آشنایی با مفاهیم و مصادیق ریسک عملیاتی

بـخش چـهـا رم

مصادیق ریسک عملیاتی براساس تعریف کمیته بال

براساس تعریف کمیته بال از ریسک عملیاتی، مهم ترین مصادیق ریسک عملیاتی به شرح زیر است:

تقلب-های داخلی: اختلاس، خیانت در امانت، ....

کلاهبرداری خارجی: چک‌های جعلی، مدارک جعلی، ...

شیوه استخدام و امنیت محل کار: عدم انطباق تخصص‌ها با وظایف

شیوه های نادرست ارائه خدمات: فرآیندهای نامناسب اعطای تسهیلات و پذیرش تعهدات،....

خسارت به دارایی-های فیزیکی: زلزله، تخریب، اغتشاشات خیابانی، ناآرامی های اجتماعی، ...

خطای سیستم و شکست تجاری: تغییر سیستم-های رایانه ای، ...

مدیریت اجرا، مدیریت تحول و فرآیندها: بخشنامه ها و دستورالعمل های مبهم، ...

البته می-توان موارد زیر را نیز به فهرست بالا اضافه کرد:

فناوری-های کاملاً خودکار : در صورت عدم امکان تغییر در برخی از روش‌ها، به منظور ارائه خدمات براساس قوانین محلی

برون سپاری : عدم توانایی شرکت‌های پیمانکار در برآورد نیازهای سازمان

با توجه به تعریفی که از ریسک عملیاتی ارایه شد، مصادیق آن به تفکیک عوامل (منابع) ایجادی عبارتند از:

رویدادهای مربوط به درون سازمان

نقض دستورالعمل‌های داخلی، سیاست ها و رویه ها.

سوء استفاده کارکنان سازمان شامل اختلاس، ارتشا، ارایه گزارش های غلط(عمدی یا سهوی به ویژه در مورد مانده حساب ها)، سرقت، مبادلات غیر قانونی به حساب شخصی خود، خیانت در امانت، جعل اسناد و چک ها، دسترسی غیر مجاز به حساب مشتریان، سوء استفاده از اطلاعات محرمانه مشتری، فعالیت های تجاری نامناسب به حساب بانک، حیف و میل اموال و دارایی ها و نادیده گرفتن مقررات.

انتشار انواع ویروس‌های رایانه ای در رایانه ها و شبکه های رایانه ای.

پولشویی.

عدم کفایت نظارت بر کارکنان.

رویدادهای مربوط به اختلالات کاری و نواقص سیستم

عدم کفایت نحوه نگهداری و مدیریت سخت افزارها و نرم افزارها، شبکه و ارایه دهنده خدمت(Server)

اختلالات کاری و نارسایی سیستم-های مختلف رایانه -ای از قبیل نواقص سخت افزاری و نرم -افزاری، مشکلات مربوط به ارتباطات از راه دور، قطع برق، آب و گاز، استفاده از فناوری های قدیمی و غیر استاندارد.

رویدادهای مربوط به خارج از موسسه

اعمال مجرمانه مانند کلاهبرداری، سرقت، جعل، سوءاستفاده از چک، جرایم رایانه ای و پولشویی

بلایای طبیعی مانند زلزله، آتش سوزی، سیل و...

عملیات تروریستی و نا آرامی های اجتماعی

شیوه های کنترل و مدیریت ریسک عملیاتی

برون سپاری امور

برون سپاری امور می تواند ریسک های متعددی از جمله ریسک های عملیاتی و شهرت را متوجه موسسه کند . از این رو، مبادرت به این امر باید در چارچوب اصول و سیاست‌های مشخص و پس از انجام بررسی ها و مطالعات لازم انجام شود. فعالیت ها و خدماتی را می توان برون سپاری کرد که قانونگذار انجام آن ها را راساً به موسسه تکلیف نکرده باشد .
علاوه بر این، برون سپاری امور نباید به گونه ای انجام شود که به موضوع اصلی فعالیت موسسه اعتباری خدشه وارد کند.

سیستم های فن آوری اطلاعات

هیات مدیره باید اطمینان حاصل کند که سیستم های فن آوری اطلاعات موسسه اعتباری از کفایت لازم برخوردار بوده و متناسب با ماهیت و حوزه عملیات آن است. کفایت و متناسب بودن سیستم های فن آوری اطلاعات باید به طور مستمر نسبت به فعالیت های موسسه و الزامات مقرر مورد ارزیابی قرار گیرد . علاوه بر این، باید بررسی شود که این سیستم ها تا چه حد فعالیت های تجاری را مطابق با مصوبات هیات مدیره مورد پشتیبانی قرار می دهند.

ثبت تراکنش ها

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 آن ها می توانند برون سپاری شوند مشروط بر اینکه موسسه اعتباری اطمینان حاصل کند که شرکت عرضه کننده خدمات فن آوری اطلاعات، در انطباق با اصول ارائه شده قرار دارد.

رویه های کنترل داخلی

موسسه اعتباری باید مدل های اجرا، استانداردها، رویه ها و کنترل هایی را برای حوزه های مختلف تعریف کند، به گونه ای که بتواند بین واحدهای کاری و واحدهای ارائه دهنده خدمات هماهنگی های لازم را ایجاد نماید . در این زمینه برای برنامه ریزی، پایش و ارزیابی امور باید گروه مجزایی، شامل نمایندگانی از واحدهای مختلف کاری تعیین شود.

مستندسازی امور

باید رویه هایی را برای گسترش سیستم ها و کنتر ل کیفی آن ها ایجاد کرد تا اطمینان حاصل شود که سیستم ها به همان ترتیبی که برنامه ریزی شده اند، کار می کنند. علاوه بر این، باید روش مستند سازی ثابتی در مورد سیستم ها وجود داشته باشد تا این اطمینان ایجاد شود که آن ها می توانند حتی در صورت تعویض کارکنان اصلی، به کار خود ادامه دهند.

امنیت اطلاعات

به منظور حفظ امینت اطلاعات ، لازم است بین امور اداری و سازمانی، پرسنلی، فیزیکی، تبادل اطلاعات و امنیت آن ها، سخت افزار و نرم‌افزار، تفکیک مناسبی انجام شود .
امنیت کلی اطلاعات شامل حفظ محرمانه بودن اطلاعات، درستی و در دسترس بودن آن ها است. دسترسی به سیستم باید کنترل شود .
استنکاف از انجام تراکنش ها در سیستم های اطلاعات و شناسایی و تایید طرف های مرتبط متقابل باید به طور مناسب انجام شود .
علاوه بر این، از قابلیت پیگیری دقیق تراکنش های پردازش شده در سیستم های اطلاعات باید اطمینان حاصل شود.

سطح امنیت اطلاعات

به طور کلی سطح امنیت اطلاعات موسسه اعتباری و سطح امنیت سیستم های مختلف اطلاعات با توجه به ماهیت و حوزه عملیات، جدی بودن تهدیدها و نیز سطح کلی توسعه تکنولوژیکی موسسه باید از کفایت لازم برخوردار باشند.