

مدیریت ریسک چیست؟

مترجم:

- لیلی نیاکان

- دانشجوی دکتری اقتصاد دانشگاه تهران، کارشناس پژوهشی
گروه پژوهشی بیمه اشخاص

۱. مقدمه

اگرچه پوششی در مقابل عناصر و وحشیگری‌های طبیعت ایجاد کرد، اما ریسک‌های جدیدی را نیز خلق کرد. ساختمان‌های ساخته‌شده برای حفاظت، در برابر آسیب ضعیف بودند و پس‌انداز کردن برای انباشت ثروت نیز ناگزیر ریسک‌های جدیدی خلق کرد. کسانی که بیشتر پس‌انداز می‌کردند، در معرض هجوم کسانی که پس‌انداز نکرده بودند، قرار می‌گرفتند (چیزی که تا به امروز ادامه دارد). چالش مقابله با ریسک در روندی رو به رشد هنوز هم ادامه دارد. هرچه روش‌های جدید مقابله با ریسک کشف می‌شوند، ریسک‌های

از زمان پیدایش تمدن، انسان‌ها با احتمال خسارت روبه‌رو بوده‌اند. اجداد ما با محیطی سرشار از خطرات و مخاطرات مواجه بوده‌اند. نخستین خطرات که طبیعت و حیوانات وحشی بودند، موجب ریسک می‌شدند و این خطرات نه تنها حیوانات وحشی بلکه شامل انسان‌ها نیز می‌شد. به تدریج انسان‌ها آموختند که به صورت جمعی و فردی، اتفاقات ناخوشایند را پیش‌بینی و خود را برای مقابله با آن آماده کنند. آنها پناهگاه ساختند و شروع به ذخیره برای آینده کردند. این تدابیر



جدیدی نیز اغلب در نتیجه پیشرفت نمود پیدا می‌کنند. مهار انرژی، زندگی را آسان‌تر کرده است، اما ریسک‌های جدیدی نیز به وجود آورده است. تا حدود ۲۰۰ سال پیش منابع عمده انرژی، انرژی عضلات (انسان و حیوان)، باد و آب بودند که ریسک‌های متعادلی به همراه داشتند. از اوایل سده ۱۸۰۰ میلادی پیشرفت در تکنولوژی، منابع انرژی در دسترس را افزایش داد که با هر کدام از منابع جدید انرژی، ریسک‌های جدیدی نیز ظهور یافتند. به‌عنوان مثال، انقلاب صنعتی شاهد استفاده از بخار برای روند تولید بود و همراه با بخار، ریسک‌های جدیدی به وجود آمدند.

باید به این نکته توجه داشت که اگرچه سیستم حقوقی، چهارچوبی برای تعریف حقوق و مسئولیت‌های فردی و حمایت از این حقوق ایجاد کرد، در عین حال سیستم حقوقی به تنهایی تبدیل به یک منبع ریسک شد؛ زیرا با ایجاد این سیستم، پرداخت خسارت افرادی که مصدوم شده یا آسیب می‌دیدند، توسط دیگران انجام می‌شد. از زمانی که مفهوم حقوق و مسئولیت‌ها گسترش پیدا کرد، دلایل رفتاری دیگری نیز پدیدار شدند: ریسک‌های حقوقی مسئولیت بالقوه در بسیاری از تخلفات جدید نظیر آسیب‌های محیطی، تبعیض شغلی، آزار جنسی و خشونت در محل کار. آخرین توسعه ریسک که ما با آن مواجه هستیم، ریسک‌های ناشی از پیشرفت و تکنولوژی است. عصر اطلاعات، انواع ریسک‌های جدید را در بر دارد. اطلاعات ارزشمند است و در معرض آسیب‌بودن آن نمایانگر وجود ریسک است. روش جمع‌آوری اطلاعات در میزان این ریسک‌ها مؤثر است. زمانی که ثبت اطلاعات و داده‌ها بر روی رسانه‌ها به سختی صورت می‌گرفت حفاظت از اطلاعات و ردیابی سیستم امنیتی آنها آسان‌تر بود. ارتباط دو جانبه اینترنت و ارتباطات الکترونیک، اطلاعات ارزشمند را به روش‌های غیر قابل‌تصور در معرض ریسک قرار می‌دهند. هک‌هایی که به خرابکاری و دستبرد الکترونیکی روی آورده‌اند، جایگزین راهزنان و سارقانی شده‌اند که بازرگانان پیشین را مورد تهدید قرار می‌دادند.

با هر پیشرفتی در تکنولوژی، ریسک‌های جدیدی ایجاد می‌شود، بسیاری از ریسک‌های قدیمی همچنان باقی می‌مانند و در نتیجه، موجودی ریسک‌ها (فراوانی تجمع ریسک‌ها) افزایش پیدا می‌کنند.

مخاطرات ایجاد شده در تأسیسات هسته‌ای، طوفان‌های ویرانگر، زلزله، بمب‌گذاری مراکز تجاری و حملات تروریستی یادآور این حقیقت‌اند که تنها طبیعت تخریب و مرگ‌آفرینی نمی‌کند، بلکه انسان نیز دست به چنین اعمالی می‌زند. اگرچه سایر خسارات تنها به این دلیل که بر یک فرد یا یک شرکت تأثیر گذارند کم‌اهمیت‌ترند، اما برای شخصی که متحمل خسارت شده است دیگر چیزی به‌عنوان کم‌اهمیت معنی نمی‌دهد.

با روند افزایشی ریسک‌ها میزان خسارات ناشی از تصادفات نیز افزایش یافته است. جالب توجه آنکه هزینه‌های فزاینده خسارات تنها تابعی از تعداد فزاینده ریسک‌هاست. حتی خساراتی که از خطرات طبیعی نظیر طوفان، زلزله و سیل ناشی می‌شوند، شدتی در حال افزایش از خود نشان داده‌اند. علاوه بر این، هزینه خسارات در انطباق با تورم افزایش مجددی یافته‌اند. اگر چه زلزله، سیل و طوفان با همان سرعت پیشین رخ می‌دهند، اما فاجعه‌ها خسارت‌تر از قبل به نظر می‌رسد. دلیل روشن این امر آن است که ثروت، سرمایه‌گذاری و دارایی بیشتری در معرض خطر قرار گرفته است.

همانگونه که بیان شد، از وجود ریسک، گریزی نیست و جامعه بشری باید در جستجوی راه‌هایی برای مقابله با آن باشد. با برخی از ریسک‌ها - عموماً از نوع بنیادی - با تلاش‌های جمعی و دولت مقابله می‌شود. پلیس شهری و آتش‌نشانی‌ها مثال‌های خوبی برای روش‌های مقابله با ریسک به‌صورت کمک‌های جمعی می‌باشند. اگر چه جامعه و دولت می‌توانند در بسیاری از موارد از فشار ریسک بکاهند، برخی از ریسک‌ها در حوزه مسئولیت افراد جامعه قرار می‌گیرند. با توجه به گستره پهناور ریسک‌هایی که افراد و مشاغل با آن مواجه می‌شوند و تنوع راه‌هایی که می‌توان به مقابله با آنها پرداخت، یک روش سیستماتیک برای مقابله با ریسک‌ها مورد نیاز است. در مقابل ریسک‌های متنوعی که با آنها مواجه می‌شویم چه می‌توانیم بکنیم؟ ابتدا کدام ریسک‌ها باید مورد توجه قرار گیرند؟ و ریسک‌ها چگونه شناخته شوند؟ این سوالات از جمله مهم‌ترین سئوالاتی هستند که در بحث مدیریت ریسک به آنها پاسخ داده می‌شود.

۲. مدیریت ریسک

هدف از مدیریت ریسک، مدیریت نااطمینانی است و شامل

- به صورت سیستماتیک کلیه وظایف، فعالیت‌ها و مراحل عملکرد خود را بررسی کرده و تشخیص دهید که برای هر کارکرد چه اتفاقی خواهد افتاد؟
- گزارشات و یادداشت‌های خود را بررسی کنید تا اشتباهاتی را که در گذشته رخ داده‌اند، شناسایی کنید؛
- سیستم‌ها و فرایندها را برای شناسایی نقاط بحرانی تحلیل کنید؛
- با کارمندان و همکاران خود مشورت کنید.

- مرحله سوم: ارزیابی ریسک

در این مرحله، احتمال و نتایج هر ریسک شناسایی شده با استفاده از سنجه‌های آماده شده تحلیل می‌شود.

- کنترل‌های موجود برای هر ریسک را مورد توجه قرار دهید. با توجه به کنترل‌های موجود چه تدابیر دیگری برای کنترل ریسک باید اندیشیده شود.

- اثربخشی کنترل‌های موجود برای پیشگیری از رخداد ریسک و کاهش اثرات آن را برآورد کنید. تناسب و عدم تناسب کنترل‌های موجود را تعیین نمایید.

احتمال^۷ در واقع توصیف کیفی احتمالات و فراوانی است: ریسک با چه احتمالی رخ می‌دهد؟ در ماتریس تحلیل ریسک^۸، بهترین توصیف از احتمال رخداد ریسک (با توجه به سنجه‌های کنترل موجود) انتخاب می‌شود.

نتایج^۹ در واقع برآمد^{۱۰} یک پیشامد یا موقعیت به صورت خسارت، آسیب، زیان یا عایدی است. نتیجه پیشامد ریسکی چیست؟ در ماتریس تحلیل ریسک، بهترین توصیف از نتایج ریسک (با توجه به سنجه‌های کنترل موجود) انتخاب می‌شود.

در ماتریس تحلیل ریسک، تلاقی احتمال و نتیجه ریسک انتخاب می‌شود. در این صورت می‌توان گفت:

برآورد نرخ ریسک = برآورد نتیجه × برآورد احتمال

فعالیت‌های شناسایی^۱، ارزیابی^۲، پایش^۳ و کاهش تأثیر ریسک‌ها بر یک کسب‌وکار می‌شود. یک برنامه مدیریت ریسک صحیح با استراتژی‌های مدیریت ریسک مناسب می‌تواند مشکلات هزینه‌بر و استرس‌زا را به حداقل رسانده و ادعای خسارت و حقیقه را کاهش دهد. بنا به نظر بوهم^۴، مدیریت ریسک، فرایندی شامل دو فاز اصلی است: تخمین ریسک که شامل شناسایی، تحلیل و اولویت‌بندی است و کنترل ریسک که مراحل برنامه‌ریزی مدیریت ریسک، برنامه‌ریزی نظارت ریسک و اقدامات اصلاحی را شامل می‌شود. به اعتقاد فیرفلی^۵، مدیریت ریسک دارای هفت فاز است:

- شناسایی عوامل ریسک؛

- تخمین احتمال رخداد ریسک و میزان تأثیر آن؛

- ارائه راهکارهایی جهت تعدیل ریسک‌های شناسایی شده؛

- نظارت بر عوامل ریسک؛

- ارائه یک طرح احتمالی؛

- مدیریت بحران؛

- احیای سازمان بعد از بحران.

براساس الگوی استاندارد سازمان^۶ انگلستان در توسعه یک برنامه مدیریت ریسک، ۵ مرحله انجام می‌شود.

- مرحله اول: شناسایی زمینه ریسک

در این مرحله، شناسایی محل و شرایط رخداد ریسک نظیر یک محل کار مشخص، اداره، یک بخش کاری یا شعبه فروشگاه خرده‌فروشی انجام می‌شود.

- مرحله دوم: شناسایی ریسک

در این مرحله ریسک‌هایی شناسایی می‌شوند که احتمالاً بر دستیابی به اهداف کسب‌وکار تأثیر می‌گذارند. ابتدا باید ریسک توصیف شود: چه اتفاقی ممکن است رخ دهد؟ چگونه و چرا اتفاق خواهد افتاد؟

پس از آن نتایج ریسک باید توصیف شود: اگر ریسک محقق شود، چه اتفاقی خواهد افتاد؟

1. Identify
2. Assess
3. Monitor
4. Boehm
5. Fairly
6. Health and Safety Executive(HSE)

7. Likelihood
8. Risk Analysis Matrix
9. Consequence
10. Outcome



جدول ۱. ماتریس تحلیل ریسک

احتمال	کم‌یاب ^۱	نامحتمل ^۲	متوسط ^۳	محتمل ^۴	مطمئن ^۵	
	پیشامد ممکن است در شرایط استثنایی رخ دهد	پیشامد ممکن است در برخی موارد رخ دهد	پیشامد احتمالاً در برخی موارد رخ خواهد داد	پیشامد در اغلب شرایط رخ خواهد داد	انتظار می‌رود پیشامد در هر شرایطی رخ دهد	
	کمتر از یک بار در سال	حداقل یک بار در سال	حداقل یک بار در ۶ ماه	حداقل یک بار در ماه	حداقل یک بار در هفته	
نتیجه	سطح	۱	۲	۳	۴	۵
ناچیز ^۶	۰	۰	۰	۰	۰	بدون آسیب، زیان مالی اندک
کم ^۷	۱	۱	۲	۳	۴	کمک‌های اولیه، زیان متوسط
جدی ^۸	۲	۲	۴	۶	۸	مراقبت‌های پزشکی، زیان مالی زیاد، ملاحظات زیست‌محیطی متوسط، زیان متوسط در اشتها، انقطاع متوسط در کسب‌وکار
بزرگ ^۹	۳	۳	۶	۹	۱۲	آسیب‌های متعدد بلندمدت، زیان مالی بزرگ، ملاحظات زیست‌محیطی شدید، زیان بزرگ در اشتها، انقطاع بزرگ در کسب‌وکار
تلفات ^{۱۰}	۴	۴	۸	۱۲	۱۶	یک فوت
متعدد ^{۱۱}	۵	۵	۱۰	۱۵	۲۰	چندین فوت و آسیب‌های جدی بلندمدت

1. Rare
2. Unlikely
3. Moderate
4. Likely
5. Certain
6. Negligible
7. Minor
8. Serious
9. Major
10. Fatality
11. Multiple

جدول ۲. علائم و اختصارات ماتریس تحلیل ریسک

توضیحات	اولویت ریسک	برآورد نرخ ریسک
بدون ریسک ^۱ : هزینه‌های برخورد با ریسک در مقایسه با نتایج ناچیز آن، بالا است.	N	۰
ریسک پایین ^۲ : نیازمند توجه به تغییرات آتی یا اعمال تغییرات آتی در محیط کار یا فرایندهاست.	L	۱-۳
ریسک متوسط: نیازمند اقدامات اصلاحی از طریق فرایند برنامه‌ریزی یا بودجه‌ریزی است.	M	۴-۶
ریسک بالا: نیازمند اقدامات اصلاحی فوری است.	H	۸-۱۲
ریسک بی‌نهایت ^۳ : نیازمند قطع فوری کار و فرایند و به دنبال آن، انجام اقدامات اصلاحی است.	E	۱۵-۲۵

به طرف دیگر یا تسهیم ریسک از طریق یک قرارداد، ترتیبات بیمه‌ای یا سرمایه‌گذاری مشترک با شرکاء.

در انتخاب بهترین روش برای برخورد با ریسک از میان پنج روش فوق، عوامل زیر باید مد نظر قرار گیرند:

- اگر فعالیت ریسکی انجام نگیرد، چه اتفاقی خواهد افتاد؟
- آیا سطح ریسک در حدی است که می‌توان با وجود آن فعالیت را ادامه داد؟

• آیا هزینه کنترل‌های مورد نیاز بالاتر از منافع حاصل از فعالیت است؟

• آیا عدم موفقیت فعالیت، پیامدهای وخیمی برای سایر حوزه‌های کسب‌وکار به دنبال خواهد داشت؟

• با توجه به دلایل اجتناب از ریسک، آیا ریسک‌گریزی کسب‌وکار شما در حدی غیر ضروری است؟

• آیا اجتناب از ریسک، بر اهمیت سایر ریسک‌ها می‌افزاید یا موقعیت‌های عایدی را با زیان مواجه می‌کند؟

- مرحله پنجم: پایش و تجدید نظر

مدیریت ریسک یک فرایند مستمر و در حال پیشرفت است. حتی در شرایطی که اگر سنج‌های موجود کنترل مناسب باشند، باید به‌طور منظم هرگونه تغییر مؤثر بر جنبه‌های شناسایی شده ریسک مورد بررسی و بازبینی قرار گیرند.

پس از تکمیل کنترل‌های مطرح شده، باید ریسک را با استفاده

اولویت‌بندی ریسک، ضرورت اجرای یک استراتژی در ارتباط با ریسک را نشان می‌دهد. درجه ریسک نشانگر اولویت‌بندی ریسک خواهد بود.

- مرحله چهارم: استراتژی‌های ریسک

هدف از این مرحله، توسعه گزینه‌های هزینه‌ای کارا برای برخورد با هر ریسک است. بهترین برخورد با ریسک از بین پنج روش زیر انتخاب می‌شود:

- حذف ریسک از طریق توقف فعالیت یا برطرف کردن خطر؛ به عبارت دیگر، از انجام فعالیت‌های ایجادکننده ریسک اجتناب شود.

- پذیرش اثرات منفی ریسک؛ ممکن است با وجود انجام همه تدابیر کاهش ریسک، باز هم نتوان ریسک را به‌طور کامل حذف کرد.

- کاهش احتمال رخداد ریسک به‌منظور کاهش برآمدهای منفی آن؛ از طریق مراقبت‌های پیشگیرانه، ضمانت و مدیریت کیفیت، تغییر سیستم‌ها و فرایندهای کسب و کار می‌توان احتمال رخداد ریسک را کاهش داد.

- کنترل یا کاهش نتایج پس از رخداد ریسک؛ از طریق برنامه‌ریزی محتمل‌الوقوع، حداقل کردن مواجهه با منابع ریسک یا جابه‌جایی فعالیت و منابع کسب‌وکار می‌توان نتایج پیشامد ریسک را کنترل کرده یا کاهش داد.

- انتقال ریسک به‌صورت کلی یا جزئی از طریق انتقال مسئولیت

1. No Risk
2. Low Risk
3. Extreme

از بازیابی‌های منظم و بررسی پیشرفت و اثربخشی استراتژی ریسک انتخابی، مورد ارزیابی مجدد قرار داد.

۳. شناسایی ریسک

در چرخه مدیریت ریسک، شناسایی ریسک و ارزیابی آن دو مرحله بسیار حائز اهمیت تلقی می‌شوند. حوادثی که می‌توانند بر اهداف یک شرکت یا فرد تأثیرگذار باشند، باید شناسایی و ارزیابی شوند تا بتوان به نحو مناسب و مقتضی به آنها واکنش نشان داد.

شناسایی ریسک باید جامع باشد تا تمامی حوزه‌های فعالیت کسب و کار طی زمان را دربرگیرد. حاصل این مرحله، فهرستی از حوادث به همراه توضیحاتی در مورد چرایی و چگونگی تأثیر این حوادث بر برنامه‌ریزی کسب و کار است. ارزیابی ریسک به عنوان گام بعدی نیازمند تعیین جایگاه تقریبی و نسبی ریسک‌های شناسایی شده و اظهارات قابل ارزیابی و اندازه‌گیری در مورد تأثیر احتمالی هر یک از این ریسک‌ها و احتمال وقوع آنها است. برخی حوادث بر اساس نحوه توزیع‌شان در مدل‌ها یا اطلاعات به دست آمده از بازار قابل اندازه‌گیری هستند؛ برخی دیگر با تشکیل سناریو یا مراجعه به پایگاه‌های اطلاعاتی و مستندات شرکت‌ها اندازه‌گیری می‌شوند. در نهایت، فهرستی از حوادث تنظیم می‌شود که براساس تأثیر احتمالی و احتمال وقوع دسته‌بندی شده‌اند. تکنیک‌های مختلفی برای شناسایی ریسک وجود دارد که در برخی از آنها ارزیابی ریسک نیز تلفیق شده است.

۳-۱. تحقیق و تفحص در مورد ریسک

یکی از ابزارهای مفید در گردآوری اطلاعات پیرامون ریسک، تحقیق و تفحص در مورد ریسک است. به عنوان مثال، مصاحبه‌هایی توسط واحد مستقل کنترل ریسک به دفعات نسبتاً نزدیک به هم اجرا می‌شود تا نسبت به روند منظم اطلاعات، اطمینان حاصل شود. در نتیجه این مصاحبه‌ها، ریسک‌های شناسایی شده با بیانی ساده تبیین می‌شوند و در مورد علل وقوع ریسک، همبستگی با دیگر ریسک‌ها و اقدامات موجود جهت تخفیف ریسک توضیحاتی ارائه می‌گردد. براساس تجربه و قضاوت مصاحبه‌شونده‌ها، ریسک‌ها با توجه به فاکتورهای نظیر خسارت احتمالی، احتمال وقوع و وضعیت کنونی کنترل ریسک ارزیابی می‌شوند. ماهیت طبیعی این فرایند، امکان

تحلیل روند و ردیابی ریسک‌ها طی چندین سال را فراهم می‌آورد. علاوه بر این، حضور طیف وسیعی از افراد درگیر، جریان افقی اطلاعات و در نتیجه تقویت فرهنگ ریسک را میسر می‌سازد.

۳-۲. گزارش موردی

برای حصول اطمینان از وجود ظرفیت بالقوه واکنش کوتاه مدت به ریسک، باید مکانیزمی وجود داشته باشد که تغییرات کوتاه‌مدت عمده در زمینه ریسک را به صورت موردی منعکس کند. شیوه‌های موجود گزارش‌دهی برای مدیریت ریسک از جمله این مکانیزم‌ها هستند.

۳-۳. بررسی بازار

یک سیستم جامع شناسایی ریسک، هم از منابع داخلی و هم منابع خارجی استفاده می‌کند. اطلاعات مورد استفاده عموم از منابعی نظیر مطبوعات تخصصی و پایگاه‌های اطلاعاتی به دست می‌آید. به یک سیستم هوشمند فیلترینگ همراه با نظارت انسانی برای استفاده بهینه از این منابع اطلاعاتی نیاز است تا ریسک‌ها شناسایی شوند. دنبال کردن منابع خارجی، این فرآیند را تکمیل می‌کند و اطمینان می‌دهد که به تمام ریسک‌های احتمالی طبق یک برنامه زمانی پرداخته می‌شود. این امر به ویژه برای نظارت بر ریسک اعتبار، شناسایی ریسک‌های نوظهور و شناخت گرایش‌های موجود در نظارت و قضاوت بین‌المللی مناسب است.

۳-۴. ریسک‌های نوظهور

ریسک‌های نوظهور از آن جهت که محدوده گسترش و تأثیرات بالقوه آن نامعلوم و مبهم است، به سادگی قابل درک نیست، اما از آن جهت که می‌توانند سریعاً تبدیل به خسارات عمده‌ای برای صنعت بیمه شوند، خطرناک می‌باشند. شناسایی و ارزیابی حرفه‌ای ریسک‌های نوظهور، عنصری نوظهور در مدیریت ریسک محسوب شده و مدیریت ریسک شرکتی را از مدیریت ریسک سنتی متمایز می‌سازد.

راهکار شرکت اسکورا^۱ برای شناسایی ریسک‌های نوظهور، تشکیل یک شبکه داخلی از مشاهدات و گزارشات کارشناسان حقوقی، متخصصان رسیدگی به خسارات، بیمه‌گران و مدیران

1. Stock Company of Reinsurance (SCOR)

شکل - ۱: فرایند شناسایی ریسک



حرفه‌ای حوادث با احتمال وقوع پایین، مدیریت ریسک شرکتی را با مدیریت استراتژیک شرکت ارتباط داده و اطمینان حاصل می‌نماید که حد تحمل ریسک شرکت لحاظ شده باشد.

۳-۶. ریسک فرایندها

یک ابزار مهم شناسایی و ارزیابی سیستماتیک ریسک فرایندها، سیستم کنترل درونی یک شرکت است. اساس سیستم کنترل درونی، درک صحیح از فرایندهای شرکت است. میان فرایندهای اصلی نظیر پرداخت خسارت یا حسابداری مالی و فرایندهای حمایتی نظیر مدیریت سرمایه‌گذاری و مدیریت زیرساخت‌های تکنولوژی اطلاعات تمایز وجود دارد. کارشناسان فرایندها براساس ماتریس کنترل ریسک، کنترل ریسک مبتنی بر فرایند را شناسایی می‌نمایند. سیستم کنترل درونی، نقش مهمی در شناسایی و تقلیل ریسک‌های عملیاتی دارد.

۳-۷. ریسک اعتباری^۱

به‌دنبال بحران مالی سال ۲۰۰۷ بسیاری از شرکت‌ها نظارت بر

ریسک است که با ترکیب منابع اطلاعاتی خارجی کارشناسان بیمه‌ای کل صنعت بیمه به فیلترینگ و ارزیابی ریسک‌های نوظهور شناسایی شده می‌پردازد. اگر چه هدف اصلی از پردازش یک ریسک نوظهور، اجتناب از زیان‌های غیر منتظره و افزایش غیر قابل پیش‌بینی آن است، می‌توان از آن برای شناسایی فرصت‌های راهبردی بالقوه مرتبط با ریسک‌های نوظهور استفاده کرد.

۳-۵. حوادث نادر با احتمال وقوع بسیار پایین

برای پردازش حوادث با احتمال وقوع پایین، می‌توان از شناسایی و کنترل کرانه‌های انتهایی تابع توزیع علل وقوع ریسک‌های عمده در حوزه‌های مختلف نظیر بیمه‌گری، نگهداری ذخیره، فعالیت اصلی بیمه‌ای، واگذاری مجدد، ریسک‌های عملیاتی و اموال و دارایی استفاده کرد. انجام این فرایند، شرکت را مطمئن می‌سازد که بر ریسک‌هایی که در معرض آن است و ناشی از عواملی است که در تابع توزیع علل اصلی وقوع ریسک می‌باشد، کنترل داشته و آنها را در حد تحمل ریسک اعلام‌شده شرکت نگه می‌دارد. یک مدیریت

1. Credit Risk



ریسک‌های اعتباری خود را افزایش داده‌اند و این امر موجب ارتقای کیفیت شناسایی و ارزیابی ریسک در این حوزه شده است. یک ارزیابی ریسک اعتباری علاوه بر اعتبار و اطمینان در بخش اموال و حوادث، شامل اقلام ترازنامه‌ای مرتبط با بیمه اتکایی زندگی، واگذاری مجدد، دارایی‌های بیمه‌گذاران و انواع قراردادهای حساس به ریسک اعتبار نیز می‌شود. همانند سایر ریسک‌های عمده، تحلیل جامع ریسک‌های اعتباری باید با سطوح تحمل ریسک شرکت قیاس شود و در صورت مغایرت، تدابیری اندیشیده شود.

در مجموع می‌توان گفت که، بهترین شیوه برای شناسایی و ارزیابی ریسک مشتمل بر یک سیستم چند بخشی است که به تناسب موقعیت خاص شرکت، ریسک‌ها و منابع، تصویر جامعی از ریسک‌هایی که شرکت در معرض آن است و شیوه‌های برخورد با آنها را فراهم می‌آورد.

۴. ارزیابی ریسک

در حقیقت از طریق ارزیابی ریسک میزان کارآمدی و اثربخشی روش‌های کنترلی موجود مشخص شده و داده‌های باارزشی برای تصمیم‌گیری در زمینه کاهش ریسک، خطرات، به‌سازی سیستم‌های کنترلی و برنامه‌ریزی برای واکنش به آنها فراهم می‌گردد.

ارزیابی ریسک کمی نیازمند محاسبه دو مؤلفه ریسک یعنی شدت پیامد رخداد و احتمال روی دادن آن رخداد است. برای به‌دست آوردن وزن احتمال یا وزن شدت پیامد سه روش وجود دارد:

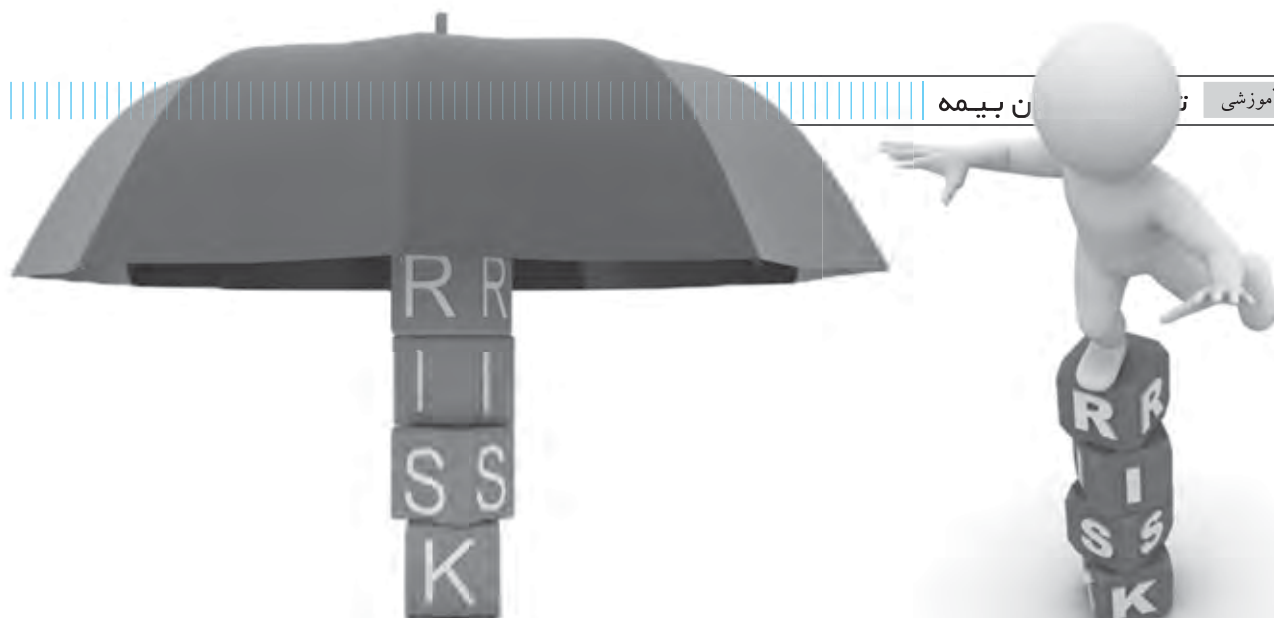
- روش‌های کمی^۱ که نتیجه در نهایت به یک عدد منتهی می‌شود؛
- روش‌های کیفی^۲ که نتیجه حاکی از کیفیت خاصی در زمینه ریسک خواهد بود؛
- روش‌های شبه کمی^۳ که در بیشتر این روش‌ها از ماتریس ریسک استفاده می‌شود.

در روش ارزیابی ریسک کمی، احتمال وقوع یک حادثه خاص و پیامدهای آن محاسبه یا برآورد می‌گردد و سپس از معیار عددی به‌دست‌آمده برای قضاوت در مورد پذیرفتنی بودن ریسک خطرات استفاده می‌شود. انجام برآورد عددی کار مشکلی است، لذا روش کیفی، کاربرد بیشتری دارد.

ارزیابی ریسک، فرایندی است که نیازمند تجربه، تخصص و دقت

1. Quantitative Methods
2. Qualitative Methods
3. Semi-Quantitative





کاربردی، زیرساخت، کنترل یا طراحی است که می‌تواند از سوی خطر در جهت مختل کردن تمامیت سیستم‌های موجود، روندهای کاری و سازمانی، مأموریت‌ها و فعالیت‌های سازمان، مورد استفاده و بهره‌برداری قرار گیرد.

در مجموع می‌توان گفت که مراحل مورد نیاز برای شناسایی حوزه کسب‌وکار و دارایی‌های موجود در آن، تهدیدهای موجود علیه دارایی‌ها، اولویت‌بندی نقاط ضعف مربوط به تهدیدها، مشخص نمودن سطح ریسک‌ها و کنترل‌های مناسب را ارزیابی ریسک گویند.

نخستین گام اجرای فرایند ارزیابی ریسک، شناسایی تمامی دارایی‌های موجود در حوزه مورد بررسی است تا پس از آن بتوان ریسک‌های متوجه هر یک از آنها را به‌طور کامل مشخص نمود. دارایی‌ها به چهار دسته دارایی‌های اطلاعاتی، نرم‌افزاری، سخت‌افزاری و انسانی تقسیم شده و برای هر یک، نمونه‌هایی ذکر شده است.

• دارایی‌های سخت‌افزاری

شامل سرورها، کامپیوترهای شخصی، انواع CD، فلاپی، پرینتر، اسکنر، نوت بوک، فلش مموری، درایورهای قابل حمل، اجزاء شبکه ارتباطی از قبیل روترها، مودم، سوئیچ، و ... است.

• دارایی‌های نرم‌افزاری

شامل نرم‌افزارهایی که در داخل سازمان تولید شده و در راستای مأموریت و فعالیت‌های سازمان مورد استفاده قرار می‌گیرند؛

بالا بوده و باید در قالب کار تیمی و با بهره‌گیری از توان مسئولین و کارشناسان انجام پذیرد. این فعالیت تیمی زمانی به نتیجه دلخواه دست خواهد یافت که تیم ارزیاب، علاوه بر برخورداری از تجربه و تخصص لازم، از زبان مشترکی نیز در درک مفاهیم و روش‌های مورد استفاده برخوردار باشند.

افراد مختلف از یک ریسک مشخص، برداشت‌های گوناگونی دارند. برآورد نرخ ریسک از سوی افراد غیرعلمی با نتایج آماری و معادلات ریاضی ریسک هم‌خوانی ندارد. بر این اساس، مفهوم ریسک دو جنبه گوناگون را دربرمی‌گیرد:

• برداشت افراد غیرعلمی از میزان ریسک که به آن ریسک ذهنی (یا درکی) می‌گویند.

• برآورد علمی بر پایه اطلاعات آماری از نرخ ریسک، که به آن ریسک واقعی می‌گویند.

ریسک ذهنی ممکن است بیشتر یا کمتر از ریسک واقعی باشد. ارزیابی ریسک ممکن است آگاهانه یا ناآگاهانه صورت گیرد. در این بین عواملی وجود دارند که بر قضاوت ناصحیح افراد مؤثر هستند و برای اصلاح سطح ریسک‌پذیری، لازم است این عوامل شناخته شوند.

- **خطر:** شرایطی که به‌طور بالقوه امکان دارد سبب ایجاد یک واقعه ناگوار (از قبیل دسترسی غیر مجاز، دستکاری، افشاء یا خرابکاری) روی دارایی‌های اطلاعاتی موجود در سازمان گردد.

- **آسیب‌پذیری:** ضعف موجود در یک سیستم، برنامه

نرم‌افزارهایی که در خارج از سازمان تهیه شده و در راستای مأموریت و فعالیت‌های سازمان مورد استفاده قرار می‌گیرند، نظیر سیستم‌های اتوماسیون اداری، نرم‌افزارهای مالی، انبارداری و ...؛ و نرم‌افزارهای معمول و موجود در بازار که برای انجام امور عادی و روزمره مورد استفاده قرار می‌گیرند، نظیر نرم‌افزارهای تایپ و صفحه گسترده، نقشه کشی و ...

• سرمایه‌های اطلاعاتی

شامل هر نوع اطلاعات چه فیزیکی (کاغذ، نامه و ...) و چه غیر فیزیکی (داده‌ها) که برای سازمان دارای ارزش باشند: اطلاعات کاری و سازمانی از قبیل سوابق پروژه‌ها و فعالیت‌های انجام شده، مأموریت و گزارش‌های سازمانی موجود، روندها و طرح‌های سازمانی و ...؛ اطلاعات پرسنلی از قبیل اطلاعات حقوقی، اطلاعات شخصی، سوابق کاری و خدمتی، شماره حساب‌های بانکی و ...؛ اطلاعات امنیتی از قبیل کلمات عبور، اطلاعات مربوط به رمزنگاری و احراز صلاحیت و احراز هویت کاربران و ...؛ بانک‌های اطلاعاتی موجود روی سرورها، فایل‌های اطلاعاتی ذخیره شده روی سرورها یا کامپیوترهای کاربران و سایر موارد.

• سرمایه‌های انسانی

سرمایه‌های انسانی شامل تمامی کارکنانی می‌شود که در سازمان مشغول به کار بوده و در صورت از دست دادن آنها، به روند اجرایی سازمان و روندهای کاری و سازمانی لطمه وارد خواهد شد: مدیران ارشد قسمت‌های مختلف سازمان و جانشینان و معاونین آنها؛ رؤسای بخش‌ها و اداره‌ها؛ پرسنل متخصص و باسابقه؛ مدیران و کارشناسان بخش تکنولوژی اطلاعات و امنیت اطلاعات؛ پرسنل متخصص و تکنیکی موجود در بخش‌ها و سایر موارد.

پس از تعیین و شناسایی دارایی‌ها، تیم ارزیابی اقدام به شناسایی ریسک‌های مربوط به هر یک از دارایی‌ها می‌نماید. همانطور که از تعریف ریسک استنباط می‌شود، هر ریسک از سه عنصر یا جزء تشکیل شده است و لذا تعریف ریسک به معنی تعیین دقیق این سه عنصر است. این سه عنصر عبارت‌اند از: عامل تهدید، سرمایه و اثر تهدید. به عبارت دیگر:

عامل تهدید + سرمایه + اثر تهدید = ریسک

همانگونه که در رابطه فوق مشاهده می‌شود، با تغییر هر یک از اجزاء موجود در طرف راست تساوی فوق، ریسک جدیدی حاصل می‌گردد. در نتیجه، در اغلب موارد امکان دارد که برای یک دارایی مشخص، چندین ریسک مختلف را با توجه به نوع عامل تهدید و انواع اثرات آن بتوان شناسایی نمود. در این صورت، برای هر مورد، یک شناسنامه ریسک به طور مجزا تهیه خواهد شد.

اعضای تیم ارزیابی ریسک می‌توانند از این دسته‌بندی نمونه‌ای ریسک‌ها به عنوان نقطه شروع جهت شناسایی انواع ریسک‌های قابل اعمال بر دارایی‌ها استفاده نمایند. نکته قابل ذکر اینکه اعضای تیم باید بر اساس تجربه و تخصص خود و با استفاده از سوابق مربوط به حوادث گذشته، تمامی ریسک‌های محتمل قابل اعمال بر مجموعه تحت بررسی خود را شناسایی نمایند. در هنگام مشخص نمودن ریسک‌ها، توجه به این نکته ضروری است که تنها از ریسک‌هایی می‌توان چشم‌پوشی کرد که احتمال آنها صفر (غیر ممکن و محال) باشد. در غیر این صورت، حتی کم‌احتمال‌ترین ریسک‌ها نیز باید ثبت شوند. نکته دیگر این است که برخی از ریسک‌ها ممکن است از سوی عوامل مختلف اعمال شوند که همانگونه که پیش از این نیز گفته شد، برای هر یک از آنها باید شناسنامه جداگانه‌ای تهیه شود.

در مجموع می‌توان گفت که، ارزیابی ریسک در نهایت به یک برنامه برای کنترل ریسک منجر خواهد شد. دنبال کردن پنج مرحله زیر برای ارزیابی ریسک ضروری است:

- مرحله اول: شناسایی خطرات؛
- مرحله دوم: تعیین اینکه چه کسی و چگونه ممکن است آسیب ببیند؛
- مرحله سوم: بررسی ریسک‌های موجود و اجرای اقدامات پیشگیرانه؛
- مرحله چهارم: ثبت یافته‌ها و نتایج؛
- مرحله پنجم: بازبینی ارزیابی صورت گرفته و روزآمد کردن آن در صورت لزوم.