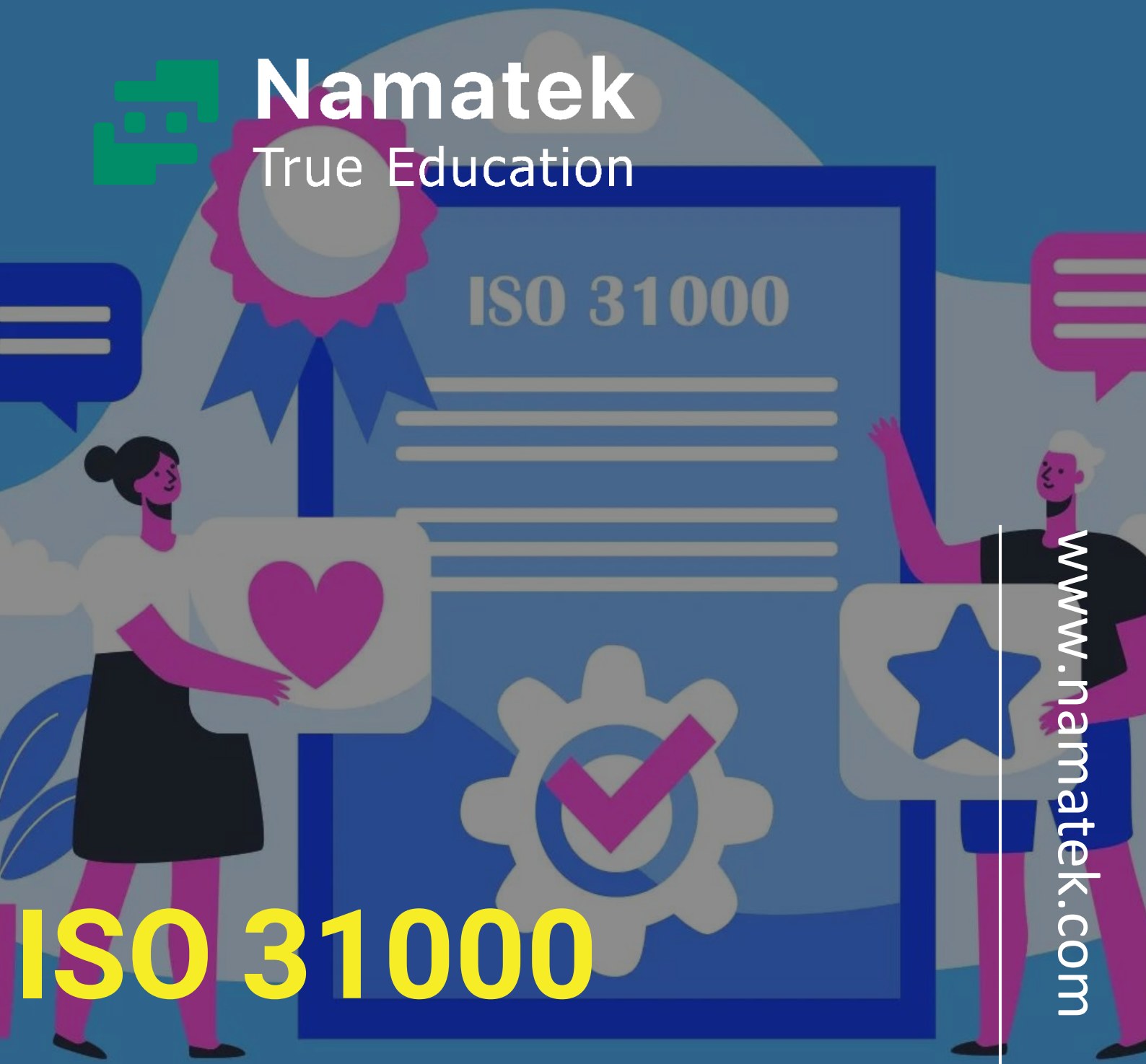
Namatek
True Education



ISO 31000

www.namatek.com

ایزو ۳۱۰۰۰

فهرست مطالب

در دنیای پیچیده و رقابتی تجارت، مدیریت ریسک به یک جزء کلیدی برای موفقیت و پایداری هر سازمان تبدیل شده است. سازمان بین‌المللی استاندارد (ISO) چارچوبی را برای مدیریت ریسک مؤثر و کارآمد در همه انواع سازمان‌ها فراهم کرده است که از این چارچوب باعنوان ایزو ۳۱۰۰۰ یاد می‌شود. در این مقاله، ما بررسی خواهیم کرد که استاندارد ایزو ۳۱۰۰۰ چیست، هدف آن چیست و چگونه می‌تواند برای شرکت شما مفید باشد.

استاندارد ایزو ۳۱۰۰۰ چیست؟

چارچوب مدیریت ریسک ایزو ۳۱۰۰۰ یک استاندارد بین‌المللی است که دستورالعمل‌ها و اصول مدیریت ریسک را در اختیار سازمان‌ها قرار می‌دهد. این استاندارد توسط سازمان بین‌المللی استاندارد (ISO) توسعه یافته است و مجموعه‌ای از اصول و دستورالعمل‌ها را برای طراحی و اجرای چارچوب مدیریت ریسک ارائه می‌دهد. این استاندارد سازمان‌ها را قادر می‌سازد تا مدیریت ریسک را برای کلیه وظایف استراتژیک، مدیریتی و عملیاتی و همچنین پروژه‌ها، عملکردها و فرآیندها اعمال کنند.

ISO 31000:2018 جدیدترین نسخه این استاندارد است. سایر استانداردهای مدیریت ریسک از جمله استاندارد ISO IEC 31010 برای مدیریت ریسک ارائه شده توسط ISO و کمیسیون بین‌المللی الکتروتکنیک نیز وجود دارد. ابتکارات انطباق با مقررات، معمولاً مختص یک کشور خاص است و برای مشاغل با اندازه خاص یا مشاغل در صنایع خاص اعمال می‌شود. با این حال، ایزو ۳۱۰۰۰ برای استفاده در سازمان‌ها با هر اندازه‌ای طراحی شده است و مفاهیم آن در بخش عمومی و خصوصی یا در مشاغل بزرگ و کوچک و سازمان‌های غیرانتفاعی به خوبی کار می‌کنند. ایزو ۳۱۰۰۰ یک استاندارد جهانی برای شاغلین و شرکت‌هایی که از فرآیندهای مدیریت ریسک استفاده می‌کنند، ارائه می‌نماید. با این کار، سازمان‌ها می‌توانند شانس شناسایی ریسک‌ها را افزایش دهند و برای تخصیص منابع برای کاهش آن‌ها به‌درستی برنامه‌ریزی کنند.

به‌عنوان یک فرآیند، هدف مدیریت ریسک، شناسایی، ارزیابی و کنترل تهدیدات سرمایه، درآمد و عملیات سازمان است. یک چارچوب مدیریت ریسک موفق به سازمان کمک می‌کند تا طیف کاملی از ریسک‌هایی را که با آن مواجه است، در نظر بگیرد و در عین حال رابطه بین ریسک‌های مختلف و تأثیری که می‌تواند داشته باشد را نیز بررسی کند. این خطرات می‌تواند از منابع مختلفی مانند عدم قطعیت‌های مالی، بدهی‌های قانونی، مسائل فناوری، اشتباهات مدیریت استراتژیک، حوادث و بلایای طبیعی ناشی شود.

چارچوب و دستورالعمل ایزو ۳۱۰۰۰

چارچوب مدیریت ریسک از شش حوزه متمایز زیر تشکیل شده است:

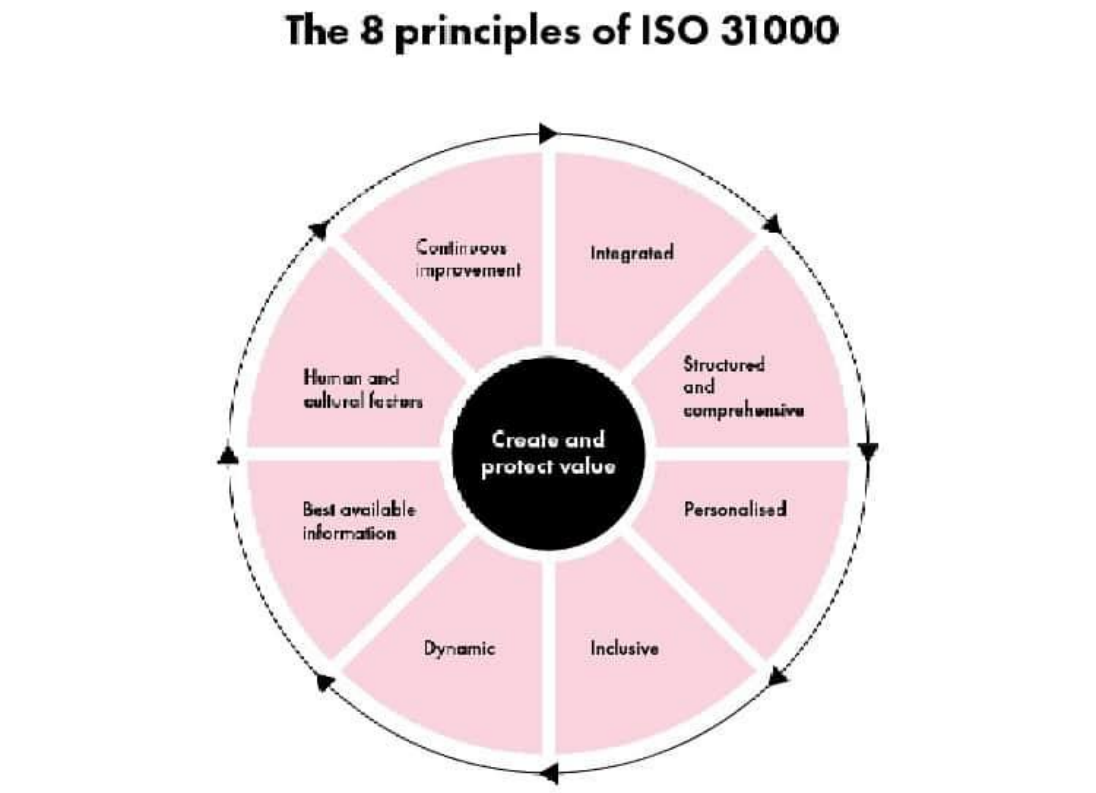
- **رهبری:** رهبران درون سازمان باید ابتکار عمل را به کار گیرند تا اطمینان حاصل کنند که ایزو ۳۱۰۰۰ به‌گونه‌ای اتخاذ و اعمال می‌شود که با فرهنگ و اهداف تجاری سازمان همسو باشد.
- **یکپارچه‌سازی:** درحالی که ادغام کاهش ریسک در بسیاری از فرآیندهای سازمانی تاثیر زیادی دارد؛ ولی مهم است که این مورد باعث ایجاد تنگناهای عملیاتی یا مانعی برای انجام فرآیندهای تجاری اصلی نشود.
- **طراحی:** سازمان‌ها باید استراتژی مدیریت ریسک را بر اساس نیاز خود طراحی کنند.
- **پیاده‌سازی:** فرآیند پیاده‌سازی، طراحی مدیریت ریسک سازمان را در فرآیندهای تجاری یکپارچه می‌کند. پیاده‌سازی معمولاً یک فرآیند رسمی با اهداف، ضرب‌الاجل‌ها و الزامات گزارش‌دهی است.

- **ارزیابی:** این قسمت طرح را ارزیابی می‌کند تا مشخص نماید چه چیزی کار می‌کند و چه چیزی ممکن است نیاز به اصلاح داشته باشد.
- **بهبود:** سازمان‌ها باید به طور مداوم به دنبال راه‌هایی برای بهبود اجرای ایزو ۳۱۰۰۰ خود باشند.

بسته به سازمان و تصمیم آن در مورد نحوه اجرای استاندارد، ممکن است چارچوب ایزو ۳۱۰۰۰ ساختار متفاوتی داشته باشد. به عنوان مثال، یک سازمان می‌تواند با استفاده از شش دستورالعمل زیر از این استاندارد پیروی کند:

- دامنه
- مراجع هنجاری
- اصطلاحات و تعاریف
- اصول
- چارچوب
- فرآیند

اصول مدیریت ریسک ایزو ۳۱۰۰۰



ایزو ۳۱۰۰۰ به‌دنبال کمک به سازمان‌ها برای اتخاذ رویکردی روشمند برای مدیریت ریسک با انجام سه کار کلیدی زیر است:

- شناسایی خطرات
- ارزیابی احتمال وقوع یک رویداد مرتبط با یک ریسک شناسایی‌شده
- تعیین شدت مشکلات ناشی از وقوع رویداد

به‌این‌ترتیب، ایزو ۳۱۰۰۰ به دنبال حذف خطرات نیست؛ زیرا حذف کامل همه خطرات غیرممکن است. در عوض، هدف آن کمک به سازمان‌ها در شناسایی ریسک‌ها و ایجاد استراتژی برای کاهش خطرات در صورت لزوم است. هشت اصل مهم ایزو ۳۱۰۰۰ که زیر اساس ایجاد یک چارچوب مدیریت ریسک هستند به شرح زیر است:

۱. **فراگیر:** برای موفقیت تلاش‌ها، ذی‌نفعان کلیدی باید درگیر شوند و دانش و دیدگاه‌های آن‌ها در نظر گرفته شود. مدیریت ریسک نیز باید شفاف و قابل درک باشد و شامل اصطلاحات گیج کننده نباشد.
۲. **پویا:** با توجه به این که سازمان‌ها در طول زمان تغییر می‌کنند، منابع ریسکی که امروز برای یک سازمان مرتبط هستند، ممکن است فردا تغییر کنند. اگر تلاش‌های کاهش ریسک سازمان‌ها به کار خود ادامه دهد، باید تحلیل ریسک مستمری را انجام دهند.
۳. **بهترین اطلاعات موجود:** تلاش‌های کاهش ریسک باید بر اساس بهترین و جدیدترین اطلاعات موجود برای ذی‌نفعان باشد. با این حال، سازمان‌ها همچنین باید بپذیرند که هرگز تمام اطلاعات موردنیاز را در اختیار نخواهند داشت و خطرات پیش‌بینی‌نشده همیشه وجود خواهند داشت.
٤. **عوامل انسانی و فرهنگی:** رفتار و فرهنگ انسانی بر مدیریت ریسک تأثیر می‌گذارد. لیست ریسک‌های شناسایی شده، باید شامل مواردی باشد که مربوط به خطای انسانی یا فرهنگ منحصربه‌فرد سازمان است.
۵. **بهبود مستمر:** پایبندی طولانی‌مدت به ایزو ۳۱۰۰۰ به معنای اتخاذ اصول بهبود مستمر برای اطمینان از بهبود تلاش‌های کاهش ریسک سازمان در طول زمان است.
٦. **یکپارچه:** مفاهیم کاهش ریسک و شناسایی باید در تمام فرآیندهای تجاری ادغام شوند.

۷. **ساختاریافته و جامع:** سازمان‌ها باید یک استراتژی جامع کاهش ریسک ایجاد کنند که تمام ریسک‌های شناخته شده را موردتوجه قرار دهد.

۸. **سفارشی:** از آنجا که هر سازمانی منحصربه‌فرد است، مفاهیم ایزو ۳۱۰۰۰ باید به‌صورت سفارشی برای سازمان تنظیم شوند تا به اهداف خود برسند.

نحوه اجرای مؤثر ایزو ۳۱۰۰۰

هر سازمانی باید رویکردی منحصربه‌فرد نسبت به ایزو ۳۱۰۰۰ داشته باشد؛ زیرا هر سازمانی متفاوت است. با این حال، استاندارد ISO سه مرحله کلیدی زیر را برای شروع مشخص می‌کند:

- **از اهداف آگاه باشید:** استراتژی کاهش ریسک یک سازمان باید با اهداف تجاری آن همخوانی داشته باشد، نه اینکه مانعی برای آن‌ها ایجاد کند.

- **ارزیابی حاکمیت موجود:** در سازمان‌های بزرگ‌تر که احتمالاً در حال حاضر ساختار حاکمیتی دارند، ساختار موجود می‌تواند در فرمول‌بندی نقش‌ها و رویه‌های مربوط به ایزو ۳۱۰۰۰ مفید باشد.
- **سطح تعهد را در نظر بگیرید:** قبل از اجرای ISO 31000، سازمان‌ها باید منابعی را که مایل به سرمایه‌گذاری در تلاش‌های کاهش ریسک خود هستند، در نظر بگیرند.

ایزو ۳۱۰۰۰ الزامات خاصی ندارد؛ اما بند ٦ آن راهنمایی کلی در مورد فرآیند مدیریت ریسک ارائه می‌دهد. مراحل فرآیند زیر در دستورالعمل‌های ایزو ۳۱۰۰۰ را می‌توان به ترتیب انجام داد که باید به طور مداوم تکرار شوند:

ارتباط و مشاوره

این فعالیت‌ها اغلب شامل آوردن زمینه‌های مختلف تخصص و درنظرگرفتن دیدگاه‌ها و سناریوهای مختلف، به سایر فعالیت‌های فرآیند مدیریت ریسک است و در تمام مراحل دیگر مدیریت ریسک انجام می‌شوند تا اطمینان حاصل شود که ذی‌نفعان مربوطه (داخلی و خارجی) از خطرات و نحوه برخورد با آن‌ها آگاه هستند و درک می‌کنند و برای تصمیم‌گیری مناسب، مدیر بازخورد و اطلاعات را دریافت می‌نماید.

محدوده، زمینه و معیارها

فرآیند مدیریت ریسک به طور مؤثر با تعریف آنچه می‌خواهیم به‌دست آوریم و تلاش برای درک عوامل خارجی و داخلی که ممکن است بر موفقیت ما تأثیر بگذارند، شروع می‌شود. این مرحله "محدوده، زمینه و معیار" نامیده می‌شود و قبل از شناسایی ریسک ضروری است.

مطابق با فرآیند مدیریت ریسکISO 31000 ، ایجاد معیارهای ریسک مناسب حیاتی است و باید در هنگام ایجاد زمینه تعریف شود و سپس در طول ارزیابی ریسک اعمال شود. معیار ریسک صرفاً به سطح ریسکی که شرکت ممکن است متحمل شود یا نشود، اشاره دارد. برای تعیین معیارهای ریسک، سازمان‌ها ممکن است موارد زیر را در نظر بگیرند:

- ماهیت و نوع عدم قطعیت‌ها
- روش تعریف و اندازه‌گیری پیامدها و احتمال
- عوامل مرتبط با زمان
- سطوح ریسک
- ظرفیت سازمان
- مدیریت ترکیبات و توالی ریسک‌های متعدد

ارزیابی ریسک

مرحله بعدی ارزیابی ریسک است که دارای سه فعالیت متوالی می‌باشد:

۱. **شناسایی ریسک**: درک عدم قطعیت‌ها، تهدیدها و سناریوها و فهرست‌کردن همه ریسک‌ها.
۲. **تجزیه‌وتحلیل ریسک**: درک عواقب و احتمال خطرات. تحلیل ریسک و در نتیجه اولویت‌بندی ریسک‌ها.
۳. **ارزیابی ریسک**: تعریف سطح اولویت هر ریسک از طریق اعمال معیارهای ریسک که در زمان ایجاد زمینه ایجاد شده‌اند.

روش‌های مختلفی مانند ماتریس احتمال و پیامد محبوب، تکنیک دلفی، مدل درخت تصمیم و FMEA (تحلیل حالت‌ها و اثرات شکست) برای ارزیابی ریسک وجود دارد.

درمان خطر

پس از مرحله ارزیابی، مرحله بعدی درمان ریسک است که شامل انتخاب و اجرای گزینه‌هایی برای رسیدگی به ریسک‌ها می‌شود. انتخاب، شامل مقایسه منافع بالقوه با هزینه‌ها یا تلاش‌های اجرای جایگزین‌ها است.

گزینه‌ها ممکن است از یک یا چند مورد زیر انتخاب شوند:

- **اجتناب**: اگر خطر خیلی زیاد است، می‌توانید تصمیم بگیرید که فعالیتی را که برنامه‌ریزی کرده بودید، شروع نکنید (یا ادامه ندهید). به عنوان مثال، اگر مقررات سخت‌گیرانه زیادی در منطقه‌ای وجود داشته باشد که می‌خواهید شعبه جدیدی از شرکت خود را افتتاح کنید، با شروع نکردن آن، از خطر جلوگیری می‌کنید.
- **اشتراک‌گذاری**: شما می‌توانید خطر را بین طرف دیگری تقسیم کنید. سرمایه‌گذاری‌های مشترک دقیقاً به همین دلیل وجود دارند. شما شعبه خود را با مشارکت با شرکت دیگری افتتاح می‌کنید که در استفاده از مقررات به نفع خود تخصص دارد.
- **انتقال**: شما می‌توانید تمام یا بخشی از ریسک را به شخص ثالث منتقل کنید. به عنوان مثال، ممکن است یک شرکت برخی از فعالیت‌های خود را از حوزه امنیت فناوری اطلاعات برون‌سپاری کند یا یک بیمه‌نامه منعقد کند.
- **پذیرش**: با دانستن و آگاهی از عواقب، ممکن است ترجیح دهید با خطر مواجه شوید. شما فقط آن شعبه را در یک منطقه بسیار منظم باز می‌کنید. پذیرش همچنین به عنوان حفظ ریسک شناخته می‌شود.

- **کاهش**: کاهش ریسک رایج‌ترین گزینه است که اقدامات کاهشی برای کاهش سطح ریسک انجام می‌شود. نمونه‌ای از این امر، آموزش کارکنان خود در مورد چگونگی شناسایی ایمیل‌های فیشینگ است یا با اجرای پشتیبان، می‌توانید خطر از دست رفتن داده‌ها را کاهش دهید. برای پیاده‌سازی، به یک طرح درمان ریسک نیاز دارید که فعالیت‌ها، منابع، طرف‌های مسئول و مهلت‌های زمانی را مشخص کند.

نظارت و بررسی

نظارت شامل بررسی مداوم عملکرد واقعی و سپس مقایسه آن با عملکرد مورد انتظار یا موردنیاز است. این بررسی شامل بررسی دوره‌ای یا بداهه وضعیت فعلی برای تغییرات در محیط، رویه‌های صنعت یا شیوه‌های سازمانی است. این فعالیتی است که برای تعیین مناسب‌بودن، کفایت و اثربخشی چارچوب و فرآیند، برای دستیابی به اهداف تعیین‌شده انجام می‌شود.

ثبت و گزارش

فرآیند مدیریت ریسک و نتایج آن باید مستند باشند و ابلاغ شوند؛ بنابراین باید ثبت و گزارش گردند. سازمان‌ها باید تصمیم بگیرند که چه چیزهایی را باید ثبت کنند (مانند حوادث، موارد نزدیک، عدم انطباق، دردسترس‌بودن سیستم و غیره). این سوابق، اطلاعاتی را برای تصمیم‌گیری برای افزایش اثربخشی فعالیت‌ها فراهم می‌کند.

گزارش‌دهی باید اطلاعاتی را به مدیریت ارشد و ذی‌نفعان سازمان ارائه دهد در مورد این که آیا ریسک‌ها در محدوده معیارهای ریسک هستند یا طرح‌های درمان ریسک معتبری وجود دارد که در نهایت به این نتیجه منجر می‌شود. علاوه بر این، ممکن است اطلاعاتی در مورد خطرات جدید و نوظهور ارائه دهد. این گزارش ممکن است بر اساس آنچه بازبینان مشاهده کرده‌اند، توصیه‌هایی برای بهبود سیستم ارائه نماید.

هدف ایزو ۳۱۰۰۰ چیست؟

هدف این استاندارد توسعه رویکرد مدیریت ریسک و آگاهی از اهمیت نظارت و مدیریت ریسک در بین کارکنان و ذی‌نفعان است. ایزو ۳۱۰۰۰ اصول، چارچوب و فرآیندی را برای کمک به سازمان‌ها، در هر اندازه یا هر صنعتی، در مدیریت ریسک‌ها به روشی سیستماتیک و مقرون‌به‌صرفه ارائه می‌کند که اصول، چارچوب و فرآیند آن، امکان مدیریت هر نوع ریسک را فراهم می‌کند (به‌عنوان مثال، خطرات امنیت اطلاعات، خطرات تداوم کسب‌وکار، ریسک‌های مالی، ریسک‌های زیست‌محیطی، ریسک‌های

کیفیت و غیره). برخلاف استانداردها و مدل‌های مدیریت ریسک مالی، که به طور گسترده مورد استفاده قرار می‌گیرد، ایزو ۳۱۰۰۰ استانداردی است که می‌تواند به راحتی توسط هر بخش دولتی، خصوصی یا سازمان غیردولتی صرف‌نظر از اندازه یا حوزه فعالیت آن اجرا شود.

مزایای استاندارد ایزو ۳۱۰۰۰

پذیرش استاندارد ایزو ۳۱۰۰۰ مزایای متعددی دارد که از جمله آن‌ها می‌توان به موارد زیر اشاره کرد:

- **اثربخشی:** از آنجایی که ایزو ۳۱۰۰۰ یک استاندارد بین‌المللی شناخته شده است، سازمان‌های بی‌شماری از آن استفاده می‌کنند. این بدان معنی است که ایزو ۳۱۰۰۰ به طور کامل بررسی شده و مؤثربودن آن ثابت شده است.
- **بررسی خطرات به روشی استاندارد:** زمانی که ایزو ۳۱۰۰۰ به‌درستی اجرا شود، به‌عنوان الگویی عمل می‌کند تا به سازمان‌ها کمک کند تا

محرک‌های اصلی ریسک را شناسایی کنند و معیارهای خطر و درمان‌های خطر را به روشی استاندارد تعیین نمایند.

- **ایجاد فرهنگ کاهش ریسک:** با گنجاندن کاهش ریسک، تقریباً در تمام فرآیندهای تجاری، کارکنان به ایده شناسایی و کاهش احتمالی خطرات عادت می‌کنند.
- **افزایش سودآوری سازمان:** هنگامی که یک سازمان خطرات غیرضروری را کاهش می‌دهد، احتمال آسیب مالی ناشی از رویدادهای مرتبط با آن خطر نیز کاهش می‌یابد.
- **اجبار سازمان به رفتار پیشگیرانه‌تر:** یک پیاده‌سازی خوب ایزو ۳۱۰۰۰ می‌تواند به سازمان کمک کند تا از واکنش‌پذیری به رویکردی فعال‌تر برای کاهش ریسک تغییر مسیر دهد.

چالش‌های استاندارد ایزو ۳۱۰۰۰

اگرچه مزایای واضحی برای پذیرش ایزو ۳۱۰۰۰ وجود دارد؛ اما چالش‌هایی نیز وجود دارد که باید در نظر گرفته شوند، از جمله موارد زیر:

- **پایبندی مستلزم تلاش مستمر است:** اگر سازمانی نتواند مفاهیم ایزو ۳۱۰۰۰ را در فرآیندهای تجاری خود بگنجاند، طرح کاهش ریسک ایجاد شده به سرعت منسوخ می‌گردد و احتمالاً توسط کارکنان نادیده گرفته خواهد شد.
- **احساس امنیت کاذب ممکن است به‌وجود آید:** حتی با وجود یک برنامه کاهش ریسک مؤثر، سازمان‌ها باید به خاطر داشته باشند که همیشه خطرات ناشناخته وجود خواهند داشت.

- **سازمان‌ها ریسک‌گریز شوند:** ریسک‌گریزی می‌تواند سرمایه‌گذاری از فرصت‌های جدید را برای سازمان دشوار کند.

زمان استفاده از مدیریت ریسک مبتنی بر ISO 31000

این استاندارد رهنمودهایی را ارائه می‌کند که می‌توانند در موقعیت‌های مختلفی که ارزیابی ریسک، درمان و نظارت بسیار مهم هستند، سازگار و اعمال شوند. در زیر مواردی وجود دارد که در آن شرکت‌ها می‌توانند از اعمال ایزو ۳۱۰۰۰ بهره‌مند شوند:

- تغییرات در اهداف سازمانی
- تحولات درونی و بیرونی سازمان
- تصمیمات استراتژیک و مهم
- وجود سناریوهای عدم قطعیت
- در زمان بررسی ریسک و اقدامات کاهشی
- اجرای انطباق قانونی
- تغییرات عملیاتی شرکت

سخن آخر

ایزو ۳۱۰۰۰ یک استاندارد بین‌المللی در زمینه مدیریت ریسک است. هدف اصلی این استاندارد، ارائه رهنمودهای سازگار برای هر نوع سازمان و زمینه خاص آن است.

برخلاف بسیاری از استانداردهای دیگرISO ، ایزو ۳۱۰۰۰ به‌دلیل مختصر بودن خود متمایز است که آن را به ابزاری مرجع برای هدایت فرآیندهای تصمیم‌گیری، برنامه‌ریزی استراتژیک و مدیریت مؤثر ریسک تبدیل می‌کند.
درحالی که بسیاری از سازمان‌ها در حال حاضر سطحی از مدیریت ریسک را اتخاذ کرده‌اند، بهترین شیوه‌های توصیه شده توسط ایزو ۳۱۰۰۰ برای بهبود و بهینه‌سازی این فرآیندها با تمرکز بیشتر بر ارتقای ایمنی محل کار فرموله شده است. علاوه بر این، این استاندارد اصول و دستورالعمل‌های جامعی را پوشش می‌دهد که سازمان‌ها را قادر می‌سازد تا تجزیه و تحلیل‌های دقیق ریسک و ارزیابی‌های قوی انجام دهند که منجر به تصمیم‌گیری آگاهانه‌تر و استراتژی‌های مدیریت کارآمدتر می‌شود.
به عبارت دیگر، اجرای اصول و دستورالعمل‌های ایزو ۳۱۰۰۰ نه‌تنها اثربخشی عملیاتی و حاکمیت سازمانی را بهبود می‌بخشد؛ بلکه اعتماد ذی‌نفعان را تقویت می‌کند و زیان‌های مالی بالقوه و آسیب به شهرت شرکت را کاهش می‌دهد.