Namatek
True Education

Risk Management Standards

www.namatek.com

استاندارد مدیریت ریسک

فهرست مطالب

استاندارد مدیریت ریسک مجموعه خاصی از فرآیندهای استراتژیک را تعیین می‌کند که با اهداف یک سازمان شروع می‌شود و قصد دارد خطرات را شناسایی کند و از طریق بهترین عملکرد، کاهش خطرات را ارتقا دهد.

استانداردها اغلب توسط آژانس‌هایی که با هم کار می‌کنند، طراحی می‌شوند تا اهداف مشترک را ارتقا دهند و به تضمین فرآیندهای مدیریت ریسک با کیفیت بالا کمک کنند. به‌عنوان مثال، استاندارد ISO 31000 در مورد مدیریت ریسک یک استاندارد بین‌المللی است که اصول و دستورالعمل‌هایی را برای مدیریت موثر ریسک ارائه می‌دهد.

در حالی که اتخاذ یک استاندارد مدیریت ریسک مزایای خود را دارد، بدون چالش نیز نیست. استاندارد جدید ممکن است با کاری که قبلا انجام می‌دادید، به راحتی مطابقت نداشته باشد، بنابراین می‌توانید روش‌های جدیدی را برای کار معرفی کنید. همچنین استانداردها ممکن است نیاز به سفارشی‌سازی برای صنعت یا تجارت شما داشته باشند.

استاندارد مدیریت ریسک چیست؟

استاندارد مدیریت ریسک مانند یک راهنما است تا اطمینان حاصل شود که مدیریت ریسک به‌روشی مناسب انجام می‌شود. استانداردها معمولاً شامل پست‌های بازرسی و نمونه‌هایی می‌شوند تا رعایت آن را برای سازمان‌ها

واقعا آسان کنند. استانداردهای مدیریت ریسک، به‌ویژه در زمینه کسب و کار و فناوری اطلاعات، دستورالعمل‌های مهمی هستند که به سازمان‌ها کمک می‌کنند تا ریسک‌ها را به‌طور موثر شناسایی، ارزیابی و مدیریت کنند.

شناخته شده‌ترین آن‌ها، استاندارد ISO 31000 برای مدیریت ریسک است. استاندارد ISO 31000:2018 به‌عنوان نقشه راه برای کسب‌وکارها برای عبور از خطرات احتمالی عمل می‌کند و اطمینان می‌دهد که هر تهدید احتمالی شناسایی، تجزیه و تحلیل و مدیریت مناسب می‌شود.

این پایبندی، نه تنها از سازمان در برابر خطرات پیش‌بینی‌نشده محافظت می‌کند؛ بلکه با نشان دادن تعهد در مدیریت ریسک به بهترین شیوه‌ها، اعتماد ذینفعان را نیز افزایش می‌دهد. این مرحله جایی است که شما گزینه‌های خود را در مورد نحوه مقابله با خطرات ارزیابی می‌کنید. اغلب، مانند انتخاب این است که خطرات خاصی را به شخص دیگری مثلاً از طریق بیمه یا برون سپاری، واگذار کنید. اگر علاقه‌مند به کسب اطلاعات بیشتری در مورد استاندارد مدیریت ریسک هستید، بیایید بیشتر به آن بپردازیم.

انواع مختلف استاندارد مدیریت ریسک

وقتی در مورد استاندارد مدیریت ریسک صحبت می‌کنیم، بر روی چند چارچوب کلیدی تمرکز می‌کنیم که به سازمان‌ها کمک می‌کنند تا از خطرات بالقوه مراقبت نمایند. این استانداردها مانند قوانین بازی برای مدیریت موثر عدم قطعیت‌ها هستند. انواع مختلف این استاندارد به صورت زیر هستند:

استاندارد مدیریت ریسک ISO 31000

ISO 31000 یک استاندارد بین‌المللی است که در سال ۲۰۰۹ منتشر شد (و در سال ۲۰۱۸ به روز شد) که اصول و دستورالعمل‌هایی را برای مدیریت موثر ریسک ارائه می‌دهد. این استاندارد، یک رویکرد کلی برای مدیریت ریسک را ترسیم می‌کند که برای انواع مختلف ریسک‌ها (ریسک‌های مالی، ایمنی، پروژه) می‌تواند اعمال شود و توسط هر نوع سازمانی مورد استفاده قرار گیرد. این استاندارد واژگان و مفاهیم یکسانی را برای بحث در مورد مدیریت ریسک فراهم می‌کند و دستورالعمل‌ها و اصولی را ارائه می‌دهد که می‌تواند به انجام یک بررسی انتقادی از فرآیند مدیریت ریسک سازمان شما کمک کند.

چارچوب مدیریت ریسک ISO 31000 که در بند ۵ تعریف شده است، نحوه مدیریت و کنترل فرآیند مدیریت ریسک را شرح می‌دهد و موفقیت مدیریت ریسک به میزان مدیریت و کنترل آن بستگی دارد.

1) مراحل فرآیند مدیریت ریسک تحت استانداردISO 31000

فرآیند مدیریت ریسک تحت استاندارد ISO 31000 مراحل زیر را به دنبال خواهد داشت:

۱. **رهبری و تعهد:** رهبری در مرکز این چارچوب قرار دارد. مدیریت ارشد نیاز به مشارکت و حمایت دارد که برای مدیریت ریسک بسیار مهم است. از فعالیت‌های مدیر می‌توان به موارد زیر اشاره کرد:
   - صدور و ابلاغ خط مشی مدیریت ریسک
   - تخصیص منابع مالی به مدیریت ریسک
   - تخصیص نقش‌ها و مسئولیت‌ها در سطوح سازمانی مناسب
   - نظارت بر ریسک‌ها و نتایج فعالیت‌های مدیریت ریسک به‌صورت سیستماتیک
   - پاسخگو بودن برای مدیریت ریسک

۲. **یکپارچه سازی**: یکپارچه سازی در مورد حصول اطمینان از این است که تمام فعالیت‌های مدیریت ریسک در عملیات روزانه و فعالیت‌های کلیدی شرکت تعبیه شده است. هنگامی که این یکپارچگی به‌درستی حاصل شود، مدیریت ریسک به بخشی طبیعی از کار تبدیل می شود، نه یک کار اضافی.

۳. **طراحی**: طراحی به درک زمینه سازمانی و بیان با مدیریت ارشد، برای چگونگی ارتباط مراحل فرآیند مدیریت ریسک و اجزای لازم با یکدیگر اشاره دارد.

٤. **پیاده‌سازی:** پیاده سازی به استقرار اسناد (به‌عنوان مثال، سیاست‌ها و رویه‌ها)، فناوری‌ها و سایر منابع اشاره دارد تا فرآیند مدیریت ریسک

طراحی شده، بتواند کار کند. شرکت در مرحله اجرا، باید یک برنامه مدیریت ریسک ایجاد کند. این طرح اقدامات خاصی را که باید انجام شود و ترتیب آن‌ها، از جمله زمان و منابع را به تفصیل بیان می‌کند و مشخص می‌نماید که چه کسی تصمیم می‌گیرد.

۵. **بررسی ارزیابی:** هنگام بررسی ارزیابی، اثربخشی فرآیند مدیریت ریسک و فعالیت‌ها اندازه‌گیری و به‌طور دوره‌ای بررسی می‌شود. براساس نتایج ارزیابی، سازمان قادر خواهد بود پیشرفت و خلأهای آن‌ها را ببیند و برای بهبود تصمیم‌گیری کند. سایر محرک‌های بهبود در کنار ارزیابی شامل در دسترس بودن دانش جدید و همچنین تغییرات قابل‌توجه در زمینه داخلی و خارجی سازمان می‌باشد.

این چارچوب بسیار شبیه به رویکرد برنامه‌ریزی (PDCA) استاندارد سیستم مدیریت است.

استاندارد مدیریت ریسک COSO ERM

استاندارد مدیریت ریسک COSO ERMکه توسط کمیته سازمان‌های حامی کمیسیون Treadway ساخته شده است، در عرصه مدیریت ریسک برجسته می‌باشد.

این چارچوب مانند بافنده اصلی است که به‌شما کمک می‌کند تا مدیریت ریسک را به‌طور یکپارچه در ساختار سازمان خود ایجاد کنید. این ویژگی که همه چیز در مورد همگام‌سازی مدیریت ریسک با اهداف و جاه طلبی‌های سازمان شما متناسب است، COSO ERMرا منحصربه‌فرد می‌کند.

این استاندارد فقط در مورد دوری از خطرات نیست؛ بلکه در مورد ریسک‌پذیری هوشمند به‌عنوان بخشی از استراتژی و فرآیند تصمیم‌گیری

مطرح است و دیدگاه کسب‌وکارها به مدیریت ریسک را تغییر می‌دهد. با استفاده از این چارچوب مدیریت ریسک به یک متحد استراتژیک تبدیل می‌شود که این به‌شما کمک می‌کند تا با اطمینان بیشتری از عدم اطمینان عبور کنید و راه را برای موفقیت پایدار هموار کنید.

COSO ERM مجموعه‌ای سفت و سخت از قوانین نیست و بیشتر شبیه یک جعبه ابزار همه‌کاره با اجزایی مانند حاکمیت، ارزیابی ریسک و پاسخ، فعالیت‌های کنترل داخلی و موارد دیگر است. این عناصر با هم کار می‌کنند تا یک رویکرد جامع برای مدیریت ریسک ایجاد کنند. هر سازمانی می‌تواند چارچوب COSO ERM را برای برآوردن نیازها و موقعیت خاص خود سفارشی کند. این انعطاف‌پذیری، COSO ERMرا به یک دارایی ارزشمند برای مدیریت موثر ریسک‌ها در حین پیگیری اهداف استراتژیک تبدیل می‌کند.

استاندارد انجام ارزیابی ریسک NIST SP 800-30

NIST SP 800-30مستقیماً به‌واسطه مؤسسه ملی استاندارد و فناوری (NIST) عرضه شده و بازیگر بزرگی در حوزه استاندارد مدیریت ریسک

امنیت اطلاعات است. این راهنما، به‌عنوان راهنمای دقیق شما برای پیمایش در دنیای پیچیده خطرات سایبری عمل می‌کند. این استاندارد نحوه انجام ارزیابی‌های کامل ریسک برای سیستم‌های اطلاعاتی را گام به گام شرح می‌دهد. همچنین یک منبع کلیدی برای هر سازمانی است که می‌خواهد از گنجینه‌های دیجیتال خود در برابر جدیدترین و بزرگترین خطرات سایبری محافظت کند.

NIST SP 800-30 می‌داند که هر سازمانی منحصربه‌فرد است، بنابراین شما را در تطبیق فرآیند با شرایط و نیازهای خاص خود راهنمایی می‌کند.

این راهنما به شما کمک می‌کند تا تهدیدات سایبری بالقوه و نقاط ضعف را شناسایی کنید و میزان احتمالی و تأثیرگذاری این تهدیدها را مشخص کنید. سپس به شما کمک می کند تا آن‌ها را براساس میزان مخاطره آمیز بودنشان مرتب کنید.

NIST SP 800-30 به شما این دانش را می‌دهد که دفاع خود را در جایی که بیشترین اهمیت را دارد، متمرکز کنید. بنابراین در دنیایی که تهدیدات سایبری همیشه در حال تغییر هستند، داشتن NIST SP 800-30 در برنامه مدیریت ریسک، بسیار مهم است.

استاندارد سیستم مدیریت امنیت اطلاعات (ISMS)

ISO/IEC 27001

ISO/IEC 27001 یک استاندارد برتر در دنیای سیستم‌های مدیریت امنیت اطلاعات (ISMS) است. این چارچوب برای سازمان‌هایی که به‌دنبال حفاظت از دارایی‌های اطلاعاتی خود هستند، مناسب می‌باشد. این استاندارد مدیریت ریسک در مورد راه اندازی سیستمی است که محرمانه بودن، یکپارچگی و در دسترس بودن مشخصات اطلاعاتی شما را تضمین می‌کند.

همچنین به سازمان‌ها کمک می‌کند تا از داده‌های حساس در برابر تهدیدات سایبری، دسترسی غیرمجاز و نقض داده‌ها محافظت کنند. بنابراین، ISO/IEC 27001 چیزی بیش از یک چک لیست است و یک چارچوب جامع است که شما را در راه‌اندازی و نگهداری یک ISMS که واقعا کار می‌کند، راهنمایی می‌نماید و شامل سیاست‌ها و رویه‌ها، اقدامات فنی و

استراتژی‌های مدیریت افراد می‌شود. این استاندارد در عصر دیجیتال امروزی، جایی که اطلاعات به اندازه طلا ارزشمند می‌باشند، بسیار مهم و حیاتی است. در دنیایی که نقض داده‌ها می‌تواند میلیون‌ها هزینه داشته باشد و به شهرت آسیب برساند، ISO/IEC 27001 فقط یک استاندارد نیست؛ بلکه یک سرمایه گذاری استراتژیک می‌باشد.

استاندارد مدیریت ریسک FERMA

FERMA (فدراسیون انجمن های مدیریت ریسک اروپا) در سال ۱۹۷٤ تاسیس شد که ۲۳ انجمن ملی مدیریت ریسک را در ۲۲ کشور اروپایی گرد هم می‌آورد. این فدراسیون بیش از ٥٦۰۰ مدیر ریسک فعال در طیف گسترده‌ای از بخش‌های تجاری از شرکت‌های بزرگ صنعتی و تجاری گرفته تا موسسات مالی و ارگان‌های دولتی محلی را نمایندگی می‌کند.

استاندارد FERMA بهترین دستورالعمل‌ها و رویکردهای مدیریت ریسک را در سراسر اروپا هماهنگ می‌کند و به موضوعاتی می‌پردازد که منحصراً به فعالیت‌های اروپایی مربوط می‌شود. این استاندارد مدیریت ریسک، راهنمایی برای کل فرآیندها، از شناسایی ریسک‌ها تا انتقال بخشی از آن ریسک به طرف دیگر را ارائه می‌دهد.

FERMA با سایر انجمن‌های مدیریت ریسک در سراسر جهان در ارتباط است و سمینارهای دوسالانه را در اکتبر برای افراد حرفه‌ای سازمان‌دهی می‌کند.

استاندارد مدیریت ریسک موسسه مدیریت پروژه (PMI)

استاندارد مدیریت ریسک موسسه مدیریت پروژه (PMI) یک راهنمای تخصصی می‌باشد که برای ادغام مدیریت ریسک در فرآیند مدیریت پروژه طراحی شده است. این چارچوب که توسط موسسه مدیریت پروژه (PMI) توسعه یافته است، یک رویکرد ساختاریافته و اثبات‌شده برای ادغام مدیریت ریسک در هر مرحله از چرخه عمر پروژه به شما ارائه می‌دهد و با ارائه یک رویکرد گام به گام به شما نشان می‌دهد که چگونه ریسک‌ها را در طول سفر پروژه خود شناسایی و ارزیابی کنید و بر آن‌ها مدیریت داشته باشید. چارچوب مدیریت ریسک PMI همچنین در مورد شناسایی پوشش‌های نقره‌ای، فرصت‌هایی که به‌عنوان ریسک پنهان می‌شوند، فعالیت می‌کند. این چارچوب که مانند یک ناوبر قابل اعتماد عمل می‌کند، به‌طور یکپارچه در فرآیند مدیریت پروژه ادغام می‌شود و به‌طور سیستماتیک شما را از طریق شناسایی و ارزیابی ریسک‌ها، استراتژی‌بندی پاسخ‌ها و نظارت مستمر بر این ریسک‌ها در حین تکامل پروژه‌تان راهنمایی می‌کند.

با استفاده از این استاندارد، می‌توانید ریسک را بخش مرکزی فرآیند برنامه‌ریزی پروژه خود قرار دهید که این روش تیم‌های پروژه را به انعطاف‌پذیری بیشتر، تصمیم‌گیری هوشمندانه‌تر مجهز می‌کند و شانس موفقیت پروژه شما را تا حد زیادی افزایش می‌دهد.

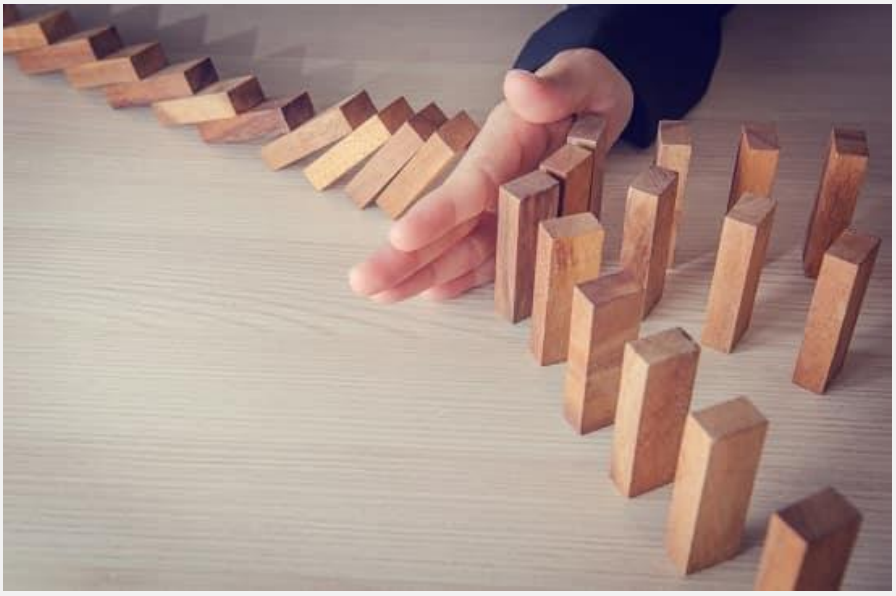
استاندارد مدیریت ریسک AS/NZS ISO 31000

AS/NZS ISO 31000 اقتباس استرالیا/نیوزیلند از استاندارد مدیریت ریسک ISO 31000 شناخته شده جهانی است و مانند استاندارد معروف مدیریت ریسک ISO 31000 می‌باشد. این انطباق منطقه‌ای از استاندارد جهانیAS/NZS ISO 31000 ، رویکردی متناسب با چشم‌اندازهای تجاری منحصربه‌فرد و چارچوب‌های نظارتی استرالیا و نیوزلند ارائه می‌دهد.

زیبایی AS/NZS ISO 31000 در تطبیق‌پذیری آن است. اگر در حال راه اندازی یک استارتاپ کوچک یا مدیریت یک شرکت بزرگ باشید، این استاندارد شما را تحت پوشش قرار می‌دهد. این استاندارد در بخش های مختلف قابل انطباق است و آن را به یک دارایی ارزشمند برای هر نوع کسب و کاری تبدیل می‌کند.

AS/NZS ISO 31000 همچنین فرهنگی را تقویت می‌کند که در آن مدیریت ریسک بخشی از استراتژی کسب و کار روزمره است. علاوه بر این، بر اهمیت ادغام ریسک با هر تصمیمی که می‌گیرید تأکید می‌کند. این بدان معنی است که هر حرکتی که کسب و کار شما انجام می‌دهد با درک کاملی از خطرات و مزایای بالقوه آن پشتیبانی می‌شود.

هدف استاندارد مدیریت ریسک چیست؟



هدف اصلی استانداردهای مدیریت ریسک این است که کارها را حتی زمانی که اتفاقات پیش‌بینی‌نشده رخ می‌دهند، به‌خوبی اجرا کنند. استفاده از استراتژی مناسب، به شما امکان می‌دهد تا ریسک‌ها را هوشمندانه و با اطمینان مدیریت کنید و به‌راحتی در دریاهای غیرقابل پیش‌بینی تجارت حرکت کنید. استانداردهای مدیریت ریسک به‌گونه‌ای طراحی شده‌اند که برای کمک به کسانی که باید فرآیندهای مدیریت ریسک را انجام دهند، راهنمایی وجود داشته باشد. این استانداردها به ایجاد یک اجماع بین‌المللی در مورد نحوه مقابله با خطرات خاص کمک می‌کنند و بهترین توصیه‌ها را در مورد نحوه برخورد با دیگران ارائه می‌دهند. همچنین به سازمان‌ها کمک می‌کنند تا استراتژی‌هایی را اجرا کنند که آزمایش‌شده و کارآمد هستند.

استاندارد مدیریت ریسک در مورد مدیریت فعالانه عدم اطمینان، تصمیم‌گیری آگاهانه و ایجاد یک سازمان، انعطاف‌پذیرتر است.نکته جالب

این است که این استانداردها فقط برای اجتناب از چیزهای بد نیستند؛ بلکه آن‌ها به‌شما کمک می‌کنند تا فرصت‌های مطلوب را به‌دست آورید. این استانداردها همگی مورد اعتماد هستند.

وقتی مشتریان و شرکا می‌بینند که شما خطرات را مانند یک مدیر حرفه‌ای مدیریت می‌کنید، به احتمال زیاد در کسب و کار خود به شما اعتماد خواهند کرد.

روش دسترسی به استاندارد مدیریت ریسک

استانداردهای مدیریت ریسک توسط تعدادی سازمان مختلف در سراسر جهان تولید می‌شوند. برای دسترسی به استانداردهای مدیریت ریسک این سازمان‌ها، باید از وب سایت این انجمن ها بازدید کنید یا از طریق دیگری با آن‌ها در تماس باشید. به‌عنوان مثال، استانداردهای مدیریت ریسک FERMA در وب سایت FERMA موجود است و برای سهولت دسترسی به چندین زبان مختلف ترجمه شده است. پیروی از برخی استانداردها می‌تواند یک سازمان را اعتباربخشی کند.

جمع‌بندی

استاندارد مدیریت ریسک معمولاً در ابتدای فرآیند مدیریت ریسک معرفی می‌شود؛ زیرا راهنمایی در مورد چگونگی تکمیل فرآیند به بهترین شکل ارائه می‌دهد. این استاندارد بر روش‌هایی که فرآیندهای مدیریت ریسک ایجاد و اجرا می‌شوند، تأثیر می‌گذارد.

آن‌ها راهنمایی در مورد تنظیم زمینه استراتژی‌ها و همچنین ارائه ایده‌هایی در مورد آن‌چه که باید و نباید به‌عنوان بخشی از استراتژی مدیریت ریسک

اجرا شود، ارائه می‌دهند. بسیاری از استانداردها توصیه هایی را در مورد چگونگی بهترین کمیت و طبقه بندی ریسک ارائه می دهند.

تصمیم‌گیری برای استفاده از کدام استاندارد می‌تواند مانند انتخاب طعم بستنی مورد علاقه خود باشد. خبر خوب این است که لازم نیست فقط یکی را انتخاب کنید. این استانداردها می‌توانند با هم همکاری کنند تا همه پایه‌های شما را پوشش دهند و مطمئن شوند که برای هر خطری که در راه است، آماده هستید. بسیاری از کسب‌وکارها بخش‌هایی از این استانداردها را با هم ترکیب می‌کنند تا استراتژی بسازند که مانند یک پوشش، با موقعیت منحصربه‌فرد آن‌ها مطابقت داشته باشد.