مدلی کاربردی برای ارزیابی ریسک تطبیق در موسسات مالی

فرزانه رجایی سلماسی[۱]

تاریخ: ۱۴۰۳/۰۷/۰۵

چکیده

امروزه دامنه موضوع رعایت قوانین و مقررات (تطبیق) از صرف مقررات و دستورالعمل‌های حاکم بر سازمان فراتر رفته و تکالیف دیگری چون استانداردهای فنی، به‌روش‌ها، منشور اخلاقی و مسئولیت‌های اجتماعی و محیطی را در برمی‌گیرد. ریسک تطبیق یا ریسک ناشی از عدم رعایت تکالیف فوق می‌تواند منجر به تبعات جدی مالی، نظارتی، حقوقی و لطمه به حسن شهرت سازمان شده و می‌بایست توسط روال مدیریت تطبیق شناسایی، ارزیابی و کنترل شود. از طرفی ظهور فناوری‌های نوین منجر به شیوه‌های تجارت و کسب و کار مدرن و در نتیجه مقررات پیچیده‌تر شده که بدین منظور رویکرد مبتنی بر ریسک با هدف اختصاص منابع به موارد پر ریسک‌تر می‌تواند راهگشا باشد. این مقاله ضمن تبیین اجزای سیستم مدیریت تطبیق و سپس بررسی اجمالی روش‌های اتخاذ شده جهت ارزیابی ریسک تطبیق توسط سایر مراجع و شرکت‌های بزرگ حسابرسی و مشاوره مالی، به ارائه مدلی به منظور ارزیابی ریسک تطبیق در موسسات مالی می پردازد. روش پیشنهادی با توجه به تعاریف مدیریت ریسک تطبیق در اسناد سازمان بین‌المللی استانداردسازی (ایزو) و ویژگی‌های این ریسک طراحی شده است. در مدل ارائه شده ضمن توجه به ریسک ذاتی عدم رعایت الزامات و تبعات احتمالی آن، ریسک باقی مانده براساس اندازه‌گیری اثربخشی قدرت راهکارهای کاهش ریسک، ارزیابی می‌گردد.

واژه‌های کلیدی: سیستم مدیریت تطبیق، ارزیابی ریسک تطبیق، ریسک ذاتی، ریسک باقی مانده، کنترل

مقدمه

بحران مالی سال ۲۰۰۷ نقطه عطفی در شناخت اهمیت موضوع رعایت قوانین و مقررات بوده است. ضعف در رعایت مقررات مالی و
نظارتی، نظام مالی کل جهان را در معرض ریسک سیستمیک[۱] قرار داده و منجر به ورشکستگی های زنجیره وار موسسات مالی برخی کشورها شد. این رخداد ضرورت شناخت محیط مقرراتی و ارزیابی ریسک عدم رعایت قوانین و مقررات را بیش از پیش مشخص نموده و به تبع آن موسسات مالی و نهادهای نظارتی را به سمت توسعه و پیاده سازی برنامه‌های موثر مدیریت ریسک عدم رعایت سوق داده است. مقررات کمیته بال برای نظارت بانک‌ها[۲] در سال ۲۰۰۵ توجه بانک‌ها و نهادهای مالی را به تبعات عدم رعایت قوانین و مقررات جلب نمود. از نظر کمیته بال، ریسک تطبیق ریسک تبعاتی مانند زیان های مالی، تحریم های حقوقی و قانونی و آسیب به شهرت بانک ها می باشد که در نتیجه عدم انطباق درست با مجموعه قوانین و مقررات، استانداردها و اصول اخلاق حرفه ای[۳] و الزامات مربوطه رخ می‌دهد [1]. عدم رعایت قوانین و مقررات مهمی مانند قوانین مبارزه با پولشویی و تامین مالی تروریسم، الزامات کفایت سرمایه و مقررات شفافیت و افشاگری مالی می تواند عواقب سنگینی برای بانک‌ها داشته باشد. بدین منظور بانک‌ها می‌بایست چارچوب قابل اتکایی به منظور مدیریت ریسک تطبیق[۴] شامل شناسایی ریسک[۵]، ارزیابی ریسک[۶] و کاهش ریسک[۷] داشته باشند [1].

[۱] مدیریت تطبیق و مبارزه با پولشویی، بانک خاورمیانه (نویسنده مسئول) f.rajaie@middleeastbank.ir

ارزیابی ریسک تطبیق یا ریسک رعایت قوانین و مقررات در بانک ها با چالش‌هایی همراه است. گستردگی محیط مقرراتی، تغییرات سریع مقررات و انواع تنبیهات[۸] تعیین شده توسط قانون‌گذار می‌تواند ارزیابی ریسک را پیچیده تر نماید. به منظور ارزیابی کاراتر ریسک می‌بایست از روش یا روش‌هایی استفاده شود که بتواند چالش های مذکور را پوشش دهد. در مقاله حاضر سعی شده که با توجه به محدودیت‌ها و چالش های موجود، مدلی کاربردی و پویا برای ارزیابی ریسک رعایت قوانین و مقررات در بانک‌ها ارائه شود. در این روش بر عواملی چون تبعات ریسک و راهکارهای کاهش ریسک در اندازه‌گیری ریسک تطبیق تمرکز بیشتری شده است. انتظار می‌رود این روش به عنوان ابزاری موثر برای بانک‌های کشور در بهبود فرایندهای ارزیابی و کاهش ریسک‌های ناشی از عدم رعایت قوانین و مقررات عمل نماید.

شایان ذکر است در این نوشته عبارات "ریسک تطبیق"، "ریسک رعایت قوانین و مقررات" و "ریسک عدم رعایت" معانی یکسانی داشته و بجای هم به کار می روند. همچنین عبارات "راهکار کاهش ریسک" و "کنترل ریسک" معانی یکسانی دارند.

پیشینه تحقیق

بررسی سوابق موجود در خصوص مدل های ارزیابی ریسک تطبیق نشان می‌دهد که این موضوع قدمت چندانی نداشته و مطالعات انجام شده محدود می‌باشد. در ادامه به سوابقی که در این حوزه یافت شده اشاره می‌گردد.

در سال ۲۰۱۵ لوزی‌ویک (Losiewicz) در مقاله ای با عنوان "پایش ریسک تطبیق در بانک‌ها" ضمن اشاره به روش اندازه-گیری بر اساس عوامل ریسک احتمال وقوع۹ و شدت تاثیر یا پیامد[۱۰] آن، شاخص‌هایی را به منظور پایش مداوم رعایت قوانین و مقررات معرفی می‌نماید. همچنین به معرفی ابزار و تکنیک هایی که به منظور پایش ریسک تطبیق در بانک های کشور لهستان استفاده شده، می پردازد. [۲]

در همان سال ۲۰۱۵ اساياس و مالر (Esayas & Mahler) در مقاله ای به نام "نگاهی ساختاریافته برای مدل کردن ریسک تطبیق" ضمن اشاره به استفاده از رویکرد مبتنی بر ریسک[۱۱] به دلیل گستردگی الزامات مقرراتی، فرایندی شامل پنج مرحله را برای شناسایی و مدل کردن ریسک تطبیق توسط ابزاری به نام Coras پیشنهاد می‌دهند. [۳]

در سال ۲۰۱۷ استفانی نیکولاس و می (Nicolas & May) در مقاله‌ای با عنوان "طراحی یک برنامه ارزیابی ریسک تطبیق برای یک موسسه مالی" به تبیین چگونگی ساختاردهی برنامه ارزیابی ریسک تطبیق با هدف شناسایی و مدیریت موثر ریسک‌های عدم رعایت در موسسات مالی می‌پردازد. در این طرح پیشنهادی سعی شده احتمال وقوع ریسک تطبیق از طریق کاهش عوامل محرک ریسک، کاهش یافته و منجر به بهبود عملکرد موسسه شود. [۴]

شیدی (Sheedy) و همکارانش در سال ۲۰۱۹ مقاله‌ای درباره‌ی "فرهنگ ریسک تطبیق" منتشر کرده است. این مقاله به بررسی تاثیر فرهنگ سازمانی بر تطبیق ریسک می‌پردازد و به این موضوع اشاره دارد که چگونه ساختارهای انگیزشی و هنجارهای رفتاری می‌توانند در تعیین اولویت‌های مدیریت ریسک در مؤسسات مالی نقش داشته باشند. این تحقیق نشان می‌دهد که تأکید بیشتر بر فرهنگ تطبیق و کاهش تمرکز بر سود کوتاه‌مدت سازمان می‌تواند به بهبود مدیریت ریسک کمک کند. [۵]

بنگار و بندک (Bongar & Benedek) در سال ۲۰۲۱ در مقاله ای با عنوان "یک روش نوین ارزیابی ریسک: مطالعه موردی روش PRISM در بخش‌های حساس به ریسک تطبیق" به معرفی روش ارزیابی ریسک PRIMS که با توجه به روش های ماتریس ریسک[۱۲] (RM) و روش آنالیز حالات شکست و تجزیه وتحلیل آثار[۱۳] (FMEA) طراحی شده می پردازد. روش PRISM همراه با فرایند تحلیل سلسله مراتبی به شناسایی و اولویت بندی ریسک‌ها بر اساس احتمال وقوع و شدت تاثیر کمک می کند. [۶و۷]

در سال ۲۰۲۴ بندک و بنگار در مقاله ای به نام " ارزیابی ریسک تطبیق: نتایج یک مرور جامع بر ادبیات موضوع"، مرور جامعی بر پژوهش‌های مرتبط با موضوع ارزیابی ریسک تطبیق ارائه داده و به بررسی روش های مختلف می پردازند. هدف این مقاله بهبود ابزارهای مورد استفاده و شناسایی بیشتر تبعات عدم رعایت در موسسات مالی است. [۸]

محمد جواد ایروانی در سال ۱۳۹۵ مقاله‌ای با عنوان "نظارت بر ریسک تطبیق در بانک" منتشر کرده است. این مقاله به اهمیت انطباق فعالیت‌های بانکی با قوانین و مقررات پرداخته و تأکید دارد که وجود یک واحد نظارتی برای مدیریت ریسک‌های تطبیق در بانک‌ها ضروری است. در این مقاله به محبوبیت رویکرد یکپارچه‌سازی ریسک‌های عملیاتی و تطبیق نیز اشاره شده است. [۹]

در سال ۱۳۹۶ حاجی شاه‌وردی و تاجینی در مقاله ای با عنوان" مروری اجمالی بر مبانی نظری مدیریت ریسک تطبیق در بانکها و موسسات مالی و اعتباری" ضمن تبیین چارچوب کلی مدیریت ریسک تطبیق در صنعت بانکداری، چارچوب کلی الزامات ناظر بر مدیریت این ریسک را حسب الزامات موجود داخلی و بین‌المللی تشریح می‌نمایند. [۱۰]
در سال ۱۳۹۹ حاجی شاه‌وردی و زمردیان در مقاله‌ای با عنوان " ارزیابی ریسک رعایت (تطبیق) با الگوگیری از اسناد سازمان بین‌المللی استانداردسازی و رهنمودهای کمیسیون تردوی" ضمن بررسی اجمالی اجزای ریسک تطبیق، به شناسایی ریسک-های تطبیق در یکی از بانک های کشور با توجه به اسناد ایزو و کمیسیون ترودوی[۱۴] (COSO) یا کوزو و با استفاده از چک لیست‌ها، نظرسنجی و مصاحبه ساخت‌یافته می‌پردازد. [۱۱]

چارچوب نظری موضوع

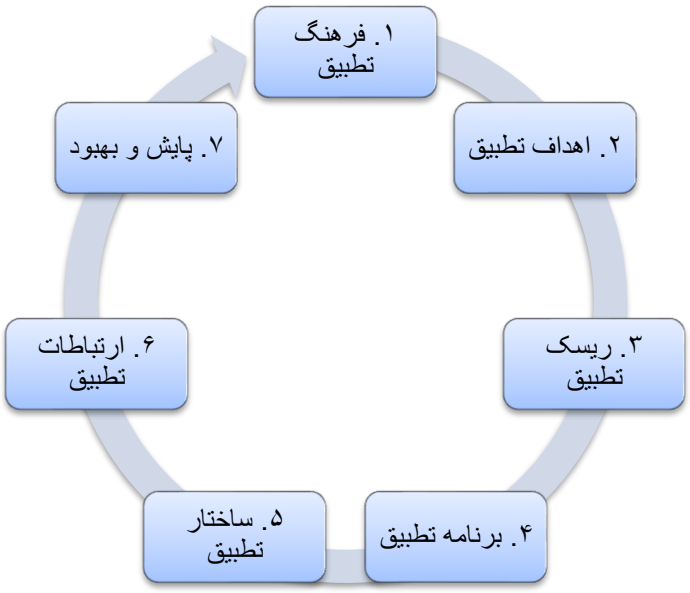
در این بخش کلیاتی از مفاهیم مهم، استانداردها و راهنماهای مربوطه ارائه می شود. بحران‌های مالی پیش آمده در دو دهه گذشته موضوع مدیریت و جلوگیری از ریسک‌ها را به نقطه ثقلی برای ماندگاری خدمات مالی تبدیل کرده است. اینکه یک سازمان بتواند چگونه موضوع عدم قطعیت را مدیریت نماید، در حسن شهرت و ماندگاری کسب و کارش بسیار حیاتی است []. موضوع رعایت قوانین و مقررات در همین سنوات اخیر به تدریج مطرح و مهم‌تر شده تا به سازمان ها کمک نماید با وجود مقررات گسترده و پر از تغییر، اهداف کسب و کار خود را عملی نمایند.
بازل ۲ در سال ۲۰۰۴ چارچوب جامعی برای مدیریت انواع ریسک‌های بانکی ارائه داد و ریسک تطبیق را ذیل ریسک‌های عملیاتی[۱۵] معرفی نمود. کمیته بال در سال ۲۰۰۵، با انتشار مقرراتی (Basel Committee on Banking Supervision) که به ریسک تطبیق توجه ویژه‌ای داشت، زمینه را برای بررسی بیشتر این موضوع فراهم کرد. این مقررات به مؤسسات مالی توصیه می‌کند که استراتژی‌های مؤثری برای شناسایی و مدیریت ریسک تطبیق در نظر بگیرند [۱].
ریسک تطبیق در معنای کلی به معنای ریسک تبعات ناشی از عدم رعایت قوانین و مقررات است. برای بانک‌ها رعایت مقررات مهمی مانند کفایت سرمایه و تسهیلات و تعهدات کلان و نبودن در معرض تبعات ناشی از عدم رعایت آن ها بسیار حیاتی است. همچنین بانک ها ملزم به رعایت مقررات مبارزه با پولشویی، مبارزه با تخلفات و تضاد منافع می‌باشند. قلمرو تطبیق علاوه بر قوانین و مقررات ابلاغ شده از سمت نهادهای قانون‌گذار[۱۶]، شامل استانداردها، اصول اخلاق و رفتار حرفه ای و مسئولیت‌های محیطی و اجتماعی نیز می‌شود. رعایت استاندارد فنی مهمی مانند PCI DSS در حوزه امنیت پرداخت و یا استاندارد ۲۷۰۰۱ در مدیریت امنیت اطلاعات علاوه بر کاهش ریسک دستکاری و یا از دست دادن داده‌ها، به حسن شهرت بانک کمک می‌کند [۱۲]. از طرف دیگر موضوع فرهنگ سازمانی و رعایت منشور اخلاقی بر صحت عملکرد کارکنان و حسن شهرت سازمان بسیار موثر است. همچنین سازمان می‌بایست دستورالعمل‌های خود را مانند کنترل دسترسی و تفکیک وظایف رعایت نماید. بنابراین می‌توان گفت گستردگی قلمرو تطبیق برای بانک‌ها از قوانین و مقررات نهادهای قانون‌گذار تا استانداردهای فنی و دستورالعمل-های داخلی بانک می‌باشد.
با توجه به بزرگی قلمرو تطبیق و اهمیت موضوع رعایت، مدیریت درست ریسک تطبیق را می‌توان از اهداف استراتژیک یک بانک دانست. مدیریت ریسک تطبیق شامل شناسایی، ارزیابی و کاهش ریسک می‌باشد. به منظور مدیریت این ریسک، فرایندها، اجزا و ابزاری کنار هم قرار می‌گیرند و چارچوب مدیریت تطبیق را شکل می‌دهند.

۱. سیستم مدیریت تطبیق

سیستم مدیریت تطبیق[۱۷] (CMS) مجموعه‌ای از استراتژی‌ها، فرایندها، ابزار و کنترل‌ها است که با هدف کاهش ریسک تطبیق با یکدیگر کار کرده و به سازمان کمک می‌کند از رعایت قوانین و مقررات و استانداردهای لازم به اجرا، اطمینان حاصل نماید. سیستم مدیریت تطبیق شامل لایه‌های مختلفی از فرهنگ تطبیق[۱۸] تا ریسک تطبیق و برنامه تطبیق[۱۹] می شود. [۱۳]
استاندارد ایزو ۳۷۳۱۰ یک استاندارد بین‌المللی است که برای ایجاد و پیاده سازی سیستم مدیریت تطبیق استفاده می‌شود [۱۴]. این استاندارد به سازمان‌ها کمک می کند تا یک سیستم مدیریت تطبیق موثر و قابل اعتماد راه اندازی کنند. استاندارد ۳۷۳۰۱ شامل راهنمایی‌هایی در مورد سازمان‌دهی، نظارت و ارزیابی مستمر سیستم مدیریت تطبیق است که بتواند سازمان‌ها را از شناسایی و مدیریت مداوم ریسک‌های تطبیق خود مطمئن نماید [۱۴]. استاندارد مذکور جایگزین استاندارد ایزو ۱۹۶۰۰

با عنوان "راهنماهای سیستم مدیریت تطبیق" می‌باشد. استانداردهای ایزو ۱۹۶۰۰ و ۳۷۳۰۱ بر رویکرد مبتنی بر ریسک در موضوع تطبیق تاکید دارند[۱۴و۱۵]. با رویکرد مبتنی بر ریسک، سازمان‌ها پس از شناسایی و ارزیابی ریسک‌های تطبیق، آنها را با توجه به اهمیت اولویت بندی کرده و با هدف مدیریت بهینه، منابع را به اولویت‌های بالاتر اختصاص می‌دهند [۱۵]. هر دو استاندارد ۱۹۶۰۰ و ۳۷۳۰۱ با استاندارد ۳۱۰۰۰ با عنوان "چارچوب مدیریت ریسک" همسو هستند. ایزو ۳۱۰۰۰ به عنوان استاندارد پایه مدیریت ریسک، اصول کلی و چارچوب ارزیابی و مدیریت انواع ریسک را ارائه می‌دهد[۱۶]، اما ایزو ۳۷۳۰۱ و ۱۹۶۰۰ اصول مذکور را برای مدیریت ریسک تطبیق به کار می‌گیرند. با وجود شباهت های بسیار دو ایزوی ۳۷۳۱۰ و ۱۹۶۰۰، تفاوت‌هایی نیز وجود دارد. ایزو ۳۷۳۰۱ قابل گواهی‌سازی[۲۰] است و سازمان‌ها می توانند با رعایت الزامات آن، اقدام به اخذ گواهینامه رسمی نمایند. هر دو استاندارد به ارائه راهنمای کلی برای پیاده سازی سیستم مدیریت تطبیق می‌پردازند اما ۳۷۳۰۱ دارای الزاماتی برای بهبود سیستم مدیریت بوده و به چرخه معروف طراحی، اجرا، پایش، اقدام[۲۱] (PDCA) پایبند است. همچنین ایزو ۳۷۳۰۱ تاکید بیشتری بر فرهنگ تطبیق دارد.

با توجه به ایزوهایی مذکور، توصیه های کمیته بال و به‌روش هایی[۲۲] که در حوزه مدیریت تطبیق انجام شده است، مدلی شامل هفت عنصر برای سیستم مدیریت تطبیق پیشنهاد شده است. این مدل شامل عناصر کلیدی است که در صورت استقرار درست، منجر به ایجاد یک سیستم موثر و پایدار در سازمان خواهند شد. شکل زیر اجزای سیستم مدیریت تطبیق نشان داده می شود. نکته مهم پایش و بهبود مستمر نهفته در این سیستم است.



شکل ۱. عناصر سیستم مدیریت تطبیق

فرهنگ تطبیق به معنای باور، تعهد و رفتارهای مشترک در تمامی سطوح سازمان برای رعایت قوانین و مقررات، استانداردهای فنی و منشور رفتار و اخلاقی حرفه ای می باشد [۱۳و۱۴]. از جمله مواردی که به جاری سازی فرهنگ تطبیق کمک می کند می توان به تعهد مدیریت ارشد و تاثیر دادن موضوع رعایت قوانین و مقررات در ارتقاء و مزایای کارکنان اشاره نمود.

اهداف تطبیق موفقیت سازمان را در پیاده سازی سیستم مدیریت تطبیق نشان می دهد. اهداف می بایست شفاف، قابل اندازه‌گیری و قابل بهبود باشند. بهینه سازی کنترل‌های کاهش ریسک تطبیق، شناسایی بیشتر نقض قوانین و مقررات و کاهش تذکرات قانون‌گذار می توانند از اهداف تطبیق باشند.

ارزیابی ریسک تطبیق شامل شناسایی ریسک تطبیق و اندازه‌گیری آن است [۲]. با نگاه مبتنی بر ریسک ارزیابی ریسک در حوزه‌های مهم‌تری مانند مبارزه با پولشویی، مبارزه با رشوه و فساد و مقررات احتیاطی[۲۳] انجام شده و با توجه به سطح ریسک‌ها

در یک برنامه تطبیق که شامل راهکارهای کاهش ریسک نیز می باشد، بهبود می یابد. منظور از مقررات احتیاطی، مقرراتی است که توسط نهادهای قانون‌گذاری مالی مانند بانک مرکزی کشورها برای حفظ و ثبات سیستم بانکی وضع شده و عدم رعایت آنها توسط بانک‌ها، تاب‌آوری[۲۴] را کاهش داده و آنها در معرض ورشکستگی قرار می‌دهد [۱۷].

برنامه تطبیق عنصر کلیدی یک سیستم مدیریت تطبیق موثر با هدف کاهش ریسک تطبیق است. این برنامه حداقل شامل فرایندهای شناسایی الزامات قوانین و مقررات، تدوین سیاست‌ها و دستورالعمل‌ها، آموزش و آگاهی رسانی، گزارش‌دهی و مستندسازی و پایش مستمر می باشد [۱۳]. در واقع خروجی ارزیابی ریسک تطبیق پیش نیاز برنامه تطبیق بوده و با توجه به آن برنامه‌ای با هدف کاهش ریسک تعیین می‌شود.

منظور از *ساختار تطبیق* این است که به منظور استقرار سیستم مدیریت تطبیق چه نقش‌ها و مسئولیت‌هایی وجود دارد و خطوط گزارش‌دهی[۲۵] چیست. در ایزو ۳۷۳۰۱ به مجموعه‌ای از بخش‌ها یا افرادی است که وظایف یا اختیاراتی را برای استقرار سیستم مدیریت تطبیق بر عهده دارند، وظیفه یا عملکرد تطبیق[۲۶] اطلاق شده است [۱۴]. بسته به نوع سازمان ممکن است وظیفه تطبیق توسط یک واحد یا چندین واحد مختلف انجام شود. ساختار تطبیق نقش افراد کلیدی را در سیستم مدیریت تطبیق بانک مشخص می‌نماید. نقش و مسئولیت‌های مدیر ارشد واحد تطبیق و همچنین نقش و مسئولیت‌های کمیته تطبیق از عوامل مهم ساختار تطبیق هستند. در این ساختار استقلال وظیفه تطبیق از سایر بخش‌های حاکمیت شرکتی[۲۷] مانند حسابرسی داخلی مشخص می‌شود[۱].

در خصوص *ارتباطات تطبیق*، ایجاد کانال‌های ارتباطی داخلی و خارجی به منظور تبادل اطلاعات آموزشی، اطلاع رسانی در داخل سازمان و آگاهی رسانی‌های مهم به سایر ذینفعان مانند سهامداران، ناظرین و قانون‌گذار حائز اهمیت است. استقرار فرایند افشای محرمانه تخلفات و نحوه رسیدگی به آن از مثال‌های موضوع ارتباطات تطبیق است.

پایش و بهبود تطبیق، هر خللی در سیستم مدیریت تطبیق را پایش نموده و واکنش نشان می دهد. سیستم مدیریت تطبیق باید ابزار و فرایندهایی داشته باشد که به طور مستمر نقض مقررات، موارد مشکوک و ریسک‌های شناسایی شده را پایش نماید. به عنوان مثال در صورت رخداد تخلف، تخلف می‌بایست مستند و گزارش شده و واکنش لازم صورت گیرد.

دو عامل مهم در بهبود و تغییر سیستم مدیریت تطبیق، بهبود مستمر و شناسایی تغییرات است. به منظور کارکرد بهینه این سیستم لازم است در تمامی هفت جزء گفته شده فرایند بهبود مستمر[۲۸] اعمال شود. همچنین هرگونه تغییر در محیط مقرراتی، کسب و کار سازمان و محصولات خدمات می‌بایست توسط سیستم درک شده و تغییرات لازم در فرایندهای مربوطه داده شود. مدیریت تطبیق باید به گونه‌ای عمل کند که سطح انطباق خود را با هر تغییر بیرونی و داخلی، به‌روزرسانی نماید.

۲. مدیریت ریسک تطبیق

مدیریت ریسک تطبیق مانند سایر ریسک‌های عملیاتی شامل فرایند شناسایی، ارزیابی، اعمال راهکارهای کاهش ریسک و پایش اثر بخشی می باشد. در ادامه مراحل مذکور را با در نظرگرفتن پیاده سازی در بانک توضیح می‌دهیم.

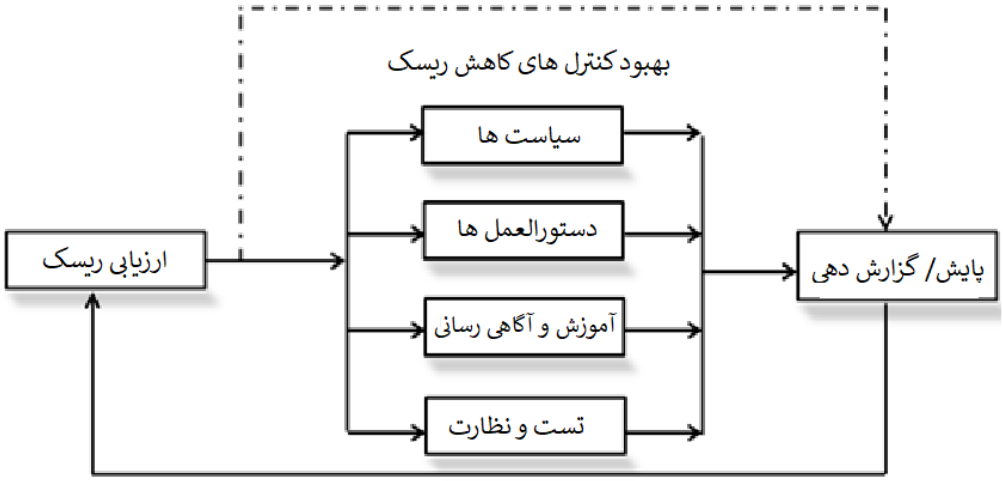
در فرایند شناسایی ریسک تطبیق کلیه الزامات مندرج در قوانین و مقررات، استانداردها و در نهایت محیط مقرراتی که به بانک مربوط است شناسایی شود. سپس ریسک‌های عدم رعایت الزامات مختلف شناسایی و در انباره ریسک تطبیق[۲۹] یا لیستی از ریسک‌های محتمل نگهداری می‌شوند[۴]. به عنوان مثال در خصوص آیین نامه اجرایی ماده ۱۴ الحاقی قانون مبارزه با پولشویی مصوب مجلس شورای اسلامی، الزامات مختلفی وجود دارد که لازم است ریسک عدم رعایت هر کدام جداگانه شناسایی و در انباره ریسک ثبت شود. به منظور شناسایی ریسک تطبیق یک محصول یا فرایند لازم است مقررات، الزامات و دستورالعمل های مربوط به فرایند یا محصول شناسایی شود و سپس ریسک تطبیق برای فرایند یا محصول از طریق ریسک‌های انباره، شناسایی شود. در مقاله حاضر از آنجا که بر ارائه روش ارزیابی ریسک تطبیق متمرکز است، صرفا ریسک عدم رعایت الزام یا مقرره در نظرگرفته شده است.

گام بعد از شناسایی ریسک تطبیق، ارزیابی ریسک شامل اندازه‌گیری و اولویت بندی آن است [۲]. ارزیابی ریسک را می توان به کل گام‌های شناسایی، اندازه‌گیری و اولویت بندی نیز اطلاق نمود. مدل یا نحوه اندازه‌گیری ریسک[۳۰] و اینکه از چه شاخص ها و عواملی استفاده می‌شود، می بایست از قبل تعیین شده باشد. روش مورد استفاده را می توان با توجه به میزان پیچیدگی

سازمان، نوع داده‌های در دسترس و منبع ریسک مشخص نمود. در بخش بعدی در خصوص روش ارزیابی ریسک تطبیق توضیح داده شده خواهد شد.

پس از اندازه‌گیری و ارزیابی ریسک تطبیق، اعمال اقدامات اصلاحی و کنترل های کاهش ریسک ضروری است. اقدامات اصلاحی و کنترل های کاهش ریسک تطبیق شامل اعمال یا بهبود سیاست ها، رویه ها، آموزش و تست و نظارت می شود. ریسک‌ها و کنترل‌های اعمال شده باید مدام پایش شوند. اینکه اقدامات اصطلاحی چقدر اثر بخش بوده و تا چه حد منجر به کاهش ریسک تطبیق مربوطه شده است. نتایج مدیریت ریسک تطبیق می‌بایست به طور منظم به مدیریت ارشد و هیات مدیره بانک گزارش شود [۱].

ارزیابی ریسک تطبیق با محرک‌هایی مانند شناسایی مقرره، محصولات و فرایندهای جدید کسب و کار، تغییر ساختار مالی و مدیریتی سازمان و اصلاح کنترل‌های کاهش ریسک، فراخوانی می شود [۱و۱۴و۱۶]. شکل زیر فرایند مدیریت ریسک تطبیق را به طور خلاصه نشان می‌دهد.



شکل ۲. فرایند مدیریت ریسک تطبیق

۳. مدل های اندازه‌گیری ریسک

ارزیابی ریسک تطبیق به عنوان یکی از ارکان مهم سیستم مدیریت ریسک تطبیق، نیازمند به کارگیری مدلی اثربخش و قابل اعتماد است. به طور کلی مدل های ارزیابی ریسک به دو دسته کمی و کیفی و ترکیبی از این دو تقسیم می شوند. مدل های کمی بر اساس داده ها و شاخص های آماری و مدل های کیفی با توجه به تجربه و تحلیل سناریو عمل می کنند [۱۸]. علاوه بر این دسته بندی، مدل‌هایی بر اساس محوریت دارایی، تهدید و آسیب پذیری[۳۱] و تبعات احتمالی مورد استفاده قرار گرفته‌اند. انتخاب روش ارزیابی بستگی به معیارهایی نظیر حجم و دقت داده ها، پیچیدگی اندازه‌گیری، ماهیت تبعات ریسک، اثربخشی راهکارهای کاهش ریسک و حیاتی بودن عامل زمان دارد. با توجه به آنکه ریسک تطبیق ذیل ریسک عملیاتی قرار می‌گیرد، در ادامه به چند مدل رایج در اندازه‌گیری ریسک عملیاتی اشاره می‌شود.

یک مدل پایه برای اندازه‌گیری ریسک‌های عملیاتی، مدل ماتریس ریسک یا حاصل ضرب احتمال وقوع در میزان یا شدت تاثیر به صورت کیفی است. در این روش عوامل احتمال وقوع و میزان تاثیر از یک تا پنج رده بندی شده و سپس در هم ضرب می شود [۲]. نتیجه حاصله نیز رده بندی شده که مبنایی برای اولویت بندی ریسک‌ها در فرایند مدیریت ریسک خواهد بود. مبنای رده بندی احتمال وقوع، شدت تاثیر و نتیجه ریسک و معنای آنها در جدول ۱ قابل مشاهده است. با ضرب دو عامل احتمال وقوع و میزان تاثیر ماتریس ریسک تشکیل می‌شود که در شکل ۳ نشان داده شده است.

جدول ۱
رده بندی عوامل احتمال وقوع، شدت تاثیر و نتیجه ریسک

رده بندی	احتمال وقوع	شدت تاثیر	نتیجه ریسک
سطح یک	بسیار کم	قابل اغماض	بسیار کم– نیازی به اقدام فوری ندارد.
سطح دو	کم	در حدود آستانه اهمیت	کم– پایش می شود و شاید نیاز به اقدام داشته باشد.
سطح سه	متوسط	تا سه برابر آستانه اهمیت	متوسط– بهتر است طرحی برای کنترل یا کاهش آن در نظر گرفته شود.
سطح چهار	زیاد	بین سه تا ده برابر آستانه اهمیت	بالا– قابل توجه بوده و باید برنامه مشخصی برای کنترل و کاهش آن تدوین و اجرا شود.
سطح پنج	خیلی زیاد	بیش از ده برابر آستانه اهمیت	بسیار بالا– باید در اولویت مدیران قرار گرفته و نیازمند اقدام فوری است.

یک روش دیگر برای اندازه‌گیری ریسک روش آنالیز حالات شکست و تجزیه و تحلیل آثار یا FMEA می باشد که در مقاله [۶] مورد استفاده قرار گرفته است. در این روش که بیشتر برای شناسایی و ارزیابی خرابی‌های احتمالی در یک سیستم می باشد، علاوه بر دو

		احتمال وقوع				
		۱	۲	۳	۴	۵
شدت تاثیر	۵	۲	۳	۴	۵	۵
	۴	۲	۳	۳	۴	۵
	۳	۱	۲	۳	۳	۴
	۲	۱	۲	۲	۳	۳
	۱	۱	۱	۱	۲	۲

شکل ۳. ماتریس ریسک بر اساس احتمال وقوع و شدت تاثیر

عامل احتمال وقوع و شدت تاثیر، قابلیت تشخیص خرابی نیز مد نظر قرار گرفته و عدد اولویت ریسک RPN از حاصل‌ضرب سه عامل بدست می‌آید تا در اولویت بندی ریسک استفاده شود.

روش ارزیابی و خود ارزیابی ریسک و کنترل‌ها[۳۲] یا RCSA روش دیگری است که صرفا در اندازه‌گیری ریسک‌های عملیاتی کاربرد دارد [۱۹]. در این روش واحدهای مختلف سازمان با مشارکت کارکنان به شناسایی ریسک‌های ذاتی[۳۳] و ارزیابی کارایی کنترل‌های موجود می‌پردازند. ریسک ذاتی به معنای ریسک قبل از اعمال کنترل‌های کاهش ریسک است. روش RCSA شامل ارزیابی ریسک ذاتی و ریسک باقی مانده[۳۴] بعد از اعمال کنترل‌ها است. منظور از کنترل راهکارها و اقداماتی است که برای کاهش تبعات ریسک انجام شده است. اثر بخشی کنترل نشان میدهد چقدر یک کنترل توانسته هدف کاهش ریسک را برآورده سازد. در واقع به کارگیری راهکار کاهش ریسک، بر احتمال وقوع تاثیر گذاشته و آن را کاهش میدهد. تعریف ریسک باقیمانده چنین است:

(۱) تاثیر کنترل – ریسک ذاتی= ریسک باقی مانده

همچنین در برخی منابع برای محاسبه ریسک باقی مانده به صورت کمی از فرمول ذیل محاسبه می شود:

(۲) (تاثیر کنترل –۱)* ریسک ذاتی= ریسک باقی مانده

در این فرمول اثربخشی کنترل عددی بین صفر و یک است. در صورتی که هیچ کنترلی نداشته باشیم این عدد صفر شده و ریسک باقیمانده همان ریسک ذاتی است و در صورتی که اثربخشی عدد ۱ باشد ریسک باقی مانده صفر خواهد شد.

۴. راهکارهای کاهش ریسک تطبیق

همانطور که در بخش‌های بالاتر گفته شد، پس از اندازه‌گیری ریسک‌های تطبیق، با توجه به رویکرد مبتنی بر ریسک راهکارها و اقداماتی برای کاهش سریعتر ریسک‌های با اولویت بالاتر می بایست اعمال شوند. کنترل‌های کاهش ریسک تطبیق ذیل کنترل‌های داخلی[۳۵] سازمان بوده و به طور کلی به سه نوع اصلی پیشگیرانه، کشف کننده و اصلاحی طبق بندی می شوند [۱۰].

کنترل‌های پیشگیرانه[۳۶] با هدف جلوگیری از وقوع ریسک استقرار می یابند. این کنترل ها می توانند احتمال وقوع ریسک را کاهش داده یا تاثیر نامطلوب ریسک را کاهش دهند. با توجه به اینکه پیش بینی وقوع ریسک امری مشکل است، شناسایی و طراحی کنترل‌های پیشگیرانه به نحوی که موثر واقع شوند، فعالیتی دشوار و پیچیده است. کنترل های پیشگیرانه می توانند بخشی از ریسک‌های ذاتی را کاهش دهند. کنترل های پیشگیرانه مواردی از جمله کنترل های فیزیکی، محدود کردن دسترسی، استفاده از رمز عبور می‌باشد. در حوزه ریسک تطبیق اعمال سیاست‌ها و رویه‌ها، آموزش و آستانه‌های تعیین شده به صورت سیستمی از نوع کنترل های پیشگیرانه می‌باشند.

کنترل های کشف کننده[۳۷] خطا یا عدم انطباق را بعد از رویداد کشف می کنند. شناسایی مشکلات و خطاها با این کنترل‌ها بوده که می تواند منجر به اقدامات اصلاحی از جمله طراحی کنترل پیشگیرانه جدید شوند. بررسی لاگ‌های سیستم و بررسی مغایرت‌ها می‌تواند از مثال‌های این نوع کنترل باشند. شناسایی تراکنش‌های مشکوک، تست و نظارت سیستمی و حسابرسی از کنترل‌های کشف کننده در حوزه تطبیق است.

کنترل های اصلاحی[۳۸] برای رفع مشکلات پس از شناسایی به کار می روند. استفاده از این نوع کنترل‌ها در سیستم‌های امنیتی بیشتر است. برنامه‌های پاسخ به حوادث سایبری و مسدود کردن کارت در صورت شناسایی تقلب مثالی برای کنترل‌های اصلاحی هستند.

با نگاهی مجدد به فرمول .. یاد آوری می‌شود که با کاهش احتمال وقوع و یا شدت تاثیر می‌توان نتیجه ریسک را کاهش داد. با اعمال کنترل‌های پیشگیرانه مطلوب احتمال وقوع ریسک کاهش می‌یابد. اما کنترل‌های کشف کننده و اصلاحی بیشتر از تاثیر نامطلوب ریسک می‌کاهند. در خصوص ریسک‌هایی که در داخل سازمان رخ می‌دهند (مانند تخلف کارکنان) می توان با قوی‌تر کردن کنترل‌های پیشگیرانه احتمال رخداد را کاهش داد. در مورد ریسک‌هایی که منشا آن در محیط بیرون است (مانند زلزله) می بایست از تبعات احتمالی آن کاست. همچنین وقتی دامنه تبعات رخداد ریسکی به بیرون از سازمان می‌رسد، تمرکز بر کاهش احتمال وقوع با استفاده بهینه‌تر از کنترل‌های پیشگیرانه راه حل بهتری است. به عنوان مثال اگر تبعات یک ریسک عملیاتی مانند خطای انسانی محدود و داخل سازمان باشد استقرار بیشتر کنترل‌های کشف کننده و اصلاحی، می تواند اثربخش باشد اما در خصوص ریسک عدم رعایت مقررات احتیاطی بانک مرکزی که تبعات آن می تواند در حد تنبیهات قانونی مراجع بیرونی باشد، تمرکز بیشتر بر اقدامات پیشگیرانه است.

هزینه اعمال کنترل‌های پیشگیرانه معمولاً بالاتر از سایر کنترل‌ها است. دیدگاه مبتنی بر ریسک می‌تواند به اولویت بندی ریسک‌هایی که نیاز بیشتر به کنترل‌های پیشگیرانه دارد کمک کند. جدول ذیل پیشنهادی برای استفاده از انواع کنترل با توجه به منشاء و دامنه تبعات در داخل یا خارج بانک می‌باشد.

جدول ۲

کنترل های مورد نیاز با توجه به منشاء و تبعات ریسک

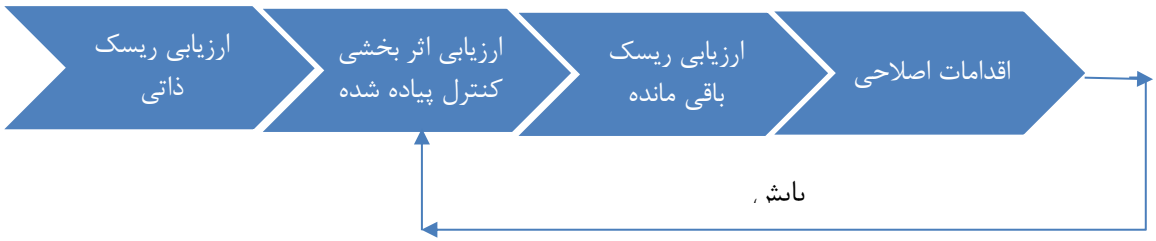
منشاء ریسک	دامنه تبعات	کنترل‌های مورد نیاز به ترتیب اولویت
داخلی	داخلی	کشف کننده_ اصلاحی_ پیشگیرانه
داخلی	بیرونی	پیشگیرانه_ کشف کننده_ اصلاحی
بیرونی	داخلی	اصلاحی_ پیشگیرانه_ کشف کننده
بیرونی	بیرونی	پیشگیرانه_ اصلاحی_ کشف کننده

ارزیابی ریسک تطبیق بر اساس روش پیشنهادی

روش پیشنهادی ترکیبی از روش‌های کمی و کیفی، ماتریس ریسک و به ویژه RCSA که در بخش نظری توضیح داده شده، می‌باشد. در این روش نیز محاسبه ریسک ذاتی و ارزیابی اثربخشی کنترل مربوطه دو عامل اندازه‌گیری ریسک می‌باشند اما محاسبه این دو عامل بر اساس تعریف ریسک تطبیق و به‌روش های مدیریت سیستم مدیریت تطبیق است. این مدل نیز مانند روش RCSA دارای مزایایی است. شفافیت در کنترل‌ها، مشارکت کارکنان، انعطاف پذیری، توانایی شناسایی سریع تغییرات و بهبود مداوم از مزایای روش‌هایی است که از قدرت یا اثربخشی کنترل در اندازه‌گیری ریسک استفاده می کنند.

شایان ذکر است روش پیشنهادی ریسک عدم رعایت یک الزام یا یک مقرره را محاسبه می نماید. برای محاسبه ریسک تطبیق یک محصول یا فرایند که چندین الزام یا مقرره در آن اعمال شده است، می بایست ابتدا ریسک عدم رعایت هر الزام با توجه به احتمال وقوع در آن محصول یا فرایند محاسبه و سپس ریسک تجمعی اندازه‌گیری شود. ریسک تطبیق فرایند یا محصول در این مقاله بررسی نمی‌شود.

به منظور ارزیابی ریسک عدم رعایت یک الزام ابتدا ریسک ذاتی مقرره یا الزام مشخص می‌شود. در مرحله بعد قدرت کنترل کاهش ریسک عدم رعایت مقرره ارزیابی می شود که از نظر قدرت اثربخشی در چه حد است. با توجه به ریسک ذاتی و قدرت کنترل پیاده شده، ریسک باقی مانده مقرره یا الزام بدست می آید. با توجه به اولویت‌ها و سطح ریسک باقی مانده وبا رویکرد مبتنی بر ریسک اقدامات اصلاحی تعیین و کنترل‌ها بهبود می‌یابند. پس از آن دوباره کنترل موجود ارزیابی و ریسک باقی مانده مجدد اندازه‌گیری شده تا از اثربخشی بهبود کنترل‌ها اطمینان حاصل شود. این فرایند پایش و بهبود مستمر منطبق با چرخه PDCA (طراحی، اعمال، ارزیابی، اقدام) که اساس برنامه تطبیق است، می باشد. فرایند مذکور در شکل ۴ نشان داده شده است.



شکل ۴. مراحل ارزیابی و کاهش ریسک مقرره

۱. ارزیابی ریسک ذاتی مقرره

همانطور که در بالاتر نیز اشاره شد، یک مدل پایه برای محاسبه ریسک ذاتی عدم رعایت یک مقرره، حاصل‌ضرب احتمال عدم رعایت در شدت تاثیر قبل از اعمال کنترل کاهش ریسک می‌باشد. در روش پیشنهادی احتمال وقوع ریسک ذاتی عدم رعایت، به دلیل عدم وجود کنترل کاهش احتمال و همچنین برای محاسبه ساده‌تر، یک فرض می‌شود. بنابراین اندازه ریسک ذاتی بر اساس شدت تاثیر تعیین می‌گردد. با توجه به تعریف ریسک تطبیق، شدت تاثیر را می‌توان با توجه به تبعات مالی، حقوقی و حسن شهرت بانک تعیین نمود.

تبعات مالی: بانک به دلیل عدم رعایت و بی توجهی به مقرره جریمه مالی می‌شود و یا به دلیل خدشه دار شدن کسب و کار متضرر می‌گردد. همچنین ممکن است بانک در صورت پیگیری‌های قانونی هزینه‌هایی متحمل شود. به منظور ارزیابی تبعات مالی بررسی سوابق مشابه در صورت وجود، پیشنهاد می‌شود.

تبعات حقوقی: تبعات حقوقی که برای بانک ممکن است از یک نامه تذکر آمیز تا اخراج، منع ارائه خدمات و ابطال مجوز باشد. همچنین ممکن است مشتریان یا دینفعان طرح دعاوی حقوقی نمایند. در خصوص ارزیابی تبعات حقوقی بسته به نوع تذکر و جریمه و ضمانت عدم اجرای مقرره، قضاوت می‌شود.

تبعات حسن شهرت: بانک به دلیل عدم رعایت مقرره یا الزام به شهرت خود لطمه می زند. خدشه دار شدن وجهه بانک می‌تواند از نزد یک مشتری، بانک دیگر، قانون‌گذار تا در سطح کشوری و بین‌المللی باشد. به منظور ارزیابی تبعات شهرت تحلیل آن با توجه به پرسش‌های ذیل و ارزش ها و فرهنگ سازمانی بانک در زمان تحلیل خواهد بود:

- شهرت بانک نزد چه افرادی خدشه دار شده است؟
- جمعیت این افراد چقدر است؟
- درجه اهمیت این افراد برای بانک چقدر است؟
- دامنه خدشه دار شدن بانک در چه سطحی است؟ (شهر، کشور، بین الملل و ....)
- آیا خدشه دار شدن شهرت بانک مربوط به یک محصول و خدمت کلیدی است؟
- آیا بانک مشتریان فعلی خود را از دست خواهد داد؟

به منظور ارزیابی تبعات همانطور که اشاره شد بررسی سوابق مشابه، بررسی تنبیهات مقرره، انجام مصاحبه با افراد متخصص، و تکمیل پرسشنامه توسط کارکنان مورد استفاده قرار می‌گیرد.

با توجه به آنکه احتمال وقوع ریسک ذاتی تطبیق عدد یک در نظرگرفته شده، ریسک مقرره بر اساس تحلیل تبعات و اثرات عدم رعایت به صورت کیفی صورت می‌گیرد. در این روش فرض می‌شود که هر سه نوع تبعات مذکور از یکدیگر مستقل بوده و تاثیری بر هم ندارند. سه سطح کم، متوسط و زیاد معادل اعداد ۱، ۳ و ۵ برای شدت هرکدام از تبعات در نظرگرفته شده و حاصلضرب آن ها سطح ریسک ذاتی عدم رعایت را تعیین می‌نماید. جدول ۳ سطوح ریسک ذاتی را بر اساس سطوح مختلف تبعات نشان می‌دهد.

جدول ۳

ارزیابی ریسک ذاتی مقرره بر اساس شدت تبعات

تبعات مالی	تبعات حقوقی	تبعات حسن شهرت	نتیجه ریسک ذاتی
۱	۱	۱	۱
۱	۱	۳	۳
۱	۱	۵	۵
۱	۳	۱	۳
۱	۳	۳	۹
۱	۳	۵	۱۵
۱	۵	۱	۵
۱	۵	۳	۱۵
۱	۵	۵	۲۵
۳	۱	۱	۳
۳	۱	۳	۹
۳	۱	۵	۱۵
۳	۳	۱	۹
۳	۳	۳	۲۷
۳	۳	۵	۴۵
۳	۵	۱	۱۵
۳	۵	۳	۴۵
۳	۵	۵	۷۵
۵	۱	۱	۵
۵	۱	۳	۱۵
۵	۱	۵	۲۵
۵	۳	۱	۱۵
۵	۳	۳	۴۵
۵	۳	۵	۷۵

۵	۵	۱	۲۵
۵	۵	۳	۷۵
۵	۵	۵	۱۲۵

سطح بندی ریسک ذاتی بر اساس عدد بدست آمده در جدول بالا در چهار سطح چنین خواهد بود:
سطح ریسک کم: ۱و۳و۵و۹
سطح ریسک متوسط: ۱۵
سطح ریسک بالا: ۲۵و۲۷و۴۵
سطح ریسک بسیار بالا: ۷۵و۱۲۵

۲. ارزیابی قدرت اثربخشی کنترل ریسک تطبیق

پس از بررسی تبعات عدم تطبیق با یک مقرره یا استاندارد و ارزیابی ریسک ذاتی آن، نوبت به ارزیابی قدرت اثربخشی کنترل کاهش ریسک می‌رسد. به منظور ارزیابی قدرت کنترل کاهش ریسک، لازم است انواع کنترل‌های اعمالی کاهش ریسک ذاتی الزام مشخص و قدرت اثربخشی و وزن هرکدام تعیین گردد. مراحل ارزیابی قدرت اثربخشی تمامی کنترل‌های یک الزام به شرح ذیل است:

شکل ۵. مراحل ارزیابی اثربخشی کنترل یک الزام

تعیین انواع کنترل اعمالی: انواع کنترل های اعمال شده با توجه به سیستم مدیریت تطبیق و به‌روش ها توسط بانک تعیین می گردند. در این روش کنترل های ذیل مد نظر قرارگرفته‌اند.
پیشگیرانه: سیاست، دستورالعمل، رویه سیستمی و آموزش
کشف کننده: تست و نظارت
اصلاحی: گزارش دهی
سنجش قدرت هرکنترل: همانطور که در بخش ۴ چارچوب نظری گفته شد، کنترل های پیشگیرانه دارای قدرت بیشتری بوده و از احتمال وقوع می‌کاهند. بنابراین اگر یک کنترل پیشگیرانه باشد، قدرت بالاتری دارد. علاوه بر اهمیت نوع کنترل، سنجش قدرت هرکنترل را می‌توان با توجه به شاخص‌هایی که در جداول ۴ تا ۹ در ذیل پیشنهاد می شود ارزیابی نمود. این شاخص‌ها صرفا جهت راهنمایی بوده و هر بانک می‌تواند شاخص‌هایی را با توجه به ساختار و شرایط خود تعیین نماید.

جدول ۴
شاخص‌های نمونه تعیین قدرت اثر بخشی سیاست و دستورالعمل

سیاست و دستورالعمل
آیا سیاست و دستورالعمل مصوبی برای الزام وجود دارد؟
آیا سیاست و دستورالعمل مصوب منطبق بر آخرین تغییرات مقرره می باشد؟
آیا سیاست و دستورالعمل مصوب به کلیه کارکنان مربوطه ابلاغ شده است؟

جدول ۵
شاخص‌های نمونه تعیین قدرت اثر بخشی آموزش و اطلاع رسانی

آموزش و آگاهی رسانی
آیا آموزش کافی برای الزام در سطوح مربوطه وجود دارد؟
آیا کارکنان از عواقب عدم رعایت الزام مطلع هستند؟
آیا آموزش های مربوطه مرتب به‌روزرسانی شده و دارای آزمون هستند؟

جدول ۶

شاخص‌های نمونه تعیین قدرت اثر بخشی رویه‌های سیستمی

رویه سیستمی
آیا تغییرات لازم جهت اعمال در سامانه‌های بانکی شناسایی و انجام شده-اند؟
آیا رویه های سیستمی پیشگیرانه بوده و آستانه های ذکرشده در الزام در سامانه ها پیاده شده است؟

جدول ۷

شاخص‌های نمونه تعیین قدرت اثر بخشی تست و نظارت

تست و نظارت بر اجرا
آیا بازرسی دوره ای از نحوه کنترل الزام انجام می شود؟
آیا برنامه‌ای برای تست‌های موردی کنترل‌ها وجود دارد؟
آیا نحوه رعایت الزام حسابرسی شده است؟
آیا نظارت سیستمی به منظور کشف سیستمی عدم رعایت الزام وجود دارد؟

جدول ۸

شاخص های نمونه تعیین قدرت اثر بخشی گزارش دهی

گزارش دهی
آیا رویه مشخصی برای گزارش دهی وضعیت رعایت الزام به سطوح بالاتر بانک تعیین شده است؟
آیا اقدامات لازم جهت اقدام اصلاحی ابلاغ و اجرا شده‌اند؟

تعیین وزن هر کنترل: بسته به الزام یا مقرره، نقش تمامی کنترل‌ها در کاهش ریسک یکسان نیست. ممکن است در یک الزام، رویه سیستمی نقش بیشتری نسبت به آموزش کارکنان داشته باشد. همچنین برخی کنترل‌ها قابل اعمال نبوده و یا نقش کمتری دارند. بنابراین به منظور ارزیابی قدرت کنترل‌ها، به هر کنترل کاهش ریسک یک مقرره، وزنی نسبت داده می‌شود. به عنوان مثال ممکن است آموزش در الزام اخلاق حرفه ای وزن بسیار بالایی داشته باشد، اما در الزام اعمال سقف نرخ سود سپرده وزنش کمتر باشد و برعکس رویه سیستمی در الزام اعمال سقف نرخ سود مهمتر باشد. تعیین وزن هر کنترل بر اساس نوع الزام و به صورت قضاوتی صورت می گیرد.

محاسبه قدرت کنترل: پس از تعیین قدرت کنترل و وزن هر کنترل نوبت به محاسبه قدرت اثر بخشی کنترل نهایی یک الزام یا مقرره بر اساس فرمول زیر است. در این فرمول که از میانگین وزنی[۳۹] استفاده شده، CS_1 تا CS_n قدرت انواع کنترل برای یک الزام هستند. قدرت هر کنترل عددی بین صفر تا یک در نظر گرفته و وزن نیز بین صفر تا یک می باشد. جمع اوزان باید برابر یک شود. بدین ترتیب خروجی عددی بین صفر و یک خواهد بود.

$$CP = \sum_{1}^{n} CSiWi \qquad where \ \sum_{1}^{n} Wi = 1 \tag{3}$$

دراین فرمول n تعداد کنترل‌ها، CS_i قدرت اثر بخشی کنترل i ام، W_i وزن هر کنترل و CP قدرت اثربخشی نهایی کنترل‌های یک الزام را نشان می‌دهد. بر اساس فرمول فوق عدد نهایی قدرت کنترل یا CP عددی بین صفر یک بدست می آید. به منظور

محاسبه نهایی ریسک باقی مانده، رده بندی CP در سه سطح در جدول ذیل که پیشنهاد می‌شود. تعداد سطوح و آستانه‌ها می‌تواند بر اساس تجربه تغییر یابد.

جدول ۹
سطح بندی قدرت اثر بخشی کنترل

CP<0.4	0.4 <=CP<0.7	0.7<= CP<=1
ضعیف	متوسط	قوی

در بخش بعدی نحوه محاسبه ریسک باقی مانده توضیح داده می شود.

۳. محاسبه ریسک باقی مانده مقرره

با توجه به ریسک ذاتی مقرره یا الزام و قدرت کنترل کاهش ریسک تطبیق آن، ریسک باقی مانده با توجه به فرمول (۲) می‌توان ریسک باقی مانده را به دست آورد. در زیربخش ۱ ریسک ذاتی با توجه به شدت تبعات مختلف در چهار سطح کم، متوسط، زیاد و خیلی زیاد رده بندی شد. در زیربخش ۲ نیز قدرت نهایی اثربخشی کنترل به سه رده کم، متوسط و قوی سطح بندی گردید. در جدول زیر سطوح کیفی برای ریسک ذاتی، قدرت کنترل و ریسک با قی مانده، پیشنهاد شده است. هر چه قدرت کنترل بیشتر باشد، ریسک ذاتی بیشتر کاهش یافته و ریسک باقی مانده کمتر می‌شود. با توجه به سطح ریسک باقی مانده که در جدول نیز اشاره شده، اقدامات اصلاحی تقویت کنترل‌ها تعیین شده و پس از اعمال تغییرات مجدد ریسک مانده ارزیابی می‌گردد. این فرایند، همان فرایند ارزیابی مستمر اثر بخشی کنترل های اعمالی کاهش ریسک تطبیق است.

جدول ۱۰
ارزیابی ریسک باقی مانده

ریسک مانده	قدرت کنترل	ریسک ذاتی
کم	ضعیف	کم
خیلی کم	متوسط	کم
خیلی کم	قوی	کم
متوسط	ضعیف	متوسط
کم	متوسط	متوسط
خیلی کم	قوی	متوسط
زیاد	ضعیف	زیاد
متوسط	متوسط	زیاد
کم	قوی	زیاد
خیلی زیاد	ضعیف	خیلی زیاد
زیاد	متوسط	خیلی زیاد
کم یا متوسط	قوی	خیلی زیاد

۴. بررسی یک مقرره نمونه

به منظور بررسی روش پیشنهادی یک مقرره برای بررسی ریسک ذاتی و قدرت اثربخشی کنترل‌ها در یک بانک انتخاب شد. مشخصات مقرره در ذیل آمده است:

نام مقرره: آیین نامه تسهیلات و تعهدات کلان مصوب سال ۱۳۹۲
مرجع تصویب: شورای پول و اعتبار
دسته بندی مقرره: مقررات احتیاطی
نسخ منسوخ شده دارد: بلی
خلاصه مقرره: این آیین نامه در اجرای بند ۴ ماده ۳۴ قانون پولی و بانکی کشور به منظور محدود نمودن اعطای تسهیلات و تعهدات به

با توجه به آنکه این مقرره از مقررات احتیاطی است و عدم رعایت آن بانک را در معرض تبعات زیاد حقوقی و مالی و شهرتی قرار میدهد، ریسک ذاتی آن خیلی زیاد ارزیابی می شود. به منظور کاهش این ریسک ذاتی بانک هر بانکی کنترل‌هایی را پیاده سازی و اعمال می نماید. در بانک نمونه، کنترل های اعمالی بررسی و امتیاز دهی شد. به عنوان نمونه برای کنترل سیاست و دستورالعمل، امتیاز دهی شاخص‌های مورد استفاده و نتیجه نهایی در شکل زیر نشان داده می‌شود.

شاخص سنجش قدرت	مقدار	امتیاز (از ۰/۲)
نوع کنترل (پیشگیرانه، کشف کننده، اصلاحی)	پیشگیرانه	۰/۲
آیا سیاست و دستورالعمل مصوبی برای الزام وجود دارد؟	بله	۰/۲
در کدام سطح دستورالعمل و سیاست تصویب شده است؟ (هیات مدیره، کمیته تطبیق، واحد اجرایی)	هیات مدیره	۰/۲
آیا سیاست و دستورالعمل مصوب منطبق بر آخرین تغییرات مقرره می باشد؟	بله	۰/۲
آیا سیاست و دستورالعمل مصوب به کلیه کارکنان مربوطه ابلاغ شده است؟	تا حدودی	۰/۱
امتیاز نهایی قدرت کنترل از ۱	۰/۹	

شکل ۶. سنجش قدرت کنترل سیاست و دستورالعمل

بعد از سنجش قدرت هر کنترل و نسبت دادن وزن بر اساس اهمیت هر کنترل در کاهش ریسک عدم رعایت مقرره آیین نامه تسهیلات و تعهدات کلان، ارزیابی قدرت اثربخشی نهایی یا همان CP انجام می شود. شکل ذیل فرایند مذکور را نمایش می-دهد.

انواع کنترل	امتیاز قدرت	وزن قدرت	حاصل
کنترل ۱: وجود سیاست و دستورالعمل (فرهنگ سازی، تهیه مستندات مربوطه و ابلاغ)	۰/۹	۰/۲	۰/۱۸
کنترل ۲: آموزش (آموزش درست به کارکنان مربوطه، آموزش دوره ای، ارزیابی اثر بخشی آموزش)	۰/۸	۰/۱	۰/۰۸
کنترل ۳: پیاده سازی سیستمی (پیاده سازی سیستمی آستانه‌های عددی مقرره، تطابق رویه سیستمی با مقرره)	۰/۵	۰/۳	۰/۱۵
کنترل ۴: تست و نظارت (بازرسی یا حسابرسی دوره ای، انجام تست موردی)	۰/۷	۰/۱	۰/۰۷
کنترل ۵: گزارش دهی (ارائه گزارش دوره ای به هیات مدیره، ابلاغ اصلاحات مورد نیاز)	۰/۴	۰/۳	۰/۱۲
ارزیابی نهایی قدرت کنترل	۰/۶ متوسط		

شکل ۷. قدرت سنجی کنترل نهایی کاهش ریسک عدم رعایت مقرره نمونه

با توجه به ریسک ذاتی عدم رعایت مقرره آیین نامه تسهیلات و تعهدات کلان که "خیلی زیاد" ارزیابی شده و ارزیابی نهایی قدرت اثربخشی کنترل کاهش این ریسک که در این نمونه "متوسط" سنجش شده، با مراجعه به جدول ۱۱ ریسک باقی مانده "زیاد" ارزیابی شده و با توجه به تعریف ریسک بالا در ستون سوم جدول ۱، قابل توجه بوده و باید برنامه مشخصی برای کنترل و کاهش آن تدوین و اجرا شود.

نگاه شرکت های بزرگ به ارزیابی ریسک تطبیق

در این بخش دیدگاه شرکت های بزرگ حسابرسی جهان[۴۰] شامل KPMG، PWC، EY و Deloitte به موضوع ریسک تطبیق به طور خلاصه مطرح می گردد.

شرکت KPMG تاکید زیادی بر ارزیابی ریسک تطبیق به عنوان بخش مهمی از برنامه موثر تطبیق دارد. این شرکت مدلی را برای ارزیابی ریسک تطبیق بر اساس شاخص‌های کلیدی ریسک[۴۱] (KRIs) با توجه به پیشرفت فناوری‌های تحلیل داده، ارائه داده است [۲۱]. ابزارهای تحلیل داده می‌توانند به شناسایی، پیشگیری وپاسخ به داده‌های هشداردهنده کمک کنند و تصمیمات مبتنی بر شواهد را ممکن سازند. شاخص‌های کلیدی ریسک یا KRIs برای شناسایی علائم هشدار دهنده‌ای که می‌تواند منجر به افزایش ریسک سازمان شود استفاده می‌شوند و کمک می‌کنند تا ریسک‌ها به موقع شناسایی و مدیریت شوند [۱۸]. شرکت KPMG همچنین یک مدل بلوغ برای ادغام تحلیل داده در مدیریت تطبیق ارائه کرده که به مدیران این امکان را می‌دهد تصمیمات بهتری برای مدیریت ریسک‌های تطبیق اتخاذ نمایند.

شرکت PWC راهنمایی را برای ارزیابی ریسک شامل ریسک تطبیق بر اساس ماتریس ریسک دو عاملی، ارائه نموده است. از نظر PWC تمرکز ارزیابی تطبیق می بایست بر تهدیدات اصلی سازمان بوده و با اشتهای ریسک و ارزیابی ریسک های کسب و کار همسو باشد. این شرکت شاید یک مدل کابردی جامع برای ارزیابی ریسک مطرح نکرده باشد اما خدمات جامعی برای مدیریت ریسک تطبیق در چارچوب حاکمیت شرکتی ارائه داده است. خدمات آنها به سازمان ها کمک می‌کند ارزیابی ریسک خود را بر اساس داده‌های تحلیلی و با استفاده از فناوری های پیشرفته مانند هوش مصنوعی[۴۲] و یادگیری ماشین[۴۳] انجام دهند. [۲۲]

شرکت EY از رویکرد سنتی را با فناوری‌های نوین ترکیب نموده تا بتواند رویکرد جامعی برای مدیریت ریسک تطبیق پیشنهاد نماید. در شناسایی زود هنگام ریسک مانند شناسایی پیش دستانه تخلف و استفاده از نظارت مستمر سیستمی برای کشف موارد عدم تطبیق، از روش های مبتنی بر هوش مصنوعی استفاده می نماید. در مدیریت ریسک تطبیق نگاه سنتی مشتمل بر اجتناب از ریسک، انتقال ریسک، مدیریت و کاهش ریسک و پذیرش ریسک را دارد. [۸]

شرکت Deloitte در راهنمایی در خصوص ارزیابی ریسک تطبیق، ارزیابی این ریسک را از ارزیابی سایر ریسک‌های سازمان متمایز کرده و بر تمرکز بر شناسایی و اولویت بندی ریسک های مهمی که تبعات جدی مالی، حقوقی، عملیاتی و شهرتی دارند، تاکید می‌کند. این شرکت پیشنهاد می نماید این ارزیابی ها باید به طور مرتب به‌روزرسانی شوند و از ماتریس ریسک برای ارزیابی دقیق تر استفاده شود. شرکت Deloitte همچنین مدلی به نام تحلیل سیستماتیک ریسک یکپارچگی[۴۴] (SIRA) برای ارزیابی ریسک تطبیق توسعه داده است. این روش نیز شامل مراحل ارزیابی ریسک ذاتی، شناسایی کنترل‌ها، بررسی اثربخشی کنترل‌ها و اقدامات اصلاحی کاهش ریسک می باشد. تفاوت اصلی مدل ارائه شده در این مقاله با مدل SIRA نحوه ارزیابی کنترل‌های کاهش ریسک می باشد. [۲۳]

این شرکت همچنین استفاده از تجزیه و تحلیل داده‌ها و رباتیک پردازش خودکار[۴۵] (RPA) را برای بهبود کارایی و افزایش قابلیت اطمینان فرایندهای مدیریت ریسک تطبیق توصیه می‌نماید.

خلاصه و نتیجه گیری

ارزیابی ریسک تطبیق یک ابزار حیاتی برای مدیریت ریسک‌های ناشی از قوانین و مقررات و استانداردهای پیچیده سازمان است. این ارزیابی ها نه تنها ریسک‌های حقوقی و مالی را کاهش می‌دهد، بلکه منجر به تقویت فرهنگ سازمانی و بهبود حسن شهرت می‌شود. در خصوص بانک‌ها چالش‌های رعایت قوانین و مقررات بیشتر است. این موسسات می‌بایست از رعایت الزامات

و مقررات داخلی و استانداردهای بین‌المللی اطمینان حاصل کنند تا مشمول جریمه‌های سنگین، آسیب‌های جبران ناپذیر به اعتبار بانک یا حتی ممنوعیت انجام برخی فعالیت‌های بانکی، نشوند. بنابراین ارزیابی مداوم ریسک‌های تطبیق به بانک‌ها کمک می‌کند با اتخاذ اقدامات پیشگیرانه و استفاده از فناوری‌های نوین، از آسیب‌های احتمالی جلوگیری نمایند. به عبارت دیگر ارزیابی ریسک تطبیق خود یک کنترل داخلی بسیار حیاتی است که تاثیر به سزایی در ادامه فعالیت بانک ها در محیط پیچیده و پرچالش مقرراتی به دارد.

با توجه به آنکه ریسک تطبیق نوعی ریسک عملیاتی است، تا کنون روش‌هایی مانند ماتریس ریسک، آنالیز حالات شکست و تجزیه و تحلیل آثار، ارزیابی و خود ارزیابی ریسک و کنترل‌ها و شاخص کلیدی ریسک مورد استفاده قرارگرفته‌اند. برخی از این روش‌ها از طرف شرکت‌های بزرگ حسابرسی نیز به همراه استفاده از ابزار تحلیل داده و فناوری های مبتنی بر هوش مصنوعی، پیشنهاد شده‌اند.

در مقاله حاضر ضمن تبیین سیستم مدیریت تطبیق و عناصر تشکیل دهنده آن، فرایند مدیریت ریسک تطبیق شامل شناسایی ریسک، اندازه‌گیری و اولویت بندی، کاهش ریسک و پایش ریسک تشریح شد. در این راستا مدل‌هایی برای اندازه‌گیری ریسک معرفی گردید.

هدف این نوشته ارائه مدلی کاربردی برای ارزیابی ریسک تطبیق در بانک‌ها می باشد. بنابراین روشی برای ارزیابی ریسک تطبیق بر اساس تعریف بازل از ریسک و راهکارهای کاهش ریسک تطبیق در بانک‌ها، پیشنهاد شده و یک نمونه هم مورد بررسی قرار گرفته است.

در روش پیشنهادی ریسک عدم رعایت یک مقرره یا الزام بر اساس ریسک ذاتی و اثربخشی راهکار کنترلی موجود آن محاسبه می‌شود. ابتدا ریسک ذاتی مقرره یا الزام بر اساس تبعات حقوقی، مالی و شهرتی عدم رعایت آن ارزیابی می گردد. سپس نوبت به ارزیابی قدرت نهایی کنترل کاهش ریسک عدم رعایت مقرره با توجه به قدرت اثربخشی هر کنترل و وزن آن است. پس از قدرت سنجی کنترل‌های اعمال شده، ریسک باقی مانده عدم رعایت مقرره بدست می‌آید. با توجه به ریسک باقی مانده می توان اقدامات اصلاحی را به منظور بهبود کنترل‌ها انجام داده و پس از آن ریسک تطبیق را مجدد ارزیابی نمود. این روش علاوه بر اینکه در ارزیابی ریسک عدم رعایت مقررات بانک کاربرد دارد، با تغییراتی نیز در ارزیابی ریسک تطبیق محصولات و خدمات و پروژه های جدید قابل استفاده است.

فهرست منابع

1) Basel Committee on Banking Supervision. (2005). Compliance *and the compliance function in banks*. Basel: Bank for International Settlements.
2) Losiewicz-Dniestrzanska, E. (2015). Monitoring of Compliance Risk in the Bank. *Procedia Economics and Finance*, 26, 800-805.
3) Esayas, S., Mahler, T. (2015). Modelling compliance risk: a structured approach. *Artif. Intell. Law*, 23 (3), 271-300.
4) Nicolas, S., May, P. V (2017). Building an effective compliance risk assessment programme for a financial institution. *In the Journal of Securities Operations & Custody*, 9 (3), 215-224.
5) Sheedy, E., Zhang, L., & Chi Ho Tam, K. (2019). Incentive and Culture in Risk Compliance. *Journal of Banking and Finance*, 107, 105611.
6) Bognár F., Benedek P. (2021). A novel risk assessment methodology: a case study of the PRISM methodology in a compliance management sensitive sector. *Acta Polytechnica Hungarica*, 18 (7), 89-108.
7) Bognár F, Benedek P. (2021). Case Study on a Potential Application of Failure Mode and Effects Analysis in Assessing Compliance Risks. *Risks 2021*, 9(9), 164.
8) Benedek P., Bognár F. (2024). Compliance risk assessment -Results of a comprehensive literature review. *Acta Polytechnica Hungarica*, 21 (6), 243.

۹) ایروانی، م. ج. (۱۳۹۵). نظارت بر ریسک تطبیق در بانک. *همایش علمی پژوهشی یافته های نوین علوم مدیریت، کارآفرینی و آموزش ایران*، ۳.

۱۰) حاجی شاهوردی، د. و تاجدینی، م. (۱۳۹۶). مروری اجمالی بر مبانی نظری مدیریت ریسک رعایت در بانکها و موسسات مالی و اعتباری. *مجله مدیریت، اقتصاد و حسابداری*، شماره ۲۶ و ۲۷.

۱۱) حاجی شاه‌وردی، د. و زمردیان، غ. (۱۳۹۹). ارزیابی ریسک رعایت (تطبیق) با الگوگیری از اسناد سازمان بین‌المللی استاندارد‌سازی و رهنمودهای کمیسیون تردوی (مطالعه موردی یکی از بانک‌های عامل)، *فصلنامه مدیریت کسب و کار*، شماره ۴۸، ۲۷۴-۲۹۱.

12) ISO. (2022). *ISO/IEC 27001:2022 Information technology – Cyber Security and privacy protection Information security management systems – Requirements*. Geneva: International Organization for Standardization.
13) Coglianese, C., & Nash, J. (2021). Compliance management systems: Do they make a difference? In B. van Rooij & D. D. Sokol (Eds.), *Cambridge handbook of compliance*, 755–775.
14) ISO. (2021). *ISO 37301:2021 Compliance management systems – Requirements with guidance for use*. Geneva: International Organization for Standardization.
15) ISO. (2014). *ISO 19600:2014 Compliance management systems – Guidelines*. Geneva: International Organization for Standardization.
16) ISO. (2018). *ISO 31000:2018 Risk management systems – Guidelines*. Geneva: International Organization for Standardization.
17) Brownbridge, M., Kirkpatrick, C., & Maimbo, S. M. (2002). Prudential regulation. *Finance and Development*, 1(1), 1.
18) Evrin, V. (2021). Risk assessment and analysis methods: Qualitative and quantitative. *ISACA JOURNAL*, 28.
19) Kumar, K. N., & Chat, P. (2020). Quantification of regulatory capital for management of operational risk in banks: study from an emerging market economy. *Journal of Operational Risk*, 15(3).
20) KPMG. (2017). *The Compliance Journey Survey – Boosting the value of compliance in changing regulatory climate*. KPMG.
21) Gerlach, J., Stryker, N., Matsuo, & A., & Dookhie, R. (2018). *Harnessing data and analytics to transform compliance*. KPMG.
22) PWC. (2008). *A practical guide to risk assessment*, PricewaterhouseCoopers.
23) Jansen, J. (2018). *Compliance Risk Management, Powers Performance*. Deloitte.

اصطلاحات انگلیسی

[1] Systemic Risk
[2] Basel Committee on Banking Supervision
[3] Ethics Code
[4] Compliance Risk Management
[5] Risk Identification
[6] Risk Assessment
[7] Risk Mitigation
[8] Penalties
[9] Likelihood
[10] Impact
[11] Risk-based Approach
[12] Risk Matrix
[13] Failure Mode and Effect Analysis
[14] Committee Of Sponsoring Organizations of the Tread Way Commission (COSO)
[15] Operational Risk
[16] Regulator
[17] Compliance Management System
[18] Compliance Culture
[19] Compliance Program
[20] Certification
[21] Plan, Do, Check, Act

[22] Best Practices
[23] Prudential Regulations
[24] Resilience
[25] Reporting Lines
[26] Compliance Function
[27] Corporate Governance
[28] Continues Improvement
[29] Compliance Risk Inventory
[30] Risk Measurement Methodology
[31] Threat and Vulnerability
[32] Risk and Control Self-Assessment
[33] Inherent Risk
[34] Residual Risk
[35] Internal Controls
[36] Preventive Controls
[37] Detective Controls
[38] Corrective Controls
[39] Weighted Average
[40] Big Four Accounting Firm
[41] Key Risk Indicators
[42] Artificial Intelligence
[43] Machine Learning
[44] Systematic Integrity Risk Analysis
[45] Robotics Process Automation