مرکز مشاوره و اطلاع رسانی

سیستم کاران

ISO 31000:2018

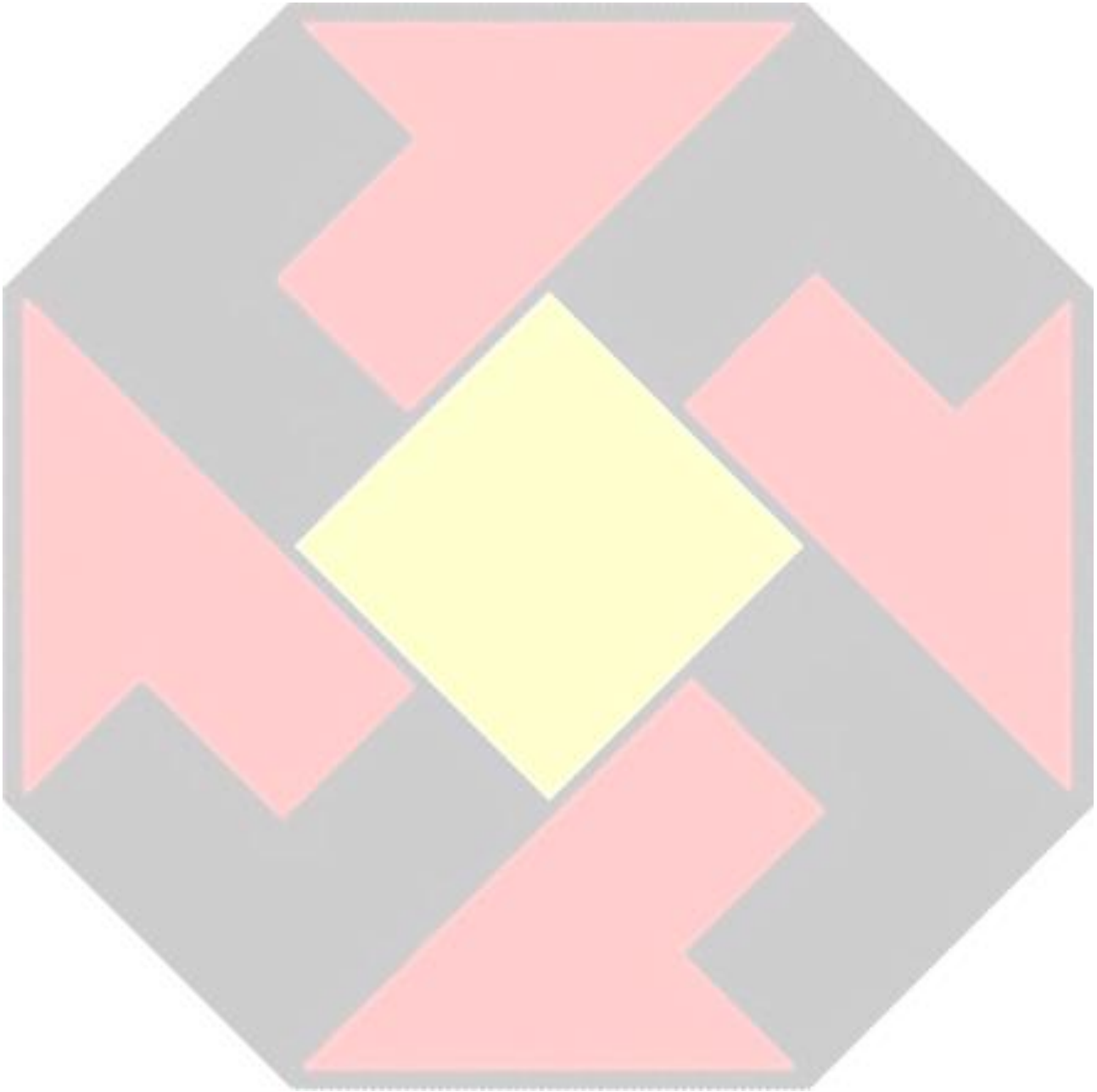
مدیریت ریسک-راهنماها

تهیه کننده :

مرکز مشاوره و اطلاع رسانی سیستم کاران

WWW.SYSTEMKARAN.ORG

فهرست



پیشگفتار

سازمان بین المللی استانداردسازی (ISO) اتحادیه نهادهای استانداردهای ملی جهانی (سازمانهای عضو ISO) میباشد. کار تهیه استانداردهای بین المللی معمولاً از طریق کمیته های فنی ISO انجام می شود. هر یک از نهادهای عضو در صورت علاقه به یک موضوع که برای آن کمیته فنی تشکیل شده است حق دارند در آن کمیته نماینده داشته باشند. سازمانهای بین المللی، دولتی و غیر دولتی در ارتباط با ISO نیز در این کار شرکت می نمایند. ISO همکاری نزدیکی در همه زمینه های استاندارد سازی الکتروتکنیک با کمیسیون بین المللی الکتروتکنیک (EC) دارد. روشهای اجرایی مورد استفاده در تدوین این مستند و آنهایی که به منظور نگهداری آتی استفاده شده اند در بخش ۱ مقررات ISO/IEC تشریح شده اند. به طور ویژه بایستی معیارهای تایید مختلفی برای انواع مستندات ISO مد نظر قرار گیرند.

www.iso.org/iso/foreword.htm1

پیش نویس این مستند مطابق با قوانین ویراستاری بخش ۲ مقررات ISO/IEC تهیه شده است. (به آدرس زیر رجوع شود)

www.iso.org/directives

بایستی توجه داشت که ممکن است برخی از بخش های این مستند شامل حق امتیاز تکثیر شوند. ISO نبایستی مسئولیتی در شناسایی قسمتی یا تمام بخشهای این حقوق داشته باشد. جزئیات هرگونه حق امتیاز مشخص شده در طی تدوین این مستند در مقدمه یا در فهرست بیانیه حق ثبت وجود خواهد داشت. (ببینید).

www.iso.org/patents

هر گونه نام تجاری استفاده شده در این مستند اطلاعات ارائه شده برای راحتی کاربران بوده و به معنای تایید آنها نیست.

برای شرح معنی واژگان و خاص ISO در خصوص ارزیابی انطباق و هم چنین کسب اطلاعاتی در مورد پیروی ISO از اصول سازمان تجارت جهانی (WTO) در موانع فنی تجارت (TBT) به آدرس ذیل مراجعه نمایید:

www.iso.org/iso/foreword.htm1

این مدرک توسط کمیته فنی ISO/TC262 مدیریت تهیه شده است.

این نسخه دوم، نسخه اول (ISO31000:2009) را که از نظر فنی تغییر یافته حذف و جایگزین آن می شود.

تغییرات اصلی در مقایسه با ویرایش قبلی به شرح زیر است:

بازنگری اصول مدیریت ریسک که معیارهای کلیدی موفقیت آن است.

پر رنگ تر نمودن رهبری توسط مدیریت ارشد و یکپارچه سازی مدیریت ریسک که با حاکمیت سازمان آغاز می شود.

تاکید بیشتر بر خاصیت تکرار شوندگی مدیریت ریسک با توجه به اینکه تجربیات، دانش و تحلیل جدید می توانند منجر به بازبینی اجزای، فرآیند فعالیتها و کنترل ها در هر مرحله از فرآیند شوند.

چابک سازی محتوا با توجه بیشتر بر حفظ یک مدل از سیستم های باز که متناسب با نیازها و فضای چندگانه میباشد.

مقدمه

این استاندارد برای استفاده افرادی است که طریق مدیریت ریسک ها، تصمیم گیری، تعیین و دستیابی به اهداف و بهبود عملکرد، به خلق و پشتیبانی ارزش میپردازند.

سازمان ها از هر نوع و اندازه ای با عوامل و اثرات داخلی و خارجی روبرو می شوند که دستیابی به اهدافشان را با عدم قطعیت همراه می نماید.

مدیریت ریسک {فعالیتی} تکرار شونده بوده و سازمان ها را در تعیین استراتژی ها، دستیابی به اهداف و تصمیم گیری آگاهانه کمک می کند.

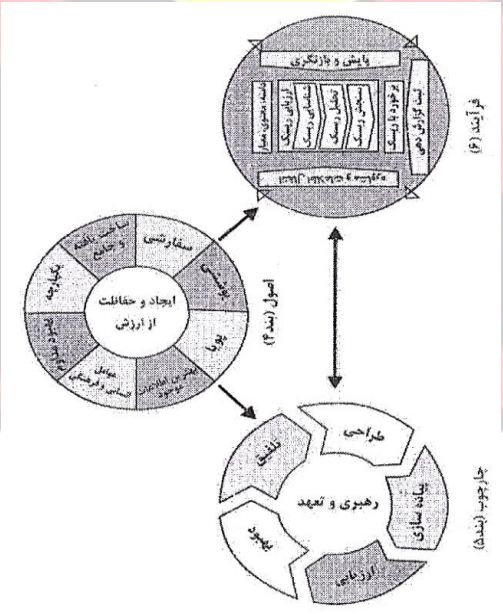
مدیریت ریسک بخشی از حاکمیت و رهبری {سازمان} بوده و مبنای چگونگی مدیریت نمودن سازمان در همه سطوح می باشد.

این امر به بهبود سیستمهای مدیریت کمک میکند.

مدیریت ریسک بخشی از کلیه فعالیتهای مرتبط با سازمان بوده و شامل تعامل با ذی نفعان است.

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

بر اساس شکل ۱ ، مدیریت ریسک براساس اصول، چهارچوب و فرآیند مشخص شده در این مدرک میباشد. این اجزا ممکن است. در حال حاضر به صورت کامل یا ناقص در سازمان وجود داشته باشند. با این وجود، ممکن است به متناسب شدن یا بهبود نیاز داشته باشند تا مدیریت ریسک کارا، اثربخش و سازگار شود.



شکل ۱: اصول، چهارچوبها و فرآیند

مدیریت ریسک - راهنماها

۱- دامنه کاربرد

این استاندارد راهنماهایی در مورد مدیریت ریسک هایی که سازمان ها با آنها روبرو میشوند را ارائه میدهد. این راهنماها می توانند به منظور استفاده در هر سازمانی با هر فضای سازمانی بومی سازی شوند.

این استاندارد رویکردی مشترک برای مدیریت هر نوع ریسکی ارائه می دهد و مختص صنعت یا بخش خاصی نیست.

۲- مراجع الزامی

در این استاندارد هیچ مرجع الزامی وجود ندارد.

۳- اصطلاحات و تعاریف

برای اهداف این استاندارد، اصطلاحات و تعاریف زیر کاربرد دارد.

{سازمانهای ISO و IEC پایگاه داده های اصطلاح شناسی برای استفاده در استانداردسازی در آدرسهای زیر دارند:

- بستر مرورگر برخط ایزو : قابل دسترسی در http://www.iso.org/obp
- الکترو پدیا TEC قابل دسترسی در http://www.electropedia.org

۳-۱- ریسک

اثر عدم قطعیت بر اهداف

نکته ۱ برای یادآوری: یک اثر یک انحراف از آنچه که مورد انتظار است میباشد. این انحراف میتواند مثبت، منفی یا هر دو باشد، و می تواند به فرصت و تهدیدها پرداخته، آنها را خلق یا منجر به آنها شود.

نکته ۲ برای یاد آوری: اهداف میتوانند جنبه ها و دسته بندی های مختلفی داشته، و میتوانند در سطوح مختلفی به کار روند.

نکته ۳ برای یادآوری: ریسک معمولاً در قالب منابع ریسک (۳-٤)، رویدادهای بالقوه (۳-۵)، پیامدهای (۳-۶) آنها و احتمال آنها (۳-۷) بیان میشود.

۳-۲- مدیریت ریسک

فعالیت های هماهنگ شده به منظور هدایت و کنترل یک سازمان با توجه به ریسک (۳-۱)

۳-۳- ذی نفع

فرد یا سازمانی که میتواند بر یک تصمیم یا فعالیت اثر گذاشته، اثر پذیرد یا دریابد که تحت تاثیر {آن تصمیم یا فعالیت} قرار می گیرد.

نکته ۱ برای یادآوری: اصطلاح "طرف ذی نفع " می تواند به جای "ذی نفع " استفاده شود.

۳-٤- منبع ریسک

فعالیت های هماهنگ شده به منظور هدایت و کنترل یک سازمان با توجه به ریسک (۳-۱) دارد.

۳-۵- رویداد

وقوع یا تغییر گروه خاصی شرایط

نکته ۱ برای یاد آوری: یک رویداد می تواند یک یا چند وقوع علت و پیامد داشته باشد، و میتواند چندین علت و پیامد (۳-۶) داشته باشد.

نکته ۲ برای یادآوری: یک رویداد همچنین می تواند امر مورد انتظاری باشد که رخ نمیدهد یا امر غیر منتظره ای باشد که رخ می دهد.

نکته ۳ برای یادآوری: یک رویداد می تواند یک منبع ریسک باشد.

۳-۶- پیامد

نتیجه یک رویداد (۳-۵) که بر اهداف اثر می گذارد

نکته یادآوری ۱: یک پیامد میتواند قطعی یا غیر قطعی باشد و می تواند اثرات مثبت یا منفی مستقیم یا غیر مستقیم بر روی اهداف داشته باشد.

نکته یادآوری ۲: پیامدها میتوانند به صورت کمی یا کیفی بیان شوند.

نکته یادآوری ۳: هر پیامدی میتواند از طریق اثرات آبشاری و تجمعی تشدید شود.

۳-۷- احتمال

فرصت وقوع چیزی

نکته یاد آوری ۱: در اصطلاح شناسی مدیریت ریسک (۳-۲)، لغت احتمال برای اشاره به فرصت وقوع چیزی استفاده می شود. خواه به صورت عینی یا ذهنی، کیفی و کمی تعریف، اندازه گیری تعیین، و با استفاده از اصطلاحات عمومی یا ریاضیاتی (از جمله احتمال یا تواتر در طول یک دوره زمانی معین) شرح داده شده باشند.

نکته یادآوری ۲: واژه انگلیسی "Likelihood" در برخی زبان ها معادل مستقیمی ندارد، به جای آن غالباً از واژه معادل "Probability" استفاده میشود. با این وجود، در زبان انگلیسی "Probability" غالباً دقیقاً به عنوان یک واژه ریاضی تفسیر می شود. بنابراین، در اصطلاح شناسی مدیریت ریسک، "Likelihood" با این هدف استفاده می شود که بایستی همان تفسیر گسترده ای را داشته باشد که اصطلاح "Probality" در بسیاری از زبان های غیر انگلیسی دارد.

۳-۸- کنترل

تمهیدی که ریسک (۳-۱) را حفظ و/ یا تعدیل نماید.

نکته یادآوری ۱: کنترلها شامل موارد زیر شده ولی محدود به آنها نمی شوند: هرگونه فرآیند، خط مشی، دستگاه رویه، با سایر و/ یا فعالیت هایی که ریسک را حفظ و یا تعدیل می نمایند.

شرایط نکته یادآوری ۲: کنترلها ممکن است همیشه اثر تعدیلی پیش فرض مورد انتظار را به وجود نیاورند.

٤- اصول

هدف مدیریت ریسک خلق و حفاظت از ارزش می باشد. این امر، عملکرد را بهبود بخشیده، نوآوری را

تشویق، دستیابی به هدف را پشتیبانی می نماید. اصولی که در شکل ۲ مشخص شده، راهنمایی هایی درباره ویژگی های مدیریت ریسک اثر بخش و کارا، اطلاع رسانی در مورد ارزش، مقصود و هدف آن را ارائه می نماید.

این اصول مبنایی برای مدیریت ریسک بوده و هنگام ایجاد چهارچوب و فرآیندهای مدیریت ریسک بایستی در نظر گرفته شوند. این اصول بایستی سازمان را قادر سازد تا اثرات عدم قطعیت بر اهداف خود را مدیریت نماید. مدیریت ریسک اثر بخش مستلزم وجود اجزای شکل ۲ بوده که می تواند به صورت زیر بیشتر توضیح داده شوند.

الف) یکپارچه

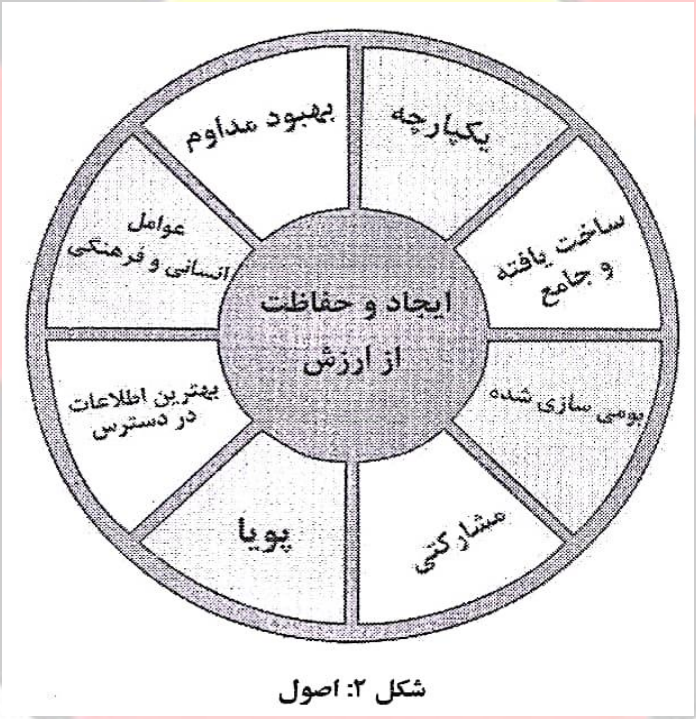
مدیریت ریسک بخشی جدایی ناپذیر در همه فعالیتهای سازمانی می باشد؛

ب) ساختار یافته و جامع

یک رویکرد ساختار یافته و جامع در مدیریت ریسک به نتایج با ثبات و قابل مقایسه منجر می شود.

ج) بومی سازی شده

چهارچوب و فرآیند مدیریت ریسک بومی سازی شده و متناسب با فضای درونی و بیرونی سازمان مرتبط با اهداف آن باشند.



شکل ۲: اصول

د) جامع

مشارکت مناسب و به موقع ذی نفعان امکان در نظر گرفتن دانش، دیدگاه ها و برداشت ها را فراهم می سازد. آگاهی و مدیریت ریسک آگاهانه می شود. این امر منجر به بهبود آگاهی و مدیریت ریسک آگاهانه می شود.

ه) پویا

با تغییر فضای درونی و بیرونی سازمان، ریسک های جدیدی امکان پدیدار شدن، تغییر یا از بین رفتن دارند. مدیریت ریسک آن تغییرات و رویدادها را به طور مناسبی و به موقع پیش بینی، شناسایی و تصدیق نموده و به آنها پاسخ می دهد.

و) بهترین اطلاعات در دسترس

ورودی ها به مدیریت ریسک بر مبنای اطلاعات فعلی و قبلی و همچنین انتظارات آینده میباشد. مدیریت ریسک هر گونه محدودیت و عدم قطعیتهای مربوط به چنین اطلاعات و انتظاراتی را به روشنی در نظر میگیرد. اطلاعات می بایست به موقع، واضح و در دسترس ذی نفعان مرتبط باشند.

ز) عوامل انسانی و فرهنگی

رفتار و فرهنگ انسانی به طور قابل توجهی بر تمام جنبه های مدیریت ریسک در هر سطح و مرحله ی گذارد.

ع) بهبود مداوم

مدیریت ریسک از طریق یادگیری و تجربه به طور مداوم بهبود می یابد.

۵- چهار چوب

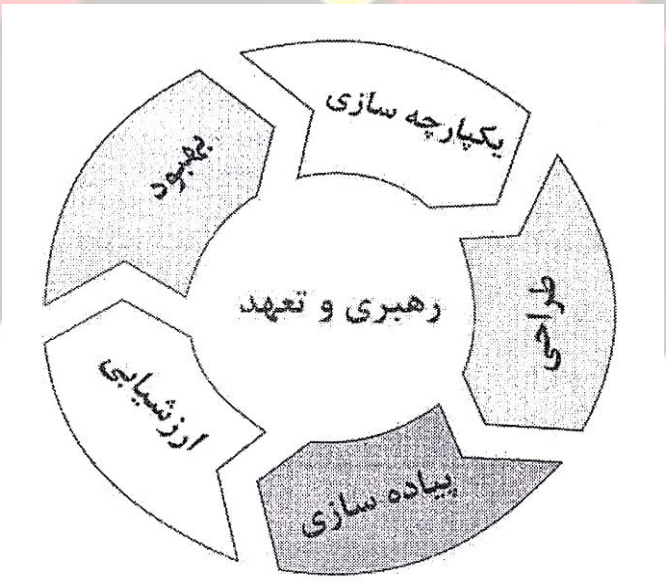
۵-۱- کلیات

مقصود چهارچوب مدیریت ریسک ، کمک به سازمان در یکپارچه ساری مدیریت ریسک درون فعالیتها و عملکردهای مهم می باشد.

اثر بخشی مدیریت ریسک بستگی به یکپارچگی با حاکمیت سازمان، شامل تصمیم گیری دارد.

این امر مستلزم پشتیبانی ذی نفعان به ویژه مدیریت ارشد است.

توسعه چهارچوب شامل یکپارچه، سازی، طراحی، اجراءِ، ارزیابی و بهبود مدیریت ریسک در سراسر سازمان می باشد. شکل ۳ اجزای یک چهارچوب را نشان میدهد.



شکل ۳: چهارچوب

سازمان بایستی رویه ها و فرآیندهای مدیریت ریسک موجود خود و هرگونه خلاءِ را ارزشیابی نموده و به آن خلاءِهای درون چهارچوب بپردازد. اجزای چهارچوب و روشی که آنها با هم کار میکنند بایستی با نیازهای سازمان بومی سازی شوند.

۵-۲- رهبری و تعهد

مدیریت ارشد و در صورت کاربرد نهادهای نظارتی، بایستی اطمینان حاصل نمایند که مدیریت ریسک درون تمام فعالیتهای سازمانی یکپارچه میشود و بایستی رهبری و تعهد {خود} را از طریق موارد زیر نشان دهد:

- بومی سازی و پیاده سازی تمامی اجزای چهارچوب.
- انتشار یک بیانیه یا خط که یک رویکرد، طرح یا را عملی را برای مدیریت ریسک ایجاد می کند.
- حصول اطمینان از اینکه منابع ضروری به مدیریت ریسک اختصاص می یابند.
- واگذاری اختیار، مسئولیت و پاسخگویی در سطوح مناسب درون سازمان. این امر به سازمان در موارد زیر کمک می کند:
- هم راستا نمودن مدیریت ریسک با اهداف، استراتژی و فرهنگ سازمان.
- شناسایی و پرداختن به تمامی ،تعهدات و همچنین تعهدات اختیاری سازمان.
- تعیین میزان و نوع ریسکی که ممکن است پذیرفته شود یا نشود تا معیارهای ریسک را مشخص کند، با حصول اطمینان از اینکه آنها به سازمان و ذی نفعان آن اطلاع رسانی می شود.
- اطلاع رسانی ارزش مدیریت ریسک برای سازمان و ذی نفعان آنها.
- ارتقای پایش سیستماتیک ریسک ها.
- حصول اطمینان از اینکه چهارچوب مدیریت ریسک متناسب با فضای سازمان باقی میماند.

مدیریت ارشد پاسخگوی مدیریت ریسک می باشد در حالی که نهادهای نظارتی پاسخگوی نظارت بر مدیریت ریسک می باشند.

اغلب از نهادهای نظارتی انتظار می رود یا ملزم هستند:

- که اطمینان حاصل نمایند که ریسکها به میزان کافی در زمان تنظیم اهداف مد نظر قرار می گیرند.
- درک ریسکهایی که سازمان به دنبال دستیابی به اهداف با آنها مواجه می شود.
- حصول اطمینان اینکه سیستمهایی برای مدیریت چنین ریسک پیاده سازی شده و به طور موثری عمل می کنند.
- حصول اطمینان از اینکه ریسکها متناسب با فضای اهداف سازمانی هستند.
- حصول اطمینان از اینکه اطلاعات چنین ریسک هایی و مدیریت آنها به طور مناسبی اطلاع رسانی میشوند .

۵-۳- یکپارچه سازی

یکپارچه سازی مدیریت ریسک به درک ساختارها و فضای سازمانی متکی است. ساختارها بسته به مقصود، اهداف و پیچیدگی سازمانی متفاوت میباشند. ریسک در هر بخش از ساختار سازمان مدیریت میشود. هر شخصی در یک سازمان در مورد مدیریت ریسک مسئولیت دارد.

جهت گیری سازمان، روابط درون و برون سازمانی، قوانین، فرآیندها و رویه های مورد نیاز به منظور دستیابی به مقصود سازمان توسط حاکمیت سازمان هدایت میشود.

ساختارهای مدیریتی، جهت گیری حاکمیتی را به استراتژی و اهداف مربوطه لازم جهت دستیابی به سطوح عملکرد پایدار و بادوام بلندمدت مورد نظر ترجمه می کنند. تعیین پاسخگویی مدیریت ریسک و نقشهای نظارتی درون سازمان بخش های جدایی ناپذیر حاکمیت سازمان میباشند.

یکپارچه سازی مدیریت ریسک در سازمان، یک فرآیند پویا و تکرار شونده بوده و بایستی متناسب با نیازها و فرهنگ سازمان بومی سازی شود. مدیریت ریسک بایستی بخشی از مقصود، حاکمیت، رهبری و تعهد، استراتژی اهداف و عملیاتهای سازمانی باشد و نه جدا از آن ها.

۵-٤- طراحی

۵-٤-۱- درک سازمان و فضای آن

هنگام طراحی چهارچوب مدیریت ریسک، سازمان بایستی فضای بیرونی و درونی خود را سنجیده و درک نماید. بررسی بافت بیرونی سازمان ممکن است شامل موارد زیر باشد ولی محدود به آن ها نیست:

- عوامل اجتماعی ،فرهنگی ،سیاسی ،قانونی، مقرراتی، مالی، فن آوری اقتصادی و زیست محیطی در سطح بین المللی، ملی، منطقه ای یا محلی.
- عوامل پیش برنده و روندهای کلیدی موثر بر اهداف سازمان.
- روابط، برداشت ها، ارزشها، نیازها و انتظارات ذی نفعان سازمانی.
- روابط و تعهدات قرار دادی.
- پیچیدگی های شبکه ها و وابستگی ها.

بررسی فضای درونی سازمان است شامل موارد زیر باشد ولی محدود به آنها نیست:

- چشم انداز، ماموریت و ارزش ها.
- حاکمیت ساختار سازمانی نقشها و پاسخ گویی ها.
- استراتژی، اهداف و خط مشی ها.
- فرهنگ سازمانی.
- استانداردها، راهنماها و الگوهای منتخب توسط سازمان.

توانایی هایی که در قالب منابع و دانش (به طور نمونه سرمایه، زمان، افراد، دارایی معنوی، فرآیندها، سیستم ها و فن آوری ها) درک می شوند؛

- داده ها، سیستم های اطلاعات و جریان های اطلاعات.

- ارتباطات با ذی نفعان داخلی، در نظر گرفتن برداشت ها در ارزشهای آنها.
- ارتباطات قراردادی و تعهدات.
- وابستگیها و ارتباطات متقابل.

۵-٤-۲- بیان تعهد مدیریت ریسک

مدیریت ارشد و در صورت کاربرد، نهادهای نظارتی بایستی تعهد مداوم خود را نسبت به مدیریت ریسک از طریق یک خط مشی، یک بیانیه با سایر اشکال که اهداف و تعهد یک سازمان به مدیریت کند نشان داده و بیان نمایند.

این تعهد بایستی حداقل شامل موارد زیر و نه فقط محدود به موارد ریسک را به وضوح منتقل می زیر باشند:

- مقصود سازمانی از مدیریت ریسک و اتصال به اهداف و سایر خط مشی های آن.
- تاکید بر نیاز به یکپارچه سازی مدیریت ریسک در فرهنگ کلی سازمان.
- هدایت یکپارچه سازی مدیریت ریسک درون فعالیت ها و تصمیم گیری های محوری کسب و کار.
- اختیارات مسئولیت ها و پاسخگویی ها.
- در دسترس قرار دادن منابع ضروری.
- روش رفتار با اهداف متناقض.
- اندازه گیری و گزارش دهی در {قالب} نشانگرهای عملکرد سازمان.
- بازنگری و بهبود.

تعهد مدیریت ریسک بایستی درون یک سازمان و به ذی نفعان به طور مناسب اطلاع رسانی شود.

۵-٤-۳- انتخاب نقش ها، اختیارات، مسئولیت ها و پاسخگویی های سازمانی

مدیریت ارشد و در صورت کاربرد، نهادهای نظارتی بایستی اطمینان گویی ها برای نقش های حاصل نمایند که اختیارات، مسئولیت ها و پاسخ مربوط به مدیریت ریسک واگذار شده و در همه سطوح سازمان اطلاع رسانی می شوند و بایستی:

- تاکید نمایند که مدیریت ریسک یک مسئولیت محوری است.

افرادی که پاسخ گویی و اختیار مدیریت ریسک را دارند (مشخص نماید مالکان ریسک).

۵-٤-٤- تخصیص منابع

مدیریت ارشد و در صورت کاربرد نهادهای نظارتی بایستی از تخصیص مناسب منابع برای مدیریت ریسک اطمینان حاصل نمایند که می تواند شامل موارد زیر باشد ولی به آنها محدود نمی شود:

- افراد، مهارت ها، تجربه و صلاحیت.
- فرآیندها، روشها و ابزارهای سازمان مورد استفاده برای مدیریت ریسک.
- فرآیندها و روشهای اجرایی مستند.
- سیستم های مدیریت اطلاعات و دانش.

- توسعه حرفه ای و نیازهای آموزشی.

سازمان بایستی توانمندیها و محدودیت های منابع موجود را مد نظر قرار دهد.

۵-٤-۵- ایجاد ارتباط و مشورت

سازمان بایستی رویکردی تایید شده برای اطلاع رسانی و مشورت به منظور پشتیانی از چهارچوب و تسهیل در به کارگیری موثر مدیریت ریسک ایجاد نماید. اطلاع رسانی شامل اشتراک اطلاعات با مخاطبان مورد نظر می باشد. مشورت همچنین شامل دریافت بازخورد از شرکت کنندگان شامل انتظارات آنان بوده که این امر به شکل دهی تصمیم گیری و سایر فعالیت ها کمک می نماید. روشها و محتوای اطلاع رسانی و مشورت اطلاع رسانی و مشورت بایستی به موقع بوده و از جمع آوری، ترتیب، تجزیه و به اشتراک گذاری اطلاعات به طور مناسب و تهیه بایستی انتظارات ذی نفعان را در جای مرتبط منعکس نماید.

اطلاع رسانی و مشورت بایستی به موقع بوده و از جمع آوری، ترتیب، تجزیه و به اشتراک گذاری اطلاعات به طور مناسب و تهیه بازخورد و ایجاد بهبودها اطمینان حاصل شود.

۵-۵- پیاده سازی

- توسعه یک طرح مناسب شامل زمان و منابع.
- مشخص نمودن اینکه انواع تصمیمات مختلف ،کجا چه زمانی می شوند.
- و چگونه و توسط چه کسی در سراسر سازمان اتخاذ میشوند.
- اصلاح فرآیندهای تصمیم گیری کاربردی در جای مورد نیاز.
- اطمینان از اینکه ترتیبات سازمانی برای مدیریت ریسک به طور روشنی درک و اجرا می شوند.

پیاده سازی موفق چهارچوب نیاز به مشارکت و آگاهی ذی نفعان دارد. این کار به طور روشن سازمان را قادر به پرداختن به عدم قطعیت ها در تصمیم گیری می نماید، در حالیکه همچنان اطمینان حاصل می نمایند که هرگونه عدم قطعیت جدید یا متعاقب، همزمان با ایجاد شدن می توانند در نظر گرفته شوند.

طراحی و پیاده سازی مناسب، چهارچوب مدیریت ریسک را مطمئن میسازد که فرآیند مدیریت ریسک بخشی از کلیه فعالیت های سراسر سازمان، شامل تصمیم گیری، بوده و تغییرات در فضاهای خارجی و داخلی سازمان به طور کافی اعمال خواهد شد.

۵-۶- ارزشیابی

به منظور ارزشیابی اثر بخشی چهارچوب مدیریت ریسک سازمان بایستی:

- به طور منظم عملکرد چهارچوب مدیریت ریسک را در مقایسه با مقصود، آن طرحهای پیاده سازی، نشانگرها و رفتار مورد انتظار اندازه گیری نماید؛
- تعیین اینکه آیا {چهارچوب مدیریت ریسک} در پشتیبانی برای دستیابی به اهداف سازمان به طور مناسب باقی می ماند یا خیر.

۵-۷- بهبود

۵-۷-۱- وفق دادن

سازمان بایستی به طور مداوم چهارچوب مدیریت ریسک را پایش و {با نیازهای سازمان} وفق تا به تغییرات درون و برون سازمان بپردازد.

در انجام این کار، سازمان میتواند ارزشهای خود را بهبود دهد.

۵-۷-۲- بهبود مداوم

سازمان بایستی به طور مداوم مناسب بودن، کفایت و اثر بخشی چهارچوب مدیریت ریسک و نحوه یکپارچه سازی فرآیند مدیریت ریسک را بهبود ببخشد. در حین شناسایی خلاءها یا فرصت های بهبود مرتبط، سازمان بایستی طرحها و وظایفی را توسعه داده و به منظور پیاده سازی به افراد مسئول واگذار نماید. پس از پیاده سازی، این بهبودها بایستی به تقویت مدیریت ریسک کمک نمایند.

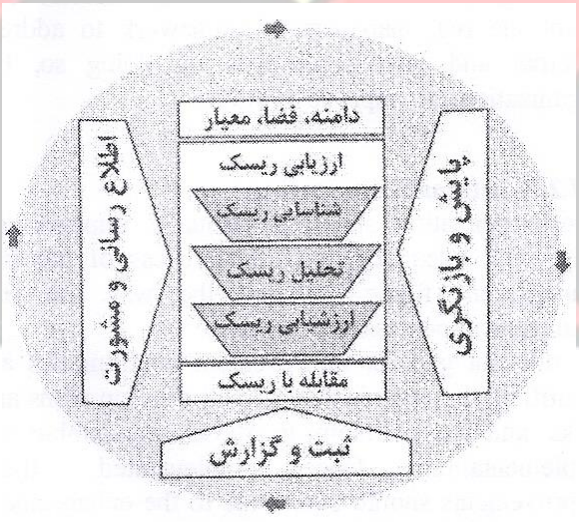
۶- فرآیند

۶-۱- کلیات

فرآیند مدیریت ریسک شامل به کارگیری سیستماتیک خط مشی ها، روش های اجرایی و رویه ها در فعالیتهای اطلاع رسانی و مشورت، درک و ارزشیابی فضای {سازمان}، مقابله، پایش، بازنگری، ثبت و گزارش دهی ریسک میباشد. این فرآیند در شکل ٤ نشان داده شده است.

مدیریت ریسک بایستی بخشی جدانشدنی از مدیریت و تصمیم گیری بوده و در ساختار، عملیاتها و فرآیندهای سازمان یکپارچه شود. این {فرآیند} میتواند در سطوح استراتژیک، عملیات، برنامه یا پروژه اعمال گردد.

فرآیند مدیریت ریسک میتواند کاربردهای زیادی درون یک سازمان داشته باشد و به منظور دستیابی به اهداف و تناسب با فضای درون و برون سازمان که در آن به کار میروند بومی سازی شود.



شکل ٤ – فرایند

طبیعت پویا و متغیر رفتار و فرهنگ انسانی بایستی در سراسر فرآیند مدیریت ریسک مد نظر قرار گیرد.

هر چند {مراحل} فرآیند مدیریت ریسک غالباً به صورت متوالی نشان داده میشوند، در عمل تکرار شونده میباشند.

۶-۲- اطلاع رسانی و مشورت

مقصود اطلاع رسانی و مشورت کمک به ذی نفعان مربوطه در درک ریسک، مبنایی برای ایجاد تصمیمات و دلایلی برای چرایی نیاز به فعالیتهای خاص میباشد. اطلاع رسانی به دنبال ارتقای آگاهی و درک ریسک بوده، حال آن که مشورت شامل قبول بازخورد و اطلاعات برای پشتیبانی از تصمیم گیری می باشد.

هماهنگی نزدیک بین این دو بایستی تبادل حقیقی، به موقع، مرتبط، دقیق و قابل درک اطلاعات را تسهیل نماید، در حالیکه محرمانگی و درستی اطلاعات و همچنین حقوق خصوصی افراد را در نظر می گیرد.

اطلاع رسانی و مشورت با ذی نفعان درونی و بیرونی مناسب بایستی درون و سرتاسر کلیه مراحل فرآیند مدیریت ریسک صورت پذیرد.

اطلاع رسانی و مشورت اهداف زیر را دنبال می نمایند:

- در کنار هم قرار دادن تخصصهای مختلف در هر مرحله از فرآیند مدیریت ریسک؛
- حصول اطمینان از اینکه هنگام تعریف معیارهای ریسک و ارزشیابی ریسک نظرات مختلف به طور مناسبی مد نظر قرار می گیرند؛
- فراهم آوری اطلاعات کافی برای تسهیل نظارت بر ریسک و تصمیم گیری؛
- ایجاد حس مشارکت و مالکیت بین افراد تحت تاثیر ریسک.

۶-۳- دامنه کاربرد، فضا و معیارها

۶-۳-۱- کلیات

مقصود از تعیین دامنه کاربرد، فضا و معیارها، بومی سازی فرآیند مدیریت ریسک، امکان پذیر نمودن ارزیابی موثر ریسک و مقابله مناسب با ریسک میباشد. دامنه کاربرد، فضا و معیارها شامل تعیین دامنه کاربرد فرآیند و درک فضای بیرونی و درونی میباشد.

۶-۳-۲- تعیین دامنه کاربرد

سازمان دامنه کاربرد فعالیت های مدیریت ریسک خود را تعیین نماید. از آنجایی که فرآیند مدیریت ریسک ممکن است در سطوح مختلف (به طور نمونه استراتژیک، عملیاتی، برنامه، پروژه و یا سایر فعالیتها) به کار رود، شفاف بودن دامنه کاربرد مورد نظر، اهداف مرتبط مدنظر و هم راستایی آنها با اهداف سازمانی مهم است.

هنگام طرح ریزی رویکرد موارد مورد نظر از قرار زیر می باشند:

- اهداف و تصمیماتی که بایستی اخذ شوند.
- نتایج مورد انتظار از مراحل فرآیند مدیریت {ریسک}.
- زمان، مکان و نکات خاصی که نیاز است مدنظر قرار گیرند یا نگیرند.

- ابزارها و تکنیک های مناسب ارزیابی ریسک.
- منابع مورد نیاز، مسئولیت ها و سوابق نیازمند نگهداری.
- روابط با سایر پروژه ها فرآیندها فعالیت ها.

۶-۳-۳- فضای درون و برون سازمانی

بافت برون و درون سازمان محیطی است که در آن سازمان به دنبال تعیین و دستیابی به اهداف خود می باشد.

فضای مدیریت ریسک بایستی از درک محیط بیرونی و درونی تشکیل شده که سازمان در آن فعالیت می کند و بایستی محیط خاص فعالیتی که فرآیند مدیریت ریسک در مورد آن اعمال می شود را منعکس نماید. درک محیط مهم است زیرا:

- مدیریت ریسک در فضای اهداف و فعالیت های سازمان صورت می پذیرد؛
- عوامل سازمانی می توانند منبعی از ریسک باشند؛
- مقصود و دامنه کاربرد فرآیند مدیریت ریسک ممکن است با اهداف سازمان به عنوان یک کل ارتباط متقابل داشته باشد.

سازمان بایستی فضای درون و بیرون فرآیند مدیریت ریسک را با در نظر گرفتن عوامل ذکر شده در بند ۱-٤-۵ تعیین نماید.

۶-۳-٤- تعیین معیارهای ریسک

سازمان بایستی میزان و نوع ریسک مرتبط با اهداف که ممکن است یا ممکن نیست با آن روبرو شود را در نظر گیرد. این امر همچنین بایستی معیارهایی را برای ارزشیابی اهمیت ریسک تعیین نموده تا فرآیندهای تصمیم گیری را پشتیبانی نماید. معیارهای ریسک بایستی با چهارچوب مدیریت ریسک هم راستا بوده و به منظور مقصود و دامنه کاربرد خاص و دامنه فعالیت مورد نظر بومی سازی شود.

معیارهای ریسک بایستی ارزش های سازمان، اهداف و منابع را منعکس نموده و با خط مشی ها و بیانیه های مدیریت ریسک متناسب باشند. این معیارها بایستی با در نظر گرفتن تعهدات و نظرات ذی نفعان سازمان تعیین شوند.

در حالیکه معیارهای ریسک بایستی در آغاز فرآیند ارزیابی ریسک ایجاد شوند، {این معیارها} پویا بوده و بایستی به طور مداوم بازنگری و در صورت نیاز اصلاح شوند.

برای تعیین معیارهای ریسک، موارد زیر بایستی مد نظر قرار گیرند:

- ماهیت و نوع عدم قطعیت هایی که می توانند بر روی نتایج و اهداف اثر بگذارند (هم نا محسوس و هم نامحسوس)؛
- چگونه پیامدها (هم مثبت و هم منفی) و احتمال، تعیین و اندازه گیری خواهند شد؛
- عوامل مربوط به زمان؛
- ثبات در استفاده از اندازه گیری ها؛

- چگونه سطح ریسک تعیین خواهد شد؛
- چگونه ترکیبات و توالی ریسکهای چندگانه در نظر گرفته می شوند؛
- ظرفیت سازمان.

۶-٤- ارزیابی ریسک

۶-٤-۱- کلیات

ارزیابی ریسک فرآیند جامع شناسایی، تحلیل و ارزشیابی ریسک است. ارزیابی ریسک بایستی به طور سیستماتیک، تکرار شونده و مشارکتی اجرا شده و دانش و نظرات ذی نفعان را مد نظر قرار دهد.

{ارزیابی ریسک} بایستی بهترین اطلاعات در دسترس را مورد استفاده قرار داده که در صورت لزوم با بررسی بیشتر تکمیل گردد.

۶-٤-۲- شناسایی ریسک

مقصود از شناسایی ریسک یافتن، شناسایی و توصیف ریسک هایی است که ممکن است به دستیابی یک سازمان به اهدافش کمک نموده یا از رسیدن به آن بازدارد. اطلاعات مرتبط، مناسب و به روز در شناسایی ریسکها اهمیت دارد. سازمان می تواند برای شناسایی عدم قطعیتهایی که ممکن است یک هدف یا بیشتر را متاثر نماید گستره ای از تکنیک ها را استفاده نماید. عوامل زیر و ارتباط بین این عوامل بایستی مد نظر قرار گیرد:

- منابع ریسک محسوس و نا محسوس؛
- دلایل و رویدادها؛
- تهدیدها و فرصت ها؛
- آسیب پذیری و قابلیت ها؛
- تغییرات در فضای بیرونی و درونی سازمان؛
- نشانگرهای ریسک های در حال ظهور؛
- ماهیت و ارزش دارایی ها و منابع؛
- پیامدها و تاثیر آنها بر اهداف؛
- محدودیتهای دانش و قابلیت اطمینان اطلاعات؛
- عوامل مرتبط با زمان؛
- جهت گیری ها، فرضیات و عقاید افراد درگیر.

سازمان بایستی ریسک ها را چه منبع آنها تحت کنترل باشد یا نباشد شناسایی کند. بایستی توجه داشت که ممکن است بیش از یک نوع نتیجه که ممکن است منجر به انواع پیامدهای محسوس یا نامحسوس شود وجود داشته باشد.

۶-٤-۳- تحلیل ریسک

مقصود از تحلیل ریسک درک ماهیت ریسک و ویژگی های آن از قبیل سطح ریسک در جایی که مناسب می باشد است. تحلیل ریسک شامل در نظر گرفتن جزئیات عدم قطعیت ها، منابع ریسک، پیامدها ،احتمال، رویدادها، سناریوها، کنترل ها و اثر بخشی آنها می باشد. یک رویداد میتواند چندین علت و پیامد داشته باشد و می تواند بر چند هدف تاثیر بگذارد.

تحلیل ریسک میتواند با درجات مختلف جزئیات و پیچیدگی بسته به مقصود تحلیل، در دسترس بودن و قابلیت اعتماد اطلاعات و منابع در دسترس انجام شود. تکنیکهای تحلیل بسته به شرایط و استفاده مورد نظر میتوانند کیفی، کمی یا ترکیبی از این دو باشد.

تحلیل ریسک بایستی عوامل از جمله موارد زیر را مدنظر قرار دهد:

- احتمال رویدادها و پیامدها؛
- ماهیت و بزرگی پیامدها؛
- پیچیدگی و اتصال؛
- عوامل مرتبط با زمان و نوسان؛
- اثر بخشی کنترل های موجود؛
- سطوح حساسیت و اطمینان.

تحلیل ریسک ممکن است تحت تاثیر هرگونه اختلاف در عقاید، تمایلات، برداشتها از ریسک و قضاوت ها قرار گیرد. سایر اثرات کیفیت اطلاعات مورد استفاده، فرضیات و استثنائات، هرگونه محدودیت تکنیکها و چگونگی اجرای آن ها می باشند. این اثرات بایستی مدنظر قرار گرفته، مستند سازی و به تصمیم گیرندگان اطلاع رسانی شوند.

کمی کردن رویدادهای با عدم قطعیت بالا می تواند دشوار باشد. هنگام تحلیل رویدادها با پیامدهای جدی این امر می تواند یک مسئله باشد. در چنین مواردی استفاده ترکیبی از تکنیک ها عموماً بینش گسترده تری را ایجاد می نماید.

تحلیل ریسک یک ورودی به ارزشیابی ریسک در خصوص تصمیماتی در مورد نیاز به مقابله با ریسک و چگونگی مقابله با آن و مناسب ترین روشها و استراتژی مقابله با ریسک ایجاد می نماید. نتایج، بینشی را برای تصمیم گیری در جایی که انتخاب ها صورت می گیرند و گزینه ها شامل انواع مختلف و سطوح ریسک میشوند ایجاد می نمایند.

۶-٤-٤- ارزشیابی ریسک

مقصود ارزشیابی ریسک پشتیبانی از تصمیمات می باشد. ارزشیابی ریسک شامل مقایسه نتایج تحلیل ریسک با معیارهای ریسک ایجاد شده است تا تعیین کند کجا فعالیت بیشتری نیاز می باشد.

این امرمی تواند به تصمیمی در موارد زیر منجر شود:

- اقدام بیشتری صورت نگیرد؛
- گزینه های مقابله با ریسک مد نظر قرار گیرد؛
- تحلیل بیشتری به منظور درک بهتر از ریسک صورت؛
- کنترل های موجود باقی بمانند؛
- اهداف مجدداً بررسی شوند.

تصمیمات بایستی فضای گسترده تر و پیامدهای واقعی و درک شده ای را برای ذی نفعان بیرونی و درونی داشته باشند.

نتایج ارزشیابی ریسک بایستی ثبت اطلاع رسانی و سپس در سطوح مناسبی از سازمان تصدیق شود.

۶-۵- مقابله با ریسک

۶-۵-۱- کلیات

مقصود از مقابله با ریسک انتخاب و پیاده سازی گزینه هایی برای پرداختن به ریسک میباشد. مقابله با ریسک شامل فرآیندی تکرار شونده به صورت زیر می باشد:

- قاعده مند کردن و انتخاب گزینه های مقابله با ریسک؛
- برنامه ریزی و پیاده سازی مقابله با ریسک؛
- ارزیابی اثر بخشی مقابله {انجام شده}؛
- تصمیم گیری {در مورد اینکه} آیا ریسک باقی مانده قابل قبول است؛
- در صورت عدم پذیرش {ریسک باقی مانده}، انجام مقابله بیشتر.

۶-۵-۲- انتخاب گزینه های مقابله با ریسک

انتخاب مناسب ترین گزینه (های) مقابله با ریسک شامل ایجاد توازن بین منافع بالقوه دریافتی برای دستیابی به اهداف در برابر هزینه ها، تلاش ها یا معایب پیاده سازی می باشد.

گزینه های مقابله با ریسک لزوماً در تمام شرایط و به صورت متقابل اختصاصی یا مناسب نمی باشند.

گزینههای مقابله با ریسک ممکن است شامل یک یا بیش از یکی از موارد زیر باشند:

- اجتناب از ریسک با تصمیم به آغاز نکردن یا ادامه ندادن فعالیتی که منجر به ریسک می شود؛
- انجام یا افزایش ریسک به منظور پیگیری یک فرصت؛
- از بین بردن منبع ریسک؛
- تغییر در احتمال؛
- تغییر در پیامدها؛
- به اشتراک گذاشتن ریسک (به طور نمونه از طریق قراردادها، خرید بیمه)؛
- حفظ ریسک از طریق تصمیم آگاهانه.

توجیه مقابله با ریسک گسترده تر از ملاحظات صرفا اقتصادی بوده و بایستی تمامی تعهدات {غیر اختیاری}، تعهدات اختیاری و نظرات ذی نفعان سازمان را لحاظ نماید. انتخاب گزینه های مقابله با ریسک بایستی در

تطابق با اهداف سازمان، معیارهای ریسک و منابع در دسترس انجام شود.

هنگام انتخاب گزینه های مقابلع با ریسک، سازمان بایستی ارزشها، برداشت ها و مشارکت بالقوه ذی نفعان و مناسب ترین روش های اطلاع رسانی و مشاوره با آنها را مد نظر قرار دهد. با وجود اثر بخشی یکسان، برخی از {گزینه های} مقابله های با ریسک می توانند برای ذی نفعان مقبول تر از دیگر {گزینه ها} باشند.

مقابله با ریسک، حتی با وجود طراحی و پیاده سازی با دقت ممکن است نتایج مورد انتظار را ایجاد نکرده و پیامدهای ناخواسته ای را ایجاد نماید. نیاز است که پایش و بازنگری به صورت بخش جدانشدنی از پیاده سازی مقابله با ریسک باشند تا اطمینان دهند که اشکال مختلفی از مقابله موثر بوده و {موثر} می مانند.

مقابله با ریسک همچنین میتوانند ریسک های جدیدی که نیاز به مدیریت دارند ایجاد نماید.

اگر هیچ گزینه در دسترس مقابله وجود نداشته باشد یا گزینه های مقابله به طور کافی ریسک را تعدیل نکنند، ریسک بایستی تحت بازنگری پیوسته ثبت و نگهداری شود.

تصمیم گیرندگان و سایر ذی نفعان بایستی از ماهیت و میزان ریسک باقی مانده پس از مقابله با ریسک آگاه باشند.

ریسک باقی مانده بایستی مستند شده و تحت پایش، بازنگری و در جای مناسب مقابله بیشتر قرار بگیرد.

۶-۵-۳- آماده سازی و پیاده سازی طرح های مقابله با ریسک

مقصود از طرح های مقابله با ریسک، مشخص کردن این امر است که گزینه های منتخب چگونه پیاده سازی خواهند شد، تا ترتیبات توسط افراد درگیر درک شده و پیشرفت مرتبط با طرح پایش شود. طرح مقابله بایستی به روشنی ترتیب پیاده سازی مقابله با ریسک را مشخص نماید.

طرح های مقابله بایستی با مشورت با ذی نفعان مناسب درون طرح های مدیریت و فرآیندهای سازمان یکپارچه شوند.

اطلاعات درج شده در طرحهای مقابله با {ریسک} بایستی شامل موارد زیر باشند:

- منطق انتخاب گزینه های مقابله شامل منافع مورد انتظار که حاصل می شوند؛
- افراد پاسخگو و مسئول تایید و پیاده سازی طرح؛
- فعالیت های پیشنهادی؛
- منابع مورد نیاز شامل موارد اقتضایی؛
- اندازه گیریهای عملکرد؛
- محدودیت ها؛
- گزارش دهی و پایش مورد نیاز؛
- زمانی که انتظار می رود فعالیت ها انجام و کامل شوند.

۶-۶- پایش و بازنگری

مقصود از پایش و بازنگری، حصول اطمینان و بهبود کیفیت و اثر بخشی طراحی، پیاده سازی و نتایج فرآیند

می باشد. پایش پیوسته و بازنگری دوره ای فرآیند مدیریت ریسک و نتایج آن بایستی بخش برنامه ریزی شده ای با مسئولیت های تعیین شده روشن از فرآیند مدیریت ریسک باشد.

پایش و بازنگری بایستی در کلیه مراحل فرآیند انجام شود. پایش و برنامه ریزی شامل برنامه ریزی، جمع آوری و تحلیل اطلاعات، ثبت نتایج و ارائه بازخورد می باشد.

نتایج پایش و بازنگری بایستی در سراسر مدیریت عملکرد، اندازه گیری و فعالیتهای گزارش دهی سازمان گنجانده شود.

۶-۷- ثبت و گزارش دهی

فرآیند مدیریت ریسک و نتایج آن بایستی از طریق ساز و کارهای مناسب مستند و گزارش دهی شود.

اهداف ثبت و گزارش دهی عبارتست از:

- اطلاع رسانی فعالیتها و نتایج مدیریت ریسک در سراسر سازمان؛
- آماده سازی اطلاعات برای تصمیم گیری؛
- بهبود فعالیت های مدیریت ریسک؛
- کمک به تعامل با ذی نفعان، شامل آن هایی که مسئول و پاسخگوی فعالیت های مدیریت ریسک می باشند؛

تصمیمات مرتبط با پدید آوری، حفظ و رسیدگی به اطلاعات مستند بایستی موارد زیر را در نظر گرفته ولی محدود به آنها نشوند: استفاده آن ها، حساسیت اطلاعات و فضای بیرونی و درونی.

گزارش دهی، بخشی جدانشدنی از حاکمیت سازمانی بوده و بایستی کیفیت گفتگو با ذی نفعان را بالا برده و مدیریت ارشد و نهادهای نظارتی را در برآورده سازی مسئولیتهای آنها پشتیبانی نماید.

عواملی که برای گزارش دهی در نظر گرفته می شود شامل موارد زیر بوده، ولی به آن ها محدود نمی شود:

- ذی نفعان مختلف و نیازهای اطلاعاتی خاص و الزامات آنها؛
- هزینه، تواتر و زمان بندی گزارش دهی؛
- روش گزارش دهی؛
- ارتباط اطلاعات با اهداف سازمانی و تصمیم گیری.