فصلنامهٔ پژوهش‌های پولی_ بانکی
سال هجدهم، شمارهٔ ۶۳، بهار ۱۴۰۴
صفحات ۱۶۷_۱۹۷

مدلی کاربردی برای ارزیابی ریسک تطبیق در مؤسسات مالی

فرزانه رجایی سلماسی *

تاریخ دریافت: ۱۴۰۳/۱۱/۱۵ تاریخ پذیرش: ۱۴۰۴/۰۳/۰۴

چکیده

امروزه، دامنهٔ موضوع رعایت قوانین و مقررات (تطبیق) از صرفِ مقررات و دستورالعمل‌های حاکم بر سازمان فراتر رفته و تکالیف دیگری چون استانداردهای فنی، به‌روش‌ها، منشور اخلاقی، و مسئولیت‌های اجتماعی و محیطی را نیز دربرمی‌گیرد. ریسک تطبیق یا ریسک ناشی از عدم‌رعایت تکالیف فوق می‌تواند به تبعات جدی مالی، نظارتی، حقوقی، و لطمه به حسن‌شهرت سازمان منجر، و می‌بایست از طریق روال مدیریت تطبیق شناسایی، ارزیابی، و کنترل شود. از طرفی، ظهور فنّاوری‌های نوین به شیوه‌های تجارت و کسب‌وکار مدرن و در نتیجه مقررات پیچیده‌تر انجامیده است که بدین منظور رویکرد مبتنی بر ریسک با هدف اختصاص منابع به موارد پُرریسک‌تر می‌تواند راهگشا باشد. این مقاله ضمن تبیین اجزای سیستم مدیریت تطبیق و سپس بررسی اجمالی روش‌های اتخاذشده برای ارزیابی ریسک تطبیق از سوی سایر مراجع و شرکت‌های بزرگ حسابرسی و مشاورهٔ مالی، به ارائهٔ مدلی به‌منظور ارزیابی ریسک تطبیق در مؤسسات مالی می‌پردازد. روش پیشنهادی با توجه به تعاریف مدیریت ریسک تطبیق در اسناد سازمان بین‌المللی استانداردسازی (ایزو) و ویژگی‌های این ریسک طراحی شده است. در مدل ارائه‌شده، ضمن توجه به ریسک ذاتی عدم‌رعایت الزامات و تبعات احتمالی آن، ریسک باقی‌مانده براساس میزان اثربخشی قدرت راهکارهای کاهش ریسک ارزیابی می‌شود. با توجه به اندازهٔ ریسک باقی‌مانده، می‌توان اقدامات اصلاحی را به‌منظور بهبود راهکارهای کنترلیِ کاهش ریسک اعمال و پس از آن ریسک تطبیق را مجدد ارزیابی کرد.

واژه‌های کلیدی: سیستم مدیریت تطبیق، ارزیابی ریسک تطبیق، ریسک ذاتی، ریسک باقی‌مانده، کنترل
طبقه‌بندی JEL: G32

* مدیریت تطبیق و مبارزه با پول‌شویی، بانک خاورمیانه (نویسندهٔ مسئول)، f.rajaie@middleeastbank.ir

۱ مقدمه

بحران مالی سال ۲۰۰۷ نقطهٔ 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[1] قرار داد و به ورشکستگی‌های زنجیره‌وار مؤسسات مالی برخی کشورها منجر شد. این رخداد ضرورت شناخت محیط مقرراتی و ارزیابی ریسک عدم‌رعایت قوانین و مقررات را بیش از پیش مشخص کرده و به‌تبع آن مؤسسات مالی و نهادهای نظارتی را به‌سمت توسعه و پیاده‌سازی برنامه‌های مؤثر مدیریت ریسک عدم‌رعایت قوانین و مقررات سوق داده است. مقررات کمیتهٔ بال برای نظارت بانک‌ها[2] در سال ۲۰۰۵ توجه بانک‌ها و نهادهای مالی را به تبعات عدم‌رعایت قوانین و مقررات جلب کرد. از نظر کمیتهٔ بال، ریسک تطبیق همان ریسک تبعاتی مانند زیان‌های مالی، تحریم‌های حقوقی و قانونی و آسیب به شهرت بانک‌ها است که در نتیجهٔ عدم‌انطباق درست با مجموعهٔ قوانین و مقررات، استانداردها و اصول اخلاق حرفه‌ای[3] و الزامات مربوطه رخ می‌دهد (کمیتهٔ بال، ۲۰۰۵). عدم‌رعایت قوانین و مقررات مهمی مانند قوانین مبارزه با پول‌شویی و تأمین‌مالی تروریسم، الزامات کفایت سرمایه و مقررات شفافیت و افشاگری مالی می‌تواند عواقب سنگینی برای بانک‌ها داشته باشد. بدین منظور بانک‌ها می‌بایست چهارچوب قابل‌اتکایی به‌منظور مدیریت ریسک تطبیق[4] شامل شناسایی ریسک[5]، ارزیابی ریسک[6]، و کاهش ریسک[7] داشته باشند (کمیتهٔ بال، ۲۰۰۵).

ارزیابی ریسک تطبیق یا ریسک رعایت قوانین و مقررات در بانک‌ها با چالش‌هایی همراه است. گستردگی محیط مقرراتی، تغییرات سریع مقررات و انواع تنبیهات[8] تعیین‌شده از سوی قانون‌گذار می‌تواند ارزیابی ریسک را پیچیده‌تر کند. به‌منظور ارزیابی کاراتر ریسک، می‌بایست از روش یا روش‌هایی استفاده شود که بتواند این چالش‌ها را پوشش دهد. در این مقال، سعی شده است با توجه به محدودیت‌ها و چالش‌های موجود، مدلی کاربردی و پویا برای ارزیابی

[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

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 به‌عنوان ابزاری مؤثر برای بانک‌های کشور در بهبود فرایندهای ارزیابی و کاهش ریسک‌های ناشی از عدم‌رعایت قوانین و مقررات عمل کند.

شایان ذکر است در این نوشته از نظر نویسندگان مقاله، عبارت‌های «ریسک تطبیق»، «ریسک رعایت قوانین و مقررات»، و «ریسک عدم‌رعایت» معانی یکسانی دارد و به‌جای هم به‌کار می‌روند. همچنین، عبارت‌های «راهکار کاهش ریسک» و «کنترل ریسک» معانی یکسانی دارند.

۲ پیشینهٔ تحقیق

بررسی سوابق موجود در مدل‌های ارزیابی ریسک تطبیق نشان می‌دهد که این موضوع قدمت چندانی ندارد و مطالعات انجام‌شده محدودند. در ادامه، به سوابقی که در این حوزه یافت شده است، اشاره خواهد شد.

لوزی‌ویک[1] (۲۰۱۵) در مقاله‌ای ضمن اشاره به روش اندازه‌گیری براساس عوامل ریسک احتمال وقوع[2] و شدت تأثیر یا پیامد[3] آن، شاخص‌هایی را به‌منظور پایش مداوم رعایت قوانین و مقررات پیشنهاد می‌دهد. همچنین، به معرفی ابزار و تکنیک‌هایی می‌پردازد که برای پایش ریسک تطبیق در بانک‌های کشور لهستان استفاده شده است. (لوزی‌ویک، ۲۰۱۵)

اسایاس و مالر[4] (۲۰۱۵) در مقاله‌ای با اشاره به استفاده از رویکرد مبتنی بر ریسک[5] به‌دلیل گستردگی الزامات مقرراتی، فرایندی پنج‌مرحله‌ای برای شناسایی و مدل‌کردن ریسک تطبیق با ابزاری به نام Coras پیشنهاد می‌دهند. (اسایاس و مالر، ۲۰۱۵)

استفانی نیکولاس و مِی[6] (۲۰۱۷) در پژوهشی به تبیین چگونگی ساختاردهی برنامهٔ ارزیابی ریسک تطبیق با هدف شناسایی و مدیریت مؤثر ریسک‌های عدم‌رعایت در مؤسسات مالی می‌پردازد. در این طرح پیشنهادی، سعی شده است احتمال وقوع ریسک تطبیق از

[1] Losiewicz
[2] likelihood
[3] impact
[4] Esayas & Mahler
[5] risk-based approach
[6] Nicolas & May

طریق کاهش عوامل محرک ریسک، کمتر و به بهبود عملکرد مؤسسه منجر شود. (نیکولاس و مِی، ۲۰۱۷)

شیدی[1] و همکاران (۲۰۱۹) در مطالعه‌ای تأثیر فرهنگ سازمانی بر تطبیق ریسک را بررسی کرده است 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. (شیدی، ۲۰۱۹)

بنگار و بندک[2] (۲۰۲۱) در دو مقاله به معرفی روش ارزیابی ریسک PRIMS که با توجه به روش‌های ماتریس ریسک[3] (RM) و روش آنالیز حالات شکست و تجزیه‌وتحلیل آثار[4] (FMEA) طراحی شده، پرداخته است. روش PRISM همراه با فرایند تحلیل سلسله‌مراتبی به شناسایی و اولویت‌بندی ریسک‌ها براساس احتمال وقوع و شدت تأثیر کمک می‌کند. (بگنار و بندک، ۲۰۲۱)

بندک و بنگار (۲۰۲۴) در پژوهشی مرور جامعی بر پژوهش‌های مرتبط با موضوع ارزیابی ریسک تطبیق ارائه داده و روش‌های مختلف را بررسی کرده‌اند. هدف این مقاله بهبود ابزارهای مورداستفاده و شناسایی بیشتر تبعات عدم‌رعایت در مؤسسات مالی است. (بندک و بگنار، ۲۰۲۴)

ایروانی (۱۳۹۵) در مطالعه‌ای 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.

حاجی‌شاه‌وردی و تاجینی (۱۳۹۶) در مقاله‌ای با عنوان «مروری اجمالی بر مبانی نظری مدیریت ریسک تطبیق در بانک‌ها و مؤسسات مالی و اعتباری» ضمن تبیین چهارچوب کلی مدیریت ریسک تطبیق در صنعت بانکداری، چهارچوب کلی الزامات ناظر بر مدیریت این ریسک را حسب الزامات موجود داخلی و بین‌المللی تشریح کردند.

حاجی‌شاه‌وردی و زمردیان (۱۳۹۹) در مقاله‌ای ضمن بررسی اجمالی اجزای ریسک تطبیق، به شناسایی ریسک‌های تطبیق در یکی از بانک‌های کشور با توجه به اسناد ایزو و

[1] Sheedy
[2] Bongar & Benedek
[3] risk matrix
[4] failure mode and effect analysis

کمیسیون تردوی[1] یاکوزو و با استفاده از چک‌لیست‌ها، نظرسنجی و مصاحبهٔ ساخت‌یافته می‌پردازند.

۳ چهارچوب نظری موضوع

در این بخش، کلیاتی از مفاهیم مهم، استانداردها، و راهنماهای مربوطه ارائه خواهد شد. بحران‌های مالی پیش‌آمده در دو دههٔ گذشته موضوع مدیریت و جلوگیری از ریسک‌ها را به نقطهٔ ثقلی برای ماندگاری خدمات مالی تبدیل کرده است. اینکه یک سازمان چگونه بتواند موضوع عدم‌قطعیت را مدیریت کند در حسن‌شهرت و ماندگاری کسب‌وکارش بسیار حیاتی است (بندک و بگنار، ۲۰۲۴). موضوع رعایت قوانین و مقررات در همین سنوات اخیر به‌تدریج مطرح و مهم‌تر شده است تا به سازمان‌ها کمک کند باوجود مقررات گسترده و پر از تغییر، اهداف کسب‌وکار خود را عملی کنند.

بازل ۲ در سال ۲۰۰۴ چهارچوب جامعی برای مدیریت انواع ریسک‌های بانکی ارائه داد و ریسک تطبیق را ذیل ریسک‌های عملیاتی[2] معرفی کرد. کمیتهٔ بال در سال ۲۰۰۵، با انتشار مجموعه‌مقرراتی[3] که به ریسک تطبیق توجه ویژه‌ای داشت، زمینه را برای بررسی بیشتر این موضوع فراهم کرد. این مقررات به مؤسسات مالی توصیه می‌کند استراتژی‌های مؤثری برای شناسایی و مدیریت ریسک تطبیق در نظر بگیرند (کمیتهٔ بال، ۲۰۰۵).

ریسک تطبیق در معنای کلی به معنای ریسک تبعات ناشی از عدم‌رعایت قوانین و مقررات است. برای بانک‌ها، رعایت مقررات مهمی مانند کفایت سرمایه و تسهیلات و تعهدات کلان و نبودن در معرض تبعات ناشی از عدم‌رعایت آن‌ها بسیار مهم است. همچنین، بانک‌ها ملزم به رعایت مقررات مبارزه با پول‌شویی، مبارزه با تخلفات و تضاد منافع هستند. قلمرو تطبیق علاوه بر قوانین و مقررات ابلاغ‌شده از سوی نهادهای قانون‌گذار[4]، شامل استانداردها، اصول اخلاق و رفتار حرفه‌ای، و مسئولیت‌های محیطی و اجتماعی نیز می‌شود. رعایت استاندارد فنی مهمی مانند PCI DSS در حوزهٔ امنیت پرداخت یا استاندارد ۲۷۰۰۱ در مدیریت امنیت اطلاعات علاوه بر کاهش ریسک دستکاری یا از دست‌دادن داده‌ها، به حسن‌شهرت بانک نیز کمک می‌کند (ایزو ۲۷۰۰۱، ۲۰۲۲). از طرف دیگر، موضوع فرهنگ سازمانی و رعایت منشور اخلاقی بر صحت عملکرد کارکنان و حسن‌شهرت سازمان بسیار مؤثر است. همچنین، سازمان

[1] Committee of Sponsoring Organizations of the Tread Way Commission (COSO)

[2] operational risk

[3] Basel Committee on Banking Supervision

[4] regulator

می‌بایست دستورالعمل‌های خود را مانند کنترل دسترسی و تفکیک وظایف رعایت کند. بنابراین، می‌توان گفت گستردگی قلمرو تطبیق برای بانک‌ها از قوانین و مقررات نهادهای قانون‌گذار تا استانداردهای فنی و دستورالعمل‌های داخلی بانک است.

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 می‌شود. به‌منظور مدیریت این ریسک، فرایندها، اجزا و ابزاری کنار هم قرار می‌گیرند و چهارچوب مدیریت تطبیق را شکل می‌دهند.

۴ سیستم مدیریت تطبیق

سیستم مدیریت تطبیق[1] مجموعه‌ای از استراتژی‌ها، فرایندها، ابزار و کنترل‌هاست که با هدف کاهش ریسک تطبیق با یکدیگر کار کرده و به سازمان کمک می‌کنند از رعایت قوانین و مقررات و استانداردهای لازم‌به‌اجرا، اطمینان حاصل شود. سیستم مدیریتِ تطبیق لایه‌های مختلفی از فرهنگ تطبیق[2] تا ریسک تطبیق و برنامهٔ تطبیق[3]را شامل می‌شود. (کاگلیانس و ناش[4]، ۲۰۲۱)

استاندارد ایزو ۳۷۳۰۱ استانداردی بین‌المللی است که برای ایجاد و پیاده‌سازی سیستم مدیریت تطبیق استفاده می‌شود. این استاندارد به سازمان‌ها کمک می‌کند تا یک سیستم مدیریت تطبیق مؤثر و قابل‌اعتماد راه‌اندازی کنند. استاندارد ۳۷۳۰۱ شامل راهنمایی‌هایی دربارهٔ سازمان‌دهی، نظارت و ارزیابی مستمر سیستم مدیریت تطبیق است که بتواند سازمان‌ها را از شناسایی و مدیریت مداوم ریسک‌های تطبیق خود مطمئن کند (ایزو ۳۷۳۰۱، ۲۰۲۱). استاندارد گفته‌شده جایگزین استاندارد ایزو ۱۹۶۰۰ با عنوان «راهنماهای سیستم مدیریت تطبیق» است (ایزو ۱۹۶۰۰، ۲۰۱۴). استانداردهای ایزو ۱۹۶۰۰ و ۳۷۳۰۱ بر رویکرد مبتنی بر ریسک در موضوع تطبیق تأکید دارند. با رویکرد مبتنی بر ریسک، سازمان‌ها پس از شناسایی و ارزیابی ریسک‌های تطبیق، آن‌ها را با توجه به اهمیت اولویت‌بندی کرده و با هدف مدیریت بهینه، منابع را به اولویت‌های بالاتر اختصاص می‌دهند (ایزو ۱۹۶۰۰، ۲۰۱۴).

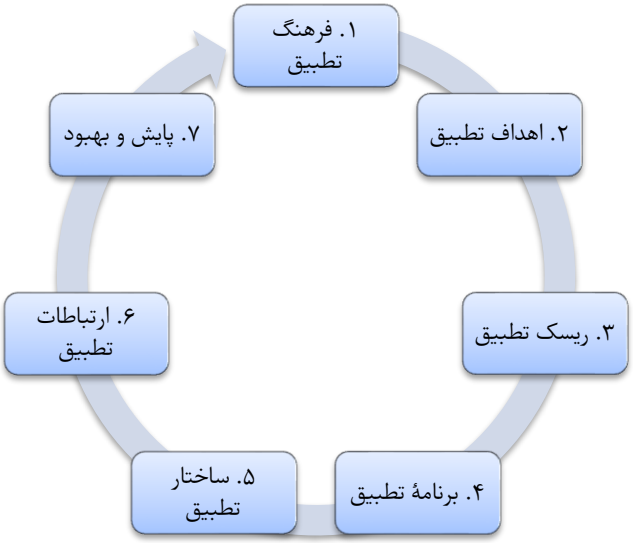
هر دو استاندارد ۱۹۶۰۰ و ۳۷۳۰۱ با استاندارد ۳۱۰۰۰ با عنوان «چهارچوب مدیریت ریسک» هم‌سو هستند. ایزو ۳۱۰۰۰ به‌عنوان استاندارد پایهٔ مدیریت ریسک، اصول کلی و چهارچوب ارزیابی و مدیریت انواع ریسک را ارائه می‌دهد(ایزو ۳۱۰۰۰، ۲۰۱۸)، اما ایزو

[1] Compliance Management System (CMS)
[2] compliance culture
[3] compliance program
[4] Coglianese and Nash

۳۷۳۰۱ و ۱۹۶۰۰ اصول پیش‌گفته را برای مدیریت ریسک تطبیق به‌کار می‌گیرند. باوجود شباهت‌های بسیار دو ایزوی ۳۷۳۱۰ و ۱۹۶۰۰، تفاوت‌هایی نیز بین آن‌ها وجود دارد. ایزو ۳۷۳۰۱ قابلیت گواهی‌سازی[1] دارد و سازمان‌ها می‌توانند با رعایت الزامات آن، اقدام به اخذ گواهینامهٔ رسمی کنند. هر دو استاندارد به ارائهٔ راهنمای کلی برای پیاده‌سازی سیستم مدیریت تطبیق می‌پردازند، اما ۳۷۳۰۱ الزاماتی برای بهبود سیستم مدیریت دارد و به چرخهٔ معروف طراحی، اجرا، پایش، اقدام[2] پایبند است. همچنین؛ ایزو ۳۷۳۰۱ تأکید بیشتری بر فرهنگ تطبیق دارد.

با توجه به ایزوهای گفته‌شده، توصیه‌های کمیتهٔ بال و به‌روش‌هایی[3] که در حوزهٔ مدیریت تطبیق انجام شده، مدلی شامل هفت عنصر برای سیستم مدیریت تطبیق پیشنهاد شده است. این مدل عناصری کلیدی را شامل می‌شود که در صورت استقرار درست، به ایجاد یک سیستم مؤثر و پایدار در سازمان منجر خواهند شد. در شکل ۱، اجزای سیستم مدیریت تطبیق نشان داده شده است. نکتهٔ مهم، پایش و بهبود مستمر نهفته در این سیستم است.

[1] certification
[2] Plan, Do, Check, Act (PDCA)
[3] best practices



شکل ۱. عناصر سیستم مدیریت تطبیق

فرهنگ تطبیق به‌معنای باور، تعهد، و رفتارهای مشترک در تمام سطوح سازمان برای رعایت قوانین و مقررات، استانداردهای فنی، و منشور رفتار و اخلاقی حرفه‌ای است (کاگلیانس و ناش، ۲۰۲۱) و (ایزو ۳۷۳۰۱، ۲۰۲۱). ازجملهٔ مواردی که به جاری‌سازی فرهنگ تطبیق کمک می‌کند، می‌توان به تعهد مدیریت ارشد و تأثیر دادن موضوع رعایت قوانین و مقررات در ارتقا و مزایای کارکنان اشاره کرد.

اهداف تطبیق موفقیت سازمان را در پیاده‌سازی سیستم مدیریت تطبیق نشان می‌دهد. اهداف می‌بایست شفاف، قابل‌اندازه‌گیری و پایش، و بهبودپذیر باشند. بهینه‌سازی کنترل‌های کاهش ریسک تطبیق، شناسایی بیشتر نقض قوانین و مقررات، و کاهش تذکرات قانون‌گذار از اهداف تطبیق هستند.

ارزیابی ریسک تطبیق شامل شناسایی ریسک تطبیق و اندازه‌گیری آن است (لوزی‌ویک، ۲۰۱۵). با نگاه مبتنی بر ریسک، ارزیابی ریسک در حوزه‌های مهم‌تری مانند مبارزه با پول‌شویی، مبارزه با رشوه و فساد، و مقررات احتیاطی[1] انجام شده و با توجه به سطح

[1] prudential regulations

ریسک‌ها در یک برنامهٔ تطبیق که راهکارهای کاهش ریسک را نیز شامل می‌شود، بهبود می‌یابد. منظور از مقررات احتیاطی مقرراتی است که سوی نهادهای قانون‌گذاری مالی مانند بانک مرکزی کشورها برای حفظ و ثبات سیستم بانکی وضع شده و عدم‌رعایت آن‌ها در بانک‌ها، تاب‌آوری[1] را کاهش و بانک‌ها را در معرض ورشکستگی قرار می‌دهد (براون بریج[2] و همکاران، ۲۰۰۲).

برنامهٔ تطبیق عنصر کلیدی یک سیستم مدیریت تطبیق مؤثر با هدف کاهش ریسک تطبیق است. این برنامه حداقل شامل فرایندهای شناسایی الزامات قوانین و مقررات، تدوین سیاست‌ها و دستورالعمل‌ها، آموزش و آگاهی‌رسانی، گزارش‌دهی و مستندسازی، و پایش مستمر است (کاگلیانس و ناش، ۲۰۲۱).

درواقع، خروجی ارزیابی ریسک تطبیق پیش‌نیاز برنامهٔ تطبیق است و با توجه به آن، برنامه‌ای با هدف کاهش ریسک تعیین می‌شود.

منظور از ساختار تطبیق این است که با هدف استقرار سیستم مدیریت تطبیق چه نقش‌ها و مسئولیت‌هایی وجود خواهد داشت و خطوط گزارش‌دهی[3] چه خواهد بود. در ایزو ۳۷۳۰۱، به مجموعه‌ای از بخش‌ها یا افرادی که وظایف یا اختیاراتی را برای استقرار سیستم مدیریت تطبیق بر عهده دارند، وظیفه یا عملکرد تطبیق[4] اطلاق شده است (ایزو ۳۷۳۰۱، ۲۰۲۱).

بسته به نوع سازمان، ممکن است وظیفهٔ تطبیق از سوی یک واحد یا چندین واحد مختلف انجام شود. ساختار تطبیق نقش افراد کلیدی را در سیستم مدیریت تطبیق بانک مشخص می‌کند. نقش و مسئولیت‌های مدیر ارشد واحد تطبیق و همچنین نقش و مسئولیت‌های کمیتهٔ تطبیق از عوامل مهم ساختار تطبیق‌اند. در این ساختار، استقلال وظیفهٔ تطبیق از سایر بخش‌های حاکمیت شرکتی[5] مانند حسابرسی داخلی مشخص می‌شود (کمیتهٔ بال، ۲۰۰۵).

دربارهٔ ارتباطات تطبیق، ایجاد کانال‌های ارتباطی داخلی و خارجی به‌منظور تبادل اطلاعات آموزشی، اطلاع‌رسانی در داخل سازمان و آگاهی‌رسانی‌های مهم به سایر ذی‌نفعان مانند سهامداران، ناظرین و قانون‌گذار حائز اهمیت است. استقرار فرایند افشای محرمانهٔ تخلفات و نحوهٔ رسیدگی به آن از مثال‌های موضوع ارتباطات تطبیق است.

پایش و بهبود تطبیق هر خللی در سیستم مدیریت تطبیق را پایش می‌کند و واکنش نشان می‌دهد. سیستم مدیریت تطبیق باید ابزار و فرایندهایی داشته باشد که به‌طور مستمر نقض

[1] resilience
[2] Brownbridge
[3] reporting lines
[4] compliance function
[5] corporate governance

مقررات، موارد مشکوک، و ریسک‌های شناسایی‌شده را پایش کند؛ به‌عنوان مثال، در صورت رخداد تخلف، می‌بایست تخلف مستند و گزارش شود و واکنش لازم صورت گیرد.

بهبود مستمر و شناسایی تغییرات دو عامل مهم در بهبود و تغییر سیستم مدیریت تطبیق هستند. برای کارکرد بهینهٔ این سیستم لازم است در تمام هفت جزء گفته‌شده فرایند بهبود مستمر[1] اعمال شود. همچنین، هرگونه تغییر در محیط مقرراتی، ساختار سازمان، و محصولات خدمات نیز می‌بایست از سوی سیستم درک و تغییرات لازم در فرایندهای مربوطه داده شود. مدیریت تطبیق باید به‌گونه‌ای عمل کند که سطح انطباق خود را با هر تغییر بیرونی و داخلی به‌روزرسانی کند.

۵ مدیریت ریسک تطبیق

مدیریت ریسک تطبیق مانند سایر ریسک‌های عملیاتی شامل فرایند شناسایی، ارزیابی، اعمال راهکارهای کاهش ریسک، و پایش اثربخشی است. در ادامه، مراحل پیش‌گفته را با درنظرگرفتن پیاده‌سازی در بانک توضیح خواهیم داد.

در فرایند شناسایی ریسک تطبیق، کلیهٔ الزامات مندرج در قوانین و مقررات، استانداردها، و در نهایت محیط مقرراتی‌ای که به بانک مربوط است، شناسایی می‌شود؛ سپس ریسک‌های عدم‌رعایت الزامات مختلف شناسایی و در انبارهٔ ریسک تطبیق[2] یا لیستی از ریسک‌های محتمل نگهداری می‌شوند (نیکولاس و مِی، ۲۰۱۷). به‌عنوان مثال، دربارهٔ آیین‌نامهٔ اجرایی مادهٔ ۱۴ الحاقی قانون مبارزه با پول‌شویی مصوب مجلس شورای اسلامی، الزامات مختلفی وجود دارد که لازم است ریسک عدم‌رعایت هرکدام جداگانه شناسایی و در انبارهٔ ریسک ثبت شود. به‌منظور شناسایی ریسک تطبیق یک محصول یا فرایند، لازم است مقررات، الزامات، و دستورالعمل‌های مربوط به فرایند یا محصول شناسایی، سپس ریسک تطبیق برای فرایند یا محصول از طریق ریسک‌های انباره شناسایی شود. در مقالهٔ حاضر، ازآنجاکه بر ارائهٔ روش ارزیابی ریسک تطبیق متمرکز است، صرفاً ریسک عدم‌رعایت مقرره در نظر گرفته شده است.

گام بعد از شناسایی ریسک، ارزیابی ریسک تطبیق شامل اندازه‌گیری و اولویت‌بندی آن است (لوزی‌ویک، ۲۰۱۵)

[1] continues improvement

[2] compliance risk inventory

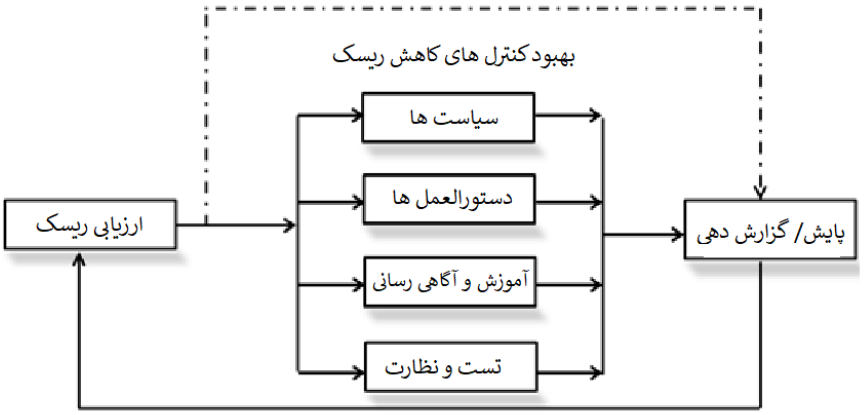
ارزیابی ریسک را می‌توان به کل گام‌های شناسایی، اندازه‌گیری، و اولویت‌بندی نیز اطلاق کرد. مدل یا نحوهٔ اندازه‌گیری ریسک[1] و شاخص‌ها و عواملی که استفاده می‌شود می‌بایست از قبل تعیین شده باشد. روش مورداستفاده را می‌توان با توجه به میزان پیچیدگی سازمان، نوع داده‌های در دسترس و منبع ریسک مشخص کرد. در بخش بعدی، دربارهٔ روش ارزیابی ریسک تطبیق توضیح داده خواهد شد.

پس از اندازه‌گیری و ارزیابی ریسک تطبیق، اعمال اقدامات اصلاحی و کنترل‌های کاهش ریسک ضروری است. اقدامات اصلاحی و کنترل‌های کاهش ریسک تطبیق شامل اعمال یا بهبود سیاست‌ها، رویه‌ها، آموزش، تست و نظارت می‌شود. ریسک‌ها و کنترل‌های اعمال‌شده می‌بایست مدام پایش شوند. باید بررسی شود که اقدامات اصطلاحی چقدر اثربخش بوده و تا چه حد به کاهش ریسک تطبیق مربوطه منجر شده است. نتایج مدیریت ریسک تطبیق می‌بایست به‌طور منظم به مدیریت ارشد و هیئت‌مدیرهٔ بانک گزارش داده شود (کمیتهٔ بال، ۲۰۰۵).

ارزیابی ریسک تطبیق با محرک‌هایی مانند شناسایی مقرره، محصولات و فرایندهای جدید کسب‌وکار، تغییر ساختار مالی و مدیریتی سازمان و اصلاح کنترل‌های کاهش ریسک، فراخوانی می‌شود(کمیتهٔ بال، ۲۰۰۵) ، (ایزو ۳۷۳۰۱، ۲۰۲۱) و (ایزو ۳۱۰۰۰، ۲۰۱۸)

شکل ۲ فرایند مدیریت ریسک تطبیق را به‌طور خلاصه نشان می‌دهد.

[1] risk measurement methodology



شکل ۲. فرایند مدیریت ریسک تطبیق

۶ مدل‌های اندازه‌گیری ریسک

ارزیابی ریسک تطبیق به‌عنوان یکی از ارکان مهم سیستم مدیریت ریسک تطبیق، مستلزم به‌کارگیری مدلی اثربخش و قابل‌اعتماد است. به‌طورکلی، مدل‌های ارزیابی ریسک به دو دستهٔ کمّی و کیفی و ترکیبی از این دو تقسیم می‌شوند. مدل‌های کمّی براساس داده‌ها و شاخص‌های آماری و مدل‌های کیفی با توجه به قضاوت کارشناسانه، تجربه، تحلیل، و توصیف عمل می‌کنند (اورین[1]، ۲۰۲۱). علاوه بر این دسته‌بندی، مدل‌هایی براساس محوریت دارایی، تهدید و آسیب‌پذیری[2]، و تبعات احتمالی مورداستفاده قرارگرفته‌اند. انتخاب روش ارزیابی به معیارهایی مانند حجم و دقت داده‌ها، پیچیدگی اندازه‌گیری، ماهیت تبعات ریسک، اثربخشی راهکارهای کاهش ریسک، و حیاتی‌بودن عامل زمان بستگی دارد. با توجه به آنکه ریسک تطبیق ذیلِ ریسک عملیاتی قرار می‌گیرد، در ادامه به چند مدل رایج در اندازه‌گیری ریسک عملیاتی اشاره خواهد شد.

مدل پایه برای اندازه‌گیری ریسک‌های عملیاتی، مدل ماتریس ریسک یا حاصل‌ضرب احتمال وقوع در میزان یا شدت تأثیر به‌صورت کیفی است. در این روش، عوامل احتمال وقوع و میزان تأثیر از یک تا پنج رده‌بندی شده، سپس در هم ضرب می‌شود (لوزی‌ویک، ۲۰۱۵)

[1] Evrin
[2] Threat and Vulnerability

نتیجهٔ حاصل‌شده نیز رده‌بندی می‌شود و مبنایی برای اولویت‌بندی ریسک‌ها در فرایند مدیریت ریسک خواهد بود. مبنای رده‌بندی احتمال وقوع، شدت تأثیر، و نتیجهٔ ریسک و معنای آن‌ها در جدول ۱ قابل مشاهده است. با ضرب دو عامل احتمال وقوع و میزان تأثیر ماتریس ریسک تشکیل می‌شود که در جدول ۲ نشان داده شده است.

جدول ۱

رده‌بندی عوامل احتمال وقوع، شدت تأثیر، و نتیجهٔ ریسک

رده‌بندی	احتمال وقوع	شدت تأثیر	نتیجهٔ ریسک
سطح یک	بسیار کم	قابل‌اغماض	بسیار کم ــ به اقدام فوری نیازی ندارد
سطح دو	کم	در حدود آستانهٔ اهمیت	کم ــ پایش می‌شود و شاید نیاز به اقدام داشته باشد
سطح سه	متوسط	تا سه برابر آستانهٔ اهمیت	متوسط ــ بهتر است طرحی برای کنترل یا کاهش آن در نظر گرفته شود
سطح چهار	زیاد	بین سه تا ده برابر آستانهٔ اهمیت	بالا ــ قابل‌توجه بوده و باید برنامهٔ مشخصی برای کنترل و کاهش آن تدوین و اجرا شود
سطح پنج	خیلی زیاد	بیش از ده برابر آستانهٔ اهمیت	بسیار بالا ــ مستلزم اقدام فوری است

روش دیگر برای اندازه‌گیری ریسک، روش آنالیز حالات شکست و تجزیه‌وتحلیل آثار یا FMEA است که در مقالهٔ بگنار و بندک، (۲۰۲۱)مورد استفاده قرار گرفته است. در این روش که بیشتر برای شناسایی و ارزیابی خرابی‌های احتمالی در یک سیستم است، علاوه بر دو عامل احتمال وقوع و شدت تأثیر، قابلیت تشخیص خرابی نیز مدنظر قرار گرفته است و عدد اولویت ریسک یا RPN از حاصل‌ضرب سه عامل مذکور به‌دست می‌آید تا در اولویت‌بندی ریسک‌ها استفاده شود. در این روش، به احتمال وقوع، شدت تأثیر، و قابلیت تشخیص خرابی عددی بین یک تا ۱۰ داده می‌شود. هرچه عدد به‌دست آمده بیشتر باشد، ریسک مربوطه در الویت بالاتری برای اعمال اقدامات اصلاحی قرار می‌گیرد. قابلیت تشخیص خرابی درواقع احتمال کشف به‌موقع خرابی، قبل از رسیدن تبعات به مشتری، است. هرچه احتمال کشف خرابی بیشتر باشد، عدد قابلیت تشخیص خرابی کمتر شده و به کاهش RPN یا اولویت ریسک منجر خواهد شد.

جدول ۲. *ماتریس ریسک براساس احتمال وقوع و شدت تأثیر*

		احتمال وقوع				
		۱	۲	۳	۴	۵
شدت تأثیر	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

روش ارزیابی و خودارزیابی ریسک و کنترل‌ها[1] یا RCSA روش دیگری است که صرفاً در اندازه‌گیری ریسک‌های عملیاتی کاربرد دارد(کومار[2]، ۲۰۲۰). در این روش، واحدهای مختلف سازمان با مشارکت کارکنان به شناسایی ریسک‌های ذاتی[3] و ارزیابی کارایی کنترل‌های موجود می‌پردازند. ریسک ذاتی به معنای ریسک پیش از اعمال کنترل‌های کاهش ریسک است. روش RCSA شامل ارزیابی ریسک ذاتی و ریسک باقی‌مانده[4] پس از اعمال کنترل‌های کاهش ریسک است. منظور کنترل راهکارها و اقداماتی است که برای کاهش تبعات ریسک انجام شده است. اثربخشی کنترل نشان می‌دهد چقدر یک کنترل توانسته هدف کاهش ریسک را برآورده سازد. درواقع، به‌کارگیری راهکار کاهش ریسک بر احتمال وقوع تأثیر گذاشته و آن را کم می‌کند. تعریف ریسک باقی‌مانده چنین است:

ریسک باقی‌مانده = ریسک ذاتی – تأثیر کنترل (۱)

همچنین در برخی منابع، برای محاسبهٔ ریسک باقی‌مانده به‌صورت کمّی از رابطهٔ زیر محاسبه می‌شود:

[1] risk and control self-assessment
[2] Kumar
[3] inherent risk
[4] residual risk

(۲) (تأثیر کنترل –۱)* ریسک ذاتی = ریسک باقی‌مانده

در این رابطه، اثربخشی کنترل عددی بین صفر و یک است. درصورتی‌که هیچ کنترلی نداشته باشیم، این عدد صفر شده و ریسک باقی‌مانده همان ریسک ذاتی است و درصورتی‌که اثربخشی عدد ۱ باشد، ریسک باقی‌مانده صفر خواهد شد.

۷ 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 می‌بایست اعمال شود. کنترل‌های کاهش ریسک تطبیق ذیلِ کنترل‌های داخلی[1] سازمان بوده و به‌طورکلی به سه نوع اصلی پیشگیرانه، کشف‌کننده، و اصلاحی طبقه‌بندی می‌شوند (موسسه کی پی ام جی، ۲۰۱۷).

کنترل‌های پیشگیرانه[2] با هدف جلوگیری از وقوع ریسک استقرار می‌یابند. این کنترل‌ها می‌توانند احتمال وقوع ریسک را کاهش دهند یا از تأثیر نامطلوب ریسک بکاهند. با توجه به اینکه پیش‌بینی وقوع ریسک امری مشکل است، شناسایی و طراحی کنترل‌های پیشگیرانه به‌نحوی که مؤثر واقع شوند، فعالیتی دشوار و پیچیده خواهد بود. کنترل‌های پیشگیرانه می‌توانند بخشی از ریسک‌های ذاتی را کاهش دهند. کنترل‌های پیشگیرانه مواردی ازجمله کنترل‌های فیزیکی، محدودکردن دسترسی، استفاده از رمز عبور را شامل می‌شوند. در حوزهٔ ریسک تطبیق، اعمال سیاست‌ها و رویه‌ها، آموزش و آستانه‌های تعیین‌شده به‌صورت سیستمی از نوع کنترل‌های پیشگیرانه‌اند.

کنترل‌های کشف‌کننده[3] خطا یا عدم‌انطباق را بعد از رویداد کشف می‌کنند. شناسایی مشکلات و خطاها با این کنترل‌هاست که می‌تواند به اقدامات اصلاحی ازجمله طراحی کنترل پیشگیرانه جدید منجر شوند. بررسی لاگ‌های سیستم و مغایرت‌ها از مثال‌های این نوع کنترل هستند. شناسایی تراکنش‌های مشکوک، تست و نظارت سیستمی، و حسابرسی از کنترل‌های کشف‌کننده در حوزهٔ تطبیق به‌شمار می‌روند.

[1] internal controls
[2] preventive controls
[3] detective controls

کنترل‌های اصلاحی[1] برای رفع مشکلات پس از شناسایی به‌کار می‌روند. استفاده از این نوع کنترل‌ها در سیستم‌های امنیتی بیشتر است. برنامه‌های پاسخ به حوادث سایبری و مسدودکردن کارت در صورت شناسایی تقلب مثالی برای کنترل‌های اصلاحی هستند.

با نگاهی مجدد به روش ماتریس ریسک یادآوری می‌شود که با کاهش احتمال وقوع یا شدت تأثیر می‌توان نتیجهٔ ریسک را کاهش داد. با اعمال کنترل‌های پیشگیرانهٔ مطلوب، احتمال وقوع ریسک و برخی تبعات کاهش می‌یابد. کنترل‌های کشف‌کننده و اصلاحی بیشتر از تأثیر نامطلوب ریسک می‌کاهند. دربارهٔ ریسک‌هایی که منشأ داخلی دارند (مانند تخلف کارکنان)، امکان کاهش احتمال وقوع با تقویت کنترل‌ها وجود دارد. دربارهٔ ریسک‌هایی که منشأ آن‌ها بیرونی است (مانند زلزله) می‌بایست از تبعات احتمالی آن کم کرد. وقتی دامنع تبعات رخداد ریسکی زیاد بوده و به بیرون از سازمان می‌رسد، تمرکز بر کاهش احتمال وقوع با استفادهٔ بهینه‌تر از کنترل‌های پیشگیرانه راه‌حل بهتری خواهد بود؛ به‌عنوان مثال، اگر تبعات یک ریسک عملیاتی مانند خطای انسانی محدود و داخل سازمان باشد، استقرار بیشتر کنترل‌های کشف‌کننده و اصلاحی می‌تواند اثربخش باشد؛ اما دربارهٔ ریسک عدم‌رعایت مقررات احتیاطی بانک مرکزی که تبعات آن ممکن است در حد تنبیهات قانونی مراجع بیرونی باشد، تمرکز بیشتر بر اقدامات پیشگیرانه است.

هزینهٔ اعمال کنترل‌های پیشگیرانه معمولاً بالاتر از سایر کنترل‌هاست. دیدگاه مبتنی بر ریسک می‌تواند به اولویت‌بندی ریسک‌هایی که نیاز بیشتری به کنترل‌های پیشگیرانه دارد کمک کند. جدول ۳ پیشنهادی برای استفاده از انواع کنترل با توجه به منشأ و دامنهٔ تبعات در داخل یا خارج بانک است.

جدول ۳

کنترل‌های موردنیاز با توجه به منشأ و تبعات ریسک

منشأ ریسک	دامنهٔ تبعات	کنترل‌های موردنیاز به ترتیب اولویت
داخلی	داخلی	کشف‌کننده – اصلاحی ـ پیشگیرانه
داخلی	بیرونی	پیشگیرانه – اصلاحی – کشف‌کننده
بیرونی	داخلی	اصلاحی – پیشگیرانه – کشف‌کننده
بیرونی	بیرونی	پیشگیرانه – اصلاحی – کشف‌کننده

[1] corrective controls

۸ ارزیابی ریسک تطبیق براساس روش پیشنهادی

با توجه به ماهیت ریسک تطبیق و اینکه نوعی ریسک عملیاتی است، روش پیشنهادی ترکیبی از روش‌های کمّی و کیفی، ماتریس ریسک و به‌ویژه روش ارزیابی و خودارزیابی ریسک و کنترل‌ها یا RCSA است که در بخش نظری توضیح داده شد. در این روش نیز محاسبهٔ ریسک ذاتی و ارزیابی اثربخشی کنترل مربوطه دو عامل اندازه‌گیری ریسک‌اند، اما محاسبهٔ این دو عامل براساس تعریف ریسک تطبیق و به‌روش‌های مدیریت سیستم مدیریت تطبیق است. این مدل نیز مانند روش RCSA مزایایی دارد. شفافیت در کنترل‌ها، مشارکت کارکنان، انعطاف‌پذیری، توانایی شناسایی سریع تغییرات، و بهبود مداوم از مزایای روش‌هایی است که از قدرت یا اثربخشی کنترل در اندازه‌گیری ریسک استفاده می‌کنند. داده‌های مورداستفاده در این مدل کاربردی در بیشتر موارد از نوع دادهٔ نرم[1] است و قابلیت جمع‌آوری برای تحلیل آماری را ندارند.

شایان ذکر است روش موردنظر این مقاله ریسک عدم‌رعایت یک الزام یا یک مقرره را محاسبه می‌کند؛ یعنی می‌توان یا ریسک کلی یک مقرره یا دستورالعمل را در نظر گرفت یا ریسک یکی از الزامات مهم آن را محاسبه کرد. برای محاسبهٔ ریسک تطبیق یک محصول یا فرایندی که چندین الزام یا مقرره‌ای در آن اعمال شده است، ابتدا می‌بایست ریسک عدم‌رعایت هر الزام یا مقرره با توجه به احتمال وقوع در آن محصول یا فرایند محاسبه و سپس ریسک تجمعی اندازه‌گیری شود. ریسک تطبیق فرایند یا محصول در این نوشتار بررسی نمی‌شود.

برای ارزیابی ریسک عدم‌رعایت یک الزام ابتدا ریسک ذاتی مقرره یا الزام تعیین می‌شود. در مرحلهٔ بعد، قدرت کنترل کاهش ریسک عدم‌رعایت مقرره ارزیابی می‌شود تا مشخص شود از نظر قدرت اثربخشی در چه حد است. با توجه به ریسک ذاتی و قدرت کنترل پیاده‌شده، ریسک باقی‌ماندهٔ مقرره یا الزام به‌دست می‌آید. با توجه به اولویت‌ها و سطح ریسک باقی‌مانده و با رویکرد مبتنی بر ریسک اقدامات اصلاحی تعیین و کنترل‌ها بهبود می‌یابند. پس از آن، دوباره کنترل موجود ارزیابی و ریسک باقی‌مانده مجدد اندازه‌گیری می‌شود تا از اثربخشی بهبود کنترل‌ها اطمینان حاصل شود. این فرایند پایش و بهبود مستمر منطبق با چرخهٔ PDCA (طراحی، اعمال، ارزیابی، اقدام) است که اساس برنامهٔ تطبیق خواهد بود. فرایند پیش‌گفته در شکل ۳ نشان داده شده است.

[1] soft data

شکل ۳. مراحل ارزیابی و کاهش ریسک مقرره

۹ ارزیابی ریسک ذاتی مقرره

همان‌طور که در قسمت بالا نیز اشاره شد، مدل پایه برای محاسبهٔ ریسک ذاتی عدم‌رعایت یک مقرره، حاصل‌ضرب احتمال عدم‌رعایت در شدت تأثیر قبل از اعمال کنترل کاهش ریسک است. در روش پیشنهادی، احتمال وقوع ریسک ذاتی عدم‌رعایت با فرض وجودنداشتن کنترلی که احتمال وقوع را کاهش دهد، یک فرض محسوب می‌شود. بنابراین، اندازهٔ ریسک ذاتی براساس شدت تأثیر تعیین می‌شود. با توجه به تعریف ریسک تطبیق، شدت تأثیر را می‌توان براساس تبعات مالی، حقوقی، و حسن‌شهرت بانک تعیین کرد.

تبعات مالی: بانک به دلیل عدم‌رعایت و بی‌توجهی به مقرره جریمهٔ مالی می‌شود یا به‌دلیل خدشه‌دارشدن کسب‌وکار متضرر می‌شود. همچنین، ممکن است بانک در صورت پیگیری‌های قانونی هزینه‌هایی نیز متحمل شود.

تبعات حقوقی: تبعات حقوقی می‌تواند شامل مواردی مانند نامهٔ تذکرآمیز، اخراج، منع ارائهٔ خدمات، و ابطال مجوز باشد. همچنین، ممکن است مشتریان یا ذی‌نفعان دعاوی حقوقی طرح کنند. تبعات حقوقی عدم‌رعایت بسته به نوع تذکر و جریمه و ضمانت عدم‌اجرای مقرره قضاوت و تعیین می‌شود.

تبعات حسن‌شهرت: بانک به‌دلیل عدم‌رعایت مقرره به شهرت خود لطمه می‌زند. خدشه‌دارشدن وجههٔ بانک می‌تواند نزد یک مشتری، بانک دیگر یا قانون‌گذار تا سطح کشوری و بین‌المللی باشد. ارزیابی تبعات شهرت می‌تواند از طریق پرسش‌های زیر و با توجه به ارزش‌ها و فرهنگ سازمانی بانک انجام شود:

- شهرت بانک نزد چه افرادی خدشه‌دار شده است؟
- جمعیت این افراد چقدر است؟
- درجهٔ اهمیت این افراد برای بانک چقدر است؟
- دامنهٔ خدشه‌دارشدن حسن‌شهرت بانک در چه سطحی است؟ (شهر، کشور، بین‌الملل و... .)

- آیا خدشه‌دارشدن حسن‌شهرت بانک مربوط به یک محصول و خدمت کلیدی است؟
- آیا بانک مشتریان فعلی خود را از دست خواهد داد؟

به‌منظور ارزیابی تبعات گفته‌شده راهکارهای بررسی سوابق مشابه، بررسی تنبیهات مقرره، انجام مصاحبه با افراد متخصص و تکمیل پرسش‌نامه از سوی کارکنان مورداستفاده قرار می‌گیرد. دربارهٔ تبعات مالی و حقوقی، در برخی موارد قانون‌گذار نهاد مالی ممکن است جرایم مالی و حقوقی عدم‌رعایت را در مقررات تعیین کرده باشد؛ به‌عنوان مثال، در قانون بانک مرکزی مصوب مجلس شورای اسلامی سال ۱۴۰۲، تنبیهاتی برای تخلف از احکام قانون نامبرده و عدم‌رعایت سایر دستورالعمل‌ها و بخشنامه‌های بانک مرکزی تعیین شده است.

با توجه به آنکه احتمال وقوع ریسک ذاتی تطبیق عدد یک در نظر گرفته شده، ریسک مقرره براساس تحلیل تبعات و اثرات عدم‌رعایت به‌صورت کیفی صورت می‌گیرد. در این روش، فرض می‌شود هر سه نوع تبعات مذکور از یکدیگر مستقل‌اند و تأثیری بر هم ندارند. سه سطح کم، متوسط، و زیاد معادل عددهای ۱، ۳، و ۵ برای شدت هرکدام از تبعات در نظر گرفته شده است و حاصل‌ضرب آن‌ها سطح ریسک ذاتی عدم‌رعایت را تعیین می‌کند. جدول ۴ سطوح ریسک ذاتی را براساس سطوح مختلف تبعات نشان می‌دهد.

جدول ۴

ارزیابی ریسک ذاتی مقرره براساس شدت تبعات

تبعات مالی	تبعات حقوقی	تبعات حسن‌شهرت	نتیجهٔ 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

سطح‌بندی ریسک ذاتی براساس عدد به‌دست‌آمده در جدول ۴ در چهار سطح چنین خواهد بود:

سطح ریسک کم: ۱ و ۳ و ۵ و ۹

سطح ریسک متوسط: ۱۵
سطح ریسک بالا: ۲۵ و ۲۷ و ۴۵
سطح ریسک بسیار بالا: ۷۵ و ۱۲۵

۱۰ 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. به‌منظور ارزیابی قدرت کنترل کاهش ریسک، لازم است انواع کنترل‌های اعمالی کاهش ریسک ذاتی یک مقرره یا یکی از الزامات آن مشخص و قدرت اثربخشی و وزن هرکدام تعیین شود. مراحل ارزیابی قدرت اثربخشی تمام کنترل‌های یک مقرره یا الزام به شرح شکل ۴ است:

شکل ۴. مراحل ارزیابی اثربخشی کنترل یک الزام

تعیین انواع کنترل اعمالی: انواع کنترل‌های اعمال‌شده با توجه به سیستم مدیریت تطبیق و به‌روش‌ها از سوی بانک تعیین می‌شوند. در این روش، کنترل‌های زیر مدنظر قرار گرفته‌اند.

پیشگیرانه: سیاست، دستورالعمل، رویهٔ سیستمی و آموزش
کشف‌کننده: تست و نظارت
اصلاحی: گزارش‌دهی

سنجش قدرت هر کنترل: همان‌طور که در بخش ۴ چهارچوب نظری گفته شد، کنترل‌های پیشگیرانه دارای قدرت بیشتری هستند 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 جدول‌های ۵ تا ۱۰ در ادامه پیشنهاد می‌شود ارزیابی کرد. این شاخص‌ها صرفاً برای راهنمایی بوده و هر بانک می‌تواند شاخص‌هایی را با توجه به ساختار و شرایط خود تعیین کند.

جدول ۵

شاخص‌های نمونهٔ تعیین قدرت اثربخشی سیاست و دستورالعمل

سیاست و دستورالعمل
آیا سیاست و دستورالعمل مصوبی برای مقرره یا الزامات آن وجود دارد؟
آیا سیاست و دستورالعمل مصوب منطبق بر آخرین تغییرات مقرره است؟
آیا سیاست و دستورالعمل مصوب به کلیهٔ کارکنان مربوطه ابلاغ شده است؟

جدول ۶

شاخص‌های نمونهٔ تعیین قدرت اثربخشی آموزش و اطلاع‌رسانی

آموزش و آگاهی‌رسانی
آیا آموزش کافی برای الزام یا مقرره در سطوح مربوطه وجود دارد؟
آیا کارکنان از عواقب عدم‌رعایت الزام مطلع‌اند؟
آیا آموزش‌های مربوطه به‌طور مرتب به‌روزرسانی شده و دارای آزمون هستند؟

جدول ۷

شاخص‌های نمونهٔ تعیین قدرت اثربخشی رویه‌های سیستمی

رویهٔ سیستمی
آیا تغییرات لازم جهت اعمال در سامانه‌های بانکی شناسایی و انجام شده‌اند؟
آیا رویه‌های سیستمی پیشگیرانه بوده و آستانه‌های ذکرشده در الزامات مقرره در سامانه‌ها پیاده شده است؟

جدول ۸

شاخص‌های نمونهٔ تعیین قدرت اثربخشی تست و نظارت

تست و نظارت بر اجرا
آیا بازرسی دوره‌ای از نحوهٔ کنترل مقرره یا الزام انجام می‌شود؟
آیا برنامه‌ای برای تست‌های موردی کنترل‌ها وجود دارد؟
آیا نحوهٔ رعایت الزام حسابرسی شده است؟
آیا نظارت سیستمی به‌منظور کشف سیستمی عدم‌رعایت الزام وجود دارد؟

جدول ۹

شاخص‌های نمونهٔ تعیین قدرت اثربخشی گزارش‌دهی

گزارش‌دهی
آیا رویهٔ مشخصی برای گزارش‌دهی 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 تمام کنترل‌ها در کاهش ریسک یکسان نیست. ممکن است در یک مقرره، رویهٔ سیستمی نقش بیشتری نسبت به آموزش کارکنان داشته باشد. همچنین، برخی کنترل‌ها قابل‌اعمال نیستند یا نقش کمتری دارند. بنابراین به‌منظور ارزیابی قدرت کنترل‌ها، به هر کنترل کاهش ریسک یک مقرره، وزنی نسبت داده می‌شود؛ به‌عنوان مثال، ممکن است آموزش در الزامات اخلاق حرفه‌ای وزن بسیار بالایی داشته باشد، اما در دستورالعمل اعمال سقف نرخ سود سپرده وزنش کمتر باشد و برعکس رویهٔ سیستمی در اعمال سقف نرخ سود مهم‌تر باشد. تعیین وزن هر کنترل براساس نوع الزام صورت می‌گیرد.

محاسبهٔ قدرت کنترل: پس از تعیین قدرت کنترل و وزن هر کنترل نوبت به محاسبهٔ قدرت اثربخشی کنترل نهایی یک الزام یا مقرره براساس رابطهٔ ۳ است. در این رابطه که از میانگین وزنی[1] استفاده شده است، CS_1 تا CS_n قدرت انواع کنترل برای یک الزام هستند. قدرت هر کنترل عددی بین صفر تا یک و وزن بین صفر تا یک در نظر گرفته می‌شود. جمع اوزان باید برابر با یک شود. بدین‌ترتیب، خروجی عددی بین صفر و یک خواهد بود.

$$CP = \sum_1^n CSiWi \qquad where \quad \sum_1^n Wi = 1 \tag{۳}$$

در این رابطه، n تعداد کنترل‌ها، CS_i قدرت اثربخشی کنترل i ام، W_i وزن هر کنترل و CP قدرت اثربخشی نهایی کنترل‌های یک الزام را نشان می‌دهد. براساس رابطهٔ ۳، عدد نهایی قدرت کنترل یا CP عددی بین صفر یک به‌دست می‌آید. به‌منظور محاسبهٔ نهایی ریسک باقی‌مانده، رده‌بندی CP در سه سطح در جدول ۱۰ پیشنهاد می‌شود. تعداد سطوح و آستانه‌ها می‌تواند براساس تجربه تغییر کند.

[1] weighted average

جدول ۱۰
سطح‌بندی قدرت اثربخشی کنترل

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

در بخش بعدی، نحوهٔ محاسبهٔ ریسک باقی‌مانده توضیح داده خواهد شد.

۱۱ محاسبهٔ ریسک باقی‌ماندهٔ مقرره

با توجه به ریسک ذاتی مقرره یا الزام و قدرت کنترل کاهش ریسک تطبیق آن، ریسک باقی‌مانده با توجه به رابطهٔ (۲)، می‌توان ریسک باقی‌مانده را به‌دست آورد. در زیربخش ۱، ریسک ذاتی با توجه به شدت تبعات مختلف در چهار سطح کم، متوسط، زیاد، و خیلی زیاد رده‌بندی شد. در زیربخش ۲، نیز قدرت نهایی اثربخشی کنترل به سه ردهٔ کم، متوسط، و قوی سطح‌بندی شد. در جدول ۱۱، سطوح کیفی برای ریسک ذاتی، قدرت کنترل، و ریسک باقی‌مانده پیشنهاد شده است. هرچه قدرت کنترل بیشتر باشد، ریسک ذاتی کاهش بیشتری داشته و ریسک باقی‌مانده کمتر می‌شود. با توجه به سطح ریسک باقی‌مانده که در جدول نیز به آن اشاره شده، اقدامات اصلاحی تقویت کنترل‌ها تعیین شده و پس از اعمال تغییرات مجدد ریسک مانده ارزیابی می‌شود. این فرایند همان فرایند ارزیابی مستمر اثربخشی کنترل‌های اعمالی کاهش ریسک تطبیق است.

جدول ۱۱
ارزیابی ریسک باقی‌مانده

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

۱۲ بررسی یک مقررهٔ نمونه

به‌منظور بررسی روش پیشنهادی، یک مقرره برای بررسی ریسک ذاتی و قدرت اثربخشی کنترل‌ها در یک بانک انتخاب شد. مشخصات مقرره در ادامه آمده است:

نام مقرره: آیین‌نامهٔ تسهیلات و تعهدات کلان مصوب سال ۱۳۹۲
مرجع تصویب: شورای پول و اعتبار
دسته‌بندی مقرره: مقررات احتیاطی
نسخ منسوخ‌شده دارد: بلی
خلاصهٔ مقرره: این آیین‌نامه در اجرای بند ۴ مادهٔ ۳۴ قانون پولی و بانکی کشور به‌منظور محدودکردن اعطای تسهیلات و تعهدات به یک ذی‌نفع واحد تصویب و ابلاغ شده است. بانک‌ها موظف‌اند حد تسهیلات و تعهداتی کلان فردی و جمعی را رعایت کرده و گزارشات لازم را به بانک مرکزی ارسال کنند.

با توجه به آنکه این مقرره از مقررات احتیاطی بوده و عدم‌رعایت آن بانک را در معرض تبعات زیاد حقوقی و مالی و شهرتی قرار می‌دهد، ریسک ذاتی آن «خیلی زیاد» ارزیابی می‌شود. به‌منظور کاهش ریسک ذاتی خیلی بالا، بانک‌ها کنترل‌هایی را پیاده‌سازی و اعمال میکنند. در بانک نمونه، کنترل‌های اعمالی بررسی و امتیازدهی شد؛ به‌عنوان مثال برای کنترل سیاست و دستورالعمل، امتیازدهی شاخص‌های مورداستفاده و نتیجهٔ نهایی در جدول ۱۲ نشان داده شده است.

جدول ۱۲

سنجش قدرت کنترل سیاست و دستورالعمل

شاخص سنجش قدرت	مقدار	امتیاز (از ۰/۲)
نوع کنترل (پیشگیرانه، کشف‌کننده، اصلاحی)	پیشگیرانه	۰/۲
آیا سیاست و دستورالعمل مصوبی برای مقرره وجود دارد؟	بله	۰/۲
در کدام سطح سازمانی دستورالعمل و سیاست مربوطه تصویب شده است؟ (هیئت‌مدیره، کمیتهٔ تطبیق، واحد اجرایی)	هیئت‌مدیره	۰/۲
آیا سیاست و دستورالعمل مصوب منطبق بر آخرین تغییرات مقرره است؟	بله	۰/۲
آیا سیاست و دستورالعمل مصوب به کلیهٔ کارکنان مربوطه ابلاغ شده است؟	تا حدودی	۰/۱
امتیاز نهایی قدرت کنترل از ۱		۰/۹

پس از سنجش قدرت هر کنترل و نسبت‌دادن وزن براساس اهمیت هر کنترل در کاهش ریسک عدم‌رعایت مقرره، آیین‌نامهٔ تسهیلات و تعهدات کلان، ارزیابی قدرت اثربخشی نهایی یا همان CP انجام می‌شود. شکل زیر فرایند مذکور را نمایش می‌دهد.

جدول ۱۳

قدرت‌سنجی کنترل نهایی کاهش ریسک عدم‌رعایت مقرره نمونه

انواع کنترل	امتیاز قدرت	وزن قدرت	حاصل
کنترل ۱: وجود سیاست و دستورالعمل (فرهنگ‌سازی، تهیهٔ مستندات مربوطه و ابلاغ)	۰/۹	۰/۲	۰/۱۸
کنترل ۲: آموزش (آموزش درست به کارکنان مربوطه، آموزش دوره‌ای، ارزیابی اثربخشی آموزش)	۰/۸	۰/۱	۰/۰۸
کنترل ۳: پیاده‌سازی سیستمی (پیاده‌سازی سیستمی آستانه‌های عددی مقرره، تطابق رویهٔ سیستمی با مقرره)	۰/۵	۰/۳	۰/۱۵
کنترل ۴: تست و نظارت (بازرسی یا حسابرسی دوره‌ای، انجام تست موردی)	۰/۷	۰/۱	۰/۰۷
کنترل ۵: گزارش دهی (ارائهٔ گزارش دوره‌ای به هیئت‌مدیره، ابلاغ اصلاحات موردنیاز)	۰/۴	۰/۳	۰/۱۲
ارزیابی نهایی قدرت کنترل	۰/۶ متوسط		

با توجه به ریسک ذاتی عدم‌رعایت مقرره، آیین‌نامهٔ 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 نتیجهٔ ریسک باقی‌مانده «زیاد» خواهد بود. با توجه به تعریف ریسک بالا در ستون سوم جدول ۱، قابل‌توجه بوده و باید برنامهٔ مشخصی برای کنترل و کاهش آن تدوین و اجرا شود.

۱۳ نگاه شرکت‌های بزرگ به ارزیابی ریسک تطبیق

در این بخش، دیدگاه شرکت‌های بزرگ حسابرسی جهان[1] شامل KPMG، PWC، EY، و Deloitte به موضوع ریسک تطبیق به‌طور خلاصه مطرح شده است.

شرکت KPMG تأکید زیادی بر ارزیابی ریسک تطبیق به‌عنوان بخش مهمی از برنامهٔ مؤثر تطبیق دارد. این شرکت مدلی را برای ارزیابی ریسک تطبیق براساس شاخص‌های کلیدی ریسک[2] با توجه به پیشرفت فنّاوری‌های تحلیل داده، ارائه داده است (گرلاچ[3] و همکاران، ۲۰۱۸). ابزارهای تحلیل داده می‌توانند به شناسایی، پیشگیری، و پاسخ به داده‌های هشداردهنده کمک کنند و تصمیمات مبتنی بر شواهد را ممکن سازند. شاخص‌های کلیدی ریسک یا KRIs برای شناسایی علائم هشداردهنده‌ای که می‌تواند منجر به افزایش ریسک سازمان شود استفاده می‌شوند تا ریسک‌ها به‌موقع شناسایی و مدیریت شوند (اروین، ۲۰۲۱)

همچنین، شرکت KPMG 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 کنند.

شرکت PWC راهنمایی را برای ارزیابی ریسک شامل ریسک تطبیق براساس ماتریس ریسک دوعاملی ارائه کرده است. از نظر PWC، تمرکز ارزیابی تطبیق می‌بایست بر تهدیدات اصلی سازمان بوده و با اشتهای ریسک و ریسک‌های کسب‌وکار همسو باشد. این شرکت شاید یک مدل کابردی جامع برای ارزیابی ریسک مطرح نکرده باشد، اما خدمات جامعی برای مدیریت ریسک تطبیق در چهارچوب حاکمیت شرکتی ارائه داده است. این خدمات به سازمان‌ها کمک می‌کند ارزیابی ریسک خود را براساس داده‌های تحلیلی و با استفاده از فنّاوری‌های پیشرفته مانند هوش مصنوعی[4] و یادگیری ماشین[5] انجام دهند. (موسسه پی دبلیو سی، ۲۰۰۸)

شرکت EY رویکرد سنتی را با فنّاوری‌های نوین ترکیب کرده تا بتواند رویکرد جامعی برای مدیریت ریسک تطبیق پیشنهاد دهد. در شناسایی زودهنگام ریسک مانند شناسایی پیش‌دستانهٔ تخلف و استفاده از نظارت مستمر سیستمی برای کشف موارد عدم‌تطبیق، از

[1] Big Four Accounting Firm
[2] Key Risk Indicators (KRIs)
[3] Gerlach
[4] artificial intelligence
[5] machine learning

روش‌های مبتنی بر هوش مصنوعی استفاده می‌کند. در مدیریت ریسک تطبیق، نگاه سنتی مشتمل بر اجتناب از ریسک، انتقال ریسک، مدیریت و کاهش ریسک و پذیرش ریسک را دارد. (بندک و بگنار، ۲۰۲۴)

شرکت Deloitte در راهنمایی برای ارزیابی ریسک تطبیق، ارزیابی این ریسک را از ارزیابی سایر ریسک‌های سازمان متمایز کرده و بر تمرکز بر شناسایی و اولویت‌بندی ریسک‌های مهمی که تبعات جدی مالی، حقوقی، عملیاتی و شهرتی دارند تأکید می‌کند. این شرکت پیشنهاد می‌دهد که این ارزیابی‌ها باید به‌طور مرتب به‌روزرسانی شوند و از ماتریس ریسک برای ارزیابی دقیق‌تر استفاده شود. شرکت Deloitte همچنین مدلی به نام تحلیل سیستماتیک ریسک یکپارچگی[1] 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 است. تفاوت اصلی مدل ارائه‌شده در این مقاله با مدل SIRA در نحوهٔ ارزیابی کنترل‌های کاهش ریسک است. (جانسن[2]، ۲۰۱۸)

شرکت مذکور همچنین استفاده از تجزیه‌وتحلیل داده‌ها و رباتیک پردازش خودکار[3] را برای بهبود کارایی و افزایش قابلیت اطمینان فرایندهای مدیریت ریسک تطبیق توصیه می‌کند.

۱۴ خلاصه و نتیجه‌گیری

ارزیابی ریسک تطبیق ابزاری حیاتی برای مدیریت ریسک‌های ناشی از قوانین و مقررات و استانداردهای پیچیدهٔ سازمان است. این ارزیابی‌ها نه‌تنها ریسک‌های حقوقی و مالی را کاهش می‌دهد، بلکه به تقویت فرهنگ سازمانی و بهبود حسن‌شهرت نیز منجر می‌شود. دربارهٔ بانک‌ها، چالش‌های رعایت قوانین و مقررات بیشتر است. این مؤسسات می‌بایست از رعایت الزامات و مقررات داخلی و استانداردهای بین‌المللی اطمینان حاصل کنند تا مشمول جریمه‌های سنگین، آسیب‌های جبران‌ناپذیر به اعتبار بانک یا حتی ممنوعیت برخی فعالیت‌های بانکی نشوند. بنابراین، ارزیابی مداوم ریسک‌های تطبیق به بانک‌ها کمک می‌کند با اتخاذ اقدامات پیشگیرانه و استفاده از فنّاوری‌های نوین، از آسیب‌های احتمالی جلوگیری کنند. به‌عبارت دیگر، ارزیابی ریسک تطبیق خود یک کنترل داخلی بسیار حیاتی است که تأثیر به‌سزایی در ادامهٔ فعالیت بانک‌ها در محیط پیچیده و پرچالش مقرراتی دارد.

[1] Systematic Integrity Risk Analysis (SIRA)

[2] Jansen

[3] Robotics Process Automation (RPA)

با توجه به آنکه ریسک تطبیق نوعی ریسک عملیاتی است، تاکنون روش‌هایی مانند ماتریس ریسک، آنالیز حالات شکست و تجزیه‌وتحلیل آثار، ارزیابی و خودارزیابی ریسک و کنترل‌ها و شاخص کلیدی ریسک مورداستفاده قرار گرفته‌اند. برخی از این روش‌ها از طرف شرکت‌های بزرگ حسابرسی نیز به‌همراه استفاده از ابزار تحلیل داده و فنّاوری‌های مبتنی بر هوش مصنوعی پیشنهاد شده‌اند.

در مقالهٔ حاضر، ضمن تبیین سیستم مدیریت تطبیق و عناصر تشکیل‌دهندهٔ آن، فرایند مدیریت ریسک تطبیق شامل شناسایی ریسک، اندازه‌گیری و اولویت‌بندی، کاهش ریسک و پایش ریسک تشریح شد. در همین راستا، مدل‌هایی نیز برای اندازه‌گیری ریسک معرفی شد.

هدف این نوشته ارائهٔ مدلی کاربردی برای ارزیابی ریسک تطبیق در بانک‌هاست. روشی برای ارزیابی ریسک تطبیق براساس تعریف بازل از ریسک و راهکارهای کاهش ریسک تطبیق در بانک‌ها پیشنهاد شده و یک نمونه هم موردبررسی قرار گرفته است.

در روش پیشنهادی، ریسک عدم‌رعایت یک مقرره یا الزام براساس ریسک ذاتی و اثربخشی راهکار کنترلی موجود آن محاسبه می‌شود. ابتدا ریسک ذاتی مقرره یا الزام براساس تبعات حقوقی، مالی، و شهرتی عدم‌رعایت آن ارزیابی می‌شود، سپس نوبت به ارزیابی قدرت نهایی کنترل کاهش ریسک عدم‌رعایت مقرره با توجه به قدرت اثربخشی هر کنترل و وزن آن است. پس از قدرت‌سنجی کنترل‌های اعمال‌شده، ریسک باقی‌ماندهٔ عدم‌رعایت مقرره به‌دست می‌آید. با توجه به ریسک باقی‌مانده، می‌توان اقدامات اصلاحی را به‌منظور بهبود کنترل‌ها انجام داده و پس از آن ریسک تطبیق را مجدداً ارزیابی کرد. این روش، علاوه بر اینکه در ارزیابی ریسک عدم‌رعایت مقررات بانک کاربرد دارد، با تغییراتی در ارزیابی ریسک تطبیق محصولات و خدمات و پروژه‌های جدید نیز قابل‌استفاده است.

فهرست منابع

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

حاجی‌شاه‌وردی، د.، و تاجدینی، م. (۱۳۹۶). مروری اجمالی بر مبانی نظری مدیریت ریسک رعایت در بانک‌ها و مؤسسات مالی و اعتباری. مجلهٔ مدیریت، اقتصاد و حسابداری، ش. ۲۶ و ۲۷.

حاجی‌شاه‌وردی، د.، و زمردیان، غ. (۱۳۹۹). ارزیابی ریسک رعایت (تطبیق) با الگوگیری از اسناد سازمان بین‌المللی استانداردسازی و رهنمودهای کمیسیون تردوی (مطالعهٔ موردی یکی از بانک‌های عامل)، فصلنامهٔ مدیریت کسب‌وکار، ش. ۴۸، ۲۷۴ـ ۲۹۱.

Basel Committee on Banking Supervision. (2005). Compliance and the compliance function in banks. Basel: Bank for International Settlements.

Losiewicz-Dniestrzanska, E. (2015). Monitoring of compliance risk in the bank. Procedia Economics and Finance, 26, 800-805.

Esayas, S., Mahler, T. (2015). Modelling compliance risk: A structured approach. Artif. Intell. Law, 23 (3), 271-300.

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.

Sheedy, E., Zhang, L., & Chi Ho Tam, K. (2019). Incentive and culture in risk compliance. Journal of Banking and Finance, 107, 105611.

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.

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.

Benedek P., Bognár F. (2024). Compliance risk assessment-results of a comprehensive literature review. Acta Polytechnica Hungarica, 21 (6), 243.

ISO. (2022). ISO/IEC 27001:2022 Information technology – Cyber security and privacy protection information security management systems – requirements. Geneva: International Organization for Standardization.

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.

ISO. (2021). ISO 37301:2021 Compliance management systems – Requirements with guidance for use. Geneva: International Organization for Standardization.

ISO. (2014). ISO 19600:2014 Compliance management systems – Guidelines. Geneva: International Organization for Standardization.

ISO. (2018). ISO 31000:2018 Risk management systems – Guidelines. Geneva: International Organization for Standardization.

Brownbridge, M., Kirkpatrick, C., & Maimbo, S. M. (2002). Prudential regulation. Finance and Development, 1(1), 1.

Evrin, V. (2021). Risk assessment and analysis methods: Qualitative and quantitative. ISACA JOURNAL, 28.

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).

KPMG. (2017). The compliance journey survey – Boosting the value of compliance in changing regulatory climate. KPMG.

Gerlach, J., Stryker, N., Matsuo, & A., & Dookhie, R. (2018). Harnessing data and analytics to transform compliance. KPMG.

PWC. (2008). A practical guide to risk assessment. Pricewaterhouse Coopers.

Jansen, J. (2018). Compliance risk management, powers performance. Deloitte.