مدیریت ریسک پروژه های فناوری اطلاعات

یگانه مهام
(دانشجوی کارشناسی ارشد فناوری اطلاعات-دانشگاه الزهرا)
Y_maham@yahoo.com

کلید واژه ها: مدیریت ریسک- فناوری اطلاعات- سیستم های اطلاعاتی- چرخه عمر ایجاد و توسعه سیستم

چکیده

عصر نوین فناوری اطلاعات و سیستم های اطلاعاتی ، محیط اطرافمان را تبدیل به محیطی پر از چالش نموده است .در این حیطه، هر روزه شاهد ورود فناوریهای جدید هستیم ولذا با قابلیت ها و هم چالشهای جدیدی دست و پنجه نرم می کنیم.
فناوری اطلاعات وسیستم های اطلاعاتی در تمام بخشهای زندگی بشر ریشه دوانیده اند و اگرچه به تسهیل زندگی وارتباطات بشر کمک می کنند ،اما مانند هر تکنولوژی نوظهور دیگر با خود ، خطراتی را نیز به همراه می آورند .به عنوان مثال ، سازمانی که برای افزایش اثربخشی و کارایی خود در ارتباطات ، از شبکه های مخابراتی و اینترنت کمک می گیرد ، بایستی ریسک ناشی از دسترسی افراد غیر مجاز یا رقبا به اطلاعات سازمان را پذیرفته و یا آنرا مدیریت کند.
با توجه به نکات ذکر شده ، در تصمیم گیری برای پیاده سازی سیستم های اطلاعاتی و بهره گیری از مزایای فناوری اطلاعات ، مانند هر نوع تصمیم گیری دیگر در زندگی ، باید به بررسی خطرات احتمالی آن پرداخته و با مدیریت ریسکهای موجود ، اثربخشی سیستم را ارتقاء بخشید.
در این مقاله ، پس از معرفی مدیریت ریسک ، ابزارهای آن ، انواع ریسکها و روشهای ارتقاء و پیاده سازی سیستم های اطلاعاتی ، به معرفی نحوه به کارگیری فرایند مدیریت ریسک در فناوری اطلاعات و هر یک از مراحل پیاده سازی سیستم های اطلاعاتی به روش SDLC ،که یکی از جامع ترین و کاملترین روشهای ایجاد سیستم است ، پرداخته می شود .درنهایت هم ،اقدام به معرفی نقشهای کلیدی و برخی از عوامل موفقیت در فرایند مدیریت ریسک ، شده است.

مقدمه

امروزه سازمانها و سیستم های آنها در محیطی پر از چالش و تحول قرار گرفته اند لذا لازمه بقاء و ادامه زیست سازمان در چنین محیطی ، همگامی با تحولات محیط و پاسخ درست و به موقع به آنهاست.
پاسخگویی درست مستلزم تصمیم گیری درست است ، که همت همه جانبه مدیران و دست اندکاران هر برنامه و تصمیم را می طلبد. واضح است که در تمام شرایط تصمیم گیری ، کلیه جوانب کار و تصمیم، مشخص نیست و بنابراین، از جمله مواردی که در حین تصمیم گیری الزاما باید مورد توجه قرار گیرد؛ خطرات احتمالی و یا قطعی موجود است که می تواند بر نتایج تصمیم اخذ شده ، تاثیر گذارد و این همان حوزه مورد بحث در مدیریت ریسک است.
در دنیای دیجیتالی امروز و عصر ارتباطات، به کارگیری فناوریهای نوین مانند ITو سیستم های اطلاعاتی ، لازمه پاسخگویی مناسب به تحولات کنونی محیط است .چرا که فناوری اطلاعات ، به نحو فزاینده ای بر چگونگی عملکرد و نحوه کارایی سازمانها، اعم از خصوصی و دولتی ، تاثیر گذاشته است.
تصمیم گیری در حوزه پروژه ها و سیستم های مبتنی بر فناوری اطلاعات نیز عاری از احتمال و ریسک نیست و لذا بایستی قوانین و رویه های مدیریت ریسک در این حوزه نیز در نظر گرفته شود و تصمیمات مربوطه را پشتیبانی کند .در هر سازمانی که برای تحقق بخشیدن به ماموریت و رسالت خویش از سیستم های خودکار فن اوری اطلاعات استفاده می کند، مدیریت ریسک در حمایت از منابع اطلاعاتی سازمان نقشی حیاتی بازی می کند . در واقع فرایند مدیریت ریسک باید به عنوان جزئی از یک برنامه قوی امنیت اطلاعاتی سازمان در نظر گرفته شود چرا که برای پشتیبانی از سازمان و ماموریت آن در محیط پویای امروزی ، اعمال مدیریت ریسک ، امری بسیار ضروری است.

۱-مروری بر مفاهیم

از جمله مفاهیمی که در این مقاله به آنها پرداخته خواهد شد ، می توان به ریسک ، مدیریت ریسک و چرخه ایجاد سیستم اشاره نمود که در زیربه بررسی مفاهیم و تعاریف ارائه شده در کتب و منابع مختلف پرداخته می شود.

۱-۱ ریسک و انواع آن

۱-۱-۱تعریف ریسک

برای واژه ریسک در منابع مختلف ، تعاریفی گوناگون ارائه شده است، که البته همگی در بر گیرنده مفهومی واحد هستند .در زیر به برخی از این تعاریف اشاره می شود:

"ریسک عبارت است از انحراف در پیشامدهایی که می توانند در طول یک دوره مشخص ،در یک موقعیت معین اتفاق بیافتند ." [۱]

این تعریف به این معناست که ؛ چنانچه تنها یک پیشامد ممکن باشد ، انحراف و ریسک صفر است و به عبارت دیگر در این صورت احتمالی وجود ندارد و آینده کاملا قابل پیش بینی است.

در جایی دیگر ریسک به صورت زیر تعریف شده است:

ریسک عبارت است از هر چیزی که مانع از رسیدن سازمان به اهدافش باشد و یا توان سازمان را در این راه بکاهد که ممکن است به یکی از صور زیر باشد:

۱ رخداد یک فاجعه یا اتفاق بد
۲ عدم وقوع مسائل آنطور که مورد انتظار است.
۳ عدم وقوع اتفاقات و مسائل خوب[۴]

تعریف دیگری از ریسک به صورت زیر بیان شده است:

ریسک در معنای عام عبارت است از تاثیر منفی ناشی از یک آسیب پذیری با در نظر گرفتن "احتمال "وقوع و "اثر "آن در فرایندهای یک سیستم.

برای محاسبه "احتمال "یک رویداد ،(مثلا در یک سیستم فناوری اطلاعات) ، آسیب پذیری های موجود و بالقوه سیستم و کنترلهای اعمال شده در سیستم مورد تحلیل و ارزیابی قرار می گیرند .همچنین "اثر "، اشاره به میزان بزرگی خسارت و ضرروارده دارد که بسته به حساسیت ، دقت و اهمیت اجزاء سیستم و داده ها می باشد.[۲]

و در نهایت تعبیری کلی از ریسک اینگونه عنوان شده است:

" امکان وقوع یک خسارت و زیان اعم از مالی و غیر مالی در نتیجه انجام یک کار. " [۶]

۱-۱-۲انواع ریسک

سه نوع کلی از ریسک موجود در ایجاد و مدیریت یک سیستم عبارتند از:

ریسک ذاتی ، ریسک باقیمانده و ریسک قابل قبول.[۴]

ریسک ذاتی :سطحی از ریسک است که در پیاده سازی سیستم مورد نظر به صورت بالقوه وجود دارد و باید برای کاهش آن چاره ای اندیشید.

۱ ریسک باقیمانده :سطحی از ریسک است که علی رغم ایجاد عوامل کنترلی و سعی در کاهش ریسک هنوز وجود دارد .

۲ ریسک قابل قبول :سطحی از ریسک باقیمانده است که اگر چه وجود دارد، اما مانعی جدی بر سر راه رسیدن به اهداف و یا ماموریت های سازمان ایجاد نمی کند .

در طبقه بندی دیگری ریسک به سه سطح پائین، متوسط و بالا تقسیم شده است .[۶]

و در کتاب"مدیریت ریسک"، ریسک در دو نوع اصلی ارائه شده است :

۱ ریسک واقعی :ریسکی است که در آن احتمال زیان وجود دارد ولی احتمال سود وجود ندارد. مانند احتمال تصادف با اتومبیل. این نوع ریسک همیشه نا خوشایند است .

۲ ریسک سوداگرانه:در این نوع ریسک علاوه بر شانس خسارت (زیان)، شانس سود هم وجود دارد .مانند توسعه کارخانه .این نوع ریسک دارای جنبه هائی از جذابیت نیز هست. [۱]

در دسته بندی دیگر ریسک به سه نوع تقسیم می شود :

۱.ریسک کسب و کار :هزینه یا کاهش در آمد و سرمایه ایست که در اثرخرابی و ضعف عملیات معمول کسب و کار به وجود می آید .مثل از کار افتادگی یک دستگاه .

۲. ریسک سازمانی : خسارت مستقیم و یا غیر مستقیم ناشی از یک یا چند مورد زیر :

- ✓ فرایندهای داخلی ناقص و یا مردود
- ✓ افراد
- ✓ سیستمها
- ✓ وقایع خارجی

۳. ریسک فناوری اطلاعات :عبارت است از عدم وجود سیستم های خود کار ، شبکه یا منابع اصلی دیگر فناوری اطلاعات که روی فرآیندهای کسب و کار تاثیر منفی می گذارد. [۷]

۲-۱مدیریت ریسک

۱-۲-۱ تعریف مدیریت ریسک

برای مدیریت ریسک نیز مانند واژه ریسک ، تعاریفی ارائه شده است که البته همه در بر گیرنده مفهومی یکسان هستند و تمرکز روی فرایند مدیریت ریسک دارند و ما گذری بر مهمترین آنها خواهیم داشت :

مدیریت ریسک فر آیند شناسائی ریسک ، کاهش آن تا سطحی قابل قبول و در نهایت ارزیابی نتایج روی سیستم است .[۲]

ویلیامز و هینز،مدیریت ریسک را به صورت زیر تعریف می کنند:

مدیریت ریسک ، فرایند شناسائی ،ارزیابی و کنترل ریسکهای اتفاقی با لقوه ای است که مشخصا پیامدهای ممکن آن خسارت یا عدم تغییر در وضع موجود می باشد. مدیریت ریسک ، ریسکها را به وسیله کنترل آنها و تامین مالی خسارت هایی که به رغم تلاشهای کنترل خسارت ، اتفاق افتاده اند ،اداره می کند. [۱]

۲-۲-۱ اهداف مدیریت ریسک و اهمیت آن

مهمترین هدف مدیریت ریسک کمک به سازمان در مدیریت بهتر ریسک های مر بوط به ماموریتش است. و هدف مدیریت ریسک IT، مدیریت ریسکهای مربوط به ماموریتهای ITاست و این از طرق زیر امکان پذیر است:

۱) تامین امنیت بیشتر سیستم های ITکه وظیفه ذخیره، پردازش و انتقال اطلاعات سازمانی را به عهده دارند.

۲) کمک به مدیر در تصمیم گیریهای آگاهانه مربوط به ریسک و در نتیجه تعدیل مخارج که بخشی از بودجه مربوط به ITاست.

۳) کمک به مدیر در ارتقاء سیستم های IT به دلیل حمایتهای ناشی از عملیات مدیریت ریسک. [۲]

به طور کلی میتوان اهداف مدیریت ریسک را به صورت زیر برشمرد:

- بقاء سازمان
- صرفه جویی در هزینه ها
- حفظ سطح قابل قبولی از نگرانی و اضطراب
- ثبات عایدات (درآمدها) ؛ از طریق محدود نمودن کاهشهای پیش بینی نشده یا جریانات نقدی ناشی از خسارات.
- عدم توقف عملیات به دنبال وقوع یک خسارت
- رشد مداوم سازمان
- ایفای مسئولیت های اجتماعی[1] و محدود نمودن خسارت به خود سازمان. [۱]

۳-۲-۱فواید و اهمیت مدیریت ریسک

مدیریت ریسک به مدیران کمک می کند تا بتوانند هزینه های عملیاتی و اقتصادی خود را تعدیل کرده و آنها را در اتخاذ بهترین تصمیمات یاری می دهد.

یک شیوه مناسب مدیریت ریسک ، چنانچه به خوبی پیاده سازی شود ؛ می تواند به مدیران در شناسایی عوامل کنترلی مناسب کمک کند تا بتوانند امنیت لازم را در تحقق ماموریت سازمان پیاده کنند و در نتیجه می تواند بقای سازمان را تضمین کرده و سازمان را از خطر ریسکهای کوچک و بزرگ موجود مصون بدارد.

می توان به طور خلاصه فواید مدیریت ریسک را به شرح زیر برشمرد:

افزایش کارایی و اثربخشی، تسهیلات و روان سازی ، کاهش هزینه ، سرعت عمل و کاهش زمان انجام عملیات ،بهبود ارتباطات ،اطمینان از کنترل روی سیستم ، شناسایی تهدیدات مربوط به پروژه یا سیستم و کمک در تحقق به موقع اهداف.

۴-۲-۱ابزارهای مدیریت ریسک

یک مدیر برای اعمال مدیریت ریسک نیاز به ابزارها و روشهای خاصی دارد که از جمله این ابزارها و روشها می توان به موارد زیر اشاره کرد:

۱. اجتناب از ریسک: دور کردن ریسک با از میان برداشتن عامل و پیامدهای ریسک.
۲. محدود کردن ریسک: کاهش احتمال وقوع خسارت ، یا در صورتی که اتفاق افتاد جلوگیری از توسعه دامنه آن.
۳. انتقال ریسک: انتقال خسارات بالقوه به طرف دیگر(مانند شرکتهای بیمه یا شرکتهایی که در زمینه پذیرش ریسک فعالیت می نمایند).
۴. تقبل ریسک : نگهداری یا تحمل این خسارات توسط خود شرکت یا سازمان (خود بیمه گری) و ادامه عملیات سیستم ، با ریسک موجود یا سطح قابل قبول ریسک.
۵. برنامه ریزی ریسک: انجام مدیریت ریسک با استفاده از یک برنامه کاهش ریسک که در آن به اولویت بندی ، اجرا و حفاظت از عوامل کنترلی پرداخته می شود.
۶. تحقیق و شناسایی: کاهش دادن ریسک از طریق شناسایی نقاط آسیب پذیر و تحقیق در مورد کنترلهای موجود برای اصلاح نقاط آسیب پذیر.[۱،۲،۶،۷]

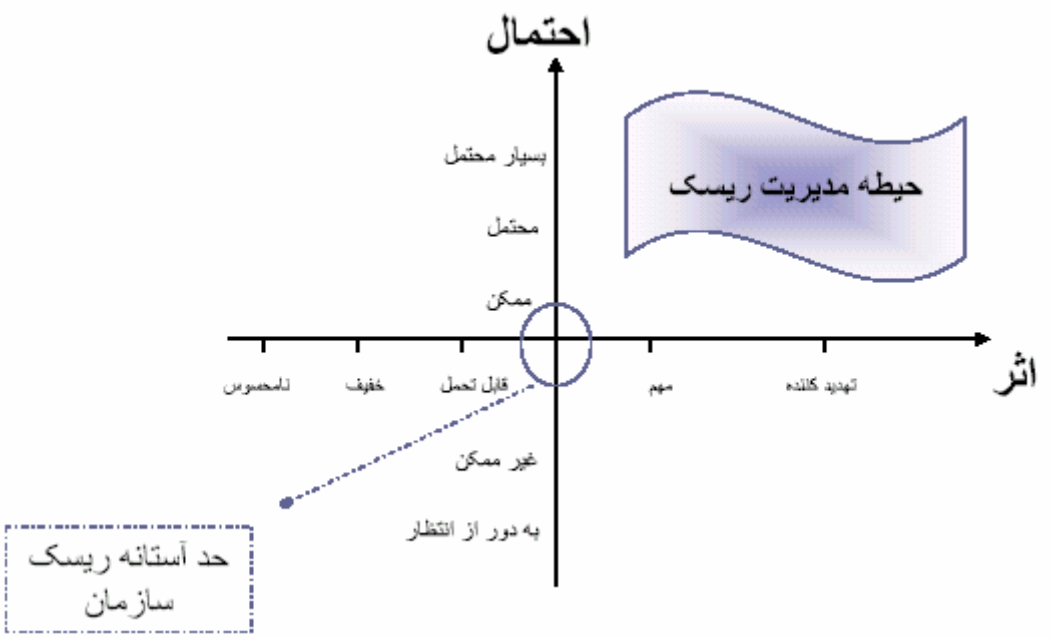
لازم به ذکر است که مدیر ریسک در انتخاب مناسب ترین ترکیب از ابزارها، باید هزینه ها و سایر جنبه های استفاده از هر ترکیب را، مورد توجه قرار دهد

---

[1] **Social responsibility**

۵-۲-۱ حیطه مدیریت ریسک

در فرایند شناسایی ریسک ، پس از تعیین اثر و احتمال ریسک ، بایستی آنها را روی یک طیف از بسیار بالا تا بسیار پایین طبقه بندی کرد . وسپس به اولویت بندی ریسکها پرداخت تا به مهم ترین آنها در اسرع وقت پاسخ گفته شود.
برای تصمیم گیری روی اولویت بندی ریسک های شناسایی شده ، بایستی مطابق شکل زیر ، با توجه به خصوصیات ، نوع عملیات و حساسیت منابع سازمان ، یک حد آستانه برای سطح ریسک سازمان تعریف کرده و برای سطوح بالاتر از آستانه ، اقدامات لازم صورت گیرد.



شکل ۱: حیطه مدیریت ریسک

۳-۱مدیریت ریسک درفناوری اطلاعات[۲]

با ظهور فناوریهای نوین اطلاعاتی و لزوم پاسخگوئی و همگامی سازمانها با این فناوری ، لزوم به کار گیری مدیریت ریسک و روشهای آن در ایجاد و نگهداری سیستم های مبتنی بر اطلاعات که با یکی از مهمترین منابع سازمان، یعنی اطلاعات ، سرو کار دارند نمایانتر شده است.
در واقع مدیریت ریسک فناوری اطلاعات به معنای شناسائی ، ارزیابی و کاهش ریسک های موجود در ایجاد و به کار گیری سیستم های اطلاعاتی تا سطح مورد قبول است .
برای ایجاد و توسعه سیستم های اطلاعاتی روشهای گو ناگونی وجود دارد که برخی از آنها عبارتنداز :

۱. چرخه عمر ایجاد و توسعه سیستم [۳]
۲. الگو سازی [۴]
۳. استفاده از بسته های نرم افزاری آماده
۴. توسعه سیستم تو سط کار بر [۵]

---

[۲] IT risk management
[۳] SDLC
[۴] prototyping

۵. خرید یا استفاده از تولید کنندگان بیرونی [۶].[۸]

در استفاده از هر یک از روشهای فوق بایستی انواع تکنیکهای مدیریت ریسک، بسته به روش استفاده در ایجاد سیستم مورد استفاده قرار گیرند و ریسکهای موجود شناسائی ، ارزیابی و مدیریت شوند. مثلا در مورد استفاده از تولید کنندگان خارجی و یا خرید سیستم اطلاعاتی ، باید ریسک در دسترس قرار گرفتن اطلاعات عملیاتی سازمان را در نظر داشته و آن را مدیریت کرد .

در این مقاله به بررسی مراحل پیاده سازی سیستم با استفاده از روش SDLC ، که یکی ار جامع ترین ، قدیمی ترین و پر کاربردترین روشهای ایجاد سیستم است ، پرداخته شده و چگونگی اعمال مدیریت ریسک، در هر یک از گامهای این روش مد نظر قرار می گیرد .

چرخه عمر ایجاد و توسعه سیستم(SDLC)[۷]

چرخه ایجاد یک سیستم مکانیزه به طور کلی شامل ۵ مرحله است:

شروع یا برنامه ریزی [۸]ایجاد و تهیه سیستم [۹]پیاده سازی سیستم [۱۰]عملیات و تعدیل [۱۱] حفاظت و واگذاری [۱۲].

در مرحله اول، نیاز به سیستم اطلاعاتی ، اهداف آن ،حوزه تحت پوشش سیستم مورد نظرو منابع و ابزار لازم مشخص و مستند می شود .

در مرحله دوم ، سیستم مورد نظر تحت مطالعات امکان سنجی قرار گرفته ودر نهایت طراحی ، برنامه ریزی،تولید یا خریداری می شود .

در مرحله سوم، سیستم پیاده سازی شده و ویژگیهای امنیتی سیستم ایجاد ، آزمایش و تصدیق می شوند. سپس مدل منطقی سیستم با مدل فیزیکی و ساختارهای فیزیکی سیستم، با در نظر گرفتن ویژگیهای امنیتی مطابقت داده می شود.

در مرحله چهارم، سیستم عملیاتی شده و شروع به انجام وظایف محوله خود می کند. در این مرحله سیستم به صورت مداوم از طریق افزودن یا کاستن سخت افزار و نرم افزار و یا تغییر در فرآیند ها ،رویه ها ، و سیاستهای سازمان،آموزش پرسنل و... مورد تعدیل و باز بینی قرار می گیرد .

در مرحله پنجم، اطلاعات ، سخت افزار و نرم افزارها در دسترس قرارداده می شوند و عملیات سیستم تحت نظارت مداوم قرار گرفته و خطاها و نیاز به بهبود شناسائی می شوند . در این مرحله ممکن است فعالیتهای چون جا به جائی ، حذف، دسته بندی یا تخریب اطلاعات صورت گیرد.[۲،۸،۹]

۳- مراحل مدیریت ریسک

همانطور که در تعریف مدیریت ریسک عنوان شد ، فر آیند مدیریت ریسک شامل سه گام شناسائی ریسک ، کاهش ، تا یک سطح قابل قبول و در نهایت ارزیابی آن است .

در پیاده سازی مدیریت ریسک، این گامها به صورت جزئی تری بررسی می شوند . در برخی از منابع در ۵ گام و در برخی دیگر در۶ گام این فر آیند را پیاده سازی می کنند .

به عنوان مثال یک فر آیند شش گامی در مدیریت ریسک به شرح زیر می باشند :

---

[۵] end user development
[۶] outsourcing
[7] system development life cycle
[۸] initiation
[۹] development or acquisition
[۱۰] implementation
[۱۱] operation or maintenance
[۱۲] disposal

۱) تشخیص و تعریف اهداف سازمان یا سیستم؛ مهمترین این اهداف بقاء سازمان ، در آمد با ثبات ، هزینه های کم در بلند مدت و آرامش خاطراست . که البته باید سطح معینی از هر یک از این اهداف را در نظر گرفت و بین آنها یک مصالحه منطقی ایجاد کرد.

۲) شناسائی ریسک های سازمان : این مرحله مشکل ترین وظیفه مدیریت ریسک است.

۳) ارزیابی ریسک؛ در این گام خسارات بالقوه در طول دوره برنامه ریزی شده مر تبط با این ریسکها ارزیابی می شوند این ارزیابی شامل تعیین :

الف) احتمال یا شانس وقوع خسارت

ب) اثری که این خسارتها بر روی وضعیت مالی سازمان خواهند داشت .و

ج) توانائی پیش بینی خساراتی که واقعا اتفاق خواهند افتاد،

می باشد.

در این مرحله اولویت بندی ریسکها مشخص شده و آنها که اقدام فوری تری می طلبند، مشخص می شوند .

۴)انتخاب یکی از ابزارهای مدیریت ریسک برای پاسخگوئی به ریسک های موجود .

۵) اجرای تصمیمات اتخاذ شده در خصوص انتخاب ابزار و نحوه پاسخگوئی به ریسک . مثلا در حالت انتقال ریسک ، باید منطقی ترین نرخ و انتخاب بیمه گر مد نظر قرار گیرد .

۶) ارزیابی مراحل گذشته و اینکه آیا ریسکها به درستی پاسخ داده شده اند یا خیر.[۱]

در جائی دیگر مراحل ۴ و ۵ از بالا در یک مرحله خلاصه شده اند . به عنوان مثال مراحل مدیریت ریسک یک سیستم IT به شرح زیر است :

۱) **تعیین اهداف IT**، به طوری که همسو با اهداف کسب و کار باشند.۷ هدف اصلی IT را که به قرار زیر است می توان در نظر گرفت :

- ✓ اثر بخشی [۱۳]
- ✓ کارایی[۱۴]
- ✓ قابلیت اطمینان [۱۵]
- ✓ انسجام[۱۶]
- ✓ در دسترس بودن [۱۷]
- ✓ برآورده کردن نیاز[۱۸]
- ✓ قابلیت اعتماد[۱۹]

۲) **شناسائی ریسک** [۲۰]:به مفهوم شناخت تمام چیزهایی است که روی توان رسیدن به اهداف بالا تاثیر می گذارد. مانند ریسک ناشی از افراد ، فر آیندها ، تکنولوژی، ریسکهای داخلی وخارجی و کلیه ریسک هایی که در بخش انواع ریسک اشاره شد.

از ریسک هایی که ممکن است روی اثر بخشی و کار ایی سیستم اثر بگذارد، می توان به مدیریت ضعیف ، نوع تکنولوژی و یا مهارت کار بران سیستم اشاره کرد .همچنین فقدان تدابیر امنیتی سیستم ،عدم آگاهی کار بران ، ویروسها و هکرها می توانند روی قابلیت اعتماد سیستم تاثیر گذارند.بعلاوه، از نقاط ضعف مر بوطه که میزان در دسترس بودن سیستم را تحت تاثیر قرار می دهند، می توان به طراحی ضعیف سیستم و شبکه ، خرابی سخت افزار ، خرابکاری عمدی در سیستم و عدم وجود نسخه پشتیبان از سیستم اشاره کرد.

از جمله ریسکهای مرتبط با تامین نیازها، می توان به عدم آگاهی از قوانین و اصول استفاده ویا نظارت ناکافی اشاره کرد.

---

[۱۳] effectiveness
[۱۴] efficiency
[۱۵] confidentiality
[۱۶] integrity
[۱۷] availability
[۱۸] compliance
[۱۹] reliability
[۲۰] risk identification

طراحی ضعیف ورودی و خروجی سیستم، دسترسی های غیر مجاز، وجود هکرها و... نیز از جمله خطرات و خسارتهای احتمالی است ، که منجر به عدم اطمیتان و انسجام سیستم می شود.

۳- ارزیابی ریسک [۲۱]: در این مرحله بایستی احتمال و اثر هر رخداد را روی اهداف سیستم اطلاعاتی مورد نظر، تعیین کرده، و این اثرات را در هر دو سطح ریسکهای ذاتی و ریسکهای باقیمانده مدیریت کرد ،تا بتوان اقدامات لازم را برای رساندن ریسک موجود به سطح قابل قبول انجام داد.

برای بررسی اثرات ممکن روی سیستم، بایستی اثرات مالی ،اثر روی اعتبار سازمان (به دلیل سیستم های ناامن)و عملیات کسب و کار ، تخریب دارائیهای با ارزش مثل داده ها و تاخیر در تصمیم گیری را در نظر گرفت .و برای مطالعه احتمال رخداد هر واقعه، باید به بررسی صنعت حاکم بر سازمان ، ساختار و فرهنگ سازمانی، نوع سیستم و کنترلهای موجود پرداخت .

۴ـ پاسخگوئی به ریسک [۲۲]

چنانچه ریسک باقیمانده هنوز بیش تر از سطح قابل قبول ریسک است ؛ مجددا باید اقداماتی برای کاهش ریسک صورت گیرد .

۵- نظارت[۲۳] :شامل بررسی کلیه مراحل بالاست .[۴]

۱-۳ شناسائی ریسک

اگر چه تمام مراحل مدیریت ریسک مهم هستند؛ اما از آنجایی که مرحله شناسایی ریسک ، مبنایی برای اتخاذ سیاستهای مدیریت ریسک و انتخاب تکنیکهای اقتصادی، ایجاد می کنداز اهمیت ویژه ای برخوردار است.

از آنجاییکه ریسک ها و تهدیدات در طول زمان تغییر می کنند، سازمانها بایستی هر چند وقت یکبار ، به شناسایی ریسک پرداخته ، و مؤثر بودن سیاستها و کنترل های اخذ شده را تایید نمایند.

شناسایی مطمئن ریسکهای امنیت اطلاعات، از شناسایی دیگر انواع ریسکها مشکل تر است، چرا که اطلاعات در مورد احتمال و هزینه عوامل ریسک فناوری اطلاعات بسیار محدود است و همچنین عوامل ریسک بطور مداوم تغییر می کنند. بعلاوه شاهدیم که هر روزه فناوری نوینی وارد عرصه بازار می شود،که این خود منجر به ایجاد منبع جدیدی از تهدید می شود.

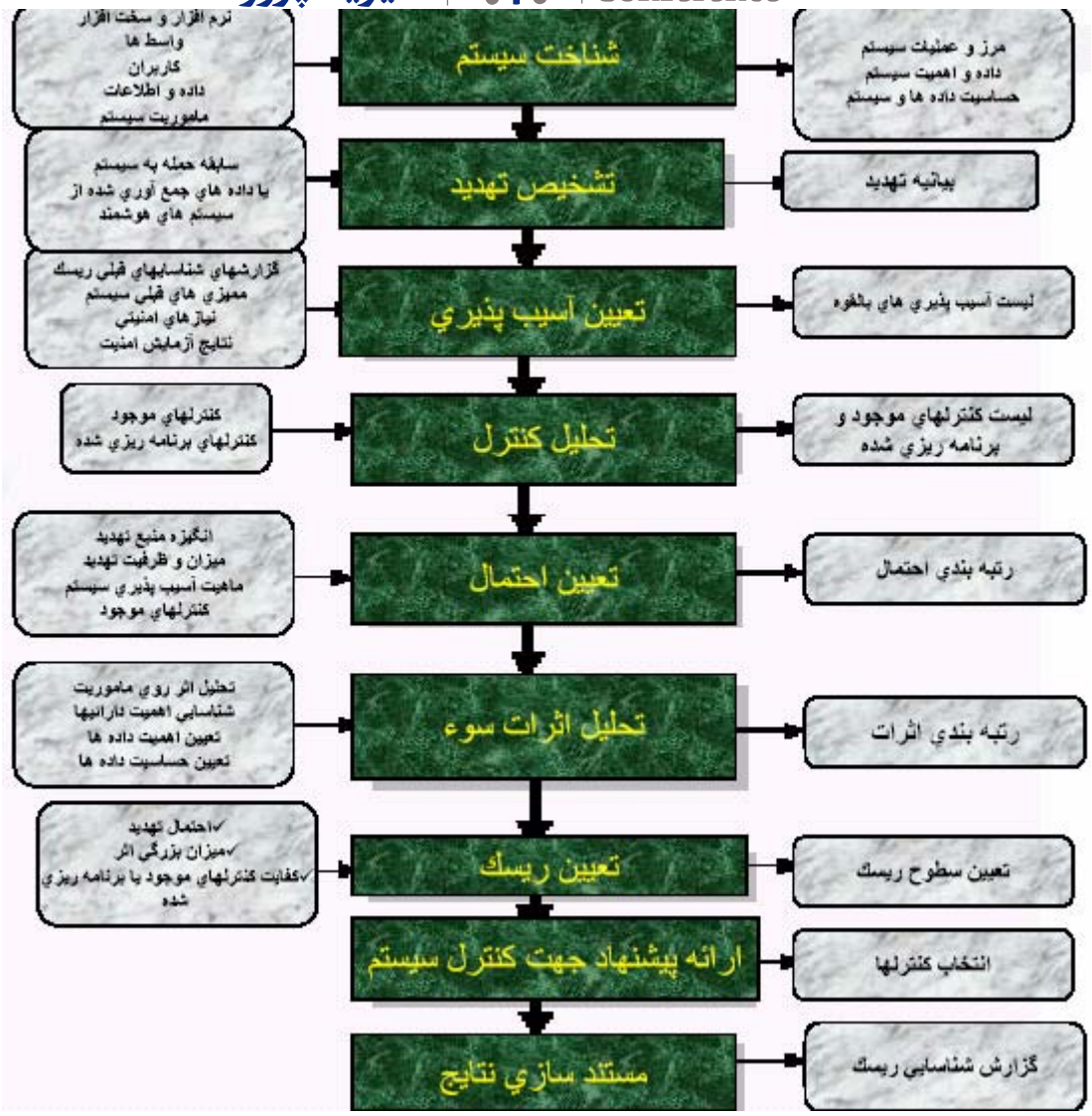
به طور کلی می توان گفت که مرحله شناسائی ریسک اولین گام در متدولوژی مدیریت ریسک است . در این گام میزان و حدود تهدیداتی که یک سیستم IT در سراسر چرخه عمرش (SDLC) با آن ممکن است مواجه شود ، تعیین می شود و خروجی این مرحله به مدیر کمک می کند تا بتواند عوامل کنترلی را برای کاهش یا حذف ریسک، در مرحله بعدی انتخاب کند.

متدولوژی شناسائی

ریسک طی ۹ گام اساسی که در شکل زیر نشان داده شده است ، فرموله می شود :

---

[۲۱] risk assessment
[۲۲] risk response
[۲۳] monitoring



شکل ۲: فرایند شناسایی ریسک

گامهای۲،۳ ،۴ و۶ می توانند به طور موازی بعد از گام ۱ انجام شوند.[۲]

همانطور که در شکل مشخص است در مرحله اول برای تعیین ویژگیهای سیستم بایستی ابتدا حوزه کار سیستم و مرز آن را مشخص کرد، سپس عملیات ، داده های ورودی، اهمیت و میزان حساسیت آنها و خود سیستم باید مشخص شوند، که برای این کار نیاز به اطلاعاتی در مورد سخت افزار، نرم افزار ، تعاملات سیستم(داخلی و خارجی)، داده ها و اطلاعات مورد نیاز سیستم ، کاربران و پشتیبانان سیستم IT ، ماموریت سیستم ، سیاستهای امنیتی حاکم بر سیستم IT ، معماری امنیتی سیستم ، توپولوژی فعلی شبکه ، پایگاه داده ، جریان اطلاعات ، کنترل های فنی به کار رفته در سیستم ، کنترل های مدیریتی و عملیاتی ، سیاستهای امنیتی محیطی و ... داریم.

برای جمع آوری این اطلاعات ، روشهای گوناگونی وجود دارد؛ مثلا می توان از پرسشنامه ها یا مصاحبه های حضوری ، مطالعه اسناد موجود سیستم و یا از ابزارهای فناوری اطلاعات ،کمک گرفت. بنابراین در اینجا کاملا مشخص است که مدیریت ریسک و فناوری اطلاعات می توانند یک تاثیر متقابل و دو جانبه داشته باشند.

در گام دوم بایستی به شناسایی تهدیدات موجود و منابع آنها پرداخت. البته بایستی توجه داشت که یک منبع تهدید ، تا زمانی که در سیستم نقطه ضعف و آسیب پذیری وجود نداشته باشد، نمی تواند تهدیدی برای سیستم ایجاد کند.

به طور کلی سه منبع اصلی تهدید وجود دارد:

- تهدیدات طبیعی مانند : سیل، زلزله، بهمن و غیره
- تهدیدات انسانی که ممکن است عمدی و یا غیر عمدی باشند.

- تهدیدات محیطی مثل آلودگی ، گرمای بیش از حد یا تغییرات محیط حقوقی ، اقتصادی و غیره.

در گام سوم ، با استفاده از اطلاعاتی از قبیل گزارشهای قبلی شناسایی ریسک، نیازمندیهای امنیتی ، نتیجه آزمایش امنیت سیستم و ... به شناسایی نقاط آسیب پذیر سیستم پرداخته می شود.

لازم به ذکر است که، نوع آسیب پذیری و شیوه شناسایی آن، بسته به طبیعت سیستم IT و مرحله ای از چرخه عمر که در آن به سر می برد ، متفاوت است. مثلا چنانچه سیستم IT هنوز طراحی نشده است، جستجو برای شناسایی نقاط آسیب پذیر باید روی سیاستهای امنیتی سازمان ، رویه های امنیتی تولید کننده سیستم، و... متمرکز باشد.اما در یک سیستم IT که در حال پیاده سازی است ، باید به ویژگیهای امنیتی برنامه ریزی شده ، توجه نمود و در سیستمی که در حال انجام عملیات است ، باید به ویژگیها و کنترل های امنیتی فنی و رویه ای سیستم پرداخت.

در این مرحله پرسنل شناسایی ریسک ، برای تعیین اینکه آیا نیازهای امنیتی که در مرحله شناسایی سیستم مشخص شده اند، با کنترل های امنیتی موجود پاسخ داده می شوند یا خیر، اقدام به تهیه چک لیست نیازهای امنیتی می کنند.

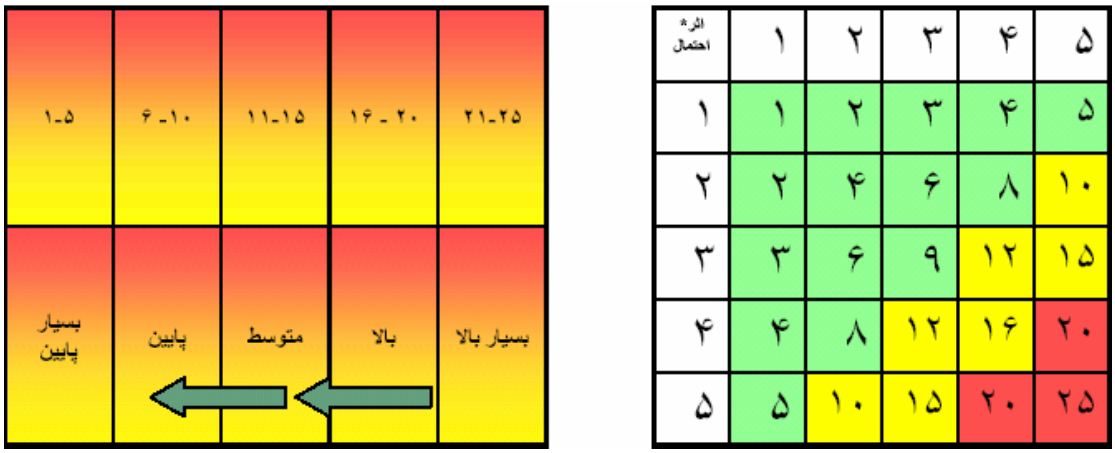
در گام چهارم ، هدف تحلیل کنترل های اعمال شده و برنامه ریزی شده در سیستم است و اینکه آیا به کاهش سطح ریسک کمک می کنند یا خیر.

در گام پنجم، با مطالعه و تحلیل توان منبع تهدید در ایجاد ریسک ، ماهیت آسیب پذیری سیستم ، کنترل های موجود و اثر بخشی آنها ، به تعیین احتمال وقوع ریسک پرداخته می شود و سپس احتمال مذکور در سطوح مختلف از کم تا زیاد رتبه بندی می شود.

در گام ششم؛ با در نظر داشتن ماموریت سیستم ، میزان حساسیت و اهمیت داده ها و دارائیهای سیستم ، اثرسوء تهدیدات روی انسجام سیستم ، در دسترس بودن و قابلیت اعتماد سیستم IT ، که از مهمترین اهداف سیستم هستند، سنجیده می شود.

این اثرات ممکن است به صورت محسوس یا نامحسوس باشند. اثرات محسوس از طریق محاسبه کاهش درآمد یا میزان هزینه لازم برای تعمیر سیستم و... قابل محاسبه هستند.ولی اثرات نامحسوس قابل اندازه گیری بر مبنای معیاری خاص، نیستند . اما می توان آنها را تحت اصطلاحات اثر زیاد، متوسط و کم روی یک طیف، طبقه بندی کرد.

در گام هفتم ، با استفاده از اطلاعات به دست آمده از تعیین احتمال ، میزان اثرات سوء تهدید و میزان کنترلهای موجود و برنامه ریزی شده ، سطح ریسک تعیین می شود. برای اندازه گیری ریسک ، مقیاس و ماتریس سطح ریسک باید ایجاد شوند. که در شکل زیر نشان داده شده است:



اثر \ احتمال	۱	۲	۳	۴	۵
۱	۱	۲	۳	۴	۵
۲	۲	۴	۶	۸	۱۰
۳	۳	۶	۹	۱۲	۱۵
۴	۴	۸	۱۲	۱۶	۲۰
۵	۵	۱۰	۱۵	۲۰	۲۵

شکل۳: ماتریس سطح و مقیاس ریسک

همانطور که در شکل مشخص است ، ماتریس سطح ریسک از طریق ضرب نرخهای احتمال تهدید و اثرات تهدید به دست می آیند. مقیاس ریسک نیز می تواند در سطوح مختلفی از بسیاربالا تا بسیارپایین دسته بندی شود.

در گام هشتم، با توجه به مراحل بالا کنترل های لازم توسط مدیر ریسک پیشنهاد می شود. این کنترل ها با در نظر گرفتن فاکتورهای اثر بخشی ، قوانین و سیاستهای سازمانی ، تاثیرات عملیاتی ، امنیت و قابلیت اعتماد ، انتخاب می شوند.

و در نهایت در گام آخر نتایج به دست آمده از مراحل بالا مستند سازی می شوند.[۲]

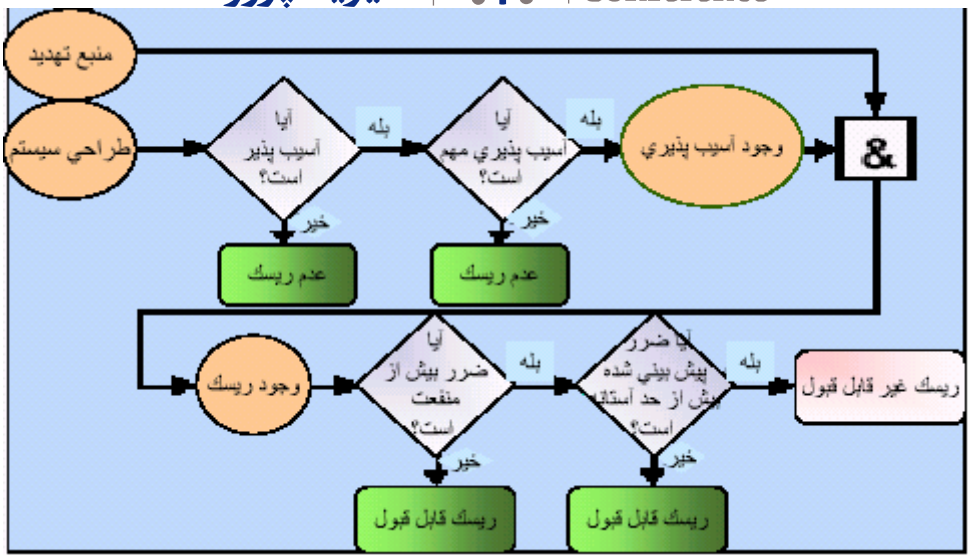
متدولوژی بالا ، یکی از جامع ترین و کاملترین متدولوژی های موجود در زمینه شناسایی ریسک در سیستم های مربوط به فناوری اطلاعات است که تقریبا در تمام سیستم های اطلاعاتی کاربرد دارد. مرحله شناسایی ریسک مهمترین و حیاتی ترین مرحله در مدیریت ریسک است و لذا هر سازمانی به این بخش از برنامه مدیریت ریسک توجه خاصی دارد و گاها فرایندهای خاصی را، با توجه به نوع فعالیت سازمان، برای شناسایی ریسک های موجود در سازمان، پیاده سازی می کنند.

در نهایت می توان موفقیت یک فرایند شناسایی ریسک را مستقیما وابسته به عوامل زیر دانست:

۱. انجام فرآیند مبتنی بر دانش و استفاده از سطح مناسبی از افراد متخصص و آگاه
۲. کنترل مرکزی و منظم به همراه رویه های از قبل تعریف شده، که موجب می شود از صحت ، دقت و کامل بودن فرایند شناسایی ریسک مطمئن شویم .
۳. پی گیری و ایجاد یک فرایند منسجم و کامل؛ از انتخاب و اجرای کنترل های لازم تا سنجش نتایج، که به انتخاب کنترلهای اعمال شده اعتبار می بخشد.
۴. تعیین مسئولیت فعالیتها: در شرکتهای بزرگ و متوسط ، مدیر امنیت اطلاعات است که مسئولیت شناسایی ریسکها و نتایج آن را می پذیرد .و مدیر ارشد مسئول تصمیمات اخذ شده در زمینه کاهش ریسک می باشد. اما در سازمانهای کوچک ، مدیر ارشد سازمان مسئولیت تمام این مراحل را می پذیرد. در اینجا لازم به ذکر است که، به طور کلی تمام سطوح سازمان با ریسک و مدیریت آن مواجه هستند، چرا که مدیریت ریسک مبتنی بر ارتباطات است. اما مسئولیت نهایی به عهده یک نفر است.
۵. مستند سازی : مستند سازی نتایج فرایند شناسایی ریسک ، باعث اطمینان از تکامل ، هماهنگی و مسئولیت پذیری در فرایند می شود . این کار می تواند نقطه شروعی برای دیگر فعالیتهای مدیریت ریسک باشد.
۶. ارتقاء دانش سازمانی :فرایند شناسایی ریسک ، دانش مدیر را در مورد سازمان خود ارتقاء می دهد و این دانش موجب می شود مدیر بتواند به سرعت به تغییرات محیطی پاسخ گفته و روی مراحل جمع آوری ، پردازش و تسهیم اطلاعات در سازمان تسلط کافی داشته باشد.
۷. به روز کردن منظم :با توجه به پیشرفت روزافزون در فناوریهای اطلاعاتی و تغییرات مداوم محیطی، سطوح ریسکی که سازمان با آنها مواجه است نیز دائما در حال تغییر است، لذا مرحله شناسایی ریسک باید به طور مداوم به روز شود و تهدیدات جدید شناسایی شده و برای کاهش آنها اقدامات لازم صورت گیرد.[۱۰]

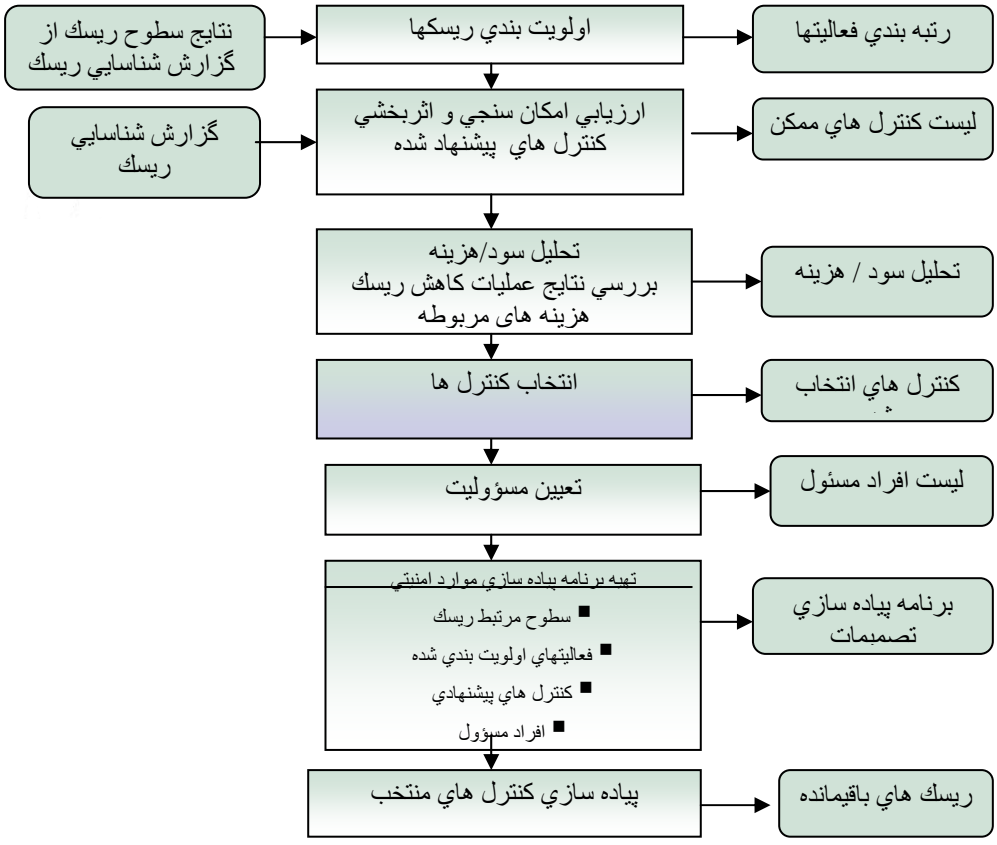
۲-۳ کاهش ریسک:

این مرحله از فرایند مدیریت ریسک ، شامل اولویت بندی ، ارزیابی و اجرای کنترلهای مناسب برای کاهش ریسک است.
حذف کامل ریسک معمولا غیر عملی و غیر ممکن است و لذا مدیر ریسک بایستی بهترین و کم هزینه ترین ابزار کنترل ریسک و یا ترکیبی از این ابزارها را که قبلا عنوان شد، به کار بگیرد تا اثرات سوء احتمالی سیستم را کاهش دهد. البته در انتخاب هر یک از این ابزارها، بایستی اهداف و ماموریت سازمان را در نظر داشت و از آنجا که پاسخگویی به تمام ریسکهای موجود و کاهش آنها ممکن است عملی نباشد ، لذابایستی اقدام به اولویت بندی ریسکهای موجود کرده و به مهمترین تهدیدات در اولین فرصت پاسخ گفت.
حال باید پرسید که مدیر تحت چه شرایطی و چه زمانی باید اقدام به استفاده از عوامل کنترلی شناخته شده و ابزارهای مدیریت ریسک کند؟ به این سوال با استفاده از نمودار زیر پاسخ می گوییم:



شکل۵: بررسی لزوم اقدام به کاهش ریسک

به طور خلاصه در اقدام برای کاهش ریسک ، بایستی ۷ مرحله زیر را که در شکل زیر نشان داده شده است طی نمود :



شکل ۶: مراحل کاهش ریسک

همانطور که در شکل می بینیم ؛ در گام اول با توجه به نتایج مرحله شناسایی ریسک که در آن سطوح ریسک مشخص شـده ، به اولویت بندی ریسکها و سپس اقدامات لازمه پرداخته می شود .

در مرحله دوم مجددا با توجه به نتایج مرحله شناسایی ریسک و با انجام مطالعات امکان سنجی و اثربخشی هر یک از ابزارهای مدیریت ریسک، به انتخاب ابزارهای ممکن پرداخته می شود .در مرحله بعدی ، تحلیل سود و هزینه اثرات سوء احتمالی ریسکها و هزینه های مربوطه صورت می گیرد.

در گام چهارم، با استفاده از نتایج به دست آمده از مراحل قبل کنترلها و ابزارهای لازم انتخاب می شوند. و در مرحله پنجم؛ تخصیص کارها صورت گرفته و مسئولیتهای افراد درگیر در پروژه مشخص می شود. سپس در مرحله ششم؛ برنامه ریزی پروژه صورت می گیرد و زمان شروع مشخص می شود وبرنامه ای مطمئن برای عملیات شکل می گیرد.

در مرحله آخر ؛ مدیریت ریسک اعمال شده و اقدام به کاهش ریسک می شود و در نهایت سطوح قابل قبول از ریسک باقی می ماند.

۳-۳ ارزیابی و نظارت

از آنجایی که روز به روز بر تکنولوژیهای اطلاعاتی افزوده می شود و لازم است که سازمانها برای بقای خود ، با تغییرات تکنولوژیکی و فرهنگی ناشی از فناوریهای جدید همراه شوند لذا لازم است که ساختار شبکه و اجزاء آن ، کاربران و پرسنل سازمان، سخت افزارها و نرم افزارها و دیگر اجزاء فناوری اطلاعات در طول زمان مطابق با تحولات محیطی تغییر کنند. و این خود موجب بروز ریسک ها و چالشهای جدیدی خواهد شد. لذا لازم است که فرآیند ریسک هم مداوم، همراه با تغییرات محیطی ، تکرار شده و به شناسایی ، کاهش و ارزیابی ریسک های به وجود آمده، بپردازد.

۴- مدیریت ریسک و چرخه ایجاد سیستم

در هر یک از مراحل ایجاد و توسعه یک سیستم، ریسک ها و خطراتی احتمالی نهفته است که برای بهبود سیستم و پیاده سازی بهینه سیستم لازم است که به شناسایی این خطرات و نقاط ضعف پرداخته و برای کاهش آنها اقدامات لازم صورت بگیرد.

در جدول زیر، هر یک از مراحل چرخه ایجاد سیستم (SDLC)، و اقدامات لازم برای پیاده سازی مدیریت ریسک در هر مرحله خلاصه شده است:[۲]

جدول ۱: مدیریت ریسک و SDLC

مراحل SDLC	ویژگیهای مرحله	فعالیتهای مدیریت ریسک
مرحله ۱: شروع یا برنامه ریزی	نیاز به سیستم IT و حوزه مربوطه مشخص می شود	در مرحله تعیین نیاز، ریسکهای شناسایی شده سیستم، نیازهای امنیتی و یک استراتژی امنیت برای سیستم، در نظر گرفته می شوند
مرحله ۲ : ایجاد وتهیه سیستم	سیستم IT طراحی، خریداری، برنامه ریزی، ایجاد ویا ساخته می شود	ریسکهای شناسایی شده در این مرحله به تحلیل مسائل امنیتی سیستم IT و در نتیجه تکمیل معماری و طراحی سیستم کمک می کند
مرحله ۳ : پیاده سازی سیستم	با در نظر داشتن ویژگیهای امنیتی، سیستم پیاده سازی می شود.	کمک به شناسایی نیازمندیهای پیاده سازی سیستم با در نظر داشتن محیط سیستم و اتخاذ تصمیماتی برای رفع ریسکهای شناسایی شده قبل از عملیاتی شدن سیستم
مرحله ٤: عملیات و تعدیل	سیستم عملیات خود را شروع کرده و به صورت مستمر از طریق اضافه یا کم کردن سخت افزار و نرم افزار یا تغییر در فرایند مورد تعدیل قرار می گیرد.	انجام فعالیتهای مدیریت ریسک برای ارتقاء دوره ای سیستم یا در هر زمانی که تغییرات مهمی در محیط عملیاتی و تولیدی سیستم IT به وقوع می پیوندد.مثل واسطهای جدید برای سیستم.
مرحله ٥ :حفاظت و واگذاری	این مرحله در بر گیرنده تغییر در آرایش اطلاعات، سخت افزار، نرم افزار و یا فعالیتهایی از قبیل حذف یا جابه جایی اطلاعات ویا نحوه قرار گیری اصولی سخت افزارها و نرم افزارهاست	فعالیتهای مدیریت ریسک برای اجزائی از سیستم که با بخشهای دیگرجایگزین می شوند، برای اطمینان از جایگزینی به جای سخت افزار و نرم افزار، و اطمینان از اینکه داده های باقیمانده به درستی کنترل می شوند و جابه جایی سیستم به شکلی مطمئن صورت می گیرد، انجام می شود.

۵- نقشهای کلیدی و عوامل موفقیت در فرایند مدیریت ریسک

از جمله کسانی که نقش فعال در پیاده سازی مدیریت ریسک در سیستم های فناوری اطلاعات دارند، می توان به افراد زیر اشاره کرد:

مدیر ارشد سازمان، مدیر ارشد اطلاعاتی[۲۴]،صاحبان و مسئولان سیستم و اطلاعات آن، مدیران عملیاتی،مدیر امنیت اطلاعات و تعلیم دهندگان مسائل امنیتی سیستم. [۲]

بعلاوه از دیگر فاکتورهایی که در فرآیند مدیریت ریسک بایستی مد نظر قرار گیرند ، عبارتند از:

مشتریان، کاربران، ،تیم پروژه،پروژه های مرتبط و تامین کنندگان.

همانطور که مشخص است فرایند مدیریت ریسک ، فرایندی مبتنی بر ارتباطات بین فاکتورهای عنوان شده در بالا می باشد و لذا فناوری اطلاعات به عنوان یک عامل کلیدی در این فرایند می باشد .خواه مدیریت ریسک روی پروژه های مبتنی بر IT باشد یا نباشد.

عوامل موفقیت مدیریت ریسک

یک برنامه موفق در مدیریت ریسک فناوری اطلاعات بستگی به عوامل زیر دارد:

- تعهد مدیر ارشد در خصوص زمان و منابع
- پشتیبانی و همکاری همه جانبه گروه
- صلاحیت تیم مدیریت ریسک IT
- آگاهی و مشارکت کاربران سیستم
- ارزیابی مستمر و شناسایی مداوم ریسکهای مربوط به ماموریت فناوری اطلاعات. [۲۶]

[24] chief information officer(CIO)

۶- نتیجه گیری

در این مقاله به معرفی انواع ریسک و نحوه مدیریت آنها در سیستم های مختلف و من جمله سیستم های اطلاعاتی پرداخته شد و مراحل شناسایی ، کاهش و ارزیابی به تفصیل بحث شد. اما همانگونه که قبلا نیز عنوان شد، زمانی که از فناوری اطلاعات صحبت به میان می آید، باید بدانیم که در حیطه ای قدم گذاشته ایم که بسیار پویا و حساس می باشد ، چراکه با مهمترین منابع سازمان یعنی اطلاعات سرو کار داریم .بعلاوه، مرتبا با یک فناوری جدید ، با ویژگیها ، مزایا و چالشهای جدیدی روبه رو می شویم که الزاما نمی توان از آن اجتناب کرد. لذا در چنین محیطی ، فرایند مدیریت ریسک مانند یک سیکل باید مرتبا تکرار شود تا بتواند برای مدیران سازمان ، بهره گیری از تکنولوژیهای جدید را با اطمینان خاطر توام نماید. ولی لازم است توجه شود که هر سازمانی بسته به نوع فعالیت و میزان حساسیت دارائیهای خود ، با سطوح متفاوتی از ریسک مواجه است که بایستی فرایند مدیریت ریسک برای آن پیاده سازی شود.

منابع:

۱. سی آرتور ویلیامز،جی آر-ریچاردام هینز، مدیریت ریسک، مترجمان: داور ونوس،ججت اله گودرزی، نشر نگاه دانش،۱۳۸۲ .

2. Gary Stoneburner, Alice Goguen, and Alexis Feringa, 'Risk Management Guide for Information Technology Systems', National Institute of Standards and Technology, July, 2002.
http://www.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

3.'Information Security Risk Assessment Practices of Leading Organizations', United States general accounting office (GAO), November, 1999.
http://www.gao.gov/cgi-bin/getrpt?GAO/AIMD-00-33

4.'IT Risk Management', prince water house coopers, 2005
http://www.swpark.or.th/itsec2003

5. Michael S. Gibson, ' The Implications of Risk Management Information Systems for the Organization of Financial Firms', 1997.
http://ideas.repec.org/p/fip/fedgif/632.html

۶. محمدی نوده، عبدارحمن، نقش فناوری اطلاعات در مدیریت ریسک، آی تی ایران، اردیبهشت ۱۳۸۴ .
http://www.donya-e-eqtesad.com/84-02-08/090208.htm

7. Julean Self, 'Risk Management Guide', office of information technology service (ITS), April, 2004.
http://www.treasury.act.gov.au

8. Kenneth c. Laudon ,Jane price Laudon , ' Management Information Systems: organizational and technology in the networked enterprise'.

9. Cattezene Ricardo, ' Data base systems: principles, design & implimentation'.

10. ' Information Security ',IT examination handbook, Federal Financial Institutions Examination Council(FFIEC), December,2002.