INSO-ISO/IEC

27005

1st. Edition

Identical with
ISO/IEC 27005:
2011
Apr.2013

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ایران ایزو-آی‌ای‌سی
۲۷۰۰۵

چاپ اول

اردیبهشت ۱۳۹۲

فناوری اطلاعات – فنون امنیتی-مدیریت مخاطرات امنیت اطلاعات

Information technology - Security techniques — Information Security risk management

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات- فنون امنیتی- مدیریت مخاطرات امنیت اطلاعات»

رئیس :	**سمت و/ یا نمایندگی**
فولادیان، مجید (فوق لیسانس مهندسی برق مخابرات)	مشاور سازمان فناوری اطلاعات ایران
دبیر :	
میراسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	مدیر کل خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضا: (اسامی به ترتیب حروف الفبا)	
بختیاری، شیرین (لیسانس مهندسی برق)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
جمیل پناه، ناصر (فوق لیسانس مدیریت)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سلطانیان همت، بهزاد (لیسانس مهندسی برق الکترونیک)	مترجم و کارشناس فنی انتشارات قدیس
سلطانی حقیقت، الهه (لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سعیدی، عذرا (فوق لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
طی نیا، رضا (فوق لیسانس مدیریت فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم

عسگرزاده، مجید (فوق لیسانس مهندسی کامپیوتر)	مدیر پروژه موسسه تحقیقات ارتباطات و فناوری اطلاعات
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
فیاضی، مهدی (لیسانس مهندسی برق الکترونیک)	کارشناس مسؤول تدوین استاندارد و امنیت شبکه
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
معروف، سینا (لیسانس مهندسی کامپیوتر- سخت‌افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
مهدوی اردکانی، علیرضا (فوق لیسانس مدیریت فناوری اطلاعات)	شرکت داده پردازان آبشار
میرزایی رضایی، طیبه (فوق لیسانس فیزیک)	رییس اداره تدوین استانداردها و نظارت بر امنیت سرویس‌ها سازمان فناوری اطلاعات ایران
موجبی، محمود (فوق لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
ناصری، علی (دکتری برق مخابرات)	عضو هیأت علمی دانشگاه امام حسین (ع)
یزدیان، علی (دکتری برق مخابرات)	عضو هیأت علمی دانشگاه تربیت مدرس

فهرست مندرجات

پیش‌گفتار

ااستاندارد « فناوری اطلاعات – فنون امنیتی-مدیریت مخاطرات امنیت اطلاعات» نخستین بار در سال ۱۳۸۸ تدوین شد. این استاندارد براساس پیشنهادهای رسیده و بررسی توسط سازمان فناوری اطلاعات و تایید کمیسیون‌های مربوط برای اولین مورد تجدید نظر قرار گرفت و در دویست و پنجاه و پنجمین اجلاس کمیته ملی استاندارد مورخ ۱۳۹۱/۱۱/۱۶ تصویب شد. اینک این استاندارد به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، بهمن ماه، ۱۳۷۱ به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ هماهنگی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استاندارد ملی ایران در مواقع لزوم تجدید نظر در کمیسیون فنی مربوط مورد نظر قرار خواهد گرفت. بنابراین، باید همواره ار آخرین تجدید نظر استانداردهای ملی استفاده کرد.

این استاندارد جایگزین استاندارد ملی ایران شماره ISIRI-ISO-IEC 27005: سال ۱۳۸۸ است.

منبع و ماخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk management

فناوری اطلاعات- فنون امنیتی- مدیریت مخاطرات امنیت اطلاعات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین راهنما برای مدیریت مخاطرات امنیت اطلاعات است.

این استاندارد ملی مفاهیم کلی مشخص شده در استاندارد[1] ISO/IEC 27001 را پوشش می‌دهد و برای کمک به پیاده‌سازی رضایت‌بخش امنیت اطلاعات براساس رویکرد مدیریت مخاطرات طراحی شده است.

دانستن مفاهیم، مدل‌ها، فرآیندها و اصطلاحات شرح داده شده در استانداردهای ملی ایران به شماره ISO/IEC 27001 و ISO/IEC 27002 برای درک کامل این استاندارد ملی مهم است.

این استاندارد ملی قابل کاربرد در تمام انواع سازمان‌هایی (مثل بنگاه‌های کسب و کار، مؤسسات دولتی، سازمان‌های غیر انتفاعی) است که در صدد هستند مخاطراتی را که به امنیت اطلاعات‌شان لطمه می‌زنند، مدیریت کنند.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می شود.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره تاریخ تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است :

2-1 ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

2-2 ISO/IEC 27001: 2005, *Information technology — Security techniques — Information security management systems — Requirements*

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به‌کار می‌رود:

یادآوری- تفاوت بین استاندارد ملی ایران به شماره ایران ایزو ۲۷۰۰۵ ویرایش اول و این استاندارد در پیوست چ نشان داده شده است.

۱-۳

پیامد[2]

نتایج **رویداد** (۳-۳) اثرگذار بر اهداف

[ISO Guide 73: 2009]

۱- معادل این استاندارد، استاندارد ملی ای‌ران به شماره ایران ایزو ۲۷۰۰۱ موجود است.

2- Consequence

یادآوری ۱- یک رویداد می‌تواند به مجموعه‌ای از پیامدها منجر شود.

یادآوری ۲- پیامد ممکن است معین یا نامعین باشد و در زمینه امنیت اطلاعات به طور معمول معنای منفی دارد.

یادآوری ۳- پیامد را می‌توان به‌صورت کمی یا کیفی بیان کرد.

یادآوری ۴- پیامدهای اولیه ممکن است به‌صورت زنجیره‌ای گسترش یابند.

۲-۳

کنترل[1]

راه‌کاری که **مخاطره** (۳-۹) را اصلاح می‌کند.

[ISO Guide 73: 2009]

یادآوری ۱- کنترل‌ها در امنیت اطلاعات شامل هر فرایند، خط‌مشی، روش اجرایی، رهنمود، عملکرد یا ساختار سازمانی می‌شود که می‌توانند ماهیت اداری، فنی، مدیریتی یا حقوقی داشته باشند و مخاطرات امنیت اطلاعات را اصلاح کنند.

یادآوری ۲- کنترل‌ها ممکن است همیشه اثر اصلاح کننده موردنظر یا فرضی را نداشته باشند.

یادآوری۳ - همچنین، کنترل مترادفی برای حفاظت۲ یا اقدام متقابل به‌کار می‌رود.

۳-۳

رویداد[3]

وقوع یا تغییر مجموعه خاصی از وضعیت‌ها

[ISO Guide 73: 2009]

یادآوری ۱- رویداد می‌تواند یک یا چند اتفاق باشد و چندین دلیل داشته باشد.

یادآوری ۲- رویداد می‌تواند چیزی که اتفاق نیفتاده است، باشد.

یادآوری ۳- رویداد را گاهی «رخداد» یا «حادثه» می‌نامند.

۴-۳

زمینه‌بیرونی[4]

محیط بیرونی که سازمان درپی دستیابی اهداف خود از طریق آن است.

[ISO Guide 73: 2009]

یادآوری- زمینه‌بیرونی می‌تواند شامل موارد زیر باشد:

- محیط فرهنگی، اجتماعی، سیاسی، حقوقی، مقرراتی، مالی، فنی، اقتصادی، طبیعی و رقابتی که می‌توانند بین‌المللی، ملی، منطقه‌ای یا محلی باشند؛

1- Control
2- Safeguard
3- Event
4- External context

- روندها و محرک‌های کلیدی اثرگذار بر اهداف سازمان؛ و
- روابط با ذی‌نفعان[1] بیرونی و برداشت‌ها و ارزش‌های مربوط.

۵-۳

زمینه‌درونی[2]

محیط درونی که سازمان درپی دستیابی اهداف خود از طریق آن است.
[ISO Guide 73: 2009]

یادآوری- زمینه‌درونی می‌تواند شامل موارد زیر باشد:

- حاکمیت[3]، ساختار سازمانی، نقش‌ها و پاسخگویی‌ها؛
- خط‌مشی‌ها، اهداف و راهبردهایی که هدف دستیابی به آن‌ها است؛
- قابلیت‌هایی که بر حسب منابع و دانش شناخته می‌شود (مثل سرمایه، زمان، افراد، فرایندها، سامانه‌ها و فناوری‌ها)؛
- سامانه‌های اطلاعات، جریان‌های اطلاعات و فرایندهای تصمیم‌گیری (رسمی یا غیررسمی)؛
- روابط با ذینفعان درونی و برداشت‌ها و ارزش‌های مربوط؛
- فرهنگ سازمانی؛
- استانداردها، رهنمودها و مدل‌های اخذشده توسط سازمان؛ و
- شکل و گستره‌ی روابط پیمانی.

۶-۳

سطح مخاطره[4]

اندازه **مخاطره (۳-۹)** که بر حسب تلفیق **پیامدها** (۳-۱) و **احتمال آن‌ها** (۳-۷) بیان می‌شود.
[ISO Guide 73: 2009]

۷-۳

احتمال[5]

شانس اتفاق افتادن چیزی
[ISO Guide 73: 2009]

یادآوری ۱- در اصطلاحات مدیریت مخاطرات واژه‌ی «احتمال» به شانس اتفاق افتادن چیزی اطلاق می‌شود که می‌تواند به‌صورت عینی یا ذهنی، کمی یا کیفی تعریف، اندازه‌گیری یا تعیین و با استفاده از واژه‌های عمومی یا به‌صورت ریاضی (مثل احتمال یا فراوانی در دوره‌ای مفروض) تشریح شود.

یادآوری ۲- واژه‌ی انگلیسی «احتمال» در برخی زبان‌ها معادل مستقیم ندارد و از معادل ریاضی آن استفاده می‌شود.

1 - Stakeholder
2- Internal context
3- Governance
4- Level of risk
5- Likelihood

۸-۳

مخاطره‌ی باقی‌مانده[1]

مخاطره (۳-۹) باقی‌مانده پس از **مقابله با مخاطره**[2] (۳-۱۷)

یادآوری ۱- مخاطره‌ی باقی‌مانده می‌تواند شامل مخاطرات شناخته نشده باشد.

یادآوری ۲- مخاطره‌ی باقی‌مانده به «مخاطره‌ی مانده» نیز معروف است

۹-۳

مخاطره

اثر عدم قطعیت بر اهداف

[ISO Guide 73: 2009]

یادآوری ۱- اثر، یک انحراف (مثبت و/یا منفی) از انتظارات است.

یادآوری ۲- اهداف، جنبه‌های مختلفی دارند (مثل اهداف مالی، سلامت و ایمنی، امنیت اطلاعات و اهداف محیطی) و در سطح‌های مختلف (مثل راهبردی، سازمانی، پروژه‌ای، محصول و فرآیند) قابل اعمال است.

یادآوری۳- مخاطره اغلب با ارجاع به رویدادهای (۳-۳) بالقوه و پیامدها (۳-۱) یا تلفیقی از این دو، بیان می‌شود.

یادآوری ۴- مخاطره‌ی امنیت اطلاعات را اغلب بر حسب تلفیقی از پیامدهای رویداد امنیت اطلاعات و احتمال (۳-۹) وقوع مربوط بیان می‌کنند.

یادآوری ۵- عدم قطعیت یک وضعیت نارسایی درک یا شناخت رویداد، پیامد یا احتمال آن است.

یادآوری ۶- مخاطره امنیت اطلاعات ظرفیت بالقوه‌ای دارد که تهدیدات از آسیب‌پذیری‌های یک یا گروهی از دارایی‌های اطلاعاتی بهره‌جویی می‌کند و در نتیجه سبب آسیب به سازمان می‌شود.

۱۰-۳

تحلیل مخاطره[3]

فرایند درک ماهیت مخاطره و تعیین **سطح مخاطره** (۳-۶).

[ISO Guide 73: 2009]

یادآوری ۱- تحلیل مخاطره پایه‌ای برای ارزیابی مخاطره و تصمیم در رابطه با مقابله با مخاطره را ارائه می‌دهد.

یادآوری ۲- تحلیل مخاطره شامل تخمین مخاطره است.

1- Residual risk
2 - Risk treatment
3- Risk Analysis

۱۱-۳

ارزشیابی مخاطره[1]

فرآیند کلی شناسایی مخاطره (۳-۱۵)، تحلیل مخاطره (۳-۱۰) و ارزیابی مخاطره (۳-۱۴)

[ISO Guide 73: 2009]

۱۲-۳

تبادل اطلاعات و رایزنی مخاطره[2]

فرایندهایی مستمر و مکرر که سازمان‌ها برای فراهم‌سازی، اشتراک گذاری یا به دست آوردن اطلاعات و تعامل با ذی‌نفعان (۳-۱۸) راجع به مدیریت مخاطرات (۳-۹) انجام می‌دهند.

[ISO Guide 73: 2009]

یادآوری ۱- این اطلاعات می‌تواند به وجود، ماهیت، شکل، احتمال، اهمیت، ارزیابی، قابلیت پذیرش و مقابله مخاطره ارتباط داشته باشد.

یادآوری ۲- رایزنی فرایند دوسویه‌ی ارتباط آگاهانه بین سازمان و ذی‌نفعان آن پیش از تصمیم‌گیری راجع به موضوعی یا تعیین مسیر آن است. رایزنی:

- فرآیندی که بر اثر نفوذ داشتن نه اعمال قدرت بر تصمیمات اثر می‌گذارد.
- ورودی تصمیم‌گیری است نه تصمیم‌گیری مشترک.

۱۳-۳

معیارهای مخاطره[3]

شاخص‌های مرجع که اهمیت مخاطره (۳-۹) برمبنای آن‌ها ارزیابی می‌شود.

یادآوری ۱- معیارهای مخاطره مبتنی بر اهداف سازمان و زمینه بیرونی و درونی است.

یادآوری ۲- معیارهای مخاطره می‌تواند از استانداردها، قوانین، خط‌مشی‌ها و سایر الزامات استخراج شود.

1- Risk Assessment
2- risk communication and consultation
3- Risk Criteria

۱۴-۳

ارزیابی مخاطره[1]

فرآیند مقایسه نتایج **تحلیل مخاطره** (۳-۱۰) با **معیارهای مخاطره** (۳-۱۳) به منظور تعیین این که مخاطره و/یا دامنه‌ی آن قابل قبول یا قابل تحمل هست یا خیر.

[ISO Guide 73: 2009]

یادآوری- ارزیابی مخاطره به تصمیم‌گیری راجع به مقابله با مخاطره کمک می‌کند.

۱۵-۳

شناسایی مخاطره[2]

فرایند یافتن، تشخیص و تشریح مخاطرات

[ISO Guide 73: 2009]

یادآوری ۱- شناسایی مخاطره شامل شناسایی منابع مخاطره، رویدادها، علل آن‌ها و پیامدهای بالقوه‌شان است.

یادآوری ۲- شناسایی مخاطره می‌تواند شامل داده‌های تاریخی، تحلیل نظری، نظرات اشخاص خبره و مطلع و نیازهای ذی‌نفعان باشد.

۱۶-۳

مدیریت مخاطره[3]

فعالیت‌های هماهنگ جهت هدایت و کنترل سازمان با در نظر گرفتن مخاطره

[ISO Guide 73: 2009]

یادآوری - در این استاندارد از واژه‌ی «فرایند» برای مدیریت مخاطرات کلی استفاده می‌شود. مؤلفه‌های فرایند مدیریت مخاطرات را «فعالیت» می‌نامند.

۱۷-۳

مقابله با مخاطره

فرایند اصلاح مخاطره

[ISO Guide 73: 2009]

یادآوری۱- مقابله با مخاطره شامل موارد زیر می‌شود:

1- Risk evaluation
2- Risk identification
3- Risk Management

- پرهیز از مخاطره با آغاز نکردن یا ادامه ندادن فعالیتی که مخاطره را افزایش می‌دهد؛
- تن دادن به مخاطره یا افزودن مخاطره به منظور استفاده از فرصت؛
- حذف منبع مخاطره؛
- تغییر دادن احتمال؛
- تغییر دادن پیامدها؛
- اشتراک گذاری مخاطره با طرف یا طرف‌های دیگر (شامل قراردادها و بیمه مخاطرات)؛
- مهار مخاطره از طریق انتخاب آگاهانه.

یادآوری ۲- رسیدگی به پیامدهای منفی در مقابله با مخاطره را گاهی «تخفیف مخاطره[1]»، «رفع مخاطره»، «جلوگیری از مخاطره» و «کاهش مخاطره[2]» می‌نامند.

یادآوری ۳- مقابله با مخاطره می‌تواند مخاطرات جدیدی پدید آورد یا مخاطرات موجود را تغییر دهد.

۱۸-۳

ذی‌نفع

شخص یا سازمانی که می‌تواند بر تصمیم‌ها یا فعالیت‌ها اثر بگذارد، یا از آن‌ها تاثیر بپذیرد یا چنین برداشتی داشته باشد.

[ISO Guide 73: 2009]

یادآوری- تصمیم گیرنده می‌تواند ذینفع باشد.

۴ ساختار این استاندارد ملی

این استاندارد شامل توصیف کلی مدیریت مخاطرات امنیت اطلاعات و فعالیت ناشی از آن است. اطلاعات مربوط به این پیش‌زمینه در بند ۵ آمده است.

مروری کلی فرآیند مدیریت مخاطرات اطلاعات نیز در بند ۶ ارائه شده است.

تمامی فعالیت‌های صورت گرفته در این فرآیند (بند ۶) به‌صورت زیر توضیح داده شده است.

- برقراری زمینه در بند ۷،
- ارزشیابی مخاطره در بند ۸،
- مقابله با مخاطره در بند ۹،
- پذیرش مخاطره در بند ۱۰،
- تبادل اطلاعات مخاطره در بند ۱۱،
- پایش و بازنگری مخاطره در بند ۱۲.

1- Risk mitigation
2- Risk reduction

اطلاعات اضافی برای انجام فعالیت‌های مدیریت مخاطرات اطلاعات نیز در پیوست‌ها ارائه شده است. برقراری زمینه، در پیوست الف آمده است. (تعریف زمینه و مرزهای موجود در فرایند مدیریت مخاطرات امنیت داده‌ها آمده است.) شناسایی و ارزیابی دارایی‌ها و اثرات ناشی از آن، در پیوست ب آمده است. در پیوست پ مثال‌هایی مربوط به تهدیدات معمول آمده است و پیوست ت در رابطه با آسیب پذیری‌ها و روش‌های ارزشیابی آسیب پذیری بحث می‌کند. مثال‌هایی در خصوص رویکردهای ارزشیابی مخاطره در پیوست ث آورده شده است.

پیوست ج نیز شامل حدود مشخص برای کاهش مخاطره است.

تفاوت استاندارد ISO/IEC 27005: 2008 با استاندارد ISO/IEC 27005: 2011 در پیوست چ آمده است.

تمامی فعالیت‌های مدیریت مخاطرات در بند ۷ تا بند ۱۲ به ترتیب زیر ارائه شده است.

ورودی: شناسایی تمامی اطلاعات مورد نیاز برای انجام فعالیت.

اقدام: توضیح فعالیت.

رهنمود پیاده‌سازی: ارائه رهنمود برای انجام اقدام. برخی از این رهنمود نمی‌تواند در تمامی موارد، مناسب باشد و بنابراین لازم است که از سایر روش‌ها، در این خصوص استفاده کرد.

خروجی: شناسایی تمامی اطلاعات به دست آمده پس از انجام فعالیت.

۵ پیش زمینه

رویکردی سیستماتیک برای مدیریت مخاطرات امنیت اطلاعات، به‌منظور شناسایی نیازهای سازمانی مربوط به الزامات امنیت اطلاعات و برقراری سامانه‌ی کارآمد مدیریت امنیت (ISMS) ضروری است. این رویکرد باید برای محیط سازمان مناسب باشد و به‌ویژه با کلیت مدیریت مخاطرات بنگاه هم راستا باشد. در اقدامات امنیتی باید به‌طور مؤثر و به‌موقع در تمام مواقع و جاهای لازم به مخاطرات رسیدگی شود. مدیریت مخاطرات امنیت اطلاعات همواره باید بخشی جدانشدنی از تمام اقدامات مدیریت امنیت اطلاعات باشد و باید در پیاده‌سازی و بهره‌برداری مداوم ISMS به‌کار رود.

مدیریت مخاطرات امنیت اطلاعات باید فرآیند مستمری باشد. این فرایند باید زمینه درونی و بیرونی را آماده سازد، مخاطرات را ارزیابی کند و با استفاده از برنامه‌ی اجرای توصیه‌ها و تصمیمات برطرف کند. مدیریت مخاطرات آن چه را قابل رخ دادن است و پیامدهای ممکن را تحلیل می‌کند و سپس راجع به آن چه باید انجام داد و زمان آن تصمیم‌گیری می‌کند تا مخاطرات به میزان قابل پذیرشی کاهش یابد.

مدیریت مخاطرات امنیت اطلاعات، باید شامل موارد زیر باشد:

- شناسایی مخاطرات
- ارزیابی مخاطرات، برحسب پیامدهای‌شان برای کسب وکار و احتمال وقوع آن‌ها
- گفتمان و درک در مورد احتمال و پیامدهای مخاطرات،
- تعیین اولویت‌ها برای کاهش مخاطره
- تعیین اولویت‌ها برای اقدامات کاهش وقوع مخاطره
- دخیل‌کردن ذی‌نفعان در اخذ تصمیمات مدیریت مخاطرات و آگاهی رساندن به آن‌ها از وضعیت مدیریت مخاطرات

- اثربخشی پایش مقابله با مخاطره
- پایش و بررسی منظم مخاطرات و فرایند مدیریت مخاطرات
- جمع‌آوری اطلاعات[1] به‌منظور بهبود رویکرد مدیریت مخاطرات
- آموزش به مدیران و کارکنان راجع به مخاطرات و اقدامات تخفیف مخاطرات

فرایند مدیریت مخاطرات امنیت اطلاعات را می‌توان به کل سازمان و هر بخش جدا از آن (مثل ادارات، اماکن، خدمات)، تمام سامانه‌های موجود یا در دست راه‌اندازی یا جنبه‌های خاص کنترل (مثل طرح‌ریزی تداوم کسب و کار) اعمال کرد.

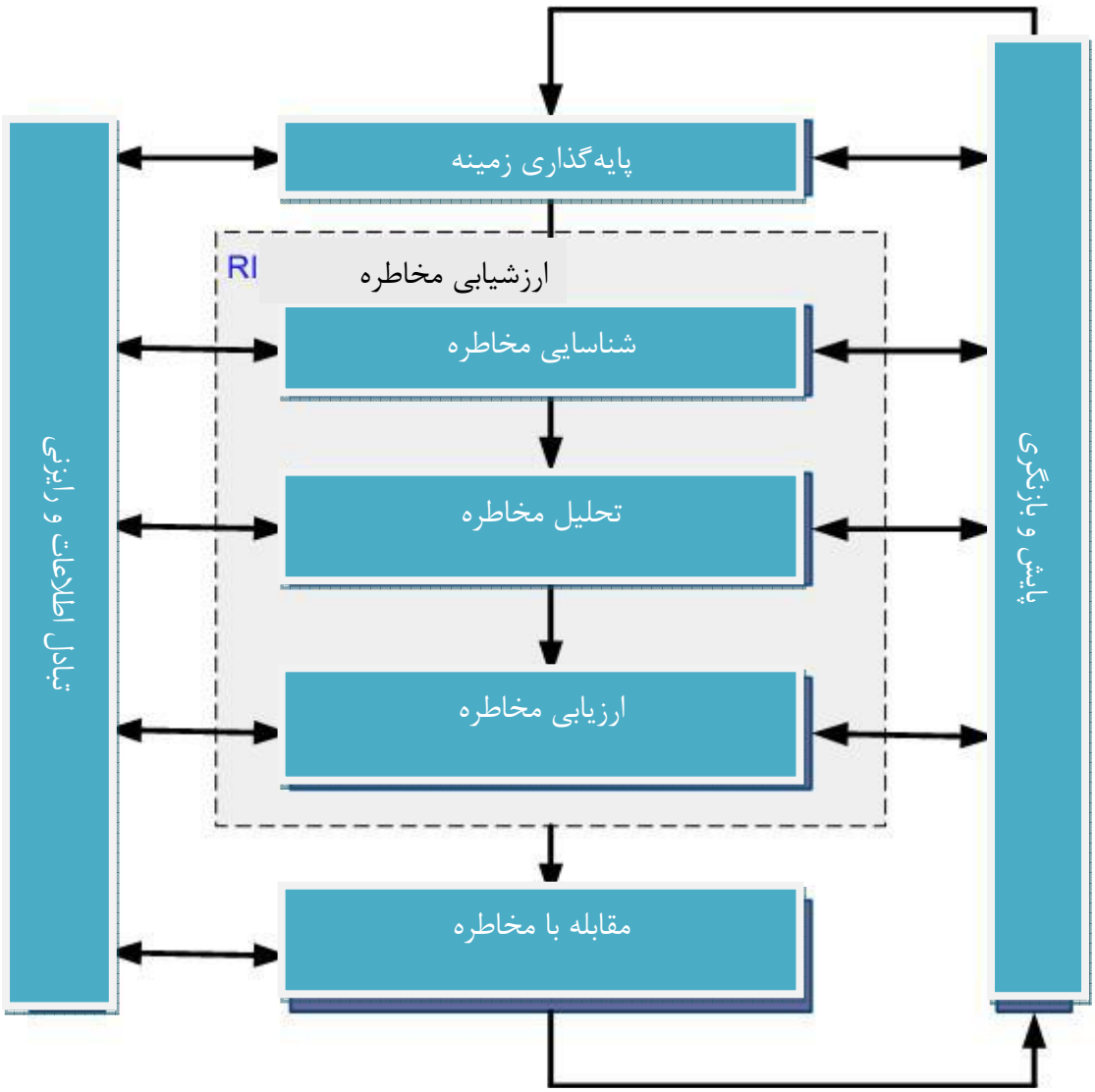
۶ مروری کلی بر فرآیند مدیریت مخاطرات امنیت اطلاعات

نمای سطح بالای فرآیند مدیریت مخاطرات در ISO 31000، مشخص شده و در شکل ۱ نشان داده شده است.

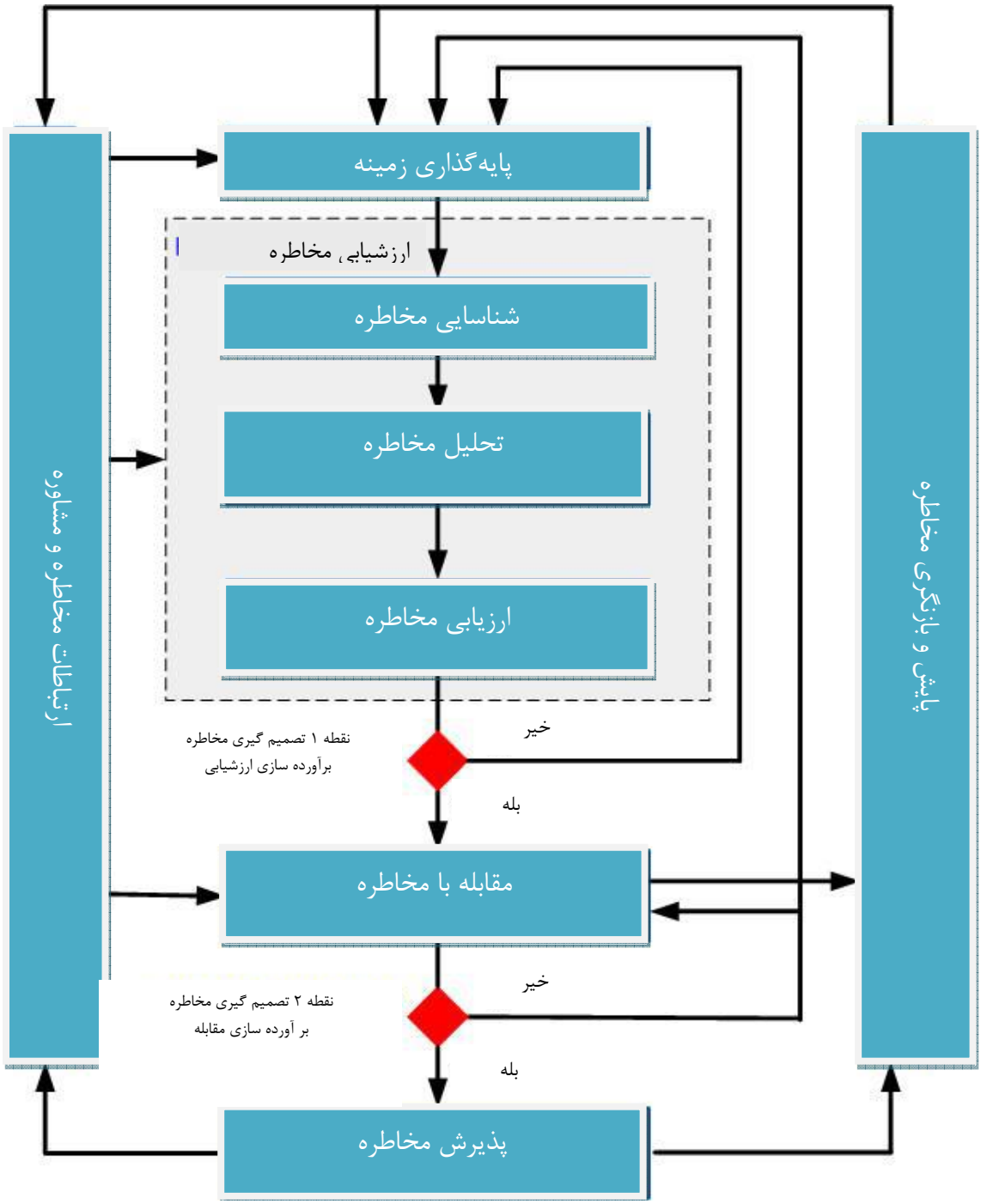
شکل ۲ نشان می‌دهد که چگونه در این استاندارد ملی فرآیند مدیریت مخاطرات اعمال می‌شود.

این فرایند شامل پایه‌گذاری زمینه (بند ۷): ارزشیابی مخاطره (بند ۸) مقابله با مخاطره (بند ۹) پذیرش مخاطره (بند ۱۰) تبادل اطلاعات و رایزنی مخاطره (بند ۱۱) پایش و بازنگری مخاطره (بند ۱۲) است.

1- Information being captured



شکل ۱ - فرآیند مدیریت مخاطرات



شکل ۲- ترسیم فرآیند مدیریت مخاطرات امنیت اطلاعات

همان‌طور که شکل۲ نیز نشان می‌دهد، فرایند مدیریت مخاطرات امنیت اطلاعات می‌تواند برای فعالیت‌های ارزشیابی مخاطره و/یا مقابله با مخاطره به‌صورت تکرارپذیر انجام گیرد. رویکرد تکرار پذیر به‌منظور هدایت ارزشیابی مخاطره می‌تواند عمق و جزییات ارزشیابی را در هر تکرار افزایش دهد. این رویکرد تکراری، هنگامی که این اطمینان به‌وجود آمد که مخاطرات بالا به‌صورت مناسبی ارزشیابی شده‌اند، تعادل مناسبی میان حداقل زمان ممکن و تلاش‌های مربوط به شناسایی کنترل‌ها، فراهم می‌آید.

ابتدا زمینه پایه‌گذاری شده، سپس ارزشیابی مخاطره هدایت می‌شود. در صورتی که این بخش بتواند اطلاعات کافی را برای تعیین مؤثر اقدامات مورد نیاز به‌منظور اصلاح مخاطرات به سطح قابل قبول فراهم آورد، آنگاه می‌توان گفت که این وظیفه کامل بوده و دربرگیرنده فرآیند مقابله با مخاطره است. در صورت کافی نبودن این اطلاعات، تکرار ارزیابی مخاطره دیگری با زمینه‌ی تجدید نظر شده‌ای هدایت می‌شود. (به عنوان مثال، معیار ارزیابی مخاطره، معیار پذیرش مخاطره و معیار اثرگذاری) همچنین قسمت‌های نامحدود این محدوده کلی نیز قابل توجه است.

اثربخشی مقابله با مخاطره، وابسته به نتایج حاصل از ارزشیابی مخاطره است.

باید توجه داشت که مقابله با مخاطره شامل فرایند چرخه‌ای زیر است:

- ارزشیابی مقابله با مخاطره؛
- تصمیم‌گیری راجع به قابل قبول بودن سطوح مخاطره‌ی باقی‌مانده؛
- اقدامی جدید برای مقابله با مخاطره در صورت قابل قبول نبودن سطوح مخاطره؛
- ارزشیابی اثربخش بودن مقابله جدید.

ممکن است مقابله با مخاطره به سرعت باعث رسیدن به سطح قابل قبول مخاطره نشود. در این موقعیت، تکرار دیگری از ارزیابی مخاطره به‌دست می آید که می‌تواند همگام با پارامترهای تغییر یافته، به‌کار گرفته شود (به‌عنوان مثال، ارزشیابی مخاطره، پذیرش آن و معیارهای اثرگذاری)، در صورت لزوم می‌توان دست به مقابله بیشتر مخاطره زد. (به شکل ۲ مراجعه شود نکته ۲ در تصمیم‌گیری مخاطره)

فعالیت پذیرش مخاطره، این اطمینان را به‌وجود می‌آورد که مخاطره‌های باقیمانده از سوی مدیران سازمان، مورد قبول، قرار می‌گیرد. این نکته، به‌ویژه در موقعیتی مهم است که پیاده‌سازی کنترل‌ها حذف شده و یا به تعویق افتد. (به‌عنوان مثال به‌دلیل هزینه)

در طول انجام فرآیند مدیریت مخاطرات امنیت اطلاعات این نکته مهم است که مخاطرات و ارزیابی آن‌ها در ارتباط با مدیران کارآمد و ستاد اجرایی شایسته قرار بگیرد. حتی پیش از مقابله با مخاطرات، اطلاعات مربوط به مخاطرات شناسایی شده از جمله عوامل ارزش‌مند برای مدیریت رویدادهای گوناگون بوده و از طرف دیگر، کمک بسیاری را به کاهش این آسیب‌های بالقوه می‌کند. آگاهی از این مخاطرات از سوی مدیران و ستاد اجرایی ماهیت کنترل این مخاطرات و زمینه اجرایی موجود در آن منوط به انجام دادن عملکردهای اثرگذار در این زمینه است. نتایج جزیی از هر یک از این فعالیت‌های صورت گرفته در فرآیند مدیریت مخاطرات امنیت اطلاعات و دو دیدگاه مورد توجه قرار گرفته شود لازم است مستند شود.

استاندارد ملی ایران به شماره ۲۷۰۰۱ مشخص می‌کند که نیاز است کنترل‌هایی که درمحدوده، مرزها و زمینه‌های ISMS وجود دارد، براساس مخاطره در نظر گرفته می‌شود. فرایند مدیریت مخاطرات امنیت اطلاعات می‌تواند این امر را برآورده سازد. رویکردهای بسیار دیگری نیز در این میان وجود دارد که می‌تواند به‌صورت موفقی در این سازمان پیاده‌سازی شود. سازمان در این بخش، از رویکردهایی استفاده می‌کند که پیامدهای آن برای هر کاربرد خاص از فرآیند مناسب باشد.

در ISMS پایه‌گذاری یک زمینه ارزشیابی مخاطره، توسعه طرح مقابله با مخاطره و پذیرش آن، بخشی از مرحله‌ی «طرح‌ریزی»، به‌شمار می‌رود. در مرحله « انجام» ISMS اقدامات و کنترل‌های صورت گرفته

به‌منظور کاهش مخاطره در سطحی قابل قبول لازم است و براساس طرح مقابله با مخاطره، انجام می‌شود. در مرحله «بررسی» ISMS مدیران خواهان تجدید نظر ارزشیابی مخاطره و مقابله با مخاطره براساس رخدادهای پیش‌آمده و بررسی تغییرات در این پیامدها هستند. در مرحله «اقدام»، هر یک از اقدامات مورد نیاز شامل کاربردهای اضافی از فرایند مدیریت مخاطرات امنیت اطلاعات در نظر گرفته می‌شود.
جدولی که در زیر به آن اشاره می‌شود، دربرگیرنده خلاصه‌ایی از فعالیت‌های مدیریت مخاطرات امنیت اطلاعات است که در ۴ مرحله از فرایندهای ISMS مطرح می‌شود.

جدول ۱- هم‌راستایی ISMS و فرآیند مدیریت مخاطرات امنیت اطلاعات

فرآیند ISMS	فرآیند مدیریت مخاطرات امنیت اطلاعات
طرح‌ریزی	زمینه‌سازی ارزشیابی مخاطره تدوین برنامه‌ی مقابله با مخاطره پذیرش مخاطره
انجام	پیاده‌سازی برنامه‌ی مقابله با مخاطره
بررسی	پایش و بازنگری مستمر مخاطره‌ها
اقدام	نگهداری و بهبود فرآیند مدیریت مخاطرات امنیت اطلاعات

۷ زمینه‌سازی[1]

۷-۱ ملاحظات کلّی

ورودی: تمامی اطلاعات در خصوص یک سازمان مربوط به زمینه‌سازی مدیریت مخاطرات امنیت اطلاعات
اقدام: زمینه داخلی و خارجی مدیریت مخاطرات امنیت اطلاعات باید پایه‌گذاری شود که شامل تنظیم معیارهای بنیادی برای مدیریت مخاطرات امنیت اطلاعات است. (۷-۲) محدوده و قلمرو تعریف شود (۷-۳) و می‌تواند عملکرد مناسب مدیریت مخاطرات اطلاعات سازمان را پایه‌گذاری کند. (۷-۴)
رهنمودهای پیاده‌سازی: لازم است که هدف مدیریت مخاطرات امنیت اطلاعات شناسایی شده و تمامی اثراتی که می‌تواند یک زمینه مشخص را به‌وجود آورد، مورد توجه قرار گیرد. این هدف عبارت است از:
- پشتیبانی از ISMS
- مدارک و شواهد قانونی، از تلاش انجام شده
- آماده سازی طرح تداوم کسب و کار
- آماده سازی طرح پاسخ به حوادث
- توصیف الزامات امنیت اطلاعات برای محصول، خدمات یا سازوکار.

1- context establishment

رهنمودهای پیاده‌سازی برای زمینه‌هایی که نیاز به پشتیبانی ISMS دارد، در بندهای ۷-۲، ۷-۳ و ۷-۴ مورد بحث قرار گرفته است.

یادآوری- استاندارد ملی ایران به شماره ۲۷۰۰۱ از اصطلاح «زمینه» استفاده نمی‌کند. گرچه، تمام بند ۷، مربوط به الزامات «تعریف محدوده و قلمرو ISMS» است. (بند ۴-۲-۱ الف) همچنین «تعریف خط‌مشی ISMS» و «تعریف رویکرد ارزشیابی مخاطره» در استاندارد ملی ایران به شماره ۲۷۰۰۱ نیز مورد توجه قرار گرفته است.

خروجی: مشخصه‌های معیار اصلی، محدوده و قلمرو و سازمان برای فرآیند مدیریت مخاطرات امنیت اطلاعات

۷-۲ معیارهای اصلی

۷-۲-۱ رویکرد مدیریت مخاطرات

براساس محدوده و اهداف مدیریت مخاطرات، می‌توان از رویکردهای گوناگون استفاده کرد. این رویکرد، برای هر تکرار، می‌تواند متفاوت باشد.

رویکرد مدیریت مخاطرات مناسب، باید به‌صورتی انتخاب یا توسعه داده شود که پوشش‌دهنده معیار اصلی از قبیل: معیار ارزیابی مخاطره، معیار اثر، معیار پذیرش مخاطره باشد.

علاوه براین، سازمان باید ارزشیابی کند که منابع لازم، برای موارد زیر در دسترس باشد:

- اجرای ارزشیابی مخاطره و پایه‌گذاری طرح مقابله با مخاطره
- تعریف و پیاده‌سازی خط‌مشی‌ها و روش‌های اجرایی، شامل پیاده‌سازی کنترل‌های انتخاب شده
- پایش کنترل‌ها
- پایش فرآیند مدیریت مخاطرات امنیت اطلاعات

یادآوری- به استاندارد ملی ایران به شماره ۲۷۰۰۱ (بند ۵-۲-۱) مربوط به شروط منابع برای پیاده‌سازی و عملیاتی کردن ISMS. مراجعه شود.

۷-۲-۲ معیار ارزیابی مخاطره

معیار ارزیابی مخاطره باید برای ارزشیابی مخاطره امنیت اطلاعات سازمان با در نظر گرفتن شرایط زیر توسعه یابد:

- ارزش راهبردی فرآیند اطلاعاتی کسب و کار
- حیاتی بودن دارایی‌های اطلاعاتی مرتبط
- الزامات قانونی و قراردادی، و تعهدات قراردادی
- عملیاتی بودن و اهمیت دسترس‌پذیری، محرمانگی و یکپارچگی برای کسب و کار
- انتظارات و ادراک ذی‌نفعان، پیامدهای منفی برای حسن نیت و اعتبار

علاوه براین، معیار ارزشیابی مخاطره می‌تواند به‌منظور اولویت‌بندی مقابله با مخاطره مورد استفاده قرار گیرد.

۷-۲-۳ معیار اثر

معیار اثر، باید باتوجه به میزان آسیب یا هزینه‌های وارده بر سازمان که توسط رویداد امنیت اطلاعات با توجه به موارد زیر، توسعه داده و مشخص شود:

- سطح طبقه بندی دارایی اطلاعات متأثر
- نقض امنیت اطلاعات (به‌عنوان مثال، از دست رفتن محرمانگی، یکپارچگی و دسترس‌پذیری)
- عملیات مخرب (داخلی یا طرف‌های سوم)
- زیان مالی و کسب و کار
- وقفه در طرح‌ها و ضرب‌الاجل‌ها
- آسیب به اعتبار
- نقض الزامات قانونی، مقرارتی یا تعهدات قراردادی

یادآوری- به استاندارد ملی ایران به شماره ۲۷۰۰۱ مرتبط با شناسایی معیار اثر برای از دست رفتن محرمانگی، یکپارچگی و دسترس پذیری، مراجعه شود.

۷-۲-۴ معیار پذیرش مخاطره

معیارپذیرش مخاطره باید توسعه داده و مشخص شود. معیار پذیرش مخاطره اغلب به خط‌مشی‌ها، مقاصد، اهداف و علایق ذی‌نفعان سازمان وابسته است.

سازمان باید مقیاس‌های خود برای سطوح پذیرش مخاطره را تعریف کند. موارد زیر در طی این توسعه، در نظر گرفته می‌شود:

- معیار پذیرش مخاطره می‌تواند شامل چندین آستانه با سطح مشخص مخاطره باشد. اما شروطی برای مدیران ارشد سازمان، برای پذیرش مخاطرات تحت شرایط پذیرفته شده است.
- معیار پذیرش مخاطره، می‌تواند مربوط به نسبت سود ارزیابی شده به مخاطره موجود باشد.
- معیار متفاوت پذیرش مخاطره می‌تواند در ارتباط با مجموعه‌های متفاوتی قرار گیرد که حاوی مخاطره است. به‌عنوان مثال، این نوع مخاطره‌ها، به‌صورتی است که نمی‌تواند در انطباق با این قوانین قرار گیرد، این در حالی است که پذیرش مخاطره‌های بزرگ، هنگامی مجاز است که بتوان شرایط قراردادی را در آن، در نظر گرفت.
- معیار پذیرش مخاطره می‌تواند شامل الزاماتی برای مقابله‌های اضافی آتی باشد. به‌عنوان مثال، مخاطره در صورتی قابل قبول است که مصوبه یا تأییدیه حاوی اقداماتی برای کاهش آن به سطح قابل قبول در دوره زمانی تعریف شده، وجود داشته باشد.

معیار پذیرش مخاطره، با توجه به مدت زمانی که انتظار می‌رود مخاطره وجود داشته، متفاوت است. به‌عنوان مثال مخاطره، ممکن است با فعالیت‌های کوتاه مدت یا موقت مرتبط باشد. معیار پذیرش مخاطره، براساس عوامل زیر برپا شود:

- شرایط کسب و کار
- جوانب قانونی و مقرراتی
- عملیات

- فناوری
- امور مالی
- عوامل اجتماعی و انسانی

یادآوری- معیار پذیرش مخاطره، با «معیار پذیرش مخاطرات و شناسایی سطح قابل قبول مخاطره» مشخص شده در استاندارد ملی ایران به شماره ۲۷۰۰۱ بند ۴-۲-۱ پ مرتبط است.

اطلاعات بیش‌تر در این زمینه در پیوست الف مشاهده می‌شود.

۷-۳ محدوده و قلمرو

سازمان باید محدوده و قلمرو مدیریت مخاطرات امنیت اطلاعات را تعریف کند.

محدوده فرآیند مدیریت مخاطرات امنیت اطلاعات برای اطمینان از این که تمامی دارایی‌های مرتبط، در ارزشیابی مخاطره در نظر گرفته شده باشد، نیاز به تعریف دارد. به علاوه قلمروها باید شناسایی شوند تا آن دسته از مخاطراتی که ممکن است در قلمرو رخ دهد، نشان داده شود. (به استاندارد ملی ایران به شماره ۲۷۰۰۱، بند ۴-۲-۱ الف مراجعه شود.)

اطلاعات مربوط به سازمان باید جمع‌آوری شود که بتواند محیط فعالیت سازمان و ارتباطش با فرآیند مدیریت مخاطرات امنیت اطلاعات را تعیین کند.

در زمان تعریف محدوده و قلمرو، سازمان باید اطلاعات زیر را مورد توجه قرار دهد:

- اهداف راهبردی کسب و کار سازمان، راهبردها و خط‌مشی‌ها
- فرآیندهای کسب و کار
- ساختار وکارکردهای سازمان
- الزامات قانونی، مقرراتی و قراردادی کاربردپذیر در سازمان
- خط‌مشی امنیت اطلاعات سازمان
- رویکرد کلی مدیریت مخاطرات سازمان
- دارایی‌های اطلاعات
- محل سازمان و مشخصه‌های جغرافیایی آن
- محدودیت‌های اثرگذار بر سازمان
- انتظارات ذی‌نفعان
- محیط اجتماعی- فرهنگی
- واسط‌ها (تبادل اطلاعات با محیط)

علاوه بر آن، سازمان باید برای هر استثنا از محدوده توجیه مناسبی ارائه دهد.

نمونه‌های محدوده مدیریت مخاطرات، ممکن است کاربرد[1]IT، زیر ساخت IT، یک فرآیند کسب و کار یا یک قسمت تعریف شده از سازمان باشد.

[1] Information Technology

یادآوری- محدوده و قلمرو مدیریت امنیت اطلاعات، وابسته به محدوده و قلمرو ISMS است که مطابق با استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، ۴-۲-۱ از پیوست الف آمده است)

اطلاعات بیش‌تر در این زمینه در پیوست الف آمده است.

۴-۷ سازمان مربوط به مدیریت مخاطرات امنیت اطلاعات

سازمان و مسئولیت‌های در نظر گرفته شده برای فرایند مدیریت مخاطرات امنیت اطلاعات باید برپا و نگهداری شود. عواملی که در زیر به آن‌ها اشاره می‌شود، نقش‌ها و مسئولیت‌های مهم سازمان است:

- تدوین فرآیند مدیریت مخاطرات امنیت اطلاعات مناسب برای سازمان
- شناسایی و تحلیل ذی‌نفعان
- تعریف نقش‌ها و مسئولیت‌های تمام طرف‌های داخلی و خارجی با سازمان
- پایه‌گذاری روابط لازم میان سازمان و ذی‌نفعان مانند واسطها به کارکردهای مدیریت مخاطرات سطح بالای سازمان (برای مثال: مدیریت مخاطرات عملیاتی)، همچون واسطها به پروژه‌ها یا فعالیت‌های مرتبط دیگر
- تعریف مسیرهای مقیاس تصمیم
- مشخصه‌های سوابقی که باید نگهداری شده

این سازمان، باید به‌وسیله مدیران مناسب سازمان، تایید شود.

یادآوری- استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، به تعیین و فراهم‌آوری منابع مورد نیاز برای پایه‌گذاری، پیاده‌سازی، عملیاتی کردن، پایش، بازنگری و نگهداری و بهبود ISMS (بند ۵-۲-۱ از پیوست الف) ملزم می‌کند. سازمان، برای عملکردهای مدیریت مخاطرات ممکن است به‌عنوان یکی از منابع مورد نیاز استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ درنظر گرفته شود.

۸ ارزشیابی مخاطره امنیت اطلاعات

۸-۱ توصیف کلی ارزشیابی مخاطرات امنیت اطلاعات

یادآوری- فعالیت ارزشیابی مخاطره به‌عنوان فرآیندی در استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ اشاره شده است.

ورودی: معیار اصلی، محدوده و قلمرو، و سازمان برای فرآیند مدیریت مخاطرات امنیت اطلاعات، که پایه‌گذاری شده است.

اقدام: مخاطرات باید تعیین، به‌صورت کمی و کیفی توصیف و نسبت به معیار ارزیابی مخاطره و اهداف مربوط به سازمان اولویت‌بندی شود.

رهنمودهای پیاده‌سازی: مخاطره، تلفیقی از پیامدهایی است که ممکن است از وقوع رویداد ناخواسته و احتمال وقوع رویداد پیروی کند. ارزشیابی مخاطره به‌صورت کمی یا کیفی مخاطره را توصیف می‌کند و مدیران را قادر می‌سازد تا براساس میزان جدی بودن مخاطره یا سایر معیارهای پایه‌گذاری شده، مخاطرات را اولویت‌بندی کنند.

ارزشیابی مخاطره، می‌تواند شامل فعالیت‌های زیر باشد:

- تعیین مخاطره (بند ۸-۲)
- تحلیل مخاطره (بند ۸-۳)
- ارزیابی مخاطره (بند ۸-۴)

ارزشیابی مخاطره، ارزش دارایی‌های اطلاعاتی را تعیین می‌کند، تهدیدهای کاربردی و آسیب‌پذیری‌هایی که وجود دارد (یا می‌تواند وجود داشته باشد) را شناسایی می‌کند، کنترل‌های موجود و اثر آن‌ها بر مخاطره‌ی شناسایی شده را شناسایی می‌کند، پیامدهای بالقوه را تعیین و در نهایت، مخاطره‌های برگرفته را اولویت‌بندی می‌کند و آن‌ها را در برابر مجموعه معیارهای ارزیابی مخاطره در زمینه پایه‌گذاری رتبه‌بندی می‌کند.

ارزیابی مخاطره اغلب در دو یا چند مرحله تکراری، انجام می‌شود. در مرحله اول، یک ارزیابی سطح بالا، به‌منظور شناسایی مخاطرات بالای بالقوه انجام می‌شود. مرحله بعدی می‌تواند شامل توجه عمیق‌تر به مخاطر ات بالقوه در مرحله اول باشد. در مواردی که این مرحله، اطلاعات ناکافی را برای ارزشیابی مخاطره فراهم کند، تحلیل مفصل‌تری نیز انجام می‌شود، ممکن است در قسمت‌هایی از کل محدوده از روش متفاوتی استفاده شود.

این به‌عهده سازمان است که رویکرد خود را برای ارزشیابی مخاطره براساس اهداف و مقاصدش از ارزشیابی مخاطره انتخاب کند.

بحث در خصوص رویکردهای ارزشیابی مخاطره امنیت اطلاعات، می‌تواند در پیوست ث یافت شود.

خروجی: فهرستی از مخاطرات ارزشیابی شده که براساس معیار ارزیابی مخاطره، اولویت‌بندی شده‌اند.

۸-۲ شناسایی مخاطره

۸-۲-۱ مقدمه‌ای بر شناسایی مخاطره

هدف از شناسایی مخاطره، تعیین این است که چه عاملی می‌تواند علت زیان بالقوه باشد و به‌دست آوردن بینش اینکه چگونه، کجا و چرا زیان ممکن است رخ دهد. گام‌هایی که در زیربند ۸-۲ در ادامه آورده شده، باید داده‌های ورودی برای فعالیت تحلیل مخاطره را جمع‌آوری کنند.

شناسایی مخاطره باید شامل مخاطراتی باشد که منبع آن‌ها تحت کنترل سازمان است یا خیر، گرچه منبع مخاطره یا علت آن مشهود نباشد.

یادآوری- فعالیت‌های توصیف شده در بندهای متوالی، در دستورات متفاوتی براساس روشگان به‌کار گرفته شده ممکن است هدایت شود.

۸-۲-۲ شناسایی دارایی‌ها

ورودی: محدوده و قلمرو برای ارزشیابی مخاطره‌ای که هدایت می‌شود، فهرستی از مؤسسان یا مالکین، موقعیت، کارکرد و سایر موارد.

اقدام: دارایی‌ها، در محدوده‌ی پایه‌گذاری شده، باید شناسایی شود. (مرتبط با استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷، زیربند ۴-۲-۱ از پیوست ت- ۱)

رهنمودهای پیاده‌سازی: دارایی، هر چیزی است که برای سازمان مهم دارای ارزش است و بنابراین، نیاز به حفاظت دارد. برای شناسایی دارایی‌ها، باید به ذهن سپرده شود که سامانه اطلاعاتی شامل چیزهایی بیش از سخت‌افزار و نرم‌افزار می‌شود.

شناسایی دارایی‌ها، باید در یک سطح مناسب از جزییاتی که اطلاعات کافی برای ارزشیابی مخاطره را فراهم می‌کند، انجام شود. سطح جزییات استفاده شده در شناسایی دارایی بر کل اطلاعات جمع‌آوری شده در طول ارزشیابی مخاطره، تاثیرگذار خواهد بود. این سطح کلی، در تکرارهای بیشتر ارزشیابی مخاطره می‌تواند تصحیح شود.

مالک دارایی برای هر دارایی باید شناسایی شده تا مسئولیت و پاسخگویی برای هر دارایی را ارائه دهد. ممکن است شخصی مالک اصلی دارایی نباشد. اما در خصوص تولید، توسعه، نگهداری، استفاده و امنیت آن به‌طور مناسب، پاسخگو است. مالک دارایی اغلب فردی مناسب برای تعیین ارزش دارایی برای سازمان است. (برای ارزیابی دارایی، به زیربند ۸-۳-۲ مراجعه شود.)

قلمرو بازنگری، منوط به دارایی‌ها سازمانی است که برای مدیریت شدن با فرآیند مدیریت مخاطرات امنیت اطلاعات تعریف شده است.

اطلاعات بیش‌تر در رابطه با شناسایی و ارزیابی دارایی‌های مرتبط با امنیت اطلاعات می‌تواند در پیوست ب یافت شود.

خروجی: فهرستی از دارایی‌ها که باید مدیریت مخاطرات شوند و فهرستی از فرآیندهای کسب و کار مرتبط با دارایی‌ها و متعلقات آن‌ها.

۸-۲-۳ شناسایی تهدیدات

ورودی: اطلاعات تهدیدات که از طریق بازنگری رخداد، مالکان دارایی، کاربران و سایر منابع از جمله کاتالوگ‌های تهدیدات بیرونی به‌دست آمده است.

اقدام: تهدیدها و منابع آن‌ها، باید شناسایی شوند. (مرتبط با استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷، زیربند ۴-۲-۱ از پیوست ت- ۲)

رهنمودهای پیاده‌سازی: تهدید، پتانسیل آسیب رساندن به دارایی‌ها از جمله اطلاعات، فرآیندها، سامانه‌ها و بنابراین سازمان‌ها را دارد. تهدیدها ممکن است منشاء طبیعی یا انسانی داشته باشند و به‌صورت تصادفی یا عمدی باشند. منابع تهدیدهای تصادفی یا عمدی باید شناسایی شوند. تهدید، ممکن است برخاسته از خارج سازمان باشد. تهدیدها، باید به‌طور کلی و بر مبنای نوع آن‌ها (برای مثال، اقدامات غیر مجاز، آسیب‌های فیزیکی، خسارات فنی) شناسایی شوند و سپس هر جا مناسب است، تهدیدهای مجزا در یک رده کلی، شناسایی شوند. به این معنی که هیچ تهدیدی نادیده گرفته نشده، شامل موارد غیر منتظره بوده، اما حجم کارهای لازم در آن محدود است.

برخی از تهدیدها ممکن است بر بیش از یک دارایی تأثیر بگذارند. در چنین مواردی، ممکن است براساس اینکه کدام دارایی تحت تأثیر قرار گرفته، سبب اثرات متفاوتی شوند.

ورودی برای شناسایی و تخمین تهدید از احتمال وقوع (به زیربند ۸-۳-۳ مراجعه شود.) ممکن است از مالکان دارایی یا کاربران، کارکنان منابع انسانی، مدیریت تسهیلات و متخصصان امنیت اطلاعات،

کارشناسان امنیت فیزیکی، سازمان‌های قانونی و سایر سازمان‌ها شامل نهادهای قانونی، متخصصان هواشناسی، شرکت‌های بیمه و مقامات دولتی ملی، به‌دست آید. جوانب زیست‌محیطی و فرهنگی هنگام نشان‌دهی تهدیدها باید در نظر گرفته شوند.

تجربه داخلی از رخدادها و ارزشیابی تهدیدهای گذشته در ارزشیابی کنونی باید در نظر گرفته شود. این نکته نیز ارزش‌مند است که از سایر کاتالوگ‌ها (که ممکن است برای سازمان یا کسب و کار، خاص باشند) به‌منظور کامل کردن فهرست تهدیدهای کلی در جایی که مرتبط است، استفاده شود. کاتالوگ‌های تهدید و آمارها، از سوی بخش‌های صنعتی، دولت‌های ملی، بخش‌های حقوقی، شرکت‌های بیمه و سایر موارد در دسترس است.

هنگام استفاده از کاتالوگ‌های تهدید یا نتایج ارزشیابی مخاطرات اخیر، باید از این نکته آگاه بود که تغییر مداوم تهدیدهای مرتبط، به‌خصوص هنگامی که محیط کسب و کار یا سامانه‌های اطلاعاتی تغییر می‌کند، وجود دارد.

اطلاعات بیش‌تر در رابطه با انواع تهدید می‌تواند در پیوست پ یافت شود.

خروجی: فهرستی از تهدیدها با شناسایی نوع و منبع تهدید.

۸-۲-۴ شناسایی کنترل‌های موجود

ورودی: مستندسازی کنترل‌ها، طرح‌های پیاده‌سازی مقابله با مخاطره

اقدام: کنترل‌های طرح‌ریزی شده و موجود باید شناسایی شود.

رهنمودهای پیاده‌سازی: شناسایی کنترل‌های موجود به‌منظور جلوگیری از کارهای غیر لازم یا هزینه باید ایجاد شود، به‌عنوان مثال در تکرار کنترل‌ها. علاوه بر آن، در هنگام شناسایی کنترل‌های موجود، یک وارسی برای اطمینان از اینکه کنترل‌ها به‌درستی کار می‌کنند باید ایجاد شود. منابع مربوط به گزارش‌های ممیزی ISMS موجود باید زمان سپری شده برای انجام این فعالیت‌ها را محدود کند. در صورتی که کنترل به‌نحوی که انتظار می‌رود، کار نکند، سبب آسیب‌پذیری می‌شود. ملاحظات باید برای وضعیتی که کنترل‌های انتخاب شده (یا راهبرد) در عملکرد شکست می‌خورند در نظر گرفته شود. در نتیجه کنترل‌های تکمیلی برای نشان دادن مؤثر بودن مخاطره شناسایی شده لازم است. با توجه به استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، در ISMS این امر با ارزشیابی اثربخشی کنترل پشتیبانی می‌شود. روش تخمین تأثیر کنترل، چگونگی کاهش احتمال تهدید یا سهولت بهره‌جویی آسیب‌پذیری اثر رخداد است. بازنگری‌های مدیریتی و گزارش‌های ممیزی اطلاعات لازم در خصوص اثربخشی کنترل‌های موجود را ارائه می‌دهند.

کنترل‌هایی که طراحی شده‌اند تا براساس طرح‌های مقابله و مقابله با مخاطره پیاده‌سازی شوند باید به همان صورت که دیگر کنترل‌ها پیاده‌سازی شده، در نظر گرفته شوند.

کنترل موجود یا طرح‌ریزی شده ممکن است به‌عنوان غیر مؤثر، یا ناکافی یا بدون توجیه تعیین شوند. کنترل باید برای تعیین اینکه آیا باید حذف یا جایگزین با کنترل مناسب دیگر شود، وارسی شود.؛ یا به‌دلایل مالی در جای خود باقی بماند.

برای شناسایی کنترل‌های طرح‌ریزی شده یا موجود، فعالیت‌های زیر، مفید هستند:

- بازنگری مستنداتی که حاوی اطلاعاتی در خصوص کنترل‌ها. (به‌عنوان مثال، طرح‌های پیاده‌سازی مقابله با مخاطره) در صورتی که فرآیند مدیریت امنیت اطلاعات، به‌خوبی کنترل‌های موجود یا طرح‌ریزی شده را مستند کند و وضعیت پیاده‌سازی آن‌ها در دسترس باشد.
- وارسی با افراد مسئول امنیت اطلاعات (به‌عنوان مثال مأمور امنیت اطلاعات، کارشناس امنیت سامانه اطلاعات، مدیر ساخت یا مدیر اجرایی) و کاربران باید دست به بررسی این طرح زده و از طرفی نیز، این نکته را مورد توجه قرار می‌دهند که کدام یک از این طرح‌ها می‌تواند برای ارزیابی سامانه اطلاعاتی به‌کار رود.
- اجرایی کردن ارزیابی‌ها در محل، برای کنترل عوامل فیزیکی، مقایسه‌های اجرایی و ارائه فهرستی از طرح‌های کنترلی، ارزیابی این عوامل و بررسی این نکته که آیا این موارد به‌درستی کار می‌کنند یا خیر.
- مرور نتایج به‌دست آمده از این برنامه‌های عملی

خروجی: فهرستی از تمامی کنترل‌های طرح‌ریزی شده و موجود، پیاده‌سازی و وضعیت استفاده از آن‌ها

۸-۲-۵ شناسایی آسیب‌پذیری‌ها

ورودی: فهرستی از تهدیدهای موجود، فهرست دارایی‌ها و کنترل موجود

اقدام: آسیب‌پذیری‌هایی که از طریق این تهدیدها می‌تواند بهره‌جویی شده و باعث آسیب به دارایی‌های سازمان شود باید شناسایی شوند. (مرتبط با استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷، زیربند ۴-۲-۱ از پیوست ت- ۳)

رهنمودهای پیاده‌سازی: آسیب پذیری‌ها ممکن است در حوزه‌های زیر شناسایی شوند:

- سازمان
- فرآیندها و روش‌های اجرایی
- رویه‌های مدیریتی
- کارکنان
- محیط فیزیکی
- پیکربندی سامانه اطلاعاتی
- سخت‌افزار، نرم‌افزار یا تجهیزات ارتباطی
- وابستگی به طرف‌های خارجی

وجود آسیب‌پذیری، نمی‌تواند به خودی خود سبب آسیب شود، از آن جا که نیاز است که تهدیدی برای بهره‌جویی آن حاضر شود. یک آسیب‌پذیری که دارای هیچ گونه تهدیدی در خود نیست نیازی به پیاده‌سازی کنترل ندارد، اما باید برای تغییرات صورت گرفته تشخیص و پایش شود. باید توجه شود که پیاده‌سازی ناصحیح یا بد عمل کردن کنترل‌ها یا استفاده نادرست از کنترل خود می‌تواند یک آسیب‌پذیری باشد. کنترل بسته به محیطی که در آن عمل می‌کند می‌تواند مؤثر یا غیرمؤثر باشد. در مقابل، تهدیدی که آسیب‌پذیری ندارد، ممکن است منجر به مخاطره نشود.

آسیب‌پذیری می‌تواند به خصوصیت‌هایی از دارایی‌ها که می‌تواند استفاده شود یا با هدفی غیر از آنچه که در هنگام خرید یا ساخت دارایی مد نظر بوده، ارتباط داشته باشد. نیاز است آسیب‌پذیری‌هایی که از منابع متفاوتی ناشی می‌شوند، در نظر گرفته شوند، برای مثال آن‌هایی که برای دارایی ذاتی یا غیر ذاتی هستند. نمونه‌هایی از آسیب‌پذیری‌ها و روش‌ها برای ارزشیابی آسیب‌پذیری در پیوست ت یافت می‌شود.

خروجی: فهرستی از آسیب‌پذیری‌های مرتبط با دارایی‌ها، تهدیدها و کنترل‌ها؛ فهرستی از آسیب‌پذیری‌هایی که ارتباطی با هیچ یک از تهدیدهای شناسایی شده برای بازنگری ندارد.

۸-۲-۶ شناسایی پیامدها

ورودی: فهرستی از دارایی‌ها، فهرستی از فرآیندهای کسب و کار و فهرستی از تهدیدها و آسیب‌پذیری‌ها و موارد وابسته به دارایی‌ها و متعلقات آن‌ها

اقدام: پیامدهایی که باعث از میان رفتن حس اعتماد، یکپارچگی شده و هیچ گونه دارایی در آن، شناسایی نمی‌شود. (مرتبط با استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷، زیربند ۴-۲-۱ از پیوست ت)

رهنمودهای پیاده‌سازی: پیامد می‌تواند از دست رفتن اثربخشی، شرایط عملیاتی نامطلوب، از دست رفتن کسب و کار، شهرت و اعتبار، خسارت و غیره باشد.

در این فعالیت، خسارات یا پیامدهای سازمان که می‌تواند نتیجه حاصل از یک سناریوی رخداد است، شناسایی می‌شود. سناریوی رخداد توصیفی از یک تهدید است که از یک آسیب‌پذیری مشخص یا مجموعه‌ای از آسیب‌پذیری‌ها در خصوص رخداد امنیت اطلاعات بهره‌جویی می‌کند. (استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷ بند۱۳) اثر ناشی از سناریوی رخداد باید با در نظر گرفتن معیار اثر تعریف شده در فعالیت برقراری زمینه تعیین شود. این بخش می‌تواند بر روی یک یا چند دارایی، یا قسمتی از دارایی اثر بگذارد. بنابراین دارایی‌ها می‌توانند دارای مقادیر تخصیص شده‌ای برای هزینه‌های مالی در صورتی که به‌دلیل پیامدهای کسب و کار آسیب دیده یا به مخاطره افتاده، باشد. پیامدها ممکن است موقت یا در شرایط آسیب دارایی، دائم باشد.

یادآوری- استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، وقوع سناریوی رخداد همچون نقص امنیتی را توصیف می‌کند.

سازمان باید پیامدهای عملیاتی سناریوهای رخداد را در این شرایط شناسایی کند (اما محدود نیست به):

- زمان مرمت و بررسی
- زمان (کاری) از دست رفته
- فرصت از دست رفته
- سلامت و ایمنی
- هزینه مالی مهارت‌های ویژه برای مرمت خسارات
- شهرت و اعتبار

جزییات مربوط به ارزشیابی این آسیب‌پذیری‌های فنی، در بخش ۸-۳ ارزشیابی اثر، یافت می‌شود.

خروجی: فهرستی از سناریوهای رخداد مربوط با دارایی‌ها و فرآیندهای کسب و کار

۸-۳-۱ روش‌های تحلیل مخاطره

تحلیل مخاطره ممکن است در حالات متفاوتی از جزییات، بسته به حیاتی بودن دارایی‌ها، گستره آسیب‌پذیری‌های شناخته شده و رخدادهای اولیه که سازمان را دربر می‌گیرد، انجام شود. روش تحلیل مخاطره ممکن است بسته به شرایط کمی یا کیفی یا تلفیقی از آن‌ها باشد. در تحلیل کیفی اغلب ابتدا به‌منظور به‌دست آوردن شاخص عمومی سطح مخاطره و آشکار کردن مخاطرات اصلی، استفاده می‌شود. بعدها ممکن است ضروری باشد که تحلیل خاص‌تر یا کمی بر روی مخاطرات اصلی انجام شود، زیرا به‌طور معمول پیچیدگی و هزینه کمتر برای انجام تحلیل کیفی نسبت به تحلیل کمی وجود دارد.

قالب تحلیل باید شامل معیارهای ارزیابی مخاطره که به‌عنوان قسمتی از پایه‌گذاری زمینه است، توسعه داده شود.

جزییات بیشتر از روش‌های تحلیل هم اکنون توصیف می‌شود.

الف- تحلیل کیفی

تحلیل مخاطره کیفی از مقیاس طبقه‌بندی ویژگی‌ها برای توصیف گستره پیامدها بالقوه (برای مثال، پایین، متوسط و بالا) و احتمالی که این پیامدها رخ خواهند داد، استفاده می‌کند. مزیّت تحلیل کیفی، سهولت فهم کارکنان مربوط است. در حالی که وابستگی به انتخاب عینی یک مقیاس از معایب آن است. این گونه مقیاس‌ها، می‌تواند برای شرایط مناسب و توصیف‌های متفاوت برای مخاطره‌های گوناگون اتخاذ یا ترتیب داده شود. ارزیابی کیفی در موارد زیر، مورد استفاده قرار می‌گیرد:

- به‌عنوان یک فعالیت کنترل اولیه برای شناسایی مخاطراتی که نیازمند تحلیل بیش‌تر هستند.
- در مواردی -که این نوع تحلیل، برای تصمیمات مناسب است.
- در مواردی که داده‌های عددی یا منابع موجود، برای تحلیل کمّی مخاطره، ناکافی باشند.

تحلیل کیفی باید در صورت در دسترس بودن از اطلاعات و داده‌های واقعی، استفاده کند.

ب - تحلیل کمّی

تحلیل کمّی از مقیاسی با مقادیر واقعی (به‌غیر از مقیاس‌های توصیفی که در تحلیل مخاطره کیفی استفاده می‌شود) برای پیامدها و احتمالات با استفاده از داده‌هایی از منابع مختلف استفاده می‌کند. کیفیت تحلیل وابسته به صحت و کامل بودن مقادیر عددی و اعتبار مدل‌های مورد استفاده است. تحلیل کمی در بسیاری از موارد کمی، از داده‌های رخداد پیشین استفاده کرده و از مزایایی که وابسته به اهداف امنیت اطلاعات و سایر نگرانی‌های سازمان است، استفاده می‌کند. نکته منفی موجود مربوط به عدم وجود داده‌های کافی در خصوص مخاطره‌های جدید و یا ضعف اطلاعات امنیتی است. این عامل، به‌ویژه در مواردی روی می‌دهد که داده‌های واقعی و قابل ارزیابی، موجود نبوده و همین امر می‌تواند اعتبار سازمان را در ارزیابی این مخاطرات به‌خطر اندازد.

روشی که در آن پیامدها و احتمالات موجود، مورد توجه قرار گرفته شده و از طرفی نیز این عوامل، در ترکیب با هم قرار می‌گیرند، به‌صورتی است که بر مبنای نوع مخاطره و هدف ارزیابی آن، متفاوت است.

احتمال و گستردگی این‌گونه از پیامدها و احتمال بروز آن‌ها نیز به‌صورت اثرگذاری در این تحلیل‌ها مطرح می‌شود.

۸-۳-۲ ارزیابی پیامدها

ورودی: فهرستی از سناریوهای وابسته که شامل شناسایی تهدیدها، در معرض مخاطره بودن آن‌ها، دارایی‌های موجود و پیامدهای حاکم بر روی دارایی‌ها و فرآیندهای کسب و کار است.

اقدام: اثرات کسب و کار موجود بر روی سازمان برگرفته از وقایع ناشی از امنیت اطلاعات واقعی و احتمالی است که باید به خوبی ارزیابی شده و از طرفی نیز موارد دیگری از این دست را نیز مورد توجه قرار دهد: نقض امنیت اطلاعات، مانند از میان رفتن اعتمادپذیری، انجام یا در دسترس بودن دارایی‌ها، (مرتبط با استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷، زیربند ۴-۲-۱ از پیوست ت- ۱)

رهنمودهای پیاده‌سازی: پس از شناسایی تمامی این دارایی‌ها، مقادیر در نظر گرفته شده در این زمینه، همواره مورد توجه قرار گرفته و از طرفی نیز پیامدها موجود، مورد توجه قرار می‌گیرد. مقادیر به‌دست آمده از طریق این اثرات کسب و کار، در قالب عوامل کیفی و کمّی مورد توجه قرار گرفته، اما هر یک از روش های ارزیابی عوامل مالی، می‌تواند اطلاعات بیش تری را برای تصمیم‌گیری فراهم آورده و بنابراین تسهیلات لازم را برای تصمیم‌گیری هر چه بیش‌تر ارایه می‌کند.

ارزیابی دارایی، منوط به طبقه‌بندی تمامی این دارایی ها، براساس اهمیت این دارایی ها و اجرایی کردن اهداف کسب و کار در سازمان است. در گام بعدی ارزش‌یابی از طریق دو مقیاس شناسایی می‌شود.

- مقدار جایگزین دارایی: هزینه بازیابی و جایگزین کردن اطلاعات موجود (در صورت امکان)
- پیامدهای کسب و کار مربوط به حذف و یا ترکیب دارایی‌ها، همچون پیامدهای کسب و کار معکوس و یا عوامل قانونی برای ارزیابی، تغییر یا عدم دسترس بودن اطلاعات و سایر دارایی‌های موجود در این بخش.

این نوع ارزشیابی می‌تواند از طریق تحلیل اثرات کسب و کار، شناسایی شود. این مقدار که از طریق پیامدهای کسب و کار شناسایی می‌شود، بسیار بیش‌تر از هزینه‌های ساده جایگزینی، خواهد بود، البته این امر وابسته به اهمیت دارایی‌های موجود در سازمان و پوشش‌دهی اهداف مربوط به آن است.

ارزشیابی دارایی، عامل کلیدی در ارزیابی اثر ناشی از یک رویداد است. زیرا، این رویداد می‌تواند اثرات بسیاری را بر روی یک دارایی یا بخشی از آن بگذارد. (دارایی‌های وابسته) تهدیدهای متفاوت و عوامل در معرض مخاطره نیز دارای اثرات گوناگونی بر روی این دارایی‌ها هستند که از جمله آن‌ها، می‌توان به از دست دادن محرمانگی، یکپارچگی و در دسترس‌پذیری دارایی‌ها، اشاره کرد. ارزیابی پیامدها موجود نیز با توجه به تحلیل‌های کسب و کار صورت گرفته، منوط به این عوامل ارزیابی است.

اثرات ناشی از این پیامدها و عوامل کسب و کار، مربوط به الگوسازی نتایج حاصل از یک رویداد یا مجموعه‌ای از رویدادها و همچنین سایر مطالعات تجربی و داده‌های گذشته است.

پیامدهای به‌دست آمده در این زمینه، می‌تواند براساس معیار پول، عوامل فنی و انسانی یا سایر موارد در زمان، مکان، گروه و موقعیت‌های متفاوت مورد نیاز باشد.

اطلاعات بیش‌تر در خصوص ارزیابی دارایی و اثرات ناشی از آن، در پیوست ب وجود دارد.

خروجی: فهرستی از این پیامدها و سناریوهای مربوط به آن نیز منوط به این معیارها است.

۸-۳-۳ ارزشیابی احتمال رخداد

ورودی: فهرستی از سناریوهای رخداد مرتبط و شناسایی شده شامل شناسایی تهدیدها، دارایی‌های اثرپذیر، آسیب‌پذیری‌ها و پیامدهای بهره‌جویی شده دارایی‌ها و فرآیندهای کسب و کار. همچنین فهرستی از تمام کنترل‌های موجود و طرح‌ریزی شده، اثربخشی، پیاده‌سازی و وضعیت استفاده از آن‌ها.

اقدام: احتمال وقوع سناریوهای گوناگون ارزیابی می‌شود. (مرتبط با استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷، زیربند ۴-۲-۱ از پیوست ت- ۲)

رهنمودهای پیاده‌سازی: پس از شناسایی سناریوی رخداد، ارزیابی احتمال هر سناریو و اثر وقوع با استفاده از فنون تحلیل کیفی و کمّی ضروری است. که این امر باید تعداد دفعات وقوع تهدید و چگونگی بهره‌جویی آسان از آسیب‌پذیری را با در نظر گرفتن موارد زیر به‌حساب آورد:

- آمار کاربردپذیری و تجربه برای احتمال تهدید
- برای منابع تهدید تعمدی: انگیزش و قابلیت‌ها که می‌تواند در طی زمان، تغییر کند و منابع در دسترس برای حمله‌کننده‌های احتمالی و نیز درک جذابیت و آسیب‌پذیری دارایی‌ها برای یک حمله‌کننده احتمالی
- منابع تهدید تصادفی: عوامل جغرافیایی (مانند نزدیکی به دستگاه (کارخانجات) شیمیایی و مواد نفتی) شرایط آب و هوایی بسیار شدید احتمالی و عواملی که می‌تواند بر خطاهای انسانی و استفاده نادرست از تجهیزات تأثیر گذارد.
- آسیب پذیری‌های انفرادی و جمعی

به‌عنوان مثال، سامانه اطلاعاتی ممکن است دارای قابلیت آسیب‌پذیری تهدیدهای ناشناس برای هویت کاربر و استفاده نادرست از منابع باشد. ممکن است آسیب‌پذیری‌های ناشناس برای هویت کاربر، به‌دلیل نداشتن احراز هویت کاربر زیاد باشد. از طرف دیگر، احتمال استفاده نادرست از منابع، با وجود نداشتن اهراز هویت ممکن است کم باشد زیرا راه‌های استفاده نادرست از منابع محدود است.

با توجه به نیاز به میزان دقت، دارایی‌ها می‌توانند گروه‌بندی شده یا در صورت نیاز دارایی‌ها را به مؤلفه‌هایشان جدا کرد و سناریوها را به مؤلفه‌ها نسبت داد. به‌عنوان مثال، در سرتاسر موقعیت‌های جغرافیایی، ماهیت تهدیدها برای انواع مشابهی از دارایی‌های ممکن است تغییر کند، یا اثربخشی کنترل‌های موجود ممکن است متغیر باشد.

خروجی: احتمال سناریوهای رخداد (کیفی یا کمّی)

۸-۳-۴ تعیین سطح مخاطره

ورودی : فهرستی از سناریوهای رخداد به همراه پیامدهای وابسته به دارایی‌ها و فرآیندهای کسب و کار و احتمال آن‌ها (کیفی یا کمی)

اقدام: سطح مخاطره برای تمامی سناریوهای رخداد مربوط باید تعیین شود. (مرتبط با استاندارد ملی ایران به شماره ۲۷۰۰۱: ۱۳۸۷، زیربند ۱-۲-۴ از پیوست ث -۴)

رهنمودهای پیاده‌سازی: تحلیل مخاطره، مقادیری را به احتمال و پیامد مخاطره تخصیص می‌دهد. این مقادیر، ممکن است کمّی یا کیفی باشد علاوه براین برای تحلیل مخاطره می‌توان، ارزش سود در نظر گرفته شده برای ذی‌نفعان و سایر متغیرها را مورد توجه قرارداد. مخاطره تخمینی، ترکیبی از احتمال سناریوی رخداد و پیامدهای آن است.

مثال‌های مختلفی از روش‌ها و رویکردهای تحلیل مخاطره امنیت اطلاعات را در پیوست ث می‌توان دید.

خروجی: فهرستی از مخاطره‌ها به همراه سطوح ارزشی تخصیص داده شده.

۴-۸ ارزشیابی مخاطره

ورودی: فهرستی از مخاطره‌ها به همراه سطوح ارزشی تخصیص داده شده و معیارهای ارزشیابی مخاطره.

اقدام: سطوح مخاطره باید با معیار ارزیابی مخاطره و معیار پذیرش آن، مقایسه شود. (مرتبط با استاندارد ملی ایران به شماره ۲۷۰۰۱: ۱۳۸۷ ، زیربند ۱-۲-۴ از پیوست ث -۴)

رهنمودهای پیاده‌سازی: ماهیت تصمیمات مربوط به ارزشیابی مخاطره و معیارهای ارزشیابی مخاطره، برای اتخاذ تصمیم‌هایی که در هنگام برقراری زمینه تصمیم‌گیری می‌شود، می‌تواند استفاده شود. این تصمیمات و زمینه در این مرحله که شناخت از مخاطره‌های خاص شناسایی شده، بیشتر است، باید با جزئیات بیشتر بازبینی شود. برای ارزشیابی مخاطره‌ها، سازمان‌ها باید مخاطره تخمینی (با استفاده از روش‌ها و رویکردهای منتخب مشابه آن‌چه در پیوست ث مطرح شده است.) را با معیارهای ارزشیابی مخاطره تعریف شده در طی برقراری زمینه، باید مقایسه کند.

معیارهای ارزشیابی مخاطره، مورد استفاده در تصمیم‌گیری، باید با زمینه مدیریت مخاطرات امنیت اطلاعات داخلی و خارجی سازگار بوده و اهداف سازمان و نظرات ذی‌نفعان را نیز، در نظر گرفته باشد. تصمیمات گرفته شده در اقدام ارزشیابی مخاطره به‌طور عمده بر پایه سطح قابل قبول مخاطره استوار است. بنابراین پیامدها، احتمال و درجه اطمینان در شناسایی و تحلیل مخاطره باید به‌خوبی در نظر گرفته شود. تجمیع چندین مخاطره کوچک یا متوسط می‌تواند منجر به مخاطره کلی بزرگتر شود و باید به‌خوبی، اداره شود.

ملاحظات باید شامل موارد زیر باشد:

- ویژگی‌های امنیت اطلاعات: در صورتی‌که یک ضابطه مرتبط با سازمان نباشد. (مانند فقدان محرمانگی) در نتیجه تمامی مخاطره اثرگذار در این ضابطه نیز مرتبط نخواهد بود.
- اهمیت فرآیند کسب و کار یا اقدام پوشش داده شده به‌وسیله دارایی ویژه یا مجموعه‌ای از دارایی‌ها: اگر فرایندی با اهمیت پایین تعیین شده باشد، مخاطره مرتبط با آن نسبت به مخاطره‌ای که به فرایندها یا اقدام‌ها اثر مهمتری دارد، ملاحظات کمتری باید در نظر گرفته شود.

ارزشیابی مخاطره، از فهم مخاطره به‌دست آمده به‌وسیله تحلیل‌های مخاطره، برای تصمیم‌گیری در خصوص اقدامات بعدی استفاده می‌کند. تصمیمات باید شامل موارد زیر باشد:

- آیا یک اقدام باید انجام گیرد.
- در اولویت‌بندی مقابله با مخاطره، سطوح تخمینی مخاطره در نظر گرفته شود.

در مرحله ارزشیابی مخاطره، الزامات قانونی، حقوقی و قراردادی، از جمله مؤلفه‌هایی هستند که علاوه بر مخاطره تخمینی باید در نظر گرفته شوند.

خروجی: فهرستی از مخاطره‌های اولویت‌بندی شده مطابق با معیارهای ارزشیابی مخاطره در ارتباط با سناریوهای رخداد که منجر به آن مخاطره شده است.

۹ مقابله با مخاطره امنیت اطلاعات

۹-۱ توصیف کلی مقابله با مخاطره

ورودی : فهرستی از مخاطره‌های اولویت‌بندی شده مطابق با معیارهای ارزشیابی مخاطره در ارتباط با سناریوهای رخداد که منجر به آن مخاطره شده است.

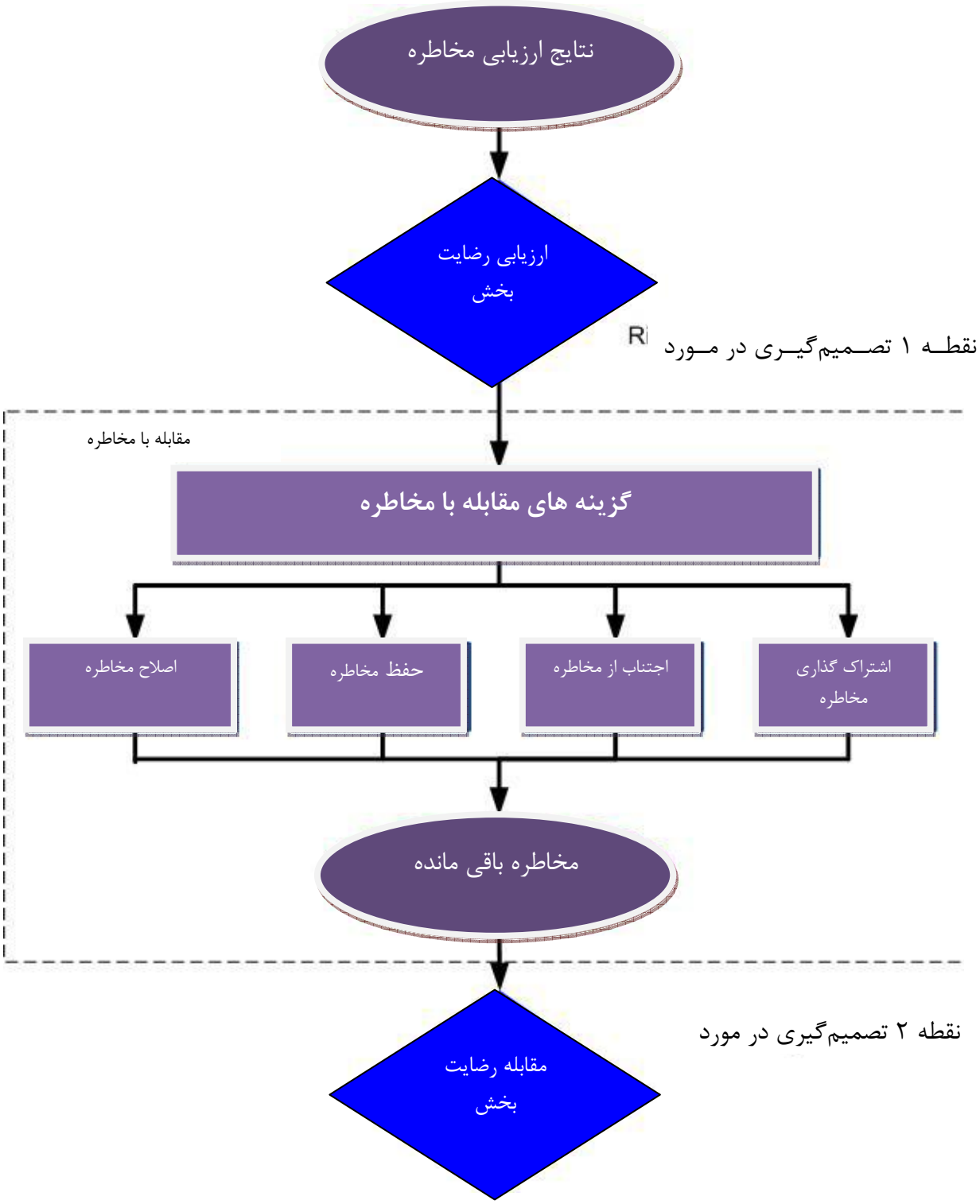
اقدام: کنترل‌هایی برای کاهش، حفظ، اجتناب نمودن یا انتقال(اشتراک) مخاطره باید انتخاب شده و طرح مقابله با مخاطره تعریف شود.

رهنمودهای پیاده‌سازی:

چهار گزینه برای ارزشیابی مخاطره وجود دارد که عبارتند از: اصلاح مخاطره (به زیربند ۹-۲ رجوع شود.) حفظ مخاطره (به زیربند ۹-۳ رجوع شود.) اجتناب از مخاطره (به زیربند ۹-۴ رجوع شود.) و اشتراک-گذاری مخاطره (به زیربند ۹-۵ رجوع شود.)

یادآوری- استاندارد ملی ایران به شماره ۲۷۰۰۱ (زیربند ۴-۲-۱ از پیوست ج ۲) از واژه پذیرش مخاطره به جای حفظ مخاطره استفاده می‌کند.

شکل ۳ اقدام مقابله با مخاطره، اطلاعات نشان‌داده شده در شکل۲ را مطابق با فرآیند مدیریت مخاطرات نمایش می‌دهد.



شکل۳- اقدام مقابله با مخاطره

گزینه‌های مقابله با مخاطره، باید براساس خروجی‌های ارزیابی مخاطره، هزینه مورد انتظار، برای پیاده-سازی گزینه‌ها و منافع مورد انتظار از این اختیارات، انتخاب شوند.
چنین گزینه‌هایی در زمانی که کاهش بزرگ در مخاطره‌ها با هزینه‌های کم مربوط می‌تواند حاصل شود، باید پیاده‌سازی شوند. گزینه‌های بیشتر برای بهبود ممکن است غیر اقتصادی باشد و برای توجیه‌پذیری آن نیاز به دادرسی خواهد بود.
به‌طور کلی پیامدهای مضر مخاطره‌ها، باید معقولیت عملی بودن و صرف‌نظر از هر معیار کامل را به‌خوبی ایجاد کند. مدیریت باید مخاطره‌های نادر ولی سخت را در نظر بگیرد. در چنین مواردی، کنترل‌هایی که به‌طور کامل بر پایه‌های اقتصادی، توجیه‌پذیر نیستند ممکن است نیاز به پیاده‌سازی داشته باشند. (به‌عنوان مثال، کنترل‌های تداوم کسب و کار در نظر گرفته شده برای پوشش مخاطره‌های بزرگ ویژه)
چهار گزینه‌ی مقابله با مخاطره دو به دو ناسازگار نیستند. گاهی اوقات سازمان می‌تواند از مزایای ناشی از ترکیب این گزینه‌ها نظیر کاهش احتمال مخاطره‌ها، کاهش پیامدها و اشتراک یا حفظ مخاطره‌های باقیمانده بهره‌مند شود.
برخی از مقابله با مخاطره، بیش از یک مخاطره را می‌تواند پوشش دهد. (مانند آموزش و آگاهی از امنیت اطلاعات) طرح مقابله با مخاطره باید به‌طور صریح شناسایی اولویت مرتب‌سازی هر یک از مقابله‌های مخاطره که باید پیاده‌سازی شود به همراه زمان‌بندی آن‌ها را تعریف کند. اولویت‌بندی‌ها، با استفاده از فنون متفاوت شامل رتبه‌بندی و تحلیل هزینه-سود می‌تواند پیاده‌سازی شود. تصمیم‌گیری برای ایجاد توازن میان هزینه پیاده‌سازی کنترل‌ها و تخصیص بودجه بر عهده مدیران سازمان است.
شناسایی کنترل‌های موجود ممکن است تعیین کند که کنترل‌های موجود از نیازهای فعلی از دیدگاه مقایسه‌های هزینه، شامل حفظ، تجاوز می‌کند. اگر حذف کنترل‌های غیرضروری و افزونه درنظر گرفته شود (به‌طور خاص اگر کنترل‌ها هزینه نگهداری زیادی داشته باشند) امنیت اطلاعات و مؤلفه‌های هزینه باید در نظر گرفته شوند. از آن‌جایی‌که کنترل‌ها ممکن است مابقی کنترل‌ها را تحت تأثیر قرار دهند، حذف کنترل‌های افزونه می‌تواند امنیت کلی در مکان را کاهش دهد. علاوه بر این باقی‌گذاردن کنترل‌های غیر ضروری و افزونه در مکان نسبت به حذف آن‌ها ممکن است ارزان‌تر باشد.
گزینه‌های مقابله با مخاطرها که باید در نظر گرفته شوند:

- چگونه مخاطره به‌وسیله طرف‌های تحت تأثیر درک می‌شود.
- بیشترین راه‌های مناسب برای ارتباط با طرف‌های تحت تأثیر

پیاده‌سازی زمینه (به بند ۷-۲ معیار ارزیابی مخاطره رجوع شود.) اطلاعاتی را برای الزامات قانونی و مقرراتی به‌همراه آن‌چه سازمان نیاز دارد برآورده کند را فراهم می‌کند.
برآورده‌سازی مخاطره‌ی سازمان‌ها اشکال دارد و گزینه‌های مقابله برای محدود کردن این امکان باید پیاده‌سازی شوند. تمامی محدودیت‌ها سازمانی، فنی، ساختاری و غیره که در اقدام پیاده‌سازی زمینه شناسایی شده‌اند باید در طی مقابله با مخاطره در نظر گرفته شوند. زمانی که طرح مقابله با مخاطره، تعریف می‌شود، نیاز به تعیین مخاطره‌های باقی مانده وجود دارد. این کار شامل به‌روزرسانی یا تکرار ارزیابی مخاطره، در نظر گرفتن اثرات مورد انتظار از مقابله با مخاطره پیشنهادی می‌شود. مخاطره‌های

باقی‌مانده که هنوز معیارهای پذیرش سازمان را برآورده نکرده‌اند، ممکن است به تکرار بیشتر مقابله با مخاطره قبل از روند پذیرش مخاطره نیاز داشته باشند.
اطلاعات بیش‌تر در این خصوص در استاندارد ملی ایران به شماره ۲۷۰۰۲: ۱۳۸۷، زیربند ۰-۳ وجود دارد.
خروجی: طرح مقابله با مخاطره و موضوع مخاطره‌های باقی‌مانده به منظور تصمیم‌گیری پذیرش از سوی مدیران سازمان.

۹-۲ اصلاح مخاطره

اقدام: سطح مخاطره، باید از طریق معرفی، حذف یا اصلاح کنترل مدیریت شود بنابراین مخاطره باقیمانده می‌تواند ارزیابی مجدد شود که به سطح قابل قبولی برسد.
رهنمودهای پیاده‌سازی: کنترل‌های مناسب و قابل توجیه، باید به‌منظور برآورده کردن الزامات شناسایی شده با ارزیابی و مقابله با مخاطره انتخاب شود. این انتخاب باید معیار پذیرش مخاطره و همچنین الزامات قانونی، مقرراتی و قراردادی را در نظر بگیرد. این انتخاب نیز باید هزینه و زمان‌بندی برای پیاده‌سازی کنترل‌ها، یا جنبه‌های فنی، محیطی و فرهنگی را درنظر گرفته باشد. در اغلب موارد، کاهش هزینه کلی مالکیت یک سامانه با انتخاب مناسب کنترل‌های امنیت اطلاعات امکان‌پذیر است.
به‌طور کلی کنترل‌ها، ممکن است یک یا چند نوع از محافظت‌های اصلاح، حذف، پیشگیری، کاهش اثرات، بازداری، تشخیص، بازیابی، پایش و آگاهی را فراهم کند. در طی انتخاب کنترل‌ها، وزن هزینه مالکیت، پیاده‌سازی، مدیریت، کارکرد، پایش و نگهداری کنترل‌ها در برابر ارزش دارایی که باید محافظت شوند مهم است. علاوه براین، برگشت‌پذیری سرمایه‌گذاری در بخش‌های کاهش مخاطره و پتانسیل بهره‌برداری از فرصت‌های کسب و کار جدید حاصل شده به‌وسیله کنترل‌های مشخص باید در نظر گرفته شود. به‌علاوه باید با توجه به مهارت‌های ویژه که ممکن است برای تعریف و پیاده‌سازی کنترل‌های جدید یا اصلاح کنترل‌های موجود مورد نیاز است، در نظر گرفته شود.
استاندارد ملی ایران به شماره ۲۷۰۰۲: ۱۳۸۷ دربرگیرنده اطلاعات مفصل در این زمینه است.
محدودیت‌های زیادی وجود دارد که انتخاب کنترل‌ها را می‌تواند تحت تأثیر قرار دهد. محدودیت‌های فنی نظیر الزامات کارایی، قابلیت مدیریت (الزامات پوششی کارکردی)، مسئله سازگاری، ممکن است مانع استفاده از کنترل معینی شود یا می‌تواند با احساس غلط امنیتی، خطای انسانی را به لغو کنترل وادار کند، یا حتی موجب افزایش مخاطره، بدون داشتن کنترل شود. (مانند نیاز به کلمه عبور پیچیده بدون آموزش و هدایت مناسب برای نوشتن کلمه عبور برای کاربران) به‌علاوه، این می‌تواند موردی باشد که می‌خواهد بر عملکرد تأثیر گذارد. مدیران باید سعی کنند راه حلی که الزامات کارایی را برآورده می‌سازد، در حالی که امنیت اطلاعات کافی را تضمین می‌کند، را شناسایی کنند. نتیجه حاصل از این گام، ارائه فهرستی از کنترل‌های ممکن با هزینه، منفعت و اولویت پیاده‌سازی آن‌ها است.
محدودیت‌های مختلف در هنگام انتخاب کنترل‌ها و در طول پیاده‌سازی باید در نظر گرفته شوند. به‌طور معمول موارد زیر در نظر گرفته می شوند:

- محدودیت‌های زمانی

- محدودیت‌های مالی
- محدودیت‌های فنی
- محدودیت‌های کارکردی
- محددیت های فرهنگی
- محدودیت‌های اخلاقی
- محدودیت‌های محیط زیست
- محدودیت‌های حقوقی
- سهولت کاربردی
- محدودیت‌های کارکنان
- محدودیت‌های مربوط به ترکیب کنترل‌های برنامه جدید و موجود

اطلاعات بیش‌تر در خصوص محدودیت‌های اصلاح کاهش مخاطره در پیوست ج مشاهده می‌شود.

۹-۳ حفظ مخاطره

اقدام: تصمیم‌گیری در خصوص حفظ مخاطره بدون اقدام بیشتر باید مرتبط با ارزشیابی مخاطره در نظر گرفته شود.

یادآوری- در استاندارد ملی ایران به شماره ۲۷۰۰۱: ۱۳۸۷، زیربند ۴-۲-۱ از پیوست ج) «پذیرش موردی و هوشمندانه مخاطره‌ها به‌طور واضح سیاست‌های سازمان و معیارهای پذیرش مخاطره را برآورده می‌کند.» اقدام مشابهی را تشریح می‌کند.

رهنمودهای پیاده‌سازی: اگر سطح مخاطره، معیار پذیرش مخاطره را برآورده کند، در نتیجه نیازی به کنترل‌های اضافی پیاده‌سازی نیست و مخاطره می‌تواند حفظ شود.

۹-۴ اجتناب از مخاطره

اقدام : اقدام یا شرایطی که مخاطره خاص را که باید از آن اجتناب شود افزایش می‌دهد.

رهنمودهای پیاده‌سازی: هنگامی که مخاطره‌های شناسایی شده، خیلی زیاد در نظر گرفته شده باشد یا هزینه پیاده‌سازی گزینه‌های دیگر مقابله با مخاطره از منافع تجاوز کند، با استفاده از صرف‌نظر کردن از فعالیت یا مجموعه‌ای از فعالیت‌های موجود یا طرح‌ریزی شده یا ایجاد تغییر در شرایطی که در آن فعالیت بهره‌برداری می‌شده است، ممکن است تصمیم به اجتناب کامل از مخاطره گرفته شود. برای مثال برای مخاطره‌های ناشی از طبیعت، جابه‌جایی فیزیکی امکانات پردازش اطلاعات به مکانی که در آن‌جا مخاطره وجود نداشته باشد یا تحت کنترل باشد، ممکن است جایگزین مقرون به‌صرفه‌تری باشد.

۹-۵ اشتراک مخاطره

اقدام: مخاطره باید با طرف دیگری که می‌تواند به‌طور کاملاً مؤثر مخاطره خاص را با توجه به ارزشیابی مخاطره مدیریت کند، اشتراک شود.

رهنمودهای پیاده‌سازی: اشتراک مخاطره، شامل تصمیمی به‌منظور اشتراک مخاطره‌های معین با طرف‌های بیرونی است. اشتراک مخاطره می‌تواند مخاطره‌های جدید ایجاد کند یا مخاطره‌های شناخته شده‌ی موجود را اصلاح کند. بنابراین مقابله با مخاطره اضافی ممکن است مورد نیاز باشد.
اشتراک مخاطره، می‌تواند به‌وسیله بیمه،که از پیامدها پشتیبانی خواهد کرد یا به‌وسیله قرارداد فرعی با یک شریک که وظیفه پایش سامانه اطلاعات و اخذ اقدام بی‌درنگ برای متوقف کردن حمله قبل از آن‌که سطح تعریف شده‌ای از خسارت را وارد کند، انجام پذیرد.
باید توجه شود که ممکن است با اشتراک پاسخگویی، مخاطره را مدیریت کرد، اما به‌طور معمول امکان ندارد مسئولیت اثر را به اشتراک گذاشت. به‌طور معمول مشتری‌ها چنین اثر معکوسی را به‌عنوان اشتباه سازمان نسبت می‌دهند.

۱۰ پذیرش مخاطره امنیت اطلاعات

ورودی: طرح مقابله مخاطره با و ارزیابی مخاطره باقی‌مانده، موضوع تصمیم پذیرش از سوی مدیران سازمان است.
اقدام: تصمیم پذیرش مخاطره‌ها و مسئولیت تصمیم‌گیری می‌بایست به طور رسمی ثبت گردد (این مرتبط است با استاندارد ملی ایران به شماره ۲۷۰۰۱: ۱۳۸۷، زیر بند ۴-۲-۱ از پیوست ح)
رهنمودهای پیاده‌سازی: طرح‌های مقابله با مخاطره، باید شرح دهد که چگونه مخاطره‌های ارزیابی شده برطرف شده است تا معیار پذیرش را برآورده کند. (به بند ۷-۲ معیار پذیرش مخاطره رجوع شود.) . برای مدیران مسئول، بازنگری و موافقت با طرح‌های مقابله با مخاطره و در نتیجه مخاطره‌های باقی‌مانده و ثبت هر یک از شرایط اختصاص داده شده با چنین موافقتی، مهم است.
معیار پذیرش مخاطره، از فقط تعیین آن‌که آیا مخاطره‌های موجود بالاتر و یا پایین تر از سطح آستانه قرار گرفته‌اند یا خیر، می‌تواند بسیار پیچیده‌تر باشد.
در برخی از موارد، سطح مخاطره باقی‌مانده، به‌دلیل آن‌که معیار اعمال شده برای وضعیت غالب در نظر گرفته نشده است، نمی‌تواند معیار پذیرش مخاطره را برآورده کند. به‌عنوان مثال، ممکن است استدلال آورده شود که پذیرش مخاطره ضروری است زیرا مزایای ناشی از همراهی مخاطره بسیار قابل توجه است یا به‌دلیل آن‌که هزینه اصلاح مخاطره، بسیار زیاد است. چنین وضعیتی نشان می‌دهد که معیار پذیرش مخاطره نامناسب است و باید در صورت امکان مورد بازبینی قرار گیرد. هرچند، بازبینی معیار پذیرش مخاطره، در طی زمان همواره امکان پذیر نیست. در چنین مواردی تصمیم‌گیرندگان، ممکن است مجبور به پذیرش مخاطره‌هایی شوند که معیار پذیرش مخاطره معمولی را برآورده نمی‌کند. اگر این امر ضروری باشد، تصمیم‌گیرنده باید به‌طور صریح مخاطره‌ها را توضیح دهند و توجیهی برای تصمیم‌گیری در خصوص لغو معیار پذیرش مخاطره معمولی را متضمن شوند.
خروجی: فهرستی از مخاطره‌های پذیرفته شده به همراه توجیهی برای آن‌هایی که معیار پذیرش مخاطره معمولی را برآورده نکرده‌اند.

۱۱ ارتباطات مخاطره امنیت اطلاعات و مشاوره

ورودی: تمام اطلاعات مخاطره به‌دست آمده از اقدام‌های مدیریت مخاطرات (به شکل ۲ رجوع شود.)
اقدام: اطلاعاتی در خصوص مخاطره باید مبادله شود و/یا مابین تصمیم‌گیرنده و سایر ذی‌نفعان اشتراک شود.

رهنمودهای پیاده‌سازی: ارتباطات مخاطره، اقدامی است به‌منظور اخذ تفاهم برای چگونگی مدیریت مخاطرات به‌وسیله مبادله و/یا اشتراک اطلاعات در خصوص مخاطره مابین تصمیم‌گیرنده و سایر ذی‌نفعان. اطلاعات شامل: ماهیت داده‌ها، شکل، احتمال، شدت، مقابله و قابلیت پذیرش مخاطره‌ها است اما تنها به این موارد محدود نمی‌شود.

ارتباطات اثربخش مابین ذی‌نفعان بسیار مهم است از این‌رو ممکن است اثر مهمی بر روی تصمیمی که نیاز است گرفته شود، داشته باشد. ارتباطات این اطمینان را تضمین می‌کند که مسئول مدیریت پیاده‌سازی مخاطره و آنهایی که به‌وسیله حقوق اعطایی پایه‌ای، از این‌که چه تصمیمی اتخاذ شده و چرا اقدام خاصی مورد نیاز است را آگاه می‌شوند. ارتباطات به‌صورت دو طرفه است.

درک مخاطره، به‌دلیل تفاوت‌های مفروضات، مفاهیم و نیازها، مسائل و نگرانی‌های ذی‌نفعان مرتبط با مخاطره یا، مسائل مورد بحث می‌تواند متفاوت باشد. ذی‌نفعان، تمایل بسیاری دارند که در خصوص قابلیت پذیرش مخاطره براساس آگاهی آن‌ها از مخاطره قضاوت کنند. به‌طور خاص مهم است اطمینان حاصل شود که آگاهی ذی‌نفعان از مخاطره به‌خوبی آگاهی از منافع می‌تواند شناسایی و مستند شده و دلایل پایه‌ای درک و اداره شوند.

ارتباطات مخاطره، باید برای دستیابی به موارد زیر، انجام شود:

- ارائه اطمینان از نتیجه حاصل از مدیریت مخاطرات سازمان
- جمع‌آوری اطلاعات مخاطره
- اشتراک نتایج به‌دست آمده در ارزیابی مخاطره و ارائه طرح مقابله با مخاطره.
- جلوگیری یا کاهش هردوی وقوع یا پیامدهای نقض امنیت اطلاعات به‌دلیل عدم وجود درک متقابل در میان تصمیم‌گیرندگان و ذی‌نفعان
- حمایت از تصمیم‌گیری
- به‌دست آوردن دانش امنیت اطلاعات جدید
- همکاری میان طرفین دیگر و طرح‌ریزی پاسخ‌هایی برای کاهش پیامدهای ناشی از هر رخداد
- ایجاد حس مسئولیت در خصوص مخاطره‌ها در تصمیم‌گیرندگان و ذی‌نفعان
- بهبود آگاهی

سازمان باید طرح‌های ارتباطات مخاطره‌ها را برای شرایط اضطراری به‌خوبی کارکرد معمولی تدوین کند. بنابراین اقدام ارتباطات مخاطره باید به‌طور مداوم انجام شود.

هماهنگی میان تصمیم‌گیرندگان اصلی و ذی‌نفعان، ممکن است به‌وسیله تشکیل کمیسیونی که در آن در خصوص مخاطره‌ها، اولویت‌بندی آن‌ها، مقابله مقتضی و پذیرش می‌تواند صورت گیرد، حاصل شود.

همکاری مابین روابط عمومی مناسب یا واحد ارتباطات در سازمان به‌منظور هماهنگی تمامی وظایف مرتبط با ارتباطات مخاطره، مهم است. این امر در رویداد اقدامات ارتباطات بحران، برای مثال در پاسخگویی به حادثه‌های خاص، مهم است.
خروجی: درک پیوسته از فرآیند مدیریت مخاطرات امنیت اطلاعات سازمان و نتایج آن.

۱۲ پایش و بازنگری مخاطره امنیت اطلاعات

۱۲-۱ پایش و بازنگری مولفه‌های مخاطره
ورودی: تمامی اطلاعات مخاطره، به‌دست آمده از اقدام‌های مدیریت مخاطرات (به شکل ۲ رجوع شود.)
اقدام: مخاطرات و مؤلفه‌های دیگر (مانند ارزش دارایی‌ها، اثرها، تهدیدها، آسیب‌پذیری‌ها، احتمال وقوع) به‌منظور شناسایی تمامی تغییرات در زمینه سازمان در مرحله اولیه و برای حفظ نمای کلی تصویر کامل مخاطره، باید مورد پایش و بازنگری قرار گیرد.
رهنمودهای پیاده‌سازی: مخاطره‌ها، ایستا نیستند. تهدیدها، آسیب‌پذیری‌ها، احتمال یا پیامدها ممکن است بدون هیچ نشانه‌ای به‌طور ناگهانی تغییر کنند. بنابراین، پایش مستمر به‌منظور تشخیص این تغییرات ضروری است. این ممکن است به‌وسیله خدمات بیرونی که اطلاعاتی در مورد تهدیدها و آسیب-پذیری‌ها ارائه می‌دهد، پوشش داده شود.
سازمان‌ها باید از پایش مستمر موارد زیر اطمینان حاصل کنند:

- دارایی های جدید در حوزه مدیریت مخاطرات
- اصلاح لازم ارزش دارایی‌ها مانند با توجه به الزامات کسب و کار تغییر یافته
- تهدیدات جدیدی که می‌توانند در داخل و خارج از سازمان فعال شده و ارزیابی شوند.
- احتمال این‌که آسیب‌پذیری‌های جدید یا افزایش یافته بتوانند اجازه دهند تهدیدها از این آسیب‌پذیری‌های جدید یا تغییر یافته بهره‌جویی کنند.
- آسیب‌پذیری‌های شناسایی‌شده برای تعیین آن‌هایی که تهدیدهای جدید یا دوباره در حال ظهور در معرض قرار می‌دهند.
- اثر یا پیامد افزایش یافته از تهدیدهای ارزیابی شده، آسیب‌پذیری‌ها و مخاطرات در نتیجه توافقات در سطح غیر قابل قبول مخاطره
- رخدادهای امنیت اطلاعات

تهدیدها، آسیب‌پذیری‌های جدید یا تغییرات در احتمال یا پیامدها می‌توانند مخاطره‌های از قبل ارزیابی شده را افزایش دهند. در بازنگری مخاطره‌های کم و پذیرفته شده به طور مجزا و تمام چنین مخاطره‌هایی چنان‌چه تجمیع شده‌باشند ارزیابی متراکم شدن بالقوه باید به‌خوبی در نظر گرفته شود. اگر مخاطره‌ها در طبقه‌بندی مخاطره کم و یا قابل پذیرش قرار نگیرند، باید آن‌ها را با استفاده از یک یا چند گزینه در نظر گرفته شده در بند ۹ برطرف کرد.
مؤلفه‌هایی که بر احتمال و پیامدهای تهدیدهای رخ داده اثر می‌گذارند، می‌توانند تغییر کنند مانند مؤلفه‌هایی که بر مطلوبیت یا هزینه گزینه‌های مقابله مختلف می‌توانند اثر گذارند. تغییرات اساسی مؤثر

بر سازمان، دلیلی برای بازنگری خاص بیشتر است. بنابراین، اقدام‌های پایش مخاطره باید به‌طور منظم تکرار شده و گزینه‌های مقابله با مخاطره به‌طور متناوب مورد بازنگری قرار گیرد.
نتیجه حاصل از اقدام‌های پایش مخاطره ممکن است ورودی دیگر اقدام‌های بازنگری مخاطره باشد. سازمان باید تمامی مخاطره‌ها را به‌طور منظم و هنگام وقوع تغییرات اساسی بازنگری کند و سایر تغییرات را نیز مورد توجه قرار دهد. (مطابق با استاندارد ملی ایران به شماره ۲۷۰۰۱: ۱۳۸۷ زیربند ۴-۲-۳)
خروجی: هم‌ترازی پیوسته مدیریت مخاطرات‌ها، با اهداف کسب و کار سازمان و با معیار پذیرش مخاطره.

۲-۱۲ پایش، بازنگری و بهبود مدیریت مخاطرات

ورودی: تمامی اطلاعات مخاطره به‌دست آمده از طریق اقدام‌های مدیریت مخاطرات (به شکل۱ رجوع شود.)
اقدام: فرآیند مدیریت مخاطرات امنیت اطلاعات باید به‌طور پیوسته پایش و بررسی شده و در صورت لزوم و به‌طور مقتضی بهبود یابد.
رهنمودهای پیاده‌سازی: پایش و بازنگری مداوم برای اطمینان از این‌که نتایج ارزیابی و مقابله با مخاطره به‌خوبی طرح‌های مدیریتی، مرتبط و متناسب با وضعیت باقی می‌ماند، ضروری است.
سازمان باید اطمینان حاصل کند که فرآیند مدیریت مخاطرات امنیت اطلاعات و اقدام‌های مرتبط، متناسب با وضعیت حاضر و در راستای آن باقی می‌ماند. توافق بهبود در فرایند یا اقدام‌های لازم به‌منظور بهبود تطابق با فرایند، باید برای اطمینان از این‌که هیچ مخاطره یا مؤلفه مخاطره‌ای چشم پوشی نشده یا دست کم گرفته نشده است و این‌که اقدام‌های لازم انجام شده است و تصمیم‌ها برای درک مخاطره واقع-بینانه و قابلیت پاسخ‌گویی اخذ شده است، به مدیران مربوطه اطلاع داده شود.
علاوه براین سازمان باید به‌طور منظم تایید کند که معیارهای مورد استفاده برای اندازه‌گیری مخاطره و مؤلفه‌های آن، هنوز معتبر و سازگار با سیاست‌ها، استراتژی‌ها و اهداف سازمان هستند و تغییرات در زمینه کسب و کار به اندازه کافی در فرآیند مدیریت مخاطرات امنیت اطلاعات درنظر گرفته شده است.
این اقدام‌های پایش و بازنگری، باید موارد زیر را پوشش دهد (ولی محدود به آن‌ها نیست):

- زمینه قانونی و زیست‌محیطی
- زمینه رقابتی
- رویکرد ارزیابی مخاطره
- ارزش و طبقه‌بندی دارایی
- معیار اثرگذاری
- معیار ارزشیابی مخاطره
- معیار پذیرش مخاطره
- هزینه کلی مالکیت
- منابع ضروری

سازمان، باید از ارزیابی مخاطره و منابع مقابله با مخاطره، که به‌طور پیوسته برای بازنگری مخاطره در دسترس است اطمینان حاصل کند تا آسیب‌پذیری‌ها یا تهدیدهای تغییر یافته یا جدید و در نتیجه توصیه مدیریت را پوشش دهد.

پایش مدیریت مخاطرات، می‌تواند منجر به اصلاح یا افزایش رویکرد، روش‌شناسی یا ابزارهای استفاده شود،که وابسته به عوامل زیر است:

- تغییرات شناسایی شده
- تکرار ارزیابی مخاطره
- هدف از فرآیند مدیریت مخاطرات امنیت اطلاعات (مانند تداوم کسب و کار، جهندگی رخداد، انطباق)
- موضوع فرآیند مدیریت مخاطرات امنیت اطلاعات (مانند سازمان، واحد کسب و کار، فرآیند اطلاعات، پیاده‌سازی فنی، کاربرد، اتصال به اینترنت)

خروجی: ارتباط مداوم میان فرآیند مدیریت مخاطرات امنیت اطلاعات با موضوع کسب و کار یا به‌روز رسانی فرآیند

پیوست الف

(اطلاعاتی)

تعریف دامنه و مرزهای فرآیند مدیریت مخاطره امنیت اطلاعات

الف۱- مطالعه‌ای بر سازمان

ارزیابی سازمان: مطالعه سازمان عوامل مشخصه تعریف هویت سازمان را فرا می‌خواند. ارزیابی شامل هدف، کسب و کار، ماموریت، ارزش‌ها و راهبردهای سازمان می‌شود. این‌ها باید در کنار عناصری شناخته شوند که در توسعه آن‌ها دخالت دارند (برای مثال مقاطعه کاری).

مشکل این تحقیق(فعالیت) در درک دقیق چگونگی ساختاربندی سازمان، نهفته است. شناسایی ساختار دقیق آن درک اهمیت و نقش هر بخش را در دستیابی به اهداف سازمان فراهم می‌کند.

برای مثال این حقیقت که مدیر امنیت اطلاعات به مدیران ارشد گزارش می‌دهد و نه مدیران IT، می‌تواند درگیری مدیران ارشد را در امنیت اطلاعات نشان دهد.

هدف اصلی سازمان: هدف اصلی یک سازمان می‌تواند به‌عنوان دلیل وجودی آن سازمان تعریف شود (حوزه فعالیت آن، بخش بازار آن و غیره).

کسب و کار سازمان: کسب و کار سازمان به‌وسیله فنون و دانش کارمندان آن مشخص می‌شود و آن را قادر می‌سازد تا مأموریت خود را کامل کند. این خاص حوزه فعالیت سازمان است و اغلب فرهنگ آن را تعریف می‌کند.

مأموریت سازمان: سازمان از طریق تکمیل مأموریت خود به اهدافش می‌رسد. برای شناسایی مأموریت آن، خدمات ارائه شده و/یا محصولات تولید شده باید در ارتباط با کاربران نهایی شناسایی شوند.

ارزش‌های سازمان: ارزش‌ها اصول اصلی یا کدهای تعریف شده اجرایی هستند که در انجام‌دادن کسب و کار به‌کار می‌روند. این ممکن است به پرسنل یا ارتباط با عوامل خارجی (مشتریان و غیره) کیفیت محصولات عرضه شده یا خدمات ارائه شده مرتبط باشد.

برای مثال سازمانی را در نظر بگیرید که هدف آن ارائه خدمات عمومی و کسب و کار آن حمل و نقل است و مأموریت آن شامل انتقال کودکان به و از مدرسه است. ارزش‌های آن می‌تواند وقت‌شناسی خدمات و ایمنی در طول انتقال باشد.

ساختار سازمان: انواع مختلف ساختار وجود دارد:

- ساختار بخشی[1]: هر بخش تحت نظارت یک مدیر بخش قرار دارد که مسئول تصمیمات راهبردی، اجرایی و عملیاتی در خصوص آن واحد است.

ساختار کارکردی: مسئولین کارکردی روی روش‌ها و طبیعت کارها و گاهی روی تصمیمات و برنامه‌ریزی‌ها کار می‌کنند. (برای مثال تولید، IT، منابع انسانی، بازاریابی و غیره)

1 -Divisional Structure

علایم:

- یک بخش در سازمان دارای ساختار بخشی می‌تواند به‌صورت یک ساختار کارکردی و برعکس سازمان یابد.
- ممکن است گفته شود که سازمان دارای ساختار ماتریسی است، در این صورت عوامل هر دو ساختار وجود دارد.
- در هر ساختار سازمانی سطوح زیر قابل شناسایی هستند:
- سطح تصمیم گیری (تعریف گرایشات راهبردی)
- سطح رهبری (همکاری و مدیریت)
- سطح عملیاتی (فعالیت‌های تولیدی و حمایتی)

نمودار سازمان: ساختار سازمان به‌صورت قیاسی در نمودار سازمان نمایش داده می‌شود. این بازنمایی باید خطوط گزارش‌دهی و اعطای نمایندگی را دربر گیرد اما باید شامل سایر روابط نیز باشد که اگرچه براساس هیچ‌یک از مسئولیت‌های رسمی نیستند اما مسیر جریان اطلاعات هستند.

راهبرد سازمان: این به بیان رسمی اصول هدایت‌کننده سازمان، نیاز دارد. راهبرد سازمان جهت و توسعه مورد نیاز برای بهره‌مندی از موارد مورد بحث و تغییرات عمده‌ای را که طرح‌ریزی شده‌اند تعیین می‌کند.

الف۲- فهرست محدویت‌هایی که سازمان را تحت تأثیر قرار می‌دهند.

تمام محدودیت‌هایی که سازمان را متأثر می‌سازند و گرایشات امنیت اطلاعات را تعیین می‌کنند باید در نظر گرفته شوند. منبع آن‌ها می‌تواند درون‌سازمانی باشد که بر آن‌ها کنترل می‌کند یا خارج از سازمان باشد و بنابراین به‌طور کلی نمی‌تواند مورد مذاکره قرار گیرد. محدودیت منابع (بودجه، پرسنل) و محدودیت‌های اضطراری از مهم ترین‌ها هستند.

سازمان اهداف خود (در خصوص کسب و کار، رفتار و غیره) را تنظیم و در مسیر معینی که به احتمال در بیش از یک مدت طولانی آن‌ها را انجام می‌دهد تعریف می‌کند که می‌خواهد چه بشود و اهدافی را تعریف می‌کند که نیاز دارد انجام دهد. در تعیین این مسیر، سازمان توسعه فنون و دانش چگونگی[1] را در نظر می‌گیرد و خواسته‌های کاربران و مشتریان و غیره را مطرح می‌کند. این اهداف می‌توانند به‌شکل راهبردهای عملیاتی یا توسعه‌ای با هدف برای مثال کاهش هزینه عملیاتی، بهبود کیفیت خدمات و غیره بیان شوند.

این راهبردها به احتمال شامل اطلاعات و سامانه اطلاعاتی (IS[2]) می‌شوند که در کاربرد آن‌ها کمک‌کننده هستند. درنتیجه خصوصیات مربوط به هویت، مأموریت و راهبردهای سازمان، عوامل اصلی در تحلیل مشکل خواهند بود، زیرا نقض جوانب امنیت اطلاعات می‌تواند به بازنگری این اهداف راهبردی منجر شود.

1 - know-how
2 -Information System

به‌علاوه، ضروری است که پیشنهادها برای الزامات امنیت اطلاعات با قواعد، استفاده‌ها و اهداف در حال اجرا در سازمان سازگار باشند.

فهرست این محدودیت‌ها شامل موارد زیر می‌شود اما به اینها محدود نمی‌شود:

محدودیت‌های طبیعت سیاسی

این محدودیت‌ها می‌تواند به مجریان دولتی، مؤسسات عمومی یا به‌صورت کلی‌تر، هر سازمان که باید تصمیمات دولت را انجام دهد مربوط شوند و به‌طور عموم تصمیماتی هستند در خصوص گرایشات راهبردی و عملیاتی که توسط بخش دولتی اتخاذ شده‌اند یا باید توسط بدنه تصمیم‌گیری و اجرا شوند.

برای مثال، رایانه‌ای کردن صورت حساب‌ها یا اسناد اجرایی، مسائل امنیت اطلاعات را مطرح می‌کنند.

محدودیت‌های طبیعت راهبردی

محدودیت‌ها می‌توانند از تغییرات برنامه‌ریزی شده یا احتمالی در ساختار یا گرایشات سازمان ایجاد شوند و در برنامه‌های راهبردی و عملیاتی سازمان بیان می‌شوند.

برای مثال، همکاری بین‌المللی در اشتراک اطلاعات حساس ممکن است به توافق در خصوص تبادل امن نیاز داشته باشد.

محدودیت‌های منطقه‌ای

ساختار و/یا هدف سازمان می‌تواند محدودیت‌های خاصی مثل توزیع سامانه‌ها بیش از کل قلمرو ملی یا خارج از آن را ایجاد کند.

برای مثال، خدمات پستی، سفارت‌خانه‌ها، بانک‌ها، مؤسسات وابسته به گروه‌های صنعتی بزرگ و غیره.

محدودیت‌های حاصل از فضای اقتصادی و سیاسی

عملیات یک سازمان می‌تواند به‌طور عمیق توسط رویدادهای خاصی مثل اعتصابات یا بحران‌های ملی یا بین‌المللی تغییر کند.

برای مثال بعضی خدمات باید بتوانند حتی در طول بحران‌های شدید ادامه یابند.

محدودیت‌های ساختاری

طبیعت ساختار یک سازمان (بخشی، کارکردی و غیره) می‌تواند به خط‌مشی خاص امنیت اطلاعات و سازمان امنیتی که سازمان برای ساختار اتخاذ نموده منجر شود.

برای مثال، یک ساختار بین‌المللی باید بتواند با الزامات خاص امنیتی خاص در هر کشور انطباق یابد.

محدودیت‌های کارکردی

محدودیت‌های کارکردی به‌طور مستقیم از مأموریت‌های عمومی و خصوصی سازمان ناشی می‌شوند.

برای مثال، سازمانی که حول زمان‌سنجی کار می‌کند باید مطمئن باشد که منابعش به‌طور دائم در دسترس هستند.

محدودیت در خصوص پرسنل

طبیعت این محدودیت‌ها به‌طور قابل توجهی تغییر می‌کند. این محدودیت‌ها به سطح مسئولیت، جذب نیروی انسانی، مهارت، آموزش، آگاهی امنیتی، انگیزه، دسترسی و غیره ارتباط دارند.

برای مثال، کل پرسنل یک سازمان دفاعی باید بتوانند به اطلاعات بسیار محرمانه دسترسی داشته باشند.

محدودیت‌های حاصل از تقویم سازمان

این محدودیت‌ها از بازسازی و تنظیم سیاست‌های ملی و بین‌المللی جدید که مهلت‌های خاصی را تحمیل می‌کنند ناشی می‌شوند.

برای مثال، ایجاد یک بخش امنیتی

محدودیت‌های مربوط به روش‌ها

روش‌های مناسب برای دانش فنی سازمان باید برای جنبه‌هایی مثل طرح‌ریزی پروژه، خصوصیات و توسعه و غیره تحمیل شوند.

برای مثال، یک محدودیت عادی از این نوع، نیاز به گنجاندن تعهدات قانونی سازمان در سیاست‌های امنیتی دارد.

محدودیت‌های طبیعت فرهنگی

در بعضی از سازمان‌ها عادات کاری یا کسب و کار اصلی به "فرهنگ" خاصی در سازمان منجر می‌شوند، چیزی که می‌تواند با کنترل امنیتی ناسازگار باشد. این فرهنگ، چارچوب کلی مرجع پرسنل است و می‌تواند توسط جنبه‌های متعدد شامل تحصیلات، دستورات، تجربه حرفه‌ای، تجربه کار بیرون، عقاید، فلسفه‌ها، اعتقادات، اوضاع اجتماعی و غیره تعیین شود.

محدودیت‌های بودجه‌ای

کنترل‌های امنیتی پیشنهاد شده ممکن است گاهی هزینه بالایی داشته باشند. اگرچه همیشه مناسب نیست که سرمایه‌گذاری امنیتی بر مبنای بهره‌وری صورت گیرد، به‌طور کلی ارایه توجیه اقتصادی توسط بخش مالی سازمان ضروری است.

برای مثال، در بخش خصوصی و بعضی سازمان‌های دولتی کل هزینه کنترل امنیتی نباید از هزینه‌های عواقب بالقوه مخاطرات بیشتر باشد. بنابراین اگر مدیریت ارشد بخواهد از هزینه‌های امنیتی اضافی اجتناب کند، باید مخاطرات را ارزیابی و برآورد کند

الف۳- فهرست مراجع قانونی و مقرراتی قابل اجرا در سازمان

الزامات مقررات قابل اجرا در مورد سازمان باید شناسایی شوند. این الزامات می‌توانند قوانین، احکام، مقررات خاص در حوزه سازمان یا مقررات داخلی و/یا خارجی را شامل شوند. این الزامات همچنین مربوط به قراردادها و توافق نامه‌ها و به‌صورت کلی‌تر هرگونه تعهداتی که طبیعت قانونی و مقرراتی داشته باشد، هستند.

الف۴- فهرست محدویت‌های اثر گذار بر روی دامنه

با شناسایی محدودیت‌ها این امکان وجود دارد تا فهرست آنهایی که روی دامنه تأثیر دارند تهیه و تعیین شود که کدامیک هنوز قابلیت اجرا دارند. آن‌ها به محدودیت‌هایی که در بالا گفته شد اضافه می‌شوند یا

احتمالاً آن‌ها را تغییر می‌دهند. پاراگراف‌های زیر یک لیست غیرجامع از انواع ممکن این محدودیت‌ها را بیان می‌کنند.

محدودیت‌های حاصل از فرآیندهای موجود از قبل

پروژه‌های کاربردی لزوماً به‌صورت همزمان توسعه نمی‌یابند. بعضی به فرآیندهای موجود از قبل بستگی دارند. با اینکه یک فرایند می‌تواند به چندین فرآیند فرعی تقسیم شود، اما فرآیند لزوماً تحت تأثیر تمام فرآیندهای فرعی فرآیندهای دیگر قرار ندارد.

محدودیت‌های فنی

محدودیت‌های فنی مربوط به زیرساخت‌ها، به‌طور کلی از سخت‌افزارها و نرم‌افزارهای نصب شده و فضاها و سامانه‌های استقرار فرآیندها، ناشی می‌شوند:

- پرونده‌ها (الزامات مربوط به سازمان، مدیریت رسانه، مدیریت قوانین دسترسی و غیره)
- معماری عمومی (الزامات مربوط به هم‌بندی (متمرکز، توزیع شده، کارخواه - کارساز[1])، معماری فیزیکی و غیره)
- نرم‌افزار کاربردی (الزامات مربوط به طراحی نرم‌افزار خاص، استانداردهای بازار و غیره)
- بسته نرم‌افزاری (الزامات مربوط به استانداردها، سطح ارزیابی، کیفیت، انطباق با هنجارها، امنیت و غیره)
- سخت‌افزار (الزامات مربوط به استانداردها، کیفیت، انطباق با هنجارها و غیره)
- شبکه‌های ارتباطی (الزامات مربوط به پوشش، استانداردها، ظرفیت، قابلیت اعتماد و غیره)
- زیر ساخت‌های ساختاری (الزامات مربوط به مهندسی عمران، ساختار، ولتاژ بالا، ولتاژ پایین و غیره)

محدودیت‌های مالی

به‌کارگیری کنترل‌های امنیتی اغلب به بودجه محدود می‌شود که سازمان می‌تواند تعهد کند. اگرچه محدودیت مالی هنوز باید در آخر مورد ملاحظه قرار گیرد زیرا تخصیص بودجه برای امنیت می‌تواند برمبنای مطالعات امنیت مورد مذاکره قرار گیرد.

محدودیت‌های زیست محیطی

محدودیت‌های زیست‌محیطی از محیط‌های جغرافیایی یا اقتصادی ناشی می‌شوند که فرآیند در آن‌ها انجام می‌شود: کشور، آب و هوا، خطرات طبیعی، موقعیت جغرافیایی، شرایط اقتصادی و غیره.

محدودیت‌های زمانی

زمان لازم برای پیاده‌سازی کنترل‌های امنیتی باید در ارتباط با توان به‌روزرسانی سامانه اطلاعات ملاحظه شود؛ اگر زمان اجرایی خیلی طولانی باشد، خطری که کنترل برای آن طراحی شده می‌تواند تغییر کند. زمان برای انتخاب راه‌حل‌ها و اولویت‌ها عامل تعیین کننده است.

محدودیت‌های مربوط به روش‌ها

1 - Client-Server

روش‌های مناسب برای دانش فنی سازمان، باید برای طرح‌ریزی پروژه‌ها، خصوصیت‌ها، توسعه‌ها و غیره به‌کار روند.

محدودیت‌های سازمانی

محدودیت‌های متعدد می‌تواند از الزامات سازمانی ناشی شود:

- عملیات (الزامات مربوط به زمان انتظار، عرضه خدمات، تجسس، پایش، برنامه‌های ضروری، عملیات تنزل‌یافته و غیره).
- نگهداشت (الزامات رفع عیب حادثه، اقدمات پیشگیرانه، اصلاح سریع و غیره)
- مدیریت منابع انسانی (الزامات مربوط به آموزش اپراتور و کاربر، صلاحیت پست‌هایی مثل مجری سامانه، مجری داده‌ها و غیره)
- مدیریت اجرایی (الزامات مربوط به مسئولیت‌ها و غیره)
- مدیریت توسعه (الزامات مربوط به ابزارهای توسعه، مهندسی نرم‌افزار مبتنی بر رایانه، برنامه‌های پذیرش، تنظیمات سازمانی و غیره)
- مدیریت روابط خارجی (الزامات مربوط به سازمان ثالث، قراردادها و غیره)

پیوست ب

(اطلاعاتی)

شناسایی و ارزیابی دارایی‌ها و ارزیابی اثرات

ب ۱ نمونه‌هایی از شناسایی دارایی‌ها

به‌منظور ارزیابی دارایی‌ها، یک سازمان ابتدا نیاز به شناسایی دارایی‌های خود دارد. دونوع دارایی قابل تشخیص وجود دارد:

دارایی‌های اولیه:

- فرآیندها و فعالیت های کسب و کار
- اطلاعات

حمایت از همه نوع از دارایی‌های موجود (که به تمام آن اجزای اولیه تکیه دارند):

- سخت‌افزار
- نرم‌افزار
- شبکه
- پرسنل
- پایگاه
- ساختار سازمان

ب ۱-۱ شناسایی دارایی‌های اولیه

به‌منظور توصیف دامنه با دقت بیشتر، می‌توان گفت که این فعالیت، شامل شناسایی دارایی‌های اولیه است (فرآیندها و فعالیت‌های کسب وکار، اطلاعات). این شناسایی از طریق گروهی ترکیبی انجام می‌شود که نمایانگر فرآیندی کلی است. (مدیران ،کاربران و متخصصان سامانه‌های اطلاعاتی)

دارایی‌های اولیه در این زمینه، همان فرآیندها و اطلاعات مربوط به فعالیت در یک دامنه است. سایر دارایی‌های اولیه، مانند فرآیندهای سازمان نیز به‌صورتی مورد توجه قرار گرفته می‌شود که برای خط‌مشی امنیت اطلاعات و طرح تداوم کسب و کار مناسب باشد. با توجه به این هدف، برخی از مطالعات صورت گرفته در این راستا هیچ‌گونه نیازی بر تحلیل کلی همه‌ی مؤلفه‌های دامنه را نخواهد داشت. در چنین مواردی مرزهای تحقیقی محدود به مؤلفه‌های کلیدی دامنه است.

دارایی‌های اولیه دو نوع هستند:

۱- فرآیندها (یا زیرفرآیندها)ی کسب و کار و فعالیت‌های مربوط به آن، به‌عنوان مثال:

- فرآیندهای مربوط به خسارات یا تخریب کسب و کار که اجرای آن‌ها، عملکرد سازمان را غیر ممکن می‌سازد.
- فرآیندهایی که شامل فرآیندهای محرمانه یا فرآیند مربوط به فناوری انحصاری است.
- فرآیندهایی که در صورت تغییر، اثرات بسیاری را بر روی عملکرد سازمان می‌گذارند.

- فرآیندهای سازمانی که برای رعایت الزامات قرار دادی، قانونی یا نظارتی لازم هستند.

۲- اطلاعات:

به‌طور کلی اطلاعات اولیه اصلی شامل موارد زیر است:

- اطلاعات ضروری برای راه‌اندازی عملکرد کسب و کار یا سازمان.
- اطلاعات فردی که می‌تواند به‌طور خاص برمبنای قوانین ملی، در مورد حریم خصوصی تعریف شود.
- اطلاعات راهبردی مورد نیاز برای دستیابی به اهداف سازمان که توسط جهت‌گیری‌های راهبردی تعیین می‌شوند.
- اطلاعاتی با هزینه بالا که جمع آوری، ذخیره‌سازی، پردازش و انتقال آن‌ها، نیازمند مدت زمان طولانی و/یا هزینه کسب بالاست.

فرآیندها و اطلاعات موجود در این بخش نمی‌تواند پس از عدم شناسایی این فعالیت‌ها، مورد توجه قرار گیرد. این امر به آن معنی است که حتی اگر چنین فرآیندها یا اطلاعاتی در ترکیب با هم قرار بگیرند، آنگاه سازمان می‌تواند با موفقیت عملکردهای خود را اجرایی کند.

با این وجود، این موارد اغلب کنترل را برای حفاظت از فرآیندها و اطلاعات حساس شناسایی شده در این راستا پیاده‌سازی می‌کنند.

ب۱-۲ فهرست و توصیفی از دارایی‌های حمایتی

این دامنه شامل دارایی‌هایی است که باید به‌خوبی شناسایی شوند. این‌گونه دارایی‌ها، دارای عوامل آسیب‌پذیری هستند که می‌توانند در ارتباط با بسیاری از تهدیدهایی قرار گیرند که هدف آن‌ها آسیب رساندن به دارایی‌های اولیه (فرایندها و اطلاعات) است. این عوامل دارای انواع گوناگونی هستند:

سخت‌افزار

سخت‌افزار، مربوط به تمامی مؤلفه‌های فیزیکی است که از این فرآیندها، حمایت می‌کنند.

تجهیزات مربوط به پردازش داده‌ها (فعال)

تجهیزات پردازش خودکار اطلاعات، شامل اقلام مورد نیاز برای اجرای مستقل

تجهیزات قابل انتقال

تجهیزات موجود در یک رایانه قابل حمل و نقل

به عنوان مثال رایانه‌ی کیفی، دستیار دیجیتال شخصی PDA [1]

تجهیزات ثابت

تجهیزات رایانه‌های مورد استفاده در فضای سازمان

به‌عنوان مثال رایانه‌ی خدمات دهنده، ریزرایانه‌های مورد استفاده به‌عنوان ایستگاه کاری

عوامل جانبی بخش پردازش

1 - Personal Digital Assistant

تجهیزات مربوط به رایانه که از طریق یک درگاه ارتباطی باعث ورود، حمل، انتقال داده‌ها می‌شود.
به عنوان مثال، چاپگر ، سخت‌دیسک قابل حمل

رسانه داده‌ها (غیر فعال)

بخش ذخیره داده‌ها و یا عملکردها

رسانه الکترونیکی

یک رسانه اطلاعاتی، رسانه‌ای است که می‌تواند به یک رایانه یا شبکه برای دخیره‌سازی اطلاعات متصل شود. علی‌رغم اندازه کوچک، این رسانه‌ها می‌توانند حاوی حجم زیادی از داده‌ها باشند. این رسانه‌ها می‌توانند توسط تجهیزات محاسبه‌گر استاندارد استفاده شوند.

به‌عنوان مثال، فلاپی دیسک، دیسک فشرده، نوار مغناطیسی، سخت دیسک قابل انتقال، حافظه فلش، نوار

سایر رسانه‌ها

رسانه ایستا؛ رسانه غیرالکترونیکی که حاوی داده‌ها است.

به‌عنوان مثال، صفحه، اسلاید، ترانسپرنسی[1]، سند پردازی، دورنگار

نرم‌افزار

نرم‌افزار شامل تمامی برنامه‌های مربوط به عملیات پردازش داده‌ها است.

سیستم عامل

سیستم عامل، شامل تمامی برنامه‌های رایانه‌ای است که به‌عنوان یک پایه عملیاتی برای اجرای سایر برنامه‌ها (خدمات یا کاربردها) به‌کار گرفته می‌شود. این سامانه شامل یک هسته اصلی و خدمت یا توابع پایه است. با توجه به این ساختار، یک سیستم عامل ممکن است تک هسته‌ای باشد یا از یک ریزهسته و یک مجموعه‌ای از سرویس‌های سیستمی ساخته شده باشند. مؤلفه‌های مهم و اساسی در یک سیستم عامل، شامل خدمات مدیریت تجهیزات (CPU[2]، حافظه، دیسک و شبکه) سرویس مدیریت فرایندها و فعالیت‌ها و سرویس مدیریت سطح دسترسی کاربران است.

نرم‌افزار خدمات، نگهداری و مدیریتی

نرم افزار موجود به‌صورتی است که در ارتباط با خدمات سیستم عامل قرار دارد و از طرفی نیز در ارتباط مستقیم با کاربران و یا عملکرد آن‌ها، قرار نگرفته است. (اگر چه عاملی اساسی و جدایی‌ناپذیر برای عملیات کلان یک سامانه اطلاعاتی به‌شمار می‌رود.)

بسته‌های نرم‌افزار یا نرم‌افزار استاندارد

این نوع نرم‌افزارها، محصولات کاملاً تجاری‌سازی شده (به‌جای نرم‌افزارهای سفارشی) به‌صورتی که شامل رسانه، نگارش و نگهداری هستند. این نرم‌افزارها خدمتی را برای کاربران و کاربردهایی فراهم می‌کنند که شخصی و خاص یک کسب و کار نیست. نمونه‌ها: نرم‌افزار مدیریت پایگاه داده، نرم‌افزار پیام‌رسان الکترونیکی، نرم‌افزار گروهی، نرم‌افزار راهنما، نرم‌افزار خدمات‌دهنده‌ی وب و سایر موارد

1 - Transparency
2 Central Processor Unit

برنامه‌های کاربردی کسب و کار

برنامه‌های کاربردی استاندارد کسب و کار

این نرم‌افزار تجاری، برای این که به کاربران دسترسی مستقیم به خدمات و عملکردهایی را که در حیطه کاری خود به آن نیاز دارند بدهد، طراحی شده است. این بخش به لحاظ نظری بسیار گسترده است و بسیاری از گزینه‌ها در آن وجود دارد.

به‌عنوان مثال، نرم‌افزار محاسباتی، ماشین افزار کنترلی، نرم‌افزار مراقبت از حق مشتری، نرم‌افزار مدیریت شایستگی پرسنل، نرم‌افزار اداری و سایر موارد

برنامه‌های کاربردی خاص کسب و کار

این نرم‌افزار، به‌صورتی خاص و دارای جوانب گوناگون (اغلب پشتیبانی، تعمیر و نگهداری، ارتقاء، و سایر گزینه‌ها) است که می‌تواند کاربران را در ارتباط مستقیم با خدمات و کارکردهای مورد نیاز آن‌ها در این سامانه قرار دهد. طیف بسیار گسترده‌ای از تئوری‌های نامحدود در این زمینه‌ها وجود دارد.

به‌عنوان مثال: مدیریت سررسید عوامل ارتباط مخابراتی با مشتریان، برنامه کاربردی پایش زمان واقعی برای انجام دستورالعمل‌ها

شبکه‌ها

انواع شبکه‌ها: مربوط به تمامی ابزارهای مخابراتی مورد استفاده، برای اتصال از راه دور رایانه‌ها و اجزای مربوط به سامانه‌های اطلاعاتی است.

محیط‌ها و حمایت‌ها

رسانه‌های ارتباطی از راه دور و ارتباطات یا تجهیزات اساسا دارای ویژگی‌های فیزیکی و فنی تجهیزات (پخش، نقطه به نقطه) پروتکل‌های ارتباطی است (اتصال یا شبکه، سطح ۲ و ۳ از الگوهای OSI 7-layer)

مثال‌ها: شبکه عمومی سوئیچینگ تلفن PSTN, Ethernet, GigabitEthernet، خط اشتراک دیجیتال نامتقارن (ADSL)، مشخصات پروتکل بی‌سیم (به عنوان مثال WiFi 802.11)، ارتباط دندان آبی، خط آتش.

رله فعال یا غیرفعال

این بخش، شامل تمامی دستگاه‌هایی است که نمی‌توانند در ارتباط با عوامل منطقی (از دید IS) قرار گیرد. اما در هر صورت از دستگاه‌های میانی یا رله در آن‌ها استفاده می‌شود. رله نیز توسط پروتکل‌های ارتباطی شبکه مشخص می‌شود. علاوه بر رله اصلی، چنین عاملی شامل مسیریابی و/یا توابع فیلتربندی و خدمات به‌کارگیری مسیریاب‌ها و کلیدزن‌های مخابراتی با فیلترها است. در اغلب موارد این عوامل، می‌توانند از راه دور اداره شوند و معمولا قادرند از لگاریتم‌های (سیاست‌های مربوطه) اجرایی، استفاده کنند.

به‌عنوان مثال پل، مسیر یاب، هاب، کلیدزن، تبادل خودکار

واسط ارتباطی

واسط‌های ارتباطی این بخش از واحدهای پردازش، به یک واحد پردازش متصل می‌شوند، اما این بخش، توسط رسانه‌ها و پروتکل‌های حمایت شده با هرگونه نصب فیلتر، الگوریتم یا هشدار اتصال عملکردها و ظرفیت‌های خود و امکان‌پذیری و الزامات مدیریت از راه دور مشخص می‌شوند.
مثال: (خدمات رادیویی بسته عمومی (GPRS[1])، آداپتور اترنت.

پرسنل
این بخش شامل همه‌ی گروه‌های افراد درگیر در یک سامانه اطلاعاتی است.
عامل تصمیم‌گیرنده
عوامل تصمیم‌گیرنده، همان مالکین دارایی‌های اولیه (اطلاعات و عملکرد) و مدیران سازمان و پروژه خاص موجود در این بخش هستند.
مثال: مدیریت ارشد، مدیر پروژه
کاربران
این کاربران، کارمندانی هستند که دارای مؤلفه‌های حساس در این زمینه بوده و هر یک از آن‌ها ، دارای مسئولیتی ویژه در این خصوص است. این موارد، به‌صورتی است که آن‌ها ممکن است حقوق دسترسی خاص برای ورود به سامانه اطلاعاتی به‌منظور اجرای عملکردهای روزانه خود را داشته باشند.
مثال: مدیریت منابع انسانی، مدیریت مالی، مدیر مخاطره
عملکرد/کارکنان حفظ و نگاه‌داری
این افراد، کارکنان عهده‌دار در بخش عملیات و حفظ و نگهداری سامانه‌های اطاعاتی هستند. این موارد، دارای حقوق خاصی برای دسترسی به سامانه اطلاعاتی برای انجام کارهای روزانه خود را دارند.
مثال: مدیر سامانه، مدیر داده‌ها، پشتیبان‌گیری، پیشخوان، متصدی به‌کارگیری نرم‌افزارهای کاربردی، ماموران بخش امنیتی
توسعه‌دهندگان
توسعه‌دهندگان مسئول توسعه برنامه‌های کاربردی سازمانی هستند. آن‌ها دسترسی به بخشی از سامانه اطلاعاتی با حق دسترسی بالا دارند اما انجام هرگونه اقدامی بر روی داده‌های تولیدی را ندارند.
مثال: برنامه‌های کاربردی توسعه‌دهندگان کسب و کار
پایگاه
این نوع مکان، شامل تمامی مکان‌هایی که دربرگیرنده یک دامنه و کاربرد یا بخشی از آن و ابزارهای فیزیکی مورد نیاز که برای آن به کار رود است.

محل
محیط خارجی

1 General Packet Radio Service

این بخش، مربوط به تمامی محل‌هایی است که در آن مفاهیم (ابزارهای) امنیتی سازمان نمی‌تواند مورد استفاده قرار گیرد.
به‌عنوان مثال: خانه‌های پرسنل، ابنیه سایر سازمان‌ها، مکان‌های خارج از سازمان

ساختمان‌ها و محوطه
این بخش منوط به عملکردهای مستقیم سازمانی است که در ارتباط با محوطه خارج آن محدود شده است. این امر، مربوط به یک مرز فیزیکی حفاظتی است که از طریق موانع فیزیکی یا مفاهیم نظارت در اطراف ساختمان به‌دست آمده است.
به‌عنوان مثال: بناء، ساختمان‌ها

منطقه
این بخش از طریق یک مرز فیزیکی حفاظتی تشکیل‌دهنده بخش‌ها درون محوطه سازمان به‌دست می‌آید. این بخش، از طریق ایجاد محدودیت‌های فیزیکی زیرساخت پردازش اطلاعات در سراسر سازمان به‌دست می‌آید.
به‌عنوان مثال: اداره‌ها، منطقه دسترسی محفوظ، منطقه امن)

خدمات اساسی
تمامی خدمات مورد نیاز برای عملی کردن تجهیزات سازمان

ارتباطات
خدمات مخابراتی و تجهیزات ارائه شده از سوی یک متصدی
به‌عنوان مثال: خط تلفن، PABX، شبکه‌های تلفن داخلی

تاسیسات
خدمات و وسایل (منابع و سیم کشی) مورد نیاز برای تامین نیرو در بخش تجهیزات فناوری اطلاعات و تجهیزات جانبی مرتبط با آن
به‌عنوان مثال: منبع نیرو با ولتاژ پایین، مبدل، مدار الکتریکی Head-End)
منبع آب
دفع زباله
خدمات و وسایل (تجهیزات، کنترل) برای خنک کردن و تصفیه هوا
به‌عنوان مثال: لوله آب سرد، دستگاه تهویه هوا

سازمان

نوع سازمان چارچوب سازمانی را نشان می‌دهد که شامل تمام ساختارهای پرسنل برای یک تکلیف خاص اختصاص داده شده و روش‌های کنترل این ساختارها است.

مقامات مسئول

اینها سازمان‌هایی هستند که سازمان‌های مورد مطالعه اختیارات خود را از آن‌ها دریافت کرده‌اند و ممکن است از نظر قانونی، وابسته یا خارجی باشند. این امر محدودیت‌هایی را از نظر قوانین و مقررات، تصمیمات و اقدامات به سازمان‌های تحت مطالعه تحمیل می‌کند.

مثال: بدنه اجرایی، بدنه مرکزی سازمان

ساختار سازمان

این ساختار شامل شعب گوناگون سازمان و فعالیت‌های میان کارکردی که کنترل آن برعهده مدیریت است، می‌شود.

مثال: مدیریت منابع انسانی، مدیریت IT، مدیریت خرید، مدیریت واحد کسب و کار، خدمات ایمنی ساختمان، خدمات آتش سوزی، مدیریت حسابرسی.

پروژه یا سامانه سازمانی

این مورد مربوط به سازمانی می‌شود که دارای یک پروژه یا خدمت ویژه است.

مثال: پروژه توسعه برنامه‌های کاربردی جدید، پروژه انتقال سامانه اطلاعاتی

پیمانکاران/ تأمین‌کنندگان/ تولیدکنندگان

این‌ها سازمان‌هایی هستند که در محدوده قرارداد، خدمات یا منابع به سازمان ارائه می‌کنند.

مثال: شرکت مدیریت تسهیلات، شرکت با منبع بیرونی، شرکت‌های مشاوره

ب ۲- ارزیابی دارایی

گام بعد از شناسایی دارایی، توافق در خصوص مقیاسی است که باید استفاده شود و معیاری برای یک محل خاص از آن مقیاس به یک دارایی معین براساس ارزیابی در نظر گرفته شود. به علت تنوع دارایی‌هایی که در بیشتر سازمان‌ها یافت می‌شود این احتمال وجود دارد که بعضی دارایی‌ها که ارزش مالی معینی دارند به واحد پول محلی ارزیابی شوند در حالی‌که بقیه دارایی‌ها که بیشتر ارزش کیفی دارند ممکن است ارزشی بین خیلی پایین تا خیلی بالا را به‌خود اختصاص دهند. تصمیم در مورد استفاده از مقیاس کمی در مقابل مقیاس کیفی اولویت‌های سازمان را منعکس می‌کند هر چند باید در ارتباط با دارایی باشد که قرار است ارزیابی شود. هر دو نوع ارزیابی می‌توانند برای یک دارایی معین استفاده شوند.

عبارات عادی مورد استفاده برای ارزیابی کیفی دارایی‌ها، شامل واژگان زیر است: ناچیز، بسیار کم، کم، متوسط، بالا، بسیار بالا، حیاتی. انتخاب و طیف عبارات مناسب برای یک سازمان تا حد زیادی به نیازهای امنیتی سازمان، اندازه سازمانی و دیگر عوامل خاص سازمانی بستگی دارد.

معیار

معیار به‌عنوان مبنای تخصیص ارزش به هر دارایی استفاده می شود که باید به‌صورت واضح نوشته شود. این اغلب یکی از سخت‌ترین جنبه‌های ارزیابی دارایی است زیرا ارزش بعضی از دارایی‌ها باید به‌صورت ذهنی تعیین شوند و بسیاری از افراد مختلف می‌توانند تعییناتی را انجام دهند. از معیارهای ممکن که

برای تعیین ارزش دارایی استفاده می شود شامل ارزش اولیه، هزینه جایگزینی و بازسازی هستند یا ارزش آن می تواند معنوی باشد برای مثال ارزش شهرت سازمانی.
مبنای دیگر ارزیابی دارایی‌ها، هزینه‌ای است که به‌علت از دست دادن محرمانگی، یکپارچگی و دردسترس بودن به‌صورت نتیجه یک رویداد متحمل می‌شود. عدم انکار، پاسخگویی، اصالت‌سنجی و قابلیت اعتماد نیز باید در صورت لزوم مورد توجه قرار گیرند. چنین ارزیابی ابعاد، عامل مهمی را برای ارزش دارایی فراهم می‌کند علاوه بر هزینه جایگزینی، برمبنای برآوردهای عواقب نامطلوب کسب و کار که از حوادث امنیتی با یک مجموعه پذیرفته شده از شرایط، ناشی می‌شوند. مورد تأکید است. این روش به نتایجی توجه دارد که برای مؤلفه‌های ارزیابی مخاطره ضروری هستند.
در طی ارزیابی ممکن است به بسیاری از دارایی‌ها چندین مقدار تخصیص داده شود. برای مثال: یک برنامه کسب وکار ممکن است براساس کار صرف شده برای پیشرفت برنامه ارزیابی شود یا ممکن است براساس کار وارد کردن داده ها ارزیابی شود و همچنین می‌تواند براساس ارزش آن نسبت به رقیب ارزیابی شود. هر یک از این ارزش‌های تخصیص داده شده می‌توانند تفاوت قابل توجهی داشته باشند. ارزش تخصیص داده شده می‌تواند حداکثر تمام ارزش‌های ممکن یا مجموع بعضی یا همه ارزش‌های ممکن باشد. در تحلیل نهایی اینکه کدام ارزش یا ارزش‌ها به دارایی اختصاص یافته باید به دقت تعیین شود زیرا ارزش نهایی تخصیص داده شده برای تعیین منابع برای حفظ دارایی صرف می‌شود.

کاهش تا مبنای مشترک

در نهایت تمام ارزش‌های دارایی باید به یک مبنای مشترک کاهش یابد.
این ممکن است با کمک معیارهایی مثل آنچه در ادامه گفته می‌شود انجام شود. معیارهایی که ممکن است برای ارزیابی عواقب احتمالی ناشی از فقدان محرمانگی، یکپارچگی، دسترس‌پذیری، عدم انکار، مسئولیت‌پذیری، سندیت، یا قابلیت اعتماد دارایی‌ها استفاده شود به‌صورت زیر است:

- نقض قوانین و/یا مقررات
- اختلال عملکرد کسب و کار
- فقدان حسن نیت/ اثر منفی روی شهرت
- نقض در ارتباط با اطلاعات شخصی
- به خطر افتادن امنیت شخصی
- عوارض جانبی بر روی اجرای قوانین
- نقض محرمانگی
- نقض نظم عمومی
- ضرر مالی
- اختلال در فعالیت‌های کسب و کار
- به خطر انداختن ایمنی محیط زیست

دیگر رویکردها در مورد ارزیابی عواقب به شرح زیر است:

- وقفه خدمات

- عدم توانایی در ارائه خدمات
- فقدان اعتماد مشتری
  - فقدان اعتبار در سامانه اطلاعات داخلی
  - آسیب به شهرت
- اختلال عملیات داخلی
  - اختلال در خود سازمان
  - هزینه‌های اضافی داخلی
- اختلال عملیات شخص ثالث
  - اختلال معاملات شخص ثالث با سازمان
  - انواع گوناگون خسارات
- تجاوز از قانون/ مقررات
  - عدم توانایی در انجام تعهدات قانونی
- نقض قرار داد
  - عدم توانایی اتمام تعهدات قراردادی
- خطر امنیت پرسنل/ کاربر
  - خطر برای پرسنل و/یا کاربران سازمان
- حمله به زندگی خصوصی کاربران
- ضرر مالی
- هزینه‌های مالی برای موارد اضطراری یا تعمیرات
  - بر حسب پرسنل
  - بر حسب تجهیزات
  - بر حسب مطالعات و گزارش کارشناسان
- فقدان کالاها/ سرمایه/ دارایی
- از دست دادن مشتریان/ از دست دادن تأمین‌کنندگان
- اقدامات قضایی و مجازات‌ها
- از دست دادن مزیت رقابتی
- از دست دادن رهبری فناوری/ فنی
- از دست دادن بازدهی/ اعتماد
- از دست دادن اعتبار فنی
- تضعیف توان مذاکره
- بحران‌های صنعتی (اعتصابات)
- بحران‌های دولتی
- اخراج

- خرابی مواد

این معیارها نمونه‌هایی از موضوعاتی است که باید برای ارزیابی دارایی در نظر گرفته شوند. برای ارزیابی یک سازمان باید معیار مربوط به هر نوع الزامات امنیت و کسب وکار را انتخاب کرد. این ممکن است به این معنی باشد که بعضی از معیارهای ذکر شده در بالا قابلیت کاربرد ندارند و بعضی دیگر ممکن است لازم باشد به فهرست اضافه شوند.

مقیاس

بعد از ایجاد معیارهای در نظر گرفته شده، سازمان باید در مورد مقیاسی توافق کند که باید در سطح سازمان مورد استفاده واقع شود. مرحله اول تصمیم در مورد تعداد سطوح مورد استفاده است. هیچ قاعده‌ای با توجه تعداد سطوح وجود ندارد که مناسب‌تر باشد. سطوح بیشتر سطح بالاتری از دانه دانه بودن را فراهم می‌آورد اما گاهی یک تمایز خوب و ظریف تکالیف سازگار در سازمان را مشکل می‌سازد. به‌طور معمول هر تعداد سطح بین ۳ (برای مثال پایین، متوسط، و بالا) و ۱۰ می‌تواند استفاده شود تا زمانی که با رویکرد سازمان سازگار باشد، رویکردی که سازمان برای کل فرایند ارزیابی خطر استفاده می‌کند.

یک سازمان ممکن است محدوده‌های خاص خود را برای ارزش دارایی تعریف کند مثل «پایین»، ‹‹متوسط›› یا ‹‹بالا››. این محدوده‌ها باید بر طبق معیار منتخب ارزیابی شوند (برای مثال برای ضرر مالی احتمالی آن‌ها باید برمبنای پولی عنوان شوند، اما برای ملاحظاتی مثل به‌خطر افتادن امنیت فردی، ارزیابی پولی می‌تواند پیچیده باشد و ممکن است برای تمام سازمان‌ها مناسب نباشد). در نهایت این به‌صورت کامل برعهده سازمان است تا تصمیم بگیرد که چه چیز نتایج "پایین" یا "بالا" را تشکیل می‌دهد. نتیجه‌ای که برای یک سازمان کوچک ممکن است فاجعه بار باشد می‌تواند برای یک مؤسسه خیلی بزرگ جزئی یا ناچیز باشد.

وابستگی‌ها

هر چه فرآیندهای کسب و کار که توسط دارایی حمایت می‌شوند متعددتر و با دارایی منطبق‌تر باشند، ارزش این دارایی‌ها بیشتر است. وابستگی به دارایی‌ها در فرآیندهای کسب و کار و دیگر دارایی‌ها باید مورد شناسایی قرار گیرد زیرا این ممکن است ارزش دارایی‌ها را تحت تأثیر قرار دهد. برای مثال محرمانه بودن داده‌ها باید در طول چرخه حیات آن‌ها حفظ شود در تمام مراحل ار جمله ذخیره و پردازش، یعنی نیاز امنیتی ذخیره داده‌ها و پردازش‌ها باید در راستای ارزش بیانگر محرمانه بودن داده‌های ذخیره و پردازش شده هدایت شود. همچنین اگر یک فرآیند کسب و کار بر یکپارچگی داده‌های خاصی تکیه کند که توسط برنامه تهیه شده‌اند، داده‌های ورودی این برنامه باید از قابلیت اعتماد مناسب برخوردار باشند. به‌علاوه یکپارچگی اطلاعات به سخت‌افزار و نرم‌افزار مورد استفاده برای ذخیره و پردازش بستگی خواهد داشت. همچنین سخت‌افزار به منبع انرژی و امکان تهویه هوا، وابسته است. بنابراین اطلاعات در مورد وابستگی‌ها در شناسایی تهدیدها و به‌خصوص آسیب‌پذیری‌ها اهمیت دارند. به‌علاوه این امر کمک می‌کند تا تضمین شود که ارزش واقعی دارایی‌ها (به واسطه روابط وابستگی) به دارایی ها داده شود و در نتیجه سطح مناسب حفاظت را نشان می‌دهد.

ارزش دارایی‌هایی که دیگر دارایی‌ها به آن‌ها وابسته هستند ممکن است به‌صورت زیر تعدیل شوند:

- اگر ارزش دارایی‌های وابسته (برای مثال داده‌ها) کمتر یا معادل ارزش دارایی‌های مورد نظر باشد (برای مثال نرم‌افزار) ارزش آن همین گونه باقی می‌ماند.
- اگر ارزش دارایی وابسته (برای مثال داده‌ها) بیشتر باشد در این صورت ارزش دارایی مورد نظر (برای مثال نرم‌افزار) باید افزایش یابد با توجه به:
  - درجه وابستگی
  - ارزش دیگر دارایی‌ها

یک سازمان ممکن است دارایی‌هایی که بیش از یکبار در دسترس هستند مثل نسخه‌های برنامه‌های نرم‌افزاری یا نوع مشابه کامپیوتر مورد استفاده در بیشتر دفاتر را داشته باشد. در نظر گرفتن این حقیقت در زمان ارزیابی دارایی‌ها اهمیت دارد. از یک طرف این دارایی‌ها به‌سادگی چشم‌پوشی می‌شوند لذا باید توجه داشت که تمام آن‌ها شناسایی شوند. از طرف دیگر آن‌ها می‌توانند استفاده شوند تا مشکلات دسترسی کاهش یابد.

خروجی

خروجی نهایی این مرحله فهرستی از دارایی‌ها و ارزش‌های خود مرتبط با افشاء (حفظ محرمانگی)، اصلاح (حفظ یکپارچگی، سندیت، عدم انکار بودن و پاسخگویی)، عدم دسترسی و تخریب (حفظ دسترسی و قابلیت اطمینان) و هزینه جایگزینی است.

ب ۳- ارزیابی اثرات

یک حادثه امنیت اطلاعات می‌تواند بیش از یک دارایی یا تنها بخشی از دارایی‌ها را تحت تأثیر قرار دهد. تأثیر به درجه موفقیت این حادثه بستگی دارد. در نتیجه یک تفاوت مهم بین ارزش دارایی و تأثیر ناشی از این حادثه وجود دارد. تأثیر می‌تواند هم اثر فوری (عملیاتی) داشته باشد یا اثری در آینده (کسب و کار)، که شامل پیامدهای مالی و بازار است، در نظر گرفته شود.

تأثیر فوری (عملیاتی) می‌تواند مستقیم یا غیر مستقیم باشد.

مستقیم

الف- ارزش مالی جایگزین دارایی یا بخشی از دارایی از دست رفته

ب- هزینه اکتساب، پیکربندی و نصب دارایی جدید یا پشتیبان

پ- هزینه تعلیق عملیات به‌علت حادثه تا زمانی که خدمات ارائه شده توسط دارایی(ها) ترمیم شود.

ت- نتایج تأثیر در نقض امنیت اطلاعات

غیر مستقیم

الف- هزینه فرصت (منابع مالی مورد نیاز برای جایگزینی یا تعمیر دارایی که در جایی دیگر استفاده می‌شود.)

ب- هزینه عملیات متوقف شده

پ- سوءاستفاده بالقوه اطلاعات حاصل از نقض‌های امنیتی

ت- نقض تعهدات قانونی یا نظارتی

ث- نقض کدهای اجرایی اخلاقی

به این ترتیب، اولین ارزیابی (بدون هیچ نوع کنترلی) اثر خیلی نزدیک به (ترکیبی از) ارزش دارایی‌های مطرح شده را تخمین می‌زند. برای تکرار بعدی هر یک از این دارایی(ها) اثر متفاوت (به‌طور معمول خیلی کوچک‌تر) به‌علت وجود و کارایی کنترل پیاده‌سازی شده، خواهد بود.

پیوست پ

(اطلاعاتی)

مثال‌های از تهدیدهای معمول

جدول زیر نمونه‌هایی از تهدیدهای معمول را ارائه می‌دهد. این فهرست می‌تواند در طول فرآیند ارزیابی تهدید مورد استفاده قرار گیرد. تهدیدها ممکن است عمدی، اتفاقی یا زیست‌محیطی (طبیعی) باشند و ممکن است موجب برای مثال آسیب یا از دست رفتن خدمات ضروری شوند. فهرست زیر به هر نوع تهدید اشاره دارد که در اینجا D (عمدی)، A (اتفاقی) و E (زیست‌محیطی) است. D برای تمام اقدامات عمدی استفاده می‌شود که دارایی‌های اطلاعاتی را هدف می‌گیرد، A برای تمام کارهایی استفاده می‌شود که توسط انسان انجام می‌پذیرد و می‌تواند به‌صورت اتفاقی به دارایی اطلاعاتی خسارت وارد کند و E برای تمام حوادثی استفاده می‌شود که براساس عملکرد انسانی نیست. گروه‌های تهدیدها به ترتیب اولویت نیستند.

جدول پ – ۱ – نمونه‌هایی از تهدیدهای معمول

نوع	تهدید	منبع
آسیب فیزیکی	آتش سوزی	A.D.E
	خرابی آب	A.D.E
	آلودگی	A.D.E
	سانحه اصلی	A.D.E
	آسیب به تجهیزات و یا رسانه	A.D.E
	آلودگی، خوردگی و انجماد	A.D.E
رویدادهای طبیعی	پدیده اقلیمی	E
	پدیده زلزله	E
	پدیده آتش‌فشانی	E
	پدیده هوا شناسی	E
	سیل	E
از دست رفتن خدمات ضروری	خرابی تهویه هوا یا سامانه تامین آب	A.D
	خرابی منبع نیرو	A,D,E
	خرابی تجهیزات مخابرات	A,D
اختلال براساس تشعشع	تشعشعات الکترو مغناطیسی	A,D,E
	تشعشع حرارتی	A,D,E
	پالس‌های الکترومغناطیسی	A,D,E

جدول پ – ۱ – ادامه

نوع	تهدید	منبع
ترکیب اطلاعات	قطع خطر سیگنال‌های مزاحم	D
	جاسوسی از دور	D
	شنود	D
	سرقت اسناد	D
	سرقت تجهیزات	D
	بازیابی رسانه بازیافتی یا رها شده	D
	افشاء	A,D
	داده‌های مربوط به منابع نامعتبر	A,D
	تحریف سخت‌افزار	D
	تحریف نرم‌افزار	A,D
	شناسایی موقعیت	D
شکست‌های فنی	خرابی تجهیزات	A
	اشباع سامانه اطلاعات	A,D
	نقص نرم‌افزار	A
	نقض نگه‌داری اطلاعات سامانه	A,D
اقدامات غیر مجاز	استفاده غیر مجاز از تجهیزات	D
	رونوشت جعلی از نرم افزار	D
	استفاده از نرم‌افزارهای تقلبی و یا کپی شده	A,D
	خرابی داده‌ها	D
	پردازش غیر قانونی داده‌ها	D
سازش عملکردها	اشکال در استفاده	A
	سوء استفاده از حقوق	A,D
	جعل حقوق	D
	محرومیت از اقدامات	D
	نقض در دسترس بودن پرسنل	A, D, E

توجه خاص باید به منابع تهدید انسانی صورت گیرد. آن‌ها به‌صورت خاص در جدول زیر طبقه‌بندی می‌شوند:

جدول پ - ۲ - منابع تهدیدهای انسانی

منبع تهدید	محرک	پیامدهای احتمالی
رخنه‌گر، نفوذگر	چالش خود برتر بینی اغتشاش موقعیت پول	• هک کردن • مهندسی اجتماعی • نفوذ در سامانه • دستیابی به سامانه غیرمجاز
جرائم رایانه‌ای	از بین بردن اطلاعات افشای غیرقانونی اطلاعات سود مالی تغییر غیرقانونی داده‌ها	• جرائم رایانه‌ای (برای مثال وسیله انتشار) • عمل کلاهبرداری (پخش، جعل هویت، نفوذ) • رشوه • حقه‌بازی • نفوذ در سامانه
تروریست	اخاذی تخریب سوءاستفاده انتقام منافع سیاسی پوشش‌دهی رسانه‌ای	• بمب /تروریسم • جنگ اطلاعاتی • حمله به سامانه (به عنوان مثال انکارتوزیع خدمات) • نفوذ در سامانه • مداخله در سامانه
جاسوسی صنعتی - (اطلاعات، شرکت-ها،دولت‌های خارجی و سایر منافع دولتی)	مزیت رقابتی جاسوسی اقتصادی	• مزایای دفاعی • مزایای سیاسی • بهره برداری اقتصادی • سرقت اطلاعات • دخالت در حریم فردی • مهندسی اجتماعی • نفوذ در سامانه • دستیابی به سامانه .غیرمجاز (دسترسی به اطلاعات طبقه‌بندی شده، اختصاصی و/یا مرتبط با فناوری)

جدول پ - ۲ - ادامه

منبع تهدید	محرک	پیامدهای احتمالی
داخلی(ضعف بخش‌های آموزش دیده، عدم رضایت، تخریب، غفلت، غیر معتمد و یا فسخ کارمندان نا معتبر)	کنجکاوی خودپسندی اطلاعات سود مالی انتقام خطاها و عملکردهای غیر عمدی (به عنوان مثال، خطای ورود داده‌ها و خطای برنامه ریزی)	• تهدید کارمند • اخاذی • جست و جوی اطلاعات مالکیت • سوءاستفاده از رایانه • کلاهبرداری و سرقت • رشوه‌دهی اطلاعاتی • ورود داده‌های نادرست یا تحریف شده • قطع • کد نادرست (ویروس،- بدافزار یا Trojan) • فروش اطلاعاتی فردی • ویروس در سامانه • اختلال در سامانه • کارشکنی • دستیابی غیرمجاز به سامانه

پیوست ت

(اطلاعاتی)

عوامل در معرض مخاطره و روش‌های مربوط به ارزیابی آن‌ها

ت - ۱ نمونه‌های آسیب‌پذیری

جدول زیر نمونه‌هایی از آسیب‌پذیری در انواع حوزه‌های امنیتی شامل نمونه‌هایی از تهدیدهایی که می‌تواند این آسیب‌پذیری‌ها را مورد سوء استفاده قرار دهد، ارائه می‌کند. این فهرست می‌تواند در طول ارزیابی تهدیدها و آسیب‌پذیری‌ها کمک کند تا سناریوهای رویدادهای مرتبط تعیین شود. تأکید می‌شود که در بعضی از موارد سایر تهدیدها می‌توانند از این آسیب‌پذیری‌ها سوءاستفاده کنند.

جدول ت - ۱ - نمونه‌هایی از آسیب‌پذیری در انواع حوزه‌های امنیتی

نوع	نمونه‌هایی از آسیب پذیری	نمونه‌هایی از تهدیدها
سخت‌افزاری	تعمیر و نگهداری ناقص رسانه‌های ذخیره‌سازی اطلاعات	نقص در سیستم اطلاعات قابل نگهداری
	نقص طرح جایگزینی تناوبی	تخریب تجهیزات و رسانه‌ها
	حساسیت به گرد و خاک و رطوبت	خوردگی، انجماد، خاک خوردگی
	حساسیت به امواج الکترو مغناطیسی	تابش الکترو مغناطیسی
	نقص تنظیمات کنترل تغییرات	خطا در استفاده
	حساسیت به تغییرات ولتاژ	از دست دادن منبع تغذیه
	حساسیت به تغییرات دما	حوادث طبیعی
	رسانه‌های ذخیره‌سازی محافظت نشده	سرقت از رسانه‌ها و یا اسناد
	نقص مراقبت در دسترس	سرقت از رسانه‌ها و یا اسناد
	کپی کردن کنترل نشده	سرقت از رسانه‌ها و یا اسناد

جدول ت - ۱ - ادامه

نوع	نمونه‌هایی از آسیب پذیری	نمونه‌هایی از تهدیدها
نرم افزار ی	نقص یا آزمون ناکافی نرم‌افزار	سوء استفاده از حقوق
	نقص شناخته شده در نرم‌افزار	سوء استفاده از حقوق
	خارج نشدن از حساب کاربری در حین خارج شدن از پشت ایستگاه کاری	سوء استفاده از حقوق
	دفع یا استفاده مجدد از رسانه‌های ذخیره‌سازی بدون پاک‌سازی مناسب	سوء استفاده از حقوق
	نقص در ممیزی	سوء استفاده از حقوق
	دادن مجوزهای دسترسی اشتباه	سوء استفاده از حقوق
	توزیع نرم‌افزار به صورت گسترده	تحریف در داده‌ها
	استفاده از برنامه‌های کاربردی برای داده‌های نادرست در زمان نامناسب	تحریف در داده‌ها
	واسط کاربری پیچیده	خطا در استفاده
	نقص در مستندسازی	خطا در استفاده
	نصب نادرست	خطا در استفاده
	تاریخ‌های نادرست	خطا در استفاده
	نقص سازوکار شناسایی و تصدیق (مانند تصدیق کاربران)	تقلب
	رمز عبورهای محافظت نشده	تقلب
	مدیریت رمز عبور ضعیف	تقلب
	خدمات غیر لازم فعال شده	پردازش غیرقانونی داده
	نرم‌افزارهای جدید تکامل نیافته	نقص نرم افزار
	مشخصه‌های ناکامل و ناواضح برای توسعه‌دهندگان	نقص نرم افزار
	نقص در کنترل تغییرات موثر	نقص نرم افزار
	دانلود و استفاده از نرم‌افزارها به صورت کنترل نشده	مداخله و سو استفاده در نرم‌افزار
	نقص در پشتیبان‌گیری مناسب	مداخله و سو استفاده در نرم‌افزار
	نقص در حفاظت فیزیکی ساختمان، درب‌ها و پنجره‌ها	سرقت رسانه‌ها و اسناد
	عدم ایجاد گزارشات مدیریتی	استفاده- ی غیر مجاز از تجهیزات
شبکه	نقص در مدارک و مستندات ارسال و دریافت پیام	انکار اعمال
	خطوط ارتباطی محافظت نشده	استراق سمع
	عبور و مرور محسوس محافظت نشده	استراق سمع
	کابل‌کشی ضعیف	معیوب بودن تجهیزات ارتباطی
	نقص در شناسایی و تصدیق فرستنده و گیرنده	تقلب
	ساختار شبکه‌ی نا امن	جاسوسی از راه دور
	انتقال رمزهای عبور	جاسوسی از راه دور
	مدیریت شبکه ی نا مناسب	اشباع سیستم اطلاعاتی
	اتصالات شبکه‌ی عمومی محافظت نشده	استفاده از تجهیزات بدون تصدیق

جدول ت - ۱ - ادامه

نوع	نمونه‌هایی از آسیب پذیری	نمونه‌هایی از تهدیدها
پرسنل	غیبت پرسنل	عدم دسترسی‌پذیری پرسنل
	فرآیند نامناسب استخدام	تخریب تجهیزات و رسانه‌ها
	آموزش ناکافی امنیتی	خطا در استفاده
	استفاده نادرست از سخت‌افزار و نرم‌افزار	خطا در استفاده
	نقص در هشدارهای امنیتی	خطا در استفاده
	نقص در نظارت و پایش سازوکارها	پردازش غیر قانونی
	نقص در سیاست‌های استفاده‌ی مناسب از رسانه‌های ارتباطی و پیام‌رسان	استفاده‌ی تصدیق نشده از تجهیزات
سایت سازمان	نقص یا بی دقتی در استفاده از کنترل‌های دسترسی فیزیکی به ساختمان و اتاق‌ها	تخریب تجهیزات یا محیط
	ناپایداری توان شبکه	نقص توان تغذیه
	نقص در پشتیبانی فیزیکی برای ساختمان و درها و پنجره‌ها	سرقت تجهیزات
	نقص در رویه-های رسمی برای دسترسی ثبت شده و ثبت نشده	سوء استفاده از حقوق
	نقص در رویه‌های برای بازبینی دسترسی صحیح (نظارت)	سوء استفاده از حقوق
	نقص یا نارسایی در تدارکات (در خصوص امنیت) در تعهدات به‌وسیله مشتریان و/یا شخص -ثالث	سوء استفاده از حقوق
	نقص در رویه‌هایی برای پایش از وسایل تحویل اطلاعات	سوء استفاده از حقوق
	نقص در بازرسی‌های قانونی (نظارت)	سوء استفاده از حقوق
	نقص در رویه‌های شناسایی ریسک و ممیزی	سوء استفاده از حقوق
	نقص در گزارشات ثبت شده اشتباه در مدیریت و ثبت وقایع	سوء استفاده از حقوق
	سرویس نامناسب نگهداری از پاسخ‌ها	نقض قوانین نگهداری سیستم اطلاعات
	نقص یا نارسایی در سطوح سرویس قراردادی	نقض قوانین نگهداری سیستم اطلاعات
	نقص در روش رسمی برای مستند سازی کنترل ISMS	تحریف داده
	نقص در روش رسمی برای نظارت بر ثبت ISMS	تحریف داده
	نقص در روش رسمی برای اجازه دسترسی عمومی اطلاعات	داده بواسطه منابع غیرقابل اعتماد
	نقص در تخصیص وظایف امنیت اطلاعات ویژه	عدم پذیرش کارها
	نقص در طرح استمرار	خرابی تجهیزات
	نقص در سیاست استفاده از ایمیل	خطا در استفاده
	نقص در رویه‌هایی برای ورود نرم‌افزار به سیستم‌های عملیاتی	خطا در استفاده
	نقص بایگانی در متولی و فهرست کارمندان	خطا در استفاده

جدول ت – ۱ – ادامه

نوع	نمونه‌هایی از آسیب پذیری	نمونه‌هایی از تهدیدها
	نقص در رویه‌هایی برای بررسی طبقه‌بندی اطلاعات	خطا در استفاده
	نقص در ضمانت امنیت اطلاعات در شرح کارها	خطا در استفاده
	نقص یا نارسایی در قوانین (درخصوص امنیت اطلاعات) در تعهدات کارمندان	تهیه کردن غیر قانونی داده‌ها
	نقص در سیاست‌های کامپیوترهای قابل حمل	سرقت تجهیزات
سایت	نقص در کنترل‌های غیر منطقی دارایی‌ها	سرقت تجهیزات
سازمان	نقص یا نارسایی در خط‌مشی میز پاک و صفحه پاک	سرقت تجهیزات
	نقص در اجازه تهیه کردن اطلاعات تجهیزات	سرقت محیط و مستندات
	نقص در سازوکارهای پایش برای شکاف‌های امنیتی	سرقت محیط و مستندات
	نقص در بازبینی‌های مدیریتی قانونمند	استفاده غیر مجاز از محیط
	نقص در رویه‌هایی برای عیوب گزارشات امنیت	استفاده غیر مجاز از محیط
	نقص در رویه‌هایی برای فراهم آوردن مطلوبیت‌ها به‌وسیله افکار صحیح	استفاده از از نرم‌افزارهای کپی یا جعلی

ت -۲ روش‌های مربوط به ارزیابی آسیب‌پذیری فنی

روش‌های پیش‌گستر مثل آزمون سامانه اطلاعات می‌توانند در شناسایی آسیب‌پذیری‌ها مورد استفاده واقع شوند. بسته به مهم بودن اطلاعات و سامانه فناوری ارتباطی (ICT) و منابع در دسترس (برای مثال سرمایه تخصیص یافته، فناوری دردسترس، افراد با تجربه برای اجرای آزمون). روش‌های آزمون به شرح زیر است:

- ابزار پویش[1] خودکار آسیب‌پذیری
- ارزیابی و آزمون امنیت
- آزمون نفوذ پذیری
- بررسی رمزها

ابزار پویش خودکار آسیب‌پذیری برای پویش گروهی از خدمات میزبان یا یک شبکه برای خدمات آسیب‌پذیر شناخته شده استفاده می‌شود (برای مثال سامانه اجازه پروتکل انتقال داده‌های (FTP[2]) بی‌نام را می‌دهد یا تقویت ارسال نامه). اگرچه باید عنوان کرد که بعضی از آسیب‌پذیری‌های بالقوه توسط ابزار پویش خودکار به‌صورت آسیب‌پذیری واقعی در متن محیط سامانه نشان داده نمی‌شوند. برای مثال بعضی از این ابزارهای پویش آسیب‌پذیری‌های بالقوه را بدون توجه به موقعیت محل و شرایط طبقه‌بندی

1 - Scan
2 - File Transfer Protocol

می‌کنند. بعضی از آسیب‌پذیری‌ها که با نرم‌افزار پویش خودکار مشخص می‌شوند ممکن است در واقع برای یک موقعیت خاص آسیب‌پذیر نباشند اما ممکن است به آن صورت پیکربندی شوند زیرا محیط به آن‌ها نیاز دارد. بنابراین این روش آزمون می‌تواند یقین‌های اشتباه ایجاد کند.

ارزیابی و آزمون امنیت (STE) [1] فن دیگری است که می‌تواند در شناسایی آسیب‌پذیری‌های سامانه ICT در طول فرآیند ارزیابی مخاطره استفاده شود. این فن شامل توسعه و اجرای برنامه آزمون می‌شود (برای مثال متن آزمون، روش آزمون، نتایج مورد انتظار آزمون). هدف آزمون امنیت سامانه، آزمون تأثیر کنترل‌های امنیتی یک سامانه ICT است زیرا که آن‌ها در محیط‌های عملیاتی استفاده می‌شوند. هدف دادن این تضمین است که کنترل‌های به‌کار رفته شرایط تأیید شده امنیت را برای سخت‌افزار و نرم‌افزار برآورده می‌کند و سیاست‌های امنیتی سازمان را به‌کار می‌برند یا استانداردهای صنعتی را دربر می‌گیرند.

آزمون نفوذ [2] می‌تواند برای تکمیل بررسی کنترل‌های امنیتی مورد استفاده قرار گیرد و تضمین کند که سامانه ICT امن است. آزمون نفوذ وقتی در فرآیند ارزیابی مخاطره استفاده می‌شود، می‌تواند برای ارزیابی توانایی سامانه ICT در تحمل تلاش‌های عمدی برای گیرانداختن امنیت سامانه مورد استفاده قرار گیرد. هدف آن آزمایش سامانه ICT از نقطه نظر منابع تهدید و شناسایی طرح‌های بالقوه حفاظتی خطاهای بالقوه در سامانه ICT، است.

بررسی رمز کامل‌ترین روش برای ارزیابی آسیب‌پذیری است. (اما خیلی گران است).

نتایج این نوع آزمون‌های امنیت به شناسایی آسیب‌پذیری‌های سامانه کمک می‌کند.

لازم به تذکر است که فنون و ابزارهای نفوذ می‌توانند نتایجی اشتباهی ارایه دهند مگر اینکه آسیب‌پذیری به‌طور موفق استخراج شود. برای استخراج آسیب‌پذیری‌های خاص فرد باید با سامانه، کاربرد و راه اندازی تکه‌های سامانه آزمایش شده به‌طور کامل آشنا باشد. اگر این داده‌ها در زمان آزمایش معلوم نباشند این امکان وجود ندارد که آسیب‌پذیری خاص به‌صورت موفق استخراج شود (برای مثال به‌دست آوردن لایه محافظ مخالف راه دور)، اگرچه هنوز این امکان وجود دارد تا فرآیند آزمایش شده یا سامانه خراب یا دوباره راه‌اندازی شود. در چنین مواردی شیء مورد آزمایش نیز باید آسیب‌پذیر برآورد شود.

روش‌ها می‌توانند شامل فعالیت‌های زیر باشند:

- مصاحبه با مردم و کاربران
- پرسش نامه
- بررسی فیزیکی
- تحلیل اسناد

1 - Security Testing and Evaluation
2 - Penetration Testing

پیوست ث

(اطلاعاتی)

روش‌های ارزیابی مخاطرات امنیت اطلاعات

ث – ۱ ارزیابی مخاطرات امنیت اطلاعات سطح بالا

ارزیابی سطح بالا اجازه تعریف اولویت‌ها و تقدم‌های تاریخی در عملیات را می‌دهد. به دلایل مختلف مثل بودجه، ممکن است پیاده‌سازی تمام کنترل‌ها به‌صورت همزمان ممکن نباشد و تنها مهم‌ترین مخاطرات در طول فرآیند عملیات مخاطره مورد خطاب قرار گیرند. همچنین این ممکن است درست نباشد که مدیریت کامل مخاطره را شروع کرد اگر پیاده‌سازی تنها پس از یک یا دو سال در نظر گرفته شده باشد. برای رسیدن به این هدف، ارزیابی سطح بالا ممکن است با ارزیابی سطح بالای نتایج به‌جای شروع با تحلیل نظام‌مند تهدیدها، آسیب‌پذیری‌ها و دارایی‌ها و پیامدها شروع شود.

دلیل دیگر برای شروع با ارزیابی سطح بالا این است که همگام با دیگر برنامه‌های مرتبط با مدیریت تغییرات (یا تداوم کسب و کار) ایجاد شود. برای مثال این درست نیست که اگر برنامه‌ریزی شود که از منابع خارجی در آینده نزدیک در آن سامانه استفاده شود، یک سامانه یا نرم‌افزار کاربردی به‌طور کامل ایمن شود اگرچه هنوز بهتر است که ارزیابی مخاطره صورت گیرد تا قرارداد منبع خارجی تعریف شود.

ویژگی‌های تکرار ارزیابی خطر سطح بالا می‌توانند شامل موارد زیر باشند:

- ارزیابی مخاطرات سطح بالا می‌تواند دیدگاه‌های کلی‌تری از سازمان و سامانه‌های اطلاعاتی آن را مخاطب سازد و جنبه‌های فناوری به‌صورت مستقل از موضوعات کسب و کار را ملاحظه کند. با انجام این کار تحلیل متن بیشتر روی کسب وکار و محیط عملیاتی متمرکز خواهد بود تا روی عناصر فناوری.
- ارزیابی مخاطره سطح بالا فهرست محدودتری از تهدیدها و آسیب‌پذیری‌های گردآوری شده در حوزه-های تعریف شده را مخاطب می‌سازد یا برای تسریع فرآیند روی سناریوی مخاطره یا تهدید در عوض عوامل خود، تمرکز می‌کند.
- مخاطرات ارائه شده در ارزیابی مخاطره سطح بالا به‌صورت عمومی، حوزه کلّی‌تری دارند تا خطراتی که به‌صورت خاص شناسایی شده‌اند. از آنجا که سناریوها یا تهدیدها در حوزه‌هایی گروه‌بندی می‌شوند که درمان مخاطره، فهرست‌هایی از کنترل در این حوزه را پیشنهاد می‌دهند. فعالیت‌های درمان مخاطره، سعی دارند که اول کنترل‌های مشترک را پیشنهاد و انتخاب کنند که در کل سامانه معتبر هستند.
- اگرچه ارزیابی سطح بالای مخاطره به‌علت اینکه به‌ندرت جزئیات فناوری را مخاطب می‌سازد، برای ارائه کنترل‌های سازمانی و غیرفنی و جنبه‌های مدیریت کنترل‌های فنی یا حفاظت‌های فنی معمول و کلیدی مثل برنامه‌های پشتیبان یا ضد ویروس مناسب‌تر است.

مزایای ارزیابی مخاطره سطح بالا به شرح زیر است:

- جای دادن رویکرد اولیه ساده، به احتمال زیاد قبولی طرح ارزیابی خطر را به‌دست می‌آورد.

- باید این امکان وجود داشته باشد که یک تصویر راهبردی از برنامه امنیت اطلاعات سازمانی ترسیم شود به‌عبارتی این به‌عنوان یک کمک خوب برنامه‌ریزی عمل خواهد کرد.
- منابع و پول می‌توانند در مکانی به‌کار روند که سودمندتر هستند و سامانه‌ای که به احتمال زیاد نیاز بیشتری به حمایت دارد می‌تواند اول مورد خطاب قرار گیرد.

از آنجا که تحلیل‌های اولیه مخاطره در سطح بالا صورت می‌گیرند و به‌طور بالقوه از دقت کمتری برخوردار هستند تنها ضعف بالقوه این است که بعضی از فرآیندها و سامانه‌های کسب و کار به‌نظر نمی‌رسد که به ارزیابی دقیق مخاطره دومی نیاز داشته باشند. اگر اطلاعات کافی از تمام جوانب سازمان و از سامانه‌ها و اطلاعات آن شامل اطلاعات حاصل از ارزیابی حوادث امنیت اطلاعات وجود داشته باشد، از این می‌توان اجتناب کرد.

ارزیابی مخاطره سطح بالا ارزش‌های کسب و کار دارایی‌های اطلاعاتی و مخاطرات حاصل از دیدگاه کسب و کار سازمان را در نظر می‌گیرد. در اولین نقطه (شکل ۲ را ببینید.) تصمیم‌گیری عوامل متعددی در تعیین اینکه آیا ارزیابی سطح بالا برای شناسایی مخاطرات کافی هستند، این عوامل شامل موارد زیر می‌شود:

- باید با استفاده از دارایی‌های اطلاعاتی گوناگون اهداف کسب وکار حاصل شوند؛
- درجه وابستگی کسب و کار سازمانی به دارایی‌های اطلاعاتی، به‌عبارتی آیا کارکردی که سازمان برای بقای خود در نظر گرفته یا اجرای مؤثر کسب و کار حیاتی به هر یک از دارایی‌ها بستگی دارند یا به رازداری، یکپارچگی، در دسترس بودن، عدم انکار، پاسخگویی، سندیت، و قابلیت اطمینان از اطلاعات ذخیره شده و پردازش شده در این دارایی‌ها ارزیابی می‌کند؛
- سطح سرمایه‌گذاری روی هریک از دارایی اطلاعاتی بر حسب توسعه، نگهداری یا جایگزین کردن دارایی؛
- دارایی‌های اطلاعاتی که سازمان به‌طور مستقیم برای آن ارزش اختصاص می‌دهد.

وقتی این عوامل ارزیابی شوند تصمیم‌گیری راحت‌تر می‌شود. اگر اهداف هر دارایی در واقع برای اجرای کسب و کار سازمان بسیار مهم باشد یا اگر دارایی‌ها در مخاطره بالایی باشند در این صورت تکرار دوم ارزیابی مخاطره دقیق باید برای دارایی‌های خاص اطلاعاتی (یا بخشی از آن) صورت گیرد.

یک قاعده کلی مورد اجرا این است که: اگر نقض امنیت اطلاعات بتواند به عوارض جانبی قابل توجهی در سازمان و فرآیندهای کسب و کار یا دارایی‌های آن منجر شود، در این صورت تکرار دوم ارزیابی مخاطره در سطح جزئیات بیشتر برای شناسایی مخاطرات بالقوه ضرورت دارد.

ث -۲ ارزیابی جزئی مخاطره امنیت اطلاعات

فرآیند ارزیابی جزئی مخاطره امنیت اطلاعات شامل شناسایی و ارزیابی دقیق دارایی‌ها، ارزیابی تهدیدها برای دارایی‌ها، و ارزیابی آسیب‌پذیری است. سپس نتایج این فعالیت‌ها برای ارزیابی مخاطرات مورد استفاده قرار می‌گیرد و بعد درمان مخاطره شناسایی می‌شود.

مرحله جزئی، به‌طور معمول به زمان، تلاش و تجربه زیادی نیاز دارد و بنابراین ممکن است برای سامانه‌های اطلاعات در مخاطره، مناسب باشند.

مرحله نهایی ارزیابی مخاطره امنیت اطلاعاتی جزئی، ارزیابی مخاطرات به‌طور کلی است که این ضمیمه بر آن متمرکز است.

پیامدها می‌توانند به چندین روش شامل استفاده از شاخص‌های کمی مثل اقدامات پول و کیفی (که می‌تواند بر اساس استفاده از صفاتی باشد مثل میانی و شدید) یا ترکیبی از هر دو راه ارزیابی شوند. برای ارزیابی احتمال وقوع تهدید، چارچوب زمانی که برمبنای آن دارایی ارزش پیدا می‌کند یا نیاز به حفاظت دارد باید ایجاد شود. احتمال وقوع یک خطر خاص تحت تاثیر عوامل زیر است:

- جذابیت دارایی یا تأثیر احتمالی کاربردی وقتی یک تهدید عمدی انسانی مورد ملاحظه است.
- سهولت تبدیل بهره‌برداری از یک آسیب‌پذیری به‌صورت پاداش به‌صورت کاربردی در جایی که تهدید عمدی انسانی مورد ملاحظه است.
- توانایی‌های فنی عامل تهدید به‌صورت کاربردی در جایی که تهدید عمدی انسانی مورد ملاحظه است.
- قرار گرفتن آسیب‌پذیری در معرض بهره‌برداری، به‌صورت کاربردی در هر دو آسیب‌پذیری‌های فنی و غیرفنی

بسیاری از روش‌ها از جدول استفاده می‌کنند و شاخص‌های ذهنی و تجربی را ترکیب می‌کنند. این مهم است که سازمان از روشی استفاده کند که سازمان با آن احساس راحتی کند و به آن اعتماد داشته و اینکه نتایج قابل تکرار ایجاد کند. تعدادی از فنون مبتنی بر جدول در زیر آورده شده است.

برای اطلاعات بیشتر در مورد فنونی که می‌تواند برای ارزیابی مخاطرات امنیت اطلاعات جزئی به‌کار رود. به IEC 31010 مراجعه کنید.

نمونه‌های زیر از اعداد استفاده می‌کنند تا ارزیابی‌های کیفی را توضیح دهند. کاربران این روش‌ها باید آگاه باشند که این ممکن است برای عملیات ریاضی بی‌اعتبار باشد چون با استفاده از اعداد انجام می‌شود که نتایج کیفی تولید شده از روش‌های ارزیابی مخاطره کیفی هستند.

ث ۲-۱ مثال۱: ماتریس با ارزش‌های از پیش تعیین شده

در روش‌های ارزیابی مخاطره از این نوع دارایی‌های فیزیکی پیشنهادی یا واقعی بر حسب هزینه‌های جایگزینی یا بازسازی ارزش‌گذاری می‌شوند. (به‌عبارتی اندازه‌گیری کمی) سپس این هزینه‌ها به مقیاس کیفی مشابه تبدیل می‌شوند که برای اطلاعات نیز استفاده می‌شود. (پایین را ببینید.) دارایی‌های نرم‌افزاری واقعی یا پیشنهادی مانند دارایی‌های فیزیکی ارزیابی می‌شوند. با توجه به هزینه خرید یا بازسازی شناخته شده و سپس به مقیاس کیفی به‌صورتی که برای اطلاعات استفاده شده تبدیل می‌شوند. به‌علاوه اگر معلوم شود که نرم‌افزار کاربردی به شرایط درونی خود برای یکپارچگی یا رازداری احتیاج دارد (برای مثال اگر کد منبع خودش از نظر تجاری حساس باشد.) به همان صورت اطلاعات ارزیابی می‌شود.

ارزش اطلاعات از طریق مصاحبه با مدیران منتخب کسب و کار ("صاحبان داده") به‌دست می‌آید، مدیرانی که به‌صورت مسئولانه در مورد داده‌ها صحبت می‌کنند تا ارزش و حساسیت داده‌ای که واقعاً مورد استفاده، ذخیره، پردازش و دسترسی است تعیین شود. مصاحبه‌ها ارزیابی ارزش‌ها و حساسیت اطلاعات را برحسب بدترین مورد سناریوها که می‌توان به‌صورت منطقی انتظار داشت، از نتایج نامطلوب

کسب و کار به‌علت افشای غیرمجاز، اصلاح غیرمجاز و عدم دردسترس بودن دوره‌های زمانی مختلف و تخریب ناشی شوند تسهیل می‌کنند.

ارزیابی با استفاده از دستورالعمل‌های ارزیابی اطلاعات که موارد زیر را پوشش می‌دهد به‌صورت:

- امنیت شخصی
- حریم و اطلاعات شخصی
- الزامات قانونی و مقرراتی
- اجرای قانون
- منافع اقتصادی و تجاری
- ضرر مالی/ اختلال فعالیت‌ها
- نظم عمومی
- سیاست و عملیات کسب و کار
- فقدان حسن نیت
- قرارداد یا توافق با مشتری

دستورالعمل شناسایی ارزش‌ها را برمبنای عددی تسهیل می‌کند مثل مقیاس ۰ تا ۴ که در ماتریس مثال زیر نشان داده شده است، بنابراین شناسایی ارزش‌های کمی در جایی که ممکن و منطقی باشد و شناسایی ارزش‌های کیفی را در جایی که ارزش‌های کمی امکان‌پذیر نیست (برای مثال به خطر افتادن زندگی انسان) ممکن می‌سازد. فعالیت اصلی بعدی تکمیل یک جفت پرسش‌نامه برای هر تهدید است برای هر گروه از دارایی‌ها که نوع تهدید به آن وابسته است و ارزیابی سطوح تهدید (احتمال وقوع) و سطوح آسیب‌پذیری (سهولت بهره‌برداری از تهدیدی که عواقب نامطلوب را موجب می‌شود) را ممکن می‌کند. پاسخ هر سئوال یک امتیاز دارد. این امتیازات از طریق یک مبنای دانش با هم جمع می‌شوند و در یک طیف مقایسه می‌شوند. این سطح شناسایی‌شده تهدید، برمبنای مقیاس بالا به پایین و سطح مشابه آسیب‌پذیری که در ماتریس نمونه زیر نیز آمده است بین انواع پیامدها در جای مربوط تمایز ایجاد می‌کند. اطلاعات برای تکمیل پرسش‌نامه باید از مصاحبه‌ها با افراد فنی و پرسنل و افراد کمکی و بازرسی موقعیت فیزیکی و بررسی اسناد گردآوری شود.

ارزش دارایی‌ها و سطوح تهدید و آسیب‌پذیری مربوط به هر پیامد در ماتریسی مثل آنچه در زیر آمده قرار داده می‌شوند تا برای هر ترکیب از اندازه‌های مرتبط مخاطره در مقیاس ۰ تا ۸ شناسایی شوند. ارزش‌ها به‌صورت دارای ساختار در ماتریس قرار می‌گیرند. یک نمونه در زیر آمده است:

جدول ث- ۱- الف

	احتمال وقوع _ تهدید	کم			متوسط			زیاد		
	سهولت بهره‌برداری	L	H	M	L	H	M	L	H	M
ارزش دارایی	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

برای هر دارایی آسیب‌پذیری‌های مربوط و تهدیدهای وابسته به خود در نظر گرفته می‌شود. اگر یک آسیب‌پذیری بدون تهدید وابسته وجود داشته باشد یا یک تهدید بدون آسیب‌پذیری وابسته احتمال خطری وجود ندارد. (اما باید دقت شود تا تغییر در موقعیت بود.) حال سطر مناسب در ماتریس توسط ارزش دارایی و ستون مناسب توسط احتمال وقوع تهدید و سهولت بهره‌برداری شناسایی می‌شود. برای مثال اگر دارایی ارزش ۳ دارد، تهدید "بالا" و آسیب‌پذیری "پایین" باشد که اندازه مخاطره ۵ می‌شود. فرض کنید یک دارایی ارزش ۲ دارد برای مثال برای اصلاح سطح تهدید "پایین" بوده و سهولت بهره‌برداری "بالا" باشد در این‌صورت اندازه خطر ۴ می‌شود. اندازه ماتریس برحسب تعداد طبقات تهدید احتمالی، سهولت طبقه‌بندی بهره‌برداری و تعداد طبقات ارزیابی دارایی می‌تواند با نیاز سازمان تنظیم شود. ستون‌ها و سطرهای اضافی اندازه‌گیری مخاطره اضافی را ضروری نشان می‌دهد. ارزش این روش در رتبه بندی مخاطراتی است که مورد خطاب قرار می‌گیرند.

ماتریسی مشابه در جدول ث-۱- ب آمده است که حاصل درنظر گرفتن احتمال یک سناریو حادثه است که در مقابل تاثیر کسب و کار برآورد شده است. احتمال وقوع یک سناریوی حادثه با توجه به یک تهدید که از آسیب‌پذیری استفاده می‌کند با یک احتمال خاص ارائه می‌شود. جدول این احتمال را در مقابل تاثیر کسب و کار مربوط به سناریوی حادثه ترسیم می‌کند. مخاطره حاصله در مقیاس ۰ تا ۸ اندازه‌گیری می‌شود که می‌تواند در مقابل معیار پذیرش مخاطره ارزیابی شود. این مقیاس مخاطره، همچنین می‌تواند در یک رتبه بندی ساده مخاطره به‌صورت کلی ترسیم شود برای مثال به‌صورت زیر:

- مخاطره پایین۲-۰
- مخاطره متوسط: ۵-۳
- مخاطره بالا: ۸-۶

جدول ث- ۱- ب

	احتمال سناریو حادثه	خیلی پایین (بسیار بعید)	پایین (بعید)	متوسط (ممکن)	بالا (احتمالا)	بسیار بالا (احتمال بسیار بالا)
تاثیر کسب و کار	خیلی پایین	۰	۱	۲	۳	۴
	پایین	۱	۲	۳	۴	۵
	متوسط	۲	۳	۴	۵	۶
	بالا	۳	۴	۵	۶	۷
	بسیار بالا	۴	۵	۶	۷	۸

ث ۲-۲ مثال ۲: رتبه‌بندی تهدیدات توسط اندازه‌گیری مخاطره

یک ماتریس یا جدول مثل آنچه در جدول ث -۲ نشان داده شده می‌تواند برای ارتباط دادن عوامل پیامد (ارزش دارایی) و احتمال وقوع تهدید (باتوجه به جنبه‌های آسیب‌پذیری) استفاده شود. مرحله اول ارزیابی پیامدها (ارزش دارایی) براساس مقیاس از پیش تعریف شده است برای مثال ۱ تا ۵ از هر دارایی تهدید شده (ستون "b" در جدول). مرحله دوم ارزیابی احتمال وقوع تهدید است در مقیاس از پیش تعریف شده برای مثال ۱ تا ۵ از هر تهدید (ستون c در جدول). مرحله سوم محاسبه اندازه مخاطره است که حاصل ضرب (c ×b) است. در نهایت تهدیدها می‌توانند براساس اندازه مخاطره مربوط به خود، رتبه‌بندی شوند. در این مثال توجه داشته باشید که ۱ به‌عنوان پایین‌ترین پیامد و پایین‌ترین احتمال وقوع در نظر گرفته شده است.

جدول ث- ۲

توصیف کننده تهدید (a)	ارزش (دارایی) پیامد (b)	احتمال وقوع تهدید (c)	اندازه گیری مخاطره (d)	رتبه بندی تهدید (e)
تهدید A	۵	۲	۱۰	۲
تهدید B	۲	۴	۸	۳
تهدید C	۳	۵	۱۵	۱
تهدید D	۱	۳	۳	۵
تهدید E	۴	۱	۴	۴
تهدید F	۲	۴	۸	۳

همان‌طور که در بالا نشان داده شده است این روشی است که به تهدیدهای مختلف با پیامدهای مختلف و احتمال وقوع متفاوت اجازه می‌دهد که با هم مقایسه شده و بر حسب اولویت رتبه‌بندی شوند همان‌طور که در اینجا نشان داده شده است. در بعضی موارد ضرورت دارد که ارزش‌های مالی وابسته با مقیاس‌های تجربی در اینجا استفاده شوند.

ث-۲-۳ مثال۳: ارزیابی ارزش برای احتمال و پیامدهای احتمالی مخاطرات

در این مثال بر پیامدهای حوادث امنیت اطلاعاتی (یعنی سناریوهای حادثه) و تعیین اینکه به کدام سامانه باید اولویت داده شود تأکید شده است. این کار با ارزیابی دو ارزش برای هر دارایی و مخاطره انجام می‌شود که به‌صورت ترکیبی امتیاز هر دارایی تعیین خواهد شد. وقتی تمام امتیازات دارایی‌ها برای سامانه جمع شدند اندازه مخاطره آن سامانه تعیین می‌شود. اول یک ارزش به هر دارایی تخصیص می‌یابد. این ارزش مربوط به پیامدهای جانبی بالقوه است که می‌تواند در صورتی ایجاد شود که دارایی تهدید شود. برای هر تهدید به‌صورت کابردی، این ارزش دارایی به دارایی تخصیص می‌یابد.
بعد ارزش احتمالی تعیین می‌شود. این از ترکیب احتمال وقوع تهدید و سهولت بهره‌برداری از آسیب‌پذیری ارزیابی می‌شود. جدول (ث - ۳) احتمال سناریو حادثه را نشان می‌دهد.

جدول ث - ۳

احتمال تهدید	**پایین**			**متوسط**			**بالا**		
سطوح آسیب پذیری	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
ارزش احتمال سناریو حادثه	۰	۱	۲	۱	۲	۳	۲	۳	۴

سپس امتیاز دارایی/ تهدید با پیدا کردن سطح مشترک ارزش دارایی و ارزش احتمالی در جدول (ث - ۴) اختصاص داده می‌شود. امتیازات دارایی/ تهدید جمع می‌شود تا یک امتیاز کلی دارایی پیدا شود. این رقم می‌تواند برای تمایز بین دارایی‌های شکل‌دهنده بخشی از سامانه استفاده شود.

جدول ث - ۴

ارزش دارایی	۰	۱	۲	۳	۴
ارزش احتمال					
۰	۰	۱	۲	۳	۴
۱	۱	۲	۳	۴	۵
۲	۲	۳	۴	۵	۶
۳	۳	۴	۵	۶	۷
۴	۴	۵	۶	۷	۸

مرحله پایانی جمع تمام امتیازت کلی هر دارایی برای به‌دست آوردن دارایی‌های سامانه که امتیاز یک سامانه را دارد است. این می‌تواند برای تمایز بین سامانه‌ها استفاده شود و برای تعیین اینکه کدام حفاظت سامانه باید اولویت پیدا کند.

در مثال‌های زیر تمام ارزش‌ها به‌صورت تصادفی انتخاب شده اند. سامانه S را در نظر بگیرید که ۳ دارایی A1,A2,A3 دارد. همچنین در نظر بگیرید که دو تهدید T2, T1 وجود دارد که در سامانه S اعمال می‌شوند. فرض کنید ارزش A1 به اندازه ۳ باشد و ارزش دارایی A2 به اندازه ۲ باشد و ارزش دارایی A3 به اندازه ۴ باشد.

اگر برای A1 و T1 احتمال تهدید پایین و سهولت بهره‌برداری از آسیب‌پذیری متوسط باشد در این‌صورت ارزش احتمال ۱ است. (به جدول ث-۳ نگاه کنید.)

امتیاز دارایی/ تهدید A1/T1 می‌تواند از جدول (ث - ۴) به‌دست آید به‌عنوان سطح مشترک ارزش دارایی ۳ و ارزش احتمالی ۱ یعنی ۴. به‌صورت مشابه برای A1/T2 احتمال تهدید متوسط و سهولت بهره‌برداری از آسیب‌پذیری بالا است و این به A1/T2 امتیاز ۶ را می‌دهد.

حال ارزش کلی دارایی A1T می‌تواند محاسبه شود یعنی ۱۰. امتیاز کلی دارایی برای هر دارایی و تهدید کاربردی محاسبه می‌شود. امتیاز کلی سامانه از مجموع A1T+A2T+A3T به‌دست می‌آید تا ST به‌دست آید.

حالا سامانه‌های مختلف می‌توانند مقایسه شوند تا اولویت‌ها و دارایی‌های مختلف در یک سامانه نیز ایجاد شوند. مثال بالا برحسب سامانه‌های اطلاعاتی نشان داده شده است اگرچه رویکرد مشابه می‌تواند در فرآیند کسب و کار به‌کار رود.

پیوست ج

(اطلاعاتی)

محدودیت‌های مربوط به کاهش مخاطره

زمانی که محدودیت‌های اصلاح مخاطره مورد توجه است. محدودیت‌های زیر باید در نظر گرفته شوند.

محدودیت‌های زمانی:

انواع زیادی از محدودیت‌های زمانی می‌تواند وجود داشته باشد. برای مثال کنترل باید در یک دوره زمانی قابل قبول برای مدیران سازمان پیاده‌سازی شود. نوع دیگر محدودیت زمانی این است که آیا کنترل می‌تواند در طول عمر اطلاعات یا سامانه پیاده‌سازی شود. نوع سوم محدودیت زمان می‌تواند دوره زمانی باشد که مدیران سازمان تصمیم می‌گیرند دوره قابل قبول برای در معرض یک مخاطره خاص قرار گرفتن است.

محدویت‌های مالی:

کنترل‌ها از نظر پیاده‌سازی و حفظ نباید گران تر از ارزش مخاطراتی باشند که برای محافظت از آن‌ها طراحی شده‌اند مگر در جایی که سازگاری اجباری است. (برای مثال به‌موجب قانون) هر تلاشی که صورت می‌گیرد نباید از بودجه تخصیصی و مزیت مالی استفاده از آن کنترل تجاوز کند. اگرچه در بعضی موارد این امکان وجود ندارد که با توجه به محدودیت مالی به امنیت یا به سطح پذیرش مخاطره مطلوب رسید. بنابراین مدیران تصمیمی برای این شرایط می‌گیرند.

باید توجه شود به‌خصوص اگر بودجه تعداد یا کیفیت کنترل‌هایی که باید صورت گیرند را کاهش داده است زیرا این به نگهداری ضمنی مخاطره بالاتری از آنچه برنامه‌ریزی شده است منجر می‌شود.

محدودیت‌های فنی:

مشکلات فنی مثل سازگاری برنامه‌ها یا سخت‌افزار اگر در طول انتخاب کنترل در نظر گرفته شود به‌سهولت می‌تواند از آن اجتناب کرد. به‌علاوه کاربردهای بازنگرانه کنترل روی یک فرآیند یا سامانه موجود اغلب توسط محدودیت‌های فنی متوقف می‌شوند. این مشکلات می‌توانند تعادل کنترل را به سوی جنبه‌های کارکردی و فیزیکی متمایل کنند. ممکن است لازم باشد که برنامه امنیت اطلاعات مورد بازبینی قرار گیرد تا اهداف امنیتی حاصل شود. این زمانی روی می‌دهد که کنترل نتایج مورد انتظار در کاهش مخاطرات را بدون تقلیل بازدهی برآورده نمی‌کند.

محدودیت‌های عملیاتی:

محدودیت‌های عملیاتی مثل نیاز به اجرای ۷×۲۴ که هنوز پشتیبان‌ها را اجرا می‌کنند می‌توانند به کاربردهای پیچیده و پرهزینه کنترل منجر شود مگر اینکه از ابتدای کار طراحی شده باشند.

محدودیت‌های فرهنگی:

محدودیت‌های فرهنگی برای انتخاب کنترل‌ها می‌تواند خاص یک کشور، بخش، سازمان یا حتی دپارتمان یک سازمان باشد. تمامی کنترل‌ها را نمی‌توان در همه کشورها پیاده‌سازی کرد. برای مثال ممکن است

بتوان جستجوی کیف‌ها را در بخش‌هایی از اروپا پیاده‌سازی کرد، اما در خاورمیانه نه. جنبه‌های فرهنگی را نمی‌توان در نظر نگرفت زیرا بسیاری از کنترل‌ها به حمایت فعال کارمندان نیاز دارد. اگر کارمند علت نیاز به کنترل را نشناسد و آن را از نظر فرهنگی قابل قبول نداند کنترل در طول زمان بی‌تأثیر خواهد شد.

محدودیت‌های اخلاقی:

محدودیت‌های اخلاقی می‌تواند کاربرد زیادی در کنترل‌ها داشته باشد زیرا اخلاق براساس هنجار اجتماعی تغییر می‌کند. این می‌تواند از پیاده‌سازی کنترل‌هایی مثل بررسی پست الکترونیکی در برخی از کشورها جلوگیری کند. حریم اطلاعات شخصی نیز می‌تواند با توجه به اخلاق منطقه یا حکومت تغییر کند. این در برخی از بخش‌های صنعتی تا دیگران برای مثال دولت یا مراقبت‌های بهداشتی بیشتر اهمیت دارد.

محدودیت‌های محیطی:

عوامل محیطی می‌توانند بر انتخاب کنترل اثر گذارند مانند فضای دسترس‌پذیری، شرایط اقلیمی، جغرافیای طبیعی و شهری اطراف. برای مثال استدلال، زمین لرزه در برخی از کشورها، مهم بوده اما در سایر موارد، ضروری نیست.

محدودیت‌های قانونی:

عوامل قانونی مانند حفظ اطلاعات شخصی، مقررات قانون جزایی برای پردازش اطلاعات می‌تواند در انتخاب کنترل‌ها اثرگذار باشد. برآوردن تنظیم و مقررات می‌توانند نوع خاصی از کنترل مانند حفاظت از داده‌ها و ممیزی مالی تعهد را کند. آن‌ها همچنین می‌توانند استفاده از بعضی از کنترل‌ها برای مثال رمزنگاری را منع کنند. دیگر قوانین و مقررات مثل قانون روابط کاری، مقررات آتش نشانی، بهداشت و سلامت و بخش قوانین اقتصادی و ... می‌توانند انتخاب کنترل را تحت تأثیر قرار دهند.

سهولت استفاده:

واسط فناوری - انسانی ضعیف می‌تواند به خطای انسانی منجر شود یا می‌تواند کنترل را بی اثر کند. کنترل‌ها باید به نحوی انتخاب شوند که سهولت استفاده بهینه را در حالی‌که سطح قابل قبولی از مخاطره باقی مانده برای کسب و کار حاصل می‌شود فراهم کنند. کنترل‌هایی که استفاده از آن‌ها مشکل است می‌توانند بر روی کارایی آن‌ها، اثر گذار باشند زیرا کاربر همواره می‌خواهد تا حد ممکن از آن پیش‌دستی کند یا فرار کند. کنترل‌های با دسترسی دشوار در یک سازمان می‌تواند کاربر را تشویق کند که یک جایگزین روش دسترسی غیرمجاز برای آن پیدا کند.

محدودیت‌های کارکنان:

دسترس‌پذیری، هزینه‌ی حقوق و دستمزد مجموعه‌ی مهارت‌های تخصصی برای پیاده‌سازی کنترل‌ها و توانایی جابجایی کارمندان بین مکان‌هایی که شرایط کارکرد جانبی دارند، باید مورد توجه قرار گیرد. برای پیاده‌سازی کنترل‌های طرح‌ریزی شده ممکن است تخصص به سهولت در دسترس قرار نگیرد یا تخصص ممکن است برای سازمان خیلی گران باشد. جنبه‌های دیگر، مانند تمایل بعضی از کارمندان برای تبعیض با سایر کارمندانی که از نظر امنیتی نظارت نمی‌شوند می‌تواند مشکلاتی در کاربرد سیاست‌ها و عمل‌های امنیتی ایجاد کند. همچنین نیاز به استخدام افراد مناسب برای کار و یافتن افراد درست می‌تواند باعث

استخدام قبل از تکمیل بازرسی امنیتی شود. نیاز به تکمیل نظارت امنیتی قبل از استخدام عادی و ایمن و عملی است.

محدودیت یکپارچه‌سازی کنترل‌های جدید و موجود:

یکپارچه‌سازی کنترل‌های جدید در زیرساخت‌های موجود و وابستگی متقابل بین کنترل‌ها اغلب مورد توجه است. اگر کنترل‌های جدید با کنترل‌های موجود در تعارض و ناهمخوانی باشد، ممکن است به‌راحتی پیاده‌سازی نشود. برای مثال یک برنامه برای استفاده از نشانه زیست سنجی[1] برای کنترل دسترسی فیزیکی می‌تواند با روش جاری سامانه مبتنی بر صفحه شناسایی[2] در تعارض باشد. هزینه تغییر کنترل از کنترل فعلی به کنترل‌های طرح‌ریزی شده باید مؤلفه‌هایی را در برگیرد که با هزینه‌های کلی مقابله با مخاطره جمع شوند. ممکن است امکان پیاده‌سازی یک کنترل منتخب به علت تداخل با کنترل‌های موجود، وجود نداشته باشد.

1 - Biometric Tokens
2 - PIN-Pad

پیوست چ

(اطلاعاتی)

تفاوت در تعاریف بین ISO / IEC 27005: 2008- و ISO / IEC 27005: 2011

یادآوری – این پیوست برای کاربران ISO/IEC27001:2005 ارائه شده است. از آنجا که بعضی اصطلاحات و تعاریف در راهنمای ISO Giude 73:2009 در مقایسه با ISO/IEC27001:2005 و در نتیجه ISO/IEC27005:2008 متفاوت است، این پیوست تمام تغییرات مربوطه را مختصر می‌سازد. (منظور از n/a در جدول زیر not available می باشد).

اصطلاحات تعریف شده در رهنمودهای ایزو 73: 2009 مورد استفاده در ISO / IEC 27005: 2011	اصطلاحات تعریف شده در استاندارد ISO / IEC 27000: 2009 مورد استفاده در ISO / IEC 27005: 2008	اصطلاحات تعریف شده در استاندارد ISO / IEC 27005: 2008
۳-۱ **پیامد** نتیجه رویداد اثرگذار بر اهداف [ISO Guide 73: 2009] **یادآوری ۱**- رویداد می‌تواند به مجموعه‌ای از پیامدها منجر شود. **یادآوری ۲**- پیامدهاممکن است معین یا نامعین باشند و در زمینه امنیت اطلاعات به‌طور معمول معنای منفی دارند. **یادآوری ۳**- پیامدها را می‌توان به‌صورت کمی یا کیفی بیان کرد. **یادآوری ۴**- پیامدهای اولیه ممکن است به‌صورت زنجیره‌ای دامن‌گستر شوند.	**n/a**	**n/a**
۳-۲ **کنترل** اندازه‌گیری اصلاح مخاطره(3.9) [ISO Guide 73: 2009] **یادآوری ۱**- کنترل‌های امنیت اطلاعات شامل هر فرایند، خط‌مشی، روش اجرایی، رهنمود، شیوه یا ساختار سازمانی می‌شود که می‌تواند ماهیت اداری، فنی، مدیریتی یا حقوقی داشته باشد که مخاطرات امنیت اطلاعات را اصلاح می‌کند. **یادآوری ۲**- کنترل ممکن است همیشه اصلاح کننده موردنظر یا فرضی را نداشته باشد. **یادآوری ۳** - همچنین، کنترل مترادفی برای محافظت یا اقدام متقابل به‌کار می‌رود.	**کنترل** با استفاده از مدیریت مخاطرات، شامل خط‌مشی‌ها، روش اجرایی‌ها، رهنمودها، روش‌ها یا ساختارهای سازمانی است که می‌توانند ماهیت اداری، فنی، مدیریتی یا حقوقی داشته باشد **یادآوری** کنترل به عنوان مترادفی برای حفاظت یا اقدام متقابل استفاده می‌شود. [ISO/IEC 27002: 2005]	**n/a**

اصطلاحات تعریف شده در رهنمودهای ایزو 73: 2009 مورد استفاده در ISO / IEC 27005: 2011	اصطلاحات تعریف شده در استاندارد ISO / IEC 27000: 2009 مورد استفاده در ISO / IEC 27005: 2008	اصطلاحات تعریف شده در استاندارد ISO / IEC 27005: 2008
۳-۳ **رویداد** وقوع یا تغییر مجموعه خاصی از وضعیت‌ها [ISO Guide 73: 2009] **یادآوری ۱**- رویداد می‌تواند یک یا چند اتفاق باشد و چندین دلیل داشته باشد **یادآوری ۲**- رویداد می‌تواند شامل مواردی باشد که اتفاق نیفتاده است. **یادآوری ۳**- رویداد را گاهی رخداد یا حادثه می‌نامند.	**n/a**	**n/a**
۴-۳ **زمینه‌بیرونی** محیط بیرونی که سازمان در آن درپی دستیابی اهداف خود است. [ISO Guide 73: 2009] **یادآوری**: زمینه‌بیرونی می‌تواند شامل موارد زیر باشد: - محیط فرهنگی، اجتماعی، سیاسی، حقوقی، مقرراتی، مالی، فنی، اقتصادی، طبیعی و رقابتی که می‌توانند بین‌المللی، ملی، منطقه‌ای یا محلی باشند؛ - محرک‌های کلیدی و تمایلاتی که بر اهداف سازمان اثر دارند؛ و - روابط با ذی‌نفعان بیرونی و برداشت‌ها و ارزش‌های مربوطه -	**n/a**	**n/a**

اصطلاحات تعریف شده در رهنمودهای ایزو 73: 2009 مورد استفاده در ISO / IEC 27005: 2011	اصطلاحات تعریف شده در استاندارد ISO / IEC 27000: 2009 مورد استفاده در ISO / IEC 27005: 2008	اصطلاحات تعریف شده در استاندارد ISO / IEC 27005: 2008
این تعریف حذف شده است.		**۳-۱** **اثر** تغییر منفی در سطح اهداف حاصله‌ی کسب و کار
این تعریف حذف شده است. (به یادآوری ۶ از بند ۳-۹ مراجعه شود.)		**۳-۲** **مخاطره امنیت اطلاعات** قابلیت تهدید فرضی در بهره‌جویی از آسیب‌پذیری‌های دارایی یا گروهی از دارایی‌ها و در نتیجه لطمه زدن به سازمان **یادآوری** - بر حسب تلفیقی از احتمال رویداد و پیامد آن اندازه‌گیری می‌شود.
۳-۵ زمینه‌درونی محیط درونی که سازمان در آن درپی دستیابی اهداف خود است. [ISO Giude 73: 2009] **یادآوری**- زمینه‌درونی می‌تواند شامل موارد زیر باشد: - حاکمیت، ساختارسازمانی، نقش‌ها و مسئولیت‌پذیری‌ها؛ - خط‌مشی‌ها، اهداف و راهبردهایی که می‌بایست به آن‌ها دست یافت؛ - قابلیت ادراک در بخش منابع و دانش (مثل سرمایه، زمان، کارکنان، فرایندها، سامانه‌ها و فناوری‌ها)؛ - سامانه‌های اطلاعاتی، جریان‌های اطلاعاتی و فرایندهای تصمیم‌گیری (رسمی یا غیررسمی) - ارتباط با ذی‌نفعان درونی و برداشت‌ها و ارزش‌های مربوطه - فرهنگ سازمانی - استانداردها، رهنمودها و حالت‌های تطبیقی توسط سازمان - شکل و گستره‌ی روابط قراردادی	**n/a**	**n/a**

اصطلاحات تعریف شده در رهنمودهای ایزو 73: 2009 مورد استفاده در ISO / IEC 27005: 2011	اصطلاحات تعریف شده در استاندارد ISO / IEC 27000: 2009 مورد استفاده در ISO / IEC 27005: 2008	اصطلاحات تعریف شده در استاندارد ISO / IEC 27005: 2008
۳-۶ **سطح مخاطره** دامنه‌ی مخاطره (۳-۹) بیان شده بر حسب تلفیقی از پیامدها و احتمال آن‌ها. [ISO Guide 73: 2009]		
۳-۷ **احتمال** شانس اتفاق افتادن چیزی [ISO Guide 73: 2009] **یادآوری ۱**- در اصطلاحات مدیریت مخاطرات واژه‌ی احتمال به شانس اتفاق افتادن چیزی اطلاق می‌شود که می‌تواند به‌صورت عینی یا ذهنی، کمی یا کیفی تعریف، اندازه‌گیری یا تعیین شده و با استفاده از واژه‌های عمومی یا ریاضی(مانند احتمال یا فراوانی در دوره‌ای مفروض) تشریح می‌شود. **یادآوری ۲**- واژه‌ی انگلیسی "احتمال" در برخی زبان‌ها معادل مستقیمی ندارد و اغلب از واژه معادل آن "احتمال قوی" استفاده می‌شود. با این حال در زبان انگلیسی "احتمال قوی" اغلب محدود به یک تفسیر واژه ریاضی است. بنابراین در اصطلاحات مدیریت مخاطرات، "احتمال" با هدفی که باید تفسیر گسترده‌ای داشته باشد استفاده می شود مانند واژه "احتمال قوی" در بسیاری از زبان‌های غیر انگلیسی.	**n/a**	**n/a**

اصطلاحات تعریف شده در رهنمودهای ایزو 73: 2009 مورد استفاده در ISO / IEC 27005: 2011	اصطلاحات تعریف شده در استاندارد ISO / IEC 27000: 2009 مورد استفاده در ISO / IEC 27005: 2008	اصطلاحات تعریف شده در استاندارد ISO / IEC 27005: 2008
۳-۸ **مخاطره‌ی باقی‌مانده** مخاطره باقی‌مانده پس از مقابله با مخاطره [ISO Guide 73: 2009] **یادآوری ۱**- مخاطره‌ی باقی‌مانده می‌تواند شامل مخاطرات شناخته نشده باشد. **یادآوری ۲**- مخاطره‌ی باقی‌مانده به مخاطره‌ی حفظ شده نیز معروف است.	**مخاطره باقی مانده** مخاطره باقی مانده پس از مقابله با مخاطره [ISO / IEC 27001: 2005]	**n/a**
۳-۹ **مخاطره** اثر عدم‌قطعیت بر اهداف [ISO Guide 73: 2009] **یادآوری ۱**- اثر انحرافی است از انتظارات- مثبت و/یا منفی **یادآوری ۲**- اهداف جنبه‌های مختلفی دارند(مانند اهداف مالی، سلامت و ایمنی، امنیت اطلاعات و اهداف محیطی) و در سطوح مختلف(مانند راهبرد، وسعت سازمان، پروژه، محصول و فرایند) قابل اعمال است. **یادآوری۳**- اغلب با ارجاع به رویدادهای بالقوه و پیامدها یا تلفیقی از این دو، مشخصات مخاطره را تعیین می‌کنند. **یادآوری ۴**- مخاطره‌ی امنیت اطلاعات را اغلب بر حسب تلفیقی از پیامدهای رویداد امنیت اطلاعات و احتمال رخداد مربوطه بیان می‌شود. **یادآوری ۵**- عدم قطعیت به معنای حالت، نارسایی اطلاعات مرتبط با درک یا دانش رویداد، پیامد یا احتمال آن. **یادآوری ۶**- مخاطره امنیت اطلاعات با قابلیت تهدید فرضی در بهره‌جویی از آسیب‌پذیری‌های دارایی یا گروهی از دارایی‌ها و در نتیجه لطمه زدن به سازمان مرتبط است.	**مخاطره** تلفیقی از احتمال رویداد و پیامدهای آن [ISO / IEC 27002: 2005]	

اصطلاحات تعریف شده در رهنمودهای ایزو 73: 2009 مورد استفاده در ISO / IEC 27005: 2011	اصطلاحات تعریف شده در استاندارد ISO / IEC 27000: 2009 مورد استفاده در ISO / IEC 27005: 2008	اصطلاحات تعریف شده در استاندارد ISO / IEC 27005: 2008
۳-۱۰ **تحلیل مخاطره** فرایند درک ماهیت مخاطره و تعیین سطح مخاطره.(3.6) [ISO Guide 73: 2009] **یادآوری ۱**- تحلیل مخاطره پایه‌ای برای ارزیابی و تصمیم‌گیری برای مقابله با مخاطره فراهم می‌کند. **یادآوری ۲**- تحلیل مخاطره شامل تخمین مخاطره.	**تحلیل مخاطره** استفاده‌ی نظام‌مند از اطلاعات برای شناسایی منابع و برآورد مخاطره [ISO / IEC 27002: 2005] **یادآوری** - تحلیل مخاطره پایه‌ای برای ارزیابی و تصمیم‌گیری برای مقابله با مخاطره فراهم می‌کند.	**n/a**
۳-۱۱ **ارزیابی مخاطره** فرآیند کلی شناسایی (۳-۱۵)، تحلیل(۳-۱۰) و ارزیابی (۳-۱۴) مخاطره [ISO Guide 73: 2009]	**ارزیابی مخاطره** فرایند کلی تحلیل و ارزیابی مخاطره [ISO / IEC 27002: 2005]	**n/a**
این اصطلاح در حال حاضر تحت پوشش رفع مخاطره می‌باشد.		**۳-۳** **اجتناب از مخاطره** تصمیم گیری به عدم درگیری در یا اقدام به صرف‌نظر کردن از شرایط مخاطره [ISO Guide 73: 2002]

اصطلاحات تعریف شده در رهنمودهای ایزو 73: 2009 مورد استفاده در ISO / IEC 27005: 2011	اصطلاحات تعریف شده در استاندارد ISO / IEC 27000: 2009 مورد استفاده در ISO / IEC 27005: 2008	اصطلاحات تعریف شده در استاندارد ISO / IEC 27005: 2008
۱۲-۳ **تبادل اطلاعات و رایزنی مخاطره** فرایندهایی مستمر و مکرر که سازمان‌ها برای فراهم‌سازی،اشتراک گذاری یا به دست آوردن اطلاعات و تعامل با ذی‌نفعان راجع به مدیریت مخاطرات انجام می‌دهند. (۳-۹) [ISO Guide 73: 2009] **یادآوری ۱**- اطلاعات می‌تواند به وجود، ماهیت، شکل، احتمال، اهمیت، ارزیابی، قابلیت پذیرش و مقابله با مخاطره ارتباط داشته باشد. **یادآوری ۲**- مشاوره فرایند دوسویه‌ی ارتباط آگاهانه بین سازمان و ذی‌نفعان آن پیش از تصمیم‌گیری راجع به موضوعی یا تعیین مسیر آن است مشاوره عبارت است از: - فرایندی که بر تصمیم‌گیری از طریق نفوذ نه اعمال قدرت اثر می‌گذارد؛ و - ورودی تصمیم‌گیری است نه تصمیم‌گیری مشترک.		**۴-۳** **تبادل مخاطره** مبادله یا اشتراک‌گذاری اطلاعات در مورد مخاطره بین تصمیم‌گیرندگان و سایر ذی‌نفعان [ISO Guide 73: 2002]
۱۳-۳ **معیارهای مخاطره** شرایط مرجع که اهمیت **مخاطره** (۳-۹) توسط آن‌ها ارزیابی می‌شود. [ISO Guide 73: 2009] **یادآوری ۱**- معیارهای مخاطره مبتنی بر اهداف سازمانی و زمینه بیرونی و درونی است. **یادآوری ۲**- معیارهای مخاطره از استانداردها، قوانین، خط‌مشی‌ها و سایر الزامات قابل استخراج است.	**n/a**	**n/a**

اصطلاحات تعریف شده در رهنمودهای ایزو 73: 2009 مورد استفاده در ISO / IEC 27005: 2011	اصطلاحات تعریف شده در استاندارد ISO / IEC 27000: 2009 مورد استفاده در ISO / IEC 27005: 2008	اصطلاحات تعریف شده در استاندارد ISO / IEC 27005: 2008
این اصطلاح حذف شده است		**۳-۵** **تخمین مخاطره** فرایند تخصیص مقدار به احتمال و پیامدهای مخاطره [ISO / IEC Guide 73: 2002]
۳-۱۴ **ارزیابی مخاطره** فرآیند مقایسه نتایج تحلیل مخاطره با معیارهای مخاطره به منظور تعیین این که مخاطره و/یا دامنه‌ی آن قابل قبول یا تحمل هست یا خیر. [ISO / IEC Guide 73: 2009] **یادآوری ۱**- ارزیابی مخاطره به تصمیم‌گیری در خصوص مقابله با مخاطره کمک می‌کند.	**ارزیابی مخاطره** فرایند مقایسه مخاطره‌ی تخمینی با معیارهای مخاطره مفروض به منظور تعیین اهمیت مخاطره [ISO / IEC 27001: 2005]	**n/a**

اصطلاحات تعریف شده در رهنمای ISOGuide 73: ۲۰۰۹ مورد استفاده در ISO / IEC 27005: 2011	اصطلاحات تعریف شده در استاندارد ISO / IEC 27000: 2009 مورد استفاده در ISO / IEC 27005: 2008	اصطلاحات تعریف شده در استاندارد ISO / IEC 27005: 2008
۳-۱۵ **شناسایی مخاطره** فرایند یافت، تشخیص و تشریح مخاطرات [ISO / IEC Guide 73: 2009] **یادآوری ۱**- شناسایی مخاطره شامل شناسایی منابع مخاطره، رویدادها، علل و پیامدهای بالقوه آن‌ها می‌باشد. **یادآوری ۲**- شناسایی مخاطره می‌تواند شامل داده‌های تاریخی، تحلیل نظری، نظرات کارشناسی و اطلاعاتی و نیازهای ذی‌نفعان شود.		۳-۶ شناسایی مخاطره فرایند یافت، فهرست و تعیین کردن مشخصات عناصر مخاطره [ISO / IEC Guide 73: 2002] **یادآوری**- در این استاندارد ملی برای شناسایی مخاطره، «فعالیت» به جای «فرایند» به کار می‌رود.
۳-۱۶ **مدیریت مخاطره** فعالیت‌های هماهنگ جهت هدایت و کنترل سازمان نسبت به مخاطره [ISO Guide 73: 2009] **یادآوری**- در این استاندارد ملی به طور کلی واژه‌ی« فرایند» برای مدیریت مخاطرات به کار می‌رود. مولفه‌های موجود در فرایند مدیریت مخاطره را «فعالیت» می‌نامند.	**مدیریت مخاطره** فعالیت‌های هماهنگ جهت هدایت و کنترل سازمان نسبت به مخاطره [IEC 27001: 2005 / ISO]	**n/a**

اصطلاحات تعریف شده در رهنمای ۲۰۰۹: ISOGuide 73 مورد استفاده در ISO / IEC 27005: 2011	اصطلاحات تعریف شده در استاندارد ISO / IEC 27000: 2009 مورد استفاده در ISO / IEC 27005: 2008	اصطلاحات تعریف شده در استاندارد ISO / IEC 27005: 2008
این اصطلاح با «اصلاح مخاطره» جایگزین شده و در حال حاضر به‌وسیله مقابله با مخاطره پوشش داده شده است.		**۳-۷** **کاهش مخاطره** اقدامات صورت گرفته برای کاهش احتمال، پیامدهای منفی، و یا هر دو، مرتبط با مخاطره [ISO Guide 73: 2009]
این اصطلاح در حال حاضر به‌وسیله مقابله با مخاطره پوشش داده شده است.		**۳-۸** **حفظ مخاطره** پذیرش بار مسئولیت از دست دادن و یا بهره مندی از سود یک مخاطره خاص [ISO/IEC Guide 73: 2002]
این اصطلاح با « اشتراک‌گذاری مخاطره» جایگزین شده و در حال حاضر به‌وسیله مقابله با مخاطره پوشش داده شده است.		**۳-۹** **انتقال مخاطره** به اشتراک گذاری بار مسئولیت با طرف دیگر از دست دادن و یا بهره‌مندی از سود یک مخاطره [ISO/IEC Guide 73: 2002] **یادآوری**- در زمینه مخاطرات امنیت اطلاعات فقط پیامدهای منفی (از دست دادن) برای انتقال مخاطره مورد نظر است.

اصطلاحات تعریف شده در رهنمای ISOGuide 73 :۲۰۰۹ مورد استفاده در ISO / IEC 27005: 2011	اصطلاحات تعریف شده در استاندارد ISO / IEC 27000: 2009 مورد استفاده در ISO / IEC 27005: 2008	اصطلاحات تعریف شده در استاندارد ISO / IEC 27005: 2008
۳-۱۷ **مقابله با مخاطره** فرایند اصلاح مخاطره [ISO/IEC Guide 73: 2009] **یادآوری۱**- مقابله با مخاطره می‌تواند شامل موارد زیر باشد: - پرهیز از مخاطره با تصمیم‌گیری بر عدم شروع یا ادامه فعالیتی که مخاطره‌افزا است. - تن دادن یا افزودن مخاطره به منظور استفاده از فرصت - حذف منبع مخاطره - تغییر دادن احتمال - تغییر دادن پیامدها - اشتراک گذاری مخاطره با طرف یا طرف‌های دیگر(شامل قراردادها و سرمایه گذاری مخاطرات) و - حفظ مخاطره از طریق انتخاب آگاهانه **یادآوری ۲**- مقابله با مخاطره که با پیامدهای منفی سرو کار دارد را گاهی «تخفیف مخاطره»، «حذف مخاطره»، «جلوگیری از مخاطره» و «کاهش مخاطره» می‌نامند. **یادآوری ۳**- مقابله با مخاطره می‌تواند مخاطرات جدیدی پدید آورد یا مخاطرات موجود را اصلاح نماید.	**مقابله با مخاطره** فرایند انتخاب و پیاده سازی از اندازه‌گیری‌ها برای اصلاح مخاطره [ISO / IEC 27001: 2001] **یادآوری**- در این استاندارد ملی اصطلاح «کنترل» معادل با « اندازه-گیری» استفاده می‌شود.	**n/a**

اصطلاحات تعریف شده در رهنمای ISOGuide 73: ۲۰۰۹ مورد استفاده در ISO / IEC 27005: 2011	اصطلاحات تعریف شده در استاندارد ISO / IEC 27000: 2009 مورد استفاده در ISO / IEC 27005: 2008	اصطلاحات تعریف شده در استاندارد ISO / IEC 27005: 2008
۳-۱۸ **ذی‌نفعان** شخص یا سازمانی که می‌تواند بر تصمیم‌ها یا فعالیت‌ها اثر بگذارد یا از آن‌ها تاثیر بپذیرد یا چنین برداشتی داشته باشد. [ISO/IEC Guide 73: 2009]	**n/a**	**n/a**
تعریف کنونی از ISO / IEC 27000: 2009 اعمال شده است.	**تهدید** عامل بالقوه‌ی رخداد ناخواسته که ممکن است به لطمه دیدن سازمان یا سامانه منجر شود [ISO / IEC 27002: 2005]	

کتاب‌نامه

[1] ISO/IEC Guide 73:2009, Risk management — Vocabulary
[2] ISO/IEC 16085:2006, Systems and software engineering — Life cycle processes — Risk management

[۳]استاندارد ملی ۲۷۰۰۲: سال ۱۳۸۷- فناوری اطلاعات- فنون امنیت – آیین‌کار مدیریت امنیت اطلاعات

[4] ISO 31000:2009, *Risk management — Principles and guidelines*
[5] NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*
[6] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology*