مجموعه مقالات مرتبط با مدل سه خط

مدل سه خط انجمن حسابرسان داخلی (IIA)

موضوع کلیدی: پاسخگویی، گزارشدهی | تفویض اختیار، هدایت، منابع، نظارت | همسویی، هماهنگی ارتباطی ، همکاری

ترجمه و گردآوری:

مرتضی اسدی

الهه مهدوی ثابت آرشینا منتظری

فهرست مندرجات

مدل چهارخط دفاعی برای موسسات مالی

مرتضی اسدی الهه مهدوی ثابت

خلاصه اجرایی[1]

طراحی و پیاده‌سازی سیستم‌های کنترل داخلی موضوعی است که از زمان بحران مالی جهانی در بین سال‌های ۲۰۰۷ تا ۲۰۰۹ توجه زیادی را در محافل حرفه‌ای و دانشگاهی به خود جلب کرده است. تحقیقات زیادی با حمایت بنیاد پژوهشی انجمن بین‌المللی حسابرسان داخلی (IIARF[i]) در خصوص ویژگی‌ها و اثربخشی وظایف حسابرسی داخلی صورت گرفته و در مجلات حرفه‌ای و دانشگاهی به چاپ رسیده است. علیرغم این تلاش‌ها، تحلیل سیستماتیک کافی در خصوص نحوه تاثیر طراحی سیستم کنترل داخلی بر کارآیی و اثربخشی فرآیندهای راهبری شرکتی علی‌الخصوص در موسسات مالی نظیر بانکها و شرکت‌های بیمه وجود ندارد. استفاده از مدل سه خط دفاعی جهت مدل‌سازی رابطه بین راهبری شرکتی و سیستم‌های کنترل داخلی از گذشته رواج داشته است. به نظر ما مدل سه خط دفاعی این قابلیت را دارد که با افزوده شدن یک توجه ویژه به مقررات گذار بانکها و شرکت‌های بیمه به طرز چشمگیری تقویت گردد. ما به این نقصان پرداخته و تلاش می‌کنیم تا میزان نیاز این موسسات مالی به یک مدل کنترل داخلی موثرتر را با توجه به الزامات مقررات گذاری خاص و ویژگی‌های متنوع آنها تعیین کنیم. هر چند که تحقیق حاضر به طور کلی به موضوع موسسات مالی می‌پردازد، اما تحلیل مشروح ما بر موسسات بانکی متمرکز خواهد بود.

ما به منظور لحاظ نمودن ویژگی‌های راهبری خاص بانکها و شرکت‌های بیمه، طرح کلی یک مدل حاوی چهار خط دفاعی را ارایه میدهیم که به حسابرسان مستقل و ناظرین، یعنی افرادی که به صورت رسمی در محیط خارج از سازمان قرار دارند، یک نقش ویژه در ساختار سازمانی سیستم کنترل داخلی اعطا می‌کند.

ما با فرض وجود یک رابطه سه جانبه بین حسابرسان داخلی، ناظرین و حسابرسان مستقل به دنبال بررسی دقیق تعاملات بین این سه گروه هستیم. ما معتقد هستیم که استقرار یک مدل دفاعی چهار خطی موجب ایجاد مسئولیت‌ها و روابط جدید بین حسابرسان داخلی، ناظرین و حسابرسان مستقل شده و تقویت سیستم‌های کنترلی را به دنبال خواهد داشت. البته بایستی به ریسک ناشی از مشکلات جدیدی نیز اشاره کنیم که می‌توانند در اثر گردش اطلاعات ناکافی در بین این نقش‌آفرینان به وجود بیاید.

---

[1] نویسندگان از بازبین‌ها به خاطر نظرات و پیشنهادات ارزشمندشان که به بهبود دقت و اعتبار این تحقیق کمک کردند، تشکر می‌کنند: پروفسور رابرت ملویل از دانشکده‌ی کسب و کار کاس، پروفسور ویلکو اوستووندر از دانشگاه اوترخت؛ و خوآن کارلوس کریسانتو، استفان هول و ریحان زامیل از موسسه ثبات مالیِ بانک تسویه بین‌المللی.

۱. مقدمه: بحران مالی جهانی، راهبری شرکتی و مدل سه خط دفاعی

اتفاق‌نظر گسترده‌ای وجود دارد که ناکامی‌های قابل توجه در راهبری شرکتی یک عامل موثر در بحران مالی جهانی (GFC[ب]) بوده است.[۲]

اگرچه برخی مفسران استدلال کرده‌اند نسبت به انتظارات بسیاری از مردم اصلاحات راهبری شرکتی تاکنون بسیار کم اتفاق افتاده است،[۳] اصلاحات بیشتر در راهبری شرکتی در کاهش ریسک تکرار بحران مالی عمده ضروری تلقی شده است. به خصوص، بحران مالی جهانی باعث بحث‌های جدید درباره اهمیت روش‌های حفاظتی در سطح هیات مدیره شده است، از جمله معرفی قوانین الزام‌آور حقوقی برای ارتقاء کمیته‌های مدیریت ریسک در سطح هیات مدیره و علاوه بر این الزام انتصاب مسئول ارشد ریسک (CRO[پ]) برای بهبود تخصص هیات مدیره در ارتباط با مسائل مدیریت ریسک است.[۴]

در سطح بین‌المللی، بحث گسترده‌ای وجود دارد که چگونه می‌توان از روش‌های راهبری شرکتی در موسسات مالی برای بهبود مدیریت ریسک استفاده کرد. برای نمونه، این کار با ایجاد کمیته مدیریت ریسک در سطح هیات مدیره؛ تغییر انگیزه‌های عضو هیات مدیره توسط طرح‌های متغیر پاداش؛ بهبود نظارت؛ و تحمیل قواعد (ضوابط) مادی دیگر بر جبران خدمت با هدف نهایی ارتقاء ثبات مالی قابل اجرا است.

راهکارهای انتشار یافته توسط کمیته نظارت بانکی بازل [ت](BCBS) در سال ۲۰۱۵ روی اصول راهبری شرکتی برای بانک‌ها بر اهمیت روش‌های مدیریت ریسک مناسب تاکید دارد، از جمله، به خصوص، «فعالیت مدیریت ریسک مستقل اثربخش، تحت هدایت مسئول اصلی ریسک، با جایگاه، استقلال، منابع و دسترسی کافی به هیات‌مدیره».[۵] علاوه بر این، «پیچیدگی مدیریت ریسک بانک و زیرساخت کنترل داخلی بایستی هماهنگ با تغییرات پروفایل ریسک بانک، چشم‌انداز ریسک بیرونی و فعالیت در صنعت باشد» به طوری که ریسک‌ها بطور مداوم بر مبنای گستره بانک و واحدهای جداگانه آن، شناسایی، پایش و کنترل شود.[۶]

سازمان توسعه و همکاری‌های اقتصادی (OECD[ج]) به نتیجه‌گیری‌های مشابه درباره این روش‌ها، به خصوص جایگاه مسئول اصلی ریسک، رسیده است، لازم است ریسک‌های ویژه تحمیلی به اقتصاد بزرگتر توسط بانک‌ها بهتر مدیریت شود، و رویکرد احتیاط خرد و کلان برای نظارت ترکیب شود. به همین ترتیب، گزارش اولیه اخیر در کمیسیون اروپا (EC[چ]) درباره‌ی طرح کلی راهبری شرکتی در موسسات مالی و سیاست‌های جبران پاداش نشان می‌دهد که مدیریت ریسک در سطح هیات مدیره بطور کافی درک نشده است. این عدم

---

[۲] مطابق با گزارش گروه لاروسیه با عنوان *گزارشی در ارتباط با آینده‌ی نظارت مالی در اتحادیه‌ی اروپا* در تاریخ ۲۵ فوریه‌ی ۲۰۰۹ در شهر بروکسل، راهبری شرکتی یکی از مهم‌ترین عناصر زیربنایی بحران مالی است؛ در متون مرتبط با این موضوع، برای مثال، این مقالات را بخوانید: هوپت، «راهبری شرکتی بانک‌ها و سایر موسسات مالی بعد از بحران مالی»، در مجله مطالعات قانون شرکتی ۲۰۱۳، ۲۲۲؛ کیتلائو و مولبرت، «نقش نامشخص راهبری شرکتی بانک‌ها در مقررات ریسک سیستماتیک»، در مقاله‌ی کاری قانون ECGI، ۲۰۱۱، شماره‌ی ۱۷۹.

[۳] این مقاله را بخوانید: هوسون، «وقتی راهبری شرکتی "خوب"، موسسات مالی "بد" به وجود می‌آورند: بحران جهانی و محدودیت‌های قوانین بخش خصوصی»، مجله‌ی قانون میشیگان، ۲۰۰۹، صفحات ۴۴ تا ۵۰. .

[۴] مولبرت، «راهبری شرکتی بانک‌ها بعد از بحران مالی-نظریه، شواهد، اصلاحات»، مقاله‌ی کاری قانون ECGI، ۲۰۰۹، شماره‌ی ۱۳۰؛ هیلب، «طراحی مجدد راهبری شرکتی؛ درس‌های آموخته شده از بحران مالی جهانی»، مجله‌ی مدیریت و راهبری، ۲۰۱۱، صفحات ۵۳۳ تا ۵۳۸.

[۵] کمیته نظارت بانکی بازل، *اصول تقویت راهبری شرکتی*، اصل ۶. همچنین این نوشته را بخوانید: کمیته‌ی اجرایی سازمان توسعه و همکاری‌های اقتصادی برای راهبری شرکتی، *راهبری شرکتی و بحران مالی*، ۱۵.

[۶] کمیته نظارت بانکی بازل، *اصول تقویت راهبری شرکتی*، اصل ۷.

کفایت‌ها، به ویژه، عبارتند از «فقدان درک ریسک‌ها»، «فقدان اختیار [...] برای جلوگیری از فعالیت‌های ریسک‌پذیر»، «فقدان تخصص [...] در مدیریت ریسک» و «فقدان اطلاعات به‌هنگام درباره ریسک‌ها».[۷] در نتیجه، این گزارش اولیه پیشنهادات ذیل را با توجه به مدیریت ریسک ترسیم می‌کند:

- تعیین مسئولیت‌ها در سطح هیات مدیره؛
- ایجاد کمیته نظارت بر ریسک در سطح هیات مدیره؛
- ایجاد جایگاه مسئول ارشد مدیریت ریسک که با «پیچیدگی سازمانی» شرکت مربوطه آشنایی دارد؛ و
- افزایش همکاری، نه تنها بین مسئولان نظارتی مربوطه و هیات مدیره‌ها، بلکه بین کمیته نظارت بر ریسک و سایر بخش‌های شرکت.

از مطالب بالا نتیجه‌گیری می‌شود که اصلاحات سیستم کنترل داخلی بایستی همراه با اصلاحات راهبری شرکتی باشد تا اطمینان حاصل شود که بانک‌ها کیفیت ریسک‌پذیری‌شان را ارتقا می‌دهند، از طریق جلوگیری از انگیزه‌های ناسازگار یا در غیر این صورت، ریسک استراتژی‌های کسب‌وکار را کاهش می‌دهند. از این جنبه برتری، بحران مالی جهانی نشان داد که ضعف یا فقدان اثربخشی این روش‌های حفاظتی در واقع عمده است.

متخصصان استدلال کرده‌اند که توجیه اولیه، اگر نگوییم تنها توجیه، برای تنظیم سیستم‌های کنترل داخلی حداکثرسازی کارآیی و اثربخشی است، که این حداکثرسازی باعث مدیریت مواجهه با ریسک می‌شود.[۸] بنابراین کارآیی، هدفی کانونی برای تدوین‌کنندگان استاندارد بین‌المللی است و به نظر می‌رسد به دستورجلسه سیاست‌گذاران و مقررات گذاران در سراسر جهان انتقال یافته است. تا جایی که مربوط به سیستم‌های کنترل داخلی باشد، مطابق دیدگاه ما، کارآیی عبارت است از روش انجام کار (در قالب شایستگی‌ها، حرفه‌ای‌گری و منابع)، مدل یا ساختار اصلی طرفین شرکت‌کننده در فرایند و تعامل بین این طرفین. این مشاهده به خصوص برای بانک‌ها صادق است.

رویدادهای پرریسک قابل ملاحظه اخیر و رسوایی‌های شرکتی به دلیل سوءرفتار در عملیات بازار مالی نشان می‌دهد که بانک‌ها بایستی معیارهای راهبری شرکتی را ارتقاء دهند.[۹] اما، از همه مهمتر، این رویدادها منجر به اولویت‌بندی دستورکارهای نظارتی و راهبری در ارتباط با پیامدهای سیستماتیک بالقوه سیستم‌های

---

[۷] کمیسیون اروپا، *راهبری شرکتی در موسسات مالی و سیاست‌های جبران پاداش*، گزارش اولیه، بخش ۳.۴، ۲۰۱۰.

[۸] تیم، «کنترل شرکتی و کارایی بانکی»، مجله‌ی بانک و تامین مالی، ۱۹۹۳، ۱۷؛ جنسن، «حداکثرسازی ارزش، نظریه‌ی ذینفعان، و عملکرد هدف شرکتی»، مقاله‌ی کاری دانشکده‌ی کسب و کار هاروارد، ۲۰۰۰، شماره‌ی ۵۸؛ چامی و فولنکامپ، «اعتماد به عنوان ابزاری برای بهبود راهبری شرکتی و کارایی»، مقاله کاری صندوق بین‌المللی پول، ۲۰۰۲؛ لوین، «راهبری شرکتی بانک‌ها: بحثی مختصر در ارتباط با مفاهیم و شواهد»، مقاله‌ی کاری تحقیقات خط‌مشی بانک جهانی، شماره‌ی ۳۴۰۴، ۲۰۰۴؛ کیرکپاتریک، «درس‌های راهبری شرکتی از بحران مالی»، مجله‌ی روندهای بازار مالی، ۲۰۰۹، ۳ (۱)؛ دی‌جونگه، دیسلی و اسکورز، «راهبری شرکتی، فعالیت‌های غیرشفاف بانکی، و کارایی ریسک/بازده»، مجله‌ی تحقیقات خدمات مالی، جلد ۴۱، شماره ۱-۲، ۲۰۱۲.

[۹] بازیابی اعتماد عمومی یکی از مهم‌ترین موضوعات مرتبط با مقررات و نظارت بر تعهدات مالی است. بازیابی چنین اعتمادی در ارتباط با رفتارها و فرهنگ در بانک‌ها می‌تواند باعث به دست آوردن دوباره‌ی اعتماد عمومی شود؛ برای مثال، این موارد را بخوانید: گروه سی‌نفره، *رفتار و فرهنگ بانکداری: درخواست برای اصلاح جامع و پایدار*، جولای ۲۰۱۵؛ FSB، هدایت در ارتباط با تعاملات نظارتی با موسسات مالی در ارتباط با فرهنگ ریسک، آوریل ۲۰۱۴.

کنترل داخلی ضعیف، شده است.[۱۰] این مطلب نیازمند برجسته‌تر شدن سیاست‌های خردﺥ در ارتباط با سوءرفتار در بانک‌ها است. علاوه بر این، نیازمند همکاری نزدیکتر بین مقررات‌گذاران ، و حسابرسان داخلی و مستقل است تا اعتماد عمومی به موسسات مالی برگردد.

سیستم‌های کنترل داخلیِ غیرکارآمد در موسسات مالی نیز از عامل‌های عمده در چند رویداد اخیر کلاهبرداری بوده‌اند: برای مثال، در Société Générale در سال ۲۰۰۸ و در UBS در سال ۲۰۱۱؛ و در چند موسسه مالی جهانی با توجه به دست‌کاری نرخ لایبور و تثبیت نرخ ارز خارجی.[۱۱] این رویدادها به ما یادآور می‌شوند که ارتباط متقابل شرکت‌کنندگان بازار مالی می‌تواند شوک‌ها را تشدید کند و به صورت بالقوه منجر به فروپاشی سیستم مالی شود.[۱۲] فقدان اعتماد عمومی تحت تحریک رسوایی‌های رفتاری می‌تواند در نهایت مانع عموم مردم شود تا از سیستم مالی استفاده کنند، بنابراین ثبات و درستی اقتصاد در سطح کلان تضعیف می‌شود.[۱۳] رفتار و فرهنگ در بانک‌ها هرگز اولویت عمده دستورجلسه سازمان‌های مقررات‌گذار در سراسر جهان نبوده است، از جمله معرفی «قانون ولکرﺩ» در ایالات متحده،[۱۴] حرکت به سمت اتحادیه بانکداری در اتحادیه اروپا (EUﺩ)[۱۵] و طرح‌هایی با هدف برقراری بازار مالی آسیا-پاسیفیک.[۱۶]

---

[۱۰] هیئت ریسک سیستماتیک اروپایی، *گزارشی در ارتباط با ریسک سوءرفتار در بخش بانکی*، ژوئن ۲۰۱۵.

[۱۱] برای مجموعه‌ای از رسوایی‌های مالی اخیر و نظرات مربوط به آن، این مقاله را بخوانید: ارهارد، جنسن، بازگرداندن درستی به بخش مالی: یک رویکرد کاملاً مثبت، مقاله‌ی کاری مالی ECGI، ۲۰۱۴، ۴۱۷، ضمیمه‌ی ۱.

[۱۲] برای تحلیل جامع در ارتباط با ریسک سیستماتیک در بخش مالی، این مقالات را بخوانید: بوریو، «کشف دوباره‌ی ریشه‌های اقتصاد کلان خط‌مشی ثبات مالی: سفر، چالش‌ها و مسیری به سمت جلو»، مقالات کاری BIS، ۲۰۱۱، شماره‌ی ۳۵۴؛ نیر و همکاران، «مدل‌های شبکه و ثبات مالی»، مجله‌ی پویایی و کنترل اقتصادی، ۲۰۰۷، ۳۱؛ آیکمن و همکاران، «ریسک نقدینگی تأمین مالی در یک مدل کمی ثبات سیستماتیک»، در مجله‌ی ثبات مالی، سیاست پولی، و بانکداری مرکزی، ویرایش شده توسط آلفارو، بانک مرکزی شیلی، ۲۰۱۱، صفحات ۳۷۱ تا ۴۱۰؛ آدرین و برونرمایر، «CoVar»، در *گزارش کارکنان بانک فدرال رزرو نیویورک*، ۲۰۰۸، شماره‌ی ۳۴۸؛ آچاریا و همکاران، *تنظیم مقررات برای وال استریت*، نیویورک، ۲۰۱۱؛ کاشیاب و همکاران، «جعبه‌ی ابزار احتیاط در سطح کلان»، مقالات مروری اقتصادی IMF، ۲۰۱۱، ۵۹ (۲)؛ کورینک، «ریسک کردن سیستماتیک: اثرات تقویت، اثرات جانبی و پاسخ‌های نظارتی»، مجموعه‌ی مقالات کاری ECB، ۲۰۱۱، شماره‌ی ۱۳۴۵؛ گودهارت و همکاران، «چهارچوب کاری یکپارچه برای تحلیل مقررات‌گذاران مالی چندگانه»،مجله‌ی بین‌المللی بانکداری مرکزی، ۲۰۱۳، ۹(۱)؛ شوآرتز، «ریسک سیستماتیک»، مجله‌ی قانون جورج‌تاون، ۲۰۰۸، ۹۷؛ اسکات، «کاهش ریسک سیستماتیک در سیستم مالی ایالات متحده»، مجله‌ی قانون و خط-مشی عمومی هاروارد، ۲۰۱۰، ۳۳؛ کیتلائو و مولبرت، «نقش نامشخص راهبری شرکتی بانک‌ها در تنظیم ریسک سیستماتیک»، مقاله‌ی کاری قانون ECGI، ۲۰۱۱، شماره‌ی ۱۷۹.

[۱۳] مطابق با آمار، بانکداری با گذر کردن از یکی از مورد اعتمادترین بخش‌های عمومی به بخشی با یکی از کمترین سطوح اعتماد تبدیل شده است: ادلمن تراست بارومتر، نیویورک، ۲۰۱۴؛ گروه ۳۰، فرهنگ و رفتار بانکی، درخواست برای اصلاح جامع و پایدار، جولای ۲۰۱۵.

کمیسیون اروپا، مقیاس مصرف‌کننده، در آدرس زیر موجود است:

ec.europa.eu/consumers/consumer_evidence/consumer_scoreboards/۱۰edition/docs/consumer_market_brochure_۱٤۱۰۲۷_en.pdf

[۱٤] قانون اصلاح وال استریت و محافظت از مصرف‌کننده‌ی داد-فرانک، § ۶۱۹. نظرات آقای ولکر در ارتباط با مقررات قانونی پیشنهادی ولکر جالب توجه است. «نیاز به محدودسازی تبادلات حق مالکیت نه تنها مسئله‌ای مرتبط با ریسک‌های آنی بازار است، بلکه این موضوع شاید از اهمیت بسیار زیادی برخوردار باشد. به نظر می‌رسد که این موضوع تبعات اجتناب‌ناپذیر فرهنگ موسسات بانکی تجاری مربوطه است که در مشوق‌های عظیم برای ریسک کردن که به صورت ذاتی در شیوه‌های جبران برای معامله‌گران بروز می‌یابد. آیا گروهی از کارکنان می‌بایست فقط به خاطر فعالیت‌های مبادلاتی حسی، غیرشخصی، و کوتاه‌مدت چنین پاداش زیادی بگیرند، در حالی که بانکداران تجاری حرفه‌ای که خدمات بانکداری تجاری ضروری را به مشتریان عرضه می‌کنند و آشنایی مناسبی با ارزش‌های امانتی دارند، محدود به ساختار پاداش‌دهی کمتری باشند؟» (ولکر، نظرات در ارتباط با محدودیت‌های مبادله‌ی اختصاصی توسط موسسات سپرده‌گذاری بیمه شده، الصاق شده به نامه‌ی نوشته شده توسط پاول ای. ولکر به آژانس‌های مقرراتی مالی، ۱۳ فوریه‌ی ۲۰۱۲).

برای اجتناب از اجرای سناریوی کلاه‌برداری تا پایان و، یک بار دیگر، در مواجهه با نگرانی‌های عمومی مرتبط با درستی بازارهای مالی، مقررات گذاران با تمرکز دقیق‌تر بر پیامدهای سیستماتیک به نواقص راهبری داخلی نزدیک می‌شوند. علاوه بر این، این موضوع پیرامون کارآیی سیستم‌های کنترل داخلی به صورت مولفه ضروری راهبری شرکتی است، و از نظر ما، عنصر اصلی برای مدلی است که نقش ایفاء شده توسط طرفین مختلف شرکت‌کننده در مدل سیستم کنترل داخلی را تصریح می‌کند.

در صنعت مالی، از بخش های عمدتا کنترل‌کننده، حسابرسان داخلی، ناظرین و حسابرسان مستقل، خواسته شده تا وظایف‌شان را در حوزه‌های مشابه و کاملاً مرتبط انجام دهند، هرچند هر یک از آنها تمرکزهای متفاوتی دارند (برای مثال، حسابرسان داخلی بر اثربخشی و کارایی عملیات تمرکز دارند، ناظرین بر مسائل نظارتی، و غیره).

با به‌رسمیت شناختن حوزه‌های همپوشانِ فعالیت‌ها و نیاز به هماهنگی میان این سه طرف، نتیجه می‌گیریم تغییر شکل ساختار کنترل داخلی موسسات مالی با استفاده از خط چهارم دفاعی برای نهادهای کنترلی برون‌سازمانی لازم است.

۲. مروری بر مدل سه خط دفاعی

به‌دنبال بحث‌های گسترده در صنایع، درنهایت، در سال ۲۰۱۳، انجمن بین‌المللی حسابرسان داخلی مدل سه خط دفاعی را ایجاد کرد.[۱۷] این مدل به رایج‌ترین معیار برای تخصیص مسئولیت‌های مدیریت ریسک و کنترل به بخش‌های کارکردی کسب‌وکار در سازمان تبدیل شد. ایده اولیه آن بود که مدلی با کاربرد عمومی برای سازمان‌ها تدوین شود. باوجود این، در این مدل، خصوصیات منحصربه‌فرد بخش‌های خاص، مشخص نشده است (برای مثال، ویژگی‌های مؤسسات مالی تحت نظارت).

ارزش‌افزایی اصلی این مدل امکان هماهنگی مسئولیت‌های کنترلی به نحو اثربخش و کارآمد است. برای رسیدن به این هدف، نیاز است که نقش‌ها و مسئولیت‌ها به‌روشنی به فعالیت‌های ریسک و کنترل اطلاع‌رسانی شود تا گروه‌های متخصص بتوانند حوزه فعالیت‌های خود و نحوه ارتباط آن حوزه با فعالیت‌های سایر گروه‌ها را درک کنند.

---

[۱۵] سخنرانی دنیله نوی، رییس هیئت نظارتی نظام نظارتی واحد ، را با عنوان چشم‌انداز بانکداری اروپایی-نتیجه‌گیری اولیه بعد از چهار ماه نظارت بانکداری مشترک و چالش‌های اصلی پیش رو ببینید. این سخنرانی در تاریخ ۱۷ مارس ۲۰۱۵ انجام شده است و در آدرس زیر قابل مشاهده است: www.bankingsupervision.europa.eu/press/speeches/date/۲۰۱۵/html/se۱۵۰۳۱۷.en.html

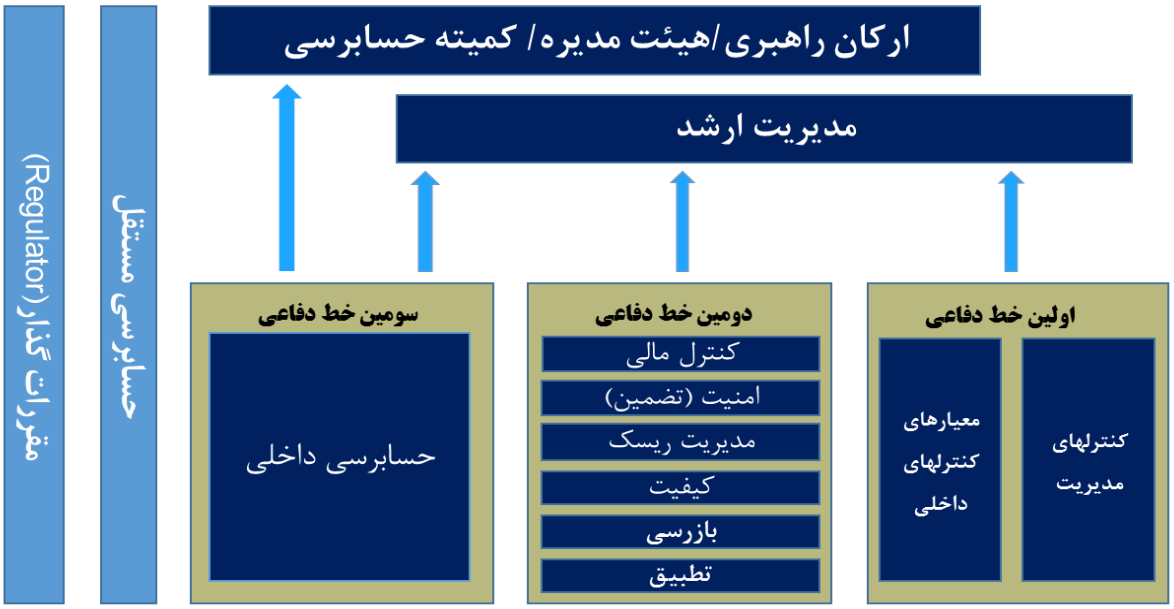
فرآیند تقریب قوانین پایه برای دستورالعمل واحد و اتحادیه‌ی بانکداری در اروپا از هدف اصلی بازیابی اعتماد عمومی الهام گرفته است. از این منظر، به عنوان مثال، «معتبرسازی دقت بانکداری» به درستی و به صورت مکرر به عنوان چالش اصلی قانونگذاران و مقررات‌گذاران در هنگام تنظیم دستورالعمل بازیابی وحل و فصل بانکی EU/۵۹/۲۰۱۴ (BRRD) شناسایی شده است. BRRD، مقدمه، نظر ۵ را بخوانید. در میان نظر محققین، به طور مثال، نوشته‌ی آرمور، با عنوان « معتبرسازی دقت بانکداری » را در فران، مولونی و پین (eds)، کتاب راهنمای مقررات مالی آکسفورد، انتشارات دانشگاه آکسفورد، ۲۰۱۴ بخوانید؛ همچنین، بایندر، «دقت: مفاهیم، الزامات و ابزارها»، مقاله‌ی پذیرفته شده در همایش بازیابی و دقت بانکی در اروپا – دستورالعمل مدیریت بحران اتحادیه‌ی اروپا در عمل، سازماندهی شده به صورت مشترک توسط نویسنده و دالویندر سینگ از دانشگاه وارویک، برگزار شده در دانشگاه توبینگن، آلمان، در تاریخ ۱۸ تا ۱۹ اکتبر، ۲۰۱۴.

[۱۶] جیمز شیپتون؛ مدیر اجرایی کمیسیون ضمانتنامه‌ها و قراردادهای آتی واسطه‌ها، هنگ‌کنگ، نظارت بر واسطه‌ها: ابتکارات کلیدی و تمرکز در سال ۲۰۱۴، ۴ ژوئن ۲۰۱۴.

[۱۷] IIA (انجمن حسابرسان داخلی)، مقاله‌ی اعلان موضع، سه خط دفاعی در اثربخشی مدیریت ریسک و کنترل ، ژانویه‌ی ۲۰۱۳.

این مدل با نمایش هندسی به صورت زیر خلاصه شده است:

نمودار ۱: مدل سه خط دفاعی (IIA (۲۰۱۳))



خصوصیات این مدل در بخش‌های زیر شرح داده شده است.

اولین خط

واحدهای کسب و کاری درآمدزا مبنای این مدل را شکل می‌دهند و با عنوان اولین خط دفاعی از آنها یاد می‌شود. بسته به نوع صنعت موردنظر، این واحدها ممکن است شامل تولید کالاهای فیزیکی یا تهیه خدمات مالی مثل تجارت، مدیریت دارایی، فروش و روابط با مشتری باشند. هدف این مدل تخصیص مسئولیت‌های کنترل و مدیریت ریسک به اولین خط دفاعی است (به‌عبارتی، کارمندان و مدیران در این واحدهای درآمدزا مشغول به کارند). در این مدل، فرض می‌شود که کنترل‌ها در اولین خط بسیار تفکیک‌شده و مبتنی بر معاملات فردی است، زیرا کارمندان به‌صورت روزانه درگیر فرایندها هستند و با گردش کاری و نقاط ضعف احتمالی کنترل آشنایند. بنابراین، پیاده‌سازی کنترل‌هایی که فرایندهای تفکیک‌شده‌تری را هدف قرار می‌دهند و تشخیص زودهنگام نقاط ضعف برای آنها آسان‌تر است. بنابراین آنها قادر به اطلاع‌رسانی فوری به سطوح مدیریتی مناسب و تضمین پیاده‌سازی به موقع اقدامات ضروری‌اند. با معرفی کنترل‌های خودکار، فراگیر کردن فعالیت‌های کنترلی (به‌عبارتی، ثبت تمام داده‌های مربوط) و دقیق‌تر کردن آنها امکان‌پذیر می‌شود، باتوجه به این‌که تنها آن موقعیت‌های استثنایی که سیستم برجسته کرده است نیازمند بررسی فوری مدیریت است. وظایف کنترلی در خط اول بر مسئولیت دوگانه واحدها نیز تأکید دارد؛ ایجاد کسب‌وکار برای سازمان، و درعین‌حال، مطلع بودن از ریسک‌ها و کنترل‌های مرتبط. این رویکرد با درس‌های آموخته‌شده از بحران مالی جهانی تقویت شده است؛ در آنجا، واحدهای ریسک‌پذیر به‌قدر کافی از رویه‌های کنترلی و ریسک آگاه نبودند.

دومین خط

در صورت ناکارا شدن سیستم‌های کنترلی ترسیم‌شده در اولین خط دفاعی، یا در غیاب آنها، دومین خط دفاعی اهمیت می‌یابد. دومین خط متشکل از وظایف مختلف تطبیق و مدیریت ریسک است (به‌عبارتی، فعالیت‌های پشتیبانی)، مانند امور مالی، تطبیق، کنترل ریسک، اعتبارسنجی مدل و دفتر پشتیبانی[ر]، که وظایف کلیدی‌شان پایش و گزارش روش‌های مرتبط با ریسک و اطلاعات و نظارت بر تمام انواع مسائل کنترلی مالی و تطبیق است. درطول بیست سال گذشته، دومین خط دفاعی در سازمان‌های مرتبط با صنعت مالی تحت نظارت به‌شکل چشمگیری تکامل یافته است. با معرفی دفتر میانی[ز]، وظایف تطبیق (معرفی بازار کارا، وظایف مدیریت ریسک عملیاتی و اعتباری، پیاده‌سازی فعالیت مستقل تایید قیمت و نقش اعتبارسنجی مستقل مدل) نشان‌دهنده افزایش توسعه نمادین است.

در پاسخ به الزامات مقرراتی سخت‌گیرانه‌تر و فرایندها و محصولات پیچیده‌تر، سازمان‌ها کارکنان و بخش‌های کارکردی بیشتری را به دومین خط افزوده‌اند. بدون کمک سازمان و هماهنگی مسئولیت‌ها، نهادهای مالی گاهی‌اوقات شکاف‌های کنترلی قابل ملاحظه‌ای بروز می‌دهند که ممکن است سلامت مالی آنها را زیرِ سؤال ببرد. از نمونه وظایف ناکافی دومین خط دفاعی می‌توان به رسوایی تجاری فریب‌کارانه Société Générale در سال ۲۰۰۸ و ضرر مالی UBS در سال ۲۰۰۷ اشاره کرد که ناشی از بحران مسکن در ایالات متحده بود و تقریباً به فروپاشی UBS انجامید.[۱۸و ۱۹]

به این ترتیب، دومین خط دفاعی الزامات کنترلی پیشگیرانه و اکتشافی[س] را تعریف می‌کند و گنجاندن این الزامات را در سیاست‌ها و رویه‌های اولین خط تضمین می‌کند. دومین خط باید مستقل از اولین خط باشد و کنترل‌ها را باید به‌صورت مستمر (مثلاً روزانه) یا دوره‌ای به‌کار بگیرد. دومین خط ممکن است مبتنی بر معیارهای روشن ارزیابی ریسک نیز باشد (برای مثال، بررسی دقیق معاملات واحدهای کسب و کاری خاصی که جابه‌جایی شغلی کارمندان در آنها بالاتر از حد معمول است یا تعداد خطاها و اصلاحات زیادتری نسبت به حالت معمول دارند).

سومین خط

سومین خط دفاعی، که سطح بعدی کنترل را نشان می‌دهد، شامل فعالیت حسابرسی داخلی است. در سال‌های اخیر، این روش توسعه یافته است، به‌نحوی‌که نسبت به حوزه وسیعی از اهداف، ازجمله کارایی و اثربخشی عملیات، حفاظت از دارایی‌ها، قابلیت اطمینان و درستی فرایندهای گزارشگری و رعایت قوانین و مقررات، به مدیریت ارشد و هیئت‌مدیره اطمینان‌بخشی مستقل ارائه می‌دهد.

برای اثربخشی این فعالیت، لازم است که این فعالیت مبتنی بر بالاترین سطح استقلال و بی‌طرفی باشد. بهترین راه برای دسترسی به آن پیاده‌سازی ساختارهایی است که در استانداردهای ویژگی‌های شخصی، استاندارد ۱۱۰۰ انجمن بین‌المللی حسابرسان داخلی (IIA) ارائه شده است و شامل استقلال سازمانی و

---

[۱۸] Société Générale ، بخش بازرسی عمومی، گزارش خلاصه، می ۲۰۰۸. .

[۱۹] UBS ، گزارش سهامداران در ارتباط با کاهش‌های ارزش UBS، آوریل ۲۰۰۸.

تعامل مستقیم با هیئت‌مدیره و ... است.[۲۰] ازجمله اقداماتی که برای اطمینان از این سطح بالای استقلال اتخاذ شده است شامل توانایی بخش حسابرسی داخلی در ملاقات با هیئت‌مدیره در غیاب مدیریت ارشد است. هیئت‌مدیره دراصل مسئول فعالیت حسابرسی مستقل است و باید به خدشه‌دار شدن احتمالی بی‌طرفی آشنا باشد.[۲۱]

کنترل‌هایی که در سومین خط دفاعی صورت می‌گیرد مبتنی بر کارایی روش‌شناختی ارزیابی ریسک است. درعمل، بخش حسابرسی باید حداقل به‌صورت سالانه به ارزیابی ریسک سازمان مبادرت کند و واحدهای کسب و کاری یا فرایندهایی که سطح ریسک باقیمانده بالایی دارند را شناسایی کند (به‌عبارتی، ریسک باقیمانده بعد از درنظر گرفتن محیط کنترل داخلی). بنابراین، سومین خط دفاعی تنها نسبت به ارزیابی مبتنی بر ریسک دوره‌ای اطمینان می‌دهد نه پایش تفکیک‌شده و مستمر که به نوعی اولین خط دفاعی است.

کنترل‌های برون‌سازمانی

در نهایت، چند سطح کنترلی برون‌سازمانی بیشتر وجود دارد که مکمل سه لایه داخلی فعلی کنترل‌هاست. حسابرسان مستقل از جمله رایج‌ترین نهادها در این دسته‌بندی‌اند، و براساس قانون، در اغلب سازمان‌ها وجودشان الزامی است. به‌ویژه در بخش مالی تحت نظارت، الزاماتی وجود دارد که باید در نهادهای مقررات گذار خاص صنعت بررسی شوند (برای مثال، مقام نظارتی بیمه یا بانک)؛ این نهادها در خارج از سازمان قرار دارند. گرچه حسابرسان مستقل در خارج از سازمان قرار دارند، برای راهبری کلی و ساختار کنترلی سازمان اهمیت دارند، زیرا استانداردها و مقررات مربوطی را که باید پیاده‌سازی شوند وضع می‌کنند و درنهایت وظیفه دارند که بررسی کنند آیا این مقررات به نحو مناسب رعایت شده‌اند یا خیر. درنتیجه، ممکن است موقعیت‌هایی پیش بیاید که در آن مسائل مقرراتی در سازمان اهمیت اصلی را بیابد و ساختارها و فرایندهای راهبری را مشخص کند.

در بحث زیر، ابتدا ویژگی‌های رایج‌ترین مدل درحال استفاده (مدل سه خط دفاعی) به‌اجمال بیان می‌شود، پس‌زمینه این مدل و دلایل اصلاح آن مطابق با نیازهای مؤسسات مالی مطرح می‌شود، و درآخر، با ارزیابی مزایا و نواقص افزایش همکاری و ارتباطات، روابط دوجانبه میان این سه فعالیت کنترلی تحلیل می‌شود.

۳. نقاط ضعف و شکست‌های گذشته‌ی مدل سه خط دفاعی

علیرغم استقبال پرشور موسسات مالی بزرگ از مدل سه خط دفاعی در طی چند سال گذشته دنباله‌ای از رسوایی‌های بانکی مختلف در این مدت روی داده‌اند که نارسایی‌های سیستم‌های کنترل داخلی نقش مهمی در آن‌ها داشته و به ضررهای مالی قابل توجه منجر شده‌اند و حتی برخی موسسات را به آستانه‌ی ورشکستگی رسانده‌اند. ما با در نظر گرفتن این شواهد ریشه‌ی دلایل این مشکلات و نقاط ضعف مدل سه خط دفاعی را در عمل تحلیل می‌کنیم:

---

[۲۰] IIA (انجمن حسابرسان داخلی)، استانداردهای ویژگی‌های شخصی ۱۱۰۰، استقلال و بی‌طرفی (واقع‌بینی).

[۲۱] OECD ، اصول راهبری شرکتی، سپتامبر ۲۰۱۵.

۱. انگیزه‌های ناسازگار برای ریسک‌پذیران در اولین خط دفاعی

بسیاری از متخصصان بر این باور هستند که اولین خط دفاعی مهم‌ترین کنترل است.[۲۲] با این‌حال این مسئولیت با اهداف اغلب ریسک‌پذیران حاضر در خط اول یعنی کسب درآمد و سود کافی برای موسسه در تضاد است. در گذشته مدیران به جای اهداف کنترل‌گرا تأکید زیادی بر روش‌های پاداش‌دهی داشتند و آن‌ها را بر اساس میزان دست‌یابی به اهداف مالی موسسه تعیین می‌کردند. یکی از دلایلی که باعث شد تا موسسه‌ی مالی UBS در طی بحران بدهی‌های آمریکا با مشکلات مالی روبه‌رو شود، رویه‌های کنترلی ناکافی و نارسایی‌های سیستم‌های گزارشگری مالی این موسسه در زمینه‌ی موقعیت‌های معاملاتی رو به رشد این شرکت بر روی اوراق بهادار آمریکا با پشتوانه‌ی وام مسکن رهنی در بانک سرمایه‌گذاری بود.[۲۳] در حالی که این موقعیت‌های معاملاتی روز به روز در بانک انباشته می‌شدند این اطلاعات به سطوح بالایی مدیریت منتقل نشده و تنها در لابه‌لای گزارش‌های کلی ارائه می‌شدند و به همین دلیل میزان واقعی آسیب‌پذیری این شرکت از بازار وام مسکن آمریکا را مخفی نگه داشته بودند. سوال اصلی این است که چطور یک بانک به معامله‌گران خود که اهداف کنترلی را رعایت می‌کنند پاداش می‌دهد اما نمی‌تواند درآمد کافی برای موسسه ایجاد کند. شاید یک راه پیش‌رو معرفی سیستم پاداش خاصی باشد که از ترکیب یک عنصر پاداش انعطاف‌پذیر و کوچک با شرط دستیابی به اهداف کنترلی پیش از دریافت پاداش تشکیل شده باشد. علاوه‌براین مشکل سطوح بالاتر سازمان را می‌توان در چارچوب ارتباطات نامناسب در نظر گرفت که در برخی از مواقع با فقدان چشم‌انداز جامع و درست افرادی که در درجه‌ی اول اهمیت هستند ترکیب می‌شود.[۲۴]

۲. فقدان استقلال سازمانی فعالیت‌هایی که در دومین خط دفاعی قرار دارند

انتقاد رایجی که غالبا در مورد اثربخشی کنترل‌های انجام شده در خط دوم دفاعی مطرح می‌شود فقدان استقلال سازمانی فعالیت‌های کنترلی است.[۲۵] اغلب وظایف مدیریت ریسک گزارش خود را به طور رسمی به هیئت مدیره ارسال می‌کنند. بااین‌حال غالباً مخاطب خطوط گزارشگری روزانه و کانال‌های ارتباطاتی به احتمال بیشتر به جای هیئت مدیره، مدیران ارشد هستند. در طول زمان ممکن است فعالیت‌های کنترلی حیاتی با ادغام در درون سازمان از طریق تعامل و مبادله‌ی اطلاعات با فعالیت‌های دیگر خطوط اول و دوم دفاعی به تدریج استقلال خود را از دست بدهند و شاید دیدگاه‌هایی را اتخاذ کنند که به جای واحدهای کنترلی از سوی واحدهای ریسک‌پذیری مطرح شده‌اند. هم‌چنین پاداش‌دهی به دومین خط دفاعی نیز نقش

---

[۲۲] لیونز، *نظارت شرکتی و خطوط دفاعی ذی‌نفعان*، گزارش عملیات اجرایی هئیت کنفرانس، شماره‌ی ۳۶۵، اکتبر ۲۰۱۱؛ کاپریلیونه و کاسالینو، «بهبود راهبری شرکتی و مهارت‌های مدیریتی در موسسات بانکی»، مجله‌ی بین‌المللی یادگیری شرکتی پیشرفته، ۲۰۱۴، جلد ۷، شماره‌ی ۳؛ اسپیرا و پیج، «مدیریت ریسک؛ ابداع دوباره‌ی کنترل داخلی و تغییر نقش حسابرسی داخلی»، *مجله‌ی حسابداری، حسابرسی و پاسخگویی*، ۲۰۰۳، جلد ۱۶، شماره‌ی ۴، صفحات ۶۴۰ تا ۶۶۱؛ کمیته‌ی سازمان‌های پشتیبان کمیسیون تریدوی (COSO)، *نظارت موثر بر ریسک واحدتجاری: نقش هیئت-مدیره‌ها*، سپتامبر ۲۰۰۹.

[۲۳] UBS ، گزارش سهامداران در ارتباط با کاهش‌های ارزش UBS، آوریل ۲۰۰۸.

[۲۴] چارچوب اجرای حرفه‌ای بین‌المللی (IPPF)، آلتامونت اسپرینگز، فلوریدا: انجمن حسابرسان داخلی، ۲۰۱۳.

[۲۵] اندرسونن و یوبنکس، بهره‌گیری از COSO در امتداد سه خط دفاعی، جولای ۲۰۱۵.

مهمی در این روند ایفا می‌کند. بانک‌ها در تعیین اهداف مناسب برای واحدهای کنترلی که بتوانند توازن مناسبی میان ریسک‌پذیری و هشیاری کنترلی برقرار کرده و در عین حال امکان کسب سود باثبات را برای سازمان فراهم کنند با دشواری‌های زیادی روبه‌رو هستند.

۳. فقدان مهارت‌ها و تخصص کافی در فعالیت‌های دومین خط

حتی اگر فعالیت‌های حاضر در خط دوم دفاعی استقلال سازمانی داشته باشند ممکن است از مهارت‌ها و تخصص کافی برای به چالش کشیدن موثر روش‌های عملکرد و شیوه‌های کنترلی خطوط اول برخوردار نباشند یعنی اقداماتی مانند تأیید اعتبار مدل‌های پیچیده (مانند مدل‌های مبتنی بر رتبه‌بندی داخلی یا ریسک نرخ بهره‌ی در دفتر بانکی) یا ارزش‌گذاری مستقل ابزارهای دارای قدرت نقدشوندگی پایین یا آنهایی که تعیین ارزش آن‌ها دشوار است. با این‌حال علیرغم مقررات سختگیرانه‌تری که در زمینه‌ی روش‌های پاداش‌دهی متغیر وضع شده‌اند، هم‌چنان پاداش‌هایی که برای فعالیت‌های اولین خط در نظر گرفته می‌شوند و هم‌چنین تخصص این فعالیت‌ها به مراتب بالاتر و مهمتر از فعالیت‌های دومین خط است. سوالی که باقی می‌ماند این است که چطور بانک‌ها می‌توانند کارکنان بسیار مجرب را به جای کار در فعالیت‌های اولین خط یا ریسک‌پذیر به سوی فعالیت‌های دومین خط جلب کنند. جروم کرویل[ش] یکی از کارکنان موسسه مالی Société Générale توانست موقعیت سفته‌بازی غیرمجاز خود را به مدت بیش از یک سال حفظ کند بدون آنکه مقامات این موسسه متوجه ماجرا شوند.[۲۶] دفاتر پشتیبانی و بخش‌های کنترل ریسک موسسه Société Générale بازرسی‌های متعددی را در رابطه با بی‌نظمی‌ها و ناسازگاری‌های ناشی از این معاملات سفته‌بازی انجام دادند اما نتوانستند هیچگونه تخلفی را تشخیص دهند چرا که کرویل توانسته بود با پاسخ‌های دروغین خود [تخلفات خود را مخفی نگه دارد] و هیچ‌یک از فعالیت‌های کنترلی حاضر در دومین خط نیز پاسخ‌های وی را به حد کافی به چالش نکشیدند.

۴. انجام ارزیابی ذهنی و نامناسب ریسک توسط حسابرسی داخلی

اثربخشی کار حسابرسان داخلی وابستگی زیادی به برنامه‌های حسابرسی معتبری دارد که براساس ارزیابی‌های سالانه، جامع وعینی ریسک تهیه شده باشند و توسط افرادی انجام شوند که درک خوبی از مجموعه ریسک های سازمان دارند. برخورداری حسابرسان داخلی از دانش، مهارت‌ها و تجربه‌ی لازم برای انجام این قضاوت‌ها به شدت به تجربه‌ی شخصی خود حسابرسان و آشنایی آن‌ها با فرآیندهای ریسک‌پذیری و فعالیت‌های مدیریتی وابسته است. هدف این ارزیابی‌های ریسک شناسایی حوزه‌ها یا فرآیندهای پرریسک سازمان است تا حسابرسی‌های دقیق‌تر و بیشتری از آن‌ها انجام شود. ناتوانی در شناسایی حوزه‌های پرریسک باعث جلب توجه حسابرسان به حوزه‌های ریسک نادرست شده و اثربخشی عملکرد سومین خط دفاعی را تضعیف می‌کند. درست همانطور که در مثال موسسه مالی UBS[۲۷] حسابرسان داخلی میزهای معاملات بحرانی مشتقات وام‌های مسکن با پشتوانه‌ی رهنی ایالات متحده را بررسی کرده و نقاط ضعفی را در روند

[۲۶] Société Générale ، بخش بازرسی عمومی، گزارش خلاصه، می ۲۰۰۸.

[۲۷] UBS ، گزارش سهامداران در ارتباط با کاهش‌های ارزش UBS، آوریل ۲۰۰۸.

کنترل آن‌ها شناسایی کردند اما نتوانستند در مدت زمان کافی گزارش حسابرسی خود را آماده کنند. تأخیر ایجاد شده در روند تأیید و تکمیل گزارش حسابرسی (که حتی به چند ماه رسید) بسیار حیاتی بود و اثربخشی گزارشی که می‌توانست کیفیت مناسبی داشته باشد را تضعیف کرد.
تعبیه کردن نقش حسابرسان مستقل در ساختار سیستم دفاعی می‌تواند کمبودهای مدل سه خط دفاعی مرسوم را تا حدودی جبران کرده و صحت و قابلیت اطمینان چارچوب مدیریت ریسک را (که بر اطلاعات و تخصص بیشتر حسابرس مستقل متکی است) افزایش دهد. در بخش بعدی با معرفی منطق مبنای مدل چهار خط دفاعی این ایده را بیشتر توضیح می‌دهیم.

۴. مفهوم مدل «چهار خط دفاعی» در موسسات مالی

از زمان ظهور بحران مالی جهانی، طراحی و پیاده‌سازی سیستم های کنترل داخلی توجه جدی محافل دانشگاهی و حرفه‌ای را به خود جلب کرده است. در همین حال، پژوهش هایی که به بررسی ویژگی‌ها و اثربخشی فعالیت حسابرسی داخلی می‌پردازد با حمایت مالی بنیاد پژوهشی انجمن بین‌المللی حسابرسان داخلی در بازه های زمانی منظم انجام شده و در مجلات دانشگاهی و تخصصی منتشر شده است.
از این رو، در طراحی و پیاده‌سازی سیستم‌های کنترلی برای تعیین حوزه‌ای که موسسات مالی به مدل کنترل داخلی نیاز دارند، رسیده‌ایم.
این که آیا مدل چهار خط دفاعی در موسسات مالی باید آنطور که بطور نظری بیان شده، به درستی قاعده-مند شده و بطور عملی اجرا شود، نقطه شروع تحلیل ما است. این پرسش را می توان زیرمجموعه ای از این پرسش دانست که آیا مناسب است که به تعاملات بین حسابرسی داخلی، ناظرین مالی و حسابرسان مستقل بپردازیم. در برخورد با این پرسش، باید بدانید که ما دامنه بررسی خود در مورد مدل سه خط دفاعی را به صنعت مالی محدود می‌کنیم.
پس از بحران مالی جهانی، پیشنهادها و اصلاحات مربوط به راهبری شرکتی موسسات مالی و، بطور خاص، مربوط به سیستم‌های کنترل داخلی، از مدل سه خط دفاعی به عنوان واحد پایه تحلیل، استفاده کردند. یعنی، ریسکی وجود داشت که این مدل نتواند راهبری شرکتی موثر را تضمین کند و در واقع ممکن است ضعف‌های اساسی راهبری شرکتی را، به خصوص در بخش های قانونمند همچون بانکداری، تشدید کند.
بطور دقیق تر، مدل سه خط دفاعی ممکن است در برخورد دقیق با ویژگی های عملیاتی سازمان که نه تنها از ماهیت آن کسب و کار[۲۸] بلکه از چارچوب اختصاصی موسسات بانکداری و بیمه (مقررات و نظارت) سرچشمه می‌گیرند، نامناسب باشد.[۲۹] هدف آن چارچوب حمایت از ذینفعان مختلف بانک‌ها و شرکت‌های

---

[۲۸] بانک‌ها کسب و کارهایی منحصر به فرد هستند که در آن‌ها واسطه‌ها بین پس‌اندازکنندگان و استفاده‌کنندگان از سرمایه وجود دارند. بانکداری به عنوان نوع خاصی از فعالیت در نظر گرفته می‌شود که پیچیدگی بالایی به دنبال دارد و منجر به درگیر شدن ذی‌نفعان متعدد و به وجود آمدن سطح بالایی از ارتباطات میان شرکت‌کنندگان بازار می‌شود. برای مثال، این مقالات را بخوانید: ده‌هان و ولاهو، «راهبری شرکتی بانک‌ها؛ یک پیمایش»، مقاله کاری DNB، ۲۰۱۳، ۳۸۶، ۲؛ مهران، موریسون و شپیرو، *راهبری شرکتی و بانک‌ها: آن چه از بحران مالی یاد گرفته‌ایم*، بانک فدرال رزرو نیویورک، ۲۰۰۱، ۵۰۲، ۳.

[۲۹] این موضوع همچنین به صورت سنتی به عنوان یک «قانون ساختاری» در تاریخچه‌ی مالی آنگلوساکسون شناخته می‌شده است: کوتس، «قانون ولکر به عنوان قانون ساختاری: تبعات برای تحلیل هزینه-فایده و قانون اداری»، مقاله‌ی کاری قانون ECGI، ۲۰۱۵، شماره‌ی ۲۹۹.

بیمه‌ای در برابر ریسک‌های خاص ذاتی چنین سازمان‌هایی، شامل آسیب پذیری در برابر فروپاشی سیستماتیک است.[۳۰و ۳۱]

مقررات در دهه گذشته بطور فزاینده‌ای تفصیلی شده‌اند. به موازات این امر، ناظرین مالی بطور فزاینده‌ای برای رسیدگی به هر جنبه‌ای از سازمان و راهبرد مربوط به حفاظت از دوام موسسات مالی هرگاه که درستی بازار در خطر بود، فراخوانده شدند.

انگیزه این نوشتار بررسی و مطالعه این موضوع است که چرا موسسات مالی از دیگر بخش‌ها متفاوتند، و بهبود اثربخشی مدل سه خط دفاعی است. همچنین مدل جدیدی پیشنهاد می‌کنیم که به جای نادیده گرفتن ویژگی‌های بخش مالی بر آنها متمرکز می‌شود. به علاوه، مدل سه خط دفاعی را می‌توان با گنجاندن ناظرین و حسابرسان مستقل به عنوان بخشی جدایی‌ناپذیر از سیستم‌های کنترل داخلی و پایش ریسک، تقویت کرد. گرچه، بسته به اندازه، ماهیت و پیچیدگی یک واحد تجاری، ممکن است طرف های دیگری نیز در مدیریت ریسک دخیل باشند. این طرف ها لازم است بخشی جدایی ناپذیر از مدل باشند: خط چهارم دفاعی به خصوص برای موسسات مالی ممکن است از طریق حسابرسان مستقل و یا مقررات‌گذاران[۳۲] به وجود آید.

برای مدتی طولانی، تدوین‌کنندگان استانداردهای بین‌المللی رابطه نزدیک بین ناظرین، و نهادها و فعالیت-های داخلی را لازم نمی دانستند.[۳۳] اخیرا، آنها خواهان تعامل قوی‌تر، به ویژه در رابطه با افزایش گفتمان با هیئت مدیره و مدیریت ارشد در مورد راهبری ریسک، شامل ایجاد چارچوب ریسک‌پذیری موسسه و ارزیابی فرهنگ ریسک آن، شده‌اند. از این لحاظ، فدرال رزرو اخیراً به این موضوع پرداخته و، بر مبنای *بیانیه خط-مشی در مورد فعالیت حسابرسی داخلی ۲۰۰۳*، بخش جدیدی تحت عنوان *روش های بهبود یافته حسابرسی داخلی* عرضه کرد. آن بخش بازرسان را ترغیب می‌کند تا «به کار انجام شده از سوی حسابرسان داخلی اتکا کرده» و «رویه های بازرسی خود را از طریق پایش مداوم و ارزیابی عناصر کلیدی حسابرسی داخلی تکمیل کنند».[۳۴] مقاله کمیته نظارت بانکی بازل در مورد وظیفه حسابرسی داخلی در بانک‌ها به هنگام توصیف رابطه بین حسابرسی داخلی و ناظرین به نتایج مشابهی می‌رسند.[۳۵] آن نه تنها مروری بر انتظارات نظارتی در رابطه با فعالیت حسابرسی داخلی (شامل ارزیابی کیفیت) را ارائه می‌دهد بلکه به صراحت بر منافع افزایش ارتباط بین ناظرین و فعالیت حسابرسی داخلی تاکید می‌کند.

---

[۳۰] هوپت، «راهبری شرکتی بانک‌ها و سایر موسسات مالی بعد از بحران مالی»، *مجله‌ی مطالعات قانون شرکتی*، ۲۰۱۳، ۲۴۳؛ وان دِر الست، «راهبری شرکتی و بانک‌ها؛ این بازی چقدر توجیه‌پذیر است»، *مقاله‌ی کاری قانون ECGI*، ۲۰۱۵، ۲۸۴، ۲۴.

[۳۱] مولبرت، «راهبری شرکتی بانک‌ها»، مجله‌ی مقالات مروری قانون سازمانی کسب و کار اروپایی، ۲۰۰۹، ۴۲۲. مقررات‌گذار، منافع طرفین همانند منافع عمومی را نمایندگی می‌کند که این گروه‌های نمایندگی شده به سبب فقدان حقوق یا مشوق‌های مناسب، قادر به محافظت از خود از طریق سازوکارهای خصوصی نیستند (برای مثال، این مقاله را ببینید: الکساندر، «راهبری شرکتی و مقررات بانکداری»، مقاله‌ی کاری کمبریج، ۲۰۰۴، ۱۷، ۳).

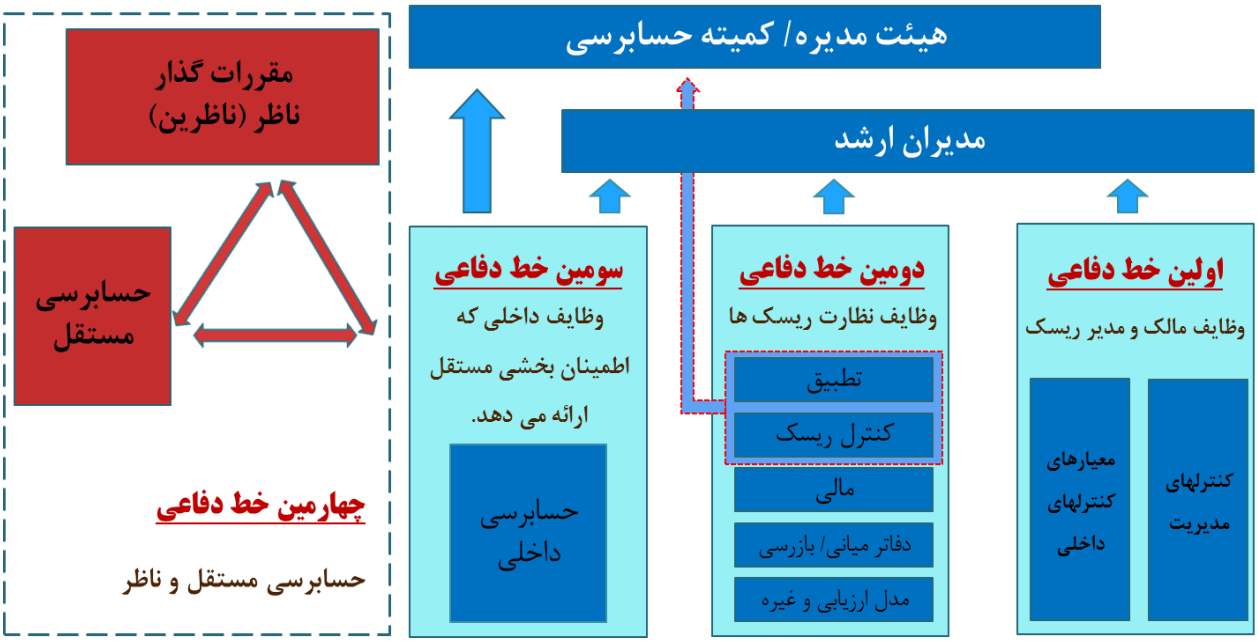
[۳۲] هاپکین، مدیریت ریسک، انتشارات کوگان پیج، ۲۰۱۳، ۱۹۳.

[۳۳] مورد اخیراً منتشر شده: هیئت ثبات مالی، شدت و اثربخشی نظارتی. گزارش پیشرفت در زمینه‌ی نظارت تقویت شده، ۷ آوریل ۲۰۱۴.

[۳۴] ارکان راهبری سیستم فدرال رزرو ، *بیانیه‌ی خط‌مشی تکمیلی در ارتباط با فعالیت حسابرسی داخلی و برون‌سپاری آن*، ۲۰۱۳.

[۳۵] کمیته نظارت بانکی بازل، فعالیت حسابرسی داخلی در بانک‌ها، ژوئن ۲۰۱۲.

نمودار ۲: مدل ۴ خط دفاعی برای موسسات مالی



از آنجا که مدل چهار خط دفاعی می‌خواهد هماهنگی بین اشخاص برون‌سازمانی و حسابرسان داخلی را افزایش دهد، ارتباط بیشتر اساس موفقیت آن است. کارهای ارتباطی از طریق کاهش، و نه حذف، اطلاعات نامتقارن میان اشخاص درگیر عمل می‌کند، البته در صورتی که رفتار (تبادل) اطلاعات طوری باشد که سیستم‌های کنترل ریسک کارامدتر شوند.

در برخی موارد، اعمال الزامات افشای بیشتر می‌تواند زیانبخش باشد، اگر باعث شود طرف‌های درگیر در لایه چهارم رفتار خود را در جهت مخالف تغییر دهند. این موضوع مشکل مخاطره اخلاقی در آسیب اثربخشی سیستم‌های کنترل داخلی را بدتر خواهد کرد.[۳۶] افزایش میزان اطلاعات به خودی خود خوب نیست، و حتی می‌تواند منجر به سیستم‌های کنترل با اثربخشی و کارایی کمتر شود.[۳۷]

از آن لحاظ، مدل چهار خط دفاعی مجموعه جدیدی از فرایندها و قواعد، به خصوص از لحاظ اطلاعاتی که حسابرسان داخلی، حسابرسان مستقل و ناظرین به ترتیب باید به اشتراک بگذارند (یا مجاز نیستند به اشتراک بگذارند) را به دنبال خواهد داشت. این قواعد دسته‌بندی‌های اطلاعاتی را که در اختیار آنها قرار می‌گیرند، رویه‌های کسب اسناد و سوابق، و قواعد محدودکننده انتشار اطلاعات مستثنا و محرمانه بازرسی و حفاظت اطلاعات محرمانه را تعیین می‌کنند.

از آنجا که در طول زمان پیچیدگی کسب و کار بانکداری افزایش یافته، وظایف ناظرین بانکی و حسابرسان مستقل واقعاً بطور فزاینده‌ای متقاضی داشته است. این مورد به خصوص در نظام‌های مقرراتی صدق می‌کند که در آن این دو (ناظرین بانکی و حسابرسان مستقل) در مقام بازرس مرکزی و مقامات بازرس ملی مشترک

---

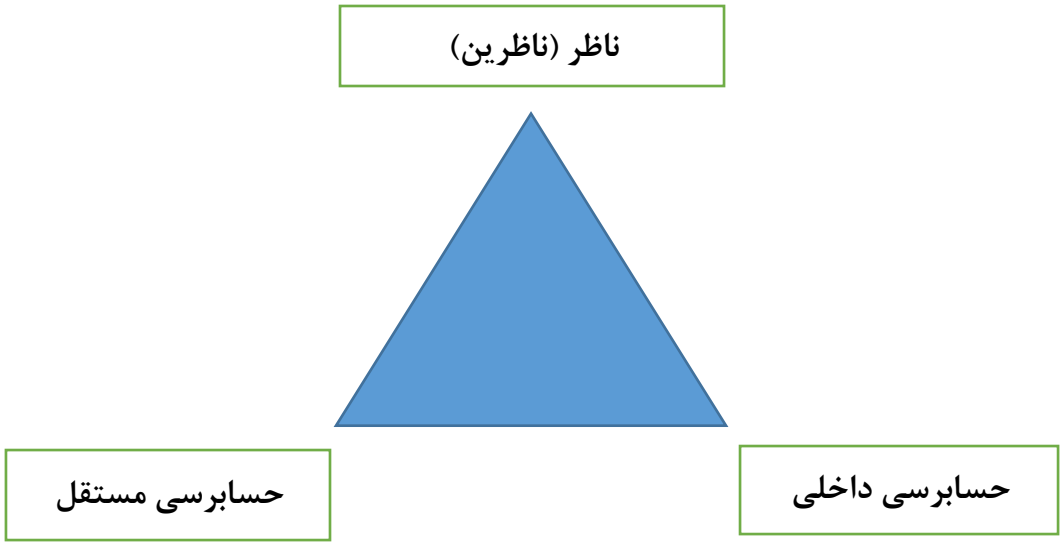
[۳۶] در نبود توافق‌نامه‌های افشاء در ارتباط با رفتار اطلاعات، حسابرسی داخلی یک بانک ممکن است اطلاعات محرمانه را در ارتباط با موقعیت بانکی دیگر افشا کند.

[۳۷] همین مشکل برای مثال در زمانی روی می‌دهد که دولت می‌بایست به صورت بهینه‌ای اطلاعات مربوط به دارایی‌های بانک‌ها را در خلال یک بحران مالی افشا کند: رجوع شود به فاریا ای کاسترو، مارتینز و فیلیپون ، "رانز در مقابل لیمونز: افشای اطلاعات، ظرفیت اقتصادی و ثبات مالی"، دفتر ملی تحقیقات اقتصادی، ۲۰۱۵.

هستند، مانند اتحادیه اروپا.[۳۸] پیچیدگی در حال افزایش معاملات و بازارها، توان سازمان های نظارتی را درکاهش عدم تقارن اطلاعات کمتر کرده است. در نتیجه، باید به دنبال رویکردهای مکمل برای کاهش این عدم تقارن‌ها بود. این خط اضافه شده دفاعی می‌تواند از این لحاظ کمک‌کننده باشد. در واقع، حسابرسان داخلی، ناظرین بانکی و حسابرسان مستقل با همین چالش‌ها روبرو هستند و نقش آنها باید بیشتر به عنوان مکمل دیده شود.

ناظرین بانکی نه تنها از حاصل کار حسابرسی داخلی نفع می‌برند بلکه برای برخی وظایف خاص دیگر یا برای گردآوری اطلاعات تکمیلی وقتی این اطلاعات به کار نظارتی آنها کمک کند به حسابرسان مستقل هم روی می‌آورند. به علاوه، همزمان حسابرسان مستقل نیز می‌توانند از رابطه با ناظرین سود ببرند. حسابرسان مستقل در انجام وظایف خود، می‌توانند به اطلاعاتی دسترسی یابند که به آنها در انجام موثرتر مسئولیت-هایشان کمک کند. این موضوع منجر به رابطه سه‌گانه بین حسابرسان داخلی، ناظرین بانکی و حسابرسان مستقل می‌شود.

نمودار ۳: مثلث مقرراتی



طبق مدل چهار خط دفاعی، حسابرسان مستقل می‌توانند ارزیابی مستقلی از سه خط اول ارائه دهند جائیکه این ارزیابی به حسابرسی گزارشگری مالی سازمان و به رعایت الزامات مقرراتی مربوط است. از این لحاظ، با ارائه اطمینان بیشتر به سهامداران و مدیریت ارشد، حسابرسان مستقل، مقررات‌گذاران و سایر نهادهای برون‌سازمانی نقش مهمی در ساختار کلی راهبری و کنترل سازمان به عهده دارند.

به علاوه، تعامل بین وظایف کنترلی (یعنی وظیفه حسابرسی داخلی) و ناظرین می‌تواند منجر به بهبود ابزارها و روش‌هایی شود که می‌توانند از سوی ناظرین برای تشدید نظارت خود بر موسسات مالی بکار روند،

[۳۸] در ارتباط با تقسیم وظایف بین ECB و NCAها، ECB، راهنمای نظارت بر بانکداری، نوامبر ۲۰۱۴ را بخوانید. در متون، این مقالات را بخوانید: فرارینی و چیارلا، «نظارت مشترک بانکداری در منطقه‌ی اروپا: نقاط قوت و ضعف»، مقاله‌ی کاری قانون ECGI، ۲۰۱۳، ۲۲۳؛ اِیلیس، «اتحادیه‌ی بانکداری اروپایی و بازار مالی یگانه‌ی اتحادیه‌ی اروپا: یکپارچگی متمایزتر یا عدم یکپارچگی؟»، مقاله‌ی تحقیقاتی دانشکده‌ی حقوق دانشگاه کمبریج، ۲۰۱۴، شماره‌ی ۲۹؛ فرارینی، «نظارت یگانه و راهبری بازارهای بانکی»، مقاله‌ی کاری قانون ECGI، ۲۰۱۵، ۲۹۴.

با این هدف که به جای نظارت منفعلانه و مبتنی بر نتیجه، نظارت پیش‌گیرانه ارائه دهند. به عبارت دیگر، از طریق کانال‌های ارتباطی بهبود یافته با حسابرسی داخلی، ناظرین می‌توانند اطلاعات مفید و قابل اتکایی برای پشتیبانی کردن از قضاوت‌های خود بدست آورند و می‌توانند آینده‌نگری بیشتری در ارزیابی‌های خود از ریسک داشته باشند. ناظرینی که اطلاعات بهتری دارند، و به اطلاعات دقیق مسلح هستند، کمک می‌کنند در اطمینان‌دهی این که پایداری بازار حفظ می‌شود.

به خصوص در زمان‌هایی که، بیش از همیشه، موسسات مالی باید اعتماد عمومی و اعتماد آنهایی را که با آنها تجارت می‌کنند را بازیابی و مدیریت کنند، رابطه نزدیک تر بین حسابرسان داخلی، ناظرین و حسابرسان مستقل، به بخش مالی اعتبار و اطمینان خواهد بخشید. درک متقابل بیشتر نقش‌ها و مسئولیت‌های مربوط به این سه نقش آفرین، اثربخشی هر حوزه را بهبود خواهد بخشید، زیرا آنها نگرانی‌های مکملی در رابطه با موضوعات یکسان دارند گرچه تمرکز نگرانی‌های آنها متفاوت است.

بر مبنای رابطه سه گانه بین حسابرسان داخلی، ناظرین و حسابرسان مستقل، بخش‌های بعدی این مقاله منافع مدل چهار خط دفاعی را از طریق بررسی هر یک از تعاملات بین آنها روشن می‌کند. بررسی سوابق فعلی موضوع نشان می‌دهد که هیچ‌یک از مطالعات مستقیماً به موضوعات مربوط به چنین مدلی نمی-پردازند. بیایید هر رابطه را به نوبت بررسی کنیم، زیرا هر کدام عنصر مهمی در بهبود سیستم کنترل اثربخش است که به بهترین تخصیص و مدیریت ریسک در درون موسسات منحصر به فرد منجر می‌شود.

۵. رابطه بین وظایف سومین و چهارمین خط دفاعی

۵.۱. رابطه بین حسابرسان مستقل و ناظرین

اولین رابطه مورد بررسی رابطه‌ای است که بین حسابرسان مستقل و مراجع مقررات گذار وجود دارد. در حالیکه هر یک از این دو فعالیت، دامنه و رویکردهای مخصوص به خود را دارند، اما با این وجود حوزه‌ها و موضوعات یکسانی میتوانند تابع تغییر تعدیل شده اطلاعات و دیدگاه‌ها باشد.[۳۹]

قبل از توضیح ویژگی‌های ارتباط و خصوصیات تعامل حسابرسان مستقل و ناظرین، ابتدا باید مسئولیت‌های آنها را تحلیل کنیم.

نقش حسابرس مستقل در درجه اول بررسی صورت‌های مالی و اطمینان از این موضوع است که آنها عاری از هرگونه تحریف بااهمیت و بر طبق یک چارچوب گزارشگری مالی مناسب تهیه شده‌اند.[۴۰] این نکته باید در ابتدا ذکر شود که اظهارنظر حسابرس در ایجاد اعتبار برای صورت‌های مالی بسیار مربوط است و باعث حمایت از سلامت مالی موسسه می‌شود. همانند حسابرسان داخلی، حسابرسان مستقل اطمینان‌دهی مستقلی برای هیئت مدیره، مدیریت ارشد و سهامداران ارائه می‌دهند. با این وجود، دامنه فعالیت حسابرس داخلی با حسابرس مستقل متفاوت است، همچنان که حسابرس مستقل در درجه اول با صورت‌های مالی سر

---

[۳۹] قدردانی از کار حسابرسی داخلی توسط کمیته نظارت بانکی اروپایی در نظراتشان مطرح شده است: «استاندارد بین‌المللی بازنویسی شده‌ی پیشنهادی در ارتباط با حسابرسی ۶۱۰- ملاحظات حسابرس در ارتباط با وظیفه حسابرسی داخلی»، مارس ۲۰۰۷.

[۴۰] ISA (استاندارد بین‌المللی حسابرسی) ۲۰۰، اهداف کلی حسابرسی مستقل و انجام حسابرسی طبق استانداردهای بین‌المللی حسابرسی، پاراگراف ۱۱.

و کار دارد. حسابرس مستقل گواهی می‌کند که صورت‌های مالی از تمام جنبه‌های بااهمیت انعکاس درستی از وضعیت و عملکرد مالی شرکت ارائه می‌دهند.[۴۱]

به منظور اطمینان از استقلال حسابرس مستقل، ترتیبات راهبری جداگانه‌ای باید بکارگرفته شود. کمیته حسابرسی هیئت مدیره باید از بین موسسات حسابرسی، کاندید مناسب را برای فعالیت به عنوان حسابرسان مستقل شناسایی و معرفی نماید و سپس با انتصاب آنها موافقت کند. چرخش‌ها و محدودیت‌های اجباری تصدی، اکنون بطور رایج در مورد حسابرسان مستقل اعمال می‌گردد، تا از شرایطی که آنها به تدریج بیطرفی و استقلال خود را در طول زمان بخاطر ارتباط نزدیک با شرکت از دست می‌دهند، اجتناب شود. گذشته از این، در برخی حوزه‌های قضایی محدودیت‌هایی برای میزان خدمات غیرحسابرسی از جانب حسابرس معرفی کرده‌اند که مانع مشارکت حسابرسان مستقل در حسابرسی کار خود می‌شود. همچنین موسسات مالی می‌توانند با افشای عمومی پرداخت‌ها به حسابرسان مستقل برای خدمات غیرحسابرسی و ممانعت از داشتن سهم توسط آنها در شرکت حسابرسی شده، استقلال حسابرسان را تقویت کنند.[۴۲]

برخی از مسئولیت‌های کلیدی ناظرین بانکداری شامل مواردی مانند «دادن مجوز به بانک‌ها، انجام نظارت مستمر، بررسی رعایت قوانین و اتخاذ اقدامات اصلاحی به موقع برای رسیدگی به نگرانی‌های مربوط به ایمنی و امنیت بخصوص در رابطه با خطرهای احتمالی برای ثبات مالی» می‌شود.[۴۳] یکی از موارد اساسی در نظارت موثر، استقلال عملیاتی ناظر به همراه چهارچوب راهبری صحیح در اختیارات نظارتی است. به دنبال تغییرات محیط نظارتی و قانونی و در پاسخ به کاستی‌های برجسته شده بخاطر بحران مالی جهانی، دامنه فعالیت‌های نظارتی برای مشمول کردن مسئولیت‌های اضافی مانند بررسی چارچوب مدیریت ریسک عملیاتی، ارزیابی چارچوب‌های کنترل داخلی و کفایت حسابرسی داخلی و مستقل افزایش یافته است.[۴۴]

در عمل، رشد پیچیدگی و بین‌المللی‌شدن رو به رشد موسسات مالی به این معنا است که یک موسسه به ندرت تابع یک مقام مقررات گذار واحد قرار می‌گیرد. موسسات ممکن است به دلایل خاص زیر تابع بیش از یک نهاد مقررات‌گذار شوند:

- گروه‌های بانکداری و بیمه برون مرزی. یک موسسه مالی می‌تواند بخشی از یک گروه بزرگ بانکداری یا بیمه فعال بین‌المللی با مالکیت خارجی باشد. در این صورت مقررات‌گذار مستقر در کشور شعبه یا شرکت فرعی «مقررات‌گذار میزبان» نامیده می‌شود در حالیکه مقررات‌گذار شرکت اصلی به عنوان «مقررات‌گذار اصلی یا مبدا» عمل می‌کند. به منظور تسهیل تبادل اطلاعات بین مقررات‌گذار اصلی و مقررات‌گذاران میزبان (متعدد)، «نهادهای نظارتی» پایه‌ریزی شده‌اند. چنین نهادهایی باید ساختارهای دایمی اما منعطفی باشند که اجازه همکاری، هماهنگی و اشتراک اطلاعات بین مراجع مقررات گذاری گروه‌های مالی برون مرزی را بدهند.[۴۵]

---

[۴۱] OECD ، اصول راهبری شرکتی، سپتامبر ۲۰۱۵.

[۴۲] OECD ، اصول راهبری شرکتی، سپتامبر ۲۰۱۵.

[۴۳] کمیته نظارت بانکی بازل، *اصول اساسی برای نظارتِ بانکی موثر*، اصل اساسی ۲۷، سپتامبر ۲۰۱۲.

[۴۴] همان ماخذ.

[۴۵] کمیته نظارت بانکی بازل، *اصولی برای دانشکده‌های نظارتی موثر*، ژوئن ۲۰۱۴.

- ساختارهای مخصوص منطقه‌ای یا کشوری. چنین ساختارهایی می‌توانند موسسات مالی را ملزم به تابعیت از ترتیب خاصی مانند یک مرجع نظارتی فراملی در کنار ناظر محلی کنند. یک نمونه از چنین نهادهای نظارتی فراملی «نظام نظارتی واحد» (SSM[ض]) است که اختیار نظارتی متمرکز بانکی واگذار شده به بانک مرکزی اروپا (ECB[ض]) را بازنمایی می‌کند. هر چند که این نهاد در سال ۲۰۱۴ تاسیس شد، اما با این وجود تقسیم دقیق قدرت هنوز نیازمند موافقت ناظران ملی مشارکت کننده و نظام نظارتی واحد است.[۴۶و ۴۷]
- نهادهای نظارتی متعدد در حوزه قضایی یکسان. بسته به تکالیف و مسئولیت‌های نظارت مالی در یک حوزه قضایی خاص، مقررات‌گذاران متعدد (برای نمونه مقررات‌گذاران بانکی و بیمه، و کمیسیون‌های بورس و اوراق بهادار) می‌توانند عهده‌دار نظارت بر یک موسسه مالی شوند.

این لایه‌های بیشتر بررسی نظارتی ممکن است باعث افزایش پیچیدگی شیوه‌ای شوند که ناظرین با حسابرسان مستقل تعامل می‌کنند. ناظرین باید مطمئن شوند که هر مقررات‌گذار دست‌اندرکار برای اجتناب از تداخل احتمالی وظایف حدود دامنه بررسی محول شده به خود را رعایت می‌کند.

بعد از تعیین مسئولیت‌های حسابرس مستقل و ناظر، ویژگی‌های رابطه آنها و چگونگی نفع رسانی به یکدیگر را با جزئیات بیشتری تجزیه و تحلیل می‌کنیم. منافع مشترک این دو در این موضوع خلاصه می‌شود که حسابرس می‌تواند اطلاعات مربوط به ریسک و اقدامات عملیاتی را کسب کند که در غیر اینصورت برای ناظرین به طور مستقیم قابل دسترسی نخواهد بود.

ناظرین می‌توانند از نتایج بررسی چارچوب کنترل داخلی که توسط حسابرس مستقل انجام می‌شود بهرمند گردند که اغلب ناظرین بخاطر محدودیت‌های منابع و بودجه قادر به انجام چنین بررسی‌هایی نیستند. اگر ناظر چنین اطلاعاتی را دریافت کند، اثر بخشی نظارت بهبود خواهد یافت. ناظرین همچنین اطلاعات را جمع‌آوری، و بررسی‌های خود را بر ارزیابی توانایی سازمان برای پیروی از مقررات مالی مرتبط با حوزه قضایی مورد بحث متمرکز می‌کنند. در همین راستا این اطلاعات می‌تواند بر صورت‌های مالی تاثیر گذارد و مورد توجه حسابرسان مستقل قرار گیرد که - بخاطر ماهیت وظایفشان – ممکن است به اطلاعات با جزئیات بیشتر دسترسی نداشته باشند. اطلاعات ارائه شده توسط ناظر می‌تواند به حسابرس مستقل این امکان را بدهد تا اظهارنظر بهتری در مورد درست بودن صورت‌های مالی ارائه دهد.[۴۸]

باید این نکته را در نظر داشت که یک رابطه سلسله مراتبی بین ناظرین و حسابرسان مستقل وجود دارد: ناظرین الزامی برای ارزیابی کفایت حسابرسی‌های مستقل دارند، قدرت این را دارند تا دامنه کاری حسابرسان مستقل را ایجاد، و ممکن است استانداردهایی برای پیروی در انجام چنین حسابرسی‌هایی تعیین کنند. ناظر همچنین ممکن است استفاده از رویکردهای خاصی را در برنامه‌ریزی و انجام حسابرسی‌های مستقل مطالبه نماید.[۴۹]

---

[۴۶] ECB ، ۲۰۱۵/۸۳۹ حکم *۲۷ آوریل ۲۰۱۵ شناسایی موسسه های اعتباری که تابع ارزیابی جامع هستند (ECB/2015/21)*.

[۴۷] مقررات‌گذار ریسک جهانی، «روابط ناظر مستقل ECB با مقامات ملی هنوز در جریان است»، *بانکدار* ، ژوئن ۲۰۱۵.

[۴۸] کمیته نظارت بانکی بازل، *حسابرسی‌های مستقل بانک‌ها*، مارس ۲۰۱۴.

[۴۹] کمیته نظارت بانکی بازل، اصول اساسی برای نظارتِ بانکی موثر، اصل اساسی ۲۷، سپتامبر ۲۰۱۲.

گذشته از این، حوزه‌های قضایی خاصی به ناظرین بانکی اجازه درخواست از موسسه‌های حسابرسی مستقل برای بررسی حوزه‌هایی فراتر از الزامات قانونی حسابرسان مستقل را در صورت صلاحدید می‌دهد.[۵۰]

در برخی از حوزه‌های قضایی، حسابرسان مستقل وظیفه گزارش موضوعات با اهمیت بالا[۵۱] را به ناظرین بر عهده دارند.[۵۲] ارزیابی انتقادی این الزام ضروری است، همچنان که این تنها در حوزه‌های قضایی ممکن است که در آن حسابرسان مستقل در برابر تعقیب یا اقدام قانونی هنگامی که افشای اطلاعات محرمانه اشخاص ثالث اتفاق می‌افتد، مصونیت دارند (حوزه امن ط).[۵۳] اگر مصونیت برای چنین حوزه امنی موجود نباشد، حسابرسان مستقل می‌توانند به اقدامات جایگزین متوسل شوند. برای نمونه آنها می‌توانند از طریق مدیریت بانک تصمیم به گزارش غیرمستقیم مسائل محرمانه به ناظرین بگیرند. از سوی دیگر حسابرسان مستقل می‌توانند همچنین کسب آشکار موافقت از هیئت مدیره و مدیریت را برای اجازه افشاء اطلاعات محرمانه به ناظرین در نظر بگیرند.[۵۴]

با این وجود، نمونه‌هایی وجود دارد که در آن حسابرسان مستقل بطور اختیاری تصمیم به گزارش مسائلی می‌گیرند که خارج از دامنه وظایف آنها قرار دارد، هرچند که در نهایت می‌تواند توجه ناظرین بانکی را جلب کند. چنین موردی ممکن است در صورتیکه حسابرس مستقل نارسایی‌های قابل توجهی در فرآیندهای کنترل داخلی، یا ساختارهای تجاری مبهمی برای دور زدن مقررات مالی کشف کند، اتفاق افتد.[۵۵]

فارغ از دامنه همکاری و تبادل اطلاعات، استقلال طرف‌های مختلف نباید مختل شود و هر طرف باید در موقعیتی قرار گیرد تا بطور مستقل در دامنه قانونی و مسئولیت‌های مرتبط به خود فعالیت کند. مرزهای مشخص مسئولیت باید وجود داشته باشد و تمامی طرفین باید از رعایت نظام‌های رازداری مطمئن شوند.

ارتباطات بین طرفین می‌تواند در قالب گزارش‌های کتبی یا گفتگوهای شفاهی مانند نشست‌های دوره‌ای یا ویژه بصورت رسمی و غیررسمی انجام شود. نشست‌ها می‌توانند ماهیت دوجانبه (یعنی بین حسابرس مستقل و ناظر) یا ماهیت سه جانبه (یعنی بین حسابرس مستقل، ناظر و رئیس کمیته حسابرسی) داشته باشند. بطور سیستماتیک بانک‌های مهم ترغیب به برگزاری نشست‌های سه جانبه شده‌اند.[۵۶] و ناظرین هم ترغیب به نوشتن گزارش‌های کتبی در مورد مسائل مهم و تبادل آنها با مدیریت، هیئت مدیره و حسابرسان مستقل می‌شوند.[۵۷]

اسناد مکتوب می‌توانند شامل گزارش‌های مبسوط در مورد صورت‌های مالی حسابرسی شده‌ای باشد که تسلیم ناظرین می‌شوند در حالیکه برای عامه مردم قابل دسترسی نیستند.

---

[۵۰] کمیته نظارت بانکی بازل، *حسابرسی‌های مستقل بانک‌ها*، مارس ۲۰۱۴.

[۵۱] اصطلاح «اهمیت بالا» نیازمند تفسیر زمینه قانون خاص مربوط به نهاد نظارتی است. یک یا چند موضوع که معمولا دارای اهمیت بالا برای فعالیت مقررات‌گذار هستند، با توجه به ماهیت یا تاثیر بالقوه مالی‌اش، به احتمال زیاد مستلزم بررسی توسط مقررات‌گذار است. (اهمیت بالا گاهی اوقات با برقراری روش قانونی منفرد تعیین می‌شود، مثلا ۵ درصد درآمد قبل از مالیات یا ۰.۵ درصد از کل دارایی‌ها).

[۵۲] کمیته نظارت بانکی بازل، *حسابرسی‌های مستقل بانک‌ها*، مارس ۲۰۱۴.

[۵۳] دستورالعمل ۶۵/۲۰۱۴/اتحادیه اروپا (MIFID II)، ماده ۷۷؛ دستورالعمل ۳۶/۲۰۱۳/اتحادیه اروپا (CRD IV)، ماده ۶۳.

[۵۴] کمیته نظارت بانکی بازل، *حسابرسی‌های مستقل بانک‌ها*، مارس ۲۰۱۴.

[۵۵] همان ماخذ.

[۵۶] کمیته نظارت بانکی بازل، *حسابرسی‌های مستقل بانک‌ها*، مارس ۲۰۱۴.

[۵۷] همان ماخذ.

در یک بررسی جالب که توسط مجمع مستقل مقررات گذاران (نهادهای ناظر) حسابرسی مستقل (IFIAR[ظ])[58] انجام شد، کیفیت کاری حسابرسان مستقل تحلیل شد. این سازمان اطلاعات بازرسی‌های کیفیت حسابرسی‌های مستقل نهادها با منافع عمومی، و موسسات مالی با اهمیت سیستماتیک (SIFI[ع]) را جمع آوری کرد. سه حوزه اصلی از یافته‌های گزارش شده در سال ۲۰۱۴ برای موسسات مالی با اهمیت سیستماتیک مربوط به حسابرسی ارزشیابی سرمایه‌گذاری و اوراق بهادار (۲۷ درصد از یافته‌های حسابرسی‌های بررسی شده)، آزمون کنترل داخلی (۲۷ درصد) و حسابرسی ذخیره برای زیان‌های وام و کاهش ارزش وام (۱۷ درصد) می‌شد.

هر یافته لزوما نشان دهنده نادرست بودن صورت‌های مالی نیست، هر چند که به این موضوع اشاره می‌کند که عملکرد حسابرس از سطح قابل انتظار پایین‌تر می‌رود که در صورت عدم افت می‌توانست نقش منافع عمومی حسابرسی را محقق کند. همچنین گویای این نکته است که حسابرسی در ارائه سطح اطمینانی برای صورت‌های مالی که مد نظر استانداردهای حرفه‌ای بوده و باید از آن اطمینان می‌داد، ناموفق عمل کرده است. اعتماد به حسابرس برای انجام چنین عملکرد اطمینان‌دهنده‌ای نباید وابسته به نتایج بررسی گذشته حسابرس باشد.

نسبت‌های سرمایه قانونی و همچنین دیگر شاخص‌های قدرت مالی مانند نسبت‌های نقدینگی و اهرمی، به همراه گزارش‌های مالی استاندارد بانک تولید می‌شوند، اما شیوه حسابرسی آنها متفاوت است. این موارد ممکن است باعث ایجاد شکاف انتظارات برای جامعه گردد: در واقع چیزی که ممکن است مورد توجه‌ترین شاخص یک بانک باشد حسابرسی نمی‌شود. حسابرسان مستقل می‌توانند وظایف اطمینان‌بخشی مرتبط با چنین نیازهای قانونی را انجام دهند (از جمله نسبت‌های سرمایه، دارایی‌های موزون به ریسک و نسبت‌های نقدینگی و اهرمی). الزامات بررسی مستقل اطلاعات سرمایه قانونی بطور تدریجی در کل دنیا تکامل یافته است؛ برخی از کشورها در دسترس بودن گزارش‌های اطمینان‌بخشی را اجباری می‌دانند و برخی تنها از موسسات مالی می‌خواهند تا مقررات گذاران را در جریان بگذارند، در حالیکه برخی دیگر درخواست هیچ نوع گزارشی را نمی‌کنند. با در نظر گرفتن اندازه و اهمیت بخش بانکداری - و خطر سیستماتیکی که متوجه بازارهای مالی جهانی است - اعتباردهی و اطمینان‌بخشی اهمیت ویژه‌ای پیدا می‌کنند.

ما برای نشان دادن اهمیت افزایش همکاری میان ناظرین بانک و حسابرسان مستقل، تحولات را در تعدادی از کشورها مورد بررسی قرار داده‌ایم:

۱. بریتانیا:

مقام مقررات‌گذار احتیاطی بریتانیا (PRA[غ]) اخیراً سندی مشاوره‌ای[59] در مورد ارائه گزارش‌های کتبی توسط حسابرسان مستقل بزرگترین بانک‌های بریتانیا به این مقام به عنوان بخشی از چرخه حسابرسی قانونی منتشر کرده است. مقام مقررات‌گذار احتیاطی از حسابرسان مستقل خواسته است که در نظارت بر شرکت‌ها با درگیر شدن مستقیم، فعالانه و سازنده برای حمایت از نظارت قضاوت محور و کمک به ارتقای ایمنی و

[58] گزارش IFIAR درباره بررسی یافته‌های بازرسی، ۳ مارس ۲۰۱۵.

[59] مقام مقررات‌گذار احتیاطی، *مشارکت بین حسابرسان مستقل و ناظرین و اجرای قدرت انتظامی PRA بر حسابرسان و اکچوئران مستقل*، مقاله مشاوره‌ای، فوریه ۲۰۱۵.

صحت شرکت‌های تحت نظارت مقام مقررات‌گذار احتیاطی مشارکت داشته باشند. بینش بدست آمده توسط حسابرسان حین حسابرسی‌های باکیفیت باید به افزایش اثربخشی رابطه میان حسابرسان و ناظر کمک کند. در سال‌های اخیر پیشرفت‌هایی مانند مشارکت نزدیک‌تر و مکررتر میان ناظرین و حسابرسان مستقل صورت گرفته است. مقام مقررات‌گذار احتیاطی به طور مستمر کیفیت ارتباط میان حسابرس و ناظر را پایش می‌کند. در یک نظرسنجی از حسابرسان مستقل ملاحظه شد که اکثراً این تعاملات را تنها «معقول» می‌دانستند و هدف مقام مقررات‌گذار احتیاطی بهبود این تعاملات در بلندمدت است. به طور خاص در مواردی هم ناظرین و هم حسابرسان اعتقاد داشتند که امکان بهبود در زمینه صداقت در به اشتراک‌گذاری اطلاعات، تکرر اشتراک‌گذاری و موارد مورد بحث در جلسات دوطرفه وجود دارد.

۲. سوئیس:

سالهاست که مقام ناظر بازار مالی سوئیس (FINMA[ف]) رویکردی دوگانه را پیش‌گرفته است که در آن بازرسی‌های در محل، به حسابرسان مستقل تاییدشده و دارای مجوز برون‌سپاری می‌شود. ارزیابی اخیر صندوق بین‌المللی پول[ق][۶۰] نشان می‌دهد که نقاط ضعف عدیده‌ای در سیستم نظارت در کشور سوئیس وجود دارد. مقام ناظر بازار مالی سوئیس باید با هدف اطمینان از هماهنگی بیشتر در نظارت میان نهادها، راهنمایی‌های بیشتری در اختیار حسابرسان قرار دهد و همچنین باید کار حسابرسان را با بازرسی‌های عمیق خود از مسائل انتخاب شده تکمیل کند. علاوه بر این پرداخت به حسابرسان توسط نهاد تحت نظارت آن‌ها مورد انتقاد قرار گرفته است و پرداخت به حسابرسان باید توسط صندوق تامین مالی اداره شده توسط مقام ناظر بازار مالی سوئیس انجام شود. صندوق بین‌المللی پول اشاره کرده که در سال‌های اخیر منابع نظارتی داخل و خارج از محل در مقام ناظر بازار مالی سوئیس افزایش یافته است ولی هنوز هم نیازمند تقویت است.[۶۱] منابع کافی برای نظارت و تنظیم کل سیستم بانکی به گونه‌ای که با اصول اصلی نظارت بانکی از جمله کار کافی و عمیق در محل و نظارت بر کار نظارتی انجام شده توسط حسابرسان مستقل به ویژه برای بانک‌های کوچک و متوسط در دسترس نمی‌باشد.

۳. ایالات متحده آمریکا:

گزارش اخیر صندوق بین‌المللی پول[۶۲] رابطه میان ناظرین و حسابرسان مستقل را مورد بررسی قرار داده و خاطر نشان کرده است که « ناظرین به صورت دوره‌ای با موسسات حسابرسی مستقل ملاقات می‌کنند تا مسائل مربوط به منافع مشترک در عملیات بانکی را مورد بحث قرار دهند.» صندوق بین‌المللی پول همچنین در این زمینه اشاره می‌کند که حسابرسان مستقل در گزارشگری مشکلات برای مقررات‌گذاران هیچ «فضای امن»ی ندارند. با این حال طبق بخش ۳۶۳ قانون صندوق بیمه سپرده فدرال (FDIC[ک])، در صورتی که بانکی از حسابرسان، اطلاعات نوشتاری مربوط به موردی از نقض دریافت کند باید تا ۱۵ روز به ناظر در این مورد اطلاع دهد. این شکاف زمانی به نحوی از طریق ارتباط مستمر میان ناظرین و حسابرسان

[۶۰] گزارش کشوری صندوق بین‌المللی پول ۱۴/۱۴۳، سوئیس: ارزیابی ثبات بخش مالی، می ۲۰۱۴.

[۶۱] گزارش کشوری صندوق بین‌المللی پول، ۱۴/۲۶۴، سوئیس: ارزیابی دقیق تطبیق - اصول اساسی بازل برای نظارت بانکی موثر.

[۶۲] گزارش کشوری صندوق بین‌المللی پول ۱۵/۱۷۰، ایالات متحده: برنامه ارزیابی بخش مالی، ژوئیه ۲۰۱۵.

در جریان برنامه‌ریزی و بررسی کاهش می‌یابد. به علاوه هرچند ناظرین نمی‌توانند دامنه حسابرسی مستقل را تعیین کنند، می‌توانند حسابرسان را تشویق کنند تا موضوعات جدیدی را مشمول حسابرسی کنند. با این حال این گزارش نقاط ضعف مربوط به نداشتن قدرت قانونی برای اضافه کردن مسئله‌ای خاص به دامنه حسابرسی مستقل توسط ناظرین را برجسته می‌کند. به این معنی که ناظرین نمی‌توانند به مسائلی که به طور معمول در حسابرسی در نظر گرفته نمی‌شوند بپردازند.

۴- هنگ‌کنگ:

مقام پولی هنگ‌کنگ (HKMA[ل]) تلاش‌های قابل‌توجهی را برای اطمینان از وجود کانال‌های ارتباطی مؤثر با حسابرسان مستقل انجام داده است. علاوه بر این توانایی این اداره برای صدور گزارش‌های حسابرسان مستقل با اهداف نظارتی، از رابطه میان مقام پولی هنگ‌کنگ و حسابرسان مستقل و درک نگرانی‌های نظارتی مقام پولی هنگ‌کنگ پشتیبانی می‌کند. با این حال گزارش اخیر صندوق بین‌المللی پول[۶۳] حاکی از آن است که دو حوزه وجود دارد که مقام پولی هنگ‌کنگ در آنها فاقد قدرت کافی است و چارچوب‌های قانونی می‌توانند بهبود یابند. اول اینکه مقام پولی هنگ‌کنگ وقتی در مورد صلاحیت یا استقلال یک حسابرس مستقل نگرانی وجود دارد، اختیاری برای رد انتصاب آن حسابرس ندارد و دوم اینکه مقام پولی هنگ‌کنگ قدرت مستقیم جهت دسترسی به اسناد کاری (پرونده‌های حسابرسی) حسابرس مستقل ندارد. حتی وقتی که مقام پولی هنگ‌کنگ قادر است پیامدهایی که به وسیله مسائل غیرمستقیم بوجود می‌آید را نشان دهد. با اینکه مقام پولی هنگ‌کنگ با وجود این محدودیت‌ها به کار خود ادامه داده است، قوانین مربوطه باید اصلاح شوند.

۵.۲. رابطه میان حسابرسان داخلی و ناظرین

دولت‌ها و سازمان‌های بین‌المللی درخواست دارند که نقش حسابرسی داخلی در بانک‌ها افزایش یابد.[۶۴] مأموران ادارات نظارتی ملی در پاسخ به بحران مالی جهانی و تاثیر کلی آن روی در معرض ریسک بودن، جلساتی را در مورد ابزارها و فرآیندهای کنترل داخلی برگزار کرده‌اند.[۶۵] فدرال رزرو[۶۶] و مقام بانکداری اروپا (EBA[م])[۶۷] و دیگر سازمان‌های نظارتی ملی در سراسر جهان هم به همین شکل نگرانی خود را از عدم انجام مدیریت ریسک و حسابرسی داخلی مؤثر اعلام کرده‌اند. در پاسخ به این گونه نگرانی‌ها تدوین‌کنندگان استانداردهای بین‌المللی کارهای انجام شده توسط فعالیت حسابرسی داخلی را تقویت کرده‌اند و به عنوان

---

[۶۳] گزارش کشوری صندوق بین‌المللی پول ۱۴/۱۳۱، جمهوری خلق چین - منطقه اداری ویژه هنگ‌کنگ، گزارش رعایت استانداردها و دستورالعمل‌ها، می ۲۰۱۴.

[۶۴] نقش حسابرسی داخلی از دیدگاه مقررات‌گذاری در همگرایی بین‌المللی اندازه‌گیری سرمایه و استانداردهای سرمایه ۲۰۰۴ در بازل II تأکید شد. در این زمینه، بند ۱۶۵ بررسیِ کل فرایند مدیریت ریسک را حداقل تا یک سال با تمرکز ویژه بر فرایندهای داخلی مربوط به گزارشگری الزامات سرمایه قانونی به حسابرسی داخلی واگذار کرد. نمونه‌هایی از این فرآیندهای داخلی اعتبارسنجی تغییرات در فرایندهای اندازه‌گیری ریسک، تایید منابع داده‌ها و صحت تخصیص فرض‌های نوسان است.

[۶۵] برنارد شریدان، مدیر حمایت از مصرف کننده، سخنرانی در کنفرانس IIA ایرلند، ۱۶ آوریل ۲۰۱۵؛ لوئیجی ماریانی، معاون رییس بخش نظارت، بانک ایتالیا، «سیستم‌های کنترل داخلی برای پولشویی»، سخنرانی در جلسه دهم در مورد انطباق، AICOM (Associazione Italiana Compliance)، ۲۵ ژوئن ۲۰۱۴.

[۶۶] فدرال رزرو، *بیانیه خط‌مشی تکمیلی در مورد فعالیت حسابرسی داخلی و برون سپاری آن*، ژانویه ۲۰۱۳.

[۶۷] EBA ، دستورالعمل‌های راهبری داخلی، سپتامبر ۲۰۱۱.

مثال با معرفی بازل ۳ درخواست کرده‌اند که بر روی فرآیندهایی خاص در مباحث محاسبات ریسک اعتباری، ریسک بازار و ریسک نقدینگی بازنگری‌های سالانه انجام شود.[۶۸]

با این وجود بحثی جدی در مورد نقش حسابرسی داخلی در فروپاشی مؤسسات مالی در حال انجام است. کارهای زیادی در شناسایی نقص‌های مربوط باقی مانده است. محققان تاکنون تجزیه و تحلیل‌های خود را تنها به فعالیت حسابرسی داخلی محدود کرده‌اند. در حالی که این مطالعات شواهد مفیدی راجع به شرایط ارتباط میان صنعت بانکداری با اثربخشی سیستم‌های کنترل داخلی ارائه می‌دهند، معمولاً بر رابطه میان حسابرسی داخلی و دیگر ارکان ساختار کنترل داخلی (یعنی خطوط اول و دوم (دفاعی)) تمرکز دارند.[۶۹]

به طور کلی تحقیقات در مورد اثر تعامل میان حسابرسان داخلی، ناظرین و حسابرسان مستقل در کارایی راهبری شرکتی اگر هم انجام شده باشد به نظر ناقص است. به طور خاص تاکنون شواهد نظری و عملی کمی در مورد میزان تناسب میان مدل سه خط دفاعی با راهبری شرکتی مؤسسات مالی وجود دارد. این شکاف چند راهکار مفید برای تحقیق در مورد این موضوع ارائه می‌دهد که در پاراگراف‌های زیر در مورد آن‌ها بحث می‌کنیم.

از آن جایی که مدل چهار خط دفاعی برای بهبود همکاری میان حسابرسان داخلی و طرف‌های برون‌سازمانی (یعنی حسابرسی مستقل و ناظرین) ساخته شده، برای تعامل میان آن‌ها تعیین تکلیف بیشتری باید انجام شود به خصوص در مورد رابطه میان وظیفه حسابرسی داخلی و ناظرین.

در یک مدل چهار خط دفاعی، تعامل میان حسابرسی داخلی و ناظرین معنی خاصی پیدا می‌کند. از سویی به مقامات نظارتی اجازه می‌دهد تا بهترین شیوه‌ها را ارتقا دهند و ریسک‌ها را قبل از این‌که به مشکلات جدی تبدیل شوند شناسایی و به آن‌ها بپردازند. از سویی دیگر این مسئله باعث می‌شود که سیستم کنترل داخلی دقیق‌تر بر اساس چهار لایه کنترلی ساختار پیدا کند.

اگر چه در چندین سیستم قضایی در سطح جهان، فعالیت حسابرسی داخلی بانک‌ها تا آنجا که برای تضمین صحت سازمان لازم است، مسئول است اطلاعات بااهمیت را فاش کند، این ارتباط یک طرفه و مهم‌تر از آن نتیجه اختیارات ناظر مالی بر وظیفه حسابرسی داخلی است.[۷۰] در واقع، این تعامل عمدتاً به ارزیابی نظارتی وظیفه حسابرسی داخلی مربوط است.

---

[۶۸] برای نمونه، عطف به سیاست مقررات در اروپا، ماده ۷۴ دستورالعمل ۳۶/۲۰۱۳ / اتحادیه اروپا (CRD IV) حاوی مفاد کلی در مورد راهبری داخلی و کنترل بر قدرت مقام بانکداری اروپا (EBA) برای صدور راهکارها در این زمینه است. دستورالعمل‌های EBA در مورد راهبری داخلی اطلاعات مربوط برای کشورهای عضو اتحادیه اروپا در زمینه پیاده‌سازی اصول نظارتی در این زمینه فراهم می‌کند. پاراگراف ۲۹ دستورالعمل‌های EBA ویژگی‌های معین فعالیت حسابرسی داخلی اثربخش و مناسب را در موسسه مالی تعیین می‌کند. با این وجود، در غیاب قاعده دقیق هماهنگ‌سازی اتحادیه اروپا در مورد این موضوع، کشورهای عضو اتحادیه اروپا مسئول تعیین و پیاده‌سازی استانداردهای دقیق در رابطه با نظارت بر فعالیت حسابرسی داخلی هستند.

[۶۹] در مورد اهمیتِ داشتنِ معیارهای کنترل دقیق و معین برای اجرای روش‌های راهبری خوب، در بین متون گسترده، SOH و مارتینوف-بنی، «فعالیت حسابرسی داخلی: ادراکات نقش‌های حسابرسی داخلی، اثربخشی و ارزیابی، *مجله حسابرسی مدیریت*، ۲۰۱۱، جلد ۲۶، نسخه ۷،صفحات ۶۰۵-۶۲۲؛» لنز و هاهن، «ترکیب تجربی منابع اثربخشی حسابرسی داخلی در اشاره به فرصت‌های جدید تحقیقاتی»، *مجله حسابرسی مدیریت*، ۲۰۱۵، جلد ۳۰، صفحات ۳۳-۵؛ چورس، دیلروی و مونرو، «فرایند حسابرسی داخلی و راهبری خوب: به سوی مدل تحقیق»، *آکادمی تحقیقات کسب و کار*، ۲۰۱۳، جلد ۱، صفحات ۵۸-۴۸، را ببینید.

[۷۰] در این میان، Deutsche Bundesbank، KWG - Gesetz über das Kreditwesen، ژانویه ۲۰۱۵؛ بانک ایتالیا، Disposizioni di vigilanza prudenziale per le banche، شماره بخشنامه ۲۸۵، ۱۷ دسامبر ۲۰۱۳، (۳)IV؛ Wet Financieel Toezicht، بخش ۳:۱۷ (۲)، هلند؛ و مقام

اصل ۲۶ کمیته نظارت بانکی بازل *اصول اساسی برای نظارت بانکی موثر*[۷۱] تعیین می‌کند که ناظر باید اطمینان دهد که بانک‌ها چارچوب‌های کنترل داخلی کافی برای ایجاد و نگهداری فعالیت مناسب محیط عملیاتی را دارند و اینکه پروفایل ریسک ویژه آن‌ها را در نظر می‌گیرد. این سنجش برای تضمین فعالیت حسابرسی داخلی مستقل به عنوان جزئی اساسی از چارچوب کلی و کافی کنترل داخلی است. برای این منظور، این سند معیار مورد استفاده توسط ناظر برای ارزیابی اینکه آیا مؤسسه فعالیت حسابرسی مستقل، دائمی و اثربخش دارد را تعریف می‌کند.

با این حال تمرکز دقیق‌تر روی کانال ارتباطی مستقیم میان حسابرسی داخلی و ناظرین یکی از نکات اصلی سند کمیته نظارت بانکی بازل است. اصل ۱۶ *فعالیت حسابرسی داخلی در بانک‌ها* بیان می‌کند که «ناظرین باید ارتباط منظمی با حسابرسان داخلی بانک داشته باشند تا ۱) در مورد حوزه‌های ریسک مشخص شده توسط دو طرف بحث شود، ۲) اقدامات کاهنده ریسک که توسط بانک اتخاذ می‌شود را درک کنند، و ۳) نقاط ضعف مشخص شده و پاسخ بانک به این نقاط ضعف را پایش کنند.»[۷۲]

قراردادن یک لایه چهارم در طراحی چارچوب کنترل داخلی، به ویژه در مورد روش چرخش اطلاعات میان حسابرسی داخلی و ناظرین دلالت‌های عملی خواهد داشت. با توجه به این مدل، ناظرین به اندازه‌ای اطلاعات دریافت می‌کنند که گویی بخشی از ساختار داخلی سازمان بوده‌اند و به اندازه دیگر واحدهای کسب‌وکار داخلی در اثربخشی فرآیند کنترل مدیریت ریسک مؤسسه مالی درگیر هستند. همچنین مقامات نظارتی تاجایی که باعث افزایش اثربخشی کار حسابرسی داخلی شود، اطلاعات مربوطه را با فعالیت حسابرسی داخلی به اشتراک خواهند گذاشت و به این طریق کانال اطلاعاتی دو طرفه شده و منافع حسابرسی داخلی و ناظرین به طور یکسان تامین می‌شود.[۷۳]

این امر می‌تواند تاثیر قابل‌توجهی بر تعامل میان وظیفه حسابرسی داخلی و ناظرین داشته باشد و همچنین می‌تواند حسابرسان داخلی را ترغیب به ارائه اطلاعات حتی به صورت داوطلبانه کند. در این دیدگاه نظریه-های روانشناسی اجتماعی، افشای اطلاعات را ارزشمند می‌دانند به این دلیل که می‌توان از آن ایده‌هایی موفق برای طراحی مکانیسم/ساختار ارتباطات میان حسابرسی داخلی و ناظرین به دست آورد. محققان اثبات کرده‌اند که مردم بیشتر رغبت دارند اطلاعات را به افرادی بدهند که به آن‌ها اعتماد دارند و با هم داد و ستد اطلاعات دارند.[۷۴] با این حال این نتیجه مؤید این مسئله نیست که رابطه سنتی و سلسله‌مراتبی میان ناظر و اشخاص تحت نظارت باید جایگزین شود بلکه می‌گوید که این رابطه باید یکپارچه شود. آن گونه که شواهد

پولی هنگ کنگ، *راهنمای سیاست نظارتی - حسابرسی داخلی*، ژوئیه ۲۰۰۹ را ببینید. برای تحلیل مقایسه‌ای، کنفدراسیون اروپایی انجمن حسابرسی داخلی، *حسابرسی داخلی بانکی در اروپا*، برلین، ۲۰۰۹، را ببینید.

[۷۱] کمیته نظارت بانکی بازل ، اصول اساسی برای نظارت بانکی موثر ، سپتامبر ۲۰۱۲.

[۷۲] کمیته نظارت بانکی بازل ، فعالیت حسابرسی داخلی در بانک‌ها ، ژوئن ۲۰۱۲.

[۷۳] در این رابطه، کمیته نظارت بانکی بازل را ببینید، فعالیت حسابرسی داخلی در بانک‌ها، §۷۵، ژوئن ۲۰۱۲.

[۷۴] سانستین، "اقتصاد رفتاری و پدر سالاری"، مجله قانون ییل، ۲۰۱۲؛ اورنستین و دانی،" تحقیقی بین فرهنگی، از خود افشاگری"، مجله علمی روانشناسی آمریکای شمالی، ۲۰۰۳، ۵ (۳)، صفحات ۳۸۶-۳۷۳؛ آنتاکی، بارنس و لئودار، "خود افشاگری به عنوان یک تمرین تعاملی "، مجله انگلیسی روانشناسی اجتماعی، ۲۰۰۵، ۴۴ (۲)، ۱۸۱-۹۹.

تجربی نشان می‌دهند، افشای اطلاعات همواره به نفع بانکداران نیست، حداقل اگر انگیزه‌ای یا پاداشی برای آن وجود نداشته باشد.[۷۵]

بر اساس ادبیات موضوع و آگاهی از یافته‌های متناقض میان کارهای انجام شده در مورد اقتصاد رفتاری و خودافشایی اطلاعات، ممکن به نظر می‌رسد که با استفاده از مفهوم‌سازی، الگوهای ارتباطات دوجانبه میان حسابرسی داخلی و ناظرین هماهنگ شوند و بهبود یابند. با استفاده از مدل چهار خط دفاعی فرض می‌کنیم که رسیدن به هر دو باید ممکن باشد:

رابطه عمودی: ماهیت این رابطه نتیجه حکمی است که به ناظر بانک سپرده شده است. این امر زمانی اتفاق می‌افتد که ناظر کیفیت فعالیت حسابرسی داخلی را ارزیابی می‌کند. این اساساً یک رابطه سلسله‌مراتبی است که در آن حسابرسی داخلی تابع و تحت بررسی ناظر است.

و

رابطه افقی: این رابطه زمانی بوجود می‌آید که ناظر به عنوان بخشی از سیستم کنترل داخلی شناخته می‌شود و در یک رابطه افقی که در آن با طرف دیگر در یک سطح است درگیر کار می‌شود. ناظر باید با به اشتراک گذاشتن اطلاعات مربوط به ریسک و اقدامات کاهنده ریسک به طور متقابل به طرف دیگر اطلاعات دهد که این خود نشان‌دهنده همکاری با حسابرسی داخلی در سطح یکسان است. ناظر باید این رابطه را مدیریت کند و به بی‌میلی حسابرسی داخلی برای افشای اطلاعات محرمانه فائق شود.

در این زمینه، یکی از مسائل اصلی که به وجود می‌آید، رفتار اطلاعات است. از آنجا که این مدل برای کاهش اطلاعات نامتقارن میان طرفین درگیر در نظر گرفته شده است باید آن را با این فرض اجرا کرد که کار با اطلاعات (رفتار اطلاعات) برای موثرتر کردن سیستم کنترل ریسک است. در زمان تصمیم‌گیری برای افشاء یا عدم افشای اطلاعات نظارتی عمومی و خصوصی و نحوه افشاء، ناظرین با چالش‌هایی در مورد جمع‌آوری اطلاعات از مؤسسات مالی و افشای این اطلاعات درگیر هستند. به هر حال، مسئولیت حسابرس داخلی در مورد افشای اطلاعات محرمانه به اشخاص ثالث باید مورد توجه قرار گیرد. اگر حسابرسان داخلی با حسن‌نیت اطلاعات محرمانه را افشا کنند باید در برابر دادرسی از آن‌ها محافظت شود (به اصطلاح ساحل امن) چون‌که چنین حفاظت قانونی برای حسابرسان مستقل وجود دارد.[۷۶] اگر چنین محافظتی وجود نداشته باشد فرض تقویت تعامل از طریق مدل چهار خط دفاعی نقض می‌شود چون حسابرسی داخلی از همکاری می‌ترسد. چنین وضعیتی باعث عدم بهبود میزان و کیفیت اطلاعاتی خواهد شد که در اختیار ناظرین قرار می‌گیرد.

علاوه بر این اعطای نقش به ناظر در سیستم کنترل داخلی ممکن است استقلال و بی‌طرف بودن او را به خطر بیاندازد. به عبارت دیگر ایجاد کانال‌های ارتباطی عمیق‌تر و گسترده‌تر شاید تاحدی باعث ورود و

---

[۷۵] استبرگ، "افشاگری، سرمایه گذاری و مقررات"، مجله واسطه‌گری‌های مالی، ۲۰۰۶، جلد ۱۵، صفحات ۳۰۶-۲۸۵؛ هرتزبرگ، لیبرتی و پاراویسینی، "اطلاعات و انگیزه‌های در داخل شرکت"، مجله تامین‌مالی، ۲۰۰۹؛ اورلوف "طراحی بهینه از افشاگری داخلی"، مقاله کاری مدرسه کسب و کار سیمون، ۲۰۱۵، شماره ۶.

[۷۶] استاندارد بین‌المللی حسابرسی ۶۱۰ را ببینید.

تاثیرگذاری ناظر در راهبرد یا مدل کسب‌وکار مؤسسه شود که به نوبه خود ممکن است ایجاد کننده دخالت-های بیجا در تصمیمات مؤسسه به عنوان نهادی خصوصی شود.

به طور کلی‌تر طبق شواهد حکایت‌شده، اعمال الزامات افشای اطلاعات بیشتر (بدون تعیین مناسب قواعد و مرزبندی‌ها) ممکن است اثرات منفی داشته باشد و موجب شود که طرف‌های درگیر در لایه چهارم رفتار خود را تغییر دهند. این موضوع باعث تشدید مشکل خطر اخلاقی به ضرر اثربخشی سیستم کنترل داخلی خواهد شد.[۷۷] در واقع افزایش میزان اطلاعات، به خودی خود مناسب نیست و حتی شاید باعث کاهش تاثیر و کارایی سیستم کنترل شود[۷۸] که می‌تواند یکی از اثرات منفی محتمل افشای اطلاعات نظارتی باشد.

در این راستا مدل چهار خط دفاعی نیازمند تنظیم جدیدی از فرآیندها و قواعد به خصوص در مورد میزان مورد نیاز و مجاز به اشتراک‌گذاری اطلاعات توسط حسابرسان داخلی، حسابرسان مستقل و ناظرین است.

این قواعد باید طبقه‌بندی اطلاعاتی را که ممکن است به اشتراک گذاشته شوند را مشخص کند و تعیین کند که این اطلاعات به چه کسانی باید داده شود. همچنین آن‌ها باید روشی برای به‌دست آوردن و حفاظت از اسناد و مدارک محرمانه و برای گذاشتن آن‌ها در اختیار تعداد محدودی دریافت‌کننده ایجاد کنند. ما نیاز به فرآیندهای رسمی‌سازی از جمله سازمان جلسات و اسناد مربوط به آن‌ها برای پایش موضوعات مورد بحث (نتایج واقعی و مورد انتظار) را تصدیق می‌کنیم. ما همچنین اهمیت زیادی برای تضمین سطح مشخصی از انعطاف‌پذیری برای تشکیل جلسات ویژه در صورت نیاز توسط هر دو طرف قائل هستیم.

بنابراین ما نیاز به ایجاد استانداردها در مورد چگونگی تقویت روابط با متعادل کردن تعهد ناظر برای ارزیابی فعالیت داخلی با نقش مشارکتی‌اش در حفظ یک رابطه باز و سازنده کاری با هدف به اشتراک گذاری اطلاعات، شناسایی می‌کنیم.

از دیدگاه سازمانی پیشنهاد می‌کنیم که «نقش ارزیاب» (رابطه عمودی) از «نقش همکار» (رابطه افقی) جدا شود، به عنوان مثال با الزام مقامات نظارتی برای تخصیص افراد/تیم‌های متفاوت برای هر نقش ارزیابی و همکاری.

از آنجایی که نقش و مسئولیت‌های حسابرسان داخلی با ناظرین بانکی از نظر قضائی متفاوت است، سیاست-گذاران و مقررات‌گذاران باید این فاصله قضائی را مرتفع کنند و لیستی یکپارچه و مرتبط از شیوه‌های استوار برای پیاده‌سازی رویکردی کلی‌گراتر از چارچوب کنترل ریسک تهیه کنند تا بتوانند نقشی خاص به حسابرسان مستقل دهند. بنابراین از دیدگاه قانون‌گذاری بسیار مهم است که به ریسک‌های بالقوه مربوط به فقدان قوانینی دقیق و هماهنگ در حوزه رابطه میان ناظرین و حسابرسان داخلی پرداخته شود. این شکاف ممکن است باعث بوجود آمدن سطح مشخصی از انعطاف‌پذیری در ایجاد و حفظ این رابطه شود که خود در نهایت منجر به نابرابری در میزان مسئولیت مؤسسات مالی و ناظرین در به اشتراک گذاشتن اطلاعات شود.

---

[۷۷] در صورت عدم وجود موافقتنامه افشا در مورد رفتار اطلاعات، حسابرسی داخلی یک بانک ممکن است اطلاعات محرمانه در مورد وضعیت بانک دیگری به دست آورد.

[۷۸] همین مشکل برای مثال در زمانی روی می‌دهد که دولت می‌بایست به صورت بهینه‌ای اطلاعات مربوط به دارایی‌های بانک‌ها را در خلال یک بحران مالی افشا کند: رجوع شود به فاریا ای کاسترو، مارتینز و فیلیپون ، رانز در مقابل لیمونز: افشای اطلاعات، ظرفیت اقتصادی و ثبات مالی، دفتر ملی تحقیقات اقتصادی، ۲۰۱۵.

۵.۳. رابطه بین حسابرسان داخلی و مستقل

همان‌طور که پیش‌تر گفته شد، یک ویژگی مشترک مسئولیت‌های هر دو طرف، فراهم‌آوردن امکان ارزیابی مستقل است. در حالی‌که حسابرس مستقل بر روی صورت‌های مالی تمرکز کرده و موظف است اعتبار صورت‌های مالی را از نظر عدم وجود هر گونه تحریف بااهمیت بررسی نماید، حوزه فعالیت‌های حسابرس داخلی بسیار وسیع‌تر بوده و شامل مواردی از قبیل ارزیابی کارآیی و اثربخشی عملیات شرکت، قابلیت اعتماد و یکپارچگی فرآیندهای گزارشگری و انطباق با قوانین و مقررات می‌شود.

در کل، چنان‌چه از کار حسابرسان داخلی به منظور حسابرسی مستقل استفاده شود، جای انتقاد دارد. گزارش اخیر بازرسی هیئت ناظر بر حسابداری شرکت‌های سهامی عام (PCAOB[۷۹]) به‌صورت انتقادی ذکر می‌کند که در بسیاری از نمونه‌ها، حسابرس مستقل مبنای کافی برای اتکا به کار واگذار شده به دیگران ندارد.[۷۹] به‌علاوه، مطالعه‌ای که اخیرا در مورد بخش‌های حسابرسی داخلی در آمریکای شمالی منتشر شد نشان می‌دهد که بیش از ۵۰٪ پاسخ‌دهندگان پیش‌بینی کردند تعداد ساعات کاری واحدهای حسابرسی داخلی به جهت ارائه کمک مستقیم به حسابرسان مستقل، افزایش پیدا کند.[۸۰]

با این وجود، از طریق هم‌سوساختن بهتر برنامه‌ها و الگوهای حسابرسی و استفاده از جلسات هماهنگی میان حسابرسان داخلی و مستقل جهت پرهیز از دوباره‌کاری، می‌توان مزایای کار برای هر دو طرف را به حداکثر رساند. به‌علاوه، هر دو طرف باید در همان ابتدای فرآیند حسابرسی در مورد هر آن‌چه حسابرس مستقل برای استفاده از کار آزمون کنترل‌های حسابرسی داخلی نیاز دارند، با هم هماهنگ کنند.[۸۱]

حسابرسان مستقل ممکن است در شرایطی خاص به کار حسابرسان داخلی اتکا کنند: نخست، حسابرسان مستقل لازم است مشخص کنند که آیا در حوزه قضایی که آنها قرار دارند، مراجع ذیصلاح به آن‌ها اجازه می‌دهند از کمک مستقیم حسابرسان داخلی بهره جویند. در برخی از حوزه‌های قضایی به‌صورت خاص اتکاء حسابرسان مستقل برای کاری که توسط حسابرسان داخلی انجام می‌شود را ممنوع می‌کنند. در جاهایی که این‌گونه نظام‌های «برون‌سپاری» مجاز است، حسابرسان مستقل ابتدا باید اثربخشی، استقلال و بی‌طرفی واحد حسابرسی داخلی را در نظر گرفته و نیز میزان کیفیت کار و مهارتشان را ارزیابی نمایند و سپس واگذاری اجرای برخی وظایف معین حسابرسی به آن‌ها را مد نظر قرار دهند. حسابرسان مستقل تشویق می‌شوند که حداقل کار ممکن را به واحد حسابرسی داخلی محول کرده و بیشتر خودشان به‌طور مستقیم کارها را انجام دهند تا اطمینان حاصل شود به‌اندازه کافی در فرآیند حسابرسی درگیر بوده‌اند.[۸۲]

پیش از استفاده از کار حسابرسان داخلی، چندین مورد باید انجام پذیرد: باید حسابرسان مستقل تاییدیه کتبی از «نماینده مجاز» موسسه مالی تحت بررسی دریافت کنند تا اطمینان حاصل شود که حسابرسان

---

[۷۹] PCAOB یک شرکت غیرانتفاعی تاسیس شده توسط کنگره برای نظارت بر حسابرسی شرکت های دولتی به منظور حفاظت از منافع سرمایه‌گذاران و پیشبرد منافع عمومی در تهیه گزارش‌های حسابرسی آگاهی‌بخش، دقیق و مستقل است.

[۸۰] انجمن حسابرسان داخلی، نقش‌های متقابل - پرورش روابط کاری موثر در میان حسابرسی مستقل، حسابرسی داخلی، و کمیته حسابرسی، مارس ۲۰۱۵.

[۸۱] همان ماخذ.

[۸۲] ISA ۶۱۰ (تجدید نظر شده ۲۰۱۳)، با استفاده از کار حسابرسان داخلی و اصلاحات منطبق بر آن . مارس.

داخلی می‌توانند بدون محدودیت وظایفشان در قبال حسابرسان مستقل را انجام دهند. به‌علاوه، حسابرسان داخلی باید به‌طور کتبی متعهد شوند که تمام موارد خاص را مطابق با دستورالعمل اعلام‌شده از سوی حسابرسان مستقل، محرمانه نگاه خواهند داشت. آن‌ها باید هر گونه موردی که ممکن است بی‌طرفی آن‌ها را به خطر اندازد را به حسابرسان مستقل اطلاع دهند.[۸۳]

در زمان اجرای عملیات رسیدگی، لازم است حسابرسان مستقل از نزدیک کار حسابرسان داخلی را نظارت و بررسی نمایند.[۸۴] حسابرسان مستقل باید تمام شواهد و یافته‌هایی که توسط حسابرسان داخلی به‌دست آمده است را مورد تردید قرار دهند. آن‌ها باید متقاعد شوند که حسابرسان داخلی شواهد و یافته‌های کافی در حمایت از نتیجه‌گیری‌هایشان دارند. در سرتاسر اجرای عملیات رسیدگی، حسابرسان مستقل باید حواسشان باشد که ممکن است ارزیابی‌های حسابرسان داخلی ناکافی باشد.

به طور موازی، حسابرس داخلی ممکن است به تبادل دیدگاه‌ها با حسابرس مستقل بپردازد.

اگرچه حسابرسی داخلی نیازمند آن است که بینش‌های دقیق‌تری از سازمان به‌دست آورد، ولی در عین‌حال می‌تواند از ارزیابی حسابرس مستقل در مورد موسسه تحت بررسی، بهره جسته و از تجربه حسابرس مستقل در کار با سایر سازمان‌های فعال در آن صنعت، استفاده کند. چندان رایج نیست که حسابرسی داخلی کار خود را به حسابرسان مستقل بسپارد. در مقابل، جهت اطمینان یافتن از حفظ استقلال خدمت‌دهنده‌ای که کار به او سپرده شده است، توصیه می‌شود حسابرسی داخلی انجام کارهای خودش را به سایر موسسات، غیر از موسسه‌ای که مسئولیت حسابرسی مستقل را برعهده دارد، واگذار کند.[۸۵]

توصیه عملی ۲۴۴۰-۱ از IIA تصریح می‌کند که منشور حسابرسی داخلی یا سیاست سازمانی ممکن است تعیین کند که نتایج حسابرسی باید به اطلاع «سایر طرف‌های علاقه‌مند یا تحت‌تاثیر» همانند حسابرسان مستقل رسانده شود.[۸۶] چنان‌چه حسابرس داخلی اطلاعات بسیار حساسی پیدا کرده و تصمیم بگیرد حسابرس مستقل را خارج از سلسله مراتب عادی در جریان بگذارد، این عمل تحت عنوان افشاگری بیرونی به حساب خواهد آمد. در چنین موردی، حسابرس داخلی باید ارزیابی کند که آیا مرجع ناظر محلی از وی در برابر دعاوی حقوقی محافظت خواهد کرد.[۸۷] به‌طور کلی، تبادل ارتباطات کتبی و گزارش‌های حسابرسی استاندارد بسیار توصیه می‌شود. متداول است که حسابرس داخلی تمام گزارش‌های حسابرسی را برای حسابرس مستقل ارسال کرده و به‌طور مشابه، حسابرس مستقل نیز نسخه‌ای از گزارش خود را در اختیار حسابرس داخلی قرار داده و در جلسه‌ای با حضور دو طرف، موارد مهم آن را برای وی توضیح دهد.

یکی از نقاط محل اختلاف در رابطه میان حسابرسان داخلی و مستقل، پرسش در مورد مسئولیت طرفین در زمینه پیگیری پیشنهادات حسابرسی مستقل است. در کل، فرآیندهای پیگیری برای اطمینان از این‌که برنامه‌های اقدام مدیریت به‌موقع و به نحو مناسب اجرا شده‌اند، ضروری هستند. استاندارد ۲۴۰۲ انجمن

---

[۸۳] همان ماخذ.

[۸۴] ISA ۲۰۰ ، اهداف کلی حسابرسی مستقل و انجام حسابرسی طبق استانداردهای بین المللی حسابرسی، بند ۱۱.

[۸۵] انجمن حسابرسان داخلی، عملکرد مشاوره‌ای ۲۰۵۰-۳، با تکیه بر کار سایر اطمینان دهندگان، اکتبر ۲۰۱۰.

[۸۶] انجمن حسابرسان داخلی، عملکرد مشاوره‌ای ۲۴۴۰-۱، انتشار نتایج، ژانویه ۲۰۰۹.

[۸۷] انجمن حسابرسان داخلی، عملکرد مشاوره‌ای ۲۴۴۰-۲، مکاتبه اطلاعات حساس در داخل و خارج از زنجیره دستور، می ۲۰۱۰.

کنترل و حسابرسی سیستم‌های اطلاعاتی (ISACA[۸۷]) مقرر می‌کند که حسابرسان مستقل می‌توانند انجام پیگیری را به واحد حسابرسی داخلی واگذار کنند. در این حالت، منشور حسابرسی یا موافقت‌نامه‌های حسابرسی باید صراحتا چنین مسئولیت‌هایی را قید نمایند.

۵.۴. گذار از سه خط دفاعی به چهار خط دفاعی: جستجویی با هدف طراحی یک مدل کارآمد برای موسسات مالی

این مقاله، اتکا متداول به مدل سه‌خط دفاعی را زیر سوال برده و ثابت می‌کند که این مدل در ساختارهای شرکتی «پیچیده»، نظیر آن‌چه در موسسات مالی دیده می‌شود، چندان کارآمد نیست. پاشنه آشیل مدل سه خط دفاعی، فقدان یک دید جامع نسبت به ساختار سازمانی است. این نتایج سبب می‌شود که اطلاعات مربوط به نحو کمتر بهینه‌ای توزیع شده و معیارهای کنترلی ناکارآمد در سطوح مختلف سازمان به کار گرفته شود. به‌علاوه، کاستی‌های این مدل در درک سیاست‌های ریسک‌پذیری سازمان، و اثرات درونی و بیرونی آن بر موسسه مالی منفرد، و نیز شیوه تفسیر داده‌های مربوط در این مدل، در کنار کوتاهی‌های فرهنگی و رفتاری، به‌عنوان رایج‌ترین دلایل رسوایی‌های شرکتی اخیر در صنعت مالی، استدلال می شود. این‌ها درس‌هایی است که تردیدهای بسیاری را در مورد کارآیی مدل سه‌خط دفاعی مطرح کرده و ما را به‌سوی یافتن مدل‌های جایگزین سوق می‌دهد.

این امکان وجود دارد که بر روی ساختار سه خط دفاعی کار کرده و تلاش کرد مدلی «نزدیک‌تر به واقعیت» پیشنهاد داد که در آن برخی مشوق‌ها با هدف ارتقای درجه استقلال و حرفه‌ای‌گری گنجانده شده باشد. با این وجود، هرچند اتخاذ چنین رویکردی می‌تواند کمک کند تا برخی از کاستی‌های کنونی برطرف شود، ولی هم‌چنان مشکل نقص اطلاعات پابرجا خواهد ماند: فقدان اطلاعات بااهمیتی که برای اطمینان از این که سیستم‌های ریسک و کنترل داخلی که قادرند ریسک‌هایی که موسسات مالی در معرض آن قرار دارند را ارزیابی، اندازه‌گیری، مدیریت و برطرف نمایند، ضروری است. چنان‌چه مدل سه خط دفاعی، آن‌طور که نظریه‌پردازان پیش‌بینی می‌کردند، نوش‌داروی عملکرد ضعیف شرکت و مدیریت ریسک گمراه‌کننده بود، تا این حد هر روز از ناظرین درخواست نمی‌شد تا فعالانه درگیر برقراری گفتگویی دوطرفه شده و نقشی انسجام‌بخش ایفا کنند.[۸۸]

انتقال به روش چهار خط دفاعی، با تعامل نزدیک‌تر میان حسابرسان داخلی، حسابرسان مستقل و ناظرین همراه خواهد بود. اگرچه، معمولا انتظار می‌رود حسابرسان داخلی، حسابرسان مستقل و ناظرین تعاملات نزدیکی با هم داشته باشند، ولی پژوهش‌های تجربی نشان داده است که واقعیت با آن‌چه نظریه‌ها پیش‌بینی می‌کنند، متفاوت است.[۸۹]

---

[۸۸] بانک انگلستان، مشارکت بین حسابرسان مستقل و ناظرین و شروع قدرت انتظامی PRA در مورد حسابرسان و اکچوئران مستقل، مقاله مشاوره | CP۸ / ۱۵؛ EBA، مشاوره در مورد دستورالعمل‌های پیشنهادی ارتباط بین مقامات صالح نظارت بر موسسات اعتباری و حسابرسی‌های قانونی، اکتبر ۲۰۱۵.

[۸۹] به فریاکو و لینکولن، ناظرین مالی و حسابرسان مستقل: همکاری برای ثبات مالی، سپتامبر ۲۰۱۵، نگاه کنید. مرکز اصلاح گزارشگری مالی (CFRR)، بانک ملی اتریش، ۲۸ سپتامبر ۲۰۱۵، وین - همچنین برای داشتن تصویری دقیق از مقررات ملی در گرو.

در بسیاری از کشورها، ناظرین بر کار انجام‌شده توسط حسابرسان مستقل، مثلا با استفاده از آن‌ها برای بازرسی‌های در محل، متکی هستند.[۹۰] در بیشتر حوزه‌های قضایی، حسابرسان موظفند در مورد موضوعاتی خاص به ناظرین بانکداری گزارش داده یا هشدار بدهند. در اتحادیه اروپا، بند ۱۲(۲) مقررات شماره ۵۳۷/۲۰۱۴ اروپایی در مورد الزامات خاص حسابرسی قانونی واحدهای تجاری سهامی عام،[۹۱] الزاماتی را شامل می‌شود که تصریح می‌کند " باید بین مراجع ذی‌صلاح قابل‌اطمینان که بر موسسات اعتباری نظارت می‌کنند از یک سو، و حسابرس(های) قانونی و موسسات حسابرسی که کار حسابرسی قانونی آن موسسات را انجام می‌دهند از سوی دیگر، گفتگوی دوطرفه کارآمد برقرار شود." هر چند، عدم وجود یک گفتگوی دوطرفه و رابطه بین حسابرسان و ناظرین محتاط در دوران پیش از بحران، به‌عنوان یک ضعف عمده شناسایی شد.[۹۲] موارد متعددی در طول یک دهه گذشته نشان داده است که حتی وقتی گفتگوی دوطرفه برقرار شده بود نیز ناظرین و حسابرسان مستقل انگیزه کافی برای مشارکت در انجام وظایف یکدیگر نداشتند. کاوشی که اخیرا توسط بانک انگلستان انجام گرفته است نشان می‌دهد که اگرچه ۷۰٪ از ناظرین به اطلاعات حسابرسی، به صورت مستقیم یا از طریق نظارت بر بانک، دسترسی داشتند، تنها ۵۰٪ از آن‌ها این اطلاعات را به‌عنوان بخشی از بازرسی‌های منظم خود از بانک‌ها، بررسی کردند.[۹۳] به‌علاوه، تنها تعداد اندکی از ناظرین به ضمیمه صورت‌های مالی، درخواست ارائه گزارش حسابرسی تفصیلی (LFAR[۹]) نمودند. همان‌طور که گفته شد، شواهد تجربی این پرسش را پیش رو می‌گذارد که آیا کار انجام‌شده توسط حسابرسان مستقل قابل اتکاست یا خیر. در حقیقت، نقایص مکرری در حسابرسی مستقل موسسات مالی با اهمیت سیستماتیک در ارتباط با اقلام برآوردی (قضاوتی) اقلام ترازنامه یا فرآیندها، شناسایی شده است.

مشکلات متناوبی که در ارتباط با ناظرین و حسابرسان مستقل وجود دارد سبب می‌شود این حوزه از منظر عملی به‌شدت مورد توجه قرار گیرد. در همین راستا، اقدامات متعددی آغاز شده است که تعامل میان ناظرین و حسابرسان مستقل را بهبود می‌بخشد.

---

[۹۰] پچیولی، "نظارت احتیاطی در بانکداری"، مقاله کاری OECD، ۱۹۸۷.

[۹۱] جدیدترین تعریف نهادهای با منافع عمومی (PIE)ها در اتحادیه اروپا در ماده ۲(۱۳) دستورالعمل (۱) ۵۶/۲۰۱۴ / اتحادیه اروپا به شرح زیر آمده است : "نهادهای عام‌المنفعه" عبارتند از:

(ا) اشخاص تحت راهبری قانون یک کشور عضو که اوراق بهادار قابل انتقال برای تجارت در یک بازار تنظیم شده از هر کشور عضو در بند ۱۴ ماده (۴) دستورالعمل ۳۹/۲۰۰۴ / EC پذیرفته شده است را داراست.

(ب) مؤسسات اعتباری با عنوان تعریف شده در بند ۱ ماده ۴۳ (۱) دستورالعمل ۳۶/۲۰۱۳ / اتحادیه اروپا و پارلمان اروپا و شورا، به غیر از موارد مندرج در ماده ۲ این دستورالعمل؛

(ج) شرکت‌های بیمه در ماده ۲(۱) دستورالعمل ۶۷۴/۹۱ / EEC؛ یا

(د) شرکت‌های تعیین شده توسط کشورهای عضو به عنوان نهادهای عام‌المنفعه، به عنوان مثال شرکت‌هایی که به لحاظ ماهیت کسب و کار خود، اندازه آنها و یا تعداد کارکنان آنها اهمیت قابل توجهی دارند. "

[۹۲] بانک انگلستان، مشارکت بین حسابرسان مستقل و ناظرین و شروع قدرت‌های انتظامی PRA در مورد حسابرسان و اکچوئران مستقل، مقاله مشاوره‌ای | ۱۵ / CP۸؛ گزارش کمیسیون پارلمانی استانداردهای بانکی، تغییر بانکداری به سمتی شایسته، جلد دوم (www.parliament.uk/documents/banking-commission/Banking-final-report-vol-ii.pdf)، جایی که پاراگراف ۱.۰۵۳ می‌گوید: کمیسیون توصیه می‌کند که دیوان بانک انگلستان یک گزارش دوره‌ای راجع به کیفیت محاورات بین حسابرسان و ناظرین را ارائه کند."

[۹۳] فریاکو و لینکولن ، ناظرین مالی و حسابرسان مستقل: همکاری برای ثبات مالی، مرکز اصلاح گزارشگری مالی (CFRR)، بانک ملی اتریش، ۲۸ سپتامبر ۲۰۱۵، وین.

به‌طور خاص، کمیته نظارت بانکی بازل تعامل میان ناظرین و حسابرسان مستقل را مورد بررسی قرار داد. در نتیجه این بررسی، هم‌بستگی مثبتی بین رابطه بیشتر بین ناظرین و حسابرسان مستقل از یک سو و کیفیت بهتر حسابرسی در مورد صورت‌های مالی بانک‌ها و نظارت کارآمدتر بانکی از سوی دیگر، مشاهده شد.[۹۴] نتیجه‌گیری‌ها و پیشنهادات مشابهی توسط سایر تدوین‌کنندگان استانداردها، مقررات گذاران و نهادهای نظارتی، هم‌چون مقام بانکداری اروپا (EBA)[۹۵]، بانک انگلستان و بانک جهانی ارائه شده است.[۹۶]

درحقیقت، حسابرس مستقل می‌تواند متحدی ارزشمند برای مراجع نظارتی، به‌خصوص در حوزه‌هایی که مهارت‌ها و منابع کمیاب است، محسوب شود.[۹۷] بحران مالی جهانی اخیر بر اهمیت همکاری نزدیک‌تر میان حسابرسان مستقل و ناظرین بانکی – که صاحب مهارت‌ها و دانش متمایزی هستند – در بهبود نظارت بر فعالیت‌های بانکی و غلبه بر نقاط ضعف در فرآیندهای مدیریت ریسک، ارزشیابی، کنترل و راهبری بانک‌ها و نیز در حسابرسی قانونی و نظارت مالی تاکید کرد.[۹۸]

مقام مقررات‌گذار احتیاطی بحث جدی را پیش کشید که از مزایای جانبی ارزشمند وجود گفتگوی دوطرفه میان حسابرسان و ناظرین و مخصوصا بحث‌هایی که حول مشکلات حسابداری و حسابرسی پیش می‌آید، پشتیبانی می‌کرد. چنین بحث‌هایی کمک می‌کند کیفیت حسابرسی‌های مستقل، به‌خصوص در شرایطی که از قبل به حسابرسان در مورد حوزه‌های کلیدی مورد توجه مقررات گذار اطلاع داده شده باشد، بهبود یابد. گفتگو پیش از شروع یک عملیات حسابرسی به حسابرس کمک می کند درک بهتری از نحوه استفاده مقررات گذاران از صورت‌های مالی در فرآیندهای تصمیم‌گیری خود، پیدا کند. هم‌چنین این تمرکز بر مشکلات مورد توجه مقررات گذار ممکن است به حسابرسان اجازه دهد تا بتوانند با موشکافی بیشتر از معمول، مدیریت شرکت را به نفع سیستم مدیریت ریسک کلی، به چالش بکشند.

ناظرین و حسابرسان مستقل نقش مهمی در ایجاد یک سیستم کنترل کارآمد ایفا کرده و از قدرت کافی برای به چالش کشیدن خود سیستم برخوردارند. ارتباط بهتر و تعامل نزدیک‌تر میان حسابرسان داخلی، ناظرین و حسابرسان مستقل می‌تواند منجر به خلق سیستم کنترلی شود که قادر است با بهره‌گیری از اطلاعاتی که به‌طور معمول در دسترس نیست، کاستی‌ها و نقاط ضعف را در همان اولین خط و دومین خط شناسایی نماید. به‌علاوه، وجود چنین تعاملی می‌تواند زمینه‌ساز خلق محیطی که از استقلال، بی‌طرفی و یکپارچگی کار حسابرسی داخلی و مستقل پشتیبانی می‌کند، شود. به این ترتیب، وقتی ناظرین اطمینان یابند که فرآیند کار حسابرس مستقل منصفانه، بی‌طرفانه، شفاف و مستقل از مدیریت بانک بوده و به‌خوبی مستندسازی شده است، قابلیت اعتماد عملکرد و خروجی حسابرسان مستقل افزایش می‌یابد.

---

[۹۴] کمیته نظارت بانکی بازل ، حسابرسی‌های مستقل بانک‌ها، مارس ۲۰۱۴.

[۹۵] EBA ، مشاوره در مورد دستورالعمل‌های پیشنهادی ارتباط بین مقامات دارای صلاحیت نظارت بر موسسات اعتباری و حسابرسان قانونی، اکتبر ۲۰۱۵.

[۹۶] بانک جهانی: مرکز اصلاح گزارشگری مالی (CFRR)، ناظرین مالی و حسابرسان مستقل: ایجاد یک رابطه سازنده، به زودی.

[۹۷] صندوق بین المللی پول، "به سوی چارچوب ثبات مالی"، نظرسنجی اقتصادی و مالی جهانی، واشنگتن، ۱۹۹۸، صفحه ۳۶.

[۹۸] ایوالد نووتنی، راهبر بانک ملی اتریش، سخنرانی در کنفرانس ناظرین و حسابرسان: ایجاد روابط سازنده، وین، ۲۸ سپتامبر ۲۰۱۵؛ کمیته نظارت بانکی بازل ، نامه‌ای به هیئت استانداردهای بین المللی حسابرسی و اطمینان‌دهی (IAASB)، آوریل ۲۰۱۳.

در نقشه‌راه پذیرش مدل نوآورانه چهارخط دفاعی، ارتباط بین سه طرف درگیر بر اساس یک رابطه مثلثی موضوعی مهم است که باید بر روی آن تمرکز شود. به‌ویژه، محدوده اطلاعات، شکل ارتباط و زمان‌بندی و تعداد دفعات ارتباط اجزای مهمی هستند که استمرار کلی کنترل‌ها را تقویت می‌کند. با ایجاد و استفاده از مدل چهارخط دفاعی، ویژگی‌های زیر باید در برقراری ارتباط اجباری شده و به‌طور کارآمد به‌کار گرفته شود:

الف) نظم و قاعده اطلاعات فراهم‌شده:

- تعریف واژگان و دامنه تعامل؛ و
- تبادل اطلاعات پیش و در خلال کار حسابرسی به نحوی که اجازه انعطاف‌پذیری را بدهد (مثلا از طریق برگزاری جلسات موقت در هرزمانی که لازم باشد)

ب) کیفیت تعاملات:

- بازخورد واقعی در مورد کیفیت تعاملات و به‌اشتراک‌گذاری اطلاعات؛ و
- ارزیابی منظم استقلال و بی‌طرفی[۹۹] هر کدام از طرف‌های درگیر (مثلا شرایط قرار ملاقات (کار) حسابرس مستقل)

ج) تعریف شفاف اختیار و دامنه کار:

- ناظرین باید قدرت درخواست دسترسی به هرگونه اطلاعات نگهداری شده توسط حسابرسی مستقل یا داخلی را داشته باشند؛
- هر سه طرف درگیر باید با هم دامنه حسابرسی موضوع کار را برای بررسی تعیین کنند (مثلا بحث مشترک در مورد صورت‌های مالی)؛ و
- هر سه طرف درگیر باید روش‌شناسی حسابرسی خود را به اشتراک گذاشته و در مورد برنامه اقدامات حیاتی صحبت کنند.

این مدل نباید بر اساس رویکرد «یک نسخه برای همه»[۱۰۰] به کار گرفته شود و باید بسته به اندازه و مقیاس عملیات و محدوده فعالیت‌هایی که دنبال می‌شود به‌صورت موردی استفاده شود.

[۹۹] رجوع شود به کمیته نظارت بانکی بازل ، فعالیت حسابرسی داخلی در بانک‌ها، آوریل ۲۰۱۲، اصل ۱۲.

[۱۰۰] در سیستم بانکی در اروپا، تناسب، یکی از اصول کلیدی استفاده از به اصطلاح تنها کتاب قانون (مجموعه‌ای هماهنگ از قوانین که تحت آن اتحادیه بانکداری عمل می‌کند) است. هر دو کمیسیون و پارلمان اروپا تاکید کرده‌اند که تنوع سیستم بانکی اتحادیه اروپا باید مورد تایید قرار گیرد. رجوع شود به EBA، کارگاه تناسب: استفاده از اصل تناسب در زمینه اصلاحات نهادی و نظارتی، ژوئیه ۲۰۱۵.

۶. نتیجه‌گیری

برگرفته از خط بحثی که در بالا پیگیری شد، نتیجه‌گیری می‌کنیم که موسسات مالی قانونمند نیازمند مدل چهار خط دفاعی مناسبی هستند که بر روابط میان حسابرسی داخلی (سومین خط دفاعی) و حسابرسی مستقل و ناظرین (که هر دو با هم چهارمین خط دفاعی را تشکیل می‌دهند) تاکید دارد. برخلاف وضعیت بیرونی، واحدهایی که خط چهارم دفاعی را تشکیل می‌دهند باید در مباحث کنترل پایش و نظارت در سازمان فعالیت داشته باشند. این بدین معناست که تعامل نزدیک میان فعالیت حسابرسی داخلی، حسابرسی مستقل و ناظرین بسیار اهمیت دارد. مزایا و ریسک‌هایی که از همکاری نزدیک میان این سه واحد ممکن است حاصل شود را برجسته کردیم. تحقیقات بیشتری برای توسعه راهکارهای ممکن جهت حل مشکلات شناسایی‌شده، لازم است.

به‌علاوه، تغییراتی که از این پس در شیوه‌های عمل نظارتی و حسابرسی در بخش مالی اعمال می‌شود تا مشکلات کلیدی در موسسات را در همان مراحل اولیه رهگیری شده و بدون خدشه واردکردن به استقلال وظایف خطوط دفاعی سوم و چهارم، عملیات روزمره سازمان از نزدیک پایش شود، باید مورد بررسی قرار گیرد.

[أ] Institute of Internal Auditors Research Foundation
[ب] Global Financial Crisis
[ت] Chief Risk Officer
[ث] **کمیته نظارت بانکی بازل** (Basel Committee on Banking Supervision) اولین استانداردگذار جهانی برای مقررات احتیاطی بانکها است و فراهم کننده مجمعی برای هماهنگی مقررات با موضوعات نظارت بانکی است. آن دارای ۴۵ عضو شامل بانک‌های مرکزی و ناظرین بانکی از ۲۸ حوزه قضایی است. علاوه بر این کمیته دارای ۹ ناظر از جمله بانک‌های مرکزی، گروه‌های نظارتی، سازمان‌های بین‌المللی و دیگر سازمانهاست. کمیته عضویت خود را در سال ۲۰۰۹ و دوباره در سال ۲۰۱۴ گسترش داده است.
کمیته بازل: در ابتدا کمیته تنظیم مقررات و شیوه‌های نظارت بانکی نامیده میشد. بوسیله راهبران بانک مرکزی کشورهای گروه ده (G۱۰) در اواخر سال ۱۹۷۴ پس از اختلالات جدی در بازارهای ارز و بانکی بین‌المللی (به ویژه شکست بانک هادوس هرستات در آلمان غربی) تاسیس شد. دفتر مرکزی کمیته بازل در بانک تسویه بین‌المللی در شهر بازل سوییس مستقر است و برای بهبود پایداری مالی و بهبود کیفیت نظارت بانکی در سراسر جهان و همچنین به عنوان یک مجمع برای همکاری منظم بین کشورهای عضو در امور نظارتی بانکی ایجاد شده است. اولین جلسه آن در فوریه سال ۱۹۷۵ برگزار شد و جلسات بطور منظم سه تا چهار بار در سال برگزار می‌شود. از زمان آغاز به کار، کمیته بازل عضویت را از گروه ۱۰ (G۱۰) تا ۴۵ موسسه از ۲۸ حوزه قضایی گسترش داده است. با شروع موافقت‌نامه بازل که ابتدا در سال ۱۹۷۵ منتشر شد و چندین بار اصلاح شد، کمیته مجموعه‌ای از استانداردهای بین‌المللی برای تنظیم مقررات بانکی را تعیین کرده است، از جمله مهمترین نشریات برجسته آن در مورد کفایت سرمایه است که معمولاً به عنوان بازل ۱، بازل ۲ و اخیراً بازل ۳ شناخته می‌شود. (بازل: سومین شهر پرجمعیت سوییس در شمال غربی سوییس در کنار رودخانه راین است، با حدود ۱۷۵۰۰۰ نفر جمعیت. زبان گویشی آنها آلمانی است. این شهر به خاطر موزه‌های بین‌المللی آن شناخته شده است.)
[ج] Organisation for Economic Co-operation and Development
[چ] European Commission
[ح] Microprudential Policies
[خ] Volcker Rule
[د] European Union
[ذ] Back Office
[ر] Middle Office
[ز] Detective
[س] Jérôme Kerviel
[ش] Single Supervisory Mechanism
[ص] European Central Bank
[ض] Safe Harbour
[ط] Independent Forum of Independent Audit Regulators
[ظ] Systemically Important Financial Institutions
[ع] Prudential Regulation Authority
[غ] Financial Market Supervisory Authority
[ف] International Monetary Fund
[ق] Federal Deposit Insurance Corporation
[ك] Hong Kong Monetary Authority
[ل] European Banking Authority
[م] Public Company Accounting Oversight Board
[ن] Information Systems Audit and Control Association
[ه] Long Form Audit Report

استفاده از چارچوب کوزو در مدل سه خط دفاعی

مرتضی اسدی **الهه مهدوی ثابت**

مقدمه

این مقاله محصول همکاری بین کمیته سازمان‌های حامی (COSO) و انجمن حسابرسان داخلی است. هدف این مقاله کمک به سازمان‌ها جهت ارتقای ساختارهای راهبری کلی آنها با ارائه رهنمودی درخصوص نحوه شرح و تخصیص نقش‌ها و مسئولیت‌های مشخص درقبال کنترل داخلی از طریق ارتباط دادن چارچوب یکپارچه کنترل داخلی کوزو به مدل سه خط دفاعی است.

خلاصه اجرایی

هر سازمانی اهدافی دارد که برای دستیابی به آنها تلاش می‌کند. در مسیر دستیابی به اهداف، سازمان با رویدادها و شرایطی مواجه می‌شود که ممکن است تحقق این اهداف را تهدید کنند. این رویدادها و شرایط بالقوه ریسک‌هایی را ایجاد می‌کنند که سازمان باید آنها را مشخص، تحلیل، تعریف و پیگیری کند. برخی ریسک‌ها (به‌طور کلی یا جزئی) ممکن است پذیرفته شوند و برخی ممکن است به‌طور کامل یا جزئی تا حدی کاهش یابند که در آن سطح برای سازمان قابل قبول باشند. روش‌های متعددی برای کاهش ریسک‌ها وجود دارد که یک روش کلیدی، طراحی و پیاده‌سازی کنترل داخلی موثر است.

چارچوب یکپارچه کنترل داخلی کوزو (چارچوب) اجزا، اصول و عوامل لازم برای یک سازمان جهت مدیریت موثر ریسک‌ها از طریق پیاده‌سازی کنترل داخلی را بیان می‌کند. با وجود این، به این مسئله نمی‌پردازد که چه کسانی مسئول انجام وظایف خاص قید شده در این چارچوب هستند. مسئولیت‌های روشنی باید تعریف شوند تا هر گروه نقش خود را در پیگیری ریسک و کنترل، ابعادی که در مقابل آن پاسخگو است، و نحوه هماهنگی تلاش‌های خود با دیگر گروه‌ها را بداند. نباید در پیگیری ریسک و کنترل «شکاف‌هایی» وجود داشته باشد، و یا اقدامی به‌طور غیرضروری یا ناخواسته تکرار شود.

مدل سه خط دفاعی به نحوه تخصیص و هماهنگ‌سازی وظایف خاص مرتبط با ریسک و کنترل در یک سازمان، صرفنظر از اندازه و پیچیدگی آن، می‌پردازد. اعضای هیئت‌مدیره و مدیریت باید تفاوت‌های مهم بین نقش‌ها و مسئولیت‌های این وظایف و نحوه تخصیص بهینه آنها برای سازمان به منظور افزایش احتمال دستیابی به اهداف را بدانند. به‌ویژه، این مدل تفاوت و رابطه میان اطمینان‌بخشی سازمان‌ها و سایر فعالیت‌های نظارتی را تصریح می‌کند؛ فعالیت‌هایی که اگر به وضوح تعریف نشوند، می‌تواند سبب سوءبرداشت شود.

ما قصد داریم در ادامه، هم از چارچوب و هم از مدل معرفی شده با این فرض استفاده کنیم که خوانندگان از پیش شناخت اولیه‌ای از چارچوب دارند. خوانندگانی که آشنایی با چارچوب ندارند، می‌توانند برای کسب اطلاعات بیشتر به سایت COSO.org مراجعه کنند. توضیحات کامل‌تر مدل در بخش ۱ این مقاله آمده است.

شکل ۱. ارتباط میان اهداف، چارچوب و مدل

۱. مدل سه خط دفاعی

این مدل به شناخت مدیریت ریسک و کنترل از طریق شفاف‌سازی نقش‌ها و وظایف کمک می‌کند. هدف اصلی آن، این است که تحت نظارت و هدایت مدیریت ارشد و هیئت‌مدیره، سه گروه مجزا (یا خطوط دفاعی) در سازمان برای مدیریت موثر ریسک و کنترل ضرورت دارند. مسئولیت‌های هر گروه (یا «خطوط») عبارتند از:

۱. **مالکیت و مدیریت** ریسک و کنترل (مدیریت عملیات خط مقدم).

۲. **پایش** ریسک و کنترل در حمایت از مدیریت (قراردادن فعالیت‌های ریسک، کنترل و تطبیق توسط مدیریت).

۳. **ارائه اطمینان‌بخشی مستقل** به هیئت‌مدیره و مدیریت ارشد درخصوص اثربخشی مدیریت ریسک و کنترل (حسابرسی داخلی).

هر یک از سه خط دفاعی در کل چارچوب راهبری سازمان نقش متمایزی دارد. هنگامی که هر کدام به‌شکلی موثر به وظیفه‌اش عمل کند، احتمال موفقیت سازمان در دستیابی به اهداف کلی خود بیشتر می‌شود.

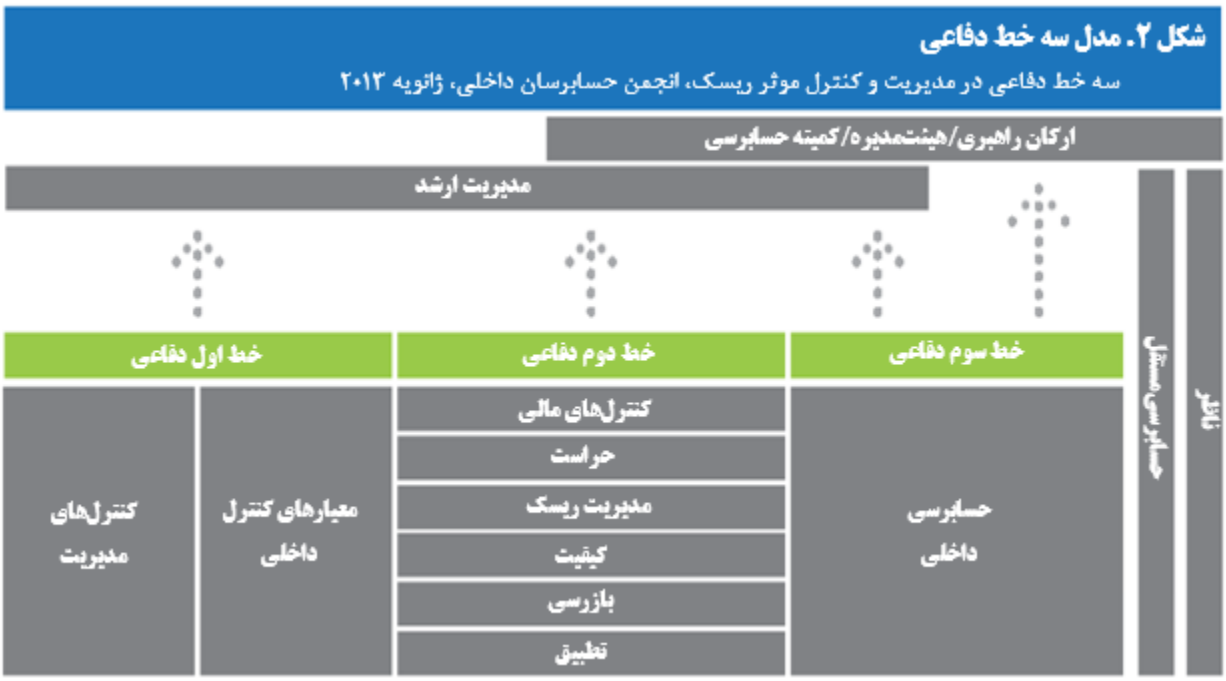
مطابق سایر نشریات کوزو، در این سند از اصطلاح «هیئت‌مدیره» برای اشاره به هیئت‌های راهبری مانند هیئت‌مدیره، هیئت‌امناء، شرکای عمومی، مالکین، یا هیئت‌های نظارتی استفاده می‌شود.

هر شخصی در سازمان در قبال کنترل داخلی مسئولیتی دارد، اما برای کمک به انجام وظایف ضروری طبق انتظار، این مدل، نقش‌ها و مسئولیت‌های مشخصی را تصریح می‌کند. هنگامی که سازمانی به‌درستی سه خط (دفاعی) را سامان‌دهی کرده باشد، و هر سه خط دفاعی به شکلی موثر عمل کنند، نباید هیچ شکافی در پوشش، و هیچ تکرار غیرضروری اقدامات مشاهده شود، و احتمال مدیریت موثر ریسک و کنترل بیشتر باشد. هیئت‌مدیره فرصت بیشتری برای دریافت اطلاعات غیرسوگیرانه درباره مهمترین ریسک‌های سازمان-و چگونگی پاسخگویی مدیریت به این ریسک‌ها دارد.

این مدل ساختار انعطاف‌پذیری دارد که می‌تواند در حمایت از چارچوب پیاده‌سازی شود. فعالیت‌های درون هر خط دفاعی در هر سازمانی متفاوت است، و برخی فعالیت‌ها ممکن است در خطوط دفاعی ترکیب یا تفکیک شوند. به عنوان مثال، در بعضی از سازمان‌ها، قسمت‌هایی از فعالیت تطبیق در خط دوم ممکن است در طراحی کنترل‌ها برای خط اول دخالت داشته باشد، در حالی که سایر قسمت‌های خط دوم در درجه اول به پایش این کنترل‌ها بپردازند.

شکل ۲. مدل سه خط دفاعی

سه خط دفاعی در مدیریت و کنترل موثر ریسک، انجمن حسابرسان داخلی، ژانویه ۲۰۱۳



صرفنظر از نحوه سامان‌دهی این سه خط دفاعی در یک سازمان، چند اصل مهم ضمنی در این مدل وجود دارد:

۱. اولین خط دفاعی با مالکین کسب و کار و فرآیند در ارتباط است که فعالیت‌های آنها ریسک‌هایی را ایجاد و/یا مدیریت می‌کند که می‌تواند دستیابی سازمان به اهدافش را تسهیل کند یا مانع آن شود. این شامل پذیرش ریسک‌های صحیح است. خط اول دفاعی مالک ریسک، و مسئول طراحی و اجرای کنترل‌های سازمان جهت پاسخ به آن ریسک‌ها است.

۲. خط دوم دفاعی به حمایت مدیریت با فراهم‌سازی تخصص، تعالی فرآیند، و پایش مدیریت در کنار خط اول قرار داده می‌شود تا مدیریت موثر ریسک و کنترل تضمین شود. فعالیت‌های خط دوم دفاعی از خط اول دفاعی مجزا هستند، اما همچنان تحت کنترل و هدایت مدیریت ارشد قرار دارند و به طور معمول برخی فعالیت‌های مدیریتی را انجام می‌دهند. خط دوم اساساً فعالیت مدیریت و/یا نظارت است که بسیاری از ابعاد مدیریت ریسک را در اختیار دارد.

۳. خط سوم به مدیریت ارشد و هیئت‌مدیره درخصوص مطابقت اقدامات خطوط اول و دوم با انتظارات آنها اطمینان می‌دهد. خط سوم دفاعی بطور معمول مجاز به انجام فعالیت‌های مدیریتی به منظور محافظت از بی‌طرفی و استقلال سازمانی خود نیست. علاوه بر این، خط سوم، خط گزارشگری اصلی به هیئت‌مدیره را در اختیار دارد. به این ترتیب، خط سوم اطمینان می‌دهد که نداشتن فعالیت مدیریتی است که آن را از خط دوم دفاعی جدا می‌کند.

هدف هر سازمانی دستیابی به اهدافش است. پیگیری این اهداف مستلزم استقبال از فرصت‌ها، پیگیری رشد، پذیرش ریسک‌ها، و مدیریت این ریسک‌ها است - همه در جهت پیشرفت سازمان هستند. قصور در پذیرش ریسک‌های مناسب، و قصور در مدیریت و کنترل صحیح ریسک‌های پذیرفته شده، می‌تواند سازمان را از دستیابی به اهدافش بازدارد. تنشی بین فعالیت‌ها جهت ایجاد ارزش و فعالیت‌های واحد اقتصادی به منظور حفظ ارزش سازمانی وجود دارد، و همیشه نیز وجود خواهد داشت. این چارچوب ساختاری برای بررسی ریسک و کنترل جهت اطمینان از مدیریت مناسب و صحیح آنها فراهم می‌آورد. این مدل رهنمودی درخصوص ساختار سازمانی که پیاده‌سازی خواهد شد، تخصیص نقش‌ها و مسئولیت‌ها به طرف‌هایی که به موفقیت در مدیریت موثر ریسک و کنترل می‌افزایند، ارائه می‌دهد.

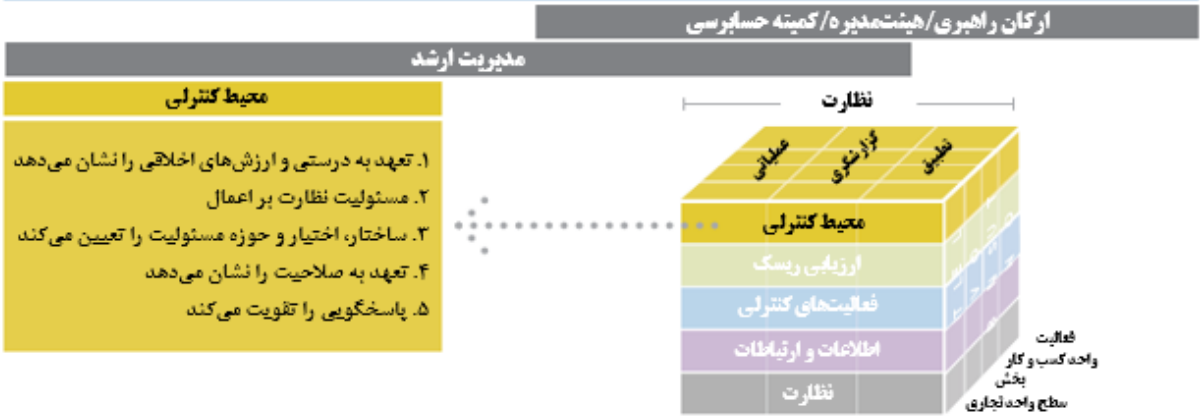
نقش‌های مدیریت ارشد و هیئت‌مدیره در مدل سه خط دفاعی

مدیریت ارشد و هیئت‌مدیره در این مدل نقش‌های جدانشدنی دارند. مدیریت ارشد در قبال انتخاب، توسعه، و ارزیابی سیستم کنترل داخلی تحت نظارت هیئت‌مدیره، پاسخگو است. اگر چه نه مدیریت ارشد و نه هیئت‌مدیره بخشی از یکی از سه خط دفاعی محسوب نمی‌شوند، این دو در مجموع در مورد تعیین اهداف سازمان، تعریف راهبردهای سطح بالا برای دستیابی به این اهداف، و ایجاد ساختارهای راهبری به منظور مدیریت ریسک به بهترین نحو، مسئولیت دارند. آنها همچنین اشخاصی هستند که در بهترین موقعیت قرار گرفته‌اند تا ساختار سازمانی بهینه را برای نقش‌ها و مسئولیت‌های مرتبط با ریسک و کنترل مشخص سازند. مدیریت ارشد باید از راهبری قوی، مدیریت ریسک و کنترل بطور کامل حمایت کند. افزون براین، این دو مسئولیت نهایی را برای فعالیت‌های خطوط اول و دوم دفاعی برعهده دارند. تعهد آنها در موفقیت مدل کلی، حیاتی است.

این چارچوب به شفاف‌سازی این مسئولیت‌های هیئت‌مدیره و مدیریت ارشد کمک می‌کند. همانطور که شکل ۳ نشان می‌دهد، مدیریت ارشد و هیئت‌مدیره در قبال محیط کنترلی سازمان که براساس ۵ اصل پشتیبانی می‌شود مسئولیت اصلی دارند که این ۵ اصل سلسله مراتب سازمانی را ایجاد می‌کند.

این مدل ساختاری را تحت چارچوب تعریف کرده است که چگونگی تخصیص نقش‌ها و مسئولیت‌ها را تشریح می‌کند. این مدل با حمایت و هدایت فعالانه هیئت‌مدیره و مدیریت ارشد به بهترین نحو پیاده‌سازی می‌شود.

شکل ۳. مسئولیت‌های نظارتی برای محیط کنترلی



خط اول دفاعی: مدیریت عملیاتی

خط اول دفاعی در این مدل در درجه اول توسط مدیران خط مقدم و خط میانی اداره می‌شود که مالکیت و مدیریت روزمره ریسک و کنترل را در اختیار دارند. مدیران عملیاتی فرآیندهای کنترل و مدیریت ریسک سازمان را تدوین و پیاده‌سازی می‌کنند. این فرآیندها عبارتند از فرآیندهای کنترل داخلی طراحی شده جهت تشخیص و ارزیابی ریسک‌های با اهمیت، اجرای فعالیت‌ها طبق هدف، آشکارسازی فرایندهای نامناسب، رفع نارسایی‌های کنترلی، و اطلاع‌رسانی به ذینفعان اصلی فعالیت. مدیران عملیاتی باید برای انجام این فعالیت‌ها در حیطه عملیاتی خود از مهارت کافی برخوردار باشند.

مدیریت ارشد در مورد کلیه فعالیت‌های خط اول مسئولیت کلی دارد. برای برخی زمینه‌های پرریسک، مدیریت ارشد نیز ممکن است حتی تا سطح انجام برخی از مسئولیت‌های خط اول، نظارت مستقیم بر مدیریت خط مقدم و خط میانی داشته باشد.

افراد در خط اول دفاعی مسئولیت‌های عمده‌ای در ارتباط با بخش‌های ارزیابی ریسک، فعالیت‌های کنترلی و اطلاعات/ارتباطات چارچوب دارند. همانطور که شکل ۴ نشان می‌دهد، مدیران عملیاتی برای ۱۲ اصل باقیمانده کنترل داخلی بیان شده در این چارچوب، مسئولیت اصلی دارند.

شکل ۴. کوزو و خط اول دفاعی

خط دوم دفاعی: پایش داخلی و فعالیت‌های نظارتی

خط دوم دفاعی شامل فعالیت‌های متنوعی در زمینه مدیریت ریسک و تطبیق است که مدیریت آنها را در نظر می‌گیرد تا کنترل‌ها و فرآیندهای مدیریت ریسک که در خط اول دفاعی پیاده‌سازی شده‌اند، طراحی مناسبی داشته باشند و طبق برنامه عمل کنند. این فعالیت‌های مدیریتی؛ از مدیریت اجرایی خط اول مجزا هستند، اما همچنان مدیریت ارشد است که آنها را کنترل و هدایت می‌کند. فعالیت‌های موجود در خط دوم به‌طور معمول، مسئول نظارت مستمر بر کنترل و ریسک هستند. آنها اغلب برای کمک به تعریف استراتژی پیاده‌سازی، ایجاد تخصص در ریسک، پیاده‌سازی سیاست‌ها و رویه‌ها، و گردآوری اطلاعات جهت خلق دیدگاه سازمانی گسترده نسبت به ریسک و کنترل، همکاری تنگاتنگی با مدیریت اجرایی دارند.

ترکیب خط دوم، بسته به اندازه سازمان و صنعت، می‌تواند به طور قابل ملاحظه‌ای، متغیر باشد. در سازمان‌های بزرگ، سهامی عام، پیچیده، و/یا دارای سطح بالای نظارتی، ممکن است همه این فعالیت‌ها مجزا و متفاوت باشند. در سازمان‌های کوچک‌تر، خصوصی، با پیچیدگی کمتر و/یا دارای سطح پایین‌تر نظارتی، ممکن است برخی از فعالیت‌های خط دوم ترکیب شده یا اصلاً وجود نداشته باشند. به عنوان مثال، برخی سازمان‌ها فعالیت‌های حقوقی و تطبیقی را در یک بخش واحد قرار می‌دهند یا ممکن است بخش بهداشت و ایمنی را با فعالیت زیست‌محیطی ادغام کنند. همچنین در سازمان‌های خاصی، ممکن است مدیران بعضی از وظایف خط دوم یا همه آنها را در چارچوب خط اول دفاعی پیش ببرند.

کارکنان خط دوم، تحت نظارت مدیریت، بر کنترل‌های خاصی نظارت نموده تا تعیین کنند که آیا کنترل‌ها طبق انتظار عمل می‌کنند یا خیر. فعالیت‌های نظارتی انجام شده توسط خط دوم به طور معمول هر سه دسته از اهداف شرح داده شده در این چارچوب را پوشش می‌دهند: اهداف عملیاتی، گزارشگری، و تطبیق.

مسئولیت‌های افراد در خط دوم دفاعی بسیار متفاوت است، اما به طور معمول شامل موارد زیر است:

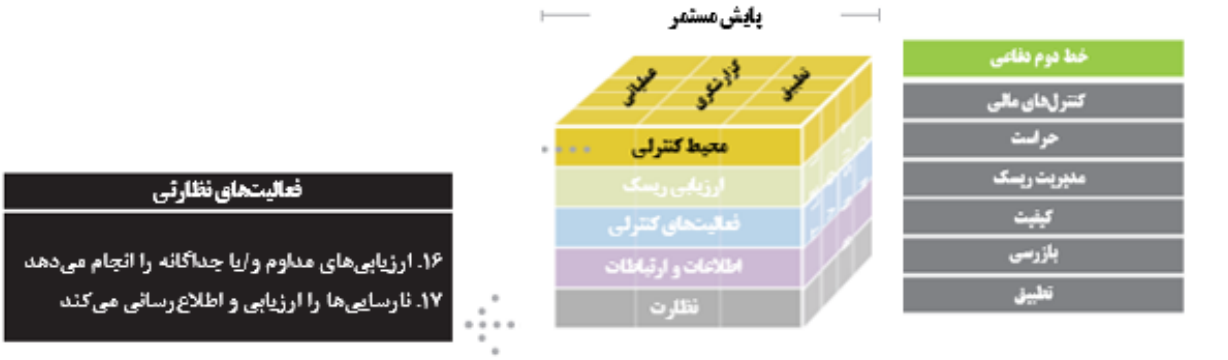
- همکاری با مدیریت در طراحی و توسعه فرآیندها و کنترل‌ها به منظور مدیریت ریسک‌ها.
- تعریف فعالیت‌هایی برای نظارت و نحوه اندازه‌گیری موفقیت در مقایسه با انتظارات مدیریت.
- نظارت بر کفایت و اثربخشی فعالیت‌های کنترل داخلی.
- ش مسائل حیاتی، ریسک‌های نوظهور و داده‌های پرت.
- ایجاد چارچوب‌هایی برای مدیریت ریسک.
- تشخیص و نظارت بر مسائل شناخته شده و نوظهوری که بر ریسک‌ها و کنترل‌های سازمان تاثیر می‌گذارند.
- تشخیص تغییرات در ریسک‌پذیری ضمنی سازمان و تاب‌آوری آن در برابر ریسک.
- ارائه راهنمایی و آموزش در رابطه با مدیریت ریسک و فرآیندهای کنترلی.

فعالیت‌های نظارتی توسط خط دوم دفاعی باید متناسب با نیازهای ویژه سازمان طراحی شوند. این فعالیت‌ها، به طور معمول، مجزا از فعالیت‌های عملیاتی روزمره هستند. در بسیاری از موارد، فعالیت‌های نظارتی در سراسر سازمان جاری هستند. با وجود این، در برخی از سازمان‌ها، فعالیت‌های نظارتی به یک یا چند حوزه محدود می‌شوند.

هر یک از فعالیت‌های خط دوم تا حدی مستقل از فعالیت‌های تشکیل‌دهنده خط اول دفاعی است، اما در ماهیت، فعالیت‌های مدیریتی محسوب می‌شوند. فعالیت‌های خط دوم ممکن است فرآیندهای سازمان در زمینه کنترل داخلی و ریسک را به طور مستقیم، توسعه دهد، پیاده‌سازی، و/یا اصلاح کند. همچنین آنها ممکن است در تصمیم‌گیری برای فعالیت‌های عملیاتی خاص نقش داشته باشند. تا آنجا که نقش فعالیت‌های خط دوم مستلزم مشارکت مستقیم آنها در فعالیت‌های خط اول باشد، فعالیت موردنظر ممکن است به طور کامل از آن فعالیت خط اول دفاعی مستقل نباشد.

هنگامی که فعالیت‌های خط دوم مستقل نیستند، نباید در اهمیت آنها بزرگ‌نمایی نمود، هرچند قوی و کارآمد باشند. از آنها انتظار می‌رود که با حد کافی از بی‌طرفی عمل کنند و از طریق خط اول دفاعی اطلاعات مهم و سودمندی را پیرامون مدیریت ریسک و کنترل در اختیار مدیریت ارشد و هیئت‌مدیره قرار دهند. آنها همچنین ممکن است اطلاعاتی در مورد ریسک و کنترل در سطح واحد تجاری را در اختیار مدیریت ارشد و هیئت‌مدیره قرار دهند که نمی‌توان از خط اول انتظار داشت. خط دوم برای آنکه به عنوان خط دفاعی، موثر واقع شود، باید در سراسر سازمان در کنار مدیریت اجرایی و رهبران از اعتبار کافی برخوردار باشد. اعتبار از اقتدار و خطوط گزارشگری مستقیم حاصل می‌شود که با خود احترام می‌آورند.

شکل ۵. کوزو و خط دوم دفاعی



خط سوم دفاعی: حسابرسی داخلی

حسابرسان داخلی به عنوان خط سوم دفاعی سازمان عمل می‌کنند. انجمن حسابرسان داخلی، حسابرسی داخلی را اینگونه تعریف می‌کند «یک فعالیت مستقل، اطمینان‌بخش واقع‌بینانه و مشاوره‌ای است که برای ارزش‌افزایی و بهبود عملیات سازمان طراحی شده است. حسابرسی داخلی با فراهم ساختن رویکردی سیستماتیک و نظام‌مند برای ارزیابی و بهبود اثربخشی فرآیندهای مدیریت ریسک، کنترل، و راهبری، سازمان را در دستیابی به هدف‌هایش یاری می‌کند.»

حسابرسی داخلی، در میان نقش‌های دیگر، اطمینانی در مورد کارایی و اثربخشی راهبری، مدیریت ریسک، و کنترل داخلی ارائه می‌دهد. دامنه کار حسابرسی داخلی می‌تواند دربردارنده تمام جوانب عملیات و فعالیت‌های سازمان باشد.

وجه تمایز حسابرسی داخلی از دو خط دفاعی دیگر، سطح بالای آن در استقلال سازمانی و بی‌طرفی است. طراحی یا پیاده‌سازی کنترل‌ها به طور معمول وظیفه حسابرسان داخلی نیست و آنها مسئول عملیات سازمان نیستند. در بیشتر سازمان‌ها، رابطه گزارشگری مستقیمی که میان رئیس واحد حسابرسی داخلی و هیئت‌مدیره وجود دارد، استقلال حسابرسی داخلی را تقویت می‌کند. به واسطه همین سطح بالای استقلال سازمانی، حسابرسان داخلی بهترین موقعیت را دارند تا به هیئت‌مدیره و مدیریت ارشد در مورد راهبری، ریسک، و کنترل اطمینانی قابل اتکا و عینی بدهند.

شکل ۶. کوزو و خط سوم دفاعی

حسابرسی داخلی به طور فعالانه به راهبری سازمانی موثر کمک می‌کند تا شرایط خاصی را فراهم سازد، شرایطی که موجب تقویت استقلال آن و حرفه‌ای‌گری می‌شود. بنابراین، برقراری فعالیت حسابرسی داخلی حرفه‌ای باید اولویت همه سازمان‌ها باشد. این امر، نه‌تنها برای سازمان‌های بزرگ‌تر، بلکه برای واحدهای تجاری کوچک‌تر نیز حائز اهمیت است. سازمان‌های کوچک‌تر که ساختار سازمانی آنها رسمیت و ثبات کمتری دارد برای اطمینان از اثربخشی فرآیندهای راهبری و مدیریت ریسک، ممکن است با محیط‌هایی با همان پیچیدگی روبه‌رو باشند، و ممکن است فاقد خط دوم دفاعی موثر باشند. همه سازمان‌ها باید برای حسابرسی داخلی کارکنان مستقل، کافی و با صلاحیت را گرد هم آورده و حفظ کنند؛ این کارکنان برای آنکه وظایف خود را، به‌طور مستقل، انجام دهند باید به سطحی در سازمان گزارش دهند که به میزان کافی عالی رتبه باشد؛ این کارکنان باید طبق مجموعه‌ای از استانداردهای مناسب و جهانی عمل کنند (مانند استانداردهای بین‌المللی انجمن حسابرسان داخلی برای اجرای حرفه‌ای حسابرسی داخلی).

حسابرسان مستقل، ناظران، و سایر نهادهای برون‌سازمانی

اگر چه طرف‌های برون‌سازمانی به طور رسمی جزو سه خط دفاعی سازمان محسوب نمی‌شوند، با وجود این، گروه‌هایی مانند حسابرسان مستقل و ناظران، اغلب نقش مهمی در ساختار کلی راهبری و کنترل سازمان دارند. ناظران، اغلب برای تقویت راهبری و کنترل، مقررات را وضع می‌کنند، و آنها سازمان‌های تحت‌نظارت خود را فعالانه مورد بررسی قرار داده و در مورد آنها گزارش می‌دهند. به همین ترتیب، حسابرسان مستقل ممکن است درخصوص کنترل‌های سازمان روی گزارشگری مالی و ریسک‌های مرتبط، مشاهدات و ارزیابی‌های مهمی را ارائه دهند.

در صورتی که هماهنگی موثری میان حسابرسان مستقل، ناظران، و سایر گروه‌های خارج از سازمان برقرار باشد، می‌توان آنها را به عنوان خطوط اضافی دفاعی در نظر گرفت، که دیدگاه‌ها و مشاهدات مهمی را در اختیار ذینفعان سازمان، از جمله هیئت‌مدیره و مدیریت ارشد، قرار می‌دهند. با وجود این، کار این گروه‌ها اهداف متفاوت و به طور کلی، متمرکزتر یا دقیق‌تری را دنبال می‌کند، چنان که حوزه‌های مورد بررسی این گروه‌ها محدودتر از حوزه‌هایی است که خطوط دفاعی داخلی سازمان ارزیابی می‌کنند. به عنوان مثال، ممکن است حسابرسی‌های نظارتی خاص تنها معطوف به مسائل تطبیقی، ایمنی، یا سایر مسائل با دامنه محدود باشد؛ در حالی که هدف از سه خط دفاعی یاد شده رسیدگی به طیف کاملی از ریسک‌های عملیاتی، گزارشگری، و تطبیقی است که پیش‌روی سازمان قرار دارد. طرف‌هایی همچون حسابرسان مستقل و ناظران، در حالی که اطلاعات ارزشمندی را ارائه می‌دهند، اما نباید به عنوان جانشینی برای خطوط دفاعی داخلی تلقی شوند زیرا مدیریت ریسک‌های سازمان مسئولیت خود سازمان است، نه مسئولیت یک گروه خارجی.

۲. سازماندهی و هماهنگی سه خط دفاعی

سازماندهی سه خط دفاعی

مدل سه خط دفاعی عامدانه طوری طراحی شده است که انعطاف‌پذیر باشد. همه سازمان‌ها باید این مدل را به نحوی پیاده‌سازی کنند که با صنعت، اندازه، ساختار عملیاتی آنها، و با رویکرد آنها به مدیریت ریسک سازگار باشد. با وجود این، به طور معمول راهبری کلی و محیط کنترلی، در حضور سه خط دفاعی مجزا و کاملاً مشخص، با قدرت بیشتری عمل می‌کند. سازمان‌ها باید بکوشند که ساختار راهبری آنها منطبق بر این مدل باشد، طوری که هر سه خط یاد شده، صرف‌نظر از اندازه یا پیچیدگی سازمان، به نوعی وجود داشته باشند. این «خطوط» باید متمایز، با نقش‌ها و مسئولیت‌های مجزا باشند، در سیاست‌ها و رویه‌های مناسب سازمان به‌روشنی بیان شود و به وسیله «فضای اخلاقی حاکم بر راس سازمان» که پیوسته وجود دارد، تقویت شود.

مرز دقیق خطوط بسته به نیازهای ویژه هر سازمان متفاوت است. در برخی از موقعیت‌ها، مانند برخی شرکت‌های کوچک‌تر یا جایی که برخی فعالیت‌ها در حال تحول هستند، نمی‌توان مرز مشخصی میان خطوط دفاعی قائل شد. به عنوان مثال، بعضی سازمان‌ها، وقتی برای نخستین بار فعالیت مدیریت ریسک را آغاز می‌کنند، ممکن است

برای تسریع در پیاده‌سازی، فعالیت دیگری را انجام دهند. با وجود این، در شرایطی که فعالیت‌های خطوط مختلف به وضوح قابل‌تفکیک نیست، هیئت‌مدیره باید تاثیرات احتمالی این ساختار را به‌دقت بررسی کند. در صورت امکان، موقعیت‌هایی که نمی‌توان در آنها خطوط دفاعی را به وضوح از هم تفکیک کرد باید کوتاه‌مدت باشند و به مرور که فعالیت‌ها توسعه می‌یابند، باید تفکیک مناسب صورت گیرد. چنانچه این موقعیت‌ها بیشتر از مدتی کوتاه یا موقت ادامه پیدا کند، هیئت‌مدیره باید بداند که تفکیک نکردن فعالیت‌های مدیریت و اطمینان‌بخشی پیامدهایی در پی دارد زیرا در این صورت، نمی‌توان سه خط دفاعی مجزا را اداره کرد.

هنگام بررسی یا تعیین وظایف خاص و هماهنگی میان فعالیت‌های مختلف سازمان در زمینه ریسک و کنترل، در نظر گرفتن نقش اساسی هر گروه در این مدل می‌تواند مفید باشد.

شکل ۷. تفاوت‌های بین سه خط دفاعی

اطمینان‌بخشی	فعالیت‌های مدیریتی	
خط سوم دفاعی	خط دوم دفاعی	خط اول دفاعی
حسابرسی داخلی استقلال بیشتر گزارش به ارکان راهبری	استقلال محدود در درجه اول به مدیریت گزارش می‌دهد	مدیریت عملیاتی

از آنجایی که استقلال و بی‌طرفی سازمانی از نشانه‌های اصلی خط سوم دفاعی است، در صورتی که سازمان فعالیت حسابرسی داخلی را با هرگونه نقش خط دوم دفاعی ترکیب کند، باید دقت ویژه‌ای را به‌کار بست. اگر فعالیت حسابرسی داخلی با هرگونه فعالیت خط دوم دفاعی ترکیب شود، مدیریت ارشد و هیئت‌مدیره باید اطمینان حاصل کنند که فعالیت‌ها به نحوی با هم ترکیب یا هماهنگ شده‌اند که استقلال یا بی‌طرفی سازمانی فعالیت حسابرسی داخلی را تهدید نمی‌کنند. حسابرسان داخلی به طور معمول نباید هرگونه مسئولیت مدیریتی را در قبال عملیاتی که حسابرسی می‌کنند، بپذیرند؛ و در سازمان‌هایی که حسابرسی داخلی در فعالیت‌های خط دوم دفاعی مشارکت دارد، این مشارکت عموماً باید کوتاه‌مدت باشد و نقش‌های متفاوت به افراد یا گروه‌های مختلف تخصیص داده شود. اگر مشارکت حسابرسی داخلی در وظایف خط دوم دفاعی کوتاه‌مدت نباشد، مدیریت ارشد و هیئت‌مدیره باید محدودیت در توانایی حسابرسی داخلی را برای ارائه اطمینان مستقل و بی‌طرف تشخیص دهند و ممکن است نیاز باشد که برای اطمینان‌بخشی درخصوص فعالیت‌های خاص تحت تاثیر به اشخاص برون‌سازمانی (مستقل) روی آورند.

هماهنگی سه خط دفاعی

سه خط دفاعی هر کدام هدف نهایی یکسانی دارند: کمک به سازمان جهت دستیابی به اهدافش با مدیریت موثر ریسک. این سه خط دفاعی به ذینفعان نهایی یکسانی خدمت‌رسانی می‌کنند، و اغلب به مسائل یکسانی مرتبط با ریسک و کنترل می‌پردازند. مدیریت ارشد و هیئت‌مدیره باید به‌وضوح انتظارشان را بیان کنند که اطلاعات اشتراک‌گذاری شود و فعالیت‌ها بین هر یک از سه خط دفاعی هماهنگ شود که این امر در آنها به اثربخشی کلی

اقدامات کمک می‌کند و از فعالیت‌های کلیدی هیچ یک از خطوط نمی‌کاهد. به عنوان مثال، سازمان‌های بسیاری شیوه‌هایی در سطح هیئت‌مدیره یا مدیریت در ارتباط با ریسک برای بیان این انتظارات اجرا کرده‌اند.

هماهنگی و ارتباط نباید با ساختار سازمانی اشتباه گرفته شوند. هرچند هدف یکسانی دارند، هر خط نقش‌ها و مسئولیت‌های ویژه خود را دارند. آنها خطوط دفاعی مجزا هستند اما نباید بدون ارتباط با یکدیگر عمل کنند. آنها باید اطلاعات مرتبط با ریسک، کنترل و راهبری را با یکدیگر به اشتراک بگذارند و اقدامات مرتبط را هماهنگ کنند. در بسیاری از موقعیت‌ها، ممکن است دیدگاه مشترکی درباره ریسک و کنترل وجود داشته باشد.

هماهنگی دقیق برای جلوگیری از تکرار غیرضروی اقدامات ضروری است، ضمن اینکه باید اطمینان حاصل شود که کلیه ریسک‌های عمده به نحوی مناسب رفع می‌شوند. این هماهنگی به قدری مهم است که براساس استاندارد ۲۰۵۰، مدیر واحد حسابرسی داخلی به طور ویژه موظف به «اشتراک‌گذاری اطلاعات و هماهنگی فعالیت‌ها با سایر ارائه‌دهندگان خدمات اطمینان‌بخشی و مشاوره‌ای درون‌سازمانی و برون‌سازمانی به منظور حصول اطمینان از پوشش مناسب و کاهش دوباره‌کاری‌ها است.»

در تعریف عملیاتی این هماهنگی، لازم است که نقش‌های کلیدی مدیران اجرایی مانند مدیر ارشد ریسک، مدیر ارشد تطبیق، یا مدیر واحد حسابرسی داخلی به‌دقت بازنگری و ساختاربندی شود تا هر یک بتواند ضمن هماهنگی و ارتباط با سایر مدیران ریسک و کنترل، مسئولیت‌های ویژه خود را انجام دهد.

اولین خط دفاعی مالکیت اصلی ریسک‌ها و روش‌های مورد استفاده در مدیریت این ریسک‌ها را دارد. خط دوم دفاعی در ریسک تخصص دارد، تنظیم استراتژی اجرایی را تسهیل می‌کند، و در پیاده‌سازی سیاست‌ها و رویه‌ها کمک می‌کند. هرچند این دو خط دفاعی در ارتباط با ریسک و کنترل، مسئولیت‌های متفاوتی دارند، لازم است که با استفاده از واژگان فنی یکسان با هم همکاری کنند، ارزیابی یکدیگر درباره ریسک‌های سازمان را درک کنند و از مجموعه مشترکی از ابزارها و فرآیندها در موارد ممکن، استفاده کنند.

فعالیت حسابرسی داخلی سازمان، یا خط سوم دفاعی، باید همه فعالیت‌های با اهمیت مرتبط با ریسک و کنترل را در دامنه کار خود در نظر بگیرد. ارتباط با فعالیت‌های موجود در خطوط اول و دوم دفاعی به حسابرسی داخلی کمک می‌کند تا از واژگان فنی مرتبط با ریسک مشابهی استفاده کند و شناخت این دو خط دفاعی را از ریسک درک کند.

حسابرسی داخلی همچنین باید اقدامات خود را با اقدامات خط دوم دفاعی هماهنگ کند. این هماهنگی بسته به ماهیت سازمان، فعالیت ویژه‌ای که هر طرف انجام می‌دهد، استقلال سازمانی فعالیت‌های خط دوم دفاعی، و انتظارات مدیریت ارشد و هیئت‌مدیره، به اشکال مختلفی صورت می‌پذیرد. در برخی موارد، ممکن است حسابرسی داخلی بتواند بخشی از ارزیابی خود را بر پایه فعالیتی که خط دوم انجام می‌دهد، بنا گذارد. در این شرایط، حسابرسی داخلی باید طراحی، برنامه‌ریزی، سرپرستی، مستندسازی، و بررسی مناسب آن فعالیت را تایید کند. گستره استفاده و سطح اتکا به کار دیگر فعالیت‌ها بسته به شرایط خاص تغییر می‌کند. حسابرسی داخلی همچنین

باید به استقلال سازمانی فعالیت‌های خط دوم که تصمیم می‌گیرد قسمتی از کار ارزیابی خود را برپایه آنها بگذارد، توجه ویژه داشته باشد. همانطور که حسابرسی داخلی با استقلال سازمانی تشکیل می‌شود تا ارزیابی‌های بدون سوگیری و بی‌طرف را ارائه دهد، فعالیتی که این کار را انجام می‌دهد که حسابرسی داخلی تصمیم می‌گیرد به آن اتکا کند، باید از سطح کافی استقلال سازمانی و بی‌طرفی برخوردار باشد. قابلیت و کارایی تنها معیارهای موجود نیستند. قابلیت خطوط دفاعی اول و دوم در انجام امور برای حسابرسی داخلی به این معنا نیست که آنها سطح استقلال و بی‌طرفی موردنیاز را فراهم می‌آورند. به طور مشابه، توانایی حسابرسی داخلی در انجام امور خط اول یا دوم به این معنا نیست که حسابرسی داخلی که امور خطوط اول یا دوم را انجام می‌دهد، الزاماً استقلال و بی‌طرفی سازمانی حسابرسی داخلی را حفظ می‌کند.

برای تسهیل اثبات این موضوع که این امور را می‌توان به نحوی کارآمد هماهنگ کرد، منشور حسابرسی داخلی باید تصریح کند که حسابرسی داخلی، مسئولیت ارزیابی عملکرد و اثربخشی امور فعالیت‌های دو خط دفاعی دیگر یا هر فعالیتی که شخص ثالث انجام می‌دهد را برعهده دارد.

هماهنگی ممکن است به فراتر از این سه خط دفاعی تعمیم پیدا کند، و سایر اشخاص برون‌سازمانی مانند حسابرسان مستقل را نیز در برگیرد. حسابرسان داخلی ممکن است به کار سایر ارائه‌دهندگان درون یا برون‌سازمانی در اطمینان‌بخشی در مورد راهبری، مدیریت ریسک و کنترل اتکا یا از آن استفاده کنند، مشروط بر اینکه از کار انجام شده، نتایج تشریح شده، و استقلال و صلاحیت طرف برون‌سازمانی شناخت کافی داشته باشند. برعکس، کار حسابرسی داخلی می‌تواند به صورت هدفمند برای برآوردن الزامات اشخاص برون‌سازمانی برنامه‌ریزی و انجام شود. هماهنگی اقدامات با اشخاص برون‌سازمانی می‌تواند منجر به بهبود کارایی شود؛ با وجود این، مدیران واحد حسابرسی داخلی و هیئت‌مدیره باید هزینه‌ها و همچنین مزایای بالقوه طراحی کار حسابرسی داخلی را برای منافع اشخاص برون‌سازمانی در نظر بگیرند.

۳. استفاده از کوزو (COSO) در (مدل) سه خط دفاعی

این چارچوب، ۵ جزء کنترل داخلی و ۱۷ اصل بیانگر مفاهیم بنیادی مربوط به این اجزا را تعریف می‌کند. نشریه COSO، کنترل داخلی-چارچوب یکپارچه، بیان می‌کند که چون این ۱۷ اصل مستقیماً از ۵ جزء کنترل داخلی برگرفته شده‌اند، می‌توان با بکارگیری هر یک از این اصول، به کنترل داخلی موثر دست یافت. مدیریت مسئولیت تخصیص وظایف ضروری مرتبط با ۱۷ اصل و تایید انجام وظایف براساس هدف موردنظر را برعهده دارد.

در پیوست، نمونه‌هایی از نحوه تخصیص مسئولیت ۱۷ اصل در بین سه خط دفاعی آمده است. کنترل داخلی-چارچوب یکپارچه همچنین «نکات محوری» مختلف مربوط به هر یک از این ۱۷ اصل را مشخص می‌کند. از آنجا که بسیاری از نکات محوری نشانگر مسئولیت‌های کلیدی افراد در این سه خط دفاعی هستند، خوانندگانی که با کنترل داخلی-چارچوب یکپارچه آشنایی دارند در می‌یابند که بسیاری از این نکات محوری در بخش بعد منعکس می‌شود.

اطلاعات درون پیوست برای ارائه مثالی درباره نحوه تخصیص وظایف بین سه خط دفاعی گنجانده شده‌اند. از آنجایی که هر سازمان منحصربفرد است، ممکن است سازمان‌ها برای تعریفی متفاوت از نقش‌ها و مسئولیت‌ها دلایل صحیحی داشته باشند. صرفنظر از نحوه تخصیص وظایف در یک سازمان، نقش‌ها و مسئولیت‌های مشخص درباره کلیه ۱۷ اصل باید به‌طور واضح تعیین و به کلیه اشخاص ذیربط اطلاع‌رسانی شوند تا شکاف‌های موجود در پوشش کنترل‌های داخلی و عدم تکرار غیرضروری اقدامات، کاهش پیدا کند.

۴. نتیجه‌گیری

هر سازمانی باید مسئولیت‌های مربوط به راهبری، ریسک و کنترل را برای تسهیل به حداقل رساندن «شکاف‌ها» در کنترل‌ها و تکرارهای غیرضروری وظایف تخصیص‌یافته مرتبط با ریسک و کنترل را به‌طور شفاف تعریف کند. مدل سه خط دفاعی شیوه موثری برای ارتقای ارتباطات درخصوص ریسک و کنترل از طریق تصریح نقش‌ها و وظایف را ارائه می‌دهد. این مدل می‌تواند برای تصریح نحوه هماهنگی مسئولیت‌های مربوط به ریسک و کنترل در سراسر یک سازمان سودمند باشد.

هدف اصلی این مدل این است که، تحت نظارت و هدایت مدیریت ارشد و هیئت‌مدیره، سه گروه مجزا (یا سه خط دفاعی) برای مدیریت موثر ریسک و کنترل لازم است. این سه گروه وظایف زیر را انجام می‌دهند:

- مالکیت و مدیریت ریسک و کنترل (مدیریت عملیاتی).
- پایش ریسک و کنترل در حمایت از مدیریت (قراردادن فعالیت‌های ریسک، کنترل، و تطبیق توسط مدیریت).
- ارائه اطمینان‌بخشی مستقل به هیئت‌مدیره و مدیریت ارشد درخصوص اثربخشی مدیریت ریسک و کنترل (حسابرسی داخلی).

هر یک از این سه «خط» دفاعی نقش متمایزی در کل چارچوب راهبری سازمان دارد و هنگامی که هر یک به‌نحوی موثر به وظیفه‌اش عمل کند، احتمال نقض با اهمیت در کنترل کاهش می‌یابد. این ساختار همچنین در دریافت اطلاعات بی‌طرف درباره مهمترین ریسک‌های سازمان-و درباره چگونگی پاسخگویی مدیریت به این ریسک‌ها، از هیئت‌مدیره پشتیبانی می‌کند.

از این مدل می‌توان در کنار کنترل داخلی COSO - چارچوب یکپارچه برای تسهیل اطمینان از شناخت افراد در هر خط دفاعی درباره گستره کامل مسئولیت‌هایشان درخصوص ریسک و کنترل، و نحوه گنجاندن وظایف آنها در ساختار کلی ریسک و کنترل، بهره گرفت.

مشاهدات کلیدی

۱. مدیریت ارشد و هیئت‌مدیره مسئولیت نهایی برای اطمینان‌دهی برای کارایی و اثربخشی راهبری، مدیریت ریسک، و فرایندهای کنترلی دارند.

۲. مدیریت ریسک زمانی به قویترین شکل صورت می‌گیرد که سه خط دفاعی روشن و مجزایی وجود دارد. هر سه خط دفاعی باید به شکلی در هر سازمان، صرفنظر از اندازه یا پیچیدگی آن، وجود داشته باشند.

۳. هر گروه در این سه خط دفاعی باید نقش‌ها و مسئولیت‌های روشنی داشته باشد که توسط خط‌مشی‌ها، رویه‌ها، و سازوکارهای گزارشگری مناسب، پشتیبانی شود.

۴. اطلاعات باید در بین هر یک از این خطوط دفاعی تشریک و فعالیت‌ها هماهنگ شوند تا کارایی بهبود یابد و از تکرار اقدامات خودداری شود، ضمن اینکه اطمینان دهد که به کلیه ریسک‌های با اهمیت رسیدگی می‌شود.

۵. خطوط دفاعی نباید به نحوی ترکیب یا هماهنگ شوند که اثربخشی آنها را به خطر بیندازد. هر خط دفاعی موضع و مسئولیت‌های منحصربفردی در سازمان دارد. در مواردی که سازمان فعالیت‌های این سه خط دفاعی را با هم ترکیب می‌کند باید دقت ویژه‌ای را به‌کار بگیرد. اگر این ترکیب، منحصربفرد بودن آن خط دفاعی را در معرض خطر قرار دهد، می‌تواند بر اثربخشی خط دوم دفاعی یا سوم تاثیر منفی بگذارد. قابلیت و کارایی تنها معیارهای موجود نیستند؛ استقلال و بی‌طرفی نیز از عناصر ضروری دیگری هستند که باید آنها را در نظر گرفت.

پیوست

اصل ۱. سازمان تعهد به درستی و ارزش‌های اخلاقی را نشان می‌دهد.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
از کلیه خطوط دفاعی باید انتظار داشت که از طریق دستورات، اقدامات، و رفتار خود، اهمیت درستی و ارزش‌های اخلاقی را نشان دهند.			
• از طریق مثال در پیاده‌سازی ارزش‌ها، یک فلسفه و یک سبک عملیاتی برای سازمان را هدایت می‌کند. • اهداف، برنامه‌ها و فعالیت‌های مرتبط با اخلاق را پیاده‌سازی می‌کند. • فرآیندهایی را برای ارزیابی عملکرد افراد و تیم‌ها در برابر استانداردهای رفتاری مورد انتظار، طراحی و اجرا می‌کند.	• ممکن است از اعضای خاص خط دوم دفاعی درخواست شود تا از خطوط تطبیق حمایت نموده، تخلفات احتمالی را بررسی، یا سایر وظایف خاص مرتبط با درستی و ارزش‌های اخلاقی را اجرا کنند.	• وضعیت فضای اخلاقی سازمان و اثربخشی استراتژی‌ها، تدابیر، ارتباطات، و سایر فرآیندهای آن را در دستیابی به سطح مطلوب تطبیق قانونی و اخلاقی ارزیابی می‌کند. • طراحی، پیاده‌سازی، و اثربخشی اهداف، برنامه‌ها و فعالیت‌های مرتبط با اخلاق سازمان را ارزیابی می‌کند. • این اطمینان را فراهم می‌کند که برنامه‌های اخلاقی به اهداف تعیین شده دست می‌یابند، ریسک‌های کلیدی به طور موثر مدیریت می‌شوند و کنترل‌ها به طور موثر عمل می‌کنند. • خدمات مشاوره‌ای را برای کمک به سازمان به منظور تدوین یک برنامه اخلاقی قوی و بهبود اثربخشی آن تا سطح عملکرد مطلوب، ارائه می‌دهد.	• هیئت‌مدیره بر فضای اخلاقی نظارت دارد و اطمینان می‌دهد که مدیریت، برنامه‌ها و فعالیت‌های مناسب مرتبط با اخلاق را دارا می‌باشد. • هیئت‌مدیره مسئول ایجاد «فضای اخلاقی موثر در راس سازمان» است. این موضوع شامل اطلاع‌رسانی انتظارات در مورد درستی، ارزش‌های اخلاقی و استانداردهای رفتاری است.

اصل ۲. هیئت‌مدیره استقلال خود از مدیریت را نشان می‌دهد و بر تدوین و اجرای کنترل داخلی نظارت دارد.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
• اطلاعات کافی در مورد تدوین و اجرای کنترل‌های داخلی به هیئت‌مدیره ارائه می‌دهد تا هیئت‌مدیره را قادر سازد وظایف امانتداری خود را انجام دهد.	• نظارت هیئت‌مدیره توسط ساختارها و فرآیندهایی که مدیریت در سطح اجرایی کسب‌وکار ایجاد می‌کند پشتیبانی می‌شود. این پشتیبانی ممکن است توسط خط اول دفاعی یا دوم ارائه شود. به عنوان مثال، یک کمیته مدیریتی یا یک گروه خط دوم دفاعی ممکن است بر موضوعاتی مانند فناوری اطلاعات یا تطبیق تمرکز کنند.	• در مورد تدوین و اجرای کنترل‌های داخلی اطمینان می‌دهد، ارزیابی می‌کند که آیا کنترل‌ها به طور مناسب طراحی شده‌اند، به طور موثر اجرا شده‌اند، و مطابق با هدف عمل می‌کنند یا خیر. • ممکن است به هیئت‌مدیره با پیشنهاد موارد دستور کار خاص مرتبط با اصل ۲ برای بحث در جلسات هیئت‌مدیره، کمک نماید.	• هیئت‌مدیره مسئول اطمینان از دارا بودن اعضای کافی مستقل از مدیریت و بی‌طرف در ارزیابی‌ها و تصمیم‌گیری است. • هیئت‌مدیره مسئولیت نظارت بر طراحی، پیاده‌سازی، و اجرای کنترل‌های داخلی توسط مدیریت را برعهده دارد: - **محیط کنترلی**- برقراری درستی و ارزش‌های اخلاقی، ساختارهای نظارتی، اختیار و مسئولیت، انتظارات از صلاحیت، و پاسخگویی به هیئت‌مدیره. - **ارزیابی ریسک**- تعامل با مدیریت برای تنظیم اشتهای ریسک. نظارت بر ارزیابی مدیریت از ریسک‌های دستیابی به اهداف، از جمله تاثیر بالقوه تغییرات با اهمیت، تقلب، زیرپاگذاری کنترل‌ها توسط مدیریت. - **فعالیت‌های کنترلی**- نظارت بر مدیریت ارشد در تدوین و اجرای فعالیت‌های کنترلی. - **اطلاعات و ارتباطات**- تجزیه و تحلیل و بحث در مورد اطلاعات مربوط به دستیابی به اهداف سازمان. - **فعالیت‌های نظارتی**- ارزیابی و نظارت بر ماهیت و دامنه فعالیت‌های نظارتی و ارزیابی مدیریت و رفع نارسایی‌ها. • هیئت‌مدیره با حسابرسی داخلی، و طرفین بالقوه در خط دوم دفاعی، مستقل از مدیریت، ملاقات می‌کند.

اصل ۳. مدیریت با نظارت هیئت‌مدیره، ساختارها، خطوط گزارشگری، و اختیارات و مسئولیت‌های مناسب را در جهت تعقیب اهداف ایجاد می‌کند.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
• ساختارها، خطوط گزارشگری، و اختیارات و مسئولیت‌های مناسب در تعقیب اهداف را ایجاد می‌کند. • اطلاعات مربوط به ساختارها، خطوط گزارشگری، و اختیارات و مسئولیت‌ها را به هیئت‌مدیره اطلاع‌رسانی می‌کند، تا هیئت‌مدیره را قادر سازد مسئولیت‌های نظارتی خود را انجام دهد.	• کار با مدیریت، ساختارهای سازمانی، خطوط گزارشگری، و اختیارات و مسئولیت‌های مناسب برای آنها به منظور اجرای مسئولیت‌هایشان.	• در مورد مناسب بودن و اثربخشی ساختارهای عملیاتی، خطوط گزارشگری، اختیارات، و مسئولیت‌ها در تعقیب اهداف، اطمینان‌دهی می‌نماید. • خط‌مشی‌ها و شیوه‌هایی را به منظور اجرای فعالیت‌ها مطابق با منشور خود از جمله خطوط گزارشگری و اختیارات مناسب، پیاده‌سازی می‌کند. • به طور دوره‌ای استقلال سازمانی و بی‌طرفی خود را به هیئت‌مدیره تصدیق می‌کند.	• هیئت‌مدیره اهداف کل سازمان را تایید می‌کند و مسئولیت نظارت بر تدوین و حفظ ساختارها، خطوط گزارشگری، و تخصیص اختیارات و مسئولیت‌های مناسب در تعقیب اهداف را برعهده دارد. • هیئت‌مدیره منشورهای مناسبی را برای ایجاد کمیته‌های خود، از جمله کمیته حسابرسی، صادر می‌کند. • کمیته حسابرسی منشورهای مناسبی را برای وظایف ریسک و کنترل که مسئول آن است از جمله حسابرسی داخلی، تصویب می‌کند.

اصل ۴. سازمان تعهد خود به جذب، توسعه، و حفظ افراد شایسته هم‌راستا با اهداف را نشان می‌دهد.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
• افراد شایسته را هم‌راستا با اهداف، جذب، توسعه و حفظ می‌کند.	• استعدادهای شایسته را به منظور دستیابی به اهداف خود، جذب و توسعه می‌دهد. • اطمینان حاصل می‌کند که افراد و فعالیت‌های خود به طور مناسب با مدیریت هم‌سو هستند. این موضوع ممکن است شامل چرخش افراد از طریق کارکردهای مختلف مدیریتی باشد.	• افراد با صلاحیت و ماهر را برای انجام ماموریت و منشور خود، جذب، توسعه و حفظ می‌کند. • ممکن است کارایی و اثربخشی خط‌مشی‌ها و فرآیندهایی مانند موارد زیر را ارزیابی و در مورد آنها اطمینان‌دهی کند: - خط‌مشی‌های منابع انسانی. - شیوه‌های استخدام. - برنامه‌های آموزشی و توسعه‌ای. - سیستم‌های ارزیابی عملکرد. - طرح‌های جبران خدمات. - طرح‌های جانشین‌پروری.	• هیئت‌مدیره برای اطمینان از اینکه مدیریت متعهد به جذب، توسعه و حفظ افراد شایسته هم‌راستا با اهداف است، نظارت می‌کند. • کمیته‌های هیئت‌مدیره اطمینان حاصل می‌کنند که کارکردهایی که کار نظارتی را انجام می‌دهند دارای افراد با صلاحیت هستند. • کمیته جبران خدمات هیئت‌مدیره اطمینان حاصل می‌کند که طرح‌های تشویقی و جبران خدمات هم‌راستا با اشتهای ریسک و اهداف بلندمدت سازمان هستند.

اصل ۵. سازمان افراد را در قبال مسئولیت‌های کنترل داخلی خود در تعقیب اهداف، پاسخگو می‌داند.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
• افراد را در قبال مسئولیت‌های کنترل داخلی در تعقیب اهداف پاسخگو می‌داند. این مسئولیت شامل اطلاع‌رسانی مسئولیت‌های خاص، پیاده‌سازی سیستم‌های ارزیابی عملکرد، و اجرای فرآیندهای پرسنلی طراحی شده به منظور پاسخگو نگهداشتن افراد در برابر اقداماتشان است.	• طبق تفویض اختیار توسط مدیریت، افراد در خط دوم دفاعی، وظیفه پایش و گزارش در مورد انجام مسئولیت‌های کنترل داخلی خاص دارند.	• در مورد انجام مسئولیت‌های کنترل داخلی خاص، اطمینان‌بخشی می‌کند. • حسابرسان داخلی ممکن است پیشنهادهایی در رابطه با پاسخگویی ارائه دهند، اما معمولاً هیچ اختیار مستقیمی برای تصمیم‌گیری در مورد اقدامات کارکنان یا سایر فرآیندهای طراحی شده به منظور پاسخگو نگهداشتن افراد برای مسئولیت‌های کنترل داخلی خود ندارند.	• هیئت‌مدیره مسئول اطمینان از این است که مدیریت افراد را در قبال مسئولیت‌های کنترل داخلی خود، پاسخگو نگه می‌دارد. • کمیته جبران خدمات هیئت‌مدیره اطمینان حاصل می‌کند که طرح‌های تشویقی و جبران خدمات با اهداف سازمان همسو هستند.

اصل ۶. سازمان اهداف را با وضوح کافی مشخص می‌کند تا امکان تشخیص و ارزیابی ریسک‌های مرتبط با اهداف را فراهم آورد.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
همه افرادی که بخشی از سیستم کنترل داخلی هستند، باید استراتژی‌ها و اهداف کلی تعیین شده توسط سازمان را درک کنند.			
• تعیین اهداف، بخش کلیدی فرآیند مدیریت مرتبط با برنامه‌ریزی استراتژیک است. • با نظارت هیئت‌مدیره، اهدافی را در سطح واحد تجاری تعیین می‌کند که با ماموریت، چشم‌انداز، و استراتژی‌های سازمان همسو باشد. • اهداف مناسب را با جزئیات کافی مشخص می‌کند تا ریسک‌های دستیابی به اهداف قابل تشخیص و ارزیابی شوند. • حدود مجاز را برای ریسک‌های خاص اعمال می‌کند. • اهداف سطح واحد تجاری را به اهداف فرعی خاص‌تری مرتبط می‌کند که در سراسر سازمان جاری هستند. • هم اهداف در سطح واحد تجاری و هم اهداف فرعی مرتبط باید مشخص، قابل اندازه‌گیری، قابل دستیابی، مربوط، و محدود به زمان باشند.	• مسئول تنظیم یا تایید اهداف در سطح واحد تجاری به عنوان یک کل نیستند؛ اما ممکن است از آنها خواسته شود تا پیش‌نویس، اجرا، پایش، و گزارش در مورد اهداف یا اهداف فرعی مرتبط با حوزه‌های تخصصی خاص خود، مانند اهداف مرتبط با تطبیق یا کنترل کیفیت را ارائه دهند. • ارزیابی می‌کنند که آیا اشتهای ریسک و توان ریسک‌پذیری مناسب در نظر گرفته شده است یا خیر.	• تایید می‌کند که اهداف در جای خود به کار گرفته می‌شوند و مشخص، قابل اندازه‌گیری یا مشاهده، قابل دستیابی، مربوط، و محدود به زمان هستند. - بررسی‌های در سطح کل واحد تجاری در مورد فرآیند هدف‌گذاری ممکن است به عنوان کارهای مستقل جداگانه انجام شوند. - اهداف یا اهداف فرعی خاص ممکن است در طول سایر کارهای حسابرسی داخلی نیز بررسی شوند. • برای حفظ استقلال سازمانی حسابرسی داخلی، حسابرسان معمولاً اهداف را (غیر از اهداف ویژه فعالیت حسابرسی داخلی)، تدوین نمی‌کنند.	• هیئت‌مدیره مسئولیت نظارت بر تنظیم اهداف را برعهده دارد و به حصول اطمینان از اینکه اهداف سطح بالا منعکس‌کننده تصمیمات مربوط به نحوه تلاش سازمان برای ایجاد، حفظ، و تحقق ارزش برای ذینفعان خود است، کمک می‌کند. • هیئت‌مدیره با مدیریت، توان ریسک‌پذیری و اشتهای ریسک مناسب را ایجاد نموده و اطمینان حاصل می‌کند که آنها در سراسر سازمان، اطلاع‌رسانی می‌شوند.

اصل ۷. سازمان ریسک‌های دستیابی به اهداف خود را در سراسر واحد تجاری مشخص نموده و ریسک‌ها را به عنوان مبنایی برای تعیین نحوه مدیریت آنها، تجزیه و تحلیل می‌کند.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
• ریسک‌های مرتبط با دستیابی به اهداف را مشخص و کنترل می‌کند. • اشتهای ریسک و توان ریسک‌پذیری سازمان را تعریف می‌کند، سیستم‌های مدیریت ریسک را برقرار نموده، و مسئولیت‌هایی را برای کنترل ریسک‌های خاص تحت نظارت هیئت‌مدیره ایجاد می‌کند.	• به یک فعالیت مدیریت ریسک سازمانی ممکن است مسئولیت‌های مهمی در رابطه با ریسک‌ها و کنترل‌ها واگذار شود. وظایف معمول می‌تواند شامل موارد زیر باشد: - ایجاد یک زبان یا واژه‌نامه ریسک مشترک. - تشریح اشتهای ریسک یا توان ریسک‌پذیری سازمان. - تشخیص و توصیف ریسک‌ها در «موجودی ریسک.» - پیاده‌سازی روش رتبه‌بندی ریسک برای اولویت‌بندی ریسک‌ها در درون فعالیت‌ها و بین آنها. - ایجاد یک کمیته ریسک و یا مدیر ارشد ریسک برای هماهنگ نمودن برخی فعالیت‌ها از سایر کارکردهای مدیریت ریسک. - ایجاد مالکیت برای ریسک‌ها و پاسخ‌های خاص. - تدوین برنامه‌های اقدام برای حصول اطمینان از مدیریت مناسب ریسک‌ها. - تدوین گزارشگری تلفیقی برای ذینفعان مختلف. - نظارت بر نتایج اقدامات انجام شده به منظور کاهش ریسک. - حصول اطمینان از پوشش کارآمد ریسک توسط حسابرسان داخلی، تیم‌های مشاوره‌ای، و سایر واحدهای ارزیابی. - تدوین یک چارچوب مدیریت ریسک که مشارکت اشخاص ثالث و کارکنان از راه دور را ممکن می‌سازد. • گروه‌های خاصی مانند کارکردهای امنیت و تطبیق ممکن است به مدیریت در تشخیص ریسک‌های مرتبط با حوزه تخصصی خود، با در نظر گرفتن سطوح اشتهای ریسک تعیین شده توسط مدیریت برای فعالیت‌ها یا بخش‌های مختلف سازمان، کمک کنند.	• چارچوب ریسک سازمان را برای اجرای یک برنامه حسابرسی مبتنی بر ریسک در سطح سازمان، در نظر می‌گیرد. • ممکن است برخی از فعالیت‌های مدیریت ریسک واحد تجاری را تا زمانی که استقلال و بی‌طرفی آسیب نبیند، تسهیل کند. • ملاحظات مربوط به تدوین برنامه حسابرسی داخلی ممکن است شامل موارد زیر باشد: - تشخیص و ارزیابی ریسک‌های ذاتی و باقیمانده. - کاهش کنترل‌ها، طرح‌های اضطراری، و نظارت بر فعالیت‌های مرتبط با ریسک‌های خاص. - صحت و کامل بودن ثبت‌های ریسک. - کفایت مستندات مربوط به فعالیت‌های ریسک و کنترل مدیریت.	• هیئت‌مدیره استراتژی کلی سازمان و اهداف آن از جمله شناخت ریسک‌های مرتبط با استراتژی را تعیین می‌کند. • هیئت‌مدیره نظارت را انجام می‌دهد و مدیریت را برای تشخیص و مدیریت ریسک‌های دستیابی به اهداف پاسخگو می‌داند.

اصل ۸. سازمان در ارزیابی ریسک‌های دستیابی به اهداف، احتمال تقلب را در نظر می‌گیرد.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
• فرآیندهایی را برای تشخیص، پیشگیری و کشف تقلب اجرا می‌کند. • آسیب‌پذیری سازمان در برابر تقلب را با حسابرسان داخلی و مستقل سازمان بررسی می‌کند.	• اطمینان حاصل می‌کند که ارزیابی‌های ریسک و کنترل شامل در نظر گرفتن خطر تقلب باشد. • گروه‌هایی مانند واحدهای تحقیقاتی ممکن است نقش مهمی در بازدارندگی و کشف تقلب داشته باشند. این گروه‌ها ممکن است مسئول توسعه و نظارت بر سیاست‌ها و رویه‌های مربوط به تقلب در سراسر واحد تجاری باشند.	• استانداردها ایجاب می‌کند که حسابرسان داخلی با در نظر گرفتن احتمال تقلب عمده در حوزه‌های مورد بررسی، مراقبت حرفه‌ای لازم را اعمال کنند. • حسابرسان داخلی ملزم به داشتن دانش کافی برای ارزیابی خطر تقلب و نحوه مدیریت آن توسط سازمان هستند، اما انتظار نمی‌رود که از تخصص فردی برخوردار باشند که مسئولیت اصلی او کشف و بررسی تقلب است.	• هیئت‌مدیره مسئول نظارت بر سیستم‌ها و فرآیندهایی است که برای جلوگیری و کشف تقلب در نظر گرفته شده است. • هیئت‌مدیره و مدیریت ارشد جوی را [در سازمان] برای پیشگیری و کشف تقلب تعیین می‌کنند. • هیئت‌مدیره باید گزارش‌های دوره‌ای در مورد آسیب‌پذیری سازمان در برابر تقلب از جمله تقلب در گزارشگری مالی را دریافت کند.

اصل ۹. سازمان تغییراتی را مشخص و ارزیابی می‌کند که می‌تواند به طور قابل ملاحظه‌ای بر سیستم کنترل داخلی تاثیر بگذارد.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
از آنجایی که تغییر می‌تواند از طیف گسترده‌ای از منابع داخلی و خارجی ناشی شود، افراد در هر سه خط دفاعی باید نسبت به مسائل نوظهوری که می‌تواند به طور قابل ملاحظه‌ای بر سیستم کنترل داخلی تاثیر بگذارد، هوشیار باشند.			
• مسئولیت اصلی برای سیستم کنترل داخلی و برای تشخیص و ارزیابی تغییراتی را دارد که می‌تواند بر سیستم کنترل داخلی تاثیر قابل ملاحظه‌ای بگذارد. • اطلاعات مربوط به تغییراتی که می‌تواند سیستم کنترل داخلی را به طور قابل ملاحظه‌ای تحت تاثیر قرار دهد با جزئیات کافی به هیئت‌مدیره منتقل می‌نماید تا هیئت‌مدیره بتواند مسئولیت‌های نظارتی خود را انجام دهد.	• ممکن است از آنها خواسته شود که در ارزیابی تاثیر تغییرات بر سیستم کنترل داخلی به مدیریت کمک کنند. • برای انطباق با تغییرات نیاز دارند که فعال باشند. • به طور منظم تغییرات مربوط به ریسک‌های قانونی، نظارتی و تطبیق سازمان را پایش و بررسی می‌کند.	• تغییراتی را مشخص و ارزیابی می‌کند که می‌تواند به طور قابل ملاحظه‌ای بر سیستم کنترل داخلی در طی ارزیابی‌های دوره‌ای ریسک و در طول کار حسابرسی داخلی تاثیر بگذارند. • به طور منظم با مدیریت گفتگو می‌کند تا تغییرات و تاثیر آن بر ارزیابی ریسک سازمانی را پیش‌بینی کند.	• هیئت‌مدیره مسئولیت حصول اطمینان از اینکه مدیریت فرآیندهایی را برای تشخیص و ارزیابی تغییراتی ایجاد نموده که می‌تواند تاثیر قابل ملاحظه‌ای بر سیستم کنترل داخلی داشته باشند را دارد.

اصل ۱۰. سازمان فعالیت‌های کنترلی را انتخاب و توسعه می‌دهد که به کاهش ریسک‌های دستیابی به اهداف تا سطوح قابل‌قبول کمک می‌کند.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
• برای اجرای رویه‌های ریسک و کنترل بر یک مبنای روزانه، کنترل‌های داخلی موثر را حفظ می‌کند. مدیریت عملیاتی ریسک‌ها را تشخیص، ارزیابی، کنترل، و کاهش می‌دهد، توسعه و اجرای سیاست‌ها و رویه‌های داخلی را هدایت می‌کند و اطمینان می‌دهد که فعالیت‌ها با اهداف و مقاصد تعیین‌شده سازگار هستند. مدیران سطح میانی از طریق یک ساختار مسئولیت‌پذیری آبشاری، رویه‌های دقیقی را طراحی و اجرا می‌کنند که به عنوان کنترل‌ها و نظارت بر اجرای آن رویه‌ها توسط کارکنان خود، عمل می‌کنند. • به طور طبیعی به عنوان اولین خط دفاعی عمل می‌کند زیرا کنترل‌ها در سیستم‌ها و فرآیندهای تحت هدایت مدیریت عملیاتی طراحی می‌شوند. باید کنترل‌های مدیریتی و نظارتی کافی برای اطمینان از تطبیق و برجسته نمودن نارسایی‌های کنترلی، فرآیندهای ناکافی و رویدادهای غیرمنتظره، وجود داشته باشند.	• کارکردها در خط دوم دفاعی معمولاً مسئول نظارت بر کنترل‌های خاص از طرف مدیریت هستند. • همانطور که توسط مدیریت تعیین شده است، افراد در خط دوم دفاعی نیز ممکن است در انتخاب و توسعه کنترل‌های خاص شرکت نمایند؛ با وجود این، مدیریت مسئولیت سیستم کنترل‌های داخلی را حفظ می‌کند.	• این اطمینان را ارائه می‌دهد که کنترل‌های اعمال شده توسط مدیریت به طور مناسب طراحی شده، به طور موثر اجرا می‌شوند، و به گونه‌ای عمل می‌کنند که برای کاهش ریسک‌های دستیابی به اهداف تا سطوح قابل قبول در نظر گرفته شده‌اند. • پیشنهادهایی را برای بهبود کارایی و اثربخشی کنترل‌های داخلی ارائه می‌کند؛ با وجود این، مدیریت مسئولیت سیستم کنترل‌های داخلی را حفظ می‌کند.	• هیئت‌مدیره اطلاعات را ارزیابی می‌نماید و نظارتی را برای کمک به حصول اطمینان از اینکه سیستم کنترل داخلی مدیریت برای کاهش ریسک‌های دستیابی به اهداف تا سطوح قابل قبول کافی است، فراهم می‌کند.

اصل ۱۱. سازمان فعالیت‌های کنترلی کلی بر روی فناوری را برای حمایت از دستیابی به اهداف، انتخاب و توسعه می‌دهد.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
• فعالیت‌های کنترلی مرتبط با فناوری را طراحی و اجرا می‌کند. این موضوع شامل ایجاد و اطلاع‌رسانی خط‌مشی‌ها و رویه‌های مربوط به فناوری و حصول اطمینان از اینکه کنترل‌های فناوری اطلاعات برای حمایت از دستیابی به اهداف کافی هستند، می‌شود. • فرآیندهایی را برای پایش و ارزیابی آسیب‌پذیری در برابر ریسک در حال توسعه مرتبط با فناوری جدید و نوظهور، ایجاد می‌کند.	• افراد در خط دوم دفاعی اغلب وظایفی در رابطه با نظارت بر کنترل‌های فناوری خاص بر عهده دارند. • گروه‌هایی مانند بخش‌های امنیت اطلاعات نیز ممکن است نقش‌های مهمی در انتخاب، توسعه، و حفظ کنترل‌ها بر فناوری، که توسط مدیریت تعیین می‌شود، ایفا کنند.	• ارزیابی می‌کند که آیا فرآیندهای راهبری فناوری اطلاعات سازمان از استراتژی‌ها و اهداف سازمان پشتیبانی می‌کند یا خیر. • در مورد کارایی، اثربخشی، و کامل بودن کنترل‌های فناوری، اطمینان‌هایی را ارائه می‌کند، و در صورت لزوم، ممکن است بهبودهایی را برای فعالیت‌های کنترلی خاص پیشنهاد کند. • برای حفظ استقلال و بی‌طرفی حسابرسی داخلی، حسابرسان داخلی معمولاً فعالیت‌های کنترلی عمومی بر روی فناوری را انتخاب یا تعیین نمی‌کنند؛ با وجود این، آنها ممکن است توصیه‌هایی در مورد کنترل‌های فناوری ارائه دهند. • حسابرسان داخلی به منظور انجام کارهای محوله باید دانش کافی از ریسک‌ها و کنترل‌های کلیدی فناوری اطلاعات داشته باشند. با وجود این، از همه حسابرسان داخلی انتظار نمی‌رود که از تخصص یک حسابرس داخلی برخوردار باشند که مسئولیت اصلی آن حسابرسی فناوری اطلاعات است.	• هیئت‌مدیره مسئولیت های نظارتی قابل توجهی در رابطه با هدایت، ارزیابی، و نظارت بر کنترل‌ها دارد. نقش نظارتی هیئت‌مدیره باید جنبه‌هایی از راهبری فناوری اطلاعات مانند موارد زیر را دربرگیرد - ساختارهای سازمانی و راهبری. - رهبری و پشتیبانی اجرایی. - برنامه‌ریزی استراتژیک و عملیاتی. - ارائه خدمات و اندازه‌گیری. - سازمان فناوری اطلاعات و مدیریت ریسک.

اصل ۱۲. سازمان فعالیت‌های کنترلی را از طریق خط‌مشی‌های تعیین‌کننده آنچه که مورد انتظار است و رویه‌هایی که سیاست‌ها را عملی نموده، به کار می‌گیرد.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
• فعالیت‌های کنترلی را برقرار می‌کند که در فرآیندهای کسب‌وکار و فعالیت‌های روزانه کارکنان از طریق خط‌مشی‌های تعیین‌کننده انتظارات و رویه‌های مربوط که اقدامات را مشخص می‌کنند، به کار گرفته می‌شوند. • مسئولیت و پاسخگویی را برای فعالیت‌های کنترلی با مدیریت (یا سایر کارکنان تعیین شده) واحد تجاری یا عملکردی که ریسک‌های مربوط در آن وجود دارد، برقرار می‌کند. • اطمینان می‌دهد که کارکنان با صلاحیت و با اختیارات کافی، فعالیت‌های کنترلی را با دقت و تمرکز مستمر، به موقع و طبق خط‌مشی‌ها و رویه‌ها، اجرا می‌کنند. • اطمینان می‌دهد که کارکنان مسئول در مورد موضوعات مشخص شده در نتیجه اجرای فعالیت‌های کنترلی، بررسی و اقدام می‌کنند. • فعالیت‌های کنترلی را به صورت دوره‌ای بررسی نموده تا مربوط بودن مستمر آنها را تعیین، و در صورت لزوم آنها را به‌روزرسانی کند.	• بر تطبیق آنها با خط‌مشی‌ها و رویه‌های خاص تعیین شده توسط مدیریت، نظارت می‌کند. • به مدیریت در تدوین و اطلاع‌رسانی خط‌مشی‌ها و رویه‌ها کمک می‌کند. • اطمینان حاصل می‌کند که ریسک‌ها در رابطه با اشتهای ریسک تعیین شده سازمان، پایش می‌شوند.	• در مورد طراحی و پیاده‌سازی خط‌مشی‌ها، رویه‌ها و سایر کنترل‌ها اطمینان‌بخشی می‌کند. • پیشنهادهایی در رابطه با خط‌مشی‌ها و رویه‌ها ارائه می‌کند اما معمولاً دارای اختیاری برای طراحی یا اجرای خط‌مشی‌ها و رویه‌ها برای عملیات خارج از فعالیت حسابرسی داخلی نیست.	• هیئت‌مدیره برای اطمینان از وجود یک سیستم قوی از خط‌مشی‌ها و رویه‌ها برای هدایت عملیات، نظارت نموده و به حصول اطمینان از دستیابی به اهداف کمک می‌کند.

اصل ۱۳. سازمان اطلاعات مربوط و با کیفیت را برای پشتیبانی از عملکرد کنترل داخلی به دست آورده یا ایجاد و استفاده می‌کند.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
• داده‌ها را به منظور نظارت بر فعالیت‌های روزانه، به اشتراک‌گذاری اطلاعات در سراسر، بالا، و پایین سازمان، ایجاد و حفظ می‌کند. • هزینه‌ها و مزایا را در نظر می‌گیرد، و اطمینان حاصل می‌کند که ماهیت، کمیت، و دقت اطلاعات اطلاع‌رسانی شده متناسب با اهداف بوده و از دستیابی به اهداف پشتیبانی می‌کند. • قابلیت اطمینان و درستی اطلاعات یک مسئولیت مدیریت است. این مسئولیت شامل تمام اطلاعات حیاتی سازمان صرفنظر از نحوه ذخیره‌سازی آنها می‌شود. قابلیت اطمینان و درستی اطلاعات شامل صحت، کامل بودن و امنیت است.	• اطلاعات را از سراسر سازمان برای استفاده در فعالیت‌های نظارتی گردآوری می‌کند.	• در مورد قابلیت اطمینان و درستی اطلاعات و ریسک‌های مرتبط با آن اطمینان بخشی می‌کند. این موضوع شامل ریسک‌های درون و برون سازمانی، و آسیب‌پذیری‌های مرتبط با روابط سازمان با واحدهای تجاری برون‌سازمانی می‌شود. • به طور دوره‌ای قابلیت اطمینان و شیوه‌های یکپارچگی اطلاعات سازمان را ارزیابی می‌کند و در صورت لزوم، بهبودها یا اجرای، کنترل‌ها و محافظت‌های جدید را پیشنهاد می‌دهد. چنین ارزیابی‌هایی می‌توانند به عنوان کارهای مستقل جداگانه انجام شوند یا در سایر حسابرسی‌ها یا کارهایی که به عنوان بخشی از برنامه حسابرسی داخلی انجام می‌شوند، ادغام گردند. • تعیین می‌کند که آیا نقص قابلیت اطمینان و درستی اطلاعات و شرایطی که ممکن است تهدیدی برای سازمان باشد، به سرعت به مدیریت ارشد، هیئت‌مدیره و فعالیت حسابرسی داخلی اعلام می‌شود یا خیر.	• مدیریت ارشد و هیئت‌مدیره اطلاعات را برای تصمیم‌گیری به منظور نظارت بر موفقیت سازمان، پیش‌بینی ریسک‌ها، و برقراری ارتباط با ذینفعان برون‌سازمانی مانند سرمایه‌گذاران، به کار می‌گیرند. • به صورت دوره‌ای گزارش‌هایی در مورد عملیات و اثربخشی سیستم کنترل داخلی سازمان، دریافت می‌کند.

اصل ۱۴. سازمان اطلاعات، از جمله اهداف و مسئولیت‌های کنترل داخلی که برای پشتیبانی از عملکرد آن ضروری است را به صورت داخلی اطلاع‌رسانی می‌کند.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
• فرآیندهایی را برای اطلاع‌رسانی اطلاعات مورد نیاز ایجاد و حفظ می‌کند تا همه کارکنان بتوانند مسئولیت‌های کنترل داخلی خود را درک نموده و انجام دهند. • اطلاعات کافی را به هیئت‌مدیره منتقل می‌کند تا آنها را قادر سازد نقش‌های خود را با توجه به اهداف واحد تجاری ایفا کنند. • مجاری ارتباطی جداگانه‌ای مانند خطوط تماس برای افشای تخلفات را ایجاد می‌کند، که به عنوان سازوکارهای ایمن برای فعال نمودن ارتباطات ناشناس یا محرمانه در زمانی که مجاری عادی غیرفعال یا غیرموثر هستند، عمل می‌کنند.	• بر اطلاعات مربوط به کنترل‌های خاص، نظارت، و آنها را جمع‌آوری می‌کند، و خلاصه‌ای از اطلاعات مذکور را به خطوط اول و سوم دفاعی و هیئت‌مدیره اطلاع‌رسانی می‌کند. • ممکن است مسئول نظارت بر مجاری ارتباطی جداگانه مانند خطوط تماس برای افشای تخلفات، باشد.	• در مورد کامل بودن، صحت، و کیفیت اطلاع‌رسانی در راستای نیازهای هیئت‌مدیره و مدیریت ارشد اطمینان‌بخشی می‌کند.	• هیئت‌مدیره فضای [اخلاقی] مورد انتظار خود را در سراسر سازمان، ایجاد و اطلاع‌رسانی می‌کند. • هیئت‌مدیره و مدیریت ارشد باید در مورد ماهیت اطلاع‌رسانی مورد انتظار از افراد در هر خط دفاعی، رهنمود ارائه دهند.

اصل ۱۵. سازمان در رابطه با موضوعاتی که بر عملکرد کنترل داخلی تاثیر می‌گذارد، با اشخاص برون‌سازمانی گفتگو می‌کند.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
• اطمینان حاصل می‌کند که فرآیندهایی برای اطلاع‌رسانی اطلاعات مربوط و به موقع به اشخاص برون‌سازمانی از جمله سهامداران، شرکا، مالکان، ناظران، مشتریان، و تحلیلگران مالی و سایر اشخاص برون‌سازمانی، وجود دارد. • مجاری ارتباطی باز را ایجاد و تضمین می‌کند تا اجازه ورود به مشتریان، مصرف‌کنندگان، تامین‌کنندگان، حسابرسان مستقل، ناظران، تحلیلگران مالی، و سایرین داده شود، و اطلاعات مربوط را به مدیریت و هیئت‌مدیره ارائه دهد. • اطلاعات مربوط را از ارزیابی‌های انجام شده توسط اشخاص برون‌سازمانی به هیئت‌مدیره اطلاع‌رسانی می‌کند. • روش‌های ارتباطی مربوط را انتخاب نموده و اطمینان می‌دهد که روش مزبور، زمانبندی، مخاطب، و ماهیت ارتباط و الزامات و انتظارات قانونی، نظارتی و امانتداری را در نظر می‌گیرد. • سیاست‌های مناسبی را برای رسیدگی به عواملی مانند مجوز لازم برای گزارشگری اطلاعات به خارج از سازمان ایجاد می‌کند؛ دستورالعمل‌های مربوط به اطلاعات مجاز و غیرمجاز که ممکن است گزارش شوند؛ افراد برون‌سازمانی مجاز به دریافت اطلاعات و انواع اطلاعاتی که ممکن است آنها دریافت کنند؛ مقررات مربوط به حریم خصوصی، الزامات نظارتی، و ملاحظات قانونی برای گزارشگری اطلاعات به خارج از سازمان؛ و ماهیت اطمینان‌بخشی‌ها، توصیه‌ها، پیشنهادها، اظهارنظرها، رهنمودها، و سایر اطلاعاتی که ممکن است در انتقال اطلاعات به خارج از سازمان گنجانده شوند.	• به استثنای برخی ارتباطات با ناظران، حسابرسان مستقل، و سایر گروه‌های خاص، معمولاً خط دوم دفاعی با اشخاص برون‌سازمانی در رابطه با موضوعات موثر بر عملکرد کنترل داخلی، ارتباط برقرار نمی‌کنند. • اگر سازمان به صورت برون‌سازمانی در مورد کنترل‌های داخلی خود گزارش دهد، عملکردهای خط دوم دفاعی، نتایج فعالیت‌های خود را در حمایت از نظرهای مدیریت، به مدیریت ارائه می‌دهد.	• اطمینان می‌دهد که اطلاع‌رسانی‌های ضروری دیگران صحیح است. • معمولاً واحد حسابرسی داخلی با اشخاص برون‌سازمانی در رابطه با موضوعات موثر بر عملکرد کنترل داخلی، گفتگو نمی‌کند.	• هیئت‌مدیره باید اطلاعات و گزارش‌هایی را از مدیریت در مورد عملکرد و اثربخشی کنترل داخلی و مبنای اظهارنظرهای مدیریت قبل از ارتباط با اشخاص برون‌سازمانی، دریافت کند. • هیئت‌مدیره باید دیدگاه‌ها و اظهارنظرهای خود را که در هر گزارشگری برون‌سازمانی در مورد سیستم‌های کنترلی سازمان، گنجانده می‌شود را با حسابرسان مستقل مورد بحث قرار دهد.

اصل ۱۶. سازمان ارزیابی‌های مستمر و/یا جداگانه را انتخاب، توسعه و اجرا می‌کند تا مطمئن شود که آیا اجزای کنترل داخلی وجود داشته و عمل می‌کنند یا خیر.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
• با در نظر گرفتن نرخ تغییر در واحد تجاری و فرآیندهای کسب و کار، و تغییر دامنه و فراوانی ارزیابی‌های جداگانه وابسته به ریسک، توازنی از ارزیابی‌های مستمر و جداگانه را انتخاب و ایجاد می‌کند. (این ارزیابی‌ها ممکن است توسط خط دوم دفاعی انجام شود.) • اطمینان حاصل می‌کند که ارزیابی‌کنندگانی که ارزیابی‌های مستمر و جداگانه را انجام می‌دهند، دانش کافی برای درک آنچه در حال ارزیابی است، دارند. • از طراحی و وضعیت فعلی سیستم کنترل داخلی می‌توان برای ایجاد یک مبنا برای ارزیابی‌های مستمر و جداگانه استفاده نمود. • به طور دوره‌ای عملکرد فعالیت‌های مدیریت ریسک سازمان را به هیئت‌مدیره گزارش می‌دهد.	• ارزیابی‌های مستمر و جداگانه را برای نظارت بر وضعیت اجزای مختلف سیستم کنترل داخلی طبق دستور مدیریت، انجام می‌دهد. • ارزیابی‌های مستمر و جداگانه را برای نظارت بر اینکه آیا دستیابی به اهداف در محدوده توان ریسک‌پذیری تعیین شده است یا خیر، انجام می‌دهد.	• این اطمینان را فراهم می‌کند که ارزیابی‌های مدیریتی مستمر در فرآیندهای کسب‌وکار گنجانده شده و در صورت لزوم با شرایط متغیر، تعدیل می‌شوند. • اطمینان می‌دهد که اطلاعات فراهم شده توسط ارزیابی‌های مدیریت، به طور منصفانه و صحیح ارائه شده است. • اطمینان می‌دهد که سیستم کنترل داخلی طبق انتظار عمل می‌کند و ریسک‌ها در چارچوب اشتهای ریسک و توان ریسک‌پذیری سازمان مدیریت می‌شوند.	• هیئت‌مدیره نظارت را بر عهده دارد و مدیریت را برای انتخاب، توسعه، و انجام ارزیابی‌هایی از اجزای کنترل داخلی، مسئول می‌داند. • گزارش‌های دوره‌ای در مورد ریسک سازمان و اثربخشی فعالیت‌های مدیریت ریسک آن را دریافت می‌کند.

اصل ۱۷. سازمان نارسایی‌های کنترل داخلی را ارزیابی و به موقع به آن دسته از اشخاصی که مسئول انجام اقدامات اصلاحی هستند، از جمله مدیریت ارشد و هیئت‌مدیره، در صورت لزوم اطلاع‌رسانی می‌کند.

خط اول دفاعی (مالکان ریسک/مدیران)	خط دوم دفاعی (ریسک، کنترل، و تطبیق)	خط سوم دفاعی (حسابرسی داخلی)	سایر
• اطلاعات مربوط به نارسایی‌ها را به اشخاصی که مسئول انجام اقدامات اصلاحی هستند و در صورت لزوم به مدیریت ارشد و هیئت‌مدیره، اطلاع‌رسانی می‌کند. • پیگیری می‌کند که آیا نارسایی‌ها به موقع برطرف شده‌اند یا خیر.	• افراد در خط دوم دفاعی ممکن است مسئولیت نظارت و گزارشگری در مورد انواع خاصی از نارسایی‌های کنترلی را به عهده داشته باشند.	• حسابرسان داخلی سیستمی را برای پایش وضعیت یافته‌ها و پیشنهادهای حسابرسی داخلی که به مدیریت اطلاع‌رسانی شده است، ایجاد و حفظ می‌کنند. این سیستم معمولاً به موارد زیر می‌پردازد: - چارچوب زمانی که در آن پاسخ مدیریت به مشاهدات و پیشنهادهای کار حسابرسی، مورد نیاز است. - ارزیابی پاسخ مدیریت. - تایید پاسخ (در صورت لزوم). - اجرای یک کار پیگیری (در صورت لزوم). - یک فرآیند که اطلاع‌رسانی پاسخ‌ها/اقدامات نامطلوب، از جمله مفروضات ریسک، را به سطوح مناسب مدیریت ارشد و هیئت‌مدیره، افزایش می‌دهد.	• هیئت‌مدیره باید اطمینان حاصل کند که اطلاعات مربوط به نارسایی‌های کنترلی را به موقع دریافت نموده و اقدامات اصلاحی به موقع و به میزان کافی به منظور پیگیری نارسایی‌های کنترلی عمده، صورت می‌پذیرد. • مدیریت و هیئت‌مدیره، در صورت لزوم، نتایج ارزیابی‌های مستمر و جداگانه را ارزیابی می‌کنند.

منبع:

- IIA (The Institute of Internal Auditors), July ۲۰۱۵, "Leveraging COSO Across the Three Lines of Defense".

مدل سه خط در راهبری و مدیریت ریسک

مرتضی اسدی **آرشینا منتظری**

مقدمه

سازمان‌ها تعهدات انسانی هستند، که در دنیایی به طور فزاینده نامطمئن، پیچیده، به هم پیوسته و متزلزل فعالیت می‌کنند. آنها اغلب دارای ذینفعان متعدد با منافع متنوع، قابل تغییر و گاهی اوقات متقابل می‌باشند. ذینفعان نظارت سازمانی را به یک هیئت مدیره (ارکان راهبری) واگذار می‌کنند، که به نوبه خود منابع و اختیارات را به مدیریت برای انجام اقدامات مناسب از جمله مدیریت ریسک تفویض می‌کند.

به این دلایل و موارد دیگر، سازمان‌ها به ساختارها و فرآیندهای مؤثر برای دستیابی به اهداف و در عین حال حمایت از راهبری قوی و مدیریت ریسک نیاز دارند. از آنجایی که هیئت مدیره گزارش‌هایی را از مدیریت در مورد فعالیت‌ها، نتایج و پیش‌بینی‌ها دریافت می‌کند، هم هیئت مدیره و هم مدیریت به حسابرسی داخلی برای ارائه اطمینان و مشاوره مستقل و عینی در مورد همه موضوعات و ترویج و تسهیل نوآوری و بهبود تکیه می‌کنند. هیئت مدیره در نهایت در قبال راهبری خود پاسخگو است که از طریق اعمال و رفتارهای هیئت مدیره و همچنین مدیریت و حسابرسی داخلی به دست می‌آید.

مدل سه خط یک رویکرد مدیریت ریسک برای کمک به سازمان ها برای تشخیص و مدیریت موثر ریسک‌ها با ایجاد سه خط دفاعی متمایز است. این مدل که توسط انجمن حسابرسان داخلی (IIA) آمریکا تعریف شده است، بر این ایده استوار است که این سه خط دفاعی با هم کار می‌کنند تا ساختاری پیرامون مدیریت ریسک و راهبری داخلی ایجاد کنند.

پس از بحران مالی ۲۰۰۷-۲۰۰۸، که تا حدی ناشی از شکست های گسترده عدم توجه کافی، به مدیریت ریسک بود محبوبیت این مدل به شدت افزایش یافت. در پاسخ به این بحران، قانون‌گذاران و مقامات نظارتی توجه فزاینده‌ای به مدیر ارشد ریسک (CRO)[1] و کمیته ریسک هیئت مدیره داشتند و شروع به توصیه مدل سه خط کردند. بیشتر کارهای آکادمیک روی این مدل نیز پس از بحران انجام شد و قبل از آن بسیاری از متخصصان مدیریت ریسک فقط نام مدل را شنیده بودند. از سال ۲۰۱۰، مدل سه خط دفاعی به طور گسترده به عنوان یک چارچوب معتبر برای مدیریت ریسک عملیاتی و مالی واحدهای اقتصادی در سراسر جهان پذیرفته شده است. هدف این مدل تعیین موقعیت‌ها و نقش‌های جدید در یک سازمان به خودی خود نبود، بلکه برای ارزیابی ساختارهای موجود برای اطمینان از پوشش کافی و استقلال برای ارائه مدیریت ریسک مؤثر بود. حتی

[1] chief risk officer

اگر امروز در برابر مدل، مورد ارزیابی قرار نگیرید، این یک چارچوب مفید برای سنجش بلوغ سازمان شما و آماده سازی خود برای بررسی‌های پیشرفته‌تر در حین رشد است.

در یک نظرسنجی که در سال ۲۰۱۵ از متخصصان حسابرسی داخلی در ۱۶۶ کشور (n = ۱۴۵۱۸) انجام شد اکثر پاسخ‌دهندگان (۷۵٪) گزارش دادند که سازمان آنها از مدل سه خط که توسط انجمن حسابرسان داخلی ارایه شده است پیروی می‌کند. همچنین نظرسنجی که از مدیران ارشد حسابرسی [۲](CAEs) در اتریش، آلمان و سوئیس (n = ۴۱۵) انجام شد، اکثر پاسخ‌دهندگان (۸۸٪) گزارش دادند که آنها این مدل را پیاده سازی کرده‌اند، به ویژه اینکه نرخ پذیرش در موسسات مالی بالا و تا ۹۶٪ می‌رسد.

مدل سه خط چیست و چه هدفی دارد؟

مدل «سه خط دفاعی» در سال ۲۰۱۳ توسط انجمن حسابرسان داخلی آمریکا برای روشن کردن نقش‌ها و مسئولیت ها برای مدیریت و کنترل موثر ریسک‌ها معرفی شد. خود نقش‌ها قبل از سال ۲۰۱۳ وجود داشته‌اند، اما به طور رسمی تعریف نشده و در سطح جزئیات مورد بحث قرار نگرفته بودند. مدل سه خط دفاعی توسط انجمن حسابرسان داخلی در مقاله‌ای با عنوان "سه خط دفاعی در کنترل و مدیریت ریسک موثر" در ژانویه ۲۰۱۳ ارایه شده است.

در سال ۲۰۲۰، در میان ریسک‌های رو به افزایش شرکت‌ها در سرتاسر جهان، مدل «سه خط دفاعی» تکامل یافت و به عنوان مدل «سه خط» اصلاح شد. مدل "سه خط" نقش ها و مسئولیت های حسابرسان داخلی را بهتر روشن می‌کند و همچنین به نیاز حسابرسان داخلی برای ارائه مشاوره برای دستیابی به اهداف کسب و کار علاوه بر نقش موجود دفاعی خود می پردازد. این موضوع در مدل قبلی نامشخص بود، جایی که مدیریت ممکن است تنها مسئول کمک به کسب و کار در دستیابی به اهداف استراتژیک خود باشد. مدل به روز شده «سه خط» نیاز عملکردهای مدیریت ریسک برای همسویی با اهداف کسب و کار سازمان را برطرف می کند. این یک تغییر قابل توجه از مدل قبلی «سه خط دفاعی» است.

تغییر اخیر به «سه خط» برای روشن کردن نقش‌ها و مسئولیت‌ها گامی در جهت درست است. رویکرد اصول محور مدل جدید یک تغییر اساسی نسبت به مدل قبلی است، زیرا اطمینان می‌دهد که تصمیمات مدیریت ریسک سازگار هستند. همچنین اطمینان می‌دهد که مدل به طور مداوم در طول زمان بهبود می‌یابد.

مدل جدید «سه خط» همچنین بر نقش حسابرس داخلی تکامل یافته به عنوان یک توانمند برای دستیابی به اهداف کسب و کار سازمان تأکید می‌کند. این مدل مشخص می‌کند که حسابرسی داخلی، همراه با سایر خطوط، باید برای ایجاد و محافظت از ارزش کسب و کار با هم کار کنند. کار باید با منافع اولویت بندی شده سازمان همسو باشد. این علاوه بر نقش سنتی موجود حسابرسان داخلی برای کمک به ارزیابی و اعتبارسنجی مستقل ریسک‌های سازمانی است.

[۲] Chief Audit Executives

این مدل به وضوح نقش‌هایی از جمله نظارت توسط هیئت مدیره، مدیریت ارشد و اطمینان بخشی مستقل را تعریف می کند.

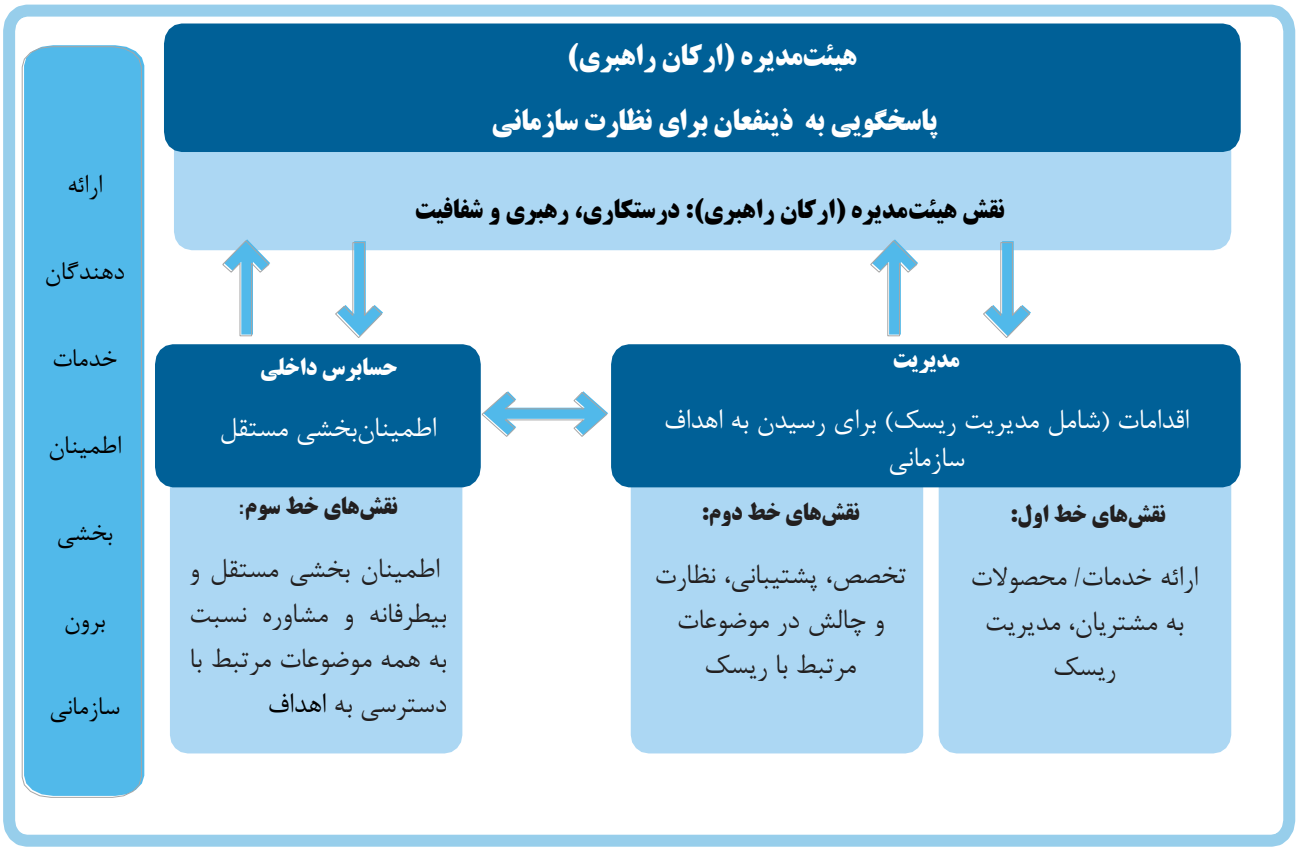
این مدل برای همه سازمان‌ها کاربرد دارد و می‌تواند موارد زیر را انجام دهد:

- سازگار شدن برای رسیدن به اهداف سازمانی.
- تمرکز بر مدیریت ریسک برای دستیابی و رسیدن به اهداف.
- شناخت نقش ها و مسئولیت ها در همه موقعیت ها در مدل و رابطه آنها با یکدیگر.
- اجرای اقدامات برای همسویی فعالیت ها و اهداف با منافع ذینفعان.

تشریح مدل سه خط

مدل سه خط از یک رویکرد جامع برای مدیریت ریسک استفاده می کند. واحدهای کسب و کار، تطبیق، حسابرسی و دیگر کارکنان مدیریت ریسک از جمله گروه هایی هستند که سه خط دفاعی را تشکیل می‌دهند و هر کدام کارکرد خاصی دارند. در اینجا به تفکیک این سه خط می‌پردازیم:

مدل سه خط انجمن حسابرسان داخلی (IIA)



موضوع کلیدی:

پاسخگویی، گزارش‌دهی

تفویض اختیار، هدایت، منابع، نظارت

همسویی، هماهنگی ارتباطی ، همکاری

- **خط اول.** مدیریت، مالکان بخش یا فرآیند - یا هر کسی که در خط مقدم است - اولین خط دفاعی است. مسئولیت اصلی آنها کنترل و در اختیار گرفتن ریسک‌های مرتبط با فعالیت‌های روزانه است. آنها همچنین کنترل‌ها را اجرا و سیاست‌های داخلی را توسعه می‌دهند، بر اجرای خط مشی کارکنان نظارت دارند و عوامل ریسک را با تصمیم گیری‌ها و اقدامات، نظارت می‌کنند.
- **خط دوم.** خط دوم دفاعی شامل مدیریت ریسک و حوزه‌های رعایت است - مانند مدیر ریسک، مسئول تطبیق یا مسئول امنیت اطلاعات. خط دوم مناطق دفاعی، وظیفه اجرای برنامه مدیریت ریسک شرکت و نظارت بر روند و اجرای این سیاست ها را بر عهده دارند. آنها همچنین ریسک های نوظهور را در عملیات روزانه کسب و کار مشخص می‌کنند.
- **خط سوم.** خط سوم دفاعی شامل حسابرسان داخلی و برون سازمانی است. مسئولیت اصلی آنها اطمینان از اثربخشی خط اول و دوم دفاعی است. آنها همچنین طراحی و اجرای برنامه مدیریت ریسک را بررسی و ارزیابی می‌کنند. حسابرسان داخلی معمولاً در مورد طراحی و عملیات مدیریت ریسک شرکت به هیئت مدیره، ناظران و حسابرسان مستقل گزارش می‌دهند.

مدل سه خط به طور گسترده توسط بسیاری از صنایع به عنوان مدل راهبری ریسک پذیرفته شده است. اجرای آن با توجه به صنایع و اندازه شرکت‌ها متفاوت است.

نقش‌های کلیدی در مدل سه خط

مدل سه خط، تقسیم روشنی از نقش‌ها و مسئولیت‌ها را برای پاسخگویی و شفافیت ایجاد می‌کند. انجمن حسابرسان داخلی موارد زیر را به عنوان نقش‌های کلیدی در مدل همراه با تفکیک مسئولیت‌ها در هر نقش فهرست می‌کند. سازمان‌ها ممکن است در توزیع مسئولیت‌ها متفاوت باشند، اما انجمن حسابرسان داخلی این بررسی‌های سطح بالا را برای هر حوزه ارائه می‌کند:

هیئت‌مدیره (ارکان راهبری)

هیئت‌مدیره مسئولیت مدیریت سازمان را از طرف ذینفعان می‌پذیرد. مسئولیت‌ها شامل موارد زیر است:

- درگیرکردن ذینفعان برای نظارت بر منافع‌شان.
- حفظ اطلاع‌رسانی باز در مورد دستاوردهای هدف.
- پرورش فرهنگ جامع نگری و مسئولیت پذیری.
- ایجاد اشتهای ریسک سازمان و نظارت بر مدیریت ریسک از جمله کنترل‌های داخلی.
- نظارت بر الزامات اخلاقی، حقوقی و قانونی.
- ایجاد و مدیریت فرآیند حسابرسی داخلی مستقل.

نقش‌های مدیریت در خط اول

نقش‌های مدیریت در خط اول، هدایت و سوق‌دادن تمام اقدامات برنامه در محل، از جمله مدیریت ریسک‌ها و به کارگیری منابع برای اهداف ریسک سازمان است. مسئولیت‌ها شامل موارد زیر است:

- حفظ ارتباط با هیئت مدیره و گزارش تمامی ریسک‌ها از جمله نتایج برنامه ریزی شده، واقعی و مورد انتظار در رابطه با اهداف شرکت.
- ایجاد و مدیریت چارچوب‌ها و رویه‌های مناسب برای مدیریت عملیات و ریسک. این شامل کنترل‌های داخلی می‌شود.
- اطمینان از رعایت اصول اخلاقی و قوانین و مقررات.

نقش‌های مدیریت در خط دوم

نقش‌های مدیریت در خط دوم، ارایه پشتیبانی و تخصص برای نظارت بر مدیریت ریسک است. مسئولیت‌ها شامل موارد زیر است:

- ایجاد فرآیندها، سیستم‌ها و نهادهای مداوم برای بهبود فرآیند مدیریت ریسک.
- دستیابی به اهداف مدیریت ریسک مانند کنترل داخلی، امنیت اطلاعات، پایداری و تضمین کیفیت.
- تحقیق و گزارش اثربخشی مدیریت ریسک از جمله کنترل داخلی.

نقش‌های حسابرسی داخلی

نقش‌های حسابرسی داخلی، مسئولیت اصلی مدیریت ریسک را در مقابل هیئت مدیره بر عهده دارد. مسئولیت‌ها شامل موارد زیر است:

- ارائه اطمینان‌بخشی مستقل و بی‌طرفانه در مورد اثربخشی کنترل‌های مدیریت ریسک به مدیریت و هیئت‌مدیره.
- اطلاع‌رسانی مسائل مربوط به استقلال و بی‌طرفی برنامه مدیریت ریسک به هیئت‌مدیره.
- انجام اقدامات مناسب برای قراردادن محافظت در محل، در صورت لزوم.

ارائه‌دهندگان خدمات اطمینان‌بخشی مستقل (حسابرسان مستقل، ناظران و ...)

این نقش‌ها کمک بیشتری برای محافظت از منافع ذینفعان و رعایت مقررات ارائه می‌کنند. مسئولیت‌ها شامل موارد زیر است:

- بررسی رعایت قوانین و مقررات و آگاهی در مورد قوانین و مقررات جدید مؤثر بر سازمان.
- افزودن منابع خارجی برای پاسخگویی به درخواست‌های مدیریت و هیئت مدیره برای کمک به منابع داخلی.

شش اصل راهنمای مدل سه خط

برای بهینه‌سازی اثربخشی مدل سه خط، سازمان‌ها باید رویکردی مبتنی بر اصول را اتخاذ کنند. انجمن حسابرسان داخلی این شش اصل را برای راهنمایی مدل سه خط دفاعی سازمان برای مدیریت ریسک فهرست می‌کند:

۱. راهبری. راهبری به ذینفعان پاسخگو است و رهبری و یکپارچگی سازمان را شکل می‌دهد. سازمان می‌تواند برای سلامت سازمان و ذینفعان خود تصمیمات مبتنی بر ریسک را اتخاذ کند. استفاده از توصیه‌های عملکرد حسابرسی داخلی به تشویق توسعه مداوم این روش‌ها، به مدیریت ریسک کمک می‌کند.

۲. نقش‌های هیئت‌مدیره. هیئت مدیره اطمینان حاصل می‌کند که رویه‌ها و چارچوب‌های لازم برای حفظ منافع ذینفعان وجود دارد. آنها همچنین اطمینان حاصل می‌کنند که استانداردهای اخلاقی و قانونی رعایت می‌شوند.

۳. مدیریت و نقش‌های خط اول و دوم. نقش‌های خط اول باید اطمینان بخشی کنند که محصولات یا خدمات به طور ایمن به مشتریان ارائه می‌شوند. نقش‌های خط دوم با ارائه تخصص و نظارت و مدیریت هر گونه مسائل نظارتی یا رفتار غیراخلاقی به مدیریت ریسک کمک می‌کند. خط دوم، مسئولیت گسترده‌تری مانند مدیریت ریسک سازمانی را ارائه می‌دهد، اما خط اول مسئولیت مدیریت ریسک در سطح بالاتر را بر عهده دارد.

۴. نقش‌های خط سوم. حسابرسی داخلی اطمینان عینی می‌دهد که ابتکارات مدیریت ریسک موثر است. حسابرسی داخلی از سیستم های مستقل و تخصصی با رویکردهایی برای بررسی فرآیندهای مدیریت ریسک استفاده می‌کند. نقش‌های خط سوم یافته‌ها را به مدیریت و هیئت مدیره گزارش می‌کنند تا هر گونه بهبود مورد نیاز را انجام دهند.

۵. استقلال خط سوم. حسابرسی داخلی یک نهاد مستقل است که اعتبار و اختیار یافته‌های خود را فراهم می‌کند. حسابرسی داخلی با مدیریت مرتبط نیست، بنابراین می‌تواند یافته‌هایی را ارائه دهد که عاری از سوگیری باشد تا از هرگونه دخالت در برنامه ریزی سازمانی جلوگیری کند.

۶. ایجاد و پشتیبانی از ارزش. هدف اصلی همکاری همه این نقش‌ها، اولویت بندی منافع ذینفعان است. آنها فعالیت‌ها را از طریق همکاری و ارتباط هماهنگ می‌کنند. تمام تصمیمات مبتنی بر ریسک باید با همسویی این حوزه‌ها شفاف و قابل اعتماد باشد.

مزایای مدل سه خط

مدل سه خط به سازمان‌ها کمک می‌کند تا به طور فعالانه ریسک‌ها را با افزایش راهبری و انعطاف‌پذیری مدیریت و رسیدگی کنند. این مدل به سازمان کمک می‌کند تا مبنایی برای رشد و موفقیت ایجاد کند. برخی از مهمترین مزایای این مدل عبارتند از:

• **پاسخگویی روشن**. تمام نقش‌ها و مسئولیت‌ها برای هر یک از خطوط مختلف دفاعی تعریف شده است. وظایف مدیریت ریسک نیز به طور مناسب تخصیص داده شده است، بنابراین مالکیت واضحی از ریسک‌ها در تمام سطوح سازمان وجود دارد. این کمک می کند تا هر گونه شکاف در نظارت بر ریسک به حداقل برسد.

• **تحلیل عینی**. خط سوم ارزیابی‌های مستقل و عینی از اثربخشی فرآیندهای مدیریت ریسک را ارائه می‌دهد. دیدگاه مستقل به ذینفعان اطمینان می‌دهد که ریسک‌ها به اندازه کافی مدیریت می‌شوند. این دیدگاه همچنین بینش‌ها را برای بهبود مستمر مدیریت می‌کند.

• **بهبود ارتباطات**. مدل سه خط دفاعی ارتباطات ساختاریافته و همکاری را در خطوط مختلف دفاعی کمیته حسابرسی ترویج می‌دهد. به اشتراک گذاری اطلاعات، بینش‌ها و بهترین شیوه‌ها برای استراتژی مدیریت ریسک موثرتر برای کل سازمان را تشویق می‌کند.

• **افزایش راهبری**. عملکردهای مدیریت ریسک و تطبیق در خط دوم به ایجاد و اجرای فرآیندهای مدیریت ریسک سازگار کمک می‌کند. این اطمینان می‌دهد که سازمان از مقررات مربوط و استانداردهای صنعت پیروی می‌کند و ریسک‌های قانونی و اعتباری را به حداقل می‌رساند.

• **تخصیص کارآمد منابع**. توزیع مسئولیت‌های مدیریت ریسک در این سه خط اطمینان می‌دهد که سازمان‌ها منابع را به طور مؤثرتری تخصیص می‌دهند. کارکنان عملیاتی می‌توانند بر مدیریت ریسک روزانه و مدیریت ریسک اختصاص داده شده و متخصصان حسابرسی می توانند بر چشم انداز کلی ریسک نظارت کنند.

• **آگاهی کامل از ریسک**. این مدل به دیدگاه کل نگر از ریسک نگاه می‌کند و ریسک‌های استراتژیک و عملیاتی را در نظر می‌گیرد. با نگاه کردن به این ریسک‌ها از منظری جامع، سازمان می‌تواند به طور فعال هرگونه ریسک نوظهور را مدیریت کرده و روی فرصت‌ها سرمایه‌گذاری کند. این مدل همچنین فرهنگ تصمیم گیری آگاهانه از ریسک را تشویق می‌کند.

چالش‌های اثربخشی مدل

مزایای زیادی برای مدل سه خط وجود دارد، اما برخی از چالش‌ها و معایب بالقوه نیز وجود دارد. سازمان‌ها می‌توانند با برنامه ریزی دقیق، ارتباط مستمر و آموزش به این چالش‌ها رسیدگی کنند.

برخی از چالش‌های اثربخشی مدل سه خط شامل موارد زیر است:

- **شکاف مهارت ها و دانش**. کارکنان عملیاتی در خط اول دفاعی ممکن است فاقد مهارت و تخصص لازم برای مدیریت جامع ریسک باشند. سازمان ها ممکن است نیاز به ارائه آموزش و پشتیبانی برای اطمینان از تشخیص و کاهش ریسک موثر داشته باشند.
- **تمرکز بیش از حد بر رعایت (انطباق)**. ممکن است به جای مدیریت ریسک‌های خاص سازمان، ذهنیت بیشتری برای برآوردن الزامات نظارتی وجود داشته باشد.
- **مدیریت تغییر**. معرفی مدل سه خط مستلزم تلاش‌های مدیریت تغییر برای جلب رضایت کارکنان در تمام سطوح دفاعی است. برخی از کارمندان ممکن است در مقابل تغییر مقاومت کنند و اثربخشی مدل را زیر سوال ببرند.
- **تخصیص منابع**. برای به دست آوردن منابع کافی، سازمان‌ها باید مسئولیت‌های مدیریت ریسک را در خطوط مختلف توزیع کنند که به پرسنل، آموزش و فناوری نیاز دارد. یافتن تعداد مناسب منابع ممکن است یک چالش باشد اگر شرکت ها بخش ریسک و حسابرسی جداگانه نداشته باشند.
- **مالکیت ریسک**. ایجاد مالکیت واضح ریسک در خطوط مختلف ممکن است چالش برانگیز باشد. کارکنان خط اول دفاعی ممکن است نقش خود را در مدیریت ریسک به طور کامل قبول نکنند. این می‌تواند منجر به تشخیص و کاهش ناکافی ریسک شود.
- **مقیاس پذیری**. اجرای مدل سه خط در یک سازمان بزرگ با چشم انداز ریسک متنوع ممکن است چالش برانگیز باشد. ریسک‌های سازمان‌های بزرگ‌تر ممکن است دائماً تغییر کنند، بنابراین تطبیق مدل برای تناسب با نیازهای خاص سازمان ممکن است فرآیند پیچیده‌ای باشد.
- **گزارشگری**. سازمان‌ها باید چگونگی تعیین کمیت و ارزیابی اثربخشی تلاش های مدیریت ریسک هر خط را تعیین کنند. این معیارها باید ارزش فعالیت های مدیریت ریسک را به ذینفعان نشان دهد.

علاوه بر این، این مدل روابط گزارش‌دهی بازیگران مختلف را نشان می‌دهد، اما نکات مهمی وجود دارد که باید به آنها توجه کرد:

- رابطه بین مدیریت ارشد و هیئت‌مدیره (ارکان راهبری) در این مدل نامشخص است.
- این مدل بر روی نشان‌دادن ریسک‌ها (دفاع) متمرکز است و نه تحقق اهداف سازمانی.

- اگرچه تعامل پایین به بالا توسط حسابرسی داخلی با ارکان راهبری و مدیریت ارشد وجود دارد، اما تعامل بین حسابرسی داخلی و دو خط دیگر مشخص نیست.

با وجود محبوبیت مدل سه خط در بسیاری از صنایع، انتقاداتی نیز به این مدل وارد است. چهار نقطه ضعف و نارسایی در این مدل شناسایی شده است:

اول، آنها استدلال می کنند که انگیزه های ریسک پذیری در خط اول اغلب گمراه کننده است. زمانی که با جایگزینی بین ایجاد سود و کاهش ریسک مواجه می شوند، از لحاظ تاریخی انگیزه‌ای برای اولویت بندی ریسک های قبلی داشته اند،

دوم، اغلب عدم استقلال سازمانی برای وظایف خط دوم وجود دارد. آنها بیش از حد به افراد سودجو نزدیک هستند که می‌تواند منجر به اتخاذ نگرش های ریسک پذیرتر شود،

سوم، عملکردهای خط دوم اغلب فاقد مهارت و تخصص لازم برای به چالش کشیدن شیوه‌ها و کنترلها در خط اول هستند. و

چهارم، اثربخشی حسابرسی داخلی به دانش، مهارت و تجربه افراد بستگی دارد که ممکن است ناکافی باشد.

یکی دیگر از انتقادات رایج این است که این مدل احساس امنیت کاذبی را ارائه می دهد. به زبان ساده، «وقتی چندین نفر مسئول هستند در واقع هیچ کس مسئول نیست»[۳] انتقاد دیگر این است که این مدل بیش از حد دیوانسالارانه و پرهزینه است. لایه‌های نظارتی بیشتر ممکن است ریسک را کاهش دهد، اما منجر به هزینه برای کارآمدی مدل می‌شود. آخرین انتقاد این که مدل به جریان اطلاعات بین خطوط بستگی دارد، اما موانع زیادی برای این موضوع وجود دارد. به عنوان مثال، ممکن است خط دوم تشخیص ندهد که آنها فقط آنچه را که خط اول برای نشان دادن آنها انتخاب می کند، می‌بینند در حالی که این انتقادات کاستی‌های مربوط را مشخص می-کند و باید جدی گرفته شود، اما مدل را به عنوان یک کل زیر سوال نمی‌برد. علاوه بر این، مدل سه خط در طول سال ها بهبود یافته است. امروزه تمرکز بر افزایش اثربخشی مدل و پاسخ به انتقادات است.

با توجه به این انتقادات، چندین مدل جایگزین پیشنهاد شده است. به عنوان مثال، مدل چهار خط را برای پاسخگویی بهتر به نیازهای موسسات مالی پیشنهاد کردند. خط چهارم متشکل از مراجع نظارتی و حسابرسی مستقل است که قرار است با حسابرسی داخلی همکاری نزدیک داشته باشند. مثال دیگر مدل پنج خطی است که به تدریج توسط چندین محقق و سازمان توسعه یافت با این حال، تغییرات پیشنهادی لزوماً مدل را بهبود نمی بخشد و همچنین ممکن است افزودن خطوط بیشتر مدل را بیش از حد پیچیده و سخت کند و شرکت ها و ناظران در حال حاضر خواهان تغییرات ساختاری نیستند. همچنین شایان ذکر است که مدل‌های جایگزین به مراتب کمتر از مدل اصلی محبوبیت دارند.

[۳] when there are several people in charge—no one really is”

منابع:

١. The Institute of Internal Auditors (IIA)," **THE IIA'S THREE LINES MODEL** An update of the Three Lines of Defense" July ٢٠٢٠

https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-٢٠٢٠/three-lines-model-updated-english.pdf

٢. Amanda Hetler, **"three lines model",** August ٢٠٢٣
https://www.techtarget.com/searchcio/definition/three-lines-model

٣. Maris Sekar, "Machine Learning for Auditors(Automating Fraud Investigations Through Artificial Intelligence) ", Aprss,٢٠٢٢

٤. Jonas Schuett, Three lines of defense against risks from AI, Springer,٢٠٢٣

جادادن ملاحظات زیست‌محیطی، اجتماعی و راهبری (ESG) و پایداری در مدل سه خط

مرتضی اسدی **الهه مهدوی ثابت**

مقدمه

دنیا با سه چالش جهانی عمده مواجه است: شرایط اضطراری اقلیم، از بین رفتن طبیعت و افزایش نابرابری. هرکدام از چالش‌های فوق تهدیدی برای کسب‌وکار است، و رویدادهای دو سال گذشته — پاندمی جهانی، بی‌ثباتی جغرافیای سیاسی (ژئوپولتیکی)، تداوم حوادث شدید آب‌وهوایی و بحران تنوع زیستی — ارتباط متقابل فزآینده محیط عملیاتی ما را نشان داد.

نیاز مبرمی به ایجاد تغییر ذهنیت جامعه تجاری جهت مقابله با این چالش‌ها، تاب‌آوری بیشتر و سازمان‌های آینده‌نگر وجود دارد. انتظارات ذینفعان از کسب و کارها به شدت افزایش یافته و پیشرفت‌های به وجود آمده در عرصه نظارتی به این معنی است که کسب و کار باید با یک رویکرد عملی و امکان‌پذیر [به این موارد] پاسخ دهد. در این محیط بی‌ثبات و نامعلوم، نیاز به ساختارهای راهبری اثربخش و فرآیندهایی است که بتواند دستیابی به اهداف، که باید موضوعات کلیدی پایداری را هم دربرگیرد، میسر سازد.

در حالی که تغییرات اقلیمی همچنان در دستور کار شرکتی محکم باقی می‌ماند، اهمیت تلاش‌های تجاری در جهت جوامع منصف و طبیعت‌گرا[۱] در حال افزایش است. بدون طبیعت کاهش گازهای گلخانه‌ای تا حد نزدیک به صفر (صفر خالص[۲]) وجود ندارد. زمانی که با مدیران عامل و مدیران ارشد مالی صحبت می‌کنیم، دیگر این پرسش مطرح نیست که آیا آنها اقدام می‌کنند یا خیر، بلکه پرسش این است که آیا کسب و کار آنها باید بخشی از راه‌حل باشد یا خیر، و چگونه. برای این منظور، سازمان‌ها باید رویکردهای عملی و معتبری را در مدل‌های تجاری و زنجیره‌های تامین خود لحاظ کنند. موضوع مهم این است که مسائل پایداری بااهمیت در فرآیندهای تصمیم‌گیری تجاری لحاظ شوند و اینکه سازوکارهای راهبری برای اطمینان از نظارت موثر بر مدیریت ریسک و کنترل‌ها وجود داشته باشند.

در سال ۲۰۲۰، انجمن حسابرسان داخلی (IIA) مدل سه خط را بروزرسانی کرد تا شامل رویکردی مبتنی بر اصول بوده که با نیازهای سازمانی سازگار است. این مدل ریشه در راهبری دارد و نیاز به مدیریت ریسک و کنترل‌های قوی به عنوان بخش اساسی راهبری را تشدید می‌کند. مدل مذکور در شناسایی ساختارها و فرآیندهای مناسب به سازمان‌ها کمک می‌کند، بنحوی که این ساختارها و فرآیندها دستیابی به اهداف تجاری برای ایجاد و حفظ ارزش برای سازمان را به بهترین شکل پشتیبانی کنند.

---

[۱] Nature-Positive
[۲] Net-Zero

در سال ۲۰۲۱، شورای تجارت جهانی برای توسعه پایدار (WBCSD)[۳] و انجمن حسابرسان داخلی همکاری مشترکی را برای استفاده از دانش و تخصص هرکدام از این سازمان‌ها، ایجاد نمودند.
رهنمود مشترک حاصل به شرح زیر است:
۱. ملاحظات چگونگی جادادن ریسک‌ها و فرصت‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری در فرآیندهای سه خط برای اطمینان از مدیریت ریسک و نظارت داخلی کارآمد و اثربخش؛ و
۲. پیشنهادها و نمونه‌های عملی برای یکپارچه‌سازی ملاحظات پایداری در نقش‌ها و مسئولیت‌های کلیدی در درون سه خط.
مخاطب موردنظر این نوشتار رهنمودی عبارتند از هیئت‌مدیره‌های شرکت‌ها، نمایندگان تیم مدیران ارشد در درون شرکت‌های بزرگ، و مدیریت ارشد به منظور فراهم نمودن اطلاعات و درک نقش خطوط مربوط در نظارت بر اثربخشی مدیریت ریسک و فرآیندهای حسابرسی داخلی.

خلاصه اجرایی

در سال ۲۰۲۰، انجمن حسابرسان داخلی مدل سه خط را بروزرسانی کرد تا سازمان‌ها را به سمت راهبری موثر، مدیریت ریسک و کنترل‌های داخلی هدایت کند. مدل سه خط از زمان ارائه آن، به سازمان‌ها در تشخیص نقش‌های مناسب که می‌توانند از دستیابی به اهداف تجاری به بهترین شکل پشتیبانی کرده و در عین حال برای سازمان، و ذینفعان آن ارزش‌آفرینی نمایند، کمک کرده است.
رهنمود موجود در این نوشتار، که پیش‌نویس آن به طور مشترک از سوی شورای تجارت جهانی برای توسعه پایدار و انجمن حسابرسان داخلی نوشته شده است، عوامل درون‌سازمانی و برون‌سازمانی را که محرک یکپارچه‌سازی [ملاحظات] زیست‌محیطی، اجتماعی، راهبری و پایداری در تصمیم‌گیری است را برجسته می‌سازد. رهنمود مذکور پیشنهادهایی را در این مورد ارائه می‌دهد که چگونه باید این ملاحظات را در درون نقش‌ها و مسئولیت‌های کلیدی لحاظ نمود که کلیات آن در مدل سه خط آمده است، نظیر ارکان راهبری، مدیران اجرایی (نقش‌های خط اول و دوم) و حسابرسی داخلی.
طبق نسخه بازنگری شده مدل سه خط، که در این رهنمود ارائه شده است، برای نهادینه کردن ملاحظات زیست‌محیطی، اجتماعی، راهبری و پایداری، تمام نقش‌ها باید به‌گونه‌ای با یکدیگر کار کنند تا از راهبری خوب اطمینان حاصل شده و مدل کسب‌وکار را آینده‌نگر نماید.

- **ارکان راهبری** به نظارت و ایجاد سازوکارهای راهبری می‌پردازد که اهداف استراتژیک را با ملاحظات زیست‌محیطی، اجتماعی، راهبری و پایداری یکپارچه‌سازی می‌سازد. این سازوکارهای راهبری باعث آگاهی بیشتر ارکان راهبری و مشارکت فعالانه‌تر آن در استراتژی گزارشگری زیست‌محیطی، اجتماعی و راهبری شرکت و تاثیر عملیات کسب‌وکار بر مسائل زیست‌محیطی، اجتماعی و راهبری می‌شود. ارکان راهبری همچنین مسئول تشخیص و ارتباط با ذینفعان گوناگونی است که از عملیات شرکت تاثیر پذیرفته‌اند.

[۳] World Business Council for Sustainable Development

- **مدیران اجرایی** رویکرد حسابداری چند-سرمایه‌ای را برای تمام سرمایه‌های مالی و غیرمالی ایجاد می‌نمایند که مدل کسب‌وکار شرکت برای اطمینان از کارکرد اثربخش عملیات خود به آن نیاز دارد. مدیران اجرایی همچنین بر نحوه ارزیابی اهمیت نظارت دارند، که میان عملیات شرکت، تاثیر آنها بر مسائل زیست‌محیطی، اجتماعی و راهبری و مربوط بودن به ذینفعان کلیدی، پیوند برقرار می‌کند.

پیامد ارزیابی اهمیت — ماتریس اهمیت دوسویه — استراتژی مدیریت ریسک زیست‌محیطی، اجتماعی و راهبری را شکل می‌دهد و به سایر نقش‌ها کمک می‌کند تا زمینه در حال تکاملی را که کسب‌وکار در آن فعالیت می‌کند، درک کنند.

- **حسابرسی داخلی**، مستقل از ارکان راهبری و مدیران اجرایی، از قابلیت اتکای فرآیندهای کنترل داخلی برای افشای داده‌های زیست‌محیطی، اجتماعی، راهبری و گزارشگری، اطمینان حاصل می‌نماید.

به‌دلیل تنوع مدل‌های راهبری، نقش‌ها و سازمان‌ها، هر شرکت باید تصمیم بگیرد که چگونه این رهنمود را طبق نیازها، اهداف استراتژیک، فرهنگ، منابع و زمینه تجاری خود بکار گیرد. برای آنکه این رهنمود کاربرد هرچه وسیع‌تری داشته باشد، پیشنهادهای ارائه شده از بینش‌های ۱۲ شرکت، کارشناسان و نهادهای نظارتی فراهم آمده، که در مصاحبه‌هایی که راهنمای محتوای این گزارش بوده است، مشارکت داشته‌اند.

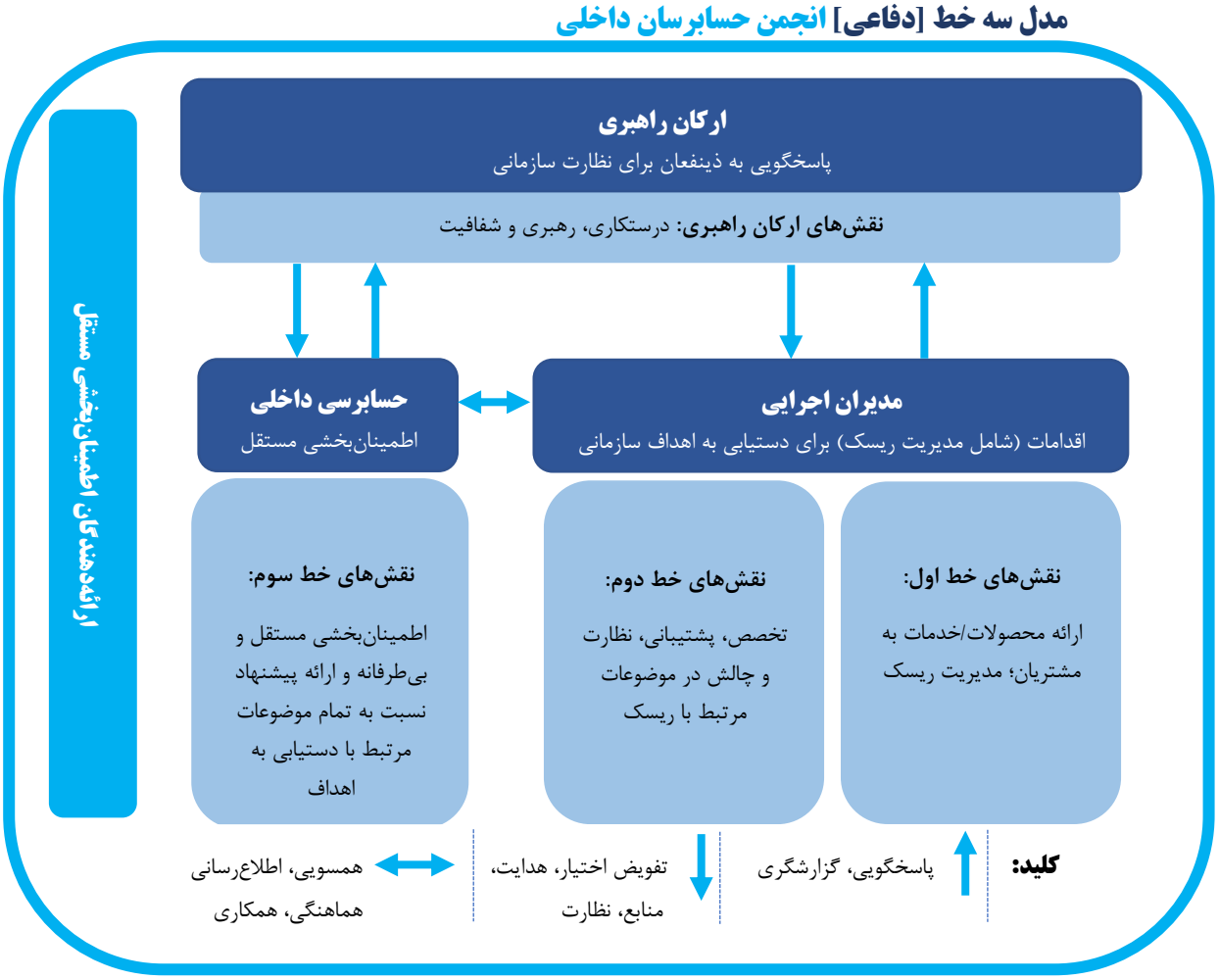
۱– مدل سه خط: بروزرسانی به‌موقع

مدل سه خط [دفاعی] انجمن حسابرسان داخلی به عنوان یکی از منابع مهم در راهبری موفق در جهان به رسمیت شناخته می‌شود. این مدل به سازمان‌ها در تشخیص ساختارها و فرآیندها برای مدیریت ریسک‌ها و دستیابی به اهداف، شامل ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری سازمان به بهترین شیوه کمک می‌کند. این مدل سه نقش اساسی را تعیین می‌کند که راهبری را در اولین سطح آن تعریف می‌نماید: پاسخگویی، اقدامات و اطمینان‌بخشی. مدل مذکور همچنین سه بازیگر اصلی را در راهبری مشخص می‌کند: ارکان راهبری، مدیران اجرایی و حسابرسی داخلی.

مسئولیت‌های خط اول عبارتند از فراهم آوردن محصولات و خدمات برای صاحبکاران یا مشتریان در انطباق با الزامات و انتظارات تعیین‌شده از سوی خط دوم، که مسئولیت نظارت، ارائه پیشنهاد و ارزیابی و اجرای فعالیت‌های مدیریت ریسک را به عهده دارد، و خط اول را، در صورت نیاز، به چالش می‌کشد. این نقش‌ها و مسئولیت‌ها مولفه‌های اساسی راهبری هستند که از سوی ارکان راهبری پشتیبانی می‌شوند، ارکان راهبری بطور قانونی مسئول پاسخگویی برای اقداماتی است که به مدیران اجرایی درخواست اجرای آنها را داده‌اند.

در اینجا یک منبع عینی و مستقل باید از تحقق موارد خواسته شده اطمینان بخشی ارایه دهد. بدون این اطمینان‌بخشی، راهبری وجود نخواهد داشت. در این مدل، حسابرسی داخلی به‌عنوان منبع هیئت‌مدیره برای اطمینان‌بخشی داخلی بی‌طرفانه، مستقل از مدیران اجرایی، مشخص شده است. فعالیت حسابرس داخلی همچنین از طریق اتکا و هماهنگی آنها می‌تواند در پشتیبانی از اطمینان‌بخشی مستقل، نقشی کلیدی را ایفا نماید.

شکل ۱: مدل سه خط انجمن حسابرسان داخلی



مدل سه خط بروزرسانی شده و نسخه ارتقایافته آن بسیار مورد توجه است.

این مدل در جولای سال ۲۰۲۰ بازنگری شد تا برخی از اصول بنیادین را شفاف‌سازی و تقویت نماید، دامنه آن را گسترش دهد، و توضیح دهد که نقش‌های سازمانی کلیدی چگونه با یکدیگر برای تسهیل راهبری و مدیریت ریسک قوی کار می‌کنند. تغییر نام مدل حاکی از تمرکز شفاف آن است. این مدل به‌جای آنکه صرفاً به عنوان ابزار دفاعی عمل کند — همانطور که از نام قدیمی می‌توان دریافت — سعی دارد نشان دهد ساختارها و فرآیندهای سازمان را چگونه باید طراحی کرد تا به‌جای تنها واکنش به شرایط، به آینده نظر داشته باشد. مدل مذکور همچنین بر نحوه کارکرد حسابرسی داخلی ورای تشخیص نگرانی‌ها تاکید می‌کند و توصیه‌ها و مشاوره آینده‌نگر در مورد مسائل کلیدی را در بر می‌گیرد.

مدل فعلی همچنین نقش‌های ضروری حسابرسی داخلی و هیئت‌مدیره در ملاحظات ریسک و نحوه تعامل خطوط سه‌گانه را بهتر نشان می‌دهد. این مدل شامل مفهوم بروزشده از ریسک است و تعریف بهتری از مسئولیت‌های مدیران اجرایی، حسابرسی داخلی و ارکان راهبری و تعاملات آنها را ارائه می‌دهد.

این تغییرات به‌موقع باعث ارتقای ارزش مدل در لحاظ نمودن ملاحظات پایداری می‌شود، و در همان حال، کسب‌وکارها را به سمت تاب‌آوری و آینده‌نگری حرکت می‌دهد.

۲– رابطه میان راهبری و کسب‌وکارهای آینده‌نگر

در سال ۲۰۲۱، شورای تجارت جهانی برای توسعه پایدار، چشم‌انداز ۲۰۵۰ را بروزرسانی نمود، در نسخه بروزرسانی شده یک چارچوب اقدام برای جهان تدوین شده است که بیش از ۹ میلیارد نفر، در محدودیت‌های سیاره‌ای، تا اواسط قرن، می‌توانند به خوبی زندگی کنند[۴]. این چشم‌انداز هنوز هم در دسترس است، اما ما باید سریع‌تر عمل کنیم و، در دهه پیش‌رو، لازم است که تمام کسب‌وکارها پایداری را در تمام جنبه‌های سیستم‌ها، فرآیندها و شیوه‌عمل‌های خود نهادینه سازند تا این چشم‌انداز را به حقیقت تبدیل نمایند.

راهبری یکی از فرآیندهای کلیدی است که به طور قابل‌ملاحظه‌ای نیاز به تکامل دارد. راهبری به عنوان مجموعه‌ای از فرآیندها تعریف می‌شود که اثربخشی کلی یک سازمان را تضمین می‌کند، و باید شامل نظارت بر مدیریت ریسک، کنترل‌ها و افشا باشد. با وجود این، در زمینه چشم‌انداز ۲۰۵۰، این راهبری باید شامل راهبری مسائل مرتبط با زیست‌محیطی، اجتماعی و راهبری، و نیز ملاحظات پایداری گسترده‌تر باشد.

راهبری موثر باعث ایجاد اطمینان ذینفعان و اعتماد آنها نسبت به تصمیمات، اقدامات، و نتایج شرکت در رسیدگی به اولویت‌ها و دستیابی به هدف شرکتی سازمان می‌شود. طبق تعریف پرفسور کولین مایر[۵]، هدف کسب‌وکار عبارت است از «تولید راه‌حل‌های سودمند برای مشکلات افراد و سیاره، و نه کسب سود از تولید مشکلات برای افراد و سیاره» است.

داشتن هدف و مدل کسب‌وکار که نقش شرکت در قبال افراد، سود و سیاره را نشان دهد به این معنی است که تصمیم‌گیری هیئت‌مدیره می‌تواند از موفقیت بلندمدت سازمان پشتیبانی کند.

مدل سه خط [دفاعی] به سازمان‌ها کمک می‌کند تا نقش‌های مورد نیاز برای راهبری موثر و مدیریت موضوعات با اهمیت زیست‌محیطی، اجتماعی و راهبری و نیز گزارشگری پایداری گسترده‌تر را در نظر بگیرند. این مدل شناخت عمیق‌تر این نقش‌ها و نحوه کار با یکدیگر را برای پشتیبانی از موفقیت سازمانی ترغیب می‌کند. سازمان‌ها می‌توانند مناسب‌ترین ساختارها برای نیازهای خود را بهتر تعیین کنند، و این مدل را در ارتباط با ملاحظات خاص خود — مقاصد، شرایط، فرهنگ، منابع — به‌عنوان شالوده ضروری برای مدیریت ریسک بکار گیرند.

برای آنکه بتوان کسب‌وکار را تاب‌آور و آینده‌نگر کرد، این ریسک‌ها را باید در برابر دورنمای به طور مداوم در حال تکامل، مدیریت نمود. استراتژی کسب‌وکار آینده‌نگر با اجماع علمی و اجتماعی در پیشرفت به سمت اقتصاد صفر خالص و طبیعت‌گرا مرتبط است. رویکرد فراگیری که ارزش را برای تمام ذینفعان در نظر گیرد، جهت مجوز اجتماعی شرکت برای عملیات از اهمیت اساسی برخوردار خواهد بود. در نظر نگرفتن ریسک‌ها و فرصت‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری ممکن است بر تاب‌آوری استراتژیک سازمان تاثیر بگذارد.

---

[۴] «خوب زندگی کردن» یعنی اینکه کرامت انسانی و حقوق هر کس محترم شمرده شود، نیازهای اولیه برآورده شود، و همگان از فرصت‌های برابر برخوردار باشند. و «در درون محدودیت‌های سیاره‌ای» به این معنی است که گرمایش جهانی بیش از $+1.5^{\circ}C$ نباشد، و سامانه‌های طبیعی به‌طور پایدار حفظ، ذخیره، و استفاده شوند. این همچنین بدان معنی است که در جوامع ظرفیت انطباقی کافی برای ساخت و حفظ تاب‌آوری در سیستم زمینی سالم و احیاکننده توسعه یافته باشد.

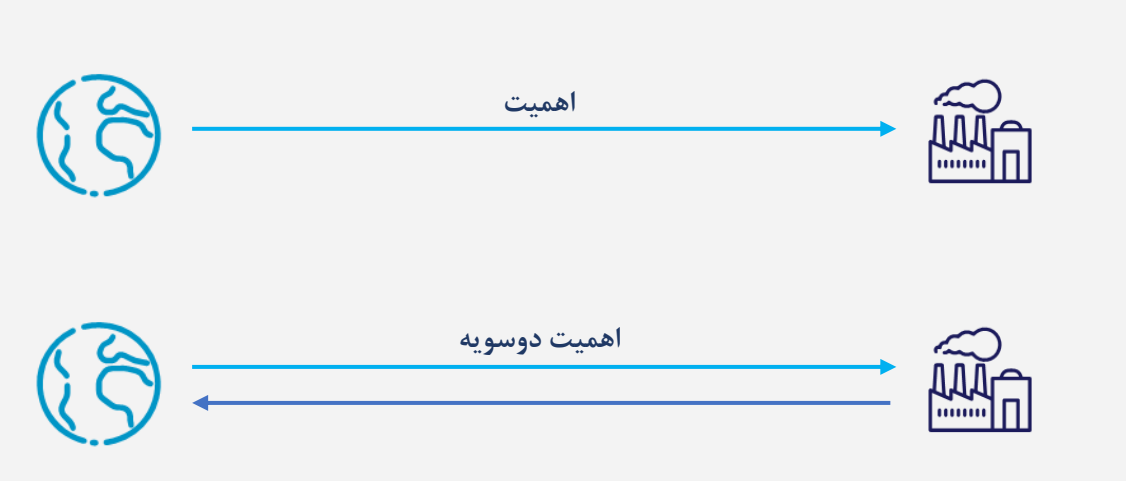
[۵] Colin Mayer

در همان زمان، مدل‌های کسب‌وکار باید ریسک شرکت در ارتباط با و یا ناشی از مسائل مرتبط با زیست‌محیطی، اجتماعی و راهبری را منعکس نموده و در نظر بگیرد، و رویکرد اهمیت دوسویه را بکار گیرد (گزارشگری غیرمالی بعلاوه گزارشگری مالی- به شکل ۲ مراجعه کنید). برای دستیابی به این هدف، شرکت‌ها باید تغییرات موردنیاز در درون فرآیندهای کسب‌وکار موجود را لحاظ کنند تا بهتر بتوانند [مسائل] زیست‌محیطی، اجتماعی و راهبری را در عملیات خود یکپارچه‌سازی نمایند.

در زمینه مدل سه خط [دفاعی]، این بدان معنی است که کلیه نقش‌ها با یکدیگر کار می‌کنند تا به صورت جمعی به ایجاد و محافظت از ارزش هنگامی که آنها با یکدیگر و با منافع اولویت‌بندی شده ذینفعان همسو هستند، یاری رسانند. انتقال به کسب‌وکار آینده‌نگر مستلزم روابط منابع طبیعی جدید به عنوان بخشی از مدل کسب‌وکار خواهد بود. طبیعت باید در کنار اقلیم مدنظر قرار گیرد، و زمانی که موضوع مدیریت ریسک‌ها و شناسایی فرصت‌های برابر بلندمدت و رشد پایدار مطرح می‌شود، باید آنها را برای کسب‌وکار حیاتی به شمار آورد.

شناخت این ریسک‌ها و فرصت‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری مستلزم آن خواهد بود که شرکت‌ها روابط داخلی و خارجی قوی داشته باشند و اطمینان یابند که کیفیت روابط از کسب‌وکارها در فرآیند ارزش‌آفرینی پشتیبانی خواهد کرد. این رهنمود از شرکت‌ها در فرآیند مذکور پشتیبانی خواهد کرد و نشان می‌دهد که چگونه باید ملاحظات پایداری و زیست‌محیطی، اجتماعی و راهبری را در درون شیوه‌عمل‌های تجاری یکپارچه‌سازی نمود.

شکل ۲: چشم‌انداز اهمیت دوسویه



چشم‌انداز اهمیت دوسویه بسط مفهوم کلیدی اهمیت در حسابداری است. مفهوم اهمیت دوسویه بیان می‌کند که شرکت‌ها باید گزارشگری در مورد مسائل پایداری را مدنظر قرار دهند (به عنوان مثال، اطلاعات مرتبط با اقلیم، که ممکن است بر عملکرد مالی شرکت تاثیر بگذارد و اطلاعات باید برای درک آثار بیرونی شرکت گزارش شوند).

ماخذ: گرافیک از «اهمیت دوسویه چیست و چرا مهم است»، موسسه پژوهشی گرانتام در مورد تغییرات اقلیم و محیط‌زیست، آوریل ۲۰۲۱، اخذ شده است.

۳– جادادن ملاحظات پایداری و زیست‌محیطی، اجتماعی و راهبری در شیوه‌های کسب‌وکار

پایداری در توصیف نحوه تاثیر سازمان‌ها بر جامعه و محیط‌زیست دیدگاه همه‌جانبه‌ای را دربردارد. پایداری به عنوان چترواژه‌ای برای توصیف اینکه یک سازمان چگونه می‌تواند در آستانه‌های زیست‌محیطی و محدوده‌های سیاره‌ای عمل کند، استفاده می‌شود. اقدامات مربوط به پایداری می‌تواند تلاش‌های یک شرکت برای کاهش تاثیرش در عین خلق ارزش در محیط بیرونی را شامل شود (به عنوان مثال، منبع‌یابی مسئولانه یا کشاورزی احیاکننده).

ملاحظات زیست‌محیطی، اجتماعی و راهبری (ESG) با پیش‌فرض تمرکز برون‌سازمانی به این نکته می‌پردازد که چگونه مسائل زیست‌محیطی، اجتماعی و راهبری (به عنوان مثال، تغییر اقلیم) از طریق ایجاد ریسک‌ها، تهدیدها و فرصت‌های جدید بر شرکت و ارزش آن تاثیر می‌گذارند. ملاحظات زیست‌محیطی، اجتماعی و راهبری داده‌محور هستند و از طریق کمی‌سازی تاثیر مسائل زیست‌محیطی، اجتماعی و راهبری بر عملکرد مالی، ذینفعان را از ارزش شرکت آگاه می‌کنند. این مسائل هنگام در نظر گرفتن ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری و یکپارچه‌سازی این موضوعات بااهمیت در فرایندهای کلیدی کسب‌وکار مورد استفاده قرار می‌گیرند.

برای درک اینکه در حال حاضر ملاحظات زیست‌محیطی، اجتماعی، راهبری و پایداری چگونه در شیوه‌های کسب‌وکار و نقش‌های تعیین شده در مدل سه خط یکپارچه‌سازی می‌شوند، شورای تجارت جهانی برای توسعه پایدار و انجمن حسابرسان داخلی، مجموعه مصاحبه‌هایی را با شرکت‌های پیشرو و کارشناسان در این زمینه انجام دادند. بینش‌های به‌دست‌آمده از این مصاحبه‌ها در سرتاسر این گزارش گنجانده شده و توصیه‌هایی را به منظور تکامل فرآیندهای آنها به شرکت‌ها ارائه می‌دهد.

این مصاحبه‌ها عوامل متعددی را برجسته می‌سازند که در میزان در نظر گرفتن ملاحظات زیست‌محیطی، اجتماعی، راهبری و پایداری در فرآیندهای تصمیم‌گیری یک شرکت نقش دارند. این عوامل در بخش‌های زیر از گزارش مورد بحث قرار می‌گیرند و عبارتند از:

۱. فرهنگ شرکتی و تغییر رفتار
۲. بلوغ یک سازمان
۳. چشم‌انداز افشای داوطلبانه و نظارتی در حال تکامل
٤. تعهدات طبیعت‌گرایی و صفر خالص
٥. اعمال فشار از سوی سرمایه‌گذاران و سایر ذینفعان
٦. اعتماد و شهرت

جادادن ملاحظات زیست‌محیطی، اجتماعی، راهبری و پایداری در شیوه‌های کسب‌وکار نیز یک فرصت است. اکنون شرکت‌های پیشرو دریافته‌اند که عمل کردن بر اساس طبیعت فرصتی است برای جلب اعتماد مشتریان، جامعه مدنی و سرمایه‌گذاران. سرمایه‌گذاران اصلی نیز متعهد می‌شوند که تا سال ۲۰۲۵ جنگل‌زدایی را از پرتفوی‌های خود حذف کنند؛ این اقدامات مبتنی بر طبیعت، کاهش خسارت ناشی از آسیب‌پذیری در برابر ریسک عمده را نشان داده و هزینه تامین سرمایه را کاهش می‌دهد.

۱. فرهنگ شرکتی و تغییر رفتار

فرهنگ شرکتی به مجموعه‌ای از باورها، رفتارها و شیوه‌های کسب‌وکار اشاره دارد که با هم تعیین می‌کنند که یک سازمان چگونه با بازیگران برون سازمانی تعامل دارد، معاملات تجاری بیرونی را مدیریت می‌کند و نگرش‌های خود نسبت به ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری را تعریف می‌نماید.

هدف و فرهنگ شرکتی به یک اندازه اهمیت دارند، چرا که توانایی رهبری را نشان می‌دهند و در عین حال مشخص می‌کنند که رهبری تا چه اندازه به عملکرد زیست‌محیطی، اجتماعی و راهبری در عملیات یک سازمان ارزش و بها می‌دهد. تغییر فرهنگ نهادینه شده شرکتی می‌تواند از دیدگاه راهبری چالش‌برانگیز باشد، زیرا شامل بررسی رفتارهای یکپارچه‌سازی شده در سراسر نقش‌ها و سطوح مختلف شرکتی است.

بینش‌های به دست آمده از مصاحبه‌ها نشان می‌دهد که هم عوامل محرک داخلی و هم عوامل بیرونی وجود دارند که می‌توانند تغییر رفتاری لازم برای توسعه یک فرهنگ شرکتی که برای عملکرد زیست‌محیطی، اجتماعی و راهبری ارزش قائل شود را تضمین کنند.[۶]

در داخل سازمان، فشار برای تغییر رفتار می‌تواند یک فرآیند بالا به پایین یا پایین به بالا باشد. زمانی که ارکان راهبری به طور مستقیم یکپارچه‌سازی ملاحظات زیست‌محیطی، اجتماعی، راهبری و پایداری را به عنوان بخشی از استراتژی شرکتی هدایت می‌کند، فرآیندی بالا به پایین است. به عنوان مثال، زمانی که سازمان می‌پذیرد که تغییر آب‌وهوا برای فعالیت‌هایش خطری کلیدی محسوب می‌شود، مدیریت مسائل با اهمیت زیست‌محیطی، اجتماعی و راهبری به بخشی از استراتژی شرکتی تبدیل می‌گردد، و پایداری بخشی از فرهنگ شرکت می‌شود.

با وجود این، زمانی که نقش‌های مدیریتی خط اول و دوم، ریسک‌ها و فرصت‌های جدید و نوظهور مرتبط با زیست‌محیطی، اجتماعی و راهبری که باید بخشی از استراتژی شرکتی شوند را مورد تاکید قرار می‌دهند، فرآیند تغییر رفتار می‌تواند پایین به بالا باشد. به عنوان مثال، ممکن است سازمان برای شناسایی ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری به جای اینکه بعد از وقوع ریسک‌ها واکنش نشان دهد و آنها را مدیریت کند، رویکردی پیشگیرانه و فعال اتخاذ نماید. در اینجا مدیران اجرایی باید در توسعه و پیاده‌سازی فرآیندهای لازم نقش ایفا کند.

در خارج از سازمان، این فشار می‌تواند از منابع مختلفی وارد شود، که در بخش‌های بعدی شرح داده شده است. این عوامل، از بیرون سازمان به طور مداوم نیاز به تغییر رفتار را در سازمان برمی‌انگیزند، و در نهایت به ایجاد فرهنگ شرکتی منتج می‌شوند که برای ملاحظات پایداری و زیست‌محیطی، اجتماعی و راهبری ارزش قائل بوده و آنها را ارتقا می‌دهد.

این عوامل رانشی، درونی و بیرونی، منافاتی با هم ندارند، بلکه می‌توانند به تغییر رفتاری مطلوبی منجر شوند که از فرهنگ شرکتی مرتبط با عملکرد زیست‌محیطی، اجتماعی و راهبری پشتیبانی کند. ارکان راهبری می‌توانند تضمین کنند که فرهنگ شرکتی، شیوه‌ها، منابع و فرآیندهایی را دربربگیرد که به مدیران اجرایی

---

[۶] مدل‌های متعددی برای تغییر رفتار وجود دارد که سازمان‌ها بتوانند اجرا کنند. متداول‌ترین عوامل رانشی (منابع و محرک‌های درونی و بیرونی) از: کرافورد هالینگورث و لیز بارکر، «مدل‌های تغییر رفتار: مروری بر دو نمونه از بهترین مدل‌های تغییر رفتار و نحوه بکارگیری آنها»، معماران رفتار، ۲۰۲۰. الهام گرفته شده است.

امکان دهد تا وضعیت موجود را به چالش کشیده، روندهای ریسک مرتبط با زیست‌محیطی، اجتماعی و راهبری را مورد تاکید قرار دهند و از مهارت‌ها، صلاحیت‌ها و انتقال دانش در سازمان اطمینان حاصل نمایند.

۲. بلوغ یک سازمان

برای بسیاری از شرکت‌ها، جادادن ملاحظات پایداری و زیست‌محیطی، اجتماعی و راهبری در سازمان‌هایشان هم چالش است هم فرصت. این بدان معنی است، زمانی که صحبت از شیوه‌های یکپارچه کسب‌وکار باشد، شرکت‌ها اغلب در سطوح متفاوتی از بلوغ قرار دارند. این بلوغ را می‌توان به عنوان مثال، از طریق شناسایی اینکه مسئولیت پایداری و پاسخگویی در برابر آن در کجای سازمان قرار دارد، یا ازطریق شناسایی همسویی بین موضوعات با اهمیت زیست‌محیطی، اجتماعی و راهبری و عوامل ریسک (به شکل ۳ مراجعه کنید)، کیفیت افشای زیست‌محیطی، اجتماعی و راهبری و نیز سازوکارهای راهبری و فرآیندهای نظارت و مدیریت این یکپارچگی، اندازه‌گیری نمود.

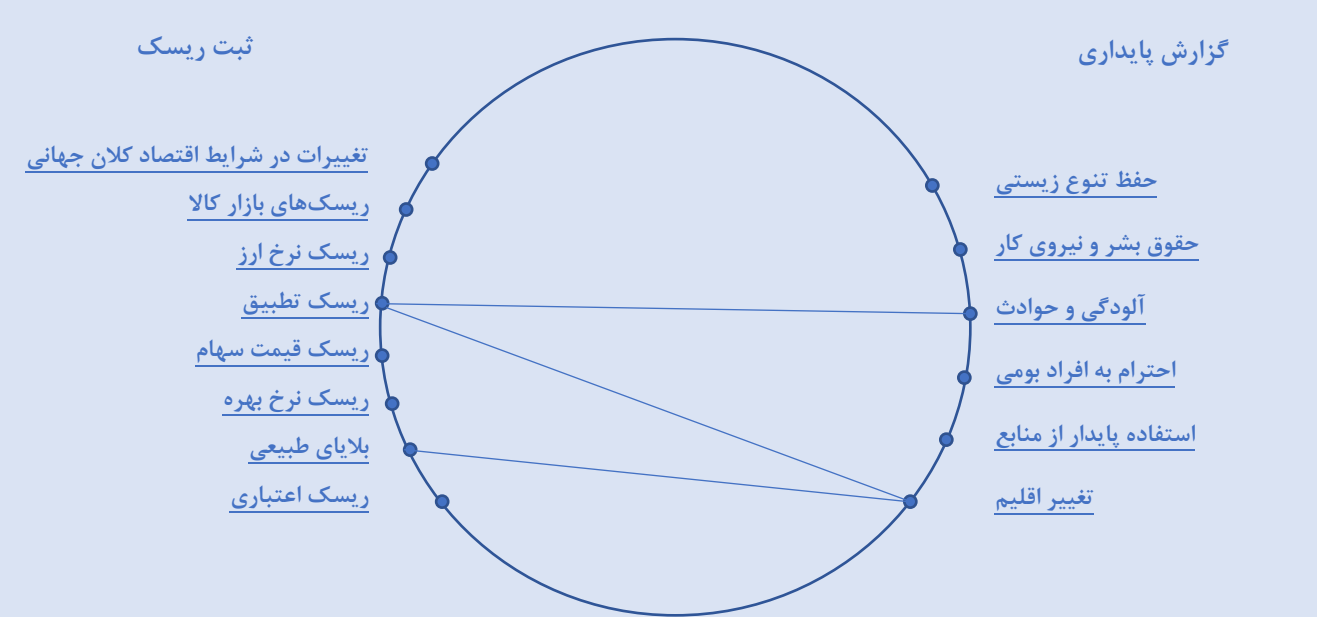
مصاحبه‌هایی که با شرکت‌ها انجام دادیم، چشم‌اندازهای جالب توجهی را درباره سطوح بلوغ ارائه می‌دهند:

۱. بنا به گفته برخی سازمان‌ها، شرکت‌ها معایب ناشی از پیشرو بودن در گنجاندن مسائل زیست‌محیطی، اجتماعی، راهبری و پایداری در راهبری، مدیریت ریسک و افشا را یک ریسک تصور می‌کنند. به عنوان مثال، افشای آثار عوامل پایداری و وابستگی‌های مربوط به آنها می‌تواند تهدیدی برای مزیت رقابتی محسوب شود. اینکه شرکت‌ها تا چه اندازه این فرصت‌ها را پیگیری کنند و ریسک‌ها را کاهش دهند، تا حد زیادی به وسیله فرهنگ شرکتی تعیین می‌شود.

۲. یکپارچه‌سازی [ملاحظات] زیست‌محیطی، اجتماعی، راهبری و پایداری برای ساختارهای سازمانی پیچیده، به عنوان مثال سازمان‌هایی که در مناطق و بخش‌های مختلف فعالیت می‌کنند و دارای واحدهای کسب‌وکاری متعددی هستند، به منابع و فرآیندهای راهبری پیچیده‌تری نیاز دارند. افشای دقیق‌تر [ملاحظات] زیست‌محیطی، اجتماعی و راهبری و مهارت‌های اولویت‌بندی ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری بسته به زمینه‌های محلی، متفاوت خواهد بود.

۳. پیشرو بودن در افشای [ملاحظات] زیست‌محیطی، اجتماعی و راهبری برای شرکت‌هایی که در مسیر پایداری خود مقدم‌تر بودند، نگرانی کمتری به همراه داشت؛ زیرا استراتژی‌های یکپارچه، فرآیندهای راهبری و سایر سیستم‌های درونی تصمیم‌گیری برای اطمینان از قابل‌اعتماد بودن و اعتبار هرگونه افشای [ملاحظات] زیست‌محیطی، اجتماعی و راهبری، در جای خود قرار داشتند.

شکل ۳: سطح هم‌سویی بین افشای پایداری و عوامل ریسک، یکی از روش‌های ارزیابی سطح یکپارچه‌سازی [ملاحظات] زیست‌محیطی، اجتماعی و راهبری است



ماخذ: پایداری و مدیریت ریسک سازمانی: نخستین گام به سوی یکپارچه‌سازی.

۳. چشم‌انداز افشای داوطلبانه و نظارتی در حال تکامل

افزایش ۱۰ برابری الزامات گزارشگری زیست‌محیطی، اجتماعی و راهبری بین سال‌های ۱۹۹۲ و ۲۰۱۷، همانطور که انتظار می‌رفت، منجر به این شده که کسب‌وکارها و نیز سرمایه‌گذاران خواستار همسویی و انسجام بیشتری در فضای گزارشگری زیست‌محیطی، اجتماعی و راهبری باشند. این تقاضای ثبات و همسویی مورد توجه استانداردگذاران در جهان قرار گرفته است. در چند ماه اخیر، هیئت استانداردهای بین‌المللی پایداری دو پیش‌نویس استاندارد را برای دریافت نظر مشاوره‌ای صادر نمود، کمیسیون بورس و اوراق بهادار ایالات متحده (SEC) قانون پیشنهادی افشای اقلیم را صادر کرده، و کمیسیون اروپا با تفویض مسئولیت به گروه مشاوره گزارشگری مالی اروپا (EFRAG)[۷] پیش‌نویس‌های میان‌مدتی را درباره استانداردهای گزارشگری پایداری در اروپا برای اخذ مشورت عمومی صادر کرده است.

بخش اعظم این فعالیت از تلاش کنونی سازمان‌های گزارشگری داوطلبانه مانند کارگروه افشای مالی مربوط به اقلیم (TCFD)[۸]، هیئت استانداردهای حسابداری پایداری، طرح گزارشگری جهانی و سایرین، الهام گرفته شده است.

این استانداردهای جدید و الزامی، ناشی از این موضوع است که ناظران (مقررات‌گذاران) و سایرین به طور فزاینده‌ای به این تشخیص رسیده‌اند که برای اطمینان از تبادل اثربخش اطلاعات مربوط به زیست‌محیطی، اجتماعی و راهبری بین شرکت‌ها و سرمایه‌گذارن، باید یک اتفاق نظر عمومی برای افشا ایجاد شود. بازارهای

[۷] European Financial Reporting Advisory Group
[۸] Task Force on Climate-Related Financial Disclosures

سرمایه برای درک خلق ارزش کوتاه‌مدت، میان‌مدت و بلندمدت شرکت‌ها به اطلاعات مفید و قابل‌اعتمادی برای تصمیم‌گیری درباره ریسک‌ها و فرصت‌های پایداری استراتژیک در این شرکت‌ها نیاز دارند.
علاوه بر افشای مالی مربوط به اقلیم، با تلاش کارگروه افشای مالی مربوط به طبیعت (TNFD)[۹]، بازار حرکت قدرتمندی را به سمت گنجاندن (طرح‌های) «طبیعت‌گرا» در افشای شرکتی آغاز کرده است. چارچوب بتای کارگروه افشای مالی مربوط به طبیعت مستلزم این است که کسب‌وکارها، ریسک‌ها و فرصت‌های مربوط به طبیعت را با استفاده از همان رویکرد چهار محوری کارگروه افشای مالی مربوط به طبیعت - راهبری، استراتژی، مدیریت ریسک و معیارها و اهداف - که بازارهای مالی و تجاری به طور گسترده‌ای آن را پذیرفته و اتخاذ کرده‌اند، افشا نمایند.

۴. تعهدات طبیعت‌گرا و صفر خالص

در مقابل چشم‌انداز نظارتی در حال تکامل و تغییر محیط عملیات، کسب‌وکارها برای تنظیم تعهدات طبیعت‌گرا و صفر خالص، تحت فشار قرار دارند. به عنوان مثال، در سال ۲۰۲۱، شورای تجارت جهانی برای توسعه پایدار شرایط عضویت خود را بروزرسانی کرد تا اعضا را ملزم کند که حداکثر تا سال ۲۰۵۰ به هدف به صفر رساندن انتشار گازهای گلخانه‌ای برسند و اهداف علمی و بلندپروازانه‌ای ایجاد کنند که به احیای طبیعت/تنوع زیستی تا سال ۲۰۵۰ کمک کند.
پویش پیشروی به سوی صفر سازمان ملل متحد نیز شرکت‌ها را وادار می‌کند که به اهداف دانش‌بنیان کاهش انتشار آلاینده‌ها پایبند باشند، اما تعهدات صفر خالص بدون عمل کردن بر اساس طبیعت محقق نخواهد شد. اگر جنگل‌زدایی در دهه جاری خاتمه نیابد و از حیات آبزیان که امروزه تا ۳۰٪ از کربن جهانی را جذب می‌کنند حفاظت نشود، مجموع ۷۰٪ از اهداف صفر خالص دولت‌ها و کسب‌وکارها دست‌نیافتنی تلقی می‌گردد.
با آغاز پیمان آب‌وهوایی (اقلیم) گلاسکو در بیست‌وششمین کنفرانس تغییرات آب‌وهوایی (اقلیمی) سازمان ملل متحد در سال ۲۰۲۱ (COP۲۶)[۱۰]، مشاهده شد که تمامی طرف‌ها موافق بودند که روی اقدام برای کاهش تغییرات اقلیمی، سازگاری با آن، تامین مالی و همکاری در زمینه تغییرات اقلیمی تمرکز کنند. به موازات آن، بیش از صد نفر از مدیران مجدداً بر تعهد خود به استفاده پایدار از زمین، و مدیریت پایدار و احیای جنگل‌ها و سایر اکوسیستم‌ها، نگهداری و حفاظت از آنها تاکید کردند.
این سطوح فزآینده بررسی‌های دقیق به این معنی است که صرف ایجاد تعهدات صفر خالص کافی نخواهد بود. شرکت‌ها باید در نظر بگیرند که چگونه اقدامات مربوط به اقلیم و طبیعت را در شیوه‌های کسب‌وکار خود نهادینه کنند و آن را به سطح زنجیره تامین خود برسانند. این تعهدات باید بر استراتژی‌های منسجم و اهداف میان‌مدت متکی باشند تا بتوان میزان پیشرفت را اندازه‌گیری نمود. لازم است که ساختارهای راهبری و مسئولیت‌های هیئت‌مدیره از نو تنظیم شود تا اطلاعات پیچیده‌تر در مورد زیست‌محیطی، اجتماعی و راهبری را شامل گردد و افشای شرکتی در زمینه زیست‌محیطی، اجتماعی و راهبری باید شفاف بوده و با سطوح بالایی از اطمینان‌بخشی برون‌سازمانی (مستقل)، همراه باشد.

---

[۹] Taskforce on Nature-related Financial Disclosures
[۱۰] ۲۰۲۱ United Nations Climate Change Conference

۵. اعمال فشار از سوی سرمایه‌گذاران و سایر ذینفعان

در سال ۲۰۲۲ لری فینک[۱۱]، رئیس هیئت‌مدیره و مدیرعامل شرکت بلک‌راک[۱۲]، در نامه خود به مدیران اجرایی بر ملاحظات سرمایه‌گذاری تمرکز کرد و بیان نمود: «تمرکز ما بر پایداری از آن جهت نیست که دوستدار محیط‌زیست هستیم، بلکه به این خاطر است که سرمایه‌دار و امانت‌دار مشتریان خود هستیم».

مطالبه سرمایه‌گذاران روشن است. در نظرسنجی اخیر موسسه پی‌دبلیوسی (PwC)[۱۳] از سرمایه‌گذاران، ۷۹٪ از پاسخ‌دهندگان ریسک‌ها و فرصت‌های زیست‌محیطی، اجتماعی و راهبری را به عنوان عامل مهمی در تصمیم‌گیری ذکر کردند، اما تنها ۳۳٪ معتقدند که کیفیت کنونی گزارشگری به طور متوسط خوب است. موسسه سرس[۱۴] از هیئت‌مدیره شرکت‌ها خواسته که «به طور نظام‌مند و دقیقی بر ریسک‌های زیست‌محیطی، اجتماعی و راهبری نظارت نمایند تا کسب‌وکارهای خود را در برابر بحران‌های جهانی رو به افزایش اقلیم و آب، مقاوم کنند».

هیئت‌مدیره در مدیریت [موقعیت‌های] چالش‌برانگیز نقشی حیاتی دارد و باید یکپارچه‌سازی اطلاعات مالی و غیرمالی را ترغیب کند تا بتوان داده‌های رتبه سرمایه‌گذاری را در اختیار ذینفعان قرار داد. اما در نقش نظارتی خود باید نگاهی فراتر از دیدگاه‌های سهامداران داشته باشد و در وهله اول مسئولیت خود برای درک دیدگاه‌های ذینفعان را در نظر بگیرد تا اطلاعات بهتری را در اختیار هیئت تصمیم‌گیری قرار دهد.

پژوهشی که توسط شورای تجارت جهانی برای توسعه پایدار و شرکت دی‌ان‌وی (DNV) انجام شده، نشان می‌دهد که فرهنگ شرکتی یکی از موانع کلیدی بر سر راه مشارکت اثربخش گروه‌های ذینفع است، چرا که در بسیاری از سازمان‌ها ارکان راهبری به طور مستقیم با گروه‌های مختلف ذینفع مشورت نمی‌کنند یا اینکه اصلا با آنها تعاملی ندارند. در این زمینه، مدیران اجرایی می‌توانند برای نمونه، از طریق ایجاد سازوکارهای راهبری برای رسمیت دادن به روابط عملیاتی بین ارکان راهبری و گروه‌های ذینفع، از این ارکان راهبری پشتیبانی نمایند.

۶. اعتماد و شهرت

برای اطمینان از اینکه تصمیم‌گیری‌های مربوط به کسب‌وکار و نیز تصمیمات سرمایه‌گذار بر تبادل اطلاعاتی که انجام می‌گیرد متکی باشد، ایجاد و حفظ اعتماد و اطمینان در ذینفعان ضروری است. در گزارش پایداری مدیران اجرایی (CxO)[۱۵] دیلویت[۱۶] در سال ۲۰۲۲: گسست بین هدف و تاثیر، ۹۷٪ از پاسخ‌دهندگان اعلام کردند که تغییرات اقلیم تاثیری منفی بر شرکت‌های آنها داشته است؛ از جمله نیمی از آنها که شاهد آثاری بر عملیات بودند، مانند اخلال‌ها در مدل‌های کسب‌وکار و شبکه‌های تامین.

آنها همچنین گزارش کردند که برای اقدام در مورد نگرانی‌های پایداری از سوی ذینفعان مختلف مانند ناظران (مقررات‌گذاران)، سهامداران، مصرف‌کنندگان و کارکنان، تحت فشار قرار دارند. ماهیت گسترده و پیچیده

---

[۱۱] Larry Fink
[۱۲] BlackRock
[۱۳] PricewaterhouseCoopers
[۱۴] Ceres
[۱۵] Chief Executive Officer
[۱۶] Deloitte

موضوعات پایداری به این معنی است که سازمان‌ها باید آگاهی را افزایش دهند و ظرفیت‌هایی را ایجاد کنند تا مطمئن شوند که بخش‌های مختلف درک می‌کنند که کسب‌وکار چگونه می‌تواند تحت تاثیر قرار گیرد.
مسئولیت شخصی اعضای هیئت‌مدیره، یکی دیگر از ملاحظات مهم است که بر فوریت در این حوزه تاکید می‌نماید.

در سال ۲۰۱۹، دادگاه عالی ایالت دل‌اِویر[۱۷] در حکم خود در مارچند[۱۸]، با اشاره به پرونده حساس شرکت Caremark، چنین اظهار کرد: «اگر شرکت مذکور یک چیز به ما آموخته باشد، این است که هیئت‌مدیره شرکت باید با حسن نیت تلاش کند تا وظایف مراقبتی خود را انجام دهد. ناتوانی در انجام این تلاش به منزله نقض وفاداری است».
ناتوانی هیئت‌مدیره در اجرای وظایف مراقبتی، طیف گسترده‌ای از ریسک‌ها را نه تنها بر سازمان بلکه بر خود هیئت‌مدیره نیز تحمیل می‌کند، ریسکی که مدیران باید نسبت به آن آگاه باشند.
افزایش دعاوی حقوقی مرتبط با زیست‌محیطی، اجتماعی و راهبری علیه شرکت‌ها و در برخی موارد علیه مدیران، به ویژه درخصوص موضوعات تغییر اقلیم و تعهدات صفر خالص، و نیز در مورد زنجیره تامین و مسائل حقوق بشری، و اختلافات غیررسمی مربوط به زیست‌محیطی، اجتماعی و راهبری در مورد اطلاعات افشا شده و اتهامات سبزشویی، همچنان به قوت خود باقی است.
پرداختن به موضوع پایداری دیگر یک «ایده‌آل»[۱۹] نیست، بلکه یکی از مسائل حیاتی کسب‌وکار است که باید در چارچوب‌های وسیع‌تر راهبری شرکتی، مدیریت ریسک، افشا و پاسخگویی شرکت مطرح گردد. بنابراین ضروری است که مدیران ماهیت وظیفه امانتداری خود را درک کنند و در شرایطی که دچار تردید می‌شوند، مشورت بگیرند.

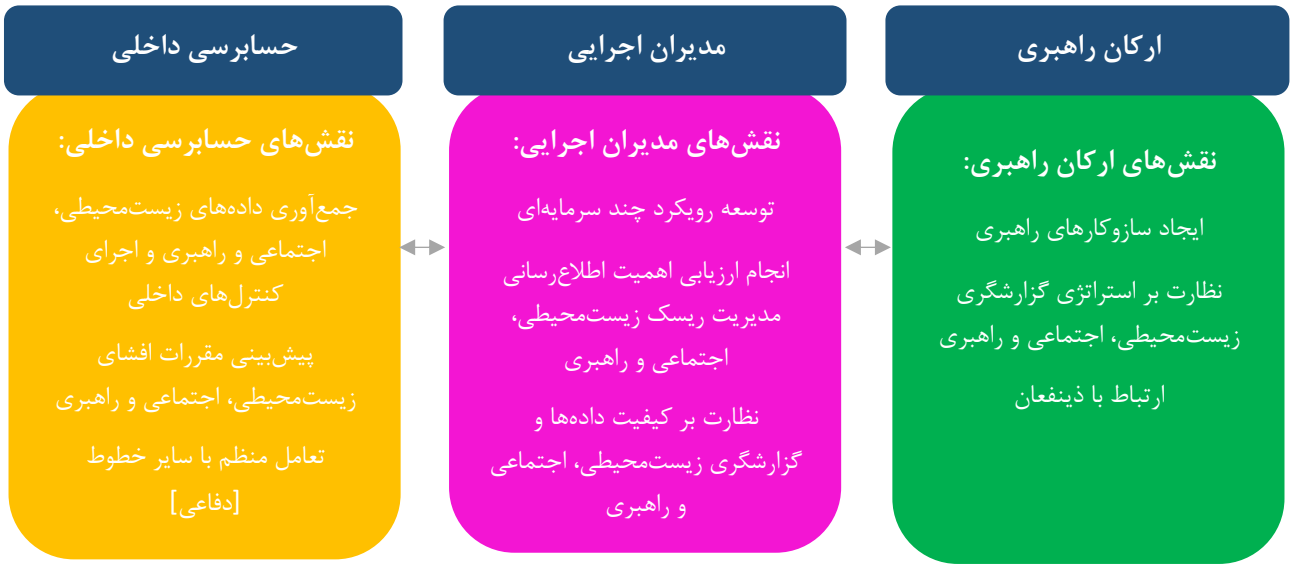
۴– مدل سه خط [دفاعی]: نقش‌ها و مسئولیت‌های مرتبط با پایداری

مدل سه خط، فرآیندها و نقش‌های روشنی را برای هدایت سازمان‌ها به سمت راهبری خوب مشخص می‌کند. سازمانی که متکی بر راهبری خوب است می‌تواند ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری را شناسایی، ارزیابی و اولویت‌بندی نموده و در تصمیم‌گیری لحاظ کند.
این بخش به نحوه یکپارچه‌سازی و جادادن ملاحظات پایداری و زیست‌محیطی، اجتماعی و راهبری در سه نقش مشخص‌شده در مدل [سه خط]: ارکان راهبری، مدیران اجرایی و حسابرسی داخلی، می‌پردازد.

[۱۷] Delaware Supreme Court
[۱۸] Marchand
[۱۹] Nice to Have

ملاحظات زیست‌محیطی، اجتماعی، راهبری و پایداری در مدل سه خط را می‌توان همانطور که در تصویر زیر تشریح شده، با هم یکپارچه نمود.

شکل ۴: اقدامات کلیدی نقش‌های مدل سه خط [دفاعی] از نظر ملاحظات پایداری و زیست‌محیطی، اجتماعی و راهبری



همه نقش‌ها اعم از ارکان راهبری، مدیران اجرایی، و حسابرسی داخلی، همکاری نزدیکی برای اطمینان از حلقه‌های بازخورد دارند. هر نقش به‌تفضیل در زیر توضیح داده شده است.

۱. نقش ارکان راهبری: سازوکارهای راهبری

ارکان راهبری، شامل هیئت‌مدیره، اهداف سازمانی، و نیز ساختارها و فرآیندهای مناسب برای راهبری موثر را تعریف می‌کند. ارکان راهبری، اهداف سازمانی را با مسائل زیست‌محیطی، اجتماعی و راهبری با اولویت بالا از نظر ذینفعان هماهنگ نموده، جهت حرکت را تعیین کرده و هدف شرکتی شامل ملاحظات گسترده‌تر پایداری را تعریف می‌کند. به‌ویژه، برای تحقق این هدف، ارکان راهبری باید بر سازوکارهای راهبری شامل ملاحظات پایداری و زیست‌محیطی، اجتماعی و راهبری، استراتژی گزارشگری زیست‌محیطی، اجتماعی و راهبری و تعامل با ذینفعان نظارت کند.

۱.۱. ایجاد سازوکارهای راهبری شامل ملاحظات پایداری و زیست‌محیطی، اجتماعی و راهبری

بسیاری از شرکت‌ها برای نظارت بر ملاحظات پایداری و زیست‌محیطی، اجتماعی و راهبری، سازوکارهای راهبری رسمی را ایجاد کرده‌اند. این امر ممکن است به یک کمیته اختصاصی، شامل اعضای هیئت‌مدیره، یا تحت مسئولیت یک کمیته از قبل موجود؛ به عنوان مثال مدیریت ریسک یا کمیته حسابرسی، محول شود. بین فعالیت حسابرسی داخلی و کمیته‌های حسابرسی رابطه‌ای وجود دارد، که فرصت اعمال نفوذ مسئولیت‌های نظارتی را فراهم می‌کند.

۱.۲. نظارت بر استراتژی گزارشگری زیست‌محیطی، اجتماعی و راهبری

ارکان راهبری مسئولیت‌هایی به منظور نظارت بر استراتژی گزارشگری زیست‌محیطی، اجتماعی و راهبری، اتخاذ تصمیم‌های گزارشگری یکپارچه استراتژیک و اتخاذ سیاست‌ها و فرآیندهایی برای تقویت راهبری از طریق مدیریت ریسک و کنترل‌های داخلی را نیز بر عهده دارند.

ارکان راهبری نقش مهمی در ایجاد و تشریح داده‌ها و شاخص‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری هم‌راستا با فرهنگ و هدف شرکتی دارد، تا به ذینفعان تعهد قوی به ملاحظات زیست‌محیطی، اجتماعی، راهبری و پایداری را نشان دهد.

مدیریت پایداری، دانش زیست‌محیطی، اجتماعی و راهبری لازم برای یکپارچه‌سازی شاخص‌های زیست‌محیطی، اجتماعی و راهبری مناسب با استراتژی کسب‌وکار و همچنین انتقال روندهای ریسک در حال تغییر مرتبط با زیست‌محیطی، اجتماعی و راهبری را به ارکان راهبری دارد.

مدل سه خط [دفاعی] برای اطمینان از ایجاد و حفظ ارزش‌های سازمان، نقش‌ها و مسئولیت‌های طرف‌های مختلف را در اجرای رویکرد یکپارچه مدیریت ریسک، کنترل‌های داخلی، افشا و اطمینان‌بخشی، شفاف می‌کند. هنگامی که ارکان راهبری درک و نظارت درستی نسبت به مساعدت این سه نقش برای ایجاد یک مدل کسب‌وکار انعطاف‌پذیر داشته باشند، انتظارات روشنی نسبت به چگونگی مشارکت هر یک از نقش‌ها در فرآیندهای گزارشگری و اطمینان‌بخشی برون سازمانی خواهند داشت.

۱.۳. تعامل با ذینفعان

بخش‌های مدیریت و پایداری در مقایسه با سایر نقش‌ها، از گذشته تاکنون تعامل بیشتری با ذینفعان سازمان داشته‌اند. ارتباط میان ارکان راهبری و ذینفعان ممکن است از طریق مجامع عمومی سالانه، گزارش‌های مدیریت یا از طریق گروه‌های مشاوره‌ای، پانل‌ها یا انجمن‌ها صورت گیرد. با وجود این، مشارکت ذینفعان باید فعالیت فرابخشی باشد که به ارکان راهبری برمی‌گردد. هنگامی که ارکان راهبری در تعامل منظم با ذینفعان باشند، و بالعکس، هر دو درک متقابلی از انتظارات و مواجهه سازمان با ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری، خواهند داشت.

بنابراین یکپارچه‌سازی مسائل زیست‌محیطی، اجتماعی و راهبری در قالب یک مدل کسب‌وکار پایدار و ارزیابی اهمیت به مشارکت ذینفعان بستگی دارد. هنگام تعامل با ذینفعان، ارکان راهبری باید از فراگیر و درهم‌تنیدگی ذینفعانی که برای سازمان مهم هستند، آگاه باشند.

۱.۳.۱. فراگیر بودن ذینفعان: تنوع بین گروه‌ها

ارکان راهبری باید از فراگیر بودن حداکثری مجموعه ذینفعان اطمینان حاصل کند. سازمان ابتدا باید آثار عملیات خود بر مسائل مختلف زیست‌محیطی، اجتماعی و راهبری (به عنوان مثال، تغییرات آب و هوا، تخریب اکوسیستم، کمبود آب) را تعریف و کمی‌سازی نموده و سپس وابستگی‌های بین هر مسئله زیست‌محیطی، اجتماعی و راهبری و یک یا چند گروه از ذینفعان مربوط را ترسیم کند. سازمان با ترسیم این وابستگی‌ها می‌تواند نحوه انتشار ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری را با توجه به سطح به هم

پیوستگی این ریسک‌ها درک نماید. رویکرد ذینفع-فراگیر ممکن است شامل سازمان‌های غیردولتی (NGOs)[۲۰]، جوامع محلی، مشتریان، کارفرمایان و تامین‌کنندگان باشد.

۱.۳.۲. درهم‌تنیدگی ذینفعان: تنوع درون‌گروهی

درهم‌تنیدگی ذینفعان می‌تواند به طور همزمان جامعه، سرمایه طبیعی و بازیگرانی از زمینه‌های فرهنگی، منطقه‌ای، و اجتماعی-اقتصادی گوناگون را، که عملیات شرکت به طور مستقیم و غیرمستقیم بر آنها موثر است، شامل شود.

اصل درهم‌تنیدگی به ارکان راهبری این امکان را می‌دهد تا نسبت به تنوع در گروه یکسانی از ذینفعان اطمینان حاصل کند.

برای نمونه، ارکان راهبری هنگام شناسایی سازمان‌های غیردولتی متاثر از عملیات سازمان، می‌تواند هم سازمان‌های غیردولتی بین‌المللی و هم سایر سازمان‌های غیردولتی حامی حقوق جوامع محلی یا فعال در محیط‌های اجتماعی-اقتصادی مختلف را لحاظ کند. به علاوه، ارکان راهبری برای اطمینان از درهم‌تنیدگی، می‌تواند از گروه‌های ذینفع و مشاوره‌ای، مانند اتحادیه‌های اصناف یا گروه‌های نماینده جوامع محلی مختلف، که شغل آنها به عملیات شرکت متکی است، کمک بگیرد. گروه‌های ذینفع انتخاب‌شده براساس اصول فراگیری و درهم‌تنیدگی این امکان را به سازمان می‌دهد تا نگاه و درک عمیق‌تری از حوزه‌ای که در آن فعالیت می‌کند داشته باشد و ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری را کمینه و پیش‌بینی کند.

یک استراتژی تعامل موثر با ذینفعان، که هماهنگ با ارکان راهبری است، راه را برای ارزیابی اهمیت هموار می‌کند.

۲. نقش مدیران اجرایی: توسعه رویکردی یکپارچه نسبت به مدیریت ریسک زیست‌محیطی، اجتماعی و راهبری

مدیران اجرایی بر دستیابی به اهداف سازمانی نظارت نموده و می‌توانند مسئولیت‌های خط اول و دوم را برای وظایف خاص زیست‌محیطی، اجتماعی و راهبری، لحاظ کنند. نقش‌های مدیریتی خط اول برای شناسایی مسائل مرتبط با زیست‌محیطی، اجتماعی و راهبری تاثیر پذیرفته از عملیات سازمان، به طور مستقیم با ارائه محصولات، خدمات و پشتیبانی کلی از سازمان همسو می‌شود.

نقش‌های مدیریتی خط دوم مسئول کمک ویژه در امور مدیریت ریسک مرتبط با زیست‌محیطی، اجتماعی و راهبری است. این نقش‌ها می‌تواند بر مولفه‌های خاصی از مدیریت ریسک مرتبط با زیست‌محیطی، اجتماعی و راهبری، مانند: رعایت قوانین یا مقررات جدید افشای زیست‌محیطی، اجتماعی و راهبری، کنترل داخلی، و مسائل زیست‌محیطی، اجتماعی و راهبری مربوط به تضمین کیفیت (درون و برون‌سازمانی) متمرکز باشند.

از سوی دیگر، نقش‌های خط دوم، در برخی سازمان‌ها بر مسئولیت گسترده‌تر مدیریت ریسک، مانند توسعه مدیریت ریسک سازمانی (ERM)[۲۱]، نظارت می‌کنند (ص‌ص. ۳-۴).

---

[۲۰] Non-governmental organizations
[۲۱] Enterprise Risk Management

در مدل سه خط [دفاعی]، مدیران اجرایی بر نقش‌های زیر نظارت دارند: ۱) توسعه رویکرد چند سرمایه‌ای؛ ۲) توسعه ارزیابی اهمیت برای اطلاع از مدیریت ریسک مرتبط با زیست‌محیطی، اجتماعی و راهبری؛ و ۳) کیفیت داده‌های زیست‌محیطی، اجتماعی و راهبری، کنترل‌های داخلی و گزارشگری.

۱.۲. توسعه رویکرد چند سرمایه‌ای

به طور سنتی، مدیران اجرایی ارزش سازمان را براساس سرمایه مالی و اقتصادی اندازه‌گیری می‌کنند. سرمایه‌های مالی و اقتصادی مربوط به دارایی‌هایی است که به راحتی قابل اندازه‌گیری بوده و سازمان به طور مستقیم آنها را کنترل می‌کند. به علاوه، رشد سرمایه مالی می‌تواند به سرمایه‌گذاران فعلی و بالقوه درباره ثبات یک سازمان اطمینان دهد. عوامل مالی و اقتصادی تنها جریان‌های سرمایه نیازمند توجه مدیران اجرایی نیستند. سازمان‌های زیادی رویکرد چند سرمایه‌ای را انتخاب می‌کنند، این رویکرد «توجه فعال سازمان به روابط بین واحدهای عملیاتی و عملکردی مختلف و سرمایه‌هایی که سازمان استفاده می‌کند یا بر آنها موثر است» را بررسی می‌کند.

مدیران اجرایی سازمان با توجه به این رویکرد چند سرمایه‌ای، روابط بین سرمایه‌های فیزیکی و نامشهود را تعریف، کمی‌سازی و ایجاد می‌کند، که مدل کسب‌وکار برای اطمینان از کارکرد مناسب عملیات سازمان و تاثیر آنها بر مسائل زیست‌محیطی، اجتماعی و راهبری، به این سرمایه‌ها نیاز دارد. شرکت با استفاده از رویکرد چند سرمایه‌ای قادر به ارزیابی آثار و وابستگی‌های خود بر سهام و جریان‌های سرمایه‌ای (به عنوان مثال، طبیعت) خواهد بود، که به‌نوبه خود به درک شرکت‌ها درباره اثربخشی تلاش‌های پایداری‌شان کمک خواهد کرد.

شورای گزارشگری یکپارچه بین‌المللی[۲۲] (IIRC)[۲۳]، یک چارچوب یکپارچه شش‌سرمایه‌ای برای کمک به مدیران اجرایی در انجام این کار ایجاد نموده است. حرکت از فرآیندهای مدیریت سنتی به‌سوی مدیریت یکپارچه زیست‌محیطی، اجتماعی و راهبری نیازمند دانشی خوب درباره شیوه‌های مدیریت و ذهنیتی تازه مبتنی بر تفکری یکپارچه است. طرز تفکر یکپارچه به معنی حرکت سازمان از تمرکز محدود بر بیشینه نمودن سرمایه‌ها و دارایی‌های مالی به‌سوی اتخاذ تصمیمات تجاری براساس روابط بین سرمایه‌های متعدد، اعم از مشهود و نامشهود، است.

اتخاذ رویکرد تفکر یکپارچه می‌تواند از موارد زیر پشتیبانی کند:

- شناسایی کافی ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری.
- درک عمیق از زمینه کلانی که سازمان در آن فعالیت می‌کند.
- ارزش‌آفرینی یک سازمان در کوتاه‌مدت، میان‌مدت، و بلندمدت.

---

[۲۲] **توجه**: در نوامبر سال ۲۰۲۰، شورای گزارشگری یکپارچه بین‌المللی و هیئت استانداردهای حسابداری پایداری اعلام کردند می‌خواهند یکپارچه‌سازی شوند و بنیاد گزارشگری ارزش (VRF) را تشکیل دهند، که به طور رسمی در ژوئن سال ۲۰۲۱ تشکیل شد. در نوامبر سال ۲۰۲۱، بنیاد استانداردهای بین‌المللی گزارشگری مالی، یکپارچه‌سازی بنیاد گزارشگری ارزش و هیئت استانداردهای افشای اقلیم را در بنیاد استانداردهای بین‌المللی گزارشگری مالی، اعلام نمود. بنیاد مذکور چارچوب گزارشگری یکپارچه را تحت مسئولیت‌های خود حفظ کرد:
https://www.ifrs.org/news-and-events/news/۲۰۲۲/۰۵/integrated-reporting-articulating-a-future-path/

[۲۳] International Integrated Reporting Council

۲.۲. توسعه ارزیابی اهمیت برای اطلاع از مدیریت ریسک زیست‌محیطی، اجتماعی و راهبری

در ارزیابی اهمیت، مسائل زیست‌محیطی، اجتماعی و راهبری نسبت به دو جنبه اولویت‌بندی می‌شوند: ۱) اهمیت این مسائل برای ذینفعان؛ و ۲) تاثیر این مسائل بر سازمان. ماتریس اهمیت دوسویه، که نتیجه ارزیابی اهمیت است، ابزار ارزشمندی برای رتبه‌بندی مسائل و اولویت‌های زیست‌محیطی، اجتماعی و راهبری در رابطه با عملیات کلیدی سازمان است.

هرچه مجموعه ذینفعان جامع‌تر و متنوع‌تر باشد، نتایج ارزیابی اهمیت برای تشخیص ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری قابل‌اتکاتر است، زیرا این ارزیابی به شناسایی و اولویت‌بندی مسائل زیست‌محیطی، اجتماعی و راهبری از نظر میزان تهدیدآمیز بودن یک ریسک برای دستیابی به استراتژی و اهداف سازمان، کمک می‌کند.

از آنجا که فرآیند ارزیابی اهمیت به همسویی موضوعات مهم مربوط به زیست‌محیطی، اجتماعی و راهبری با استراتژی شرکت کمک می‌کند، درنتیجه به افشای داده‌های زیست‌محیطی، اجتماعی و راهبری نیز کمک خواهد کرد و باید به عنوان یک ابزار مهم میان‌بخشی که می‌تواند به همه نقش‌های موجود در مدل سه خط [دفاعی] (ارکان راهبری، مدیران اجرایی، حسابرسی داخلی) کمک نماید، در نظر گرفته شود.

بهترین شیوه‌ها در ارزیابی‌های اهمیت

ارزیابی‌های اهمیت در موارد زیر موثرتر و معنادارتر هستند:

۱. هدف روشنی داشته باشند
۲. افق‌های زمانی و چرخه‌های بررسی را به‌خوبی تشریح کرده باشند
۳. نتایج را در طول زمان مقایسه کنند
٤. دیدگاه‌های مورد استفاده را به‌خوبی تشریح کنند
٥. شامل و دربردارنده تجزیه و تحلیل کامل ذینفعان باشند
٦. تفاوت‌های تقسیمی و منطقه‌ای را در نظر بگیرند
۷. به موضوعات از جنبه‌های متعدد امتیاز دهند
۸. ریسک‌های زیست‌محیطی، اجتماعی و راهبری مرتبط با هر موضوع بااهمیت را شناسایی کنند
۹. کیفیت بالای اطلاعات را تضمین کرده و پشتیبان اطمینان‌بخشی باشد.

برگرفته از شورای تجارت جهانی برای توسعه پایدار، دانشکده اقتصاد اراسموس، واقعیت اهمیت: بینش‌هایی از کاربردهای دنیای واقعی ارزیابی اهمیت زیست‌محیطی، اجتماعی و راهبری، ۲۰۲۱.

روش‌های سنتی ارزیابی و اولویت‌بندی ریسک‌ها، مبتنی بر معیارهای تاثیر و احتمال ریسک هستند، اما تکنیک‌های کمی و کیفی دیگری نیز برای یکپارچه‌سازی ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری وجود دارد که موجب اجرای مناسب‌ترین پاسخ ریسک می‌شوند. این تکنیک‌ها، مانند تجزیه و تحلیل سناریوی ریسک، احتمال وقوع ریسک زیست‌محیطی، اجتماعی و راهبری را با روندهای آینده یا تحولات محیطی موردانتظار ترکیب می‌کنند. علاوه بر تجزیه و تحلیل سناریوی زیست‌محیطی، اجتماعی و راهبری، نگاشت همپوشانی ریسک‌ها و نحوه تاثیرگذاری آنها بر یکدیگر، بینش‌هایی درباره سرعت آثار آنها، و انتشار ریسک‌ها در عملیات مختلف، بالادستی و پایین‌دستی، که سازمان مدیریت می‌کند، فراهم می‌آورد.

براساس مصاحبه‌ها، شیوه‌های راهبری خوب نقشی حیاتی در نظارت و حصول اطمینان از درک مدیران اجرایی نسبت به آثار بالقوه مسائل و ریسک‌های زیست‌محیطی، اجتماعی و راهبری بر دستیابی به اهداف استراتژیک سازمان دارند. برخی شرکت‌کنندگان در طول مصاحبه‌ها تاکید داشتند که این امر ماحصل تجمیع عملکردهای مدیریتی مختلف بوده است؛ به عنوان مثال، استفاده همزمان از پایداری و مدیریت ریسک مالی برای تعریف استراتژی مدیریت ریسک یکپارچه، یا تنظیم مناسب‌ترین شاخص‌های عملکرد کلیدی مالی و غیرمالی (KPIs)[۲۴] و حوزه‌های مسئولیت‌های کلیدی (KRA)[۲۵].

برخی شرکت‌ها از کمیته‌های پایداری مخصوصی شامل نقش‌های مدیریتی (مالی و غیرمالی)، یا اعضای هیئت‌مدیره یا حسابرسی داخلی برای نظارت و هدایت کلیه مسائل زیست‌محیطی، اجتماعی و راهبری استفاده می‌کنند. نقش‌های مدیریت ریسک معمولاً از وجود این کمیته‌ها استقبال می‌کنند، زیرا این جلسات امکان بحث‌های منظم درباره مسائل زیست‌محیطی، اجتماعی و راهبری و یکپارچه‌سازی آنها در استراتژی شرکتی را فراهم می‌آورد.

هنگامی که شرکت‌ها رویه‌های روشنی برای تشخیص، اندازه‌گیری، کنترل و گزارش ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری داشته باشند، آنها می‌توانند در محیط‌های عملیاتی بی‌ثبات نیز تاب‌آوری بیشتری داشته باشند. به عنوان مثال، ممکن است واحدهای تجاری نمای کلی‌تری از حوزه فعالیت شرکت در سطح کشور داشته باشند و بتوانند ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری را مشخص کرده و سریعاً اقداماتی در پاسخ به ریسک اجرا کنند. این اطلاعات حیاتی ریسک می‌تواند به سطح گروه برسد و در فرآیند مدیریت ریسک سراسر سازمان گنجانده و ملاحظه شود.

۲.۳. کیفیت و گزارشگری داده‌های زیست‌محیطی، اجتماعی و راهبری

شرکت‌کنندگان در مصاحبه پیشنهاد کردند که جمع‌آوری داده‌های زیست‌محیطی، اجتماعی و راهبری باکیفیت بالا می‌تواند دشوار باشد و ماهیت مسائل زیست‌محیطی، اجتماعی و راهبری، به این معنی است که آثار و وابستگی‌ها اغلب فراتر از مرزهای عملیاتی شرکت هستند. به عنوان مثال، داده‌های انتشار آلاینده‌های محدوده ۳ را می‌توان از طریق تامین‌کنندگان یا میانگین‌های صنعت جمع‌آوری نمود. همچنین برخی شرکت‌ها پیشنهاد دادند که دلیل انتخاب سطوح پایین‌تر اطمینان‌بخشی برون‌سازمانی برای موارد افشای پایداری توسط شرکت‌ها، عدم اطمینان به اطلاعات جمع‌آوری‌شده توسط حسابرسی داخلی است.

اطمینان به رویکردی منسجم برای جمع‌آوری، گزارشگری و افشای داده‌ها، لازمه اطمینان از مفید بودن اطلاعات برای تصمیم‌گیری است. درک افراد، فرآیندها و سیستم‌های درون یک سازمان و نحوه راهبری آنها برای اطمینان از صحت و اعتبار داده‌ها، اهمیتی حیاتی برای بهبود کیفیت اطلاعات زیست‌محیطی، اجتماعی و راهبری دارد.

افشا و گزارشگری داده‌های زیست‌محیطی، اجتماعی و راهبری باید تمرینی آینده‌نگر برای هدایت نقش‌های مختلف به‌سوی یکپارچه‌سازی زیست‌محیطی، اجتماعی و راهبری، مدیریت ریسک موثر و مشارکت ذینفعان

[۲۴] Key Performance Indicators
[۲۵] Key Responsibilities Areas

باشد. افشای زیست‌محیطی، اجتماعی و راهبری باید با صورت‌های مالی و گزارش پایداری همسو باشد، زیرا گروه‌های مختلف ذینفعان برای تصمیم‌گیری آگاهانه به دنبال اطلاعات منسجم و سازگار هستند.

اطمینان از کیفیت، صحت و اعتبار داده‌های زیست‌محیطی، اجتماعی و راهبری

هنگام تعیین داده‌های زیست‌محیطی، اجتماعی و راهبری که باید استفاده شوند، و نحوه جمع‌آوری و تجمیع آنها در شاخص‌ها، توجه به سه عامل اهمیت دارد: کیفیت، صحت و اعتبار. این عوامل اهمیت ویژه‌ای در مسائل یا ریسک‌های زیست‌محیطی، اجتماعی و راهبری جدید یا نوظهور دارند. مدیران اجرایی خط دوم در ارزیابی کیفیت، صحت و اعتبار داده‌ها، باید سوالات زیر را بپرسند:

۱. آیا کیفیت داده‌ها برای تولید نتایج قابل‌اعتماد، کافی است؟ آیا خواست سازمان اندازه‌گیری داده‌های زیست‌محیطی، اجتماعی و راهبری است؟ (به عنوان مثال، داده‌های انتشار آلاینده‌های محدوده ۳، ضایعات تولید شده، برق تولید شده)
۲. آیا کنترل‌هایی برای داده‌های جمع‌آوری شده داخلی وجود دارد؟ چه کسی بر فرآیند جمع‌آوری داده‌ها نظارت داشته است؟
۳. آیا داده‌ها مطابق با استاندارد صنعت یا یک استاندارد شناخته شده بین‌المللی جمع‌آوری شده‌اند؟
٤. آیا داده‌های ثانویه در دسترس (منبع باز) دیگری برای به چالش کشیدن مفروضات مدل یا مقایسه با نتایج سایر روش‌ها وجود دارد؟

مدیران اجرایی بر این فرآیندها نظارت نموده و ممکن است به آموزش منظم در زمینه افشای داده‌های زیست‌محیطی، اجتماعی و راهبری و همچنین آموزش طراحی تحقیقاتی شاخص‌ها برای درک سوگیری‌ها و مسائل صحت در اندازه‌گیری نیاز داشته باشند.

ماخذ: کارگروه سازمان‌های پشتیبان مالی کمیسیون تردوی (COSO)-شورای تجارت جهانی برای توسعه پایدار، بکارگیری مدیریت ریسک سازمانی برای ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری، ۲۰۱۸.

۳. نقش حسابرسی داخلی- کنترل‌های داخلی و تطبیق

حسابرسی داخلی به طور ایده‌آل به دنبال کمک به شرکت‌ها برای ارزیابی فرصت‌ها، بررسی تغییرات عملیات و گزارشگری، رعایت مقررات، و تسریع نوآوری و بهبود پایداری است. اگر چه شیوه فعلی متفاوت است، ولی حسابرسی داخلی به طور معمول در ارتباط با اطلاعات زیست‌محیطی، اجتماعی و راهبری نقشی پیشرو ندارد. این فرصت برای ارکان راهبری وجود دارد که تشخیص دهد حسابرسی داخلی می‌تواند برای شرکت ارزش‌آفرین باشد و در صورت یکپارچه‌سازی با فعالیت پایداری می‌تواند فراتر از تطبیق رفته و رویکرد فعال‌تری برای پایش موضوعات با اهمیت پایداری اتخاذ کند.

واحد حسابرسی داخلی همچنین روابط نزدیکی با کمیته حسابرسی دارد، که این امر فرصت بیشتری برای ارائه رویکردی یکپارچه‌تر در سطح هیئت‌مدیره فراهم می‌کند. با توجه به پیشرفت‌های نظارتی در حال تحول در اتحادیه اروپا، (دستورالعمل گزارشگری پایداری شرکتی، و دستورالعمل بررسی دقیق پایداری شرکتی)، ممکن است کمیته‌های حسابرسی مسئول «نظارت بر گزارشگری پایداری و فرآیندهای مرتبط با تشخیص اطلاعات گزارش‌شده» شوند.

حسابرسی داخلی و فعالیت‌های پایداری فرصت پیش‌بینی روندهای آتی افشای زیست‌محیطی، اجتماعی و راهبری را دارند. به عنوان مثال، حسابرسان داخلی می‌توانند بر چشم‌انداز نظارتی در حال تحول و سطح هماهنگی بین چارچوب‌های نظارتی مختلف نظارت کنند.

حسابرسان داخلی همچنین می‌توانند کنترل‌های داخلی در مورد افشای زیست‌محیطی، اجتماعی و راهبری را آزمون نموده و اطمینان حاصل کنند که داده‌های زیست‌محیطی، اجتماعی و راهبری به طور مداوم جمع‌آوری می‌شوند تا اطمینان در فرآیند جمع‌آوری داده‌ها تضمین شود. محیط کنترل داخلی شیوه‌های روشنی را برای اطمینان از وجود ارتباطات دوطرفه و حلقه‌های بازخورد بین مدیران اجرایی و حسابرسی داخلی ارائه می‌دهد. چارچوب یکپارچه کنترل داخلی کوزو در سال ۲۰۱۳، شیوه‌هایی را برای ایجاد یک محیط کنترل داخلی موثر، مجموعه‌ای از استانداردها، فرآیندها و ساختارهایی که یک سیستم اثربخش کنترل داخلی بر آنها متکی است، معرفی می‌کند. محیط کنترل داخلی سازمان‌ها را قادر می‌سازد تا:

۱) به اهداف استراتژیک دست یابند،

۲) گزارشگری مالی و غیرمالی قابل‌اعتماد به ذینفعان درون و برون‌سازمانی ارائه کنند،

۳) عملیات خود را به طور کارا و اثربخش انجام دهند،

۴) قوانین و مقررات را رعایت کنند، و

۵) از کنترل داخلی دارایی‌های خود در سراسر سازمان محافظت کنند.

حسابرسی داخلی [باید] مستقل از مدیران اجرایی باشد تا بتوان از بی‌طرفی، اختیار و اعتبار آن اطمینان حاصل نمود. حسابرسی داخلی، اطمینان و مشاوره‌ای مستقل و بی‌طرفانه درباره فرآیندها و ساختارهای مدیریت ریسک زیست‌محیطی، اجتماعی و راهبری و راهبری اثربخش ارائه می‌کند. فعالیت حسابرسی داخلی باید به منابع خوبی دسترسی داشته باشد و برای اطمینان از درستی، اعتماد، شفافیت، تطبیق و پاسخگویی باید در جایگاه مناسبی قرار بگیرد. چارچوب بین‌المللی اجرای حرفه‌ای (IPPF)[۲۶] انجمن حسابرسان داخلی شامل استانداردهای شناخته شده جهانی و رهنمودهای معتبر برای انجام با کیفیت بالای کار حسابرسی داخلی است. این امر از طریق افشای منظم گزارش‌های پایداری و مالی، تضمین فرآیندهای منظم جمع‌آوری داده‌ها، و تخصص در شاخص‌های زیست‌محیطی، اجتماعی و راهبری حاصل می‌شود. حسابرسی داخلی یافته‌های خود را به منظور ارتقا و تسهیل بهبود مستمر، به مدیریت و ارکان راهبری گزارش می‌کند.

[۲۶] International Professional Practices Framework

یک واحد حسابرسی داخلی با منابع خوب و دارای جایگاه مناسب:

۱. نسبت به ارکان راهبری پاسخگو است

۲. در برنامه‌ریزی و عملیات خود مستقل از دخالت مدیران اجرایی است

۳. مجوز دسترسی به همه افراد، داده‌ها، و منابع مورد نیاز برای انجام کارش را دارد

۴. مسئول تصمیم‌گیری‌های اجرایی نیست

۵. دانش کاملی درباره تمامی جنبه‌های سازمان دارد

۶. استانداردهای بین‌المللی برای اجرای حرفه‌ای حسابرسی داخلی را رعایت می‌کند

ماخذ: کارگروه سازمان‌های پشتیبان مالی کمیسیون تردوی (COSO)-شورای تجارت جهانی برای توسعه پایدار، بکارگیری مدیریت ریسک سازمانی برای ریسک‌های مرتبط با زیست‌محیطی، اجتماعی و راهبری، ۲۰۱۸. متن کامل در www.wbcsd.org/erm موجود است.

۵– پیشنهادها و سوالات کلیدی

این جدول پیشنهادها برای شرکت‌ها در زمینه یکپارچه‌سازی ملاحظات زیست‌محیطی، اجتماعی، راهبری و پایداری در نقش‌های تعیین‌شده در مدل سه خط [دفاعی] را خلاصه می‌کند. هدف از طرح این سوالات کلیدی، تحریک گفتگو در درون و بین نقش‌های مختلف درباره میزان یکپارچه‌سازی ملاحظات پایداری و زیست‌محیطی، اجتماعی و راهبری در فرآیندها و شیوه‌های موجود، است.

	ارکان راهبری	مدیران اجرایی	حسابرسی داخلی
پیشنهادها	• در نظر گرفتن رویکرد چند سرمایه‌ای برای جریان‌های سرمایه • مشارکت با ذینفعان برای درک آثار پایداری و پیوند با مدل کسب‌وکار • در نظر گرفتن تنوع ذینفعان در هرگونه فعالیت‌های مشارکتی ذینفعان • اطمینان از نظارت ارکان راهبری بر مدیریت ریسک • اطمینان از دسترسی حسابرسی داخلی به منابع مناسب (که در نهایت ممکن است هزینه‌های اطمینان‌بخشی مستقل را کاهش دهد)	• انجام ارزیابی اهمیتی که برای فرآیندهای مدیریت ریسک سازمانی اطلاعات فراهم می‌کند • ترکیب کارکردهای پایداری و مالی برای تعریف استراتژی مدیریت ریسک یکپارچه • همسو کردن کیفیت و گزارشگری داده‌های زیست‌محیطی، اجتماعی و راهبری با چرخه‌های گزارشگری مالی	• نظارت بر قابلیت اطمینان جمع‌آوری داده‌های زیست‌محیطی، اجتماعی و راهبری و فرآیندهای کنترل داخلی • ایجاد دانش درباره پایداری و آثار زیست‌محیطی، اجتماعی و راهبری شرکت • اطمینان از تعاملات منظم میان حسابرسان داخلی و نقش‌های خط اول و دوم

	ارکان راهبری	مدیران اجرایی	حسابرسی داخلی
سوالات کلیدی برای ارزیابی سطح یکپارچه‌سازی [ملاحظات] زیست‌محیطی، اجتماعی و راهبری/پایداری	ارکان راهبری تا چه حدی بر یکپارچه‌سازی [ملاحظات] زیست‌محیطی، اجتماعی و راهبری نظارت دارد؟ تعامل ارکان راهبری با سایر کارکردها درباره مسائل با اهمیت زیست‌محیطی، اجتماعی و راهبری در حال حاضر چگونه است؟ و چه اقداماتی برای بهبود آن می‌توان انجام داد؟ اطلاعات مرتبط با ریسک چگونه در اختیار ارکان راهبری قرار می‌گیرد؟ موانع فعلی یکپارچه‌سازی ریسک‌های زیست‌محیطی، اجتماعی و راهبری چه هستند؟ فرهنگ شرکتی چه نقشی در سازمان ایفا می‌کند؟ آیا شامل مسائل زیست‌محیطی، اجتماعی و راهبری برای دستیابی به پایداری بلندمدت می‌شود؟	مدیران اجرایی چگونه می‌توانند تاثیر عملیات شرکت بر مسائل زیست‌محیطی، اجتماعی و راهبری را درک و اندازه‌گیری نمایند؟ مدیران اجرایی چگونه می‌توانند از کامل و صحیح بودن داده‌های زیست‌محیطی، اجتماعی و راهبری اطمینان حاصل کنند؟ تفاوت ارزیابی و اولویت‌بندی ریسک‌های زیست‌محیطی، اجتماعی و راهبری در سطوح مدیریت عملیاتی و استراتژیک چیست؟ چه شیوه‌ها و سیاست‌هایی تضمین‌کننده رویکرد جامع نقش‌های مدیریتی خط اول و دوم نسبت به مدیریت ریسک زیست‌محیطی، اجتماعی و راهبری هستند؟	حسابرسی داخلی چگونه می‌تواند با حسابرسان مستقل برای اطمینان از قابلیت اتکا و سازگاری اطلاعات، همکاری نماید؟ حسابرسی داخلی چه نقشی می تواند در کمک به آمادگی سازمان برای افشای غیرمالی از طریق مشاوره و اطمینان‌بخشی در مورد ساختارها، سیستم‌ها و فرآیندهای تصمیم‌گیری و گزارشگری ایفا کند؟ چه کنترل‌هایی تضمین‌کننده مفید بودن شیوه جمع‌آوری، تجزیه‌وتحلیل و گزارش داده‌های پایداری برای تصمیم‌گیرندگان هستند؟ چه فرآیندها و سیاست‌هایی برای اندازه‌گیری، پایش و گزارش پیشرفت در راستای تعهدات شرکت، اتخاذ می‌شود؟ حسابرسی داخلی چگونه می‌تواند با حمایت از تغییر ذهنیت سازمانی، پایداری را با راهبری و عملیات، یکپارچه‌سازی کند؟

منبع:

- WBCSD (World Business Council for Sustainable Development) & IIA (The Institute of Internal Auditors), July ۲۰۲۲, "Embedding ESG and sustainability considerations into the Three Lines Model".

نقش‌های سه خط دفاعی برای راهبری و امنیت اطلاعات

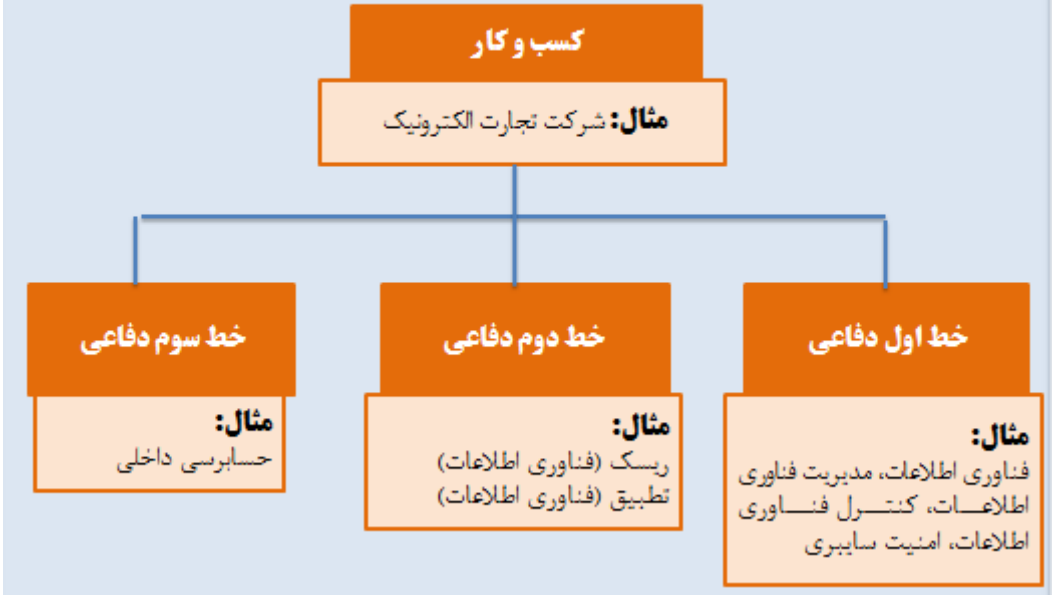
مرتضی اسدی

در حالی که سه خط دفاعی اطمینان بخشی، راهبری، ریسک، تطبیق، امنیت اطلاعات و وظیفه امنیت سایبری را پوشش می دهد، می‌توانند همه به یک شکل یا به نوعی بر روی راهبری و امنیت اطلاعات کار کنند، می‌توان اهداف، نقش‌ها و فعالیت‌های این عملکردها را برای کشف راه‌های بهینه سازی خروجی ها بررسی کرد. خروجی‌های بهینه شده به این معنی است که خروجی‌های ترکیبی طرف‌های مختلف که روی امنیت اطلاعات کار می‌کنند به حداکثر می رسد، که اجازه می دهد منابع با افزایش بهره وری به وسیله کاهش تکرار، به کار گرفته شوند.

نقش‌ها و مسئولیت‌های عملکردهای مختلف

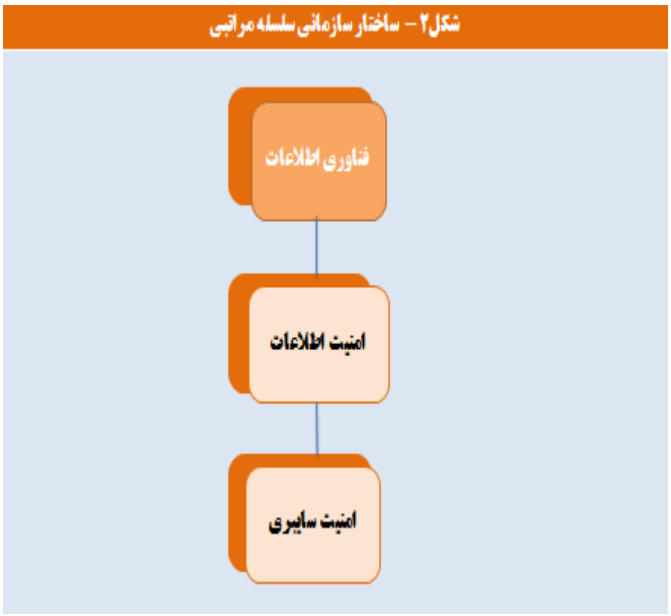
هدف سازمان‌ها دستیابی به اهداف خود در عین مدیریت ریسک در چارچوب ریسک پذیری خود است. یک ساختار راهبری خوب برای مدیریت ریسک، ایجاد سه خط دفاعی است. به طور خلاصه، اولین خط دفاعی عملکردی است که ریسک را در اختیار دارد و مدیریت می‌کند. در اولین خط دفاعی، کسب و کارها می‌توانند عملکردهای کنترلی (به عنوان مثال، کنترل فناوری اطلاعات، که به بخش فناوری اطلاعات گزارش می‌دهد) را برای تسهیل مدیریت ریسک تنظیم کنند. خط دوم دفاعی، عملکرد کنترل مستقل است (به عنوان مثال، ریسک فناوری اطلاعات، انطباق فناوری اطلاعات) که بر ریسک نظارت می‌کند و کنترل‌های خط اول دفاعی را نظارت می کند. می‌تواند اثربخشی کنترل‌ها و مدیریت ریسک را در سراسر سازمان به چالش بکشد. سومین خط دفاعی حسابرسی داخلی است که اطمینان بخشی مستقلی را ارائه می‌دهد. شکل ۱ نمونه‌هایی از عملکردهای زیر سه خط دفاعی را نشان می دهد.

شکل ۱ – سه خط دفاعی



هدف عملکردهای مختلف کسب و کار این است کـه اطمینـان حاصـل شـود کـه سـازمان‌هـا ریسـک را در چارچوب ریسک پذیری خود مدیریت می‌کنند. به طور خاص، راهبری فناوری اطلاعات، سازگاری، فرآیندها، استانداردها و قابلیت تکرار مورد نیاز برای عملیات مؤثر فنـاوری اطلاعـات را در حـین نظـارت بـر بودجـه و انطباق با الزامات نظارتی و/یا سازمان فراهم می‌کند. مدیریت ریسک فناوری اطلاعات باید به عنوان بخشی از چارچوب مدیریت ریسک سازمانی عمل کند و به انواع مختلف ریسک و چالش‌ها و فرصت‌هایی کـه ریسـک ارائه می‌کند، رسیدگی کند. این کمک می کند تا راهبری فناوری اطلاعات، امنیت و سرمایه گذاری در حریم خصوصی را در حوزه‌هایی که برای دستیابی به اهداف سازمانی حیاتی هستند، متمرکز کنـد. هـدف امنیـت اطلاعات محافظت از داده ها و سیستم هـای اطلاعـاتی در برابـر دسترسـی نامناسـب، دسـتکاری، اصـلاح و تخریب است، بنابراین از محرمانه بودن، یکپارچگی و در دسترس بودن سیستم/داده‌ها اطمینان حاصل مـی-کند. امنیت سایبری که شامل فناوری، فرآینـدها، سیاسـت‌ها و افـراد می‌شـود، بـر اسـتفاده از محرک‌هـای کسب‌وکار برای هدایت فعالیت‌های امنیتی تمرکز می‌کند و در عین حال اطمینان می‌دهد که عوامل ریسک امنیت سایبری در فرآیندهای مدیریت ریسک سازمان گنجانده شده است.

این عملکرد اطمینان بخشی حسابرسی داخلی است، که ماموریـت آن را مـی تـوان ارائـه اطمینـان بخشـی بیطرفانه و مبتنی بر ریسک برای ارزیابی اثربخشی فرآیندهای راهبـری، مـدیریت ریسـک و کنتـرل، جهـت ارتقاء و محافظت از ارزش سازمانی تعریف کرد.



ساختار سازمانی وظایف مختلف

تیم های مختلف را می توان به روش های مختلفی سازماندهی کرد، همانطور که در شکل های ۲ و ۳ نشان داده شده است. شکل ۲ نشان می دهد که چگونه تیم هـای ریسـک فنـاوری اطلاعـات، امنیـت اطلاعـات و امنیت سایبری می توانند به روشی سلسله مراتبی سازماندهی شوند. تحت ایـن سـاختار سـازمانی، احتمـال کمتری وجود دارد که وظایف/فعالیت‌های آن‌ها تکراری شود، زیرا امنیت سایبری در امنیـت اطلاعـات قـرار دارد، به این معنی که دومی کاملاً از فعالیت‌ها و نقش اولی آگاه است. شکل ۳، از سوی دیگـر، نمونـه ای از تیم های ریسک فناوری اطلاعات، امنیت اطلاعات و امنیت سایبری است که در یک ساختار مسطح به عنوان

همتای یکدیگر سازماندهی شده اند. با این نوع ساختار سازمانی، احتمال بیشتری وجود دارد که فعالیت‌های آن‌ها همپوشانی داشته باشد، زیرا ممکن است تیم‌های مختلف از کاری که دیگری انجام می‌دهد آگاه نباشند. به عنوان مثال، تیم امنیت اطلاعات می‌تواند تنظیمات و کنترل‌های امنیت اطلاعات را روی همه سیستم‌عامل‌ها بررسی کند، در حالی که تیم امنیت سایبری می‌تواند تنظیمات و کنترل‌های وب سرور را که ممکن است همان سرور را پوشش دهد، بررسی کند. مثال دیگر ممکن است امنیت اطلاعات مسئول برنامه ریزی بازیابی فاجعه یا مدیریت سطح خدمات باشد، در حالی که تیم امنیت سایبری مسئول رسیدگی به ریسک خارج شدن از خدمات‌دهی (DoS) است. در حالی که بازیابی فاجعه و مدیریت سطح خدمات، کنترل‌هایی برای رسیدگی به ریسک خارج شدن از خدمات‌دهی (DoS) هستند.

شکل ۳ – ساختار سازمانی درختی

فعالیت‌های عملکردهای مختلف و/یا سه خط دفاعی

برای دستیابی به هدف نهایی سازمان در مدیریت ریسک (به عنوان مثال، ریسک اطلاعات و فناوری) در چارچوب ریسک پذیری، عملکردهای مختلف تجاری و/یا سه خط دفاعی باید فعالیت هایی مانند جمع آوری اطلاعات، ارزیابی ریسک، بررسی، تجزیه و تحلیل، گزارش دهی را انجام دهند و نظارت بر ریسک که ممکن است در بین سه خط مشترک باشد. یکی از راه‌های پی بردن به این مشترکات، ارتباط مکرر است که به اشتراک گذاری اطلاعات را تسهیل می‌کند. برای تسهیل ارتباطات و بحث در مورد ریسک در یک سازمان، عملکردهای مختلف تجاری می توانند از مجموعه‌ای از دسته بندی ریسک و طبقه بندی یکسان استفاده کنند.

اشتراک‌گذاری ورودی‌ها

عملکردهای مختلف تجاری که روی ریسک فناوری اطلاعات کار می‌کنند می‌توانند اطلاعات داخلی مفیدی مانند اطلاعات منبع (به عنوان مثال، داده های تراکنش)، اطلاعات ریسک (به عنوان مثال، روندها یا آمارهایی مانند درصد در دسترس بودن برنامه وب) و داده های زیان داخلی (مانند حوادث امنیت فناوری اطلاعات شامل جزئیات و/یا ماهیت حوادث) را به اشتراک بگذارند. از طریق به اشتراک گذاری اطلاعات داخلی، عملکردهای تجاری می‌توانند با انجام تجزیه و تحلیل مربوط، ارزیابی ریسک و نظارت، و کنترل برنامه ریزی بازنگری (به عنوان مثال، برنامه ریزی انطباق یا حسابرسی) وظایف خود را انجام دهند.

همچنین، اطلاعات را می‌توان از طریق یک پایگاه داده زیان خارجی در داخل صنعت بـه اشـتراک گذاشـت، همانطور که ORX[1] داده های زیان را برای صنعت بانکداری و بیمه ذخیره می کنـد. از طریـق بـه اشـتراک گذاری اطلاعات ریسک خارجی، عملکردهای مختلف کسب و کار را می‌توان بهتر در مورد چگونگی شناسایی و جلوگیری از ریسک مشابه آگاه کرد. به عنوان مثال، در سـال ۲۰۱۶، درخواسـت انتقـال پـول غیرمجـاز از طریق بانک بنگلادش وجود داشت که توسط یکی از بانک‌های مسیریابی شناسایی شد که تنها به دلیل غلط املایی کلمه «Fandation»، تراکنش را برای بررسی بیشتر علامت گذاری کرد، که منجـر بـه توقـف انتقـال شد.

اطلاعات همچنین می تواند در داخل یـک کشـور بـه اشـتراک گذاشـته شـود. بـه عنـوان مثـال، مشـارکت اشتراک‌گذاری اطلاعات امنیت سایبری (CiSP) بریتانیا یک ابتکار مشـترک صـنعت/دولت اسـت کـه بـرای تبادل اطلاعات تهدیدات سایبری در زمان واقعی در یک محیط امن، محرمانه و پویا، افزایش آگاهی موقعیتی و کاهش تأثیر بر سازمان های بریتانیا راه‌اندازی شده است. اطلاعات همچنین مـی توانـد بـین کشـورها بـه اشتراک گذاشته شود. به عنوان مثال، اشتراک گذاری بین کشوری مانند تیم واکنش اضـطراری کـامپیوتری آسیا و اقیانوسیه (APCERT) برای تشویق و حمایت از همکاری بین CERTهـای ملـی در منطقـه آسـیا و اقیانوسیه (APAC) وجود دارد. تیم واکنش اضطراری رایانه‌ای آسیا و اقیانوسیه یک شـبکه قابـل اعتمـاد از کارشناسان امنیت رایانه را در منطقه آسیا و اقیانوسیه برای بهبود آگاهی و شایسـتگی منطقـه در رابطـه بـا حوادث امنیتی رایانه ای حفظ می‌کند.

به اشتراک گذاری پردازش

علاوه بر اشتراک گذاری ورودی‌ها، پردازش نیز می تواند به اشتراک گذاشته شود. عملکردهای مختلف ممکن است از ابزارهایی برای توسعه اقدامات نظارتی برای اهداف پیشگیرانه و/یا اکتشافی استفاده کنند. به اشتراک گذاشتن این ابزارها می تواند کار تکراری را در بین تیم های مختلف کاهش دهد. برای مثال، خط اول یا دوم دفاعی ممکن است استفاده از رگتچ (RegTech - برنامه کاربردی فناوری برای اطمینان از انطباق با آخرین الزامات ناظرین و/یا شرکت) یا استفاده از یادگیری ماشین برای شناسایی حملات خارج شدن از خدمات‌دهی توزیع شده (DDoS) براساس الگوهای مشابه گذشته خارج شدن از خدمات‌دهی توزیع شده است. ابزارهای توسعه یافته توسط خط اول می تواند توسط خط دوم استفاده شود و بالعکس. حسابرسی داخلی می‌تواند اسکریپت‌های خودکاری را برای انجام آزمون یا حسابرسی مستمر ایجاد کند (به عنوان مثال، استفاده از ربات‌ها برای رفتن به وب‌سایت‌های ارائه‌دهندگان خدمات برای بررسی اینکه آیا آخرین وصله‌های سیستم یا امضاهای ویروس توسط سازمان استفاده می‌شوند)، که می‌تواند توسط خط اول نیز استفاده شود یا توسط خط دوم دفاعی برای اهداف نظارت مستمر استفاده شود.

[1] O.R.X یک انجمن صنعتی غیرانتفاعی است که در ژنو، سوئیس ایجاد شده است و بزرگترین انجمن مدیریت ریسک عملیاتی در خدمات مالی است.

به اشتراک‌گذاری خروجی‌ها

نتایج بررسی‌های انجام شده توسط یک طرف را می توان به اشتراک گذاشت. به عنوان مثال، اولین خط دفاعی می‌تواند خودآزمایی پایبندی به دستورالعمل‌های بانکداری الکترونیکی ناظر بانکی هنگ کنگ (موسسه پولی هنگ کنگ) را برای مدیریت تطبیق انجام دهد. خط دوم دفاعی می تواند از این خودآزمایی برای گزارش های نظارتی استفاده کند.

مثال دیگر عملکرد راهبری است. خطوط دفاعی دوم و سوم می‌توانند از گزارشگری استثنای خط اول و/یا نتایج بررسی کنترل شخص ثالث (به عنوان مثال، ناظر یا حسابرس خارجی) برای شناسایی مسائل سیستمی استفاده کنند. خط سوم همچنین می تواند از نتایج بررسی کنترل خط اول یا دوم برای ارزیابی اثربخشی خط اول و دوم دفاعی استفاده کند.

کار عملکرد اطمینان‌بخشی

در حالی که بررسی های انجام شده توسط عملکرد اطمینان بخشی می‌تواند مشابه مواردی باشد که توسط خطوط دفاعی اول یا دوم انجام می شود، تنها بخش حسابرسی داخلی یا ارائه دهندگان خدمات خارجی می توانند اطمینان لازم را ارائه دهند زیرا از نظر عملکرد مستقل از کسب و کار هستند و دارای خطوط گزارشگری و اقتداری هستند که با خط اول و دوم دفاعی متفاوت است. از این رو، تیم های حسابرسی نیاز به انجام کار خاص برای ارزیابی اثربخشی فرآیندهای راهبری، مدیریت ریسک و کنترل دارند.

بررسی های مختلفی وجود دارد که می‌تواند توسط تیم‌های حسابرسی انجام شود. اگر تیم‌های حسابرسی عملکرد مجدد را انجام دهند، مقرون به صرفه نیست، زیرا با انجام مجدد کنترلی مانند بررسی استخراج ایمیل‌های نمونه‌برداری شده برای تشخیص هرگونه اطلاعات رمزگذاری نشده شخصی مشتریان (PII) یا بررسی مستقل صحت پردازش توسط مشتری، تلاش‌ها را تکرار می‌کند. برنامه کاربردی شرکت حتی اگر تیم حسابرسی کنترلی مانند کنترل برنامه کاربردی را برای سال اول مجدداً انجام دهد، حسابرسی می تواند با انجام کارهای انجام مجدد کنترل گسترده را در سال بعد کاهش دهد (بنابراین صرفه جویی در زمان و تلاش در حین دستیابی به اطمینان مورد نظر). آزمون‌های دیگری مانند کنترل‌های مدیریت تغییر یا بررسی آخرین تاریخ تغییر برای مشاهده اینکه آیا تغییری از آخرین حسابرسی، زمانی که آزمون عملکرد مجدد برای تأیید پردازش دقیق درخواست شرکت انجام شد، اعمال شده است یا خیر.

حسابرسی همچنین می‌تواند حسابرسی مستمر را انجام دهد تا اطمینان را به‌موقع‌تر، بر اساس جامعه داده‌های بزرگ‌تر در حال آزمایش، ارائه دهد. با این حال، اگر مدیریت نظارت مستمر مشابه و مؤثری را اجرا کرده باشد، دامنه حسابرسی مستمر به طور بالقوه می تواند کاهش یابد. بین کفایت نظارت مدیریت و فعالیت های مدیریت ریسک و میزانی که حسابرسان باید آزمون دقیق کنترل ها و ارزیابی ریسک را انجام دهند، رابطه معکوس وجود دارد. رویکرد واحد حسابرسی به حسابرسی مستمر و میزان آن، بستگی به میزان اجرای نظارت مستمر و اثربخشی آن توسط مدیریت دارد.

تخصیص اقتصادی منابع

اگر یک واحد تجاری فاقد منابع لازم برای انجام وظایف مورد نیاز باشد، می تواند منابع را در داخل به دست آورد. به عنوان مثال، آزمون IT's Sarbanes-Oxley Act (SOX) می‌تواند توسط منابع داخلی مانند تیم حسابرسی داخلی/ تطبیق/ ریسک انجام شود، بسته به اینکه کدام تیم منابع مورد نیاز را دارد، زیرا همه عملکردها الزامات انجام آزمون SOX را برآورده می‌کنند.

برای بررسی‌های اجباری نهادناظر که انجام آن به یک طرف مستقل نیاز دارد، یک سازمان می‌تواند منابع داخلی با مهارت‌های کافی را برای برآورده کردن نیاز انتخاب کند، زیرا منابع داخلی معمولاً هزینه کمتری نسبت به منابع خارجی دارند. اگر منابع داخلی مهارت ها/ابزارهای لازم را نداشته باشند (به عنوان مثال، تست های نفوذ یا هک اخلاقی) و نتوانند اطمینان لازم را ارائه دهند، بدون در نظر گرفتن هزینه های نسبتاً بالاتر، باید منابع خارجی بکار گرفته شوند.

هنگام بررسی نقش ها و اهداف سه خط دفاعی شامل اطمینان بخشی، راهبری، ریسک، تطبیق، امنیت اطلاعات و امنیت سایبری، می تواند فعالیت های مشترک یا همپوشان وجود داشته باشد. یک ساختار سازمانی سلسله مراتبی می‌تواند شانس وظایف/فعالیت‌های تکراری را در میان عملکردها یا تیم‌ها کاهش دهد، زیرا هر تیم از نقش و فعالیت‌های تیم‌های دیگر در ساختار سلسله مراتبی آگاهی بیشتری دارد. راه دیگر برای بهینه‌سازی خروجی‌ها و صرفه‌جویی در منابع و هزینه‌ها برای سازمان، به اشتراک گذاشتن ورودی‌ها، پردازش‌ها و خروجی‌های عملکردها و تیم‌های مختلف کسب و کار (از جمله خروجی‌های سازمان‌های عمومی یا غیرانتفاعی در سراسر صنعت و کشور) است که می‌توان از آن برای ساده‌سازی فعالیت‌های هر عملکرد استفاده کرد.

با این حال، عملکرد اطمینان بخشی تنها توسط اشخاص مستقل مانند تیم حسابرسی داخلی و حسابرسان مستقل قابل ارائه است. منابع داخلی هزینه کمتری نسبت به منابع خارجی دارند، اما ممکن است منابع اولیه مورد نیاز برای انجام برخی وظایف را نداشته باشند. برای این موارد، ممکن است با وجود هزینه های نسبتاً بالاتر، به حسابرسان مستقل برای مطمئن ساختن از اینکه اطمینان بخشی لازم وجود دارد، نیاز باشد.

منابع:

١. Lainhart, J W.; Z. Fu; C. Ballister; “Holistic IT Governance, Risk Management, Security and Privacy: Needed for Effective Implementation and Continuous Improvement,” ISACA Journal, vol. ٥, ٢٠١٦, www.isaca.org/resources/isaca-journal/issues

٢. The Institute of Internal Auditors, “Supplemental Guidance, Model Internal Audit Activity Charter,” ٢٠١٧

٣. Schwartz, M.; “Bangladesh Bank Hackers Steal $١٠٠ Million,” Bank Info Security, ١٠ March ٢٠١٦, https://www.bankinfosecurity.com/bangladesh-bank-hacers-steal-١٠٠-million-a-٨٩٥٨

٤. National Cyber Security Centre, Cyber Security Information Sharing Partnership, ٢٠ March ٢٠١٨, https://www.ncsc.gov.uk/cisp

٥. Asia Pacific Computer Emergency Response Team, https://www.apcert.org

٦. Coderre, D.; “Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment,” The Institute of Internal Auditors, ٢٠٠٥,

https://www.iia.nl/SiteFiles/IIA_leden/Praktijkgidsen/GTAG٣.pdf

Amelia Ho, CISA, CISM, CA, CFE, CIA, CISSP, FRM, PMP
Is a senior vice president with Citibank and has more than ٢٠ years of experience in the financial services industry in a number of internal audit, risk management and compliance roles. She has contributed to ISACA as an article author and expert reviewer of ISACA publications. She is the recipient of the ٢٠١٣ Ted Keys Honorable Mention Award for her article “Emerging Risk Audits” in Internal Auditor published by The Institute of Internal Auditors.

مدل سه خط دفاعی در برابر ریسک‌های ناشی از هوش مصنوعی

مرتضی اسدی **آرشینا منتظری**

خلاصه

سازمان‌هایی که سیستم‌های هوش مصنوعی (AI) را توسعه و استقرار می‌دهند، به دلایل اقتصادی، قانونی و اخلاقی، باید ریسک‌های مرتبط را مدیریت کنند. با این حال، همیشه مشخص نیست که چه کسی مسئول مدیریت ریسک های ناشی از هوش مصنوعی است. مدل سه خط دفاعی (3LoD)[1] که بهترین روش برای بسیاری از صنایع در نظر گرفته می‌شود، ممکن است راه حلی در این خصوص ارائه دهد. این مدل یک چارچوب مدیریت ریسک برای کمک به سازمان‌ها است تا نقش‌ها و مسئولیت‌های مدیریت ریسک را تعیین و هماهنگ کنند. این مقاله، روش‌هایی را پیشنهاد می‌دهد که شرکت‌های هوش مصنوعی می‌توانند این مدل را پیاده سازی کنند. همچنین در مورد اینکه چگونه این مدل می‌تواند به کاهش ریسک‌های ناشی از هوش مصنوعی کمک کند، بحث می‌شود. بطوریکه شکاف‌های پوشش ریسک را مشخص کرده و بتواند اثربخشی شیوه‌های مدیریت ریسک را افزایش دهد و هیئت مدیره را قادر سازد تا مدیریت را به طور مؤثرتری نظارت کند. هدف این مقاله اطلاع رسانی به تصمیم گیرندگان در شرکت های پیشرو هوش مصنوعی، قانونگذاران[2] و نهادهای استانداردگذار[3] است.

۱. مقدمه

سازمان‌هایی که سیستم‌های هوش مصنوعی را توسعه و به کار می‌گیرند، به دلایل اقتصادی، باید ریسک‌های مرتبط را مدیریت کنند، زیرا رویدادها و موارد سوء استفاده می‌توانند تهدیدی برای عملکرد کسب‌وکار باشند. به دلایل قانونی ممکن است مقررات آتی هوش مصنوعی، آنها را ملزم به اجرای یک سیستم مدیریت ریسک کند و به دلایل اخلاقی، آنها موظف به جلوگیری از آسیب هستند.

با این حال، همیشه مشخص نیست که چه کسی مسئول مدیریت ریسک هوش مصنوعی است: محققان و مهندسان؟ بخش حقوقی و تطبیق[4]؟ تیم راهبری؟ مدل سه خط ممکن است راه حلی ارائه دهد. این یک چارچوب مدیریت ریسک است که به منظور بهبود راهبری ریسک سازمان با تخصیص و هماهنگ کردن نقش‌ها و مسئولیت‌های مدیریت ریسک طراحی شده است. این بهترین مدل در بسیاری از صنایع مانند مالی و هوانوردی در نظر گرفته می‌شود. این مقاله، مدل سه خط را در زمینه هوش مصنوعی اعمال می‌کند.

---

[1] The three Lines of Lefense
[2] Regulators
[3] Standard-Setting Bodies
[4] Compliance

تا به امروز، کارهای آکادمیک زیادی روی اشتراک هوش مصنوعی و مدل سه خط انجام نشده است. استفاده از مدل برای کاهش ریسک های متمایز[۵] ناشی از هوش مصنوعی پیشنهادهایی ارایه می‌دهد، اما این متن مختصر و مفید است. همچنین برخی ادبیات در مورد اینکه چگونه شرکت‌ها می‌توانند از هوش مصنوعی برای حمایت از مدل سه خط استفاده کنند وجود دارد، اما من عمدتاً به نحوه اداره شرکت‌های هوش مصنوعی علاقه مند هستم، نه نحوه استفاده از هوش مصنوعی برای اداره شرکت‌های غیرهوش مصنوعی. همچنین پیشنهاد شده است که دولت‌ها می‌توانند از مدل سه خط برای مدیریت ریسک های شدید ناشی از هوش مصنوعی استفاده کنند، اما در اینجا روی چالش‌های شرکت‌ها تمرکز می‌شود، نه دولت.

انجمن حسابرسان داخلی[۶] یک مجموعه سه قسمتی را که در آن چارچوب حسابرسی هوش مصنوعی[۷] را پیشنهاد می‌کند منتشر کرده است، هر چند مطالب آنها حاوی اشاره‌ای به مدل سه خط است، اما نقش کلیدی ایفا نمی‌کند. در نهایت، مدل سه خط در کتابچه‌ای که توسط موسسه ملی استانداردها و فناوری (NIST)[۸] در کنار چارچوب مدیریت ریسک هوش مصنوعی منتشر کرده است، ذکر شده است. با این حال، این کتابچه[۹] فقط اجرای مدل سه خط (یا مکانیزم مشابه) را پیشنهاد می‌کند و نحوه انجام این کار را مشخص نمی‌کند. روی هم رفته، حداقل دو شکاف در ادبیات کنونی وجود دارد. مورد اول کاربردی است: به نظر نمی رسد پیشنهاد مشخصی برای اینکه چگونه سازمان‌هایی که سیستم‌های هوش مصنوعی را توسعه و استقرار می‌دهند می‌توانند مدل سه خط را پیاده‌سازی کنند، وجود داشته باشد و معدود پیشنهادهایی که وجود دارند به اندازه کافی دقیق نیستند تا راهنمایی‌های معناداری را ارائه کنند. مورد دوم دستوری است: به نظر نمی‌رسد بحث کاملی در مورد اینکه آیا اجرای مدل مطلوب است یا نه وجود داشته باشد. با توجه به اینکه این مدل مورد انتقاد قرار گرفته و شواهد تجربی زیادی برای اثربخشی آن وجود ندارد، پاسخ به این سوال واضح نیست. با توجه به این موضوع، مقاله به دنبال پاسخ به دو سوال زیر است:

سوالات تحقیق:

سوال۱ : سازمان‌هایی که سیستم‌های هوش مصنوعی را توسعه و استقرار می‌دهند چگونه می‌توانند مدل سه خط را پیاده‌سازی کنند؟

سوال۲ : اجرای مدل سه خط تا چه اندازه به کاهش ریسک های ناشی از هوش مصنوعی کمک می‌کند؟

---

۵ Discrimination Risks
۶ Institute of Internal Auditors
۷ AI Auditing Framework (IIA)
۸ The National Institute of Standards and Technology
۹ Playbook

مقاله بر سه حوزه متمرکز است. **اول**، بر سازمان‌هایی تمرکز می‌کند که سیستم‌های هوش مصنوعی پیشرفته را توسعه می‌دهند و به کار می‌گیرند، به ویژه آزمایشگاه‌های تحقیقاتی متوسط (مثلاً Google DeepMind[۱۰] و OpenAI[۱۱]) و شرکت‌های فناوری بزرگ (مانند مایکروسافت و متا)، اگرچه مرزهای بین این دو دسته مبهم است (به عنوان مثال Google DeepMind یکی از شرکت‌های تابعه Alphabet است و OpenAI با مایکروسافت شراکت استراتژیک دارد). در ادامه از عبارت "شرکت های هوش مصنوعی" برای اشاره به همه آنها استفاده می‌شود. این مقاله انواع دیگر شرکت‌ها (مانند شرکت‌های سخت‌افزار)، غیرانتفاعی یا مؤسسات دانشگاهی را پوشش نمی‌دهد، اما ممکن است آن‌ها نیز از تحلیل‌ها سود ببرند. **دوم**، این مقاله بر بعد سازمانی مدیریت ریسک هوش مصنوعی تمرکز دارد. موضوع این نیست که چگونه شرکت‌های هوش مصنوعی باید ریسک‌های ناشی از هوش مصنوعی را تشخیص، ارزیابی و پاسخ دهند در عوض، این در مورد چگونگی تعیین و هماهنگی نقش‌ها و مسئولیت‌های مدیریت ریسک است. **سوم**، مقاله بر توانایی مدل برای جلوگیری از آسیب‌های اجتماعی تمرکز دارد. به ریسک‌هایی که برای خود شرکت‌ها وجود دارد کمتر پرداخته شده است (مثلاً ریسک های دعاوی حقوقی یا شهرت (اعتبار))[۱۲]، اگرچه گاهی اوقات منافع خصوصی و عمومی همسو می‌شوند (مثلاً یکی از راه‌های کاهش ریسک دعاوی حقوقی، جلوگیری از اتفاقات است).

ادامه این مقاله به شرح زیر است. بخش ۲ یک نمای کلی از ساختار اساسی مدل، تاریخچه، انتقادها و پایه شواهد ارائه می دهد. بخش ۳ راه‌هایی را پیشنهاد می‌کند که شرکت‌های هوش مصنوعی می‌توانند مدل را پیاده سازی کنند. بخش ۴ چگونگی کمک به کاهش ریسک‌های ناشی از هوش مصنوعی را توضیح می‌دهد. بخش ۵ نتیجه گیری و سوالاتی را برای تحقیقات بیشتر پیشنهاد می‌کند.

۲. مدل سه خط

در این بخش، یک نمای کلی از ساختار اصلی (بخش ۲.۱) و تاریخچه مدل سه خط (بخش ۲.۲) ارائه می‌شود. همچنین برخی از انتقادهای اصلی بیان می‌شود، به طور خلاصه درباره مدل‌های جایگزین بحث می‌شود (بخش ۲.۳)، و شواهد تجربی را برای اثربخشی آن بررسی می‌کنیم (بخش ۲.۴).

---

[۱۰] Deep Mind در سال ۲۰۱۰ با رویکردی بین رشته ای برای ساخت سیستم های هوش مصنوعی عمومی شروع به کار کرد. این آزمایشگاه تحقیقاتی ایده‌ها و پیشرفت‌های جدید در یادگیری ماشین، علوم اعصاب، مهندسی، ریاضیات، شبیه‌سازی و زیرساخت‌های محاسباتی را همراه با روش‌های جدید سازمان‌دهی تلاش‌های علمی گرد هم آورد.

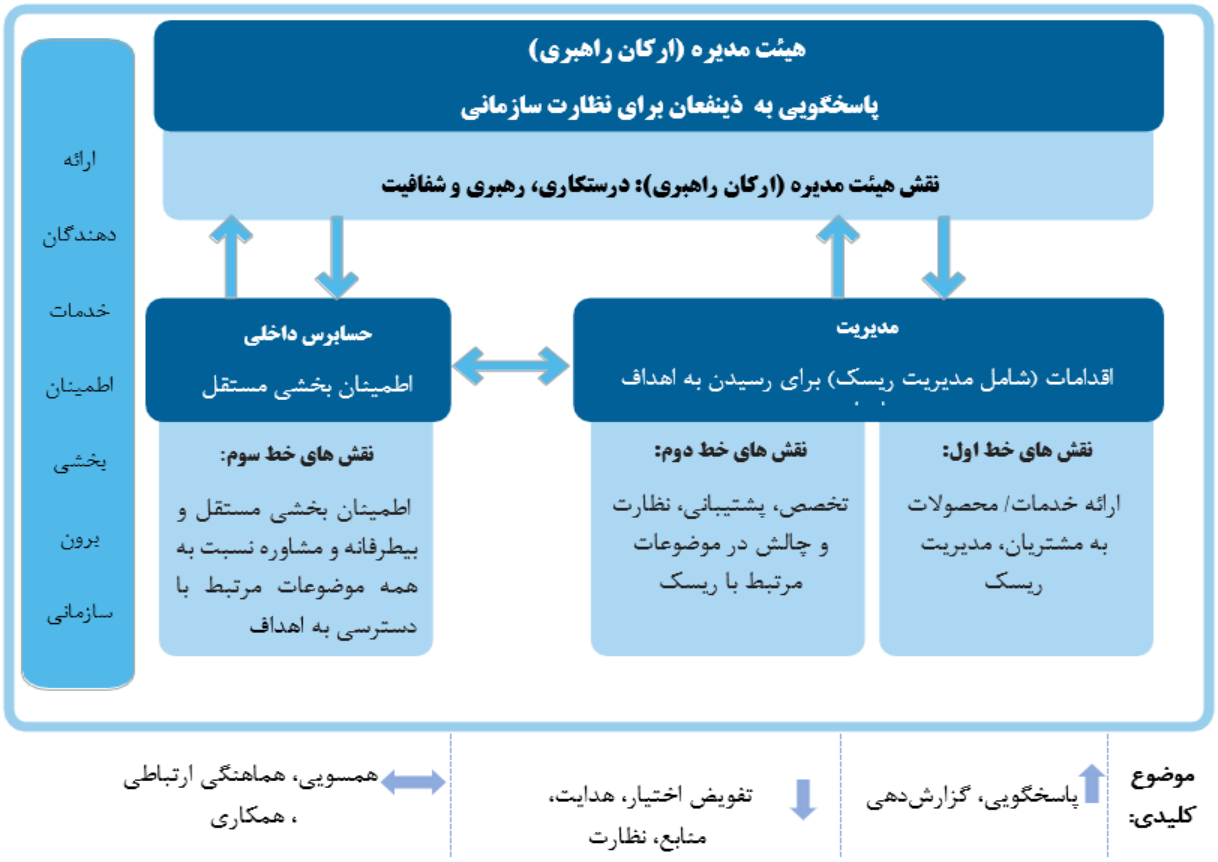
[۱۱] Open AI یک آزمایشگاه تحقیقاتی خصوصی است که هدف آن توسعه و هدایت هوش مصنوعی (AI) به روش هایی است که به نفع بشریت به عنوان یک کل نگر باشد. این شرکت توسط ایلان ماسک، سام آلتمن و دیگران در سال ۲۰۱۵ تاسیس شد و دفتر مرکزی آن در سانفرانسیسکو قرار دارد.

[۱۲] Litigation or Reputation Risks

۲.۱. ساختار اصلی

نسخه های مختلفی از مدل سه خط وجود دارد. اکثر متخصصان و محققان با نسخه منتشر شده توسط (IIA۲۰۱۳) آشنا هستند. پس از یک فرآیند بررسی، آنها نسخه به روز شده (IIA۲۰۲۰a) را منتشر کردند که به طور فزاینده‌ای جایگزین نسخه اصلی می‌شود. این مقاله عمدتاً از نسخه به روز شده استفاده می‌کند.

شکل۱: مدل سه خط توصیف شده توسط IIA۲۰۲۰a



همانطور که در شکل ۱ نشان داده شده است. مدل به روز شده دارای سه نوع آیتم است: بازیگران، نقش‌ها، و روابط.

این مدل بین چهار بازیگر که به عنوان جعبه آبی نشان داده می‌شوند تمایز قائل می‌شود: **هیئت‌مدیره** که برای نظارت سازمانی به ذینفعان پاسخگو است. **مدیریت** که برای دستیابی به اهداف سازمان اقداماتی را انجام می‌دهد. **حسابرسی داخلی**، که خدمات اطمینان‌بخشی مستقلی را به هیئت‌مدیره ارائه می‌دهد، و همچنین **ارائه‌دهندگان خدمات اطمینان‌بخشی برون‌سازمانی**.

این مدل بیشتر بین چهار نقش که به صورت جعبه های خاکستری نشان داده شده اند تمایز قائل می شود. **نقش هیئت‌مدیره** نشان دادن درستکاری، رهبری و شفافیت است. علاوه بر آن، این مدل شامل سه نقش است که آنها را «خطوط دفاعی» می‌نامد. **خط اول** محصولات و خدمات را به مشتریان ارائه می‌دهد و ریسک‌های مرتبط را

مدیریت می کند. **خط دوم** به خط اول در رابطه با مدیریت ریسک کمک می‌کند. این تخصص و پشتیبانی تکمیلی را ارائه می دهد، همچنین شیوه‌های مدیریت ریسک را نظارت و به چالش می‌کشد. **خط سوم** اطمینان بخشی و مشاوره مستقل و عینی را در مورد کلیه موارد مربوط به دستیابی به اهداف ریسک ارائه می‌دهد. دو خط اول بخشی از مدیریت هستند، در حالی که خط سوم مترادف با حسابرسی داخلی است.

در نهایت، سه نوع رابطه بین بازیگران مختلف وجود دارد که به صورت فلش نشان داده می‌شوند. روابط از **بالا به پایین** وجود دارد: هیئت مدیره مسئولیت را به مدیریت محول می‌کند و بر حسابرسی داخلی نظارت می‌کند. برعکس، روابط **پایین به بالا** وجود دارد: مدیریت و حسابرسی داخلی پاسخگو هستند و به بدنه راهبری گزارش می‌دهند. و در نهایت، یک رابطه **افقی** بین بازیگرانی وجود دارد که کارشان باید همسو باشد، یعنی بین مدیریت و حسابرسی داخلی.

۲.۲. تاریخچه مختصر

منشاء مدل مبهم است. تئوری‌هایی وجود دارد که ریشه‌های نظامی، ورزشی یا کنترل کیفیت را نشان می‌دهد احتمالاً در اواخر دهه ۱۹۹۰ یا اوایل دهه ۲۰۰۰ توسعه یافته است. در سال ۱۹۹۹، کمیته بازل[۱۳] در مورد نظارت بانکی (BCBS) رویکرد مشابهی را برای نظارت بر ریسک پیشنهاد کرد اما اولین اشاره صریح به این مدل احتمالاً در گزارشی توسط سازمان خدمات مالی بریتانیا [۱۴](۲۰۰۳) یا مقاله‌ای از این مدل بود.

پس از بحران مالی ۲۰۰۷-۲۰۰۸، که تا حدی ناشی از شکست‌های گسترده مدیریت ریسک بود، محبوبیت این مدل به شدت افزایش یافت. در پاسخ به بحران، قانونگذاران و مقامات نظارتی توجه فزاینده‌ای به مسئول ارشد ریسک (CRO)[۱۵] و کمیته ریسک هیئت‌مدیره[۱۶] معطوف داشتند و شروع به توصیه مدل سه خط کردند. بیشتر کارهای آکادمیک روی این مدل نیز پس از بحران انجام شد و قبل از آن بسیاری از متخصصان مدیریت ریسک فقط نام مدل جدید را شنیده بودند. امروزه اکثر شرکت های بورسی مدل سه خط را پیاده سازی کرده‌اند. در یک نظرسنجی در سال ۲۰۱۵ از متخصصان حسابرسی داخلی در ۱۶۶ کشور (n = ۱۴۵۱۸) اکثر پاسخ دهندگان (۷۵٪) گزارش دادند که سازمان آنها از مدل سه خط دفاعی که توسط انجمن حسابرسان داخلی ارائه شده است پیروی می کند. در میان مسولان ارشد حسابرسی (CAEs)[۱۷] در اتریش، آلمان و سوئیس (n = ۴۱۵)، از یافته‌های آنها پشتیبانی می‌کند. اکثر پاسخ دهندگان (۸۸٪) گزارش دادند که آنها این مدل را پیاده سازی کرده‌اند، به ویژه نرخ پذیرش بالا در بین موسسات مالی تا ۹۶٪ است.

در مقابل، به نظر نمی رسد شرکت های بزرگ فناوری مدل سه خط را پیاده سازی کنند. در هیچ یک از پرونده‌های آنها به کمیسیون بورس و اوراق بهادار ایالات متحده (SEC)[۱۸] یا سایر نشریات ذکر نشده است. این مدل همچنین

[۱۳] Basel Committee
[۱۴] UK Financial Services Authority
[۱۵] Chief risk officer
[۱۶] Risk Committee of the Board
[۱۷] Chief Audit Executives
[۱۸] Securities and Exchange Commission

به صراحت در الزامات راهبری شرکتی توسط نزدک ذکر نشده است، جایی که همه شرکت‌های بزرگ فناوری فهرست شده‌اند. با این حال، شایان ذکر است که شیوه های نظارت بر ریسک در شرکت های بزرگ فناوری شباهت هایی با مدل سه خط دارد. به عنوان مثال، به نظر می رسد همه آنها یک عملکرد حسابرسی داخلی را دارند (به عنوان مثال مایکروسافت ؛ آلفابت). بر اساس اطلاعات عمومی، آزمایشگاه‌های تحقیقاتی هوش مصنوعی با اندازه متوسط نیز به نظر نمی‌رسد این مدل را پیاده‌سازی کنند.

۲.۳. انتقادها و مدل‌های جایگزین

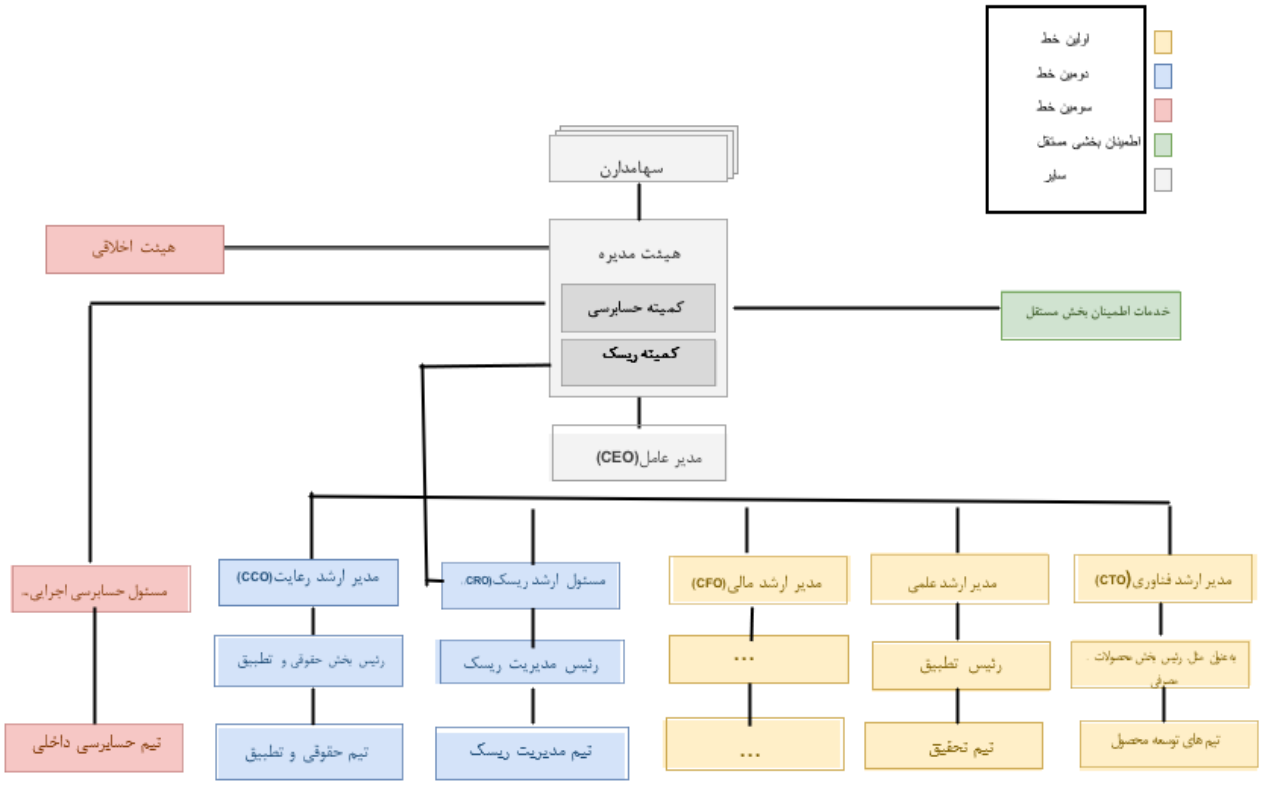
با وجود محبوبیت این مدل در بسیاری از صنایع، این مدل نیز مورد انتقاد قرار گرفته است چهار نقطه ضعف و شکست در مدل سه خط شناسایی شده است. **اول**، آنها استدلال می کنند که انگیزه‌های ریسک پذیری در خط اول اغلب نادرست است. زمانی که با جایگزینی بین ایجاد سود و کاهش ریسک مواجه می‌شوند، از لحاظ تاریخی انگیزه‌ای برای اولویت‌بندی ریسک‌های قبلی داشته‌اند. **دوم**، اغلب عدم استقلال سازمانی برای وظایف خط دوم وجود دارد. آنها بیش از حد به افراد منفعت طلب(سودجو) نزدیک هستند که می تواند منجر به اتخاذ نگرش‌های ریسک‌پذیرتر شود. **سوم**، عملکردهای خط دوم اغلب فاقد مهارت و تخصص لازم برای به چالش کشیدن شیوه‌ها و کنترل‌ها در خط اول است. و **چهارم**، اثربخشی حسابرسی داخلی به دانش، مهارت و تجربه افراد بستگی دارد که ممکن است ناکافی باشد. یکی دیگر از انتقادهای رایج این است که این مدل احساس امنیت کاذبی را ارائه می‌دهد. به زبان ساده، «وقتی چندین نفر مسئول هستند در واقع هیچ کس مسئول نیست»[۱۹] انتقاد دیگر این است که این مدل بیش از حد بوروکراتیک و پرهزینه است. لایه‌های نظارتی اضافی ممکن است ریسک را کاهش دهد، اما به قیمت کارآمدی مدل تمام می‌شود. آخرین انتقاد این مدل به جریان اطلاعات بین خطوط بستگی دارد، اما موانع زیادی برای این موضوع وجود دارد. به عنوان مثال، ممکن است خط دوم تشخیص ندهد که آنها فقط آنچه را که خط اول برای نشان دادن آنها انتخاب می‌کند، می‌بینند در حالی که این انتقادها کاستی‌های مربوط را مشخص می‌کند و باید جدی گرفته شود، اما مدل را به عنوان یک کل زیر سوال نمی‌برد. علاوه بر این، مدل سه خط در طول سالیان بهبود یافته است. امروزه تمرکز بر افزایش اثربخشی مدل و پاسخ به انتقادات است. با توجه به این انتقادات، چندین مدل جایگزین پیشنهاد شده‌اند. به عنوان مثال، مدل چهار خطی را برای پاسخگویی بهتر به نیازهای موسسات مالی پیشنهاد کردند. خط چهارم متشکل از مراجع نظارتی و حسابرسی برون سازمانی است که قرار است با حسابرسی داخلی همکاری نزدیک داشته باشند. مثال دیگر مدل پنج خطی است که به تدریج توسط چندین محقق و سازمان توسعه یافت با این حال، تغییرات پیشنهادی لزوماً مدل را بهبود نمی‌بخشد. استدلال شده است که افزودن خطوط بیشتر مدل را بیش از حد پیچیده می‌کند و شرکت ها و قانونگذاران در حال حاضر خواهان تغییرات ساختاری نیستند. همچنین شایان ذکر است که مدل های جایگزین به مراتب کمتر از مدل اصلی محبوب هستند. در مقایسه با این مدل‌های جایگزین، مدل سه خط همچنان «بادقت‌ترین سیستم مدیریت ریسک که تاکنون توسعه یافته است» باقی می‌ماند. اما چه شواهد تجربی برای اثربخشی آن داریم؟

[۱۹] when there are several people in charge—no one really is”

۲.۴. شواهد تجربی

منظور من از «اثربخشی» تعیین درجه‌ای که مدل مورد نظر به سازمان‌ها برای دستیابی به اهدافشان کمک می‌کند است.[۲۰] برای هدف این مقاله، من بیشتر به دستیابی به اهداف ریسک علاقه‌مند هستم. این ممکن است شامل موارد زیر باشد: (۱) کاهش ریسک‌های مربوط به سطح قابل قبول، (۲) اطمینان از آگاهی مدیریت و هیئت‌مدیره از ماهیت و مقیاس ریسک‌های کلیدی، و (۳) تطبیق با مقررات مربوط به ریسک. من کمتر به اهداف دیگر علاقه‌مند هستم (مثلاً بهبود عملکرد مالی)، اگر چه ممکن است همپوشانی‌هایی وجود داشته باشد (مثلاً کاهش ریسک آسیب به افراد ممکن است خطر زیان مالی ناشی از پرونده‌های دعاوی را کاهش دهد).

شکل ۲: نمونه نمودار سازمانی یک شرکت هوش مصنوعی با مسئولیت‌های معادل برای هر یک از سه خط



به نظر نمی‌رسد هیچ مطالعه (با کیفیت بالا) در مورد اثربخشی مدل سه خط به معنای فوق الذکر وجود داشته باشد. فقط به نظر می‌رسد که شواهدی برای اثربخشی حسابرسی داخلی وجود دارد به عنوان مثال، یک نظرسنجی از مسئولان اجرایی حسابرسی در شرکت های چند ملیتی در آلمان (n = ۳۷) واحدهای تجاری حسابرسی شده و حسابرسی نشده را مقایسه کرد. آنها دریافتند که مدیران واحدهای حسابرسی شده نسبت به مدیران واحدهای حسابرسی نشده کاهش ریسک بیشتری را تجربه می‌کنند. مطالعات دیگر نشان می دهد که حسابرسی داخلی به تقویت سیستم‌های کنترل داخلی کمک می‌کند و تاثیر مثبتی بر پیشگیری و شناسایی تقلب دارد به نظر می‌رسد

[۲۰] I mean the degree to which the model helps organizations to achieve their objectives.

این واقعیت که مدل سه خط قادر به جلوگیری از رسوایی‌ها و بحران‌های گذشته نبود، شواهد ضعیفی علیه اثربخشی آن ارائه می‌کند (اگرچه توضیح دیگر می‌تواند شامل ضعیف بودن مدل در اجرا باشد)، در حالی که به نظر می‌رسد محبوبیت مداوم مدل شواهد ضعیفی را ارائه می‌کند. به نفع اثربخشی آن (اگرچه محبوبیت مدل همچنان می‌تواند بسته به مسیر تشریح شود). در نهایت، شواهدی در هر دو جهت وجود دارد به طور کلی، با وجود محبوبیت این مدل، «اثربخشی آن آزموده نشده باقی می‌ماند» و «براساس هیچ مدرک روشنی نیست» که ما شواهد محکمی مبنی بر ناکارآمدی مدل داشته باشیم و هنوز هم بسیار قابل قبول است که این مدل می تواند مؤثر باشد، اما مطالعات (با کیفیت بالا) شواهد تجربی برای اثربخشی آن به معنای فوق الذکر ارائه نداده است.

این نقص (کمبود) شگفت انگیز شواهد، به طور بالقوه می‌تواند با دلایل زیر توضیح داده شود. **اول**، از آنجایی که اجرای کارآزمایی‌های تصادفی‌سازی و کنترل‌شده در مورد مداخلات سازمانی امکان‌پذیر نیست، جمع‌آوری شواهد قوی ذاتاً دشوار است. **دوم**، این مدل به گونه‌ای طراحی شده است که منعطف و سازگار باشد، به این معنی که یک نقشه راه واحد و استاندارد برای پیاده سازی آن وجود ندارد. این عدم استانداردسازی می تواند مقایسه پیاده سازی‌های مختلف مدل و ارزیابی اثربخشی آنها را دشوار کند. **سوم**، از آنجایی که بیشتر شاغلین عمدتاً به عملکرد مالی اهمیت می‌دهند، ممکن است محققان تشویق شوند تا بر معیارهای اقتصادی اثربخشی تمرکز کنند تا ارتباط کار خود را توجیه کنند (اگرچه شواهد زیادی در مورد آن وجود ندارد).

حتی اگر شواهد تجربی بیشتری از سایر صنایع داشته باشیم، ممکن است ارزش اطلاعاتی آن همچنان محدود باشد. یک دلیل این است که یافته ها ممکن است به هوش مصنوعی تعمیم نیابد.

یادداشت. شرکت‌های هوش مصنوعی از نظر ساختاری با سایر شرکت‌ها متفاوت هستند، زیرا تمرکز ویژه‌ای بر تحقیق دارند، و از آنجایی که هوش مصنوعی یک فناوری همه منظوره است، ریسک‌های ناشی از هوش مصنوعی گسترده‌تر از ریسک‌های سایر محصولات و خدمات است. دلیل دیگر این است که بزرگترین محرک توانایی مدل برای کاهش ریسک‌ها، احتمالاً روش مشخصی است که در آن اجرا می‌شود. بنابراین، شرکت‌های هوش مصنوعی به جای اینکه بپرسند «آیا مدل سه خط مؤثر است؟» باید بپرسند «چگونه می‌توانیم مدل را به روشی مؤثر پیاده‌سازی کنیم. »

۳. استفاده از مدل سه خط در زمینه هوش مصنوعی

این بخش راه‌هایی را پیشنهاد می‌دهد که شرکت‌های هوش مصنوعی می‌توانند مدل سه خط را پیاده سازی کنند. برای هر یک از سه خط، نقش ها و مسئولیت‌های معادل را پیشنهاد می‌دهد. ابتدا، محتوای مسئولیت‌های آن‌ها را شرح می‌دهد، سپس در مورد اینکه کدام تیم یا فردی مسئول است، همانطور که در شکل ۲ نشان داده شده است، بحث می‌شود.

۳.۱. خط اول

خط اول دو مسئولیت اصلی دارد: ارائه محصولات و خدمات به مشتریان، که مربوط به تحقیق و توسعه محصول هوش مصنوعی است، و مدیریت ریسک‌های مرتبط. در زیر، روی دومی تمرکز شده است.

خط اول مسئول ایجاد و حفظ ساختارها و فرآیندهای مناسب برای مدیریت ریسک است که شامل اقداماتی در تمام مراحل فرآیند مدیریت ریسک است. برای تشخیص ریسک‌ها، خط اول می تواند از تجزیه و تحلیل رویداد طبقه‌بندی ریسک استفاده کند. برای تخمین احتمال و تأثیر ریسک‌های مشخص‌شده، برای ارزیابی‌های احتمالی ریسک ممکن است از مطالعات دلفی[۲۱] یا از ماتریس‌های ریسک[۲۲] استفاده کنند. این تخمین‌ها معمولاً با ارزیابی مدل، به طور بالقوه با تمرکز بر قابلیت‌های مدل پر ریسک، و ارزیابی پادمان‌های شرکت اطلاع‌رسانی می‌شوند. برای کاهش ریسک‌ها، خط اول می‌تواند مدل را بر روی یک مجموعه داده انتخاب شده از طریق یادگیری تقویتی از بازخورد انسانی (RLHF)[۲۳] ، یا یادگیری تقویتی از بازخورد هوش مصنوعی (RLAIF)[۲۴]، که بیشتر به عنوان «هوش مصنوعی قانونی» شناخته می‌شود، تنظیم کند. برای جلوگیری از فاش شدن یا سرقت و ضریب اطمینان مدل، خط اول ممکن است اقداماتی را برای تقویت امنیت اطلاعات شرکت انجام دهد و برای جلوگیری از سوء استفاده، سیاستی را برای انتشار تحقیقات بالقوه مضر معرفی کنند همچنین ممکن است منطقی باشد که رویکردی جامع‌تر داشته باشیم و چارچوب مدیریت ریسک ویژه هوش مصنوعی را پیاده‌سازی و یا یک چارچوب کلی‌تر مدیریت ریسک سازمانی (ERM)[۲۵] را سفارشی سازی کنیم. چندین سازمان راهنمایی در مورد نحوه اعمال این چارچوب ها برای نیازهای خاص توسعه دهندگان هوش مصنوعی مرزی[۲۶] ارائه می‌دهند. و یا فقط اجازه دسترسی به مدل‌ها را از طریق یک رابط برنامه نویسی کاربردی (API)[۲۷] می‌دهند. در ماه‌های اخیر، ایجاد سیاست‌های خاص برای توسعه و استقرار مسئولانه سیستم‌های هوش مصنوعی مرزی، که به عنوان «سیاست‌های مقیاس‌پذیری مسئول» یا «سیاست‌های استقرار مبتنی بر ریسک» شناخته می‌شوند، رایج شده است. برای اکثر اقدامات ذکر شده در بالا، خط اول نیاز به حمایت خط دوم دارد.

خط اول همچنین مسئول اطمینان از تطبیق با انتظارات قانونی، مقرراتی و اخلاقی است. تعهدات قانونی ممکن است ناشی از قانون ضد تبعیض[۲۸] باشد.

قانون حفاظت از داده ها یا قانون ضد تراست یک مثال قابل توجه از مقررات هوش مصنوعی، قانون پیشنهادی هوش مصنوعی اتحادیه اروپا (کمیسیون اروپایی ۲۰۲۱)[۲۹] است که ارائه دهندگان سیستم های هوش مصنوعی پر

---

[۲۱] در سناریوهای ارزیابی ریسک، روش دلفی به شناسایی ریسک های بالقوه و ارزیابی احتمالات و اثرات آنها کمک می کند .کارشناسان دید جامعی از ریسک ها ارائه می دهند و سازمان ها را قادر می سازند تا استراتژی های مدیریت ریسک موثری را طراحی کنند.

[۲۲] ماتریس ریسک ماتریسی است که در هنگام ارزیابی ریسک برای تعریف سطح ریسک با در نظر گرفتن مقوله احتمال در مقابل دسته شدت پیامد استفاده می شود. این یک مکانیسم ساده برای افزایش دید ریسک ها و کمک به تصمیم گیری مدیریت است.

[۲۳] Reinforcement learning from human feedback

[۲۴] Reinforcement learning from AI feedback

[۲۵] Enterprise Risk Management

[۲۶] Frontier AI هوش مصنوعی مرزی واژه‌ای است که برای توصیف مدل‌های هوش مصنوعی استفاده می‌شود که از نظر قابلیت‌ها یا وظایف مختلف با مدل‌های پیشرفته هوش مصنوعی موجود مطابقت دارند یا بهتر عمل می‌کنند. در حال حاضر، «هوش مصنوعی مرزی» به معنای مدل‌های پایه یا هوش مصنوعی همه منظوره (GPAI) است. این اصطلاح به مدل‌های پایه بسیار توانمندی که می‌توانند قابلیت‌های خطرناکی داشته باشند اشاره می‌کند به عبارت دیگر، «هوش مصنوعی مرزی» حدس و گمان است و حتی هنوز وجود هم ندارد، اما می تواند در گوشه و کنار وجود داشته باشد.

[۲۷] Application Programming Interface

[۲۸] Anti-Discrimination

[۲۹] EU AI Act (European Commission)

ریسک را ملزم به پیاده سازی یک سیستم مدیریت ریسک می‌کند. انتظارات اخلاقی ممکن است ناشی از اصول اخلاقی هوش مصنوعی باشد که سازمان ها به صورت داوطلبانه اتخاذ کرده اند. برای اطمینان از تطبیق، خط اول به پشتیبانی خط دوم متکی است.

در نهایت، خط اول مسئول اطلاع رسانی به ارکان راهبری در مورد نتایج اقدامات ذکر شده در بالا، میزان برآورده شدن اهداف ریسک و سطح کلی ریسک است. این باید به شکل یک گفتگوی مستمر، از جمله گزارش در مورد نتایج مورد انتظار و واقعی باشد. گزارش‌ها معمولاً شامل سوابق ریسک و ماتریس‌های ریسک می‌شوند، اما می‌توانند شامل اطلاعاتی در مورد مدل‌های خاص، به شکل کارت‌های مدل، برگه‌های داده باشند و باید توجه داشته باشید که یک خط گزارش از مسئول ارشد ریسک (CRO) به مسئول ارشد اجرایی (CEO)[۳۰] و کمیته ریسک هیئت‌مدیره نیز وجود داشته باشد.

مدیران عملیاتی، اغلب در یک ساختار مسئولیت آبشاری، مسئول هستند. در شرکت‌های بزرگ فناوری، کمترین سطح مسئولیت متوجه مدیرانی است که مسئولیت توسعه تک تک محصولات هوش مصنوعی را بر عهده دارند. اگر محصول مستقل هوش مصنوعی وجود نداشته باشد و سیستم‌های هوش مصنوعی تنها بخشی از یک محصول را تشکیل می‌دهند مثلاً WaveNet[۳۱] به عنوان بخشی از Google Assistant، کمترین سطح مسئولیت بر عهده مدیرانی است که توسعه بخش هوش مصنوعی را رهبری می‌کنند. در آزمایشگاه‌های تحقیقاتی متوسط، پایین‌ترین سطح مسئولیت مدیریت ریسک بر عهده رهبران تحقیقاتی است، یعنی محققان ارشدی که مسئول پروژه‌های تحقیقاتی فردی هستند.

معمولاً یک یا چند سطح متوسط از مسئولیت وجود خواهد داشت که ممکن است شامل تعدادی از مدیران سطح متوسط باشد که مسئول حوزه‌های گسترده‌تر محصول (مانند بازی) یا حوزه‌های تحقیقاتی (مانند یادگیری تقویتی) هستند، اگرچه جزئیات این موضوع به ساختارهای سازمانی خاص بستگی دارد. مسئولیت نهایی مدیریت ریسک هوش مصنوعی بر عهده آن دسته از مدیران C-suite[۳۲] است که مسئولیت توسعه محصول به عنوان مثال مدیر ارشد فناوری (CTO)[۳۳] یا تحقیق مثلاً مدیر ارشد علمی (CSO)[۳۴]را بر عهده دارند. در حالی که امکان تقسیم مسئولیت ها بین دو یا چند مدیر اجرایی وجود دارد اغلب این موضوع توصیه نمی‌شود، زیرا می‌تواند باعث کاهش مسئولیت‌ها شود.

---

[۳۰] Chief Executive Officer

[۳۱] WaveNet یک شبکه عصبی عمیق برای تولید صدای خام است که توسط محققان شرکت هوش مصنوعی مستقر در لندن Deep Mind ایجاد شده است.

[۳۲] گروهی از مدیران اجرایی است که مسئولیت اداره یک سازمان را بر عهده دارند

[۳۳] Chief Technology Officer

[۳۴] E Chief Scientific Officer

۳.۲. خط دوم

با توجه به مدیریت ریسک خط دوم تخصص و پشتیبانی تکمیلی را ارائه می‌دهد، اما همچنین شیوه‌های مدیریت ریسک را نیز نظارت و به چالش می‌کشد.

برخی از فعالیت های مدیریت ریسک به تخصص خاصی نیاز دارند که خط اول آن را ندارد. ممکن است شامل تخصص حقوقی باشد به عنوان مثال: نحوه انطباق با الزامات مدیریت ریسک مندرج در قانون پیشنهادی هوش مصنوعی اتحادیه اروپا، تخصص فنی به عنوان مثال: نحوه ارزیابی قابلیت های مدل پر ریسک یا توسعه مدل های زبانی واقعی‌تر یا تخصص اخلاقی به عنوان مثال: چگونگی تعریف آستانه‌های هنجاری برای مطلوبیت ممکن است شامل تخصص ویژه ریسک باشد به عنوان مثال: مدل‌های زبانی[۳۵] چه ریسک‌هایی دارند یا تخصص ویژه مدیریت ریسک به عنوان مثال: بهترین شیوه‌ها برای فیلترهای ایمنی تیم قرمز. خط دوم می‌تواند خط اول را با تهیه پیش نویس خط مشی‌ها، فرآیندها و رویه‌ها و همچنین چارچوب‌ها، قالب‌ها و طبقه‌بندی‌ها پشتیبانی کند. همچنین ممکن است در مورد مسائل خاص توصیه کند به عنوان مثال: چگونه یک چارچوب مدیریت ریسک را سفارشی سازی کنیم تا نیازهای خاص شرکت را بهتر برآورده کنیم. راهنمایی‌های کلی ارائه کنیم به عنوان مثال نحوه اطمینان از انطباق با سیاست‌های مربوط به ایمنی در بین محققان و مهندسان یا ارائه آموزش به عنوان مثال: نحوه پردازش داده‌های آموزشی به روشی مطابق با مقررات عمومی حفاظت از داده‌ها (GDPR)[۳۶].

خط دوم همچنین مسئول نظارت و به چالش کشیدن کفایت و اثربخشی شیوه‌های مدیریت ریسک است. اگر اهداف ریسک برآورده نشود (مثلاً شرکت قوانین و مقررات مربوط را رعایت نکند، یا نتواند ریسک‌ها را تا حد قابل قبولی کاهش دهد) شیوه‌های مدیریت ریسک غیراثربخش است یا اگر می‌توانست با منابع کمتر به نتایج مشابهی دست یابد، آنها ناکافی هستند. خط دوم معمولاً از تعدادی شاخص کلیدی عملکرد (KPI)[۳۷] برای ارزیابی ابعاد مختلف کفایت و اثربخشی مدیریت ریسک (مثلاً تعداد ریسک‌های شناسایی شده، تعداد اتفاقات یا درصد پرسنل آموزش دیده در مورد موضوعات خاص) استفاده می‌کند.

مسئولیت های خط دوم در چندین تیم تقسیم می‌شود که معمولاً شامل تیم مدیریت ریسک و همچنین تیم حقوقی و انطباق می‌شود. اگرچه اکثر شرکت‌های بزرگ فناوری در حال حاضر یک تیم مدیریت ریسک دارند، اما این تیم‌ها بیشتر درگیر ریسک‌های تجاری هستند (مانند دعوی قضایی یا ریسک شهرت). ریسک‌های ناشی از هوش مصنوعی، به ویژه ریسک‌های اجتماعی، معمولاً یک نگرانی عمده نیستند. اگر شرکت‌های بزرگ فناوری بخواهند این را تغییر دهند، می‌توانند مسئولیت‌های تیم‌های موجود را گسترش دهند. راه اندازی یک تیم جدید مدیریت ریسک ویژه هوش مصنوعی چندان مطلوب به نظر نمی‌رسد، زیرا می تواند منجر به پراکندگی مسئولیت‌ها شود. احتمالاً یک ساختار مسئولیت آبشاری وجود دارد که در آن مسئول ارشد ریسک به عنوان واحد پاسخگویی

---

[۳۵] مدل‌های زبان هوش مصنوعی جزء کلیدی پردازش زبان طبیعی (NLP) هستند، حوزه‌ای از هوش مصنوعی (AI) که بر توانمندسازی رایانه‌ها برای درک و تولید زبان انسان متمرکز است.

[۳۶] General Data Protection Legislation

[۳۷] Key Performance Indicators

برای فرآیند مدیریت ریسک عمل می‌کند. آزمایشگاه‌های تحقیقاتی متوسط معمولاً تیم مدیریت ریسک اختصاصی ندارند. یک استثنای قابل توجه مربوط به تیم جدید آمادگی OpenAI است. آنها می‌توانند یک تیم جدید راه‌اندازی کنند یا یک یا چند نفر را در تیم‌های دیگر با عملکردهای پشتیبانی مرتبط با مدیریت ریسک مأمور کنند.
همه شرکت‌های هوش مصنوعی فراتر از مرحله راه‌اندازی اولیه، یک تیم حقوقی و انطباق دارند. سرپرست تیم، و در نهایت مسئول ارشد انطباق (CCO)[۳۸] یا مسئول ارشد حقوقی (CLO)[۳۹]، مسئول پشتیبانی حقوقی و انطباق مرتبط با ریسک خواهد بود. شایان ذکر است که تیم حقوقی و انطباق نیز در صورتی که واقعاً مسئولیت اطمینان از انطباق را بر عهده داشته باشند، می توانند جزء خط اول باشند. اگر قدرت تصمیم گیری نداشته باشند و فقط از خط اول حمایت کنند (مثلاً با نوشتن نظرات حقوقی) جزء خط دوم هستند. تیم حقوقی و انطباق نیز می‌توانند از شرکت های حقوقی برون سازمانی پشتیبانی بگیرند.
بسیاری از سازمان‌هایی که سیستم‌های هوش مصنوعی را توسعه و استقرار می‌دهند، تیم‌های دیگری دارند که می‌توانند مسئولیت‌های خط دوم را بر عهده بگیرند که ممکن است شامل تیم‌های ایمنی فنی، اخلاقی، خط مشی یا راهبری باشد. با این حال، در عمل، این تیم ها به ندرت خود را مسئول مدیریت ریسک می دانند. این موضوع باید هنگام اجرای مدل سه خط در نظر گرفته شود (به عنوان مثال با راه اندازی کارگاه‌ها برای حساس کردن آنها به مسئولیت گسترده خود). به طور کلی، شرکت‌های هوش مصنوعی باید از واگذاری مسئولیت‌های خط دوم به آنها اجتناب کنند.

۳.۳. خط سوم

خط سوم مسئول ارائه اطمینان بخشی مستقل است. کار دو خط اول را ارزیابی می کند و هر گونه کاستی را به ارکان راهبری گزارش می دهد.
در حالی که خط دوم در حال حاضر کفایت و اثربخشی شیوه های مدیریت ریسک را نظارت می‌کند و به چالش می‌کشد، خط سوم به طور مستقل کار آنها را ارزیابی می‌کند و به اصطلاح بر سرپرستان نظارت می‌کنند. آنها می‌توانند این کار را با انجام مصاحبه (مثلاً با رهبران تحقیقاتی) و شرکت در جلسات (به عنوان مثال جلسات منظم تیم‌های توسعه) انجام دهند. آنها همچنین می توانند حسابرسی داخلی انجام دهند یا حسابرسی برون سازمانی را سفارش دهند، چنین حسابرسی می‌تواند اهداف و دامنه‌های متفاوتی داشته باشد. آنها می‌توانند انطباق با قوانین، استانداردها یا اصول اخلاقی («حسابرسی رعایت») را ارزیابی کنند یا به دنبال شناسایی ریسک‌های جدید به روشی بازتر باشند («حسابرسی ریسک»). آنها همچنین می‌توانند خود مدل را ارزیابی کنند، از جمله مجموعه داده‌ای که بر روی آن آموزش داده شده است («حسابرسی مدل»)، تاثیر مدل («حسابرسی تاثیر»)، یا راهبری شرکتی («حسابرسی راهبری»). به طور مشابه، خط سوم می تواند یک تیم قرمز را قبل یا بعد از استقرار یک مدل درگیر کند تا ارزیابی کند که آیا دو خط اول قادر به شناسایی کلیه ریسک‌های مربوط هستند یا خیر. علاوه بر آن، خط سوم می‌تواند خط‌مشی‌ها و فرآیندهای کلیدی را برای یافتن نقص‌ها و آسیب‌پذیری‌ها بررسی کند مثلاً

[۳۸] Chief Compliance Officer
[۳۹] Chief Legal Officer

خط‌مشی مقیاس‌پذیری مسئولانه یک شرکت یا پروتکل استقرار آنها. (توجه داشته باشید که این باید شامل یک فرا ارزیابی از اجرای خود مدل سه خط نیز باشد).

خط سوم همچنین با ارائه اطلاعات مستقل و بی‌طرفانه در مورد شیوه‌های مدیریت ریسک شرکت، از ارکان راهبری، معمولاً هیئت مدیره، پشتیبانی می‌کند. مخاطبان اصلی آنها معمولاً کمیته حسابرسی است که عمدتاً از مدیران غیرموظف تشکیل شده است. اما از آنجایی که مدیران غیرموظف فقط به صورت پاره وقت کار می‌کنند و به شدت به اطلاعاتی که توسط مدیران به آنها ارائه می‌شود وابسته هستند، آنها به یک متحد[۴۰] مستقل در شرکت برای نظارت مؤثر بر مدیران نیاز دارند. خط سوم با حفظ درجه بالایی از استقلال از مدیریت و گزارش مستقیم به ارکان راهبری با پیروی از بهترین شیوه‌ها، این کار را انجام می‌دهد. اغلب به عنوان «چشم و گوش»[۴۱] ارکان راهبری توصیف می‌شوند.

خط سوم یک جایگاه سازمانی کاملاً مشخص دارد: حسابرسی داخلی. توجه داشته باشید که در این زمینه، حسابرسی داخلی به یک واحد سازمانی خاص اشاره دارد . این صرفاً به معنای حسابرسی نیست که به صورت داخلی انجام شود در عوض، این به معنای «آن دسته از افرادی است که به طور مستقل از مدیریت برای ارائه اطمینان و بینش، در مورد کفایت و اثربخشی راهبری و مدیریت ریسک (از جمله کنترل داخلی) فعالیت می‌کنند. به طور معمول، شرکت‌ها یک تیم حسابرسی داخلی اختصاصی دارند که توسط CAE[۴۲] یا رئیس حسابرسی داخلی رهبری می‌شود. اکثر شرکت‌های بزرگ فناوری چنین تیمی دارند، اما مشابه تیم مدیریت ریسک، اغلب از ریسک-های اجتماعی ناشی از هوش مصنوعی غفلت می‌کنند. به جای ایجاد یک تیم حسابرسی داخلی جداگانه مخصوص هوش مصنوعی، آنها باید یک تیم فرعی در تیم حسابرسی داخلی موجود خود ایجاد کنند یا به سادگی یک یا چند عضو تیم را موظف کنند تا بر فعالیت‌های مدیریت ریسک خاص هوش مصنوعی تمرکز کنند. آزمایشگاه‌های تحقیقاتی متوسط معمولاً تیم حسابرسی داخلی ندارند. آنها باید یک تیم یا وظیفه جدید حداقل یک نفر با مسئولیت‌های خط سوم ایجاد کنند. به طور خلاصه، شرکت‌های بزرگ فناوری باید «هوش مصنوعی را به حسابرسی داخلی بیاورند»،[۴۳] در حالی که آزمایشگاه‌های تحقیقاتی باید «حسابرسی داخلی را به هوش مصنوعی بیاورند». شایان ذکر است که اگرچه پیشرفت‌های امیدوارکننده‌ای وجود دارد اما حرفه حسابرسان داخلی خاص هوش مصنوعی هنوز در مراحل ابتدایی خود است.

برخی از شرکت‌های هوش مصنوعی دارای یک هیئت اخلاقی هستند (مانند کمیته اتر مایکروسافت و هیئت نظارت متا) که معمولاً علاوه بر حسابرسی داخلی می‌تواند مسئولیت‌های خط سوم را نیز بر عهده بگیرد. باید از نظر سازمانی مستقل از مدیریت باشد، اما همچنان بخشی از سازمان باشد (برخلاف ارائه دهندگان اطمینان بخشی برون سازمانی). اگر سازمان‌ها قبلاً یک هیئت مستقل اخلاقی داشته باشند (مثلاً متشکل از نمایندگان دانشگاه و جامعه مدنی)، می‌توانند یک گروه کاری تشکیل دهند که مسئولیت‌های خط سوم را بر عهده می‌گیرد.

---

[۴۰] Ally
[۴۱] Eyes and Ears
[۴۲] Head of Internal Audit
[۴۳] Bring AI to Internal Audit

۴. چگونه مدل سه خط می‌تواند به کاهش ریسک‌های ناشی از هوش مصنوعی کمک کند

در حالی که دلایل زیادی وجود دارد که چرا شرکت‌های هوش مصنوعی ممکن است بخواهند مدل سه خط دفاعی را پیاده‌سازی کنند، اما این بخش فقط بر سه استدلال در مورد توانایی این مدل برای جلوگیری از آسیب‌های فردی، جمعی و اجتماعی تمرکز می‌کند. این مدل می‌تواند با شناسایی و بستن شکاف‌ها به کاهش ریسک‌های ناشی از هوش مصنوعی کمک کند. در پوشش ریسک (بخش ۴.۱)، افزایش اثربخشی شیوه‌های مدیریت ریسک (بخش ۴.۲)، و قادر ساختن ارکان راهبری برای نظارت مؤثرتر بر مدیریت (بخش ۴.۳) همچنین یک نمای کلی از مزایای دیگر ارائه می‌شود (بخش ۴.۴). شایان ذکر است که در غیاب شواهد تجربی قوی ، بحث زیر نظری باقی می‌ماند و اغلب بر ملاحظات قابل قبول انتزاعی تکیه می‌کند.

۴.۱. تشخیص و بستن شکاف‌ها در پوشش ریسک

مدیریت ریسک هوش مصنوعی شامل افراد مختلف از تیم های مختلف با مسئولیت‌های متفاوت است. اگر این مسئولیت‌ها به اندازه کافی هماهنگ نباشند، شکاف‌هایی در پوشش ریسک ممکن است رخ دهد. چنین شکاف‌هایی ممکن است دلایل مختلفی داشته باشند. به عنوان مثال، ممکن است هیچ کس مسئول مدیریت یک ریسک خاص نباشد (مثلاً ممکن است نقطه کوری[۴۴] برای ریسک‌های پراکنده[۴۵] وجود داشته باشد)، یا ممکن است مشخص نباشد که چه کسی مسئول است (مثلاً ممکن است دو تیم به اشتباه تصور کنند که تیم دیگر در حال حاضر از یک ریسک مراقبت می کند). همچنین ممکن است فرد مسئول نتواند ریسک را به طور موثر مدیریت کند (به عنوان مثال به دلیل نداشتن تخصص، اطلاعات یا زمان لازم). اگر یک ریسک خاص به اندازه کافی توسط سیستم مدیریت ریسک پوشش داده نشود، نمی‌توان آن را تشخیص داد و ممکن است منجر به ارزیابی ریسک نادرست شود مثلاً ریسک کل یک سیستم هوش مصنوعی ناایمن[۴۶]، قابل قبول ارزیابی شود و یک پاسخ ریسک ناکافی (مثلاً ناایمن) دریافت و سیستم هوش مصنوعی بدون اقدامات احتیاطی کافی مستقر شده باشد.

مدل سه خط می تواند با تشخیص و بستن شکاف‌ها در پوشش ریسک از این امر جلوگیری کند. می‌تواند این کار را با ارائه روشی نظام‌مند برای تخصیص و هماهنگ کردن نقش‌ها و مسئولیت‌های مرتبط با مدیریت ریسک انجام دهد. این موضوع اطمینان بخشی می‌کند که افرادی که نزدیک به ریسک هستند، مسئولیت مدیریت ریسک (خط اول) را بر عهده دارند و حمایت مورد نیاز خود را دریافت می کنند (خط دوم). راه دیگری که مدل سه خط می تواند به تشخیص نقاط کور کمک کند، از طریق عملکرد حسابرسی داخلی (خط سوم) است. آنها مسئول ارزیابی کفایت و اثربخشی کل الگوی[۴۷] مدیریت ریسک هستند که شامل شکاف‌های بالقوه در پوشش ریسک است.

ممکن است کسی اعتراض کند که در عمل، وجود شکاف در پوشش ریسک نادر است، و حتی اگر رخ دهد، فقط به ریسک‌های جزئی مربوط می شود (مثلاً به این دلیل که شرکت های هوش مصنوعی راه‌های دیگری برای

[۴۴] Blind Spot
[۴۵] Diffuse Risks
[۴۶] Total Risk of an unsafe AI system
[۴۷] Regime

رسیدگی به بزرگترین ریسک‌ها پیدا کرده‌اند). با این حال، پایگاه داده رویدادهای هوش مصنوعی[۴۸] حاوی ورودی‌های متعددی است، از جمله موارد متعددی که به عنوان «متوسط» یا «شدید»[۴۹] طبقه‌بندی شده‌اند، که نشان می‌دهد رویدادها چندان غیر معمول نیستند. در حالی که این رویدادها دلایل مختلفی داشتند، به نظر می‌رسد که حداقل برخی از آنها به شکاف‌هایی در پوشش ریسک مرتبط باشند. اما از آنجایی که به نظر نمی‌رسد اطلاعات عمومی در این مورد وجود داشته باشد، این موضوع همچنان حدس و گمان است.

حتی اگر کسی فکر کند که شکاف در پوشش ریسک یک مشکل رایج در میان شرکت‌های هوش مصنوعی است، ممکن است توانایی مدل برای تشخیص و بستن آن‌ها را زیر سوال ببریم. ممکن است کسی مشکوک شود که افراد درگیر و توانایی و تمایل آنها برای تشخیص شکاف ها نقش بسیار بیشتری ایفا می‌کنند. در حالی که مطمئناً درست است که اجرای مدل به تنهایی کافی نیست، داشتن پرسنل توانا و مشتاق نیز کافی نیست. هر دو ضروری هستند و تنها با هم می توانند کافی باشند (اگرچه عوامل دیگری مانند اشتراک اطلاعات بین واحدهای سازمانی مختلف نیز ممکن است نقش داشته باشند).

به طور کلی، به نظر می‌رسد که اجرای مدل سه خط به کشف برخی از شکاف‌ها در پوشش ریسک کمک کند که در غیر این صورت مورد توجه قرار نمی‌گیرند.

۴.۲. افزایش اثربخشی شیوه‌های مدیریت ریسک

برخی از شیوه‌های مدیریت ریسک بی‌اثر هستند، ممکن است روی کاغذ خوب به نظر برسند، اما در عمل کارایی ندارند. شرکت‌های هوش مصنوعی ممکن است در تشخیص ریسک‌های مربوط شکست بخورند، احتمال یا تأثیر آنها را اشتباه ارزیابی کنند یا نتوانند آنها را به سطح قابل قبولی کاهش دهند. شیوه‌های ناکارآمد مدیریت ریسک می‌توانند دلایل مختلفی داشته باشند، مانند تکیه بر یک معیار واحد (مثلاً استفاده از یک طبقه‌بندی واحد برای تشخیص طیف وسیعی از ریسک‌ها)، عدم پیش‌بینی تلاش‌های عمدی برای دور زدن اقدامات (مانند سرقت یک مدل منتشر نشده)، عدم پیش‌بینی تغییرات مرتبط در چشم انداز ریسک (به عنوان مثال: ظهور ریسک‌های سیستماتیک به دلیل اتکای فزاینده سوگیری‌های شناختی مدیران ریسک بر روی مدل های پایه به عنوان مثال: سوگیری در دسترس بودن، یعنی تمایل به "ارزیابی فراوانی یک طبقه یا احتمال یک رویداد با سهولت یادآوری موارد یا رخدادها"، و سایر خطاهای انسانی (مثلاً فردی که یک ثبت ریسک را پر می‌کند و اشتباه بیرون می‌زند). مدل سه خط می تواند اثربخشی شیوه‌های مدیریت ریسک را با تشخیص چنین کاستی‌هایی[۵۰] افزایش دهد. همانطور که در بالا ذکر شد، حسابرسان داخلی اثربخشی رویه‌های مدیریت ریسک را ارزیابی می‌کنند و هرگونه کاستی را به ارکان راهبری گزارش می‌دهند که می‌تواند با مدیریت برای بهبود این شیوه‌ها تعامل داشته باشد.

ممکن است کسی اعتراض کند که بیشترکاستی‌ها فقط در موقعیت‌های کم ریسک رخ می‌دهند. در موقعیت‌های پرریسک، شیوه‌های مدیریت ریسک موجود مؤثرتر هستند. برای مثال، شرکت‌های هوش مصنوعی اغلب

[۴۸] AI Incident Database
[۴۹] “Moderate” or “Severe”
[۵۰] Shortcomings

ارزیابی‌های گسترده‌ای از ریسک، قبل از استقرار مدل‌های پیشرفته انجام می‌دهند که این ممکن است در موارد آشکار، صادق باشد ولی در موارد کمتر آشکار به اندازه مورد نظر مؤثر نباشد مثلاً به این دلیل که نسبت به خطاهای انسانی یا تلاش های عمدی برای دور زدن آنها حساس نیستند. به عنوان مثال، اخیرا یک پست وبلاگی منتشر کرده است که در آن برخی از چالش‌هایی را که در هنگام ارزیابی مدل‌ها با آن مواجه شده‌اند، بیان می‌کند. در برابر این موضوع، من مطمئناً نمی‌خواهم به این استدلال متقابل تکیه کنم که اثربخشی شیوه‌های مدیریت ریسک در حال حاضر به اندازه کافی با ریسک‌های موجود افزایش می‌یابد.

برخی از شرکت‌های هوش مصنوعی ممکن است اعتراض کنند که از قبل معادل یک عملکرد حسابرسی داخلی داشتند، بنابراین پیاده‌سازی مدل سه خط تنها یک پیشرفت حاشیه‌ای خواهد بود. اگرچه ممکن است درست باشد که برخی از افراد در برخی از شرکت‌ها وظایفی مشابه آنچه حسابرسان داخلی انجام می‌دهند انجام می‌دهند، تا آنجا که من می‌دانم، ارزیابی اثربخشی رویه‌های مدیریت ریسک مسئولیت اصلی آنها نیست و بهترین شیوه‌ها را دنبال نمی‌کنند و مانند حرفه حسابرسی داخلی، مستقل بودن سازمانی از مدیریت را ندارند، که می‌تواند به تفاوت‌های قابل توجهی منجر شود.

به طور کلی، من فکر می‌کنم این یکی از بهترین استدلال‌ها برای پیاده سازی مدل سه خط است. بدون تلاش جدی برای تشخیص شیوه‌های ناکارآمد مدیریت ریسک ، انتظار می‌رود حداقل برخی از کاستی‌ها مورد توجه قرار نگیرد. میزان صحت این موضوع عمدتاً به توانایی و تمایل حسابرسی داخلی برای انجام این وظیفه بستگی دارد.

۴.۳. توانمندسازی ارکان راهبری برای نظارت موثرتر بر مدیریت

ارکان راهبری، بطور معمول هیئت مدیره، مسئول نظارت بر مدیریت است. برای انجام این کار، آنها به اطلاعات مستقل و عینی در مورد شیوه‌های مدیریت ریسک شرکت نیاز دارند. با این حال، آنها به شدت به اطلاعاتی که مدیران اجرایی در اختیار آنها قرار می‌دهند، متکی هستند. برای نظارت موثر بر مدیران، آنها به یک متحد(هم پیمان) مستقل در شرکت نیاز دارند.

حسابرسی داخلی این وظیفه را با حفظ درجه بالایی از استقلال از مدیریت و گزارش مستقیم به کمیته حسابرسی هیئت مدیره انجام می دهد. این موضوع می تواند مهم باشد زیرا در مقایسه با سایر بازیگران، هیئت مدیره تأثیر قابل توجهی بر مدیریت دارد. برای مثال، آنها می‌توانند مدیر عامل را عوض کنند (مثلاً اگر مکرراً سود را بر ایمنی (صحت و سقم) اولویت می‌دهد)، تصمیم‌های راهبردی بگیرند (مثلاً جلوگیری از مشارکت راهبردی با ارتش)[۵۱]، و تغییراتی در راهبری ریسک شرکت ایجاد کنند (مثلاً ایجاد یک هیئت اخلاقی). توجه داشته باشید که یک خط گزارش تکمیلی از مسئول ارشد ریسک به کمیته ریسک هیئت‌مدیره وجود دارد.

ممکن است کسی اعتراض کند که این عملکرد می تواند توسط بازیگران دیگر نیز انجام شود. برای مثال، حسابرسان شخص ثالث[۵۲] نیز می‌توانند اطلاعات مستقل و عینی را در اختیار هیئت مدیره قرار دهند. در حالی که حسابرسی-های برون سازمانی قطعاً می توانند نقش مهمی ایفا کنند، آنها در مقایسه با حسابرسی داخلی دارای معایبی

[۵۱] blocking a strategic partnership with the military
[۵۲] third-party auditors

هستند: ممکن است فاقد زمینه‌های مهم شناخت باشند[۵۳]، شرکت‌ها ممکن است نخواهند اطلاعات حساسی را با آنها به اشتراک بگذارند (مثلاً در مورد پروژه های تحقیقاتی در حال انجام)، و حسابرسی‌ها معمولاً فقط گزارش لحظه‌ای[۵۴] در یک زمان هستند. بنابراین، شرکت‌های هوش مصنوعی باید حسابرسی برون سازمانی را مکمل حسابرسی داخلی بدانند، نه یک جایگزین. به همین دلیل است که مدل سه خط، بین حسابرسی داخلی و ارائه دهندگان اطمینان بخشی برون سازمانی تمایز قائل می‌شود.

می‌توان به این نکته اشاره کرد که در صنایع دیگر، حسابرسی داخلی اغلب دیر مداخله می‌کند و به جای نظارت بر آنها، با مدیریت همکاری می‌کند و این واقعاً مشکل ساز خواهد بود. با این حال، همانطور که در بالا مورد بحث قرار گرفت، به نظر نمی رسد که این ویژگی ذاتی حسابرسی داخلی باشد. در عوض، به نظر می‌رسد که عمدتاً به روشی خاص راه‌اندازی می‌شود و افراد درگیر هدایت می‌شوند. با این حال، شرکت های هوش مصنوعی باید این نگرانی را جدی بگیرند و اقداماتی را برای رفع آن انجام دهند.

به طور کلی، من فکر می‌کنم که پیاده سازی مدل سه خط می تواند به طور قابل توجهی پایگاه اطلاع رسانی هیئت‌مدیره را افزایش دهد. این تأثیر در آزمایشگاه‌های تحقیقاتی متوسط قابل توجه‌تر خواهد بود، زیرا اکثر شرکت‌های فناوری بزرگ در حال حاضر دارای یک عملکرد حسابرسی داخلی هستند، البته نه مختص هوش مصنوعی.

۴.۴. سایر مزایا

پیاده‌سازی مدل سه خط مزایای زیادی به جز کاهش ریسک برای افراد، گروه ها یا جامعه دارد. اگرچه این مزایا فراتر از محدوده این مقاله هستند، به نظر می رسد حداقل ارائه یک نمای کلی ضروری است. در زیر به طور خلاصه به چهار مورد از آنها می پردازیم.

اول، اجرای مدل سه خط می تواند از تکرارهای غیر ضروری پوشش ریسک جلوگیری کند. افراد مختلف در تیم های مختلف می توانند کار مدیریت ریسک یکسان یا بسیار مشابهی را انجام دهند و این موضوع اغلب مطلوب است زیرا می تواند از شکاف در پوشش ریسک جلوگیری کند . اما اگر چنین تکراری ضروری نباشد، می‌تواند منابعی مانند نیروی کار را که می‌تواند در جاهای دیگر به نحو مؤثرتری مورد استفاده قرار گیرد، هدر دهد. بنابراین شرکت‌های هوش مصنوعی با یک مبادله اثربخشی – کارایی – مواجه هستند. اینکه چگونه این مبادله باید حل شود، به زمینه خاص آنها بستگی دارد. به عنوان مثال، هنگام برخورد با ریسک‌های فاجعه بار، اثربخشی (جلوگیری از شکاف در پوشش ریسک) مهمتر از کارایی (جلوگیری از تکرارهای غیر ضروری پوشش) به نظر می‌رسد. در این مورد، شرکت‌های هوش مصنوعی باید به‌جای ریسک شکاف‌ها در حوزه‌های مهم، در مورد پوشش بیش از حد توجه کنند.

به طور کلی، به نظر می‌رسد اگر به طور عمده به کاهش ریسک توجه شود این مزیت اغراق آمیز و کمتر مرتبط باشد.

[۵۳] They might lack important context
[۵۴] Snapshots

دوم، شرکت‌های هوش مصنوعی که مدل سه خط را پیاده‌سازی کرده‌اند، ممکن است مسئول‌تر تلقی شوند. به طور کلی، شیوه‌های مدیریت ریسک در شرکت‌های هوش مصنوعی در مقایسه با بسیاری از صنایع دیگر (مانند حمل و نقل هوایی یا بانکی) کمتر پیشرفته به نظر می‌رسد. با تطبیق بهترین شیوه‌های موجود از سایر صنایع، آنها نشان می‌دهند که قصد دارند تا شیوه‌های مدیریت ریسک خود را حرفه‌ای‌تر کنند، که می‌تواند به عنوان مسئولیت‌پذیرتر تلقی شود. این تصور ممکن است فواید زیادی داشته باشد. به عنوان مثال، جذب و حفظ استعدادهایی که به اخلاق و ایمنی(صحت و سقم) اهمیت می دهند را آسان‌تر می‌کند. همچنین می‌تواند به جلوگیری از اقدامات بیش از حد سنگین از سوی ناظران کمک کند. حتی ممکن است در پرونده‌های دعاوی قضایی برای این سوال که آیا یک سازمان وظیفه مراقبت خود را انجام داده است یا خیر مفید باشد. با این حال، به نظر می‌رسد که آیا پیاده‌سازی مدل سه خط تا این حد بر ادراک تأثیر می‌گذارد، به ویژه در مقایسه با سایر اقدامات راهبری (مثلاً انتشار اصول اخلاقی هوش مصنوعی یا راه‌اندازی یک هیئت اخلاق هوش مصنوعی)، عمدتاً به این دلیل که اکثر ذینفعان، از جمله بیشتر کارمندان، مدل را نمی‌دانند و نمی‌توانند ارتباط آن را ارزیابی کنند. یک استثنا ممکن است ناظران و دادگاه‌هایی باشند که بیشتر به جزئیات شیوه‌های مدیریت ریسک اهمیت می‌دهند. بهترین حدس من این است که پیاده‌سازی مدل، تأثیرات قابل‌توجهی بر درک چند ذینفع خواهد داشت، در حالی که بیشتر ذینفعان دیگر اهمیتی نمی‌دهند.

سوم، پیاده‌سازی مدل سه خط می‌تواند استخدام استعدادهای مدیریت ریسک را آسان‌تر کند. حرفه مدیریت ریسک هوش مصنوعی در مراحل ابتدایی خود است. من فرض می‌کنم که شرکت‌های هوش مصنوعی استخدام افرادی با مهارت‌های هوش مصنوعی و مدیریت ریسک را چالش برانگیز می‌دانند. در بیشتر موارد، آنها می‌توانند کارشناسان هوش مصنوعی را استخدام کرده و آنها را در زمینه مدیریت ریسک آموزش دهند، یا کارشناسان مدیریت ریسک را از سایر صنایع استخدام کرده و آنها را در زمینه هوش مصنوعی آموزش دهند. پیاده‌سازی مدل سه خط می‌تواند استخدام کارشناسان مدیریت ریسک از سایر صنایع را آسان‌تر کند، زیرا آنها قبلاً با این مدل آشنا هستند. اگر فرض کنیم که شرکت‌های هوش مصنوعی می‌خواهند استعدادهای مدیریت ریسک بیشتری را استخدام کنند، زیرا سیستم‌ها توانمندتر می‌شوند و در موقعیت‌های حساس‌تر ایمنی استفاده می‌شوند به عنوان مثال، ممکن است اهمیت بیشتری پیدا کند. با این حال، من این استدلال را چندان قانع کننده نمی دانم. من شک دارم که اجرای مدل سه خط تفاوت معنی داری در تصمیم گیری‌های مربوط به استخدام (به عنوان مثال در تصمیم یک داوطلب برای درخواست یا پذیرش یک پیشنهاد) ایجاد کند. از آنجایی که مدل مربوط به بعد سازمانی مدیریت ریسک است، تأثیر قابل توجهی بر کار روزمره مدیریت ریسک ندارد. با این اوصاف، ممکن است مزایای کوچکتری وجود داشته باشد (به عنوان مثال آسان کردن فرآیند ورود). بهترین حدس من این است که تأثیر خلاف واقع اجرای مدل براستخدام کم است.

چهارم، اجرای مدل سه خط ممکن است هزینه‌های تامین مالی را کاهش دهد. آژانس‌های رتبه‌بندی تمایل دارند به شرکت‌هایی که چارچوب ERM را پیاده‌سازی کرده‌اند رتبه‌بندی بهتری بدهند (زیرا انجام این کار بهترین عمل در نظر گرفته می‌شود)، و شرکت‌هایی با رتبه‌بندی بهتر تمایل دارند هزینه‌های تامین مالی کمتری داشته باشند

زیرا شرایط اعتباری بهتری دارند. ممکن است اثر مشابهی با توجه به اجرای مدل سه خط وجود داشته باشد. هزینه های تامین مالی کمتر به ویژه اگر فرض کنیم که هزینه‌های توسعه سیستم های هوش مصنوعی پیشرفته به دلیل افزایش تقاضا برای محاسبات افزایش می‌یابد به ویژه مهم است. در سناریوهایی که فشار تجاری بسیار بالاتر از امروز است، هزینه‌های تامین مالی پایین‌تر نیز می‌تواند برای ادامه تحقیقات ایمنی که به توسعه محصول کمکی نمی‌کند، مهم باشد. با این حال، من مطمئن نیستم که تا چه حد یافته‌های چارچوب‌های ERM به مدل سه خط تعمیم می‌یابند. بهترین حدس من این است که پیاده‌سازی مدل سه خط تأثیر معناداری بر هزینه‌های مالی آزمایشگاه‌های تحقیقاتی متوسط امروزی نخواهد داشت. اما من انتظار دارم که با سودآورتر شدن آزمایشگاه ها و استفاده فزاینده از سایر منابع مالی (مانند اعتبارات یا اوراق قرضه) این موضوع تغییر کند.

۵. نتیجه‌گیری

این مقاله، مدل سه خط را در زمینه هوش مصنوعی اعمال کرده است. راه‌های مشخصی را پیشنهاد کرده است که در آن توسعه‌دهندگان هوش مصنوعی مانند OpenAI، Google DeepMind و Anthropic می‌توانند این مدل را برای کاهش ریسک های ناشی از هوش مصنوعی پیاده‌سازی کنند. استدلال می‌کند که اجرای این مدل می‌تواند از آسیب‌های فردی، جمعی یا اجتماعی با تشخیص و بستن شکاف‌ها در پوشش ریسک، افزایش اثربخشی شیوه‌های مدیریت ریسک، و توانمند ساختن ارکان راهبری برای نظارت مؤثرتر بر مدیریت، جلوگیری کند. به این نتیجه رسید که، در حالی که محدودیت‌هایی وجود دارد و نباید اغراق آمیز درباره آثار صحبت کرد، اما این مدل می‌تواند به طور قابل قبولی به کاهش ریسک های ناشی از هوش مصنوعی کمک کند.

بر اساس یافته های این مقاله، سوالات زیر برای تحقیقات بیشتر پیشنهاد می شود. اول، بحث در مورد توانایی مدل برای کاهش ریسک های ناشی از هوش مصنوعی عمدتاً نظری بود و بر ملاحظات قابل قبول انتزاعی تکیه داشت. سایر محققان را تشویق می‌کنم که این ادعاها را به صورت تجربی ارزیابی کنند. یک مطالعه موردی صنعتی مشابه آنچه که موکاندر و فلوریدی (۲۰۲۲) برای حسابرسی مبتنی بر اخلاق انجام دادند، می‌تواند اولین گام باشد. دوم، اگرچه به نظر نمی‌رسد شرکت‌های هوش مصنوعی مدل سه خط را پیاده‌سازی کنند، اما بسیاری از فعالیت‌های ذکر شده در بالا را قبلا انجام داده اند. برای هدف‌گیری بهتر کار در آینده، بازنگری شیوه‌های مدیریت ریسک موجود در این شرکت‌ها و انجام تجزیه و تحلیل شکاف، مفید خواهد بود. از آنجایی که داده‌های عمومی کمیاب است، محققان باید مصاحبه یا نظرسنجی انجام دهند (مثلاً «نظرسنجی معیار مدیریت ریسک هوش مصنوعی»)، اگرچه من انتظار دارم محرمانه بودن یک مانع بزرگ باشد مهم است که بدانیم آیا مقررات موجود یا آینده ممکن است حتی شرکت های هوش مصنوعی را ملزم به اجرای این مدل کند. به عنوان مثال، در حالی که ماده ۹ قانون پیشنهادی هوش مصنوعی اتحادیه اروپا به مدل سه خط اشاره نمی‌کند اما پیشنهاد شده است که استانداردهای هماهنگ آینده یا مشخصات مشترک باید شامل این مدل باشند. در نهایت، مقاله مدل سه خط را به صورت مجزا بررسی کرده است. عوامل زمینه‌ای مانند فرهنگ ریسک در شرکت‌های هوش مصنوعی را که ممکن است بر

اثربخشی مدل نیز تأثیر بگذارد، حذف کرده است. درک بهتر این عوامل، پایگاه اطلاعاتی را برای تصمیم گیرندگان در شرکت های هوش مصنوعی و فراتر از آن بهبود می بخشد.
همانطور که جرج باکس (۱۹۷۶) گفته است، «همه مدل‌ها اشتباه هستند، اما برخی از آنها مفید هستند»[۵۵]. با همین روحیه، می توان گفت که مدل سه خط گلوله‌ای(تیری) نقره‌ای در برابر ریسک‌های ناشی از هوش مصنوعی نیست، اما همچنان می‌تواند نقش مهمی ایفا کند. شرکت های هوش مصنوعی باید آن را به عنوان ابزار راهبری مفید ببینند که می‌توانند برای مقابله با تهدیدات امروز و فردا از هوش مصنوعی استفاده کنند.

منبع:

- Jonas Schuett, Three lines of defense against risks from AI, Springer,۲۰۲۳

[۵۵] All models are wrong, but some are useful