

استاندارد مدیریت ریسک

مترجم و نویسنده : دکتر مجتبی رستمی نوروزآباد

شناسنامه گزارش

عنوان نسخه اصلی : استاندارد مدیریت ریسک

تدوین کنندگان نسخه اصلی : موسسه مدیریت ریسک ، انجمن مدیران بیمه و ریسک و انجمن مدیریت ریسک بخش عمومی

سال انتشار نسخه اصلی : ۲۰۰۲

نهاد پذیرنده سند : فدراسیون انجمن های مدیریت ریسک اروپا

مترجم و نویسنده بخش ارزیابی تحلیلی : دکتر مجتبی رستمی نوروزآباد

حوزه تخصصی : مدیریت ریسک سازمانی ، حاکمیت ریسک و استانداردهای مدیریت ریسک

انتشار ترجمه فارسی : شهریورماه ۱۴۰۵

تحلیل تخصصی موضوعات مالی و حسابداری - Rashtiani.Ir

فهرست مطالب

۴	مقدمه مترجم
۶	مقدمه
۸	۱- ریسک
۸	۲- مدیریت ریسک
۹	۲-۱ - عوامل بیرونی و درونی
۱۱	۳- ارزیابی ریسک
۱۱	۴- تحلیل ریسک
۱۱	۴-۱ - شناسایی ریسک
۱۲	۴-۲ - توصیف ریسک
۱۳	۴-۳ - برآورد ریسک
۱۴	۴-۴ - روش ها و تکنیک های تحلیل ریسک
۱۵	۴-۵ - پروفایل ریسک
۱۵	۵- ارزشیابی ریسک
۱۵	۶- گزارش دهی و ارتباطات ریسک
۱۵	۶-۱ - گزارش دهی داخلی
۱۷	۶-۲ - گزارش دهی بیرونی

۱۸	۷- مواجهه یا ریسک
۱۹	۸- پایش و بازنگری فرایند مدیریت ریسک
۲۰	۹- ساختار و اداره مدیریت ریسک
۲۰	۹-۱ - خط مشی مدیریت ریسک
۲۰	۹-۲ - نقش هیئت مدیره
۲۱	۹-۳ - نقش واحدهای کسب و کار
۲۱	۹-۴ - نقش واحد مدیریت ریسک
۲۲	۹-۵ - نقش حسابرسی داخلی
۲۲	۹-۶ - منابع و اجرا
۲۳	۱۰- پیوست
۲۵	۱۱- ارزیابی تحلیلی استاندارد مدیریت ریسک ۲۰۰۲
۲۵	۱۱-۱ - جایگاه تاریخی سند
۲۶	۱۱-۲ - نقاط قوت ماندگار سند
۲۶	۱۱-۲-۱ - پیوند مدیریت ریسک با اهداف و راهبرد
۲۶	۱۱-۲-۲ - شناسایی دو سوی ریسک
۲۷	۱۱-۲-۳ - سادگی و قابلیت فهم برای مدیران
۲۷	۱۱-۲-۴ - تأکید بر مسئولیت سازمانی
۲۸	۱۱-۲-۵ - پرهیز از تجویزگرایی و صدور گواهی
۲۸	۱۱-۳ - محدودیت های مفهومی و روش شناختی
۲۸	۱۱-۳-۱ - تعریف ریسک
۲۸	۱۱-۳-۲ - فقدان تفکیک روشن میان اصول، چارچوب و فرایند
۲۹	۱۱-۳-۳ - غلبه نگاه فرایندی و نسبتاً خطی

۲۹	۱-۳-۴- ابهام میان معیار ریسک، تحمل ریسک و اشتباهی ریسک
۳۰	۱-۳-۵- محدودیت مقیاس های ارزیابی
۳۰	۱-۳-۶- توجه محدود به عوامل انسانی و فرهنگی
۳۰	۱-۳-۷- نگاه محدود به وابستگی و پویایی ریسک ها
۳۱	۱-۴- مقایسه با ایزو ۲۰۱۸:۳۱۰۰۰
۳۳	۱-۵- ارزیابی حاکمیت و مسئولیت های سازمانی
۳۳	۱-۵-۱- نقش هیئت مدیره
۳۳	۱-۵-۲- نقش واحدهای کسب و کار
۳۳	۱-۵-۳- نقش واحد مدیریت ریسک
۳۴	۱-۵-۴- نقش حسابرسی داخلی
۳۴	۱-۶- موضوعاتی که برای استفاده امروزی باید به سند افزوده شوند
۳۴	۱-۶-۱- مدیریت ریسک به عنوان پشتیبان تصمیم گیری
۳۵	۱-۶-۲- فرهنگ و رفتار ریسک
۳۵	۱-۶-۳- تاب آوری سازمانی
۳۵	۱-۶-۴- ریسک های نوظهور و به هم پیوسته
۳۵	۱-۶-۵- سنجش اثربخشی مدیریت ریسک
۳۶	۱-۷- حدود کاربرد سند در سازمان های امروزی
۳۷	۱-۸- جمع بندی و داوری نهایی
۳۷	منابع

مقدمه مترجم

ترجمه سندی که بیش از دو دهه از انتشار آن می گذرد، زمانی ارزشمند است که به فهم بهتر مسائل امروز نیز کمک کند. «استاندارد مدیریت ریسک» از این ظرفیت برخوردار است. این سند در متنی کوتاه، مدیریت ریسک را به اهداف و راهبرد سازمان پیوند می دهد، مسئولیت آن را در سراسر سازمان توزیع می کند و مخاطب را با مراحل اصلی شناسایی، تحلیل، ارزشیابی، مواجهه، گزارش دهی و پایش ریسک آشنا می سازد. همین ترکیب اختصار و نگاه سازمانی، دلیل اصلی انتخاب آن برای ترجمه و بررسی بوده است.

یکی از نکات آموزنده سند آن است که بسیاری از مسائل مطرح در مدیریت ریسک امروز، در سال ۲۰۰۲ نیز مورد توجه نهادهای حرفه ای قرار داشته اند. مسئولیت هیئت مدیره در نظارت بر ریسک، مالکیت ریسک در واحدهای کسب و کار، ضرورت پیوند مدیریت ریسک با فرهنگ سازمان و توجه هم زمان به تهدیدها و فرصت ها، از جمله این موضوعات اند. مطالعه سند نشان می دهد که دشواری مدیریت ریسک همیشه ناشی از فقدان مفهوم یا چارچوب نیست؛ تبدیل این مفاهیم به تصمیم ها، رفتارها و مسئولیت های واقعی سازمان نیز اهمیت دارد.

ارزش کاربردی سند به ویژه در بخش هایی آشکار می شود که انتظارات مدیریتی را روشن می کنند. الگوی توصیف ریسک، تفکیک اطلاعات مورد نیاز هیئت مدیره و واحدهای کسب و کار و توضیح مسئولیت های سازمانی، همچنان برای آموزش و گفت و گو درباره مدیریت ریسک مفیدند. این مطالب می توانند به مدیران کمک کنند تا مدیریت ریسک را فراتر از تکمیل فرم ها، تهیه نقشه حرارتی یا تنظیم گزارش های دوره ای ببینند.

با این حال، این ظرفیت نباید موجب نادیده گرفتن محدودیت های سند شود. تعریف ریسک، سامان دهی مراحل ارزیابی، مقیاس های احتمال و پیامد و برخی توصیف های مربوط به نقش های سازمانی، متأثر از ادبیات حرفه ای زمان انتشار آن هستند. برای مثال، تعریف ریسک به عنوان ترکیبی از احتمال وقوع رویداد و پیامدهای آن، با تعریف «اثر عدم قطعیت بر اهداف» در ایزو ۳۱۰۰:۲۰۱۸ تفاوت دارد. همچنین، سند به فرهنگ، اشتیاق ریسک و پیوند با راهبرد اشاره می کند، اما این مفاهیم را با تفصیل و انسجام لازم برای پاسخ گویی به همه نیازهای اجرایی امروز توسعه نمی دهد.

ارزیابی چنین متنی مستلزم رعایت دو ملاحظه است. نخست، باید آن را در بستر تاریخی و با توجه به هدف و دامنه اعلام شده خود مطالعه کرد. از یک راهنمای عمومی و فشرده نمی توان انتظار داشت تمام جزئیات استقرار مدیریت ریسک یا روش های تخصصی تحلیل را پوشش دهد. دوم، ارزش تاریخی سند نباید مانع بررسی محدودیت های کاربرد امروزی آن شود. ممکن است توصیه ای در زمان انتشار مفید بوده باشد، اما اجرای آن در سازمان امروز به توضیح، تعدیل یا تکمیل نیاز داشته باشد.

در ترجمه حاضر، ساختار، ترتیب مطالب و مقصود متن اصلی مبنا قرار گرفته است. جمله بندی فارسی با هدف انتقال دقیق معنا و روانی بیان تنظیم شده و مفاهیم جدید به متن ترجمه افزوده نشده اند. معادل های انگلیسی و توضیحات تکمیلی در پانویس ها ارائه شده اند تا خواننده بتواند محتوای سند را از توضیحات مترجم تشخیص دهد.

برای حفظ این تمایز، مقدمه سند اصلی و بخش های ۱ تا ۱۰ به ترجمه اختصاص یافته اند و ارزیابی تفصیلی پس از پایان ترجمه، در بخش مستقل ۱۱ آمده است. بخش ۱۱ تألیف اینجانب است و جزئی از استاندارد سال ۲۰۰۲ به شمار نمی رود. در این بخش، مفاهیم و توصیه های سند با مراجعه به ادبیات مدیریت ریسک سازمانی، حاکمیت ریسک و مدیریت ریسک راهبردی و با مقایسه با ایزو ۳۱۰۰:۲۰۱۸، چارچوب مدیریت ریسک سازمانی کوزو و مدل سه خطی مؤسسه حسابرسان داخلی بررسی شده اند.

هدف این ارزیابی، روشن کردن نسبت میان آموزه های سند و نیازهای سازمان های امروزی است. در هر مورد باید مشخص شود که توصیه ای همچنان قابل استفاده است، برای اجرا به توضیح بیشتری نیاز دارد یا باید در چارچوبی گسترده تر باز تفسیر شود. به همین دلیل، موضوع اصلی تحلیل صرفاً قدمت سند نیست؛ کفایت مفاهیم و ابزارهای آن برای تصمیم و کاربرد مورد نظر نیز بررسی می شود.

امید است این ترجمه و ارزیابی، هم برای آشنایی با یکی از متون حرفه ای مدیریت ریسک سودمند باشد و هم به مطالعه دقیق تر استانداردها کمک کند. استانداردها زمانی به سازمان یاری می رسانند که منطق، دامنه کاربرد و محدودیت های آنها شناخته شود و آموزه هایشان در تصمیم گیری، تخصیص منابع و پاسخ گویی مدیران به کار گرفته شود.

مقدمه

این استاندارد مدیریت ریسک حاصل کار گروهی متشکل از نمایندگان نهادهای اصلی مدیریت ریسک در بریتانیا، از جمله مؤسسه مدیریت ریسک، است.

علاوه بر این، گروه تدوین کننده طی یک دوره مشورتی گسترده، دیدگاه ها و نظرات طیف وسیعی از دیگر نهادهای حرفه ای علاقه مند به مدیریت ریسک را نیز دریافت کرد.

مدیریت ریسک حوزه ای است که به سرعت در حال توسعه است و درباره اینکه مدیریت ریسک چه موضوعاتی را در بر می گیرد، چگونه باید اجرا شود و چه هدفی دارد، دیدگاه ها و توصیف های متعدد و متفاوتی وجود دارد. وجود نوعی استاندارد برای اطمینان از دستیابی به توافق درباره موارد زیر ضروری است:

-اصطلاحات مرتبط با واژه های به کار رفته؛

-فرایندی که مدیریت ریسک از طریق آن اجرا می شود؛

-ساختار سازمانی مدیریت ریسک؛

-هدف مدیریت ریسک.

نکته مهم آن است که این استاندارد، ریسک را دارای هر دو جنبه مثبت و منفی می داند.

مدیریت ریسک تنها مختص شرکت ها یا سازمان های عمومی نیست، بلکه درباره هر فعالیتی، اعم از کوتاه مدت یا بلندمدت، کاربرد دارد. منافع و فرصت ها را نباید فقط در چارچوب خود فعالیت در نظر گرفت، بلکه باید آنها را در ارتباط با ذی نفعان متعدد و گوناگونی بررسی کرد که ممکن است تحت تأثیر قرار گیرند.

برای تحقق اهداف مدیریت ریسک، روش های متعددی وجود دارد و نمی توان همه آنها را در یک سند بیان کرد. بنابراین، هدف از تدوین این سند ارائه استانداردی تجویزی نبوده است که سازمان ها را به رعایت صوری و چک لیستی الزامات سوق دهد. همچنین، این سند برای ایجاد فرایندی که مبنای صدور گواهی قرار گیرد تدوین نشده است. سازمان ها می توانند اجزای مختلف این استاندارد را، هر چند به روش های متفاوت، اجرا کنند و سپس انطباق خود را با آن گزارش دهند. این استاندارد بیانگر رویه برتری است که سازمان ها می توانند وضعیت خود را با آن مقایسه و ارزیابی کنند.

در این استاندارد، تا حد امکان، از اصطلاحات مربوط به ریسک استفاده شده است که سازمان بین المللی استانداردسازی در سند جدید خود، «راهنمای ۷۳ ایزو/آی ای سی؛ مدیریت ریسک، واژگان و رهنمودهایی برای استفاده در استانداردها»، ارائه کرده است.

با توجه به تحولات سریع این حوزه، نویسندگان از سازمان هایی که این استاندارد را به کار می گیرند درخواست کرده اند دیدگاه ها و بازخوردهای خود را برای آنان ارسال کنند (نشانی های مربوط در پشت جلد این راهنما درج شده اند). قرار بر این بوده است که استاندارد با توجه به تحولات رویه های برتر، به طور منظم اصلاح شود.

۱-ریسک

ریسک را می توان ترکیبی از احتمال وقوع یک رویداد و پیامدهای آن تعریف کرد.

در هر نوع فعالیت، ممکن است رویدادها و پیامدهایی به وجود آیند که فرصت هایی برای کسب منفعت، یعنی جنبه مثبت ریسک، یا تهدیدهایی برای موفقیت، یعنی جنبه منفی ریسک، ایجاد کنند.

امروزه بیش از پیش پذیرفته شده است که مدیریت ریسک یا هر دو جنبه مثبت و منفی ریسک سروکار دارد. از این رو، این استاندارد ریسک را از هر دو جنبه بررسی می کند.

در حوزه ایمنی، عموماً پذیرفته شده است که پیامدها فقط جنبه منفی دارند؛ بنابراین، مدیریت ریسک ایمنی بر پیشگیری از زیان و کاهش آن متمرکز است؛

۲-مدیریت ریسک

مدیریت ریسک بخش اصلی مدیریت راهبردی هر سازمان است. مدیریت ریسک فرایندی است که سازمان ها از طریق آن، ریسک های مرتبط با فعالیت های خود را به صورت نظام مند مدیریت می کنند تا در هر فعالیت و در مجموعه تمام فعالیت ها، به منفعتی پایدار دست یابند.

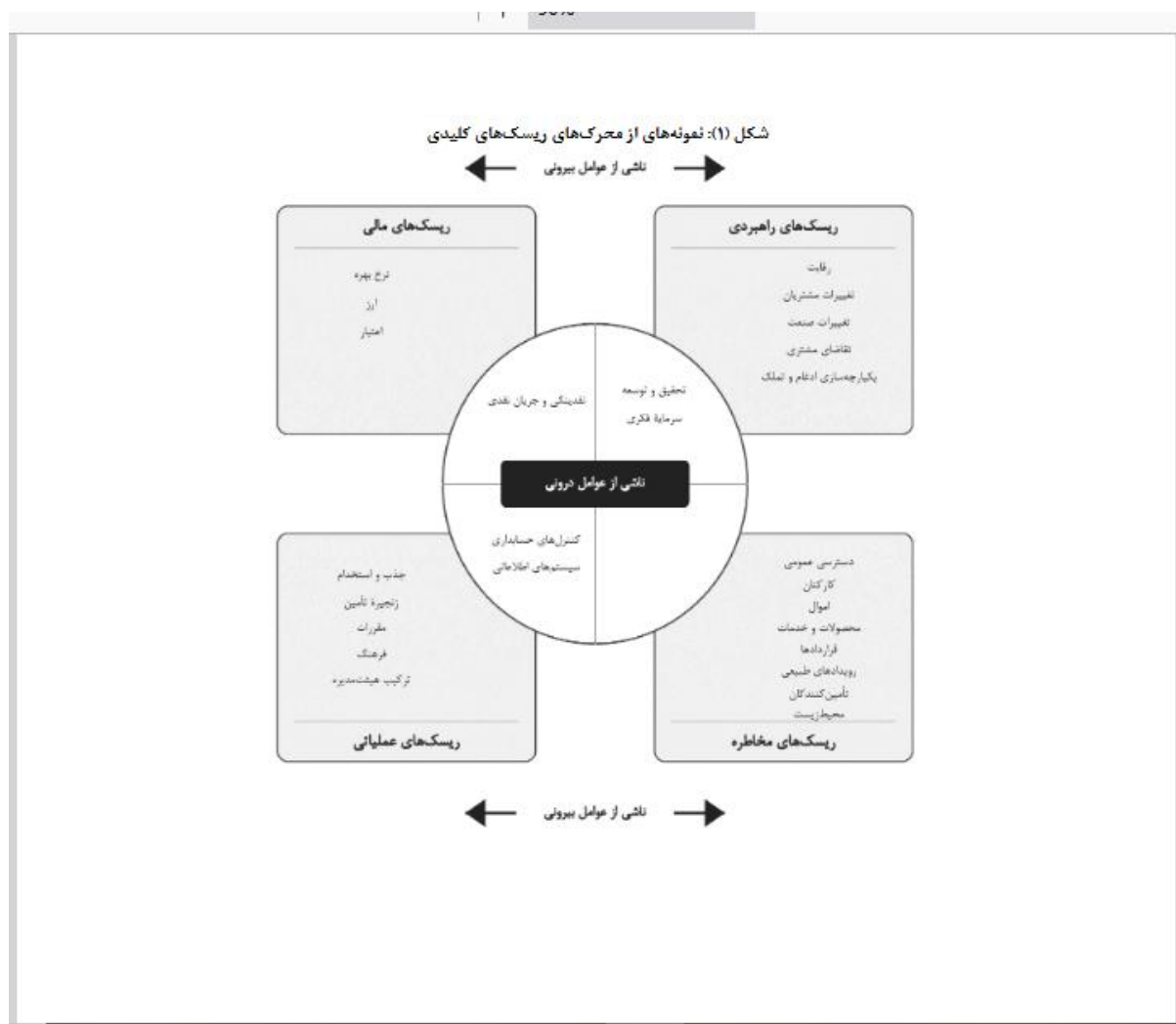
مدیریت ریسک مناسب بر شناسایی و مواجهه با این ریسک ها تمرکز دارد. هدف آن، ایجاد بیشترین ارزش پایدار در تمام فعالیت های سازمان است. مدیریت ریسک، شناخت عوامل دارای پیامدهای مثبت یا منفی برای سازمان را سامان می دهد. این کار احتمال موفقیت را افزایش می دهد و در مقابل، احتمال شکست و عدم قطعیت در دستیابی به اهداف کلی سازمان را کاهش می دهد.

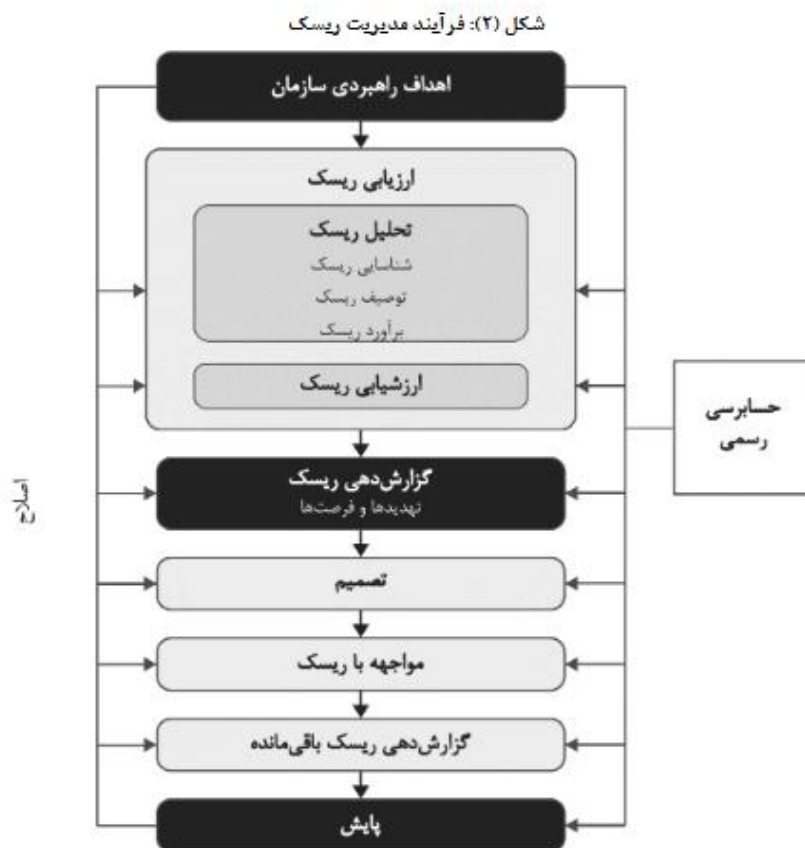
مدیریت ریسک باید فرایندی مستمر و در حال توسعه باشد که در سراسر راهبرد سازمان و اجرای آن جریان داشته باشد. این فرایند باید تمام ریسک های مرتبط با فعالیت های گذشته، حال و به ویژه آینده سازمان را به صورت نظام مند در برگرد مدیریت ریسک باید از طریق یک خط مشی اثربخش و برنامه ای تحت هدایت عالی ترین سطح مدیریت، در فرهنگ سازمان ادغام شود. این فرایند باید راهبرد را به اهداف تاکتیکی و عملیاتی تبدیل کند و مسئولیت ها را در سراسر سازمان به گونه ای تعیین کند که مدیریت ریسک، بخشی از شرح وظایف هر مدیر و هر کارمند باشد. مدیریت ریسک از پاسخ گویی، ارزیابی عملکرد و نظام پاداش پشتیبانی می کند و از این طریق، کارایی عملیاتی را در تمام سطوح سازمان افزایش می دهد.

۲-۱- عوامل بیرونی و درونی

ریسک های پیش روی سازمان و عملیت آن ممکن است از عوامل بیرونی یا درونی سازمان ناشی شوند.

نمودار (۱)، نمونه هایی از ریسک های اصلی در این دو حوزه را به طور خلاصه نشان می دهد. این نمودار همچنین نشان می دهد که برخی ریسک های مشخص ممکن است هم زمان محرک های بیرونی و درونی داشته باشند و در نتیجه، در هر دو حوزه قرار گیرند. این ریسک ها را می توان به انواع دیگری مانند ریسک های راهبردی، مالی، عملیاتی، مخاطره آمیز و موارد مشابه نیز طبقه بندی کرد.





مدیریت ریسک با کمک به تحقق اهداف سازمان، از سازمان و ذی نفعان آن محافظت می‌کند و برای آنها ارزش می‌آفریند.

این امر از راه‌های زیر تحقق می‌یابد:

- فراهم کردن چارچوبی برای سازمان که امکان می‌دهد فعالیت‌های آتی به صورت منسجم و کنترل شده انجام شوند؛
- بهبود تصمیم‌گیری، برنامه‌ریزی و اولویت‌بندی از طریق شناختی جامع و ساختار یافته از فعالیت‌های کسب و کار، نوسان‌پذیری و فرصت‌ها و تهدیدهای مرتبط با پروژه‌ها؛
- کمک به استفاده و تخصیص کارآمدتر سرمایه و منابع در سازمان؛
- کاهش نوسان‌پذیری در بخش‌های غیرمحموری کسب و کار؛
- حفاظت از دارایی‌ها و اعتبار شرکت و ارتقای آنها؛
- توسعه و پشتیبانی از کارکنان و پایگاه دانشی سازمان؛
- بهینه‌سازی کارایی عملیاتی.

۳- ارزیابی ریسک

راهنمای ۷۳ ایزو/آی ای سی، ارزیابی ریسک را فرایند کلی تحلیل ریسک و ارزشیابی ریسک تعریف می کند (به پیوست مراجعه کنید).

۴- تحلیل ریسک

۴-۱- شناسایی ریسک

هدف از شناسایی ریسک، شناسایی میزان مواجهه سازمان با عدم قطعیت است. این کار مستلزم شناختی عمیق از سازمان، بازاری که در آن فعالیت می کند و محیط قانونی، اجتماعی، سیاسی و فرهنگی پیرامون آن است. همچنین، باید شناختی دقیق از اهداف راهبردی و عملیاتی سازمان، عوامل حیاتی موفقیت آن و تهدیدها و فرصت های مرتبط با دستیابی به این اهداف به دست آید.

شناسایی ریسک باید به صورت نظام مند انجام شود تا اطمینان حاصل شود که تمام فعالیت های با اهمیت سازمان شناسایی و ریسک های ناشی از آنها تعریف شده اند. همچنین، تمام نوسان های مرتبط با این فعالیت ها باید شناسایی و طبقه بندی شوند.

فعالیت ها و تصمیمات کسب و کار را می توان به روش های مختلف طبقه بندی کرد. نمونه هایی از این طبقه بندی عبارت اند از:

- **راهبردی:** این ریسک ها به اهداف راهبردی بلندمدت سازمان مربوط می شوند. عواملی مانند دسترسی به سرمایه، ریسک های حاکمیتی و سیاسی، تغییرات قانونی و مقرراتی، شهرت و تغییرات محیط فیزیکی می توانند بر آنها اثر بگذارند.

- **عملیاتی:** این ریسک ها به مسائل روزمره ای مربوط می شوند که سازمان در مسیر تحقق اهداف راهبردی خود با آنها روبه رو است.

- **مالی:** این ریسک ها به مدیریت و کنترل اثربخش منابع مالی سازمان و آثار عوامل بیرونی مانند دسترسی به اعتبار، نرخ ارز، تغییرات نرخ بهره و دیگر مواجهه های بازار مربوط می شوند.

- **مدیریت دانش:** این ریسک ها به مدیریت و کنترل اثربخش منابع دانشی و چگونگی ایجاد، حفاظت و انتقال آنها مربوط می شوند. عوامل بیرونی ممکن است شامل استفاده یا بهره برداری غیرمجاز از مالکیت فکری، قطع برق منطقه و فناوری های رقابتی باشند. اختلال در عملکرد سیستم ها یا از دست دادن کارکنان کلیدی نیز ممکن است از عوامل درونی باشند.

–**انطباق:** این ریسک ها موضوعاتی مانند بهداشت و ایمنی، محیط زیست، مشخصات و اطلاعات تجاری، حمایت از مصرف کننده، حفاظت از داده ها، رویه های استخدامی و مسائل مقرراتی را در بر می گیرند.

اگر چه شناسایی ریسک می تواند به وسیله مشاوران بیرونی انجام شود، رویکرد درون سازمانی که از فرایندها و ابزارهای مشخص، سازگار و هماهنگ برخوردار باشد و به خوبی در سراسر سازمان انتقال یافته باشد، احتمالاً اثربخشی بیشتری خواهد داشت (به پیوست، مراجعه کنید). وجود «مالکیت» درون سازمانی نسبت به فرایند مدیریت ریسک ضروری است.

۴-۲- توصیف ریسک

هدف از توصیف ریسک، نمایش ریسک های شناسایی شده در قالبی ساختار یافته، برای مثال در یک جدول، است جدول توصیف ریسک که در ادامه آمده است، می تواند توصیف و ارزیابی ریسک ها را تسهیل کند. استفاده از ساختاری مناسب برای اطمینان از جامعیت فرایند شناسایی، توصیف و ارزیابی ریسک ضروری است. با بررسی پیامد و احتمال هر یک از ریسک های درج شده در جدول، باید بتوان ریسک های کلیدی را که به تحلیل دقیق تری نیاز دارند، اولویت بندی کرد. ریسک های مرتبط با فعالیت های کسب و کار و تصمیم گیری را می توان در گروه های راهبردی، پروژه ای یا تاکتیکی و عملیاتی طبقه بندی کرد. مدیریت ریسک بایداز مرحله شکل گیری مفهوم اولیه پروژه در آن گنجانده شود و در سراسر عمر هر پروژه نیز ادامه یابد.

جدول (۱): توصیف ریسک

ردیف	مؤلفه	شرح
۱	نام ریسک	-
۲	دامنه ریسک	توصیف کیفی رویدادها، اندازه، نوع، تعداد و وابستگی های آنها
۳	ماهیت ریسک	برای مثال، راهبردی، عملیاتی، مالی، مدیریت دانش یا انطباق
۴	ذی نفعان	ذی نفعان و انتظارات آنها
۵	کمی سازی ریسک	میزان اهمیت و احتمال
۶	تحمل ریسک یا اشتباهی ریسک	ظرفیت بالقوه زیان و اثر مالی ریسک؛ ارزش در معرض ریسک؛ احتمال و اندازه زیان ها یا منافع بالقوه؛ هدف یا اهداف کنترل ریسک و سطح عملکرد مورد نظر
۷	مواجهه با ریسک و سازوکارهای کنترلی	روش های اصلی مدیریت فعلی ریسک؛ میزان اطمینان به کنترل های موجود؛ تعیین رویه های پایش و بازنگری
۸	اقدامات بالقوه برای بهبود	توصیه هایی برای کاهش ریسک
۹	تحولات راهبرد و خط مشی	تعیین واحد مسئول تدوین راهبرد و خط مشی

۴-۳- برآورد ریسک

برآورد ریسک می تواند با توجه به احتمال وقوع و پیامد احتمالی آن، به صورت کمی، نیمه کمی یا کیفی انجام شود.

برای مثال، پیامدهای مربوط به تهدیدها، یعنی ریسک های دارای جنبه منفی، و فرصت ها، یعنی ریسک های دارای جنبه مثبت، می توانند زیاد، متوسط یا کم باشند (جدول ۲). احتمال نیز می تواند زیاد، متوسط یا کم باشد؛ اما تعریف این سطوح برای تهدیدها و فرصت ها متفاوت است (جدول های ۳ و ۴).

نمونه هایی در جدول های بعد ارائه شده اند. سازمان های مختلف ممکن است معیارهای متفاوتی را برای سنجش پیامد و احتمال متناسب با نیازهای خود بدانند.

برای مثال، بسیاری از سازمان ها ارزیابی پیامد و احتمال در سه سطح زیاد، متوسط و کم را برای نیازهای خود کافی می دانند و نتایج را در قالب ماتریس ۳ در ۳ ارائه می کنند. برخی دیگر از سازمان ها نیز بر این باورند که ارزیابی پیامد و احتمال با استفاده از ماتریس ۵ در ۵، ارزشیابی مناسب تری در اختیار آنها قرار می دهد.

جدول (۲): پیامدها برای تهدیدها و فرصت ها

سطح	شرح
زیاد	اثر مالی بر سازمان احتمالاً بیش از مبلغ «X» پوند خواهد بود اثر بااهمیتی بر راهبرد یا فعالیت های عملیاتی سازمان خواهد داشت نگرانی قابل توجهی برای ذی نفعان ایجاد خواهد کرد.
متوسط	اثر مالی بر سازمان احتمالاً بین مبالغ «X» و «Y» پوند خواهد بود. اثر متوسطی بر راهبرد یا فعالیت های عملیاتی سازمان خواهد داشت نگرانی متوسطی برای ذی نفعان ایجاد خواهد کرد.
کم	اثر مالی بر سازمان احتمالاً کمتر از مبلغ «Y» پوند خواهد بود. اثر اندکی بر راهبرد یا فعالیت های عملیاتی سازمان خواهد داشت نگرانی اندکی برای ذی نفعان ایجاد خواهد کرد.

جدول (۳): احتمال وقوع تهدیدها

برآورد	توصیف	شاخص ها
زیاد (محتمل)	احتمال دارد هر سال رخ دهد یا احتمال وقوع آن بیش از ۲۵ درصد است.	ممکن است در دوره زمانی مورد نظر، برای مثال طی ده سال، چندین بار رخ دهد. به تازگی رخ داده است.
متوسط (ممکن)	احتمال دارد طی یک دوره ده ساله رخ دهد یا احتمال وقوع آن کمتر از ۲۵ درصد است	ممکن است در دوره زمانی مورد نظر، برای مثال طی ده سال، بیش از یک بار رخ دهد. ممکن است به دلیل برخی عوامل بیرونی، کنترل آن دشوار باشد. آیا سابقه وقوع دارد؟
کم (بعید)	احتمال نمی رود طی یک دوره ده ساله رخ دهد یا احتمال وقوع آن کمتر از ۲ درصد است	تاکنون رخ نداده است احتمال وقوع آن اندک است.

جدول (۴): احتمال وقوع فرصت ها

برآورد	توصیف	شاخص ها
زیاد (محتمل)	احتمال دارد نتیجه مطلوب طی یک سال محقق شود یا احتمال وقوع آن بیش از ۷۵ درصد است	فرصتی روشن است که با اطمینان معقول می توان بر تحقق کوتاه مدت آن بر پایه فرایندهای مدیریتی موجود تکیه کرد
متوسط (ممکن)	چشم انداز معقولی برای دستیابی به نتایج مطلوب طی یک سال وجود دارد و احتمال وقوع آن بین ۲۵ تا ۷۵ درصد است	فرصت هایی که ممکن است تحقق یابند، اما به مدیریت دقیق نیاز دارند. فرصت هایی که ممکن است افزون بر موارد پیش بینی شده در برنامه ایجاد شوند.
کم (بعید)	احتمال دستیابی به نتیجه مطلوب در میان مدت وجود دارد یا احتمال وقوع آن کمتر از ۲۵ درصد است.	فرصتی بالقوه که مدیریت هنوز آن را به طور کامل بررسی نکرده است. فرصتی که با توجه به منابع مدیریتی اختصاص یافته در حال حاضر، احتمال موفقیت آن اندک است.

۴-۴- روش ها و تکنیک های تحلیل ریسک

برای تحلیل ریسک ها می توان از تکنیک های مختلفی استفاده کرد. برخی از این تکنیک ها به ریسک های دارای جنبه مثبت یا ریسک های دارای جنبه منفی اختصاص دارند و برخی دیگر قابلیت بررسی هر دو را دارند. نمونه هایی از این تکنیک ها در پیوست ارائه شده اند.

۴-۵- پروفایل ریسک

از نتایج فرایند تحلیل ریسک می توان برای تهیه پروفایل ریسک استفاده کرد. پروفایل ریسک به هر ریسک امتیازی بر اساس میزان اهمیت آن اختصاص می دهد و ابزاری برای اولویت بندی اقدامات مواجهه با ریسک فراهم می کند. به این ترتیب، ریسک های شناسایی شده بر اساس اهمیت نسبی آنها رتبه بندی می شوند.

این فرایند امکان می دهد هر ریسک به حوزه کسب و کار تحت تأثیر آن مرتبط شود، رویه های کنترلی اصلی موجود برای آن تشریح شوند و حوزه هایی مشخص شوند که ممکن است لازم باشد میزان سرمایه گذاری در کنترل ریسک در آنها افزایش، کاهش یا باز تخصیص یابد.

پاسخ گویی کمک می کند تا «مالکیت ریسک» به رسمیت شناخته شود و منابع مدیریتی مناسب به آن اختصاص یابد.

۵- ارزشیابی ریسک

پس از تکمیل فرایند تحلیل ریسک، لازم است ریسک های برآورد شده با معیارهای ریسک تعیین شده از سوی سازمان مقایسه شوند. معیارهای ریسک ممکن است هزینه ها و منافع مرتبط، الزامات قانونی، عوامل اجتماعی، اقتصادی و زیست محیطی، نگرانی های ذی نفعان و موارد مشابه را در برگیرند. بنابراین، از ارزشیابی ریسک برای تصمیم گیری درباره میزان اهمیت ریسک ها برای سازمان و اینکه هر ریسک مشخص باید پذیرفته شود یا برای مواجهه با آن اقدام شود، استفاده می شود.

۶- گزارش دهی و ارتباطات ریسک

۶-۱- گزارش دهی داخلی

سطوح مختلف سازمان به اطلاعات متفاوتی از فرایند مدیریت ریسک نیاز دارند.

هیئت مدیره باید:

-از مهم ترین ریسک های پیش روی سازمان آگاه باشد؛

-آثار احتمالی انحراف از دامنه های مورد انتظار عملکرد بر ارزش سهام داران را بداند؛

-از وجود سطح مناسبی از آگاهی در سراسر سازمان اطمینان حاصل کند؛

-بداند سازمان چگونه بحران را مدیریت خواهد کرد؛

-از اهمیت اعتماد ذی نفعان به سازمان آگاه باشد؛

-در موارد مقتضی، نحوه مدیریت ارتباطات با جامعه سرمایه گذاران را بداند؛

-اطمینان یابد که فرایند مدیریت ریسک به طور اثربخش عمل می کند؛

-خط مشی روشنی درباره مدیریت ریسک منتشر کند که فلسفه و مسئولیت های مدیریت ریسک را در برگیرد.

واحدهای کسب و کار باید:

-از ریسک هایی که در حوزه مسئولیت آنها قرار می گیرند، آثار احتمالی این ریسک ها بر سایر حوزه ها و پیامدهایی که سایر حوزه ها ممکن است برای آنها ایجاد کنند، آگاه باشند؛

-شاخص های عملکردی در اختیار داشته باشند که امکان پایش فعالیت های اصلی کسب و کار و فعالیت های مالی، میزان پیشرفت در دستیابی به اهداف و شناسایی تحولاتی را فراهم کنند که به مداخله نیاز دارند؛ مانند پیش بینی ها و بودجه ها؛

-از سیستم هایی برخوردار باشند که انحراف از بودجه ها و پیش بینی ها را در فواصل زمانی مناسب گزارش کنند تا امکان انجام اقدامات لازم فراهم شود؛

-هر ریسک جدید یا ناکارآمدی مشاهده شده در کنترل های موجود را به صورت نظام مند و به موقع به مدیریت ارشد گزارش دهند.

افراد باید:

-پاسخ گویی خود را در قبال ریسک های مشخصی که بر عهده آنان قرار دارد، درک کنند؛

-بدانند چگونه می توانند به بهبود مستمر اقدامات سازمان در مواجهه با ریسک کمک کنند؛

-درک کنند که مدیریت ریسک و آگاهی از ریسک، بخش مهمی از فرهنگ سازمان است؛

-هر ریسک جدید یا ناکارآمدی مشاهده شده در کنترل های موجود را به صورت نظام مند و به موقع به مدیریت ارشد گزارش دهند.

۶-۲- گزارش دهی بیرونی

شرکت باید به طور منظم، خط مشی های مدیریت ریسک خود و میزان اثربخشی آنها در دستیابی به اهداف را به ذی نفعان گزارش کند.

ذی نفعان بیش از پیش از سازمان ها انتظار دارند شواهدی از مدیریت اثربخش عملکرد غیرمالی خود در حوزه هایی مانند امور اجتماعی، حقوق بشر، رویه های استخدامی، بهداشت و ایمنی و محیط زیست ارائه کنند.

حاکمیت شرکتی مطلوب ایجاب می کند که شرکت ها رویکردی نظام مند به مدیریت ریسک در پیش گیرند که:

-از منافع ذی نفعان آنها محافظت کند؛

-اطمینان دهد که هیئت مدیره وظایف خود را در زمینه هدایت راهبرد، ایجاد ارزش و نظارت بر عملکرد سازمان انجام می دهد؛

-اطمینان دهد که کنترل های مدیریتی برقرار هستند و به طور مناسب عمل می کنند.

ترتیبات گزارش دهی رسمی مدیریت ریسک باید به روشنی بیان و در دسترس ذی نفعان قرار داده شود.

گزارش دهی رسمی باید موضوعات زیر را در برگیرد:

-روش های کنترل، به ویژه مسئولیت های مدیریت در قبال مدیریت ریسک؛

-فرایندهای مورد استفاده برای شناسایی ریسک ها و نحوه رسیدگی سیستم های مدیریت ریسک به آنها؛

-سیستم های کنترلی اصلی موجود برای مدیریت ریسک های با اهمیت؛

-سیستم موجود برای پایش و بازنگری.

هرگونه نارسایی بااهمیتی که به وسیله سیستم یا در خود سیستم شناسایی شود، باید همراه با اقداماتی که برای رسیدگی به آن انجام شده است، گزارش شود.

۷- مواجهه با ریسک

مواجهه با ریسک، فرایند انتخاب و اجرای اقداماتی برای تعدیل ریسک است. کنترل یا کاهش ریسک، بخش اصلی مواجهه با ریسک را تشکیل می دهد؛ اما دامنه آن گسترده تر است و مواردی مانند اجتناب از ریسک، انتقال ریسک، تأمین مالی ریسک و سایر اقدامات را نیز در بر می گیرد.

یادداشت: در این استاندارد، تأمین مالی ریسک به سازوکارهایی مانند برنامه های بیمه ای اشاره دارد که برای تأمین منابع مالی لازم جهت جبران پیامدهای مالی ریسک به کار گرفته می شوند. تأمین مالی ریسک معمولاً به معنای تأمین منابع لازم برای پرداخت هزینه های اجرای اقدامات مواجهه با ریسک نیست.

هر نظام مواجهه با ریسک باید حداقل موارد زیر را فراهم کند:

-فعالیت اثربخش و کارآمد سازمان؛

-کنترل های داخلی اثربخش؛

-رعایت قوانین و مقررات.

فرایند تحلیل ریسک با شناسایی ریسک هایی که به توجه مدیریت نیاز دارند، به فعالیت اثربخش و کارآمد سازمان کمک می کند. مدیریت باید اقدامات کنترل ریسک را بر اساس ظرفیت آنها برای ایجاد منفعت برای سازمان اولویت بندی کند. اثربخشی کنترل داخلی به میزان حذف یا کاهش ریسک در نتیجه اجرای کنترل های پیشنهادی اشاره دارد.

مقرون به صرفه بودن کنترل داخلی از مقایسه هزینه اجرای کنترل با منافع مورد انتظار حاصل از کاهش ریسک مشخص می شود.

کنترل های پیشنهادی باید با مقایسه آثار اقتصادی احتمالی انجام ندادن اقدام با هزینه اقدامات پیشنهادی ارزیابی شوند. این ارزیابی همواره به اطلاعات و مفروضاتی دقیق تر از آنچه بلافاصله در دسترس است نیاز دارد.

ابتدا باید هزینه اجرا تعیین شود. این هزینه باید با دقت مناسبی محاسبه شود؛ زیرا به سرعت به خط مبنایی تبدیل می شود که مقرون به صرفه بودن اقدامات با آن سنجیده خواهد شد. زیان مورد انتظار در صورت انجام ندادن اقدام نیز باید برآورد شود. مدیریت با مقایسه نتایج می تواند درباره اجرا یا عدم اجرای اقدامات کنترل ریسک تصمیم بگیرد.

رعایت قوانین و مقررات اختیاری نیست. سازمان باید قوانین حاکم بر فعالیت خود را بشناسد و برای اطمینان از رعایت آنها، نظامی از کنترل ها را اجرا کند. فقط در مواردی خاص ممکن است اندکی انعطاف وجود داشته باشد؛ آن هم زمانی که هزینه کاهش یک ریسک با اندازه آن ریسک کاملاً نامتناسب باشد.

یکی از روش های تأمین حمایت مالی در برابر آثار ریسک ها، استفاده از تأمین مالی ریسک است که بیمه را نیز در بر می گیرد. با این حال، باید توجه داشت که برخی زیان ها یا اجزای یک زیان بیمه ناپذیرند. برای مثال، هزینه های بیمه نشده مرتبط با حوادث شغلی در حوزه های بهداشت، ایمنی یا محیط زیست ممکن است آسیب به روحیه کارکنان و شهرت سازمان را نیز شامل شوند.

۸- پایش و بازنگری فرایند مدیریت ریسک

مدیریت ریسک اثربخش به ساختاری برای گزارش دهی و بازنگری نیاز دارد تا اطمینان حاصل شود که ریسک ها به طور اثربخش شناسایی و ارزیابی شده اند و کنترل ها و اقدامات مناسب برای مواجهه با آنها برقرار هستند. میزان انطباق با خط مشی ها و استانداردها باید به طور منظم ممیزی و عملکرد در برابر استانداردها بازنگری شود تا فرصت های بهبود شناسایی شوند. باید به خاطر داشت که سازمان ها پویا هستند و در محیط هایی پویا فعالیت می کنند. تغییرات سازمان و محیط فعالیت آن باید شناسایی و اصلاحات متناسب در سیستم ها اعمال شوند.

فرایند پایش باید اطمینان دهد که کنترل های مناسبی برای فعالیت های سازمان برقرار هستند و رویه ها به درستی درک و اجرا می شوند. تغییرات سازمان و محیط فعالیت آن باید شناسایی و تغییرات متناسب در سیستم ها اعمال شوند.

هر فرایند پایش و بازنگری باید مشخص کند که آیا:

-اقدامات انجام شده به نتایج مورد نظر منجر شده اند؛

-رویه های انتخاب شده و اطلاعات گردآوری شده برای انجام ارزیابی مناسب بوده اند؛

-برخورداری از دانش بیشتر می توانست به اتخاذ تصمیمات بهتر کمک کند و چه درس هایی را می توان برای ارزیابی ها و مدیریت ریسک های آینده آموخت.

۹- ساختار و اداره مدیریت ریسک

۹-۱- خط مشی مدیریت ریسک

خط مشی مدیریت ریسک سازمان باید رویکرد آن به ریسک، اشتباهی ریسک و رویکرد آن به مدیریت ریسک را مشخص کند. این خط مشی همچنین باید مسئولیت های مدیریت ریسک را در سراسر سازمان تعیین کند.

افزون بر این، خط مشی باید به تمام الزامات قانونی مربوط به بیانیه های خط مشی، برای مثال در حوزه بهداشت و ایمنی، اشاره کند.

فرایند مدیریت ریسک با مجموعه ای یکپارچه از ابزارها و تکنیک ها همراه است که در مراحل مختلف فرایند کسب و کار به کار گرفته می شوند. اثربخشی فرایند مدیریت ریسک مستلزم موارد زیر است:

-تعهد مدیرعامل و مدیریت اجرایی سازمان؛

-تعیین مسئولیت ها در سازمان؛

-تخصیص منابع مناسب برای آموزش و افزایش آگاهی تمام ذی نفعان از ریسک.

۹-۲- نقش هیئت مدیره

هیئت مدیره مسئول تعیین جهت گیری راهبردی سازمان و ایجاد محیط و ساختارهایی است که امکان عملکرد اثربخش مدیریت ریسک را فراهم می کنند.

این مسئولیت ممکن است از طریق یک گروه اجرایی، کمیته غیرموظف، کمیته حسابرسی یا هر رکن دیگری انجام شود که با شیوه فعالیت سازمان تناسب داشته و بتواند نقش «حامی» مدیریت ریسک را ایفا کند.

هیئت مدیره باید هنگام ارزیابی سیستم کنترل داخلی، حداقل موارد زیر را در نظر بگیرد:

-ماهیت و میزان ریسک های دارای پیامد منفی که شرکت با توجه به نوع فعالیت خود پذیرش آنها را قابل قبول می داند؛

-احتمال تحقق این ریسک ها؛

-نحوه مدیریت ریسک های غیرقابل قبول؛

-توانایی شرکت برای به حداقل رساندن احتمال وقوع این ریسک ها و آثار آنها بر کسب و کار؛

-هزینه ها و منافع ریسک و فعالیت های کنترلی انجام شده؛

- اثربخشی فرایند مدیریت ریسک؛

- پیامدهای ریسکی تصمیمات هیئت مدیره.

۹-۳- نقش واحدهای کسب و کار

این نقش موارد زیر را در بر می گیرد:

- واحدهای کسب و کار مسئولیت اصلی مدیریت روزمره ریسک را برعهده دارند؛

- مدیریت واحدهای کسب و کار مسئول ترویج آگاهی از ریسک در فعالیتهای خود است و باید اهداف مدیریت ریسک را در کسب و کار خود وارد کند؛

- مدیریت ریسک باید یکی از موضوعات ثابت جلسات مدیریت باشد تا امکان بررسی میزان مواجهه با ریسک و اولویت بندی مجدد فعالیت ها بر پایه تحلیل اثربخش ریسک فراهم شود؛

- مدیریت واحدهای کسب و کار باید اطمینان حاصل کند که مدیریت ریسک از مرحله شکل گیری مفهوم اولیه پروژه در آن گنجانده شده و در سراسر اجرای پروژه نیز ادامه می یابد.

۹-۴- نقش واحد مدیریت ریسک

بسته به اندازه سازمان، واحد مدیریت ریسک ممکن است از یک نفر در نقش مروج مدیریت ریسک یا یک مدیر ریسک پاره وقت تا یک واحد کامل مدیریت ریسک متغیر باشد. نقش واحد مدیریت ریسک باید موارد زیر را در برگیرد:

- تدوین خط مشی و راهبرد مدیریت ریسک؛

- ایفای نقش مروج اصلی مدیریت ریسک در سطوح راهبردی و عملیاتی؛

- ایجاد فرهنگ آگاه از ریسک در سازمان، همراه با آموزش مناسب؛

- تدوین خط مشی داخلی ریسک و ایجاد ساختارهای لازم برای واحدهای کسب و کار؛

- طراحی و بازنگری فرایندهای مدیریت ریسک؛

- هماهنگ کردن فعالیتهای کارکردی مختلفی که درباره موضوعات مدیریت ریسک در سازمان مشاوره ارائه می کنند؛

- طراحی فرایندهای مواجهه با ریسک، از جمله برنامه های اقتضایی و تداوم کسب و کار؛

- تهیه گزارش های ریسک برای هیئت مدیره و ذی نفعان؛

۹-۵- نقش حسابرسی داخلی

نقش حسابرسی داخلی احتمالاً از سازمانی به سازمان دیگر متفاوت است. در عمل، نقش حسابرسی داخلی ممکن است برخی یا تمام موارد زیر را در برگیرد:

- تمرکز فعالیت های حسابرسی داخلی بر ریسک های بااهمیتی که مدیریت شناسایی کرده است و حسابرسی فرایندهای مدیریت ریسک در سراسر سازمان؛

- ارائه اطمینان بخشی درباره مدیریت ریسک؛

- حمایت فعال از فرایند مدیریت ریسک و مشارکت در آن؛

- تسهیل شناسایی و ارزیابی ریسک و آموزش کارکنان صف در زمینه مدیریت ریسک و کنترل داخلی؛

- هماهنگ کردن گزارش دهی ریسک به هیئت مدیره، کمیته حسابرسی و سایر ارکان مربوط.

حسابرسی داخلی هنگام تعیین مناسب ترین نقش برای یک سازمان مشخص باید اطمینان حاصل کند که الزامات حرفه ای مربوط به استقلال و بی طرفی نقض نمی شوند.

۹-۶- منابع و اجرا

منابع مورد نیاز برای اجرای خط مشی مدیریت ریسک سازمان باید در هر سطح مدیریت و در هر واحد کسب و کار به روشنی تعیین شوند.

افرادی که در مدیریت ریسک مشارکت دارند، علاوه بر سایر وظایف عملیاتی احتمالی خود، باید نقش مشخصی در هماهنگ کردن خط مشی و راهبرد مدیریت ریسک داشته باشند. نقش افرادی که در حسابرسی و بازنگری کنترل های داخلی یا تسهیل فرایند مدیریت ریسک مشارکت دارند نیز باید به همین اندازه روشن تعریف شود.

مدیریت ریسک باید از طریق فرایندهای راهبرد و بودجه در سازمان نهادینه شود. همچنین، باید در آموزش های بدو ورود و تمام برنامه های آموزشی و توسعه ای دیگر و نیز در فرایندهای عملیاتی، مانند پروژه های توسعه محصول یا خدمت، مورد تأکید قرار گیرد.

۱۰- پیوست

نمونه هایی از تکنیک های شناسایی ریسک

- طوفان فکری؛

- پرسشنامه ها؛

- بررسی های کسب و کار که هر یک از فرایندهای کسب و کار را مطالعه و فرایندهای درونی و عوامل بیرونی مؤثر بر آنها را

توصیف می کنند؛

- الگوبرداری از صنعت؛

- تحلیل سناریو؛

- کارگاه های ارزیابی ریسک؛

- بررسی رویدادها؛

- حسابرسی و بازرسی؛

- مطالعه مخاطره و قابلیت بهره برداری.

نمونه هایی از روش ها و تکنیک های تحلیل ریسک

ریسک های دارای جنبه مثبت

- پیمایش بازار

- فرصت یابی

- بازاریابی آزمایشی؛

- تحقیق و توسعه؛

تحلیل اثر کسب و کار

ریسک های دارای هر دو جنبه مثبت و منفی

-مدل سازی وابستگی ها؛

-تحلیل نقاط قوت، نقاط ضعف، فرصت ها و تهدیدها؛

-تحلیل درخت رویداد؛

-برنامه ریزی تداوم کسب و کار؛

-تحلیل عوامل کسب و کار، سیاسی، اقتصادی، اجتماعی و فناوری؛

-مدل سازی اختیار واقعی؛

-تصمیم گیری در شرایط ریسک و عدم قطعیت؛

-استنباط آماری؛

-شاخص های گرایش مرکزی و پراکندگی؛

-تحلیل عوامل سیاسی، اقتصادی، اجتماعی، فنی، قانونی و زیست محیطی.

ریسک های دارای جنبه منفی

-تحلیل تهدید؛

-تحلیل درخت خطا؛

-تحلیل حالات خرابی و آثار آن.

۱۱- ارزیابی تحلیلی استاندارد مدیریت ریسک ۲۰۰۲

«استاندارد مدیریت ریسک» در سال ۲۰۰۲، در مقطعی منتشر شد که مدیریت ریسک در حال گذار از فعالیت هایی تخصصی و نسبتاً پراکنده به رویکردی سازمانی و مرتبط با مدیریت راهبردی بود. در آن دوره، مدیریت ریسک در بسیاری از سازمان ها عمدتاً با بیمه، ایمنی، کنترل زیان، تداوم کسب و کار یا مدیریت ریسک های مالی شناخته می شد و هنوز زبان مشترک و معماری نسبتاً تثبیت شده امروزی برای مدیریت ریسک سازمانی شکل نگرفته بود. اهمیت تاریخی این سند را باید در همین بستر ارزیابی کرد.

سند حاضر کوشید اصطلاحات، فرایند، ساختار سازمانی و هدف مدیریت ریسک را در قالب راهنمایی کوتاه و قابل فهم برای مدیران بیان کند. نویسندگان نیز از ابتدا تصریح کردند که هدف آنان تدوین استاندارد تجویزی، ایجاد رویکردی مبتنی بر رعایت صوری الزامات یا طراحی فرایندی قابل صدور گواهی نبوده است. از این رو، این سند بیش از آنکه یک نظام جامع برای استقرار مدیریت ریسک باشد، راهنمایی عمومی برای آشنایی با منطق، مراحل و مسئولیت های اساسی مدیریت ریسک است.

پس از گذشت بیش از دودهه، سند را نمی توان بدون توجه به تحولات بعدی مدیریت ریسک ارزیابی کرد. انتشار چارچوب مدیریت ریسک سازمانی کوزو و بازنگری آن در سال ۲۰۱۷، انتشار ایزو ۳۱۰۰۰ و ویرایش سال ۲۰۱۸ آن، توسعه ادبیات حاکمیت ریسک، مدل سه خطی مؤسسه حسابرسان داخلی و افزایش توجه به فرهنگ ریسک، اشتباهات ریسک، تاب آوری و تصمیم گیری در شرایط عدم قطعیت، معیارهای ارزیابی یک نظام مدیریت ریسک را تغییر داده اند. بنابراین، پرسش اصلی این نیست که آیا سند سال ۲۰۰۲ تمام انتظارات امروز را برآورده می کند؛ بلکه باید دید این سند چه نقشی در تحول مدیریت ریسک داشته، کدام آموزه های آن همچنان معتبرند و برای استفاده امروزی در چه زمینه هایی باید تکمیل یا بازتفسیر شود.

۱۱-۱- جایگاه تاریخی سند

یکی از مهم ترین ویژگی های سند آن است که مدیریت ریسک را بخشی محوری از مدیریت راهبردی سازمان معرفی می کند. این برداشت در زمانی بیان شد که مدیریت ریسک هنوز در بسیاری از سازمان ها فعالیتی تخصصی و عمدتاً معطوف به جلوگیری از زیان تلقی می شد. سند، مدیریت ریسک را به تحقق اهداف، فعالیت های جاری و آتی سازمان، تخصیص سرمایه و منابع، تصمیم گیری، برنامه ریزی و اولویت بندی پیوند می دهد. از این نظر، می توان آن را یکی از اسناد حرفه ای مؤثر در گذار از مدیریت ریسک های منفرد به مدیریت ریسک سازمانی دانست.

توجه هم زمان به جنبه های مثبت و منفی ریسک نیز از ویژگی های مهم سند است. در این متن، ریسک فقط احتمال زیان یا شکست نیست، بلکه می تواند در بردارنده فرصت هایی برای کسب منفعت باشد. چنین برداشتی در زمان انتشار سند، گامی برای فاصله

گرفتن از نگاه صرفاً حفاظتی به مدیریت ریسک بود. این رویکرد بعدها در استانداردها و چارچوب های مدیریت ریسک توسعه یافت و با مفاهیمی مانند خلق و حفظ ارزش، بهره گیری از فرصت ها و بهبود تصمیم گیری پیوند خورد.

سند همچنین بر فراگیری مسئولیت مدیریت ریسک در سراسر سازمان تأکید می کند. بر اساس آن، مدیریت ریسک وظیفه انحصاری واحد مدیریت ریسک نیست و هر مدیر و کارمند باید مسئولیت مرتبط با ریسک را در شرح وظایف خود بپذیرد. این دیدگاه با یکی از مبانی اصلی مدیریت ریسک سازمانی سازگار است: ریسک در همان جایی باید مدیریت شود که فعالیت، تصمیم یا فرایند ایجاد کننده آن قرار دارد. واحد مدیریت ریسک می تواند سیاست گذاری، هماهنگی، تسهیل گری و گزارش دهی را بر عهده گیرد، اما مالکیت ریسک اصولاً در واحدهای کسب و کار باقی می ماند.

در عین حال، نباید جایگاه تاریخی سند را با جامعیت آن اشتباه گرفت. اثر گذاری آن بیشتر ناشی از ارائه تصویری روشن فشرده و مدیریتی از مدیریت ریسک است، نه برخورداری از معماری مفهومی و اجرایی کامل بخشی از آنچه امروزه بدیهی به نظر می رسد، در زمان انتشار این سند هنوز در ادبیات حرفه ای تثبیت نشده بود. در نتیجه، ارزش سند بیش از هر چیز در نقش انتقالی آن میان رویکردهای سنتی و نگاه یکپارچه به مدیریت ریسک قرار دارد.

۱۱-۲- نقاط قوت ماندگار سند

۱۱-۲-۱- پیوند مدیریت ریسک با اهداف و راهبرد

سند، مدیریت ریسک را فعالیتی جدا از مدیریت سازمان نمی داند. در آن تأکید شده است که فرایند مدیریت ریسک باید در سراسر راهبرد سازمان و اجرای آن جریان داشته باشد و اهداف راهبردی را به اهداف تاکتیکی و عملیاتی پیوند دهد. این برداشت همچنان معتبر است. مدیریت ریسک زمانی ارزش ایجاد می کند که به انتخاب اهداف، تخصیص منابع، ارزیابی گزینه ها و تصمیم گیری کمک کند؛ نه آنکه صرفاً به تهیه و به روزرسانی فهرستی از ریسک ها محدود شود.

با این حال، نحوه بیان این ارتباط در سند عمدتاً یک سویه است: ابتدا اهداف راهبردی تعیین می شوند و سپس ریسک های مرتبط با آنها ارزیابی می شوند. در ادبیات جدیدتر، رابطه راهبرد و ریسک دو طرفه است. ملاحظات ریسک نه تنها پس از انتخاب راهبرد، بلکه هنگام تعیین اهداف، مقایسه گزینه های راهبردی و تصمیم گیری درباره میزان ریسکی که سازمان حاضر است بپذیرد، باید وارد فرایند شوند. بنابراین، سند پیوند ریسک و راهبرد را به درستی تشخیص داده است، اما این پیوند را تا سطح اثرگذاری ریسک بر شکل گیری راهبرد توسعه نمی دهد.

۱۱-۲-۲- شناسایی دو سوی ریسک

تفکیک میان فرصت های منفعت آفرین و تهدیدهای متوجه موفقیت، از نقاط قوت روشن سند است. این تفکیک نشان می دهد که مدیریت ریسک فقط برای کاهش زیان نیست و می تواند در بهره برداری سنجیده از فرصت ها نیز نقش داشته باشد. چنین برداشتی با منطق مدیریت ریسک سازمانی سازگار است؛ زیرا سازمان بدون پذیرش ریسک نمی تواند به اهداف خود دست یابد یا ارزش ایجاد کند.

با این حال، کاربرد این برداشت در بخش های بعدی سند کاملاً متوازن نیست. هرچند در سطح تعریف و طبقه بندی به فرصت ها توجه شده، بخش عمده ابزارهای ارزیابی، کنترل و تأمین مالی ریسک همچنان متأثر از منطق مدیریت تهدید و کاهش زیان است. به بیان دیگر، سند از نظر مفهومی ریسک مطلوب را می پذیرد، اما برای سنجش، انتخاب و بهره برداری از آن ابزارهای چندان توسعه یافته ای ارائه نمی کند.

۱۱-۲-۳- سادگی و قابلیت فهم برای مدیران

سند کوتاه، مستقیم و از پیچیدگی غیرضروری دور است. فرایند مدیریت ریسک را به مجموعه ای قابل فهم از مراحل شامل شناسایی، توصیف، برآورد، ارزیابی، گزارش دهی، تصمیم گیری، مواجهه و پایش تقسیم می کند. الگوی توصیف ریسک، تفکیک نیازهای اطلاعاتی سطوح مختلف سازمان و تعیین اجمالی نقش هیئت مدیره، واحدهای کسب و کار، واحد مدیریت ریسک و حسابرسی داخلی، کاربرد آموزشی آن را افزایش داده اند.

این سادگی یکی از دلایل ماندگاری سند است، اما ممکن است به برداشت تقلیل گرایانه نیز بینجامد. سازمانی که مدیریت ریسک را صرفاً به اجرای متوالی مراحل نمودار سند محدود کند، احتمالاً به فرایندی اداری و گزارش محور خواهد رسید. سادگی هنگامی مزیت است که به فهم بهتر منطق مدیریت ریسک کمک کند؛ نه هنگامی که پیچیدگی واقعی تصمیم ها، وابستگی میان ریسک ها و پویایی محیط را پنهان سازد.

۱۱-۲-۴- تأکید بر مسئولیت سازمانی

سند به درستی میان نقش های مختلف سازمان تمایز قائل می شود. هیئت مدیره مسئول تعیین جهت گیری راهبردی و ایجاد محیط و ساختار مناسب معرفی شده است؛ واحدهای کسب و کار مسئولیت اصلی مدیریت روزمره ریسک را بر عهده دارند؛ واحد مدیریت ریسک سیاست گذاری، هماهنگی، آموزش، تسهیل ارزیابی و گزارش دهی را پشتیبانی می کند؛ و حسابرسی داخلی می تواند در ارائه اطمینان و ارزیابی فرایند نقش داشته باشد.

این تقسیم کلی همچنان قابل دفاع است. به ویژه، تأکید سند بر مسئولیت واحدهای کسب و کار مانع از آن می شود که مدیریت ریسک به واحدهای ستادی واگذار و از تصمیم های واقعی سازمان جدا شود. همچنین، قرار گرفتن موضوع مدیریت ریسک در سطح هیئت مدیره نشان می دهد که نویسندگان آن را موضوعی صرفاً عملیاتی یا فنی تلقی نکرده اند.

۱۱-۲-۵- پرهیز از تجویزگرایی و صدور گواهی

نویسندگان تصریح کرده اند که سند برای ایجاد فرایندی قابل صدور گواهی تدوین نشده است. این موضوع از نظر حرفه ای همچنان اهمیت دارد. اثربخشی مدیریت ریسک را نمی توان صرفاً بر پایه وجود اسناد، فرم ها، کمیته ها یا رعایت مجموعه ای از الزامات ظاهری سنجید. سازمان ممکن است همه اجزای رسمی یک نظام مدیریت ریسک را ایجاد کند، اما مدیریت ریسک در تصمیم گیری، تخصیص منابع و رفتار مدیران آن نقشی نداشته باشد.

با این حال، خود سند در بخشی از مقدمه از امکان اعلام انطباق سازمان با اجزای استاندارد سخن می گوید. این بیان با تأکید آن بر غیرتجویزی بودن تا اندازه ای تنش دارد. اگر معیارهای روشن بلوغ و اثربخشی تعریف نشوند، انطباق ممکن است به همان رویکرد صوری بینجامد که سند قصد پرهیز از آن را دارد. این ابهام در بسیاری از استانداردهای اصول محور نیز دیده می شود؛ انعطاف پذیری مزیت آنهاست، اما همین انعطاف پذیری می تواند ارزیابی کیفیت اجرا را دشوار کند.

۱۱-۳- محدودیت های مفهومی و روش شناختی

۱۱-۳-۱- تعریف ریسک

سند، مطابق راهنمای ۷۳ ایزو و آی ای سی در آن دوره، ریسک را ترکیب احتمال وقوع یک رویداد و پیامدهای آن تعریف می کند. این تعریف برای بسیاری از کاربردهای عملی، به ویژه در ایمنی، بیمه و تحلیل رویدادهای زیان بار، روشن و قابل استفاده است. با این حال، ریسک را عمدتاً به رویداد، احتمال و پیامد وابسته می کند و رابطه آن با اهداف را مستقیماً در متن تعریف وارد نمی سازد. در ایزو ۳۱۰۰۰:۲۰۱۸، ریسک «اثر عدم قطعیت بر اهداف» تعریف شده است. این تغییر صرفاً تفاوتی واژگانی نیست. تعریف جدیدتر توجه را از خود رویداد به اثر عدم قطعیت بر آنچه سازمان در پی دستیابی به آن است منتقل می کند. در این برداشت، بدون شناخت هدف نمی توان ریسک را به درستی تعریف یا ارزیابی کرد. همچنین، منشأ ریسک ممکن است فقط یک رویداد مشخص نباشد؛ تغییر تدریجی شرایط، فرض نادرست، پیچیدگی روابط، فقدان اطلاعات یا نوسان متغیرهای محیطی نیز می توانند دستیابی به اهداف را تحت تأثیر قرار دهند.

تعریف سال ۲۰۰۲ نادرست نیست، اما دامنه ای محدودتر دارد. برای استفاده امروزی، بهتر است رویداد، علت، پیامد و احتمال در چارچوب اثر عدم قطعیت بر اهداف تحلیل شوند، نه آنکه خود این عناصر جایگزین مفهوم ریسک شوند.

۱۱-۳-۲- فقدان تفکیک روشن میان اصول، چارچوب و فرایند

یکی از تفاوت های اساسی سند با ایزو ۳۱۰۰۰:۲۰۱۸ آن است که معماری سه لایه اصول، چارچوب و فرایند در آن وجود ندارد. سند سال ۲۰۰۲ مستقیماً وارد تعریف، فرایند، گزارش دهی، مواجهه و نقش های سازمانی می شود. در نتیجه، مشخص نمی کند که

یک نظام اثربخش مدیریت ریسک باید بر چه اصولی استوار باشد، چگونه در حاکمیت و مدیریت سازمان ادغام شود و از چه ساز و کاری برای طراحی، اجرا، ارزیابی و بهبود برخوردار باشد.

این کاستی می تواند به استقرار فرایند بدون ایجاد زیرساخت سازمانی لازم منجر شود. شناسایی و ارزیابی ریسک، بدون حمایت هیئت مدیره، تخصیص منابع، تعیین مسئولیت ها، دسترسی به اطلاعات، توسعه شایستگی ها و سازوکار بهبود، به فعالیتی مقطعی تبدیل می شود سند به برخی از این عناصر اشاره می کند، اما آنها را در قالب چارچوبی منسجم و به هم پیوسته سامان نمی دهد.

۱۱-۳-۳- غلبه نگاه فرایندی و نسبتاً خطی

نمودار مدیریت ریسک در سند، توالی روشنی از اهداف راهبردی تا ارزیابی، گزارش دهی، تصمیم گیری، مواجهه و پایش ارائه می کند. این نمودار برای آموزش اولیه مفید است، اما ممکن است این تصور را ایجاد کند که مدیریت ریسک فرایندی خطی و دارای نقطه آغاز و پایان مشخص است.

در عمل، مدیریت ریسک ماهیتی تکرار شونده و تعاملی دارد. شناسایی ریسک می تواند موجب بازنگری در اهداف شود؛ تحلیل ریسک ممکن است نیازمند جمع آوری اطلاعات جدید باشد؛ ارزیابی گزینه های مواجهه می تواند معیارهای ریسک را تغییر دهد؛ و پایش محیط ممکن است تعریف مسئله را به طور اساسی دگرگون کند. از این رو، مراحل مدیریت ریسک باید حلقه های بازخورد و امکان بازگشت به مراحل پیشین داشته باشند.

سند از استمرار و توسعه فرایند سخن می گوید و «اصلاح» را در نمودار خود منظور می کند، اما پویایی واقعی مدیریت ریسک و رابطه رفت و برگشتی آن با تصمیم گیری را به طور کامل نشان نمی دهد.

۱۱-۳-۴- ابهام میان معیار ریسک، تحمل ریسک و اشتباهی ریسک

در الگوی توصیف ریسک، «تحمل یا اشتباهی ریسک» در کنار ظرفیت زیان، ارزش در معرض ریسک، احتمال و اندازه زیان یا منفعت و اهداف کنترل قرار گرفته است. این مجموعه برای توصیف عملی ریسک مفید است، اما چند مفهوم متمایز را در یک ردیف گرد می آورد.

اشتهای ریسک بیانگر نوع و میزان ریسکی است که سازمان در مسیر دستیابی به اهداف و ایجاد ارزش، حاضر به پذیرش آن است. تحمل ریسک نیز معمولاً حدود قابل قبول انحراف از اهداف یا معیارهای عملکرد را مشخص می کند. معیارهای ریسک نیز مبنای مقایسه نتایج تحلیل ریسک و تصمیم گیری درباره اهمیت آن هستند. ظرفیت ریسک به حداکثر میزانی مربوط است که سازمان از نظر مالی، عملیاتی یا قانونی قادر به تحمل آن است. یکسان گرفتن یا مبهم گذاشتن این مفاهیم می تواند موجب شود تصمیم های پذیرش ریسک فاقد مبنای روشن باشند.

سند، اهمیت این موضوع را زودتر از بسیاری از متون مدیریتی تشخیص داده است؛ اما برای تبدیل اشتباهای ریسک به حدود، شاخص ها، اختیارهای تصمیم گیری و سازوکارهای ارجاع، راهنمای کافی ارائه نمی کند.

۱۱-۳-۵- محدودیت مقیاس های ارزیابی

سند استفاده از مقیاس های سه درجه ای و ماتریس های سه در سه یا پنج در پنج را مطرح می کند و نمونه هایی برای ارزیابی احتمال و پیامد تهدیدها و فرصت ها ارائه می دهد. این ابزارها برای غربالگری اولیه، ایجاد زبان مشترک و اولویت بندی مقدماتی مفیدند، اما نباید با اندازه گیری دقیق ریسک اشتباه گرفته شوند.

مقیاس های ترتیبی «زیاد، متوسط و کم» فاصله های کمی مشخصی ندارند و ترکیب آنها ممکن است تصویری دقیق تر از واقعیت القا کند. تعریف احتمال نیز در نمونه های سند کاملاً همگن نیست؛ برای مثال، افق زمانی، درصد احتمال و تکرار وقوع هم زمان به کار رفته اند افزون بر این، ارزیابی جداگانه ریسک ها می تواند وابستگی، هم بستگی، تمرکز و آثار زنجیره ای آنها را پنهان کند.

ماتریس ریسک همچنان می تواند ابزاری ارتباطی باشد، اما برای ریسک های مهم باید با تحلیل سناریو، آزمون تنش، تحلیل حساسیت، داده های رویداد، نظر خبرگان و سایر روش های متناسب تکمیل شود. انتخاب روش نیز باید به ماهیت تصمیم، کیفیت داده ها، افق زمانی و هزینه خطا وابسته باشد.

۱۱-۳-۶- توجه محدود به عوامل انسانی و فرهنگی

سند به ادغام مدیریت ریسک در فرهنگ سازمان و ضرورت آموزش و افزایش آگاهی اشاره می کند، اما فرهنگ را عمدتاً به عنوان بستری برای اجرای فرایند در نظر می گیرد. در ادبیات جدیدتر، فرهنگ ریسک صرفاً آگاهی کارکنان یا برگزاری دوره های آموزشی نیست؛ الگوهای واقعی تصمیم گیری، نحوه واکنش مدیران به خبرهای نامطلوب، نظام پاداش، امنیت روانی، تمایل به طرح مخالفت و سازگاری رفتار رهبران با ارزش های اعلام شده را نیز در بر می گیرد.

همچنین، سند نقش سوگیری های شناختی، قضاوت گروهی، اعتماد بیش از حد، فشارهای سازمانی و منافع متعارض را در شناسایی و ارزیابی ریسک بررسی نمی کند. در حالی که بسیاری از شکست های مدیریت ریسک نه از فقدان فرم یا مدل، بلکه از نادیده گرفتن اطلاعات نامطلوب، سکوت سازمانی، خوش بینی افراطی یا غلبه اهداف کوتاه مدت ناشی می شوند.

۱۱-۳-۷- نگاه محدود به وابستگی و پویایی ریسک ها

طبقه بندی ریسک ها به راهبردی، مالی، عملیاتی، مخاطره ای، دانشی و انطباقی برای ایجاد نظم اولیه سودمند است، اما ممکن است به شکل گیری سیلوهای جدید بینجامد. ریسک های مهم معمولاً در یک طبقه باقی نمی مانند. یک اختلال سایبری می تواند هم زمان پیامدهای عملیاتی، مالی، حقوقی، اعتباری و راهبردی ایجاد کند. به همین ترتیب، تغییر مقررات، بحران زنجیره تأمین یا تحول فناوری ممکن است مجموعه ای از ریسک های وابسته و تقویت کننده یکدیگر را فعال سازد.

سند به هم پوشانی عوامل داخلی و خارجی اشاره می کند، اما برای تحلیل وابستگی ها، سرعت گسترش اثر، نقاط تمرکز، آثار آبخاری و ریسک های نوظهور ابزار مشخصی ارائه نمی دهد. برای محیط امروز، ثبت و رتبه بندی جداگانه ریسک ها کافی نیست و سازمان باید چگونگی تعامل ریسک ها و اثر تجمعی آنها بر اهداف را نیز تحلیل کند.

۱۱-۴- مقایسه با ایزو ۳۱۰۰۰:۲۰۱۸

برای روشن شدن جایگاه استاندارد مدیریت ریسک ۲۰۰۲ در ادبیات امروز، جدول (۵) آن را در محورهای منتخب با ایزو ۳۱۰۰۰:۲۰۱۸ مقایسه می کند. مقایسه بر تعریف ریسک، هدف و ساختار مدیریت ریسک، پیوند با راهبرد، مسئولیت های مدیریتی و سازوکارهای اجرا و بازنگری متمرکز است. در تفسیر تفاوت ها باید زمان انتشار، هدف و دامنه هر سند را در نظر گرفت؛ اشاره نشدن یا پرداخت مختصر به یک موضوع، لزوماً به معنای رد یا نادیده گرفتن آن نیست. ستون «نتیجه تحلیلی» نیز برداشت نویسنده این بخش از مقایسه دو سند است و باید از مفاد خود اسناد متمایز دانسته شود.

جدول (۵): مقایسه استاندارد مدیریت ریسک با ایزو ۳۱۰۰۰:۲۰۱۸

محور مقایسه	استاندارد مدیریت ریسک ۲۰۰۲	ایزو ۳۱۰۰۰:۲۰۱۸	نتیجه تحلیلی
تعریف ریسک	ترکیب احتمال وقوع رویداد و پیامدهای آن	اثر عدم قطعیت بر اهداف	تعریف سال ۲۰۰۲ رویداد محورتر و تعریف ایزو هدف محورتر است
غایت مدیریت ریسک	دستیابی به منفعت پایدار، افزایش احتمال موفقیت و کاهش احتمال شکست	خلق و حفظ ارزش	هر دو بر ارزش تأکید دارند، اما ایزو آن را به صورت اصل محوری بیان می کند.
ساختار کلی	مجموعه ای از مراحل فرایندی و مسئولیت های سازمانی	اصول، چارچوب و فرایند	ایزو معماری منسجم تری برای طراحی و استقرار نظام مدیریت ریسک ارائه می کند.
ارتباط با راهبرد	مدیریت ریسک باید در راهبرد و اجرای آن جریان داشته باشد	مدیریت ریسک باید با همه فعالیت ها و تصمیم های سازمان یکپارچه شود	سند ۲۰۰۲ جهت گیری درستی دارد، اما ایزو دامنه و سازوکار یکپارچگی را روشن تر می کند
رهبری و تعهد	بر نقش مدیریت ارشد و هیئت مدیره تأکید دارد	رهبری و تعهد جزء مرکزی چارچوب است	در ایزو، مسئولیت رهبری با طراحی، منابع، پاسخ گویی و بهبود چارچوب پیوند نظام مندتری دارد

عوامل انسانی و فرهنگی	فرهنگ، آموزش و آگاهی را مطرح می کند	عوامل انسانی و فرهنگی یکی از اصول مدیریت ریسک است	سند ۲۰۰۲ اهمیت فرهنگ را تشخیص می دهد، اما آن را به صورت عمیق تحلیل نمی کند
پویایی ریسک	بر استمرار و توسعه فرایند تأکید دارد	مدیریت ریسک باید پویا و پاسخ گوی تغییر باشد	ایزو توجه صریح تری به تغییرات محیطی و ریسک های نوظهور دارد
اشتهای ریسک	در جدول توصیف ریسک مطرح شده است	اصطلاح محوری متن استاندارد نیست و در قالب معیارهای ریسک و تصمیم گیری بازتاب می یابد	سند ۲۰۰۲ مفهوم را مطرح می کند، اما روابط آن با ظرفیت، تحمل و معیارهای ریسک را تفکیک نمی کند.
ارتباطات و مشورت	بیشتر بر گزارش دهی داخلی و خارجی متمرکز است	ارتباطات و مشورت جزء مستمر فرایند است	در ایزو، ارتباطات دوسویه و مشارکت ذی نفعان گسترده تر از انتقال گزارش است
پایش و بهبود	پایش و بازنگری را از اجزای فرایند می داند	پایش، بازنگری، انطباق و بهبود مستمر در چارچوب و فرایند حضور دارند	ایزو بهبود نظام مدیریت ریسک را منسجم تر و در سطح چارچوب دنبال می کند.
تجویز و گواهی	غیرتجویزی و غیرقابل صدور گواهی	راهنمای اصول محور و غیرقابل صدور گواهی	در این زمینه، جهت گیری دو سند تا حد زیادی همسو است

این مقایسه نشان می دهد که دو سند در بسیاری از جهت گیری های اصلی اشتراک دارند، اما ایزو ۳۱۰۰۰:۲۰۱۸ این موضوعات را در ساختاری متشکل از اصول، چارچوب و فرایند سامان می دهد. پیوند با اهداف، ادغام در سازمان، مسئولیت مدیریت ارشد، توجه به عوامل انسانی و ضرورت بهبود مستمر در هر دو سند وجود دارد. تفاوت اصلی در میزان انسجام مفهومی و بلوغ ساختاری آنهاست.

از این رو، نباید رابطه این دو سند را به صورت تقابل میان متنی منسوخ و متنی جدید تصویر کرد. سند ۲۰۰۲ بخشی از مسیر تحول اندیشه ای است که بعداً در ایزو ۳۱۰۰۰ صورت بندی منظم تری یافت. با این حال، برای طراحی و ارزیابی نظام مدیریت ریسک امروزی، اتکا به سند ۲۰۰۲ به تنهایی قابل دفاع نیست.

۱۱-۵- ارزیابی حاکمیت و مسئولیت های سازمانی

۱۱-۵-۱- نقش هیئت مدیره

سند، هیئت مدیره را مسئول تعیین جهت گیری راهبردی و ایجاد محیط و ساختار لازم برای مدیریت ریسک می داند. همچنین، انتظار دارد هیئت مدیره از مهم ترین ریسک ها، آثار احتمالی انحراف از عملکرد مورد انتظار، نحوه مدیریت بحران و اثربخشی فرایند مدیریت ریسک آگاه باشد. این انتظارات همچنان معتبرند و نشان می دهند که نظارت بر ریسک از همان زمان به عنوان بخشی از وظایف حاکمیتی هیئت مدیره شناخته شده بود.

با این حال، متن میان مسئولیت هیئت مدیره در نظارت بر ریسک و مسئولیت مدیریت اجرایی در مدیریت ریسک مرز کاملاً روشنی ترسیم نمی کند. همچنین، درباره نقش کمیته ریسک، رابطه آن با کمیته حسابرسی، تصویب و پایش اشتهای ریسک، کیفیت اطلاعات ریسک و ارزیابی فرهنگ ریسک توضیح کافی نمی دهد. در الگوهای جدیدتر، هیئت مدیره نباید مستقیماً مالک یا مدیر ریسک های اجرایی باشد، بلکه باید جهت گیری، حدود پذیرش ریسک، پاسخ گویی مدیریت و اثربخشی نظام نظارت را تعیین و ارزیابی کند.

۱۱-۵-۲- نقش واحدهای کسب و کار

قرار دادن مسئولیت اصلی مدیریت روزمره ریسک بر عهده واحدهای کسب و کار از نقاط قوت مهم سند است. ریسک در جریان تصمیم ها و فعالیت های این واحدها ایجاد یا پذیرفته می شود و مدیران آنها باید پیامدهای تصمیم های خود را بشناسند و در برابر آن پاسخ گو باشند.

با این حال، مسئولیت واحد کسب و کار نباید به تکمیل ارزیابی های دوره ای یا ارائه اطلاعات به واحد مدیریت ریسک محدود شود. مالک ریسک باید اختیار، منابع و مسئولیت لازم برای انتخاب و اجرای پاسخ مناسب را داشته باشد و عملکرد او نیز بر مبنای رعایت حدود مصوب و کیفیت تصمیم ها ارزیابی شود. این پیوند میان مالکیت ریسک، اختیار تصمیم گیری و پاسخ گویی در سند به طور کامل توسعه نیافته است.

۱۱-۵-۳- نقش واحد مدیریت ریسک

سند طیف نسبتاً گسترده ای از وظایف را برای واحد مدیریت ریسک برمی شمارد: تدوین سیاست و راهبرد، ترویج فرهنگ ریسک، طراحی و بازنگری فرایندها، هماهنگی فعالیت ها، توسعه پاسخ های ریسک و تهیه گزارش برای هیئت مدیره و ذی نفعان. این توصیف، واحد مدیریت ریسک را فراتر از یک واحد اندازه گیری یا گزارش دهی معرفی می کند.

با این حال، استقلال، جایگاه سازمانی، دسترسی مستقیم به هیئت مدیره، اختیار طرح موضوعات مهم و حفاظت از مسئول واحد مدیریت ریسک در برابر فشارهای اجرایی، در متن جایگاه روشنی ندارند. میان نقش تسهیل گری و نظارتی واحد مدیریت

ریسک و مسئولیت اجرایی واحدهای کسب و کار مرز دقیقی تعیین نشده است. اگر واحد مدیریت ریسک خود مسئول طراحی و اجرای پاسخ های ریسک شود، احتمال انتقال مالکیت ریسک از مدیریت اجرایی به واحد ستادی افزایش می یابد.

۱۱-۵-۴- نقش حسابرسی داخلی

سند برای حسابرسی داخلی نقش هایی مانند تمرکز بر ریسک های مهم، حسابرسی فرایندهای مدیریت ریسک، ارائه اطمینان، پشتیبانی از فرایند، تسهیل شناسایی و ارزیابی ریسک، آموزش کارکنان و هماهنگی گزارش دهی ریسک را مطرح می کند. در پایان نیز هشدار می دهد که استقلال و بی طرفی حرفه ای حسابرسی داخلی نباید نقض شود.

این هشدار درست است، اما فهرست نقش های پیشنهادی بسیار گسترده است. مشارکت فعال در فرایند، تسهیل ارزیابی و هماهنگی گزارش دهی، اگر با حفاظت های روشن همراه نباشد، ممکن است حسابرسی داخلی را در موقعیتی قرار دهد که بعداً ناچار شود فعالیت های طراحی شده یا اجرا شده خود را ارزیابی کند. بر اساس مدل سه خطی مؤسسه حسابرسان داخلی، حسابرسی داخلی باید اطمینان مستقل و عینی ارائه کند و نقش های مشورتی آن نباید به پذیرش مسئولیت های مدیریتی بینجامد.

بنابراین، بخش مربوط به حسابرسی داخلی نیازمند بازتفسیر جدی است. حسابرسی داخلی می تواند بلوغ و اثربخشی مدیریت ریسک را ارزیابی کند، اما تعیین اشتباهی ریسک، مالکیت ریسک، انتخاب پاسخ ها و مدیریت فرایند گزارش دهی اجرایی نباید به آن واگذار شود.

۱۱-۶- موضوعاتی که برای استفاده امروزی باید به سند افزوده شوند

۱۱-۶-۱- مدیریت ریسک به عنوان پشتیبان تصمیم گیری

سند از بهبود تصمیم گیری سخن می گوید، اما فرایند مدیریت ریسک را عمدتاً حول شناسایی و ارزیابی ریسک های موجود سازمان می چیند. در رویکردهای جدیدتر، نقطه آغاز می تواند خود تصمیم باشد؛ چه گزینه هایی پیش روی سازمان است، هر گزینه با چه عدم قطعیت ها و پیامدهایی همراه است، فرض های اساسی تصمیم کدام اند و چه اطلاعاتی می تواند انتخاب را تغییر دهد؟

این تغییر زاویه نگاه اهمیت زیادی دارد. اگر مدیریت ریسک پس از اتخاذ تصمیم وارد عمل شود، معمولاً به ثبت و کنترل ریسک های تصمیمی می پردازد که پیش تر گرفته شده است. مدیریت ریسک مؤثر باید پیش از تصویب راهبرد، سرمایه گذاری، محصول، قرارداد یا پروژه مهم، کیفیت تصمیم را بهبود دهد.

۱۱-۶-۲- فرهنگ و رفتار ریسک

برای تکمیل سند، فرهنگ ریسک باید از سطح آموزش و آگاهی فراتر رود و در رفتارهای قابل مشاهده تعریف شود. نحوه طرح خبرهای نامطلوب، تحمل دیدگاه مخالف، واکنش مدیران به عبور از حدود ریسک، ارتباط پاداش با ریسک پذیری، کیفیت گفت و گوی هیئت مدیره و مدیریت و امکان گزارش نگرانی ها، از اجزای واقعی فرهنگ ریسک اند.

بدون این عناصر، سیاست ها و فرایندهای رسمی ممکن است صرفاً نمایی از کنترل ایجاد کنند. وجود کمیته ریسک، سجل ریسک یا داشبورد به تنهایی نشان نمی دهد که سازمان در تصمیم های دشوار نیز حدود ریسک را رعایت می کند.

۱۱-۶-۳- تاب آوری سازمانی

سند عمدتاً بر شناسایی، ارزیابی و کنترل ریسک ها تمرکز دارد. تجربه سازمان ها نشان داده است که همه اختلال ها قابل پیش بینی یا پیشگیری نیستند. از این رو، مدیریت ریسک باید با تداوم کسب و کار، مدیریت بحران و تاب آوری سازمانی پیوند یابد.

تاب آوری صرفاً کاهش احتمال وقوع رویداد نیست؛ توان پیش بینی، جذب شوک، پاسخ، بازیابی و سازگار شدن با شرایط جدید را نیز در برمی گیرد. این موضوع به ویژه برای ریسک های پیچیده، بحران های فراگیر و رویدادهایی که منشأ و مسیر آنها از پیش مشخص نیست، اهمیت دارد.

۱۱-۶-۴- ریسک های نوظهور و به هم پیوسته

تحولات فناوری، امنیت سایبری، داده، هوش مصنوعی، تغییرات اقلیمی، تنش های ژئوپلیتیکی و وابستگی های زنجیره تأمین، محیط ریسک سازمان ها را پیچیده تر کرده اند. مسئله فقط افزوده شدن چند عنوان جدید به فهرست ریسک ها نیست؛ بلکه سرعت تغییر، وابستگی متقابل و امکان گسترش زنجیره ای پیامدها افزایش یافته است.

برای مواجهه با این وضعیت، سازمان به دیده بانی محیط، تحلیل سناریو، شناسایی علائم ضعیف، ارزیابی وابستگی ها و سازوکار ارجاع سریع ریسک های نوظهور نیاز دارد. طبقه بندی و امتیازدهی دوره ای ریسک ها، به تنهایی برای این منظور کافی نیست.

۱۱-۶-۵- سنجش اثربخشی مدیریت ریسک

سند توضیح می دهد که مدیریت ریسک باید پایش و بازنگری شود، اما معیارهای اثربخشی آن را به طور دقیق مشخص نمی کند. سنجش اثربخشی نباید فقط بر تعداد ریسک های شناسایی شده، جلسات برگزار شده یا گزارش های تهیه شده متکی باشد.

ارزیابی باید نشان دهد که مدیریت ریسک تا چه اندازه کیفیت تصمیم ها را بهبود داده، غافل گیری های مهم را کاهش داده، تخصیص منابع را هدفمندتر کرده، حدود پذیرش ریسک را در تصمیم ها وارد ساخته و توان سازمان برای دستیابی به اهداف و بازیابی پس

از اختلال را افزایش داده است. این آثار همیشه به صورت مستقیم و کوتاه مدت قابل اندازه گیری نیستند، اما بدون توجه به آنها، نظام مدیریت ریسک ممکن است به تولید مستندات و گزارش های فاقد اثر مدیریتی محدود شود.

۱۱-۷- حدود کاربرد سند در سازمان های امروزی

استاندارد مدیریت ریسک ۲۰۰۲ همچنان برای آموزش مقدماتی، ایجاد زبان مشترک و توضیح مراحل عمومی مدیریت ریسک مفید است. الگوی توصیف ریسک، تقسیم مسئولیت ها، تفکیک نیازهای اطلاعاتی سطوح سازمان و تأکید بر ارتباط مدیریت ریسک با اهداف می توانند در طراحی اولیه یا بازنگری فرایندها مورد استفاده قرار گیرند.

با این حال، استفاده از سند به عنوان مبنای یگانه طراحی یا ارزیابی نظام مدیریت ریسک سازمان امروزی توصیه نمی شود. این سند برای موضوعاتی مانند اصول مدیریت ریسک، طراحی چارچوب، اشتباهات ریسک، فرهنگ و رفتار، حاکمیت ریسک، استقلال واحد مدیریت ریسک، مدیریت ریسک راهبردی، تحلیل وابستگی ها، تاب آوری و ریسک های نوظهور راهنمای کافی ارائه نمی کند.

کاربرد درست آن، استفاده به عنوان یک متن پایه و تاریخی در کنار منابع جدیدتر است. برای طراحی نظام مدیریت ریسک، ایزو ۳۱۰۰۰:۲۰۱۸ می تواند مبنای اصول، چارچوب و فرایند قرار گیرد. برای پیوند ریسک با راهبرد و عملکرد می توان از چارچوب مدیریت ریسک سازمانی کوزو استفاده کرد. مدل سه خطی مؤسسه حسابرسان داخلی نیز برای تفکیک نقش های هیئت مدیره، مدیریت، واحدهای نظارتی و حسابرسی داخلی اهمیت دارد. افزون بر این، الزامات قانونی و استانداردهای تخصصی هر صنعت باید جداگانه در نظر گرفته شوند.

در سازمان های ایرانی، یک محدودیت دیگر نیز باید مورد توجه قرار گیرد. استقرار مدیریت ریسک در بسیاری از موارد تحت تأثیر الزامات مقرراتی آغاز می شود و در معرض تبدیل شدن به فرایندی صوری و مستند محور قرار دارد. سادگی سند ۲۰۰۲ می تواند برای آغاز کار مفید باشد، اما اگر بدون توجه به حاکمیت، اختیار، پاسخ گویی و تصمیم گیری به کار رود، همین سادگی ممکن است رویکرد صوری را تقویت کند. بنابراین، استفاده از سند باید با ارزیابی بلوغ سازمان، ویژگی های صنعت، ساختار مالکیت، الزامات نظارتی و ظرفیت های اطلاعاتی همراه باشد.

۱۱-۸- جمع بندی نهایی

استاندارد مدیریت ریسک ۲۰۰۲ را باید سندی مهم در مسیر تحول مدیریت ریسک دانست. این سند در زمانی که مدیریت ریسک هنوز در بسیاری از سازمان ها مجموعه ای از فعالیت های تخصصی و پراکنده بود، بر ارتباط آن با راهبرد، اهداف، تصمیم گیری، مسئولیت مدیران و خلق ارزش تأکید کرد. شناسایی دو سوی مثبت و منفی ریسک، پذیرش مسئولیت مدیریت ریسک در سراسر سازمان، توجه به نقش هیئت مدیره و پرهیز از رویکرد تجویزی و قابل صدور گواهی، از آموزه های ماندگار آن هستند.

در مقابل، تعریف رویداد محور ریسک، فقدان معماری روشن اصول، چارچوب و فرایند، غلبه نگاه نسبتاً خطی، ابهام میان اشتها و تحمل ریسک، اتکای زیاد به مقیاس ها و ماتریس های ساده، توجه محدود به عوامل رفتاری و وابستگی ریسک ها و تعیین نکردن مرز دقیق برخی مسئولیت های سازمانی، استفاده از آن را به عنوان مرجع مستقل محدود می کنند.

کاستی های یاد شده را نباید بدون توجه به زمان انتشار سند داوری کرد. بخش قابل توجهی از مفاهیمی که امروز برای مدیریت ریسک ضروری تلقی می شوند، پس از سال ۲۰۰۲ توسعه یافته یا صورت بندی منسجم تری پیدا کرده اند. اهمیت سند در این نیست که پاسخ کامل مسائل امروز را ارائه می کند؛ اهمیت آن در این است که بسیاری از جهت گیری های بنیادی مدیریت ریسک سازمانی را در متنی کوتاه و مدیریتی صورت بندی کرده است.

داوری نهایی آن است که این سند هنوز ارزش تاریخی، آموزشی و حرفه ای دارد، اما برای طراحی، استقرار یا ارزیابی کامل نظام مدیریت ریسک یک سازمان امروزی کافی نیست. از آن می توان برای فهم منطق پایه، آموزش مدیران و بررسی سیر تحول مدیریت ریسک استفاده کرد؛ مشروط بر آنکه مفاهیم و ابزارهای آن با استانداردها، چارچوب ها و الزامات جدید تکمیل شوند.

ارزش ماندگار سند در سادگی آن است و محدودیت اصلی آن نیز از همین سادگی ناشی می شود. این متن به خوبی توضیح می دهد که مدیریت ریسک چیست و چه اجزایی دارد، اما برای پاسخ به این پرسش که چگونه باید مدیریت ریسک را در ساختار حاکمیت، فرهنگ، راهبرد و تصمیم های واقعی یک سازمان امروزی نهادینه کرد، به منابع تکمیلی نیاز دارد

منابع

- ایزو . (۲۰۱۸). ایزو ۳۱۰۰۰: ۲۰۱۸؛ مدیریت ریسک - راهنماها . سازمان بین المللی استاندارد سازی
- رستمی نوروزآباد، مجتبی؛ شهرآزی، میلاد (۱۴۰۴). مدیریت ریسک سازمانی (از تئوری تا عمل)، انتشارات ترمه .
- کوزو. (۲۰۱۷). مدیریت ریسک سازمانی: یکپارچه سازی با راهبرد و عملکرد. کمیته سازمان های حامی کمیسیون ترویدی.
- موسسه حسابرسان داخلی. (۲۰۲۰). مدل سه خطی موسسه حسابرسان داخلی: به روز رسانی مدل سه خط دفاعی
- Institute of Risk Management, Association of Insurance and Risk Managers, & National Forum for Risk Management in the Public Sector. (2002). A Risk management standard of Risk Management.