یادگیری،شناسایی وکنترل ریسک ها وروشهای برنامه ریزی در مقابله باخطرات



مدیریت ریسک

مدرس: امیرهادی کا مبوزیا

سرفصل دروس:

۱. مفعوم ودامنه ریسک

۲. فرآیند مدیریت ریسک

۳. شناسائی ریسک

۴. ارزیابی ریسک

۵. کنترل ریسک

۶. نظارت

۷. مدیریت ریسک درعمل

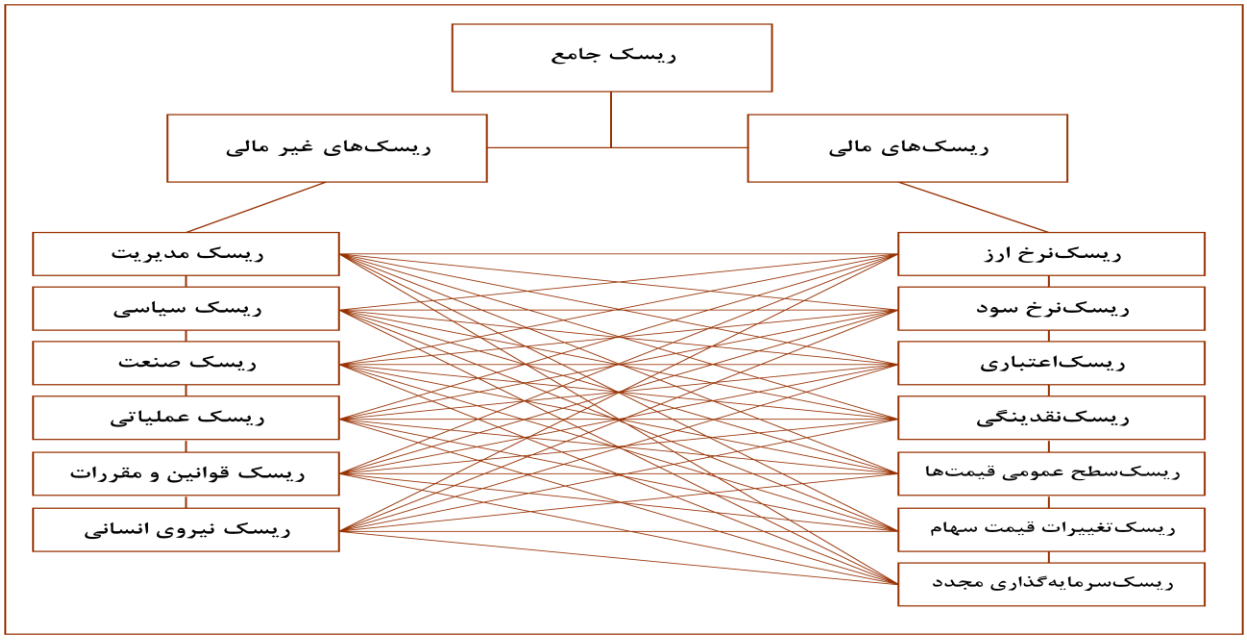
۱.مفهوم ودامنه ریسک

احتمال تفاوت بازده واقعی از بازده مورد انتظار

احتمال نوسان پذیری واحتمال وقوع رویدادی که پیش بینی نکرده ایم و یا احتمال انحراف از چیزی که پیش بینی کرده بودیم.

منابع ریسک

نمودار زیر انواع ریسک‌ها و رابطهٔ آنها را نشان می‌دهد. در این نمودار ارتباط شبکه‌ای انواع ریسک به مفهوم روابط پیچیده‌ای است که هر یک از انواع ریسک با انواع دیگر دارد.



ریسک تغییر پیش‌فرض‌ها: طبیعی‌ست که پیش‌فرض‌های ما از دنیای پیرامونی دستخوش تغییر و تحول قرار بگیرد. برای ما که در ایران زندگی می‌کنیم، تغییر یک‌شبه نرخ ارز چیز عجیبی نیست و همین یک مولفه می‌تواند به‌تنهایی تمام تصمیم‌گیری استراتژیک سازمان را به خطر بیاندازد. در تدوین استراتژی می‌توانیم با این ریسک به دو شیوه مواجه شویم: نخست آنکه در پیش‌فرض‌ها سناریوهایی برای نوسان پیش‌فرض‌ها در نظر بگیریم و به‌جای اتکا به یک نرخ ارز (یا حتی بازه‌ای از نرخ‌ها)، چند سناریوی مختلف را برای نرخ ارز در نظر بگیریم. رویکرد دوم شناسایی متغیرهای اهرمی در تدوین استراتژی است. هرگونه نوسان در متغیرهای اهرمی می‌تواند منجر به تغییرات قابل‌ملاحظه‌ای در استراتژی شود. شناسایی این متغیرها و سپس درنظرگرفتن راهکارهایی برای پوشش یا انتقال ریسک ناشی از آنها می‌تواند مانایی استراتژی‌ها را افزایش دهد.

ریسک حصول اهداف: اصولاً وقتی اهداف را مشخص می‌کنیم، تصوری از مدینه فاضله در ذهن داریم. اما واقعیت این است که تعیین اهداف باید با ترسیم موقعیت دستیابی به آنها همراه شود. آیا حصول اهداف ریسک جدیدی را به ما تحمیل می‌کند؟ برای مثال، ممکن است دستیابی به سهم بالاتری از بازار، منجر به تغییر کلاس رقابتی سازمان‌مان و به تبع، پیدایش

شکل جدیدی از فشارهای رقابتی شود. زمان حصول اهداف نیز مهم است. عرضه تجاری واکسن کرونا می‌تواند یک هدف استراتژیک باشد، اما زمان عرضه و پیشگامی در بازار است که به این هدف ارزش می‌بخشد.

ریسک واکنش ذی‌نفعان :غیرممکن است که تصمیم استراتژیک جدیدی بگیریم و یکی از گروه‌های ذی‌نفع به مخالفت با این تصمیم نپردازد. با تصمیم به افزایش کیفیت محصول برای جلب رضایت مشتری، باید انتقادهای سهامدار به‌دلیل کاهش حاشیه سود را بپذیریم. به همین دلیل، تدوین استراتژی بدون تحلیل انتظارات ذی‌نفعان چیز خوبی از آب در نمی‌آید! البته نباید این نکته را از یاد ببریم که هیچ‌وقت نمی‌شود همه را راضی نگه داشت و تحلیل ریسک ذی‌نفعان هم با اتکا روی همین نکته، توجه ما را به سمت ذی‌نفعان پرریسک جلب می‌کند.

ریسک عملیاتی اجرا :بلاخره استراتژی باید به عملیات تبدیل شود و خودش را به شکل‌هایی مثل سرمایه‌گذاری در ظرفیت تولید، تنوع‌بخشی به کسب‌وکارها، راه‌اندازی یک طرح توسعه، آموزش نیروی انسانی و موارد مشابه نمایان سازد. این اقدامات یا هر اقدام اجرایی دیگری ریسک‌های عملیاتی خاص خودش را دارد. این ریسک‌ها ممکن است در سطح صورت‌مسئله‌های کوچکی نظیر دیر رسیدن مواد و مصالح ساخت‌وساز باشند،

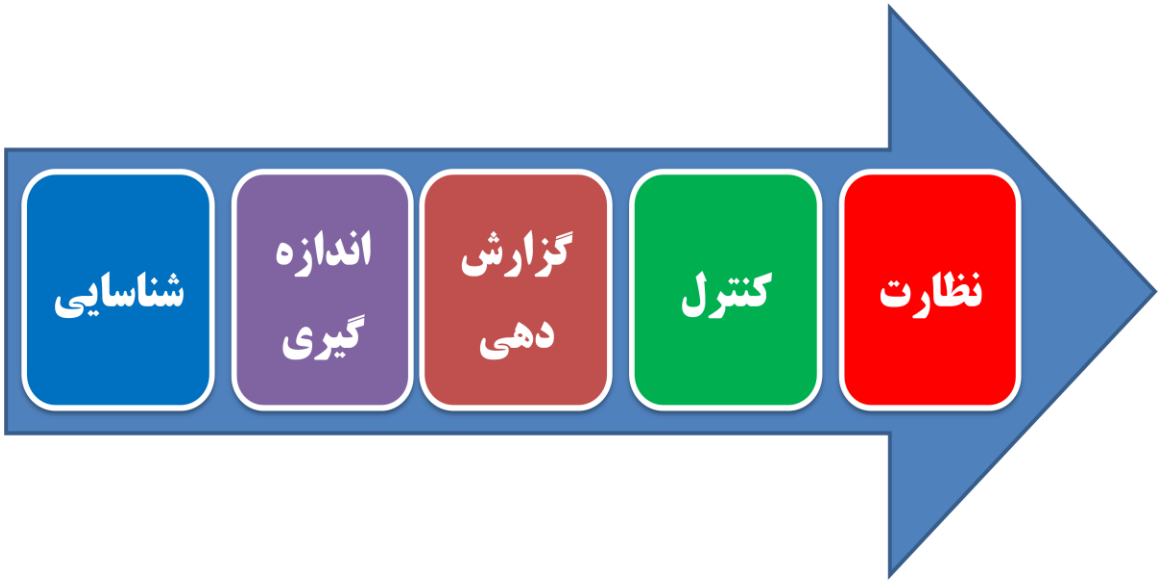
اما به هر حال نمی‌توان آنها را نادیده گرفت. عدم توجه به این ریسک‌های عملیاتی سبب می‌شود پای استراتژی هرگز به زمین نرسد!

ارزیابی ریسک استراتژی محدود به همین چهار سرفصل نیست؛ اما پرداختن به همین موارد و تحلیل آنها در قالب پیوست‌هایی به استراتژی سازمان می‌تواند ما را یک گام جلو ببرد، گامی که به ویژه در محیط نامطمئن، آشفته، و بی‌ثبات امروز ارزشش را دارد!

مدیریت ریسک

هدف مدیریت ریسک کنترل پیامدهای نامطلوب ناشی از تحمل ریسک و همچنین اطمینان یافتن از دستیابی به فوائد پذیرش ریسک است.

۲.فرایند مدیریت ریسک



۳.شناسایی ریسک

پس از اینکه فرآیندها مشخص شد، باید ریسک های هر فرآیند هم شناسایی شود. در این مرحله می توان با برگزاری جلسات طوفان فکری و همفکری گروهی ریسک های هر فرآیند را شناسایی کرد. در شناسایی ریسک ها باید به دنبال این باشیم که اگر فلان اتفاق افتاد،

آنگاه چه پیامدهایی برای ما بوجود مـی آیـد. (توصـیه مـی شـود از دو کلمه اگر .... آنگاه استفاده شود تا ریسـک هـا بهتـر شـناخته شـوند.) بـه عنوان مثال اگر در تولیـد مشـکلی بوجـود بیایـد، پیامـد آن تحویـل بـا تاخیر محصول برای مشـتری اسـت و پیامـد نهـایی نارضـایتی مشـتری و احتمالاً پرداخت جریمه تاخیر است.

برای تمام فرآیند بایستی همه ریسک هـا و پیامـدهای آن هـا را محاسـبه کنیم.

این نکته را هم باید مد نظر قرار داد کـه فرآینـد شناسـایی ریسـک یـک اقدام یک روزه نیست، بلکه با توجه بـه ماهیـت فرآینـدها و چرخـه عمـر یک پروژه، ممکن است ریسک های جدید بوجـود بیایـد یـا ریسـک هـایی که قبلاً شناسـایی نشـده بـود، شناسـایی شـود. لـذا لازم اسـت فراینـد شناسایی ریسک همواره فعال باشد.

مزایای شناسایی ریسک

از آغاز یک پروژه تا پایان آن ریسک اجتناب‌ناپذیر است. ریسک همیشه وجود دارد و در برنامه‌های بزرگتر که شامل یک سرمایه‌گذاری قابل توجه است، حضور پررنگ‌تری خواهد داشت.

- شناسائی موارد مهم جهت رفع سریع

مزیت مهم شناسایی ریسک، تجزیه و تحلیل کامل و کشف این مسئله است که چه ریسک‌هایی باید برطرف شوند تا براساس احتمالات و تأثیر آنها، روند کار متوقف نشود. سپس با توجه به هزینه یا زمان مناسب برای رسیدگی به آنها برنامه‌ریزی لازم انجام می‌شوند.

- **آگاهی از دامنه پروژه**

مزیت دیگر شناسایی ریسک مستلزم آگاهی از دامنه کامل یک پروژه است که به شما کمک می‌کند کاملا درباره آن فکر کنید و به موقع جوانب مثبت و منفی را بسنجید. این مسئله تا در هنگام طراحی استراتژی‌های کاهش ریسک‌ها کنترل شود.

- **کشف روش‌های مدیریتی**

کلیه ریسک‌ها شناسایی شده با یک برنامه‌ریزی دقیق برطرف می‌شوند بدون اینکه به اهداف پروژه و نتیجه نهایی مورد نیاز خدشه‌ای ایجاد کنند. همه فرضیات را می‌توان در یک لیست ذکر کرد و استراتژی مورد نیاز آنها را تجزیه و تحلیل کرد. تجزیه و تحلیل به حذف نادرستی‌های احتمالی ابتدای پروژه کمک می‌کند.

- **شناسائی ریسک‌های مثبت و منفی**

ریسک‌ها همیشه منفی نیستند و می‌توانند مثبت تلقی شوند. آنها ممکن است در دستیابی به اهداف یک پروژه نقش مهمی داشته باشد. همچنین به فرصت‌هایی منجر شوند که در ابتدای کار برنامه‌ریزی نشده بودند اما در طی مراحل شناسایی، به چشم آمده و تیم یا شرکت می‌تواند از این "ریسک‌های فرصت آفرین" بیشترین استفاده را ببرد.

۴.اندازه گیری وارزیابی ریسک

پس از شناسایی ریسک ها ما با تعداد زیادی از ریسک ها روبرو هستیم و مسلماً برنامه ریزی و کنترل همه این ریسک ها نمی تواند بصورت یکجا انجام شود، لذا باید این ریسک ها اولویت بندی شوند. سازمان ها باید با استفاده از روش های مختلف مانند روش FMEA ریسک ها را ارزیابی کرده و آن ها را اولویت دهی کنند.

به عنوان مثال می توان به هر ریسک یک عدد شدت ریسک و یک عدد احتمال وقوع ریسک اختصاص داد و با ضرب این دو عدد، میزان عددی هر ریسک را شناسایی کرد و با همین روش ریسک ها را اولویت بندی نمود. (این موضوع در دوره مجازی ایزو ۹۰۰۱ بصورت کامل و به همراه مثال توضیح داده شده است.

برآورد میزان ریسک

افراد مختلف از یک ریسک مشخص، برداشت‌هایی گوناگون دارند. برآورد میزان ریسک از سوی افراد غیرعلمی با نتایج آماری و معادلات ریاضی ریسک همخوانی ندارد.

مفهوم ریسک دو جنبه گوناگون را در بر می‌گیرد:

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

. برآورد علمی بر پایه اطلاعات آماری از میزان 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 ریسک پذیری، لازم است این عوامل شناخته شوند.

تعاریف:

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

آسیب‌پذیری :ضعف موجود در یک سیستم، برنامه کاربردی، زیرساختار، کنترل یا طراحی است که می‌تواند در جهت مختل کردن تمامیت سیستم‌های موجود و روال‌های کاری و سازمانی و مأموریت‌ها و فعالیت‌های سازمان، از سوی خطر مورد استفاده و بهره‌برداری قرار گیرد.

ریسک :احتمال اینکه یک خطر مشخص بتواند از یک آسیب‌پذیری (نقطه ضعف) خاص موجود در سیستم‌های سازمان استفاده نماید.

ارزیابی ریسک :مراحل مورد نیاز برای شناسایی حوزه و دارایی‌های موجود در آن، تهدیدهای موجود علیه دارایی‌ها، اولویت بندی نقاط ضعف مربوط به تهدیدها و مشخص نمودن سطح ریسک‌ها و کنترل‌های مناسب را گویند.

روش اجرا:

نخستین گام اجرای فرایند ارزیابی ریسک، شناسایی تمامی دارایی‌های اطلاعاتی 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 شده‌است

دسته بندی داراییها

سرمایه عبارتست از دارایی فیزیکی یا اطلاعاتی که برای سازمان دارای ارزش و اهمیت بوده و باید به‌طور خاص مورد محافظت قرار گیرد.

الف. دارایی‌های سخت‌افزاری

شامل سرورها، کامپیوترهای شخصی، انواعCD ، فلاپی، پرینتر، اسکنر، نوت بوک، Flash memory، درایورهای قابل حمل، اجزاء شبکه ارتباطی ازقبیل روترها، مودم، سوئیچ، .

ب. داراییهای نرم‌افزار

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

ج. سرمایه‌های اطلاعاتی

شامل هر نوع اطلاعات (چه فیزیکی از قبیل کاغذ و 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 گزارش‌ها 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 بر روی سرورها، فایل‌های اطلاعاتی ذخیره شده بر روی سرورها یا کامپیوترهای کاربران سایر موارد.

د. سرمایه‌های انسانی

سرمایه‌های انسانی شامل تمامی کارکنانی می‌شود که در سازمان مشغول بکار بوده و در صورت از دست دادن آنها، به روند اجرایی سازمان و روال‌های کاری و سازمانی لطمه وارد خواهد شد. نظیر: مدیران ارشد قسمت‌های مختلف سازمان و جانشینان و معاونین آنها ، رؤسای بخش‌ها و دوایر ، پرسنل متخصص و با سابقه ، مدیران و کارشناسان بخش IT و امنیت اطلاعات ، پرسنل متخصص و تکنیکی موجود در دوایر و 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 ارائه شده برای ریسک استنباط می‌شود، هر ریسک از سه عنصر یا جزء تشکیل شده است. لذا تعریف ریسک به معنی تعیین دقیق این سه عنصر است. این سه عنصر عبارتند از عامل تهدید، سرمایه و اثر تهدید. به عبارت دیگر:

ریسک = عامل تهدید + سرمایه + اثر تهدید

همان‌گونه که از رابطه فوق بر می‌آید، با تغییر هر یک از اجزاء موجود در طرف چپ تساوی فوق، ریسک جدیدی حاصل می‌شود. 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 به‌طور مجزا تهیه خواهد شد. در ادامه به مشخص کردن انواع عوامل تهدید قابل اعمال بر روی دارایی‌های اطلاعاتی، و نیز اثرات ناشی از آن‌ها می‌پردازیم

۲ -دسته بندی عوامل تهدید

تهدیدات طبیعی

طوفان، زمین لرزه، گردباد، رانش زمین، بهمن، طوفان‌های الکتریکی و رویدادهای مشابه.

تهدیدات انسانی

رویدادها و اتفاقاتی که منشاء انسانی غیر عمدی دارند (اشتباهات و غفلتها) مانند عدم بکارگیری صحیح تجهیزات، عدم نصب صحیح نرم‌افزارها و برنامه‌های کاربردی، آلوده نمودن غیر عمدی شبکه به ویروس، دسترسی ناخواسته به اطلاعات محرمانه و... رویدادها و اتفاقاتی که منشاء انسانی عمدی دارند چه از داخل سازمان و چه از خارج از آن (سوء استفاده، نرم‌افزار مخرب، دسترسی غیرمجاز، کدهای مخرب، ویروس، بمبها، اخلال‌گری الکترونیکی، آتش‌سوزی عمدی، قطع برق عمدی و ...). بر طبق آمار، تهدیداتی که موجب وارد شدن بیشترین آسیب به منابع اطلاعاتی می‌شوند، دارای منشاء انسانی هستند.

تهدیدات محیطی

قطع طولانی مدت برق، آلودگی، مواد شیمیایی، نشت مایعات، آتش‌سوزی غیر عمدی، استهلاک تجهیزات و لوازم و...

۵.مدیریت وکنترل ریسک

بعد از اولویت بندی ریسک ها و شناسایی مهم ترین ریسک ها و آن هایی که نیاز به اقدام فوری دارند، باید برنامه کنترل و مدیریت ریسک را تهیه کرد. اینکه با هر ریسک چگونه باید رفتار کرد.

معمولاً روش های زیر را برای کنترل و مدیریت ریسک توصیه می کنند:

حذف ریسک:

در این روش از سازمان ها خواسته می شود که ریسک خود را حذف کنند. به عنوان مثال وقتی در فرآیند تولید خطری وجود دارد که می تواند به پرسنل من آسیب بزند، اگر بتوانم با بازمهندسی دستگاه، بگونه آن را بروز کنم که میزان بروز خطر صفر شود، توانسته ام ریسک را حذف کنم.

یا سازمانی که می خواهد وارد یک قرارداد پر ریسک شود و پس از بررسی متوجه می شود که کوچکترین اشتباه در این پروژه ریسک سنگینی دارد و در مقابل پروژه عواید مالی قابل توجهی هم ندارد، تصمیم می گیرد اصلاً وارد این پروژه و وارد این ریسک نشود. در این مواقع اصطلاحاً گفته می شود از ریسک اجتناب شده است.

کنترل ریسک یا کاهش احتمال وقوع:

اگر بتوانم اقدامی تعریف کنم که احتمال وقوع ریسک کم شود و یا پیامدهای بروز ریسک پایین بیاید توانسته ام ریسک ها کنترل کنم. به عنوان مثال در مذاکره با مشتری سعی می کنم جریمه تاخیر ارسال محصول را به عدد ناچیزی کاهش دهم یا برای دستگاهی که احتمال برق گرفتگی برای پرسنل سازمان با برق ولتاژ بالا را دارد، اقدامی تعریف می کنم که ولتاژ برق ناحیه خطر کم شود تا در صورت بروز خطر، پرسنل آسیبی نبینند.

به اشتراک گذاری ریسک:

وقتی سازمانی از بیمه آتش سوزی یا بیمه بار استفاده می کند، عملاً ریسک خودش را با شرکت بیمه ای به اشتراک گذاشته است و در صورت بروز اتفاق، شرکت بیمه می تواند پاسخ گو و کمک کننده شرکت باشد

دسته‌بندی ابزارهای کنترل از نظر توالی انجام کنترل

به طور کلی ابزارهای کنترلی را از نظر توالی و مؤثر بودن به ۶ گروه تقسیم می‌کنند:

کنترل‌های ایمنی محل کار

۱.حذف کردن(Elimination)

۲.جایگزینی(substitution)

۳.جداسازی(Isolation)

۴.کنترل مهندسی(Engineering control)

کنترل‌های ایمنی انسان

۵.کنترل اداری(Administive Control)

۶.تجهیزات ایمنی شخصی(Personal protective equipment)

۱.حذف خطر (Elimination) حذف کردن خطر یک راه حل ایده‌آل برای کنترل ریسک است. بنابراین در کنترل ریسک می بایست در رتبه اول تا جایی که ممکن است خطرات را حذف کرد. مثال‌هایی از حذف کردن خطر: تعمیر سقف سوله، پرکردن ناهمواری های کف سالن، حذف مواد پاک کننده شیمیایی مثل تینر

۲.جایگزینی :(Substantiation) **در صورتی که حذف خطر ممکن و میسر نباشد می‌بایست به دنبال کاهش وخامت آن به وسیله جایگزینی بود. تعیین فرآیند جایگزین بسیار مهم است چرا که فرآیند جدید ممکن است خطرات جدیدی را نیز در برداشته باشد. پس به یاد داشته باشیم فرآیندهای جدید نیز باید مشمول ارزیابی ریسک قرار گیرند. مثال: استفاده از تسمه نقاله ها و لیفتراک‌ها به جای حمل و نقل دستی، استفاده از پرینتر لیزری به جای پرینترهای سوزنی، جایگزینی موتورهای الکتریکی به جای موتورهای بنزینی و یا گازی در لیفتراک‌ها**

۳.جداسازی :(Isolation) **زمانی که حذف یا کاهش وخامت خطر تا حد ممکن انجام شد در صورت وجود خطر نوبت به جداسازی می‌رسد. جداسازی به منظور کاهش رخداد خطر انجام می‌گیرد.**

انواع جداسازی به شرح زیر است:

- **جداسازی (حصارکشی) کلی**(Total enclosure)
- **جداسازی جزئی**(Partial enclosure)
- **جداسازی افراد از خطر**
- **کاهش مواجهه با خطر**

جداسازی کلی: در این نوع جداسازی منبع خطر به طور کلی ایزوله می‌شود. مانند مکان‌های تابش اشعه‌های رادیواکتیو.

جداسازی جزئی: در این نوع جداسازی منبع خطر به طور کلی ایزوله می‌شود اما باز هم خطر مواجهه با آن وجود دارد. مثل حفاظ‌های تابلوی برق.

جداسازی افراد از خطر: تا حد ممکن افراد را از منبع خطر دور می‌کنند.

کاهش مواجهه با خطر: محدودیت‌هایی را در این زمینه وضع می‌کنند مانند عدم ورود افراد متفرقه به محل

۴.کنترل مهندسی (Engineering control): در این مرحله تعدیل و تصحیح ابزارآلات و ماشین‌ها و تسهیلات ایستگاه کاری مدنظر قرار می‌گیرد.
مثال: گذاشتن حفاظ کناری برای تسمه نقاله‌ها، تغییر دادن فرم دسته ابزار
۵.کنترل اداری (Administration control): این دسته از کنترل‌ها را می‌توان به سه گروه تقسیم کرد:
۱. آموزش و اطلاع دهی نسبت به خطرات
۲. سرپرستی، نظارت و راهنمایی
۳.استفاده از سیستم های ایمنی کار و مجاز بودن به کار (قوانین و مجوزهای کاری)

مثال: استفاده از گردش کاری مخصوصاً برای کارهای کسل‌آور، تعدیل شیفت‌های کاری

آموزش، نظارت و سرپرستی برای حصول اطمینان از اینکه کارکنان وظایف خود را با کیفیت مطلوب و بدون دردسر انجام داده‌اند لازم می‌باشد، دارا بودن دانش و توانایی کار برای آنها الزامی است.

سیستم‌های ایمنی کار روش‌های مستند شده‌ای برای استفاده مطمئن از تجهیزات، فرآیندها می‌باشند. مجوزهای کار برای کارهایی مانند جوشکاری اکسید استیلن و کار در فضاهای بسته، به دلیل کنترل کردن عملیات‌هایی که ذاتاً خطرناک هستند بکار می‌روند.

۶.تجهیزات ایمنی شخصی(Personal safety equipment)

حتی زمانی که یک خطر از بین رفته است، استفاده از تجهیزات ایمنی شخصی می‌تواند ضرورت داشته باشد برای اطمینان از اینکه خطر دوباره بوجود نیاید. تجهیزات ایمنی شخصی شامل:

- لباس کار: لباس کار باید در وضعیت مناسب با کار و اندازه مناسب برای پرسنل باشد.
- کفش ایمنی: استفاده از کفش‌های ایمنی با محافظ استیل توصیه می‌شود. همچنین در جاهایی که کف سالن مرطوب است از کفش‌های لاستیکی استفاده شود.

- کلاه ایمنی: قبل از ورود به محل در مواقعی که ایجاب می‌کند باید حتماً از کلاه ایمنی استفاده کرد. همیشه مطمئن باشید که کلاه ایمنی را به همراه دارید.
- گوشی ایمنی: از متداول‌ترین خطرات می‌توان سر و صدا را نام برد. برای جلوگیری از آسیب و یا از دست دادن شنوایی در مواقع لازم باید از آن استفاده کرد.
- دستکش ایمنی: دستکش‌های ایمنی چند لایه و استاندارد، پوست را از گزند مواد شیمیایی و همچنین از دیگر آسیب‌ها مانند کوفتگی، خراش، پاره‌گی و ... حفظ می‌کنند.
-

۶.نظارت

پس از شناسایی ریسک ها، ارزیابی آن ها و تدوین برنامه هایی برای کنترل و مدیریت ریسک، سازمان باید به سراغ اجرای فعالیت ها برود تا بتواند ریسک ها را مدیریت کند. شاید بتوان گفت قسمت مهم مدیریت ریسک اینجاست، چرا که تا زمانی که فعالیت ها انجام نشوند، عملاً هیچ کاری صورت نگرفته است.

۷.مدیریت ریسک درعمل

الف.ریسک های مالی

ریسک هایی هستند که به طور مستقیم بر سود آوری شرکت ها اثر می گذارند که تغییرات قیمت مالی می تواند با عث بروز این نوع ریسک میگردد.

.ریسک نرخ سود

نرخ سود و تغییرات آن در اقتصاد کنونی یکی از عوامل مهم ریسک مالی محسوب می شود.روش های علمی برای مدیریت ریسک نرخ سود، استراتژی های مصون سازی و تطابق دیرش را می توان نام برد.

.ریسک نکول

زمانی رخ می دهد که وام گیرنده به علت عدم توان یا تمایل ،به تعهدات خود در مقابل وام دهنده و در تاریخ سررسید عمل نمی کند. ریسک نرخ سودنرخ سود و تغییرات آن در اقتصاد کنونی یکی از عوامل مهم ریسک مالی محسوب می شود.

روش های علمی برای مدیریت ریسک نرخ سود، استراتژی های مصون سازی و تطابق دیرش را می توان نام برد.

.ریسک نقدینگی

ریسک نبود وجه نقد جهت بازپرداخت تعهدات است.

. ریسک سطح عمومی

قیمت هاوتورم اصولا باعث افزایش سطح عمومی قیمت هاشده،بهای تمام شده کلیه نهاده های یک شرکت را افزایش می دهد و در نهایت سطح عملکرد شرکت را متاثر می سازد. این ریسک به عنوان ریسک قدرت خرید نیز شناخته می شود.

ب.ریسک های غیرمالی

تصمیمات نادرست مدیران اجرائی شرکت ها و موسسات می تواند تبعات منفی برای یک سازمان به دنبال داشته باشد.

.ریسک سیاسی

تغییر قوانین و مقررات و احزاب و قانون مالیات تجارت بازرگانی و مواردی از این قبیل .

.ریسک صنعت

نوسانات بازدهی سرمایه گذاری که براثر اتفاقات یا وقایع خاص و تغییرات در یک صنعت خاص محتمل است.

- ✓ **چرخه عمر صنعت**
- ✓ **مسائل زیست محیطی**
- ✓ **مالیات محصولات یک صنعت**
- ✓ **...**

.ریسک قوانین و مقررات

این ریسک به علت تغییرات در قوانین مختلف در یک جامعه اقتصادی به وجود می آید.

- ✓ **لغو مجوز تولید یک محصول**
- ✓ **تغییر تعرفه واردات کالای خارجی**

.ریسک عملیاتی

ریسک عملیاتی عبارتست از زیان غیرمنتظره ناشی از خطاهای انسانی، تقلب، بروز اشکال در روشهای انجام کار، ضعف و فرسودگی فناوری و یا

عوامل بیرونی. اهمیت و نقش ریسک عملیاتی بیشتر در فعالیت بانکها پررنگ میشود چرا که استفادهٔ بانکها از سیستمهای شبکهای و نرمافزارهای مختلف به مراتب گسترده تر از سایر نهادهای مالی است و بروز هرگونه نقصی در این سیستمها (چه نیروی انسانی و چه فنآوری) موجب بروز

خسارتها و زیانهای هنگفتی میگردد.

هنگامیکه یک سازمان عملیات خود را به خوبی انجام ندهند.به طور کلی یا سیستم داخلی و روش های انجام کار به درستی تعریف نشده اند و یا بدرستی اجرا نمی شوند.

منابع ریسک های عملیاتی

ریسک فناوری اطلاعات: شامل اشکال در سیستم، ویروس اینترنتی، دادههای نادرست، خطوط ارتباطی ضعیف و... .

ریسک منابع انسانی: رویه های استخدام، گروهکاری غیر متخصص، سیاست تعطیلات کاری و ... .

ریسک صدمه به داراییها: ریسکی که طی آن داراییهای آسیب دیده موجب ایجاد وقفه در امر تجارت میشود. آسیب ممکن است ناشی از آتش سوزی، سیل یا زمین لرزه باشد.

ریسک روابط با مشتریان: تغییرات در مقررات، مطالبات، رضایت مشتری، دعاوی حقوقی و... . ریسکهای مذکور یا از سوی شرکت پذیرفته میشوند. یا شرکت از آنها اجتناب میکند.

.ریسک نیروی انسانی شرکت های با نیروی انسانی متبهر در صورت از دست دادن آنان با مشکل مواجه می شوند.

ج.ریسک اعتباری

نهاد های مالی پول هایی را که گرفته اند وام میدهند.ریسک اعتباری یعنی جریان نقدی که ما انتظار داریم در برابر وام هایی که داده ایم بدست آید،احتمال تحقق نیافتن پیدا کند.ممکن است وام گیرندگان موفق به بازپرداخت وام خود نشوند.

.ریسک خارج از ترازنامه

یک سری فعالیت ها و خدمات نهاد مالی در ترازنامه منعکس نمی شود و انواعی دارد،مثل وامی که بانک ها میدهند و وام تعهدی است، یعنی اگر رد دوره معینی فرد مراجعه کرد ،وام به او پرداخت شود؛بر خلاف وام فوری

یا وقتی بانک ها برای شرکت ها LC یا اعتبار اختصاص می دهند.مثلا شرکتی قصد دارد مواد اولیه خود را از شرکتی خارجی بگیرد و شرایطی برای شیوه پرداخت تعیین شود.بانک ایرانی عامل شرکت ایرانی و بانک خارجی عامل شرکت خارجی می شود.بانک ایرانی گشایش اعتبار می کند،یعنی تعهد می کند وقتی کالا رسید پول را به حساب خارجی بریزد .این گشایش اعتبار بانک را با ریسک مواجه می کند.چون بانک های عامل با هم طرف میشوند و معامله از طریق آن ها انجام می گیرد

.ریسک ارزخارجی وحاکمیت

ریسک ناشی از تغییر نرخ برابری ارز را ریسک نرخ ارز گویند.وقتی بانک ایرانی به بانک آمریکایی وام می دهد،با این خطر مواجه است که حاکمیت در آمریکا عوض شود،به این نوع ریسک ،ریسک کشوری یا حاکمیت گویند.

ارکان مدیریت ریسک

رکن اول:الزام کفایت سرمایه

لازم است مقدار حداقلی از سرمایه بانک برای پوشش زیان هایی که ازناحیه ریسک های اعتباری و عملیاتی و بازاردر جریان فعالیتهای کسب و

کا رایجاد می شود،کنار گذاشته شود تا بقای بانک و ادامه فعالیت آن تضمین شود.

رکن دوم:بازبینی نظارتی

این رکن جهت تضمین این است که بانک ها فرایند های دقیق را دنبال کنند،ریسک هایشان را از روشی قابل اتکا اندازه بگیرند و سرمایه کافی جهت محافظت از جامعه بانکداری بزرگتر در مقابل عوارض سیستماتیک ریسک هایی که متحمل می شوند نگه دارند.

رکن سوم:انظباط بازار

این رکن به عنوان اهرمی جهت تقویت و قابلیت اتکای سیستم بانکداری از طریق افشای بهتر وضعیت ریسک و سطوح سرمایه بانک عمل میکندبه گونه ای که صنعت و سرمایه گذار بهتر بتوانند سطح قدرت پرداخت دین یک بانک را تخمین زنند.