شماره: مب/ ۳۲٤٤

تاریخ: ۱۳۸٦/۸/۳

«بسمه تعالی»

جهت اطلاع مدیران عامل محترم کلیه بانک‌های دولتی، غیردولتی، شرکت دولتی پست بانک و موسسه اعتباری توسعه ارسال گردید

با احترام؛

همان‌گونه که استحضار دارند از جمله مهم‌ترین ریسک‌هایی که تقریباً تمامی فعالیت‌های موسسه اعتباری در معرض آن قرار دارند، **ریسک عملیاتی** است. ریسکی که **ناشی از نامناسب بودن و عدم کفایت فرآیندها و روش‌ها، افراد و سیستم‌های داخلی و یا ناشی از وقوع رویدادهای خارج از موسسه اعتباری** است. تاثیرات این شاخه از ریسک گاه ممکن است به حدی گسترده باشد که به ورشکستگی موسسات اعتباری بیانجامد. از این‌رو، مراجع نظارتی و موسسات اعتباری در سراسر دنیا، تلاش‌های فراوانی را جهت شناخت دقیق و مدیریت موثر این ریسک آغاز نموده‌اند. اقدامات یاد شده در صدد تعریف و تبیین ریسک عملیاتی، پیش‌بینی رفتار و در نهایت کاهش آن هستند و در قالب سه محور "شناسایی، ارزیابی و اندازه‌گیری"؛ "پایش و گزارش‌دهی" و "کنترل و کاهش" ریسک عملیاتی پیگیری می‌شوند.

اگرچه اهمیتی که به این شاخه نسبتاً جوان ریسک داده می‌شود در درجه نخست، مرهون گستردگی حیطه عملکرد آن و تاثیرات بالقوه زیادی است که گاه ممکن است یک موسسه اعتباری را تا آستانه ورشکستگی سوق دهد لیکن پس از منظور نمودن مقادیری برای پوشش آن در نسبت کفایت سرمایه توافق‌نامه بال ۲، جایگاه این ریسک اهمیتی دو چندان یافت.

نظر به اهمیت و لزوم برخورداری بانک‌ها و موسسات اعتباری کشور از نظام مناسبی برای مدیریت اثربخش ریسک عملیاتی، به پیوست "**مجموعه رهنمودها برای مدیریت موثر ریسک عملیاتی**" جهت اجرا و فراهم‌سازی بستر لازم برای مدیریت موثر این ریسک ابلاغ می‌گردد. در این خصوص لازم است بانک‌ها و موسسات اعتباری غیربانکی، با طراحی سازمان مناسب و تمهید ساز و کارهای اجرایی لازم، زمینه اجرای موثر این بخشنامه را فراهم آورده، برحسن اجرای آن نظارت دقیق و مستمر نمایند.

شایان ذکر است که در تهیه این مجموعه، از منابع تخصصی فراوانی به خصوص اسناد کمیته نظارت بانکی بال (از جمله توافق‌نامه کفایت سرمایه بال ۲) استفاده شده است. از آنجا که رویکرد بانک مرکزی، هدایت تدریجی شبکه بانکی کشور به سمت پیاده‌سازی توافق‌نامه بال ۲ می‌باشد و اجرای محور اول این توافق‌نامه در زمینه کفایت سرمایه، منوط به کمی نمودن ریسک عملیاتی است، اجرای موثر این رهنمود بسیار ضروری می‌باشد.

در ضمن، مجموعه پیوست در بخش پایانی خود مشتمل بر الزامات احتیاطی مهمی است که تحت عنوان "مباحث ویژه مدیریت ریسک عملیاتی" تدوین شده‌اند. این مباحث شامل الزامات احتیاطی برای هریک از موضوعات "فرآیندها"، "ریسک قانونی (ریسک حقوقی)"، "کارکنان"، "محصولات و خدمات جدید"، "استمرار عملیات کاری"، "برون‌سپاری امور"، "سیستم‌های فن‌آوری اطلاعات"، "سیستم‌ها و خدمات پرداخت" و "شناسایی کافی مشتریان" است و اجرای موثر این رهنمود، مستلزم رعایت دقیق مفاد الزامات هریک از این مباحث می‌باشد.

با عنایت به مراتب فوق، خواهشمند است دستور فرمایند رهنمودهای پیوست ـ پس از اتخاذ تدابیر لازم در سطوح هیات مدیره و مدیریت ارشد ـ به تمامی واحدهای ذی‌ربط در آن بانک/موسسه ابلاغ و ضمن نظارت موثر برحسن اجرای آن ـ پس از مدت ٦ ماه ـ گزارشی از پیشرفت کار در زمینه مذکور برای این بانک ارسال شود./ص

اداره مطالعات و مقررات بانکی

حمید تهرانفر	**صدیقه رهبرشمس‌کار**
۳۸۱۶	**۳۸۳۱-۳**

بانک مرکزی جمهوری اسلامی ایران

مدیریت کل نظارت بر بانکها و موسسات اعتباری

مجموعه‌ی رهنمودها
برای
"مدیریت مؤثر ریسک عملیاتی"

آبان ۱۳۸۶

فهرست مطالب

عنوان **صفحه**

عنوان	صفحه

بسمه تعالی

مجموعه‌ی رهنمودها
برای
مدیریت مؤثر ریسک عملیاتی

۱- اهداف:

در اجرای موثر بند "ب" از ماده ۱۱ قانون پولی و بانکی کشور، مصوب تیرماه ۱۳۵۱ و اصلاحات پس از آن و به منظور کمک به حفظ و ارتقای کارآیی موسسات اعتباری از طریق تشویق آن‌ها به اتخاذ تدابیر لازم برای پیشگیری از بروز زیان‌های احتمالی ناشی از وقوع اختلالاتی که به هر دلیل ممکن است در فرآیند انجام عملیات رخ دهد و نیز اجتناب از بروز خساراتی که در صورت وقوع، به موجب تکالیف مقرر در بند "ج" ماده ۳۵ همان قانون مسئولیت جبران آن با موسسه اعتباری است، "مجموعه‌ی رهنمودها برای مدیریت موثر ریسک عملیاتی" که از این پس "رهنمود" نامیده می‌شود، تدوین می‌گردد.

۲- تعاریف:

گستره شمول تعاریف ذیل، محدود به این "رهنمود"می‌باشد:

۲-۱- موسسه اعتباری: بانک یا موسسه اعتباری غیربانکی است که تحت عناوین مذکور از بانک مرکزی جمهوری اسلامی ایران مجوز دریافت نموده، تحت نظارت این بانک قرار دارد.

۲-۲- مدیریت ارشد اجرایی: مدیرعامل/ اعضای هیات عامل و آن گروه از کارکنان ارشد موسسه اعتباری است که مستقیماً زیرنظر هریک از اعضای هیات‌عامل/ مدیرعامل قرارداشته، مسئولیت اجرای استراتژی‌ها و سیاست‌های مصوب هیات مدیره/ هیات عامل را حسب مورد برعهده دارند.

۳-۲- ریسک عملیاتی: احتمال بروز زیان ناشی از نامناسب بودن و عدم کفایت فرآیندها و روش‌ها، افراد و سیستم‌های داخلی و یا ناشی از رویدادهای خارج از موسسه اعتباری.

این تعریف شامل ریسک حقوقی (قانونی) نیزمی‌باشد، لیکن ریسک‌های شهرت و راهبردی را در بر نمی‌گیرد.

۴-۲- سیستم: ترکیبی از اجزا و قسمت‌های مختلف یک مجموعه است که به یکدیگر وابسته‌اند و روابط متقابل آن‌ها به شکلی خاص و در جهت اهداف مشخصی است.

سیستم در این رهنمود، شامل تمامی سیستم‌های دستی و رایانه‌ای و نیز شبکه‌های خدمات‌رسانی هم‌چون آب و برق و گاز، شبکه‌های ارتباطی و ... است که بروز هرگونه اختلال در آن‌ها بر روی ریسک عملیاتی موسسه اعتباری تاثیر می‌گذارد.

۵-۲- ریسک حقوقی (قانونی): احتمال بروز زیان ناشی از مشاوره یا مستندسازی نامناسب، اشتباهات حقوقی، تفاسیر و برداشت‌های متفاوت از قوانین و مقررات و همچنین عدم کفایت قوانین و مقررات موجود برای حل موضوعات حقوقی مبتلابه موسسه اعتباری و نیز تغییر قوانین و مقررات مزبور.

۶-۲- ریسک شهرت: احتمال بروز زیان در اثر از دست دادن حسن شهرت به دلایلی از جمله وضعیت نامطلوب مالی، تنزل رتبه اعتباری و یا از دست دادن اعتماد عمومی.

۷-۲- ریسک راهبردی (استراتژیک): احتمال بروز زیان ناشی از تدوین برنامه‌های راهبردی و عملیاتی نامناسب، ایجاد تغییر نامناسب در این برنامه‌ها، سازمان‌دهی یا تجدید سازمان‌دهی نامناسب موسسه و نیز پیاده‌سازی برنامه‌ای است که با عوامل درونی و برونی محیط ناسازگار بوده و می‌تواند بر درآمدها، سرمایه و حیات حرفه‌ای موسسه تاثیرگذار باشد.

۸-۲- برنامه راهبردی: برنامه‌ای است بلندمدت (برای یک دوره ۳ تا ۵ ساله) که تصویری کلی از اهداف، نگرش و جهت‌گیری عملیاتی موسسه اعتباری ارائه می‌دهد.

۹-۲- برنامه عملیاتی: برنامه‌ای است کوتاه مدت (حداکثر یک‌ساله) که چارچوب کلی عملیات هر موسسه برای پشتیبانی از اجرای برنامه راهبردی را مشخص نموده، برای هر واحد کاری، اجرای برنامه را زمان‌بندی می‌کند.

۱۰-۲- مدیریت ریسک عملیاتی: عبارت است از فرآیند شناسایی، ارزیابی و اندازه‌گیری، تجزیه و تحلیل و واکنش مناسب نسبت به ریسک عملیاتی و نیز نظارت (شامل پایش و گزارش‌دهی و ...)، مستمر بر آن با توجه به شرایط متغیر محیطی (اقتصادی، اجتماعی، سیاسی، تکنولوژیک و ...).

۱۱-۲- برون‌سپاری: به مفهوم استفاده موسسه اعتباری از خدمات شخص ثالث (اعم از وابسته یا غیر از آن) برای انجام مستمر برخی فعالیت‌ها در زمان حال یا آینده است.

برون‌سپاری می‌تواند انتقال اولیه یک فعالیت (یا بخشی از آن) از موسسه اعتباری به شخص ثالث، یا انتقال بعدی یک فعالیت (یا بخشی از آن)، از یک ارائه دهنده خدمات به شخص دیگر باشد.

۱۲-۲- استمرار عملیات کاری: توانایی موسسه اعتباری برای ادامه وظایف و خدمات خود ـ تحت هر شرایط ـ به طور مستمر و بدون وقفه.

۱۳-۲- مدیریت استمرار عملیات کاری: رویکرد جامعی است که تمامی فعالیت‌های موسسه اعتباری را در برگرفته، شامل خط مشی‌ها، استانداردها و رویه‌هایی است که اطمینان می‌دهند در صورت بروز اختلال، بعضی از عملیات خاص، شرایط خود را حفظ نموده، یا طی چارچوب زمانی معین، به شرایط عادی خود باز می‌گردند. هدف از مدیریت استمرار عملیات کاری، به حداقل رسانیدن آثار منفی عملیاتی، مالی، قانونی، شهرت ناشی از بروز اختلال می‌باشد.

۲-۱۴- برنامه‌ریزی استمرار عملیات کاری: به عنوان بخشی از مدیریت استمرار عملیات کاری، تدوین برنامه‌ای است مکتوب و جامع برای انجام اموری که رویه‌ها و سیستم‌های ضروری را جهت تداوم یا بازیابی عملیات موسسه اعتباری ـ در صورت بروز اختلال ـ مشخص می‌نماید.

۲-۱۵- سیستم پرداخت: سیستمی است که امکان استفاده از ابزارهای متنوع پرداخت را فراهم می‌نماید. ابزارهای پرداخت شامل کارت‌های پرداخت، چک و سایر ابزارهایی است که برای پرداخت، برداشت یا انتقال وجوه مورد استفاده قرار می‌گیرند.

۲-۱۶- حفظ امنیت اطلاعات: به مفهوم حفاظت از اطلاعات و حفظ امنیت و تهیه نسخه پشتیبان از آن‌ها، تحت شرایط عادی و اضطراری از طریق اقدامات اجرایی، فنی و ... می‌باشد.

۳- رویدادهای موثر در بروز ریسک عملیاتی:

از انواع رویدادهایی که می‌توانند زیان‌های عمده ناشی از ریسک عملیاتی را در پی داشته باشند، عبارتند از:

۳-۱- رویدادهای مربوط به فرآیندها و روش‌ها

- عدم کفایت یا نامناسب بودن رهنمودها، سیاست‌ها و رویه‌ها؛
- عدم کفایت ارتباطات و یا ایجاد وقفه در آن‌ها؛
- خطاهای مربوط به ورود اطلاعات؛
- عدم سازگاری فرآیندها و روش‌ها و یا ناکافی بودن آن‌ها؛
- مستندسازی ضعیف و ناقص اطلاعات مشتریان؛
- مستندسازی ضعیف و ناکافی امور حقوقی؛
- عدم کفایت کنترل‌های امنیتی؛

- نقض قانون، مقررات و عدم رعایت الزامات؛
- نامناسب بودن تغییرات انجام شده در فرآیندها، روش‌ها، ساختارها و ... ؛
- وجود نارسایی در برنامه‌های اقتضایی و یا احتیاطی از جمله برنامه‌های مربوط به استمرار عملیات کاری؛
- وجود نارسایی در مدیریت وثائق؛
- وجود نارسایی در مدیریت اجرائی، عرضه محصولات و فرآیندها.

۲-۳- رویدادهای مربوط به درون سازمان

- نقض دستورالعمل‌های داخلی، سیاست‌ها و رویه‌ها؛
- عدول از اختیارات واگذار شده؛
- سوء استفاده کارکنان سازمان شامل اختلاس، ارتشا، ارائه گزارش‌های غلط (عمدی یا سهوی به ویژه در مورد مانده حساب‌ها)، سرقت، مبادلات غیرقانونی به حساب شخصی خود، خیانت در امانت، جعل اسناد و چک‌ها، دسترسی غیرمجاز به حساب مشتریان، سوء استفاده از اطلاعات محرمانه مشتری، فعالیت‌های تجاری نامناسب به حساب بانک، حیف و میل اموال و دارایی‌ها، نادیده گرفتن مقررات، انتشار انواع ویروس‌های رایانه‌ای در رایانه‌ها و شبکه‌های رایانه‌ای، پولشوئی و ارائه محصولات فاقد مجوز.
- عدم کفایت تفکیک وظایف و کنترل‌های دوگانه؛
- عدم شفافیت وظایف و مسئولیت‌ها؛
- بی‌تجربگی کارکنان؛
- عدم برخورداری از کارکنان متخصص و پای‌بند به منشور اخلاقی موسسه؛
- عدم کفایت نظارت بر کارکنان؛
- نقض قوانین مربوط به سلامت و ایمنی کارکنان؛

۳-۳- رویدادهای مربوط به اختلالات کاری و نواقص سیستم

- عدم کفایت نحوه نگهداری و مدیریت سخت‌افزارها و نرم‌افزارها، شبکه و ارائه‌دهنده خدمت (Server)، اختلالات کاری و نارسایی سیستم‌های مختلف (رایانه‌ای و ...) از قبیل نواقص سخت‌افزاری و نرم‌افزاری، مشکلات مربوط به ارتباطات از راه دور، قطع برق، آب و گاز، استفاده از فن‌آوری‌های قدیمی و غیر استاندارد.

۴-۳- رویدادهای مربوط به خارج از موسسه

- اعمال مجرمانه مانند کلاهبرداری، سرقت، جعل، سوء استفاده از چک و جرایم رایانه‌ای؛
- عملکرد اشتباه فروشنده و اختلافات با فروشنده دارایی‌های مورد نیاز موسسه اعتباری (مانند تجهیزات، مستغلات و ...)؛
- عملیات تروریستی و ناآرامی‌های اجتماعی؛
- بلایای طبیعی مانند زلزله، آتش‌سوزی، سیل و ... ؛
- علل مختلف سیاسی، حقوقی و مقرراتی از جمله دعاوی مربوط به عملکرد استخدامی و ایمنی محیط کار (دعاوی مربوط به جبران خدمات کارکنان، فعالیتهای سازمان یافتهٔ نیروی کار، دعاوی ناشی از وجود تبعیض و مسئولیت عمومی، استخدام نامناسب کارکنان، جبران ناعادلانه خدمات کارکنان، سوء رفتار با کارکنان که به مواردی هم‌چون دعاوی حقوقی، استعفا و اعتراضات منجر شود و ...).

۴- محیط ریسک عملیاتی:

۱-۴- ساختار سازمانی برای مدیریت ریسک عملیاتی، وظایف و مسئولیت‌ها

مدیریت ریسک عملیاتی مستلزم مشارکت طیف گسترده‌ای از افراد و واحدهای سازمانی است. هریک از این افراد و واحدها، وظایف و مسئولیت‌های متفاوتی را در این زمینه برعهده دارند. لازم است هریک از افراد و واحدهای

مزبور، درک روشنی از وظایف، سطح اختیارات و مسئولیت‌های خود در ساختار سازمانی موسسه و نیز ساختار مدیریت ریسک آن داشته باشند. ایجاد واحدهای سازمانی و کمیته‌هایی ویژه در ساختار سازمانی موسسه اعتباری، به هیات مدیره و مدیریت ارشد در ایفای مسئولیت‌های خود در زمینه شناخت و مدیریت ریسک عملیاتی یاری می‌رساند.

۱-۱-۴-هیات مدیره، وظایف و مسئولیت‌ها

هیات مدیره می‌بایست به اهمیت نقش ریسک عملیاتی به عنوان شاخه مجزایی از ریسک که نیاز به مدیریت دارد آگاهی داشته، تدابیر لازم را برای مدیریت موثر آن اتخاذ نماید. مسئولیت نهایی مدیریت ریسک عملیاتی برعهده هیات مدیره می‌باشد.

وظایف و مسئولیت‌های هیات مدیره در رابطه با مدیریت ریسک عملیاتی شامل موارد ذیل است:

- تصویب راهبردها، سیاست‌ها و فرآیندهای کلی ریسک عملیاتی و نیز شیوه مدیریت آن در چارچوب استراتژی کلی موسسه اعتباری؛
- تصویب میزان ریسک‌پذیری موسسه در زمینه ریسک عملیاتی؛
- بررسی و تصویب رویکردهای پیشنهادی کمیته عالی مدیریت ریسک (موضوع پیوست شماره ۲ بخشنامه شماره ۱۱۷۲ مورخ ۱۳۸٦/۳/۳۱) در زمینه شیوه مدیریت ریسک عملیاتی و ابلاغ رویکردهای مصوب به مدیریت ارشد جهت اجرا؛
- بررسی گزارش دریافتی از کمیته حسابرسی در مورد بازبینی و ارزیابی کفایت فرآیند حسابرسی داخلی و رفع نارسایی‌های کشف شده؛
- بررسی و تصویب استراتژی‌ها (راهبردها)، خط مشی‌ها و رهنمودهای پیشنهادی از سوی کمیته حسابرسی و کمیته عالی مدیریت ریسک؛
- حصول اطمینان از این که واحد حسابرسی داخلی به طور منظم، کفایت و جامعیت مدیریت ریسک عملیاتی موسسه را مورد ارزیابی قرار می‌دهد؛

- **تصویب نظام مدیریت ریسک عملیاتی موسسه و بازنگری ادواری یا موردی آن (حسب ضرورت)؛**

  این نظام می‌بایست ضمن ارائه تعریفی شفاف، دقیق و جامع از ریسک عملیاتی، در مورد نحوه مدیریت (شناسایی، ارزیابی، پایش، گزارش‌دهی و کنترل/کاهش) آن، رهنمودهای لازم را ارائه نماید؛
- **تصویب و بازنگری ادواری (و یا موردی) چارچوب حاکمیت شرکتی موسسه اعتباری به منظور مدیریت شفاف ریسک عملیاتی؛**
- **تصویب سیاست‌های کلی در زمینه مستندسازی اقدامات کنترلی و فعالیت‌های مربوط به مدیریت تراکنش‌ها و حصول اطمینان از اجرای آن‌ها؛**
- **تصویب خط مشی‌های افشای اطلاعات مربوط به ریسک عملیاتی موسسه اعتباری در چارچوب قوانین و مقررات و بازنگری ادواری و یا موردی آن‌ها؛**
- **تصویب خط مشی‌های لازم درخصوص محصولات و خدمات جدید و بازنگری دوره‌ای آن (به ضمیمه شماره ٤-٦ از مباحث ویژه مدیریت ریسک‌عملیاتی رجوع شود)؛**
- **تصویب خط مشی‌های لازم برای مدیریت ریسک عملیاتی فعالیت‌هایی که برون‌سپاری می‌شوند (به ضمیمه شماره ٦-٦ از مباحث ویژه مدیریت ریسک‌عملیاتی رجوع شود)؛**
- **حصول اطمینان از این که برای مدیریت ریسک عملیاتی، برنامه‌ها و رویه‌های مناسبی وجود دارد؛**
- **حصول اطمینان از استقرار نظام جامعی از کنترل‌های داخلی در موسسه اعتباری (موضوع بخشنامه شماره مب/١١٧٢ مورخ ١٣٨٦/٣/٣١)؛**
- **حصول اطمینان از وجود فرهنگ سازمانی مناسب و توانمند برای مدیریت کارآمد ریسک عملیاتی و تاکید بر اجرای کنترل‌های داخلی مناسب در موسسه اعتباری؛**
- **حصول اطمینان از این که نظام مدیریت ریسک عملیاتی، تحت حسابرسی داخلی جامع و کارآمدی قرار دارد که به وسیله کارکنان شایسته ـ برخوردار از استقلال عمل و آموزش مناسب ـ انجام می‌شود؛**

- حصول اطمینان از این که مسئولین حسابرسی داخلی به طـور مسـتقیم در فرآیند مدیریت ریسک عملیاتی مسئولیتی به عهده نداشته باشند؛
- حصول اطمینـان از ایـن کـه موسسـه اعتبـاری از اصـول مناسـبی بـرای شناسایی، ارزیابی، پایش، گزارش‌دهی، کاهش و کنترل ریسـک عملیـاتی استفاده می‌کند؛
- حصول اطمینان از وجود برنامه‌های اقتضایی مناسب برای استمرار عملیات کاری و بازنگری ادواری آن‌ها (بـه ضـمیمه شـماره ٥-٦ از مباحـث ویـژه مدیریت ریسک‌عملیاتی رجوع شود)؛
- حصول اطمینان از استقرار یک نظام موثر و کارآمد گزارش‌دهی در سرتاسر موسسه اعتباری و این که اطلاعات شفاف، جـامع، مـرتبط، قابـل اعتمـاد، قیاس‌پذیر و مهم مربوط به حوزه‌های مختلف کاری موسسـه اعتبـاری بـه موقع، در اختیار کاربران ذی‌ربط قرار می‌گیرد؛
- حصول اطمینان از این که مدیریت ارشد و نیز تمامی افـرادی کـه مسـئول مدیریت ریسک عملیاتی هستند ضمن آگاهی کامل به ریسک‌های عملیاتی عمده در حوزه‌های کاری خود، از وظایف و مسئولیت‌های خود در این زمینـه مطلع بوده و نیز از تجربه و دانش کافی در مورد وظایف محولـه برخـوردار می‌باشند. همچنین وظایف و مسئولیت‌های خود در رابطه با مدیریت ریسک عملیاتی را به شیوه مناسبی انجام می‌دهند؛
- حصول اطمینان از اجرای نظام مدیریت ریسک عملیاتی توسـط مـدیریت ارشد؛
- الزام مدیران ارشد اجرایی به ارائه گزارش جـامع و مکتـوب، درخصـوص مدیریت ریسک عملیاتی، حداقل هر شش مـاه یکبـار و نیـز ارائـه سـایر گزارش‌های مورد نیاز هیات مدیره.

۲-۱-۴- مدیریت ارشد، وظایف و مسئولیت‌ها

مسئولیت اجرای چارچوب‌های مصوب هیات مدیره و نیـز تعیـین خـط

مشی‌ها، فرآیندهای مدیریت ریسک عملیاتی درخصوص تمامی محصولات، فعالیت‌ها، فرآیندها و سیستم‌های مهم موسسه اعتباری برعهده مدیریت ارشد است.

اهم وظایف و مسئولیت‌های مدیریت ارشد در زمینه مدیریت ریسک عملیاتی به شرح ذیل است:

- تعیین و توسعه خط مشی‌ها، فرآیندها و رویه‌های اجرایی ذی‌ربط مدیریت ریسک عملیاتی در زمینه تمامی محصولات، خدمات، حوزه‌های کاری فرآیندها و سیستم‌های مهم موسسه اعتباری در چارچوب قوانین و مقررات؛
- اجرای استراتژی‌ها (راهبردها)، خط مشی‌ها و رهنمودهای پیشنهادی از سوی کمیته حسابرسی و کمیته عالی مدیریت ریسک که به تصویب هیات مدیره رسیده باشد؛
- ایجاد ساختار مدیریتی مناسب برای مدیریت موثر و کارآمد ریسک عملیاتی؛
- پیاده‌سازی نظام جامعی از کنترل‌های داخلی در موسسه اعتباری؛
- پیشنهاد راهبردها و سیاست‌های ذی‌ربط ریسک عملیاتی به هیات مدیره، جهت تصویب؛
- پیشنهاد خط مشی‌های لازم برای مدیریت ریسک عملیاتی فعالیت‌هایی که برون‌سپاری می‌شوند؛
- فراهم آوردن تمهیدات لازم برای اجرای برنامه‌های اقتضایی مربوط به ریسک عملیاتی از جمله برنامه‌های اقتضایی مربوط به استمرار عملیات کاری موسسه؛
- تعیین ساختار سازمانی برای مدیریت ریسک عملیاتی و ابلاغ مسئولیت‌ها و وظایف تمامی واحدها و افراد به آن‌ها؛
- ارزیابی میزان تناسب فرآیند مدیریت ریسک عملیاتی با نوع ریسک موجود در فعالیت واحد ذی‌ربط؛

- تلاش در جهت ایجاد فرهنگ سازمانی مناسب و توانمند ـ در گفتار و عمل ـ و تاکید بر اجرای کنترل‌های داخلی مناسب در موسسه اعتباری؛
- ارزیابی روایی فرآیند نظارت بر مدیریت ریسک عملیاتی؛
- حصول اطمینان از سازگاری سیاست‌های ریسک‌پذیری موسسه اعتباری با نظام جبران خدمات کارکنان آن، به گونه‌ای که مانع از نقض مقررات توسط کارکنان گردد؛
- اجرای سیاست‌های مصوب هیات مدیره در زمینه استقرار یک نظام موثر و کارآمد گزارش‌دهی در سرتاسر موسسه اعتباری؛
- فراهم آوردن تمهیدات لازم برای آموزش کارکنان در زمینه مدیریت ریسک عملیاتی؛
- حصول اطمینان از وجود هماهنگی و ارتباط موثر بین کارکنان واحد ریسک عملیاتی و کارکنان دیگر واحدهای ریسک و نیز بین آن‌ها و ارائه‌دهندگان خدمات در خارج از سازمان؛
- حصول اطمینان از رعایت الزامات افشای اطلاعات مربوط به ریسک عملیاتی؛
- دریافت گزارش‌های منظم درخصوص ریسک‌های عملیاتی و خسارات وارده؛
- ارزیابی منظم به هنگام بودن، صحت و مرتبط بودن رویه‌های مورد استفاده و نظام‌های گزارش‌گری.

۳-۱-۴-کمیته عالی مدیریت ریسک، وظایف و مسئولیت‌ها

کمیته‌ای است تخصصی که از سوی هیات مدیره موسسه اعتباری و به منظور یاری رسانیدن به آن (در امر نظارت بر مدیریت مؤثر ریسک‌هایی که موسسه اعتباری در معرض آن‌ها قرار دارد) تشکیل شده، در چارچوب اختیارات، مقررات، خط مشی‌ها و حدود وظایف تعیین شده از سوی هیات مدیره موسسه اعتباری انجام وظیفه می‌نماید (موضوع پیوست شماره ۲ بخشنامه شماره ۱۱۷۲ مورخ ۱۳۸٦/۳/۳۱).

اهم وظایف و مسئولیت‌های کمیته عالی مدیریت ریسک در رابطه با مدیریت ریسک عملیاتی، علاوه بر وظایف و مسئولیت‌های کلی مندرج در پیوست شماره ۲ بخشنامه شماره مب/۱۱۷۲ مورخ ۱۳۸٦/۳/۳۱ این بانک ـ به شرح زیر می‌باشد:

- **تدوین چارچوبی برای خط مشی‌ها، راهبردها و دستورالعمل‌های اجرایی ریسک عملیاتی با مشارکت کمیته فرعی مدیریت ریسک عملیاتی ـ پس از دریافت نظرات واحد اجرایی ریسک عملیاتی به منظور پیشنهاد به هیات مدیره. چارچوب پیشنهادی می‌بایست با خط مشی‌ها و راهبردهای کلی موسسه اعتباری سازگاری داشته و حتی‌الامکان سایر ریسک‌های مهم موسسه اعتباری را پوشش داده و به گونه‌ای شفاف، وضعیت ریسک عملیاتی را تبیین نماید.**
- **بررسی و پیشنهاد میزان تحمل ریسک عملیاتی به هیات مدیره جهت تصویب؛**
- **بررسی کفایت خط مشی‌ها و سیستم‌های مربوط به مدیریت ریسک عملیاتی و مطابقت خط مشی‌ها با سطح قابل قبول ریسک عملیاتی مصوب هیات مدیره؛**
- **بررسی وضعیت ریسک عملیاتی موسسه اعتباری، شرکت‌های تابعه و وابسته به آن، برحسب میزان ریسک‌پذیری مقرر، توسط هیات مدیره و در صورت لزوم، مشاوره با کمیته حسابرسی، مدیران واحدها، حسابرسان داخلی و مستقل در این زمینه؛**
- **بررسی و اظهارنظر درخصوص رویکردهای پیشنهادی کمیته فرعی مدیریت ریسک عملیاتی در مورد شیوه‌های مدیریت ریسک عملیاتی و ارائه پیشنهادها در این زمینه جهت تصویب هیات مدیره؛**
- **دریافت مستمر اطلاعات مربوط به برنامه‌های مدیریت ریسک عملیاتی، قبل از شروع و طی مراحل اجرایی؛**

- بررسی اهداف و راهبردهای پیشنهادی برای مدیریت ریسک عملیاتی و نیز اثربخشی خط مشی‌های مدیریت مالی و عملیاتی موسسه اعتباری و ارائه توصیه در این زمینه؛
- بررسی شیوه پایش و گزارش‌دهی عملکرد مدیریت ریسک عملیاتی؛
- بررسی سیاست‌ها، رویه‌ها و فرآیندهای پیشنهاد شده از سوی واحدهای ذی‌ربط در زمینه مدیریت ریسک عملیاتی تمامی محصولات، فعالیت‌ها، فرآیندها، سیستم‌های اصلی، برون‌سپاری فعالیت‌ها، برنامه‌های اقتضایی برای استمرار عملیات کاری و ارائه نقطه‌نظرات به هیات مدیره در این خصوص؛
- حصول اطمینان از رعایت چارچوب‌های مصوب هیات مدیره در زمینه مدیریت ریسک عملیاتی؛
- حصول اطمینان از مناسب بودن رویه‌های مدیریت ریسک عملیاتی؛
- بازبینی گزارش‌های ارائه شده از سوی مدیران ذی‌ربط در رابطه با ریسک عملیاتی موسسه اعتباری و بررسی اقدامات انجام شده از سوی آن‌ها برای اداره مؤثر ریسک‌های مزبور و ارائه پیشنهادهای لازم به هیات مدیره؛
- ارزیابی عملکرد نظام‌های کنترل داخلی و مدیریت ریسک عملیاتی، همکاری با کمیته حسابرسی برای بررسی گزارش‌های دریافتی مدیران ذی‌ربط در رابطه با اجرا، تصویب و کنترل آن و نیز گسترش نظام‌های کنترل داخلی؛
- بررسی موارد عمده تخطی از حدود مقرر برای ریسک عملیاتی، دریافت و اظهارنظر در مورد گزارش‌های توضیحی مدیران در این خصوص ؛
- بررسی توصیه‌های حسابرسان داخلی و مستقل در رابطه با مدیریت ریسک عملیاتی ؛

- شناسایی هریک از اجزای مدیریت ریسک عملیاتی که نیاز به بهبود دارند و انجام اقدامات اصلاحی لازم برای رفع نارسایی‌های موجود در آن‌ها؛
- بررسی پیشنهادهای مدیران ذی‌ربط در مورد چگونگی به حداقل رسانیدن خسارات (مستقیم و غیرمستقیم) ناشی از ریسک عملیاتی هریک از خطوط کاری موسسه، با توجه به فراوانی و شدت هریک از رویدادهای موثر بر ریسک عملیاتی ؛
- اطلاع‌رسانی به هیات مدیره موسسه اعتباری در مورد ریسک‌های عمده و بالقوه عملیاتی که موسسه اعتباری در معرض آن قرار دارد و نیز اثربخشی سیستم مدیریت ریسک عملیاتی؛
- ارائه گزارش به هیات مدیره در رابطه با نتایج حسابرسی‌های داخلی مربوط به ریسک عملیاتی و میزان مناسب بودن اقدامات انجام شده توسط واحدهای اجرایی.

۴-۱-۴- کمیته فرعی ریسک عملیاتی، وظایف و مسئولیت‌ها

به منظور بررسی موارد مرتبط با مدیریت ریسک عملیاتی، کمیته عالی مدیریت ریسک لازم است کمیته‌ای تحت عنوان « کمیته فرعی ریسک عملیاتی» ایجاد نماید (به پیوست شماره ۱ رجوع شود).

اعضای کمیته فرعی ریسک عملیاتی از میان مدیران و یا کارشناسان واحدهای ذیربط موسسه اعتباری و پس از دریافت نقطه نظرات مشورتی کمیته حسابرسی و کمیته عالی مدیریت ریسک، توسط هیات مدیره تعیین می‌شوند. توصیه می‌شود در ترکیب کمیته فرعی ریسک عملیاتی، عضو یا اعضایی از واحدهای ذیل نیز حضور داشته باشند:

- واحدهای اجرایی مدیریت ریسک؛

- **واحد فن‌آوری اطلاعات؛**
- **واحد حقوقی؛**
- **واحدهای مرتبط با منابع انسانی.**

کمیته فرعی ریسک عملیاتی در راستای پاسخگویی به کمیته عالی مدیریت ریسک وظایف زیر را بر عهده دارد:

- **نظارت بر ریسک عملیاتی در تمامی سطوح موسسه اعتباری و حصول اطمینان از رعایت حدود مصوب هیات مدیره؛**
- **پیشنهاد خط‌مشی‌های شفاف به کمیته عالی مدیریت ریسک در مورد روش‌های مدیریت ریسک عملیاتی، برون سپاری و استمرار عملیات کاری؛**
- **طراحی و پیشنهاد استراتژی‌های ریسک عملیاتی به کمیته عالی مدیریت ریسک، جهت تصویب در هیات مدیره؛**
- **بازبینی مستندات مربوط به فعالیت‌های در معرض ریسک عملیاتی؛**
- **ارائه پیشنهاد به کمیته عالی مدیریت ریسک درخصوص تفویض اختیارات لازم در موارد زیر:**
  - **تعیین حدود اختیارات سطوح مختلف، جهت تصویب منابع در معرض ریسک عملیاتی؛**
  - **تعیین حدود احتیاطی مربوط به منابع حایز اهمیت در معرض ریسک عملیاتی؛**
  - **تعیین معیارهای لازم برای برون‌سپاری و استمرار عملیات کاری.**
- **دریافت گزارش از واحدهای اجرایی ذی‌ربط در رابطه با اقدامات انجام شده در زمینه ریسک عملیاتی؛**
- **بازبینی نتایج حسابرسی‌های داخلی در رابطه با ریسک عملیاتی و**

تناسب اقدامات اصلاحی انجام شده از سوی واحدهای اجرایی با فراوانی، شدت و نوع ریسک عملیاتی؛

- ارایه گزارش به کمیته عالی مدیریت ریسک در رابطه با کفایت منابع (از جمله منابع انسانی) برای مدیریت موثر ریسک عملیاتی.

۵-۱-۴- واحد مدیریت ریسک عملیاتی، وظایف و مسئولیت‌ها

- به منظور کنترل و پایش این موضوع که منابع در معرض ریسک عملیاتی در چارچوب معیارها و حدود مصوب هیات مدیره قرار دارد و نیز برای تسهیل نظارت موثر بر مدیریت ریسک عملیاتی و حسن اجرای آن در فرایندهای کنترلی ذیربط، لازم است هیات مدیره، واحد اجرایی مدیریت ریسک عملیاتی را متناسب با اندازه، پیچیدگی و تنوع فعالیت‌های موسسه اعتباری ایجاد نماید.

این واحد اجرایی، تحت عنوان «واحد مدیریت ریسک عملیاتی» (به پیوست شماره ۱ رجوع شود.) ایجاد می‌شود. عمده وظایف این واحد به شرح ذیل است:

- پیگیری اجرای سیاست‌ها و حدود احتیاطی مقرر از سوی هیات مدیره در زمینه ریسک عملیاتی و حصول اطمینان از اجرای چارچوب‌های تعیین شده؛
- اجرای نظام‌ها و رویه‌های مرتبط با شناسایی ریسک، نظام اطلاعات مدیریت و نیز ایجاد نظامی برای ارائه هشدارهای اولیه و شناسایی و اصلاح به موقع نارسایی‌ها؛

- **انجام بررسی‌های لازم برای انتخاب رویکرد مناسب در رابطه با شیوه‌های مدیریت ریسک عملیاتی جهت پیشنهاد به کمیته عالی مدیریت ریسک؛**
- **دریافت گزارش‌های ادواری و به روز از سایر واحدهای اجرایی در مورد موضوعات مربوط به ریسک عملیاتی از جمله حفاظت فیزیکی و صیانت از اطلاعات، استمرار عملیات کاری، برون‌سپاری امور و تطبیق با ضوابط ذی‌ربط؛**
- **دریافت گزارش از واحد اجرایی مدیریت ریسک عملیاتی، در رابطه با آن گروه از رویدادهای درونی و بیرونی که ممکن است اثرات مهمی بر فعالیت‌های مدیریت ریسک عملیاتی داشته باشند؛**
- **مشارکت در تدوین چارچوب‌ها و دستورالعمل‌های مدیریت ریسک عملیاتی و ارزیابی آن‌ها به منظور تعیین شاخص‌های ریسک عملیاتی و ارایه پیشنهادهایی در زمینه کنترل و کاهش آن‌ها؛**
- **مشارکت یا ارایه پیشنهاد در زمینه سازماندهی نظام مدیریت ریسک عملیاتی واحدهای کاری مختلف بر اساس چارچوب‌ها و دستورالعمل‌های مقرر برای مدیریت ریسک عملیاتی؛**
- **ابلاغ خط مشی‌ها، رویه‌ها و روش‌های مدیریت ریسک عملیاتی به تمامی واحدهای کاری ذیربط ؛**
- **اطلاع رسانی کافی در زمینه مباحث مربوط به ریسک عملیاتی به منظور شناخت و آگاهی تمامی سطوح کارکنان موسسه اعتباری از مباحث مذکور؛**

- هماهنگی، مشاوره یا مشارکت در تهیه، آزمون و بررسی برنامه استمرار کاری برای یکایک واحدهای اجرایی و ارایه گزارش در مورد ریسک‌های مختلف به کمیته فرعی ریسک عملیاتی و مدیریت ذیربط؛
- مطالعه، پیگیری و توسعه دانش مربوط به ریسک عملیاتی در موسسه اعتباری به منظور گسترش و تجزیه و تحلیل فنون جدید مدیریت ریسک مذکور.

۶-۱-۴- کمیته حسابرسی، وظایف و مسئولیت‌ها

کمیته‌ای است تخصصی که از سوی هیات مدیره موسسه اعتباری و به منظور یاری رسانیدن به آن (در امر نظارت بر مسئولیت‌های آن‌ها در حیطه فرآیند گزارش‌گری مالی، نظام کنترل داخلی، فرآیند حسابرسی و فرآیند تطبیق با قوانین و مقررات و ضوابط اخلاقی) تشکیل شده، در چارچوب اختیارات، مقررات، خط مشی‌ها و حدود وظایف تعیین شده از سوی هیات مدیره موسسه اعتباری انجام وظیفه می‌نماید (موضوع پیوست شماره ۱ بخشنامه شماره مب/۱۱۷۲ مورخ ۱۳۸٦/۳/۳۱).

اهم وظایف و مسئولیت‌های کمیته حسابرسی در رابطه با مدیریت ریسک عملیاتی، علاوه بر وظایف و مسئولیت‌های کلی مندرج در پیوست شماره۱ بخشنامه شماره مب/۱۱۷۲ مورخ ۱۳۸٦/۳/۳۱ این بانک ــ به شرح زیر می‌باشد:

- نظارت بر فرآیند تهیه گزارش‌های سالانه و میان‌دوره‌ای در رابطه با ریسک عملیاتی؛
- همکاری با کمیته عالی مدیریت ریسک درخصوص ارزیابی محیط ریسک عملیاتی و چگونگی مدیریت آن و ارائه نظرات مشورتی در این خصوص به کمیته مذکور؛
- دریافت گزارش‌های منظم از واحد حسابرسی داخلی درخصوص هرگونه تغییر مهم در وضعیت ریسک عملیاتی و تشکیل جلسه با رئیس آن واحد، در صورت لزوم؛

- دریافت گزارش‌های توضیحی از مسئولین واحدهای ذی‌ربط درخصوص علل بروز تغییرات مهم در وضعیت ریسک عملیاتی موسسه؛
- بررسی گزارش‌های دریافتی و همکاری با کمیته عالی مدیریت ریسک درخصوص ارائه راهکارهای مناسب به منظور مدیریت موثر ریسک عملیاتی؛
- ارزیابی کفایت نظام کنترل داخلی موسسه برای مدیریت موثر ریسک عملیاتی؛
- ارزیابی کیفیت دستورالعمل‌های اجرایی مدیریت ریسک عملیاتی و همکاری با کمیته عالی مدیریت ریسک در رابطه با ارائه پیشنهادهای لازم به هیات مدیره؛
- بررسی و تبادل نظر با مدیران واحدهای ذی‌ربط ریسک عملیاتی در مورد مقدار منابع عمده در معرض ریسک مزبور و اقدامات انجام شده جهت نظارت و کنترل آن؛
- بررسی ریسک عملیاتی ناشی از معاملات غیر متعارف (ناشی از تخلفات عمدی و سهوی)، ازجمله با اشخاص وابسته؛
- بررسی سیاست‌های مدیریت ریسک عملیاتی و چگونگی شناسایی رویدادهای موثر در بروز ریسک مذکور و چگونگی مواجهه با آن‌ها و همکاری با کمیته عالی مدیریت ریسک برای ارائه پیشنهادهای لازم به هیات مدیره.

۷-۱-۴- واحد حسابرسی داخلی، وظایف و مسئولیت‌ها

واحد حسابرسی داخلی در ارزیابی اثربخشی، کارآیی و ارتقای استانداردهای کنترلی موسسه اعتباری و کمک به حفظ ثبات مالی آن، از اهمیت و جایگاه ویژه‌ای برخوردار است.

ساختار سازمانی واحد حسابرسی داخلی موسسه می‌بایست متناسب با اندازه، ویژگی‌ها، گستره و نوع فعالیت‌های موسسه اعتباری باشد. به منظور

افزایش اثربخشی فعالیت‌های کنترلی، حسابرسان داخلی شاغل در این واحد می‌بایست واجد ویژگی‌های ذیل باشند:

- **برخورداری از دانش کافی حسابرسی و تجربه لازم؛**
- **برخورداری از دانش کافی در مورد موضوعات و فعالیت‌هایی که تحت حسابرسی قرار می‌گیرند؛**
- **برخورداری از استقلال کافی برای انجام وظیفه؛**

برای تعریف استقلال، به بند ۲۱ از بخش "ب" نشریه اصول و ضوابط حسابداری و حسابرسی آئین رفتار حرفه‌ای (منتشره از سوی کمیته فنی سازمان حسابرسی) تحت عنوان احکام قابل اجرا در مورد حسابداران حرفه‌ای مستقل رجوع شود؛

- **برخورداری از دانش و توانمندی لازم برای انجام تجزیه و تحلیل، تصمیم‌گیری و مهارت‌های برقراری ارتباط از جمله نگارش و ارائه مطلب، به ویژه ارائه پیشنهاد در مورد حل مشکلات شناسایی شده؛**
- **شناخت کافی از اصول و ضوابط حرفه‌ای حسابداری و حسابرسی.**

واحد حسابرسی داخلی می‌بایست ضمن توجه به تمامی ریسک‌ها، کارآیی نظام مدیریت ریسک عملیاتی را ـ در زمینه‌های مرتبط با فعالیت‌های آن واحد ـ به طور مستمر مورد آزمون و ارزیابی قرار دهد.

اهم وظایف و مسئولیت‌های واحد حسابرسی داخلی در رابطه با مدیریت ریسک عملیاتی به شرح ذیل می‌باشد:

- **بررسی و تطبیق تراکنش‌های انجام شده با برنامه حسابرسی و تائید آن‌ها، به منظور ارتقای سیستم اطلاعات مدیریت؛**
- **مشارکت در ارتقای کارآیی فرآیند مدیریت ریسک عملیاتی موسسه اعتباری؛**
- **بررسی ریسک عملیاتی در حوزه‌های تعیین شده و براساس**

برنامه‌ها و معیارهـای مقـرر در دسـتورالعمل حسابرسـی و تهیـه گزارش‌های لازم در این خصوص همراه با ارائه پیشنهاد برای رفع مشکلات، به کمیتـه فرعـی مـدیریت ریسـک عملیـاتی و کمیتـه حسابرسی؛

- حصول اطمینان از انجام کامل و صحیح تمامی تراکنش‌ها مطابق با اختیارات مصوب و ارائه گزارش موارد عدم تطبیق؛
- حصول اطمینان از قابل اعتماد بودن گزارش‌های مالی و کنترلی؛
- حصول اطمینان از انجام اقدامات اصلاحی در مورد عملیات مغـایر با قوانین، مقررات و یا مصوبات هیـات مـدیره و خـط مشـی‌هـا و رویه‌های تعیین شده از سوی مدیریت ارشد؛
- بررسی و حصول اطمینان از این که سیستم حفاظت از دارایی‌ها در چارچوب مصوبات هیات مدیره قرار دارد؛
- حصول اطمینان از این کـه نظـام مـدیریت ریسـک عملیـاتی در حوزه‌های مختلف کاری، در انطباق بـا دسـتورالعمل‌هـای مصـوب وجود دارند.

۸-۱-۴- حسابرس مستقل، وظایف و مسئولیت‌ها

- منظور از حسابرس مستقل، شخص حقیقی یا حقوقی‌ای است که یا به طور مستقیم توسط مجمع عمـومی موسسـه اعتبـاری و یـا بـه طـور غیرمستقیم، توسط بـازرس قـانونی منتخـب مجمـع عمـومی بـرای رسیدگی و اظهارنظر پیرامون تمامی امور مالی و حسابداری موسسه و نیز انجام دیگر وظایف محوله انتخاب می‌شود.
- حسابرسان مستقل می‌بایست علاوه بر برخورداری از دانـش کـافی و تجربه لازم در زمینه‌های مرتبط و حفظ استقلال عمل در تمامی مراحل حسابرسی، از اهداف، استراتژی‌ها و زمینه‌های کاری موسسه اعتباری آگاهی کامل داشته باشند؛

- این اشخاص می‌بایست اطلاعات لازم و ضروری مورد نیاز سهامداران را تهیه نمایند. در این راستا لازم است حسابرسان مستقل، نظام‌های حسابرسی داخلی و مدیریت ریسک (از جمله مدیریت ریسک عملیاتی) را مورد بررسی و ارزیابی قرار دهند. حسابرسان مستقل می‌بایست با استفاده از روش‌های مختلف، مکفی و متناسب با شرایط تجاری و محیط کاری، به ارزیابی گزارش‌های مالی بپردازند.

۲-۴- فرهنگ ریسک عملیاتی

- استقرار و تعمیق فرهنگ مناسبی در زمینه مدیریت ریسک عملیاتی، زمینه اثربخشی مدیریت این ریسک را فراهم می‌آورد. هیات مدیره و مدیریت ارشد وظیفه دارند، ضمن گسترش این فرهنگ در تمامی موسسه اعتباری، از آن در گفتار و عمل حمایت نمایند. تمامی کارکنان نیز وظیفه دارند از نقش خود در زمینه ریسک عملیاتی آگاهی داشته، مسئولیت‌های خود را در این خصوص به نحو احسن انجام دهند.

مهم‌ترین عواملی که به ایجاد فرهنگ مناسبی در زمینه مدیریت ریسک عملیاتی یاری می‌رسانند عبارتند از:

- اهداف موسسه، میزان ریسک‌پذیری موسسه در زمینه ریسک عملیاتی، چارچوب مدیریت ریسک، نقش و مسئولیت برای اجرای چارچوب مزبور باید به وضوح برای تمامی کارکنان تبیین شود به گونه‌ای که هریک از افراد و واحدها به خوبی از وظایف و مسئولیت‌های خود، در رابطه با مدیریت ریسک عملیاتی مطلع باشند؛
- در فرهنگ ریسک عملیاتی باید بر معیارهای عالی اخلاقی تاکید شود. این فرهنگ می‌بایست به تمامی کارکنان و واحدهای موسسه ابلاغ شود. تدوین منشور اخلاقی و نیز اصول و ضوابطی برای انجام کار و پای‌بندی مدیریت به آن‌ها می‌تواند به تعمیق این فرهنگ در موسسه اعتباری یاری رساند؛

- اثربخشی فرهنگ ریسک عملیاتی منوط بـه حمایـت هیـات مـدیره و مدیریت ارشد از این فرهنگ ـ در گفتار و عمل ـ و پای‌بندی کارکنـان موسسه به هنجارها و ارزش‌هـای فرهنـگ مـذکور در تمـامی سـطوح سازمان است؛
- برخورداری از یک فرهنگ مناسب در زمینه مدیریت ریسـک عملیـاتی منوط به تفکیک روشن وظایف و مسئولیت‌ها در کلیه سـطوح موسسـه اعتباری است؛
- از الزامات یک فرهنـگ مناسـب ریسـک عملیـاتی، واگـذاری امـور و مسئولیت‌ها به افرادی است که در زمینه شغلی خود از دانش، تجربـه و تخصص کافی و نیز مهارت‌های فنی لازم برخوردارند؛
- حیطه اختیارات و مسئولیت‌های هریک از افراد و واحدها می‌بایست بـه گونه‌ای طراحی و تبیین شود که مانع از ایجاد انگیزه برای سوء استفاده از اختیارات محوله و نادیده گرفتن ارزش‌های فرهنگ ریسک عملیـاتی شود؛
- نظام حقوق و مزایای کارکنان موسسه اعتباری می‌بایست بـه گونـه‌ای طراحی و به اجرا در آید که انگیزه کارکنان در تخطی از اصول و ضوابط مدیریت ریسک عملیاتی (مواردی همچون اختلاس، ...) را بـه حـداقل ممکن کاهش دهد؛
- اثربخشی فرهنگ ریسک عملیاتی مسـتلزم اسـتقرار محـیط مناسـبی است که در آن، هریک از کارکنان بتوانند مسائل و مشکلات مربوط بـه ریسک عملیاتی را به راحتی و آزادانه به اطلاع افراد و واحدهای ذی‌ربط در موسسه برسانند.

۳-۴- اطلاعات، ارتباطات و نظام گزارش‌دهی

واحدهای مختلف موسسه اعتباری بـه انـواع متفـاوتی از اطلاعـات در رابطه با مدیریت ریسک نیاز دارند.

از عوامل مهم برای مدیریت موثر ریسک عملیاتی، ارائه به موقع گزارش‌های ادواری درخصوص وضعیت کلی این ریسک به سطوح ذی‌ربط تصمیم‌گیری و پایش و ارائه گزارش‌های موردی در رابطه با وقوع حوادث غیرمنتظره و تغییر در وضعیت ریسک موسسه می‌باشد.

تهیه به موقع گزارش‌های موردی برای تصمیم‌گیرندگان، این امکان را برای آن‌ها فراهم می‌آورد که به محض بروز زیان یا فراتر رفتن شاخص‌ها از آستانه مقرر (در قالب یک سیستم هشدار دهنده اولیه)، بتوانند به موقع اقدامات لازم را به عمل آورند.

اهم گزارش‌های موسسه اعتباری که می‌بایست به طور روشن و با جزییات مناسب تشریح شوند، به شرح ذیل می‌باشند:

- **عملکرد مالی؛**
- **وضعیت مالی (از جمله سرمایه، توانایی پرداخت بدهی‌ها و نقدینگی)؛**
- **راهبردها و روش‌های مدیریت ریسک؛**
- **مقدار منابع در معرض ریسک (شامل ریسک‌های اعتباری، بازار، نقدینگی، عملیاتی، قانونی و سایر ریسک‌ها)؛**
- **موارد مهم ریسک عملیاتی که موسسه در معرض آن قرار دارد و یا قرار خواهد گرفت؛**
- **وقایع مهم ریسک و مواردی که نیاز به اقدامات جبرانی و اصلاحی دارند؛**
- **وضعیت ریسک عملیاتی و تاثیر اقدامات انجام شده بر آن؛**
- **گزارش‌های موردی؛**
- **مواردی که از خط مشی‌های مقرر هیات مدیره ـ با مجوز یا بدون مجوز ـ انحراف ایجاد شده است؛**
- **خط مشی‌های حسابداری؛**
- **اطلاعات اصلی در زمینه امور کاری، مدیریت و حاکمیت شرکتی.**

- برای گردآوری، بررسی و تجزیه و تحلیل داده‌ها و اطلاعات آماری مختلف و ارائه گزارش‌های مناسب می‌بایست ابزارهای لازم در اختیار افراد و واحدهای ذی‌ربط موسسه اعتباری قرار گیرد؛
- لازم است تمامی فرآیندها و روش‌های انجام کار مستندسازی شده، در مورد هریک از فعالیت‌های موسسه، سوابق کافی نگهداری شود. این سوابق می‌بایست به گونه‌ای تهیه و نگهداری شوند که بتوان آن‌ها را به موقع در اختیار ناظران بانکی و دیگر افراد و مراجع ذی‌صلاح قرار داد؛
- لازم است با ایجاد یک نظام منطقی و جامع؛ داده‌ها، اطلاعات و گزارش‌های موجود در موسسه اعتباری طبقه‌بندی شده، برای هر طبقه ضمن تعریف افراد (به اعتبار شخص یا پست سازمانی) و واحدهای سازمانی مجاز، سطح دسترسی به طور دقیق تبیین شود؛
- دستیابی به اهداف موسسه اعتباری و استقرار نظام مناسبی برای مدیریت موثر ریسک عملیاتی، مستلزم وجود سیستمی اثربخش و مناسب از ارتباطات درتمامی موسسه است. ساختار سازمانی موسسه اعتباری باید به گونه‌ای باشد که جریان آزاد اطلاعات را در تمامی سطوح (از بالا به پایین، از پایین به بالا و در عرض سازمان) تسهیل نماید.

استقرار شبکه‌های ارتباطی موثر و توسعه مجاری ارتباطی در میان واحدهای گوناگون موسسه، از وظایف مهم هیات مدیره و مدیریت ارشد است. اطلاعاتی که در ارتباطات از بالا به پایین منتقل می‌شوند عموماً شامل اهداف، استراتژی‌ها، انتظارات، سیاست‌ها و رویه‌ها است؛ در حالی که در ارتباطات از پایین به بالا، معمولاً اطلاعات مربوط به عملکرد ریسک هر فعالیت منعکس می‌شود. در ارتباطات هم عرض نیز کارکنان به تبادل اطلاعات با یکدیگر می‌پردازند.

- شیوه ارتباط و نظام‌گزارش‌دهی در موسسه اعتباری می‌بایست به گونه‌ای طراحی و استقرار یابد که اطلاعات مربوط به ریسک عملیاتی موسسه به طور واضح، صحیح و به موقع در اختیار افراد و واحدهای ذی‌ربط قرار گیرد. اطلاعات

ارسال شده، می‌بایست از این ویژگی برخوردار باشد که هیات مدیره و مـدیریت ارشد با کمک آن‌ها بتوانند نسبت به اصلاح به موقع خط مشی‌های جاری و رفـع نارسایی‌های موجود در نظام مدیریت ریسک و نظام کنترلی اقدامات لازم را بـه عمل آورند؛

- لازم است هیات مدیره و مدیریت ارشد تدابیری اتخاذ نمایند تا موانع ارتبـاطی میان افراد را به حداقل ممکن کاهش دهند؛

عمده‌ترین این موانع شامل موانع ادراکی و شناختی، موانع ناشی از تـنش‌هـای اجتماعی، موانع ارزشی (ناشی از تفاوت‌های فرهنگی)، موانع زبانی (مثل احتمال تفسیر به رای یا برداشت‌های متفاوت)، موانع انگیزشی (ناشی از حـالات روانـی افـراد و هیجانـات روحی آن‌ها)، موانع ناشی از عدم اطمینان به منابع اطلاعاتی، موانع ناشی از عدم وضـوح علایم و دریافت علایم متناقض، کیفیت صدا و موانع ناشی از بـروز اخـتلال در ارتباطـات می‌باشند؛

- از جمله راهکارهایی که هیات مدیره و مدیریت ارشد می‌توانند بـه کمـک آن‌هـا فرآیند ارتباطات را بهبود بخشند عبارتند از:
  - بهبود اثربخشی و کارآیی سیستم ارتباطی و رفع نارسایی‌های آن با استفاده از سیستم بازخور موثر و مناسب؛
  - توجه به عواملی نظیر عوامل روحی، روانی و فرهنگی و اهتمـام بـه درک معانی در هنگام مطالعه ارتباطات بین افراد؛
  - توجه به موانع عمده ارتباطی نظیر تفاوت‌های فرهنگـی، زبـانی و انگیزشی و هم‌چنین ناهمـاهنگی‌هـای شـناختی و عوامـل ایجـاد اختلال در ارتباطات؛
  - اسـتفاده از شـیوه ارتباطـات دو جانبـه بـرای بهبـود فرآینـدها و سیستم‌های فرعی بازخور؛
  - شناسایی مراحل اصلی فرآیند پیچیده ارتباطات سازمان و علایم و نمادهای مورد استفاده در آن، برای بهبود و درک و تحلیل آن.

هرگونه تغییر در شیوه گزارش‌دهی، فن‌آوری اطلاعات، محتوا و مجرای ارائه گزارش‌ها و اثرات احتمالی آن‌ها بر ریسک عملیاتی موسسه و نیز شیوه تاثیر آن‌ها می‌بایست مورد بررسی قرار گرفته، به تائید مراجع ذی‌ربط رسانیده شود.

افشای اطلاعات مربوط به ریسک عملیاتی

- موسسه اعتباری می‌بایست در مورد ریسک‌های عملیاتی و حقوقی موارد لازم را افشا نماید. افشاهای مربوط به ریسک‌های عملیاتی باید شامل اطلاعات مربوط به انواع اصلی ریسک‌های مزبور و نیز هرگونه مشکل خاص و حایز اهمیت باشد و به اشخاص ذی‌ربط منعکس شود. در مواردی، ممکن است علاوه بر مدیران و کارشناسان موسسه، اطلاع‌رسانی در زمینه ریسک عملیاتی به عموم نیز ضرورت یابد.
- در ریسک حقوقی نیز موارد افشا، شامل رویدادهای حقوقی (از جمله اقدامات حقوقی در جریان) و بررسی و تخمین مطالبات احتمالی بالقوه‌ای است که تغییرات محیط قانونی و مقرراتی متوجه بانک می‌کند. لازم است در مورد شیوه مدیریت و کنترل ریسک‌های مزبور از سوی موسسه اعتباری، اطلاعات لازم ارائه شود.

۵- مدیریت ریسک عملیاتی شامل نظام‌ها و رویه‌ها برای شناسایی، ارزیابی و اندازه‌گیری؛ پایش و گزارش‌دهی؛ کنترل و کاهش ریسک عملیاتی؛

هر موسسه اعتباری صرف‌نظر از اندازه یا پیچیدگی‌های آن ـ می‌بایست چارچوبی را برای مدیریت ریسک عملیاتی ایجاد نماید. هدف این چارچوب، حصول اطمینان از این موضوع است که ریسک‌های عملیاتی به شیوه‌ای سازگار و به طور جامع مورد شناسایی، ارزیابی و اندازه‌گیری؛ پایش و کنترل (یا کاهش) قرار گرفته و گزارش

شوند. چارچوب ایده‌آل برای مدیریت پیشرفته ریسک عملیاتی در پیوست شماره (۲) ارائه شده است.

نظارت منظم بر وضعیت ریسک عملیاتی موسسه اعتباری و وجوه عمده‌ای که در معرض زیان قرار دارند مستلزم به کارگیری فرآیندی موثر و کارآ از سوی هیات مدیره و مدیریت ارشد می‌باشد.

فعالیت‌های نظارتی منظم از این مزیت برخوردارند که نارسایی‌های موجود در خط مشی‌ها، فرآیندها و رویه‌های مربوط به اداره ریسک عملیاتی را به سرعت کشف و اصلاح می‌نمایند. پیگیری و شناسایی سریع این قبیل نارسایی‌ها می‌تواند به کاهش قابل ملاحظه فراوانی و یا شدت بالقوه زیان‌ها بیانجامد.

در این راستا، موسسه اعتباری باید نسبت به مدیریت موثر آن گروه از ریسک‌های عملیاتی که جزء تفکیک ناپذیر تمامی محصولات، فعالیت‌ها، فرآیندها و سیستم‌های مهم به حساب می‌آیند، اقدام نماید. علاوه بر این، لازم است قبل از معرفی و سپردن هرگونه تعهد درخصوص ارائه محصولات، فعالیت‌ها، فرآیندها، سیستم‌های جدید و یا برون‌سپاری امور، از وجود تمهیدات مناسب و مکفی برای مدیریت موثر ریسک عملیاتی موجود در این موارد، اطمینان حاصل نماید.

مدیریت ریسک عملیاتی از سه جزء ذیل تشکیل می‌شود:

۱-۵- شناسایی، ارزیابی و اندازه‌گیری ریسک عملیاتی؛

۲-۵- پایش ریسک عملیاتی و گزارش‌دهی؛

۳-۵- کنترل ریسک عملیاتی و کاهش آن.

۱-۵- شناسایی، ارزیابی و اندازه‌گیری ریسک عملیاتی

به منظور کنترل و محدود نمودن ریسک‌های عملیاتی، که جزء تفکیک‌ناپذیر تمامی محصولات، فعالیت‌ها، فرآیندها و سیستم‌های مهم می‌باشند، لازم است هیات مدیره و مدیریت ارشد اقدامات لازم را از جمله شناسایی، ارزیابی و اندازه‌گیری ریسک‌های بالقوه به عمل آورند.

هیات مدیره و مدیریت ارشد موسسه اعتباری می‌بایست اطمینان حاصل کنند که ریسک‌های عملیاتی موجود در فعالیت‌های موسسه، به طور منظم، حداقل یک‌بار در سال یا در مواقعی که وضعیت ریسک عملیاتی موسسه به دلایل مختلف تغییر می‌کند، مورد شناسایی، ارزیابی و اندازه‌گیری قرار می‌گیرند؛

- شناسایی ریسک‌های عملیاتی می‌بایست تمامی سطوح سازمانی موسسه اعتباری ـ از مدیریت تا کارکنان عملیاتی را ـ در بر گرفته و نیز در تمامی واحدهای کاری موسسه به اجرا درآید؛
- فرآیند شناسایی ریسک عملیاتی می‌بایست در چارچوب خط مشی‌ها و دیگر ضوابط تعیین شده از سوی هیات مدیره و مدیریت ارشد به اجرا در آید.

۱-۱-۵- ابزارهای شناسایی و ارزیابی ریسک عملیاتی

گام نخست در مدیریت موثر ریسک عملیاتی، شناسایی دقیق ریسک‌های عملیاتی موجود در تمامی سطوح موسسه، فرآیندها، فعالیت‌ها و محصولات آن است. در شناسایی ریسک‌های مزبور، می‌بایست به عوامل داخلی و خارجی مانند ساختار کاری، ساختار مدیریت موسسه، فرهنگ ریسک، شیوه مدیریت منابع انسانی، تغییرات سازمانی، میزان جابجایی کارکنان، ارائه محصولات جدید، موقعیت رقابتی، تحولات فن‌آوری و ... توجه شود. شناسایی، ارزیابی و اندازه‌گیری ریسک می‌تواند توسط کارکنان مجرب موسسه یا اشخاص ثالث و در چارچوب خط مشی‌های موسسه انجام شود. ابزارهای مناسب برای شناسایی، ارزیابی و اندازه‌گیری ریسک عملیاتی باید با ماهیت، حیطه کاری عملیات و میزان ریسک‌پذیری موسسه اعتباری سازگار باشد.

این ابزارها می‌توانند به طور انفرادی یا توامان مورد استفاده قرار گیرند. مصادیقی از ابزارهای شناسایی و ارزیابی ریسک عملیاتی در پیوست شماره (۳) ارائه می‌شود.

۲-۱-۵- اندازه‌گیری ریسک عملیاتی (روش‌ها)

پس از شناسایی ریسک‌های عملیاتی موجود در موسسه اعتباری ، فرآیندها و واحدهای کاری آن، با کمک روش‌ها و شاخص‌های مناسب می‌بایست مقدار منابع در معرض ریسک عملیاتی موسسه اندازه‌گیری شود.

با توجه به این که رویکرد بانک مرکزی جمهوری اسلامی ایران، اجرای استانداردهای کفایت سرمایه در توافق‌نامه بال ۲ می‌باشد و نیز به دلیل ضرورت منظور نمودن ریسک عملیاتی در محاسبه نسبت کفایت سرمایه، در رویکرد مذکور، لازم است موسسه اعتباری به هر روش ممکن ریسک‌های عملیاتی خود را کمی نماید. انتخاب روش برای این کار، به اندازه، حیطه و درجه پیچیدگی فعالیت‌های موسسه اعتباری بستگی دارد.

تاکید می‌گردد انتخاب هر روش منوط به تصویب هیات مدیره موسسه اعتباری است، مشروط بر آن که به تایید مرجع نظارتی (بانک مرکزی جمهوری اسلامی ایران) نیز رسانیده شود. در ضمن لازم است این نکته مورد توجه قرار گیرد که در صورت انتخاب روش پیشرفته‌تر برای محاسبه ریسک عملیاتی، موسسه اعتباری مجاز به تغییر آن به روش ساده‌تر نمی‌باشد. در شرایط خاص ـ ادغام و یا خرید شرکت‌های مجاز و یا تملیک ـ موسسه اعتباری می‌تواند پس از کسب موافقت مرجع نظارتی، تا زمان تطبیق خطوط کاری و فعالیت‌های شرکت(های) یادشده، ریسک عملیاتی آن شرکت(ها) را به روش ساده‌تر محاسبه کند. در پیوست شماره (٤) به دو روش از روش‌های متداول اندازه‌گیری پوشش سرمایه‌ای برای ریسک عملیاتی اشاره می‌شود.

۲-۵- پایش ریسک عملیاتی و گزارش‌دهی

پایش ریسک عملیاتی ابزاری است که به موسسه اعتباری کمک می‌کند تا قابلیت سیستم‌های کنترلی و کارآمدی آن‌ها را مورد ارزیابی قرار دهد. چنانچه سیستم‌های کنترلی موسسه از کارآیی مکفی برخوردار باشند وضعیت ریسک آن بهبود می‌یابد. از این رو، موسسه اعتباری می‌بایست دارای سیستمی مستمر و منسجم برای پایش ریسک‌های عملیاتی و گزارش‌دهی امور مربوط به ریسک باشد. بعضی از نکات مهمی که در این

رابطه می‌بایست مورد توجه قرار گیرند، به شرح ذیل می‌باشند:

- موسسه اعتباری می‌بایست با تمهید ساز و کارهای مناسب، امکان گردش اطلاعات و ارائه به موقع گزارش‌های مربوط به ریسک عملیاتی را به سطوح ذی‌ربط فراهم آورد؛
- گزارش‌های ریسک عملیاتی موسسه اعتباری می‌بایست دارای ویژگی‌هایی هم‌چون جامعیت، مرتبط و به موقع بودن، قابلیت اعتماد و قیاس‌پذیری بوده؛ از اهمیت لازم نیز برخوردار باشند. همچنین در این گزارش‌ها می‌بایست احتمال وقوع و فراوانی و شدت ریسک‌های عملیاتی هر یک از حوزه‌های فعالیت، فرآیندها و خدمات موسسه اعتباری و نیز شاخص‌های مربوط به اندازه‌گیری هر یک از ریسک‌های مذکور به دقت تعریف و مشخص شوند؛
- تعداد دفعات پایش ریسک، به روش‌ها و عوامل ریسک که توسط موسسه اعتباری تعیین شده است، بستگی دارد. در صورتی که عوامل ریسک عملیاتی به طور دائم و با سرعت دچار تغییر شوند لازم است پایش ریسک در فواصل زمانی کوتاه‌تر (به طور مثال روزانه یا هفتگی) انجام شود. چنانچه عوامل ریسک به طور جزئی و با روندی کند تغییر نمایند پایش ریسک به تشخیص مدیریت‌های ذی‌ربط و در فواصل زمانی پیشنهادی آن‌ها انجام می‌شود.

۳-۵- کنترل ریسک عملیاتی و کاهش آن

با کاهش احتمال وقوع رویدادهای ریسک می‌توان زیان‌های ناشی از ریسک‌های عملیاتی را تقلیل داد و از این طریق، آسیب‌پذیری موسسه اعتباری را نسبت به حوادث مزبور به حداقل ممکن کاهش داد. از آنجا که "ارزش زیان مورد انتظار"، نتیجه حاصل ضرب دو عامل "احتمال وقوع ریسک عملیاتی" و "خسارت ناشی از وقوع یا تاثیر ریسک" است، تقلیل هر یک از این دو عامل یاد شده، می‌تواند به کاهش ارزش زیان مورد انتظار بیانجامد. از این رو، در ارزیابی ریسک‌های عملیاتی، احتمال وقوع رویدادهای ریسک و خسارات ناشی از آن‌ها باید توسط واحدهای کاری ذی‌ربط محاسبه شوند؛

- موسسه اعتباری می‌بایست هم‌زمان با شناسایی، ارزیابی و اندازه‌گیری ریسک‌های عملیاتی، درخصوص شیوه کنترل آن‌ها نیز تصمیم‌گیری نماید. به عنوان مثال در این مورد تصمیم‌گیری کند که آیا مصمم است ریسک‌های مزبور را تحمل نماید یا آن‌ها را محدود کند یا از فعالیتی که موجب بروز این ریسک است، خارج شود؛

ارزیابی ریسک‌های عملیاتی مستلزم تجزیه و تحلیل عوامل درونی و بیرونی موسسه است. از جمله عوامل درونی می‌توان به تغییرات ساختاری و سازمانی، پیچیدگی محصولات، کیفیت نیروی انسانی و میزان جابجایی کارکنان اشاره نمود. پیشرفت‌های فنی و گسترش فعالیت‌های بین‌المللی، از جمله عوامل بیرونی تاثیرگذار بر ریسک عملیاتی موسسه اعتباری است؛

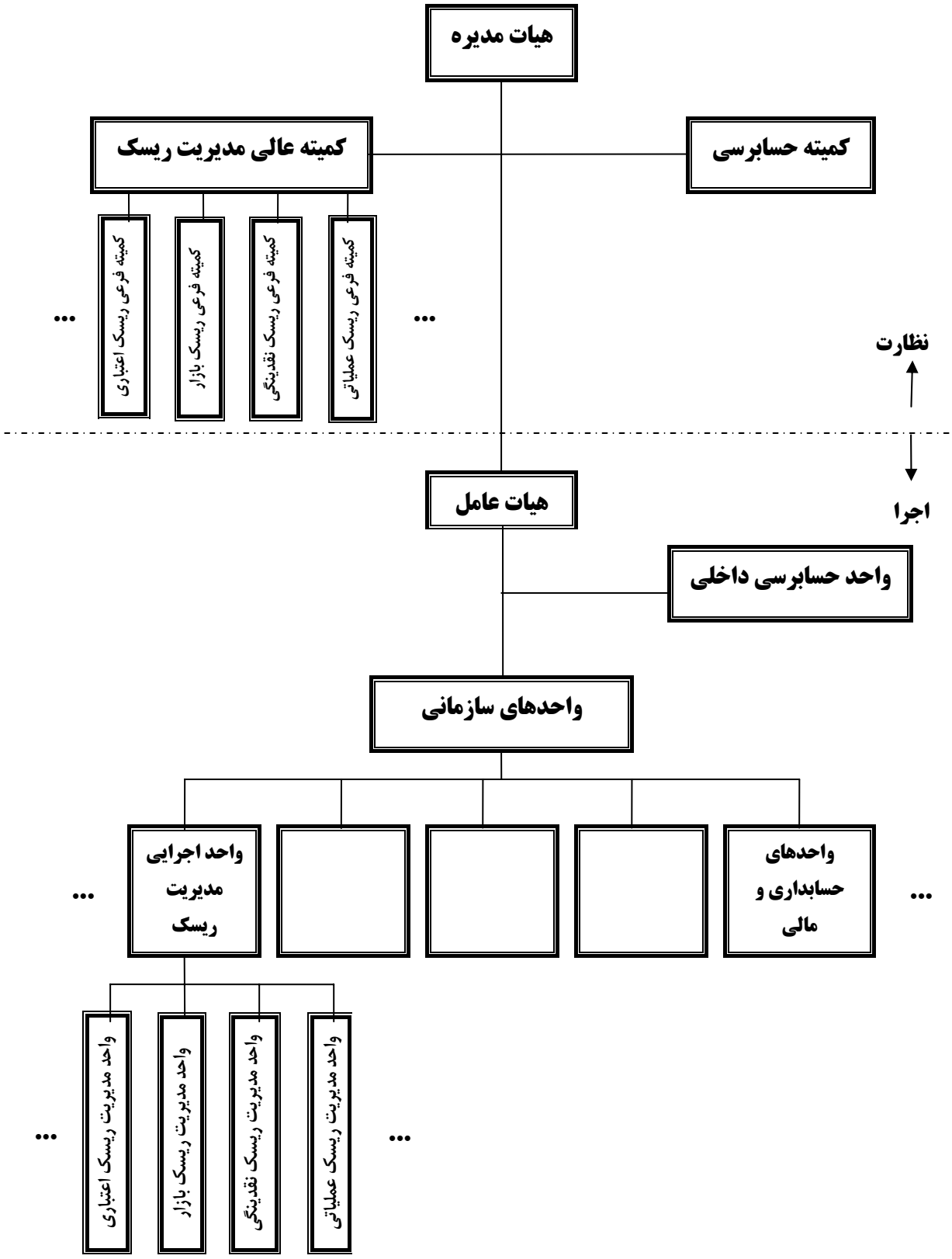
موسسه اعتباری می‌تواند ریسک عملیاتی خود را با کاهش هریک از دو عامل "احتمال وقوع و فراوانی" ریسک عملیاتی و "خسارت ناشی از وقوع یا تاثیر ریسک (شدت)" و یا تقلیل هم زمان هر دو عامل مزبور بهبود بخشد. روش موثر برای کاهش "احتمال وقوع و فراوانی" رویدادهای ریسک عملیاتی، تقویت نظام کنترل داخلی موسسه اعتباری است. برای کاهش "شدت" رویدادهای مزبور نیز، علاوه بر تقویت نظام کنترل داخلی موسسه، می‌توان برای استمرار عملیات کاری و بازگشت به حالت عادی برنامه‌ریزی نمود و یا با استفاده از روش‌هایی هم‌چون بیمه، تبدیل به اوراق بهادار کردن دارایی‌ها و ... ریسک را به شخص ثالث منتقل کرد.

- در صورت استفاده از بیمه برای پوشش ریسک عملیاتی موسسه، لازم است موارد ذیل مورد توجه قرار گیرند؛
- مدیریت ارشد باید ضمن توجه به روند تغییرات در فعالیت‌های موسسه، اطمینان حاصل کند پوشش بیمه‌ای از کفایت لازم برخوردار بوده؛ به طور منظم مورد ارزیابی قرار می‌گیرد؛
- هنگام استفاده از خدمات بیمه برای پوشش ریسک‌های عملیاتی، موسسه اعتباری می‌بایست ضمن ارزیابی اعتباری شرکت بیمه مورد نظر، از سلامت مالی و توانایی آن در ایفای تعهداتش اطمینان حاصل نماید؛

تمهید تدابیر لازم برای استمرار عملیات کاری ـ در صورت بروز هرگونه اختلال ـ از دیگر مواردی است که موسسه اعتباری می‌بایست به آن توجه ویژه‌ای داشته باشد.

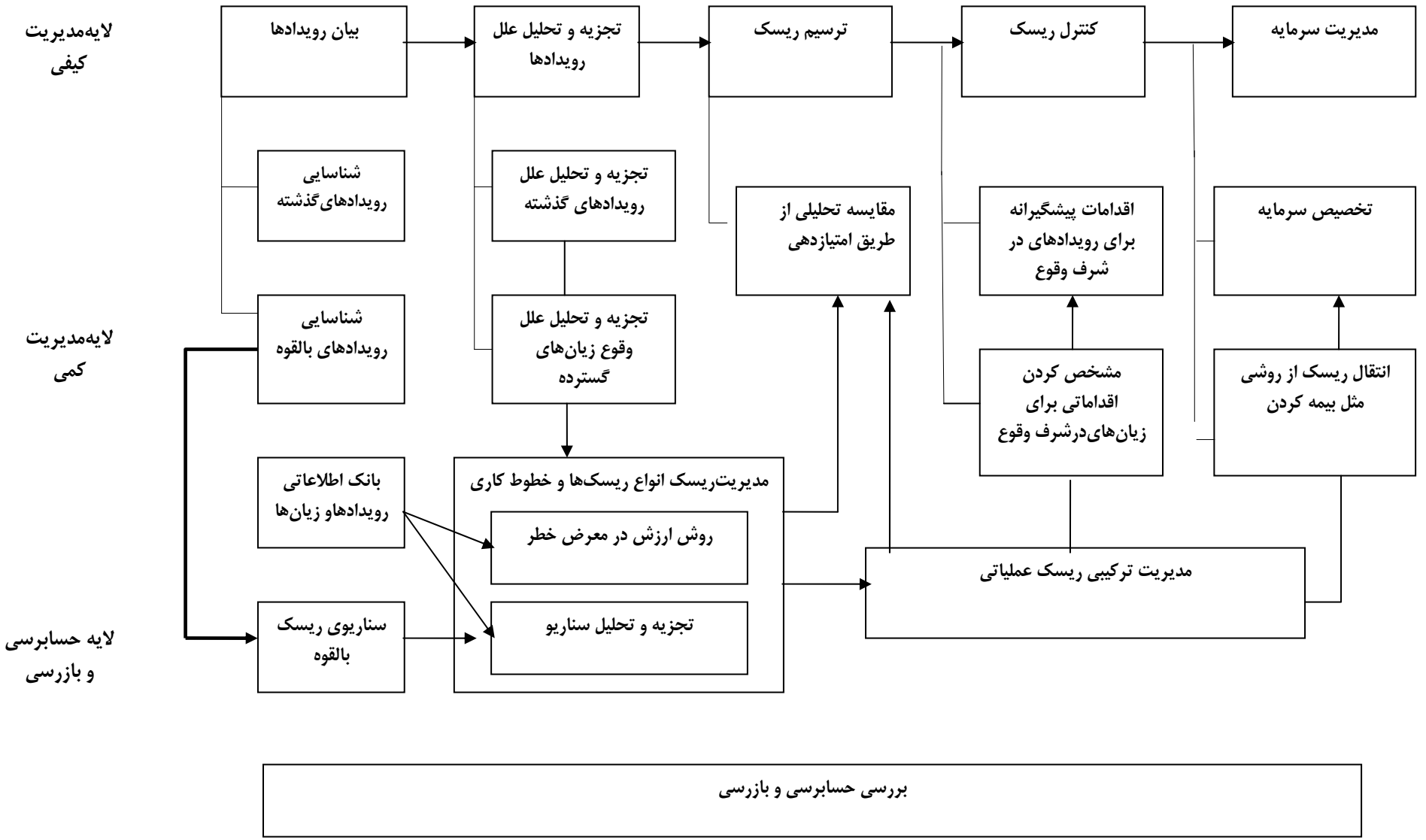
پیوست شماره ۱

جایگاه کمیته عالی مدیریت ریسک در ساختار سازمانی
موسسه اعتباری (نمونه ایده‌آل)



پیوست شماره ۲

چارچوبی برای مدیریت پیشرفته ریسک عملیاتی (نمونه ایده‌آل)



پیوست شماره ۳

ابزارهای شناسایی و ارزیابی ریسک عملیاتی

- **استفاده از بانک اطلاعاتی رویدادها و زیان‌های گذشته**

این بانک اطلاعاتی به موسسه اعتباری کمک می‌کند از احتمال وقوع و فراوانی و شدت ریسک عملیاتی واحدهای مختلف کاری آگاهی یافته، ریسک‌های عملیاتی را که در آینده ممکن است به وقوع پیوندد ـ در صورت عدم تغییر قابل ملاحظه عوامل محیطی ـ برآورد نماید.

گردآوری اطلاعات مربوط به زیان‌های گذشته می‌بایست جزییاتی از موارد ذیل را نیز در برگیرد:

- **انواع زیان‌ها؛**
- **علل، تاثیر و ارزش زیان؛**
- **سطح ریسک با توجه به احتمال وقوع و فراوانی و شدت آن؛**
- **واحد کاری مسئول؛**
- **دستورالعمل‌های موجود در رابطه با کنترل و کاهش ریسک.**

- **استفاده از روش خود ارزیابی**

هدف اصلی از این روش جمع‌آوری مجموعه‌ای جامع از انواع ریسک‌های عملیاتی جهت بهبود فرآیندهای مدیریت ریسک عملیاتی و ارتقای عملکرد موسسه است. از جمله ابزارهایی که در این شیوه به کار گرفته می‌شوند عبارتند از:

- **دریافت و جمع‌آوری نقطه‌نظرات کارکنان و واحدهای مختلف درخصوص انواع ریسک‌های عملیاتی بالقوه و موجود ذی‌ربط با استفاده از پرسش‌نامه؛**
- **تشکیل گروه‌های کاری برای شناسایی ریسک‌های عملیاتی بالقوه و موجود در محصولات، فعالیت‌ها، فرآیندها و سیستم‌ها؛**

- انجام مصاحبه با افراد و واحدهای ذی‌ربط، به منظور تکمیل نقطه‌نظرات جمع‌آوری شده در رابطه با انواع ریسک‌های عملیاتی بالقوه و موجود اثرگذار بر موسسه.

- **تجزیه و تحلیل سناریو**

در این روش، بر اساس فروض مختلف احتمالی؛ سناریوهای متفاوتی (برای آینده موسسه یا هر یک از فرآیندها و واحدهای کاری آن) تدوین می‌گردد و برای هر سناریو، ریسک‌های عملیاتی مربوط شناسایی شده؛ اثرات احتمالی آن‌ها مورد ارزیابی قرار می‌گیرند؛

- **تجزیه و تحلیل محیطی**

در این روش، موسسه اعتباری اقدام به شناسایی نقاط قوت و ضعف داخلی و نیز فرصت‌ها و تهدیدهای خارجی نموده، بر این اساس، ریسک‌های عملیاتی موجود در موسسه، فرآیندها و واحدهای کاری آن را مورد شناسایی قرار می‌دهد.

- **استفاده از روش امتیازدهی**

با استفاده از روش امتیازدهی، ارزیابی‌های کیفی به مقادیر کمی تبدیل می‌شوند و پس از ارزیابی فراوانی و شدت زیان‌های حاصله، با کمک این روش ریسک‌های عملیاتی مختلف از نظر میزان اهمیت؛ درجه‌بندی و اولویت‌بندی می‌گردند.

- **استفاده از روش ترسیم ریسک**

در این روش با استفاده از نمودارها، جداول (ماتریسی و ...) و ... ریسک‌های عملیاتی و نقاط ضعف موجود در فرآیندها و واحدهای کاری شناسایی شده، با توجه به آن‌ها اقدامات آتی مدیریت اولویت‌بندی می‌گردد. از مصادیق این روش می‌توان به موارد ذیل اشاره نمود:

- **نمودار جریان کار:** با ترسیم این نمودار، ریسک‌های عملیاتی مربوط به هر فعالیت و در هر مرحله از کار شناسایی شده، سپس با کمک علائم تعریف شده، بر روی آن مشخص می‌گردد؛
- **ماتریس ریسک:** با استفاده از این ماتریس، احتمال وقوع و فراوانی ریسک‌های عملیاتی و شدت اثرگذاری آن‌ها از نظر کیفی طبقه‌بندی شده، سپس نتایج حاصل از ترکیب‌های مختلف احتمال وقوع و فراوانی ریسک‌های عملیاتی و شدت اثرگذاری آن‌ها، در جدولی مانند جدول زیر ترسیم و ریسک‌ها اولویت‌بندی می‌شوند:

اولویت‌بندی ریسک‌های عملیاتی

(براساس ۹ ناحیه ریسک)

احتمال وقوع و فراوانی / شدت	کم	متوسط	زیاد
کم	ریسک کم	ریسک نسبتاً متوسط	ریسک متوسط
متوسط	ریسک نسبتاً متوسط	ریسک متوسط	ریسک نسبتاً زیاد
زیاد	ریسک متوسط	ریسک نسبتاً زیاد	ریسک زیاد

- به منظور اولویت‌بندی ریسک‌های عملیاتی موسسه و اتخاذ استراتژی مناسب برای مدیریت مؤثر آن‌ها، لازم است با ترکیب کیفی عوامل "احتمال وقوع و فراوانی" ریسک عملیاتی و "شدت" زیان‌های حاصله، ماتریسی با حداقل ٤ ناحیه تشکیل داد. نمونه‌ای از ماتریس مذکور در شکل زیر ترسیم شده است:

اولویت‌بندی ریسک‌های عملیاتی

(براساس ۴ ناحیه ریسک)

احتمال وقوع و فراوانی / شدت	کم	زیاد
کم	۱	۲
زیاد	۳	٤

منطقه (۱) مربوط به آن گروه از رویدادهای ریسک عملیاتی است که احتمال وقوع و نیز میزان تاثیر آن‌ها کم است (مانند قطع برق).

منطقه (۲) مربوط به آن گروه از رویدادهای ریسک عملیاتی است که احتمال وقوع آن‌ها زیاد است ولی میزان تاثیر آن‌ها بر موسسه کم است (مانند اشتباهات نیروی انسانی، عدم رعایت اصول حسابداری).

منطقه (۳) مربوط به آن گروه از رویدادهای ریسک عملیاتی است که احتمال وقوع آن‌ها کم است ولی میزان تاثیر آن‌ها بر موسسه زیاد است (مانند تاثیر بلایای طبیعی یا حوادثی مانند ۱۱ سپتامبر بر فعالیت تعدادی از موسسات اعتباری بین‌المللی).

منطقه (٤) مربوط به آن گروه از رویدادهای ریسک عملیاتی است که احتمال وقوع و نیز میزان تاثیر آن‌ها بر موسسه زیاد است.

ماتریس فوق، رهنمودی کیفی و اولیه برای اولویت‌بندی رویدادهای مربوط به ریسک عملیاتی موسسه اعتباری است.

موسسه اعتباری می‌بایست برای هر یک از نواحی ماتریس فوق، استراتژی مناسبی را تدوین و به اجرا درآورد. در این ارتباط می‌توان با انجام تقسیم‌بندی‌های بیشتر براساس دو عامل "احتمال وقوع و فراوانی" و "شدت"، نواحی بیشتری را در ماتریس "فراوانی ـ شدت" ایجاد نموده، استراتژی‌های دقیق‌تری را برای هریک از نواحی تدوین نمود.

نمونه‌ای از ماتریس "فراوانی ـ شدت" با تعداد نواحی بیشتر و همراه با تدابیر لازم برای هریک از نواحی آن در ذیل آمده است.

اولویت‌بندی ریسک‌های عملیاتی

(براساس ۱۶ ناحیه ریسک)

احتمال وقوع و فراوانی / شدت	بسیار کم	کم	زیاد	بسیارزیاد
بسیار کم	۱	۲	۳	٤
کم	٥	٦	۷	۸
زیاد	۹	۱۰	۱۱	۱۲
بسیار زیاد	۱۳	۱٤	۱٥	۱٦

استراتژی‌های موسسه اعتباری برای نحوه مواجهه با ریسک‌های عملیاتی
پس از اولویت‌بندی آن‌ها

	شماره ناحیه	احتمال‌وقوع‌وفراوانی‌رویداد	شدت	استراتژی
ناحیه ریسک‌های عملیاتی با درجه اهمیت جزئی	۱	بسیار کم	بسیار کم	اغماض نسبت به ریسک
	۲	کم	بسیار کم	تحمل ریسک
	۳	زیاد	بسیار کم	تحمل ریسک
	٤	بسیار زیاد	بسیار کم	کاهش ریسک
ناحیه ریسک‌های عملیاتی با درجه اهمیت متوسط	٥	بسیار کم	کم	تحمل ریسک
	٦	کم	کم	تحمل ریسک
	۷	زیاد	کم	کاهش ریسک
	۸	بسیار زیاد	کم	کاهش ریسک
ناحیه ریسک‌های عملیاتی حایز اهمیت	۹	بسیار کم	زیاد	کاهش ریسک
	۱۰	کم	زیاد	کاهش ریسک
	۱۱	زیاد	زیاد	عدم پذیرش ریسک
	۱۲	بسیار زیاد	زیاد	عدم پذیرش ریسک
ناحیه ریسک‌های عملیاتی حایز اهمیت بسیار (بحرانی)	۱۳	بسیار کم	بسیار زیاد	عدم پذیرش ریسک
	۱٤	کم	بسیار زیاد	عدم پذیرش ریسک
	۱٥	زیاد	بسیار زیاد	عدم پذیرش ریسک
	۱٦	بسیار زیاد	بسیار زیاد	عدم پذیرش ریسک

- **استفاده از شاخص‌های ریسک**

در این روش از مقادیری استفاده می‌شود که اغلب به صورت شاخص‌های مالی بیان می‌شوند و به شناخت از وضعیت ریسک عملیاتی موسسه کمک

می‌کنند. از مزایای این شاخص‌ها، برخـورداری از امکـان بـازنگری ادواری است. در استفاده از این ابزار، موسسات اعتباری باید توجه داشته باشند که شاخص‌های مزبور دارای ویژگی‌های ذیل باشند:

- **در مورد افزایش خطر زیان‌های آتـی، نقـش هشـدار دهنـده‌ای داشته باشند؛**
- **آینده نگر بوده، بتوانند علل بالقوه بروز ریسک عملیـاتی از قبیـل رشد سریع، ارائه محصولات جدید، نقل و انتقال کارکنان، فسـخ معاملات، از کار افتادن سیستم و ... را به موقع منعکس نماینـد. از جمله این شاخص‌ها می‌توان به تعداد معاملات نـاموفق، نـرخ نقل و انتقال کارکنان، فراوانی یا میزان اهمیت اشتباهات اشـاره نمود.**

پیوست شماره ۴

روش‌های اندازه‌گیری پوشش سرمایه‌ای برای ریسک عملیاتی

۱- روش شاخص پایه:

در این روش لازم است موسسه اعتباری شاخص‌های اصلی ریسک عملیاتی را در موسسه مشخص نماید. مقدار ریسک عملیاتی، معادل متوسط مجموع حاصل ضرب ضریب α در درآمد ناخالص موسسه، مشروط به مثبت بودن آن در هر سال، طی سه سال مالی متوالی است که از رابطه ذیل قابل محاسبه می‌باشد.

$$K_{BIA} = \left[\sum (GI_i \times \alpha) \right] / i, \quad ۱ \le i \le ۳, \quad i \in N \qquad \text{رابطه ۱)}$$

K_{BIA} = مقدار پوشش سرمایه‌ای ریسک عملیاتی در روش شاخص پایه؛[۱]

GI = درآمد ناخالص سالانه‌ـطی سه سال قبل ـ مشروط به مثبت بودن‌آن؛

i = تعدادسال‌ها از سه سال گذشته، که در آن، درآمد ناخالص مثبت است (حداقل یک و حداکثر سه سال).

در صورتی که درآمد ناخالص یک سال منفی یا صفر باشد، لازم است آن سال و درآمد ناخالص متناظر آن از محاسبه خارج شود؛

چنانچه درآمد ناخالص موسسه اعتباری، طی هیچ یک از سه سال گذشته مثبت نباشد، مرجع نظارتی (بانک مرکزی جمهوری اسلامی ایران) نسبت به تعیین پوشش سرمایه‌ای ریسک عملیاتی موسسه اقدام‌می‌نماید.

α =این‌ضریب که پس از انجام مطالعات میدانی در این مورد، توسط کمیته بال تعیین شده است، سطح سرمایه مورد نیاز را (با توجه به زیان احتمالی) نسبت به درآمد ناخالص موسسه بیان می‌کند و در حال حاضر ۱۵٪ است.

محاسبه درآمد ناخالص در رابطه فوق به شرح ذیل انجام می‌شود:

درآمد حاصل از سود بانکی

سود دریافتی ناشی از اعطای تسهیلات
وجه التزام
کارمزد وام قرض‌الحسنه

کسر می‌شود سود پرداختی به مشتریان

خالص درآمد حاصل از سود بانکی (۱) ⇐ × × × × × ×

---

۱ - Basic Indicator Approach.

درآمد حاصل از خدمات بانکی (۲)

کارمزد دریافتی بابت ارائه خدمات بانکی؛
(کسر می‌شود کارمزد پرداختی[۱])

سایر درآمدهای عملیاتی (۳)

خالص درآمدهای ناشی از معاملات ارزی؛
سود سهام و سرمایه‌گذاری در اوراق بهادار

در آمد ناخالص در محاسبه مورد نظر برابر حاصل جمع اقلام (۱) و (۲) و (۳) می‌باشد لازم است در محاسبات مذکور به موارد ذیل توجه گردد:

- ذخیره مطالبات مشکوک‌الوصول و هزینه‌های عملیاتی از مجموع درآمد ناخالص کسر نمی‌شوند؛
- سود و زیان غیرمترقبه و سود و زیان حاصل از فروش سرمایه‌گذاری‌ها و هرگونه سود و زیان غیرعملیاتی (خارج از فعالیت اصلی و عادی موسسه مندرج در بند "موضوع اساسنامه") در محاسبه درآمد ناخالص منظور نمی‌گردند.

۲- روش استاندارد شده:

در این روش، فعالیت‌های موسسه اعتباری به ۸ گروه کاری تقسیم می‌شود. ریسک عملیاتی هر خط کاری، از حاصل ضرب ضریب β متناظر در درآمد ناخالص هر خط کاری قابل احتساب است. چنانچه مجموع حاصل ضرب‌های درآمد ناخالص واحدهای کاری هشت‌گانه در ضرایب β متناظر آن‌ها منفی یا مساوی صفر گردد، برای آن عدد صفر منظور می‌شود. نحوه محاسبه در رابطه ذیل بیان می‌شود:

$$K_{TSA} = \left\{ \sum_{years\,۱-۳} Max\left[\sum \left(GI_{۱-۸} \times \beta_{۱-۸} \right), ۰ \right] \right\} / ۳$$ رابطه۲)

K_{TSA}[۲] = پوشش سرمایه‌ای در روش استاندارد شده

$GI_{۱-۸}$ = درآمد ناخالص سالانه یک سال مشخص، مطابق رویه‌ای که در روش شاخص پایه تعریف شده، برای هریک از ۸ خط کاری انجام شود.

۱- کارمزد پرداختی نباید از اقلام هزینه‌های عملیاتی باشند زیرا هزینه‌های عملیاتی از درآمد ناخالص کسر نمی‌شوند.

۲ - The Standardized Approach.

β = درصدی است ثابت که توسط کمیته بال تعیین شده است و سطح سرمایه مورد نیاز را (با توجه به زیان احتمالی) نسبت به سطح درآمد ناخالص هر واحد کاری مشخص می‌کند.

رابطه شماره (۲) به شکل ساده ذیل نیز قابل بیان است:

$$K_{TSA} = \left[\sum_{i=1}^{3} \sum_{j=1}^{8} (GI.\beta)_{ij} \right] / 3$$

i = تعداد سه سال متوالی از سنوات قبل؛

j = تعداد خطوط کاری (هشت خط)؛

GI = درآمد ناخالص هر خط کاری؛

β = مطابق تعریف ارائه شده در قبل؛

- چنانچه مجموع ($GI.\beta$) برای هشت خط کاری در یک سال مالی منفی باشد به جای عدد منفی، در رابطه فوق، عدد صفر قرار داده می‌شود.
- چنانچه درآمد ناخالص در یک خط کاری به واسطه عدم وجود مصادیق عملیات بانکی قابل محاسبه نباشد، به جای آن عدد صفر منظور می‌شود.

مقدار ضرایب با توجه به خطوط کاری به شرح ذیل است.

خطوط کاری	ضریب β
تامین مالی شرکتی	٪۱۸
فروش و بازرگانی	٪۱۸
بانکداری خرده	٪۱۲
بانکداری تجاری	٪۱۵
پرداخت و تسویه	٪۱۸
خدمات عاملیت	٪۱۵
مدیریت دارایی	٪۱۲
واسطه‌گری خرده	٪۱۲

- **لازم است موسسه اعتباری با تـدوین و گسـترش سیاسـت‌هـای مشخص، معیارهای مستندی را برای انطباق فعالیت‌هـای خـود بـا خطوط کاری یادشده در جدول فوق داشته باشد و نسبت به اصلاح معیارها در هنگام تحولات و تغییرات در فعالیت‌های تجاری اقـدام نماید. برای اطلاع از مصادیق خطوط کاری هشت‌گانه بـه پیوسـت شماره (۵) رجوع شود.**

پیوست شماره ۵

مصادیق فعالیت‌های خطوط کاری هشت‌گانه

مصادیق خطوط کاری هشت‌گانه به شرح ذیل اعلام می‌گردند:

۱- **تامین مالی شرکتی:** شامل مواردی مانند اعطای تسهیلات سندیکایی، اعطای تسهیلات به شرکت‌های بزرگ برای ادغام با دیگر شرکت‌ها، تعهدات ناشی از پذیره‌نویسی و ... ؛

۲- **فروش و بازرگانی:** شامل مواردی مانند فروش اقساطی، معاملات سلف، مشارکت حقوقی، معاملات ارزی، سرمایه‌گذاری‌ها و ... ؛

۳- **بانکداری خرد:** افتتاح انواع سپرده، اعطای انواع تسهیلات، صدور کارت‌های اعتباری و ارائه خدمات بانکی به اشخاص در مقیاس خرد؛

٤- **بانکداری تجاری:** افتتاح انواع سپرده، اعطای تسهیلات و ارائه خدمات بانکی به اشخاص در مقیاس کلان و در کلیه بخش‌های اقتصادی؛

٥- **پرداخت و تسویه:** ارائه انواع خدمات بانکی از قبیل پرداخت‌ها، دریافت‌ها، حواله‌ها، انتقال وجوه، صدور انواع چک. درخصوص مورد اخیر، خسارات ناشی از پرداخت‌ها و تسویه‌های مربوط به فعالیت‌های خود بانک می‌بایست در خسارات مربوط به خط کاری ذی‌ربط گنجانیده شود.

٦- **خدمات عاملیت:** قبول عاملیت توسط موسسه اعتباری برای اداره وجوه مشتریان، افتتاح سپرده قرض‌الحسنه ویژه و اعتبارات اسنادی(بانک گشایش‌کننده و کارگزار)، نگه‌داری امانات، ارائه خدمات مربوط به پذیره‌نویسی و انتشار اوراق مشارکت؛

۷- **مدیریت دارایی‌ها:** مدیریت وجوه صندوق بازنشستگی کارکنان؛

۸- **واسطه‌گری خرد:** -------

چنانکه فعالیت‌های موسسه اعتباری به گونه‌ای باشد که فاقد مصداق مشخصی برای یک یا تعداد بیشتری از خطوط کاری هشت‌گانه باشد لازم است در محاسبات مربوط به آن / آن‌ها عدد صفر برای درآمد ناخالص آن خط کاری منظور گردد.

۶- مباحث ویژه

مدیریت ریسک عملیاتی

ضمیمه شماره ۱-۶

الزامات احتیاطی

برای

فرآیندها

- لازم است تمامی فرآیندهای موسسه مورد تجزیه و تحلیل قرار گیرند تا مخاطرات عملیاتی مربوط به مراحل مختلف کار شناسایی شوند و برای کاهش آن‌ها تدابیر لازم اتخاذ شود.
- مدیریت فرآیندهای کاری توسط اشخاص ذی‌ربط باید به گونه‌ای انجام شود که ضمن جلب رضایت مشتریان، اثربخشی کار و جنبه‌های کیفی آن را افزایش دهد.
- لازم است موسسه اعتباری فرآیندهای مهم کاری خود را شناسایی نماید و تقابل بین واحدهای سازمانی درون موسسه و سازمآن‌های مختلف، روابط و فعالیت‌ها و پرداخت‌های برون‌مرزی را مورد توجه ویژه قرار دهد.
- برای رویدادهای با فراوانی زیاد و نیز تراکنش‌های حائز اهمیت، لازم است مستندسازی به حد کافی انجام شده، دستورالعمل‌های لازم تدوین گردد. این دستورالعمل‌ها در صورت لزوم می‌بایست مورد تجدیدنظر قرار گرفته، به هنگام شوند.
- لازم است فرآیندها، در مراحل مختلف، به ویژه در رابطه با تحولات مربوط به حیطه، موضوع عملیات و یا تغییرات آن کنترل شوند. کیفیت کنترل‌ها باید به طور منظم مورد ارزیابی قرار گیرند. مشارکت حداقل دو نفر برای اجرای تراکنش‌ها از مصادیق روش‌های کنترلی است.
- فرآیندهای مهم باید به طور مکتوب مستند شوند. این مستندات می‌بایست حتی‌الامکان به طور یکسان مواردی مانند وظایف مرتبط با فرآیندها، مراحل و وابستگی‌های متقابل آن‌ها، گردش اطلاعات، گزارش‌دهی، اشخاص ذینفع

فرآیند (مسئول فرآیند، مشتریان، کارکنانی که در فرآیند شرکت دارند، واحدهای سازمانی، سایر سازمآن‌ها یا طرف‌های ذینفع) و سیستم‌های مدیریت اطلاعات مربوط به فرآیندها را در برگیرند.

- **کارشناسانی که مراحل مختلف کار را اجرا می‌کنند می‌بایست موظف شوند فرآیند انجام کار را با دقت مکتوب نمایند. در صورت هرگونه تغییر در فرآیند، لازم است این توضیحات به هنگام شوند.**
- **برای اجرای پروژه‌های بزرگ لازم است اصول متحدالشکلی تدوین و رعایت شوند. در این گونه موارد، ارزیابی پروژه‌ها می‌بایست با فوریت بیشتری انجام شود.**

ضمیمه شماره ۲-۶

الزامات احتیاطی
برای
ریسک حقوقی

تمامی فعالیت‌های موسسه اعتباری ممکن است در معرض ریسک حقوقی قرار گیرند. تفسیر، حوزه اجرا و اعتبار قانونی مواد و مقررات قابل اجرا با عوامل نامطمئنی سر و کار دارند که می‌توانند سبب وارد آمدن زیان‌های قابل توجهی به موسسه اعتباری شده، مسئولیت حقوقی و تعهدات احتمالی را برای موسسه اعتباری در پی داشته باشند. علاوه بر این، اختلافات و تفاسیر متفاوت در رابطه با اعتبار و مفاد قراردادها ممکن است اثرات نامطلوبی بر فعالیت‌های موسسه اعتباری داشته باشد.

- هیات مدیره باید ریسک‌های حقوقی حایز اهمیت موسسه اعتباری را شناسایی نموده، اطمینان حاصل کند که مدیریت این ریسک‌ها به شیوه مناسبی انجام می‌شود؛
- مدیریت ارشد باید برای مدیریت موثر ریسک حقوقی، تدابیر لازم را جهت شناسایی، ارزیابی، پایش و کاهش ریسک حقوقی در خطوط کاری مختلف موسسه اتخاذ نماید؛
- موسسه اعتباری باید از قوانین و مقررات ناظر بر فعالیت‌های خود آگاهی کامل داشته باشد. به ویژه کارکنان آن می‌بایست بر این مقررات تسلط کافی داشته باشند؛
- مسئولیت‌های مربوط به مدیریت ریسک حقوقی می‌بایست به طور شفاف تبیین شوند؛
- به منظور مدیریت مناسب ریسک‌های حقوقی، موسسه اعتباری باید دانش و مهارت کافی در مورد شیوه انعقاد قراردادها و سایر تعهدات قانونی داشته باشد. به منظور حصول اطمینان از اعتبار قانونی قراردادها، موسسه اعتباری باید

از قوانین لازم‌الاجرا درخصوص حدود اختیارات تصمیم‌گیری اشخاصی که در انعقاد قرارداد شرکت می‌نمایند، اطلاع کافی داشته باشد؛

- **مستندسازی قرارداد باید به طور مناسب انجام شود. اعتبار قانونی قراردادها، احتمال تفاسیر متفاوت از آن‌ها و بروز اختلافات در این زمینه می‌بایست تحت پایش قرار گیرد؛**
- **لازم است موسسه اعتباری تغییرات مربوط به قوانین و مقررات را در سطوح ملی و بین‌المللی پیگیری نماید تا در چارچوب قوانین جاری کشور، برای انطباق با الزامات بین‌المللی جدید آمادگی داشته باشد؛**
- **موسسه اعتباری باید از شیوه قانونی زمینه‌های فعالیت خود آگاهی داشته باشد. علاوه بر این، شرکت‌های مادر باید اطمینان حاصل کنند که شرکت‌های تابعه و وابسته به آن‌ها، از قوانین و مقررات ناظر بر فعالیت‌های خود اطلاع دارند؛**
- **موسسه اعتباری که فعالیت‌های برون‌مرزی دارد باید به این موضوع توجه داشته باشد که اصول قانونی فعالیت‌ها و رویه‌ها در کشورها متفاوت است. از این‌رو، لازم است از قوانین و مقررات کشور میزبان آگاهی داشته باشد.**

ضمیمه شماره ۳-۶

الزامات احتیاطی
برای
کارکنان

- هیات مدیره و مدیریت ارشد می‌بایست اطمینان حاصل کنند که موسسه اعتباری از کارکنانی برخوردار است که واجد دانش، بینش، توانایی، مهارت و تجربه کافی در زمینه رویارویی با ریسک‌های عملیاتی مربوط به امور محوله به آن‌ها هستند.
- مدیریت ارشد باید اطمینان یابد که در صورت بروز هرگونه اختلال در روند عملیات موسسه، از کارکنان واجد شرایط کافی برای بازگرداندن به موقع امور به حالت عادی برخوردار است. در این زمینه می‌بایست تدابیر احتیاطی لازم برای جایگزینی افراد ذی‌صلاح (در صورت وقوع بیماری، حادثه، یا هرگونه رویداد غیرمنتظره دیگر) اتخاذ شود.
- هیات مدیره می‌بایست برای نظام‌های پاداش، اصول و ضوابطی را تصویب نماید. این اصول می‌بایست اطمینان دهند که جهت‌گیری نظام‌های پاداش، به گونه‌ای نیست که از رویه‌های نامطلوب و ریسک‌پذیری غیرقابل کنترل حمایت کنند.
- هیات مدیره و مدیریت ارشد موسسه اعتباری می‌بایست امکانات لازم را برای آموزش مباحث مربوط به شیوه مدیریت مؤثر ریسک عملیاتی، برای کارکنان در تمامی سطوح فراهم آورند.

ضمیمه شماره ۴-۶

الزامات احتیاطی
برای
محصولات و خدمات جدید

- موسسه اعتباری باید دستورالعمل‌هایی برای تبیین فرآیند ارائه محصولات و خدمات جدید داشته باشد. تصمیم‌گیری در مورد ارائه محصولات یا خدمات جدید باید منطبق با حدود اختیارات مقرر توسط هیات مدیره باشد و در هر مورد می‌بایست مستندات مربوط پیوست گردد.
- مخاطرات مربوط باید پیش از ارائه محصولات و خدمات جدید بررسی شوند. علاوه بر این، در زمان ارائه خدمات جدید و نیز زمانی که محصولات و خدمات با روشی جدید به طور هم‌زمان ارائه می‌شوند می‌بایست ارزیابی مجددی انجام گیرد.
- به منظور نظارت اثربخش، نظام‌های کنترل داخلی و مدیریت ریسک می‌بایست با توجه به ویژگی‌های مربوط به محصولات و خدمات جدید تعدیل و اصلاح شوند.
- زمانی که موسسه اعتباری فعالیت‌های خود را به بازارهایی که در آن فاقد تجربه بوده گسترش می‌دهد باید مراقبت ویژه به عمل آورد و از فعالیتی که از انجام آن منع شده است، خودداری نماید.
- برای ارائه محصولات و خدمات جدید، رعایت موارد ذیل الزامی است:
  - تشریح محصولات یا خدمات؛
  - انطباق محصولات یا خدمات جدید با راهبرد عملیاتی موسسه؛
  - مطالعه ریسک (ارزیابی ریسک‌های مربوط به محصول یا خدمت)؛
  - اجرای نظام کنترل داخلی و مدیریت ریسک (حداقل در مورد ریسک‌های اعتباری، بازار، نقدینگی و عملیاتی)؛
  - کنترل فرآیند مربوط به محصول یا خدمت (بازاریابی، شناسایی مشتری، فروش، تولید، تسویه و پرداخت‌ها)؛

- **بررسی مسائل حقوقی و اختیار انعقاد قرارداد؛**
- **کفایت سیستم‌های فن‌آوری اطلاعات، مبادله داده‌ها و امنیت اطلاعات؛**
- **کفایت رویه‌های حسابداری داخلی و مستقل؛**
- **بازبینی موضوعات مربوط به مالیات؛**
- **بازبینی قیمت‌گذاری، گزینه‌های موجود برای ارزش‌گذاری و مدل‌های قیمت‌گذاری؛**
- **ارزیابی تاثیر ارائه خدمات و محصولات جدید بر سودآوری و کفایت سرمایه؛**
- **بررسی نیازهای آموزشی کارکنان و وجود دستورالعمل‌های لازم در این خصوص.**

ضمیمه شماره ۵-۶

الزامات احتیاطی
برای
استمرار عملیات کاری

مدیریت استمرار عملیات کاری، بخش مهمی از مدیریت ریسک عملیاتی است. این فعالیت، رویکردی کل‌نگر به عملیات کاری داشته؛ شامل خط مشی‌ها، استانداردها و رویه‌هایی برای حصول اطمینان از این موضوع است که در صورت وقوع هرگونه اختلال، می‌توان عملیات ویژه را در شرایط عادی خود حفظ نمود و یا در یک الگوی زمانی مناسب، آن را به شرایط معمول خود بازگرداند. هدف از این فعالیت، به حداقل رساندن تبعات عملیاتی، مالی، قانونی، شهرت و دیگر پیامدهای مهمی است که از ایجاد اختلال ناشی می‌شود. مدیریت موثر استمرار عملیات کاری به جای تمرکز بر روی منشاء ایجاد اختلال، به تاثیر آن توجه می‌نماید. این امر به فعالان صنعت مالی و مراجع آن، این توانایی را می‌دهد که در پیگیری طیف وسیعی از اختلالات، از انعطاف لازم برخوردار باشند. هرچند سازمآن‌ها نمی‌توانند ماهیت ریسک‌هایی را که در معرض آن قرار دارند، نادیده بگیرند. به عنوان مثال، سازمآن‌هایی که در مناطق زلزله‌خیز قرار دارند معمولاً برای تاثیر اختلالات عملیاتی عمده‌ای که ناشی از زلزله است، برنامه‌ریزی می‌کنند. مدیریت موثر استمرار عملیات کاری معمولاً شامل تجزیه و تحلیل‌های تاثیر اختلالات، استراتژی‌های بازگشت عملیات به حالت عادی و برنامه‌های استمرار عملیات کاری و نیز برنامه‌هایی برای آزمون، آموزش و اطلاع‌رسانی، برنامه‌های مربوط به ارتباطات و مدیریت بحران است. در ذیل به اهم مواردی که می‌بایست در این خصوص مورد توجه موسسات اعتباری قرار گیرند اشاره می‌شود:

- موسسه اعتباری می‌بایست برای مدیریت استمرار عملیات کاری، رویکردهای موثر و جامعی داشته باشد. هیات مدیره و مدیریت ارشد، در زمینه استمرار عملیات کاری موسسه دارای مسئولیت جمعی هستند؛
- لازم است مدیریت استمرار عملیات کاری، بخش جدایی‌ناپذیری از برنامه کلی

مدیریت ریسک موسسه را تشکیل دهد. سیاست‌ها، استانداردها و فرآیندهای مربوط به مدیریت استمرار عملیات کاری می‌بایست در تمامی موسسه و یا حداقل، در عملیات مهم آن به اجرا درآیند. مدیریت جامع استمرار عملیات کاری باید نه تنها ابعاد فنی، بلکه جوانب انسانی را نیز در برگیرد؛

- هیات مدیره و مدیریت ارشد می‌بایست اطمینان یابند که برای گزارش موارد مربوط به استمرار عملیات کاری به آن‌ها، تدابیر لازم اتخاذ شده است. این موارد شامل گزارش‌های مربوط به وضعیت اجرا و پیاده‌سازی عملیات، وقایع روی داده، نتایج آزمون نظام مدیریت استمرار عملیات کاری و برنامه‌های عملیاتی مربوط به تقویت توان بازگشت عملیات موسسه به حالت عادی است. مدیریت استمرار عملیات کاری موسسه می‌بایست توسط یک شخصیت مستقل همچون حسابرسان داخلی یا مستقل مورد بازبینی قرار گرفته؛ یافته‌های مهم آن‌ها به موقع به اطلاع هیات مدیره و مدیریت ارشد بانک رسانیده شود؛
- وظایف، مسئولیت‌ها و اختیارات تمامی واحدها و کارکنان درخصوص استمرار عملیات کاری می‌بایست به دقت تعریف و مشخص شده، به آن‌ها ابلاغ شود. در صورت ایجاد اختلال در عملیات موسسه، می‌توان اقدام به تشکیل گروه مدیریت بحران؛ متشکل از مدیرانی نمود که براساس موضوع و متناسب با سطح مسئولیت مدیریتی آن‌ها انتخاب شده‌اند. لازم است مدیریت ارشد ـ متناسب با شدت اختلال ـ در ارائه واکنش مناسب به آن مشارکت نماید؛
- برنامه‌ریزی استمرار عملیات کاری، به مفهوم آمادگی برای رویارویی با قطع فعالیت‌های کاری است به گونه‌ای که موسسه بتواند به عملیات خود ادامه داده، زیان‌های ناشی از اختلالات مختلف کاری را کاهش دهد. این اختلالات ممکن است به دلیل صدمات وارده به کارکنان، ابزار کاری، سیستم‌های فن‌آوری یا مبادله اطلاعات، اقدامات بین‌المللی، خسارات ناشی از آب، آتش‌سوزی و فرسودگی تجهیزات باشند؛
- در برنامه‌ریزی استمرار عملیات کاری موسسه، با توجه به این که کدام یک از

فعالیت‌های بانک علی‌رغم بروز اختلال می‌تواند تدوام یابد می‌بایست برنامه‌هایی برای خطوط کاری مهم تدوین شود؛

- مسئولیت به هنگام نمودن و حصول اطمینان از کفایت برنامه‌های موسسه برای استمرار عملیات اصلی آن بر عهده هیات مدیره است. مدیریت ارشد باید برنامه‌ریزی استمرار عملیات کاری موسسه را برای کارکنان تبیین نماید؛
- موسسه اعتباری باید مدلی شفاف برای آمادگی، حفظ و آزمون برنامه‌های استمرار عملیات کاری آن و نیز برای کنترل برنامه‌ریزی مذکور داشته باشد؛
- برنامه‌ریزی استمرار عملیات کاری موسسه اعتباری، با ترسیم فرآیندهای کاری اصلی آن آغاز می‌گردد. در این برنامه‌ریزی، اولویت به فرآیندها داده می‌شود و حداقل زمان بازگشت به حالت عادی، برای این فعالیت‌ها، یا حداکثر زمان قابل قبول برای قطع آن‌ها ـ به گونه‌ای که اختلال قابل ملاحظه در آن فعالیت تلقی نشود ـ تعریف می‌گردد. مدل‌های جایگزین و رویه‌های بازگشت به شرایط عادی برای رویارویی با اختلال باید برای فرآیندهای دارای اولویت، طرح‌ریزی شود. به ویژه باید نسبت به برگشت و به هنگام شدن اطلاعات اصلی برای بازگشت فعالیت‌ها به حالت عادی اطمینان حاصل شود؛

- از آنجا که ممکن است بازگشت کامل عملیات به حالت عادی، مستلزم دسترسی به منابع مورد نیازی باشد که در زمان ایجاد اختلال دسترسی به آن‌ها محدود است موسسه اعتباری می‌بایست از طریق تجزیه و تحلیل تاثیرات کاری فعالیت‌ها، به شناسایی آن گروه از وظایف و عملیاتی اقدام نماید که بازیابی آن‌ها از اولویت بیشتری برخوردار است و برای بازگشت آن‌ها به حالت عادی، اهدافی را وضع نماید؛
- هیات مدیره و مدیریت ارشد باید با ایجاد فرهنگ مناسبی در تمامی موسسه، بر اولویت بیشتر استمرار عملیات کاری تاکید نمایند. این امر می‌بایست از طریق تهیه منابع مالی و انسانی کافی، رویکرد مدیریت استمرار عملیات کاری موسسه را اجرا و مورد حمایت قرار دهد؛

- **سطوح بازیابی عملیات (بازگشت به حالت عـادی) و زمـان آن بـرای بعضـی از فعالیت‌های خاص می‌بایست تعریف شود؛**
- **با توجه به این که شدت، گستره و مدت اثرگذاری اختلال‌های عملیاتی متفـاوت می‌باشد لازم است توانایی نظام مدیریت استمرار عملیـات کـاری ـ در مقـاطع زمانی مناسب ـ مورد بررسی و آزمون قرار گیرد. اهم مواردی که می‌بایسـت در این زمینه مورد توجه قرار گیرند عبارتند از:**
  - **اطمینان حاصل شود که سایت جایگزین به اندازه کافی از محل اصـلی عملیات (سایت اصلی) دور است و در صورت امکان، از زیرساخت‌هـای فیزیکی مشابه استفاده نمی‌کند. این موضوع سبب به حـداقل رسـیدن ریسک تاثیر آن‌ها از رویداد مشابه می‌شود. بـه عنـوان مثـال بهتـرین حالت آن است که سایت جایگزین از شبکه ارتبـاطی و بـرق متفـاوتی استفاده نماید (شبکه برق و ارتباطات هر دو سایت یکسان نباشد) ؛**
  - **باید اطمینان حاصل شود در مواقعی که به واحـدهای اصـلی خسـارات جدی وارد شده یا دسترسی به مناطق متاثر از بـروز اخـتلال، محـدود می‌باشد؛ سایت جایگزین برای بازگشـت بـه حالـت عـادی یـا حفـظ عملیات و خدمات مهم، از سیسـتم‌هـا و تجهیـزات مـورد نیـاز و نیـز داده‌های جاری کافی برخوردار است؛**
  - **از آنجا که در خلال بروز یک اختلال، امکان عدم دسترسی به کارکنـان سایت اصلی (اولیه) وجود دارد لازم است در برنامه اسـتمرار عملیـات کاری، شیوه تامین کارکنان مورد نیاز که دارای تخصص و مهارت‌هـای کافی باشند، گنجانده شود (به عنوان مثـال از طریـق تـامین آن‌هـا از منـاطق جغرافیـایی مختلـف، اسـتقرار کارکنـان دائمـی در سـایت جایگزین و ...).**

- سیستم‌های فن‌آوری اطلاعات و تجهیزات با توجه به این که آن‌ها با چه سرعتی باید به وضعیت عادی خود ـ پیش از بروز اختلال ـ بازگردند باید اولویت‌بندی شوند. برنامه‌های بازگشت به شرایط عادی باید برای سیستم‌های فن‌آوری اطلاعات تدوین شوند. این برنامه‌ها باید تشریح نمایند که سیستم‌های مختلف فن‌آوری اطلاعات چگونه می‌توانند در صورت بروز اختلال، مجدداً فعال شوند. نسخه‌برداری‌های پشتیبان و تجهیزات رایانه‌ای آماده جایگزینی باید در مکانی دور از مرکز معمول فن‌آوری اطلاعات قرار داده شوند تا از امکان از بین رفتن هم‌زمان اطلاعات و اطلاعات پشتیبان پیشگیری شود؛
- برنامه‌های استمرار عملیات کاری موسسه اعتباری باید بر مبنای تجزیه و تحلیل تهدیدها و آسیب‌پذیری فعالیت‌های آن باشد. در این برنامه‌ها باید به این تهدیدها و آسیب‌ها توجه شود. حیطه برنامه‌ها باید با توجه به ماهیت، حوزه و پیچیدگی عملیات موسسه اعتباری تعدیل شود. این برنامه‌ها باید عملیات را در صورت بروز اختلال پیش برده، اطلاعات درونی موسسه و نیز اطلاعات اشخاص ذینفع موسسه اعتباری، در زمان ایجاد اختلال را در برگیرد؛
- موسسه اعتباری باید برای رویارویی با بروز اختلالات در فعالیت‌های اشخاص ذینفع خارجی مثل پیمانکارها، ارائه‌دهندگان خدمات به موسسه اعتباری و نیز مشتریان مهم آمادگی داشته باشد؛
- مسئولیت نهایی فعالیت‌هایی که برون‌سپاری می‌شوند همچنان برعهده هیات مدیره و مدیریت ارشد موسسه اعتباری است و برون‌سپاری امور، رافع مسئولیت این دو سطح مدیریتی نمی‌باشد؛
- لازم است موسسه اعتباری برای حفظ موثر ارتباطات خود با شخصیت‌های حقیقی و حقوقی درون و بیرون از موسسه (در صورت بروز یک اختلال مهم)، رویه‌های لازم را اتخاذ نموده، به اجرا درآورد. در این زمینه می‌توان از رویه‌ها و پروتکل‌هایی جامع (همه جانبه) در زمینه ارتباطات اضطراری و نیز به کارگیری افرادی برای هماهنگی استفاده نمود؛

- به منظور تبادل اطلاعات و حفظ موثر ارتباطات موسسه اعتباری با موسسات و مراکز برون‌مرزی، در صورت بروز اختلال، موسسه اعتباری می‌بایست اقدامات لازم را به عمل آورد (از جمله این اقدامات می‌توان به امضای پروتکل‌هایی برای همکاری، تبادل اطلاعات و تسویه در موقعیت‌های بحرانی اشاره نمود)؛
- موسسه اعتباری می‌بایست در مقاطع زمانی مناسب (به طور ادواری و با توجه به شرایط محیط درونی و بیرونی موسسه)، برنامه‌های استمرار عملیات کاری موسسه را مورد آزمون قرار داده؛ اثربخشی آن‌ها را ارزیابی کند و در صورت نیاز، آن‌ها را به روزآوری نماید. آزمون برنامه‌های یاد شده می‌بایست به طور منظم انجام شود. افراد مسئول کنترل به هنگام نمودن و آزمون برنامه‌های استمرار عملیات کاری موسسه اعتباری باید مشخص و پاسخ‌گو باشند؛
- فرآیند برنامه‌ریزی استمرار عملیات کاری موسسه اعتباری موارد ذیل را نیز در بر می‌گیرد:
  - تدوین اصول مربوط به آمادگی و سایر دستورالعمل‌های کلی برای استمرار عملیات کاری؛
  - تهیه و تدوین برنامه‌های استمرار عملیات کاری؛
  - آموزش کارکنان واحدهای کاری برای اجرای برنامه استمرار عملیات کاری؛
  - ایجاد سازمان بحران و تهیه و نگه‌داری فهرست اشخاص رابط؛
  - تهیه و تدوین رویه‌های لازم برای فعالیت‌های اطلاع‌رسانی؛
  - تهیه برنامه‌های بازگشت به شرایط عادی از طریق سیستم فن‌آوری اطلاعات؛
  - نگه‌داری برنامه‌های استمرار عملیات کاری و بازگشت به حالت عادی؛
  - آزمون برنامه‌های استمرار عملیات کاری و برنامه‌های بازگشت به شرایط عادی؛
  - پایش برنامه‌ریزی استمرار عملیات کاری، هماهنگ نمودن این برنامه‌ها و ارزیابی میزان مناسب بودن آن‌ها.

ضمیمه شماره ۶-۶

الزامات احتیاطی

برای

برون‌سپاری امور

برون‌سپاری امور موسسه اعتباری می‌تواند ریسک‌های متعددی از جمله ریسک‌های عملیاتی و شهرت را متوجه موسسه نماید. از این‌رو، مبادرت به این امر می‌بایست در چارچوب اصول و سیاست‌های مشخص و پس از انجام بررسی‌ها و مطالعات لازم انجام شود.

فعالیت‌ها و خدماتی را می‌توان برون‌سپاری نمود که قانونگذار انجام آن‌ها را راساً به موسسه اعتباری تکلیف نکرده باشد. علاوه بر این، برون‌سپاری امور نباید به گونه‌ای انجام شود که به موضوع اصلی فعالیت موسسه اعتباری خدشه وارد نماید.

در برون‌سپاری، بررسی‌های مورد نیاز شامل تهیه گزارش هزینه ـ فایده‌ای است که می‌بایست ضمن اشاره به دلایل توجیهی ضرورت انجام برون‌سپاری، نقاط ضعف و قوت مدیریتی و اهداف آتی موسسه اعتباری در این خصوص را در برگیرد. اهم مواردی که می‌بایست در رابطه با برون‌سپاری مورد توجه قرار گیرند به شرح ذیل می‌باشند:

- لازم است موسسه اعتباری برای برون‌سپاری امور خود، سیاست‌ها و معیارهایی را تدوین نماید. مسئولیت نهایی تمامی امور مربوط به برون‌سپاری امور موسسه اعتباری در چارچوب سیاست‌های تعیین شده برعهده هیات مدیره است. سیاست‌های برون‌سپاری می‌بایست موارد ذیل را در برگیرد:
  - معیارها برای تشخیص مناسب بودن برون‌سپاری امور از جمله حفظ کارآیی و اختیارات نظارتی موسسه بر آن فعالیت؛
  - تعیین حداکثر قابل قبول برای برون‌سپاری کلی امور موسسه اعتباری؛
  - درجه ریسک‌پذیری موسسه اعتباری برای تحمل ریسک‌های ناشی از برون‌سپاری امور.
- موسسه اعتباری باید برنامه جامعی برای مدیریت ریسک امور برون‌سپاری شده تدوین نماید. این برنامه، برای ارزیابی ریسک‌های مربوط می‌بایست موارد ذیل را در برگیرد:
  - حیطه امور برون‌سپاری شده؛

- اهمیت امور برون‌سپاری شده؛
- نحوه مدیریت امور برون‌سپاری شده؛
- پایش و کنترل ریسک امور برون‌سپاری شده؛
- نحوه پوشش ریسک‌های بالقوه توسط ارائه‌دهنده خدمات برون‌سپاری شده.

از دیگر مواردی که در برنامه جامع مدیریت ریسک امور برون‌سپاری شده می‌بایست مورد توجه قرار گیرند می‌توان به نکات ذیل اشاره نمود:

- بروز هرگونه اختلال در انجام امور برون‌سپاری و تاثیر آن بر وضعیت مالی، شهرت و عملیاتی موسسه اعتباری و خسارات ناشی از آن؛
- تاثیر برون‌سپاری امور بر نحوه اجرای الزامات قانونی و مقرراتی موسسه اعتباری؛
- بررسی ارتباط و همبستگی متقابل بین امور برون‌سپاری شده با سایر فعالیت‌های موسسه اعتباری؛
- تاثیر وجود رابطه مالکیتی بین موسسه اعتباری و ارائه‌دهنده خدمات برون‌سپاری؛
- شخصیت حقوقی ارائه‌دهنده خدمات برون‌سپاری به ویژه از نظر نظارت پذیری آن (مراجع نظارتی ذی‌ربط) ؛
- بررسی و امکان کنترل ریسک‌ها، به ویژه در موارد متعدد بودن ارائه‌دهندگان خدمات برون‌سپاری شده؛
- بررسی نحوه حفاظت از اطلاعات و امنیت آن‌ها؛
- بررسی ریسک کشوری، ریسک سیاسی و شرایط قانونی در مورد برون‌سپاری امور به ارائه‌دهندگان خارجی خدمت و ارائه‌دهندگان داخلی که در خارج از کشور فعالیت دارند؛
- تعیین نحوه و مکان رسیدگی به اختلافات موسسه اعتباری با ارائه‌دهندگان خدمات برون‌سپاری در خارج از کشور؛

- **بررسی نحوه حفظ امنیت فن‌آوری اطلاعات توسط ارائه‌دهنده خدمات برون‌سپاری؛**
- **بررسی هزینه حق انتخاب‌های جایگزین برای موسسه اعتباری در صورت بروز اختلال در ادامه فعالیت ارائه‌دهنده خدمات برون‌سپاری؛**
- **تدوین الزامات احتیاطی برای موظف نمودن ارائه‌دهنده خدمات برون‌سپاری به حفظ اطلاعات موسسه اعتباری و مشتریان و نیز ممانعت از افشای آن‌ها به اشخاص (به جز مراجع ذی‌صلاح)؛**
- **پیش‌بینی فرآیند انجام اقدامات اصلاحی به هنگام وقوع رویدادهای غیرمنتظره؛**
- **لازم است موسسه اعتباری نسبت به شناسایی کافی اشخاصی که انجام امور به آن‌ها برون‌سپاری شده است، اقدامات لازم را به عمل آورد؛**
- **با توجه به این که تغییر ارائه کننده خدمات برون‌سپاری، مستلزم صرف هزینه می‌باشد از این‌رو، انتخاب ارائه‌دهنده خدمات برون‌سپاری، توسط موسسه اعتباری می‌بایست براساس بالاترین استانداردها و با دقت انجام شود. در مورد ارائه‌دهندگان خدمات برون‌سپاری که در خارج از کشور فعالیت می‌کنند لازم است وضعیت اقتصادی، سیاسی و قانونی کشور مربوطه نیز مورد بررسی قرار گیرد؛**
- **به منظور پیشگیری از ریسک عدم اجرای تعهدات توسط ارائه‌دهنده خدمات برون‌سپاری، لازم است روابط بین موسسه اعتباری و ارائه‌دهنده خدمات و نیز حقوق، تعهدات و شروط مورد نظر آن‌ها، به طور شفاف در قرارداد منعقده قید شود، در قرارداد منعقده:**
  - **لازم است ماده‌ای از قرارداد، به نحوه فسخ قرارداد (termination clause) اختصاص داده شود و امکان انتقال فعالیت به شخص ثالث و شرایط احتمالی آن و یا انتقال مجدد فعالیت به موسسه اعتباری، پیش‌بینی‌های لازم انجام شود؛**
  - **لازم است با ارائه‌دهنده خدمات برون‌سپاری شروطی مبنی بر حفاظت از اطلاعات موسسه اعتباری و مشتریان گنجانده شود؛**
  - **لازم است شروطی درج گردد که به موجب آن‌ها برای انجام وظایف ناظران بانک مرکزی جمهوری اسلامی هیچ‌گونه محدودیتی توسط**

- ارائه‌دهنده خدمات برون‌سپاری ایجاد نشود و حق ناظران مزبور برای نظارت بر امور برون‌سپاری شده ـ در موسسه ارائه‌دهنده این خدمات ـ محفوظ بماند.

- انتقال فعالیت‌های کاری یا سایر امور برون‌سپاری به یک نمایندگی، نافی مسئولیت موسسه اعتباری در قبال تعهداتش نمی‌باشد. از این‌رو، هر موسسه اعتباری از سوی ارائه دهنده خدمات، در برابر خسارت وارده موظف به پاسخ‌گویی به مشتریان یا سایر طرف‌های قراردادش می‌باشد؛
- مدیریت ارشد مسئولیت دارد از فراهم شدن ترتیبات لازم برای مدیریت ریسک عملیاتی و کنترل اموری که برون‌سپاری شده‌اند اطمینان حاصل کند. علاوه بر این، مدیریت ارشد، موظف است از کیفیت اطلاعات مربوط به اموری که برون‌سپاری شده‌اند و کنترل منظم امنیت آن‌ها اطمینان حاصل کند. در این زمینه:
  - موسسه اعتباری باید از استمرار امور برون‌سپاری شده اطمینان حاصل کند و برای رویارویی با بروز هرگونه اختلال مهم در فعالیت‌های پیمانکار و ارائه دهنده خدمات آمادگی داشته باشد؛
  - موسسه اعتباری باید اطمینان حاصل کند که ارائه دهنده خدمات برون‌سپاری، از منابع و دانش فنی لازم برای ارائه آن خدمات برخوردار است؛
  - موسسه اعتباری باید تدابیری اتخاذ نماید که از تمرکز امور برون‌سپاری شده مختلف نزد یک ارائه‌کننده خدمات، پیشگیری شود؛
  - موسسه اعتباری باید اطمینان حاصل کند که تمامی اطلاعات مورد نیاز در زمینه مدیریت ریسک و کنترل‌های داخلی برای انجام نظارت توسط موسسه اعتباری و یا مراجع ذی‌صلاح قابل دسترسی است.

ضمیمه شماره ۷-۶

الزامات احتیاطی
برای
سیستم‌های فن‌آوری اطلاعات

- هیات مدیره باید اطمینان حاصل نماید که سیستم‌های فن‌آوری اطلاعات موسسه اعتباری از کفایت لازم برخوردار بوده و متناسب با ماهیت و حوزه عملیات آن می‌باشد. کفایت و متناسب بودن سیستم‌های فن‌آوری اطلاعات می‌بایست به طور مستمر نسبت به فعالیت‌های موسسه و الزامات مقرر توسط هیات مدیره مورد ارزیابی قرار گیرد. علاوه بر این، می‌بایست بررسی شود که این سیستم‌ها تا چه حد فعالیت‌های تجاری را مطابق با مصوبات هیات مدیره مورد پشتیبانی قرار می‌دهند؛
- برای ثبت الکترونیکی، انتقال، پردازش، بایگانی و نگهداری اطلاعات، موسسه اعتباری باید از سازمان، نظام کنترل داخلی و نیروی متخصص لازم، برخوردار باشد. بخشی از این وظایف یا تمامی آن‌ها می‌توانند برون‌سپاری شوند مشروط بر اینکه موسسه اعتباری اطمینان حاصل کند که شرکت عرضه کننده خدمات فن‌آوری اطلاعات در انطباق با اصول ارائه شده تحت عنوان "الزامات احتیاطی برای برون سپاری امور"، ضمیمه شماره (٦-٦)، این رهنمود قرار دارد؛
- به منظور تامین نیازهای حال و آینده موسسه اعتباری، هیات مدیره باید راهبردی را تصویب کند که در مورد وجود، حفظ و گسترش محیط فن‌آوری اطلاعات اطمینان ایجاد کند. علاوه براین، هیات مدیره باید اطمینان یابد که موسسه از رویه‌های لازم برای بودجه‌بندی و پایش هزینه‌های فن‌آوری اطلاعات برخوردار است؛
- موسسه اعتباری باید مدل‌های اجرا، استانداردها، رویه‌ها و کنترل‌هایی را

برای حوزه‌های فرعی مختلف فن‌آوری اطلاعات تعریف کند به گونه‌ای که بتواند بین واحدهای کاری و واحدهای ارائه دهنده خدمات فن‌آوری اطلاعات هماهنگی ایجاد نماید. در این زمینه، مدیریت ارشد موظف است برنامه‌ریزی، پایش و ارزیابی امور مربوط به فن‌آوری اطلاعات را انجام دهد. در صورت لزوم، می‌بایست گروه مجزایی، شامل نمایندگانی از واحدهای مختلف کاری را برای انجام این هماهنگی‌ها تعیین نماید؛

- موسسه اعتباری باید اطمینان حاصل کند که واحد فن‌آوری اطلاعات مستقل از کاربران، واحد فن‌آوری اطلاعات مسئول بهبود و عملکرد سیستم‌های فن‌آوری اطلاعات است تا جایی که کاربران از قابل اتکا بودن اطلاعات پردازش شده، اطمینان حاصل کنند؛
- لازم است وظایف توسعه سیستم و تولید از یکدیگر مجزا باشند به گونه‌ای که کارکنان فقط بر اساس رویه‌های مشخص و تحت مراقبت، به اطلاعات یکدیگر دسترسی داشته باشند؛
- موسسه اعتباری باید اطمینان حاصل کند که واحد حسابرسی داخلی از قابلیت لازم برای ارزیابی عملکرد و کنترل‌های داخلی فعالیت‌های فن‌آوری اطلاعات برخوردار است؛
- موسسه اعتباری باید رویه‌هایی را برای گسترش سیستم‌ها و کنترل کیفی آن‌ها ایجاد نماید تا اطمینان حاصل کند که سیستم‌ها به همان ترتیبی که برنامه‌ریزی شده‌اند، کار می‌کنند؛

علاوه بر این، باید روش مستند سازی ثابتی در مورد سیستم‌ها وجود داشته باشد تا این اطمینان ایجاد شود که آن‌ها می‌توانند حتی در صورت تعویض کارکنان اصلی، به کار گرفته شده، بهبود یابند؛

- موسسه اعتباری باید برای خریداری نرم‌افزارها و سخت‌افزارها یا انعقاد قراردادها با ارائه کنندگان خدمات، رویه تعریف شده‌ای داشته باشد تا به کمک آن، از انطباق تجهیزات خریداری شده و قراردادهای منعقده با

نیازهای موسسه اعتباری، استانداردهای معتبر و استمرار خدمات اطمینان حاصل شود؛

- موسسه اعتباری باید ریسک ناشی از قطع خدمات مربوط به فن‌آوری اطلاعات را (در اثر عواملی مثل آتش‌سوزی، سیل، قطع برق، خرابی سخت‌افزار و ...) از طریق رویه‌ها و مدل‌هایی که با امنیت فیزیکی سر و کار دارند و نیز از طریق تجهیزات آماده جایگزینی، به حداقل رساند. علاوه بر این، می‌بایست دسترسی به اقلام حیاتی (مانند سخت‌افزارها، برق، وسایل ارتباط جمعی، اسناد و ...) با تعیین افراد مشخص، محدود گردد.
- به منظور حفظ امنیت اطلاعات، لازم است بین امور اداری و سازمانی، پرسنلی، فیزیکی، تبادل اطلاعات و امنیت آن‌ها، سخت‌افزار و نرم‌افزار تفکیک مناسبی انجام شود. امنیت کلی اطلاعات شامل حفظ محرمانه بودن اطلاعات، درستی و در دسترس بودن آن‌ها می‌باشد. در این خصوص توجه به موارد ذیل ضروری است:
  - دسترسی به سیستم باید کنترل شود. استنکاف از انجام تراکنش‌ها در سیستم‌های اطلاعات و شناسایی و تایید طرف‌های مرتبط متقابل باید به طور مناسب انجام شود. علاوه بر این، از قابلیت پیگیری دقیق تراکنش‌های پردازش شده در سیستم‌های اطلاعات باید اطمینان حاصل شود؛
  - سطح امنیت اطلاعات موسسه اعتباری به طور کلی و سطح امنیت سیستم‌های مختلف اطلاعات ـ با توجه به ماهیت و حوزه عملیات، جدی بودن تهدیدها ـ و نیز سطح کلی توسعه تکنولوژیکی موسسه باید از کفایت لازم برخوردار باشند؛
  - هیات مدیره موسسه اعتباری موظف است اطمینان حاصل نماید که امنیت اطلاعات موسسه در حد کفایت قرار دارد. علاوه بر این هیات مدیره باید سطح کلی امنیت اطلاعات در موسسه را تعریف و تصویب نماید؛

- هیات مدیره باید منابع کافی فراهم نماید و مسئولیت‌ها را برای حفظ کفایت سطح امنیت اطلاعات تعریف کند و آن را به طور منظم مورد ارزیابی قرار دهد. در صورت عدم دسترسی به متخصص امنیت اطلاعات، موسسه اعتباری می‌تواند کار ارزیابی را به شخص یا اشخاص خارج از سازمان که از تخصص و صلاحیت کافی برای این کار برخوردارند واگذار نماید. در ضمن در مورد نارسایی‌های شناسایی شده می‌بایست اقدامات لازم انجام شود؛
- سطح امنیت اطلاعات در موسسه می‌بایست بر اساس ارزیابی ریسک‌های مرتبط با آن به طور منظم بررسی شود. در ارزیابی‌های ریسک، منابع و وظایف اصلی موسسه اعتباری باید مشخص شوند. تهدیدها و آسیب‌پذیری منابع و کارکرد موسسه از ناحیه تهدیدهای مورد بحث و تاثیر آن‌ها بر عملیات موسسه می‌بایست مورد ارزیابی قرار گیرند. به منظور مدیریت ریسک‌های شناسایی شده، کنترل‌های کافی باید انجام شود. این ریسک‌ها در زمان ارائه خدمات و فنون جدید می‌بایست ارزیابی شوند؛
- ارزیابی ریسک‌های مربوط به امنیت اطلاعات باید با مدیریت ریسک موسسه مرتبط باشد تا اطمینان حاصل شود که هیات مدیره و مدیریت ارشد از کل اثرات ریسک‌های مهم در فعالیت‌های موسسه آگاهی دارند؛
- موسسه اعتباری باید فرد / افرادی را به عنوان مسئول نگاه‌داری اطلاعاتی که ذخیره و پردازش می‌شوند و سیستم‌هایی که مورد استفاده قرار می‌گیرند مشخص نماید. این فرد / افراد در مورد اصول به کارگیری، حق دسترسی و امنیت اطلاعات و سیستم مسئولیت دارند؛
- موسسه اعتباری باید از نظر الزامات امنیتی مرتبط، اطلاعات ذخیره و پردازش شده را طبقه‌بندی نماید و مقرراتی برای سطح دسترسی به طبقات مختلف اطلاعات تدوین کند؛
- موسسه اعتباری باید برای دسترسی به اطلاعات، برنامه‌ها و سیستم‌ها،

مجوز اعطا نماید و سیستم‌هایی را که بر طبق اصول متحدالشکل مصوب مدیریت مورد استفاده قرار می‌گیرند تحت پایش قرار دهد. مجوز، باید مطابق با وظایف کاربران داده شود. به منظور محدود نمودن سطح دسترسی به اطلاعات، برنامه و سیستم، موسسه اعتباری می‌بایست برای کاربران مجاز از ابزارهای فنی (شناسه‌های کاربران، کلمه عبور و ...) استفاده کند و ترتیبی اتخاذ نماید که هرگونه گزارش در مورد نقض شرایط مجوز، مورد رسیدگی قرار گیرد؛

- موسسه اعتباری باید شرایط اصول مربوط به امنیت اطلاعات را که به تصویب هیات مدیره رسیده است به هنگام نماید. تدوین دستورالعمل‌هایی برای مدیریت مجوز دسترسی، مقابله با نرم‌افزارهای مخرب و استفاده از اینترنت و پست الکترونیکی از جمله اهداف معمول برای امنیت اطلاعات محسوب می‌شوند. موسسه اعتباری باید به طور شفاف امنیت اطلاعات را تعریف نماید. در این رابطه لازم است کارکنان، به طور منظم برای آشنایی با مسئولیت‌های خود در زمینه امنیت اطلاعات آموزش داده شوند. ارتقای دانش کارکنان در زمینه امنیت اطلاعات، باید طی فرآیند مستمری انجام شود و مسئولیت‌های مرتبط با آن در سطح مدیریت مشخص شود.
- رویدادهای مربوط به امنیت اطلاعات می‌بایست مورد توجه ویژه قرار گرفته، تجزیه و تحلیل، نگهداری و به فرد مسئول آن گزارش گردد؛
- امنیت خدمات On-line شامل امنیت رویه‌ها (مثل مراحل دستی)، برنامه‌های کاربردی، سیستم‌های فنی و انتقال داده‌ها می‌شود؛
- پیش از ارائه خدمات جدید به صورت On-line، لازم است موسسه اعتباری با انجام بررسی‌های کافی از مناسب بودن ارائه خدمات اطمینان حاصل کند. ریسک‌های مهم موجود در این خدمات و اقدامات مرتبط با مدیریت ریسک باید مستندسازی شوند و مدیریت ریسک باید به تناسب آن توسعه داده شود.

- طراحی نظام کنترل‌های داخلی و مدیریت ریسک عملیات On-line ، سیستم‌های فن‌آوری اطلاعات و فرآیندهای داخلی آن می‌بایست براساس ماهیت و حیطه عملیات موسسه اعتباری و تهدیدهایی که متوجه آن عملیات است انجام شوند؛
- موسسه اعتباری باید به طور ادواری کل ریسک‌های موجود در عملیات On-line را ارزیابی کند یا انجام این ارزیابی را به اشخاص ثالث واگذار نماید. موسسه اعتباری باید به طور مستمر سیستم‌های فن‌آوری اطلاعات ، امنیت آن‌ها و نیز کفایت حفاظت آن‌ها در برابر بروز اختلال‌های مختلف و سوء استفاده‌های احتمالی را مورد ارزیابی قرار داده، بهبود بخشد؛

موسسه اعتباری پیش از ارائه هر خدمت می‌بایست با کمک اقدامات حداقلی ذیل، از کفایت امنیت اطلاعات ذی‌ربط اطمینان حاصل کند:

- تجزیه و تحلیل فرآیند ارائه خدمت و اقدامات لازم برای مدیریت ریسک آن؛
- بررسی امنیت ویژه سیستم فن‌آوری اطلاعات و نیز پایش مستمر سطوح مختلف سیستم‌های مزبور؛
- تجزیه و تحلیل آسیب‌پذیری سیستم، فن‌آوری اطلاعات و کفایت آن ، به هنگام نمودن و انجام اصلاحات لازم در این زمینه؛
- پیگیری مستمر هرگونه اختلال، سوء استفاده یا تلاش برای سوء استفاده و ارائه گزارش در مورد آن به مدیریت ذی‌ربط در چارچوب ضوابط مقرر؛
- تدوین برنامه‌های ویژه بازگشت سیستم به حالت عادی، به منظور حصول اطمینان از استمرار عملیات کاری موسسه؛
- تدارک تجهیزات آماده جایگزینی (در صورت بروز اختلال) پیش از اجرای برنامه‌های ویژه مربوط به استمرار عملیات کاری حصول اطمینان از مؤثر بودن آن‌ها برای بازگشت عملیات به وضعیت عادی؛
- آزمون عملکرد سیستم‌ها در صورت لزوم و حصول اطمینان از اینکه

سیستم‌های فن‌آوری اطلاعات، در ساعاتی که استفاده از آن‌ها توسط کاربران موازی به حداکثر خود می‌رسد از توان کافی برخوردارند؛

- تجهیز سیستم‌ها به برنامه‌های مناسب ضد ویروس و ساز و کارهای لازم برای رویارویی با نرم‌افزارهای مخرب؛
- پشتیبانی از سیستم‌ها و سایر خطوط ارتباطی مربوط به اطلاعات در برابر حملات به سیستم‌ها و نیز بار اضافی تحمیلی به آن‌ها؛
- پیش‌بینی تجهیزات آماده جایگزینی برای رویارویی با موانع ناشی از سنگینی بار در مواقع اتصال به شبکه اینترنت؛
- حصول اطمینان از این که برای کنترل دسترسی به سیستم‌های مختلف فن‌آوری اطلاعات، ساز و کارهای مناسبی وجود دارد و مدیریت مناسبی در زمینه صدور مجوز دسترسی به اطلاعات و سیستم‌های فن‌آوری اعمال می‌شود؛
- اتخاذ تدابیر لازم برای تفکیک شبکه‌های اینترنت از شبکه‌های داخلی از طریق تجهیزات امنیتی؛
- آزمون منظم سیستم‌های فن‌آوری اطلاعات، به ویژه پس از انجام هرگونه تغییر در آن‌ها؛
- شناسایی نارسایی‌های امنیتی موجود در سیستم‌های فن‌آوری اطلاعات و رفع سریع آن‌ها به منظور پیشگیری از استفاده غیر مجاز و سوء استفاده‌های احتمالی؛
- حصول اطمینان از این که انتقال اطلاعات بین مشتریانی که از خدمات On-line استفاده می‌کنند با ارائه‌دهنده خدمت و نیز پردازش اطلاعات در سیستم‌های ارائه‌دهنده خدمت به درستی انجام شده و کلیه طرف‌های مذکور در فوق، به حفظ محرمانه بودن اطلاعات پای‌بند هستند؛
- شناسایی و تائید طرف‌های مقابل در سیستم، با شیوه‌ای مطمئن و در حد کفایت؛

- **تجهیز سیستم‌های فن‌آوری اطلاعات به ساز و کارهای تائید و ردگیری حسابرسی، به منظور حصول اطمینان از دقت و درستی داده‌ها و ستاده‌ها، مناسب بودن مجوزها، بازیابی اطلاعات در صورت بروز وقفه در پردازش آن‌ها و برخورداری از قابلیت ردگیری تراکنش‌ها؛**
- **امکان‌پذیر بودن ردگیری دقیق تراکنش‌های پردازش شده در سیستم‌های فن‌آوری اطلاعات؛**
- **وجود کنترل‌های لازم در سیستم‌های فن‌آوری اطلاعات، به منظور تطبیق تراکنش‌های انجام شده در سیستم‌های فرعی مختلف؛**
- **امکان ردیابی زنجیره تراکنش‌ها از مشتری تا سیستم اصلی موسسه؛**
- **مخفی نگه‌داشتن کلمات عبور هر مشتری در قالب رمز، در سیستم و نیز در زمان انتقال آن‌ها بین سیستم‌های مختلف؛**
- **خودداری از انجام توامان وظایف ایجاد، پردازش و ابلاغ شناسه و کلمه عبور ویژه مشتریان، توسط یک فرد (به دلیل مخاطره‌آمیز بودن آن)؛**
- **حصول اطمینان از این که سیستم‌های فن‌آوری اطلاعات موسسه می‌توانند هرگونه اتصال به سیستم یا تلاش برای انجام این امر و نیز استفاده از سیستم‌های فن‌آوری اطلاعات را به طور صحیحی ثبت نمایند؛**
- **کنترل منظم گزارش‌های مربوط به اتصال / اتصال‌ها به سیستم؛**
- **وجود رویه‌هایی برای گزارش تلاش‌های غیرمجاز با هدف دسترسی به سیستم‌ها و سایر موارد سوءاستفاده از اتصال‌ها و نیز کنترل و انطباق گزارش‌ها با الزامات قانونی؛**
- **رعایت اصل محرمانه نگه‌داشتن اطلاعات و حریم خصوصی مشتریان؛**
- **وجود دستورالعمل‌هایی مشتمل بر اطلاعات کافی در مورد ارائه‌دهنده خدمات، تخصیص و مسئولیت‌ها به بین ارائه‌کننده خدمت و کاربر و استفاده مطمئن از خدمت توسط کاربر.**

ضمیمه شماره ۸-۶

الزامات احتیاطی
برای
سیستم‌ها و خدمات پرداخت

ثبات سیستم‌های پرداخت از اهمیت بسیار بالایی برخوردار است. نظر به این که تمامی پرداخت‌های جامعه از طریق این سیستم‌ها انجام می‌شوند، مدت زمانی که سیستم‌های مورد بحث دچار توقف و یا اختلال می‌گردند برای اقتصاد کشور بسیار حیاتی است، زیرا علاوه بر ایراد لطمه به پرداخت‌های مشتریان، به اقتصاد کل کشور نیز آسیب جدی وارد می‌نماید. از جمله مواردی که در رابطه با سیستم‌ها و خدمات پرداخت می‌بایست مورد توجه قرار گیرد می‌توان به نکات ذیل اشاره نمود:

- لازم است هیات مدیره برای سیستم‌های پرداختی که موسسه اعتباری در آن عضویت دارد و نیز برای خدمات پرداختی که به مشتریان ارائه می‌کند اصولی را تدوین نماید. این اصول، می‌بایست به گونه‌ای باشند که علاوه بر این که عملیات جاری موسسه را در بر می‌گیرند تحولات آتی در این زمینه را نیز مدنظر قرار دهند؛
- به منظور حصول اطمینان از اثربخشی و مطمئن بودن خدمات پرداخت و نیز پایش آن، لازم است هیات مدیره اهدافی را برای خدمات پرداخت تعیین نماید؛
- مدیریت ارشد مسئولیت دارد از کفایت تخصص، منابع و کنترل‌های داخلی برای عملکرد اثربخش و مطمئن خدمات پرداخت اطمینان حاصل کند؛
- موسسه اعتباری باید ریسک‌های مربوط به سیستم‌ها و خدمات پرداختی را که ارائه می‌شود، شناسایی و آن را به طور منظم به هنگام نماید؛
- سیستم‌های پرداخت موسسه اعتباری باید مطمئن و امن باشند؛
- موسسه اعتباری باید تدابیری اتخاذ نماید تا بروز اختلالات در سیستم‌های

پرداخت مورد استفاده خود را بـه حـداقل برسـاند. سیسـتم‌هـا و خـدمات پرداخت می‌بایست با تجهیزات آماده جایگزینی (در صورت بـروز اخـتلال) پشتیبانی شوند؛

- **موسسه اعتباری لازم است قبل از به کارگیری فن‌آوری‌ها و ابزارهای جدید پرداخت، نسبت بـه دریافـت مجوزهـای لازم از بانـک مرکـزی جمهـوری اسلامی ایران اقدام نماید.**
- **موسسه اعتباری می‌بایست نتایج حاصـل از ارزیـابی‌هـای خـود از ریسـک خدمات پرداخت و فن‌آوری‌های جدید را قبل از اجرا برای دریافت مجوزهای لازم به بانک مرکزی جمهوری اسلامی ایران ارائه نماید. هرگونـه تغییـر در خدمات پرداخت جاری نیز مستلزم رعایت مورد فوق می‌باشد.**

ضمیمه شماره ۹-۶

الزامات احتیاطی

برای شناسایی کافی مشتریان

لازم است موسسه اعتباری سیاست‌ها و رویه‌های شفافی در رابطه با شناسایی و پذیرش مشتریان تدوین نماید. اهم نکاتی که در این رابطه می‌بایست مورد توجه قرار گیرد به شرح ذیل می‌باشند:

- موسسه اعتباری می‌بایست تمامی اطلاعات مورد نیاز برای شناسایی هر مشتری جدید را تهیه نماید. کیفیت و کمیت این اطلاعات به نوع متقاضی (اشخاص حقیقی و حقوقی)، گردش مالی مورد انتظار از حساب افتتاح شده بستگی دارد؛
- در مورد اشخاص حقیقی، لازم است حداقل، اطلاعات ذیل اخذ شود:

نام و نام‌خانوادگی فرد، ملیت، شماره شناسنامه، کدملی، تاریخ و محل تولد، نام پدر، نشانی کامل و ثابت، شماره تلفن، شغل، نوع حساب و ماهیت روابط بانکی مربوط به آن، امضا؛

- در مورد اشخاص حقوقی، لازم است اطلاعات ذیل اخذ شود:

نام موسسه، تصویر روزنامه رسمی مبنی بر ثبت شرکت، اصل یا رونوشت (کپی) تائید شده گواهی‌نامه ثبت شرکت، شرکت‌نامه و اساسنامه، مصوبه هیات مدیره درخصوص افتتاح یک حساب (به نام شرکت) و تعیین هویت فرد/افرادی که حق برداشت از آن حساب را دارند، محل اصلی عملیات تجاری موسسه، آدرس پستی، شماره‌های تلفن و دورنگار؛

- الزامات مربوط به شناسایی مشتری، به زمان افتتاح حساب محدود نمی‌شود بلکه پس از افتتاح حساب برای هریک از مشتریان (اشخاص حقیقی و حقوقی) لازم است عملکرد حساب وی به طور مستمر تحت نظارت

قرار گیرد و با استفاده از ابزارهای مناسب، مبادلاتی که خارج از فعالیت‌های معمول آن حساب قرار دارد، شناسایی شوند؛

- **موسسه اعتباری می‌بایست سیستم جامعی از مدیریت اطلاعات را ایجاد نماید، که در آن، اطلاعات مربوط به تمامی مشتریان گردآوری و پردازش شده، در اختیار کارکنان ذی‌ربط تمامی واحدها و گروه‌های بانکی وابسته قرار گیرد؛**
- **لازم است اطلاعات مربوط به اشخاص مرتبط مشتریان (اشخاص حقیقی و حقوقی، براساس تعاریف مندرج در آئین‌نامه اشخاص مرتبط، موضوع بخشنامه‌های شماره مب/ ۱۹٦٤ و شماره مب/ ۱۹٦٥ مورخ ۱۳۸۲/۱۱/۲۹ بانک مرکزی جمهوری اسلامی ایران) در سیستم جامع اطلاعات مدیریت نگهداری شود.**