استاندارد بین المللی

ویرایش نهایی

IEC/DFIS
31000

مدیریت ریسک ـــــ اصول و خط‌مشی‌ها

شماره منبع

ISO/FDIS 31000:2009(E)

استاندارد بین‌المللی ایزو ۳۱۰۰۰

چاپ اول :۲۵/۸/۱۳۸۸

مدیریت ریسک- اصول و خط‌مشی‌ها

فهرست مطالب:

پیشگفتار

ایزو یا سازمان جهانی استاندارد فدراسیونی متشکل از سازمان‌های استاندارد ملی کشورهای مختلف جهان است. کار تهیه استانداردهای جهانی معمولاً از طریق کمیته‌های فنی ایزو صورت می‌گیرند. کلیه کشورهای عضو که به موضوع کمیته‌های فنی تشکیل شده علاقه‌مند هستند حق معرفی نماینده در آن کمیته‌ها رادارند. سازمان‌های بین المللی، سازمان‌های دولتی و غیردولتی نیز با هماهنگی قبلی با ایزو می‌توانند دراین کمیته‌ها شرکت داشته باشند. سازمان جهانی استاندارد همکاری نزدیکی با کمیسیون جهانی الکتروتکنیکال[1] در کلیه موارد مربوط به استانداردهای الکتروتکنیکال دارد. استانداردهای جهانی براساس قوانین موجود در بحش دوم دستور ایزو و آی ایی سی (IEC) تهیه می‌شوند. وظیفه اصلی کمیته‌های فنی تهیه استانداردهای بین‌المللی است. پیش‌نویس استانداردهای بین‌المللی تهیه شده در این کمیته‌ها برای رای‌گیری بین سازمان‌های استاندارد کشورهای عضو توزیع می‌شوند. انتشار یک استاندارد بین‌المللی منوط به تایید ۷۵درصد اعضای شرکت کننده در رای‌گیری می‌باشد.

توجه: استفاده کنندگان از این استاندارد را به این نکته جلب می‌نماییم که بخش‌هایی از این استاندارد ممکن است تحت پوشش قوانین مربوط به ثبت اختراعات باشد. ایزو مسئولیت شناسایی تمام ویا بخشی از چنین حقوقی را برعهده نمی گیرد.

ایزو۳۱۰۰۰ توسط گروه کاری هیات مدیریت فنی در زمینه مدیریت ریسک تهیه گردیده است.

مقدمه

سازمان‌ها در اندازه‌های مختلف با عوامل و تاثیر گذارنده‌های درونی و بیرونی مواجه می‌شوند که دستیابی به اهداف و مقاصدشان را بطور کلی و یا از نظر زمانی مورد تردید و عدم‌اطمینان قرار می‌دهند.اثری که این عدم‌اطمینان بر اهداف ومقاصد یک سازمان دارد ریسک نامیده می‌شود.

همه فعالیت‌های یک سازمان در بردارنده ریسک است. سازمان‌ها ریسک را از طریق شناسایی، تحلیل و ارزیابی اینکه آیا باید با آن با استفاده از روش‌های مقابله برخورد شود یا نه مدیریت می‌کنند. درطول این فرایند، سازمان‌ها با گروه‌های ذینفع مشاوره و ارتباط برقرار کرده و ریسک و کنترل‌هایی که برای مهار و مقابله با آن اتخاذ کرده را مورد نظارت و بررسی قرار داده تا اطمینان یابند که روش‌های بیشتری برای مهار و مقابله با ریسک مورد نیاز نمی‌باشند. این استاندارد بین‌المللی این فرایند سیستماتیک و منطقی را به تفصیل توضیح می‌دهد.

در عین حال که کلیه سازمان‌ها ریسک را تا درجاتی مدیریت می‌کنند، استاندارد ایزو۳۱۰۰۰ اصلی را پایه‌ریزی می‌کند که برای رسیدن به یک مدیریت ریسک کارا باید مورد توجه قرار گیرند. این استاندارد بین‌المللی پیشنهاد می‌کند که سازمان‌ها چهارچوبی را تهیه، اجرا ودائماً بهبود دهند که هدفش یکپارچه کردن فرایند مدیریت ریسک در فرایندهای اداره، استراتژی وبرنامه‌ریزی، مدیریت و گزارش‌دهی، سیاست‌ها، ارزش‌ها و فرهنگ آن سازمان باشد.

[1] International Electrotechnical Commission-IEC

مدیریت ریسک می‌تواند در مورد تمامی یک سازمان، کلیه محدوده‌ها وسطوح آن، در هر زمانی و یا در مورد کارکردها، پروژه‌ها و یا فعالیت‌های خاصی بکار گرفته شود.

اگرچه عمل مدیریت ریسک در طول زمان و در بخش‌های مختلف به منظور رفع نیازهای گوناگونی شکل گرفته است ولی بکارگیری فرایندهای سازگار در چهارچوبی جامع می‌تواند به مدیریت کارا وهماهنگ ریسک در تمامی یک سازمان کمک نماید. روش کلی ارائه شده دراین استاندارد بین‌المللی اصول و خط‌مشی‌های مدیریت انواع ریسک‌ها به شیوه‌ای نظام‌مند، شفاف و معتبر در هر شرایط و محیطی می‌باشد.

هر بخش و یا کاربرد خاص چهارچوب مدیریت ریسک با خود نیازهای فردی، مخاطبان، برداشت‌ها و معیارهای مخصوص را به همراه می‌آورد. بنابراین، ویژگی کلیدی این استاندارد بین‌المللی وارد کردن بحث ایجاد زمینه و شرایط مدیریت ریسک به عنوان یک فعالیت از همان ابتدای کار است. ایجاد زمینه و شرایط در بر گیرنده اهداف ومقاصد سازمان، محیطی که درآن این اهداف دنبال می‌شوند، گروه‌های ذینفع وتنوع معیارهای ریسک است که همه آنها کمک می‌کنند تا ماهیت وپیچیدگی ریسک آشکار و ارزیابی شود.

رابطه بین اصول مدیریت ریسک، چهارچوبی که این کار در آن صورت می‌گیرد و فرایند مدیریت ریسک در این استاندارد بین‌المللی درنمودارشماره ۱ نشان داده شده است.

زمانیکه مدیریت ریسک مطابق با این استاندارد تهیه ونگهداری شود، سازمان قادر خواهد بود تا به عنوان مثال:

- احتمال دستیابی به اهداف و مقاصدش را افزایش دهد؛
- مدیریت فعالانه راتشویق نماید؛
- از نیاز به شناسایی و مقابله با ریسک در سراسر سازمان آگاه باشد؛
- شناسایی فرصت‌ها وتهدیدات رابهبود بخشد؛
- با پیش نیازهای قانونی ومقرراتی مربوطه و رویه‌های معمول جهانی هم سو و هماهنگ باشد؛
- گزارش‌دهی اجباری و یا داوطلبانه رابهبود دهد؛
- اداره سازمان را تقویت بخشد؛
- اعتماد واطمینان گروه‌های ذینفع رابالا ببرد؛
- پایه و اساسی قابل اتکا برای تصمیم‌گیری وبرنامه‌ریزی ایجاد نماید؛
- کنترل‌ها را بهبود بخشد؛
- منابع را به شکلی کارا برای مقابله با ریسک تخصیص ومورد استفاده قرار دهد؛
- کارایی وبهره‌وری عملیاتی را افزایش دهد؛
- عملکرد سازمان در زمینه ایمنی و بهداشت و مراقبت‌های محیطی را تقویت کند؛
- پیشگیری از زیان‌ها ومدیریت سانحه را بهبود بخشد؛
- زیان‌ها را به حداقل برساند؛
- یادگیری سازمانی را تقویت کند؛

- تاب‌آوری سازمانی[1] را افزایش دهد.

انتظار می‌رود که این استاندارد بین‌المللی نیازهای تعداد زیادی از گروه‌های ذینفع از جمله موارد زیر را برآورده سازد:

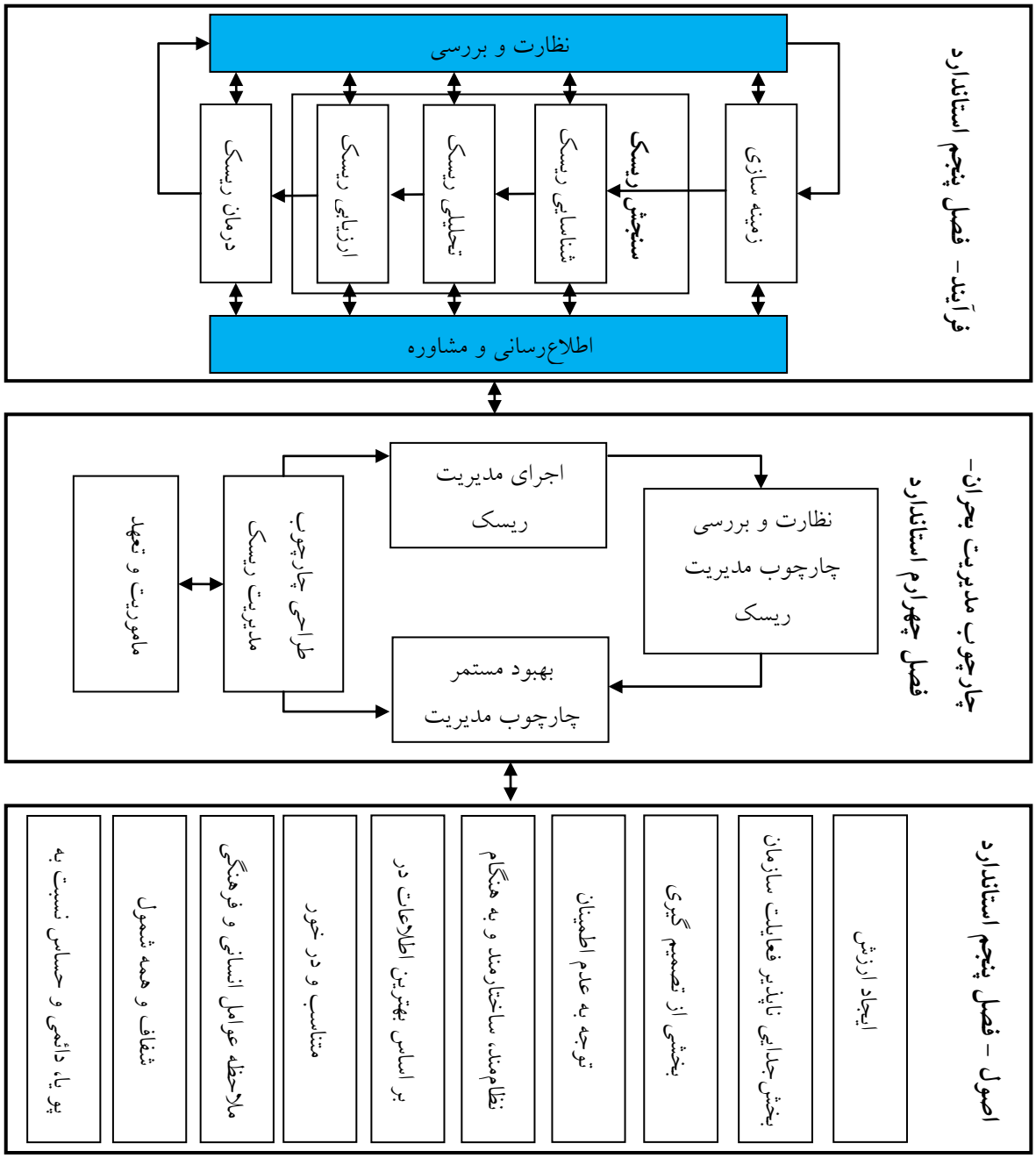
الف) کسانی که مسئولیت تهیه سیاست مدیریت ریسک در سازمان‌هایشان رابرعهده دارند؛

ب) کسانیکه باید در برابر مدیریت کارای ریسک در کل سازمان و یا در محدوده، پروژه ویافعالیت خاصی پاسخگو باشند؛

ج) آنهایی که باید کارایی سازمان در زمینه مدیریت ریسک را ارزیابی کنند؛

د) تهیه‌کنندگان استانداردها، دستورالعمل‌ها، خط‌مشی‌ها و کدهای عملی اعم از کلی و یا جزیی که به دنبال ارائه نحوه مدیریت ریسک در بخشهای خاصی از این اسناد می‌باشند.

[1] Organizational resilience



نمودار شماره ۱. اجزا و عناصر مدیریت ریسک در ایزو ۳۱۰۰۰

فرایندها و عملکردهای رایج مدیریتی بسیاری از سازمان‌ها دربردارنده ابعاد و عناصری از مدیریت ریسک می‌باشند و بسیاری از آنها ممکن است از مدت‌ها قبل فرایندهای مدیریت ریسک را برای تمام ویا بخش‌های خاصی از فعالیت‌هایشان و یا انواع خاصی از ریسک‌ها تهیه واجرا کرده باشند. در این موارد، سازمان‌ها می‌توانند با استفاده از این استاندارد بین‌المللی به ارزیابی انتقادی فرایندها وعملکردهای خود بپردازند.

دراین استاندارد بین‌المللی عبارتهای "مدیریت ریسک[1]" و "مدیریت کردن ریسک[2]" هردومورد استفاده قرار می‌گیرند. بطورکلی مدیریت ریسک به معماری (اصول،چهارچوب وفرایند) مدیریت کارای ریسک مربوط می‌شود در حالیکه مدیریت کردن ریسک به اجرای آن معماری درمورد یک ریسک خاص اطلاق می‌شود.

مدیریت ریسک: اصول وخط‌مشی ها

۱. محدوده

استاندارد ایزو ۳۱۰۰۰ اصول وخط‌مشی‌های کلی مدیریت ریسک را ارائه می‌کند. این استاندارد بین‌المللی می‌تواند توسط کلیه سازمان‌های عمومی، خصوصی ویا اجتماعی، انجمن، گروه و یا فرد مورد استفاده قرار گیرد. بنابراین، این استاندارد بین‌المللی منحصر به یک فعالیت و یا بخش خاصی نیست.

نوجه کنید که برای ساده شدن کار، برای کلیه استفاده‌کنندگان از این استاندارد عنوان سازمان بکار برده می‌شود.

این استاندارد بین‌المللی می‌تواند در طول عمر یک سازمان و در مورد طیف وسیعی از فعالیت‌ها از جمله استراتژی‌ها و تصمیمات، عملیات، فرایندها، وظایف، پروژه‌ها، محصولات، خدمات و دارایی‌های یک سازمان بکار گرفته شود.

این استاندارد بین‌المللی می‌تواند در مورد انواع گوناگون ریسک‌ها، با هر ماهیت واثراتی اعم از مثبت و یا منفی بکار گرفته شود.

اگرچه این استاندارد بین‌المللی خط‌مشی‌های کلی را ارائه می‌کند، ولی هدف آن یکسان‌سازی مدیریت ریسک در همه سازمان‌ها نیست. طراحی وپیاده‌سازی برنامه‌های مدیریت ریسک وچهارچوب‌های آن باید براساس نیازها وشرایط خاص هرسازمان و یا اجتماع از نظر عملکردی، مالی، عملیاتی، پروژه‌ای، ساختاری، محتوایی و اهداف و مقاصد مورد نظر باشد.

هدف این استاندارد هماهنگ کردن فرایندهای مدیریت ریسک در استانداردهای جهانی موجود و آتی می‌باشد. این استاندارد روش مشترکی را در کمک به استانداردهایی که با ریسک‌ها یا بخش‌های خاصی سروکار دارند فراهم می‌نماید ولی جایگزین آنها نمی‌شود.

این استاندارد بین‌المللی به منظور ارائه گواهینامه[3] تهیه نشده است.

۲. اطلاحات وتعاریف

برای اهداف موردنظر این استاندارد، اصطلاحات و تعاریف زیربکار گرفته می‌شوند.

.۲.۱

[1] Risk Management
[2] Managing Risk
[3] Certifaication

ریسک[1]

تاثیر عدم‌اطمینان[2] بر اهداف[3]

نکته ۱، منظور از تاثیر فاصله گرفتن از اهداف است – مثبت یا منفی

نکته ۲، اهداف جنبه‌های گوناگونی می‌توانند داشته باشند (مانند مالی، بهداشتی، ایمنی و محیطی) و می‌توانند در سطوح مختلف اعمال گردند (مانند سطوح استراتژیک، کل سازمان، محصول و فرایند).

نکته ۳، ریسک اغلب بامراجعه به حوادث بالقوه (۲.۱۷) و پیامدها (۲.۱۸) و یا ترکیبی از این دو تبیین می‌شود.

نکته ۴،ریسک اغلب به صورت ترکیبی از پیامدهای حادثه (شامل تغییر در شرایط) واحتمال وقوع (۲.۱۹) آن حادثه بیان می‌شود.

نکته ۵،عدم‌اطمینان حالتی است که در آن کمبود اطلاعات، هرچندجزئی، درزمینه فهم و یا آگاهی از یک حادثه، پیامدها و یا احتمال وقوع آن وجود داشته باشد.

(راهنمای شماره۷۳ ایزو، تعریف شماره ۱.۱)

۲.۲

مدیریت ریسک[4]

فعالیت‌های هماهنگی که برای هدایت و کنترل سازمان در ارتباط با ریسک بکار گرفته می‌شوند.

(راهنمای شماره ۷۳ ایزو، تعریف شماره ۲.۱)

۲.۳

چهارچوب مدیریت ریسک[5]

مجموعه‌ای از اجزا که زیربناها وترتیبات سازمانی برای طراحی، اجرا، نظارت(۲.۲۸)، بررسی و بهبود مستمر مدیریت ریسک(۲.۲) درتمامی سازمان را فراهم می‌آورند.

نکته ۱،زیربناها شامل سیاست، اهدا، ماموریت‌ها، وتعهدات لازم برای مدیریت کردن ریسک(۲.۱) می‌باشند.

نکته ۲،ترتیبات سازمانی شامل برنامه‌ها، روابط، مسئولیت‌پذیری و پاسخگویی[6]، منابع، فرایندها وفعالیت‌ها می‌شوند.

نکته ۳، چهارچوب مدیریت ریسک در درون استراتژی‌ها، سیاست‌ها ورویه‌های کلی سازمان قراردارد.

(راهنمای شماره ۷۳ ایزو، تعریف شماره ۲.۱.۱)

۲.۴

---

[1] Risk
[2] Uncertainty
[3] Objective
[4] Risk Management
[5] Risk management framework
[6] Accountabilities

سیاست مدیریت ریسک[1]

عبارت و یا سندی که نیت و جهت‌گیری کلی سازمان در رابطه با مدیریت ریسک منعکس می‌کند(۲.۲)

(راهنمای شماره ۷۳ ایزو، تعریف شماره ۲.۱.۲)

۲.۵

طرز برخورد با ریسک[2]

روش سازمان برای ارزیابی و در نهایت پیگیری، مراقبت، قبول و یا پرهیز از ریسک

(راهنمای شماره۷۳ ایزو،تعریف شماره ۳.۷.۱.۱)

۲.۶

برنامه مدیریت ریسک[3]

طرحی در درون چهارچوب مدیریت ریسک(۲.۳)که روش، اجزا مدیریت و منابع مورد استفاده در مدیریت کردن ریسک(۲.۱)را مشخص می‌کند.

نکته ۱، اجزا مدیریت بطور معمول شامل رویه‌ها، کارها، تقسیم کارها، زمان‌بندی وسلسله مراتب امور می‌شود.

نکته ۲، برنامه مدیریت می‌تواند درمورد یک محصول خاص، فرایند یا پروژه، تمام و یا بخشی از سازمان اعمال می‌شود.

(راهنمای شماره ۷۳ ایزو،تعریف شماره ۲.۱.۳)

۲.۷

مالک (صاحب) ریسک[4]

فرد یا نهادی که مسئولیت واختیارات مدیریت ریسک(۲.۱)رابرعهده دارد.

(راهنمای شماره ۷۳ ایزو،تعریف شماره ۳.۵.۱.۵)

۲.۸

فرایند مدیریت ریسک[5]

کاربرد سیستماتیک سیاست‌ها، اقدامات و فعالیت‌های مدیریتی در زمینه‌های ارتباطی، مشاوره‌ای، زمینه‌سازی و شناسایی، تحلیل، ارزیابی، مقابله، نظارت(۲.۲۸) و بررسی ریسک(۲.۱)

(راهنمای شماره ۷۳ ایزو، تعریف شماره۳.۱)

۲.۹

زمینه‌سازی[1]

---

[1] Risk management policy
[2] Risk attitude
[3] Risk management plan
[4] Risk owner
[5] Risk management process

شناخت وتعریف پارامترهای درونی و بیرونی که سازمان باید برای مدیریت ریسک، تعیین حدود و ثغور و معیارهای ریسک (۲.۲۲) و سیاست مدیریت ریسک (۲.۴) درنظر گیرد.

(راهنمای شماره ۷۳ ایزو،تعریف شماره ۳.۳.۱)

۲.۱۰

زمینه بیرونی[۲]

محیط بیرونی که سازمان درآن به دنبال رسیدن به اهدافش می‌باشد.

نکته، زمینه بیرونی شامل موارد زیر می‌شود:

- ✓ محیط فرهنگی، اجتماعی، سیاسی، قانونی، مقرراتی، مالی، فنی، اقتصادی، طبیعی و رقابتی؛
- ✓ روندها ومحرکه‌هایی که براهداف سازمان تاثیر گذارند؛
- ✓ روابط با گروه‌های ذینفع بیرونی(۲.۱۳) و دیدگاه‌ها وارزش‌های آنها

۲.۱۱

زمینه درونی[۳]

محیط درونی که سازمان در آن به دنبال رسیدن به اهدافش می‌باشد.

نکته، زمینه درونی شامل موارد زیر می‌شود:

- اداره، ساختارسازمانی، وظایف ومسئولیت‌ها؛
- سیاست‌ها، اهداف و استراتژی‌های موجود برای رسیدن به آنها؛
- توانایی‌ها، برحسب منابع، دانش وآگاهی(مانند سرمایه، وقت، مردم، فرایندها، سیستم‌ها وتکنولوژی)
- سیستم‌های اطلاعاتی، جریان اطلاعات، فرایندهای تصمیم‌گیری مربوطه (رسمی وغیررسمی)؛
- درک وبرداشت وارزش‌های گروه‌های ذینفع درونی و روابط با آنها؛
- فرهنگ سازمان؛
- استانداردها، راهنماها و مدل‌های بکارگرفته شده توسط سازمان.

۲.۱۲

ارتباطات ومشاوره[۴]

فرایندهای مستمر ودائمی که یک سازمان برای تهیه، توزیع و دستیابی به اطلاعات و وارد شدن به گفتگو با طرفهای ذینفع(۲.۱۳) در ارتباط با مدیریت ریسک(۲.۱) بکار می‌گیرد.

نکته ۱، اطلاعات می‌تواند در مورد وجود، ماهیت، شکل، احتمال[۵](۲.۱۹)، بزرگی، ارزیابی، قابل قبول بودن ونحوه مهار و درمان ریسک در مدیریت ریسک باشد.

---

[1] Establishing the context
[2] External context
[3] Internal context
[4] Communication and consultation
[5] Likelihood

نکته ۲، مشاوره فرایندی دوطرفه از برقراری ارتباط همراه با تبادل اطلاعات بین سازمان وطرف‌های ذینفع در هر زمینه پیش از تصمیم‌گیری و یا جهت‌گیری در آن زمینه می‌باشد.

مشاوره عبارت است از:

- فرایندی که بر تصمیم‌گیری از طریق تاثیرگذاری[1] ونه اعمال قدرت اثر می‌گذارد؛
- داده‌ای که برای تصمیم‌گیری و نه تصمیم‌گیری مشترک بکار گرفته می‌شود.

(راهنمای شماره ۷۳ ایزو، تعریف شماره ۳.۲.۱.)

۲.۱۳

ذینفع[2]

فرد و یا سازمانی که می‌تواند بر یک تصمیم و یا فعالیت اثر گذاشته، از آن متاثر شده و یا تصور متاثرشدن از آن را داشته باشد.

نکته، تصمیم‌گیرنده می‌تواند ذینفع هم باشد.

(راهنمای شماره ۷۳ ایزو، تعریف شماره ۳.۲.۱.۱.)

۲.۱۴

سنجش ریسک[3]

فرایند کلی شناسایی ریسک[4](۲.۱۵)، تحلیل ریسک[5](۲.۲۱) وارزیابی ریسک[6].

(راهنمای شماره ۷۳ ایزو، تعریف شماره۳.۴.۱)

۲.۱۵

شناسایی ریسک

فرایند پیداکردن، تشخیص دادن و تشریح ریسک.

نکته ۱، شناسایی ریسک شامل تعیین منابع ریسک[7](۲.۱۶)، سوانح(۲.۱۷) و علل و پیامدهای (۲.۱۸) بالقوه آنها می‌باشد.

نکته ۲، شناسایی ریسک می‌تواند از طریق داده‌های تاریخی تحلیل‌های نظری، نظرات کارشناسان و افراد مطلع و نیازهای افراد ذینفع صورت گیرد.

(راهنمای شماره ۷۳ ایزو،تعریف شماره ۳.۵.۱)

۲.۱۶

منبع ریسک[1]

---

[1] Influence
[2] Stakeholders
[3] Risk assessment
[4] Risk Identification
[5] Risk analysis
[6] Risk evaluation
[7] Risk sources

عنصری که به تنهایی و یا با ترکیبی از عناصر دیگر دارای پتانسیل ذاتی در بروز وظهور ریسک باشد.

نکته، منبع ریسک می‌تواند ملموس و یا ناملموس باشد.

(راهنمای شماره ۷۳ ایزو،تعریف شماره ۳.۵.۱.۲)

۲.۱۷

حادثه[۲]

وقوع و یا تغییر مجموعه مشخصی از شرایط و وضعیت‌ها.

نکته ۱، حادثه می‌تواند شامل یک ویا چند رویداد باشد و همچنین می‌تواند دلایل متعددی داشته باشد.

نکته ۲، حادثه می‌تواند شامل چیزی باشد که اتفاق نیفتد.

نکته ۳، حادثه گاهی اوقات ممکن است به عنوان سانحه ویا تصادف نیز مورد اشاره قرار گیرد.

نکته ۴، یک حادثه بدون پیامدها(۲.۱۸) را می‌توان به عنوان "حادثه عقیم" و یا سانحه و یا "نزدیک به سانحه" نام برد.

(راهنمای شماره ۷۳ ایزو، تعریف شماره ۳.۵.۱.۳)

۲.۱۸

پیامدها[۳]

نتایج وخروجی‌های یک حادثه (۲.۱۷) که بر اهداف اثر گذارند.

نکته ۱، حادثه می‌تواند منجر به دامنه وسیعی از پیامدها شود.

نکته ۲، پیامد می‌تواند قطعی و یا غیرطبیعی باشد و می‌تواند تاثیرات مثبت و یا منفی بر اهداف داشته باشد.

نکته ۳، عواقب می‌توانند به صورت کمی و یا کیفی بیان شوند.

نکته ۴، پیامدهای اولیه می‌توانند از طریق اثرات بعدی گسترش یابند.

(راهنمای شماره ۷۳ ایزو،تعریف شماره۳.۶.۱.۳)

۲.۱۹

احتمال وقوع[۴]

شانس وقوع چیزی

نکته ۱، در واژه شناسی مدیریت ریسک، لغت "احتمال وقوع" برای بیان شانس وقوع چیزی بکار گرفته می‌شود، اعم از آنکه به صورت عینی ویا ذهنی تعریف، اندازه گیری ویا تعیین شود ویا به صورتی کلی و یا ریاضی توصیف شود (مانند احتمال و یا فراوانی در دوره زمانی معین)

نکته ۲، واژه احتمال وقوع معادل مشابه مستقیمی در برخی زبان‌ها ندارد و بنابراین از واژه احتمال آماری[۱] به جای آن استفاده می‌شود. در زبان انگلیسی واژه احتمال آماری اغلب به صورت ریاضی بیان می‌شود. بنابراین، در

---

[1] Risk source
[2] Event
[3] Consequences
[4] Likelihood

واژه شناسی مدیریت ریسک"احتمال وقوع" با این نیت بکار گرفته می‌شود که همان معنای احتمال آماری در سایر زبان‌ها بجز انگلیسی را دارد.

(راهنمای شماره ۷۳ ایزو، تعریف شماره ۳.۶.۱.۱)

۲.۲۰

پروفیل ریسک[۲]

تشریح و توصیف مجموعه‌ای از ریسک‌ها.

نکته، مجموعه ریسک‌ها می‌توانند شامل آنهایی که به کل سازمان، بخشی از سازمان وغیره مرتبط می‌شوند باشد.

(راهنمای شماره ۷۳ ایزو،تعریف شماره ۳.۸.۲.۵)

۲.۲۱

تحلیل ریسک[۳]

فرایند شناخت ماهیت ریسک(۲.۱) وتعیین سطح ریسک[۴] (۲.۲۳)

نکته ۱، تحلیل ریسک پایه واساس ارزیابی ریسک (۲.۲۴) وتصمیم‌گیری در زمینه مقابله ودرمان ریسک[۵] (۲.۲۳) را تشکیل می‌دهد.

نکته ۲، تحلیل ریسک شامل تخمین ریسک می‌شود.

(راهنمای شماره ۷۳ ایزو،تعریف شماره ۳.۸.۲.۵)

۲.۲۲

معیارهای ریسک[۶]

معیارها ونقاط مبنایی که اندازه واهمیت ریسک (۲.۱) درمقایسه با آنها سنجیده می‌شود.

نکته ۱، معیارهای ریسک بر مبنای اهداف سازمان و زمینه‌های درونی و بیرونی بنا نهاده می‌شوند.

نکته ۲، معیارهای ریسک می‌توانند از استانداردها، قوانین، سیاست‌ها وسایر الزامات اتخاذ شوند.

(راهنمای شماره ۷۳ ایزو،تعریف شماره ۳.۳.۱.۳)

۲.۲۳

سطح ریسک

اندازه ریسک(۲.۱) یا ترکیبی از ریسک‌ها که به صورت ترکیبی از پیامدها (۲.۱۸) واحتمال (۲.۱۹) وقوع آنها بیان می‌شوند.

---

[1] Probability
[2] Risk profile
[3] Risk analysis
[4] Risk level
[5] Risk treatment
[6] Risk criteria

(راهنمای شماره ۷۳ ایزو،تعریف شماره ۳.۶.۱.۸)

۲.۲۴

ارزیابی ریسک[1]

فرایند مقایسه نتایج سنجش ریسک(۲.۱) با معیارهای ریسک (۲.۲۲) برای تعیین قابل قبول بودن و یا نبودن ریسک.

نکته ارزیابی ریسک به تصمیم‌گیری در مورد نحوه مقابله و برخورد با ریسک (۲.۲۵) کمک می‌کند.

(راهنمای شماره ۷۳ ایزو،تعریف شماره ۳.۷.۱)

۲.۲۵

درمان ریسک

فرایند اصلاح[2] ریسک (۲.۱)

نکته ۱، مقابله و درمان شامل موارد زیر می‌باشد:

- اجتناب از ریسک از طریق تصمیم به شروع نکردن و یا ادامه ندادن فعالیتی که باعث ظهور ریسک می‌شود؛
- قبول و یا افزایش ریسک به منظور دستیابی به یک فرصت؛
- حذف و از بین بردن منبع ریسک(۲.۱۶)؛
- تغییر احتمال (۲.۱۹)؛
- تغییر پیامدها (۲.۱۸)؛
- تقسیم ریسک با گروه ویا گروه‌های دیگر (شامل قراردادها وتامین مالی ریسک)؛

و

- نگهداری ریسک از طریق تصمیم‌گیری آگاهانه.

نکته ۲، روش‌های مقابله با ریسک که با پیامدهای منفی سروکار دارند برخی اوقات به عنوان روش‌های "کاهش اثرات ریسک[3]"، روش‌های "پیشگیری ریسک[4]" و یا روش‌های "کاهش ریسک[5]" شناخته می‌شوند.

نکته ۳ ، روش‌های مقابله با ریسک ممکن است ریسک‌های جدیدی ایجاد کرده ویا ریسک‌های موجود را اصلاح نمایند.

(راهنمای شماره ۷۳ ایزو،تعریف شماره ۳.۸.۱)

۲.۲۶

کنترل[6]

---

[1] Risk evaluation
[2] Modify
[3] Risk mitigation
[4] Risk prevention
[5] Risk reduction
[6] Controls

روش و یا اقدامی که ریسک (۲.۱) را اصلاح می‌کند.

نکته ۱، کنترل‌ها شامل هر فرایند، سیاست، ابزار، اقدام و یا سایر اعمالی که ریسک را اصلاح می‌کند می‌شوند.

نکته، کنترل‌ها همیشه دارای اثرات اصلاحی مورد نظر و یا پیش‌بینی شده بر ریسک نیستند.

(راهنمای شماره ۷۳ ایزو، تعریف شماره ۳.۸.۱.۱)

۲.۲۷

ریسک باقیمانده[1]

مقدار ریسکی که بعد از اعمال روش‌های مقابله ودرمان ریسک (۲.۲۵) باقی می‌ماند.

نکته ۱، ریسک باقیمانده ممکن است شامل ریسک‌های شناسایی نشده نیز باشند.

نکته ۲، ریسک باقیمانده می‌تواند شامل ریسک نگهداری شده[2] هم بشود.

(راهنمای شماره ۷۳ ایزو،تعریف شماره ۳.۸.۱.۶)

۲.۲۸

نظارت[3]

چک کردن مستمر ودائمی، نظارت، مشاهده نقادانه و تعیین وضعیت به منظور شناسایی هر گونه تغییر جهت از سطح عملکرد مطلوب یا مورد انتظار.

نکته، نظارت می‌تواند در مورد چهارچوب مدیریت ریسک (۲.۳) فرایند مدیریت ریسک (۲.۸) ریسک (۲.۱) ویا کنترل (۲.۲۶) بکار گرفته شود.

(راهنمای شماره ۷۳ ایزو،تعریف شماره ۳.۸.۲.۱)

۲.۲۹

بررسی[4]

فعالیتی که به منظور تعیین مناسب بودن، درست بودن وکارایی موضوع مورد نظر برای تحقق اهداف تعیین شده بکار گرفته می‌شود.

نکته، بررسی می‌تواند در مورد چهار چوب مدیریت ریسک (۲.۳) فرایند مدیریت ریسک (۲.۸) وریسک (۲.۱) بکار برده شود.

(راهنمای شماره ۷۳ ایزو،تعریف شماره ۳.۸.۲.۲)

۳.اصول

برای اینکه مدیریت ریسک مؤثر باشد، سازمان باید در هر سطحی اصول زیر را مراعات کند.

---

[1] Residual risk
[2] Retained risk
[3] Monitoring
[4] Review

الف) مدیریت ریسک ایجاد ارزش کرده و از آن حفاظت می‌کند.

مدیریت ریسک به دستیابی رضایت بخش سازمان به اهداف و بهبود کارایی، به عنوان مثال سلامت و بهداشت انسانی، امنیت، رعایت قوانین و مقررات، مقبولیت عمومی، حفاظت محیطی، کیفیت تولید، مدیریت پروژه، کارایی عملیاتی واعتبار کمک می‌کند.

ب) مدیریت ریسک بخشی جدایی‌ناپذیر از کلیه فرایندهای سازمان است.

مدیریت ریسک فعالیتی مستقل وجدای از فعالیت‌ها وفرایندهای اصلی سازمان نیست.

مدیریت ریسک بخشی از مسئولیت‌های مدیریت بوده و بخشی جدایی ناپذیر از فرایندهای سازمان مانند برنامه ریزی استراتژیک، مدیریت پروژه وتغییر می‌باشد.

پ) مدیریت ریسک بخشی از تصمیم‌گیری است.

مدیریت ریسک به تصمیم‌گیران کمک می‌کند تا تصمیماتی همراه با اطلاع و آگاهی گرفته، اقدامات را اولویت بندی کرده واقدام مناسب را از بین آنها انتخاب نمایند.

ت) مدیریت ریسک به روشنی عدم‌اطمینان را مورد توجه قرار می‌دهد.

مدیریت ریسک به وضوح عدم‌اطمینان، ماهیت آن و نحوه برخورد با آن را مورد توجه قرار می‌دهد.

ث) مدیریت ریسک نظام مند، ساختارمند وبه هنگام است.

روش نظام مند، به هنگام وساختارمند در مدیریت ریسک به کارایی ودستیابی به نتایج سازگار، قابل مقایسه ونتایج قابل اعتماد کمک می‌کند.

ج) مدیریت ریسک براساس بهترین اطلاعات در دسترس انجام می‌شود.

داده‌های فرایند مدیریت ریسک براساس منابع اطلاعاتی نظیر داده‌های تاریخی، تجربیات، نظرات گروه‌های ذینفع، مشاهدات، پیش‌بینی‌ها و قضاوت‌های کارشناسان می‌باشند. هرچند، تصمیم‌گیران خودشان باید هرگونه محدودیت در اطلاعات و داده‌ها، مدل‌سازی‌ها و یا احتمال اختلاف نظر بین کارشناسان را مورد توجه قرار دهند.

چ) مدیریت ریسک متناسب با شرایط سازمان است.[1]

مدیریت ریسک با زمینه‌ها و شرایط داخلی و خارجی سازمان هماهنگ ومتناسب می‌باشد.

ح) مدیریت ریسک عوامل انسانی وفرهنگی را در نظر می‌گیرد.

مدیریت ریسک ظرفیت‌ها، برداشت‌ها ونیات افراد درونی و بیرونی که می‌توانند تسهیل‌کننده و یا مانع سازمان در تحقق اهدافش باشند را مورد توجه قرار می‌دهد.

خ) مدیریت ریسک شفاف وهمه شمول[2] است.

مشارکت ودخالت دادن به هنگام و مناسب گروه‌ها و افراد ذینفع و بخصوص تصمیم‌گیران در کلیه سطوح سازمان، اطمینان می‌دهد که مدیریت ریسک همچنان مربوط و به روز باقی بماند. مشارکت دادن همچنین به گروه‌های ذینفع امکان حضور و ارائه نقطه نظراتشان برای تعیین معیارهای ریسک را می‌دهد.

د) مدیریت ریسک پویا، دائمی و حساس نسبت به تغییر و تحولات است.

---

[1] Risk management is tailored.

[2] Inclusive

مدیریت ریسک به طور دائمی تغییر و تحولات را ملاحظه و نسبت به آنها واکنش نشان می‌دهد. همزمان با وقوع حوادث درونی وبیرونی، تغییر وضعیت و اطلاعات، انجام نظارت وبررسی ریسک‌ها، ریسک‌های جدیدی پیدا،ریسک‌های موجود تغییر و برخی از آنها از بین می‌روند.

ذ) مدیریت ریسک پیشرفت دائمی ومستمر سازمان را تسهیل می‌کند.

سازمان‌ها باید استراتژی‌هایی را برای بهبود وبلوغ مدیریت ریسک‌شان در کنار سایر جنبه‌ها مورد توجه قرار دهند.

ضمیمه الف توصیه‌های بیشتری را برای سازمان‌هایی که علاقه‌مند به مدیریت کاراتر ریسک هستند ارائه می‌کند.

۴.چهارچوب

۴.۱ کلیات

موفقیت مدیریت ریسک به کارایی چهارچوب مدیریتی که زیربناها و ترتیبات آن را در کلیه سطوح سازمان فراهم می‌کند بستگی دارد. این چهارچوب به مدیریت کارای ریسک از طریق بکارگیری فرایند مدیریت ریسک (به فصل ۵مراجعه شود) در سطوح مختلف و در زمینه‌ها و شرایط خاص سازمان کمک می‌کند. این چهارچوب اطمینان می‌دهد که اطلاعات ریسک که از فرایند مدیریت ریسک استخراج شده‌اند به درستی گزارش شده و در تصمیم‌گیری و پاسخگویی مورد استفاده قرار گیرند. این بخش اجزای مهم چهارچوب مدیریت ریسک و نحوه ارتباط متقابل آنها با یکدیگر آنگونه که در نمودار شماره ۲ ارائه شده است را توضیح می‌دهد.

این چهار چوب به دنبال ارائه یک نسخه واحد برای سیستم مدیریتی نیست، بلکه به دنبال کمک به سازمان‌ها برای ادغام مدیریت ریسک در سیستم کلی مدیریتی‌شان است. بنابراین، سازمان‌ها باید اجزا این چهارچوب را متناسب با نیازهای خاص خودشان تطبیق دهند. اگر روش‌ها و فرایندهای فعلی مدیریت در یک سازمان دارای عناصری از مدیریت ریسک می‌باشد و یا سازمان از قبل و به طور رسمی فرایند مدیریت ریسک را برای ریسک‌ها و یا وضعیت‌های خاصی اجرا کرده است، باید آنها را بطور نقادانه و با استفاده از این استاندارد بین‌المللی و ویژگی‌های ذکر شده در ضمیمه الف مورد بررسی قرار داده و کارایی و مناسب بودن آنها را ارزیابی کند.

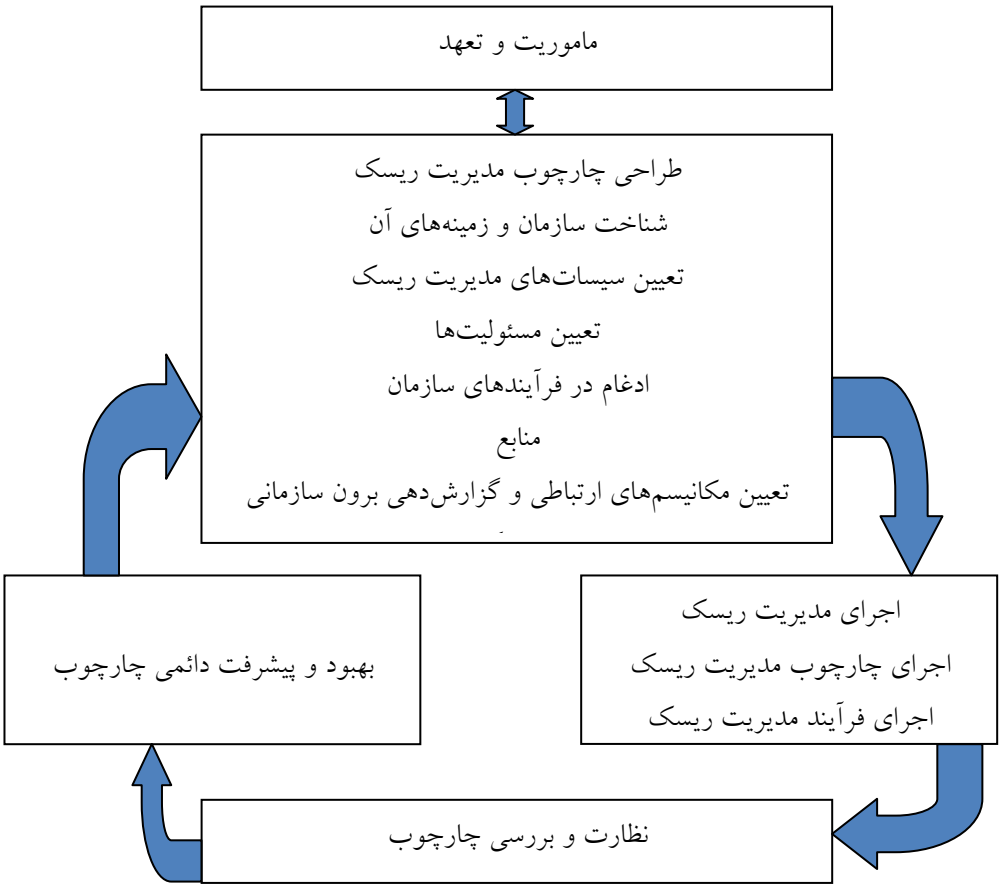
۴.۲. ماموریت وتعهد[1]

ایجاد مدیریت ریسک و اطمینان دادن از مؤثربودن دائمی آن نیازمند تعهد قوی و پایدار مدیریت سازمان وهمچنین برنامه‌ریزی دقیق و استراتژیک برای اجرای این تعهدات در کلیه سطوح دارد. مدیریت باید:

- سیاست مدیریت ریسک را تصویب و تایید نماید؛
- اطمینان به اجرای قوانین و مقررات دهد؛

[1] Mandate and commitment

- شاخص‌های اندازه‌گیری عملکرد مدیریت ریسک که هماهنگ با شاخص‌های اندازه‌گیری عملکرد در سازمان هستند را تعیین نماید؛
- اهداف مدیریت ریسک را با اهداف و استراتژی‌های سازمان هماهنگ نماید؛
- مسئولیت‌ها و وظایف در سطح سازمان را بطور مناسبی تخصیص و تقسیم نماید؛
- اطمینان دهد که منابع مورد نیاز برای مدیریت ریسک تخصیص داده شده‌اند؛
- منافع مدیریت ریسک را به اطلاع کلیه گروه‌های ذینفع برساند؛
- اطمینان دهد که چهارچوب مدیریت ریسک همواره مناسب و درست است.



نمودار شماره ۲. رابطه بین عناصر تشکیل‌دهنده چارچوب مدیریت ریسک

۴.۳ طراحی چهارچوب مدیریت ریسک

۴.۳.۱. شناخت سازمان وعرصه‌های آن

قبل از شروع طراحی و اجرای چهارچوب مدیریت ریسک، ارزیابی و شناخت عرصه‌های درونی و بیرونی سازمان بسیار مهم می‌باشند، زیرا این شناخت بر طراحی چهارچوب مورد نظر تاثیرات زیادی دارد. ارزیابی محیط و عرصه بیرونی سازمان شامل موارد زیر می‌شود:

الف) محیط اجتماعی وفرهنگی، سیاسی، قانونی، مقرراتی، مالی، تکنولوژی، اقتصادی، طبیعی ورقابتی، اعم از بین المللی، ملی، منطقه‌ای و یا محلی؛

ب) روندها ونیروهایی که بر اهداف سازمان تاثیر می‌گذارند؛

پ) ارتباط و درک و برداشت و ارزش‌های گروه‌های ذینفع؛

ارزیابی عرصه ومحیط درونی سازمان شامل موارد زیر می‌شوند:

- اداره، ساختار سازمانی، نقشها و وظایف؛
- سیاست‌ها، اهداف واستراتژی‌هایی که برای تحقق آنها ایجاد شده‌اند؛
- توانایی‌ها بر حسب منابع، دانش و آگاهی (مانند سرمایه، وقت، نیروی انسانی، فرایندها، سیستم‌ها و تکنولوژی)؛
- سیستم‌های اطلاعاتی، جریان اطلاعات و فرایندهای تصمیم‌گیری مربوطه (رسمی و غیررسمی)؛
- روابط با گروه‌های ذینفع درونی و شناخت بینش و ارزش‌های آنها؛
- فرهنگ سازمان؛
- استانداردها، راهنماها و مدل‌های بکار گرفته شده توسط سازمان؛
- شکل و زمینه روابط قراردادی.

۴.۳.۲.ایجاد سیاست مدیریت ریسک

سیاست مدیریت ریسک باید اهداف و تعهدات سازمان در برابر ریسک را با توجه به موارد زیر به روشنی بیان نماید:

- دلایل و عقلانیت‌های سازمان برای مدیریت کردن ریسک؛
- روابط بین اهداف و سیاست‌های سازمان و سیاست مدیریت ریسک؛
- وظایف و مسئولیت‌ها برای مدیریت ریسک؛
- نحوه برخورد با منافع متضاد[1] در مدیریت ریسک؛
- تعهد نسبت به در اختیار گذاشتن منابع و امکانات لازم برای کمک به کسانی که مسئولیت و وظیفه مدیریت ریسک را برعهده دارند؛
- روشی که براساس آن عملکرد مدیریت ریسک اندازه‌گیری و گزارش می‌شود؛
- تعهد نسبت به بررسی و بهبود دوره‌ای سیاست مدیریت ریسک و چهارچوب آن و در واکنش به یک حادثه و یا تغییر در شرایط و وضعیت.

۴.۳.۳.پاسخگویی

سازمان باید اطمینان دهد که پاسخگویی، احساس مسئولیت، اختیار و صلاحیت لازم برای مدیریت ریسک شامل اجرا و نگهداری از فرایند مدیریت ریسک و اطمینان از مناسب بودن وکارایی کنترل‌های بکارگرفته شده وجود دارند. این کار می‌تواند از طریق زیر تسهیل گردد:

- شناسایی صاحبان ریسک که وظیفه واختیار مدیریت ریسک را دارند؛
- شناسایی کسانی که مسئول تهیه، اجرا ونگهداری چهارچوب مدیریت ریسک هستند؛
- شناسایی سایر مسئولیت‌های افراد در کلیه سطوح سازمان در خصوص مدیریت ریسک؛

[1] Conflivting intrests

- ایجاد روش‌های اندازه گیری عملکرد و فرایندهای گزارش‌دهی داخلی و خارجی؛
- اطمینان از سطوح مناسب تشخیص[1].

۴.۳.۴. ادغام در فرایندهای سازمانی

مدیریت ریسک باید به گونه‌ای مناسب، مربوط و کارا در فعالیت‌ها و فرایندهای سازمان گنجانده شود. فرایند مدیریت ریسک باید بخشی از جدایی ناپذیر از فرایندهای سازمان باشد.

به طور مشخص، مدیریت ریسک باید درسیاست‌گذاری، برنامه‌ریزی استراتژیک وفعالیت‌ها وبازنگری‌های بعدی آنها و فرایندهای مدیریت تغییر گنجانیده و ادغام شود. برنامه جامع و فراگیر مدیریت ریسک باید در سازمان وجود داشته باشد تا اطمینان دهد که سیاست مدیریت ریسک اجرا شده و مدیریت ریسک در کلیه فعالیت‌ها و فرایندهای سازمان ادغام گردیده است. برنامه مدیریت ریسک می‌تواند در سایر برنامه‌های سازمان مانند برنامه استراتژیک ادغام شود.

۴.۳.۵. منابع

سازمان باید منابع لازم برای مدیریت ریسک را تخصیص دهد.

موارد زیر در این خصوص باید مورد توجه قرار گیرند:

- افراد، مهارت‌ها، تجربه وصلاحیت‌ها؛
- منابع مورد نیاز برای هر مرحله از فرایند مدیریت ریسک؛
- فرایندهای سازمانی، روش‌ها و ابزارهای مورد استفاده برای مدیریت ریسک؛
- سیستم‌های مدیریت اطلاعات ودانش؛
- برنامه‌های آموزشی.

۴.۳.۶. ایجاد مکانیسم‌های ارتباطی و گزارش‌دهی درون سازمانی

سازمان باید مکانیسم‌های ارتباطی و گزارش‌دهی درون سازمانی را برای پشتیبانی از مسئولیت‌ها ومالکیت ریسک تاسیس کند. این مکانیسم‌ها باید اطمینان دهند که:

- اجزای کلیدی چهارچوب مدیریت ریسک و هرگونه اصلاحات بعدی آن به طرز مناسبی به اطلاع افراد درون سازمان می‌رسند؛
- روش گزارش‌دهی درون سازمانی مناسبی در مورد چهارچوب، کارایی و نتایج آن وجود دارد؛
- اطلاعات مربوطی که از کاربرد مدیریت ریسک بدست آمده‌اند در سطوح مناسب و در زمان مناسب در اختیار قرار می‌گیرند؛
- فرایندهایی برای مشاوره و تبادل نظر با گروه‌های ذینفع درون سازمان وجود دارد.

این مکانیسم‌ها در مواردی که امکان‌پذیر است باید فرایندهایی برای جمع‌آوری اطلاعات ریسک از منابع گوناگون همراه با ملاحظه حساسیت‌های اطلاعاتی ایجاد نمایند.

۴.۳.۷. ایجاد مکانیسم‌های ارتباطی وگزارش‌دهی برون سازمانی

[1] Recognition

سازمان‌ها باید برنامه‌ای برای نحوه اطلاع‌رسانی در مورد ریسک به گروه‌های ذینفع برون سازمانی تهیه و اجرا نمایند. این برنامه باید شامل موارد زیر باشد:

- مشارکت دادن گروه‌های ذینفع بیرونی مربوطه و اطمینان از تبادل موثر اطلاعات با آنها؛
- گزارش‌دهی بیرونی در راستای اجرای قوانین و مقررات ودرخواست‌های دولت؛
- تهیه پاسخ و گزارش در مورد ارتباطات ومشاوره‌ها؛
- استفاده اطلاع‌رسانی به منظور ایجاد اعتماد در سازمان؛
- ارتباط با گروه‌های ذینفع در صورت بروز بحران و حوادث پیش‌بینی نشده.

این مکانیسم‌ها در مواردی امکان پذیر است باید فرایندهایی برای جمع آوری اطلاعات ریسک از منابع گوناگون همراه با ملاحظه حساسیت‌های اطلاعاتی ایجاد نمایند.

۴.۴ اجرای مدیریت ریسک

۴.۴.۱ اجرای چهارچوب مدیریت ریسک.

دراجرای چهارچوب مدیریت ریسک، سازمان باید:

- زمان و استراتژی مناسب برای اجرای چهارچوب را تعیین نماید؛
- فرایند وسیاست مدیریت ریسک را در فرایندهای سازمانی اعمال نماید؛
- ملزومات قانون ومقرراتی را اجرا نماید؛
- اطمینان یابد که تصمیم‌گیری، از جمله تهیه و تعیین اهداف با خروجی‌های فرایند مدیریت ریسک در یک راستا قرار دارند؛
- نشست‌های اطلاع‌رسانی و آموزشی برقرار کند؛
- باگروهای ذینفع ارتباط و مشاوره داشته تا اطمینان یابد که چهارچوب مدیریت ریسک همچنان مناسب باقی بماند.

۴.۴.۲. اجرای فرایند مدیریت ریسک

مدیریت ریسک باید با اطمینان از بکارگیری فرایند مدیریت ریسک از طریق برنامه مدیریت ریسک در کلیه سطوح و فعالیت‌های مربوطه به عنوان بخشی از فرایندها و اقدامات سازمان که در بخش ۵ ارائه می‌شود اجرا شود.

۴.۵ نظارت و بررسی چهارچوب

به منظور حصول اطمینان از کارایی و استمرار مدیریت ریسک در پشتیبانی از عملکرد سازمان،سازمان باید:

- عملکرد مدیریت ریسک را با شاخص‌هایی که مرتباً از نظر مناسب بودنشان بررسی می‌شوند مورد اندازه گیری قرار دهد؛
- بطور دوره‌ای پیشرفت‌های حاصله در راستای برنامه و دور شدن از برنامه را اندازه گیری کند؛
- بطور دوره‌ای به بررسی اینکه آیا چهارچوب مدیریت، سیاست و برنامه ریسک سازمان هنوز با توجه به شرایط داخلی و خارجی سازمان مناسب می‌باشد و یا خیر بپردازد؛

- ریسک و پیشرفت‌های بدست آمده در زمینه برنامه مدیریت ریسک و میزان اجرای سیاست مدیریت ریسک را گزارش دهد؛
- کارایی چهارچوب مدیریت ریسک را بررسی کند.

۴.۶.بهبود دایمی و مستمر چهارچوب

براساس نتایج حاصل از نظارت وبررسی، سازمان باید در مورد اینکه چگونه می‌توان چهارچوب، سیاست و برنامه مدیریت ریسک را بهبود بخشید تصمیم‌گیری کند. این تصمیمات باید منجر به بهبود مدیریت ریسک و فرهنگ مدیریت ریسک در سازمان شوند.

۵.فرایند

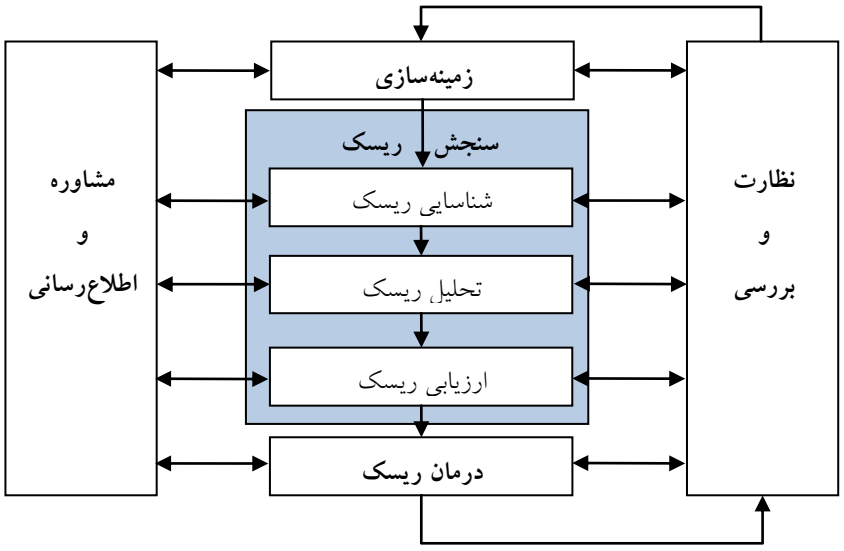
۵.۱ کلیات

فرایند مدیریت ریسک باید:

- بخشی جدایی ناپذیر از مدیریت؛
- گنجانده شده در فرهنگ وعمل؛ و
- جهت دهی شده در راستای فرایندهای سازمان

باشد.

این فرایند شامل فعالیت‌های که در بخشهای ۵.۲ تا ۵.۶ توضیح داده می‌شوند می‌گردد. فرایند مدیریت ریسک در نمودار ۳ نشان داده شده است.



نمودار شماره ۳. فرآیند مدیریت ریسک

۵.۲ اطلاع‌رسانی ومشاوره

مشاوره واطلاع‌رسانی به گروه‌های ذینفع درونی و بیرونی باید در کلیه مراحل فرایند مدیریت ریسک صورت پذیرند. بنابراین، برنامه‌های مشاوره و اطلاع‌رسانی باید در مراحل اولیه کار تهیه شوند. این برنامه‌ها باید مسائل

مربوط به خود ریسک، عوامل ایجاد کننده و پیامدهای آنها(درصورت معلوم بودن) و روش‌های بکار گرفته شده برای مقابله و درمان آنها را مورد توجه قرار دهند. مشاوره و اطلاع‌رسانی کارا باید اطمینان دهد که هم کسانی که مسئولیت اجرای فرایند مدیریت ریسک را دارند وهم گروه‌های ذینفع اصول و مبانی که بر اساس آنها تصمیمات گرفته شده و دلیل اینکه برخی اقدامات خاص مورد نیاز می‌باشند، را می‌شناسند.

روش مشاوره گروهی می‌تواند:

- به ایجاد زمینه‌سازی درست کمک کند؛
- اطمینان دهد که منافع گروه‌های ذینفع شناخته شده و مورد توجه قرار گیرند؛
- اطمینان دهد که ریسک‌ها به درستی شناسایی شوند؛
- حوزه‌های مختلف کارشناسی را برای تحلیل ریسک‌ها گردهم آورد؛
- اطمینان دهد که نقطه نظرهای گوناگون و مختلف به هنگام تعریف معیارهای ریسک و ارزیابی ریسک‌ها مورد ملاحظه قرار گیرند؛
- برنامه مقابله با ریسک را تایید و حمایت نماید؛
- مدیریت مناسب تغییر در طول فرایند مدیریت ریسک را تقویت نماید؛ و
- برنامه اطلاع‌رسانی و مشاوره مناسب درونی و بیرونی را تهیه نماید.

مشاوره و اطلاع‌رسانی به گروه‌های ذینفع بسیار اهمیت دارد زیرا این افراد در مورد ریسک براساس برداشت‌ها و تصوراتشان قضاوت می‌کنند. این برداشت‌ها می‌توانند بسته به تفاوت‌های موجود در ارزش‌ها، نیازها، فروض، مفاهیم وسایر ملاحظات گروه‌های ذینفع بسیار متنوع باشند. از آنجا که دیدگاه‌های گروه‌های ذینفع می‌توانند تاثیرات مهمی بر تصمیمات گرفته شده داشته باشند؛ درک و برداشت این گروه‌ها از ریسک باید شناسایی، ثبت و در فرایند تصمیم‌گیری مورد توجه قرار گیرند.

مشاوره و اطلاع‌رسانی باید تبادل مفید، مربوط، دقیق وقابل فهم اطلاعات را با ملاحظه ابعاد محرمانه بودن، صداقت وامانت‌داری تسهیل نماید.

۵.۳. زمینه‌سازی

۵.۳.۱. کلیات

با ایجاد زمینه، سازمان اهداف خودش را اعلام کرده، پارامترهای درونی و بیرونی مورد ملاحظه در مدیریت ریسک را تعریف کرده و حدود و معیارهای ریسک برای فرایند باقیمانده را تنظیم می‌کند. با آنکه بسیاری از این پارامترها بسیار شبیه به آنهایی هستند که در طراحی چهارچوب مدیریت ریسک مورد توجه قرار گرفتند (به بخش ۴.۳.۱. نگاه کنید) ، زمانی که زمینه‌سازی برای فرایند مدیریت ریسک صورت می‌گیرد این موارد باید با جزئیات بیشتر و بخصوص از این نظر که تا چه اندازه به حوزه فرایند مدیریت ریسک خاصی مربوط می‌شوند مورد ملاحظه قرار گیرند.

۵.۳.۲. ایجاد زمینه بیرونی

زمینه بیرونی همان محیط خارجی است که سازمان در آن در جستجوی رسیدن به اهداف خود می‌باشد. شناخت زمینه بیرونی به منظور اطمینان یافتن از اینکه اهداف وملاحظات گروه‌های ذینفع به هنگام تهیه معیارهای ریسک مورد توجه قرار گرفته اند از اهمیت برخوردار است. اگرچه این‌ها براساس حوزه عمل وسیع سازمان تعیین می‌شوند، ولی الزامات قانون و مقرراتی، برداشت‌ها و تصورات گروه‌های ذینفع و سایر جنبه‌های خاص ریسک مرتبط با فرایند مدیریت ریسک باید با جزئیات بیشتر مورد توجه قرار گیرند.

زمینه بیرونی شامل موارد زیر می‌شود:

- محیط فرهنگی، اجتماعی، سیاسی، قانونی، مقرارتی، مالی، فنی، اقتصادی، طبیعی و رقابتی اعم از بین المللی، ملی، منطقه‌ای ومحلی؛
- روندها و محرکه‌هایی که بر اهداف سازمان تاثیر می‌گذارند؛
- روابط و برداشت‌ها و ارزش‌های گروه‌های ذینفع بیرونی.

۵.۳.۳.ایجا د زمینه درونی

زمینه درونی همان محیط درونی است که سازمان در آن به دنبال رسیدن به اهدافش می‌باشد. فرایند مدیریت ریسک باید با فرهنگ، فرایندها، ساختار و استراتژی سازمان سازگار باشد. زمینه درونی شامل کلیه پدیده‌های درون یک سازمان است که بر نحوه مدیریت ریسک توسط سازمان تاثیر می‌گذارد. زمینه‌سازی درونی به دلایل زیر باید صورت پذیرد:

الف) مدیریت ریسک در محدوده و فضای سازمان صورت گیرد؛

ب) اهداف و معیارهای یک پروژه، فرایند و یا فعالیت خاص باید با ملاحظه اهداف کلی سازمان تعریف و تعیین شوند؛

ج) برخی سازمان‌ها موفق به شناسایی فرصت‌ها برای رسیدن به اهداف استراتژیک، پروژه ویا فعالیت خود نمی شوند و این بر تعهدات سازمانی، اعتبار، اعتماد و ارزش‌ها تاثیر منفی می‌گذارد.

شناخت زمینه و محیط درونی لازم است. زمینه درونی شامل موارد زیر می‌شود:

- اداره، ساختار سازمانی، نقش‌ها، ومسئولیت‌ها؛
- سیاست‌ها، اهداف واستراتژی‌های موجود برای رسیدن به آنها؛
- توانایی‌ها، بر حسب منابع، دانش و آگاهی(مانند سرمایه، زمان، مردم، فرایندها، سیستم‌ها، وتکنولوژی)
- سیستم‌های اطلاعاتی جریان اطلاعات و فرایندهای تصمیم‌گیری مربوطه (رسمی و غیر رسمی)
- شکل و اندازه روابط قراردادی.

۵.۳.۴. ایجاد زمینه و محیط فرایند مدیریت ریسک

اهداف، استراتژی‌ها، حدود و ثغور و پارامترهای فعالیت‌های سازمان، یا آن بخش‌هایی از سازمان که در آنها فرایند مدیریت ریسک اعمال می‌شود باید ایجاد شوند.

مدیریت ریسک باید با ملاحظه کامل نیاز به توجیه اقتصادی منابع بکار گرفته شده برای اجرای مدیریت ریسک صورت پذیرد. منابع مورد نیاز، مسئولیت‌ها و اختیارات و مواردی که باید مثبت و ضبط شوند باید مشخص گردند.

زمینه فرایند مدیریت ریسک بسته به نیازهای یک سازمان فرق می‌کند ولی می‌تواند شامل موارد زیر باشد:

- تعریف اهداف و مقاصد فعالیت‌های مدیریت ریسک؛
- تعریف مسئولیت‌های فرایند مدیریت ریسک واجزای آن؛
- تعریف حدود و ثغور و طول و ابعاد واندازه فعالیت‌های مدیریت ریسک که باید انجام شوند شامل مواردی که باید گنجانیده و یا نباید گنجانده شوند؛
- تعریف فعالیت، فرایند، وظیفه، پروژه، محصول، خدمت و یا دارایی برحسب زمان و مکان؛
- تعریف رابطه بین یک پروژه، فرایند، یا فعالیت خاص با سایر پروژه ها، فرایندها و یا فعالیت‌های سازمان؛
- تعریف روش‌شناسی‌های سنجش ریسک؛
- تعریف راه‌های ارزیابی کارایی و عملکرد مدیریت ریسک؛
- شناسایی و مشخص کردن تصمیماتی که باید اتخاذ شوند، و
- شناسایی ملاحظه و تعریف مطالعات مورد نیاز و اندازه و اهداف آنها و منابع مورد نیاز برای انجام این مطالعات.

توجه: این عوامل و سایر عوامل مربوط باید کمک کنند تا اطمینان دهند که روش مدیریت ریسک اعمال شده متناسب با شرایط و اوضاع سازمان و ریسک‌هایی که دستیابی به اهداف آن را تحت تاثیر قرار دهند می‌باشند.

۵.۳.۵.تعریف معیارهای ریسک

سازمان باید معیارهایی که برای ارزیابی اهمیت ریسک مورد استفاده قرار می‌گیرند را تعریف نماید. معیارها باید منعکس کننده ارزش‌ها،اهداف و منابع سازمان باشند. برخی از معیارها ممکن است از قوانین و مقررات و سایر الزاماتی که سازمان وابسته به آنهاست. استخراج شوند. معیارهای ریسک باید با سیاست ریسک سازمان (۴.۳.۲) سازگار بوده و در ابتدای هر فرایند مدیریت ریسک تعریف شده و مرتباً مورد بازنگری قرار گیرند. هنگام تعریف معیارهای ریسک،عواملی که باید در نظر گرفته شوند عبارتند از:

- ماهیت علل و انواع پیامدهای ممکن ونحوه اندازه‌گیری آنها؛
- نحوه تعریف احتمال؛
- چهارچوب زمانی احتمال و یا پیامدها؛
- نحوه تعیین سطح ریسک؛
- دیدگاه گروه‌های ذینفع؛
- سطحی که در آن ریسک قابل قبول و یا قابل تحمل می‌شود؛
- آیا ترکیبی از چند ریسک باید در نظر گرفته شود و در این صورت چه ترکیبی و چگونه باید در نظر گرفته شود.

۵.۴. سنجش ریسک[1]

۵.۴.۱ کلیات

سنجش ریسک فرایند کلی شناسایی ریسک و ارزیابی ریسک می‌باشد.

توجه: ایزو/آی ایی سی ۳۱۰۱۰ در مورد تکنیک‌های سنجش ریسک راهنمایی می‌کند.

۵.۴.۲. شناسایی ریسک

سازمان باید منبع ریسک، نواحی تاثیرگذار، حوادث (شامل تغییر در شرایط و وضعیت) و علل و پیامدهای بالقوه آنها را شناسایی کند. هدف این مرحله آن است که در آن فهرست جامعی از ریسک‌ها براساس حوادثی که ممکن است دستیابی سازمان به اهدافش را ایجاد تقویت کند تشدید و یا با تاخیر مواجه سازند تهیه شود و در اینجا شناسایی ریسک‌هایی که همراه با فرصت نیستند نیز اهمیت دارد.

شناسایی جامع ریسک‌ها بسیار حیاتی است زیرا ریسکی که در این مرحه شناسایی نشده باشد در مراحل بعدی وارد نمی شود. شناسایی باید ریسک‌ها را اعم از آنکه منبع ایجاد کننده آنها تحت کنترل سازمان باشد و یا نباشد و یا منبع و یا علت آنها آشکار باشد و یا خیر را شامل گردد.

شناسایی ریسک باید بررسی اثرات جانبی پیامد مورد نظر از جمله اثرات ثانویه و انباشتی را در نظر بگیرد. این مرحله همچنین باید دامنه وسیعی از انواع پیامدها را صرف نظر از آنکه منبع و یا علت ریسک آشکار باشد و یا خیر مورد توجه قرار دهد. ضمن شناسایی اینکه چه اتفاقی ممکن است رخ دهد در نظر گرفتن علل وسناریوهایی که نشان می‌دهند چه پیامدهایی می‌توانند در رآینده رخ دهند نیز ضروری است. همه علل و پیامدهای مهم باید در نظر گرفته شوند. سازمان باید ابزارها و روش‌های شناسایی ریسکی را بکار گیرد که با اهداف و توانایی‌های سازمان و ریسک‌هایی که با آن مواجه می‌باشد تناسب داشته باشند. اطلاعات مربوط و به روز در شناسایی ریسک بسیار مهم می‌باشند. این اطلاعات شامل اطلاعات پیش‌زمینه مناسب در مواردی که امکان‌پذیر است می‌گردد. افراد دارای دانش و آگاهی مناسب باید در شناسایی ریسک‌ها ی بکار گرفته شوند.

۵.۴.۳. تحلیل ریسک

تحلیل ریسک شامل ایجاد شناخت از ریسک می‌شود. تحلیل ریسک داده‌هایی برای ارزیابی ریسک و تصمیم‌گیری در مورد اینکه آیا باید با ریسک مقابله شود و یا نه و اینکه مناسبترین راه‌ها و روش‌های مقابله و درمان ریسک کدامند تهیه می‌کند. تحلیل ریسک همچنین باید داده‌های لازم برای تصمیم‌گیری در مورد گزینه‌هایی که دارای انواع و سطوح مختلفی از ریسک هستند فراهم کند.

تحلیل ریسک در بر گیرنده ملاحظات مربوط به علل و منشاء ریسک، پیامدهای مثبت و منفی آن و احتمال وقوع پیامدها می‌باشد. عواملی که بر پیامدها و احتمال وقوع آنها تاثیر می‌گذارند باید شناسایی شوند. ریسک از طریق تعیین پیامدها و احتمال آنها و سایر خصایص تحلیل می‌شود. هرحادثه ممکن است پیامدهای چندی به همراه داشته باشد.

[1] Risk assessment

کنترل‌های موجود و کارایی آنها نیز باید در محاسبات وارد شوند. شیوه‌ای که پیامدها و احتمالات بر اساس آنها بیان می‌شوند و روش‌هایی که آنها را با هم ترکیب می‌کنند تا سطح ریسک را تعیین نمایند باید منعکس کننده نوع ریسک، اطلاعات در دسترس و هدفی که برای آن خروجی‌های سنجش ریسک مورد استفاده قرار می‌گیرند باشد.

همه اینها باید با معیارهای ریسک سازگار باشند. همچنین ملاحظه وابستگی درونی انواع ریسک‌ها و منبع ومنشا آنها نیز از اهمیت برخوردار است.

میزان اعتماد و دقت در تعیین سطح ریسک و حساسیت آن نسبت به پیش‌شرط‌ها و فروض باید در تحلیل ریسک در نظر گرفته شده و به صورتی موثر به اطلاع تصمیم‌گیران و در موارد مناسب سایر گروه‌های ذینفع رسانده شود. عواملی مانند اختلاف نظر در بین کارشناسان، عدم‌اطمینان، در دسترس بودن[1]، کیفیت، کمیّت و مربوط بودن اطلاعات، یا محدودیت‌های مدل‌سازی باید ذکر و مورد تاکید قرار گیرند.

تحلیل ریسک می‌تواند با سطوح مختلفی از جزئیات بسته به ریسک، هدف تحلیل، و اطلاعات، داده‌ها و منابع در دسترس انجام شود. تحلیل ریسک می‌تواند به صورت کمّی، نیمه کمّی، و یا کیفی و یا ترکیبی از اینها بسته به شرایط باشد.

پیامدها و احتمال وقوع آنها می‌توانند از طریق مدل سازی نتایج یک حادثه و یا مجموعه‌ای از حوادث و یا ازطریق برون‌یابی[2] از مطالعات تجربی و یا داده‌های موجود تعیین گردند. پیامدها ممکن است به صورت ملموس بیان شوند. دربرخی موارد ممکن است پیش از یک مقدار عددی برای تعیین پیامدها و یا احتمال وقوع آنها در زمان‌ها، مکان‌ها، گروه‌ها و وضعیت‌های مختلف لازم باشد.

۵.۴.۴. ارزیابی ریسک

هدف ارزیابی ریسک کمک به تصمیم‌گیری، براساس خروجی‌های تحلیل ریسک در مورد اینکه با کدام ریسک‌ها باید مقابله شده و اولویت بندی اقدامات مقابله چگونه باشد می‌باشد. ارزیابی ریسک شامل مقایسه سطح و میزان ریسک تعیین شده در فرایند تحلیل ریسک با معیارهای ریسکی که در مرحله زمینه‌سازی چهارچوب مدیریت ریسک تعیین شدند می‌باشد. براساس این مقایسه، نیاز و یا عدم نیاز به مقابله و درمان ریسک معلوم می‌شود.

این تصمیمات باید با ملاحظه محدوده گسترده‌تر ریسک صورت گرفته و میزان تحمل ریسک توسط سایر گروه‌ها را نیز مورد توجه قرار دهد.

تصمیمات باید بر اساس الزامات قانونی، مقرراتی و سایر موارد باشند و در برخی شرایط، ارزیابی ریسک می‌تواند به تصمیم‌گیری برای انجام تحلیل‌های بیشتر بیانجامد.

ارزیابی ریسک ممکن است همچنین منجر به اتخاذ تصمیمی می‌شود که براساس آن نیاز به مقابله با ریسک به هیچ صورت بجز حفظ کنترل‌های موجود نباشد. این تصمیم از بینش سازمان درباره ریسک و معیارهای ریسک تعیین شده متاثر می‌شود.

---

[1] Availability
[2] Extrapolation

۵.۵ مقابله ودرمان ریسک

۵.۵.۱. کلیات

مقابله و کنترل ریسک شامل انتخاب یک و یا چند گزینه برای اصلاح ریسک‌ها واجرای گزینه‌های انتخابی می‌باشد. زمانیکه این گزینه‌ها اجرا شوند راه‌حل‌های ارائه شده کنترل‌ها ی ریسک را ایجاد می‌نماید. مقابله با ریسک دربرگیرنده فرایندی سیکلی از:

- سنجش راه‌های مقابله با ریسک؛
- تصمیم‌گیری در مورد اینکه آیا مقادیر ریسک‌های باقیمانده قابل تحمل می‌باشند یا خیر؛
- اگر قابل تحمل نیستند راه جدید مقابله با ریسک ایجاد شود؛ و
- کارایی این روش جدید سنجیده شود.

گزینه‌های مقابله با ریسک شامل موارد زیر می‌شوند:

الف) اجتناب از ریسک از طریق توقف و یاعدم شروع فعالیت‌هایی که باعث بروز ریسک می‌شوند؛

ب) قبول یا افزایش ریسک به منظور دستیابی به یک فرصت؛

پ) از بین بردن منشا ریسک؛

ت) تغییر احتمال وقوع؛

ث) تغییر پیامدها؛

ج) تقسیم ریسک با یک گروه ویا گروه‌های دیگر (شامل قراردادها و تامین مالی ریسک)؛ و

چ) حفظ و نگهداری آگاهانه ریسک.

۵.۵.۲. انتخاب گزینه‌های مقابله و درمان ریسک

انتخاب مناسب‌ترین گزینه مقابله با ریسک شامل مقایسه بین هزینه‌ها و منافع اقدامات اجرای آن همراه با ملاحظه الزامات قانون و مقرراتی و سایر الزامات مانند مسئولیت اجتماعی و حفاظت از محیط طبیعی می‌باشد. این تصمیمات باید ریسک‌هایی که نیاز به استفاده از گزینه‌های مقابله‌ای دارند ولی دارای توجیه اقتصادی نمی‌باشند مانند ریسک‌های دارای پیامدهای بسیار جدی و احتمال بسیار کم را نیز در نظر بگیرد.

گزینه‌های مختلف مقابله و درمان ریسک را می‌توان به صورت انفرادی ویا ترکیبی از آنها مورد استفاده قرار داد. سازمان‌ها معمولاً از بکارگیری ترکیبی از روش‌های مقابله با ریسک استفاده می‌کنند.

هنگام انتخاب گزینه‌های مقابله با ریسک، سازمان باید ارزش‌ها و دیدگاه‌های گروه‌های ذینفع و مناسب‌ترین روش‌های برقراری ارتباط با آنها را مورد توجه قرار دهد. در مواردی که گزینه‌های مقابله باریسک ممکن است بر میزان ریسک در بخش‌های دیگر سازمان و یا گروه‌های ذینفع اثر گذارند، این‌ها را باید در تصمیم‌گیری ملحوظ نمود. اگرچه ممکن است برخی از گزینه‌های مقابله و برخورد با ریسک دارای تاثیرات یکسانی باشند ولی باید توجه داشت که برخی از گروه‌های ذینفع ممکن است تعدادی از گزینه‌ها را بر گزینه‌های دیگر ترجیح دهند.

برنامه مقابله باریسک‌ها باید به وضوح ترتیب و اولویت استفاده از روش‌های مقابله با ریسک‌هایی که باید اجرا شوند را ارائه نماید.

مقابله با ریسک خود می‌تواند اجرا شده باشد. یکی از ریسک‌هایی مهم می‌تواند شکست و یا ناکارایی شیوه مقابله با ریسک اجرا شده باشد. از این رو نظارت باید جزیی پیوسته از برنامه مقابله با ریسک باشد تا اطمینان لازم از کارایی روش‌های بکار گرفته شده را بوجود آورد.

روش‌های مقابله با ریسک ممکن است منجر به بروز ریسک‌های ثانویه که باید مورد سنجش، مقابله، نظارت و بررسی قرار گیرند بشوند.

این نوع ریسک‌های ثانویه درهمان برنامه اولیه مقابله با ریسک و درکنار ریسک‌های اولیه و نه به عنوان ریسک‌های جدید مورد توجه قرار گیرند. ارتباط بین این نوع ریسک‌ها باید شناسایی و حفظ شود.

۵.۵.۳. تهیه و اجرای برنامه‌های مقابله و درمان ریسک

هدف برنامه‌های مقابله و درمان ریسک مستندسازی نحوه اجرای گزینه‌های انتخاب شده برای مقابله با ریسک‌ها می‌باشد.

اطلاعات ارائه شده در برنامه‌های مقابله و درمان ریسک باید شامل موارد زیر بشود:

- علل انتخاب گزینه‌های مقابله با ریسک شامل منافع مورد انتظاری که بدست خواهند آمد؛
- کسانی که مسئول تصویب برنامه و کسانی که مسئول اجرای برنامه هستند؛
- اقدامات پیشنهادی؛
- منابع مورد نیاز؛
- معیارهای سنجش عملکرد و محدودیت‌ها؛
- الزامات گزارش‌دهی و نظارت؛
- برنامه زمان بندی.

برنامه‌های مقابله با ریسک باید با فرایندهای مدیریتی سازمان ادغام شده و با گروه‌های ذینفع مربوطه مورد بحث و بررسی قرار گیرند.

تصمیم‌گیران و سایر گروه‌های ذینفع باید از ماهیت و میزان ریسک باقیمانده بعد از اعمال روش‌های مقابله وکنترل ریسک اطلاع داشته باشند. ریسک‌های باقیمانده باید مستند شده و مورد نظارت و بررسی ودر صورت لزوم مقابله بیشتر قرار گیرند.

۵.۶. نظارت و بررسی

نظارت و بررسی بخشی از برنامه‌ریزی شده از فرایند مدیریت ریسک بوده و شامل بررسی‌ها و مراقبت‌های مرتب باشند. نظارت و بررسی می‌تواند دوره‌ای و یا به صورت موردی باشند.

مسئولیت‌های نظارت و بررسی باید به روشنی تعریف شوند.

فرایند نظارت وبررسی سازمان باید کلیه جنبه‌های فرایند مدیریت ریسک برای تحقق اهداف زیر را شامل شود:

- اطمینان از اینکه کنترل‌ها هم از نظر طراحی و هم از نظر اجرا کارا و موثر هستند
- جمع آوری اطلاعات بیشتر برای تقویت سنجش ریسک

- تحلیل و یادگیری از حوادث،تغییرات، روندها و شکست‌ها و موفقیت‌ها
- شناسایی تغییرات در محیط درونی و بیرونی شامل تغییرات در معیارهای ریسک و خود ریسک که ممکن است نیازمند بازنگری در مقابله با ریسک واولویت‌ها باشد و
- شناسایی ریسک‌های نوظهور.

پیشرفت در زمینه اجرای برنامه‌های مقابله با ریسک نوعی معیار سنجش عملکرد به دست می‌دهد. نتایج آن را می‌توان در گزارشات درونی و بیرونی سازمان در زمینه عملکرد کلی سازمان وارد نمود. نتایج اقدامات بازرسی و نظارت باید ثبت وضبط شده و به صورت درونی و بیرونی در حد مناسبی گزارش شده و همچنین باید به صورت داده‌ای برای بازنگری در چهار چوب مدیریت ریسک مورد استفاده قرار گیرند (به قسمت ۴.۵ مراجعه کنید.)

۵.۷. ثبت و ضبط فرایند مدیریت ریسک

فعالیت‌های مدیریت ریسک باید قابل ردیابی باشند. در فرایند مدیریت ریسک رکوردها زیر بنای بهبود در روش‌ها، ابزراها و فرایند کلی را فراهم می‌کنند.

تصمیمات در مورد ایجاد رکوردها باید با ملاحظه موارد زیر صورت پذیرند:

- نیازهای سازمان به یادگیری پیوسته
- منافع استفاده مجدد از اطلاعات در فرایند مدیریت
- هزینه‌ها و تلاش‌های مورد نیاز برای ایجاد و حفظ رکوردها
- نیازهای قانون و مقرراتی و عملیاتی رکوردها
- روش دسترسی، سهولت بازیابی و ذخیره سازی رکوردها
- دوره نگهداری[1] داده‌ها
- حساسیت اطلاعات.

ضمیمه الف

ویژگی‌های مدیریت ریسک برتر

الف -۱ کلیات

کلیه سازمان‌ها باید سطح قابل قبولی از عملکرد چهارچوب مدیریت ریسک را در راستای اهمیت تصمیماتی که باید اتخاذ نمایند هدف گیری کنند. فهرست زیر ویژگی‌های عملکردی یک مدیریت ریسک سطح بالا را ارائه می‌دهد.

به منظور کمک به سازمان‌ها در اندازه گیری عملکردشان در برابر این معیارها، تعدادی شاخص ملموس برای هر ویژگی ارائه می‌شود.

[1] Retention

الف.۲ خروجی‌های کلیدی

الف۲.۱. سازمان دارای شناختی دقیق، به روز و جامع از ریسک است.
الف۲.۲.ریسک‌های سازمان منطبق با معیارهای ریسک سازمان هستند.

الف.۳ ویژگی‌ها

الف ۳.۱. بر بهبود مستمر مدیریت ریسک از طریق وضع اهدافی برای اندازه گیری عملکرد سازمان، اندازه گیری، بررسی و در صورت لزوم اصلاح فرایندها، سیستم‌ها، منابع توانایی‌ها و مهارت‌ها تاکید می‌شود.

این مسئله می‌تواند از طریق وجود اهداف عملکردی مشخص که با استفاده از آنها عملکرد مدیران اندازه گیری می‌شوند حاصل گردد. عملکرد سازمان می‌تواند منتشر و به اطلاع علاقه‌مندان رسانیده شود. معمولاً، حداقل سالی یک بار عملکردها مورد بررسی قرار گرفته و به دنبال آن بازنگری در فرایندها صورت گرفته و مجموعه جدیدی از اهداف عملکردی برای دوره بعدی تعیین می‌گردند. این سنجش عملکرد مدیریت ریسک بخشی جدایی ناپذیر از سنجش عملکرد کل سازمان ونوعی سیستم اندازه‌گیری برای بخش‌ها و افراد می‌باشد.

الف ۳.۲. مدیریت ریسک برتر شامل مسئولیت پذیری و پاسخگویی جامع، کاملاً تعریف‌شده و قابل قبول برای ریسک‌ها، کنترل‌ها، واقدامات مقابله با ریسک می‌باشد.

افراد تعیین شده مسئولیت‌پذیر و دارای مهارت‌های لازم بوده و منابع کافی برای چک کردن کنترل‌ها، نظارت بر ریسک بهبود کنترل‌ها و اطلاع‌رسانی موثر درباره ریسک و مدیریت آنها به گروه‌های ذینفع درونی و بیرونی در اختیار دارند. این موضوع از طریق میزان آگاهی کلیه اعضای سازمان از ریسک‌ها، کنترل‌ها واقداماتی که مسئول آن هستند معلوم می‌گردد. تعریف نقش‌ها، وظایف و مسئولیت‌های مدیریت ریسک باید بخشی از برنامه‌های آموزشی کلیه سازمان‌ها باشد.

سازمان باید اطمینان دهد که کلیه افرادی که مسئولیت دارند برای انجام نقش‌ها ومسئولیت‌های خود از طریق واگذاری اختیارات، زمان، آموزش، منابع و مهارت‌های کافی تجهیز شده‌اند.

الف ۳.۳. کاربرد مدیریت ریسک در کلیه تصمیم‌گیری‌ها

کلیه تصمیم‌گیری‌ها در یک سازمان صرف‌نظر از اهمیت و اندازه آنها، نیازمند توجه لازم به ریسک‌ها و کاربرد مدیریت ریسک در حد مناسب خود می‌باشند. این مساله را می‌توان از طریق ثبت وضبط جلسات و تصمیمات گرفته شده در آنها و اینکه تا چه حد در تصمیمات گرفته شده موضوع ریسک‌ها آشکارا مطرح شده‌اند مشخص کرد.

بعلاوه باید دید که تا چه اندازه کلیه عناصر و اجزای مدیریت ریسک در فرایندهای کلیدی برای تصمیم‌گیری در سازمان مانند تصمیم‌گیری در سرمایه‌گذاری در پروژه‌های بزرگ و یا تغییرات ساختاری در سازمان حضور دارند. به این دلایل، مدیریت ریسکی که به درستی بنیان نهاده شده باشد به عنوان پایه‌ای برای اداره کارای سازمان دیده می‌شود.

الف ۳.۴. اطلاع‌رسانی مستمر

مدیریت ریسک برتر شامل اطلاع‌رسانی مستمر با گروه‌ها ذینفع درونی و بیرونی از طریق گزارش‌دهی در مورد عملکرد مدیریت ریسک به عنوان بخشی از اداره خوب[1] می‌باشد. این را می‌توان از طریق تماس و ارتباط با گروه‌های ذینفع به عنوان بخشی مهم و تفکیک ناپذیر از مدیریت ریسک تشخیص داد. ارتباطات فرایندی دوطرفه است، به گونه که با کمک آنها می‌توان تصمیماتی آگاهانه در مورد سطح و اندازه ریسک‌ها و نیاز به مقابله با ریسک با استفاده از معیارهای ریسک که به درستی وضع شده اند اتخاذ نمود. گزارش‌دهی درونی و بیرونی مرتب و جامع در مورد ریسک‌های مهم وعملکرد مدیریت ریسک می‌تواند به میزان زیادی به اداره کارای یک سازمان کمک نمایند.

الف ۳.۵. ادغام و یکپارچگی کامل در ساختار اداره سازمان

به مدیریت ریسک در مرکزیت فرایندهای مدیریتی سازمان نگاه می‌شود، به گونه‌ای که ریسک‌ها به صورت اثر عدم‌اطمینان بر اهداف سازمان در نظر گرفته می‌شوند. ساختار و فرایند اداره سازمان برپایه مدیریت ریسک استوار می‌باشد. مدیریت کارای ریسک از نظر مدیران برای دستیابی و تحقق اهداف سازمان ضروری هستند. این را می‌توان از طریق زبان بکار گرفته شده توسط مدیران و بررسی نوشته‌های مهم آنها در مورد عدم‌اطمینان در ارتباط با ریسک تشخیص داد. این خصیصه معمولاً در متن سیاست‌های سازمان‌ها بخصوص آنها که به مدیریت ریسک مربوط می‌شوند منعکس می‌شود. وجود این خصیصه در یک سازمان را می‌توان معمولاً از طریق مصاحبه با مدیران و یا شواهد گفتاری و عملی آنها بررسی نمود.

منابع

[1] ISO Guide 73:2009, *Risk management — Vocabulary*

[2] IEC 31010, Risk management — Risk assessment guidelines

[1] Good governance