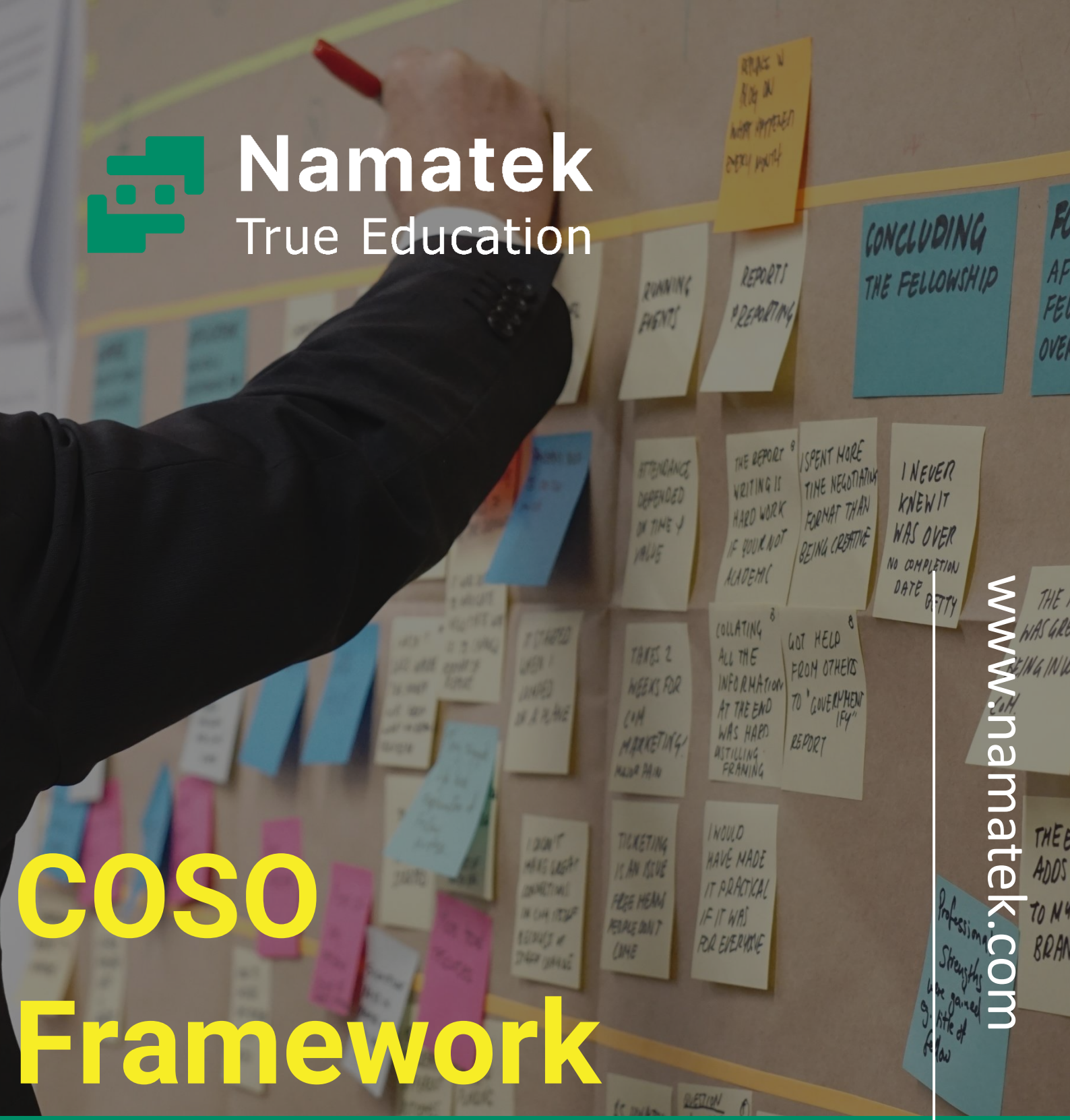


Namatek
True Education

COSO Framework

مدل کوزو

www.namatek.com

فهرست مطالب

کنترل‌های داخلی بخش مهمی از ارزیابی و مدیریت ریسک هستند؛ اما گنجاندن کنترل‌های داخلی در فرآیندهای تجاری همیشه آسان نیست.

مدل کوزو (COSO) به‌عنوان یک مدل کنترل داخلی یک مسیر استراتژیک رو به جلو به سازمان‌ها ارائه می‌دهد. این مدل به کسب و کارها کمک می‌کند تا کنترل‌های داخلی و نرم‌افزار مدیریت کنترل‌های داخلی را در فعالیت‌های روزمره خود تعبیه کنند و هنگامی که به طور موثر مورد استفاده قرار گیرد، به سهامداران و هیئت مدیره اطمینان می‌دهد که سازمان، استانداردهای اخلاقی و امنیتی را رعایت می‌کند.

همچنین سازمان‌هایی که مدل کنترل داخلی را اتخاذ می‌کنند، می‌توانند کارآمدتر، ایمن‌تر و در نهایت انعطاف‌پذیرتر باشند؛ زیرا چشم‌انداز ریسک در حال تکامل است. این مقاله پنج ستون و هفده اصل مدل کوزو و همچنین نحوه پیاده‌سازی و استفاده از آن را به عنوان پایه‌ای برای کنترل‌های داخلی مدرن و بازدارندگی از تقلب شرح می‌دهد.

مدل کوزو (COSO) چیست؟

مدل کوزو سیستمی است که برای ایجاد کنترل‌های داخلی به منظور ادغام در فرآیندهای تجاری استفاده می‌شود. در مجموع، این کنترل‌ها اطمینان معقولی را ارائه می‌دهند که سازمان به صورت اخلاقی، شفاف و مطابق با

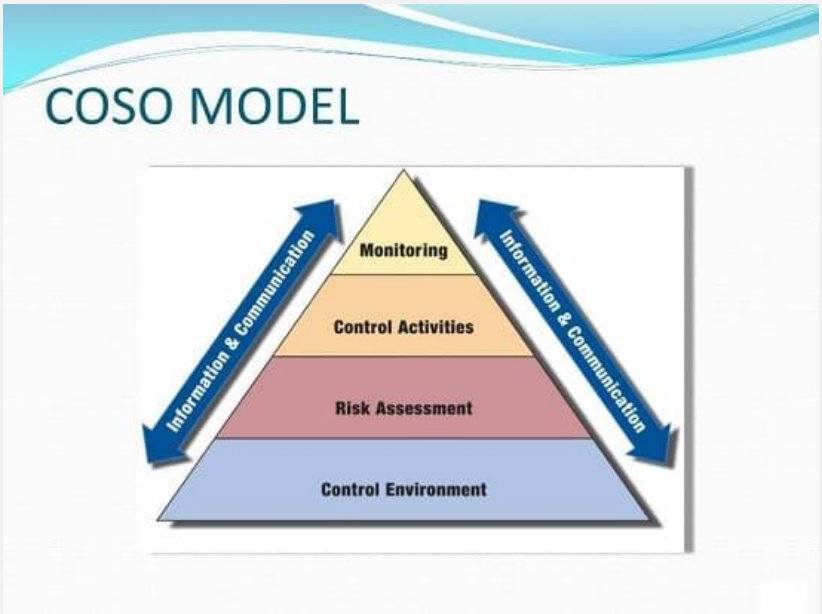
استانداردهای صنعت کار می‌کند. COSO مخفف Committee of Sponsoring Organizations و به معنای کمیته سازمان‌های حامی است. این کمیته در سال ۱۹۹۲ مدلی را ایجاد کرد که توسط معاون اجرایی و مشاور عمومی جیمز تردوی جونیور به همراه چندین سازمان بخش خصوصی، از جمله موارد زیر، رهبری می‌شد:

- انجمن حسابداری آمریکا
- مدیران مالی بین المللی
- موسسه حسابرسان داخلی
- موسسه حسابداران رسمی آمریکا
- موسسه حسابداران مدیریت (انجمن ملی حسابداران بهای تمام شده سابق)

مدل کوزو در سال ۲۰۱۳ به‌روز شد تا مکعب COSO را شامل شود. این مکعب یک نمودار سه بعدی است که نشان می‌دهد چگونه همه عناصر یک سیستم کنترل داخلی به هم مرتبط هستند. در سال ۲۰۱۷ این کمیته، مدل مدیریت ریسک سازمانی COSO خود را معرفی کرد.

مدل COSO ERM با هدف کمک به سازمان‌ها در درک و اولویت‌بندی ریسک‌ها و ایجاد ارتباط قوی بین ریسک، استراتژی و نحوه عملکرد یک کسب‌وکار است.

هرم کوزو

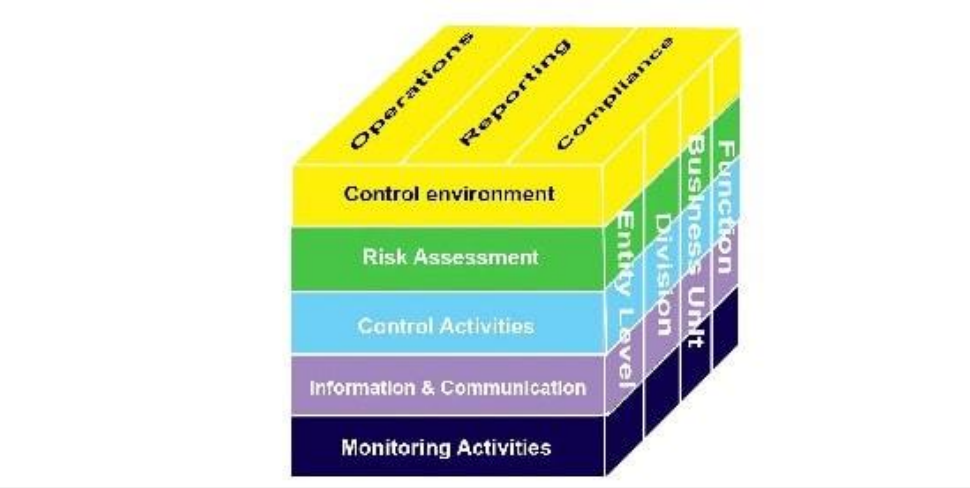


مدل کوزو در سال ۱۹۹۲، توسط یک هرم نشان داده شد. این هرم پنج جزء کنترل COSO را نشان می‌دهد که این پنج اصل عبارت‌اند از:

۱. محیط کنترل
۲. ارزیابی ریسک
۳. کنترل فعالیت‌ها
٤. اطلاعات و ارتباطات
۵. فعالیت‌های نظارتی

بعداً در مورد این اصول با جزئیات بیشتر صحبت خواهیم کرد. خوبی این طرح هرمی این است که نشان می‌دهد تکمیل یک سطح، به طور طبیعی منجر به تکمیل سطح چند بعدی می‌شود. هر سطح با هم کار می‌کند تا از ماموریت کلی مدیریت ریسک، استراتژی و اهداف تجاری مرتبط پشتیبانی کنند.

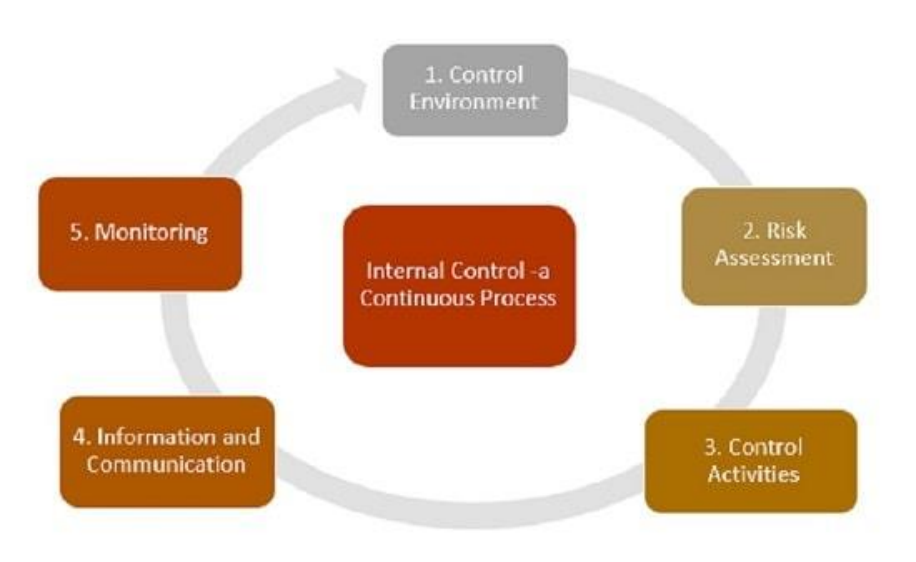
مکعب کوزو



مدل کوزو بعداً برای جایگزینی طرح هرمی با یک مکعب به‌روز شد. این دوباره کاری زمانی به‌وجود آمد که مدل اصلی COSO بسیار ساده تلقی می‌شد و فاقد جهت بود و شرکت‌ها برای پیاده‌سازی سیستم‌های کنترل مؤثر مشکل داشتند. بعدها، دستورالعمل‌های جدید در سال ۲۰۱۳ ایجاد شد که به عنوان مدل COSO 2013 نامیده شد.

این مدل ابزارهای جدیدی را به شرکت‌ها داد تا به آن‌ها کمک کند تا یک مدل مدیریت ریسک را طراحی و پیاده سازی کنند و هرم COSO را به مکعب تغییر دهند. مکعب COSO دارای ۷۷ نقطه فوکوس است. این‌ها در ۱۷ ویژگی جدید تقسیم می‌شوند که تحت پنج اصل اساسی که در هرم کوزو شرح داده شده است، سازماندهی شده‌اند.

پنج رکن مدل کوزو چیست؟



پنج ستون مدل کوزو که در جلوی مکعب نشان داده شده‌اند، از اهداف کنترل‌های داخلی پیرامون عملیات، گزارش‌دهی و انطباق با ارائه برخی راهنمایی‌ها در مورد نحوه اجرای کنترل‌های موثر پشتیبانی می‌کنند. این ارکان به ۱۷ اصل تقسیم می‌شوند. پنج رکن و ۱۷ ویژگی مدل کوزو به شرح زیر هستند:

محیط کنترلی

محیط کنترلی یک سازمان به مجموعه کلی کنترل‌های داخلی اشاره دارد و از سطوح بالا به پایین ایجاد می‌شود. ایجاد یک محیط کنترلی مطابق با مدل‌های کوزو مستلزم نشان دادن اصول زیر است:

۱. شرکت به یکپارچگی و ارزش‌های اخلاقی متعهد است.

۲. هیئت مدیره استقلال خود را از مدیریت حفظ کرده و بر برنامه‌های کنترل داخلی نظارت می‌کند.

۳. مدیریت ساختار سازمانی، اختیارات، خطوط گزارش‌دهی و مسئولیت‌ها را برای اجرا، گزارش‌دهی و انطباق اهداف عملیاتی و تجاری شرکت تعریف می‌کند.
٤. شرکت استخدام، توسعه و حفظ افراد توانمند و با صلاحیت را در اولویت قرار می‌دهد که با اهداف کنترل‌های داخلی همسو هستند.
۵. شرکت مسئولیت‌های کنترل را ایجاد می‌کند.

دستیابی به این اصول می‌تواند از طریق موارد زیر، چه از طریق ممیزی داخلی یا ممیزی انطباق خارجی، انجام شود:

- مستندسازی خط مشی‌ها
- بیانیه‌های ماموریت و چشم‌انداز
- اسناد برنامه‌ریزی استراتژیک
- یادداشت‌های جلسه
- ارزیابی دوره‌ای برنامه کنترل‌های داخلی شرکت

ارزیابی ریسک

رکن بعدی مدل کوزو، نیاز به ارزیابی‌های دوره‌ای یا مستمر ریسک براساس سیستم کنترل‌های داخلی سازمان را مشخص می‌کند. این ارزیابی‌های ریسک را می‌توان توسط پرسنل داخلی، مانند تیم حسابرسی داخلی یا اشخاص ثالث، مانند شرکت مشاوره یا CPA انجام داد. مدل کوزو چهار اصل اصلی را برای ارزیابی ریسک و درمان ریسک مشخص می‌کند که در زیر فهرست شده است:

۱. شرکت اهدافی را با مشخصات کافی تعیین می‌کند تا امکان شناسایی و ارزیابی خطرات مربوط به اهداف را فراهم نماید.

۲. شرکت ریسک‌های مربوط به اهداف را شناسایی می‌کند و ریسک‌های شناسایی‌شده را به‌منظور توسعه یک برنامه عملیاتی برای درمان ریسک بررسی می‌نماید.
۳. هنگام ارزیابی خطرات، تقلب به صراحت به‌عنوان بخشی از ارزیابی در نظر گرفته می‌شود.
٤. سازمان هرگونه تغییری را که ممکن است بر کنترل‌های داخلی تأثیر بگذارد، پیش بینی و ارزیابی می‌کند.

ریسک‌ها باید در فهرست ریسک یا موجودی ریسک ثبت شوند که این ارزیابی ریسک، احتمال تحقق ریسک، تاثیر در صورت تحقق ریسک، جدول زمانی برنامه کاهش ریسک را توصیف می‌کند. برای کاهش خطر و شخص یا افراد مسئول آن خطر، ارزیابی ریسک باید حداقل سالیانه انجام شود و با کشف یا کاهش خطرات، ثبت ریسک باید به‌روز شود. در نظر گرفتن این ارزیابی‌های ریسک و ثبت ریسک باید در فرآیند تصمیم‌گیری سازمان گنجانده شود و با میزان تحمل ریسک سازمان، هماهنگ باشد.

فعالیت‌های کنترلی

هنگامی که یک سازمان اهداف خود را تعریف کرد و یک محیط کنترل اخلاقی ایجاد و ارزیابی ریسک را انجام داد یا آغاز کرد، مدل کوزو سطح عمیق‌تر می‌کند. فعالیت‌های کنترلی، فعالیت‌ها، اقدامات و ارتباطاتی هستند که برای کاهش خطرات و حفظ کنترل‌های داخلی قوی انجام می‌شوند. سه اصل دیگر COSO در این ستون قرار می‌گیرند:

۱. فعالیت‌های کنترلی، خطرات مربوط به اهداف شرکت را بررسی می‌کنند و کاهش می‌دهند.

۲. شرکت در راستای اهدافش، فعالیت‌های کنترلی بر روی فناوری ایجاد می‌کند.
۳. خط مشی‌ها و رویه‌ها، فعالیت‌های کنترلی را که باید در شرکت به‌عنوان بخشی از برنامه کنترل‌های داخلی انجام شود، تعریف می‌نماید.

نمونه‌ای از یک فعالیت کنترلی ممکن است این باشد که تغییرات کد باید:

- توسط یک فرد مناسب بررسی شود.
- که این فرد توسعه‌دهنده کد نیست.
- توسط آن شخص در سیستم تأیید شود.

یکی دیگر از فعالیت‌های کنترلی ممکن است فسخ حساب کارمند در ۲۴ ساعت از آخرین روز کاری آن‌ها باشد.

اطلاعات و ارتباطات

یکی دیگر از جنبه‌های حیاتی یک برنامه موفق، انطباق و کنترل‌های داخلی، توزیع مناسب، منسجم و به موقع اطلاعات و ارتباطات با ذینفعان مربوطه است. این یک مدل چندبخشی می‌باشد و با شکستن بیشتر آن، مدل کوزو، شرکت‌ها را ملزم می‌کند تا براساس این اصول با یکدیگر ارتباط برقرار کنند و اطلاعات را به اشتراک بگذارند.

اصول این بخش به‌شرح زیر هستند:

۱. شرکت از داده‌ها و اطلاعات باکیفیت برای پشتیبانی از اهداف کنترلی استفاده می‌کند.
۲. شرکت اطلاعات مربوطه، اهداف و تکالیف و مسئولیت‌های مربوط به فعالیت‌های کنترل داخلی را به اطلاع می‌رساند.

۳. در صورت لزوم، شرکت با نهادهای خارجی در خصوص کنترل‌های داخلی ارتباط برقرار می‌کند.

شرکت‌های بیشتری، به‌ویژه سازمان‌هایB2B ، بندهایی را در قراردادهای خود لحاظ می‌کنند که نیازمند افشای نقض داده‌ها، حوادث، حملات سایبری و سایر موارد کنترل داخلی به نهادهای خارجی است. دستورالعمل‌های HIPAAمستلزم گزارش نقض داده‌ها به طرف‌های تحت تأثیر است. یک برنامه ارتباطی که به‌خوبی سازماندهی شده باشد، می‌تواند دردسر ایجاد یک برنامه COSO را برطرف کند.

فعالیت‌های نظارتی

پنجمین و آخرین رکن مدل کوزو، شامل نظارت، اندازه‌گیری و گزارش‌دهی سیستم کنترل‌های داخلی شرکت است و شامل اصول زیر می‌باشد:

۱. ارزیابی‌های منظم یا مداوم برای تعیین این‌که آیا برنامه کنترل‌های داخلی به‌طور موثر عمل می‌کند یا خیر، انجام می‌شود.

۲. هرگونه نقص کنترل داخلی، به طرف‌های پاسخگو از جمله هیئت مدیره و مدیریت عالی در صورت لزوم، به‌موقع گزارش می‌شود.

مراحل پیاده‌سازی و استفاده از مدل کوزو چیست؟

یک سازمان برای ایجاد و ادغام یک برنامه موثر کوزو، می‌تواند این مراحل کلی را دنبال کند:

برنامه‌ریزی

سازمان‌ها برای این که بیشترین بهره را از مدل کوزو ببرند، باید کارهای قانونی را از قبل انجام دهند.سازمان‌ها باید درک کنند که چرا از این مدل استفاده می‌کنند و مدل چگونه در نقشه راه استراتژیک کلی آن‌ها قرار می‌گیرد.در عین حال سازمان‌ها باید درک روشنی از ۱۷ اصل خود مدل داشته باشند. از آن‌جایی که COSO برای کل سازمان اعمال می‌شود، توسعه یک برنامه دقیق و کامل برای راه‌اندازی و حفظ یک سیستم کنترل داخلی براساس COSO بسیار مهم است.

سرمایه‌گذاری در نرم‌افزار مدیریت انطباق برای هماهنگ کردن فعالیت‌های کنترل COSO، هم برنامه‌ریزی و هم اجرا را تسهیل می‌نماید.

ارزیابی و مستندسازی

پس از برنامه‌ریزی، درک بلوغ برنامه کنترل‌های داخلی سازمان و این که چه مستنداتی برای پشتیبانی از اهداف و ارکان وجود دارد، مهم است. در این مرحله، تیم مسئول باید اسناد موجود در مورد کنترل‌های داخلی سازمان را جمع‌آوری کند و درنظر بگیرد که آیا فرآیندهای مشترک، مدیریت رسمی ریسک سازمانی (ERM) یا فعالیت‌های کنترلی مناسب وجود دارد یا خیر. اگر اسناد موجود برای پشتیبانی از اهداف سازمان و الزامات مدل کوزو کافی نباشد، باید این موارد برای اصلاح، به‌عنوان شکاف ردیابی شوند.

اصلاح

از آنجایی که ارزیابی‌های کنترل داخلی شکاف‌هایی را در برنامه کنترل‌های داخلی سازمان نشان می‌دهد، طرف‌های مسئول، فعالیت‌ها یا حوزه‌های کنترلی فعالیت‌های اصلاح یا کاهش خطر را انجام می‌دهند. اگر شکاف کنترل داخلی پیدا شود، تیم یا تیم‌های مسئول، مراحل اصلاح یا کاهش خطر، جدول زمانی و مسئولیت‌ها را برنامه‌ریزی می‌کنند و سپس آن طرح را اجرا می‌کنند.

تست و گزارش

هنگامی که یک شرکت مراحل قبل را کامل کرده باشد و از تطابق شرکت با مدل COSO اطمینان خاطر پیدا کند، در این مرحله، آزمایش و گزارش گیری انجام می‌شود.آزمایش شامل ارزیابی طراحی و اثربخشی عملیات کنترل‌های داخلی و همچنین تأثیر کنترل بر ریسک‌های مرتبط است.

آزمایش یک کنترل مدیریت حادثه، ممکن است شامل بازرسی گزارش حوادث برای یک دوره معین و تعیین این که آیا مستندات مناسب برای زیرمجموعه انتخابی از آن حوادث تکمیل شده است یا خیر، باشد و مدیریت باید گزارش‌های منظمی در مورد برنامه کنترل‌های داخلی و نتایج آزمایش دریافت کند. به‌طور خلاصه می‌توان گفت، مدل COSO تعیین می‌نماید که چگونه سازمان، تمام فرآیندهای تجاری را تکمیل کرده و مدیریت ریسک را در تمام بخش‌های سازمان تعبیه می‌نماید و انطباق قانونی و مقرراتی را تسهیل می‌کند. هنگامی که همه کنترل‌ها برقرار شدند، مدل نظارت را در اولویت قرار می‌دهد که این به سازمان‌ها کمک می‌کند تا رعایت کنترل‌های داخلی را قبل از به‌وجود آمدن خطرات نوظهور، بررسی کنند.

کاربرد مدل کوزو

مدل کوزو به شدت توسط شرکت‌های سهامی عام و شرکت‌های حسابداری و مالی استفاده می‌شود. این چارچوب به دنبال ایجاد کنترل‌های داخلی که نحوه انجام فرآیندهای تجاری کلیدی را رسمیت می‌بخشند، است. این مدل به سازمان‌ها کمک می‌کند تا به الزامات قانونی و اخلاقی پایبند باشند و در

عین حال بر ارزیابی و مدیریت ریسک نیز تمرکز کنند. این مدل، با توجه به این‌که مربوط به استفاده از حسابرسان داخلی برای نظارت بر پایبندی به کنترل‌های تعیین‌شده است، علاوه بر ادغام چنین کنترل‌هایی در فرآیندهای تجاری کلیدی، تأکید زیادی بر نظارت و گزارش‌دهی دارد.

مزایا و محدودیت‌های مدل کوزو

مدل کوزو یک مسیر استراتژیک رو به جلو برای مدیریت ریسک ایجاد می‌کند و مزایا و محدودیت‌هایی نیز دارد که سازمان‌ها باید از آن‌ها آگاه باشند. مزایای مدل کوزو در زیر یاد شده است، این سه مزیت کلیدی است که سازمان‌ها می‌توانند با پیروی از مدل کنترل داخلی COSO انتظار داشته باشند:

۱. **استاندارد کردن فرآیندهای کسب و کار:** هنگامی که سازمان‌ها مدل COSO را اجرا می‌کنند، نحوه انجام کار تیم‌های خود را نیز استاندارد می‌کنند که این کارایی سازمان را بهبود بخشیده و داده‌ها را متمرکز می‌کند و در عین حال، ریسک را نیز کاهش می‌دهد.

۲. **جلوتر بودن از خطرات:** 42 درصد از مشاغل با درآمد بین ۱ تا ۱۰ میلیارد دلار در سال گذشته، جرایم سایبری را تجربه کرده‌اند. مدل کوزو با استفاده از بهترین شیوه‌ها، سازمان‌ها را در مقابل این خطرات مصون نگه می‌دارد.
۳. **کاهش هزینه‌ها:** وقتی همه تیم‌ها از مجموعه کنترل‌های داخلی یکسانی پیروی کنند، کسب و کار کارآمدتر می‌شود. بسیاری از سازمان‌هایی که از مدل COSO پیروی می‌کنند، استراتژیک‌تر عمل می‌کنند که این باعث می‌شود تا هزینه‌ها را در طول زمان کاهش دهند.

همان‌طور که مدل COSO می‌تواند موثر باشد، می‌تواند به روش‌های زیر محدودکننده نیز باشد:

- **چالش برای پیاده سازی:** مدل کوزو از نظر طراحی گسترده است. در حالی که این به بسیاری از انواع مختلف سازمان‌ها اجازه می‌دهد تا از مدل پیروی کنند؛ اما فاقد راهنمایی خاص در پیاده‌سازی و نگهداری مدل در یک دوره طولانی‌تر است. سازمان‌ها ممکن است برای اتخاذ این مدل دچار مشکل شوند، به‌ویژه اگر از قبل استراتژی مدیریت ریسک مؤثری نداشته باشند.
- **ساختار سفت و سخت:** مدل کوزو ساختار خاصی دارد. بسیاری از سازمان‌ها می‌توانند در این مدل به دسته‌های متعددی تقسیم شوند که شناسایی بهترین مسیر برای تیم‌های خود را برای کسب‌وکارها دشوار می‌کند.

جمع‌بندی

اعتماد یک جزء اصلی در معاملات تجاری است. با این حال، تشخیص آن می‌تواند سخت باشد، به‌خصوص زمانی که انجام هر کار به افراد متکی باشد. با گذشت زمان، سازمان‌های مستقلی مانند کمیته سازمان‌های حامی کمیسیون تردوی (COSO) برای هدایت عملیات تجاری به وجود آمدند. مدل کوزو دستورالعملی برای ایجاد کنترل‌های داخلی در یک سازمان برای مبارزه با تقلب است. این مدل عملکردهای اجرایی، فعالیت‌های مالی، مدیریت ریسک و اخلاقیات را ارزیابی می‌کند تا اطمینان حاصل شود که یک تجارت شفاف، قانونی، کارآمد و مؤثر عمل می‌کند.

بسته به حقایق و شرایط یک شرکت، پیاده‌سازی یا انتقال به مدل می‌تواند زمان‌بر باشد، بنابراین ایده خوبی است که این فرآیند را در اسرع وقت آغاز کنید. شرکت ها باید با آشنایی با ۱۷ اصل و سایر دستورالعمل‌های کوزو شروع کنند. سپس شرکت‌ها می‌توانند وضعیت فعلی سیستم کنترل داخلی خود را ارزیابی کنند و برنامه‌ای برای اصلاح هرگونه ضعف تدوین کنند.