ISIRI
13245
1st. Edition

جمهوری اسلامی ایران
Islamic Republic of Iran
مؤسسه استاندارد و تحقیقات صنعتی ایران
Institute of Standards and Industrial Research of Iran

استاندارد ملی ایران
۱۳۲۴۵
چاپ اول

مدیریت ریسک – اصول و رهنمودها

Risk management — Principles and guidelines

ICS:03.100.01

به‌نام خدا

آشنایی با مؤسسهٔ استاندارد و تحقیقات صنعتی ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تن‌ها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان مؤسسه* صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیر دولتی حاصل می‌شود. پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون‌های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش نویس استانداردهایی که مؤسسات و سازمان‌های علاقه مند و ذیصلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که مؤسسه استاندارد تشکیل می‌دهد به تصویب رسیده باشد.

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران می‌تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. مؤسسه می‌تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان-ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست-محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، مؤسسهٔ استاندارد این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این مؤسسه است.

---

* موسسهٔ استاندارد و تحقیقات صنعتی ایران

1- International organization for Standardization
2 - International Electro technical Commission
3- International Organization for Legal Metrology (Organization International de Metrology Legal)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« مدیریت ریسک – اصول و رهنمودها »

رئیس:	**سمت و/ یا نمایندگی**
ذره، مهدی (کارشناسی ارشد مهندسی برق)	کارشناس استاندارد
دبیر:	
بستان دوست راد، احسان (کارشناسی مهندسی صنایع)	عضو هیات مدیره شرکت مهندسی مدیریت قابلیت اعتماد توازن
اعضاء: (اسامی به ترتیب حروف الفبا)	
اسمی خان، علی (کارشناس مهندسی مکانیک)	کارشناس
افراز، شهاب (کارشناسی مهندسی رایانه)	کارشناس شرکت مهندسی مدیریت قابلیت اعتماد توازن
حسن آبادی، سیاوش (کارشناسی ارشد زبان انگلیسی)	عضو هیات علمی دانشگاه هوایی و کارشناس استاندارد
حکیمی زاده، صدف (کارشناسی ارشد مترجمی زبان)	کارشناس شرکت مهندسی مدیریت قابلیت اعتماد توازن
راعی، جلال (فوق لیسانس مدیریت)	دانشگاه هوایی شهید ستاری عضو هیات علمی دانشکده‌ی برق
سیدی نیاکی، کیوان (کارشناسی ارشد مهندسی مکانیک)	عضو هیات علمی سازمان پژوهش‌های علمی و صنعتی ایران
قربان اشرفی، افشین (کارشناسی مهندسی برق- الکترونیک)	مدیر عامل شرکت خدمات فنی و مهندسی نهال

فهرست مندرجات

عنوان	صفحه
آشنایی با مؤسسهٔ استاندارد و تحقیقات صنعتی ایران	ب
کمیسیون فنی تدوین استاندارد	ج
پیش گفتار	و
مقدمه	ز
۱ هدف و دامنه کاربرد	۱
۲ اصطلاحات و تعاریف	۱
۳ اصول	۹
۴ چارچوب	۱۰
۴-۱ کلیات	۱۰
۴-۲ اختیار و تعهد	۱۱
۴-۳ طراحی چارچوب برای اداره‌ی ریسک	۱۲
۴-۳-۱ فهمیدن سازمان و فضا آن	۱۲
۴-۳-۲ برقراری خط مشی مدیریت ریسک	۱۳
۴-۳-۳ پاسخگویی	۱۳
۴-۳-۴ انسجام با فرآیندهای سازمان	۱۳
۴-۳-۵ منابع	۱۴
۴-۳-۶ برقراری تبادل اطلاعات داخلی و ساز و کارهای گزارش دهی	۱۴
۴-۳-۷ برقراری تبادل اطلاعات خارجی و ساز و کارهای گزارش دهی	۱۴
۴-۴ پیاده سازی مدیریت ریسک	۱۵
۴-۴-۱ پیاده سازی چارچوب برای اداره‌ی ریسک	۱۵
۴-۴-۲ پیاده سازی فرآیند مدیریت ریسک	۱۵
۴-۵ پایش و بازنگری چارچوب	۱۵
۴-۶ بهبود مداوم چارچوب	۱۶
۵ فرآیند	۱۶
۵-۱ کلیات	۱۶
۵-۲ تبادل اطلاعات و مشاوره	۱۷
۵-۳ برقراری فضا	۱۸
۵-۳-۱ کلیات	۱۸
۵-۳-۲ برقراری فضای خارجی	۱۸
۵-۳-۳ برقراری فضای داخلی	۱۹

ادامه‌ی فهرست مندرجات

عنوان	صفحه
۵-۳-۴ برقراری فضای فرآیند مدیریت ریسک	۱۹
۵-۳-۵ تعریف معیارهای ریسک	۲۰
۵-۴ ارزیابی ریسک	۲۱
۵-۴-۱ کلیات	۲۱
۵-۴-۲ شناسایی ریسک	۲۱
۵-۴-۳ تحلیل ریسک	۲۱
۵-۴-۴ سنجش ریسک	۲۲
۵-۵ برخورد با ریسک	۲۲
۵-۵-۱ کلیات	۲۲
۵-۵-۲ انتخاب گزینه‌های برخورد با ریسک	۲۳
۵-۵-۳ آماده سازی و پیاده سازی طرح‌های برخورد با ریسک	۲۴
۵-۶ پایش و بازنگری	۲۴
۵-۷ ثبت فرآیند مدیریت ریسک	۲۵
پیوست الف (اطلاعاتی) وصفی‌های مدیریت ریسک ارتقا یافته	۲۶
کتابنامه	۲۸

پیش گفتار

استاندارد «مدیریت ریسک – اصول و رهنمودها » که پیش نویس آن در کمیسیون‌های مربوط توسط شرکت مهندسی سیستم‌های قابلیت اعتماد توازن تهیه و تدوین شده و در یکصد و سیزدهمین اجلاس کمیته‌ی ملی استاندارد مدیریت کیفیت مورخ ۱۳۸۹/۱۱/۱۷مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و ماخذی که برای تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO 31000, 2009: Risk management — Principles and guidelines

مقدمه

سازمان‌ها فارغ از نوع و اندازه با عوامل تأثیرگذار داخلی و خارجی روبرو می‌شوند که رسیدن و زمان رسیدن سازمان به اهدافش را غیر قطعی[1] می‌کند. تأثیری که این عدم قطعیت[2] بر اهداف سازمان دارد «ریسک» نام دارد.

ریسک در تمامی فعالیت‌های یک سازمان وجود دارد. سازمان‌ها ریسک را با شناسایی آن، تحلیل آن و سپس سنجش اینکه آیا ریسک را بایستی به منظور برآورده ساختن معیارهای ریسک، توسط «برخورد با ریسک[3]» تعدیل نمود یا خیر، مدیریت می‌کند. در طی این فرآیند، آن‌ها با علاقمندان[4] تبادل اطلاعات و مشاوره کرده و ریسک‌ها و کنترل‌هایی را مورد پایش و بازنگری قرار می‌دهند که ریسک را تعدیل می‌کنند تا اطمینان حاصل شود که نیازی به برخورد بیشتری با ریسک نیست. این استاندارد این فعالیت سیستماتیک و منطقی را به طور مشروح توصیف می‌کند.

با اینکه تمامی سازمان‌ها تا حدودی مدیریت ریسک را انجام می‌دهند ولی این استاندارد تعدادی قواعد را که برآورده شدنشان برای اثربخشی مدیریت ریسک مورد نیاز می‌باشند را برقرار می‌کند. این استاندارد توصیه می‌کند که سازمان چارچوبی را به مقصود ادغام فرآیند اداره‌ی ریسک در حکمرانی کلی سازمان، راهبرد، طرح ریزی و مدیریت آن و همچنین برای فرآیندهای گزارش‌دهی، خط مشی‌ها، ارزش‌ها و فرهنگ سازمان، تکوین و اجرا کند و به طور مستمر آن را بهبود دهد.

مدیریت ریسک را می‌توان در کل سازمان، در بسیاری از حوزه‌ها و سطوح آن، در هر زمان و همچنین برای وظایف، پروژه‌ها و فعالیت‌های خاصی به کار برد.

اگرچه رویه‌ی مدیریت ریسک در طی زمان و در بخش‌های زیادی به منظور تأمین نیازهای گوناگون تکوین شده است، ولی پذیرش فرآیندهای سازگار در قالب یک چارچوب جامع می‌تواند برای حصول اطمینان از اینکه ریسک به نحوی اثربخش، کارا و منسجم در طول سازمان مدیریت شده است، کمک کند. رویکرد عامی که در این استاندارد توصیف شده است قواعد و رهنمودهایی را برای مدیریت هر شکلی از ریسک به طریقی سیستماتیک، شفاف و معتبر و درون هر دامنه کار و فضایی[5]، فراهم می‌سازد.

هر بخش خاص یا کاربردی خاص از مدیریت ریسک، با خود نیازها، مخاطبان، ادراکات و معیارهایی را به همراه دارد. بنابراین یکی از خصیصه‌های کلیدی این استاندارد گنجاندن «برقراری فضا[6]» به عنوان فعالیتی در شروع این فرآیند عام مدیریت ریسک می‌باشد. برقراری فضا، اهداف سازمان، محیطی که سازمان درون آن اهدافش را تعقیب می‌کند و علاقمندانش و گوناگونی معیارهای ریسک(که همگی آن‌ها ماهیت و پیچیدگی ریسک‌های سازمان را آشکار و ارزیابی می‌کنند) را ثبت و ضبط می‌کند.

1- Uncertain
2- Uncertainty
3- Risk treatment
4- Stakeholders
5- Context
6- Establishing the context

ارتباط بین قواعد اداره‌ی ریسک، چارچوبی که در آن مدیریت ریسک اتفاق می‌افتد و فرآیند مدیریت ریسک که در این استاندارد توصیف شده اند در شکل ۱ نمایش داده شده است.
هنگامی که مدیریت ریسک مطابق با این استاندارد اجرا و نگهداری شد، سازمان را به طور مثال برای موارد زیر قادر می‌سازد:

- افزایش احتمال نائل شدن به اهداف
- ترغیب به مدیریت پیشگیرانه‌ی فعال
- آگاهی از نیاز به شناسایی و برخورد با ریسک در سرتاسر سازمان
- بهبود شناسایی فرصت‌ها و تهدیدها
- انطباق با الزامات قانونی و نظارتی و نُرم‌های بین‌المللی مربوطه
- بهبود گزارش‌دهی اجباری و داوطلبانه
- بهبود حکمرانی
- بهبود اطمینان و اعتماد علاقمندان
- برقراری یک اساس قابل اطمینان برای تصمیم گیری و طرح ریزی
- بهبود کنترل‌ها
- تخصیص و استفاده‌ی اثربخش از منابع برای برخورد با ریسک
- بهبود اثربخشی و کارایی عملیاتی
- ارتقاء عملکرد سلامت و ایمنی و همچنین حفاظت‌های زیست محیطی
- بهبود ممانعت از تلفات و مدیریت حوادث
- حداقل ساختن تلفات
- بهبود یادگیری سازمانی و
- بهبود برگشت‌پذیری سازمانی[1]

این استاندارد به منظور برآورده ساختن نیازهای گستره‌ی وسیعی از علاقمندان، از جمله موارد زیر می‌باشد:

الف) افرادی که مسئول تدوین خط مشی مدیریت ریسک درون سازمان می‌باشند
ب) افراد پاسخگو در برابر حصول اطمینان از اینکه ریسک درون سازمان به عنوان یک کل و یا درون ناحیه‌ای، پروژه‌ای یا فعالیتی خاص به نحوی کارا مدیریت می‌شود
پ) آن‌هایی که نیازمند ارزیابی اثربخشی سازمان در اداره‌ی ریسک هستند
ت) تدوین کنندگان استانداردها، راهنماها، روش‌های اجرایی و آیین نامه‌ها(به صورت کل یا جزء) که تدوین می‌کنند که ریسک چگونه باید در محتوای خاص این مستندات مدیریت شود.

1- Organizational resilience

رویه‌ها و فرآیندهای جاری مدیریت ریسک در بسیاری از سازمان‌ها شامل اجزایی از مدیریت ریسک می-باشد و بسیاری از سازمان‌ها قبلاً یک فرآیند مدیریت ریسک رسمی را برای انواع خاصی از ریسک یا اوضاع و احوال برگزیده‌اند. در چنین مواردی سازمان می‌تواند تصمیمی مبتنی بر اجرای بازنگری نقادانه‌ی رویه‌ها و فرآیندهای موجود در پرتو این استاندارد، اتخاذ کند.

در این استاندارد عبارات «مدیریت ریسک[1]» و «اداره کردن ریسک[2]» هر دو استفاده شده‌اند. به صورت کلی «مدیریت ریسک» به معماری(قواعد، چارچوب و فرآیند) برای اداره‌ی اثربخش ریسک اشاره دارد، درحالی‌که «اداره کردن ریسک» به کاربرد معماری برای ریسک‌های خاص اشاره می‌کند.

1- Risk management
2- Managing risk

شکل۱-ارتباطات بین قواعد، چارچوب و فرآیند مدیریت ریسک

مدیریت ریسک – اصول و رهنمودها

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ارائه‌ی اصول و رهنمودهایی عام در مورد مدیریت ریسک است.
این استاندارد می‌تواند مورد استفاده هر بنگاه عمومی، خصوصی یا اجتماعی، انجمن، گروه یا فرد قرار گیرد. بنابراین این استاندارد خاص هیچ صنعت یا بخشی نیست.

یادآوری - برای راحتی، به تمام کاربران مختلف این استاندارد با اصطلاح کلی «سازمان» اشاره می‌شود.

این استاندارد را می‌توان در کل عمر یک سازمان و در گستره‌ای وسیع از فعالیتها به کار برد، از جمله راهبردها و تصمیمات، عملیات، فرآیندها، وظایف، پروژه‌ها، محصولات، خدمات و دارایی‌ها.
این استاندارد را می‌توان در مورد هر نوع ریسک با هر ماهیتی به کار برد، چه دارای عواقب مثبت باشد و چه منفی.
گرچه این استاندارد رهنمودهایی عام ارائه می‌دهد، ولی مقصود از آن ترویج مدیریت ریسک هم شکل بین سازمان‌ها نیست. طراحی و پیاده سازی طرح‌ها و چارچوب‌های مدیریت ریسک نیازمند در نظر گرفته شدن نیازهای مختلف سازمانی خاص، اهداف، فضا، ساختار، عملیات، فرآیندها، وظایف، پروژه‌ها، محصولات، خدمات یا دارایی‌های خاص آن و رویه‌های خاص به کار گرفته شده، می‌باشد.
مقصود از این استاندارد استفاده از آن برای هماهنگ سازی فرآیندهای مدیریت ریسک در استانداردهای موجود و استانداردهای آتی است. این استاندارد رویکردی مشترک در پشتیبانی از استانداردهایی ارائه می-دهد که به ریسک‌ها و/یا بخش‌های خاصی می‌پردازند و جایگزینی برای آن استانداردها نیست.
این استاندارد برای مقصود صدور گواهی در نظر گرفته نشده است.

۲ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌روند.

۲-۱

ریسک **risk**

تأثیر عدم قطعیت بر اهداف

یادآوری ۱- تأثیر انحراف از آن چه مورد انتظار است – مثبت و/یا منفی.

یادآوری ۲- اهداف ممکن است جنبه‌های مختلفی داشته باشند (مانند اهداف مالی، بهداشت و ایمنی و محیطی) و ممکن است در سطوح مختلفی به کار روند (مانند راهبردی، در سطح سازمان، پروژه، محصول و فرآیند).

یادآوری ۳- ریسک اغلب با رجوع به **رخدادهای** (۲-۱۷) بالقوه و **عواقب** (۲-۱۸) یا ترکیبی از این‌ها توصیف می‌شود.

یادآوری ۴- ریسک اغلب به صورت ترکیبی از عواقب یک رخداد (از جمله تغییراتی در اوضاع و احوال) و **احتمال** (۲-۱۹) وقوع مربوطه بیان می‌شود.

یادآوری ۵- عدم قطعیت، حالت یا حتی جزئی از نقص اطلاعات مربوط به درک یا دانش یک رخداد، عاقبت یا احتمال آن است.

(ISO Guide 73:2009، تعریف ۱-۱)

۲-۲

مدیریت ریسک **risk management**

فعالیت‌های هماهنگ شده برای هدایت و کنترل یک سازمان با توجه به **ریسک** (۲-۱)

(ISO Guide 73:2009، تعریف ۲-۱)

۳-۲

چارچوب مدیریت ریسک **risk management framework**

مجموعه ای از اجزاء که بنیادها و تمهیدات سازمانی را برای طراحی، پیاده سازی، **پایش** (۲-۲۸) بازنگری و بهبود مداوم **مدیریت ریسک** (۲-۲) در کل سازمان فراهم می‌سازند

یادآوری ۱- بنیادها شامل خط مشی، اهداف، دستور و تعهد به مدیریت **ریسک** (۲-۱) می‌شوند.

یادآوری ۲- تمهیدات سازمانی شامل طرح‌ها، روابط، مسئولیت‌ها، منابع، فرآیندها و فعالیت‌ها می‌شوند.

یادآوری ۳- چارچوب مدیریت ریسک در خط مشی‌ها و رویه‌های کلی راهبردی و بهره برداری سازمان تعبیه شده است.

(ISO Guide 73:2009، تعریف ۲-۱-۱)

۴-۲

خط مشی مدیریت ریسک **risk management policy**

بیانیه‌ی مقاصد کلی و هدایت یک سازمان که مربوط به **مدیریت ریسک** (۲-۲)

(ISO Guide 73:2009، تعریف ۲-۱-۲)

۵-۲

نگرش به ریسک **risk attitude**

رویکرد سازمان به ارزیابی و در نهایت دنبال کردن، حفظ، پذیرفتن یا دور شدن از **ریسک** (۲-۱)

(ISO Guide 73:2009، تعریف ۳-۷-۱-۱)

۶-۲

طرح مدیریت ریسک **risk management plan**

برنامه درون **چارچوب مدیریت ریسک** (۲-۳) که رویکرد، اجزاء مدیریت و منابعی را که قرار است در مدیریت **ریسک** (۲-۱) به کار روند، مشخص می‌کند

یادآوری ۱- اجزاء مدیریت معمولاً شامل روش‌های اجرایی، رویه‌ها، انتصاب مسئولیت‌ها، توالی و زمان بندی فعالیت‌ها می‌شوند.

یادآوری ۲- طرح مدیریت ریسک را می‌توان در محصول، فرآیند و پروژه‌ای خاص و قسمتی از سازمان یا کل آن به کار برد.

(ISO Guide 73:2009، تعریف ۲-۱-۳)

۷-۲

صاحب ریسک **risk owner**

فرد یا مقوله ای با مسئولیت و اختیار برای اداره‌ی **ریسک** (۲-۱)

(ISO Guide 73:2009، تعریف ۳-۵-۱-۵)

۸-۲

فرآیند مدیریت ریسک **risk management process**

به کار گیری سیستماتیک خط مشی‌ها، روش‌های اجرایی و رویه‌های مدیریت در فعالیت‌های تبادل اطلاعات، مشاوره، ایجاد فضا و شناسایی، تحلیل، سنجش، برخورد، **پایش** (۲-۲۸) و بازنگری **ریسک** (۲-۱)

(ISO Guide 73:2009، تعریف ۳-۱)

۹-۲

برقراری فضا **establishing the context**

تعریف پارامترهای خارجی و داخلی که هنگام اداره کردن ریسک و تنظیم دامنه کاربرد و **معیارهای ریسک** (۲-۲۲) برای **خط مشی مدیریت ریسک** (۲-۴) در نظر گرفته می‌شوند.

(ISO Guide 73:2009، تعریف ۳-۳-۱)

۱۰-۲

فضای خارجی **external context**

محیط خارجی که در آن سازمان به دنبال دستیابی به اهدافش است

یادآوری - فضای خارجی می‌تواند شامل موارد زیر باشد:

- محیط فرهنگی، اجتماعی، سیاسی، قانونی، مالی، فناوری، اقتصادی، طبیعی و رقابتی، چه بین المللی باشد و چه ملی، منطقه‌ای یا محلی؛

- محرک‌های کلیدی و روندهای تأثیرگذار بر اهداف سازمان؛ و
- روابط با و برداشت‌ها و ارزش‌های **علاقمندان** (۲-۱۳) خارجی.

(ISO Guide 73:2009، تعریف ۳-۳-۱-۱)

۲-۱۱

فضای داخلی **internal context**

محیط داخلی که در آن سازمان به دنبال دستیابی به اهدافش است

یادآوری- فضای داخلی می‌تواند شامل موارد زیر باشد:

- حکمرانی ، ساختار سازمانی، نقش‌ها و مسئولیت‌ها؛
- خط مشی ها، اهداف و راهبردهایی که برای دستیابی به آن‌ها در کارند؛
- توانمندی‌ها که با توجه به منابع و دانش درک می‌شوند (مثلاً سرمایه، زمان، افراد، فرآیندها، سیستم‌ها و فناوری‌ها)؛
- سیستم‌های اطلاعاتی، جریان‌های اطلاعات و فرآیندهای تصمیم گیری (هم رسمی و هم غیر رسمی)؛
- روابط با **علاقمندان داخلی** (۲-۱۳) و برداشت‌ها و ارزش‌های آنان؛
- فرهنگ سازمان؛
- استانداردها، رهنمودها و مدل‌های اتخاذ شده توسط سازمان؛ و
- شکل و میزان روابط قراردادی.

(ISO Guide 73:2009، تعریف ۳-۳-۱-۲)

۲-۱۲

تبادل اطلاعات و مشاوره **communication and consultation**

فرآیندهای مداوم و تکرار شونده که سازمانی انجام می‌دهد تا اطلاعات را فراهم سازد، در اطلاعات شریک شود یا اطلاعات را کسب کند و وارد گفتگویی در مورد مدیریت **ریسک** (۲-۱) با **علاقمندان** (۲-۱۳) شود.

یادآوری ۱ اطلاعات می‌تواند مربوط به وجود، ماهیت، شکل، **احتمال** (۲-۱۹)، اهمیت، سنجش، قابلیت پذیرش و برخورد با مدیریت ریسک باشد.

یادآوری ۲ مشاوره فرآیندی دو سویه از تبادل آگاهانه اطلاعات است بین یک سازمان و علاقمندانش در مورد مسئله‌ای پیش از تصمیم گیری یا تعیین سمت و سویی در مورد آن مسئله مشاوره عبارت است از:

- فرآیندی که از طریق تأثیر و نه قدرت بر تصمیمی اثر می‌گذارد؛ و
- یک ورودی به تصمیم گیری و نه تصمیم گیری مشترک.

(ISO Guide 73:2009، تعریف ۳-۲-۱)

۲-۱۳

علاقمند **stakeholder**

فرد یا سازمانی که می‌تواند بر تصمیم یا فعالیت تاثیر بگذارد، از آن تاثیر بپذیرد یا خود را تحت تاثیر آن بداند

یادآوری – تصمیم گیرنده می‌تواند علاقمند باشد..

(ISO Guide 73:2009، تعریف ۳-۲-۱-۱)

۱۴-۲

ارزیابی ریسک **risk assessment**

فرآیند کلی **شناسایی ریسک** (۲-۱۵)، **تحلیل ریسک** (۲-۲۱) و **سنجش ریسک** (۲-۲۴)

(ISO Guide 73:2009، تعریف ۳-۴-۱)

۱۵-۲

شناسایی ریسک **risk identification**

فرآیند یافتن، به رسمیت شناختن و توصیف **ریسک**ها (۲-۱)

یادآوری ۱- شناسایی ریسک شامل شناسایی **منابع ریسک** (۲-۱۶)، **رخداد**ها (۲-۱۷)، دلایل آن‌ها و **عواقب** (۲-۱۸) بالقوه آن‌ها می‌شود.

یادآوری ۲- شناسایی ریسک می‌تواند شامل داده‌های تاریخچه ای، تحلیل نظری، نظرات افراد مطلع و متخصص و نیازهای **علاقمند** (۲-۱۳) باشد.

(ISO Guide 73:2009، تعریف ۳-۵-۱)

۱۶-۲

منبع ریسک **risk source**

عنصری که به تنهایی یا به صورت ترکیبی دارای قابلیت ذاتی افزایش **ریسک** (۲-۱)است

یادآوری- منبع ریسک می‌تواند ملموس یا ناملموس باشد.

(ISO Guide 73:2009، تعریف ۳-۵-۱-۲)

۱۷-۲

رخداد **event**

وقوع یا تغییر مجموعه ای خاص از اوضاع و احوال

یادآوری ۱- رخداد می‌تواند یک یا چند اتفاق باشد و می‌تواند چندین دلیل متعدد داشته باشد.

یادآوری ۲- رخداد می‌تواند متشکل از چیزی باشد که اتفاق نمی‌افتد.

یادآوری ۳- رخداد گاهی می‌تواند «رویداد» یا «حادثه» نام گیرد.

(ISO Guide 73:2009، تعریف ۳-۵-۱-۳)

۱۸-۲

عاقبت **consequence**

پیامد یک **رخداد** (۲-۱۷) که بر اهداف تأثیر می‌گذارد

یادآوری ۱- یک رخداد می‌تواند منجر به گستره‌ای از عواقب شود.

یادآوری ۲- عاقبت می‌تواند قطعی یا غیر قطعی باشد و بر اهداف تأثیرات مثبت یا منفی بگذارد.

یادآوری ۳- عواقب را می‌توان به صورت کمی یا کیفی بیان کرد.

یادآوری ۴- عواقب اولیه می‌توانند از طریق تأثیرات ثانوی[1] افزایش یابند.

(ISO Guide 73:2009، تعریف ۳-۶-۱-۳)

۱۹-۲

راستنمایی **likelihood**

شانس وقوع یک امر

یادآوری ۱- در اصطلاح شناسی مدیریت ریسک، واژه «احتمال» به معنای شانس وقوع یک امر به کار می‌رود، چه تعریف شده باشد و چه اندازه گیری شده یا به طور عینی یا فردی، کیفی یا کمی تعریف شده باشد و یا با استفاده از اصطلاحات کلی یا به صورت ریاضیاتی توصیف شده باشد (مانند احتمال یا فراوانی در مدت زمانی معین).

یادآوری ۲- واژه‌ی احتمال[2] دارای تعبیر ریاضیاتی می‌باشد، بنابراین در اصطلاح شناسی مدیریت ریسک از راستنمایی[3] استفاده می‌شود و مقصود این است که تعبیری گسترده‌تر داشته باشد.

(ISO Guide 73:2009، تعریف ۳-۶-۱-۱)

۲۰-۲

پروفایل ریسک **risk profile**

توصیف هر مجموعه ای از **ریسک**‌ها (۲-۱)

یادآوری- مجموعه‌ی ریسک‌ها می‌تواند دربردارنده ریسک‌هایی باشد که مربوط به کل سازمان یا بخشی از آن هستند یا به صورتی دیگر تعریف شوند.

(ISO Guide 73:2009، تعریف ۳-۸-۲-۵)

1 -Knock-on effect
2- Probability
3 -Likelihood

۲۱-۲

تحلیل ریسک **risk analysis**

فرآیندی برای درک ماهیت **ریسک** (۲-۱) و تعیین **سطح ریسک** (۲-۲۳)

یادآوری ۱- تحلیل ریسک، پایه ای برای **سنجش ریسک** (۲-۲۴) و تصمیماتی در مورد **برخورد با ریسک** (۲-۲۵) فراهم می‌سازد.

یادآوری ۲- تحلیل ریسک شامل برآورد ریسک می‌شود.

(ISO Guide 73:2009، تعریف ۳-۶-۱)

۲۲-۲

معیارهای ریسک **risk criteria**

حدود اختیار که اهمیت **ریسک** (۲-۱) در مقابل آن‌ها سنجیده می‌شود

یادآوری ۱- معیارهای ریسک بر پایه اهداف سازمانی و **فضای خارجی** (۲-۱۰) و **داخلی** (۲-۱۱) هستند.

یادآوری ۲- معیارهای ریسک را می‌توان از استانداردها، قوانین، خط مشی‌ها و دیگر الزامات به دست آورد.

(ISO Guide 73:2009، تعریف ۳-۳-۱-۳)

۲۳-۲

سطح ریسک **level of risk**

بزرگی یک **ریسک** (۲-۱) یا ترکیبی از ریسک‌ها، که به صورت ترکیبی از **عواقب** (۲-۱۸) و **راستنمایی** (۲-۱۹) آن‌ها بیان می‌شود.

(ISO Guide 73:2009، تعریف ۳-۶-۱-۸)

۲۴-۲

سنجش ریسک **risk evaluation**

فرآیند مقایسه نتایج **تحلیل ریسک** (۲-۲۱) با **معیارهای ریسک** (۲-۲۲) برای تعیین این که آیا **ریسک** (۱-۱) و/یا بزرگی آن قابل قبول یا قابل تحمل است

یادآوری- سنجش ریسک در تصمیم گیری در مورد **برخورد با ریسک** (۲-۲۵) کمک کننده است.

(ISO Guide 73:2009، تعریف ۳-۷-۱)

۲۵-۲

برخورد با ریسک **risk treatment**

فرآیندی برای تعدیل **ریسک** (۲-۱)

یادآوری ۱- برخورد با ریسک می‌تواند شامل موارد زیر باشد:

- اجتناب از ریسک از طریق تصمیم به عدم آغاز یا ادامه فعالیتی که ریسک را افزایش می‌دهد؛
- پذیرش ریسک یا افزایش آن به منظور دنبال کردن یک فرصت؛
- از میان برداشتن **منبع ریسک** (۲-۱۶)؛
- تغییر دادن **راستنمایی** (۲-۱۹)؛
- تغییر دادن **عواقب** (۲-۱۸)؛
- به اشتراک گذاشتن ریسک با طرف یا طرف‌های دیگر (از جمله قراردادها و تأمین مالی ریسک؛ و
- حفظ ریسک با تصمیم‌گیری آگاهانه.

یادآوری ۲- برخورد با ریسک‌هایی که به عواقب منفی می‌پردازند، گاهی «تخفیف ریسک»، «رفع ریسک»، «ممانعت از ریسک» و «کاهش ریسک» نام می‌گیرند.

یادآوری ۳- برخورد با ریسک می‌تواند ریسک‌هایی جدید ایجاد کند یا ریسک‌های موجود را تعدیل نماید.

(ISO Guide 73:2009، تعریف ۳-۸-۱)

۲۶-۲

کنترل **control**

اقدامی که **ریسک** (۲-۱) را تعدیل می‌کند

یادآوری ۱- کنترل‌ها شامل هر فرآیند، خط مشی، تدبیر، رویه یا اقدام دیگری هستند که ریسک را تعدیل می‌کند.

یادآوری ۲- کنترل‌ها ممکن است همیشه تأثیر تعدیلی مورد نظر یا مفروض را دربر نداشته باشند.

(ISO Guide 73:2009، تعریف ۳-۸-۱-۱)

۲۷-۲

ریسک باقی مانده **residual risk**

ریسک (۱-۱) باقی مانده پس از **برخورد با ریسک** (۲-۲۵)

یادآوری ۱- ریسک باقی مانده می‌تواند دربردارنده ریسک شناسایی نشده باشد.

یادآوری ۲- ریسک باقی مانده همچنین می‌تواند «ریسک حفظ شده» نام گیرد.

(ISO Guide 73:2009، تعریف ۳-۸-۱-۶)

۲۸-۲

پایش **monitoring**

وارسی، نظارت و مشاهده نقادانه مداوم یا تعیین وضعیت به منظور شناسایی تغییر از سطح عملکرد مورد الزام یا انتظار

یادآوری- پایش می‌تواند در **چارچوب مدیریت ریسک** (۲-۳)، **فرآیند مدیریت ریسک** (۲-۸)، **ریسک** (۲-۱) یا **کنترل** (۲-۲۶) به کار رود.

(ISO Guide 73:2009، تعریف ۳-۸-۲-۱)

۲-۲۹

بازنگری **review**

فعالیتی که برای تعیین مناسب بودن، کفایت و اثربخشی موضوع برای دستیابی به اهداف برقرار شده انجام می‌گیرد

یادآوری- بازنگری می‌تواند در **چارچوب مدیریت ریسک**(۲-۳)، **فرآیند مدیریت ریسک** (۲-۸)، **ریسک** (۲-۱) یا **کنترل** (۲-۲۶) به کار رود.

(ISO Guide 73:2009، تعریف ۳-۸-۲-۲)

۳ اصول

برای این که مدیریت ریسک اثربخش واقع شود، سازمان بایستی در تمامی سطوح، منطبق با اصول زیر باشد.

الف) مدیریت ریسک ارزش را ایجاد و حفاظت می‌کند.

مدیریت ریسک در دستیابی قابل اثبات اهداف و بهبود عملکرد مثلاً در بهداشت و ایمنی انسان، امنیت، انطباق قانونی و نظارتی، پذیرش عمومی، حفاظت محیطی، کیفیت محصول، مدیریت پروژه، کارایی در بهره برداری ها، حکمرانی و اعتبار، مشارکت می‌کند.

ب) مدیریت ریسک به عنوان یک قسمت جدایی ناپذیر از فرآیندهای سازمانی

مدیریت ریسک یک فعالیت مستقل مجزا از فعالیت‌ها و فرآیندهای اصلی سازمان نیست. مدیریت ریسک قسمتی از مسئولیت‌های مدیریت و یک قسمت جدایی ناپذیر تمام فرآیندهای سازمانی است، از جمله طرح-ریزی راهبردی و کل فرآیندهای مدیریت پروژه و مدیریت تغییر.

پ) مدیریت ریسک قسمتی از تصمیم گیری است.

مدیریت ریسک به تصمیم گیرندگان کمک می‌کند انتخاب‌های آگاهانه‌ای داشته باشند، اقدامات را اولویت بندی کنند و بین راه کارهای مختلف تمایز قائل شوند.

ت) مدیریت ریسک تصریحاً به عدم قطعیت می‌پردازد.

مدیریت ریسک تصریح عدم قطعیت، ماهیت این عدم قطعیت و نحوه پرداختن به آن را در نظر می‌گیرد.

ث) مدیریت ریسک سیستماتیک، ساختار یافته و به هنگام است.

رویکردی سیستماتیک، به هنگام و ساختار یافته به مدیریت ریسک در کارایی و نتایجی پایدار، قابل مقایسه و قابل اطمینان کمک می‌کند.

ج) مدیریت ریسک بر اساس بهترین اطلاعات موجود قرار دارد.

ورودی‌ها به فرآیند اداره‌ی ریسک بر اساس منابع اطلاعاتی مانند داده‌های تاریخچه ای، تجربه، بازخورد علاقمند، مشاهده، پیش بینی‌ها و کارشناسی تخصصی قرار دارند. با این حال، تصمیم گیرندگان بایستی خود را از هر محدودیت در داده‌ها یا مدلسازی به کار رفته یا احتمال تباین[1] بین متخصصین آگاه ساخته و این موارد را به حساب آورند.

چ) مدیریت ریسک سازگارسازی شده است.

مدیریت ریسک با فضای خارجی و داخلی سازمان و پروفایل ریسک همراستا است.

ح) مدیریت ریسک عوامل انسانی و فرهنگی را به حساب می‌آورد.

مدیریت ریسک توانمندی ها، ادراک‌ها و مقاصد افراد خارجی و داخلی را که می‌توانند دستیابی به اهداف سازمان را تسهیل نموده یا مانع آن‌ها شوند، به رسمیت می‌شناسد.

خ) مدیریت ریسک شفاف و جامع است.

مداخله مناسب و به هنگام علاقمندان و به ویژه تصمیم گیرندگان در تمامی سطوح سازمان، مرتبط و به روز باقی ماندن مدیریت ریسک را تأمین می‌کند. مداخله همچنین به علاقمندان این امکان را می‌دهد که نظراتشان به طور مناسب نشان داده شوند و در تعیین معیارهای ریسک به حساب آید.

د) مدیریت ریسک پویا، تکراری[2] و پاسخگو به تغییر است.

مدیریت ریسک بطور مداوم تغییر را حس می‌کند و به آن پاسخ می‌گوید. با وقوع رخدادهای خارجی و داخلی، فضا و دانش تغییر می‌کند، پایش و بازنگری ریسک‌ها روی می‌دهد، ریسک‌های جدیدی ظاهر می-شوند، برخی از آن‌ها تغییر می‌یابند و بقیه ناپدید می‌شوند.

ذ) مدیریت ریسک بهبود مداوم سازمان را میسر می‌کند.

سازمان‌ها بایستی راهبردهایی برای بهبود تکامل مدیریت ریسکشان در کنار تمام جنبه‌های دیگر سازمانشان تکوین و پیاده سازی کنند.

پیوست الف توصیه‌های بیشتری برای سازمان‌هایی ارائه می‌دهد که مایلند ریسک را به صورتی اثربخش‌تر مدیریت کنند.

۴ چارچوب

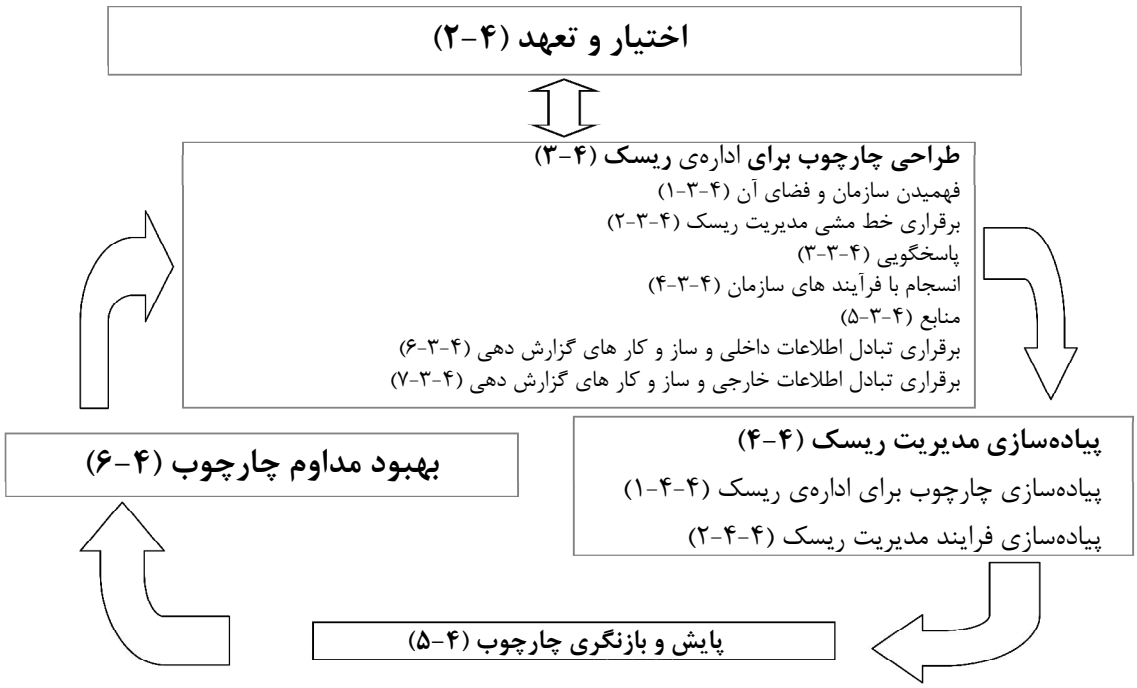
۴-۱ کلیات

موفقیت مدیریت ریسک بسته به اثربخشی چارچوب مدیریت است که بنیادها و تمهیداتی را که در کل سازمان در تمامی سطوح در آن تعبیه شده اند، فراهم می‌سازد. چارچوب در اداره‌ی اثربخش ریسک‌ها از طریق به کار گیری فرآیند مدیریت ریسک (به بند ۵ مراجعه کنید) در سطوح مختلف و در فضای خاص

1 - Divergence
2 - Iterative

سازمان، کمک کننده است. چارچوب اطمینان می‌دهد که اطلاعات در مورد ریسک که از فرآیند مدیریت ریسک به دست آمده است، به نحو مناسب گزارش شده و به عنوان اساسی برای تصمیم گیری و پاسخگویی در تمام سطوح سازمانی مربوطه به کار می‌رود.

این بند اجزاء ضروری چارچوب را برای اداره‌ی ریسک و نحوه ارتباط آن‌ها با یکدیگر به صورتی تکراری را چنان که در شکل ۲ نشان داده شده است، توصیف می‌کند.



شکل ۲ – ارتباط بین اجزاء چارچوب برای اداره‌ی ریسک

مقصود از چارچوب، تجویز سیستم مدیریت نیست، بلکه کمک به سازمان در گنجاندن مدیریت ریسک در سیستم کلی مدیریتش است. بنابراین سازمان‌ها بایستی اجزاء چارچوب را با نیازهای خاصشان منطبق سازند. اگر رویه‌ها و فرآیندهای موجود سازمانی شامل اجزاء مدیریت ریسک می‌شود یا اگر سازمان از قبل یک فرآیند مدیریت ریسک رسمی را برای انواع خاصی از ریسک‌ها یا موقعیت‌ها اتخاذ نموده، آن گاه این امور بایستی به صورت نقادانه در مقابل این استاندارد ، از جمله وصفی‌های موجود در پیوست الف، بازنگری و ارزیابی شوند تا کفایت و اثربخشی آن‌ها تعیین شود.

۴-۲ اختیار و تعهد

اعمال مدیریت ریسک و حصول اطمینان از اثربخشی پیوسته آن مستلزم تعهد قوی و مداوم مدیریت سازمان و همچنین طراحی راهبردی و شدید برای دستیابی به تعهد در تمامی سطوح است. مدیریت بایستی:

- خط مشی مدیریت ریسک را تعریف و تأیید کند؛
- اطمینان یابد که فرهنگ سازمان و خط مشی مدیریت ریسک همراستا با یکدیگر هستند؛

- شاخص‌های عملکرد مدیریت ریسک را تعیین کند که همراستا با شاخص‌های عملکرد سازمان هستند؛
- اهداف مدیریت ریسک را با اهداف و راهبردهای سازمان همراستا سازد؛
- از انطباق قانونی و نظارتی اطمینان حاصل کند؛
- پاسخگویی‌ها و مسئولیت‌ها را در سطوح مناسبی درون سازمان منصوب کند؛
- اطمینان یابد که منابع ضروری به مدیریت ریسک تخصیص می‌یابند؛
- مزایای مدیریت ریسک را به تمام علاقمندان منتقل سازد؛ و
- اطمینان یابد که چارچوب اداره‌ی ریسک همچنان مناسب باقی می‌ماند.

۴-۳ طراحی چارچوب برای اداره‌ی ریسک

۴-۳-۱ فهمیدن سازمان و فضای آن

پیش از آغاز طراحی و پیاده سازی چارچوب برای اداره‌ی ریسک، مهم است که هم فضای خارجی و هم داخلی سازمان درک و سنجیده شود، چرا که این موارد می‌توانند به طور قابل توجهی بر طراحی چارچوب اثر بگذارند.

سنجش فضای خارجی سازمان ممکن است شامل موارد زیر باشد، اما محدود به آن‌ها نیست:

الف) محیط اجتماعی و فرهنگی، سیاسی، قانونی، نظارتی، مالی، فناوری، اقتصادی، طبیعی و رقابتی، چه بین المللی باشد و چه ملی، منطقه ای یا محلی؛

ب) محرک‌ها و روندهای کلیدی تأثیرگذار بر اهداف سازمان؛ و

پ) روابط با علاقمندان خارجی و ادراک‌ها و ارزش‌های آنان.

سنجش فضای داخلی سازمان ممکن است شامل موارد زیر باشد، اما محدود به آن‌ها نیست:

- حکمرانی، ساختار سازمانی، نقش‌ها و پاسخگویی‌ها؛
- خط مشی‌ها، اهداف و راهبردهایی که برای دستیابی به آن‌ها در کارند؛
- توانمندی‌ها، که با توجه به منابع و دانش درک می‌شوند (مثلاً سرمایه، زمان، افراد، فرآیند ها، سیستم‌ها و فناوری‌ها)؛
- سیستم‌های اطلاعاتی، جریان‌های اطلاعاتی و فرآیندهای تصمیم‌گیری (هم رسمی و هم غیر رسمی)؛
- روابط با علاقمندان داخلی و ادراک‌ها و ارزش‌های آنان؛
- فرهنگ سازمانی؛
- استاندارد ها، رهنمودها و مدل‌های اتخاذ شده توسط سازمان؛ و
- شکل و میزان روابط قراردادی.

۴-۳-۲ برقراری خط مشی مدیریت ریسک

خط مشی مدیریت ریسک بایستی به روشنی اهداف سازمان را برای مدیریت ریسک و تعهد آن به مدیریت ریسک را بیان کند و به ویژه به موارد ذیل می‌پردازد:

- منطق اساسی سازمان برای ادراه‌ی ریسک؛
- پیوندهای بین اهداف و خط مشی‌های سازمان و خط مشی مدیریت ریسک؛
- پاسخگویی‌ها و مسئولیت‌ها برای اداره‌ی ریسک؛
- نحوه برخورد با منافع ناسازگار؛
- تعهد به در دسترس قرار دادن منابع ضروری برای کمک به افرادی که پاسخگو و مسئول در برابر اداره‌ی ریسک هستند؛
- نحوه اندازه گیری و گزارش عملکرد مدیریت ریسک؛ و
- تعهد به بازنگری و بهبود خط مشی و چارچوب مدیریت ریسک به صورت دوره ای و در پاسخ به رخداد یا تغییری در اوضاع و احوال.

خط مشی مدیریت ریسک بایستی به طور مناسب در سازمان انتقال داده شود.

۴-۳-۳ پاسخگویی

سازمان بایستی اطمینان حاصل کند که برای اداره‌ی ریسک، پاسخگویی، اختیار و شایستگی مناسبی موجود است، از جمله پیاده سازی و حفظ فرآیند مدیریت ریسک و حصول اطمینان از کفایت، اثربخشی و کارایی هر کنترل. این امر به طرق زیر میسر می‌شود:

- شناسایی صاحبان ریسک که از پاسخگویی و اختیار برای مدیریت ریسک برخوردارند؛
- شناسایی فردی که پاسخگو تکوین، پیاده سازی و حفظ چارچوب برای اداره‌ی ریسک است؛
- شناسایی دیگر مسئولیت‌های افراد در تمام سطوح سازمان برای فرآیند مدیریت ریسک؛
- برقراری اندازه گیری عملکرد و گزارش دهی خارجی و/یا داخلی و فرآیندهای افزایش؛ و
- تأمین سطوح مناسب شناخت.

۴-۳-۴ انسجام با فرآیندهای سازمان

مدیریت ریسک بایستی در تمام رویه‌ها و فرآیندهای سازمان تعبیه شود، به نحوی که مرتبط، اثربخش و کارآمد باشد. فرآیند مدیریت ریسک بایستی قسمتی از این فرآیندهای سازمانی باشد و از آن‌ها مجزا نباشد. به ویژه، مدیریت ریسک بایستی در تکوین خط مشی، کسب و کار و طراحی و بازنگری راهبردی تعبیه شود و فرآیندهای مدیریت را تغییر دهد.

بایستی یک طرح مدیریت ریسک در سطح سازمان موجود باشد تا اطمینان حاصل کند که خط مشی مدیریت ریسک پیاده‌سازی می‌شود و این که مدیریت ریسک در تمام رویه‌ها و فرآیندهای سازمان تعبیه شده است. طرح مدیریت ریسک می‌تواند با دیگر طرح‌های سازمانی مانند طرح راهبردی، انسجام یابد.

۴-۳-۵ منابع

سازمان بایستی منابع مناسبی به مدیریت ریسک تخصیص دهد.

به موارد زیر بایستی توجه شود:

- افراد، مهارت‌ها، تجربه و شایستگی؛
- منابع مورد نیاز برای هر گام از فرآیند مدیریت ریسک؛
- فرآیند ها، روش‌ها و ابزارهای مورد استفاده سازمان برای اداره‌ی ریسک؛
- فرآیندها و روش‌های اجرایی مستند؛
- سیستم‌های مدیریت اطلاعات و دانش؛ و
- برنامه‌های آموزشی.

۴-۳-۶ برقراری تبادل اطلاعات داخلی و ساز و کارهای گزارش دهی

سازمان بایستی تبادل اطلاعات داخلی و ساز و کارهای گزارش‌دهی را برقرار نماید تا پاسخگویی و مالکیت ریسک را پشتیبانی و تشویق نماید. این ساز و کارها بایستی اطمینان حاصل کنند که:

- تبادل اطلاعات اجزاء کلیدی چارچوب مدیریت ریسک و هر تعدیل بعدی به طور مناسب انجام گیرد؛
- گزارش دهی داخلی کافی در مورد چارچوب، اثربخشی و پیامدهای آن موجود است؛
- اطلاعات مربوطه به دست آمده از به کارگیری مدیریت ریسک در سطوح و زمان‌های مناسب در دسترس است؛ و
- فرآیندهایی برای مشاوره با علاقمندان داخلی موجود هستند.

این ساز و کارها بایستی (بر حسب اقتضا)، شامل فرآیندهایی برای یکی کردن اطلاعات ریسک از منابع مختلفی شوند و ممکن است نیاز باشد که حساسیت اطلاعات را در نظر بگیرند.

۴-۳-۷ برقراری تبادل اطلاعات خارجی و ساز و کارهای گزارش دهی

سازمان بایستی طرحی مبنی بر این که چگونه با علاقمندان خارجی تبادل اطلاعات می‌کند، تکوین و پیاده سازی کند. این طرح بایستی شامل موارد زیر باشد:

- دخیل کردن علاقمندان خارجی مناسب و حصول اطمینان از مبادله اثربخش اطلاعات؛
- گزارش دهی خارجی برای انطباق با الزامات قانونی، نظارتی و حکومتی؛
- ارائه‌ی بازخور و گزارش دهی در مورد تبادل اطلاعات و مشاوره؛

- استفاده از تبادل اطلاعات برای ایجاد اعتماد در سازمان؛ و
- تبادل اطلاعات با علاقمندان در صورت رخداد بحران یا اتفاقی تصادفی.

این ساز و کارها بایستی (بر حسب اقتضا)، شامل فرآیندهایی برای یکی کردن اطلاعات ریسک از منابع مختلفی شوند و ممکن است نیاز باشد که حساسیت اطلاعات را در نظر بگیرند.

۴-۴ پیاده سازی مدیریت ریسک

۴-۴-۱ پیاده سازی چارچوب برای اداره‌ی ریسک

در پیاده سازی چارچوب سازمان برای اداره‌ی ریسک، سازمان بایستی:

- زمانبندی و راهبرد مناسب را برای پیاده سازی چارچوب تعریف کند؛
- خط مشی و فرآیند مدیریت ریسک را در فرآیندهای سازمانی به کار برد؛
- منطبق با الزامات قانونی و نظارتی باشد؛
- اطمینان یابد که تصمیم‌گیری، از جمله تکوین و تنظیم اهداف با پیامدهای فرآیندهای مدیریت ریسک همراستا است؛
- جلسات اطلاعاتی و آموزشی برگزار کند؛ و
- با علاقمندان تبادل اطلاعات نموده و مشاوره کند تا اطمینان یابد که چارچوب مدیریت ریسک آن مناسب باقی می‌ماند.

۴-۴-۲ پیاده سازی فرآیند مدیریت ریسک

مدیریت ریسک بایستی با حصول اطمینان از این که فرآیند مدیریت ریسک خلاصه شده در بند ۵ از طریق یک طرح مدیریت ریسک در تمام سطوح وظایف سازمانی مربوطه به عنوان قسمتی از رویه‌ها و فرآیندهایش به کار می‌رود، پیاده سازی شود.

۴-۵ پایش و بازنگری چارچوب

به منظور حصول اطمینان از این که مدیریت ریسک اثربخش است و همچنان عملکرد سازمانی را پشتیبانی می‌کند، سازمان بایستی:

- عملکرد مدیریت ریسک را در مقابل شاخص‌هایی اندازه‌گیری کند که به صورت دوره‌ای برای مناسب بودن بازنگری می‌شوند؛
- به صورت دوره‌ای پیشروی را در مقابل طرح مدیریت ریسک و انحراف از آن، اندازه گیری کند؛
- به صورت دوره‌ای بازنگری کند که آیا چارچوب، خط مشی و طرح مدیریت ریسک با در نظر گرفتن فضای خارجی و داخلی سازمان، همچنان مناسب هستند؛

- درمورد ریسک، پیشروی طبق طرح مدیریت ریسک و این که خط مشی مدیریت ریسک تا چه حد مورد پیروی قرار می‌گیرد، گزارش دهد؛ و
- اثربخشی چارچوب مدیریت ریسک را بازنگری کند.

۶-۴ بهبود مداوم چارچوب

بر اساس نتایج پایش و بازنگری ها، بایستی تصمیماتی در این مورد اخذ شود که چارچوب، خط مشی و طرح مدیریت ریسک چگونه می‌تواند بهبود یابد. این تصمیمات بایستی منجر به بهبودهایی در مدیریت ریسک سازمان و فرهنگ مدیریت ریسک آن شوند.

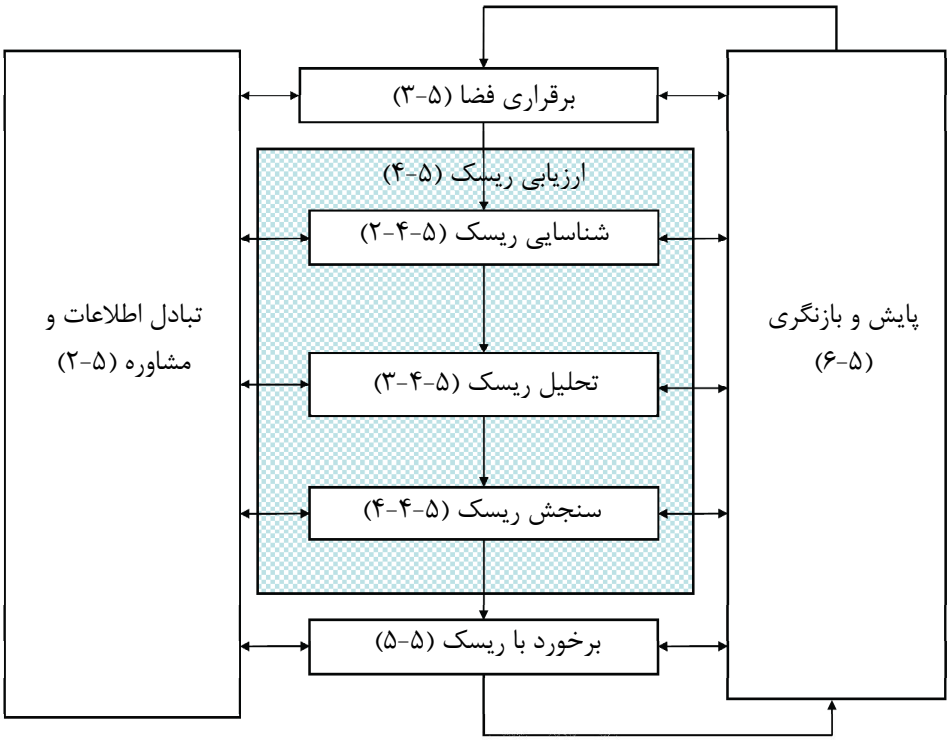
۵ فرآیند

۵-۱ کلیات

فرآیند مدیریت ریسک بایستی

- یک قسمت جدا نشدنی از مدیریت باشد؛
- در فرهنگ و رویه‌ها تعبیه شده باشد؛ و
- با فرآیندهای کسب و کار سازمان سازگارسازی شده باشد.

این امر شامل فعالیت‌های توصیف شده در بند ۵-۲ تا ۵-۶ است. فرآیند مدیریت ریسک در شکل ۳ نشان داده شده است.



شکل ۳ – فرآیند مدیریت ریسک

۵-۲ تبادل اطلاعات و مشاوره

تبادل اطلاعات و مشاوره با علاقمندان خارجی و داخلی بایستی در کلیه مراحل فرآیند مدیریت ریسک رخ دهد.

بنابراین طرح‌هایی برای تبادل اطلاعات و مشاوره بایستی در اولین مرحله تکوین شوند. این موارد باید به مسائلی مربوط به خود ریسک، دلایل آن، عواقب آن (اگر از آن‌ها اطلاعاتی موجود باشد) و اقداماتی که برای برخورد با آن انجام می‌گیرند، بپردازند. تبادل اطلاعات اثربخش خارجی و داخلی و مشاوره بایستی رخ دهد تا اطمینان حاصل شود که افراد پاسخگو برای پیاده سازی فرآیند مدیریت ریسک و علاقمندان پایه تصمیم گیری‌ها و دلایل نیاز به اقداماتی خاص را درک کنند.

یک رویکرد گروه مشاوره ممکن است:

- به برقراری مناسب فضا کمک کند؛
- اطمینان یابد که منافع علاقمندان درک شده‌اند و در نظر گرفته می‌شوند؛
- به اطمینان از این امر کمک کند که ریسک‌ها به طور کافی شناسایی شده اند؛
- حوزه‌های مختلف تخصصی را برای تحلیل ریسک‌ها گرد هم آورد؛
- اطمینان یابد که نظرات مختلف در زمان تعریف معیارهای ریسک و در سنجش ریسک‌ها به طور مناسب در نظر گرفته شده اند؛
- پشتیبانی و حمایت را برای طرح برخورد با ریسک تأمین کند؛

- مدیریت تغییر مناسب را در طول فرآیند مدیریت ریسک تقویت کند؛ و
- یک طرح تبادل اطلاعات و مشاوره مناسب داخلی و خارجی را تکوین نماید.

تبادل اطلاعات و مشاوره با علاقمندان اهمیت دارد، چرا که آن‌ها بر اساس ادراکشان از ریسک، در مورد ریسک کارشناسی می‌کنند. این ادراک‌ها ممکن است بنا به تفاوت‌هایی در ارزش‌ها، نیازها، فرضیات، مفاهیم و دغدغه‌های علاقمندان متفاوت باشند. از آنجا که نظرات علاقمندان می‌تواند تأثیری قابل توجه بر تصمیمات گرفته شده داشته باشد، ادراک آن‌ها بایستی شناسایی و ثبت شده و در فرآیند تصمیم گیری به حساب آید.
تبادل اطلاعات و مشاوره بایستی مبادله اطلاعات صادقانه، مرتبط، صحیح و قابل فهم را میسر سازد و جنبه-های انسجام محرمانه و شخصی را به حساب آورد.

۵-۳ برقراری فضا

۵-۳-۱ کلیات

سازمان با برقراری فضا اهدافش را بیان می‌کند، پارامترهای خارجی و داخلی را که قرار است در زمان اداره‌ی ریسک به حساب آیند، تعریف می‌کند و دامنه کاربرد و معیارهای ریسک را برای فرآیند باقی مانده تنظیم می‌کند. در عین این که بسیاری از این پارامترها مشابه پارامترهای در نظر گرفته شده در طراحی چارچوب مدیریت ریسک (به ۴-۳-۱ مراجعه کنید) هستند، در زمان برقراری فضا برای فرآیند مدیریت ریسک، نیاز است که با تفصیل بیشتری در نظر گرفته شوند و به ویژه به نحوه ارتباط آن‌ها با دامنه کاربرد فرآیند مدیریت ریسک خاص توجه شود.

۵-۳-۲ برقراری فضای خارجی

فضای خارجی، محیط خارجی است که سازمان در آن به دنبال دستیابی به اهدافش است.
درک فضای خارجی مهم است تا اطمینان حاصل شود که اهداف و دغدغه‌های علاقمندان خارجی در تکوین معیارهای ریسک در نظر گرفته می‌شوند. این امر بر پایه فضا در گستره سازمان است، اما با جزئیات خاص الزامات قانونی و نظارتی؛ ادراک‌های علاقمندان و دیگر جنبه‌های ریسک‌ها که خاص دامنه کاربرد فرآیند مدیریت ریسک هستند.
فضای خارجی می‌تواند شامل موارد زیر باشد، اما محدود به آن‌ها نیست:

- محیط اجتماعی و فرهنگی، سیاسی، قانونی، نظارتی، مالی، فناوری، اقتصادی، طبیعی و رقابتی، چه بین المللی باشد و چه ملی، منطقه ای یا محلی؛
- محرک‌ها و روندهای کلیدی تأثیرگذار بر اهداف سازمان؛ و
- روابط با علاقمندان خارجی و ادراک‌ها و ارزش‌های آنان.

۵-۳-۳ برقراری فضای داخلی

فضای داخلی، محیط داخلی است که سازمان در آن به دنبال دستیابی به اهدافش است.

فرآیند مدیریت ریسک بایستی با فرهنگ، فرآیندها، ساختار و راهبرد سازمان همراستا باشد. فضای داخلی هر چیزی درون سازمان است که می‌تواند بر نحوه مدیریت ریسک سازمان اثر بگذارد. این امر باید برقرار شود چون:

الف) مدیریت ریسک در فضای اهداف سازمان رخ می‌دهد؛

ب) اهداف و معیارهای پروژه، فرآیند یا فعالیتی خاص بایستی از لحاظ اهداف سازمان به طور کلی در نظر گرفته شوند؛ و

پ) برخی سازمان‌ها نمی توانند فرصت‌های دستیابی به اهداف راهبردی، پروژه ای یا کسب و کار خود را تشخیص دهند و این امر بر تعهد، اعتبار، اعتماد و ارزش پیوسته سازمانی اثر می‌گذارد.

درک فضای داخلی ضروری است. این امر می‌تواند شامل موارد زیر باشد، اما محدود به آن‌ها نیست:

- حکمرانی، ساختار سازمانی، نقش‌ها و پاسخگویی‌ها؛
- خط مشی‌ها، اهداف و راهبردهایی که برای دستیابی به آن‌ها در کارند؛
- توانمندی‌ها که با توجه به منابع و دانش درک می‌شوند (مثلاً سرمایه، زمان، افراد، فرآیند ها، سیستم‌ها و فناوری‌ها)؛
- روابط با علاقمندان داخلی و ادراک‌ها و ارزش‌های آنان؛
- فرهنگ سازمانی؛
- سیستم‌های اطلاعات، جریان‌های اطلاعات و فرآیندهای تصمیم گیری (هم رسمی و هم غیررسمی)؛
- استاندارد ها، رهنمودها و مدل‌های اتخاذ شده توسط سازمان؛ و
- شکل و میزان روابط قراردادی.

۵-۳-۴ برقراری فضای فرآیند مدیریت ریسک

اهداف، راهبردها، دامنه کاربرد و پارامترهای فعالیت‌های سازمان یا قسمت‌هایی از سازمان که در آن‌ها فرآیند مدیریت ریسک به کار می‌رود، بایستی برقرار شوند. مدیریت ریسک بایستی با در نظر گرفتن کامل نیاز به توجیه منابع به کار رفته در انجام مدیریت ریسک اجرا شود. منابع مورد الزام، مسئولیت‌ها و اختیارات و سوابقی که قرار است نگه داشته شوند نیز بایستی مشخص شوند.

فضای فرآیند مدیریت ریسک بنا به نیازهای سازمان متفاوت خواهد بود. این امر می‌تواند شامل موارد زیر باشد اما محدود به آن‌ها نیست:

- تعریف اهداف و مقاصد فعالیت‌های مدیریت ریسک؛
- تعریف مسئولیت‌ها برای فرآیند مدیریت ریسک و درون آن؛

- تعریف دامنه کاربرد و همچنین عمق و وسعت فعالیت‌های مدیریت ریسک که قرار است انجام گیرند، از جمله شامل کردن‌ها[1] و مستثنی کردن‌های[2] خاص؛
- تعریف فعالیت، فرآیند، وظیفه، پروژه، محصول، فرآیند، فعالیت و دیگر پروژه ها، فرآیندها یا فعالیت-های سازمان؛
- تعریف روش شناسی‌های ارزیابی ریسک؛
- تعریف نحوه سنجش عملکرد و اثربخشی در مدیریت ریسک؛
- شناسایی و مشخص کردن تصمیماتی که باید اخذ شوند؛ و
- شناسایی، تعیین دامنه کاربرد یا تعیین چارچوب مطالعات مورد نیاز، میزان و اهداف آن‌ها و منابع الزامی برای چنین مطالعاتی.

توجه به این موارد و دیگر فاکتورهای مربوطه بایستی به حصول اطمینان از این امر کمک کند که رویکرد مدیریت ریسک اتخاذ شده برای اوضاع و احوال ، سازمان و ریسک‌های تأثیرگذار بر دستیابی به اهدافش مناسب است.

۵-۳-۵ تعریف معیارهای ریسک

سازمان بایستی معیارهای مورد استفاده برای سنجش اهمیت ریسک را تعریف کند. معیارها بایستی منعکس کننده ارزش ها، اهداف و منابع سازمان باشند. برخی معیارها ممکن است توسط الزامات قانونی و نظارتی و دیگر الزاماتی که سازمان متعهد به آن ها است، تحمیل شوند یا از آن‌ها مشتق شوند. معیارهای ریسک بایستی سازگار با خط مشی مدیریت ریسک باشند (به بند ۴-۳-۲ مراجعه کنید)، در آغاز هر فرآیند مدیریت ریسک تعریف شوند و به طور مداوم بازنگری شوند.

در تعریف معیارهای ریسک، فاکتورهایی که قرار است در نظر گرفته شوند، بایستی شامل موارد زیر باشند:

- ماهیت و انواع دلایل و عواقبی که ممکن است رخ دهند و نحوه اندازه گیری آن ها؛
- نحوه تعریف راستنمایی؛
- چارچوب (های) زمانی راستنمایی و/یا عاقبت/ عواقب؛
- نحوه تعیین سطح ریسک؛
- نظرات علاقمندان؛
- سطحی که در آن ریسک قابل قبول یا قابل تحمل می‌شود؛و
- این که آیا ترکیباتی از ریسک‌های چندگانه بایستی به حساب آیند و در این صورت، نحوه در نظر گرفتن ترکیبات و این که کدام ترکیبات بایستی در نظر گرفته شوند.

1-Specific inclusion
2-exclusion

۵-۴ ارزیابی ریسک

۵-۴-۱ کلیات

ارزیابی ریسک فرآیند کلی شناسایی ریسک، تحلیل ریسک و سنجش ریسک است.

یادآوری ISO/IEC 31010[1] رهنمودهایی درباره تکنیک‌های ارزیابی ریسک ارائه می‌دهد.

۵-۴-۲ شناسایی ریسک

سازمان بایستی منابع ریسک، حوزه‌های تأثیرات، رخدادها (از جمله تغییرات در اوضاع و احوال) و دلایل آن-ها و عواقب احتمالی آن‌ها را شناسایی کند. هدف از این گام ایجاد فهرستی جامع از ریسک‌ها بر پایه رخداد-هایی است که ممکن است دستیابی به اهداف را ایجاد، تقویت و ممانعت کننده آن را تنزل دهند، سرعت بخشند یا به تاخیر بیاندازند. شناسایی ریسک‌های مربوط به عدم تعقیب یک فرصت، دارای اهمیت است. شناسایی جامع مهم است، چرا که ریسکی که در این مرحله شناسایی نمی شود، در تحلیل‌های آتی گنجانده نخواهد شد.

شناسایی بایستی شامل تمامی ریسک‌ها شود چه منبع آن‌ها تحت کنترل سازمان باشد و چه نباشد، هر چند منبع ریسک یا دلیل آن ممکن است روشن نباشد. شناسایی ریسک بایستی شامل بررسی تأثیرات پیوسته عواقبی خاص باشد، از جمله تأثیرات آبشاری و تجمعی. شناسایی همچنین بایستی گستره وسیعی از عواقب را در نظر بگیرد، حتی اگر منبع ریسک یا دلیل آن آشکار نباشد. علاوه بر شناسایی آنچه ممکن است روی دهد، ضروری است که دلایل و سناریوهای ممکن در نظر گرفته شوند که نشان می‌دهند چه عواقبی ممکن است رخ دهند. تمام دلایل و عواقب قابل توجه بایستی در نظر گرفته شوند.

سازمان بایستی ابزارهای شناسایی ریسک و تکنیک‌هایی را به کار گیرد که برای اهداف و توانمندی‌های آن و ریسک‌هایی که با آن مواجه می‌شود، مناسب هستند. اطلاعات مربوطه و به روز در شناسایی ریسک‌ها مهم است. این امر بایستی شامل اطلاعات پیش زمینه‌ای مناسب در جای ممکن باشد. افرادی که دارای دانش مناسب هستند بایستی در شناسایی ریسک‌ها دخیل باشند.

۵-۴-۳ تحلیل ریسک

تحلیل ریسک شامل تکوین درکی از ریسک می‌شود. تحلیل ریسک یک ورودی به سنجش ریسک و تصمیماتی در مورد این که آیا نیاز است با ریسک‌ها برخورد شود و مناسب‌ترین راهبردها و روش‌های برخورد با ریسک چیست، ارائه می‌دهد. تحلیل ریسک همچنین یک ورودی به تصمیم‌گیری در زمانی ارائه می‌دهد که باید انتخابی صورت گیرد و گزینه‌ها شامل انواع و سطوح مختلفی از ریسک هستند.

تحلیل ریسک شامل در نظر گرفتن دلایل و منابع ریسک، عواقب مثبت و منفی آن‌ها و احتمال وقوع این عواقب است. فاکتورهایی که بر عواقب و احتمال اثر می‌گذراند بایستی شناسایی شوند. ریسک با تعیین عواقب و احتمال آن‌ها و دیگر وصفی‌های ریسک تحلیل می‌شود. یک رخداد می‌تواند عواقب چندگانه ای

---

۱ -استاندارد ملی ایران با استفاده از این منبع در حال تدوین است.

داشته باشد و می‌تواند بر چندین هدف اثر بگذارد. کنترل‌های موجود و اثربخشی و کارایی آن‌ها نیز بایستی به حساب آید.

نحوه بیان عواقب و احتمال آن‌ها و نحوه ترکیب آن‌ها برای تعیین سطح ریسک بایستی نوع ریسک، اطلاعات موجود و مقصود استفاده از خروجی ارزیابی ریسک را منعکس سازد. این موارد بایستی با معیارهای ریسک سازگار باشند. همچنین در نظر گرفتن وابستگی متقابل ریسک‌های مختلف و منابع آن‌ها مهم است.

اطمینان در تعیین سطح ریسک و حساسیت آن به پیش شرط‌ها و مفروضات بایستی در تحلیل در نظر گرفته شود و به طور اثربخش به تصمیم گیرندگان و در صورت مناسب بودن، دیگر علاقمندان انتقال یابد. فاکتورهایی چون واگرایی نظرات بین متخصصین، عدم قطعیت، در دسترس بودن، کیفیت، کمیت و مرتبط بودن پیوسته اطلاعات یا محدودیت‌ها در مدل‌سازی بایستی بیان شده و می‌توانند مورد تاکید قرار گیرند.

تحلیل ریسک می‌تواند با درجات مختلفی از جزئیات انجام گیرد که به ریسک، مقصود از تحلیل و اطلاعات، داده‌ها و منابع موجود بستگی دارد. تحلیل می‌تواند بسته به اوضاع و احوال، کیفی، نیمه کمّی یا کمّی یا ترکیبی از این‌ها باشد.

عواقب و احتمال آن‌ها می‌تواند با مدلسازی پیامدهای یک رخداد یا مجموعه ای از رخدادها یا با برون یابی از مطالعات آزمایشی یا از داده‌های موجود تعیین شود. عواقب را می‌توان از نظر تأثیرات محسوس و نامحسوس بیان کرد. در برخی موارد بیش از یک مقدار عددی یا توصیف گر برای مشخص کردن عواقب و احتمال آن‌ها برای زمان‌ها، مکان‌ها، گروه‌ها یا موقعیت‌های مختلف مورد الزام است.

۵-۴-۴ سنجش ریسک

مقصود از سنجش ریسک کمک در تصمیم گیری، بر اساس پیامدهای تحلیل ریسک در مورد این است که چه ریسک‌هایی نیاز به برخورد دارند و ارجحیت برای اجرای برخورد کدام است.

سنجش ریسک شامل مقایسه سطح ریسک یافت شده در طول فرآیند تحلیل با معیارهای ریسک است که در زمان بررسی فضا برقرار شده‌اند. براساس این مقایسه، نیاز به برخورد می‌تواند بررسی شود.

تصمیمات بایستی فضای گسترده‌تر ریسک را به حساب آورند و شامل در نظر گرفتن رواداری ریسک‌هایی شوند که طرفین متحمل می‌شوند، به جز سازمانی که از ریسک سود می‌برد. تصمیمات باید مطابق با الزامات قانونی و نظارتی و غیره گرفته شوند.

در برخی اوضاع و احوال، سنجش ریسک می‌تواند منجر به تصمیم به انجام تحلیل بیشتر شود. سنجش ریسک همچنین می‌تواند منجر به تصمیم به عدم برخورد با ریسک به طریقی جز حفظ کنترل‌های موجود شود. این تصمیم تحت تأثیر نگرش سازمان به ریسک و معیارهای ریسک برقرار شده است.

۵-۵ برخورد با ریسک

۵-۵-۱ کلیات

برخورد با ریسک شامل انتخاب یک یا چند گزینه برای تعدیل ریسک‌ها و اجرای این گزینه ها است. به محض اینکه برخوردها اجرا می‌شوند کنترل‌ها را فراهم یا تعدیل می‌کنند.

برخورد با ریسک شامل فرآیند گردشی موارد زیر است:

- ارزیابی برخورد با ریسک؛
- تصمیم در این مورد که آیا سطوح ریسک باقی مانده قابل تحمل هستند؛
- در صورتی که قابل تحمل نباشند، ایجاد برخورد با ریسکی جدید؛ و
- ارزیابی اثربخشی این برخورد.

گزینه‌های برخورد با ریسک لزوماً دو به دو متناظر نبوده یا در تمام اوضاع و احوال مناسب نیستند. گزینه‌ها می‌توانند شامل موارد زیر باشند:
الف) اجتناب از ریسک از طریق تصمیم به عدم آغاز یا ادامه به فعالیتی که ریسک را افزایش می‌دهد؛
ب) پذیرش ریسک یا افزایش آن به منظور تعقیب یک فرصت؛
پ) از میان برداشتن منبع ریسک؛
ت) تغییر راستنمایی؛
ث) تغییر عواقب؛
ج) به اشتراک گذاشتن ریسک با طرف یا طرف‌های دیگر (از جمله قراردادها و سرمایه گذاری ریسک)؛ و
چ) حفظ ریسک با تصمیم آگاهانه.

۵-۵-۲ انتخاب گزینه‌های برخورد با ریسک

انتخاب مناسب ترین گزینه برخورد با ریسک شامل ایجاد تعادل بین هزینه‌ها و تلاش‌های پیاده سازی و سود به دست آمده، با توجه به الزامات قانونی، نظارتی و دیگر الزامات از قبیل مسئولیت اجتماعی و حفاظت از محیط طبیعی است. تصمیمات بایستی همچنین ریسک‌هایی را به حساب آورند که می‌توانند برخورد با ریسکی را گارانتی کنند که بر اساس اقتصاد توجیه پذیر نیست، مانند ریسک‌های شدید (دارای عواقب بسیار منفی) اما نادر (با احتمال پایین).
تعدادی از گزینه‌های برخورد را می‌توان به صورت منفرد یا ترکیبی در نظر گرفته و به کار برد. سازمان معمولاً می‌تواند از اتخاذ ترکیبی از گزینه‌های برخورد سود ببرد.
در هنگام انتخاب گزینه‌های برخورد با ریسک، سازمان بایستی ارزش‌ها و ادراک‌های علاقمندان و مناسب ترین راه‌ها برای تبادل اطلاعات با آنان را در نظر بگیرد. هنگامی که گزینه‌های برخورد با ریسک می‌توانند در جای دیگری در سازمان یا بر علاقمندان تأثیرگذار باشند، این موارد بایستی در تصمیم گیری دخالت داشته باشند. برخی برخوردها با ریسک با این که به طور مساوی اثربخش هستند، می‌توانند برای برخی علاقمندان بیش از بقیه قابل قبول باشند.
طرح برخورد بایستی به روشنی ترتیب اولویتی را که طبق آن هر گزینه‌ی برخورد با ریسک‌های بایستی اجرا شوند، شناسایی کند.
خود برخورد با ریسک ممکن است ریسک‌هایی در بر داشته باشد. یک ریسک قابل توجه می‌تواند عدم موفقیت یا عدم اثربخشی اقدامات برخورد با ریسک باشد. نیاز است که پایش یک قسمت جدا نشدنی از طرح برخورد با ریسک باشد تا تضمین شود که اقدامات اثربخش باقی می‌مانند.

برخورد با ریسک همچنین می‌تواند ریسک‌های ثانوی را معرفی کند که نیاز است ارزیابی شوند، با آن‌ها برخورد شود و مورد پایش و بازنگری قرار گیرند. این ریسک‌های ثانوی بایستی در طرح برخوردی یکسان با ریسک اصلی جای گیرند و به عنوان ریسکی جدید با آن‌ها برخورد نشود. پیوند بین دو ریسک بایستی شناسایی و برقرار شود.

۵-۵-۳ آماده سازی و پیاده سازی طرح‌های برخورد با ریسک

مقصود از طرح‌های برخورد با ریسک، مستندسازی نحوه اجرای گزینه‌های برخورد انتخاب شده است. اطلاعات ارائه شده در طرح‌های برخورد بایستی شامل موارد زیر باشد:

- دلایل انتخاب گزینه‌های برخورد، از جمله سودهایی که انتظار می‌رود به دست آید؛
- افرادی که پاسخگوی تأیید طرح و افرادی که مسئول پیاده سازی طرح هستند؛
- اقدامات پیشنهادی؛
- الزامات منابع از جمله احتمال وقوع؛
- اقدامات و محدودیت‌های عملکرد؛
- الزامات گزارش دهی و پایش؛ و
- زمانبندی و برنامه زمانی.

طرح‌های برخورد بایستی در فرآیندهای مدیریت سازمان گنجانده شوند و با علاقمندان مناسب در مورد آن‌ها بحث شود.

تصمیم گیرندگان و دیگر علاقمندان بایستی از ماهیت و میزان ریسک باقی مانده پس از برخورد با ریسک آگاه باشند. ریسک باقی مانده بایستی مستند شود و مورد پایش، بازنگری و بر حسب اقتضا مورد برخورد بیشتر قرار گیرد.

۵-۶ پایش و بازنگری

پایش و همچنین بازنگری بایستی قسمتی طراحی شده از فرآیند مدیریت ریسک باشند و شامل وارسی یا نظارت منظم قرار گیرند. این امر می‌تواند دوره ای یا به صورت کاربرد موردی باشد.

مسئولیت‌های پایش و بازنگری بایستی به روشنی تعریف شوند.

فرآیندهای پایش و بازنگری بایستی برای مقاصد زیر دربردارنده تمام جنبه‌های فرآیندهای مدیریت ریسک باشند:

- حصول اطمینان از این که کنترل‌ها هم در طراحی و هم در بهره برداری اثربخش و کارآمد هستند؛
- کسب اطلاعات بیشتر برای بهبود ارزیابی ریسک؛
- تحلیل و درس گرفتن از رویدادها (از جمله عدم دستیابی به هدف)، تغییرات، روند ها، موفقیت‌ها و شکست ها؛

- کشف تغییرات در فضای خارجی و داخلی، از جمله تغییراتی در معیارهای ریسک و خود ریسک که می‌تواند مستلزم بازنگری برخورد با ریسک و اولویت‌ها باشد؛ و
- شناسایی ریسک‌هایی که ظاهر می‌شوند.

پیشروی در پیاده سازی طرح‌های برخورد با ریسک، مقیاسی عملکردی را فراهم می‌سازد. نتایج را می‌توان در مدیریت عملکرد کلی سازمان، اندازه گیری و فعالیت‌های گزارش دهی خارجی و داخلی جای داد.
نتایج پایش و بازنگری بایستی ثبت شوند و به طور مناسب به صورت خارجی و داخلی گزارش شوند و همچنین بایستی به عنوان ورودی‌های بازنگری چارچوب مدیریت ریسک به کار روند (به ۴-۵ مراجعه کنید).

۵-۷ ثبت فرآیند مدیریت ریسک

فعالیت‌های مدیریت ریسک بایستی قابل ردیابی باشند. در فرآیند مدیریت ریسک، سوابق اساسی را برای بهبود در روش‌ها و ابزارها و همچنین در فرآیند کلی فراهم می‌سازند.
تصمیمات در مورد ایجاد سوابق بایستی موارد زیر را به حساب آورند:

- نیازهای سازمان برای یادگیری مداوم؛
- مزایای استفاده مجدد از اطلاعات برای مقاصد مدیریتی؛
- هزینه‌ها و تلاش‌های به کار رفته در ایجاد و حفظ سوابق؛
- نیازهای قانونی، نظارتی و بهره برداری برای سوابق؛
- روش‌های دسترسی، راحتی قابلیت بازیابی و رسانه‌های ذخیره؛
- دوره نگهداری؛ و
- حساسیت اطلاعات.

پیوست الف

(اطلاعاتی)

وصفی‌های مدیریت ریسکِ ارتقا یافته

الف -۱ کلیات

تمامی سازمان‌ها بایستی برای سطح مناسب عملکرد چارچوب مدیریت ریسکشان، در کنار اهمیت تصمیماتی که قرار است اخذ شود، تلاش کنند. فهرست وصفی‌های زیر نمایش دهنده سطح بالایی از عملکرد در اداره‌ی ریسک است. برای کمک به سازمان در اندازه‌گیری عملکرد خود مطابق این معیارها، برخی از شاخص‌های محسوس برای هر وصفی ارائه شده اند.

الف -۲ پیامدهای کلیدی

الف-۲-۱ سازمان دارای درک جاری، صحیح و جامعی از ریسک هایش است.

الف-۲-۲ ریسک‌های سازمان در معیارهای ریسکش هستند.

الف -۳ وصفی ها

الف -۳-۱ بهبود مداوم

تاکید بر بهبود مداوم در مدیریت ریسک از طریق تعیین اهداف عملکرد سازمانی، اندازه‌گیری، بازنگری و تعدیل بعدی فرآیند ها، سیستم ها، منابع، توانمندی و مهارت‌ها صورت می‌گیرد.

این امر را می‌توان با وجود اهداف عملکرد صریح نشان داد که عملکرد سازمان و عملکرد مدیر در مقایسه با آن اندازه گیری می‌شود. عملکرد سازمان را می‌توان منتشر ساخته و انتقال داد. معمولاً حداقل یک بازنگری سالانه عملکرد و سپس تجدید نظر فرآیندها و تنظیم اهداف عملکرد اصلاح شده برای دوره بعدی وجود خواهد داشت.

ارزیابی عملکرد مدیریت ریسک قسمتی اصلی از ارزیابی عملکرد کلی سازمان و سیستم اندازه گیری برای بخش‌ها و افراد است.

الف -۳-۲ پاسخگویی کامل برای ریسک ها

مدیریت ریسک ارتقا یافته شامل پاسخگویی جامع، کاملاً تعریف شده و کاملاً پذیرفته شده برای ریسک ها، کنترل‌ها و تکالیف برخورد با ریسک است. افراد تعیین شده کاملاً پاسخگویی را بر عهده می‌گیرند، دارای مهارت‌های مناسب هستند و از منابع کافی برای وارسی کنترل ها، پایش ریسک ها، بهبود کنترل‌ها و تبادل اطلاعات مناسب در مورد ریسک‌ها و مدیریت آن‌ها با علاقمندان خارجی و داخلی برخوردارند.

این امر را می‌توان به این صورت نشان داد که تمام اعضای یک سازمان از ریسک ها، کنترل‌ها و تکالیفی که پاسخگوی آن‌ها هستند، آگاهی کامل داشته باشند. معمولاً این امر در توصیفات شغل/منصب، پایگاه‌های داده‌ها یا سیستم‌های اطلاعاتی ثبت می‌شود. تعریف نقش‌های مدیریت ریسک، پاسخگویی‌ها و مسئولیت‌ها بایستی قسمتی از تمام برنامه‌های القاء سازمان باشد.
سازمان اطمینان می‌دهد که افرادی که پاسخگو هستند دارای تجهیزات لازم برای ایفای نقش خود هستند. این کار با فراهم ساختن اختیار، زمان، آموزش، منابع و مهارت‌های کافی برای آنان، برای به عهده گرفتن پاسخگویی شان انجام می‌گیرد.

الف-۳-۳ کاربرد مدیریت ریسک در کل تصمیم گیری ها

کل تصمیم گیری‌ها در سازمان، با هر سطح اهمیت و معناداری، به میزان مناسبی شامل در نظر گرفتن آشکار ریسک‌ها و به کارگیری مدیریت ریسک می‌باشد.
این امر را می‌توان با سوابق جلسات و تصمیماتی برای نشان دادن این که بحث‌های آشکار درمورد ریسک صورت گرفته اند، نشان داد. به علاوه بایستی نمایش تمام اجزاء مدیریت ریسک در فرآیندهای کلیدی برای تصمیم گیری در سازمان امکان پذیر باشد، مثلاً برای تصمیماتی در مورد تخصیص سرمایه، در مورد پروژه-های اصلی و در مورد ساختار بندی مجدد و تغییرات سازمانی. به این دلایل مدیریت ریسک با پایه صحیح در سازمان اساس حکمرانی اثربخش را فراهم می‌سازد.

الف -۳-۴ تبادل اطلاعات مداوم

مدیریت ریسک ارتقا یافته شامل تبادل اطلاعات مداوم با علاقمندان داخلی و خارجی است، از جمله گزارش دهی جامع و تکراری عملکرد مدیریت ریسک به عنوان قسمتی از حکمرانی خوب.
این امر را می‌توان با تبادل اطلاعات با علاقمندان به عنوان قسمتی جدا نشدنی و اساسی از مدیریت ریسک نشان داد. تبادل اطلاعات به درستی فرآیندی دوطرفه محسوب می‌شود، چنان که تصمیمات آگاهانه مناسب را می‌توان در مورد سطح ریسک‌ها و همچنین نیاز به برخورد با ریسک مطابق با معیارهای ریسک جامع و برقرار شده به طور مناسب، اتخاذ کرد.
گزارش دهی جامع و تکراری خارجی و داخلی در مورد ریسک‌های قابل توجه و عملکرد مدیریت ریسک به طور اساسی به حکمرانی اثربخش درون سازمان کمک می‌کند.

الف-۳-۵ انسجام کامل در ساختار حکمرانی سازمان

مدیریت ریسک در بین فرآیندهای مدیریت سازمان، فرآیندی مرکزی محسوب می‌شود، چنان که ریسک‌ها را با توجه به تأثیر عدم قطعیت روی اهداف در نظر می‌گیرند. ساختار و فرآیند حکمرانی بر اساس مدیریت ریسک هستند. مدیران، مدیریت ریسک اثربخش را برای دستیابی به اهداف سازمان ضروری می‌دانند.
این امر با زبان مدیران و مواد مکتوب مهم در سازمان با استفاده از اصطلاح «عدم قطعیت» در ارتباط با ریسک ها، نشان داده می‌شود. این وصفی همچنین معمولاً در بیانیه‌های خط مشی سازمان، به ویژه موارد مربوط به مدیریت ریسک منعکس می‌شود. معمولاً این وصفی از طریق مصاحبه با مدیران و شواهد اقدامات و گفته‌هایشان تصدیق می‌شود.

کتابنامه

[1] ISO Guide 73:2009, Risk management — Vocabulary[1]
[2] ISO/IEC 31010, Risk management — Risk assessment techniques[2]

۱- استاندارد ملی ایران با استفاده از این منبع در حال تدوین است.
۲- استاندارد ملی ایران با استفاده از این منبع در حال تدوین است.