



بانک مرکزی جمهوری اسلامی ایران

مدیریت کل مقررات، مجوزهای بانکی و مبارزه با پولشویی

اداره مطالعات و مقررات بانکی

«دستورالعمل حداقل الزامات مدیریت ریسک عملیاتی در مؤسسات اعتباری»

مهر ماه ۱۴۰۰

«بسمه تعالی»

«دستورالعمل حداقل الزامات مدیریت ریسک عملیاتی در مؤسسات اعتباری»

در اجرای بند «ب» ماده (۱۱) قانون پولی و بانکی کشور و همچنین به استناد ماده (۶۲) آیین نامه نحوه تأسیس و اداره مؤسسات اعتباری غیردولتی مصوب شورای پول و اعتبار و به منظور فراهم نمودن زمینه اجرای مؤثر ماده (۱۲۰) اساسنامه بانک‌های تجاری غیردولتی و ایجاد نظام مؤثر مدیریت ریسک عملیاتی در شبکه بانکی کشور، «دستورالعمل حداقل الزامات مدیریت ریسک عملیاتی در مؤسسات اعتباری» که از این پس به اختصار «دستورالعمل» نامیده می‌شود به شرح زیر تدوین می‌گردد:

فصل اول: تعاریف و کلیات

ماده ۱- در این دستورالعمل، عناوین زیر به جای عبارت‌های مربوط بکار می‌روند:

۱-۱- بانک مرکزی: بانک مرکزی جمهوری اسلامی ایران؛

۱-۲- مؤسسه اعتباری: بانک یا مؤسسه اعتباری غیربانکی که با مجوز بانک مرکزی تأسیس شده و تحت نظارت بانک مرکزی قرار دارد؛

۱-۳- نظام کنترل داخلی: مجموعه‌ای از فرایندها و رویه‌هایی است که توسط هیأت مدیره مؤسسه اعتباری، هیأت عامل و دیگر کارکنان آن برای حصول اطمینان از کارایی و اثر بخشی عملیات به منظور نیل به اهداف مقرر، همچنین تهیه گزارش‌های مالی قابل اتکا و انطباق با قوانین و مقررات طراحی و پیاده‌سازی می‌شود.

۱-۴- تضاد منافع: هر گونه تعارض میان منافع مؤسسه اعتباری، سهامداران یا منافع مشتریان با منافع هیأت مدیره و هیأت عامل، به نحوی که دستیابی به هر یک مستلزم چشم پوشی از تمام یا بخشی از دیگری باشد؛

۱-۵- ریسک‌پذیری: سطح کلی ریسک و انواع آن که در مسیر دستیابی به اهداف راهبردی و برنامه‌های کسب و کار، مؤسسه اعتباری مایل به پذیرش آن بوده و از قبل در خصوص پذیرش آن تصمیم‌گیری نموده است؛

۱-۶- ظرفیت ریسک: حداکثر میزان ریسکی که مؤسسه اعتباری با توجه به سرمایه نظارتی، مدیریت ریسک، اقدامات کنترلی و ریسک‌پذیری خود و همچنین حدود نسبت‌های احتیاطی قادر به پذیرفتن آن است؛

۱-۷- مدیریت ریسک: بکارگیری مجموعه‌ای از راهبردها، سیستم‌ها و ابزارهای کارآمد و نظارت مستمر بر آن‌ها به منظور شناسایی، ارزیابی، اندازه‌گیری، کنترل و کاهش ریسک‌هایی که تأثیرات نامطلوبی بر دستیابی به اهداف مؤسسه اعتباری دارند؛

- ۸-۱- ریسک عملیاتی: احتمال وقوع زیان ناشی از نقصان و یا عدم کفایت فرایندهای داخلی، روش‌ها و سیستم‌ها، عملکرد و اقدامات افراد و یا ناشی از رویدادهای خارج از مؤسسه اعتباری؛
- ۹-۱- ریسک ذاتی: ریسک ناشی از بروز یک رویداد در حالتی که هیچ گونه تمهید یا اقدام کنترلی به منظور کاهش تبعات یا احتمال وقوع رویداد مزبور به کار گرفته نشود؛
- ۱۰-۱- ریسک باقی‌مانده: ریسک ناشی از بروز یک رویداد با در نظر گرفتن اثر تمهیدات یا اقدامات کنترلی که به منظور کاهش تبعات یا احتمال وقوع رویداد مزبور به کار گرفته شده‌اند؛
- ۱۱-۱- مشخصه ریسک عملیاتی: نوع، ماهیت و میزان ریسک عملیاتی هر یک از خطوط کسب و کار مؤسسه اعتباری و ارتباط آن با وقایع و رویدادهای موجد ریسک؛
- ۱۲-۱- محیط کنترلی: مجموعه‌ای از ضوابط، فرایندها و ساختارهایی است که مبنای پیاده‌سازی نظام کنترل داخلی را در مؤسسه اعتباری فراهم می‌کند.

فصل دوم: وظایف و مسئولیت‌های هیأت مدیره

- ماده ۲- هیأت مدیره مؤسسه اعتباری موظف است چارچوب مدیریت ریسک عملیاتی مؤسسه اعتباری را با لحاظ حداقل موارد زیر، تدوین، تصویب و به طور دوره‌ای بازبینی نماید:
- ۲-۱- گلوگاه‌های بروز ریسک عملیاتی (منابع اصلی موجد ریسک) و شرح و طبقه‌بندی زیان‌های ناشی از آن‌ها بر اساس میزان و شدت آن در تمامی سطوح مؤسسه اعتباری؛
- ۲-۲- ساختارهای حاکمیتی مورد نیاز برای مدیریت ریسک عملیاتی از قبیل خطوط گزارش‌دهی و پاسخگویی؛
- ۲-۳- ابزارهای ارزیابی و اندازه‌گیری ریسک عملیاتی و چگونگی استفاده از آن‌ها؛
- ۲-۴- میزان پذیرش و تحمل ریسک عملیاتی با توجه به ماهیت، انواع و سطوح ریسک؛
- ۲-۵- خط مشی‌ها، راهبردها و ابزارهای کنترل و کاهش ریسک عملیاتی از جمله برنامه یا برنامه‌های تداوم کسب و کار و خط‌مشی لازم در خصوص فرایند بررسی و تأیید محصولات، فعالیت‌ها، فرایندها و نظام‌های جدید از منظر مدیریت ریسک عملیاتی در سطح مؤسسه اعتباری. فرایند مزبور باید حداقل موارد زیر را در برگیرد:
- ۵-۲-۱- ریسک ذاتی محصولات، فعالیت و خدمات جدید؛
- ۵-۲-۲- تغییر در مشخصه ریسک عملیاتی، ریسک‌پذیری، حدود تحمل ریسک، و ریسک فعالیت‌ها و محصولات موجود؛
- ۵-۲-۳- کنترل‌های ضروری، فرایندهای مدیریت ریسک و راهبردهای کاهش ریسک؛
- ۵-۲-۴- ریسک باقی‌مانده؛
- ۵-۲-۵- تغییر در آستانه‌ها یا حدود ریسک؛
- ۵-۲-۶- فرایندها و شاخص‌های مربوطه به مدیریت ریسک محصولات و یا فعالیت‌های جدید؛
- ۵-۲-۷- پیش‌بینی سرمایه‌گذاری مناسب در زمینه منابع انسانی و زیرساخت‌های فن‌آوری مورد نیاز برای ارایه محصولات جدید؛

۶-۲- سیستم‌های اطلاعات مدیریت و گزارشگری ریسک. چارچوب گزارش‌گری مناسب به منظور مدیریت مؤثر ریسک عملیاتی در تمام سطوح مؤسسه اعتباری باید حداقل دربرگیرنده موارد زیر باشد:

۶-۲-۱- بررسی شاخص‌های مالی، ریسک عملیاتی، رعایت قوانین و مقررات و اطلاعات محیطی، اطلاعات بازار، رویدادها و شرایطی بیرونی مؤثر بر تصمیم‌گیری‌های مؤسسه اعتباری؛

۶-۲-۲- منابع اصلی ریسک عملیاتی؛

۶-۲-۳- موارد نقض مرتبط با بیانیه ریسک‌پذیری مؤسسه اعتباری؛

۶-۲-۴- جزئیات رویدادهای داخلی و زیان‌های حایز اهمیت ریسک عملیاتی؛

۶-۲-۵- رویدادهای بیرونی مرتبط و تأثیرات بالقوه آن‌ها بر سرمایه مؤسسه اعتباری و سرمایه پوششی ریسک عملیاتی؛

۶-۲-۷- ایجاد درک مشترکی از مفاهیم ریسک عملیاتی به منظور حصول اطمینان از وجود سازگاری بین کارکردهای شناسایی ریسک، طبقه‌بندی منابع در معرض ریسک و اهداف مدیریت ریسک؛

۶-۲-۸- فراهم‌سازی امکان بررسی و ارزیابی مستقل و مناسب از ریسک عملیاتی؛

۶-۲-۹- الزام به بررسی و بازنگری در خط‌مشی‌های مدیریت ریسک عملیاتی در مواقع بروز تغییرات حایز اهمیت در مشخصه ریسک عملیاتی مؤسسه اعتباری.

ماده ۳- هیأت مدیره مؤسسه اعتباری موظف است ضوابط ناظر بر نحوه ارائه خدمات اجاره صندوق امانات به مشتریان را که حداقل باید شامل موارد زیر باشد، به تصویب برساند:

۳-۱- مفاد قرارداد فیما بین، حقوق، مسئولیت‌ها و تعهدات طرفین؛

۳-۲- اخذ تأییدیه از مشتری دایر بر اطلاع از عدم پوشش بیمه‌ای برای محتوای صندوق و الزامی نبودن ابراز محتوای صندوق؛

۳-۳- شرایط دسترسی به محتوای صندوق از جمله نحوه تمهید محیط مناسب خصوصی برای این منظور؛

۳-۴- نحوه اعمال کنترل‌های لازم برای حصول اطمینان از عدم دسترسی اشخاص غیرمجاز به محتوای صندوق؛

۳-۵- محافظت از کلیدهای اصلی و جایگزین و تعویض قفل صندوق‌های تخلیه شده؛

۳-۶- فرآیند احراز هویت و شناسایی اشخاص دارای دسترسی به هر صندوق؛

۳-۷- نگهداری فهرست مراجعات و سوابق فراهم شدن دسترسی برای اشخاص موصوف؛

۳-۸- فرآیند استعلام از مراجع داخلی و بیرونی ذی‌ربط و نیز تشریفات و حداقل تعداد نمایندگان حاضر از طرف مؤسسه اعتباری و تنظیم صورت‌جلسه مقتضی به منظور فراهم نمودن دسترسی برای ضابطان قضایی و انتظامی یا سایر اشخاص ذی‌صلاح.

فصل سوم: وظایف و مسئولیت‌های هیأت عامل

ماده ۴- هیأت عامل مؤسسه اعتباری در راستای مدیریت ریسک عملیاتی موظف به انجام وظایف زیر است:

۴-۱- پیاده‌سازی چارچوب مدیریت ریسک عملیاتی از طریق استقرار نظام‌ها و فرایندهای سازگار با مشخصه ریسک عملیاتی و میزان تحمل و پذیرش ریسک مؤسسه اعتباری در تمامی محصولات و فعالیت‌ها و نیز به کارگیری راهبردهای مصوب هیأت مدیره در خصوص مدیریت ریسک به صورت کارا و اثربخش؛

۴-۲- تعیین واحد اجرایی مسئول مدیریت ریسک عملیاتی و یا عنداللزوم ایجاد واحد مزبور به صورت مستقل با تعیین شرح وظایف و اختیارات تفصیلی مطابق با ضوابط ناظر بر حاکمیت شرکتی؛

۴-۳- شناسایی، ارزیابی، اندازه‌گیری، کنترل و کاهش مؤثر ریسک عملیاتی مؤسسه اعتباری ناشی از:
۴-۳-۱- عوامل بیرونی نظیر وقوع بلایای طبیعی و اقدامات مجرمانه از سوی اشخاص غیرکارمند که منجر به ایراد خسارت به مؤسسه اعتباری می‌گردد؛
۴-۳-۲- عوامل درونی نظیر نامناسب بودن سیاست‌ها، رویه‌ها و کنترل‌های موجود در مؤسسه اعتباری، خطاهای مربوط به ورود اطلاعات، مستندسازی ناصحیح، نگهدای نامناسب از سخت‌افزارها، نرم‌افزارها و تجهیزات؛

فصل چهارم: سایر

ماده ۵- ضوابط اجرایی ناظر بر مفاد این دستورالعمل و مباحث ویژه در مدیریت ریسک عملیاتی نظیر محصولات و خدمات جدید، برون‌سپاری، سیستم‌ها و زیرساخت‌های فناوری اطلاعات توسط بانک مرکزی تدوین و به شبکه بانکی ابلاغ می‌شود.

«دستورالعمل حداقل الزامات مدیریت ریسک عملیاتی در مؤسسات اعتباری» مشتمل بر ۵ ماده در چهلمین جلسه مورخ ۱۴۰۰/۸/۸ هیأت عامل بانک مرکزی به تصویب رسید و از تاریخ ابلاغ، لازم‌الاجرا می‌باشد.