مدیریت ریسک در سیستمهای فناوری اطلاعات

نیلوفر ظهوریان فولادی[1]

مقدمه

مدیریت ریسک رویکردی است که به شناسایی و ارزیابی ریسک و انجام اقداماتی برای کاهش آن تا سطح قابل قبول می پردازد. عمده ترین هدف سازمانها در بکارگیری مدیریت ریسک، کاهش تاثیرات منفی و نیاز به زیربنایی محکم در تصمیم گیری های سازمانی می باشد. مدیریت ریسک دارای نقش کلیدی در حفظ اطلاعات شرکت است. فرآیند تاثیرگذار مدیریت ریسک، مولفه اصلی در برنامه امنیت فناوری اطلاعات به شمار می آید. هدف عمده و اساسی فرآیند مدیریت ریسک سیستمهای فناوری اطلاعات، تنها به پشتیبانی از سیستمهای فناوری اطلاعات خلاصه نمی شود بلکه حمایت از شرکت و پشتیبانی از اجرای ماموریتهای آن را نیز در بر می گیرد. بنابراین، فرآیند مدیریت ریسک را نباید تنها به عنوان فعالیتی فنی که توسط متخصصان سیستمهای فناوری اطلاعات انجام می شود، لحاظ کرد بلکه نیازمند اعمال مدیریت از جانب مدیران اصلی شرکت یا سازمان می باشد. مقصود از مدیریت ریسک، توانمندسازی سازمانها در انجام ماموریتها و اهدافشان ضمن حفظ اطلاعات، بودجه، رویکردها و سیستمهای فناوری اطلاعات می باشد. در این مقاله، راهکاری مناسب در خصوص مدیریت ریسک سیستمهای فناوری اطلاعات ارائه شده است تا به سازمانها در اداره بهینه و موثر سیستمهای فناوری اطلاعات کمک نماید[2]. مدیریت ریسک به مدیران فناوری اطلاعات در ایجاد توازن در هزینه های اقتصادی و عملیاتی فناوری اطلاعات کمک کرده و باعث می شود تا سیستمهای فناوری اطلاعات در حمایت از ماموریت سازمان موفق عمل نمایند.

نگاهی اجمالی به مدیریت ریسک

چرخه حیات سیستمهای فناوری اطلاعات دارای پنج مرحله راه اندازی، فرآگیری و توسعه، اجرا، زمان عملیات یا تعمیر و نگهداری و زمان انقضا می باشد. در برخی از سیستمهای فناوری اطلاعات، ممکن است چند

---

[1] – دانشجوی کارشناس ارشد آموزش زبان روسی و کارشناس شرکت بیمه ملت.

[2] – این راهکار از شماره مخصوص مجله موسسه ملی استاندارد و تکنولوژی (National Institute of Standards and Technology – NIST) با نام اصول مهندسی در امنیت سیستهمای فناوری اطلاعات (Engineering Principles for IT Security) اقتباس شده است.

مرحله به صورت همزمان انجام شوند، با این وجود روش تحلیل مدیریت ریسک، به این مراحل توجهی نداشته و در هر مرحله قابل اجرا می باشد. جدول ۱ خصوصیات مراحل چرخه سیستم فناوری اطلاعات و نحوه مدیریت ریسک در آنها را نشان می دهد. لازم به ذکر است موارد اجرایی تنها توسط متخصصان بخش فناوری اطلاعات انجام نگرفته و لازم است تا تمامی مسئولان اعم از مدیران ارشد، مدیران اطلاعات، صاحبان سیستم و اطلاعات، مدیران کسب و کار و عملیاتی، ارائه دهندگان ایزو، متصدیان امر امنیت فناوری اطلاعات و متخصصان بخش امنیت در این خصوص به فعالیت بپردازند.

۱- ارزیابی ریسک

ارزیابی ریسک اولین مرحله در روش تحلیل مدیریت ریسک می باشد. سازمانها با ارزیابی ریسک به تعیین دامنه تهدیدات بالقوه و ریسکهای موجود در سیستم فناوری اطلاعات در چرخه زندگی شان می پردازند. در نتیجه این مرحله باعث می شود تا نظارت صحیح انجام گرفته و معیارهای مناسب برای کاهش و حذف ریسک در مرحله تخفیف ریسک شناسایی و تعیین شوند.

برای تعیین احتمالات در بروز حوادث نامساعد، لازم است تا تهدیدات سیستم فناوری اطلاعات در تقارن با آسیب های بالقوه و ابزارهای مکانی سیستمهای فناوری ارتباطات مورد بررسی قرار گیرند. روش تحلیل مدیریت ریسک در ۹ مرحله خلاصه می شود که به اختصار به توضیح هر یک از آنها می پردازیم.

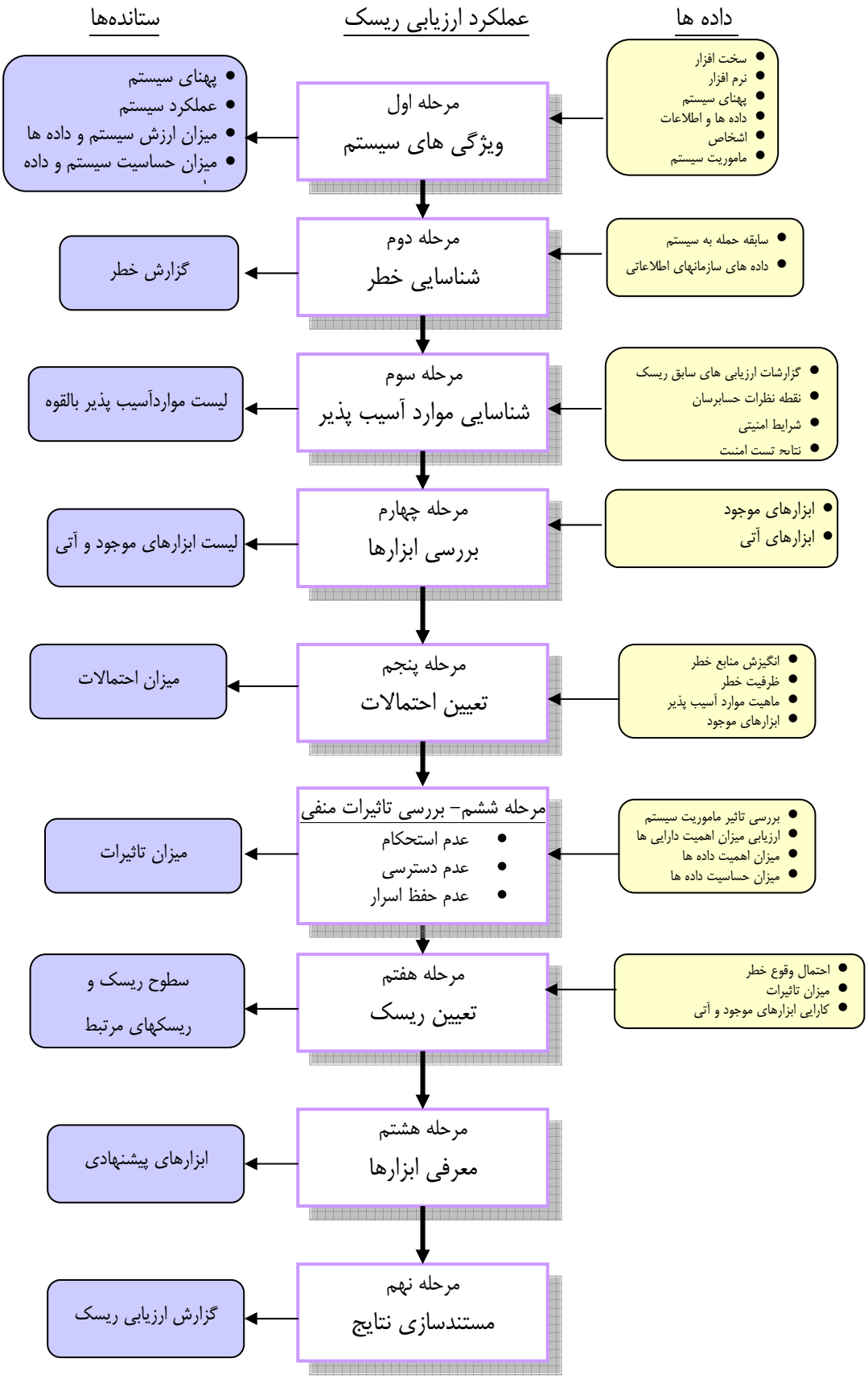
- مرحله اول- ویژگی های سیستم
- مرحله دوم- شناسایی خطر
- مرحله سوم- شناسایی موارد آسیب پذیر
- مرحله چهارم- بررسی ابزارها(آنالیز ابزارها)
- مرحله پنجم- تعیین احتمالات
- مرحله ششم- بررسی تاثیرات منفی(آنالیز تاثیرات)
- مرحله هفتم – تعیین ریسک
- مرحله هشتم- معرفی ابزارها(توصیه‌های کنترل)
- مرحله نهم- مستندسازی نتایج

مراحل دوم، سوم، چهارم و ششم را می توان به صورت همزمان و پس از اتمام مرحله اول انجام داد.

جدول ۱ – یکپارچگی مدیریت ریسک درون چرخه سیستمهای فناوری اطلاعات

مراحل چرخه سیستمهای فناوری اطلاعات	خصوصیات مرحله	عملکرد مدیریت ریسک
مرحله اول – راه اندازی	نیاز به سیستم فناوری اطلاعات اعلام و هدف و محدوده این سیستمها مستند می شوند.	ریسکهای شناسائی شده برای پشتیبانی از نیازهای سیستم شامل امنیت و جنبه های امنیتی عملیات، بکار می رود.
مرحله دوم – فرآگیری و توسعه	سیستم فناوری اطلاعات طراحی، خریداری، برنامه ریزی و تدوین می شود.	ریسکهای شناسایی شده در طول مدت این دوره برای پشتیبانی از بررسیهای ایمنی سیستمهای فناوری اطلاعات که برای برنامه ریزی و تدوین استفاده می شوند، بکار می‌روند.
مرحله سوم – اجرا	جوانب امنیتی سیستم ایجاد، قابل اجرا، ارزیابی و تایید می شوند.	عملکرد مدیریت ریسک به پشتیبانی از ارزیابی کارکرد سیستمها در محیط عملیاتی می پردازد. تصمیمات مربوط به شناسایی ریسک می بایست قبل از شروع عملیات سیستم اتخاذ شوند.
مرحله چهارم– اجرا یا نگهداری	سیستم، عملکرد خود را آغاز کرده و با کمک نرم افزارها و سخت افزارهای اضافی و با انجام تغییراتی با سیاستها و اهداف شرکت سازگار می شود.	عملکرد مدیریت ریسک برای صدور مجدد مجوز یا اعطای مجدد اعتبار به سیستم چرخه ای یا هنگام اعمال تغییرات عمده در محیط عملیاتی قابل اجراست.
مرحله پنجم– زمان انقضا	در این مرحله اطلاعات، نرم افزارها و سخت افزارها سازماندهی شده و فعالیتها در صورت نیاز مشمول جابجایی، بایگانی، تخلیه یا انهدام اطلاعات یا پاکسازی نرم افزارها و سخت افزارها می شوند.	عملکرد مدیریت ریسک برای اطمینان از مواردی نظیر مولفه های غیرقابل استفاده سیستم ، نرم افزارها و سخت افزارهای جایگزین یا اطمینان از مناسب بودن اطلاعات و روش کار سیستم کاربرد دارد.

شکل ۱- نمودار فرآیندی روش ارزیابی ریسک



- مرحله اول: ویژگی های سیستم

تعیین محدوده فعالیت، اولین گام در ارزیابی ریسک سیستمهای فناوری اطلاعات می باشد. در این مرحله محدوده عملیاتی سیستم فناوری اطلاعات، منابع و اطلاعات موجود در سیستم مشخص خواهند شد. با تعیین ویژگی های سیستم، محدوده فعالیت در ارزیابی ریسک مشخص شده، حدود اختیارات عملیاتی ترسیم شده و اطلاعات ضروری مربوط به شناسایی ریسک تهیه می شوند. برای شناسایی ریسک سیستمهای فناوری اطلاعات، به درک بسیار بالایی در مورد محیط پردازش سیستم احتیاج است. افرادی که در زمینه ارزیابی ریسک فعالیت می کنند، می بایست اطلاعات مرتبط با سیستم که شامل سخت افزار، نرم افزار، پهنای سیستم، داده ها و اطلاعات، کاربران و افراد پشتیبان سیستم فناوری اطلاعات، نوع ماموریت سیستم، میزان ارزش سیستم و داده ها، میزان حساسیت سیستم و داده ها می باشد را جمع آوری نمایند. علاوه بر موارد فوق الذکر اطلاعات مرتبط دیگری نیز وجود دارند که به برخی از آنها اشاره می کنیم:

- شرایط عملکرد سیستم فناوری اطلاعات
- کاربران سیستم
- سیاستهای امنیتی مرتبط با سیستم فناوری اطلاعات
- ساختار امنیتی سیستم
- بررسی شبکه موجود
- محل حفظ اطلاعات که دسترسی، سلامت و حفظ اسرار سیستم و داده ها را تضمین می کند.
- معیارهای تکنیکی مورد استفاده در سیستم فناوری اطلاعات
- معیارهای مدیریتی مورد استفاده در سیستم فناوری اطلاعات
- معیارهای عملیاتی مورد استفاده در سیستم فناوری اطلاعات
- محیط امنیتی فیزیکی در سیستم فناوری اطلاعات

در سیستمهایی که در مرحله ابتدایی قرار دارند، سیستم اطلاعاتی از مدارک تدوین شده مشتق می شوند؛ سیستم فناوری اطلاعات که در مرحله توسعه قرار دارد به قوانین امنیتی کلیدی و شاخصهای مربوط به سیستم فناوری اطلاعات نیاز دارد. مدارک طراحی سیستم و برنامه امنیت سیستم، اطلاعات مفیدی در مورد امنیت سیستم فناوری اطلاعات را در خود جای داده اند. در زمان کار سیستم و در مرحله عملیات، اطلاعات مربوط به سیستم از محیط محصولات سیستم شامل داده ها در مورد وضعیت کلی، ارتباطات، مراحل مستند و غیر مستند بدست می آیند.تهیه

پرسشنامه، گفتگو با متخصصان در محل نصب سیستم، بازبینی مدارک و استفاده از ابزارهای خودکار دقیق بررسی، از راههای جمع آوری اطلاعات می باشند.

- مرحله دوم: شناسایی خطر

خطر، تهدید بالقوه ای است که می تواند باعث صدمه به موارد آسیب پذیر گردد. در این مرحله، هدف اصلی شناسایی منابع خطر و گردآوری گزارش شامل لیستی از منابع مرتبط با سیستم فناوری اطلاعات می باشد. منابع خطر، شرایط یا موقعیتهای بالقوه ای هستند که باعث ایجاد صدمه به سیستمهای فناوری اطلاعات می شوند. طبیعت، محیط و انسان از جمله منابع خطر به شمار می آیند. در ارزیابی منابع خطر، تمامی منابع بالقوه که به سیستمها آسیب می رسانند می بایست مد نظر قرار گیرند.

گزارش خطر یا لیست منابع خطر می بایست با ساختار سازمان و محیط پردازش آن متناسب باشد. اطلاعات مربوط به خطرات طبیعی می بایست در هر زمان و به آسانی در دسترس قرار گیرند.

- **خطرات طبیعی- طوفان، زلزله، گردباد، ریزش کوه، بهمن، رعد و برق وغیره**
- **خطرات انسانی – اعمالی که توسط انسانها انجام می گیرد، مانند کارهای غیرعمد (ثبت داده ها به صورت اشتباه) یا عمدی (حمله به شبکه، دسترسی غیرمجاز به اطلاعات سری، اعمال خصمانه)**
- **خطرات محیطی – خرابی های طولانی مدت در انرژی، آلودگی، مواد شیمیایی، نشت مایعات)**

- مرحله سوم: شناسایی موارد آسیب پذیر

در بررسی خطرات احتمالی وارد بر سیستم فناوری اطلاعات، لازم است تا به بررسی موارد آسیب پذیر موجود در سیستم نیز پرداخته شود. هدف از این مرحله تهیه لیستی شامل سیستم های آسیب پذیر می باشد. روش پیشنهادی برای شناسایی سیستمهای آسیب پذیر، استفاده از منابع آسیب پذیر، انجام آزمایشات امنیت سیستم، و تهیه فهرستی در مورد شرایط امنیتی می باشد. لازم به ذکر است که تعداد موارد آسیب پذیر در سیستم فناوری اطلاعات به ماهیت سیستم فناوری اطلاعات و مرحله ای که سیستم در آن قرار دارد، بستگی دارد:

- هنگامی که سیستم در مرحله ابتدایی قرار دارد، شناسایی موارد آسیب پذیر با تمرکز بر سیاستهای امنیتی سازمان، مراحل طرح ریزی شده امنیتی و بررسی نتایج کارهای امنیتی امکان پذیر است.

- هنگامی که سیستم در مرحله اجرا است، شناسایی موارد آسیب پذیر می بایست اطلاعات جزئی تری را در بر گیرد. مانند جنبه های مختلف امنیتی که در مدارک سازمان به آنها اشاره شده است و نیز نتایج آزمایشات و ارزیابی های استاندارد در مورد سیستم.
- هنگامی که سیستم در مرحله عملیات و تعمیر و نگهداری قرار دارد، روند شناسایی بررسی جنبه های مختلف امنیتی سیستم فناوری اطلاعات، ابزارهای امنیتی و موارد تکنیکی محافظ سیستم را در بر می گیرد.

آزمایش امنیت سیستم از طریق سه روش انجام می گیرد.

۱- ابزارهای کنترل دقیق اجزای آسیب پذیر سیستم

۲- آزمایش و ارزیابی امنیت

۳- آزمایش نفوذ

در روش اول، شبکه به منظور شناسایی اجزا آسیب پذیر به دقت مورد بررسی قرار می گیرد. با این وجود در این روش نمی توان تمامی اجزا آسیب پذیر بالقوه درشبکه را شناسایی کرد یا ممکن است اجزایی در ماهیت اصلی خود آسیب پذیر نباشند ولی با قرار گرفتن در محیطی خاص به این عنوان شناخته شوند. در روش دوم، موارد آسیب پذیر موجود در سیستم، در طی مرحله ارزیابی ریسک، شناسایی می شوند. هدف از این آزمایش، بررسی میزان تاثیر ابزارها بر سیستم فناوری اطلاعات و اطمینان از حفظ امنیت سخت افزارها و نرم افزارها در محیط عملیاتی و مطابق با استانداردهای صنعتی است. آزمایش نفوذ، بررسی ابزارها را کامل کرده و از امنیت اجزا مختلف سیستم اطمینان حاصل می نماید. هنگامی که از این آزمایش در روند ارزیابی ریسک استفاده می شود توانایی مقاومت سیستم فناوری اطلاعات در تلاشهای داخلی برای احاطه امنیت سیستم ارزیابی می شوند. هدف از انجام این روش، آزمایش سیستم فناوری اطلاعات از نقطه نظر منابع خطر و شناسایی نقاط ضعف طرح حفظ امنیت سیستم می باشد.

تهیه لیست از موارد امنیتی وظیفه ای است که بر عهده سه حوزه مدیریت، عملیاتی و فنی می باشد. جدول ۲ موارد مهم امنیتی مربوط به هرحوزه را مشخص کرده است.

جدول ۲ – ضوابط ایمنی

محدوده ایمنی	ضوابط ایمنی
ایمنی مدیریت	• تعیین مسئولیتها • تداوم در پشتیبانی • مسئولیت واکنش در برابر پیشامدهای ناگوار • بررسی دوره ای ابزارهای امنیتی • تایید صلاحت و عدم سوء پیشینه کارکنان • ارزیابی ریسک • آموزش های امنیتی و فنی • تقسیم وظایف • صدور مجوز برای سیستم • برنامه امنیتی سیستم و کاربرد آن
ایمنی عملیاتی	• کنترل آلاینده های هوا • کنترل و ایجاد اطمینان از کیفیت تامین کننده های برق • دسترسی به داده های رسانه ها و اداره آنها • پخش داده های خارجی و رده بندی آنها • حفظ امنیت تاسیسات • کنترل رطوبت • کنترل دما • کامپیوترهای شخصی، لپ تاپ و کامپیوترهای واقع در سایت
ایمنی فنی	• سیستم ارتباطی • رمز نویسی • کنترل دسترسی اختیاری • شناسایی و تایید • شناسایی مزاحمتها • استعمال مجدد از وسایل • بررسی دقیق سیستم

- مرحله چهارم: بررسی ابزارها

هدف از این مرحله، تجزیه و تحلیل ابزارهایی است که توسط سازمان برای کاهش یا حذف احتمال بروز خطر بکارگرفته شده یا در آینده از آنها استفاده خواهد شد. برای پی بردن به میزان احتمال وقوع خطر در اجزای آسیب پذیر سیستم، لازم است تا عملکرد ابزارهای موجود و آتی مورد توجه قرار گیرند. روشهای کنترل شامل دو گروه فنی و غیر فنی می شوند. ابزارهای فنی به عنوان محافظهایی به سخت افزار، نرم افزار و سفت افزار های کامپیوتر مربوط می شوند. ابزارهای غیر فنی، همان ابزارهای مدیریتی و عملیاتی هستند که می توان به مواردی چون آیین نامه های ایمنی، مراحل عملیاتی، ایمنی محیط، کارمندان و دستگاهها اشاره کرد.

ابزارهای کنترل در قسمت فنی و غیر فنی به دو گروه بازدارنده یا کاشف تقسیم بندی می شوند. این ابزارها به شرح زیر هستند:

- ابزارهای بازدارنده با استفاده از روشهایی نظیر کدگذاری و غیره از هر نوع اقدام برای تجاوز خطمشی ایمنی سازمان جلوگیری می کنند.
- ابزارهای کاشف، انجام یا تلاش برای انجام تخلف را خطمشی ایمنی سازمان هشدار داده و شامل ابزارهایی نظیر ابزارهای ردگیری، روشهای کشف مزاحمت و غیره می باشند.

- مرحله پنجم: تعیین احتمالات

برای تعیین احتمال وقوع حادثه در سیستمهای آسیب پذیر، توجه به عوامل زیر دارای اهمیت می باشد:

- توانایی و انگیزه منابع خطر
- ماهیت موارد آسیب پذیر
- وجود و کارائی ابزارهای موجود

احتمال وقوع حادثه به موارد آسیب پذیر در سیستم ، به سه سطح زیاد، متوسط و کم تقسیم می شود. جدول ۳ سطوح این احتمال را توصیف می‌نماید.

جدول ۳ – تعاریف احتمال

سطح احتمال	تعریف احتمال
زیاد	منبع خطر دارای قابلیت و انگیزه فراوان است و ابزارهای مدافع بی تاثیر هستند.
متوسط	منبع خطر دارای قابلیت و انگیزه می باشد ولی ابزارها ممکن است در دفع خطرات موفق عمل نمایند.
کم	منبع خطر قابلیت و انگیزه چندانی ندارد یا ابزار به صورت کامل خطر را دفع کرده یا در مکان مناسبی برای دفع خطر قرار دارند.

- مرحله ششم: آنالیز تاثیرات

بزرگترین گام در اندازه گیری سطح ریسک، تعیین تاثیرات منفی در شناسایی موارد آسیب پذیر می‌باشد. قبل از بررسی و تجزیه و تحلیل تاثیرات، لازم است تا اطلاعات ضروری زیر را بدست آوریم:

- ماموریت سیستم (به عنوان مثال روندی که سیستم فناوری اطلاعات دنبال می کند.)
- درجه اهمیت سیستم و داده‌ها(به عنوان مثال ارزش سیستم یا اهمیت آن برای سازمان)
- میزان حساسیت سیستم و داده‌ها

این اطلاعات را می توان از مستندات سازمان تهیه نمود. در صورت عدم وجود مستندات، میزان حساسیت سیستم و داده ها را می توان بنا بر درجه اهمیت حفظ ایمنی آنها تشخیص داد.

بنابراین تاثیرات منفی موارد ایمنی را می توان با عنوان عدم وجود یا افت این موارد توضیح داد. سلامت سیستم، دسترسی و حفظ موارد محرمانه آن سه عامل اصلی در حفظ ایمنی می باشند و نبود یکی از آنها باعث بروز تاثیرات منفی خواهد شد.

- عدم سلامت: سلامت سیستم و داده ها به پیش شرطهایی مربوط می شود که اطلاعات را در برابر اصلاحات نامناسب محفوظ می دارد. در صورت اعمال تغییرات بدون مجوز، در داده ها یا سیستم فناوری اطلاعات به طور عمدی یا غیر عمدی، سلامت سیستم از بین خواهد رفت. در حالتی که این نقص برطرف نشده و از سیستم یا داده ها استفاده شود، این عمل می تواند منجر به کلاهبرداری یا اخذ تصمیمات خطا و اشتباه گردد. همچنین عدم حفظ سلامت سیستم، اولین خطر در بروز حملات

و افشای اطلاعات خواهد بود. بنا بر دلایل ذکر شده، عدم سلامت سیستم، باعث کاهش اطمینان از امنیت سیستم فناوری اطلاعات می شود.

- عدم دسترسی: در صورتیکه ماموریت حیاتی سیستم فناوری اطلاعات برای آخرین کاربران قابل اجرا نباشد، این کمبود بر ماموریت کلی شرکت نیز تاثیر می گذارد. به عنوان مثال، عدم عملکرد مناسب و تاثیر اندک سیستم ممکن است به کاهش زمان موثر منجر شده و در نتیجه کاربران نهایی که در جهت دستیابی به اهداف شرکت تلاش می کنند، قادر به دریافت خدمات سیستم فناوری اطلاعات نخواهند بود.
- عدم حفظ اسرار: اسرار سیستم و داده ها به حفظ و مراقبت از اطلاعات در برابر افشای بدون اجازه آنها مربوط می شود. افشای اطلاعات محرمانه می تواند باعث به خطر انداختن ایمنی ملی و نیز افشای قوانین محرمانه گردد. افشای اینگونه اطلاعات، موجب سلب اعتماد عمومی، آشفتگی و انجام اقدامات قانونی علیه سازمان شود.

برخی از تاثیرات منفی را می توان با پرداخت جریمه یا هزینه تعمیر سیستم جبران نمود لیکن آن دسته از تاثیراتی که قابل اندازه‌گیری نیستندبه سه گروه تاثیر شدید، تاثیر متوسط و تاثیر کم دسته بندی کرده ایم (جدول ۴).

جدول ۴- تعریف میزان تاثیرات

میزان تاثیر	تعریف تاثیر
شدید	ایجاد صدمه به موارد آسیب پذیر ممکن است: ۱- موجب خسارت سنگین و غیرقابل بازگشت به داراییها و منابع شود؛ ۲- به طور جدی به ماموریت، اعتبار، شهرت و منافع سازمان آسیب رساند؛ ۳- باعث مرگ افراد یا جراحات جدی شود.
متوسط	ایجاد صدمه به موارد آسیب پذیر ممکن است: ۱- موجب خسارت به داراییها و منابع شود؛ ۲- به گونه ای به اعتبار، شهرت و منافع سازمان آسیب رساند؛ ۳- باعث بروز جراحات گردد.
کم	ایجاد صدمه به موارد آسیب پذیر ممکن است: ۱- موجب خسارت به بعضی از داراییها یا منابع شود؛ ۲- به صورت محسوس بر ماموریت، اعتبار و منافع سازمان تاثیر گذارد.

- مرحله هفتم: تعیین ریسک

هدف از این مرحله، ارزیابی سطح ریسک در سیستمهای فناوری اطلاعات می باشد. برای محاسبه ریسک لازم است تا از مقیاس ریسک و ماتریکس اندازه ریسک استفاده شود. تعیین نهایی ریسک از ضرب اندازه احتمال خطر در تاثیر

خطر بدست می آید. جدول ۵ تعیین مقدار ریسک را با استفاده از ماتریس ۳×۳ نشان می دهد. داده های این ماتریس اندازه احتمال خطر (زیاد، متوسط، کم) و میزان تاثیرات منفی (شدید، متوسط و کم) می باشند. شایان ذکر است که این ماتریس را می توان به ماتریس ۴×۴ یا ۵×۵ نیز بسط داد و البته این مسئله به بزرگی سایت و حجم فعالیت سازمان بستگی دارد در این صورت می توان متغیرهای بسیار زیاد یا بسیار کم را نیز به احتمال خطر و میزان تاثیرات اضافه نمود. تعیین ریسکها یا اندازه ها به صورت تحلیلی است.

جدول ۵- ماتریس اندازه ریسک

احتمال خطر	میزان تاثیرات		
	کم (۱۰)	متوسط (۵۰)	شدید (۱۰۰)
زیاد (۱,۰)	کم ۱۰ ×۱,۰ = ۱۰	متوسط ۵۰ × ۱,۰ = ۵۰	زیاد ۱۰۰ × ۱,۰ = ۱۰۰
متوسط (۰,۵)	کم ۱۰ × ۰,۵ = ۵	متوسط ۵۰ × ۰,۵ = ۲۵	متوسط ۱۰۰ × ۰,۵ = ۵۰
کم (۰,۱)	کم ۱۰ × ۰,۱ = ۱	کم ۵۰ × ۰,۱ = ۵	کم ۱۰۰× ۰,۱ = ۱۰

جدول ۶ به شرح هر یک سطوح ریسک در ماتریس فوق پرداخته و با توجه به آن مدیر ارشد و مسئولان مرتبط با سیستم فناوری اطلاعات می بایست به انجام اقداماتی بپردازند.

جدول ۶- مقیاس ریسک و اقدامات ضروری

سطح ریسک	تفسیر ریسک و اقدامات ضروری
زیاد	در صورتیکه نتیجه مشاهدات، ریسک زیاد را نشان داد، لازم است تا اقدامات ضروری برای اصلاح اشتباهات انجام گیرند. ممکن است سیستم موجود به فعالیت خود ادامه دهد ولی بدیهی است که موارد اصلاحی می بایست هر چه سریعتر جایگزین شوند.
متوسط	در صورتیکه نتیجه مشاهدات، ریسک متوسط را نشان داد، لازم است تا در زمان مناسب اقدامات اصلاحی و برنامه ریزی های جدید اعمال شوند.
کم	در صورتیکه نتیجه مشاهدات، ریسک کم را نشان داد، لازم است تا مشخص شود که اقدامات اصلاحی نیاز است یا پذیرش ریسک بلامانع است.

- مرحله هشتم: توصیه‌های کنترل

در این مرحله ابزارهای مناسب برای کاهش یا حذف ریسک معرفی می شوند. هدف از کنترلهای توصیه شده، کاهش سطح ریسک در سیستم های فناوری اطلاعات و داده های آنها تا حد قابل قبول است. در توصیه ابزارها، مولفه های زیر می بایست مد نظر قرار گیرند:

- کارائی ابزارهای پیشنهادی
- قوانین و مقررات
- سیاست شرکت
- تاثیر عملیات
- ایمنی و قابلیت اطمینان

توصیه‌های کنترل، نتیجه بررسی ریسک می باشد و اطلاعاتی را برای کاهش ریسک در اختیار قرار می دهد. شایان ذکر است که تمامی ابزارهای پیشنهادی قابلیت کاهش خسارت را نداشته و بنابر نوع نیاز و اهداف سازمان متفاوت می باشند. برای کاهش ریسک ترکیب انواع ابزارها اعم از ابزارهای ایمنی فنی، ابزارهای ایمنی مدیریت، ابزارهای ایمنی عملیات مطابق با نیاز سازمان ضروری است. در ادامه به تشریح هر یک از این ابزارها می پردازیم:

- ابزارهای ایمنی فنی: این ابزارها شامل ابزارهای فنی حمایتی، ابزارهای فنی بازدارنده و ابزارهای فنی کاشف، برای محافظت سیستم در مقابل انواع خطرات کاربرد داشته و ترکیبی از نرم افزارها، سخت افزارها و سفت افزارها می باشد. هدف اصلی این ابزارها حمایت از سیستم، پیشگیری از وقوع خطر و کشف خطرات است. ابزارهای فنی حمایتی شامل ابزارهایی شناسایی، ابزارهای رمز گشا و ابزارهای ایمنی اجرا می باشند. ابزارهای شناسایی، منابع اطلاعاتی، کاربران و پردازشگرها را شناسایی می کنند. ابزارهای ایمنی اجرا، نصب صحیح و اجرای درست سیستمهای فناوری اطلاعات را کنترل می کنند. ابزارهای فنی بازدارنده، هویت کاربران (درخواست شناسه کاربری و رمز) را کنترل کرده، به کاربران برای استفاده مشترک از سیستمها مجوز داده، دسترسی به اطلاعات را ممکن ساخته، ایمنی اطلاعات رد و بدل شده را ضمن حفظ آدرس مبدا و مقصد تایید کرده، ایمنی سیستم را حفظ کرده و از افشای اطلاعات حین انتقال آنها جلوگیری می کنند. ابزارهای فنی کاشف موارد تخلف یا در شرف آن را گزارش می دهند. این ابزارها شامل ابزارهای بررسی و نظارت بر وقایع قبل و بعد از بروز خطر، ابزارهای کشف و جلوگیری از مزاحمت، ابزارهای تایید سلامت سیستم، ابزارهای کشف و انهدام ویروس و در نهایت ابزاری که سیستم را به شرایط ایمنی گذشته باز می گرداند، می باشند.

- ابزارهای ایمنی مدیریت: ابزارهای مدیریتی در تلفیق با ابزارهای فنی و عملیاتی برای کاهش ریسک و حفظ ایمنی سیستم کاربرد دارند. این ابزارها بر سیاست حفظ اطلاعات، دستورالعملها و استانداردها نظارت دارد.
- ابزارهای ایمنی عملیات: استانداردهای ایمنی سازمان، لیست ابزارها و دستورالعملهایی که برای استفاده سازمان در سیستمهای فناوری اطلاعات لازم است را تهیه می کنند. نظارت بر اجرای این دستورالعملها و اطمینان از نصب ابزارهای مناسب عملیاتی از وظایف مهم بخش مدیریت می باشد. برای اطمینان از ایمنی عملیات، لازم است تا ابزارهای عملیات به وضوح تعیین، ثبت و نگهداری شوند. این ابزارها شامل ابزار دسترسی به داده های رسانه ها، ابزار استفاده محدود ازداده های خارجی، ابزارهای کنترل ویروسهای نرم افزار، ابزارهای تعیین سیستمهای امنیتی، مکانهای نگهداری کابلها، تامین توانایی گرفتن ذخیره اطلاعات، حفاظت از لب تاپها، کامپیوترهای شخصی و کامپیوترهای مستقر در ایستگاهها، حفاظت از سیستمهای فناوری اطلاعات در مقابل آتش سوزی، تامین منبع ضروری قدرت، کنترل رطوبت و دما با استفاده از دستگاههای محاسبه گر، تامین ایمنی فیزیکی، تضمین ایمنی محیط می شوند.

- مرحله نهم: مستند سازی نتایج

هنگامی که ارزیابی ریسک به پایان رسید، لازم است تا مشاهدات به صورت مستند و طی گزارشی رسمی ارائه شوند. گزارش ارزیابی ریسک به مدیران ارشد کمک می کند تا در برنامه ریزی های خود اعم از مالی و عملیاتی، تغییرات لازم را اعمال نمایند. گزارش ارزیابی ریسک، برخلاف گزارش حسابرسان و ناظران که در پی کشف تخلفات می باشند، به صورت سیستماتیک و تحلیلی بوده تا بدین طریق مدیران ارشد را قادر سازد تا با انجام اقدامات مناسب، سطح ریسک را کاهش دهند.

۲- کاهش ریسک

کاهش ریسک، پس از ارزیابی ریسک، دومین گام در مدیریت ریسک بوده و شامل اولویت بندی، برآورد و استفاده مناسب از ابزارهای کاهش ریسک می باشد. با توجه به عدم توانایی در حذف ریسک، مدیران ارشد، عملیاتی و کسب و کار سازمانها وظیفه دارند تا با استفاده از کم هزینه ترین امکانات، مناسبترین ابزارها را برای کاهش سطح ریسک ضمن اثرگذاری اندک در ماموریت و منابع سازمان به کار برند. کاهش ریسک روشی سیستماتیک است که

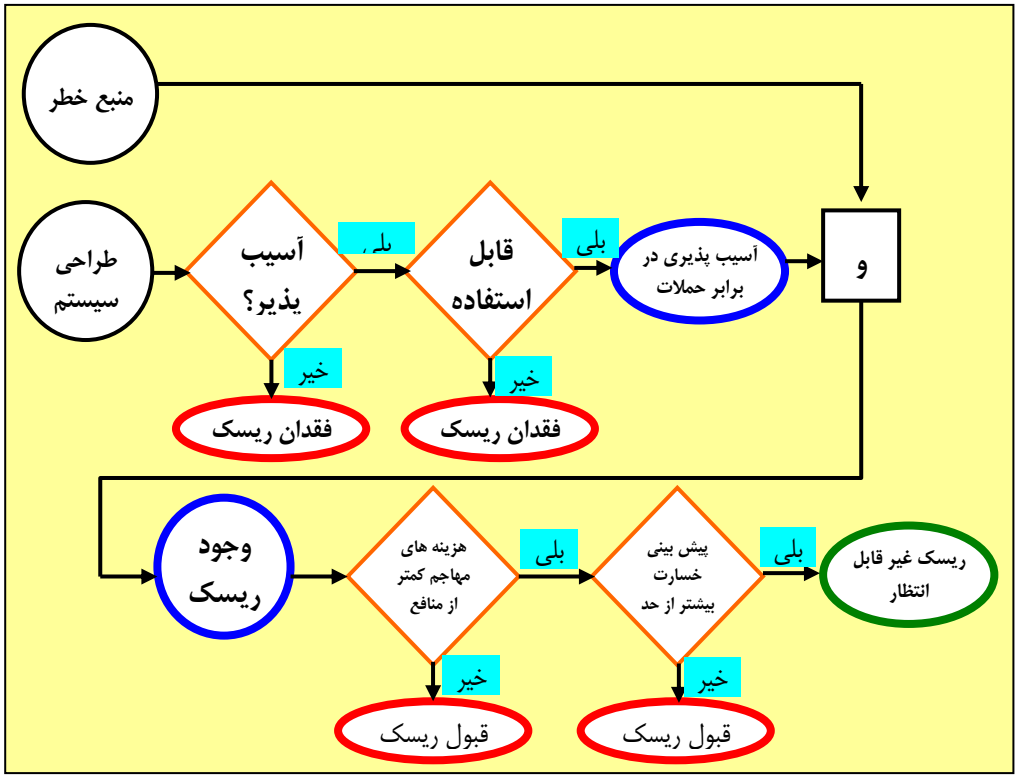
مدیر ارشد از طریق آن به کاهش سطح ریسک می پردازد. استفاده از هر یک از روشهای زیر، باعث کاهش سطح ریسک خواهد شد.

- قبول ریسک: پذیرش ریسک بالقوه و ادامه فعالیت سیستمهای فناوری اطلاعات یا استفاده از ابزارها به منظور کاهش سطح ریسک تا حد قابل قبول.
- پرهیز از ریسک: جلوگیری از ریسک با حذف شرایط و/یا علتهای پیدایش ریسک (به عنوان مثال خاموش کردن سیستمها، هنگام شناسایی ریسک).
- محدود سازی ریسک: محدود سازی ریسک با استفاده از ابزارهای کاهنده تاثیرات منفی خطرات بر موارد آسیب پذیر
- برنامه ریزی ریسک: مدیریت ریسک با استفاده از برنامه ریزی در کاهش ریسک بدین صورت که ابزارها دسته بندی و نگهداری شده و از آنها برای کاهش ریسک استفاده شود.
- انجام تحقیقات: با انجام تحقیقات و شناسایی موارد آسیب پذیر می توان سطح ریسک را کاهش داد.
- انتقال ریسک: انتقال ریسک با استفاده از روشهایی برای جبران خسارات نظیر خرید بیمه نامه.

برای استفاده از راههای فوق، در ابتدا می بایست اهداف سازمان مشخص شوند. بعلاوه استفاده از تمامی روشها غیر عملی بوده و به دلیل تفاوت محیط کاری و مقاصد سازمانها، استفاده از ابزارها و روشهای کاهش ریسک بسیار متفاوت می باشند.

نکته قابل توجه دیگر در مدیریت ریسک، زمان استفاده از ابزار برای کاهش ریسک می باشد. نمودار ۷ زمان مناسب استفاده از ابزار را نشان می دهد. با توجه به جدول، هنگامی که وجود موارد آسیب پذیر تایید شد، استفاده از تکنیکهای مطمئن برای کاهش ریسک ضروری است. هنگامی که موارد آسیب پذیر با خطر مواجه شدند، حفاظت لایه ای، طراحی های فنی و استفاده از ابزار های اجرایی برای کاهش خطر لازم است. در زمانی که هزینه مهاجمان کمتر از منافع بالقوه باشد، لازم است تا از سیستمهای حفاظتی برای کاهش حملات مهاجمان استفاده نمود. هنگامی که میزان خسارت شدید باشد، استفاده از اصول طراحی و سیستمهای محافظتی فنی و غیر فنی برای کاهش میزان حمله و در نتیجه خسارات بالقوه ضروری است.

نمودار۷- مراحل انجام کاهش ریسک



در استفاده از ابزارها لازم است تا مراحل زیر به صورت متوالی سپری شوند:

۱- درجه بندی وقایع از میزان زیاد به کم

۲- تهیه لیستی از ابزارهای مناسب

۳- بررسی هزینه ها و تشریح میزان منافع در استفاده یا عدم استفاده از ابزارها

۴- انتخاب ابزارها

۵- تهیه لیستی از نام افراد متعهد و متخصص، متناسب با نوع ابزارها

۶- تضمین برنامه اجرایی که می بایست اطلاعات زیر را در بر داشته باشد: انواع ریسکهای اصلی و فرعی، ابزارهای پیشنهادی، درجه بندی وقایع، انتخاب ابزارهای مورد نیاز، منابع مورد نیاز برای استفاده از ابزارهای انتخابی، لیست افراد و گروههای متعهد و متخصص، تاریخ شروع کار، تاریخ انقضای کار، شروط لازم برای تعمیر و نگهداری اجزای سیستم.

۷- ریسک باقیمانده: سازمانها قادرند میزان گسترش ریسک کاهشی توسط ابزارها را تجزیه و تحلیل نمایند. با وجود تمامی تلاشها در جهت جلوگیری از ریسک و کاهش آن، همواره احتمال وجود ریسک امکان پذیر است. برای

جلوگیری از بروز خطرات ریسکهای باقیمانده بهتر است موارد آسیب پذیر سیستم حذف شده یا از ابزارهای قویتری استفاده شده و یا میزان تاثیرات منفی کاهش یابد.

در خاتمه یاد آور می شویم که ارزیابی ریسک می بایست به صورت دوره ای انجام گیرد زیرا در سازمانها، سیستم فناوری اطلاعات خود به خود به روز شده و اجزاء و نرم افزارهای آن تغییر می کنند. همچنین ممکن است کارمندان و متخصصان جایگزین شده و یا سیاستهای جدیدی در سازمان تعیین شوند. بنابراین مدیریت ریسک می بایست دارای انعطاف و تغییرپذیر باشد تا بتوان تغییرات عمده را در سیستم فناوری اطلاعات اعمال کرد.

منابع و ماخذ:

1- *Risk Management Guide for Information Technology Systems*, Special Publication800-30, No. 7/2002, NIST