COSO

کارگروه سازمان‌های پشتیبانی مالی کمیسیون تردوی

راهبری و کنترل داخلی

استفاده از چارچوب کوزو در مدل سه خط دفاعی

توسط

انجمن حسابرسان داخلی

برگردان به فارسی

مرتضی اسدی الهه مهدوی ثابت

استفاده از چارچوب کوزو در مدل سه خط دفاعی

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 (مدیرت 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.

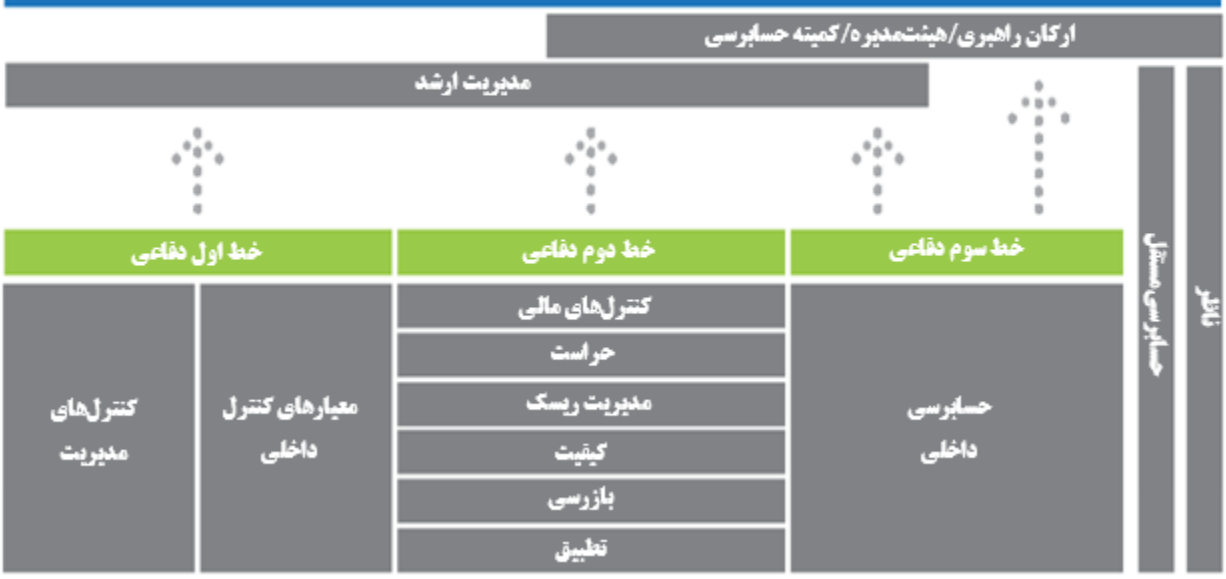
مطابق سایر نشریات کوزو، در این سند از اصطلاح «هیئت‌مدیره» برای اشاره به هیئت‌های راهبری مانند هیئت‌مدیره، هیئت‌امناء، شرکای عمومی، مالکین، یا هیئت‌های نظارتی استفاده می‌شود.

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.

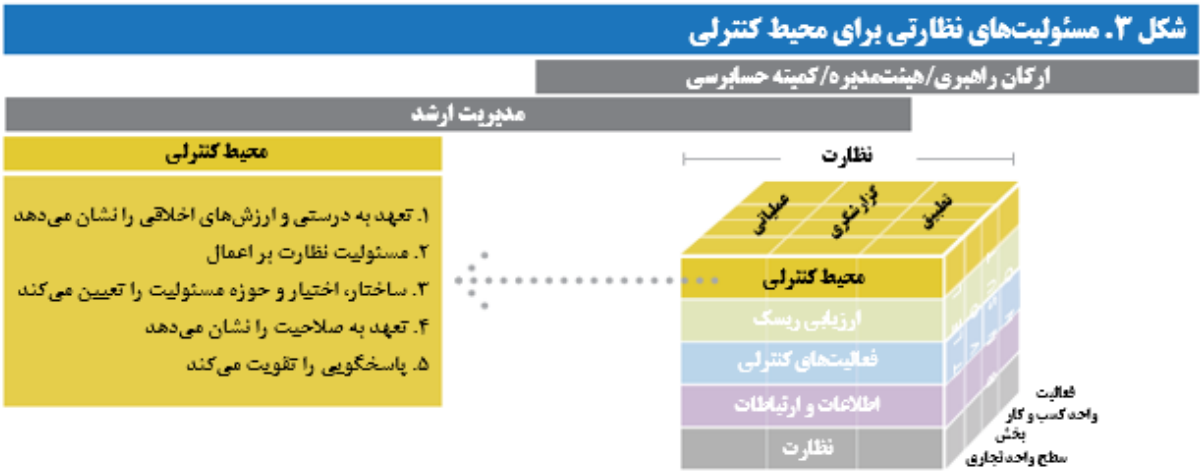
هدف هر سازمانی دستیابی به اهدافش است. پیگیری این اهداف مستلزم استقبال از فرصت‌ها، پیگیری رشد، پذیرش ریسک‌ها، و مدیریت این ریسک‌ها است - همه در جهت پیشرفت سازمان هستند. قصور در پذیرش ریسک‌های مناسب، و قصور در مدیریت و کنترل صحیح ریسک‌های پذیرفته شده، می‌تواند سازمان را از دستیابی به اهدافش بازدارد. تنشی 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.



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.

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:

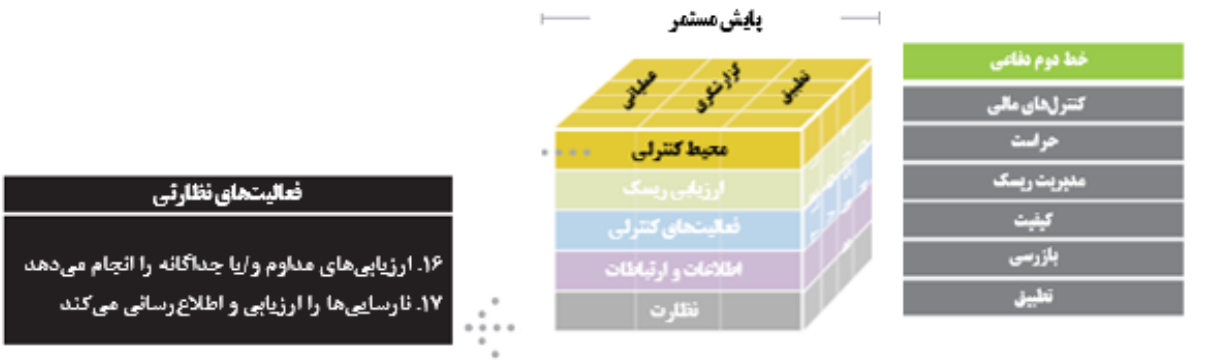
- همکاری با مدیریت در طراحی و توسعه فرآیندها و کنترل‌ها به منظور مدیریت ریسک‌ها.
- تعریف فعالیت‌هایی برای نظارت و نحوه اندازه‌گیری موفقیت در مقایسه با انتظارات مدیریت.
- نظارت بر کفایت و اثربخشی فعالیت‌های کنترل داخلی.
- ش مسائل حیاتی، ریسک‌های نوظهور و داده‌های پرت.
- ایجاد چارچوب‌هایی برای مدیریت ریسک.
- 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 (مدیرت 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 2015, “Leveraging COSO Across the Three Lines of Defense”.**