شرکت ملی پالایش و پخش فرآورده های نفتی ایران

روش اجرایی مدیریت ریسک سازمانی

شماره: 2110105/1

تاریخ تصویب/ بازنگری	شرح بازنگری
1400/03/09	
1402/08/21	بازنگری ساختار و مسئولیت ها

فهرست

فهرست اشکال

فهرست جداول

مقدمه

مدیریت ریسک سازمانی، روش ی سیستماتیک برای مدیریت ریسک های سازمان به صورت سازگار و همراستا با استراتژی‌های فراهم نموده و بر خلق، حفظ و توسعه ارزش اثر گذار خواهد بود. روش اجرایی مدیریت ریسک سازمانی[1] بدنبال ارائه راهنما به منظور تبیین چگونگی بکارگیری مدیریت ریسک جامع و یکپارچه است. سند پیش‌رو، که منطبق با چارچوب کوزو [2] طراحی و تنظیم گردیده است، فعالیت‌های کلیدی مورد نیاز برای یک رویکرد مدیریت ریسک موثر را شناسایی می‌کند.

1. هدف

هدف از تدو ین این روش اجرا یی حصول اطم ینان از مد یریت اثر بخش ر یسک‌های سازمانی (شامل شناسایی، تحلیل، ارز یابی و برخورد با ر یسک) بصورت سیستماتیک در جهت کاهش اثرات منف ی، دستیابی به اهداف سازمانی و نهایتا برخورداری از مزایای مدیریت ریسک است.

مزایای مدیریت ریسک عبارتند از:

- فراهم ساختن یک رویکرد سیستماتیک برای شناسایی و مدیریت ریسک؛
- ارتقای تاب‌آوری[3] بنگاه
- افزایش دامنه فرصت‌ها
- افزایش نتایج و مزیت‌های مثبت ضمن کاهش اثرات منفی
- ثبات عملکرد و کاهش انحرافات عملکردی
- بهبود به کارگیری منابع

2 دامنه کاربرد

این روش اجرایی برای کلیه اهداف و سطوح سازمانی در شرکت ملی پالایش و پخش فرآورده های نفتی ایران و شرکت‌های فرعی کاربرد دارد.

1.Enterprise risk management
2.COSO
3. Resilience

3 تعاریف

3-1. سازمان

منظور از سازمان در این سند، شرکت ملی پالایش و پخش فرآوردههای نفتی ایران است.

3-2. عدم قطعیت [1]

عدم قطعیت وضعیتی از یک رویداد است که به دلیل نقص در شناخت، دانش یا اطلاعات مرتبط، نتیجه آن احتمالی و غیرقطعی است. عدم قطعیت زمانی وجود دارد که احتمال وقوع رویداد نامعلوم است . ریسک‌ها به عنوان عدم قطعیت‌های موجود در فعالیت‌های شرکت شناخته می‌شوند که درصورت وقوع، اثرات مثبت یا منفی بر اهدافی چون زمان، هزینه و کیفیت خواهند داشت.

3-3. ریسک

ریسک متغیری است که می‌تواند منجر به انحراف از یک خروجی مورد انتظار شده و در نتیجه می‌تواند دستیابی به اهداف استراتژیک و عملکرد کلی سازمانی را تحت تاثیر خود قرار دهد.

3-4. مدیریت ریسک سازمانی [2]

مدیریت ریسک سازمانی فرآیند شناسایی، اندازه‌گیری، تصمیم‌گیری و نظارت بر انواع ریسک‌های مطرح سازمان به منظور کهینه‌سازی تغییرات عملکرد غیرمنتظره و بیشینه‌سازی ارزش ذاتی فعالیت‌های شرکت است در این سند دو عبارت مدیریت ریسک و مدیریت ریسک سازمانی معادل هستند.

3-5. احتمال وقوع ریسک [3]

امکان وقوع یک رویداد ریسک است که به صورت درصد و یا به گونه جامع‌تر به صورت نمودار توزیع احتمالی بیان می‌شود.

---

1. Uncertainty
2. Enterprise risk management
3.Probability of risk

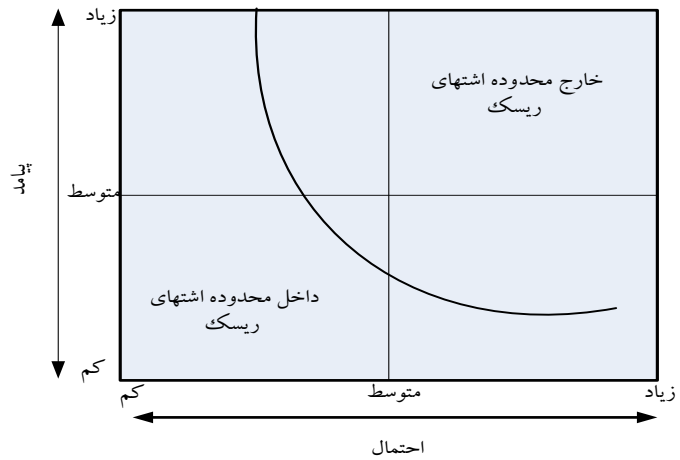
3-6. شدت اثر ریسک [1]

تغییرات برنامه‌ریزی نشده در جهت تحقق اهداف شرکت که در نتیجه وقوع یک ریسک ایجاد خواهد شد و می‌تواند به صورت مثبت یا منفی باشد.

3-7. اشتهای ریسک [2]

منظور از اشتهای ریسک نوع و میزان ریسکی که هیئت مدیره شرکت مایل به پذیرش آن برای کسب ارزش افزوده بیشتر است . . اشتهای ریسک در قالب نقشه اشتهای ریسک مانند آنچه در شکل 1 نشان داده شده، قابل تفسیر است. در این نقشه محدوده‌ای که سازمان با توجه به احتمال و پیامد وقوع یک ریسک را می‌پذیرد مشخص می‌گردد. این نقشه بیان می‌دارد که سازمان تا چه حدی، وقوع رویداد با احتمال کم و اثر منفی (زیاد) یا رویداد با احتمال زیاد و اثر کم را می‌پذیرد. فلسفه مدیریت ریسک و تاثیر آن بر فرهنگ سازمان در سندی بعنوان سند بیانیه اشتهای ریسک منتشر می‌شود.

شکل 1- نقشه اشتهای ریسک



3-8. چارچوب مدیریت ریسک سازمانی [3]

چارچوب مدیریت ریسک سازمانی برگرفته از چارچوب کوزو ویرایش 2017 و شامل 3 جزء به شرح ذیل است:

1.Severity of risk
2.Risk appetite
3. Enterprise risk management framework

- **استراتژی و هدف گذاری:** فرآیند مدیریت ریسک سازمان و فرآیند توسعه استراتژی ، سیاستهای حاکمیتی و مدل کسب و کار در کنار هم عمل می‌کنند.
- **عملکرد**[1]: سازمان ریسک‌هایی که بر تحقق استراتژی و اهداف تاثیر می گذارد را شناسایی و ارزیابی می‌کند. ریسک‌های سازمان بر مبنای شدت آنها و اشتهای ریسک اولویت بندی می‌شود. سازمان پاسخ به ریسک‌ها را انتخاب و اقدامات انجام شده برای تغییرات را پایش می کند. به این طریق دیدگاه پورتفوی[2] برای میزان ریسکی که سازمان در مسیر استراتژی و اهداف خود متحمل شده است توسعه می‌یابد.
- **بازبینی و بازنگری**[3]: با بازبینی عملکرد مدیریت ریسک، سازمان می تواند بررسی کند عملکرد مدیریت ریسک چقدر توانسته در طی زمان ارزش ایجاد کند و چه تغییرات اصلاحی مورد نیاز است

3-9. بیانیه اشتهای مدیریت ریسک[4]

بیانیه اشتهای ریسک، سیاستی تایید شده توسط هیئت مدیره است که انواع و میزان ریسک را تعریف کرده و سطوح ریسکی را تجمیع می‌نماید که سازمان به منظور دستیابی با اهداف خود قادر به پذیرش آنها است. راهنمای بیانیه اشتهای ریسک در پیوست ب اشاره شده است.

3-10. ریسک قابل پذیرش[5]

ریسک قابل پذیرش به سطح ریسک قابل قبول جهت دستیابی به هدف تعریف شده اطلاق می‌گردد. این سطوح حدود آستانه کمی هستند که اشتهای ریسک سازمان را به انواع بخصوصی از ریسک واحدهای کسب و کار نسبت می‌دهد. با توجه به اهداف مختلف، ریسک قابل پذیرش ممکن است متفاوت باشد. بطور مثال برای تغییرات درآمدی، مواجهه با نرخ بهره، تطابق با قوانین و مقررات و ... ریسک قابل پذیرش متفاوت خواهد بود.

توجه: اشتهای ریسک و ریسک قابل پذیرش تفاوت دارند. اشتهای ریسک مفهومی استراتژیک است که در سطح هیئت مدیره تعریف می‌گردد در حالیکه ریسک قابل پذیرش مفهوم تاکتیکال دارد و بعنوان عملکرد ارزیابی شده در دسترسی به هدف تعریف می‌گردد.

1.Performance
2. Portfolio View
3.Review and revision
4.Risk appetite satement
5.Acceptable risk

3-11. ریسک ذاتی[1]

عاملی که بدون هیچ اقدام مدیریتی می‌تواند بر احتمال و پیامد ریسک اثر گذارد، منجر به پیدایش ریسک ذاتی می گردد. در صورتی که هیچ اقدامی برای کنترل ریسک صورت نپذیرد سازمان را در دستیابی به اهدافش با محدودیت مواجه نماید.

3-12. ریسک باقیمانده هدف[2]

مقدار ریسکی است که سازمان ترجیح می‌دهد در اجرا و پیگیری استراتژی و تحقق اهداف بپذیرد.

3-13. ریسک باقیمانده واقعی[3]

مقدار ریسک باقیمانده بعد از اقدامات مدیریتی و تغییر شدت ریسک است.

3-14. پروفایل ریسک[4]

مجموعه ریسک‌های احصا شده در سازمان که انواع، شدت ، احتمال وقوع ، وابستگی متقابل ریسک‌ها و چگونگی اثرگذاری ریسک‌ها بر عملکرد سازمان در انطباق با اهداف استراتژیک را بیان می‌نماید، پروفایل ریسک نام دارد. پروفایل ریسک تصویری لحظه‌ای از پورتفوی ریسک‌های یک سازمان در مقطعی خاص از زمان است. ضروری است که پروفایل ریسک با مدل کسب و کار و استراتژی سازمان تطابق داشته باشد.

3-15. ذینفعان

هر گروه یا فردی که از بقا و موفقیت شرکت حمایت کرده و بر آن تاثیر گذاشته یا از آن تاثیر می‌پذیرد را می‌توان به عنوان یک ذینفع در نظر گرفت . شخص یا گروه متاثر از عملکرد شرکت شامل مشتریان، مالکان پروژه، سرمایه‌گذاران، تامین‌کنندگان، همکاران و جامعه است.

3-16. مالک ریسک[5]

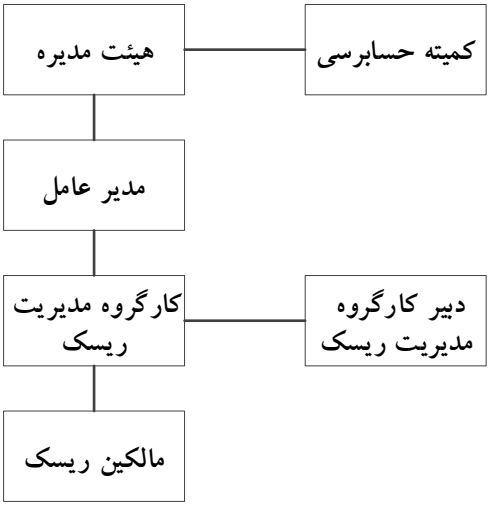
شخص یا مدیریتی که عهده دار مسئولیت شناسایی و پایش ریسک مشخصی است و مسئولیت نهایی تحت کنترل درآوردن ریسک‌های شناسایی شده تا سطح ریسک قابل تحمل بر عهده او است.

1.Inherent risk
2.Target residual risk
3.Actual residual risk
4.Risk profile
5.Risk owner

4 ساختار و مسئولیت ها

4-1. ساختار مدیریت ریسک

ساختار غیر موظف مدیریت ریسک در شکل 2 ترسیم شده است.



شکل 2-ساختار غیرموظف مدیریت ریسک

سازمان بطور مداوم ساختار خود را بازنگری می کند تا اطمینان یابد مسئولیت ها به روشنی در سطوح هیئت مدیره و مدیریت تخصیص و تعریف شده‌اند و ساختار موجود از برخورد مطلوب با ریسک پشتیبانی می‌کند.

4-2. مسئولیت ها

4-2-1- هیئت مدیره شرکت

- تصویب سند بیانیه اشتهای ریسک
- تصویب راهبردها و سیاست‌های کلی مدیریت ریسک و استراتژی‌های پاسخ به ریسک
- پایش کلان و تعیین جهت‌گیری‌های سازمان با توجه به گزارش‌های دوره‌ای و بازخوردهای لازم
- تخصیص منابع مورد نیاز مدیریت ریسک

4-2-2. مدیر عامل

- حصول اطمینان از این که سازمان از اصول مناسبی برای شناسایی، ارزیابی، پایش، گزارش‌دهی، کاهش و کنترل ریسک استراتژیک استفاده می‌کند.
- حصول اطمینان از اطلاع رسانی و بکارگیری فرهنگ آگاهی از ریسک در سازمان
- حصول اطمینان از همسوسازی رفتارها و تصمیم‌گیری مبتنی بر ریسک با عملکرد سازمان
- نظارت بر فعالیت کارگروه مدیریت ریسک سازمانی
- ابلاغ بیانیه اشتهای ریسک
- تایید گزارش کنترل و پایش ریسک جهت ارایه به هیئت مدیره
- حصول اطمینان از این که اطلاعات شفاف، جامع، مرتبط، قابل اعتماد، قابل‌سنجش و مهم مربوط به حوزه های مختلف کاری سازمان به موقع، در اختیار افراد قرار می‌گیرد.
- تصویب و ابلاغ دستورالعمل‌های تخصصی

3-2-4. کارگروه مدیریت ریسک سازمانی

هدف از تشکیل کارگروه مدیریت ریسک سازمانی ، ارائه نظرات مشورتی و کمک به ایفای مسئولیت نظارتی هیئت مدیره شرکت و بهبود آن جهت کسب اطمینان معقول از تحقق موارد زیر و کسب اطمینان از استقرار ساز و کارهای مناسب برای مدیریت ریسک است:

- سیاست‌گذاری و تعیین خطمشی‌های شرکت در حوزه ریسک
- استقرار فرآیندهای شناسایی، ارزیابی، تجزیه و تحلیل و پاسخ به ریسک
- وجود فرآیندها و سامانه‌های الزام برای گزارش‌دهی ریسک‌های شرکت
- مدیریت موثر ریسک‌ها و اطمینان معقول از دستیابی به اهداف و ارزش‌های اصلی شرکت
- تعیین اشتهای ریسک شرکت

این کارگروه متشکل از مدیران برنامه‌ریزی تلفیقی، هماهنگی و نظارت بر عملیات، مهندسی ساختار، بهداشت، ایمنی، محیط زیست و پدافند غیرعامل، بازرگانی، و رئیس دفتر مدیرعامل و دبیر جلسات هیئت مدیره و دو نفر از کارشناسان خبره مدیریت ریسک به انتخاب مدیر عامل است و جلسات آن حداقل هر سه ماه یکبار برگزار می‌شود. ریاست کارگروه بر عهده مدیر برنامه‌ریزی تلفیقی و دبیر کارگروه رئیس دفتر مدیرعامل و دبیر جلسات هیئت مدیره می‌باشد. در صورت نیاز و با توجه به طبقه-بندی ریسک از سایر مدیریت‌ها و واحدهای بالافصل مدیرعامل نماینده دعوت می‌گردد. شرکت‌های فرعی

موظفند نسبت به تشکیل کارگروه مدیریت ریسک با اعضای متناظر در سطح آن شرکت اقدام و گزارش‌های ادواری لازم را به کارگروه شرکت اصلی ارسال نمایند . احکام اعضای کارگروه توسط مدیر عامل شرکت صادر می‌گردد.

کارگروه وظایف و مسئولیت‌های زیر را بر عهده دارد:

- بررسی و ارزیابی مدیریت ریسک در شرکت
- بررسی وضعیت ریسک های شرکت بر حسب درجه ریسک پذیری و اشتهای ریسک تعیین شده هیئت مدیره و در صورت لزوم ارایه مشاوره به مدیر عامل و یا سایر واحدها
- پیشنهاد رویکردها، راهبردها و سیاستهای مدیریت ریسک به هیئت مدیره شرکت
- نظارت بر استقرار برنامه یا چارچوب سیستم مدیریت ریسک یکپارچه در شرکت و پیگیری اجرای آن
- نظارت بر عملکرد واحد مدیریت ریسک شرکت
- شناسایی نارسایی‌های موجود در مدیریت ریسک جهت طرح در هیئت مدیره
- حصول اطمینان معقول از عدم همپوشانی و شکاف های احتمالی در نظارت از طریق برگزاری جلسات با سایر کارگروههای هیئت مدیره
- حصول اطمینان معقول از ایجاد و ارتقای آگاهی نسبت به ریسک در سطح شرکت
- ارایه گزارش‌های مستمر در مورد وضعیت انواع ریسک های شرکت از قبیل مالی و اعتباری، حقوقی و قانونی، راهبردی و تجاری، عملیاتی، ریسک های مربوط به تکنولوژی، فناوری اطلاعات و ارتباطات به هیئت مدیره
- بررسی عملکرد، پایش دوره ای برنامه یا چارچوب مدیریت ریسک شرکت و ارزیابی اثربخشی آن و ارایه گزارش به هیئت مدیره
- استفاده از بسترهای لازم جهت دریافت گزارش ها و موضوعات مرتبط با ریسک از کلیه ذینفعان شرکت
- سایر موارد به تشخیص هیئت مدیره شرکت

هیئت مدیره شرکت در چارچوب مسئولیت های کارگروه ریسک به آن اختیارات ذیل را می دهد:

-

- دسترسی به منابع اطلاعاتی مورد نیاز برای انجام وظایف
- استفاده از مشاوران خارج از شرکت جهت انجام وظایف و مسئولیت‌های کارگروه در مواقع لزوم
- برگزاری جلسه با کارکنان، مدیران یا اشخاص بیرونی جهت انجام وظایف کارگروه و کسب اطلاعات از آنها
- دعوت از اشخاص مستقل و صاحب‌نظر دارای تجربه و تخصص جهت حضور در جلسات (بدون حق رای)
- برقراری تعاملات با مدیران اجرایی شرکت در حوزه مدیریت و نظارت بر ریسک های شرکت
- سایر اختیارات به تشخیص هیئت مدیره شرکت

4-2-4. دبیر کارگروه مدیریت ریسک

دبیر کارگروه وظایف و مسئولیت‌های زیر را بر عهده دارد:

- تشکیل جلسات کارگروه
- هدایت، راهبری و دبیری جلسات کارگروه و پیگیری اخذ اسناد راهبردی (شامل سند استراتژی شرکت، سیاستهای حاکمیتی و الزامات و مقررات رگولاتوری و ...)
- تهیه و بروزآوری داشبورد مدیریت ریسک سازمان
- اخذ و تحلیل گزارش های ریسک/پایش ریسک از مالکین
- تکمیل پروفایل ریسک و نگهداری داده‌های جمع‌آوری شده برای شناسایی ریسک
- بررسی، تنظیم و بازنگری روش اجرایی مدیریت ریسک
- تنظیم گزارش مدیریت ریسک جهت ارائه به مدیرعامل/هیات مدیره
- بررسی و تنظیم دستورالعمل‌های تخصصی

4-2-5. متولیان / مالکین ریسک

مالک ریسک مسئولیت‌های ذیل را بر عهده دارد:

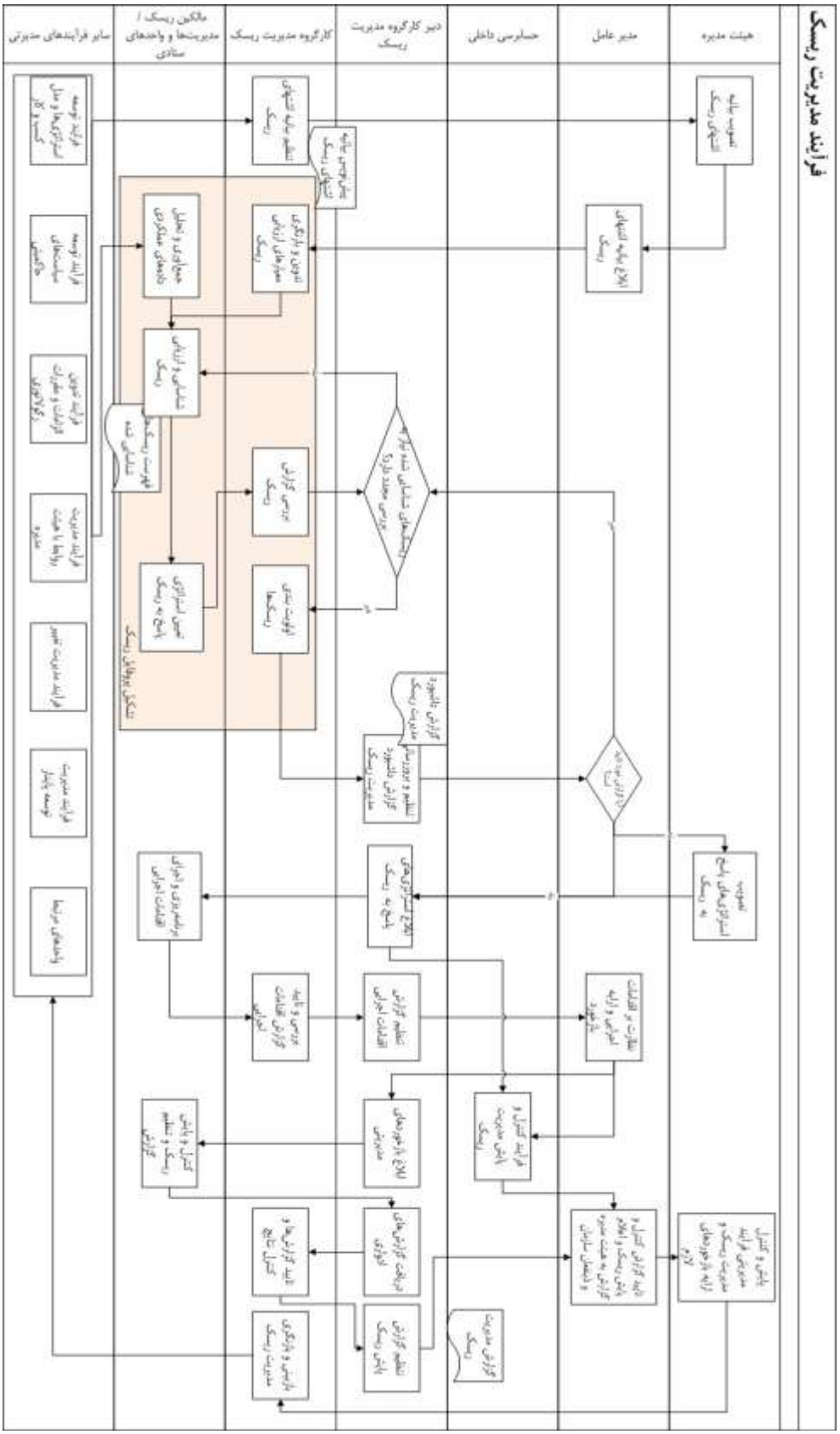
- مطالعه و بررسی فضای سازمان و اسناد راهبردی

- جمع‌آوری داده‌های اطلاعاتی از منابع مختلف برای شناسایی ریسک
- شناسایی، تحلیل، ارزیابی، اولویت‌بندی و تعیین استراتژی‌ها و برنامه های مقابله با ریسک در حوزه کاری مربوطه (تهیه پروفایل ریسک)
- تهیه و بازنگری دستورالعمل تخصصی مدیریت ریسک در حوزه مربوطه (حسب نیاز)
- بازنگری ریسک و شناسایی منابع و رویدادهای جدید
- برنامه‌ریزی اقدامات اجرایی و گزارش‌دهی برنامه‌ها و اقدامات مقابله با ریسک
- تحلیل علل عدم اجرا یا عدم اثربخشی اقدامات مرتبط با ریسک
- تشکیل کارگروه های فرعی مدیریت ریسک با دعوت از کلیه شرکتها / مدیریتها/واحدهای مرتبط و موثر بر ریسک های مربوطه (حسب نیاز)

5 مراحل اجرایی مدیریت ریسک سازمانی

5-1. نمودار ارتباطات فرآیندی

شکل 3 نمودار ارتباطات فرآیندی مدیریت ریسک سازمانی را نشان می‌دهد.



شکل 3- مراحل فرآیند مدیریت ریسک

5-2. تنظیم بیانیه اشتهای ریسک

کارگروه مدیریت ریسک، پیش‌نویس بیانیه اشتهای ریسک را در ارتباط با خلق، حفظ و درک ارزش های سازمان تنظیم می‌نماید. راهنمای تدوین بیانیه اشتهای اشتهای ریسک در پیوست ب- ارائه شده است. پیش‌نویس بیانیه اشتهای ریسک توسط دبیر کارگروه جهت طرح و تصویب در هیئت مدیره به مدیر عامل شرکت ارسال می‌شود. هیئت مدیره شرکت باید در ارتباط با همراستایی و یکپارچگی استراتژی با مفاد بیانیه اشتهای ریسک سازمان تصمیم‌گیری نماید. بیانیه اشتهای ریسک به صورت سالیانه یا در اثر تغییر سند استراتژیک بازنگری و توسط مدیر عامل ابلاغ می‌گردد.

5-3. تشکیل پروفایل ریسک

5-3-1. تدوین و بازنگری معیارهای ارزیابی ریسک

کارگروه مدیریت ریسک مجموعه‌ای از معیارهای مشترک را تدوین و توسعه و توسط دبیر کارگروه به مالکین ریسک برای ارزیابی ریسک اعلام می‌نماید.

5-3-2. جمع آوری و تحلیل داده‌های عملکردی

در این مرحله مالکین ریسک با ردیابی داده های ناشی از وقوع رویدادهای گذشته و تاثیرات آن بر اهداف استراتژیک درک بهتری از ریسک های موثر بدست می آورند. مالکین ریسک یک پایگاه داده زیان/رویداد برای ثبت کلیه زیان‌ها و رویدادهای اساسی را ایجاد می‌کنند. این پایگاه داده بصورت مداوم توسط مالکین ریسک توسعه می‌یابد. سوابق تاریخی تاثیرات هر یک از رویدادها بر دستیابی به اهداف استراتژیک سازمان جمع‌آوری و در پایگاه داده نگهداری می‌گردد. این رویدادها شامل موارد ذیل می‌باشد:

- تغییرات در محیط داخلی و خارجی سازمان برای مثال تغییرات برنامه‌های 5 ساله
- تغییرات در فرآیندهای کاری و عملیات جاری مانند تغییر در تکنولوژی و بهره برداری از یافته‌های جدید در شرکت‌های مشابه
- نتایج یافته‌های بازنگری مدیریت ریسک که حاکی از عدم اثر بخشی اقدامات انجام یافته
- روند تغییرات پیش‌بینی شده مانند تغییرات در روند مصرف، تولید و ...
- رویدادهای اقتصادی خارجی[1]
- وقایع و رویدادهای طبیعی
- رویدادهای سیاسی
- عوامل اجتماعی

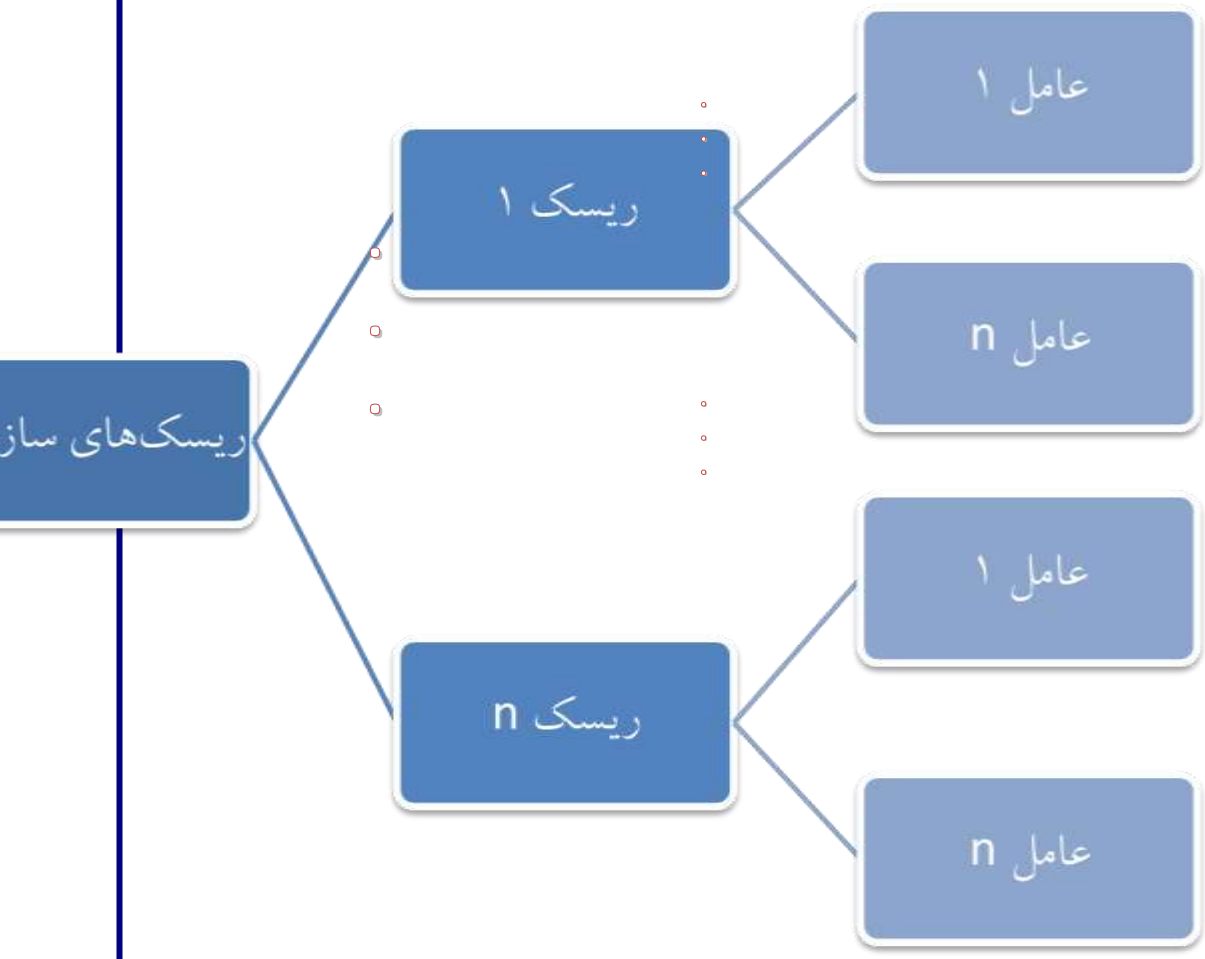
1.External economic events

برای پشتیبانی از تصمیمات آگاه از ریسک [1] داده‌های با کیفیت حفظ و نگهداری می‌شود. دبیر کارگروه مدیریت ریسک و مالکین ریسک باید اطمینان حاصل کنند داده ها و اطلاعات استاندارد شده‌ی با کیفیت بهنگام و بی‌وقفه[2] در دسترس کاربر نهایی قرار دارد. مسیرهای اطلاعاتی مناسب در سازمان تعریف شده و هر گونه تغییر در عوامل موثر بر ریسک گزارش می‌گردد. مالکین ریسک باید اطلاعات ریسک حوزه کاری خود را تجمیع و نگهداری کنند.

3-3-5. شناسایی و ارزیابی ریسک

سازمان ریسک‌هایی که بر عملکرد استراتژی‌ها و هدف‌گذاری تدوین شده تاثیر می‌گذارد را شناسایی می‌کند ساختار نمونه‌ای شکست ریسک (**RBS**[3]) در شکل 4 نشان داده شده است مالکین ریسک می‌بایست ریسک‌های فرآیندها و فعالیت‌های حوزه کاری خود را به صورت ادواری (هر سه ماه یکبار) شناسایی و ارزیابی نمایند انتخاب رویکرد مناسب برای شناسایی ریسک توسط مالکین ریسک مشخص شود.

1 .Risk-aware
2. Real-time
3. Risk breakdown structure



شکل 4- ساختار شکست ریسک

مالکین ریسک پس از شناسایی ریسک، اقدام به ارزیابی ریسک می‌نمایند. ارزیابی ریسک شامل ارزیابی شدت ریسک، تعیین شدت ریسک با توجه به معیارهای ابلاغ شده (بند 5-3-1) است. مقدار شدت ریسک بر مبنای دو عامل احتمال وقوع (**P**) و پیامد (**I**) حاصل از یک رویداد و از حاصلضرب این دو عامل در یکدیگر تعیین می‌شود.

شدت ریسک[1] = پیامد (**I**) × احتمال وقوع (**P**). احتمال وقوع و شدت اثر مطابق با جداول 1 و2 تعیین می‌گردد.

معیارها	مقیاس				
	تاثیر ناچیز	تاثیر کم	تاثیر نسبی	تاثیر زیاد	تاثیر شدید

1.Severity of Risk

	1	2	3	4	5
معیار 1 . . معیار N					

جدول 1- شدت اثر ریسک

مقیاس		درصد احتمال	فرکانس وقوع(تجربیات گذشته)
خیلی کم	1	احتمال کمتر از20درصد وقوع رویداد	تا بحال در سازمان رخ نداده است.
کم	2	احتمال بین 20 تا40 درصد وقوع رویداد	هر 3 تا 5 سال یکبار روی می‌دهد.
متوسط	3	احتمال بین 40 تا60درصد وقوع رویداد	هر 1 تا 3 سال روی می‌دهد.
زیاد	4	احتمال بین 60 تا80 درصد وقوع رویداد	هر سال یکبار روی می‌دهد.
خیلی زیاد	5	احتمال بیش از 80 درصد وقوع رویداد	هر سال بیش از یکبار رخ می‌دهد.

جدول 2- احتمال وقوع ریسک

4-3-5. تعیین استراتژی پاسخ به ریسک

مالکین ریسک با توجه به شدت ریسک و بیانیه اشتهای ریسک، استراتژی پاسخ به ریسک را تعیین نمایند انتخاب استراتژی مناسب برای پاسخ به ریسک متواند بر اساس یک‌یا چند عامل زیر باشد

- فضای کسب و کار
- هزینه‌ها و مزایا
- الزامات و مقررات
- اولویت‌بندی‌های ریسک
- اشتهای ریسک
- شدت ریسک

4 استراتژی پاسخ به ریسک عبارتند از:

- اجتناب از ریسک و جلوگیری از بروز ریسک[1]
- کاهش ریسک[2]

1.Risk avoidance
2.Risk reduction

- پذیرش ریسک[1]
- اشتراک ریسک[2]

مسئولیت تصویب استراتژی پاسخ به ریسک‌های[3] شناسایی شده در سطوح مختلف مطابق جدول 3 می‌باشد.

سطح ریسک	عدد ریسک	تصویب استراتژی پاسخ به ریسک، کنترل و پایش ریسک
1	25-20	هیئت مدیره
2	19-13	کارگروه مدیریت ریسک
3	12-7	مالک ریسک
4	6-1	مدیریا رئیس واحد

جدول 3- سطوح تصمیم‌گیری

جهت توضیح بیشتر به پیوست ج رجوع شود.

5-3-5. تدوین و ارسال گزارش ریسک‌های شناسایی شده

ریسک‌های شناسایی شده و استراتژی های پاسخ به ریسک، توسط مالکین ریسک به دبیر کارگروه مدیریت ریسک گزارش می شود. گزارش ریسک‌های شناسایی شده می‌بایست در قالب فرم شناسایی ریسک (پیوست د) تهیه و شامل موارد ذیل است:

- ریسک‌های شناسایی شده و نتایج ارزیابی
- شرح ریسک
- منابع مورد نیاز
- اولویت‌بندی ریسک‌های تحت مالکیت
- استراتژی پاسخ به ریسک‌های شناسایی شده

5-3-6. بررسی و تایید گزارش ریسک

ریسک‌های سازمانی در حوزه های مختلف کاری توسط دبیر کارگروه جمع‌آوری و در کارگروه مدیریت ریسک مطرح و بررسی می‌شود.

کارگروه مدیریت ریسک نسبت به بررسی گزارش با ملحوظ نمودن معیارهای ذیل اقدام می‌نماید:

1.Risk acceptance
2.Risk sharing
3.Risk response

- تطبیق ریسک‌های شناسایی شده با اهداف سازمانی
- اثرگذاری و ارتباط بین رخدادها و تاثیر وقوع یک رخداد بر ریسک های شناسایی شده و ارتباط بین آنها (تحلیل اثر رخدادی مشترک بر فرصت‌های پیش‌روی سازمان و وقوع سایر ریسک‌های سازمانی)
- صحه‌گذاری نتایج ارزیابی ریسک و تحلیل تناسب استراتژی‌های پاسخ به ریسک (منظور از صحه‌گذاری، بررسی احتمال برآورد شده و شدت اثر وقوع ریسک با توجه به تحلیل هزینه- منفعت و تایید استراتژی مناسب است)

پس از تایید صحت نتایج ارزیابی ریسک، سطح ریسک قابل پذیرش[1] برای هر یک از ریسکها تعیین می‌شود. در صورت نیاز به بررسی مجدد ریسکها، مراتب توسط دبیر کارگروه به مالکین ریسک اعلام میشود.

7-3-5. اولویت‌بندی ریسک

سازمان ریسک ها را اولویت بندی می کند تا تصمیم گیری درخصوص اقدامات اجرایی پاسخ به ریسک، آگاهانه انجام و تخصیص منابع بهینه سازی شود. با در نظر گرفتن منابع در دسترس باید موازنه بین تخصیص منابع برای واکنش به یک ریسک در مقایسه با ریسک دیگر ارزیابی شود . دبیر کارگروه پس از تجمیع گزارشات اقدام به برگزاری جلسه کارگروه مدیریت ریسک نموده و ریسک های مهم سازمان بر اساس معیارهای اولویت‌بندی ریسک، شناسایی می‌گردد.

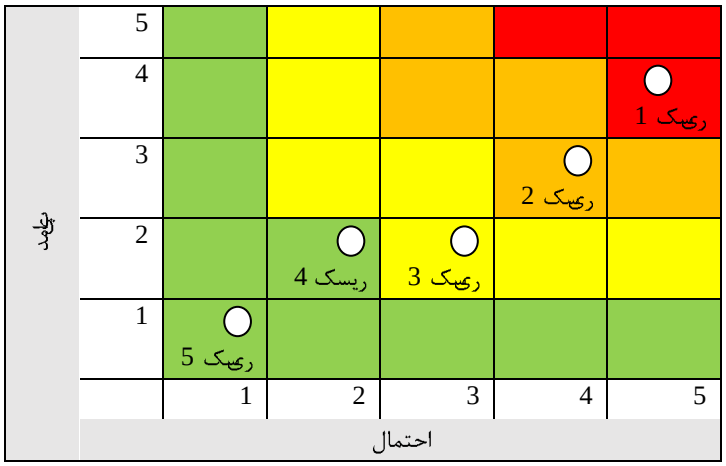
معیارهای اولویت‌بندی ریسک عبارتند از:

- شدت اثر ریسک
- وفق‌پذیری: قابلیت انطباق با تغییرات پیش بینی نشده (برای مثال پاسخ به تغییرات تقاضا و یا تغییرات جمعیتی در افزایش مصرف سوخت)
- پیچیدگی: دامنه و ماهیت ریسک و وابستگی متقابل بین ریسکها
- شتاب: سرعت تاثیر ریسک بر شرکت
- ماندگاری: مدت زمان تاثیرگذاری یک ریسک بر سازمان
- بازیابی: قابلیب بازگشت به وضعیت تحمل‌پذیر (مانند تداوم فعالیت بعد از بلایای طبیعی)

1.Acceptable risk level

4-5. تنظیم داشبورد مدیریت ریسک

ریسک‌های شناسایی شده توسط دبیر کارگروه در پروفایل مدیریت ریسک سازمانی با اختصاص شماره ریسک منحصر بفرد (پیوست الف) ثبت، نگهداری و بروزرسانی می‌شود. نتایج حاصل از تشکیل پروفایل با استفاده از داشبورد مدیریت ریسک که گزارش‌هایی تلفیقی و بروز در ارتباط با وضعیت ریسک های موجود در سازمان ارائه می‌دهد، گزارش می‌شود. داشبورد مدیریت ریسک شامل نقشه حرارتی ریسک‌های سازمانی (شکل 5) و نتایج حاصل از ارزیابی ریسک است. بر مبنای شدت ریسک، سطوح ریسک (جدول 4) تعریف می‌شود. 4 سطح ریسک برای سازمان در جدول 4 مشخص شده است. الزامات داشبورد ریسک و بازنگری آن توسط دبیر کارگروه مدیریت ریسک مشخص می‌شود.



شکل 5- نقشه حرارتی ریسک های سازمانی

سطح	عدد ریسک	رنگ	تعریف
1	25-20		ریسک با اهمیت خیلی زیاد (Very High Risk)
2	19-13		ریسک با اهمیت زیاد (High Risk)
3	12-7		ریسک با اهمیت متوسط (Medium Risk)
4	6-1		ریسک با اهمیت کم (Low Risk)

جدول 4- سطوح ریسک

در صورت تایید ریسک‌های سازمانی توسط مدیر عامل، گزارش ریسک‌های با اهمیت زیاد و استراتژی‌های پاسخ به ریسک جهت تصویب به هیئت مدیره ارسال می شود. در صورت نیاز به بازنگری گزارش ریسک‌های سازمانی و استراتژی‌های تعیین شده، مراتب به دبیر کارگروه جهت بازبینی و انجام اصلاحات لازم ارجاع می‌شود.

5-5. تصویب و ابلاغ استراتژی پاسخ به ریسک

هیئت مدیره شرکت در خصوص موارد ذیل تصمیم‌گیری می‌نماید:

- تخصیص منابع لازم برای حفظ و نگهداشت ریسک در محدوده اشتهای ریسک
- تصویب استراتژی‌های پاسخ به ریسک

استراتژی‌های مصوب در هیات مدیره، توسط دبیر کارگروه به کلیه مالکین ریسک، ذینفعان، مدیریت‌ها و شرکت‌های فرعی جهت کنترل و پایش فرآیند مدیریت ریسک ابلاغ می‌شود.

5-6. برنامه‌ریزی، اجرا و گزارش‌دهی اقدامات پاسخ به ریسک

مالکین ریسک برنامه های اجرایی مناسب با استراتژی های پاسخ را تنظیم و پس از اخذ تایید کارگروه اجرا می‌نمایند. گزارش پیشرفت اقدامات اجرایی برای استراتژی های کاهش و اشتراک ریسک به صورت ادواری (هر سه ماه یکبار) به دبیر کارگروه جهت طرح در جلسات کارگروه مدیریت ریسک و تهیه گزارش خلاصه مدیریتی (جهت مدیر عامل/هیات مدیره) و دریافت بازخورد ارسال می‌شود. بازخوردهای مدیریتی اخذ شده از مدیر عامل/هیات مدیره، توسط دبیر کارگروه به مالکین ریسک ابلاغ می‌شود.

5-7. کنترل و پایش ریسک‌ها

ریسک‌های سازمانی باید همواره تحت کنترل بوده و پایش شوند. مالکین ریسک با ملحوظ نمودن بازخوردهای مدیریتی اصلاحات لازم جهت دستیابی به ریسک باقیمانده هدف را انجام می‌دهند. نهایتا ریسک باقیماندهٔ واقعی در دوره‌های زمانی سه ماهه ، محاسبه و ثبت می‌شود. در صورت عدم اثربخشی اقدامات تعیین شده (با توجه به ریسک باقیمانده هدف) ممکن است مجددا اقدامات کنترلی بیشتر تعریف و اجرا شود. مالکین ریسک موظفند اثربخشی اقدامات اجرایی جهت کاهش عدد ریسک‌های باقیمانده را کنترل و نتایج آنرا به دبیر کارگروه مدیریت ریسک گزارش نمایند.

ریسک‌های باقیمانده واقعی طبق جدول 5 تحت کنترل قرار می‌گیرند. طبق این جدول، شدت ریسک بزرگتر یا مساوی 20 در ناحیهٔ غیرقابل پذیرش، شدت ریسک کوچکتر از 20 و بزرگتر از 6 در ناحیهٔ **ALARP** [1] ونمرهٔ اولویت کوچکتر از 6 در ناحیهٔ قابل پذیرش است.

محدوده شدت اثر ریسک	نحوهٔ برخورد شرکت با ریسک
غیرقابل پذیرش (نمره ریسک≥20)	اعمال کنترل ونظارت‌های جدید و بازنگری روش کاهش ریسک ضروری است.
ALARP (20>نمره>6)	کنترل و پایش مستمر ریسک ضروری است.
قابل پذیرش نمره ≤6	درحال حاضر،کنترل /نظارت بیشتری مورد نیاز نیست. و کنترل /نظارتهای موجود باید استمرار یابد.

جدول 5 – سنجش ریسک

5-8. پایش، بازبینی و بهبود مستمر عملکرد مدیریت ریسک سازمانی

این بخش به پایش، بازبینی و بهبود مستمر عملکرد اجزای مدیریت ریسک سازمانی در گذر زمان و در اثر تغییرات معنی‌دار محیطی (داخلی و بیرونی) می‌پردازد. ورودی های مرتبط با تغییرات محیطی از **فرایند توسعه استراتژی ها و مدل کسب و کار** دریافت و همچنین خروجی های پایش عملکرد مدیریت ریسک به منظور **بازبینی اهداف و استراتژی‌ها در فرایند مذکور** بهره برداری خواهد گردید. این پایش و بازبینی مشتمل بر موارد ذیل خواهد بود:

- بازبینی رویدادهای موثر بر وقوع ریسک (مطابق بند 5-3-2)
- بازبینی نحوه اولویت‌بندی ریسک‌ها
- بازنگری استراتژی پاسخ به ریسک‌ها
- بازنگری اشتهای ریسک

همچنین فرصت‌های بهبود عملکرد مدیریت ریسک می‌تواند در هر حوزه‌های ذیل رخ دهد:

1. As low as reasonably practicable

- فناوری‌های نو
- مشکلات قبلی و دروس آموخته
- تغییرات سازمانی
- اشتهای ریسک
- توسعه حوزه‌های ریسک
- کانال‌های ارتباطی
- بهینه کاوی[1]
- آهنگ تغییرات محیطی

کارگروه مدیریت ریسک به صورت سالانه اقدام به بازنگری فرآیند مدیریت ریسک می‌نماید.

6. تاریخ تصویب و اجرا

علیرضا هاشمی	فاطمه سرلک	محمد صادق عظیمی‌فر
رئیس دفتر مدیر عامل	مدیر مهندسی ساختار	مدیر عامل شرکت ملی پالایش و پخش

1. Banchmarking

منابع و مراجع

- جیمز لم، ترجمه: شرکت تامین سرمایه امید، پیاده‌سازی مدیریت ریسک سازمانی

- Committee of Sponsoring Organization of the Treadway Commission, Enterprise Risk Management: integrating with strategy and performance, 2017.

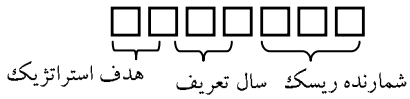
- Committee of Sponsoring Organization of the Treadway Commission, Creating and Protecting Value: Understanding and Implementing Enterprise Risk Management, 2020

- Committee of Sponsoring Organization of the Treadway Commission, Risk Appettite- Critical to Success: Understanding Risk Appetite to Thrive in Changing World, 2020

پیوست ها

الف- نحوه کدگذاری ریسک های سازمانی شناسایی شده

شماره ریسک از 6 کاراکتر تشکیل شده است. دو کاراکتر اول بیانگر هدف استراتژیک و مخفف دو حرف اول معادل انگلیسی هدف استراتژیک است. دو کاراکتر دوم نشانگر سال تعریف ریسک است و سه کاراکتر سوم بیانگر شمارنده ریسک در هدف استراتژیک می‌باشد.



ب- راهنمای بیانیه اشتهای ریسک [1]

یک بیانیه اشتهای ریسک، سیاستی تایید شده توسط هیئت مدیران است که انواع ریسک را تعریف کرده و سطوح ریسکی را تجمیع می‌نماید که یک سازمان به منظور دست یابی به اهداف خود قادر به پذیرش آنها است. سازمان باید موضع خود در قبال ریسک را در بیانیه اشتهای ریسک مشخص کند. همچنین باید اشتهای مختلفی که برای هر یک از حوزه‌های مختلف کسب و کار وجود دارد را تعیین نماید. بعنوان مثال ممکن است شرکت برای انطباق با قانون گذاری، ریسک گریز و برای توسعه صادرات فرآورده‌های نفتی و افزایش تولید ریسک‌پذیر باشد. این بیانیه شامل عبارات کیفی و همچنین معیارهای کمی و حدود در معرض ریسک خواهد بود.

چارچوب اشتهای ریسک باید شامل عناصر زیر باشد:

- ظرفیت ریسک (تحت عنوان ظرفیت تحمل ریسک هم شناخته می‌شود) نشان‌دهنده توانایی کل شرکت برای جذب و تحمل زیان‌های بالقوه است.
- پروفایل ریسک
- آستانه تحمل ریسک
- رویکردهای ریسک

مراحل تعیین چارچوب اشتهای ریسک

1. **تعیین زمینه اشتهای ریسک:** درک و شناخت جایگاهی است که سازمان در حال حاضر در محیط داخلی و خارجی خود قرار گرفته است.

1 Risk appetite statement

2. **تعیین اهداف استراتژیک سازمانی:** مولفه کلیدی اهداف سازمانی، شناخت محرک های این اهداف، بهره ی ذینفعان کلیدی و انتظارات آنها است. با تغییر استراتژی سازمان؛ اشتهای ریسک باید مورد بازبینی قرار گیرد تا تایید کند که اشتها ی ریسک از دستیابی به اهداف سازمان حمایت خواهد کرد.
3. **یکپارچه‌سازی اشتهای ریسک با استراتژی‌های کسب و کار و مدیریت سرمایه**
4. **بیان اشتهای ریسک در حدود عملیاتی**
5. **تعیین آستانه‌های ریسک**

ج- استراتژی‌های پاسخ به ریسک

1- اجتناب از ریسک و جلوگیری از بروز ریسک [1]

در این استراتژی اجتناب، بهره ی انجام ندادن فعالیتی که باعث ریسک می‌شود. به‌عنوان مثال ورود به یک کسب و کار مورد چشم پوشی قرار گیرد، تا از مشکلات آنها اجتناب شود. بجز حالتی که سازمان اشتهای ریسک پایینی داشته باشد انتخاب این استراتژی بسیار سخت می‌باشد. درس آموخته‌های قبلی از تجارب گذشته می‌تواند برای انتخاب این استراتژی مفید باشد.

2- کاهش ریسک [2]

استراتژی کاهش، بهره ی به‌کارگیری شیوه هایی که باعث کاهش شدت زیان می‌شود. این استراتژی زمانی کابرد دارد که شدت ریسک بیش از اشتها ی ریسک می‌باشد. ریسک‌های سازمان می‌تواند به سطح مشخصی کاهش یابد. به‌عنوان مثال می توان به تنوع محصولات تولیدی و تنوع سبد مصرف سوخت برای کاهش اتکای به یک فرآورده و کاهش ریسک تقاضا اشاره کرد .برخی اقداماتی که برای کاهش ریسک صورت می‌گیرد می‌تواند شامل سرمایه‌گذاری در:

- استراتژی: تدوین یک استراتژی جدید یا اهداف جدید برای کاهش ریسک
- کارکنان: ایجاد تیم کاری جدید به منظور خلق نوآوری‌های جدید یا برگزاری دوره‌های آموزشی و یا حمایت از پژوهش‌ها و مطالعات و توسعه تکنولوژی‌های جدید

1.Risk avoidance
2.Risk reduction

- فرآیندهای کاری: ایجاد مجموعه قوانین رفتاری[1] جدید در سازمان یا واحد برای تدوین استانداردهای کاری، دستورالعمل‌های و روش‌های جدید
- سیستم‌ها: استقرار سیستم‌های مدیریتی برای پایش منظم و مستمر ریسک با توجه به مجموعه قوانین رفتاری یا استانداردهای مناسب

3- پذیرش ریسک[2]

استراتژی پذیرش، یعنی اقدامی برای کاهش ریسک انجام نمی‌شود. این استراتژی زمانی کاربرد دارد که ریسک در محدوده ریسک قابل پذیرش و یا کمتر از اشتهای ریسک می‌باشد. در واقع خود-تضمینی یا تضمین شخصی در این طبقه جای می‌گیرد. پذیرش ریسک یک استراتژی قابل قبول برای ریسک‌های کوچک است که هزینه حفاظت در مقابل ریسک ممکن است از نظر زمانی بیشتر از کل زیانهای حاصله باشد. کلیه ریسک‌هایی که قابل اجتناب و اشتراک نیستند، ضرورتاً قابل پذیرش هستند. اینها شامل ریسک‌هایی می‌شود که خیلی بزرگ هستند که یا محافظت در مقابل آن امکان پذیر نیست یا پرداخت هزینه بیمه آن شانس عملی نباشد. در این زمینه، جنگ به خاطر ویژگیهایش و عدم وجود تضمین نسبت به ریسک‌هایش، مثالی مناسبی است.

4- اشتراک ریسک[3]

در این استراتژی بخش یا تمام مالکیت ریسک به عامل سوم که توانایی بهتری در استفاده از فرصت دارد منتقل می‌شود. بطور مثال در بسیاری از موارد در هنگام عقد قرارداد با پیمانکاران این استراتژی اعمال می شود. واقعیت این است که انتقال مالکیت ریسک به پیمانکاران (عامل سوم) تضمینی بر بهره برداری کامل از ریسک نمی‌باشد در این وضعیت نیز پروژه باید از وجود سیستم کارآمد در شرکت پیمانکار به منظور برخورد مناسب با ریسک اطمینان حاصل نماید. در بعضی متون از اشتراک ریسک به عنوان انتقال ریسک[4] نیز نام برده شده است.

1.Code of conduct
2.Risk acceptance
3.Risk sharing
4.Risk transfer

د- فرم شناسایی ریسک

مشخصات ریسک																
نام ریسک:	حوزه و جنس ریسک			منبع ریسک												
کد ریسک:	☐ راهبردی ☐ عملیاتی ☐ گزارشگری/مالی ☐ تطبیقی			شرکت	مدیریت	محیط بیرونی										
مالک ریسک:																
ریسک ذاتی				اشتهای ریسک												
احتمال ریسک (P)	پیامد ریسک (I)	شدت ریسک (P×I)	شاخص کلیدی ریسک KRI			اولویت ریسک										
			معیار	شاخص												
		1														
شرح ریسک (عوامل تحریک، زمان وقوع و شدت ریسک، عوامل تشدید، تبعات وقوع):																
استراتژی پاسخ به ریسک	☐ اجتناب از ریسک ☐ پذیری ریسک		☐ کاهش ریسک ☐ اشتراک ریسک	بودجه پاسخ		هزینه پاسخ										
منابع مورد نیاز																
تهیه کننده	تایید کننده					تصویب کننده										
نام و نام خانوادگی	نام و نام خانوادگی					نام و نام خانوادگی										
تاریخ و امضا	تاریخ و امضا					تاریخ و امضا										