



عنوان پایان نامه :

نقش مدیریت ریسک در پروژه های IT

ارائه شده به:

جناب آقای مهندس رامین مشایخی

گردآورنده:

عبیدالله دهانی

دانشجوی کارشناسی IT دانشگاه بین المللی چابهار

تابستان 1390

پیشگفتار

شدت و سرعت پیشرفت تکنولوژی در دهه های اخیر شگفت آور بوده است. این پیشرفت ها شکل دنیای ما را تغییر داده . و عملاً همه ی جنبه های زندگی را تحت تاثیر قرار داده اند. به نظر نمی رسد که سرعت کنونی تغییرات , به این زودی ها کم شود. تکنولوژی از دیدگاه , IT کاتالیزستی است که در همه ی زمینه های تولیدی ثروت به بار می آورد که از تولید محصولات فنی گرفته تا خدمات فناوری و اطلاعات روز دنیا همچون حمل و نقل , تجارت مجازی و حتی زمینه ی خرده فروشی ها را محیا می کند .

به عنوان محقق IT شاهد بوده ام که این ارتقا بارها اتفاق افتاده است هدف ما بر این بوده که پروژه ای بنویسیم که دانشجویان دیگر رشته ها را با رشته IT هر بیشتر آشنا سازد .

بنده در این مقاله به لزوم تدوین قانون مناسب و بررسی قوانین مشابه مدیریت ریسک پرداخته و در نهایت قانون فناوری اطلاعات , یعنی مدیریت ریسک را در IT مورد بررسی قرار داده ام که آیا مدیریت ریسک باعث ارتقای سطح پروژه های IT شده , یا سبب افول این پروژه ها می گردد.

با توجه به منابع محدودی که در اختیار داشته ام , تأمل نموده ام پروژه ای انجام دهم که با سایر پروژه های IT متمایز باشد .

تحقیق حاضر در برگیرنده ی یافته های این جانب در طی 30 روز , در حوزه ی مدیریت ریسک در پروژه های IT است .

از استاد ارجمند جناب آقای مهندس رامین مشایخی که با در اختیار گذاشتن جزوات دروس ارائه مطالب فنی و کنترل پروژه , و همچنین از زحمات زیادی که در طول دوران تحصیلی متحمل شده اند تشکر می کنم و توفیق روزافزونشان را از خداوند منان خواهانم.

همچنین در انتها جا دارد از مسؤل کتابخانه دانشگاه ایرانشهر , و دانشجویان گرامی جناب آقای الهی بخش از مونس , جناب آقای شعیب بلوچی و عبدالرحمن دامنی که مرا در این امر یاری نموده اند تقدیر و تشکر به عمل آورم.

7	1. مقدمه.....
8	2. جایگاه مدیریت ریسک در پروژه های IT.....
8	2.1 ریسک
8	2.2 مدیریت ریسک
9	2.3 چارچوب مدیریت ریسک.....
11	2.4 برنامه ریزی ریسک.....
11	2.5 شناسایی ریسک.....
14	2.6 برآورد و تخمین ریسک
17	2.7 استراتژی برخورد با ریسک.....
19	2.8 کنترل و نظارت ریسک.....
19	2.9 پاسخ به ریسک.....
21	2.10 ارزیابی ریسک.....
21	3. کاربرد و نقش مدیریت ریسک در موضوع فناوری اطلاعات.....
21	3.1 مدیریت ریسک در فناوری اطلاعات
22	3.2 چرخه عمر ایجاد و
23	3.3 تعیین اهداف IT
23	3.4 مدیریت ریسک و اهمیت آن در

3.5. فواید و اهمیت ریسک.....24.

3.6. حیطه مدیریت ریسک.....24.

4. تعیین عوامل کلیدی مدیریت ریسک در.....25.

4.1. اهمیت مدیریت ریسک در فناوری اطلاعات.....25.

4.2. شناسایی ریسک.....26.

4.3. نحوه شناسایی ریسک های موجود در.....28.

4.4. ارزیابی ریسک های برون سپاری.....28.

4.5. مدیریت ریسک پروژه های IT در سازمان های مجازی28

4.6. عوامل موفقیت مدیریت ریسک.....29.

4.7. عوامل حیاتی موفقیت در مدیریت ریسک پروژه های در.....30.

5. مدیریت ریسک در تکنولوژی پیشرفته30.

5.1. ریسک فراوان در عرصه تکنولوژی و31.

5.2. ریسک و موفقیت پروژه31.

5.3. مدیریت ریسک یا تعامل با مشکلات32.

5.4. ابزارهای بنگاه برای مدیریت ریسک.....32.

5.5. دسته بندی رویکرد های مدیریت ریسک در.....33.

5.6. معیارهای موفق مدیریت ریسک در عرصه34.

6. نتیجه و بحث.....34.

7. منابع.....35.

چکیده

امروزه اطلاعات بعنوان عاملی پر ارزش در کنار سایر عوامل تولید بشمار می آید. با تغییرات سریع تکنولوژیک، جهانی شدن و گسترده تر شدن دامنه فعالیت موسسات، وجود سیستمهای اطلاعاتی کارآمد از الزامات رسیدن به مزیت رقابتی است. این مقاله تلاشی است در جهت تبیین نقش مدیریت ریسک در موفقیت پروژه های فن آوری اطلاعات و چگونگی مدیریت موثر آن. و به این نتیجه می رسیم که شناسایی و مدیریت ریسکهای مشاهده شده قبل و حین اجرای پروژه های IT نقش اساسی ایفا می کند. مدیریت ریسک باید یک فعالیت پیشگیرانه باشد. و برای موفقیت لازم است از یک روش استاندارد (چارچوب) استفاده شود. بهره گیری از چارچوب و روش استاندارد باعث میشود مدیران از اشتباهاتی مثل ازدست دادن فرصت ها و تهدیدات و صرف زمان و منابع زیاد مصون بمانند. و درنهایت، موفقیت در شناسایی و کاهش ریسکهای پروژه میتواند مخاطرات و مشکلات فنی و غیرفنی را برای مدیران و ذینفعان کلیدی مشهود کرده منابع را درحوزه هایی که ریسک بالاست متمرکز نماید و ضمن قراردادن ریسک ها در محدوده های منطقی آنها را به شیوهای صحیح و قابل سنجش مدیریت کنند فناوری اطلاعات به نحوه فرآیندی بر چگونگی عملکرد و نحوه کارآیی سازمان ها ارگان ها و سیستم های مبتنی بر شرکت های دولتی و خصوصی اثر گذاشته است. نقش سیستم های مبتنی بر فن آوری اطلاعات در انجام کارآمد امور اداری و تجاری انکارناشدنی جلوه می کند. تنوع و گستره فعالیتها موجب می گردد تا امکان پرداختن به همه امور میسر بنا شود. پس طبقه بندی کردن امور و اولویت دادن به برخی امور مهم نسبت به برخی دیگر از اهمیت زیادی برخوردار نمی باشند ضرورت پیدا می کند.

امروزه بهره گیری از فن آوری اطلاعات در مدیریت ریسک حدیث متفاوتی را باز می گوید و تأثیری عمیق بر چگونگی سر و سامان دادن به فعالیت های اتوماسیون سازمان ها و مدیریت چرخه ایجاد سیستم های مکانیزه می گذارد.

کلید واژه: مدیریت ریسک - برنامه ریزی ریسک - فناوری اطلاعات - سیستم اطلاعات - حیطه مدیریت ریسک - تصمیم گیری

1. مقدمه

امروزه سازمانها و سیستمهای آنها در محیطی پر از چالش و تحول قرار گرفتهاند لذا لازمه بقاء و ادامه زیست سازماندر چنین محیطی همگامی با تحولات محیط و پاسخ درست و به موقع به آنهاست.

پاسخگویی درست مستلزم تصمیمگیری درست است که همت همه جانبه مدیران و دست اندرکاران هر برنامه و تصمیمرا میطلبد , واضح است که در تمام شرایط کلیه جوانب کار و تصمیم مشخص نیست و بنابراین از جمله مواردی که در حین تصمیمگیری الزاماً باید مورد توجه قرار گیرد خطرات احتمالی و یا قطعی موجود است که میتواند بر نتایج تصمیم اخذ شده تأثیر گذارد. مزایای غیرقابل انکار فن آوری اطلاعات (IT) در افزایش دقت و سرعت جریان امور، افزایش کیفیت جهانی، کاهش هزینه ها و رضایت بیشتر مشتریان باعث شده سازمانها به سرعت به استقرار و استفاده از سیستمهای اطلاعاتی روی آورند آنگاه که کسب منافع گوناگون مالی و اقتصادی تنها دلیل اجرای یک پروژه فناوری اطلاعات است از این رو تعریف موفقیت در ابتدای پروژه و شناسایی و مدیریت ریسک ها و مخاطرات و روشی که بتوان آنها را پیگیری نمود، از الزامات اساسی موفقیت پروژه های فن آوری اطلاعات است.

فناوری اطلاعات یا IT تمام جنبه های زندگی را تحت تاثیر قرار داده است و از این رو اقتصاد جهانی، بیش از پیش به توجهات ویژه به مدیریت ریسک بدلیل توسعه اینترنت در سازمانها و سیستم های آی تی نیازمند گردیده است , و این همان حوزه بحث در مدیریت ریسک است. در دنیای دیجیتالی امروز و عصر ارتباطات به کارگیری فناوریهای نوین مانند IT و سیستمهای اطلاعاتی لازمه پاسخگویی مناسب به تحولات کنونی محیط است. چرا که فناوری اطلاعات به نحو فزایندهای بر چگونگی عملکرد و نحوه کارآیی سازمانها اعم از خصوصی و دولتی تأثیر گذاشته است. جستجو برای یافتن آسیب هایی که منجر به ضرر در بیزینس شده و شبیه سازی مشکلات آینده و تصمیم سازی قبل از وقوع از جمله فاکتورهایی است که مدیریت ریسک آنرا به مدیران ارشد امنیت اطلاعات در سازمان (CISOS) و مدیران اجرایی سازمان (CIOS) یاد می دهد.

بسته به حجم سازمان و میزان مبادلات مالی و میزان استفاده از اینترنت و فناوری های رایانه ای مدیریت ریسک می تواند شدت و حدت خاص خود را داشته در سازمانهای مبتنی بر IT دو نوع مدیریت اطلاعات یا CIO داریم: مدیریت زیرساختها و فرا ساختارهای سازمانی و مدیریت استراتژیک و متفکران استراتژیست که دومی در زمینه مدیریت ریسک موفق تر اقدام می کند چرا که ملموس تر با مقوله بیزینس درگیر است. تصمیمگیری در حوزهها، پروژهها و سیستمهای مبتنی بر فناوری اطلاعات نیز عاری از احتمال و ریسک نیست و لذا بایستی قوانین و رویههای مدیریت ریسک در این حوزه نیز در نظر گرفته شود و تصمیمات مربوطه را پشتیبانی کند در هر سازمانی که برای تحقق بخشیدن به مأموریت و رسالت خویش از سیستمهای خودکار فناوری اطلاعات استفاده میکند. مدیریت ریسک در حمایت از منابع اطلاعاتی سازمان نقش حیاتی بازی میکند . مدیریت ریسک فناوری اطلاعات کاملاً فناوری محور بوده و با نرم افزار و سخت افزار و اطلاعات و دیتا سر و کار دارد اما سر و کارش لزوماً با افراد کاملاً فنی نیست. چراکه ممیزین، رهبران بیزینس، گروه های حقوقی نیز در این راستا با مدیریت خطر روبرو شده و به نوعی پاسخگو می شوند. بنابراین ارتباط تنگاتنگی بین IT و غیر IT در این حوزه

به چشم می خورد. شناسایی هدف پروژه نیز از دیگر گامهای عملی برای مدیریت صحیح ریسک در فناوری اطلاعات به شمار می رود. به هر حال مدیریت ریسک در IT مقوله ای امنیتی است که به تبع اطلاعات سازمانی و حجم دیتای انتقالی اهمیت می یابد.

2. جایگاه مدیریت ریسک در پروژه های IT

2.1 ریسک:

مدیریت پروژه در دستیابی به اهداف از پیش تعیین شده پروژه، با تهدیدها فرصت هایی در رابطه با سه عنصر کلیدی پروژه، یعنی زمان، کیفیت و هزینه مواجه است. ریشه این تهدیدها و فرصت ها را می توان در مجموعه ای از شرایط غیر قطعی یا عدم اطمینان جستجو کرد که دارای منشأ های مختلفی مانند مسایل تکنیکی، مدیریتی، بازرگانی و مسایل داخلی و خارجی می باشند. در همین راستا، ریسک پروژه به صورت زیر تعریف می شود:

رویداد ها یا شرایطی غیر قطعی که در صورت وقوع، اثری مثبت یا منفی بر اهداف پروژه خواهند گذاشت.

با توجه به اینکه اهداف پروژه ها بر اساس سه عنصر کلیدی مذکور (زمان، هزینه و کیفیت) بیان می شوند لذا اهم ریسک ها، قصور در رسیدن به ان اهداف می باشند. هرچند که بر اساس تعریف ارائه شده، وقوع ریسک همیشه دارای اثرات منفی نبوده و ممکن است به صورت فرصت ها نیز بیان شوند

PMBOK ریسک پروژه را بصورت زیر تعریف می کند: "یک اتفاق غیر منتظره یا شرایطی که در صورت وقوع، تاثیرات منفی یا مثبت بر روی اهداف پروژه می گذارند." این تعریف نقطه شروع مهمی برای درک ریسک های پروژه است. ریسک پروژه ناشی از موقعیت غیر قابل اطمینان است. شرایط غیر مطمئن ناشی از تلاش ما در جهت پیش بینی آینده بر اساس تخمین ها، فرضیات و دانش اندک ماست. هر چند که ریسک حاصل از تهدیدات و مشکلات غیر قابل انتظار، باعث توقف و صدمه می شوند. اما تمرکز مدیریت ریسک بر جنبه مثبت اتفاقات و فرصت هاست. بنابراین دانستن اینکه چه اتفاقی ممکن است تاثیر مثبت بر روی پروژه داشته باشد بسیار حائز اهمیت است

2.2 مدیریت ریسک :

ریسک، پدیده‌ای جدایی ناپذیر از پروژه است. لذا باید آن را مدیریت کرد. هدف از مدیریت ریسک، برنامه ریزی، سازمان دهی، هدایت و کنترل فعالیت و فرآیندهای پروژه است، به گونه ای که اثرات مثبت فرصت ها بیشینه و اثرات منفی تهدید ها کمینه گردد. بر این اساس مدیریت ریسک به این صورت تعریف شده است:

فرآیند سیستماتیک برنامه ریزی برای شناسایی، آنالیز، پاسخگویی و زیر نظر گرفتن ریسک پروژه. این مدیریت شامل فرآیندها، ابزارها و تکنیک هایی است که به مدیر پروژه برای بیشینه سازی احتمال نتایج رویدادهای مثبت و کمینه سازی احتمال نتایج رویدادهای مضر کمک می کند.

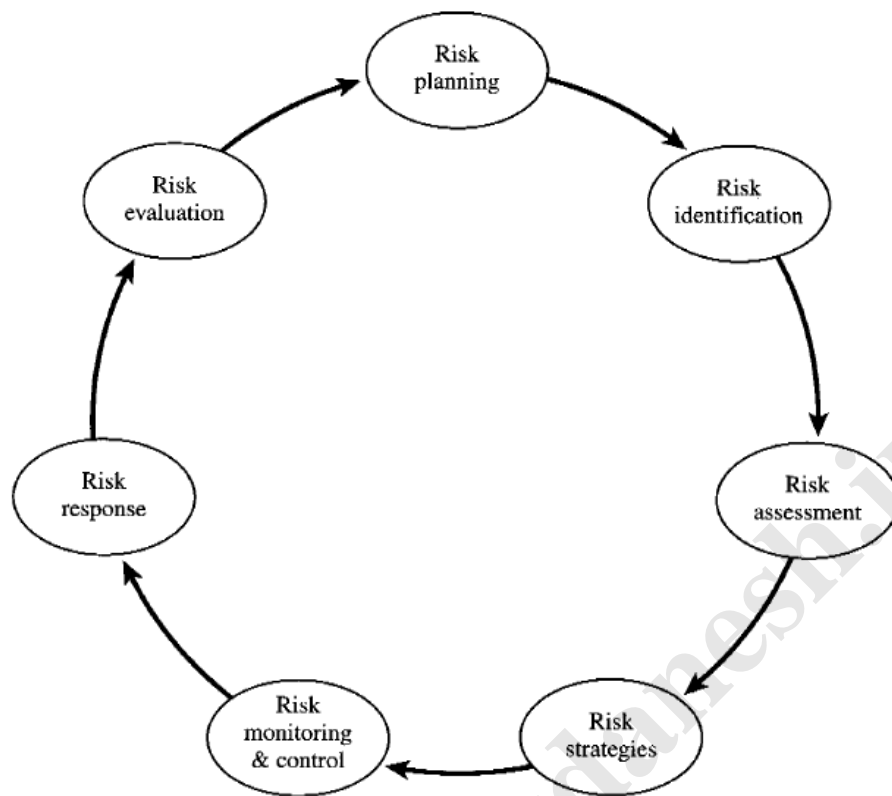
با به کار گیری فرآیند کامل مدیریت ریسک می توان ادعا کرد که این مدیر پروژه است که بر شرایط غیر قطعی پروژه اشراف دارد، نه آن که شرایط و اتفاقات، مدیریت را اسیر خود کند. مدیریت ریسک، در هر پروژه ای از هر نوع که باشد، باید به کار گرفته شود و بدینوسیله ضررهای احتمالی تا حد امکان کاهش یابد. مقصد اصلی مدیریت ریسک پروژه، بهبود عملکرد پروژه از طریق شناسایی، ارزیابی و مدیریت نظام مند پروژه، در ارتباط با ریسک است. مدیریت ریسک پروژه، دارای مزایای متعددی می باشد. گرایش به سوی یک تجارت مفید، کمک به اجرای هر چه موفق تر برنامه راهبردی سازمان، کاهش رویدادهای غیر قابل پیش بینی هزینه زا، تخصیص هر چه کارا تر و اثربخش تر منابع، دریافت نتایج بهتر از پروژه ها و برنامه ها، کمک به داشتن تعریف شفاف از نظام بیمه ای پروژه ها، اطلاعات بهتر برای تصمیم گیری، برآوردن احتیاجات سلسله مراتبی پروژه، تمهید شرایط برای بازرسی ها، کاستن ریسک انسانی پروژه ها و متعادل سازی فرصت ها و تهدیدها از جمله مزایای اجرای مناسب مدیریت ریسک پروژه می باشد

PMBOK مدیریت ریسک پروژه را به این ترتیب شرح می دهد: "یک فرآیند سیستماتیک از شناخت، آنالیز و پاسخگویی به ریسک. این فرآیند، احتمال و نتایج مثبت اتفاقات را افزایش و نتایج منفی آنرا کاهش می دهد" این تعریف بیان می دارد که فرایند سیستماتیک نیاز به مدیریت ریسک پروژه بصورت موثر دارد.

هدف از اجرای مدیریت ریسک این است که سازمان بتواند به اهداف ذیل جهت سیستم های مبتنی بر فن آوری اطلاعات خود دست یابد. تأمین امنیت بیشتر برای سیستم های مبتنی بر ذخیره سازی پردازش و انتقال اطلاعات سازمانی اعمال مدیریت برای توجیه و تصویب و تأیید سیستم ها IT. مدیریت ریسک فرآیندشناسایی ارزیابی و کنترل ریسک های اتفاقی بالقوه ای است که مشخصاً پیامدهای ممکن آن خسارت یا عدم تغییر در وضع موجود می باشد. مدیریت ریسک، ریسکها را به وسیله کنترل آنها و تأمین مالی خسارت هایی که به رغم تلاش های کنترل خسارت اتفاق افتاده اند

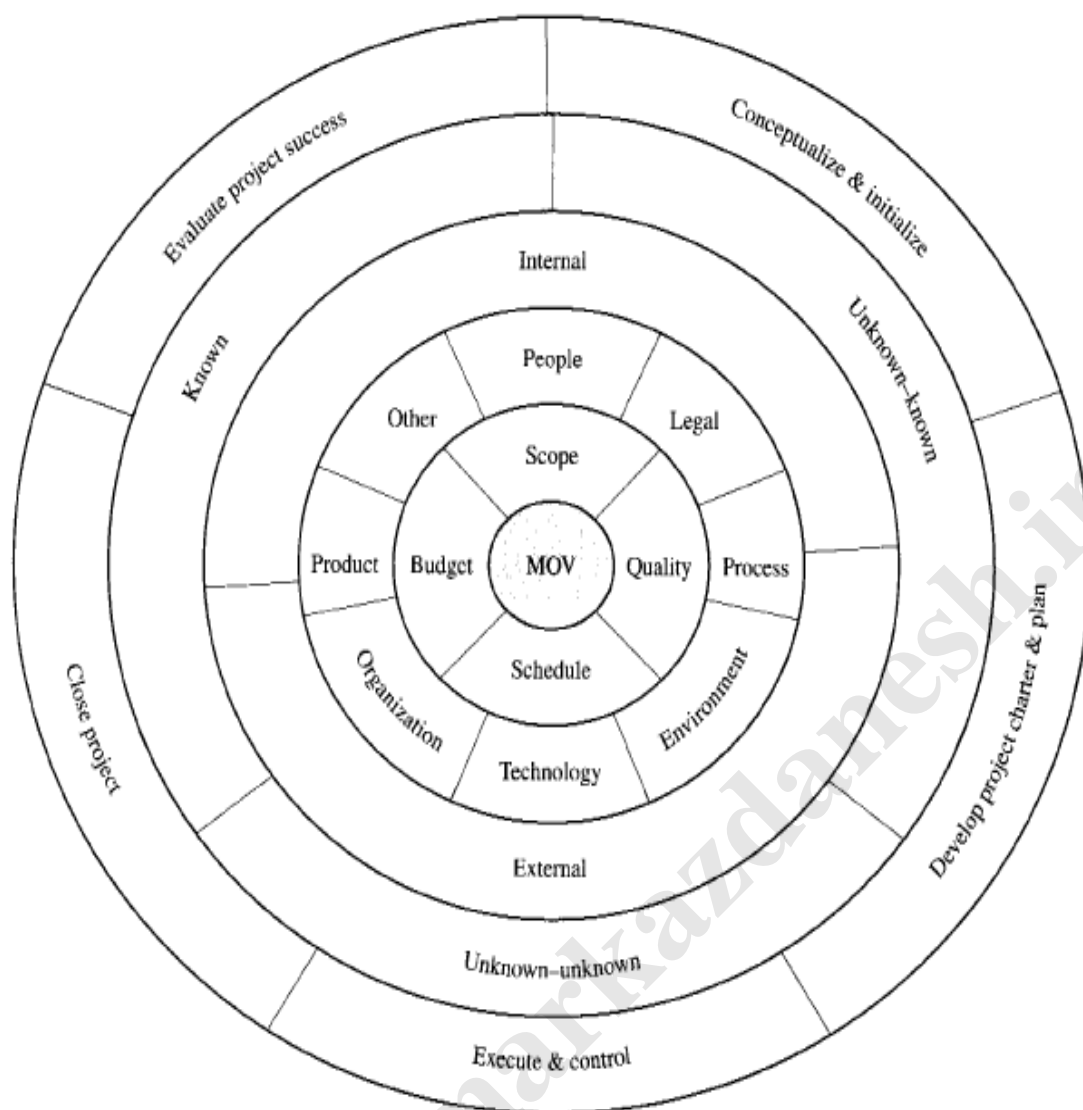
اداره می کند. شکل 1-2 هفت مرحله مدیریت ریسک پروژه های IT را نشان می دهد

شکل 1-2 مراحل مدیریت ریسک



2.3 چارچوب مدیریت ریسک پروژه های IT :

فرآیند و تکنیک های مختلفی برای شناسایی و تخمین ریسک ها بکار گرفته می شود. شکل 2-2 چارچوبی برای شناسایی و درک منشا و تاثیرات ریسک های پروژه های IT را نشان می دهد.



شکل 2-2: چارچوب ریسک های پروژه های IT

همانطور که می بینیم MOV (Measurable Organization Value) هسته مرکزی این چارچوب است. MOV در واقع هدف اصلی یک پروژه است و value های قابل اندازه گیری که یک سازمان از پروژه انتظار دارد را معین می کند. لایه بعدی شامل اهداف پروژه در قالب Scope، کیفیت، زمانبندی و بودجه است. لایه سوم بر روی منشا ریسک پروژه های IT تکیه می کند. لایه بعد بر منشا ریسک تاکید دارد که بصورت داخلی و یا خارجی به پروژه تحمیل شده است. لایه پنجم شامل 3 نوع ریسک: ریسک های شناخته شده، ریسک های شناخته-ناشناخته و ریسک های ناشناخته - نا شناخته می باشد. لایه آخر، بکاربردن چارچوب مدیریت ریسک پروژه های IT می باشد. تیم پروژه می تواند از فازهای پروژه تعریف شده در لایه خارجی چارچوب شروع کند. با استفاده از WBS¹ (استفاده از ساختار تجزیه کاری پروژه WBS) و بسته های کاری مجزا، تیم می تواند ریسک های در فازهای

¹ WorkBreak Down Structure

مختلف پروژه را تشخیص دهد. زمانی که طرح برای پاسخگویی ریسک آماده شد، Trigger های مختلف بایستی مرتباً به منظور دنبال نمودن ریسک پروژه های IT، عمل مانیتورینگ را انجام دهند. بعلاوه فرصت ها و تهدیدهای جدیدی ممکن است ظاهر شوند. بنابراین باید ذینفعان پروژه مراقب باشند. کنترل و مانیتورینگ ریسک جزیی از کنترل و مانیتورینگ پروژه است که بر پایه متریک هایی برای کمک به شناخت ریسکها و ارتباط با آنها استوار است. آنالیز ریسک هم به منظور تعیین فرصت ها و تهدیدهای حاصل از ریسک است که تاچه حد و به چه نوع تهدید و فرصتی باید سریعاً پاسخ داد و توجه نمود.

آنالیز و تشخیص ریسک روشی سیستماتیک برای ارزیابی ریسک هایی است که ذینفعان پروژه می شناسند. هدف از آنالیز ریسک تعیین احتمال ریسک های شناخته شده و اثر آنها بر روی پروژه است. اما در مورد مطالعه ما 7 مرحله مدیریت ریسک که شکل آن را مشاهده کردیم به شرح زیر در نظر گرفته می شود

2.4 برنامه ریزی ریسک

در این مرحله باید لیست ذینفعان و تعهدات آنها برای مدیریت ریسک گرفته می شود. در این پروژه لیست ذینفعان شامل: دانشجو، استاد راهنما، مدیر گروه، اداره آموزش، شورای بخش، دفتر بخش، مسئول کتابخانه، ممتحن، محقق و مرکز جمع آوری مستندات علمی می باشند که هر کدام باید تعهدات مربوط به خود برای مدیریت ریسک را داشته باشند.

2.5 شناسایی ریسک

پس از تعریف اهداف در بخش برنامه ریزی مدیریت ریسک، گام بعدی شناسایی مناطق و حوزه های ریسک و عدم قطعیت است که مانع از دستیابی به اهداف می گردند. شناسایی و طبقه بندی ریسک ها سخت ترین و مهم ترین بخش از فرآیند چرخه مدیریت ریسک می باشد. زیرا در صورت عدم شناسایی ریسک، آن ریسک از تحلیل های بعدی حذف شده و نمی توان برنامه ریزی مناسبی جهت پاسخ به آن انجام داد. ورودی این فاز، مواردی چون برنامه مدیریت ریسک، خروجی های برنامه ریزی پروژه (ساختار شکست فعالیت ها، برنامه ریزی منابع، منطق و برنامه زمانبندی و ...) تجارب و اسناد ثبت شده و گزارشات رسمی پروژه می باشد.

در این راستا روش های مختلفی جهت شناسایی ریسک ها وجود دارد.

برخی از مهمترین این روش ها عبارتند از: تحلیل سوابق تاریخی و گزارشات نهایی، طوفان ذهنی، فهرست های ساختار شکست ریسک، تکنیک دلفی و تحلیل سناریو ها (چه می شود اگر؟)

در استاندارد PMBOK روش ساختار شکست ریسک از اهمیت ویژه ای برخوردار است.

جدول زیر 1-2 دسته بندی کلی برای ریسکهای ممکن در نظر گرفته

شده و پس از آن لیست ریسک های پیش بینی شده آورده شده است:

عنوان فاکتور ریسک	توصیف ریسک	اثرات ناشی از ظهور ریسک	روش های کاهش ریسک
1 ریسک دسترسی	منظور از ریسک دسترسی، خدشه «دسترسی غیر مجاز» به منابع اطلاعاتی، سخت افزار و نرم افزارهای کامپیوتری و (هر آنچه به عنوان سرمایه اصلی ذینفعان و متولی طرح می باشد) است که میزان اهمیت هر یک از اقلام سرمایه ای، می توان درجه ریسک آن را معین نمود	*از دست دادن اطلاعات محرمانه *از کار افتادن سخت افزار و نرم افزارهای کامپیوتری *از دست دادن فرصت های توسعه فناوری اطلاعات	*افزایش امنیت نرم افزاری و سخت افزاری *سطح بندی مناسب منابع سرمایه ای بر اساس اختیار افراد و تدوین سیاست های کنترلی
2 ریسک خدمت رسانی و پاسخگویی به کاربران	چنانچه در ارائه خدمات به کاربران، نظارت و کنترلی صورت نپذیرد و میزان رضایتمندی یا دریافت خدمات توسط کاربران بررسی نشود، ریسک خدمت رسانی و پاسخگویی به کاربران رخ می دهد.	*نارضایتی کاربران و کاهش اعتبار سازمان ها *از دست دادن فرصت های بهره گیری مؤثر از فناوری اطلاعات	*پیش بینی دلایل شکست پاسخگویی به کاربران و تمهید راه حل های مناسب*دریافت فیدبک از کاربران و بهبود مستمر در روش ارائه خدمت به آنان
3 ریسک جامعیت داده	اگر برای گزارشات مدیریتی یا توسعه خدمات سازمان ها، از داده نادرست استفاده	*از دست دادن فرصت های سازمان ها	*اختصاص راه حل امنیتی و سطح دسترسی به اقلام

		<p>شود، ریسک جامعیت داده رخ می‌دهد.</p> <p>همچنین از منظر برون سازمانی نیز، چنانچه اطلاعات کاربران درست به سازمان‌ها ارائه نگردد یا داده نادرست به کاربران و ذینفعان ارائه گردد. نیز خود باعث برهم ریختگی و اختلال در خدمت‌رسانی سازمان‌ها گردیده و ریسک جامعیت داده رخ می‌دهد.</p>	<p>*ظاهر شدن ناکارآمدی در فرآیندهای خدمت‌رسانی سازمان‌ها</p> <p>*تأثیر منفی بر کاربران</p>	<p>داده‌ای</p> <p>*کنترل و نظارت پیوسته بر یکپارچگی داده</p>
4	ریسک سوءاستفاده	<p>امکان اختلال در منابع سازمانی، یا دستکاری و از بین بردن رکوردهای سازمانی به عنوان ریسک سوءاستفاده دیده می‌شود. از برون سازمان، افراد غیر مجاز نیز ممکن است به کانال‌های ارتباطی نفوذ نمایند و به اطلاعات محرمانه دسترسی پیدا کنند یا اینکه از منابع و دارایی‌های سازمان، استفاده نادرست نمایند که این امر خود منجر به وقوع ریسک سوءاستفاده خواهد شد.</p>	<p>*اختلال در ارائه خدمات سازمان‌ها</p> <p>*از دست دادن اطلاعات محرمانه و منابع با ارزش سازمانی</p> <p>*کاهش اعتبار و اعتماد سازمانی</p> <p>*از دست دادن فرصت‌های بهره‌گیری مؤثر از فناوری اطلاعات در خدمت‌رسانی</p>	<p>*افزایش امنیت دسترسی به اطلاعات و منابع سازمانی</p> <p>*کنترل و نظارت پیوسته بر دسترسی به منابع سازمانی</p>
5	ریسک حقوقی - قانونی	<p>در ارائه خدمات دولتی بر بستر فناوری اطلاعات می‌بایست بررسی شود که نیازمندی‌های حقوقی-قانونی آن پوشش داده شود، در صورت عدم پوشش نیازمندی‌های حقوقی-قانونی، ریسک حقوقی-قانونی رخ می‌دهد.</p>	<p>*انحرافات حقوقی-قانونی</p> <p>*ایجاد مشکل در ارائه خدمات</p>	<p>*تعیین نیازمندی‌ها و بررسی وجود بستر حقوقی-قانونی قبل از ارائه خدمات و رفع موانع موجود</p>
6	ریسک فرهنگی - آموزشی	<p>آماده‌پذیری کارکنان داخل سازمان‌ها برای ارائه خدمات و همچنین کاربران برای دریافت خدمات، می‌بایست قبل از ارائه خدمات و همچنین همزمان با آن، مورد بررسی قرار گیرد که در صورت عدم وجود بستر فرهنگی ریسک فرهنگی-آموزشی مورد توجه قرار گیرد.</p>	<p>*تعطل و کندی در ارائه خدمات</p> <p>*عدم استقبال یا رضایت از ارائه خدمات</p>	<p>*بستر سازی فرهنگی و آموزش اختصاصی کارکنان سازمان برای ارائه خدمات</p> <p>*آموزش‌های عمومی کاربران و ایجاد فضای مناسب برای استقبال و پذیرش خدمات سازمان‌ها</p>
7	ریسک صدمه‌پذیری (از کار افتادن) منابع سخت‌افزاری	<p>این ریسک در صورتی رخ می‌دهد که منابع سخت‌افزاری که در دسترسی</p>	<p>*ناکارایی در فرآیندهای ارائه خدمات</p>	<p>*اخذ سیاست‌های تست منابع سخت‌افزاری و رفع خرابی‌ها</p>

و استفاده کارکنان	*نارضایتی	*در نظر گرفتن
سازمان یا کاربران	کاربران و کاهش	نسخه‌های
است، دچار وقفه یا خرابی	اعتبار بهره‌گیری	پشتیبانی برای
گردد. میزان اهمیت	از فناوری	سخت افزارها
تجهیزات سخت‌افزاری در	اطلاعات در ارائه	
ارائه خدمات، بحرانی	خدمات	
بودن و نسبت درجه ریسک		
را مشخص می‌نماید.		

جدول 1-2: دسته بندی کلی ریسکها

2.6 برآورد و تخمین ریسک

بعد از شناسایی ریسک ها در این مرحله احتمال وقوع و تاثیر آن بر روی پروژه باید بررسی شود که برای این منظور از روش کمی استفاده شده و یک سری پارامترهایی برای احتمال وقوع و اثر ریسک در نظر گرفته شده که جداول آن به صورت زیر می باشد و بعد با توجه به آنها درجه و رتبه ریسک مشخص شده است

مقدار عددی	احتمال وقوع
1	Low
2	Moderate
3	High

جدول 2-2 : احتمال وقوع ریسک و مقدار عددی متناظر

مقدار عددی	اثر ریسک
------------	----------

1	ناچیز
2	قابل تحمل
3	خطرناک
4	فاجعه انگیز

جدول 2-3: اثر ریسک و مقدار عددی متناظر

با توجه به جداول بالا رتبه ریسک به صورت زیر محاسبه می شود:

رتبه ریسک : احتمال وقوع ریسک * تاثیر ریسک

که برای ریسک های پروژه مورد نظر احتمال وقوع و تاثیر ریسک و رتبه ریسک به صورت زیر خواهد بود.

ردیف	شرح ریسک	احتمال وقوع	تاثیر ریسک	رتبه ریسک
1	اختلالات شبکه ای و قطعی شبکه و در نتیجه در دسترس نبودن به موقع منابع	2	3	6
2	از کار افتادن سیستم های اطلاعاتی	2	3	6
3	عدم هماهنگی و وجود اختلاف بین نسخه اصلی و دیجیتالی	1	2	2
4	عدم ذخیره سازی مناسب و پشتیبان گیری از فایل ها	2	4	8
5	استفاده غیر قانونی از پایان نامه ها و رساله ها (Copyright)	3	3	9
6	عدم بکارگیری سیاست لازم برای دریافت هزینه دسترسی	2	3	6
7	کارایی پایین نرم افزار و	1	2	2

			فاصله زمانی زیاد از لحظه جستجو تا زمان دیدن فایل	
6	3	2	تخمین نادرست هزینه لازم	8
4	2	2	عدم بکارگیری استانداردها برای یکپارچه شدن با سیستم های الکترونیکی دیگر مانند استاندارد مربوط به Meta Data یا فرمت فایل های ذخیره شده	9
9	3	3	دزدی اطلاعات	10
6	3	2	عدم وجود زیرساخت سخت افزاری و نرم افزاری لازم	11
4	2	2	عدم وجود افراد متخصص در این زمینه	12
6	3	2	عدم وجود تیم پشتیبان اجرایی	13
4	2	2	عدم پشتیبانی توسط اساتید و دانشجویان	14
8	4	2	کناره گیری افراد با مهارت از تیم پروژه	15

جدول 2-4: احتمال وقوع و تاثیر ریسک و رتبه ریسک

2.7 استراتژی برخورد با ریسک

هدف این مرحله رسیدگی به ریسکهای مختلف می باشد که استراتژی و نحوه برخورد با ریسک باید مشخص شود که در کل چهار نوع استراتژی برای برخورد با ریسک وجود دارد که عبارتند از:

- قبول یا رد ریسک
- اجتناب کامل از ریسک
- کاهش احتمال یا اثر ریسک
- انتقال ریسک به یک فرد دیگر

که برای ریسکهای شناسایی شده مربوط به پروژه مربوطه استراتژی برخورد در جدول زیر ارائه شده است.

ردیف	شرح ریسک	استراتژی برخورد	نوع استراتژی
1	اختلالات شبکه ای و قطعی شبکه و در نتیجه در دسترس نبودن به موقع منابع	ایجاد تیم کنترل و مسئول شبکه	کاهش احتمال یا اثر ریسک
2	از کار افتادن سیستم های اطلاعاتی	ایجاد رویه های جایگزین یه صورت دستی	کاهش احتمال یا اثر ریسک
3	عدم هماهنگی و وجود اختلاف بین نسخه اصلی و دیجیتالی	آموزش افراد برای کنترل نسخه دیجیتالی	اجتناب کامل از ریسک
4	عدم ذخیره سازی مناسب و پشتیبان گیری از فایل ها	ایجاد رویه های پشتیبان گیری خودکار و یا تیم مسئول پشتیبان گیری	اجتناب کامل از ریسک
5	استفاده غیر قانونی از	تعیین رویه های	اجتناب

کامل از	سیاستی لازم برای	پایان نامه ها و رساله ها	
ریسک	کنترل حق مالکیت	(Copyright)	
کاهش	ایجاد رویه های	عدم کارایی سیاست به کار	6
احتمال	کنترلی نرم افزاری	گرفته شده برای دریافت	
یا اثر		هزینه دسترسی از کاربران	
ریسک			
کاهش احتمال	استفاده از تکنولوژی	کارایی پایین نرم افزار و فاصله زمانی زیاد از لحظه	7
یا اثر ریسک	های مناسب برای	جستجو تا زمان دیدن فایل	
	پیاده سازی نرم		
	افزار		
کاهش	استفاده از روشهای	تخمین نادرست هزینه لازم	8
احتمال	تخمین پروژه برای		
یا اثر	رسیدن به تخمین و		
ریسک	برآورد صحیح		
کاهش	بررسی استانداردهای موجود و هماهنگی	عدم بکارگیری استانداردها برای یکپارچه شدن با	9
احتمال	لازم با آنها و قراردادن امکان تغییر	سیستم های الکترونیکی دیگر مانند استاندارد	
یا اثر	ساختارهای اساسی به صورت پویا	مربوط به Meta Data یا فرمت فایل های	
ریسک		ذخیره شده	
کاهش	ایجاد مکانیزم های کنترل دسترسی	دزدی اطلاعات	10
احتمال			
یا اثر			
ریسک			

2.8 کنترل و نظارت ریسک

کنترل ریسک فرآیندی است که به منظور اطمینان کامل از اجرای برنامه های مدیریت ریسک و اثر بخشی تحقق این برنامه ها در کاهش ریسک های پروژه انجام می گیرد. در این فرآیند علاوه بر پیگیری ریسک های شناسایی شده، کنترل ریسک های باقیمانده و نیز شناسایی ریسک های جدید در طول چرخه حیات پروژه نیز مدنظر می باشد. اجرای موفقیت آمیز این فرآیند منتج به تهیه اطلاعات مناسب برای کمک به تصمیم سازی موثر و کارآمد در موقعیت های خاص احتمال وقوع هر ریسک می گردد. در پایان این مرحله برنامه واکنش به ریسک به هنگام شده و سوابق ریسک ها به منظور استفاده در پروژه های مشابه در یک پایگاه داده جمع آوری می گردد.

2.9 پاسخ به ریسک

مفهوم پاسخگویی به ریسک، اتخاذ اقدام مناسب و واکنش نشان دادن در مقابل ریسک است برنامه ریزی برای واکنش در برابر ریسک، مرحله مهمی است، زیرا تصمیماتی که در این مرحله گرفته می شود مستقیماً ریسک پروژه را تحت تاثیر قرار می دهند. در این راستا چهار نوع پیمانۀ مطرح است. دو تای اول عبارتند از پیمانۀ های پیشگیرانه و محدود کننده که به ترتیب برای کاهش احتمال ریسک و کاهش شدت اثر تهدیدها به کار می روند و دو تای بعدی نیز متناظر دو مورد اول بوده لیکن برای فرصت ها مطرح می شوند که به ترتیب برای افزایش احتمال ریسک و افزایش شدت اثر فرصت ها به کار می روند. مجموعه پیمانۀ های جلوگیری کننده و محدود کننده را تهدید ریسک می نامند. به ازای هر پیمانۀ، می توان مجموعه ای از اقدامات را طراحی کرد. از برنامه ریزی روی مجموعه اقدامات پیشنهادی، با عنوان برنامه اقدام یاد می شود. در ذیل برخی از اقدامات قابل اتخاذ را ملاحظه می کنید:

اجتناب از ریسک: طی این اقدام، عدم اطمینان از پروژه حذف می گردد. به عبارت بهتر تلاش می شود تا احتمال ریسک به سمت صفر میل کند. این اقدام از نوع پیشگیرانه می باشد.

انتقال ریسک: یافتن یک شخص خطر پذیر دیگر که توانایی بهتری در اداره کردن ریسک دارد. یعنی کسی که مسئولیت انجام عمل را به عهده بگیرد.

تخفیف ریسک: کاستن از میزان ریسک در راستای قابل قبول کردن آن برای پروژه یا سازمان از طریق کاهش تاثیر یا احتمال ریسک.

پذیرش ریسک: این ریسک ها را باید پذیرفت و به آن واکنش نشان داد خواه به صورت فعال از طریق تخصیص هزینه مناسب یا به صورت انفعالی بدون انجام هیچ کاری.

حفاظت مالی: با استفاده از امکاناتی نظیر سرویس های بیمه، می توان پروژه را نسبت به رخ دادن رویدادهای تهدیدکننده بیمه کرد. بیمه از رویداد ریسک جلوگیری نمی کند لیکن از کل و یا قسمتی از اثرات آن جلوگیری می کند.

اقدامات قابل اتخاذ برای پاسخ به فرصت ها مطابق ذیل پیشنهاد شده است. این اقدامات درحقیقت از اقدامات تهدید مشتق شده اند:

بهره گیری از ریسک: این اقدام، موازی با اقدام اجتناب از ریسک است که روشی برای حذف عدم اطمینان است. این اقدام در تلاش است تا فرصت ها حتما رخ دهد و یا به عبارت بهتر احتمال وقوع فرصت ها به 100 میل کند.

سهیم شدن در ریسک: اقدام انتقال دادن، تفویض کردن مسئولیت به شخص سومی است که بهتر می تواند تهدیدات در کمین سازمان را اداره کند. در این روش، ما در جستجوی شرایطی هستیم که توانایی بیشتری در اداره کردن فرصت ها دارد. یعنی کسی که می تواند شانس وقوع فرصت را به حداکثر برساند و فواید بالقوه آن را افزایش دهد.

تشدید ریسک: همسنگ اقدام تخفیف تهدیدها، اقدام تشدید فرصت ها مطرح است. تخفیف دادن، درجه تهدید را از طریق کاهش احتمال یا تاثیر پایین می آورد. در حالی که اقدام تشدید ریسک در پی افزایش احتمال در راستای به حداکثر رساندن مزایای پروژه است.

نادیده گرفتن ریسک: اقدام پذیرش ریسک، به جز تهدیداتی که احتمال اثر گذاری نسبی در پروژه دارند برای مابقی تهدیدات هیچ برنامه ای را در نظر نمی گیرد. بنابراین، فرصت های جزئی نیز می توانند تحت استراتژی نادیده گرفتن قرار گیرند. در این اقدام، یک روش واکنشی بدون انجام یک عملکرد روشن اتخاذ می گردد. اجرای اقدامات پیشگیرانه معمولاً در صورت رخ دادن یا رخ ندادن رویداد، هزینه زاست، در صورتی که اقدامات محدودسازی فقط زمانی هزینه می برند که رویداد رخ دهد، ازطرفی اقدامات محدودسازی گرانتر از اقدامات پیشگیرانه است که این موضوع با فوایدی که متعاقب آن برقرار است، جبران می شود.

2.10 ارزیابی ریسک

در این مرحله کلیه ریسک های شناسایی شده در مرحله قبل، مورد تجزیه و تحلیل قرار گرفته و کاملاً تعریف می شوند. همچنین نوع، میزان و اثر هر کدام از آن ها در قالب جزیی از یک سیستم کلی مورد بررسی قرار گرفته و تاثیرشان در پروژه مشخص می گردد.

برای ارزیابی ریسک در پروژه های IT روش های کمی و کیفی وجود دارد ان چنان که استاندارد PMBOK توصیه می کند که این مرحله می تواند ابتدا با ارزیابی کیفی ریسک ها آغاز شده و سپس در صورت نیاز در مورد برخی از با اهمیت ترین آن ها، ارزیابی کمی نیز انجام گیرد.

در فرآیند ارزیابی کیفی ریسک، ارزیابی دقیقی در مورد تواتر وقوع و نتایج هریک از ریسک های شناسایی شده صورت می گیرد و سپس ریسک های مختلف را بر اساس مقادیر بدست آمده رتبه بندی می کنند. به عبارت بهتر، رویداد های بالقوه مخاطره آمیز بر اساس اثرات هر کدام از ریسک ها بر اهداف پروژه، اولویت بندی می شوند به این وسیله امکان مقایسه ریسک ها با یکدیگر فراهم می گردد.

ارزیابی کیفی را می توان با استفاده از تکنیک های احتمال وقوع و تاثیر، آزمون فرضیات پروژه و رتبه بندی حدود صحت اطلاعات انجام داد.

ارزیابی کیفی، احتمال وقوع پیامدهای موثر بر اهداف پروژه را مشخص می سازد. تکنیک های متداول در این مرحله عبارتند از: تجزیه و تحلیل حساسیت، درخت تصمیم گیری و شبیه سازی مونت کارلو.

انتخاب هر یک از این روش ها بستگی به خصوصیت ریسک و حوزه ارزیابی دارد.

3. کاربرد و نقش مدیریت ریسک در موضوع فناوری اطلاعات

3.1 مدیریت ریسک در فناوری اطلاعات

با ظهور فناوری های نوین اطلاعاتی و لزوم پاسخگویی و همگامی سازمان ها با این فناوری لزوم به کارگیری مدیریت ریسک روش های آن در ایجاد و نگهداری سیستم های مبتنی بر اطلاعات که با یکی از مهم ترین منابع سازمان یعنی اطلاعات سر و کار دارند نمایان تر شده است. در واقع مدیریت ریسک فناوری اطلاعاتی به معنایی شناسایی ارزیابی و کاهش ریسک های موجود در ایجاد و به کارگیری سیستم های اطلاعاتی تا سطح قبول مورد قبول است برای ایجاد و توسعه سیستم های اطلاعاتی روش های گوناگونی وجود دارد که برخی از آنها عبارتند از:

1. چرخه عمر ایجاد و توسعه سیستم

2. الگو سازی

3. استفاده از بسته های نرم افزاری آماده

4. توسعه سیستم توسط کاربر

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

3.2 چرخه عمر ایجاد و توسعه سیستم (SDLC)

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

شروع یا برنامه ریزی ایجاد و تهیه سیستم پیاده سازی سیستم عملیات و تعدیل حفاظت گذاری در مرحله نیاز به سیستم اطلاعاتی اهداف آن حوزه تحت پوشش سیستم مورد نظر و منابع و ابزار لازم مشخص و مستند می شود . در مرحله دوم سیستم مورد نظر تحت مطالعات امکان سنجی قرار گرفته و در نهایت طراحی و برنامه ریزی تولید یا خریداری می شود. در مرحله سوم سیستم پیاده سازی شده ویژگیهای امنیتی سیستم ایجاد آزمایش و تصدیق می شوند سپس مدل منطقی سیستم با مدل فیزیکی و ساختارهای فیزیکی سیستم با در نظر گرفتن ویژگی های 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 فرآیندها و رویه ها و سیاست های سازمان آموزش پرسنل و ... مورد تعدیل و بازبینی قرار می گیرد. در مرحله پنجم : اطلاعات سخت افزار و نرم افزارها در دسترس قرار داده می شوند و عملیات سیستم تحت نظارت مداوم قرار گرفته و خطاها و نیاز به بهبود شناسایی می شوند. در این مرحله ممکن است فعالیتهایی چون جا به جایی حذف دسته بندی یا تخریب اطلاعات صورت گیرد.

3.3 تعیین اهداف IT

به طوری که همسو با اهداف کسب و کار باشند. هدف اصلی IT را که به قرار زیر است می توان نظر گرفت

1. اثربخشی

2. کارایی

3. قابلیت اطمینان

4. انسجام

5. در دسترس بودن

6. برآورده کردن نیاز

7. قابلیت اعتماد

3.4 اهداف مدیریت ریسک و اهمیت آن در IT

مهمترین هدف مدیریت کمک به سازمان در مدیریت بهتر ریسک های مربوطه به مأموریتش است. و این از طریق زیر امکان پذیر است:

- 1 - تأمین امنیت بیشتر سیستم های IT که وظیفه
- 2 - ذخیره پردازش و انتقال اطلاعات سازمان را به عهده دارند.
- 3 - کمک به مدیر در تصمیم گیری های آگاهانه مربوط به ریسک و در نتیجه تعدیل مخارج که بخشی از بودجه مربوط به IT است.
- 4 - کمک به مدیر ارتقاء سیستم IT به دلیل حمایت های ناشی از عملیات مدیریت ریسک بطور کلی می توان اهداف مدیریت ریسک را به صورت زیر بر شمرد :

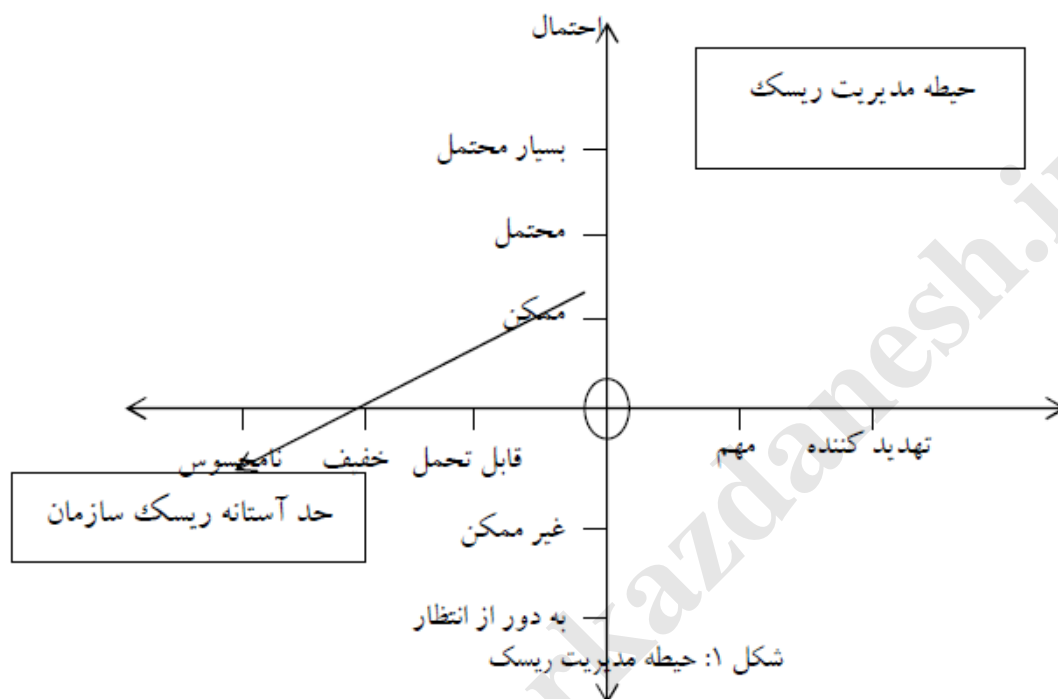
1- بقاء سازمان، 2- صرفه جویی در هزینه ها، 3- حفظ سطح قابل قبولی از نگرانی و اضطراب، 4- ثبات عایدات (درآمدها) از طریق محدود نمودن کاهش های پیش بینی نشده یا جریانهای نقدی ناشی از خسارات، 5- عدم توقف عملیات به دنبال وقوع یک خسارت، 6- رشد مداوم سازمان، 7- ایفای مسئولیت اجتماعی و محدود نمودن خسارت به خود سازمان

3.5 فواید و اهمیت ریسک :

مدیریت ریسک به مدیران کمک می کند تا بتواند 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 بتواند امنیت لازم را در تحقیق مأموریت سازمان پیاده کنند و در نتیجه می تواند بقای سازمان را تضمین کرده و سازمان را از خطر ریسک های کوچک و بزرگ موجود مصون بدارد به طوری خلاصه فواید مدیریت ریسک را به طور اجمال می تواند بررسی کنیم. 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 تحقیق به موقع اهداف

3.6 حیطه مدیریت ریسک در فرآیند شناسایی ریسک پس از تعیین اثر

احتمال ریسک بایستی آنها را روی یک طیف از بسیار بالا تا بسیار پایین طبقه بندی کرد و سپس به اولویت بندی ریسکها پرداخت تا به مهمترین آنها در اسرع وقت پاسخ گفته شود. برای تصمیم گیری روی اولویت بندی ریسک های شناسایی شده بایستی مطابق شکل زیر باتوجه 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.



4. تعیین عوامل کلیدی موفقیت در مدیریت ریسک پروژه های IT

4.1 اهمیت مدیریت ریسک در فناوری اطلاعات:

کاهش اثر منفی ریسک در سازمان و رسیدن یک مبنای درست تصمیم گیری دلایلی هستند که سازمان را وادار به اجرای روند مدیریت ریسک در سیستم های مبتنی بر IT می سازند. ریسک عبارت است از تأثیر منفی ناشی از یک آسیب پذیری و در نظر گرفتن احتمال وقوع و اثر آن در فرآیندهای یک سیستم در پروژه IS ریسک را می توان هر رویدادی که ممکن است برآورده ساختن اهداف پروژه را به مخاطره انداز تعریف کرد. مدیریت ریسک به تنهایی نمی تواند کاملاً ریسک را حذف کند اما می تواند به جلوگیری از ریسک یا کاهش اثر آن در هنگام وقوع

رویدادی مخاطره آمیز کمک نماید. مدیریت ریسک طبق تعریف باید یک فرآیند پیشگیرانه باشد. با این فرض که کنترل ریسک های بالقوه قبل از وقوع آنها اجازه می دهد یک پاسخ اصولی و مورد توافق به هر ریسک داده شود. برای مؤثر بودن راهبرد IT سازمان بایستی با راهبرد اصلی آن همسو شود تا مدیران شرکت و سازمان تشویق گردند برای اطلاعات به عنوان یکی از منابع سازمان ارزش قایل شوند برای همراهی مدیران شرکت و سازمان تشویق گردند برای اطلاعات بعنوان IT برای مؤثر بودن راهبرد IT یا راهبرد سازمان ضروری است مدیران IT اقدامات اساسی زیر را انجام دهند

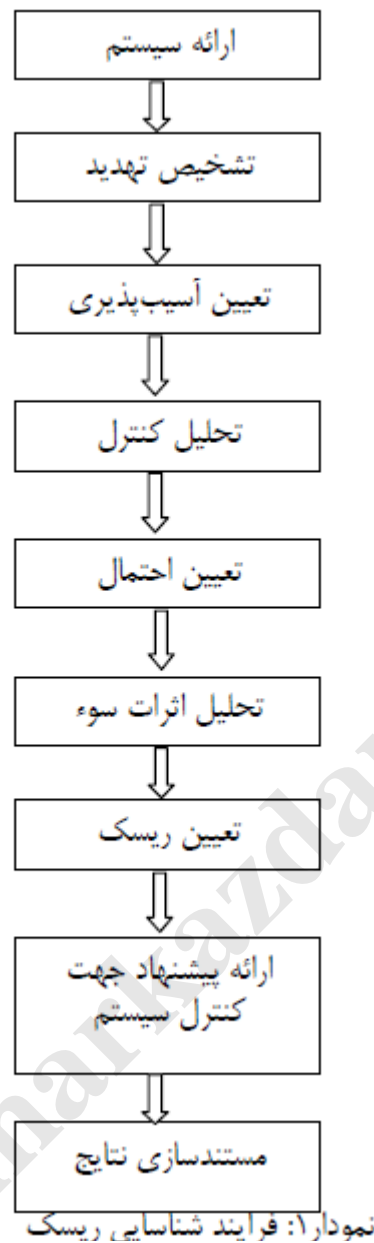
1. آگاه کردن افراد کلیدی از ارزش اطلاعات
2. نشان دادن اینکه چگونه پروژه IT می تواند به ارزش افزوده عملیات کاری بیفزاید
3. اساس و بنیانی برای اصلاح و بهبود فرایندهای کاری فراهم شود. موفقیت مدیران یک سازمان در گروه داشتن مهارت های مدیریتی زیر می باشد:

1. مهارت های مدیریت پروژه
 2. مهارت های مدیریتی (مانند تفویض اختیار مدیریت تغییر)
 3. مهارت های تجاری (مانند بودجه ریزی - تهیه توجیه اقتصادی - برنامه ریزی استراتژیک و عملیاتی و آزمایشی)
 4. مهارت های بین فردی (مدیریت تعارضات - مذاکره مدیریت تیم و تیم سازی)
 5. مهارت های شخصی (مانند خلاقیت - تصمیم گیری)
- علاوه به موارد ذکر شده یک مدیر موفق برای اجرایی کردن یک پروژه IT بایستی مهارت و تجربه لازم را داشته باشد

4.2 شناسایی ریسک

اگرچه تمام مراحل مدیریت ریسک مهم هستند. اما از آنجایی که مرحله شناسایی ریسک مبنایی برای اتخاذ سیاست های مدیریت ریسک و انتخاب تکنیک های اقتصادی ایجاد می کند. از اهمیت ویژه ای برخوردار است از آنجایی که ریسک ها و تهدیدات در طول زمان تغییر می کنند. سازمان ها بایستی هر چند وقت یکبار به شناسایی ریسک پرداخته و مؤثر بودن سیاست ها و کنترل های اخذ شده را تأیید نمایند. شناسایی مطمئن ریسک های امنیت اطلاعات از شناسایی دیگر انواع ریسک ها 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. به علاوه شاهدیم که هر روز فناوری نوین وارد عرضه بازار می شود که این خود منجر به ایجاد منبع جدیدی از تهدید می شود به طور کلی می توان گفت که مرحله شناسایی 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.

مرحله 9 گانه اساسی ریسک به صورت زیر فرمول می شود



همانطور که در نمودار مشخص است در مرحله اول برای تعیین ویژگی های 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 پشتیبانان سیستم IT، مأموریت سیستم سیاست های امنیتی حاکم بر سیستم IT معماری امنیتی سیستم توپولوژی فصلی شبکه، پایگاه داده، جریان اطلاعات، کنترل های فنی به کار رفته در سیستم کنترل های مدیریتی و عملیاتی سیاست های امنیتی محیطی داریم، در نهایت می توان موفقیت یک فرایند شناسایی ریسک را مستقیماً وابسته به عوامل زیر دانست

1. انجام فرایند مبتنی بر دانش و استفاده از سطح مناسبی افراد متخصص و آگاه

2. کنترل مرکزی و منظم به همراه رویه‌های از قبل تعریف شده که موجب می‌شود که از صحت دقت و کامل بودن فرآیند شناسایی ریسک مطمئن شویم.

3. پیگیری ایجاد یک فرآیند منجسم و کامل

4. تعیین مسئولیت فعالیت‌ها

5. مستندسازی

6. ارتقاء دانش سازمانی

7. به روز کردن منظم

4.3 نحوه‌ی شناسایی ریسک‌های موجود در پروژه‌های فناوری اطلاعات:

بسیاری از ریسک‌ها می‌توانند بزرگ‌ترین پروژه‌ها به شیوه‌های مختلفی و در طی مراحل متفاوت چرخه‌ی حیات پروژه اثر بگذارند. بنابراین، فرآیند و تکنیک‌هایی که برای شناسایی ریسک‌ها به کار گرفته می‌شوند باید شامل دیدی وسیع از پروژه باشد. برای شناسایی ریسک‌های پروژه‌های فناوری اطلاعات در سازمان‌های مجازی، می‌توان از راه‌هایی همچون چرخه‌ی یادگیری، طوفان فکری، مصاحبه، چکلیست و علت و معلول استفاده کرد.

4.4 ارزیابی ریسک‌های برون‌سپاری سیستم‌های اطلاعاتی

تحلیل و ارزیابی ریسک یک رویکرد سیستماتیک برای ارزیابی ریسک‌هایی که ذی‌نفعان پروژه شناسایی می‌کنند، فراهم می‌کند. هدف تحلیل ریسک تعیین احتمال هر یک از ریسک‌های شناسایی شده و تأثیر آن بر روی پروژه است. از سوی دیگر، ارزیابی ریسک، بر اولویت‌بندی ریسک‌ها تمرکز دارد و در نتیجه می‌توان استراتژی مؤثر ریسک تنظیم کرد. دو رویکرد اصلی برای تحلیل و ارزیابی ریسک پروژه وجود دارد. رویکرد کیفی (شامل ارزیابی ذهنی بر پایه تجربه یا شهود) و رویکرد کمی (بر پایه تکنیک‌های ریاضی و آماری). روش مورد استفاده در این پژوهش جدول تأثیر ریسک از رویکرد کیفی است. در این حالت احتمال وقوع ریسک در میزان تأثیر ریسک ضرب می‌شود که در این حالت میزان تأثیر ریسک بر اساس اعدادی از صفر تا 10 است. که صفر به مفهوم عدم تأثیر و 10 به معنی بیشترین میزان تأثیر است.

4.5 مدیریت ریسک پروژه‌های فناوری اطلاعات در سازمان‌های مجازی

اکثر پژوهش‌های قبل در مورد ریسک پروژه‌های فناوری اطلاعات در سازمان‌های سنتی انجام شده است و پژوهش‌های کمی بر روی مدیریت ریسک پروژه‌های فناوری اطلاعات در سازمان مجازی تمرکز کرده‌اند. تعاریف مختلف و بعضاً مشابهی از سازمان مجازی توسط اندیشمندان مختلف مطرح شده است. سازمان مجازی، به شکل جدیدی از سازمان‌ها اطلاق می‌شود که از مشخصه‌های آن جمع شدن گروهی از افراد است که از نظر جغرافیایی پراکنده‌اند و به سازمان‌های یکسانی نیز وابسته نیستند و برای رسیدن به یک هدف واحد از طریق فناوری اطلاعات با هم در تماس هستند. با بررسی تعاریف مختلف می‌توان نتیجه گرفت که یک سازمان مجازی، به طور خلاصه دارای ویژگی‌های زیر است:

- سازمان‌های مجازی دارای گروه‌ها یا بخش‌های موقت هستند.
- بخش‌ها، گروه‌ها و یا سازمان‌های مختلف مربوط به یک سازمان مجازی دارای پراکندگی جغرافیایی هستند و یکجا جمع نمی‌شوند.
- ارتباطات الکترونیکی و فناوری اطلاعات در سازمان‌های مجازی بسیار مؤثرند.
- کارهای سازمان به سازمان‌ها و بخش‌های خارجی محول می‌شود.
- دارا بودن کارکنان ویژه و ماهر که بدون حضور فیزیکی می‌توانند وظایف خود را انجام دهند.
- سازمان‌های مجازی در برگزیده‌ی شکل‌های متنوع سازمانی هستند.
- افراد داخل سازمان باید به یکدیگر اعتماد زیادی داشته باشند؛ زیرا کارشان را اغلب دور از هم انجام می‌دهند.
- اکثر پژوهش‌های قبل در مورد ریسک پروژه‌های فناوری اطلاعات در سازمان‌های سنتی انجام شده است و پژوهش‌های کمی بر روی مدیریت ریسک پروژه‌های فناوری اطلاعات در سازمان مجازی تمرکز کرده‌اند. در حالی که، کارهای اجرایی و تکنولوژی مورد استفاده در سازمان مجازی ممکن است ماهیتاً ریسک‌زا باشند. خطاهای انسانی و ساختار سازمانی از دیگر عوامل ریسک هستند، همچنین ساختارهای مدیریت مجازی، می‌تواند ارتباطات فیزیکی را کاهش دهد. سرانجام، فرهنگ‌های سازمانی ممکن است، پیغام‌های گیج‌کننده یا متناقض در مورد تلرانس ریسک در سازمان‌های مجازی بفرستند.
- در سال 2007، انجمن سیستم‌های اطلاعاتی تحقیقی تحت عنوان "عوامل ریسک حیاتی پروژه برای پروژه‌های نرم‌افزاری مجازی" انجام داده است که در آن، لیستی از مهم‌ترین عوامل ریسک پروژه‌های مجازی را شناسایی کرده است. منظور از پروژه‌های مجازی در پژوهش گفته شده، تیم‌های توزیع شده‌ای هستند که در مناطق مختلف قرار دارند و ارتباطات آنها برای انجام پروژه، بیشتر به صورت الکترونیکی است تا حضوری. نتیجه‌ی این بررسی به شناسایی 55 ریسک منجر شده است که در هشت گروه طبقه‌بندی شده‌اند.

4.6 عوامل موفقیت مدیریت ریسک

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

1. تعهد مدیر ارشد در خصوص زمان و منابع

2. پشتیبانی و همکاری همه جانبه گروه

3. صلاحیت تیم مدیریت ریسک IT

4. آگاهی و مشارکت کاربران سیستم

5. ارزیابی مستمر و شناسایی مداوم ریسک های مربوطه به مأموریت فناوری اطلاعات

4.7 عوامل حیاتی موفقیت در مدیریت ریسک پروژه های فناوری اطلاعات در سازمان های مجازی

استویس (2004) استراتژی هایی که موجب کاهش ریسک های دارای احتمال و اثر بالا و در نتیجه کاهش هزینه که در نهایت به افزایش سود و موفقیت سازمان منجر می شود را از جمله عوامل مؤثر در موفقیت میدانند. تا کنون پژوهشی بر روی عوامل کلیدی موفقیت پروژه های فناوری اطلاعات در سازمان های مجازی، در ایران انجام نشده است . لینت و دیگران (2006) عوامل مؤثر در موفقیت مدیریت ریسک پروژه های تکنولوژی اطلاعات را موارد زیر می داند:

- پایگاه داده مسایل و مشکلات : که شامل تلاشها و پروژه های سیستم های اطلاعاتی است . این پایگاههای داده یکمخزنی برای مشکلات و فرصت ها است.
- مشارکت : در مقابل خروجی های پروژه شما باید حمایت سیاسی دیگران را برای تصمیمات و فعالیت های بعدی به دست آورید
- مشخص کردن سریع نتایج : به دست آوردن خروجی های بالقوه افراد را در مورد پروژه ها و کارها واقع گرا می سازد
- فعال کردن تحلیل و ردیابی نتایج : یک رویکرد ساختار یافته برای امتحان و ارزیابی نتایج لازم است.
- ارتباطات و گزارش کردن نتایج : همانند مشخص کردن وضعیت کاری شما باید پیرامون نتایج با مدیریت ، کاربران ، فروشندگان و کارکنان سیستم های اطلاعاتی ارتباط برقرار کند. بهبود تدریجی : همان طور که شما مشکلات یکسانی را مکرر حل میکنید ، در مورد مدیریت مشکلات بهبود پیدا می کنید، تجربیات بیشتری به دست می آورید و درس هایی می آموزید که در کارایی کلی شما بسیار مؤثر است

5. مدیریت ریسک در تکنولوژی پیشرفته

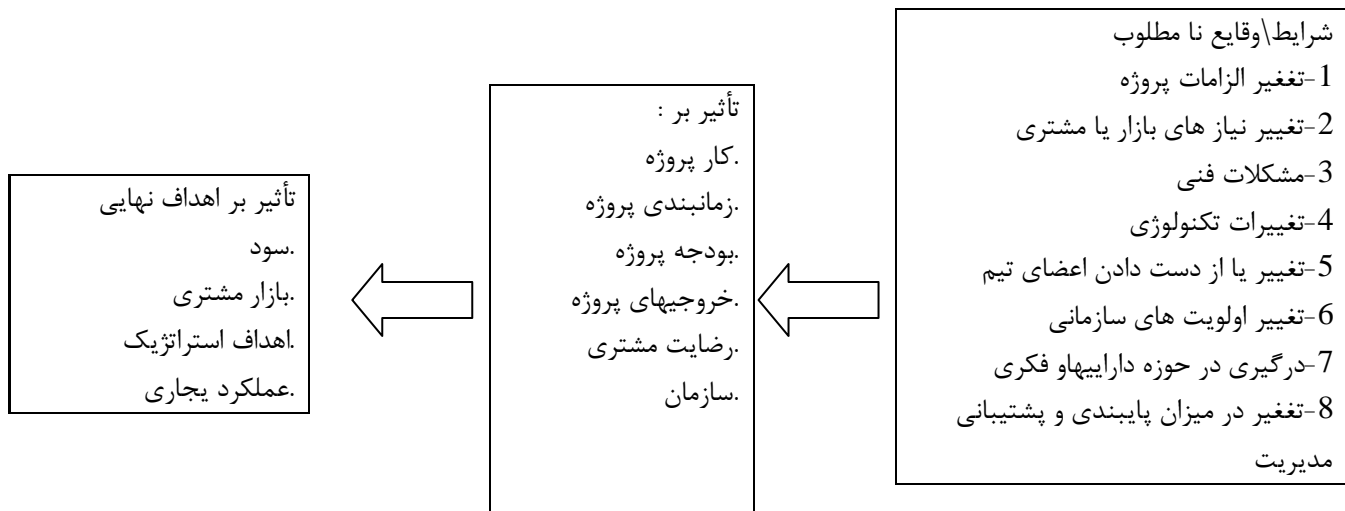
5.1 ریسک فراوان در عرصه تکنولوژی و فناوری اطلاعات

عدم قطعیت در اکثر پروژه های IT حقیقتی انکار نشدنی است و تعجبی ندارد که بسیاری از این پروژه ها شکست خواهند خورد با این وجود سالانه دهها هزار توسعه محصول جدید و پروژه پیچیده نیز با موفقیت تمام می شوند. پروژه پیچیده ای همچون مریخ پیما از این دسته هستند. انجام پروژه ها در حوزه IT و گسترش حوزه فعالیتها در گرو انواع و اقسام متغیرهای پیچیده و بهم پیوسته است. اما بنظر می رسد که یکی از عوامل اصلی موفقیت، توان تعامل سازنده با خطرات و ریسک های گریز ناپذیر باشد. طبق تعریف ریسک زمانی وجود دارد که عدم قطعیت ها مطرح شوند که این قطعیت ها نهایتا اهداف پروژه را تحت تأثیر قرار می دهند. به همین جهت، فنون متنوعی برای تعامل با ریسک مطرح شده است که از فنون بسیار ساده گرفته تا بسیار پیچیده را شامل می شود. هدف همه این فنون برای تعیین دقیق تر خروجی ها در مراحل مختلف چرخه عمر پروژه طراحی شده اند. بطور نمونه: سه سال پیش زمانی که شرکت اینتل سرمایه گذاری 28 میلیارد دلاری خود را برای ساخت کارخانه جدید و توسعه تحقیقات را شروع کرد، کریج برت بعنوان مدیر عامل شرکت هیچ تصویری نداشت که رکورد طولانی صنعت نیمه هادیها چه زمانی پایان می گیرد. تقاضای ناکافی در زمان راه اندازی کارخانه های جدید می توانست پایان کار باشد، اما برت پیش می رفت. او می گوید: سؤال اصلی این بود که چه زمانی اوضاع رو به بهبود می رود. رکورد سه ساله در صنعت ما حدودا دو برابر بدترین رکوردی است که من به یاد می آورم. اینتل بشدت تلاش می کند تا بتواند پاسخگوی تقاضای بازار برای کامپیوتر های همراه سنترینو باشد که در آنها از پردازنده پنتیوم و تراشه وای فا استفاده شده است. با توجه به حاشیه سود درصدی، درآمد شرکت اینتل در سال 2003 به 4\5 میلیارد دلار رسید که نسبت به سال قبل از آن 60 درصد افزایش نشان می دهد.

یکی از دلایل مشکلات موجود در تعامل با ریسک، پیچیدگی محیط کار است. تحقیقات نشان داده که ریشه اصلی خطرات توسعه محصول را می توان در تغییرات سازمانی ماهیت میان رشته ای محیط کسب و کار جستجو کرد. پدیده ای که در پروژه های IT بنیان ابعاد ی دو چندان دارد. افراد، فرایندها و تکنولوژی های متعددی که مرزهای سازمان را در مینورند و به گروه های پشتیبانی و ادارات دولتی تعمیم می یابد. عدم قطعیت ها را تشدید کرده و ریسک را میان شرکایش توزیع می کنند. بسیاری از ابزارهای مدیریت ریسک که در محیط های سنتی و با ثبات موثر بودند، در شرایط پر از تغییر و غیر خطی پروژه های IT- بنیان جواب نمی دهد.

5.1 ریسک و موفقیت پروژه

ما برای این موضوع تقریبا حدود 100 ریسک منحصر به فرد را شناسایی و در 8 گروه ریسک با اثرات نا مطلوب به ترتیب فراوانی آنها دسته بندی کردیم این وقایع نا مطلوب یا عوامل ریسک تأثیر منفی بر پروژه خروجیها و اهداف آن اثر می گذارند



شکل 5- 1 تأثیر وقایع نا مطلوب بر کار و اهداف پروژه

وقایع نا مطلوب تأثیر معمولاً ریشه در چندین مشکل دارند که یا قابل پیش بینی نبوده اند یا رفع آنها در مراحل اولیه چرخه توسعه محصول امکان پذیر نبوده است. وقایعی چون استعفای یکی از اعضای تیم می تواند به مشکلات طراحی، سردرگمی، اختلافات سازمانی و کاهش روحیه تیم می انجامد که در شکل 1 به صورت چکیده آمده است. تمام این عوامل می تواند به تأخیر زمانبندی و ناهماهنگی سیستم منجر شود. که باعث تأخیر انجام پروژه می شود. با این وجود طبق تعریف می توان ریسک ها را تحت مدیریت در آورد که این همان هنر و علم مدیریت پروژه است

5.3 مدیریت ریسک یا تعامل با مشکلات

مشاهدات میدانی به خوبی نشان داده که تأکید اکثر مدیرات پروژه بر حل مشکلات بعد از وقوع آنها است. یعنی علیرغم آشنایی مدیران پروژه با علل ریسک تأکید آنها بر معلولهایی همچون زمانبندی و بودجه است. جالب است بدانید که مدیران پروژه علت مشکلات پروژه و شکستها را عمدتاً بر گردن عوامل خارج از حوزه کنترل خود همچون تغییر اهداف پروژه، تغییر شرایط بازار و مشکلات پشتیبانی پروژه می اندازد. اما انگشت اتهام مدیران ارشد متوجه خود مدیران پروژه است و از ضعف برنامه ریزی، رد یابی و کنترل، ارتباطات نامناسب و ضعف رهبری مدیران پروژه به عنوان عوامل اصلی شکست نام می برد. بسیاری از عوامل ریسک ریشه در خارج از پروژه دارند و به نوعی تحت کنترل مدیران ارشد سازمان هستند لذا شناخت این متغیرها و تأثیرات بالقوه آنها بر محیط کاری، برای میریت بسیار مهم است. به همین خاطر، مدیران پروژه باید با مدیران ارشد تعامل مثبت داشته باشند تا فضای سازمانی مناسبی برای عملکرد نو آورانه تیمی بوجود آید

5.4 ابزار های بنگاه برای مدیریت ریسک

بسیاری از شرکت ها، تحت فشار رقابت و پیشرفت تکنولوژی اطلاعات، سرمایه گذاری سنگینی در فنون کنترل پروژه کرده اند تا با افزایش توان مواجهه خود با حوادث پیش بینی نشده، بتواند احتمال موفقیت پروژه های IT را افزایش دهند. هر چند رویکرد های تحلیلی، کماکان جایگاه مهم و عمده ای در مدیریت ریسک پروژه های IT دارند. اما عمدتاً از آنها برای کمی سازی احتمالات ریسک و تبدیل این احتمالات به پارامتر های زمانی و بودجه ای خاص استفاده می شود. با این وجود، بکارگیری بسیاری از روش های تحلیلی، با این پیش فرض صورت می گیرد که ریسک و عوامل مسبب آنها را می توان در طول چرخه عمر پروژه بصورت کمی پیش بینی کرد.

5.5 دسته بندی رویکرد های مدیریت ریسک در پروژه های IT

با دسته بندی رویکرد های مدیریت ریسک برای توسعه پروژه های IT به پنج گروه مختلف می توان چارچوب مناسبی برای پروژه های IT بدست آورد.

1-شناسایی و مدیریت عوامل ریسک: نمونه چنین رویکردی، پیش بینی تغییر انتظارات، شرایط تکنولوژی است. اگر امکان پذیری وقوع این تغییرات مشخص شود، احتمال وقوع و میزان تأثیر آن ها قابل ارزیابی است. بنابراین می توان منابع احتیاطی برای کاهش اثرات آنها کنار گذاشت. در چنین مواردی سناریوهای ریسک شناخته شده اند و می توان با انجام اقدامات پیشگیرانه اثرات مخرب در زمان وقوع خطر را به حداقل رساند.

2-پیاده سازی محصول و طرح آن: هر گونه نوآوری که باعث کاهش پیچیدگی، زمان توسعه، منابع لازم، تجهیزات لازم تولید و مونتاژ شود به نوبه خود وقوع حوادث خطرناک را در طول چرخه توسعه نیز کاهش می دهند.

3-ساده سازی فرایند توسعه: در این ارتباط می توان به مثالهایی همچون نوآوری در فرایند کار یا میریت پروژه اشاره کرد. تمامی این سیستم ها به منظور تقویت هماهنگی و ایجاد اتحاد میان تیم پروژه و سازمان میزبان طراحی شده اند.

4-کاهش زمان توسعه پروژه: این کار از طریق ساده سازی پروژه و فرایند قابل حصول است. اما فعالیت های توسعه ای موازی نیز می تواند نیز به تحقق ایت هدف کمک کند. هرچه چرخه عمر توسعه پروژه کوتاهتر باشد، تغییرات و حوادث پیش بینی نشده کمتری در توسعه پروژه و زیر سیستم های اجتماعی و تکنولوژیکی آن رخ می دهد.

5-بررسی زود هنگام امکان پذیری پروژه: در گذشته بررسی های بسیار مهم که اعتبار پروژه را نشان می داد، معمولاً در اواخر چرخه توسعه انجام می شد. اما امروزه با پیشرفت IT، می توان این بررسی ها را در همان مراحل اولیه توسعه پروژه انجام داد.

5.6 معیارهای موفق مدیریت ریسک در عرصه تکنولوژی

بر خلاف پیچیدگی فرایند توسعه پروژه های IT و عدم قطعیت های گریز ناپذیر چرخه توسعه ریسک شکست پروژه نه تنها اتفاقی نیست، بلکه قابل مدیریت است. مشاهدات نشان می دهد که مواجهه با ریسک پروژه های IT از سه طریق امکان پذیر است که مدیریت ریسک پروژه های IT در هر کدام از این سه بخش تا حدی امکان پذیر است.

1- کار و فرایند کار

2- ابزار ها و روش های تحلیلی

3- افراد

چکیده نکات کلیدی و مهمی که در این فصل به تفسیر آنها پرداختیم :

ریسک زمانی در پروژه های IT مطرح است که پای عدم قطعیت در میان باشد و همین عدم قطعیت بتواند اثر نامطلوبی بر عملکرد و فعالیت پروژه بر جای بگذارد ریشه بسیاری از ریسکهای پروژه را می توان در پویایی پروژه و ماهیت فرارشته ای محیط کسب و کار نوین جویا شد. مدیریت ریسک در پروژه های IT صرف موضوعاتی همچون زمانبندی و بودجه می شود. مدیران موفق از صرف شناسایی ابزارها و فنون مدیریت ریسک فراتر می روند. آنها پویایی پروژه را درک می کنند و از عهده مواجهه با مسائل پیچیده ای اجتماعی، فنی و اقتصادی بر می آیند.

6. نتیجه گیری و بحث:

تعریف ریسک پروژه فعالیتی بی ارزش است مگر آنکه ریسک ها در طول پروژه مدیریت شود- همچنین برای رفع مسایل و مخاطرات پروژه باید ساز و کارهایی وجود داشته باشد- مدیریت ریسک فرآیندی است که باید با شروع پروژه آغاز شود و تا تکمیل و خاتمه پروژه ادامه یابد- اگر قبل از تحویل پروژه تغییرات لازم در سازمان انجام نشود. احتمال بسیار است که ورود سیستم های IT به سازمان در ارائه هر گونه منافع با شکست مواجه شود. همانطور که بررسی شد برای مدیریت ریسک در پروژه های IT لازم است از چارچوب مناسب استفاده شود. این چارچوب مدیران پروژه را در کاهش اثر پذیری از ریسک بسیار کمک کند، برای استفاده از این چارچوب نیاز به ابزارهایی است که هر مدیری از ابزار و روش خاص بهره می گیرد- از آنجا که پروژه های IT زمان برو پر هزینه اند، و نرخ بالای شکست پروژه های IT موجب شده که سازمان ها توجه بیشتری به ریسک های موجود در این پروژه ها داشته باشند

اگر مدیران، قوی و با تجربه باشند و از همان آغاز پروژه ریسک‌ها را مشاهده شده قبل و حین اجرای پروژه‌های IT بررسی کنند و بتوانند روش‌هایی را بیابند که بتوانند آنها را پیگیری کنند، که در این صورت می‌توان گفت مدیریت ریسک می‌تواند سبب موفقیت پروژه‌های IT شود و در غیر اینصورت امکان پذیر نیست.

7. منابع:

1. David L.Olson and McGraw-Hill. 'Introduction to information system management' 2004

2.J.H.M. TAH, V. CARR. Information modelling for a construction project risk management system

3.Jack T Marchewka.() 'Information technology project management'. 2003.

4. www.donya.Egtesad.com

5.www.modir.ir/articles/1009.aspx

6.<http://www.civilica.com/pager-ipmco.116.html>

7.<http://journals.ut.ac.ir>

8. دیوید، فردار، مدیریت استراتژیک، ترجمه دکتر علی پارسائیان.

9. سی آر تور ویلیامز، جی آر-مدیریت ریسک مترجمان: داور ونوس، حجت الله گودرزی.

10. محمدی نوده، عبدالرحمن، نقش فناوری اطلاعات در مدیریت ریسک آی تی ایران

11.Julean self, Risk Management Guide

12.Grawboskim, K.H. Roberts. Risk monitoring in virtual organizations.

13.www.intel.com/products

14. سیستم‌های اطلاعاتی مدیریت پیشرفته-دکتر هوشنگ مؤمن

15. راهنمای مدیران فناوری اطلاعات-بیل هولش نایدر-ترجمه دکتر رضا منصفی

16.Barlett, J. (2002) Risk concept Mapping

www.markazdanesh.ir