

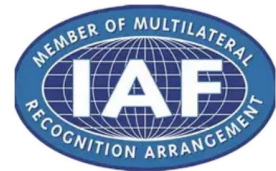


BRS

BRS.COMPANY



BRS به عنوان یک نهاد بین المللی با هدف ارائه خدمات با تمرکز بر انجام فعالیت های ممیزی سیستم های مدیریت، آموزش و صدور گواهینامه به منظور پوشش انتظارات سازمان مشتری BRS توسط سازمان معتبر بین المللی مانند IAF بدنبال اعتبار می باشد این شرکت با تلفیق مهارت ها، تجربیات و شایستگی ها و بهره مندی از کارشناسان فنی و ممیزان از طریق ممیزی دوستانه و بی طرفانه به دنبال توسعه ارزش افزوده برای سازمان های مشتری خود است فعالیت های خود را برای تعیین سطح انطباق سیستم های مدیریت سازمان های مشتری با توجه به الزامات استانداردهای بین المللی انجام می دهد. مادائماً مشتریان خود را مالک اصلی سازمان خود می دانیم. سازمان ما در تلاش است تا با شناسایی مستمر نیازهای مشتریان و ارائه خدمات توسعه یافته و متمایزتر، جایگاه بین المللی مشتریان را حفظ کرده و مسیر توسعه آنها را کوتاه کند. ما از طریق ارتباط مستمر با مشتریان خود به دنبال بهبود و توسعه خود هستیم و با رویکردی تخصصی در جهت توسعه مستمر سیستم های مدیریتی، تلاش می کنیم تا شما را به اهداف خود نزدیکتر کنیم.



آدرس: شهرک غرب - خیابان فرحزادی - ابتدای سیمای ایران - مجتمع تجاری
لیدوما - طبقه B1

شماره تماس: + 982186090160

تلگرام / واتس اپ : +989910338152

Email: marketing@brs.company



فرآیند مدیریت ریسک امنیت اطلاعات





متن فارسی استاندارد بین المللی ISO 31000 ویرایش 2018

ISO 31000:2018

استاندارد ایزو مدیریت ریسک

WWW.BRS.COMPANY

جهت دریافت گواهینامه های بین المللی ISO و گواهینامه انطباق اروپا CE با

تلفن های ۰۲۱-۸۶۰۹۰۱۶۰ و ۰۲۱-۸۶۰۹۰۶۲۲ تماس بگیرید.



پیش‌گفتار

استاندارد «مدیریت ریسک - رهنمودها» که نخستین بار در سال ۱۳۸۹ تدوین و منتشر شد، بر اساس پیشنهادهای دریافتی و بررسی و تایید کمیسیون‌های مربوط، برای اولین بار مورد تجدیدنظر قرار گرفت و در دویست و چهل و دومین اجلاس کمیته ملی استاندارد مدیریت کیفیت مورخ ۱۳۹۸/۱۰/۲۵ تصویب شد. اینک این استاندارد به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شماره ۵ (استانداردهای ملی ایران - ساختار و شیوه نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد جایگزین استاندارد ملی ایران شماره ۱۳۲۴۵: سال ۱۳۸۹ می‌شود.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است.

ISO 31000: 2018, Risk management – Guidelines

مقدمه

این استاندارد برای استفاده کسانی تهیه شده است که با مدیریت ریسک‌ها، تصمیم‌گیری‌ها، تعیین و تحقق اهداف و بهبود عملکرد در سازمان‌ها ارزش ایجاد کرده و از آن ارزش محافظت می‌کنند.

سازمان‌هایی در هر نوع و اندازه، با عوامل و تاثیرات خارجی و داخلی مواجه هستند که احتمال دستیابی آن‌ها به اهداف خود را نامعلوم می‌سازد.

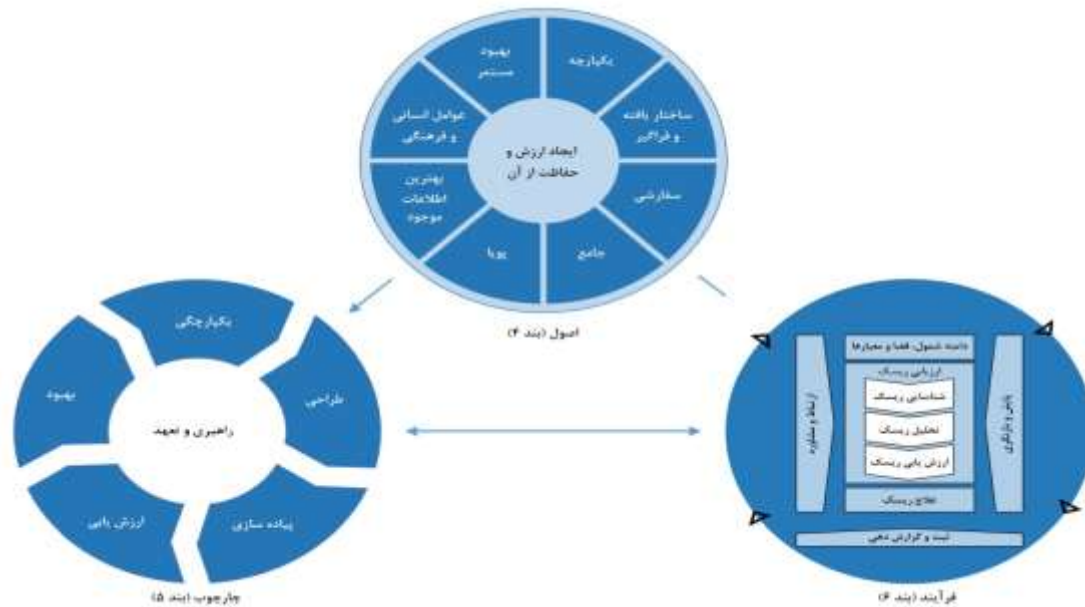
مدیریت ریسک، فرآیندی تکراری است که در تنظیم راهبرد، دستیابی به اهداف و تصمیم‌گیری آگاهانه، به سازمان‌ها کمک می‌کند.

مدیریت ریسک، قسمتی از حکمرانی^۱ و راهبری است و در چگونگی مدیریت یک سازمان در تمامی سطوح، نقشی اساسی داشته و به بهبود سیستم‌های مدیریت کمک می‌کند.

مدیریت ریسک، قسمتی از همه فعالیت‌های مرتبط با یک سازمان بوده و شامل تعامل با ذی‌نفعان است.

مدیریت ریسک، فضای خارجی و داخلی سازمان، شامل رفتارهای انسانی و عوامل فرهنگی را در نظر می‌گیرد.

مدیریت ریسک، بر اصول، چارچوب و فرآیند ترسیم‌شده در این استاندارد، همان‌طور که در شکل ۱ نشان داده شده است، استوار است. ممکن است این مؤلفه‌ها به‌صورت کامل یا جزئی در یک سازمان وجود داشته باشد، ولی به‌منظور مدیریت ریسک کارآمد، مؤثر و پایدار، ممکن است تطبیق یا بهبود آن‌ها لازم باشد.



شکل ۱ - اصول، چارچوب و فرآیند



مدیریت ریسک – رهنمودها

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، ارائه رهنمودهایی در رابطه با مدیریت ریسکی است که سازمان‌ها با آن مواجه هستند. این رهنمودها را می‌توان متناسب با هر سازمان و فضای آن، سفارشی‌سازی کرده و به کار برد.

این استاندارد، رویکردی مشترک را برای مدیریت هر نوع ریسک بیان کرده و مختص صنعت یا بخش خاصی نیست.

این استاندارد، در تمام طول عمر یک سازمان کاربرد داشته و قابلیت آن را دارد تا برای هر فعالیتی از جمله تصمیم‌سازی در همه سطوح به کار رود.

۲ مراجع الزامی

این استاندارد مراجع الزامی ندارد.

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌رود^۱:

۱-۳ ریسک

risk

تأثیر عدم قطعیت بر اهداف است.

یادآوری ۱- یک تأثیر، انحراف از انتظارات سازمان بوده و می‌تواند مثبت، منفی یا هر دو باشد و می‌تواند به فرصت‌ها و تهدیدها پرداخته، آن‌ها را ایجاد کرده یا منجر شود.

یادآوری ۲- اهداف می‌توانند جنبه‌ها و طبقه‌بندی‌های مختلفی داشته و در سطوح مختلفی به کار روند.

یادآوری ۳- معمولاً ریسک به صورت منابع ریسک (به زیربند ۳-۴ مراجعه شود)، رویدادهای (به زیربند ۳-۵ مراجعه شود) بالقوه، پیامدها (به زیربند ۳-۶ مراجعه شود) و احتمال (به زیربند ۳-۷ مراجعه شود) آن‌ها تعریف می‌شود.

۲-۳ مدیریت ریسک

risk management

۱- اصطلاحات و تعاریف به کار رفته در استانداردهای ISO و IEC در وبگاه‌های www.iso.org/obp و www.electropedia.org/ قابل دسترسی است.



فعالیت‌های هماهنگ‌شده برای هدایت و کنترل یک سازمان با توجه به ریسک (به زیربند ۳-۱ مراجعه شود) است.

۳-۳ ذی‌نفع

stakeholder

شخص یا سازمانی که می‌تواند تأثیر گذاشته، تأثیر پذیرفته، یا خود را در معرض آثار یک تصمیم یا فعالیت قرار دهد.

یادآوری - اصطلاح «شخص علاقه‌مند»^۱ را می‌توان به‌عنوان جایگزینی برای «ذی‌نفع» به‌کار برد.

۴-۳ منبع ریسک

risk source

عنصری که به تنهایی یا به‌صورت ترکیبی، قابلیت افزایش ریسک (به زیربند ۳-۱ مراجعه شود) را دارد.

۵-۳ رویداد

event

وقوع یا تغییر مجموعه خاصی از وقایع است.

یادآوری ۱- یک رویداد می‌تواند یک یا چند بار به‌وقوع بپیوندد و می‌تواند دلایل و پیامدهای (به زیربند ۳-۶ مراجعه شود) مختلفی داشته باشد.

یادآوری ۲- همچنین یک رویداد می‌تواند موردی باشد که انتظار آن می‌رود ولی اتفاق نمی‌افتد یا موردی باشد که انتظار نمی‌رود ولی اتفاق می‌افتد.

یادآوری ۳- رویداد می‌تواند منبع ریسک باشد.

۶-۳ پیامد

consequence

برونداد یک رویداد (به زیربند ۳-۵ مراجعه شود) که بر اهداف تأثیر می‌گذارد.

یادآوری ۱- یک پیامد می‌تواند قطعی یا غیرقطعی بوده و به‌صورت مستقیم یا غیر مستقیم بر اهداف، تأثیر مثبت یا منفی بگذارد.

یادآوری ۲- پیامدها را می‌توان به‌صورت کیفی یا کمی بیان کرد.

یادآوری ۳- هر پیامدی می‌تواند از طریق تأثیرات آبخاری^۲ و انباشته^۳ تشدید شود.

1- Interested party
2- Cascading
3- Cumulative



۷-۳ احتمال

likelihood

شانس اتفاق افتادن یک مورد است.

یادآوری ۱- در اصطلاح‌شناسی مدیریت ریسک (به زیربند ۳-۲ مراجعه شود)، واژه «احتمال» برای اشاره به شانس اتفاق افتادن موردی به کار می‌رود، خواه به‌طور عینی یا ذهنی، کیفی یا کمی، تعریف، اندازه‌گیری یا تعیین شده و با استفاده از اصطلاحات عمومی و ریاضی (مانند احتمال^۱ یا فراوانی در سراسر دوره زمانی معین) توصیف شده باشد.

یادآوری ۲- اصطلاح انگلیسی «likelihood»، در برخی زبان‌ها معادل مستقیم ندارد؛ در عوض، اغلب معادل اصطلاح «probability» استفاده می‌شود. با این حال، در زبان انگلیسی «probability» اغلب سرسختانه به‌عنوان یک اصطلاح ریاضی تعبیر می‌شود. بنابراین، در اصطلاح‌شناسی مدیریت ریسک، «likelihood» با این منظور به کار می‌رود که توصیه می‌شود همان تعبیر گسترده‌مانند اصطلاح «probability» را داشته باشد که در بسیاری از زبان‌ها، غیر از زبان انگلیسی دارد.

۸-۳ کنترل

control

سنجه‌ای که ریسک (به زیربند ۳-۱ مراجعه شود) را حفظ^۲ و/یا تعدیل می‌کند.

یادآوری ۱- کنترل‌ها شامل هر فرآیند، خط مشی، وسیله، رویه یا سایر شرایط و/یا اقداماتی هستند که ریسک را حفظ و/یا تعدیل می‌کند ولی محدود به آن‌ها نیست.

یادآوری ۲- کنترل‌ها ممکن است همیشه اثر تعدیلی مورد انتظار یا مفروض را اعمال نکنند.

۴ اصول

مقصود از مدیریت ریسک، ایجاد ارزش و حفاظت از آن است. مدیریت ریسک، عملکرد را بهبود بخشیده، نوآوری را تقویت کرده و از دستیابی به اهداف پشتیبانی می‌کند.

اصول مطرح شده در شکل ۲، راهنمایی را در مورد مشخصه‌های یک مدیریت ریسک کارآمد و مؤثر ارائه می‌کند که با ارزش آن ارتباط برقرار کرده و منظور و هدف آن را توضیح می‌دهد. این اصول، اساس مدیریت ریسک بوده و توصیه می‌شود در زمان تدوین چارچوب و فرآیندهای مدیریت ریسک سازمان، در نظر گرفته شوند. توصیه می‌شود این اصول، سازمان را قادر سازد تا تأثیرات عدم قطعیت بر اهداف سازمان را مدیریت کند.

1-Probability
2-Maintain



شکل ۲- اصول

مدیریت ریسک کارآمد، به عناصری که در شکل ۲ نشان داده شده نیاز دارد. این عناصر را می‌توان به صورت زیر، بیشتر توضیح داد:

الف- یکپارچه

مدیریت ریسک، بخشی جدایی‌ناپذیر از همه فعالیت‌های سازمانی است.

ب- ساختاریافته و فراگیر

رویکردی ساختاریافته و فراگیر برای مدیریت ریسک، که به نتایج پایدار و قابل مقایسه کمک می‌کند.

پ- سفارشی

چارچوب و فرآیند مدیریت ریسک، با فضای خارجی و داخلی مرتبط با اهداف سازمان، تنظیم و متناسب می‌شود.

ت- جامع

مشارکت مناسب و به موقع ذی‌نفعان باعث می‌شود که دانش، دیدگاه‌ها و یافته‌های آن‌ها در نظر گرفته شده و در نتیجه منجر به بهبود آگاهی و مدیریت ریسک آگاهانه می‌شود.

ث- پویا

با تغییر فضای خارجی و داخلی یک سازمان، ریسک‌ها ممکن است آشکار شده، تغییر یافته یا محو شوند. مدیریت ریسک، این تغییرات و رویدادها را پیش‌بینی، شناسایی و تایید کرده و به شیوه‌ای مناسب و به موقع پاسخ می‌دهد.

ج- بهترین اطلاعات موجود

ورودی‌های مدیریت ریسک، بر مبنای اطلاعات قدیمی و جاری و همچنین انتظارات سازمان از آینده است. مدیریت ریسک، همه محدودیت‌ها و عدم قطعیت‌های مرتبط با این اطلاعات و انتظارات را به وضوح در نظر می‌گیرد. توصیه می‌شود اطلاعات، به موقع و واضح ارائه شده و در دسترس ذی‌نفعان مرتبط قرار گیرد.

چ- عوامل انسانی و فرهنگی

فرهنگ و رفتار انسانی، به نحو قابل توجهی بر همه جنبه‌های مدیریت ریسک، در هر سطح و مرحله تأثیر می‌گذارد.

ح- بهبود مستمر

مدیریت ریسک، از طریق یادگیری و تجربه، به طور مستمر بهبود می‌یابد.

۵ چارچوب

۱-۵ کلیات

مقصود از چارچوب مدیریت ریسک، کمک به سازمان برای یکپارچه‌سازی مدیریت ریسک در فعالیت‌ها و کارکردهای مهم است. اثربخشی مدیریت ریسک، به یکپارچگی آن در حکمرانی سازمان، شامل تصمیم‌سازی، بستگی دارد. تحقق این امر، به پشتیبانی ذی‌نفعان، به خصوص مدیریت ارشد سازمان نیاز دارد.

توسعه چارچوب، شامل یکپارچه‌سازی، طراحی، پیاده‌سازی، ارزش‌یابی و بهبود مدیریت ریسک در سرتاسر سازمان است. شکل ۳، اجزای یک چارچوب را نشان می‌دهد.



شکل ۳- چارچوب



توصیه می‌شود سازمان، رویه‌ها و فرآیندهای مدیریت ریسک موجود خود و همه شکاف‌ها را ارزش‌یابی کرده و آن شکاف‌ها را درون چارچوب، شناسایی کند.

توصیه می‌شود اجزای چارچوب و نحوه تعامل آن‌ها با یکدیگر، متناسب با نیازهای سازمان تنظیم شود.

۲-۵ راهبری و تعهد

توصیه می‌شود در صورت امکان، مدیریت ارشد و نهادهای نظارتی اطمینان حاصل کنند که مدیریت ریسک در همه فعالیت‌های سازمانی، یکپارچه شده و راهبری و تعهد را با انجام موارد زیر اثبات کند:

- سفارشی‌سازی و پیاده‌سازی تمام اجزای چارچوب؛
 - صدور یک بیانیه یا خط‌مشی که رویکرد، طرح یا نحوه کار^۱ مدیریت ریسک را تعیین کند؛
 - اطمینان از اختصاص منابع لازم به مدیریت ریسک؛
 - تفویض و تعیین اختیارات، مسئولیت‌ها و وظایف در سطوح مناسب درون سازمان.
- انجام امور فوق به سازمان کمک خواهد کرد تا:
- مدیریت ریسک را با اهداف، راهبرد و فرهنگ خود، هم‌راستا سازد؛
 - همه وظایف و همچنین تعهدات داوطلبانه خود را شناسایی کرده و به آن‌ها بپردازد؛
 - میزان و نوع ریسکی را که ممکن است به‌عنوان راهنمایی برای توسعه معیارهای ریسک در نظر گرفته شود را تعیین کرده، و از برقراری ارتباط این موارد با سازمان و ذی‌نفعان آن، اطمینان حاصل کند؛
 - ارزش مدیریت ریسک را به سازمان و ذی‌نفعان آن منتقل کند؛
 - پایش نظام‌مند ریسک‌ها را ترویج کند؛
 - از تناسب میان چارچوب مدیریت ریسک با فضای سازمان، اطمینان حاصل کند.
- مدیریت ارشد سازمان پاسخگوی اجرای مدیریت ریسک است، در حالی که نهادهای نظارتی سازمان، پاسخگوی نظارت بر مدیریت ریسک هستند. اغلب، انجام موارد زیر از نهادهای نظارتی انتظار می‌رود یا ملزم به انجام آن‌ها هستند:
- در زمان تنظیم اهداف سازمان، از در نظر گرفتن ریسک‌ها به‌طور کامل اطمینان حاصل کنند؛
 - در پیگیری اهداف، ریسک‌های پیش روی سازمان را شناسایی کنند؛
 - از پیاده‌سازی و بهره‌برداری مؤثر سیستم‌ها برای مدیریت این‌گونه ریسک‌ها اطمینان حاصل کنند؛
 - از مناسب بودن این ریسک‌ها در محدوده اهداف سازمان اطمینان حاصل کنند؛

– از ارتباط صحیح اطلاعات مرتبط با این ریسک‌ها و مدیریت آن‌ها، اطمینان حاصل کنند.

۳-۵ یکپارچگی

یکپارچه‌سازی مدیریت ریسک، به شناخت ساختارها و فضای سازمانی بستگی دارد. ساختارها، بسته به مقاصد، اهداف و پیچیدگی سازمان، متفاوت هستند. ریسک، در هر قسمت از ساختار سازمان، مدیریت می‌شود. همه افراد یک سازمان، در قبال مدیریت ریسک مسئولیت دارند.

حکمرانی، هدایت سازمان، روابط خارجی و داخلی آن، قوانین، فرآیندها و رویه‌های لازم برای دستیابی به مقاصد سازمان را بر عهده دارد. ساختارهای مدیریت، جهت‌گیری حکمرانی را به سوی راهبرد و اهداف مرتبط مورد نیاز برای دستیابی به سطوح مطلوب عملکرد پایدار و رشد و ترقی بلند مدت، میسر می‌سازد. تعیین مسئولیت پاسخگویی و نقش‌های نظارتی مرتبط با مدیریت ریسک در یک سازمان، قسمت‌های جدایی‌ناپذیر از حکمرانی آن سازمان محسوب می‌شوند.

یکپارچه‌سازی مدیریت ریسک در یک سازمان، فرآیندی پویا و تکراری محسوب شده و توصیه می‌شود، متناسب با نیازها و فرهنگ سازمان، سفارشی‌سازی شود. بهتر است مدیریت ریسک، قسمتی از مقاصد، حکمرانی، راهبری و تعهد، راهبرد، اهداف و عملکردهای سازمانی بوده و جدا از آن‌ها نباشد.

۴-۵ طراحی

۱-۴-۵ شناسایی سازمان و فضای آن

در زمان طراحی چارچوب مدیریت ریسک، توصیه می‌شود سازمان، فضای خارجی و داخلی خود را مورد بررسی قرار داده و شناسایی کند.

بررسی فضای خارجی سازمان، ممکن است شامل موارد زیر باشد ولی به آن‌ها محدود نمی‌شود:

– عوامل اجتماعی، فرهنگی، سیاسی، قانونی، نظارتی، مالی، فناورانه، اقتصادی و زیست محیطی، اعم از بین‌المللی، ملی، منطقه‌ای یا محلی؛

– محرک‌ها و گرایش‌های کلیدی که بر اهداف سازمان تاثیر می‌گذارند،

– روابط، یافته‌ها، ارزش‌ها، نیازها و انتظارات ذی‌نفعان خارجی؛

– روابط و تعهدات قراردادی؛

– پیچیدگی شبکه‌ها و وابستگی‌ها؛

بررسی فضای داخلی سازمان ممکن است شامل موارد زیر باشد ولی به آن‌ها محدود نمی‌شود:

– چشم‌انداز، ماموریت و ارزش‌ها؛

– حکمرانی، ساختار سازمانی، نقش‌ها و پاسخگویی‌ها؛



- راهبرد، اهداف و خط‌مشی‌ها؛
- فرهنگ سازمان؛
- استانداردها، رهنمودها و مدل‌های اتخاذ شده توسط سازمان؛
- قابلیت‌هایی که به‌عنوان منابع و دانش شناخته می‌شوند (برای مثال، سرمایه، زمان، نیروی انسانی، مالکیت معنوی، فرآیندها، سیستم‌ها و فناوری‌ها)؛
- داده‌ها، سیستم‌های اطلاعاتی و جریان‌های اطلاعات؛
- روابط با ذی‌نفعان داخلی، با درنظر گرفتن یافته‌ها و ارزش‌های آن‌ها؛
- روابط و تعهدات قراردادی؛
- وابستگی‌های متقابل و ارتباطات داخلی.

۲-۴-۵ تشریح تعهد به مدیریت ریسک

- توصیه می‌شود مدیریت ارشد و نهادهای نظارتی، در صورت امکان، تعهد مستمر خود به مدیریت ریسک را از طریق یک خط‌مشی، یک بیانیه یا آشکال دیگری که به روشنی، حکایت از اهداف سازمان و تعهد به مدیریت ریسک دارد، اثبات و تشریح کند. توصیه می‌شود این تعهد، شامل موارد زیر بوده ولی به آن‌ها محدود نشود:
- مقصود سازمان از مدیریت ریسک و ارتباطات با اهداف و سایر خط‌مشی‌های سازمان؛
 - تقویت نیاز به یکپارچه‌سازی مدیریت ریسک در فرهنگ کلی سازمان؛
 - هدایت یکپارچه‌سازی مدیریت ریسک در فعالیت‌های اصلی کسب‌وکار و تصمیم‌سازی؛
 - اختیارات، مسئولیت‌ها و پاسخگویی‌ها؛
 - در دسترس قراردادن منابع لازم؛
 - شیوه‌ای که از طریق آن به اهداف متناقض رسیدگی می‌شود؛
 - اندازه‌گیری و گزارش‌دهی در شاخص‌های عملکرد سازمان؛
 - بازنگری و بهبود.

توصیه می‌شود تعهد مدیریت ریسک، به‌صورتی که مناسب است، درون سازمان و به ذی‌نفعان ابلاغ شود.

۳-۴-۵ واگذاری نقش‌ها، اختیارات، مسئولیت‌ها و پاسخگویی‌های سازمانی

- توصیه می‌شود مدیریت ارشد و نهادهای نظارتی، هر جا که قابل اجرا است، اطمینان حاصل کنند که اختیارات، مسئولیت‌ها و پاسخگویی‌های نقش‌های مرتبط، با درنظر گرفتن مدیریت ریسک، در همه سطوح سازمان، واگذار و ابلاغ شده و توصیه می‌شود:



- تاکید کند که مدیریت ریسک از مسئولیت‌های اصلی است؛
- افرادی که پاسخگویی و اختیار برای مدیریت ریسک دارند (مالکان ریسک) را شناسایی کند.

۴-۴-۵ تخصیص منابع

توصیه می‌شود مدیریت ارشد و نهادهای نظارتی، هر جا که قابل اجرا باشد، از تخصیص منابع مناسب برای مدیریت ریسک، اطمینان حاصل کنند. این منابع می‌تواند، شامل موارد زیر بوده ولی به آن‌ها محدود نمی‌شود:

- افراد، مهارت‌ها، تجربه و شایستگی؛
 - فرآیندها، روش‌ها و ابزارهای سازمان که برای مدیریت ریسک به کار می‌روند؛
 - فرآیندها و روش‌های اجرایی مستند؛
 - سیستم‌های مدیریت اطلاعات و دانش؛
 - نیازهای توسعه و آموزش حرفه‌ای.
- توصیه می‌شود سازمان، قابلیت‌ها و محدودیت‌های منابع موجود را در نظر بگیرد.

۵-۴-۵ برقراری ارتباط و مشاوره

توصیه می‌شود سازمان، به منظور حمایت از این چارچوب و تسهیل استفاده مؤثر از مدیریت ریسک، رویکردی مصوب در رابطه با ارتباط و مشاوره برقرار سازد. ارتباط، شامل به اشتراک گذاشتن اطلاعات با جامعه هدف است. مشاوره نیز شامل شرکت‌کنندگانی است که انتظارات خود را در تصمیم‌گیری‌ها و شکل آن یا سایر فعالیت‌ها بازخورد می‌دهند. توصیه می‌شود روش‌های ارتباط و مشاوره و محتوا، در جایی که مرتبط است، منعکس‌کننده انتظارات ذی‌نفعان باشد.

توصیه می‌شود ارتباط و مشاوره، به موقع انجام شود و اطمینان دهد که اطلاعات مرتبط، به‌طور مناسب، جمع‌آوری، تطبیق^۱، ترکیب^۲ و به اشتراک گذاشته شده و بازخورد ارائه می‌شود و بهبودها صورت می‌گیرد.

۵-۵ پیاده‌سازی

توصیه می‌شود سازمان، چارچوب مدیریت ریسک را با استفاده از موارد زیر پیاده‌سازی کند:

- توسعه طرحی مناسب شامل زمان و منابع؛
- شناسایی این‌که انواع مختلف تصمیم‌ها در سرتاسر سازمان، کجا، چه وقت و چگونه و توسط چه کسی گرفته می‌شوند؛

1- Collated
2- Synthesised



– تغییر فرآیندهای تصمیم‌سازی قابل اجرا در مواقع لزوم؛

– اطمینان از این که ترتیبات سازمان در خصوص مدیریت ریسک، به‌طور واضح، شناسایی و اعمال شده است.

پیاده‌سازی موفق چارچوب مدیریت ریسک، نیازمند مشارکت و آگاهی ذی‌نفعان است. این امر، سازمان‌ها را قادر می‌سازد تا به‌طور صریح، عدم‌قطعیت را در تصمیم‌سازی در نظر گیرند، همچنین اطمینان حاصل کنند که هر عدم‌قطعیت جدید یا بعدی را، همان‌طور که هست، می‌توان در نظر گرفت.

چارچوب مدیریت ریسکی که به‌طور مناسب طراحی و پیاده‌سازی شده باشد، تضمین خواهد کرد که فرآیند مدیریت ریسک، قسمتی از همه فعالیت‌های سرتاسر سازمان، شامل تصمیم‌سازی و تغییراتی در فضاهای خارجی و داخلی است که به قدر کفایت، گرفته خواهد شد.

۵-۶ ارزش‌یابی

به‌منظور ارزش‌یابی اثربخشی چارچوب مدیریت ریسک، توصیه می‌شود سازمان:

– به‌صورت دوره‌ای، عملکرد چارچوب مدیریت ریسک را در برابر مقصود، طرح‌های اجرایی، شاخص‌ها و رفتار مورد انتظار خود، اندازه‌گیری کند؛

– تعیین کند که آیا چارچوب مدیریت ریسک برای پشتیبانی از سازمان در دستیابی به این اهداف مناسب است یا خیر.

۵-۷ بهبود

۵-۷-۱ تطبیق دادن

توصیه می‌شود سازمان، به‌طور مستمر چارچوب مدیریت ریسک را پایش کرده و آن را با تغییرات خارجی و داخلی تطبیق دهد. با انجام این کار، سازمان می‌تواند ارزش خود را بهبود دهد.

۵-۷-۲ بهبود مستمر

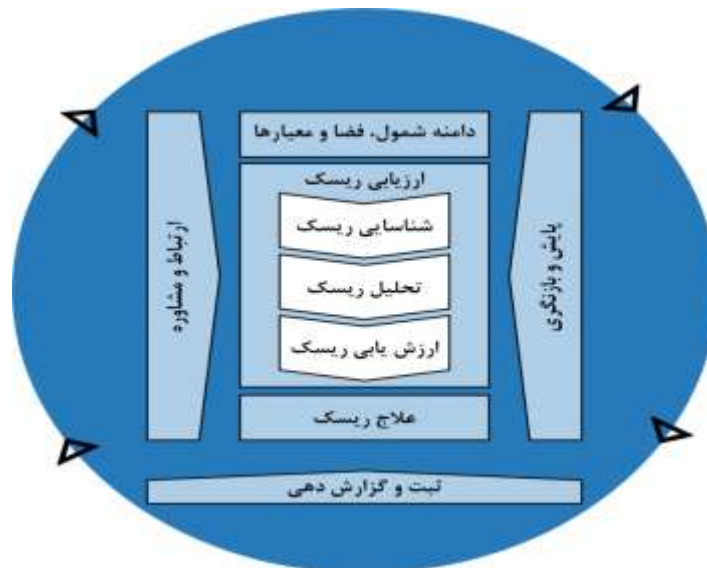
توصیه می‌شود سازمان، به‌طور مستمر، شایستگی، کفایت و اثربخشی چارچوب مدیریت ریسک و نحوه یکپارچه‌سازی فرآیند مدیریت ریسک را بهبود بخشد.

با شناسایی شکاف‌ها یا فرصت‌های بهبود مرتبط، توصیه می‌شود سازمان، طرح‌ها و وظایف را توسعه داده و آن‌ها را به افرادی که در پیاده‌سازی، پاسخگو هستند واگذار کند. توصیه می‌شود این بهبودها، به محض اجرا، به پیشرفت مدیریت ریسک کمک کند.

۶ فرآیند

۱-۶ کلیات

فرآیند مدیریت ریسک، شامل به کارگیری منظم خط‌مشی‌ها، روش‌های اجرایی و اقداماتی برای فعالیت‌های ارتباط و مشاوره، برقراری فضا و ارزیابی، علاج،^۱ پایش، بازنگری، ثبت و گزارش ریسک است. این فرآیند در شکل ۴ نشان داده شده است.



شکل ۴- فرآیند

توصیه می‌شود فرآیند مدیریت ریسک جزئی جدایی‌ناپذیر از مدیریت و تصمیم‌سازی بوده و در ساختار، عملیات و فرآیندهای سازمان، یکپارچه شود. فرآیند مدیریت ریسک می‌تواند در سطوح راهبردی، عملیاتی، برنامه‌ریزی یا پروژه، به کار گرفته شود.

کاربردهای زیادی از فرآیند مدیریت ریسک می‌تواند در یک سازمان وجود داشته و به‌منظور دستیابی به اهداف و مناسب‌کردن فضای خارجی و داخلی که در آن به کار گرفته می‌شود، سفارشی‌سازی شود.

توصیه می‌شود ماهیت پویا و متغیر رفتار و فرهنگ انسانی، در سرتاسر فرآیند مدیریت ریسک، در نظر گرفته شود.

گرچه فرآیند مدیریت ریسک اغلب به صورت ترتیبی ارائه می‌شود، ولی در عمل، تکراری است.

۲-۶ ارتباط و مشاوره

مقصود از ارتباط و مشاوره، کمک به ذی‌نفعان مرتبط در شناسایی ریسک است، که بر اساس آن، تصمیم‌گیری می‌شود و دلایل لزوم اقدامات خاص است. ارتباط، به دنبال ارتقاء آگاهی و شناسایی ریسک



است حال آن که مشاوره، شامل دستیابی به بازخورد و اطلاعات لازم برای پشتیبانی از تصمیم‌سازی است. توصیه می‌شود هماهنگی نزدیک میان این دو، با در نظر گرفتن محرمانه بودن و یکپارچگی اطلاعات و همچنین رعایت حریم خصوصی افراد، تبادل اطلاعات واقعی، به موقع، مرتبط، درست و قابل شناسایی را تسهیل کند.

توصیه می‌شود ارتباط و مشاوره با ذی‌نفعان مناسب خارجی و داخلی، در سرتاسر همه مراحل فرآیند مدیریت ریسک انجام شود.

ارتباط و مشاوره، به منظور دستیابی به اهداف زیر انجام می‌شود:

- گرد هم آوردن حوزه‌های تخصصی مختلف برای هر مرحله از فرآیند مدیریت ریسک؛
- حصول اطمینان از در نظر گرفتن مناسب دیدگاه‌های مختلف در زمان تعریف معیارهای ریسک و ارزش‌یابی ریسک‌ها؛
- تامین اطلاعات کافی، به منظور تسهیل نظارت بر ریسک و تصمیم‌سازی؛
- ایجاد حس فراگیر بودن و مالکیت در میان افرادی که تحت تأثیر ریسک هستند.

۳-۶ دامنه شمول، فضا و معیارها

۱-۳-۶ کلیات

مقصود از تعیین دامنه شمول، فضا و معیارها، سفارشی‌سازی فرآیند مدیریت ریسک، توانایی ارزیابی موثر ریسک و علاج مناسب ریسک است. دامنه شمول، فضا و معیارها، شامل تعریف دامنه شمول فرآیند و شناسایی فضای خارجی و داخلی است.

۲-۳-۶ تعریف دامنه شمول

توصیه می‌شود سازمان، دامنه شمول فعالیت‌های مدیریت ریسک خود را تعریف کند. از آنجا که فرآیند مدیریت ریسک ممکن است در سطوح مختلفی (مانند سطوح راهبردی، عملیاتی، برنامه‌ریزی، پروژه یا سایر فعالیت‌ها) به کار رود، واضح بودن اهداف مورد نظر مربوطه و هم‌ترازی آن‌ها با اهداف سازمانی دامنه شمول مورد نظر، مهم است.

در زمان طرح‌ریزی رویکرد، ملاحظات شامل موارد زیر است:

- اهداف و تصمیماتی که باید اتخاذ شوند؛
- بروندهایی که انتظار می‌رود از مراحل مختلف فرآیند به دست آید؛
- زمان، مکان، موارد شمول و خارج از شمول خاص؛
- ابزارها و تکنیک‌های مناسب ارزیابی ریسک؛



- منابع مورد نیاز، مسئولیت‌ها و سوابقی که باید نگه‌داری شود؛
- روابط با سایر پروژه‌ها، فرآیندها و فعالیت‌ها.

۳-۳-۶ فضای خارجی و داخلی

فضای خارجی و داخلی، محیطی است که سازمان در آن به دنبال تعریف و دستیابی به اهداف خود است. توصیه می‌شود فضای فرآیند مدیریت ریسک، بر مبنای شناسایی محیط خارجی و داخلی که سازمان در آن فعالیت می‌کند، برقرار شود و بهتر است منعکس‌کننده محیط خاص فعالیتی باشد که فرآیند مدیریت ریسک قرار است بر آن اعمال شود.

شناسایی این فضا به دلایل زیر اهمیت دارد:

- مدیریت ریسک در محدوده اهداف و فعالیت‌های سازمان انجام شود؛
 - عوامل سازمانی می‌توانند یک منبع ریسک باشند؛
 - هدف و دامنه شمول فرآیند مدیریت ریسک ممکن است به طور کلی، به اهداف سازمان وابسته باشد.
- توصیه می‌شود سازمان، فضای خارجی و داخلی فرآیند مدیریت ریسک را با در نظر گرفتن عواملی که در زیربند ۴-۵-۱ به آن‌ها اشاره شد، برقرار کند.

۴-۳-۶ تعریف معیارهای ریسک

توصیه می‌شود سازمان، میزان و نوع ریسکی که ممکن است در ارتباط با اهداف خود با آن‌ها روبرو شود یا نشود را مشخص کرده و همچنین معیارهایی را به منظور ارزش‌یابی اهمیت ریسک و پشتیبانی از فرآیندهای تصمیم‌سازی، تعریف کند. بهتر است معیارهای ریسک، با چارچوب مدیریت ریسک هم‌راستا بوده و با هدف و دامنه شمول خاص فعالیت مورد نظر، سفارشی‌سازی شده باشد. توصیه می‌شود معیارهای ریسک، منعکس-کننده ارزش‌ها، اهداف و منابع سازمان بوده و با خط مشی‌ها و بیانیه‌های مدیریت ریسک، سازگار باشد. بهتر است این معیارها، با در نظر گرفتن تعهدات سازمان و دیدگاه‌های ذی‌نفعان تعریف شود.

در حالی که توصیه می‌شود معیارهای ریسک، در ابتدای فرآیند ارزیابی ریسک، تعریف شود، با این حال، این معیارها پویا بوده و در صورت لزوم، بهتر است به‌طور مستمر مورد بازنگری و اصلاح قرار گیرد.

به‌منظور تنظیم معیارهای ریسک، توصیه می‌شود موارد زیر در نظر گرفته شود:

- ماهیت و نوع عدم قطعیت‌هایی که می‌تواند بر بروندها و اهداف (محسوس و نامحسوس) اثر گذارند؛
- چگونگی تعریف و اندازه‌گیری پیامدها (مثبت و منفی) و احتمال؛
- عوامل مرتبط با زمان؛
- ثبات در استفاده از اندازه‌گیری‌ها؛



- چگونگی تعیین سطح ریسک؛
- چگونگی در نظر گرفتن ترکیبات و توالی‌های چندین ریسک؛
- ظرفیت سازمان.

۴-۶ ارزیابی ریسک

۱-۴-۶ کلیات

ارزیابی ریسک به معنای فرآیند کلی شناسایی، تحلیل و ارزش‌یابی ریسک است.

توصیه می‌شود ارزیابی ریسک، به‌طور منظم، تکرار شونده و مشارکتی، با در نظر گرفتن دانش و دیدگاه‌های ذی‌نفعان اجرا شود. بهتر است این امر، با استفاده از بهترین اطلاعات در دسترس و در صورت لزوم، با تحقیقات بیشتر صورت گیرد.

۲-۴-۶ شناسایی ریسک

مقصود از شناسایی ریسک، یافتن، تشخیص و توصیف ریسک‌هایی است که ممکن است سازمان را در دستیابی به اهداف خود یاری رسانده یا مانع آن شوند. اطلاعات مرتبط، مناسب و به روز، در شناسایی ریسک‌ها، مهم است.

سازمان می‌تواند به‌منظور شناسایی عدم قطعیت‌هایی که ممکن است بر یک یا چند هدف تأثیر بگذارند، از گستره وسیعی از تکنیک‌ها استفاده کند. توصیه می‌شود عوامل زیر و رابطه میان آن‌ها، در شناسایی ریسک، مد نظر قرار گیرد:

- منابع محسوس و نامحسوس ریسک؛
- علل و رویدادها؛
- تهدیدها و فرصت‌ها؛
- آسیب‌پذیری‌ها و قابلیت‌ها؛
- تغییرات در فضای خارجی و داخلی؛
- شاخص‌های ریسک‌های نوظهور؛
- ماهیت و ارزش دارایی‌ها و منابع؛
- پیامدها و تأثیر آن‌ها بر اهداف؛
- محدودیت‌های دانش و قابلیت اتکا به اطلاعات؛
- عوامل مرتبط با زمان؛



– گرایش‌ها^۱، فرضیات و عقاید افراد دخیل.

فارغ از این که منابع ریسک، تحت کنترل سازمان باشد یا نباشد، توصیه می‌شود سازمان، ریسک‌ها را شناسایی کند. بهتر است ملاحظاتی در نظر گرفته شود که ممکن است بیش از یک نوع برون‌داد، حاصل شود که این امر خود می‌تواند به انواع پیامدهای محسوس یا نامحسوس منجر شود.

۳-۴-۶ تحلیل ریسک

مقصود از تحلیل ریسک، شناسایی ماهیت ریسک و مشخصه‌های آن، شامل سطح ریسک، در جای مناسب است. تحلیل ریسک، شامل در نظر گرفتن دقیق عدم قطعیت‌ها، منابع ریسک، پیامدها، احتمال، رویدادها، سناریوها، کنترل‌ها و میزان اثربخشی آن‌ها است. یک رویداد می‌تواند علل و پیامدهای متعددی داشته و بر اهداف متعددی اثر گذارد.

تحلیل ریسک می‌تواند بسته به مقصود آن، در دسترس بودن و اعتبار اطلاعات و منابع در دسترس، با درجات مختلفی از جزئیات و پیچیدگی انجام شود. بسته به شرایط و کاربرد مورد نظر، تکنیک‌های تحلیل ریسک می‌تواند کیفی، کمی یا ترکیبی از آن‌ها باشد.

توصیه می‌شود در تحلیل ریسک، عوامل زیر در نظر گرفته شود:

– احتمال رویدادها و پیامدها؛

– ماهیت و بزرگی پیامدها؛

– پیچیدگی و اتصال^۲؛

– عوامل مرتبط با زمان و بی‌ثباتی‌ها^۳؛

– اثربخشی کنترل‌های موجود؛

– سطوح حساسیت و اطمینان.

تحلیل ریسک ممکن است تحت تأثیر هرگونه اختلاف نظرها، گرایش‌ها، یافته‌ها و قضاوت‌ها قرار گیرد. تاثیرات دیگر، کیفیت اطلاعات مورد استفاده، فرضیات و ممنوعیت‌ها و همه محدودیت‌های تکنیک‌ها و نحوه اجرای آن‌ها است. توصیه می‌شود این تاثیرات، در نظر گرفته شده، مستند شده و به تصمیم‌سازان ابلاغ شود.

برآورد کمی رویدادهای با عدم قطعیت بالا می‌تواند دشوار باشد. این امر می‌تواند در زمان تحلیل رویدادهایی با پیامدهای شدید، مشکل‌ساز باشد. در چنین مواردی، به کار بردن ترکیبی از تکنیک‌ها، بینش بهتری را فراهم می‌آورد.

1- Biases
2- Connectivity
3- Volatility



تحلیل ریسک، اطلاعات ورودی لازم برای ارزش‌یابی ریسک و تصمیم‌سازی درباره نیاز به علاج ریسک و چگونگی آن و همچنین مناسب‌ترین راهبرد و روش‌های علاج ریسک را فراهم می‌کند. نتایج به‌دست آمده، بینش لازم برای تصمیم‌ها را در جایی که انتخاب‌ها انجام می‌شود و گزینه‌های دخیل در انواع و سطوح مختلف ریسک، تامین می‌کند.

۴-۴-۶ ارزش‌یابی ریسک

مقصود از ارزش‌یابی ریسک، پشتیبانی از تصمیم‌ها است. ارزش‌یابی ریسک شامل مقایسه نتایج تحلیل ریسک با معیارهای ایجادشده ریسک است. این مقایسه برای تعیین این است که در چه مکانی نیاز به اقدام اضافی است. این امر می‌تواند به تصمیم‌گیری برای موارد زیر منجر شود:

- کار بیشتری انجام نشود؛
 - گزینه‌های علاج ریسک در نظر گرفته شود؛
 - به‌منظور درک بهتر ریسک، تحلیل بیشتری انجام شود؛
 - کنترل‌های موجود حفظ شود؛
 - اهداف، تجدیدنظر شوند.
- توصیه می‌شود تصمیم‌ها، فضای وسیع‌تر و پیامدهای حقیقی و استنباط‌شده در رابطه با ذی‌نفعان خارجی و داخلی را در نظر داشته باشد.
- توصیه می‌شود برون‌داد ارزش‌یابی ریسک، در سطوح مناسب سازمان، ثبت، ابلاغ و سپس تایید شود.

۵-۶ علاج ریسک

۱-۵-۶ کلیات

مقصود از علاج ریسک، انتخاب و پیاده‌سازی گزینه‌هایی به‌منظور مقابله با ریسک است.

علاج ریسک، شامل فرآیندی تکراری شامل موارد زیر است:

- فرمول‌بندی و انتخاب گزینه‌های علاج ریسک؛
- طرح‌ریزی و پیاده‌سازی علاج ریسک؛
- ارزیابی اثربخشی علاج ریسک؛
- تصمیم‌گیری در خصوص قابل قبول بودن ریسک باقی‌مانده؛
- علاج بیشتر ریسک در صورت قابل قبول نبودن ریسک باقی‌مانده؛

۲-۵-۶ انتخاب گزینه‌های علاج ریسک

انتخاب مناسب‌ترین گزینه(های) علاج ریسک شامل ایجاد تعادل میان مزایای بالقوه حاصل شده مربوط به دستیابی به اهداف در مقابل هزینه‌ها، تلاش یا معایب ناشی از پیاده‌سازی آن است.

گزینه‌های علاج ریسک، الزاما به‌طور متقابل، انحصاری یا مناسب همه شرایط نبوده و ممکن است شامل یک یا چند مورد از موارد زیر باشند:

- جلوگیری از ریسک، با تصمیم‌گیری در مورد عدم شروع یا ادامه فعالیت‌هایی که باعث افزایش ریسک می‌شود؛

- از بین بردن یا افزایش ریسک، به‌منظور دستیابی به یک فرصت؛

- حذف منبع ریسک؛

- تغییر احتمال؛

- تغییر پیامدها؛

- به اشتراک‌گذاری ریسک (به‌عنوان مثال از طریق قراردادهای خرید بیمه)؛

- حفظ ریسک، با تصمیم آگاهانه.

توجه فرآیند علاج ریسک، از ملاحظات اقتصادی به‌تنهایی، فراتر بوده و توصیه می‌شود همه وظایف، تعهدات داوطلبانه و عقاید ذی‌نفعان سازمان را در نظر گیرد. توصیه می‌شود انتخاب گزینه‌های علاج ریسک، مطابق با اهداف سازمان، معیارهای ریسک و منابع موجود انجام گیرد.

در زمان انتخاب گزینه‌های علاج ریسک، توصیه می‌شود سازمان، ارزش‌ها، یافته‌ها و مشارکت بالقوه ذی‌نفعان و مناسب‌ترین راه‌ها برای تعامل و مشاوره با ایشان را مد نظر قرار دهد. علیرغم تاثیرگذاری برابر، برخی از گزینه‌های علاج ریسک ممکن است برای برخی ذی‌نفعان، نسبت به سایر ذی‌نفعان، بیشتر قابل قبول باشد.

علاج‌های ریسک، حتی اگر با دقت، طراحی و اجرا شوند، ممکن است بروندهای مورد انتظار را ارائه نداده و می‌تواند پیامدهای ناخواسته‌ای به دنبال داشته باشد. به‌منظور حصول اطمینان از این‌که اشکال مختلف علاج ریسک، مؤثر واقع شده و مؤثر باقی بمانند، باید پایش و بازنگری، به‌عنوان بخشی جدایی‌ناپذیر از این فرآیند باشد.

علاج ریسک نیز می‌تواند منجر به معرفی ریسک‌های جدیدی شود که نیاز به مدیریت دارند.

اگر هیچ گزینه در دسترس، برای علاج ریسک وجود نداشته باشد یا اگر گزینه‌های علاج ریسک، به اندازه کافی، ریسک را اصلاح نکنند، توصیه می‌شود ریسک، ثبت شده و مورد بازنگری مداوم قرار گیرد.



توصیه می‌شود تصمیم‌سازان و سایر ذی‌نفعان، نسبت به ماهیت و ابعاد ریسک باقیمانده، پس از علاج ریسک، آگاه باشند. بهتر است این ریسک باقیمانده، مستند شده و مورد پایش، بازنگری و در جای مناسب، علاج بیشتر قرار گیرد.

۳-۵-۶ آماده‌سازی و پیاده‌سازی طرح‌های علاج ریسک

مقصود از طرح‌های علاج ریسک، این است که مشخص شود گزینه‌های منتخب علاج ریسک، بهتر است چگونه اجرا گردند تا این تمهیدات، توسط افراد دخیل، درک شده و پیشرفت به موازات طرح، قابل پایش باشد. توصیه می‌شود طرح علاج ریسک، به روشنی، ترتیبی که بهتر است علاج ریسک اجرا شود را مشخص کند.

توصیه می‌شود طرح‌های علاج، با مشورت با ذی‌نفعان شایسته، در طرح‌ها و فرآیندهای مدیریتی سازمان، یکپارچه شود.

توصیه می‌شود اطلاعات ارائه‌شده در طرح علاج ریسک، شامل موارد زیر باشد:

- توضیح منطقی برای انتخاب گزینه‌های علاج ریسک، شامل مزایای قابل دستیابی مورد انتظار؛
- کسانی که در تصویب و اجرای طرح، پاسخگو و مسئول هستند؛
- اقدامات پیشنهادی؛
- منابع مورد نیاز شامل موارد احتمالی^۱؛
- اندازه‌گیری‌های عملکرد؛
- محدودیت‌ها؛
- گزارش‌دهی و پایش مورد نیاز؛
- زمان مورد انتظار برای اجرا و تکمیل اقدامات.

۶-۶ پایش و بازنگری

مقصود از پایش و بازنگری، حصول اطمینان و بهبود کیفیت و اثربخشی طراحی، پیاده‌سازی و برون‌دادهای فرآیند است. توصیه می‌شود پایش مداوم و بازنگری دوره‌ای فرآیند مدیریت ریسک و برون‌دادهای آن، قسمت طرح‌ریزی شده فرآیند مدیریت ریسک، با مسئولیت‌های تعریف‌شده واضح باشد.

توصیه می‌شود پایش و بازنگری، در تمام مراحل فرآیند انجام شود. پایش و بازنگری شامل طرح‌ریزی، جمع‌آوری و تحلیل اطلاعات، ثبت نتایج و ارائه بازخورد است.



توصیه می‌شود نتایج پایش و بازنگری، در سرتاسر فعالیت‌های مرتبط با مدیریت عملکرد، اندازه‌گیری و گزارش‌دهی سازمان، گنجانده شود.

۶-۷ ثبت و گزارش‌دهی

توصیه می‌شود فرآیند مدیریت ریسک و برون‌دادهای آن از طریق سازوکارهای مناسب، ثبت و گزارش شود. ثبت و گزارش‌دهی با اهداف زیر صورت می‌گیرد:

- ابلاغ فعالیت‌های مدیریت ریسک و برون‌دادهای آن در سرتاسر سازمان؛
 - تامین اطلاعات به‌منظور تصمیم‌سازی؛
 - بهبود فعالیت‌های مدیریت ریسک؛
 - کمک به تعامل بهتر با ذی‌نفعان، شامل افراد مسئول و پاسخگوی فعالیت‌های مدیریت ریسک.
- توصیه می‌شود تصمیم‌های مربوط به تهیه، نگهداری و رسیدگی به اطلاعات مستند شده، متناسب با مواردی نظیر کاربرد، حساسیت اطلاعاتی و فضای خارجی و داخلی و نه محدود به این موارد، در نظر گرفته شوند.
- گزارش‌دهی، قسمتی جدایی‌ناپذیر از حکمرانی سازمان بوده و توصیه می‌شود کیفیت گفتگو با ذی‌نفعان را بالا برده و از مدیریت ارشد و نهادهای نظارتی در رویارویی با مسئولیت‌هایشان، پشتیبانی کند. عواملی که توصیه می‌شود هنگام گزارش‌دهی در نظر گرفته شود شامل موارد زیر بوده ولی به آن‌ها محدود نمی‌شود:
- تنوع ذی‌نفعان و نیازها و الزامات اطلاعاتی مخصوص ایشان؛
 - هزینه، توالی و بهنگام بودن^۱ گزارش‌دهی؛
 - روش گزارش‌دهی؛
 - مرتبط بودن اطلاعات، با اهداف و تصمیم‌سازی سازمانی.



استاندارد ملی ایران شماره ۱۳۲۴۵ (تجدیدنظر اول): سال ۱۳۹۸

کتابنامه

[1] IEC 31010, Risk management - Risk assessment techniques

یادآوری - استاندارد ملی ایران شماره ۱۴۵۶۰: سال ۱۳۹۱، مدیریت ریسک - تکنیک‌های ارزیابی ریسک، با استفاده از استاندارد IEC/ISO 31010: 2009 تدوین شده است.