوردار است.
این توسعه کمیته باسل را به سمت نظارت به جهت انجام مطالعاتی بر پیاده سازی مدیریت ریسک در بانکداری الکترونیکی و پول

الکترونیکی در سال 1998 هدایت کرد. این مطالعات اولیه نیاز واضحی برای کار بر روی ناحیه مدیریت ریسک بانکداری الکترونیکی را به نمایش گذارد، و گروه شامل سرپرستان بانک ها و بانک های مرکزی، گروه بانکداری الکترونیک،که در نوامبر 1999 تشکیل شد، این ماموریت را عهده دار شدند.

1. برای هدف این گزارش اینترنت دارای تمام تکنولوژی های تواناساز وب و شبکه های ارتباط تلفنی باز در محدوده ارتباط شماره گیری مستقیم، وب وسیع عمومی، و شبکه های خصوصی مجازی تعریف شده است.

2- برای هدف این گزارش، بانکداری الکترونیک، یا ایبانکینگ، شامل قید خرده فروشی و محصولات بانکداری کم ارزش و سرویس های از طریق کانال های الکترونیکی به بزرگی ارزش پرداخت الکترونیکی و سرویس های بانکداری الکترونیکی که بصورت الکترونیکی تحویل شده، می باشد.

3- سرویس تجمیع حساب به مشتری اجازه می دهد که اطلاعات یکپارچه ای را در مورد حساب های مالی و غیر مالی در یک جا داشته باشد. یک تجمیع کننده اصولا به عنوان عاملی برای مشتریان جهت تامین اطلاعات یکپارچه در حساب مشتری در مقابل خیل نهادهای مالی است. مشتریان کلمه عبور یا شماره شناسه شخصی خود را برای دسترسی و تحکیم اطلاعات حساب ها عمدتا از طریق صفحات تکه شده به تجمیع کننده ها می دهند، فرایندی که در گیر جمع آوری داده ها از بقیه وب سایت های نهادهاست، اغلب بدون دانش آنها، یا از طریق داده های مستقیم مرتب شده توسط قرارداد بین موسسات مالی بدان تزریق شده است.

4- بدلیل تغییرات سریع در تکنولوژی اطلاعات، هیچ توصیفی از این نوع ریسک ها نمی تواند جامع باشد. هرچند، ریسک هایی که با بانک روبرو می شوند در بانکداری الکترونیکی بکار گرفته می شوند و بطور کلی نو نیستند و شامل گروه های ریسک مشخص شده در اصول پایه ای برای نظارت اثر بخش بانکداری کمیته باسل است. سپتامبر 1997. این راهنما پنج محدوده ریسک که شامل محدوده ریسک اعتبار، ریسک انتقال و کشور، ریسک بازار، ریسک نرخ بهره، ریسک

شناوری، ریسک عملیاتی، ریسک معتبر و ریسک مجاز است، را مشخص می کند. اصول پایه ای در وب سایت BIS در http://www.bis.org موجود است.

5- مدیریت ریسک برای بانکداری الکترونیک و فعالیت های پول الکترونیک، مارچ 1998، در وب سایت بانکداری پرداخت های بین المللی در http://www.bis.org موجود است.

کمیته باسل گزارش گروه کسب و کار الکترونیک را در مدیریت ریسک و نظارت بر موضوع هایی که بواسطه توسعه بانکداری الکترونیکی ایجاد شده است را در اکتبر 2000 منتشر ساخته است. این گزارش ریسک های اساسی ملحق به بانکداری الکترونیک، عمدتا ریسک های استراتژیک، ریسک های معتبر، ریسک های عملیاتی (شامل ریسک های مجاز و امنیت)، و ریسک های، اعتبار، شناوری، و بازار را مطرح ساخته و ارزیابی می نماید. گروه کسب و کار الکترونیک نتیجه می گیرد که فعالیت های بانکداری الکترونیکی ریسک هایی که در کارهای قبلی کمیته باسل مشخص نشده اند را ایجاد نمی نماید. هر چند، آن همچنین بیان می کند که بانکداری الکترونیک، برخی از این ریسک های سنتی را تغییر داده و برخی را افزایش می دهد، بنابراین بر روی پروفایل کلی ریسک بانکداری تاثیر گذار است. بطور مشخص، ریسک استراتژیک، ریسک عملیاتی، و ریسک های معتبر مطمئنا با معرفی سریع و پیچیدگی تکنولوژی در زیر قرار گرفته فعالیت های بانکداری الکترونیکی افزایش می یابند.

الف. چالش مدیریت ریسک

گروه کسب و کار الکترونیک خصوصیات اساسی بانکداری الکترونیک (و بطور عموم تر تجارت الکترونیک) را برجسته می نماید و تعادی از چالش های مدیریت ریسک را بصورت زیر مطرح می نماید:

- سرعت تغییرات وابسته به تکنولوژی و نو آوری های سرویس مشتری در بانکداری الکترونیک بی سابقه است. بصورت تاریخی، برنامه های کاربردی بانکداری جدید در تناوب های طولانی از زمان و تنها بعد از تست عمقی شدید انجام می گرفته است. هرچند، امروزه بانک ها فشار رقابتی برای جمع آوری برنامه های کاربردی کسب و کار جدید را در فریم های زمانی بسیار فشرده، تجربه می کنند. که اغلب تنها چند ماه

از مفهوم تا تولید است. این رقابت، چالش های مدیریتی جهت تضمین ارزیابی استراتژیک کافی، تحلیل ریسک و نظارت امنیتی بر اساس پیاده سازی برنامه های کاربردی جدید بانکداری الکترونیک، را تشدید می کند.

- وب سایت های تراکنش های بانکداری الکترونیکی و وابسته به خرده فروشی و برنامه های کاربردی کسب و کار عمده فروشی که بطور معمول تا حد ممکن با سیستم های کامپیوتری موروثی یکپارچه هستند که اجازه پردازش تراکنش های الکترونیکی بصورت سرراست را می دهند. این پردازش سرراست اتوماتیک فرصت ها را برای اشتباهات انسانی و تقلب که در پردازش های دستی انجام می گیرد، کاهش می دهد، اما این مورد همچنین وابستگی به طراحی سیستم و معماری آنرا همانند مقیاس پذیری سیستم هماهنگی بین قسمت ها و عملیات ها را افزایش می دهد.
- بانکداری الکترونیکی وابستگی بانکها به فناوری اطلاعات را افزایش میدهد، بنابراین افزایش پیچیدگی تکنیکالی موضوع امنیت و جلوبردن روند مشارکت بیشتر، پیوستگی و برون کار سازی مقدمات با شخص ثالث، که اکثر آنها نا منظم است را منجر می شود. این توسعه منجر به خلق مدل های کسب و کار جدید که درگیر موجودیت های بانکی و نابانکی، مانند تامین کنندگن سرویس اینترنت، شرکت های ارتباطات و بقیه شرکت های فناوری می گردد.
- اینترنت در همه جا حاضر و طبعا سراسری است. در اصل شبکه قابل دسترسی باز از هرجا در جهان توسط اشخاص مجهول است، این کار با مسیر یابی پیام ها از موقعیت های نامعلوم و از طریق ابزار بدون سیم باسرعت انجام می گیرد. بنابراین، بطور قابل ملاحظه ای اهمیت کنترل های حفاظتی، تکنیک های تصدیق مشتری، حفاظت داده، شیوه های رد ممیزی و استانداردهای حریم مشتری را تقویت می کند.

ب. اصول مدیریت ریسک

بر اساس کارهای اولیه گروه کسب و کار الکترونیک، کمیته ای که شامل آن است، تاوقتی که اصول مدیریت ریسک بانکداری سنتی بر فعالیت های بانکداری الکترونیکی قابل اعمال است، مشخصات پیچیده کانال توزیع اینترنتی که این اصول قابل اعمال است، بایستی با آنها متناسب شود و نسبت به فعالیت های بانکداری آنلاین و چالش های وابسته به مدیریت ریسک تکدوزی گردد.

برای همین منظور، کمیته بر این باور است که ناگزیر بر اساس اعضای هیئت مدیره و مدیریت ارشد بانک ها برای برداشتن قدم هایی جهت تضمین اینکه هرجا لازم است، سیاست های مدیریت ریسک و فرآیند هایی برای پوشاندن فعالیت های بانکداری الکترونیکی برنامه ریزی شده یا موجود، نهادهایشان بازدید شده و تغییر یافتند، است. ثانیا، همانطور که کمیته باور دارد بانک ها بایستی روش مدیریت ریسک یکپارچه را برای تمام فعالیت های بانکیشان تعدیل کنند، همچنین نظارت بر مدیریت ریسکی که موجب می شود فعالیت های بانکداری الکترونیکی به عنوان قسمت کاملی از چهارچوب مدیریت ریسک ناظر بر نهادهای بانکداری الکترونیکی گردند، بحرانی است.

برای آسان ساختن این توسعه، کمیته از گروه کسب و کار الکترونیک می خواهد که اصول کلیدی مدیریتی را که نهادها را برای توسعه سیاست های نظارتی ریسک های موجود و پردازش جهت پوشاندن فعالیت های بانکداری الکترونیکی آنها و، در ادامه، بهبود توزیع الکترونیک امن از محصولات بانکداری و سرویس ها را انجام دهد، را مشخص کند.

این اصول مدیریت ریسک برای بانکداری الکترونیک، که در این گزارش مشخص شده است، به عنوان نیازمندی های مطلق و حتی «بهترین روش» مطرح نمی شوند اما بشکل رهنمودی برای بهبود فعالیت های صحیح و تندرست بانکداری الکترونیکی است. کمیته معتقد است که مشخص کردن جزئیات نیازمندی های مدیریت ریسک در ناحیه بانکداری الکترونیک، تنها بخاطر اینکه می تواند بسیار سریع نا بروز گردد، با تغییرات مربوط به تکنولوژی و نو آوری محصولی، می تواند مضر باشد. بنابراین این اصول شامل توقعات

مباشرانه مربوط به اهداف کلی نظارت بانکداری برای تضمین امنیت و صحت در سیستم های مالی نسبت به مقررات دقیق است.
این کمیته اعتقاد دارد که این توقعات مباشرانه بایستی بر اساس کانال های توزیع بانکداری الکترونیکی تعدیل شده و تکدوزی شده اما بطور اصولی متفاوت با آنچه بر روی فعالیت های بانکداری از طریق بقیه کانال های توزیع ، ارائه می شود، گردد. در نتیجه، اصولی که در ذیل ارائه شده اند بطور وسیعی از اصول نظارتی که توسط کمیته یا ناظران بین المللی در سالهای متمادی بیان شده، مشتق و تعدیل گردیده است. در برخی نواحی، مانند مدیریت ارتباطات برون کار، کنترل امنیت و مدیریت ریسک معتبر و مجاز، خصوصیات و پیاده سازی کانال توزیع اینترنت نیازی را برای اصول جزئی نسبت به مواردی که نسبت به روز اظهار شده اند، معرفی کرده اند. کمیته تشخیص می دهد که بانک ها نیاز به توسعه فرآیندهای مدیریت ریسک مناسب برای پروفایل ریسک شخصی، ساختار عملیاتی و فرهنگ نظارت سازمانی، همانند متابعت با نیازمندی های مدیریت ریسک خاص و سیاست هایی برای بیان ناظران بانک در صلاحیت های خاص دارند. مضاف اینکه، تعداد زیادی از روش های مدیریت ریسک بانکداری الکترویینک در این گزارش، در حالی که نماینده عملی مناسب صنعت حاضر اند، نبایستی در برگیرنده تمام یا قطعی، تاوقتی که تعداد زیادی از کنترل های امنیتی و بقیه تکنیک های مدیریت ریسک درگیر سرعت برنامه های کاربردی تجاری و تکنولوژی های جدید اند، مطرح شوند. این گزارش تلاش نمی کند که راه حل تکنیکال خاصی را برای بیان ریسک های خاص یا نصب استاندارهای خاص مربوط به بانکداری الکترونیکی دیکته نماید. موضوع تکنیکال بر اساس اصول در حال انجام هر دوی نهادهای بانکداری و بدنه های استانداردهای متنوع همانند تکنولوژی دخیل، لازم است. مضاف، همانطور که صنعتی عنوان ساختن موضوعات تکنیکال بانکداری الکترونیکی را ادامه می دهد، که شامل چالش های امنیتی، نوآوری های متنوع و راه حل های مدیریت ریسک کارایی که محتمل است پدیدار می گردد. این راه حل ها همچنین محتمل است که موضوعات مربوط به قانونی که از بانکی به بانک

دیگر متفاوت، فرهنگ مدیریت ریسک و پیچیدگی که در حوزه خاصی نسبت به چهارچوب نتظیمی و مجاز متفاوت است، بیان کند.
بهمین دلیل، کمیته اعتقاد به روش «یک سایز اندازه همه است» در مدیریت ریسک بانکداری ندارد، و بلکه بهروش ها و استانداردهایی را برای بیان ابعاد ریسک هایی مطرح شده باکانال توزیع بانکداری الکترونیکی تقویت می کند. مطابق با این فلسفه مباشرانه، انتظار می رود، اصول مدیریت ریسک و روش های مناسب مشخص شده در این گزارش به عنوان وسیله ای برای نظارت بین المللی و پیاده سازی تعدیل برای منعکس ساختن نیازمندی های بین المللی خاص هرجا لازم است، استفاده شود. و با این کار کمکی برای فعالیت ها و عملیات بانکداری الکترونیکی مناسب و امن بنماید. کمیته تشخیص داده که هر پروفایل ریسک بانک متفاوت است و نیازمند این است که روش کاهش ریسکی مناسب با هر سایز از عملیات بانکداری الکترونیکی،نمایش مادیت ریسک ها، و رضایت و توانایی نهادها برای مدیریت این ریسک ها است. این تفاوت ها دلالت بر این دارند که اصول مدیریت ریسکی که در این گزارش بیان شده اند به اندازه کافی برای پیاده سازی در تمام حوزه هایی مربوط به بنگاه انعطاف پذیر هستند. ناظران بین المللی مادیت ریسک های مربوط به فعالیت های بانکداری الکترونیکی که در بانک داده شده، بیان شده اند، و اینکه تا چه حدی، اصول مدیریت ریسک برای بانکداری الکترونیک بنحو کافی مطابق چهارچوب مدیریت ریسک است، را ارزیابی می کنند.

2. اصول مدیریت ریسک برای بانکداری الکترونیکی

اصول مدیریت ریسک بانکداری الکترونیکی که در این گزارش مشخص شده اند به سه پهنه تعلق دارند، و اغلب با اقلام برآمد همپوشانی دارند. هر چند، این اصول بر اساس نظم برتری و اهمیت وزن دهی نشده اند. و این تنها به این دلیل است که در زمان های مختلف ممکن است تغییر یابند، ترجیح داده می شود که بی طرف باقی بمانیم و آنها را رتبه بندی ننماییم.

الف. اشتباهات سهوی اعضای هیئت مدیره و مدیریت (اصول 1 تا 3)

1. اشتباهات سهوی مدیریت کارا در فعالیت های بانکداری الکترونیکی.
2. برپایی فرآیند کنترل امنیت جامع.
3. کوشش پیوسته جامع و فرآیند اشتباهات سهوی مدیریت برای ارتباطات برون کاوی و ارتباطات شخص ثالث دیگر.

ب. کنترلهای امنیتی (اصول 4 تا 10)

4. تصدیق مشتریان بانکداری الکترونیکی.
5. غیر قابل فسخ و جوابگویی برای تراکنش های بانکداری الکترونیکی.
6. اندازه گیری های مناسب برای تضمین جداسازی وظایف.
7. کنترل اختیارات مناسب با سیستم های بانکداری الکترونیکی، پایگاه های داده و برنامه های کاربردی.
8. یکپارچگی داده ها برای تراکنش های بانکداری الکترونیکی، رکوردها و اطلاعات.
9. برپایی پیگیری ردیابی صریح برای تراکنش های بانکداری الکترونیکی.
10. محرمانگی اطلاعات کلیدی بانک.

ج. مدیریت ریسک مجاز و معتبر (اصول 11 تا 14)

11. افشاسازی مناسب برای سرویس های بانکداری الکترونیکی.
12. پوشیدگی اطلاعات مشتریان.
13. دوام کسب و کار ، ظرفیت و برنامه ریزی احتمالی برای تضمین دسترسی به سیستم هاو سرویس های بانکداری.
14. برنامه ریزی پاسخ حادث.

هر کدام از موضوعات فوق با جزئیات بیشتر ، همانطور که آنها به بانکداری الکترونیکی مربوط است و اصول مدیریت ریسک اساسی که بایستی توسط بانک ها برای بیان این موضوع مطرح شود، در بخش زیر مورد بررسی قرار می گیرند. هر جا لازم است، روش های مناسب که به عنوان راه های کارایی برای بیان این ریسک ها مورد ملاحظه قرار گیرند، در ضمیمه بیان شده اند.

الف. اشتباهات سهوی اعضای هیئت مدیره و مدیریت (اصول 1 تا 3)

هیئت مدیره و مدیرت ارشد مسئول توسعه استراتژی کسب و کار نهادهای بانکداری است. یک تصمیم استراتژیک صریح بایستی این باشد که آیا هیئت می خواهد بانک سرویس های تراکنش بانکداری الکترونیک را قبل از شورع پیشنهاد این سرویس ها، تامین کند یا خیر. بطور خاص، هیئت بایستی تضمین کند که برنامه ریزی های بانکداری الکترونیکی بوضوح با اهداف استراتژیک سازمان یکپارچه است، یک تحلیل ریسک بر روی فعالیت پیشنهادی بانکداری الکترونیکی اعمال می شود، برای مشخص کردن ریسک ها، کاهش ریسک های مناسب و فرآیندهای مانیتورینگ برپا می شود، و مرور مداومی برای هدایت ارزیابی نتایج بانکداری الکترونیکی در مقابل برنامه های بانکداری کسب و کار نهادها و اهداف آنها انجام می گیرد. مضاف، هیئت مدیره و مدیریت ارشد بایستی این را که ابعاد ریسک های عملیاتی و امنیتی استراتژی های کسب و کار بانکداری الکترونیکی نهادها به نحو مناسبی مطرح شده و بیان گشته اند، را تضمین کنند. شرط یک سرویس مالی بر اینترنت می تواند تغییر بنحو مناسب و/ یا حتی افزایش ریسک بانکداری سنتی باشد (برای مثال. ریسک استراتژیک، معتبر، عملیاتی، اعتبار و شناوری). بنابراین قدم ها بایستی برای تضمین اینکه فرآیند مدیریت ریسک موجود بانک، فرآیند کنترل امنیت، بر اساس تلاش و فرآیندهای اشتباهات سهوی برای ارتباطات برون کاری بنحو مناسبی ارزیابی شده و برای تطبیق سرویس های بانکداری الکترونیکی تعدیل می شود.

اصل اول: هیئت مدیره و مدیریت ارشد بایستی در اشتباهات سهوی مدیریتی کارایی را، برای ریسک هایی که با فعالیت های بانکداری الکترونیکی ملحق است ارائه دهد، که شامل تشکیل مسئولیت خاص، سیاست ها و کنترلهایی برای مدیریت این ریسک هاست.

اشتباهات سهوی مدیریت هوشیار برای امداد کنترل داخلی کارا در فعالیتهای بانکداری الکترونیکی ضروری است. مضاف بر مشخصات خاص برای کانال توزیع اینترنت که در مقدمه بحث شد، جنبه های زیر

بانکداری الکترونیکی ممکن است چالش های مهمی را برای فرآیند مدیریت ریسک سنتی مطرح سازد:

- عناصر اصلی از کانال توزیع (اینترنت و تکنولوژی های وابسته) خارج از کنترل مستقیم بانک هاست.
- اینترنت تحویل سرویس هایی در مقابل چندین حوزه ملی را آسان می نماید، که شامل آنهایی است که تا کنون با نهادها از طریق مکان فیزیکی آنها سرو نشده است.
- پیچیدگی این موضوع که تابع بانکداری الکترونیکی که درگیر زبان تکنیکال و مفهوم ها در بسیاری از حالات خارج از تجربه سنتی هیئت مدیره و مدیریت ارشد است.

در پرتو مشخصات یکتای بانکداری الکترونیکی، پروژه های بانکداری الکترونیکی جدید که می تواند تاثیر مهمی بر پروفایل ریسک بانک ها و استراتژی هایی که بایستی توسط هیئت مدیره و مدیریت ارشد مرور شده و تحت تحلیل استراتژیک و هزینه/پاداش قرار گیرند. بدون مرور صادقانه و مناسب استراتژی و ارزیابی کارایی مداوم برای برنامه ریزی ، بانک ها در ریسک، تخمین کم زدن هزینه و/ یا تخمین زیاد زدن میزان باز پرداخت در پیشقدمی بانکداری الکترونیک می افتند. مضافا، هیئت و مدیریت ارشد بایستی این را که بانک ها به کسب و کار بانکداری الکترونیکی جدیدی وارد نمی شوند یا تکنولوژی های جدید را تعدیل می کنند مگر اینکه خبرگی لازم را برای تامین اشتباهات سهوی مدیریت ریسک با صلاحیت داشته باشند، تضمین کنند. مدیریت و کارمندان خبره بایستی متناسب با ماهیت تکنیکال و پیچیدگی بانکداری الکترونیکی برنامه کاربردی بانک ها و تکنولوژی در زیر قرار داده شده، باشد. تخصص کافی صرفنظر از اینکه آیا سیستم های بانکداری الکترونیکی بانک ها و سرویس ها در داخل مدیرت می شوند یا به شخص ثالثی برون کار می شوند، ضروری است.فرآیند اشتباهات نحوی مدیریت ارشد بایستی بر اساس مداخله کارا و تصحیح مشکلات هر ماده سیستم های بانکداری الکترونیکی یا رخنه های امنیتی که ممکن است اتفاق بیفتد، عمل کند. افزایش ریسک های معتبر ملحق به

بانکداری الکترونیکی ناگزیر به مانیتورینگ هوشیار عملیاتی سیستم ها و رضایت مشتری را مانند گزارش دهی حادث به هیئت مدیره و مدیریت ارشد می سازد.

در نهایت نیز، مدیریت ارشد بایستی تضمین کند که روند مدیریت ریسک برای فعالیت های بانکداری الکترونیکی در روش کلی مدیریت ریسک بانک گنجانده شده است. سیاست های مدیریت ریسک کنونی و فرآیندهای مربوط بدان بایستی برای تضمین داشتن مقاومت کافی برای پوشاندن ریسک های مطرح شده توسط فعالیت های بانکداری الکترونیکی کنونی و طرح ریزی شده، آزموده شود.

قدم های مدیریت ریسک سهوی دیگری که هیئت مدیره و مدیریت ارشد بایستی مد نظر قرار دهند عبارتند از:

- گرایش های ریسک سازمان بانکداری که با بانکداری الکترونیکی ارتباط دارند بنحو مناسبی تدوین گردد.
- باید مکانیزم های گزارش دهی و نمایندگان کلیدی آنها ایجاد شود. این مکانیزم ها بایستی شامل روند های تعدیل کننده مواردی از قبیل رویدادهایی که امنیت بانکداری را تحت تاثیر قرار می دهند، باشد. (برای مثال نفوذ به شبکه، تخلف امنیتی کارمندان و هر سوء استفاده از ابزار کامپیوتری در این حیطه قرار می گیرند)
- بایستی فاکتورهای ریسکی که امنیت، یکپارچگی و در دسترس بودن محصولات و سرویس های بانکداری الکترونیکی را تضمین می کند، مشخص شود. در ضمن این فاکتور ها بایستی توسط شخص ثالث و آنفردی که بانک سیستم یا برنامه کاربردی اش را به او برون سپاری کرده، نیز اندازه گیری شود.
- بایستی تضمین شود که تحلیل ریسک مناسبی و تلاش مضاعفی در این ضمینه پیش از آنکه فعالیت های بانکداری الکترونیکی فراتری انجام گیرد، اعمال شده است. اینترنت بانک ها را قادر ساخته که محصولات و سرویس های خود را در محدوده جغرافیایی واقعی نامحدودی توزیع کنند، این مرز ها و محدوده ها شامل در مقابل مرز های ملی قرار می گیرند. این فعالیت های بانکداری الکترونیک فرا مرزی،

مخصوصا در صورتی که بدون لایسنس ارائه فیزیکی در «کشور میزبان» ارائه گردد، بطور پتانسیل ریسک های مقررات، و قانون کشوری را بدلیل تفاوت هایی که ممکن است بین محدوده های حکومتی با توجه به لایسنس بانک، نظارت و نیازمندی های حفاظت مشتری وجود دارد، افزایش می دهد.بدلیل نیاز به جلوگیری از این خطا های سهوی عدم موفقیت در مقرارات یا قانون کشور، همانند مدیریت فاکتورهای ریسک مربوط به کشور، بانک ها بدین نتیجه رسیده اند که فعالیت های بانکداری الکترونیکی فرا مرزی نیازمند این است که بطور کامل این ریسک ها را پیش از آنکه عملیاتی از این قبیل را بپذیرند کشف کنند و سعی کنند آنها را به نحو کارایی مدیریت نمایند. بسته به دامنه و پیچیدگی فعالیت های بانک داری الکترونیکی، دامنه و ساختار برنامه های مدیریت ریسک بین سازمان های بانکداری تغییر می کند. منابعی که برای سرپرستی سرویس های بانکداری الکترونیک لازم اند، بایستی با قابلیت تراکنش ها و حساسیت سیستم ، آسیب پذیری شبکه و حساسیت اطلاعاتی که در حال انتقال است، متناسب باشد.

اصل 2: رئیس هیئت مدیره و مدیریت ارشد بایستی جنبه های کلیدی فرآیند کنترل امنیت بانک را مرور کرده و آن را تایید نمایند.

رئیس هیئت مدیره و مدیریت ارشد بایستی توسعه و نگهداری مداوم زیرساخت کنترل امنیتی که بنحو مناسبی سیستم های بانکداری الکترونیکی و داده ها را از هر دوی تهدیدات داخلی و خارجی حفظ می کند، سرپرستی کنند. این امر شامل ایجاد امتیازهای دسترسی مناسب، کنترل دسترسی ها بصورت فیزیکی ومنطقی، و امنیت مناسب زیر ساخت ها برای نگهداری از مرزها و محدودیات در هر دو فعالیت داخلی و خارجی است. حفاظت از سرمایه های بانک یکی از وظایف امانتداری هیئت مدیره و وظیفه اساسی مدیریت ارشد است. هر چند این امر وظیفه چالش بر انگیزی در فضای بانکداری الکترونیک سریع است، چرا که ریسک های امنیتی پیچیده ای تابع کار در شبکه عمومی اینترنت و استفاده از تکنولوژی نوآور است. برای تضمین کنترل های امنیتی مناسب برای فعالیت های بانکداری

الکترونیک، هیئت مدیره و مدیریت ارشد نیاز دارند که معلوم کنند آیا بانک دارای فرآیند امنیتی پیچیده ای است، و این فرآیند باید شامل روند ها و سیاست ها، که تهدید های امنیتی داخلی و خارجی، هر دو در شرایط جلوگیری و پاسخ به رویدادها شود. اجزای کلیدی فرآیند امنیت بانکداری الکترونیک کارا شامل موارد ذیل است:

- تخصیص وظیفه واضحی به مدیریت و کارمندان برای سرپرستی ایجاد و نگهداری سیاست های امنیتی سازمان. این وظیفه بطور معمول نبایستی قسمتی از وظیفه بازبینی باشد، که این وظیفه نظارت بر امنیت که آیا بصورت کارایی اجرا شده یا نه را دارد.
- کنترلهای فیزیکی کافی برای جلوگیری از دسترسی های فیزیکی بدون اجازه به محیط محاسبه بایستی انجام گیرد.
- کنترل های منطقی کافی و فرآیندهای مانیتورینگ برای جلوگیری از دسترسی داخلی و خارجی بدون اجازه به برنامه های کاربردی و پایگاه های داده بانکداری الکترونیکی لازم است انجام شود.
- بایستی معیار های امنیتی بطور مرتب، تست، بررسی و کنترل گردند. این موارد بایستی شامل ردیابی دائم توسعه های امنیتی صنعت کنونی و نصب بروزرسانیهای مناسب نرم افزاری، بسته های سرویس و معیار های لازم دیگر است. ضمیمه الف شامل روش های مضاف دیگری برای کمک به تضمین امنیت بانکداری الکترونیکی است.

اصل 3: هیئت مدیره و مدیریت ارشد بایستی تلاش مستمر و فرآیند سرپرستی جامعی و مداومی را برای مدیریت ارتباط های برون سپاری و باقی وابستگی های به پشتیبانی بانکداری الکترونیک انجام دهند.

افزایش اعتماد بر شریک ها و تامین کنندگان سرویس شخص ثالث جهت اعمال توابع بحرانی بانکداری الکترونیکی به بانک ها کنترل مستقیم مدیریت را آموخته است. بنابراین، فرآیند جامعی برای مدیریت ریسک های ناشی از برون سپاری و باقی وابستگی های شخص

ثالث لازم است. این فرآیند بایستی فعالیت های شخص ثالث از شریک ها و تامین کنندگان سرویس را، شامل زیر قرارداد بندی فعالیت های برون سپاری شده که می تواند تاثیر مادی بر بانک داشته باشد را در بر بگیرد. بشکل تاریخی، برون سپاری اغلب به تامین کننده سرویس یکتایی برای قابلیت هایی که می دهد، محدود می شود. هر چند، در سال های اخیر، ارتباطات برون سپاری بانکی در مقیاس و پیچیدگی به دلیل تاثیر مستقیم پیشرفت در فناوری اطلاعات و ظهور بانکداری الکترونیکی افزایش یافته است. افزایش پیچیدگی حقیقتی است که موجب شده سرویس های بانکداری الکترونیکی به تامین کنندگان سرویس مضاف و یا کشورهای خارجی بصورت زیر قرارداد، واگذار گردد. مضافا، با توجه به آنکه برنامه های کاربردی و سرویس های بانکداری الکترونیکی بیشتر بصورت تکنولوژیکی پیشرفته اند و از لحاظ اهمیت استراتژیک رشد کرده اند، محدوده قابلیت های خاص بانکداری الکترونیکی وابسته به تعداد کمتری از تامین کنندگان سرویس و شرکت های متخصص وابسته است. این توسعه های می تواند منجر به افزایش دغدغه های ریسکی که گواهی توجه به بانک های شخصی همانند نقطه نظر صنعتی سیستماتیک می باشد. این فاکتور ها با هم بر نیاز به ارزیابی جامع و مداوم ارتباطات برون سپاری و باقی وابستگی های خارجی، شامل التزام اشتراک برای پروفایل ریسک بانکی و توانایی های مدیریت ریسک اشتباهات، تاکید می کند. اشتباهات ارتباطات برونسپاری و وابستگی به شخص ثالث، مدیریت ارشد و هیئت مدیره بایستی بطور خاص بر روی تضمین موارد زیر متمرکز گردد:

- بانک بایستی بطور کامل ریسک های ناشی از ورود به قرار دادهای شخص ثالث و شراکت برای سیستم ها و برنامه های بانکداری الکترونیکی را درک نماید.
- بایستی تلاش بسیاری در جهت مرور شایستگی و توانایی مالی هر تامین کننده سرویس شخص ثالث یا شریک قبل از اقدام برای سرویس های بانکداری الکترونیکی انجام گیرد.
- مسئولیت قراردادی تمام طرفین برای ارتباط شراکت یا برون سپاری بایستی کاملا شفاف تعریف شود. برای مثال، وظایف

تامین اطلاعات و دریافت اطلاعات از تامین کننده سرویس بایستی کاملا شفاف مشخص شود.

- تمام عملیات و سیستم های بانکداری الکترونیک برون سپاری شده بایستی هدف مدیریت ریسک، سیاست های امنیتی و حفاظتی که متناسب با استانداردهای شخصی هر بانکی است قرار بگیرد.
- بازبینی داخلی و یا خارجی وابستگی ها بصورت دوره ای روی عملیات های برون سپاری شده بایستی انجام گیرد و این مورد در صورتی کهاین عملیات بصورت داخلی انجام گیرد، حداقل دامنه مشابهی را می طلبد.
- برنامه ریزی وابستگی مناسب برای فعالیت های بانکداری الکترونیک برون سپاری شده بایستی موجود باشد.

ضمیمه دو شامل لیستی از روش های مناسب مضافی جهت مدیریت سیستم های بانکداری الکترونیک برون سپاری شده و وابستگی های دیگر شخص ثالث است.

ب. کنترل های امنیتی (اصل 4 الی 10)

با توجه به آنکه اعضای هیئت مدیره وظیفه تضمین فرآیند کنترل امنیت مناسبی که در بانکداری الکترونیکی وجود دارد، را بر عهده دارند، اساس این فرآیند نیازمند توجه مدیریت ویژه ای به دلیل افزایش چالش های امنیتی ناشی از بانکداری الکترونیک است.
موارد زیر بطور خاص به این امر وابسته است:

- تصدیق Authentication
- غیر قابل انکار Non-repudiation
- یکپارچگی داده ها و تراکنش ها
- جداسازی وظایف
- کنترل بر دسترسی ها
- اعمال از بررسی های دنباله دار
- محرمانگی اطلاعات کلیدی بانک

اصل 4: بانک ها بایستی معیارهای مناسبی را جهت تصدیق هویت و دسترسی های مشتری و هر که با او کسب و کار اینترنتی انجام می دهند، در نظر بگیرند.

در بانکداری تایید اینکه ارتباط، تراکنش، یا درخواست دسترسی خاصی قانونی است، ضروریست. بنابراین بانک ها بایستی از روش های قابل اعتمادی را برای تصدیق هویت و دسترسی مشتریان جدید، همانند تصدیق هویت و دسترسی مشتریان قبلی که بدنبال انجام تراکنش الکترونیکی خاصی اند، استفاده کنند. تصدیق مشتری در حین ایجاد حساب بانکی در کاهش ریسک هویت دزدیه شده، کار روی حساب بصورت مجرمانه و پول شویی، اهمیت دارد. عدم موفقیت در شناسایی مناسب مشتری می تواند منجر به دسترسی غیر مجاز اشخاص به حساب بانک الکترونیک و نهایتا ضرر مالی و شهرتی به بانک از طریق کلاهبرداری، فاش سازی اطلاعات محرمانه یا درگیری در اعمال بزهکارانه بصورت سهوی گردد. ایجاد سیستم تشخیص هویت و کنترل دسترسی در فضای شبکه الکترونیکی خالص باز می تواند وظیفه مشکلی باشد. دسترسی قانونی کاربران می تواند از طریق تکنیک های عمومی بسیاری که تحت عنوان حقه بازی spoofing معروف است، مشتبه شود. هکر های آنلاین همچنین می توانند به session یک شخص دارای قابلیت دسترسی قانونی از طریق نرم افزار های آماری شبکه sniffer دست یابند و فعالیت هایی با ماهیت موذیانه و مجرمانه انجام دهند. فرآیند کنترل دسترسی همچنین می تواند با تغییر پایگاه داده دسترسی ها مورد حیله گیری قرار گیرد. بنابراین، داشتن سیاست رسمی و فرآیندهایی برای تشخیص متودولوژی های مناسب جهت تضمین اینکه بانک به نحو مناسبی هویت ها را شناسایی کرده و دسترسی به اشخاص، عامل ها یا سیستم می دهد، برای بانکها امری حیاتیست. این امر بدن معناست که این دسترسی ها موضعی و تا جایی که کاربردی باشد، مستثنی کننده اشخاص و افرادی که اجازه دسترسی ندارند، می باشد. بانکها روش های متعددی برای تامین تصدیق دارند که این روش ها شامل: شماره هویت شخصی PIN، کلمه عبور، کارت های هوشمند، زیست سنجی، و گواهینامه های دیجیتال است. این متد ها هر کدام می توانند بصورت تک فاکتوره یا چندین فاکتوره (برای مثال استفاده از هر دوی تکنولوژی کلمه عبور و زیست سنجی برای تصدیق) باشند. تصدیق چندین فاکتوره معمولا دارای تضمین محکم تری است.

بانک بایستی مشخص کند، که کدام متد تصدیق را با توجه به ارزیابی مدیریت از ریسک های مطرح در سیستم بانکداری الکترونیکی به طور عمده یا در تک تک زیر مولفه ها می خواهد استفاده نماید. این تحلیل ریسک بایستی توانایی های تراکنشی سیستم بانکداری (برای مثال انتقال وجه، پرداخت صورتحساب، ایجاد وام، تجمیع حساب و ..)، حساسیت و ارزش داده های بانکداری الکترونیکی، و سادگی استفاده از روش های تصدیق برای مشتری را ارزیابی کند. بطور خاص فرآیندهای مستحم تعیین هویت مشتری و دسترسی، در مفهوم ارتباط متقاطع بانکداری الکترونیکی، مشکلاتی را به دلیل انجام الکترونیکی کسب و کار در مقابل مرز های ملی، شامل ریسک های عظیم تر تشخیص جعل هویت و سختی مضاعفی برای انتقال ارزیابی اعتبار کارا برای مشتریان پتانسیل، ارائه می دهد.

در ضمن اینکه روش های تصدیق نمو پیدا میکنند، بانک ها علاقه دارند که روش های مناسب صنعتی را در این ناحیه تعدیل و مانیتور نمایند که این موارد بصورت لیست ذیل می باشد:

- پایگاه داده هایی که دسترسی به حساب های بانکداری الکترونیکی یا سیستم های حساس دارند بایستی از مداخله و فساد محافظت شوند. هر کدام از این مداخله ها بایستی مشخص شوند و با بررسی های دنباله دار مستند گردند.
- هر اضافه، حذف یا تغییر از طرف هر فرد، عامل یا سیستم در پایگاه داده تصدیق بایستی حسب الوظیفه و با اجازه دسترسی که در منبع تصدیق وجود دارد انجام گیرد.
- اندازه گیری های مناسب بایستی جهت کنترل ارتباطات سیستم بانکداری الکترونیکی مانند شخص ثالث که نمی تواند مشتری مشخصی را جایگزین کند، انجام گیرد.
- جلسه session بانکداری الکترونیکی تصدیق بایستی در تمام فرصت جلسه امن باشد و در صورتی که تاریخ انقضای آن به اتمام رسید جلسه بایستی نیاز به تصدیق مجدد داشته باشد.

اصل 5: بانک ها بایستی از روش های تصدیق تراکنشی که اجازه نفی انجام عملی را نمی دهد nonrepudeation استفاده نمایند و مسئولیت برای انجام عمل های بانک داری الکترونیکی ایجاد نمایند.

Nonrpudeation یعنی اثبات هایی برای منشاء یا تحویل اطلاعات الکترونیکی جهت حمایت کردن فرستنده در مقابل در دریافت کننده ای که داده ها را به غلط دریافت کرده، یا حمایت از دریافت کننده ای در مقابل انکار غلط توسط فرستنده ای که داده ها را فرستاده است. ریسک انکار تراکنش موضوعی مطرح در تارکنش های مرسوم مانند کارت اعتباری ها و امنیت تراکنش ها نیز بوده است. هر چند، بانکداری الکترونیکی این ریسک را بدلیل مشکلات تصدیق مطلق هویت ها و تصدیق طرف هایی که تراکنش را انجام میدهند، پتانسیل تراکنش های الکترونیکی ربایی، و پتانسیل کاربران بانکداری الکترونیکی در ادعایی که تراکنش های مجرمانه تغییر یافته اند، افزایش داده است.

برای بیان این ارتباط های مشخص شده، بانک ها نیاز دارند که تلاش معقولی انجام دهند، و متناسب با مادیت و نوع تراکنش بانکداری الکترونیکی این فعالیت را به نحوی انجام دهند که موارد زیر را تضمین نماید:

- سیستم های بانکداری الکترونیکی برای کاهش احتمال اینکه کاربران مجاز تراکنش نا مقبولشان را انجام دهند و درک مشتریان از ریسک هایی که توسط تراکنش هایی که انجام داده اند رخ داده، می باشد.
- تمام طرفین تراکنش بایستی بنحو مطلوبی تصدیق شوند و کنترلی در بر کانال تصدیق انجام گیرد.
- داده تراکنش مالی از تغییرات حفظ می شود و هر تغییری در آن قابل شناسایی باشد.

سازمان های بانک داری انجام تکنیک های مختلفی که جلوی انکار را می گیرد و محرمانگی و یکپارچگی تراکنش های بانکداری الکترونیکی را تامین می کند، مانند گواهینامه هایی الکترونیکی که از زیر ساخت کلید عمومی استفاده می کند، را شروع کرده اند.

یک بانک ممکن است از گواهینامه الکترونیک برای مشتری یا یک طرف جهت ایجاد امکان برای تشخیص هویت و تصدیق و کاهش ریسک انکار تراکنش استفاده نماید.
با وجود اینکه در بعضی از کشورها مشتریان حق دعاوی در مقابل تراکنش هایی که در شرایط خاص قانونی انجام گرفته را می دهند، در محدوده های قضایی مشخصی امضای الکترونیکی را بطور قانونی لازم الاجرا نموده است. پذیرفتن قضایی وسیع تر این تکنیک ها با توجه به نمو و ادامه تکنولوژی انجام خواهد گرفت.

اصل 6: بانک ها بایستی تضمین نمایند که معیارهای مناسبی جهت بهبود تفکیک مناسب وظایف در سیستم های بانکداری الکترونیکی، پایگاه داده ها و برنامه های کاربردی وجود دارد.

تفکیک وظایف یکی از پایه های داخلی معیار های کنترل است که برای کاهش ریسک کلاهبرداری در فرآیندهای عملیاتی و سیستم ها و تضمین اینکه تصدیق تراکنش ها و دارایی های شرکت بنحو مناسبی تصدیق می شوند، بایگانی و حراست می باشد. تفکیک وظایف برای تضمین دقت و یکپارچگی داده هایی که برای ایجاد مانع جهت آماده سازی کلاه برداری های شخصی استفاده می شود، بسیار بحرانیست. اگر وظایف بنحو مناسبی تفکیک شده باشند، کلاه برداری می تواند تنها با ساخت و پاخت انجام گیرد. سرویس های بانکداری الکترونیکی ممکن است منجر به تغییر روش هایی که تفکیک وظایف بر مبنای آنها صورت می گرفته شوند، دلیل این امر آنست که تراکنش هایی که در سیستم های الکترونیکی انجام می گیرند بنحوی اند که براحتی قابل جعل و نمادین عمل کردن می باشند. مضافا، قابلیت های مبتنی بر تراکنش و عملیاتی در بسیار از حالات در برنامه های کاربردی بانکداری الکترونیکی فشرده شده و یکپارچه شده می شوند. بنابراین، این کنترل بطور عادی نیازمند انجام تفکیک وظایف اند که بتواند مرور شده و برای تضمین سطح مناسبی از کنترل تعدیل گردند. با توجه به آنکه دسترسی به پایگاه داده های با امنیت ضعیف می تواند براحتی از طریق شبکه های داخلی یا خارجی انجام گیرد، روندهای تصدیق و تشخیص هویت سختگیرانه، با معماری امن و مناسب از فرآیندهای مستقیم، و روند های ادامه دار بررسی مناسب بایستی مورد تاکید قرارگیرند. روش های معمول

مورد استفاده برای تدوین و انجام تفکیک وظایف یک محیط بانکداری الکترونیکی شامل موارد ذیل می باشد:

- فرآیندهای تراکنش و سیستم بایستی بنحوی طراحی گردند که تضمین کننده هیچ تامین کننده یکتای کارمند یا تامین کننده سرویس بروسپاری شده بتواند وارد سیستم شود، تصدیق گردد و تراکنشی را انجام دهد.
- تفکیک بایستی بین آنهایی که داده های استاتیک (شامل محتویات صفحه وب) و آنهایی که مسئول تضمین یکپارچگی هستند انجام گیرد.
- سیستم های بانکداری بایستی چک شوند تا تضمین کنند که تفکیک وظایف قابل عبور نباشد.
- تفکیک بایستی بین آنهایی که سیستم را توسعه می دهند و آنهایی که بانکداری الکترونیکی را مدیریت می کنند، انجام گیرد.

اصل 7 : بانک ها بایستی تضمین کنند که کنترل دسترسی و دسترسی های مجاز مناسبی در سیستم بانکداری الکترونیکی، پایگاه داده ها، و برنامه های کاربردی وجود دارد.

برای نگهداری تفکیک وظایف، بانک لازم است، بنحو سختگیرانه ای کنترل دسترسی ها و دسترسی های مجاز را انجام دهد. قصور از تامین کنترل های دسترسی مناسب می تواند به اشخاص اجازه دهد که اختیار خودشان را تغییردهند، با حیله گری از تفکی پیش دستی کنند و به سیستم های بانک داری الکترونیکی، پایگاه داده ها یا برنامه های کاربردی که مجاز به دسترسی نیستند، دست یابند. در سیستم های بانکداری الکترونیکی، حق دسترسی می تواند بصورت متمرکز یا بروش توزیع شده از بانک باشد و بطور کلی در پایگاه داده ها ذخیره شده باشد. حفاظت آن پایگاه داده ها از مداخله و فساد بنابراین جهت کنترل کارای دسترسی ها امری بحرانیست. ضمیمه سه تعدادی از روش های مناسبی جهت کنترل مطلوب حق دسترسی ها به سیستم های بانکداری الکترونیکی، پایگاه های داده و برنامه های کاربردی را مشخص می نماید.

اصل 8: بانک ها بایستی تضمین نمایند که معیار های مناسبی در حفاظت از یکپارچگی تراکنش های بانکداری الکترونیکی، رکوردها و اطلاعات وجود دارد.

یکپارچگی داده ها به این اشاره می کند که اطلاعاتی که در حال انتقال اند یا ذخیره شده اند بدون حق دسترسی تغییر ننمایند. قصور در برقراری یکپارچگی داده در تراکنش ها، رکور دها و اطلاعات میتواند موجب ایجاد ضرر های مالی مانند ریسک های قانونی قابل توجه و انکار مواجه سازد. خاصیت ذاتی فرآیندهای مستقیم برای بانکداری الکترونیکی می تواند خطاهای برنامه نویسی یا فعالیت های کلاهبردارانه را برای مشخص شدن در مراحل اولیه بسیار مشکل تر نماید. بنابراین اینکه بانک ها پردازش های مستقیم را به روشی که امنیت و مطلوبیت و یکپارچگی داده را افزایش دهد، انجام دهند، امری بسیار مهم است.

با توجه به انجام بانکداری الکترونیکی در شبکه های عمومی، تراکنش ها با تهدید های مظاف فساد اطلاعات، کلاه برداری و مداخله در رکورد ها مواجه اند. بنابراین، بانک ها بایستی اینکه معیار های مناسبی برای معین کردن دقت، کمال، و قابلیت اعتماد تراکنش های بانکداری الکترونیکی، رکوردها و اطلاعاتی که در اینترنت جابجا می شوند، مستقر شدن بر پایگاه داده های بانک، یا ذخیره سازی و نگهداری توسط تامین کننده سرویس شخص ثالث به جای بانک، وجود دارد را تضمین نمایند. روش های معمولی که برای ایجاد یکپارچگی در محیط بانکداری الکترونیکی بکار می رود شامل موارد ذیل می باشد:

- تراکنش های بانکداری الکترونیکی بایستی به نحوی انجام گیرند که آنها را در مقابل یکپارچگی فرآیند مقاوم سازد.
- رکوردهای بانکداری الکترونیکی بایستی به نحوی که آنها را در مقابل تغییرات مقاوم سازد، نگهداری، دسترسی و تغییر یابند.
- تراکنش ها و فرآیندهای نگهداری رکورد ها بایستی بنحوی طراحی شوند که تشخیص با حیله گری دور زدن تغییرات غیر مجاز را بصورت مجازی غیر ممکن سازند.

- سیاست های تغییر مناسب، شامل روند های مانیتورینگ و تستینگ، بایستی در مقابل هر تغییر سیستم بانکداری که ممکن است سهوی یا از روی خطا کنترل یا اعتماد به داده را ایجاد کند، وجود داشته باشد.
- هر تغییردر تراکنش های بانکداری الکترونیکی یا رکوردها توسط قابلیت های پردازش تراکنش، مانیتورینگ و نگهداری رکورد بایستی قابل شناسایی باشد.

اصل 9: بانکها بایستی تضمین نمایند که بررسی های دنباله دار واضحی برای تراکنش های بانکداری الکترونیکی وجود داشته باشد.

تحویل سرویس های مالی در اینترنت می تواند برای بانکها جهت اعمال و اجرای کنترل داخلی و انجام بررسی های دنباله دار در صورتی که این اندازه گیری ها در محیط بانکداری الکترونیکی تعدیل نگردند، مشکل تر باشد. بانک ها تنها برای تضمین اینکه کنترل داخلی می تواند در فضای بسیار اتوماتیک تامین شود، به چالش کشیده نمی شوند، بلکه چالش دیگر این است که کنترل ها می توانند بطور مستقل بررسی شوند، و این امر بطور خاص برای تمام رویداد های و برنامه های کاربردی بحرانی بانکداری الکترونیک وجود دارد. این به این دلیل است که بیشتر، اگر تمام نباشد، رکوردها و شواهد پشتیبانی تراکنش های بانکداری الکترونیکی به فرمت الکترونیکی است. برای مشخص کردن اینکه کجا روند های واضحی بایستی وجود داشته باشد، انواع تراکنش های بانکداری الکترونیکی زیر بایستی مورد توجه قرار گیرند:

- باز کردن، تغییر و بستن حساب مشتری.
- هر تراکنشی که نتیجه اش بصورت مالی باشد.
- هر دسترسی که به مشتری برای تجاوز از حد وجود دارد.
- هر ایجاد، تغییر یا فسخ حق دسترسی به سیستم و اجازه ها.

ضمیمه چهار روش های متعدد مناسبی را برای کمک به تضمین اینکه بررسی های دنباله داری برای تراکنش های بانک داری الکترونیکی وجود دارد، بیان می نماید.

اصل 10: بانک ها بایستی معیار های مناسبی را برای حفظ محرمیت اطلاعات کلیدی بانکداری الکترونیک داشته باشند. معیارهایی که

برای حفظ محرمانگی انتخاب می شوند بایستی متناسب با حساسیت اطلاعاتی که انتقال می یابند و یا در پایگاه داده ذخیره می شوند، باشد.

محرمانگی تضمین این است که اطلاعات کلیدی برای بانک بصورت شخصی باقی بماند و برای افرادی که مجاز نیستند نمایش داده نشود و مورد استفاده قرار نگیرد. سوء استفاده یا فاش سازی نامجاز داده ها بانک ها را با جفت ریسک های قانونی و انکار مواجه می سازد. بانکداری الکترونیکی نوظهور چالش های امنیتی را برای بانک ها ایجاد کرده است که این بدلیل افزایش مواجهه با اطلاعات انتقال یافته در شبکه عمومی یا نگهداری شده در پایگاه داده هاست که ممکن است توسط افراد غیر مجاز یا طرفهای نا مناسب مورد دسترسی قرار گرفته یا بنحوی استفاده شود که مشتری نمی خواسته اطلاعات مورد استفاده قرار گیرند.

مضافا، افزایش استفاده از تامین کنندگان سرویس ممکن است داده های کلیدی بانک را با طرف های دیگری مواجه سازد.

برای مواجه با این چالش ها که متوجه حفاظت از محرمانگی اطلاعات کلیدی بانکداری الکترونیکی است، بانک ها نیاز دارند که موارد ذیل را تضمین نمایند:

- تمام داده های بانک محرمانه و رکوردها تنها توسط افراد، عامل ها یا سیستم های مجاز و تصدیق شده قابل دسترسی باشد.
- تمام داده های بانک محرمانه بروش امن نگهداری شده و از نمایش یا تغییر برای افراد غیر مجاز در نمایش یا تغییرات در حین انتقال به شبکه های داخلی، شخصی یا عمومی حفاظت شوند.
- مطابق با استانداردها و کنترلهایی برای داده جهت استفاده و حفاظت بایستی، وقتی شخص ثالثی دسترسی به اطلاعات از طریق ارتباط های برون سپاری شده دارند، وجود داشته باشد
- تمام دسترسی ها به اطلاعات محرمانه نگهداری شده و تلاش مناسبی جهت تضمین محافظت این log ها در مقابل مداخلات وجود دارد.

ج. مدیریت ریسک های انکار و قانونی (اصول 11 الی 14)

قوانین و مقررات حفاظت از مشتری خاص و محرمانگی از محدوده قضایی به محدوده قضایی دیگر متفاوت است. هرچندبانک ها بطور کلی وظیفه واضحی برای تامین سطح هایی از آسودگی با توجه به عدم فاش سازی اطلاعات، حفاظت از داده ها مشتری و در دسترس بودن کسب و کاری که نزدیک به سطحی که در کسب و کار تراکنشهای از طریق کانال های توزیع بانکداری سنتی دارند، تامین نمایند.

اصل 11: بانک ها بایستی تضمین کنند که اطلاعات مناسبی برای تامین در وب سایتشان جهت ایجاد امکان برای مشتریان پتانسیل برای مطلع ساختن نتایج در مورد هویت بانک و حالت قانونی بانک با توجه به ورود به تراکنش های بانکداری الکترونیکی تامین مینمایند.

جهت کاهش ریسک های قانونی و انکار در فعالیت های بانکداری در هردوی درون مرزی و برون مرزی، بانک ها بایستی تضمین کنند که اطلاعات مناسبی در وب سایت آنها برای ایجاد امکان به مشتریان جهت تصمیم گیری های با اطلاع در مورد هویت و وضعیت قانونی بانک، قبل از آنکه به تراکنش های بانکداری الکترونیکی وارد شوند، تامین نمایند.

مثال هایی از این نوع اطلاعات که بانک میتواند در وب سایت خودش تامین نماید شامل موارد ذیل است:

- نام بانک و مکان دفتر مرکزی آن (و دفتر محلی اگر قابل انجام باشد)
- مشخص کردن اختیارات سرپرستی بانک مسئول برای نظارت بر دفتر مرکزی بانک.
- نحوه ای که مشتریان می توانند به مراکز سرویس مشتریان بانک بر اساس مشکلات سرویس ها، شکایات، سوء استفاده های مشکوک از حساب ها و ...
- چگونه مشتریان می توانند به وکیل ها یا طرح های شکایت مصرف کنندگان دسترسی یابند.

- چگونه مشتریان میتوانند به بیمه جبران یا سپرده پوشش دهنده سطحی از امنیتی که می توانند تهیه کنند (یا پیوند به وب سایت هایی که اینگونه اطلاعات را تامین نماید) دسترسی یابند.
- باقی اطلاعاتی که شاید مناسب باشد یا مورد نیاز محدوده قضایی خاصی باشد.

اصل 12: بانک ها بایستی معیار های مناسبی را برای تضمین الصاق به نیازمندی های حریم مشتری قابل اعمال بر حوزه قضایی که در آن بانک محصولات یا سرویس های بانکداری الکترونیکی را تامین می کنند، انتخاب کرده باشند.

نگهداری حریم اطلاعات مشتری وظیفه اساسی برای بانک است. سوء استفاده یا فاش سازی نا مجاز داده های محرمانه مشتری بانک را با ریسک های امنیتی و انکار مواجه می سازد. جهت مواجه شدن با این چالش ها که حفاظت از حریم اطلاعاتی مشتری را بر عهده دارند، بانک ها بایستی تلاش معقولانه ای را جهت تضمین موارد ذیل به انجام رسانند:

- سیاست های حریم مشتری بانک و استانداردهای برداشت از حساب و تطابق آ« با تمام قوانین حریم و مقرارت قابل اجرا در محدوده قضایی که محصول یا سرویس بانکی در آن ارائه می گردد.
- مشتریان از سیاست های حریم بانکی و موضوع های مربوط مورد توجه به استفاده از محصولات و سرویس های بانکداری الکترونیکی با خبرباشند.
- ممکن است مشتریان نپذیرند که بانک اطلاعات متقاطع کسب کار را به شخص ثالث در مورد نیازها، تمایلات، وضعیت مالی یا فعالیت های بانکداری شخصی مشتری رائه نماید.
- داده های مشتری برای هدفی فراتر از آنچه آنهابطور خاص اجازه اش را داده اند یا برای استفاده فرآتر از انچه مشتری دسترسی دارد استفاده نمی شود.

- استانداردهای بانک برای استفاده مشتری از داده بایستی، وقتی که شخص ثالثی دسترسی به داده های مشتری از طریق ارتباط های برون سپاری دارد، استفاده شود.

ضمیمه 5 روش های متعددی را برای کمک به نگهداری حریم اطلاعات مشتری در بانکداری الکترونیکی ارائه می دهد.

اصل 13: بانک ها بایستی ظرفیت کارا، دوام کسب و کار و فرآیند برنامه ریزی احتمال برای کمک به تضمین در دسترس بودن سیستم و سرویس بانکداری الکترونیکی داشته باشند.

برای حفاظت از بانک در مقابل ریسک کسب و کار، قوانین و انکار، سرویس های بانکداری الکترونیکی بایستی مطابق انتظارات مشتری بصورت استوار و بصورت بهنگام ارائه گردد. برای دسترسی به این امر، بانک بایستی توانایی ارائه سرویس های بانکداری الکترونیکی به کاربران نهایی چه بصورت اولیه (برای مثال سیستم ها و برنامه های کاربردی داخلی) یا منبع ثانویه (برای مثال سیستم ها و برنامه های کاربردی تامین کننده سرویس) را داشته باشند. نگهداری در دسترس بودن مناسب همچنین وابسته به توانایی وابستگی سیستم پشتیبان برای مقابله با حمله برای نابودی سرویس (denial of service) یا باقی رویدادهاییکه می تواند بصورت پتانسیل موجب شکستن سیستم شود، است. چالش نگه داشتن در دسترسی متوالی سیستم های بانکداری الکترونیکی و برنامه های کاربردی می تواند با پتانسیل داده شده برای تقاضای بالای تراکنش ها مخصوصادر دوره زمانی پیک، قابل ملاحظه باشد.

مضافا، توقعات بالای مشتریان براساس زمان سیکل کوتاه پردازش تراکنش ها و در دسترس بودن ثابت اهمیت ظرفیت مناسب، استمرار کسب و کار و برنامه ریزی احتمال را افزایش داده است.جهت تامین مشتری با پیوستگی سرویس های بانکداری الکترونیکی که انتظار میرود، بانک ها نیاز دارند که موارد ذیل را تضمین نمایند:

- ظرفیت کنونی سیستم بانکداری الکترونیکی و توسعه پذیری آینده بایستی تحلیل شوند و این تحلیل بایستی بر اساس پویایی بازار برای تجارت الکترونیک و نرخ طرح ریزی

مشتریانی که محصولات و سرویس های بانکداری الکترونیک را قبول می کنند باشد.

- ظرفیت پردازش تراکنش های بانکداری الکترونیکی بایستی تدوین شود، تحت فشار تست شود و بطور دوره ای مرور گردد.
- پیوستگی کسب و کار مناسب و طرح های احتمال برای فرآیندهای بحرانی بانکداری الکترونیک و تحویل سیستم ها بایستی وجود داشته و بطور مرتب تست گردد.

ضمیمه 6 تعداد زیادی از روش های طرح ریزی احتمالی و استمرار کسب و کار، ظرفیت های مناسب را مشخص می کند.

اصل 14: بانک ها بایستی برنامه های پاسخ به رویداد مناسبی رابرای مدیریت، شامل شدن، و مینیمم سازی مشکلاتی که از رویدادهای غیر منتظره، شامل حملات داخلی و خارجی، که ممکن است قید سیستم بانکداری الکترونیکی و سرویس ها را مختل کند،را توسعه دهند.

مکانیزم های کارای پاسخ به رویدادها برای کمینه سازی ریسک های عملیاتی، قانونی و انکاری که از رویدادهای غیر منتظره ای مانند حملات داخلی و خارجی که ممکن است بر قید سیستم ها و سرویس های بانکداری الکترونیکی تاثیر بگذارد، بحرانی است.

بانک ها بایستی طرح های مناسب پاسخ به رویدادها را که شامل، استراتژی های ارتباطی، برای تضمین پیوستگی کسب و کار، کنترل ریسک انکار و محدود کردن مسئولیت ناشی از شکستن سرویس های بانکداری الکترونیک، شامل آنهایی که از سیستم ها و عملیات برون سپاری شده ساخته می شوند، را توسعه دهند.

برای تضمین پاسخ کارا به رویدادهای پیش بینی نشده، بانک ها بایستی موارد ذیل را توسعه دهند:

- برنامه های پاسخ به رویداد هایی برای انجام بازیافت سیستم های بانکداری الکترونیکی و سرویسهایی در سناریوها، کسب و کار و مناطق جغرافیایی متعدد. این تحلیل سناریو ها بایستی شامل بررسی احتمال ریسک رخ داده و تاثیر آن بر بانک است. سیستم های بانکداری الکترونیکی که به تامین

کننده سرویس شخص ثالثی برون سپاری مشود نیز بایستی جزء این مجموعه برنامه ها باشند.

- مکانیزم هایی برای مشخص کردن رویداد یا بحران بلافاصله بعد از آنکه رخ داده، ارزیابی موجودیت آن، و کنترل ریسک انکار که از طریق شکستن سرویس رخ می دهد.
- استراتژی ارتباط برای ارائه دغدغه های مدیا و بازار که ممکن است در رویدادهایی از رخنه های امنیتی، حمله آنلاین و یا قصور در سیستم های بانکداری الکترونیکی بوجود می آید.
- فرآیند واضحی برای تغییر مجوز های قانونی مناسب در ایجاد رویدادهای رخنه امنیتی مادی یا رویدادهای بر هم زننده.
- تیم های پاسخ به رویدادها با دسترسی هایی برای کار در شرایط اورژانسی و آموزش کافی برای تحلیل رویدادها و شناسایی آنها و پاسخ به آنها و تفسیر خروجی های مربوط بی اهمیت.
- زنجیره واضحی از دستورات، که عملیات داخلی را مانند عملیات برونسپاری شده احاطه می کند، که تضمین کند که عمل سریع بطور مناسبی برای اهمیت رویداد انجام می گیرد. مضافا، تعدیل و روندهای ارتباطی داخلی بایستی توسعه یابند و شامل اخطار به هیئت مدیره هر جا لازم باشد است.
- فرآیندی برای تضمین تمام طرف های خارجی، شامل مشتریان بانک ها، نقاط مقابل، و مدیا، در زمان مناسب و بنحو مناسبی از بهم ریختگی مواد بانکداری الکترونیکی و توسعه تجدید کسب و کار، اطلاع داده شود.
- فرآیندی برای جمع آوری تمام شواهد جهت ادعای دادگاهی برای مرور مناسب پس از واقعه هر رویداد بانکداری الکترونیکی مانند همکاری در تعقیب قانونی حمله کنندگان.

ضمیمه 1

روش های مناسب کنترل امنیت برای بانکداری الکترونیکی

1. بایستی پروفایل امنیتی تهیه گردد و بر اساس دسترسی های مجاز اختصاص داده شده به تمام کاربران سیستم بانکداری

الکترونیکی و برنامه های کاربردی، شامل تمام مشتریان، کاربراین داخلی بانک ها و تامین کنندگان سرویس های برون سپاری شده نسبت داده شوند. کنترل های دسترسی منطقی بایستی همچنین برای پشتیبانی از تفکیک وظایف طراحی شوند.

2. داده ها و سیستم های بانکدار الکترونیکی بایستی بر اساس حساسیت و اهمیت آنها کلاسه بندی شوند و برطبق آنها محافظت گردند. مکانیزم های مناسب، مانند رمز گذاری، کنترل دسترسی و برنامه ریزی بازیافت داده بایستی برای حفاظت از تمام اطلاعات حساس و برنامه های کاربردی، پایگاه داده ها، سرور ها و سیستم های بانکداری الکترونیکی با ریسک زیاد بکار روند.
3. ذخیره داده با ریسک بالا و حساس بر لب تاپ یا میزکار کامپیوتر بایستی کمینه گردد و بنحو مناسبی توسط رمز گذاری، کنترل دسترسی و برنامه های بازیافت داده حفاظت گردند.
4. کنترل فیزیکی مناسب بایستی برای مشخص کردن دسترسی های غیر مجاز برای تمام برنامه های کاربردی و پایگاه داده ها، سرورها، و سیستم های بانکدار الکترونیکی انجام گیرد.
5. تکنیکهای مناسبی برای برطرف کردن تحدیدات خارجی برای سیستم بانکداری شامل موارد ذیل بایستی انجام گیرد.:
   - نرم افزار های کاووشگر ویروس در تمام نقاط ورودی (برای مثال سرورهای دسترسی متحرک، سرور های پروکسی ایمیل) و بر هر سیستم شخصی.
   - نرم افزارهای تشخیص نفوذ و باقی نرم افزارهای ارزیابی امنیت برای کاووش دوره ای شبکه، سرورها و فایلها برای ضعف ها ویا تجاوز از کنترلها و سیاست های امنیتی.
   - تست نفوذ از داخل و خارج شبکه.
6. فرآیند مرور امنیتی سختی بایستی برای تمام کارمندان و تامین کنندگانی که موقعیت حساسی دارند بایستی انجام گیرد.

ضمیمه 2: روش های مناسب برای مدیریت سیستم های بانکدار الکترونیکی برون سپاری شده و سرویس ها

1. بانک ها بایستی فرآیندهای مناسبی را برای ارزیابی تصمیماتی برای برون سپاری سیستم ها و سرویس های بانکدار الکترونیکی تعدیل نمایند.

- مدیریت بانک بایستی بنحو واظحی هدف های استراتژیک، عواید و هزینه هایی که در ورود به ترتیبات برون سپاری برای بانکداری الکترونیکی با شخص ثالث وجود دارد، را مشخص نماید.
- تصمیم برای برون سپاری قابلیت های کلیدی بانک داری الکترونیکی یا سرویس بایستی شامل استراتژی های کسب و کار بانک باشد، و بر اساس نیازهای واضح تعریف شده کسب و کار، و تشخیص ریسک های مشخصی که برون سپاری را شامل می شوند، است.
- تمام نوحی بانک که تحت تاثیر قرار می گیرند، لازم است درک کنند که چگونه تامین کننده سرویس استراتژیبانکداری الکترونیک بانک را پشتیبانی کرده و متناسب با ساختار اجرایی آن است.

2. بانک ها بایستی تحلیل ریسک مناسبی انجام دهند و تلاش زیادی در انتخاب تامین کننده سرویس بانکداری الکترونیک و بازه های مناسب بعد آن انجام دهند.

- بانک ها بایستی به فرآیند توسعه برای تقاضای پروپوزال برای تامین کنندگان سرویس بانکداری متعدد و محدوده هایی برای انتخاب بین پروپوزال های متعدد توجه نمایند.
- بلافاصله بعد از اینکه تامین کننده سرویس پتانسیلی مشخص شد، بانک بایستی تلاش بسیاری در مرور مناسب، شامل تحلیل ریسک قدرت مالی تامین کننده سرویس، انکار، سیاست های مدیریت ریسک و کنترل ها، و توانایی انجام وظایف، انجام دهند.

- پس از آن، بانک ها بایستی بطور مرتب توانایی تامین کننده سرویس را مانیتور، اگر مناسب بود، تلاش در مرورآن بنمایند، و مدیریت ریسک را در حین قرار داده انجام دهند.
- بانک ها نیاز دارند که تضمین کنند که منابع کافی در ترتیبات برون سپاری برای پشتیبان بانکداری الکترونیکی سپرده شده است.
- مسئولیت سرپرستی ترتیبات برون سپاری بایستی بنحو واضحی سپرده شده باشد.
- استراتژی خروجی مناسب برای بانک جهت مدیریت ریسک بایستی ارتباطات برون سپاری را متوقف.

3. بانک ها بایستی روند های مناسبی را برای مدیریت مناسب قرار دادهای بانکداری الکترونیک تعدیل نمایند. قراردادهای مدیریت فعالیت های بانکداری الکترونیکی برون سپاری شده بایستی ارائه گردد، برای مثال موارد ذیل:

- مسئولیات قرار دادی از طرفین مخصوص مانند وظایفی برای تصمیم گیری، شامل هر سرویس مادی زیر قراردادی بنحو واضحی تعریف گردد.
- وظایفی برای تامین اطلاعات برای دریافت اطلاعاتی برای تامین کننده سرویس بنحو واضحی تعریف گردند. اطلاعات از تامین کننده سرویس بایستی سروقت و به اندازه کافی جامع باشد که به بانک اجازه دهد، بنحو مناسبی سطح سرویس ها و ریسک را ارزیابی کند. آستانه موجودیت و روند هایی برای استفاده جهت اعلام به بانک سرویس های شکسته شده، رخنه های امنیتی و باقی رویدادهایی که منجر به ریسک به بانکی می شود، بایستی مشخص شود.
- مقرراتی که پوشش بیمه را مشخص می کند، مالکیت داده ای که بر سرورها یا پایگاه داده های تامین کننده سرویس ذخیره می شود، و حق بانک برای بازیافت داده هایش بر اساس انقضاء یا توقف قرار داد، بایستی بنحو واضحی تعریف گردد.
- انتظارات کارایی، بر اساس هر دوی مقتضیات و وابستگی ها، تعریف می شوند.

- معنای کافی و گارانتی هایی، برای مثال از طریق ماده های پیگیری، برای تضمین اینکه تامین کننده سرویس با سیاست های بانک موافقت دارد، تعریف می شود.
- مقررات برای مداخله مرتب و سر وقت و همسوسازی در رویداد از کارایی زیر استاندارد با تامین کننده سرویس انجام می گیرد.
- برای ترتیبات برون سپاری برون مرزی، مشخص کردن اینکه قوانین کدام کشور و مقررات، شامل آنهایی که مرتبط با حریم و باقی محافظت های مشتری است، قابل اعمال اند.
- حق بانک برای انجام مرور مستقل و یا بررسی امنیت، کنتل های داخلی و کنترل داخلی و تداوم کسب و کار و برنامه وابستگی بایستی بنحو واضحی تعریف شود.

4. بانک ها بایستی تضمین کنند که بررسی های دوره ای داخلی و یا خارجی بر عملیات برون سپاری شده حد اقل بر دامنه مشابهی برای عملیاتی که داخلی انجام می شود، انجام می گیرد.
   - برای ارتباط های برون سپاری شده شامل برنامه های کاربردی و بانکداری الکترونیکی پیچیده از لحاظ تکنولوژیکی، بانک ها ممکن است نیاز به ترتیباتی برای باقی مرور های دوره ای برای انجام توسط شخص ثالث مستقل با تخصص تکنیکال کافی باشد.
5. بانک ها بایستی برنامه احتیاطی مناسبی را برای فعالیت های بانکداری الکترونیکی توسعه دهند.
   - بانک ها نیاز به توسعه و تست دوره ای برنامه های احتیاطی برای تمام سیستم ها و سرویس های بانکداری الکترونیکی بحرانی که به شخص ثالثی برون سپاری شده است، دارند.
   - برنامه های احتیاطی بایستی سناریوهای بدترین حالت معتبر را برای تامین یکپارچگی سرویس های بانکداری الکترونیکی در رویدادهایی شکستن تاثیر گذار بر فرآیندهای برون سپاری را ارائه دهند.

- بانک ها بایستی تیم مشخص شده ای را که برای معنای بازیافت و ارزیابی تاثیر مالی بر شکستن در سرویس های بانکداری الکترونیکی برون سپاری شده، داشته باشند.

6. بانک هایی که سرویس های بانکداری الکترونیکی را برای شخص هیا ثالث تامین میکنند، بایستی تضمینکنند که عملیات، مسئولیتها، و قابلیت اطمینان بحد کافی واضح است، به نحوی که سازمان های سرویس گیرنده میتوانند بنحو کافی مرور پیوسته را اشتباهاتشان را در ارتباط انجام دهند.

- بانک ها وظیفه دارند که برای نهادهای مورد سرویسشان اطلاعات لازم برای تشخیص هویت، کنترل و مانیتور کردن هرریسکی که در ترتیبات بانکداری الکترونیکی وجود دارد، راتامین کنند.

ضمیمه 3: روش های دسترسی مناسب برای برنامه های کاربردی بانکداری الکترونیکی

1. اجازه دسترسی خاصی بایستی برای هر شخص، عامل، یا سیستم، که فعالیت های بانکداری الکترونیک را انجام می دهد، بایستی نسبت داده شود.
2. تمام سیستم های بانک داری الکترونیکی بایستی برای تضمین اینکه ارتباط با یک پایگاه داده دسترسی انجام می گیرد، ساخته شود.
3. هیچ عامل یا سیستمی نبایستی مجاز باشد که دسترسی خودش را در پایگاه داده دسترسی بانکداری الکترونیکی تغییر دهد.
4. هر شخص، عامل یا سیستم یا تغییرات برای دسترسی در پایگاه داده دسترسی های بانکداری الکترونیک بایستی اجازه دسترسی با منبع تصدیق صاحب اختیار با اجازه مناسب و موضوعی برای بررسی روند ها و نظارت و مناسب و سروقت داشته باشد.
5. معیار های مناسبی بایستی برای مقاوم سازی معقولانه پایگاه داده های دسترسی بانکداری الکترونیکی بایستی انجام گیرد. هر تغییری از این نوع بایستی از طریق

فرآیندهای مانیتورینگ ادامه دار قابل شناسایی باشد. بررسی های ادامه دار کافی بایستی برای مستند سازی این تغییرات انجام گیرد.

6. هر پایگاه داده دسترسی بانکداری الکترونیک که تغییر کرده باشد، نبایستی تا وقتی که با پایگاه داده معتبر جایگزین می شود، استفاده شود.
7. کنترل هایی برای جلوگیری از تغییرات در سطح دسترسی در جلسه تراکنش بانکداری الکترونیک انجام گیرد و هر تلاش برای تغییر دسترسی بایستی ثبت شود و به اطلاع مدیریت رسد.

ضمیمه 4 : روش های مناسب بررسی دنباله دار سیستم های بانکداری الکترونیکی

1. ثبت وقایع کافی بایستی برای تمام تراکنش های بانکداری الکترونیکی نگهداری شود تا در بررسی دنباله دار و همکاری در حل نزاع بنماید.
2. سیستم های بانکداری الکترونیکی بایستی طراحی شوند و برپاسازی شوند که شواهد دادگاهی را گرفته ونگهداری کنند و این کار را به نحوی انجام دهند که کنترل بر شواهد را نگهداری نموده، و از تغییر و جمع آوری شواهد غلط جلوگیری کنند.
3. در نمونه هایی که سیستم های پردازش و بررسی های دنباله دار مرتبط در وظیفه تامینکننده سرویس شخص ثالث اند:

- بانک بایستی تضمین کند که دسترسی به بررسی های دنباله دار توسطه تامین کننده نرم افزار نگهداری می شود.
- بررسی های دنباله دار نگهداری شده توسط تامین کننده سرویس مطابق استانداردهای بانک است.

ضمیمه 5: روش های مناسب برای نگهداری حریم اطلاعات مشتری بانکداری الکترونیک

1. بانک ها بایستی تکنیک های پنهانی مناسبی را، پروتکل های خاص یا باقی کنترل هایامنیتی را برای تضمین

محرمانگی داده های مشتری بانکداری الکترونیک انجام دهند.

2. بانک ها بایستی روندها و کنترل های مناسبی را برای ارزیابی دوره ای زیر ساخت امنیت مشتری و پروتکل هایی برای بانکداری الکترونیکی توسعه دهند.
3. بانک ها بایستی تضمین نمایند که تامین کنندگان سرویس شخص ثالث دارای سیاست های محرمانگی و حریم هستند که در آن استوار اند.
4. بانک ها بایستی قدم های مناسبی را برای اطلاع مشتریان بانکداری الکترونیکی در مورد محرمانگی و حریم اطلاعات آنها را بردارند. این قدم ها عبارتند از:

- به مشتری از سیاست حریم بانک اطلاع داده شود، در صورت امکان در وب سایت بانک باشد. وضوح، زبان مختصر در این عبارت برای تضمین اینکه مشتری کاملا سیاست حریم را درک می کند، بسیار ضروری است. توصیفات طولانی، هر چند دقیق، این احتمال را ایجاد می کنند که مشتریان زیادی آن را مطالعه نکنند.
- به مشتریان اطلاع داده شود که بایستی از کلمه عبور، شماره شخصی هویت، و باقی داده های شخصی یا بانکی استفاده کنند.
- به مشتریان اطلاعاتی در مورد عموم امنیت کامپیوتر شخصی آنها، شامل عواید استفاده از نرم افزارهای حفاظت در مقابل ویروس، کنترل های دسترسی فیزیکی و دیوار های آتش شخصی برای ارتباط های استاتیک اینترنت داده شود.

ضمیمه 6: روش های مناسب، تداوم کسب و کار و برنامه ریزی احتمال برای بانکداری الکترونیکی

1. تمام سرویس ها و برنامه های کاربردی بانکداری الکترونیکی، شامل آنهایی که تامین کننده سرویس شخص

ثالث ارائه میشود، بایستی برای بحران مشخص شده و ارزیابی گردد.

2. ارزیابی ریسک برای هر کدام از سرویس های بانک داری الکترونیکی و برنامه های کاربردی آن، شامل دلالت پتانسیل هر کدام از ریسک های در هم ریختگی های کسب و کار در کارت اعتبار بانک، بازار، شناوری، قانونی، عملیاتی و انکار بایستی اداره شوند.
3. معیار های کارایی برای هر کدام از سرویس های بانکداری الکترونیکی بحرانی و برنامه های کاربردی بایستی ایجاد شوند، و سطح های سرویس بایستی در مقابل این معیار ها مانیتور شوند. معیار های مناسب بایستی برای تامین اینکه سیستم های بانکداری الکترونیک میتوانند تراکنش های با حجم بالا و پایین را برطرف کنند و اینکه کارایی سیستم ها و ظرفیت آنها با انتظارهای بانکی برای نمو آینده در بانکداری الکترونیک، استوار است، برگزیده شود.
4. بایستی به توسعه روش های دیگری برای مدیریت تقاضا وقتی سیستم بانکداری به نقطه تعریف شده ظرفیت می رسد، توجه شود.
5. پیوستگی کسب وکارهای بانکداری الکترونیک بایستی فرول بندی شده تا اعتماد بر تامین کنندگان سرویس شخص ثالث و هر کدام از وابستگیهای خارجی دیگر که برای رسیدن به بازیافت لازم است، ارائه شود.
6. طرح های احتیاطی بانکداری الکترونیکی بایستی برای فرآیندهایی جهت دوباره ذخیره سازی یا جایگزینی توانایی های فرآیندی، ساخت مجدد اطلاعات تراکنش پشتیبانی، و شامل اندازه گیری برای انجام دسترسی به سیستم های بانکداری الکترونیکی بحرانی و برنامه های کاربردی در رویدادهای آشفتگی کسب و کار بایستی تنظیم گردد.

فهرست منابع

[1] Risk Management Principles for Electronic Banking May 2001,Basel Committee on Banking Supervision

گروه بانکداری الکترونیکی باسل درنظارت بانک ها :

Chairman:
Mr John Hawke, Jr - Comptroller of the Currency, Washington DC
Members:
Commission Bancaire et Financière, Belgium Mr Jos Meuleman
Mr Koen Algoet
Office of the Superintendent of Financial Institutions, Canada Ms Judy Cameron
Mr Brad Sullivan
Commission Bancaire, France Mr Alain Duchâteau
Mr Jerôme Deslandes
Bundesaufsichtsamt für das Kreditwesen, Germany Mr Stefan Czekay

Deutsche Bundesbank, Germany Ms Magdalene Heid
Mr Andi Kloefer
Banca d'Italia, Italy Mr Filippo Siracusano
Financial Supervisory Agency, Japan Mr Kazuo Kojima
Mr Tadaaki Kawamura
Bank of Japan, Japan Mr Toshihiko Mori
Mr Hiroaki Kuwahara
Ms Tomoko Suzuki
Commission de Surveillance du Secteur Financier, Luxembourg Mr David Hagen
Mr Claude Bernard
De Nederlandsche Bank N.V., The Netherlands Mr Erik Smid
Banco de España, Spain Ms Maria Jesús Nieto
Financial Supervisory Authority, Sweden Mr Jan Hedqvist
Federal Banking Commission, Switzerland Mr Daniel Schmid
Financial Services Authority, United Kingdom Mr Jeremy Quick
Ms Katy Martin
Office of the Comptroller of the Currency (OCC), Mr Hugh Kelly
United States Mr Clifford Wilke
Board of Governors of the Federal Reserve System, Ms Heidi Richards
United States Mr Jeff Marquardt
Federal Deposit Insurance Corporation, United States Ms Sandra Thomson
Mr John Carter
Federal Reserve Bank of New York, United States Mr George Juncker
Ms Barbara Yelcich
Mr Christopher Calabia
Mr Thomas Whitford
Secretariat, Basel Committee on Banking Supervision, Mr J-P Svoronos
Bank for International Settlements

Observers:

Australian Prudential Regulation Authority: Mr Graham Johnson
European Central Bank: Mr Michael Olsen
Hong Kong Monetary Authority: Mr Brian Lee
Monetary Authority of Singapore: Mr Enoch Ch'ng