ارزیابی ریسک

ارزیابی ریسک کیفی یک روش منطقی برای تعیین اندازه کمّی و کیفی خطرات و بررسی پیامدهای بالقوه ناشی از حوادث احتمالی بر روی افراد، مواد، تجهیزات و محیط است. در حقیقت از این طریق میزان کارآمدی روش‌های کنترلی موجود مشخص شده و داده‌های باارزشی برای تصمیم‌گیری در زمینه کاهش ریسک، خطرات، بهسازی سیستم‌های کنترلی و برنامه‌ریزی برای واکنش به آن‌ها فراهم می‌شود.[۱]

ارزیابی ریسک کمّی نیازمند محاسبه دو مؤلفه ریسک یعنی شدت پیامدِ رخداد و احتمالِ روی دادن آن رخداد می‌باشد. برای بدست آوردن وزن احتمال یا وزن شدت پیامد سه نوع راهکار وجود دارد.[۲]

- روش‌های عددی (به انگلیسی: Quantitative) که نتیجه در نهایت به یک عدد منتهی می‌شود
- روش‌های کیفی (به انگلیسی: Qualitative) که نتیجه حاکی از کیفیت خاصی در زمینه ریسک خواهد بود.
- روش‌های نیمه‌کمی (به انگلیسی: Semi-Quantitative) که در بیشتر این روش‌ها از ماتریس ریسک استفاده می‌شود.

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

برآورد میزان ریسک

افراد مختلف از یک ریسک مشخص، برداشت‌هایی گوناگون دارند. برآورد میزان ریسک از سوی افراد غیرعلمی با نتایج آماری و معادلات ریاضی ریسک همخوانی ندارد. مفهوم ریسک دو جنبه گوناگون را در بر می‌گیرد[۳]:

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

- برآورد علمی بر پایه اطلاعات آماری از میزان ریسک، که به آن ریسک واقعی می‌گویند.

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

تعاریف

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

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

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

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

روش اجرا

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

۱- دسته بندی داراییها

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

الف- دارایی‌های سخت‌افزاری

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

ب- داراییهای نرم‌افزاری

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

ج- سرمایه‌های اطلاعاتی

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

د- سرمایه‌های انسانی

سرمایه‌های انسانی شامل تمامی کارکنانی می‌شود که در سازمان مشغول بکار بوده و در صورت از دست دادن آ

نها، به روند اجرایی سازمان و روال‌های کاری و سازمانی لطمه وارد خواهد شد. نظیر: - مدیران ارشد قسمت‌های مختلف سازمان و جانشینان و معاونین آنها - رؤسای بخش‌ها و دوایر - پرسنل متخصص و با سابقه - مدیران و کارشناسان بخش IT و امنیت اطلاعات - پرسنل متخصص و تکنیکی موجود در دوایر و بخش‌ها - سایر موارد.

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

ریسک = عامل تهدید + سرمایه + اثر تهدید

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

شد. در ادامه به مشخص کردن انواع عوامل تهدید قابل اعمال بر روی دارایی‌های اطلاعاتی، و نیز اثرات ناشی از آن‌ها می‌پردازیم.

۲- دسته بندی عوامل تهدید

- تهدیدات طبیعی

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

- تهدیدات انسانی

o رویدادها و اتفاقاتی که منشاء انسانی غیر عمدی دارند (اشتباهات و غفلتها) مانند عدم بکارگیری صحیح تجهیزات، عدم نصب صحیح نرم‌افزارها و برنامه‌های کاربردی، آلوده نمودن غیر عمدی شبکه به ویروس، دسترسی ناخواسته به اطلاعات محرمانه و ...

o رویدادها و اتفاقاتی که منشاء انسانی عمدی دارند چه از داخل سازمان و چه از خارج از آن (سوء استفاده، نرم‌افزار مخرب، دسترسی غیرمجاز، کدهای مخرب، ویروس، بمبها، اخلال‌گری الکترونیکی، آتش‌سوزی عمدی، قطع برق عمدی و ...). بر طبق آمار، تهدیداتی که موجب وارد شدن بیشترین آسیب به منابع اطلاعاتی می‌شوند، دارای منشاء انسانی هستند.

- تهدیدات محیطی

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

۳-انواع اثرات تهدیدات

اثر تهدید به نتایج و پیامدهای منفی حاصل از وقوع تهدید گفته می‌شود که می‌توانند بر روی سرمایه‌های اطلاعاتی سازمان، تأثیر منفی در پی داشته باشند.

- سوء استفاده از دارایی اطلاعاتی - دستکاری غیر مجاز - افشاء غیر مجاز - سرقت - عدم سرویس دهی یا قطع مقطعی آن - کپی و تکثیر غیر مجاز - تخطی از قواعد و قوانین سازمانی - کاهش کارایی سازمان - کاهش ایمنی افراد - از دست رفتن جامعیت اطلاعات - از دست رفتن دسترس‌پذیری اطلاعات (در زمان لزوم، در مکان مورد نیاز نباشد) - فعالیتهای بیهوده مالی (زیان مالی) - تهدیدهای مربوط به محیط زیست - اختلال در فرایندهای سازمانی - از بین رفتن دارایی

در پایان این مرحله، باید برای تمامی دارایی‌های موجود در حوزه بررسی، ریسک‌های مربوطه مطابق فرمول یادشده شناسایی شده و در بخش اول شناسنامه ثبت شوند. به عنوان مثال، برخی از ریسک‌های شناسایی شده ممکن است به صورت زیر ثبت شوند:

۱. کاربران به دلیل بی‌توجهی (سهل انگاری) باعث خراب شدن هارد کامپیوتر سرور دبیرخانه شوند.

۲. به دلیل ویروسی شدن، هارد کامپیوتر سرور اینترنت قابل استفاده و دسترسی نباشد.

تعداد بیشتری از ریسک‌ها ی ممکن در ذیل ارائه شده‌است.

نمونه‌ای از ریسک‌ها قابل شناسایی در سازمان:

اعضای تیم ارزیابی ریسک می‌توانند از این فهرست نمونه‌ای ریسک‌ها به عنوان نقطه شروعی جهت شناسایی انواع ریسک‌ها قابل اعمال بر دارایی‌های اطلاعاتی سازمان مطبوع خود استفاده نمایند. نکته‌ای که در اینجا ذکر آن ضروری است این است که این فهرست تنها به عنوان نمونه و نه یک فهرست جامع و کامل از تمامی ریسک‌ها موجود و محتمل می‌باشد و اعضای تیم می‌بایست بر اساس تجربه و تخصص خود و با استفاده از سوابق مربوط به حوادث گذشته، تمامی ریسک‌ها محتمل قابل اعمال بر مجموعه تحت بررسی خود را شناسایی نمایند. در هنگام مشخص نمودن ریسکها، توجه به این نکته نیز ضروری است که تنها از ریسکهایی می‌توان چشم پوشی نمود که احتمال آن‌ها صفر (غیر ممکن و محال) باشد. در غیر اینصورت حتی کم احتمال‌ترین ریسک‌ها نیز می‌بایست ثبت شوند. نکته دیگر این است که برخی از ریسک‌ها ممکن است از سوی عوامل مختلف اعمال شوند که همانگونه که پیش از این نیز گفته شد، برای هر یک از آن‌ها می‌بایست شناسنامه جداگانه‌ای تهیه شود.

فهرست نمونه‌ای از انواع ریسک‌های قابل اعمال بر سازمان مبتنی بر IT

- خرابی هارد کامپیوتر سرور/ شخصی به دلیل سهل انگاری مسئول/ کاربر مربوطه - خرابی هارد کامپیوتر سرور/ شخصی به دلیل نفوذ ویروس از طریق اینترنت - خرابی هارد کامپیوتر سرور/ شخصی به دلیل نفوذ ویروس از طریق کاربران - دسترسی غیر مجاز به اطلاعات موجود در کامپیوتر سرور/ شخصی توسط کاربران داخلی - دسترسی غیر مجاز به اطلاعات موجود در کامپیوتر سرور/ شخصی از طریق اینترنت - افشاء غیر مجاز اطلاعات موجود در کامپیوتر سرور/ شخصی به دلیل سهل انگاری کاربر مجاز - افشاء غیر مجاز اطلاعات موجود در کامپیوتر سرور/ شخصی از طریق اینترنت - سرقت اطلاعات موجود در کامپیوتر سرور/ شخصی از طریق اینترنت - سرقت اطلاعات موجود در کامپیوتر سرور/ شخصی به دلیل سهل انگاری کاربر مجاز - عدم سرویس دهی کامپیوتر سرور/ شخصی بعلت نفوذ ویروس از طریق اینترنت - عدم سرویس دهی کامپیوتر سرور/ شخصی بعلت نفوذ ویروس از طریق کاربر مجاز - عدم سرویس دهی کامپیوتر سرور/ شخصی بعلت قطع برق و نبود UPS

شرح ریسک‌های مرتبط با محرمانگی سرمایه‌های اطلاعاتی سازمان

- داده / اطلاعات به‌طور نادرستی توسط مسئول مربوطه یا کاربر برچسب‌گذاری شود. - داده / اطلاعات به‌طور نادرستی توسط مسئول مربوطه یا کاربر دسته‌بندی شود. - داده / اطلاعات قبل از اینکه از طریق کانال‌های مناسب انتشار یابد به اشتراک گذاشته شود. - استفاده از سیستم‌های غیر امن برای انتقال داده / اطلاعات حساس - افشای اطلاعات و نقض قوانین حریم شخصی و مالکیت - عدم وجود توضیحات شفاف در مورد قوانین محرمانگی - محافظت نامناسب از فهرست کلمات عبور - وجود backdoor در نرم‌افزارها داده‌ها و برنامه‌های کاربردی - مدیر اجرایی عصبانی وناراضی که دارای

امتیازات و توانایی‌های امنیتی بالایی باشد. - عدم بررسی کامل اثرات نهفته و مخفی قبل از اعمال نمودن تغییرات مورد نیاز بر روی سیستم‌ها و برنامه‌های مورد استفاده سازمان - توانایی حدس زدن مشخصات فردی دیگر توسط کاربران سازمان یا هکرها - کارمندان و افراد از طریقه نحوه صحیح انتشار یا ذخیره کردن اطلاعات موجود بر روی وب ناآگاه باشند. - دستپاچه و گیج شدن مسئولین امنیتی شبکه در مورد جایی که اطلاعات حساس در آنجا ذخیره شده‌است. - دادن قابلیت دسترسی به افرادی که از نظر شغلی نیازی به داشتن این امتیاز نداشته باشند. - اطلاعات مربوط به سیستم‌های داخلی به‌طور سهوی انتشار یابند که ممکن است در آینده برای حمله به سیستم مورد استفاده قرار گیرند. - استفاده ازIDهای مشترک توسط کاربران سازمان - دسترسی به فایل‌های پشتیبانی‌کننده توسط مدیر اجرایی سیستم به‌طور مناسبی کنترل نشود. - تکنولوژی‌های جدید باعث نفوذ در مسائل محرمانگی شوند. - تلاش‌ها وتصمیماتی برای تغییر دادن مدل امنیتی صورت گیرد. - عدم تشریح مسائل محرمانگی برای افراد غیر کارمند موجود در سازمان - ردیابی بسته‌ها توسط افراد غیر مجاز از خارج سایت اینترنتی سازمان - جریمه‌های در نظر گرفته شده برای تخطی کردن از مقررات امنیتی آنقدر کافی نباشد که باعث جلوگیری کردن از فعالیت‌های نامناسب افراد گردد. - امکان وجود تجهیزات استراق سمع الکترونیکی در محل‌های مختلف مجموعه مورد نظر

شرح ریسک‌های مرتبط با تمامیت سرمایه‌های اطلاعاتی سازمان

- پایگاه داده توسط خطای سخت‌افزاری، نرم‌افزار بد، یا نادرست خراب شود. - عدم گزارش کردن نکات و موارد مربوط به تمامیت توسط کاربران سازمان - اجرای ناقص یک روند یا عدم توانایی در اجرای صحیح روند توسط افراد باعث خراب شدن داده شود. - نبود پردازش‌های داخلی برای ایجاد کنترل و مدیریت داده در حین انجام فعالیت‌های مختلف - عدم تشخیص و اعلام مشکلات تمامیت به وجود آمده توسط کاربران و مسئولین امنیتی شبکه سازمان - امکان دسترسی اشخاص ثالث به اطلاعات محرمانه موجود در سازمان - عدم تعیین صلاحیت منشأ تقاضاکننده درخواست در روال‌ها و سیاست‌های موجود در سازمان - عدم قابلیت دسترسی به اطلاعاتی که مجاز به دسترسی به آن‌ها می‌باشید. - کارمندان مربوطه آموزش‌های لازم برای انجام تغییرات مورد نیاز را دریافت نکرده باشند. - عدم پاسخ دهی مناسب به تقاضاهای انجام شده در مدت زمان مورد نظر - تغییرات انجام شده در داده/نرم‌افزارهای سیستم یا برنامه‌های کاربردی ذخیره نشده باشند. - استفاده کاربران از کپی‌هایی از داده که از رده خارج شده باشند. - وجود مشکلات همسان سازی و یکنواخت کردن در هنگام استفاده از وسیله‌های جبران ساز و بازگرداننده توسط کاربران - تغییر داده‌ها بعلت وجود ویروس - عدم گزارش کردن بموقع وضعیت کاربران، توسعه دهندگان، پشتیبانی کنندگان وغیره... توسط مسئولین مربوطه

شرح ریسک‌های مرتبط با در دسترس بودن سرمایه‌های اطلاعاتی سازمان

- هکرها سایت مجموعه مورد نظر را تعطیل نمایند. - نفوذکنندگان قادر به دسترسی فیزیکی به تجهیزات و امکانات مجموعه مورد نظر شوند. - وجود خطای سخت‌افزاری در مورد سرور اینترنت - ارتباطات موجود با تهیه‌کننده سرویس قطع شود. - سایت میزبان، محافظهای فیزیکی مناسبی برای اطلاعات نداشته باشد. - ارتباط با سیستم‌های پشتیبان اداره قطع شود. - طراحی کلی سیستم پیچیده باشد. - ایجاد تغییرات نادرست نرم‌افزار یا سخت‌افزار سیستم توسط کاربران مجاز - مقادیر وپیش بینی‌های مورد استفاده و معمول غیرقابل انتظار باشند. - روندهای برنامه استمرارپذیری سازمان آزمایش نشده باشند. - هیچ تضمینی برای آماده بودن سرور توسط تهیه‌کننده سرویس داده نشده باشد. - اقدامات و اعتصاب‌هایی

در سازمان تهیه‌کننده سرویس، بوقوع بپیوندد. - تعمیر و نگهداری برنامه‌ریزی شده معمولی، باعث آماده و در دسترس نبودن سرویس شود. - طراحی توپولوژی مانع کارایی / قابل قبول بودن میزان در دسترس بودن سرویس‌های عمومی شود. - سرمایه گذاری‌های نامناسب سازمان برای قابلیت‌های پشتیبانی - حملات برنامه‌ریزی شده توسط معترضان و مخالفین سازمان - ساختار بندی سیستم برای در دسترس بودن زیاد مناسب نباشد. - منابع و افراد تکنیکی سازمان آموزش‌های مناسب ندیده باشند. - تراکم موجود در اینترنت باعث عدم رضایت کاربران شود. - بعلت وجود ویروس، ممکن است داده / اطلاعات در دسترس نباشند. - بعلت عدم نظارت کافی بر سایت وب سازمان، ممکن است آماده نبودن سیستم گزارش نشود. - بعلت نقص در روتر یا دیواره آتش، ممکنست دسترسی به سرویس‌ها امکان‌پذیر نباشد. - پشتیبان‌های موجود در سازمان کافی نباشند. - سوء استفاده کاربران از امکانات شبکه، کلمات عبور سایر افراد

حوزه ریسک

منظور تعیین گروه دارایی مورد بررسی است. همانگونه که پیش از این نیز ذکر شد، حوزه ریسک می‌تواند یکی از حوزه‌های کلی سخت‌افزار، نرم‌افزار، نیروی انسانی و اطلاعات باشد.

تعیین طبیعت ریسک

ریسک‌ها را می‌توان با توجه به ماهیت وجودی خود و با توجه به ابعاد، حوزه و گستره اثرگذاری، دسته‌بندی نمود. این دسته‌بندی که به تعیین «طبیعت ریسک» موسوم است، به ارزیاب کمک می‌کند تا با توجه به حوزه‌های اثرگذاری ریسک، قادر باشد با دقت بیشتری به شناسایی اثرات و عواقب تهدید اقدام نماید. به‌طور کلی، ریسک‌ها را می‌توان به حوزه‌های زیر تقسیم نمود: - استراتژیک: ریسکهایی که تمامیت، موجودیت و بقای سازمان را با خطر مواجه می‌کنند مانند فقدان اطلاعات کلیدی و استراتژیک - مالی: اثرات و عواقب مالی به‌دنبال دارند نظیر غیرقابل استفاده شدن سخت‌افزارها و تجهیزات - عملیاتی: در انجام فعالیت‌ها و فرایندهای سازمان خلل ایجاد می‌کنند مانند قطع سرویس سرور - تکنولوژیکی: اطلاعات فنی یا سخت‌افزارهای کلیدی را مورد هجوم قرار می‌دهند - محیطی: بر نیروی انسانی یا شرایط زیست‌محیطی سازمان تأثیرگذار هستند نظیر آتش‌سوزی از آنجاییکه اغلب هر تهدید (ریسک) بیش از یک اثر به‌دنبال خواهد داشت، لذا با توجه به تنوع اثرات، ممکن است طبیعت یک ریسک در بیش از یک حوزه یا حتی تمامی حوزه‌ها قرار گیرد.

زیان دیدگان (ذینفعان) ریسک

منظور از زیان دیده، تمامی افراد یا واحدهایی از سازمان است که به‌طور مستقیم یا غیرمستقیم تحت تأثیر نتایج تهدید قرار می‌گیرند. این ذینفعان ممکن است یک یا تمامی موارد ذیل باشند:

- کاربر - مسئول واحد - مدیریت ارشد سازمان - کارکنان واحد - تمامی کارکنان سازمان - سهامداران - جامعه - ...

تعیین آثار ریسک

کلیه نتایج و عواقب بروز ریسک است که می‌تواند هر یک از ذینفعان اطلاعات یا ویژگی‌های آن را تحت تأثیر قرار دهد، در این بخش در نظر گرفته می‌شود. بهتر است در این بند، بیشتر به اثرات مستقیم ریسک اشاره شود و در صورت وجود ابهام یا کلی گویی، به توالی تبعات و اثرات آن اشاره نمود. این اثرات را می‌توان در یک یا چند مورد از انواع ذکر شده، جستجو نمود.

تعیین مشخصه‌های کمی ریسک

۱- ریسک سخت‌افزار:

برای تعیین مشخصه‌های کمی ریسک (احتمال و اثر) دارایی‌های سخت‌افزاری، باید از جداول ۱و۲ استفاده نمود. در این جداول، هر دو مشخصه احتمال و اثر، با توجه به تعاریف و مثال‌های ارائه شده، در گستره ۱ تا ۱۰ طبقه‌بندی شده‌اند.

لازم به ذکر است که جداول مذکور، استاندارد بوده و بر اساس روش ارزیابی ریسک FEMA، بومی سازی شده‌اند.

۲- ریسک نرم‌افزار:

مشابه تعیین مشخصه‌های کمی ریسک دارایی‌های سخت‌افزاری انجام خواهد شد.

۳- ریسک اطلاعات:

همانند دو دارایی قبل انجام می‌شود.

۴- ریسک نیروی انسانی:

در مورد دارایی‌های انسانی، با توجه به تفاوت ماهیت این نوع دارایی با دارایی‌های قبلی، از روش جداگانه‌ای استفاده خواهد شد. در این روش، هفت مؤلفه به عنوان مؤلفه‌های ارزش نیروی انسانی تعیین می‌شوئد که عبارتند از: تخصص، سابقه، رتبه، سختی کار، مدرک تحصیلی، وجود جایگزین و سطح دسترسی. هر یک از کارکنان سازمان، مطابق راهنمای ارائه شده صفحه بعد، در هر یک از موارد مذکور، امتیازی بین ۱ تا ۱۰ دریافت خواهند کرد.

پانویس

1. *ابوالفضل قهرمانی*. *«ارزیابی ریسک آتش‌سوزی»* *(https://web.archive.org/web/20130130013212/http://www.ensani.ir/fa/content/69254/default.aspx)* . *پژوهشگاه علوم انسانی. بایگانی‌شده از اصلی (http://www.ensani.ir/fa/content/69254/default.aspx)* *در ۳۰ ژانویه ۲۰۱۳*.
2. *مهران قلعه نوی*. *«تکنیک‌های ارزیابی ریسک ابزاری کارآمد و گمراه‌کننده»* *(https://web.archive.org/web/20130130183850/http://ghalenoy.persianblog.ir/post/350)* . *بهداشت حرفه‌ای و ایمنی صنعتی. بایگانی‌شده از اصلی (http://ghalenoy.persianblog.ir/post/350/)* *در ۳۰ ژانویه ۲۰۱۳*.
3. *شیرازه ارقامی، عوامل مؤثر بر ریسک پذیری*

منابع

[۱] TECHNICAL REPORT: ISO/IEC TR ۱۳۳۳۵-۳:۱۹۹۸(E) Information technology — Guidelines for the management of IT Security -Part ۳:Techniques for the management of IT Security

[۲] TECHNICAL REPORT: ISO/IEC TR ۱۳۳۳۵-۲: Dec ۱۵، ۱۹۹۷، Information technology - Guidelines for the management of IT Security - Part ۲: Managing and planning IT Security

[۳] NIST Computer Security Documents:

a. Draft ۸۰۰-۳۰

b. Draft ۸۰۰-۵۰

c. Draft ۸۰۰-۶۰

d. Draft ۸۰۰-۶۱

e. Draft ۸۰۰-۶۵

[۴] THE ISO ۲۷۰۰۰ SERIES:

f. ISO ۲۷۰۰۰

g. ISO ۲۷۰۰۲

h. ISO ۲۷۰۰۳

[۵] NSW

[۶] نوشته مهندس فرشاد سرایی / انتشارات نگارنده HAZOP STUDY کتاب شناسایی مخاطرات فرایندی به روش دانش

جستارهای وابسته

- تجزیه و تحلیل ریسک
- مدیریت و ارزیابی ریسک
- تاریخ فناوری
- مهندسی فناوری اطلاعات

آخرین ویرایش ۱۱ ماه پیش توسط Barana1378 انجام شده