



روش اجرایی مدیریت ریسک سازمانی

شماره: ۲۱۱۰۱۰۵/۱

شرح بازنگری	تاریخ تصویب / بازنگری
	۱۴۰۰/۰۳/۰۹
بازنگری ساختار و مسئولیت ها	۱۴۰۲/۰۸/۲۱
انطباق با آیین نامه انتظام بخشی، شفاف سازی و ضابطه مندی سازی درآمدها و هزینه های شرکت های دولتی	۱۴۰۴/۰۵/۰۶



فهرست

۶	مقدمه.....
۶	۱. هدف.....
۷	۲. دامنه کاربرد.....
۷	۳. تعاریف.....
۷	۱-۳. سازمان.....
۷	۲-۳. عدم قطعیت.....
۷	۳-۳. ریسک.....
۷	۴-۳. مدیریت ریسک سازمانی.....
۸	۵-۳. احتمال وقوع ریسک.....
۸	۶-۳. شدت اثر ریسک.....
۸	۷-۳. اشتهای ریسک.....
۹	۸-۳. چارچوب مدیریت ریسک سازمانی.....
۹	۹-۳. بیانیه اشتهای مدیریت ریسک.....
۹	۱۰-۳. ریسک قابل پذیرش.....
۱۰	۱۱-۳. ریسک ذاتی.....
۱۰	۱۲-۳. ریسک باقیمانده هدف.....
۱۰	۱۳-۳. ریسک باقیمانده واقعی.....
۱۰	۱۴-۳. پروفایل ریسک.....
۱۰	۱۵-۳. ذینفعان.....
۱۱	۱۶-۳. مالک ریسک.....
۱۱	۴. ساختار و مسئولیت‌ها.....
۱۱	۱-۴. ساختار مدیریت ریسک.....
۱۱	۲-۴. مسئولیت‌ها.....
۱۶	۵. مراحل اجرایی مدیریت ریسک سازمانی.....
۱۶	۱-۵. نمودار ارتباطات فرآیندی.....
۱۸	۲-۵. تنظیم بیانیه اشتهای ریسک.....
۱۸	۳-۵. تشکیل پروفایل ریسک.....
۲۳	۴-۵. تنظیم داشبورد مدیریت ریسک.....

۲۴	۵-۵. تصویب و ابلاغ استراتژی پاسخ به ریسک
۲۵	۶-۵. برنامه‌ریزی، اجرا و گزارش دهی اقدامات پاسخ به ریسک
۲۵	۷-۵. کنترل و پایش ریسک‌ها
۲۶	۸-۵. پایش، بازبینی و بهبود مستمر عملکرد مدیریت ریسک سازمانی
۲۸	۶. تاریخ تصویب و اجرا
۲۹	منابع و مراجع
۳۰	پیوستها
۳۰	الف- نحوه کدگذاری ریسک‌های سازمانی شناسایی شده
۳۰	ب- راهنمای پیانیه اشتباهی ریسک
۳۱	ج- تعیین آستانه‌های ریسک
۳۱	استراتژی‌های پاسخ به ریسک
۳۱	۱- اجتناب از ریسک و جلوگیری از بروز ریسک
۳۱	۲- کاهش ریسک
۳۲	۳- پذیرش ریسک
۳۲	۴- اشتراک ریسک
۳۴	د- فرم شناسایی ریسک

فهرست اشکال

۸	شکل ۱- نقشه اشتباهی ریسک.....
۱۱	شکل ۲- ساختار غیرموظف مدیریت ریسک.....
۱۷	شکل ۳- مراحل فرآیند مدیریت ریسک.....
۱۹	شکل ۴- ساختار شکست ریسک.....
۲۴	شکل ۵- نقشه حرارتی ریسک‌های سازمانی.....

فهرست جداول

جدول ۱ - شدت اثر ریسک.....	۲۰
جدول ۲ - احتمال وقوع ریسک.....	۲۰
جدول ۳ - سطوح تصمیم‌گیری.....	۲۱
جدول ۴ - سطوح ریسک.....	۲۴
جدول ۵ - سنجش ریسک.....	۲۵



مقدمه

مدیریت ریسک سازمانی، روشی سیستماتیک برای مدیریت ریسک‌های سازمان به صورت سازگار و همراستا با استراتژی‌های سازمان فراهم نموده و بر خلق، حفظ و توسعه ارزش اثر گذار خواهد بود. روش اجرایی مدیریت ریسک سازمانی^۱ بدنبال ارائه راهنما به منظور تبیین چگونگی بکارگیری مدیریت ریسک جامع و یکپارچه است. سند پیش‌رو، که منطبق با چارچوب کوزو^۲ طراحی و تنظیم گردیده است، فعالیت‌های کلیدی مورد نیاز برای یک رویکرد مدیریت ریسک موثر را شناسایی می‌کند.

۱. هدف

هدف از تدوین این روش اجرایی حصول اطمینان از مدیریت اثر بخش ریسک‌های سازمانی (شامل شناسایی، تحلیل، ارزیابی و برخورد با ریسک) بصورت سیستماتیک در جهت کاهش اثرات منفی، تهدیدها یا از دست دادن فرصت‌ها، دستیابی به اهداف سازمانی و نهایتاً برخورداری از مزایای مدیریت ریسک است.

مزایای مدیریت ریسک عبارتند از:

- فراهم ساختن یک رویکرد سیستماتیک برای شناسایی و مدیریت ریسک؛
- ارتقای تاب‌آوری^۳ بنگاه
- آمادگی پاسخگویی بموقع و موثر به رویداد های احتمالی
- افزایش دامنه فرصت‌ها
- افزایش نتایج و مزیت‌های مثبت ضمن کاهش اثرات منفی
- ثبات عملکرد و کاهش انحرافات عملکردی
- بهبود به کارگیری منابع

^۱. Enterprise risk management

^۲. COSO

^۳. Resilience



۲. دامنه کاربرد

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

۳. تعاریف

۳-۱. سازمان

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

۳-۲. عدم قطعیت^۱

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 در صورت وقوع، اثرات مثبت یا منفی بر منابعی چون زمان، هزینه و کیفیت خواهند داشت.

۳-۳. ریسک

ریسک متغیری است از احتمال و پیامد ناشی از وقوع یک رخداد در آینده 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 تأثیر خود قرار دهد. ریسک را می‌توان احتمال وقوع یک واقعه ضرب در اثر آن تعریف کرد.

۳-۴. مدیریت ریسک سازمانی^۲

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

^۱. Uncertainty

^۲. Enterprise risk management

۵-۳. احتمال وقوع ریسک^۱

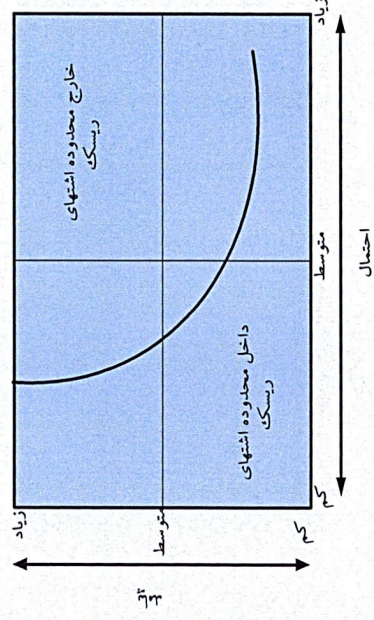
مقیاس کمی امکان وقوع یک رویداد (ریسک) است که به صورت درصد و یا به گونه جامع‌تر به صورت نمودار توزیع احتمالی بیان می‌شود.

۶-۳. شدت اثر ریسک^۲

مقیاس کمی 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.

۷-۳. اشتهای ریسک^۳

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 ۱ 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



شکل ۱- نقشه اشتهای ریسک

اثر منفی (زیاد) یا رویداد با احتمال زیاد و اثر کم را می‌پذیرد. فلسفه مدیریت ریسک و تاثیر آن بر فرهنگ سازمان در سندی به عنوان سند بیانیه اشتهای ریسک منتشر می‌شود.

۱. Probability of risk
۲. Severity of risk
۳. Risk appetite

۸-۳. چارچوب مدیریت ریسک سازمانی^۱

چارچوب مدیریت ریسک سازمانی برگرفته از چارچوب کوزو و ویرایش ۲۰۱۷ و شامل ۳ جزء به

شرح ذیل است:

- **استراتژی و هدف‌گذاری:** فرآیند مدیریت ریسک سازمان و فرآیند توسعه استراتژی، سیاست‌های

حاکمیتی و مدل کسب و کار در کنار هم عمل می‌کنند.

- **عملکرد:** سازمان ریسک‌هایی که بر تحقق استراتژی و اهداف تاثیر می‌گذارد را شناسایی و ارزیابی

می‌کند. ریسک‌های سازمان بر مبنای شدت آنها و اشتباهی ریسک اولویت‌بندی می‌شود. سازمان

پاسخ به ریسک‌ها را انتخاب و اقدامات انجام شده برای تغییرات را پایش می‌کند. به این طریق

دیدگاه پورتنوی^۳ برای میزان ریسکی که سازمان در مسیر استراتژی و اهداف خود متحمل شده

است توسعه می‌یابد.

- **بازبینی و بازنگری:** با بازبینی عملکرد مدیریت ریسک، سازمان می‌تواند بررسی کند عملکرد

مدیریت ریسک چقدر توانسته در طی زمان ارزش ایجاد کند و چه تغییرات اصلاحی مورد نیاز

است.

۹-۳. بیانیه اشتباهی مدیریت ریسک^۵

بیانیه اشتباهی ریسک، سیاستی تایید شده توسط هیئت مدیره است که انواع 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 اشتباهی ریسک در پیوست ب اشاره شده است.

۱۰-۳. ریسک قابل پذیرش^۶

ریسک قابل پذیرش به سطح ریسک قابل قبول جهت دستیابی به هدف تعریف شده اطلاق می‌گردد. این

سطوح حدود آستانه کمی هستند که اشتباهی ریسک سازمان را به انواع بخصوصی از ریسک واحدهای

کسب و کار نسبت می‌دهد. با توجه به اهداف مختلف، ریسک قابل پذیرش نیز ممکن است متفاوت باشد.

۱. Enterprise risk management framework

۲. Performance

۳. Portfolio View

۴. Review and revision

۵. Risk appetite statement

۶. Acceptable risk



بطور مثال برای تغییرات درآمدی، مواجهه با نرخ بهره، تطابق با قوانین و مقررات و ... ریسک قابل پذیرش متفاوت خواهد بود.

توجه: اشتباهات ریسک و ریسک قابل پذیرش تفاوت دارند. اشتباهات 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.

۱۱-۳. ریسک ذاتی^۱

عاملی که بدون هیچ اقدام مدیریتی می‌تواند بر احتمال و یا پیامد ریسک اثر گذارد، منجر به پیدایش ریسک ذاتی می‌گردد. در صورتی که هیچ اقدامی برای کنترل یا رویارویی با آن انجام نشود می‌تواند سازمان را در دستیابی به اهدافش با محدودیت مواجه نماید.

۱۲-۳. ریسک باقیمانده هدف^۲

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

۱۳-۳. ریسک باقیمانده واقعی^۳

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

۱۴-۳. پروفایل ریسک^۲

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 پوررتفوی 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.

۱۵-۳. ذینفعان

در مقوله ریسک، ذینفع کسی است که بر احتمال وقوع و شدت اثر یک ریسک می‌تواند اثر بگذارد و یا از آن اثر بپذیرد.

ذینفعان ریسک تعریف محدودتری دارند و با تعریف ذینفعان سازمان متفاوت است.

^۱. Inherent risk

^۲. Target residual risk

^۳. Actual residual risk



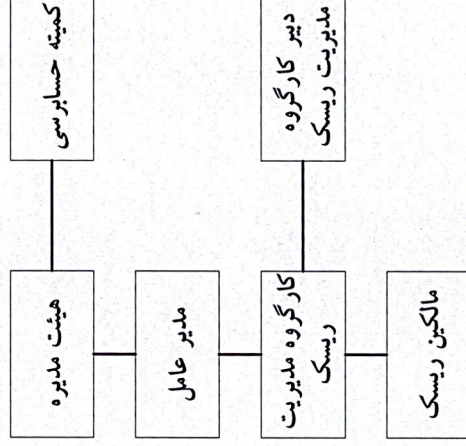
۳-۱۶. مالک ریسک^۱

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.

۴. ساختار و مسئولیت‌ها

۴-۱. ساختار مدیریت ریسک

ساختار غیر موظف مدیریت ریسک در شکل ۲ ترسیم شده است.



شکل ۲- ساختار غیرموظف مدیریت ریسک

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

۴-۲. مسئولیت‌ها

۴-۲-۱- هیئت مدیره شرکت

- تصویب سند بیانیه اشتباهات ریسک

- تصویب راهبردها و سیاست های کلی مدیریت ریسک و استراتژی های پاسخ به ریسک
- پایش کلان و تعیین جهت گیری های سازمان با توجه به گزارش های دوره ای و بازخوردهای لازم
- تخصیص منابع مورد نیاز مدیریت ریسک

۲-۲-۴. مدیر عامل

- حصول اطمینان از این که سازمان از اصول مناسبی برای شناسایی، ارزیابی، پایش، گزارش دهی، کاهش و کنترل ریسک استراتژیک استفاده می کند.

- حصول اطمینان از اطلاع رسانی و بکارگیری فرهنگ آگاهی از ریسک در سازمان

- حصول اطمینان از همسوسازی رفتارها و تصمیم گیری مبتنی بر ریسک با عملکرد سازمان

- نظارت بر فعالیت کارگروه مدیریت ریسک سازمانی

- ابلاغ بیانیه اشتباهی ریسک

- تأیید گزارش کنترل و پایش ریسک جهت ارایه به هیئت مدیره

- حصول اطمینان از این که اطلاعات شفاف، جامع، مرتبط، قابل اعتماد، قیاس پذیر و مهم مربوط به

حوزه های مختلف کاری سازمان به موقع، در اختیار افراد قرار می گیرد.

- تصویب و ابلاغ دستورالعمل های تخصصی

۳-۲-۴. 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:

- سیاست گذاری و تعیین خط مشی های شرکت در حوزه ریسک
- استقرار فرآیندهای شناسایی، ارزیابی، تجزیه و تحلیل و پاسخ به ریسک
- وجود فرآیندها و سامانه های الزام برای گزارش دهی ریسک های شرکت
- مدیریت موثر ریسک ها و اطمینان معقول از دستیابی به اهداف و ارزش های اصلی شرکت
- تعیین اشتباهی ریسک شرکت



این کارگروه متشکل از مدیران برنامه‌ریزی تلفیقی، هماهنگی و نظارت بر عملیات، بهداشت، ایمنی، محیط زیست و پدافند غیرعامل، حقوقی، بازرگانی، پژوهش و فناوری، امور مصرف، متنوع‌سازی سبدساخت و پیشگیری از قاچاق 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 تدوین و راهبری ریسک (در ساختار سازمانی پیشنهادی لحاظ شده است) می‌باشد. در صورت نیاز و با توجه به طبقه‌بندی ریسک از سایر مدیریت‌ها و واحدهای بلافصل مدیر عامل 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 نماید. 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 ریسک‌های شرکت بر حسب درجه ریسک‌پذیری و اشتباهی ریسک تعیین شده
- هیئت مدیره و در صورت لزوم ارابه 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 اجرای شناسایی شدن ریسک‌های هر اداره/مدیریت توسط مالکین ریسک‌ها
- شناسایی نارسایی‌های موجود در مدیریت ریسک جهت طرح در هیئت مدیره
- حصول اطمینان معقول از عدم همپوشانی و شکاف‌های 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 ریسک‌های شرکت از قبیل مالی و اعتباری، حقوقی و قانونی، راهبردی و تجاری، عملیاتی، ریسک‌های مربوط به تکنولوژی، فناوری اطلاعات و ارتباطات به هیئت مدیره
 - بررسی عملکرد، پایش دوره‌ای برنامه یا چارچوب مدیریت ریسک شرکت و ارزیابی اثربخشی آن و ارایه گزارش به هیئت مدیره
 - استفاده از بسترهای لازم جهت دریافت گزارش‌ها و موضوعات مرتبط با ریسک از کلیه ذینفعان شرکت
 - ایجاد بانک اطلاعاتی سیستماتیک و جامع از ریسک‌های شناسایی شده در سازمان از ابتدای شروع فرآیند بررسی و شناسایی ریسک‌ها بمنظور تسهیل دسترسی اعضای کارگروه و همچنین تهیه درس آموخته‌های مربوط به راهکارهای موفق مقابله با ریسک‌های تأیید شده
 - سایر موارد به تشخیص هیئت مدیره شرکت
- هیئت مدیره شرکت در چارچوب مسئولیت‌های کارگروه ریسک به آن اختیارات ذیل را می‌دهد:
- 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 ریسک‌های شرکت
 - سایر اختیارات به تشخیص هیئت مدیره شرکت

۴-۲. دبیر کارگروه مدیریت ریسک

دبیر کارگروه وظایف و مسئولیت‌های زیر را بر عهده دارد:

- تشكيل جلساء كارءروه
- هءاءاء، راهبرى و ءببرى جلساء كارءروه و پىءبرى اخء اسءاء راهبرى (شامل سءء اسءراءئزى شرءك، سىاسءهاى ءاكمىءى و الزاماء و مءقرراء رءءلاءئورى و ...)
- ءهپه و بروزآورى ءاءبوءرء مءبرىء رىسك ساءامان
- اخء و ءءللل ءراءش هاى رىسك/پاءش رىسك از مالكىن
- ءكمبل بروفائل رىسك و نءءءاءرى ءاءه هاى ءمع آورى شءه براءى شناسائى رىسك
- بربرسى، ءنظىم و بازنءبرى روش اءراءى مءبرىء رىسك
- ءنظىم ءراءش مءبرىء رىسك ءءء اراءه به مءبرءامل/هفاء مءبره
- بربرسى و ءنظىم ءسءورءعمل هاى ءءءصصى

۵-۲-۴. مءوليان/ مالكىن رىسك

مالك رىسك مسءولفاء هاى ذبل را بر عهءه ءارء:

- مطالعه و بربرسى فضاء ساءامان و اسءاء راهبرى
- ءمع آورى ءاءه هاى اءلاءاءى از منابع مءءءف براءى شناسائى رىسك
- شناسائى، ءءللل، ارزىابى، اولوءبءبءى و ءعىن اسءراءئزى ها و بربنامه هاى مءابله با رىسك ءر ءوزه كارى مربوءه (ءهپه بروفائل رىسك)
- ءهپه و بازنءبرى ءسءورءعمل ءءءصصى مءبرىء رىسك ءر ءوزه مربوءه (ءسب نىاز)
- بازنءبرى رىسك و شناسائى منابع و روبءاءه هاى ءءبء
- بربنامه ربزى اءءاماء اءراءى و ءراءش ءهى بربنامه ها و اءءاماء مءابله با رىسك
- ءءللل علل ءءم اءرا يا ءءم اءربءش اءءاماء مربءب با رىسك
- تشكيل كارءروه هاى فرعى مءبرىء رىسك با ءعوء از كلبه شرءءها/ مءبرىءءها/واءءه هاى مربءب و موءر برب رىسك هاى مربوءه (ءسب نىاز)



۶-۲-۴. حسابرسی داخلی

- ارائه گزارش اثربخشی سیستم‌های کنترل داخلی شرکت شامل کنترل فناوری اطلاعات و حفظ

امنیت آن‌ها

- کسب اطمینان معقول از کفایت دامنه بررسی حسابرسان داخلی از نظام کنترل‌های داخلی شرکت
- کسب اطمینان معقول از اثربخشی فرآیند مدیریت ریسک مشتمل بر شناسایی، اندازه‌گیری، تجزیه و تحلیل، ارزیابی، مدیریت و نظارت بر سیستم مدیریت ریسک
- بررسی ارزیابی حسابرس داخلی از کنترل‌های داخلی و اظهار نظر حسابرس مستقل نسبت به

کنترل‌های داخلی

- پیگیری اجرای توصیه‌ها و رفع نقاط ضعف کنترل‌های داخلی که توسط حسابرسان داخلی و یا مستقل به کارگروه گزارش می‌شود.

- ارائه گزارش کنترل‌های داخلی به هیئت مدیره شامل ارزیابی و اظهار نظر نسبت به کنترل‌های

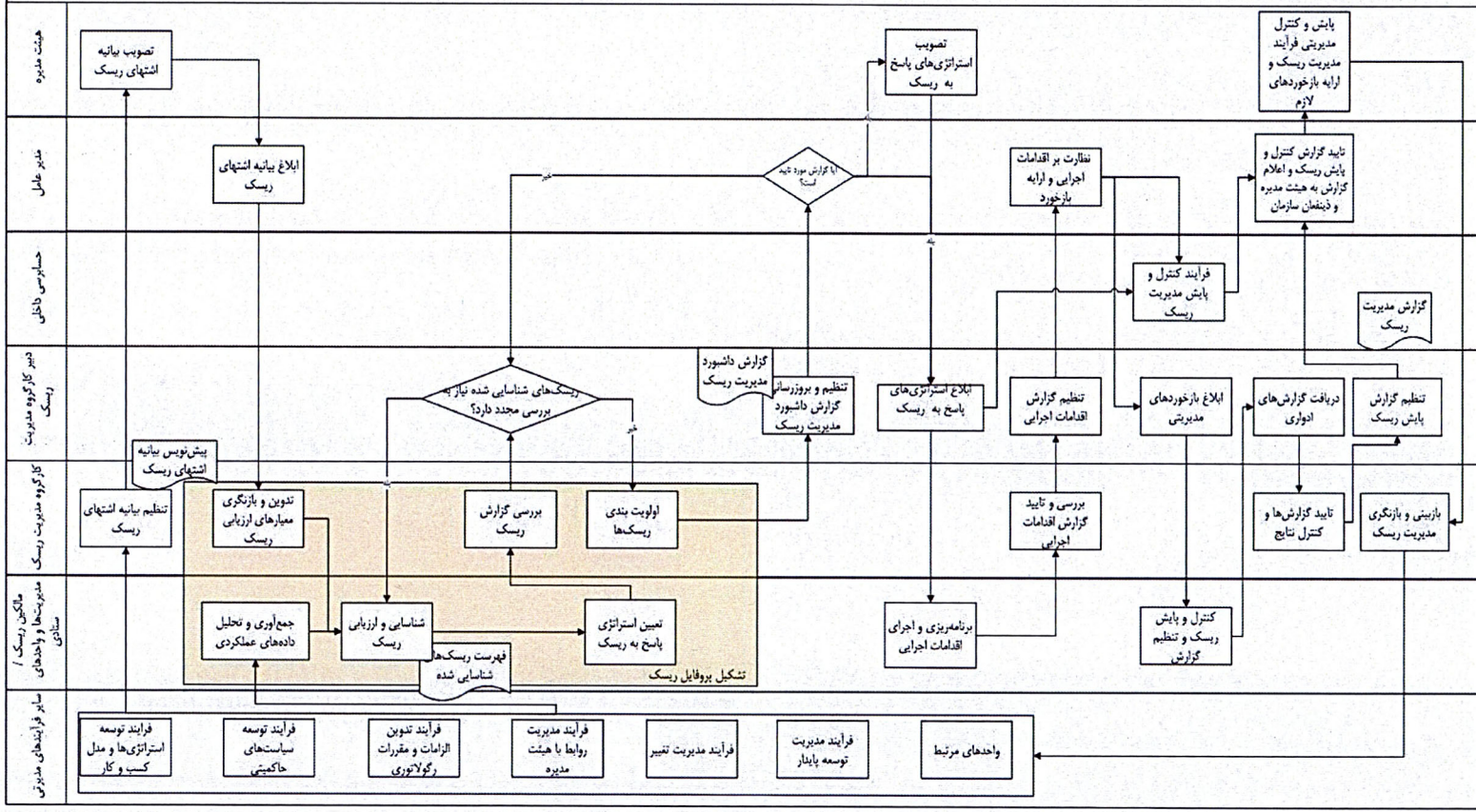
داخلی شرکت‌های فرعی

۵. مراحل اجرایی مدیریت ریسک سازمانی

۱-۵. نمودار ارتباطات فرآیندی

شکل ۳ نمودار ارتباطات فرآیندی مدیریت ریسک سازمانی را نشان می‌دهد.

فرآیند مدیریت ریسک



شکل ۳- مراحل فرآیند مدیریت ریسک

۲-۵. تنظیم بیانیه اشتباهی ریسک

کارگروه مدیریت ریسک، پیش‌نویس بیانیه اشتباهی ریسک را در ارتباط با خلق، حفظ و درک ارزش‌های سازمان تنظیم می‌نماید. راهنمای تدوین بیانیه اشتباهی ریسک در پیوست ب- ارائه شده است. پیش‌نویس بیانیه اشتباهی 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 اشتباهی ریسک سازمان تصمیم‌گیری نماید. بیانیه اشتباهی ریسک به صورت سالیانه یا در اثر تغییر سند استراتژیک بازنگری و توسط مدیر عامل ابلاغ می‌گردد.

۳-۵. تشکیل پروفایل ریسک

۱-۳-۵. 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.

۲-۳-۵. جمع‌آوری و تحلیل داده‌های عملکردی

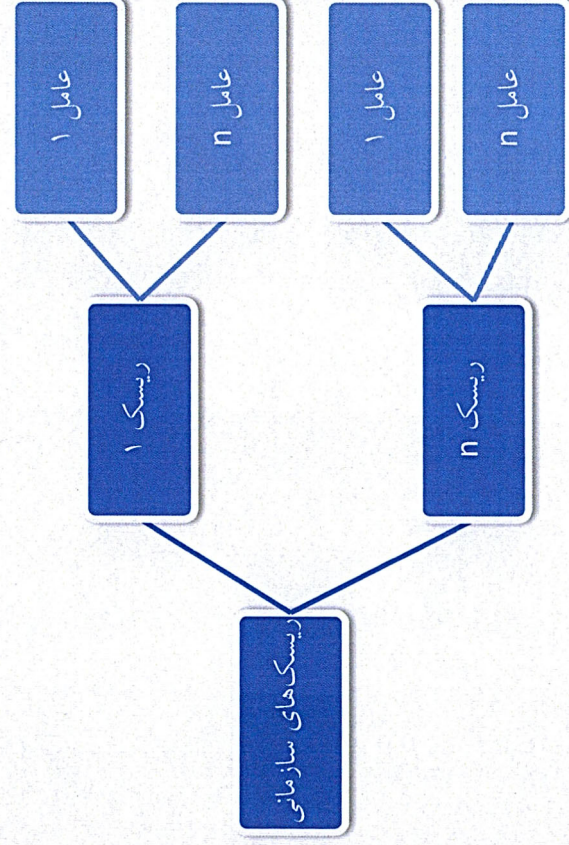
در این مرحله مالکین ریسک با ردیابی داده‌های ناشی از وقوع رویدادهای گذشته و تأثیرات آن بر اهداف استراتژیک درک بهتری از ریسک‌های موثر بدست می‌آورند. مالکین ریسک یک پایگاه داده زیان/رویداد برای ثبت کلیه زیان‌ها و رویدادهای اساسی را ایجاد می‌کنند. این پایگاه داده بصورت مداوم توسط مالکین ریسک توسعه می‌یابد. سوابق تاریخی تأثیرات 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 ۵ ساله
- تغییرات در فرآیندهای کاری و عملیات جاری مانند تغییر در تکنولوژی و بهره‌برداری 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^۱
- وقایع و رویدادهای طبیعی
- رویدادهای سیاسی
- عوامل اجتماعی

برای پشتیبانی از تصمیمات آگاه از ریسک^۲ داده‌های با کیفیت حفظ و نگهداری می‌شود. دبیر کارگروه مدیریت ریسک و مالکین ریسک باید اطمینان حاصل کنند داده‌ها و اطلاعات استاندارد شده‌ی با کیفیت به‌نگام و بی‌وقفه^۳ 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.

۳-۳-۵. شناسایی و ارزیابی ریسک
سازمان ریسک‌هایی که بر عملکرد استراتژی‌ها و هدف‌گذاری تلدین شده تاثیر می‌گذارد را شناسایی می‌کند. ساختار نمونه‌ای شکست ریسک^۴ (RBS) در شکل ۴ نشان داده شده است. مالکین ریسک می‌باید 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 می‌شود.



شکل ۴- ساختار شکست ریسک

۱. External economic events
۲. Risk-aware
۳. Real-time
۴. Risk breakdown structure



مالکین ریسک پس از شناسایی ریسک، اقدام به ارزیابی ریسک می‌نمایند. ارزیابی ریسک یا ارزیابی شدت ریسک، تعیین شدت ریسک با توجه به معیارهای ابلاغ شده (بند ۵-۳-۱) است. مقدار شدت ریسک بر مبنای دو عامل احتمال وقوع (P) و پیامد (I) حاصل از یک رویداد و از حاصل ضرب این دو عامل در یکدیگر تعیین می‌شود.

شدت ریسک^۱ = پیامد (I) × احتمال وقوع (P). احتمال وقوع و شدت اثر مطابق با جداول ۱ و ۲

تعیین می‌گردد.

مقیاس					معیارها
تأثیر شدید	تأثیر زیاد	تأثیر نسبی	تأثیر کم	تأثیر ناچیز	
۵	۴	۳	۲	۱	معیار ۱ N

جدول ۱- شدت اثر ریسک

فرکانس وقوع (تجربیات گذشته)	درصد احتمال	مقیاس
تا بحال در سازمان رخ نداده است.	احتمال کمتر از ۲۰ درصد وقوع رویداد	۱ خیلی کم
هر ۳ تا ۵ سال یکبار روی می‌دهد.	احتمال بین ۲۰ تا ۴۰ درصد وقوع رویداد	۲ کم
هر ۱ تا ۳ سال روی می‌دهد.	احتمال بین ۴۰ تا ۶۰ درصد وقوع رویداد	۳ متوسط
هر سال یکبار روی می‌دهد.	احتمال بین ۶۰ تا ۸۰ درصد وقوع رویداد	۴ زیاد
هر سال بیش از یکبار رخ می‌دهد.	احتمال بیش از ۸۰ درصد وقوع رویداد	۵ خیلی زیاد

جدول ۲- احتمال وقوع ریسک



۳-۴. تعیین استراتژی پاسخ به ریسک

مالکین ریسک با توجه به شدت ریسک و پیاپی اشتباهای ریسک، استراتژی پاسخ به ریسک را تعیین می‌نمایند. انتخاب استراتژی مناسب برای پاسخ به ریسک می‌تواند بر اساس یک یا چند عامل زیر باشد:

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

۴ استراتژی پاسخ به ریسک عبارتند از:

- اجتناب از ریسک و جلوگیری از بروز ریسک^۱
- کاهش ریسک^۲
- پذیرش ریسک^۳
- انتقال یا (اشتراک) ریسک^۴

مسئولیت تصویب استراتژی پاسخ به ریسک‌های^۵ شناسایی شده در سطوح مختلف مطابق جدول ۳ می‌باشد.

سطح ریسک	عدد ریسک	تصویب استراتژی پاسخ به ریسک، کنترل و پایش ریسک
۱	۲۵-۳۰	هیئت مدیره
۲	۱۹-۱۳	کارگروه مدیریت ریسک
۳	۱۲-۷	مالک ریسک
۴	۶-۱	مدیر یا رئیس واحد

جدول ۳- سطوح تصمیم‌گیری

۱. Risk avoidance
۲. Risk reduction
۳. Risk acceptance
۴. Risk sharing or Risk Transfer
۵. Risk response



جهت توضیح بیشتر به پیوست ج رجوع شود.

۵-۳-۵. تدوین و ارسال گزارش ریسک های شناسایی شده
ریسک های شناسایی شده و استراتژی های پاسخ به ریسک، توسط مالکین ریسک به دبیر کارگروه مدیریت ریسک گزارش می شود. گزارش ریسک های شناسایی شده می بایست در قالب فرم شناسایی ریسک (پیوست د) تهیه و شامل موارد ذیل است:

- ریسک های شناسایی شده و نتایج ارزیابی
- شرح ریسک
- منابع مورد نیاز
- اولویت بندی ریسک های تحت مالکیت
- استراتژی پاسخ به ریسک های شناسایی شده

۵-۳-۶. بررسی و تایید گزارش ریسک

ریسک های سازمانی در حوزه های مختلف کاری توسط دبیر کارگروه جمع آوری و در کارگروه مدیریت ریسک مطرح و بررسی می شود.

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

- تطبیق ریسک های شناسایی شده با اهداف سازمانی
- اثر گذاری و ارتباط بین رخدادهای و تاثیر وقوع یک رخداد بر ریسک های شناسایی شده و ارتباط بین آنها (تحلیل اثر رخدادی مشترک بر فرصت های پیش روی سازمان و وقوع سایر ریسک های سازمانی)

- صحه گذاری نتایج ارزیابی ریسک و تحلیل تناسب استراتژی های پاسخ به ریسک (منظور از صحه گذاری، 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^۱ برای هر یک از ریسک ها تعیین می شود. در صورت نیاز به بررسی مجدد ریسک ها، مراتب توسط دبیر کارگروه به مالکین ریسک اعلام می شود.

^۱ Acceptable risk level



۵-۳-۷. اولویت‌بندی ریسک

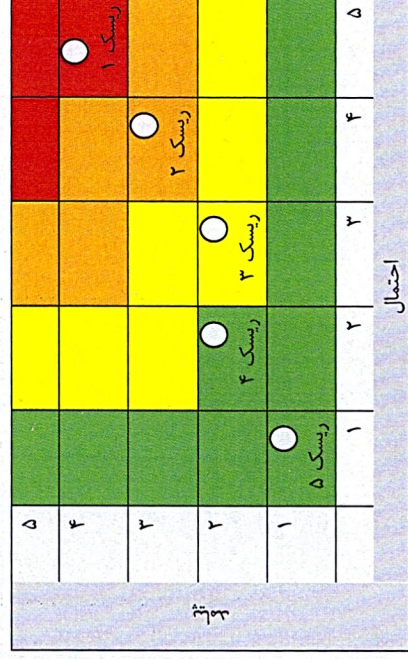
سازمان ریسک‌ها را اولویت‌بندی می‌کند تا تصمیم‌گیری درخصوص اقدامات اجرایی پاسخ به ریسک، آگاهانه انجام و تخصیص منابع بهینه‌سازی شود. با در نظر گرفتن منابع در دسترس باید موازنه بین تخصیص منابع برای واکنش به یک ریسک در مقایسه با ریسک دیگر ارزیابی شود. دبیر کارگروه پس از جمع‌گزارشات اقدام به برگزاری جلسه کارگروه مدیریت ریسک نموده و ریسک‌های مهم سازمان بر اساس معیارهای اولویت‌بندی ریسک، شناسایی می‌گردند.

معیارهای اولویت‌بندی ریسک عبارتند از:

- شدت اثر ریسک
- وفق‌پذیری: قابلیت انطباق با تغییرات پیش‌بینی 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: قابلیت بازگشت به وضعیت تحمل‌پذیر (مانند تداوم فعالیت بعد از بلایای طبیعی)

۵-۴. تنظیم داشبورد مدیریت ریسک

ریسک‌های شناسایی شده توسط دبیر کارگروه در پروفایل مدیریت ریسک سازمانی با اختصاص شماره ریسک منحصر بفرد (پوست 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 ریسک‌های موجود در سازمان ارائه می‌دهد، گزارش می‌شود. داشبورد مدیریت ریسک شامل نقشه حرارتی ریسک‌های سازمانی (شکل ۵) و نتایج حاصل از ارزیابی ریسک است. بر مبنای شدت ریسک، سطوح ریسک (جدول ۴) تعریف می‌شود. ۴ سطح ریسک برای سازمان در جدول ۴ مشخص شده است. الزامات داشبورد ریسک و بازیگری آن توسط دبیر کارگروه مدیریت ریسک مشخص می‌شود.



شکل ۵- نقشه حرارتی ریسک‌های سازمانی

سطح	عدد ریسک	رنگ	تعبیر
۱	۲۵-۲۰	Red	ریسک با اهمیت خیلی زیاد (Very High Risk)
۲	۱۹-۱۳	Orange	ریسک با اهمیت زیاد (High Risk)
۳	۱۲-۷	Yellow	ریسک با اهمیت متوسط (Medium Risk)
۴	۶-۱	Green	ریسک با اهمیت کم (Low Risk)

جدول ۴- 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 می‌شود. در صورت نیاز به بازنگری گزارش ریسک‌های سازمانی و استراتژی‌های تعیین شده، مراتب به دبیر کارگروه جهت بازبینی و انجام اصلاحات لازم ارجاع می‌شود.

۵-۵. 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 اشتباهی ریسک
- تصویب استراتژی‌های پاسخ به ریسک

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



۶-۵. برنامه‌ریزی، اجرا و گزارش دهی اقدامات پاسخ به ریسک

مالکین ریسک برنامه‌های اجرایی متناسب با استراتژی‌های پاسخ را تنظیم و پس از اخذ تایید کارگروه اجرا می‌نمایند. گزارش پیشرفت اقدامات اجرایی برای استراتژی‌های 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.

۷-۵. 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. نهایتاً ریسک باقیمانده 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 مجدداً 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 ۵ تحت کنترل قرار می‌گیرند. طبق این جدول، شدت ریسک بزرگتر یا مساوی ۲۰ در ناحیه غیرقابل پذیرش، شدت ریسک کوچکتر از ۲۰ و بزرگتر از ۶ در ناحیه^۱

ALARP و نمره اولویت کوچکتر از ۶ در ناحیه^۱ قابل پذیرش است.

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

جدول ۵- سنجش ریسک

۱. As low as reasonably practicable

۸-۵. پایش، بازبینی و بهبود مستمر عملکرد مدیریت ریسک سازمانی

این بخش به پایش، بازبینی و بهبود مستمر عملکرد اجرای مدیریت ریسک سازمانی در گذر زمان و در اثر تغییرات معنی‌دار محیطی (داخلی و بیرونی) می‌پردازد. ورودی‌های مرتبط با تغییرات محیطی از فرایند توسعه استراتژی‌ها و مدل کسب و کار دریافت و همچنین خروجی‌های پایش عملکرد مدیریت ریسک به منظور بازبینی اهداف و استراتژی‌ها در فرایند مذکور بهره‌برداری خواهد گردید. این پایش و

بازبینی مشتمل بر موارد ذیل خواهد بود:

- بازبینی رویدادهای موثر بر وقوع ریسک (مطابق بند ۵-۳-۲)
- بازبینی نحوه اولویت‌بندی ریسک‌ها
- بازنگری استراتژی پاسخ به ریسک‌ها
- بازنگری اشتباهات ریسک

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

- فناوری‌های نو
- مشکلات قبلی و دروس آموخته
- تغییرات سازمانی
- اشتباهات ریسک
- توسعه حوزه‌های ریسک
- کانال‌های ارتباطی
- بهینه‌کاری^۱
- آهنگ تغییرات محیطی

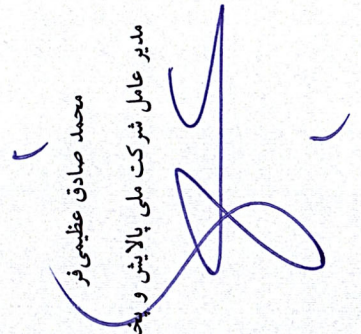
کارگروه مدیریت ریسک به صورت سالانه اقدام به بازبینی فرایند مدیریت ریسک می‌نماید.

علاوه بر کارگروه، حسابرسی داخلی می‌بایست کارایی فرآیند مدیریت ریسک را مستمرا ارزیابی و ممیزی نماید و گزارش‌های مربوطه، جهت طرح در هیئت مدیره به مدیر عامل گزارش می‌شود.

۶. تاریخ تصویب و اجرا

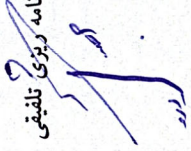
این سند توسط مدیریت مهندسی ساختار و مدیریت برنامه ریزی تلفیقی در ۶ بند تدوین و تنظیم یافته و در تاریخ **۱۴۰۴/۵/۲۸** به تصویب معاون محترم وزیر و مدیرعامل شرکت رسیده و در سطح شرکت ملی پالایش و پخش و شرکتهای فرعی و وابسته به آن لازم الاجرا می‌باشد.

محمد صادق عظیمی فر
مدیر عامل شرکت ملی پالایش و پخش



فاطمه سرلک
مدیر مهندسی ساختار

جواد بهشتی
مدیر برنامه ریزی تلفیقی



۶- ۱۴۰۴/۵/۲۸

منابع و مراجع

- جیمز لم، ترجمه: شرکت تامین سرمایه امید، پیاده‌سازی مدیریت ریسک سازمانی ۲۰۱۷.
- Committee of Sponsoring Organization of the Treadway Commission, Enterprise Risk Management: integrating with strategy and performance, ۲۰۱۷.
- Committee of Sponsoring Organization of the Treadway Commission, Creating and Protecting Value: Understanding and Implementing Enterprise Risk Management, ۲۰۲۰.
- Committee of Sponsoring Organization of the Treadway Commission, Risk Appetite- Critical to Success: Understanding Risk Appetite to Thrive in Changing World, ۲۰۲۰.



پیوست‌ها

الف- نحوه کدگذاری ریسک‌های سازمانی شناسایی شده

شماره ریسک از ۶ 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 شماره‌دهنده ریسک در هدف استراتژیک می‌باشد.

شماردهنده ریسک سال تعریف هدف استراتژیک

ب- راهنمای بیانیه اشتباهی ریسک^۱

یک بیانیه اشتباهی ریسک، سیاستی تأیید شده توسط هیئت مدیران است که انواع ریسک را تعریف کرده و سطوح ریسکی را تجمیع می‌نماید که یک سازمان به منظور دست‌یابی به اهداف خود قادر به پذیرش آنها است. سازمان باید موضوع خود در قبال ریسک را در بیانیه اشتباهی ریسک مشخص کند. همچنین باید اشتباهی مختلفی که برای هر یک از حوزه‌های مختلف کسب و کار وجود دارد را تعیین نماید. بعنوان مثال ممکن است شرکت برای انطباق با قانون‌گذاری، ریسک‌گریز 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 اشتباهی 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

^۱ Risk appetite statement



مراحل تعیین چارچوب اشتباهی ریسک

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

۲. تعیین اهداف استراتژیک سازمانی: مولفه کلیدی اهداف سازمانی، شناخت محرک‌های این اهداف، یعنی ذی‌نفعان کلیدی و انتظارات آنها است. با تغییر استراتژی سازمان؛ اشتباهی ریسک باید مورد بازبینی قرار گیرد تا تایید کند که اشتباهی ریسک از دستیابی به اهداف سازمان حمایت خواهد کرد.

۳. یکپارچه‌سازی اشتباهی ریسک با استراتژی‌های کسب و کار و مدیریت سرمایه

۴. بیان اشتباهی ریسک در حدود عملیاتی

ج- تعیین آستانه‌های ریسک- استراتژی‌های پاسخ به ریسک

۱- اجتناب از ریسک و جلوگیری از بروز ریسک
در این استراتژی اجتناب، یعنی انجام ندادن فعالیت‌هایی که باعث ریسک می‌شود. به‌عنوان مثال ورود به یک کسب و کار مورد چشم‌پوشی قرار گیرد، تا از مشکلات آنها اجتناب شود. بجز حالتی که سازمان اشتباهی ریسک پایینی داشته باشد انتخاب این استراتژی بسیار سخت می‌باشد. درس آموخته‌های قبلی از تجارب گذشته می‌تواند برای انتخاب این استراتژی مفید باشد.

۲- کاهش ریسک

استراتژی کاهش، یعنی به‌کارگیری شیوه‌هایی که باعث کاهش شدت زیان می‌شود. این استراتژی زمانی کاربرد دارد که شدت ریسک بیش از اشتباهی ریسک می‌باشد. ریسک‌های سازمان می‌تواند به سطح مشخصی کاهش یابد. به‌عنوان مثال می‌توان 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 حمایت از پژوهش‌ها و مطالعات و توسعه تکنولوژی‌های جدید
- فرآیندهای کاری: ایجاد مجموعه قوانین رفتاری^۱ جدید در سازمان یا واحد برای تدوین استانداردهای کاری، دستورالعمل‌های و رویه‌های جدید
- سیستم‌ها: استقرار سیستم‌های مدیریتی برای پایش منظم و مستمر ریسک با توجه به مجموعه قوانین رفتاری یا استانداردهای مناسب

۳- پذیرش ریسک

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 کلیه 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 شاید عملی نباشد. در این زمینه، جنگ به‌خاطر ویژگیهایش و عدم وجود تضمین نسبت به ریسک‌هایش، مثال مناسبی است.

۴- اشتراک ریسک

در این استراتژی بخش یا تمام مالکیت ریسک و مسئولیت تبعات آن به عامل سوم که دارای صلاحیت و توانایی بهتری در استفاده از فرصت دارد منتقل (برون سپاری) می‌شود. بطور مثال در بسیاری از موارد در هنگام عقد قرارداد با پیمانکاران این استراتژی اعمال می‌شود. واقعیت این است که انتقال مالکیت ریسک به پیمانکاران (عامل سوم) تضمینی بر بهره برداری کامل از ریسک نمی‌باشد در این وضعیت تیم 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 نیز نام برده شده است.

^۱. Code of conduct

این نوع ریسک‌ها را به علت این که رصد و مدیریت دائم آن‌ها می‌تواند بسیار پرهزینه باشند، می‌توان انتقال داد. این نوع ریسک‌ها، احتمال نسبتاً کم اما تأثیر زیاد در صورت وقوع دارند.

مثال دیگر خرید بیمه و اشتراک هزینه‌های زیان احتمالی با شرکت‌های بیمه‌گذار می‌باشد.

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

د- فرم شناسایی ریسک

روش اجرایی: مدیریت ریسک‌های سازمانی

