ISMS

سیستم مدیریت امنیت اطلاعات

Information Security Management System

گردآوری و تدوین :

مهندس حسین ملکی

کارشناس فناوری اطلاعات

ISMS

استانداردهای

سیستم مدیریت امنیت اطلاعات

((حوزه IT))

گردآوری و تدوین :

مهندس حسین ملکی

کارشناس فناوری اطلاعات

مقدمه گردآورنده

در حال حاضر وضعیت امنیت فضای تبادل اطلاعات کشور،به ویژه در حوزه دستگاهای دولتی،درسطح نامطلوبی قرار دارد. از جمله دلایل اصلی وضعیت موجود، می توان به فقدان زیر ساخت های فنی و اجرائی امنیت و عدم انجام اقدامات موثر در خصوص ایمن سازی فضای تبادل اطلاعات دستگاه های دولتی اشاره نمود. بخش قابل توجهی از وضعیت نامطلوب امنیت فضای تبادل اطلاعات کشور،بواسطه فقدان زیر ساخت هائی از قبیل نظام ارزیابی امنیتی فضای تبادل اطلاعات، نظام صدور گواهی و زیرساختار کلید عمومی ، نظام تحلیل و مدیریت مخاطرات امنیتی، نظام پیشگیری و مقابله با حوادث فضای تبادل اطلاعات،نظام مقابله با جرائم فضای تبادل اطلاعات و سایر زیر ساخت های امنیت اطلاعات در کشور می باشد. از سوی دیگر، وجود زیر ساخت های فوق، قطعاً تاثیر بسزائی در ایمن سازی فضای تبادل اطلاعات دستگاه های دولتی خواهد داشت . صرف نظر از دلایل فوق، نابسامانی موجود در وضعیت امنیت فضای تبادل اطلاعات دستگاه های دولتی ، از یک سو موجب بروز اخلال در عملکرد صحیح دستگاه ها شده و کاهش اعتبار این دستگاه ها را در پی خواهد داشت. و از سوی دیگر،موجب اتلاف سرمایه های ملی خواهد شد. لذا همزمان با تدوین سند راهبردی امنیت فضای تبادل اطلاعات کشور، توجه به مقوله ایمن سازی فضای تبادل اطلاعات دستگاه های دولتی،ضروری به نظر می رسد. این امر علاوه بر کاهش صدمات و زیانهای ناشی از وضعیت فعلی امنیت دستگاه های دولتی،نقش موثری در فرآیند تدوین سند راهبردی امنیت فضای تبادل اطلاعات کشور خواهد داشت.سیستم مدیریت امنیت اطلاعات (ISMS)با ارائه اولین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵ نگرش سیستماتیک به مقوله ایمن سازی فضای تبادل اطلاعات شکل گرفت. بر اساس این نگرش، تامین امنیت فضای تبادل اطلاعات سازمانها، دفعتاً مقدور نمی باشد و لازم است این امر بصورت مداوم در یک چرخه ایمن سازی شامل مراحل طراحی، پیاده سازی، ارزیابی و اصلاح انجام گیرد.

ایجاد و توسعه سیستم مدیریت امنیت اطلاعات در کنار توسعه و گسترش کاربرد فناوری اطلاعات در شرکت ها ، وزارتخانه های مختلف ، سازمانها و موسسات و نهادهای انقلابی موجب خواهد شد کشور با آمادگی بیشتری وارد جامعه اطلاعات شود ، رویکردی نظام مند در این حوزه نیز ضرورت استفاده از استانداردها را مورد تاکید قرار می دهد.

استانداردهای سامانه مدیریت امنیت اطلاعات که بدین منظور در این مجموعه انتخاب شده است تحت عنوان :

۱. **استاندار ملی ایران به شماره ISO/IEC 2700- مروری کلی واژگان.**
۲. **استاندار ملی ایران به شماره ISO/IEC 27001 – الزامات.**
۳. **استاندارد ملی ایران به شماره ISO/IEC 27002- آئین نامه کار.**
۴. **استاندار ملی ایران به شماره ISO/IEC 27003– راهنمایی پیاده سازی سامانه.**
۵. **استاندارد ملی ایران به شماره ISO/IEC 27004- سنجش.**
۶. **استاندارد ملی ایران به شماره ISO/IEC 27005 – مدیریت مخاطرات.**
۷. **استاندارد ملی ایران به شماره ISO/IEC 27006 – الزامات نهادهای ارایه دهنده خدمات ممیزی و صدور گواهی.**
۸. **استاندارد ملی ایران به شماره ISO/IEC 2007 – راهنمایی ممیزی سامانه ها.**

می باشند.

حسین ملکی

کارشناس فناوری اطلاعات

تابستان ۹۲

عنوان	فهرست مطالب	صفحه

فصل اول :

سامانه های مدیریت امنیت اطلاعات- مرورکلی و واژگان(ISO/IEC-۲۷۰۰۰)

فصل دوم :

سیستم های مدیریت امنیت اطلاعات – الزامات(ISO/IEC-۲۷۰۰۱)

فصل سوم:

آئین کار مدیریت امنیت اطلاعات (ISO/IEC-۲۷۰۰۲)

فصل چهارم :

راهنمای اجرای سامانه مدیریت امنیت اطلاعات (ISO/IEC-۲۷۰۰۳)

فصل پنجم :

مدیریت امنیت اطلاعات – سنجش ((۲۷۰۰۴)-۱۴۰۹۶-ISO/IEC)

فصل ششم :

مدیریت مخاطرات امنیت اطلاعات (ISO/IEC-۲۷۰۰۵)

فصل هفتم :

الزامات نهادهای ممیزی کننده و گواهی کننده مدیریت امنیت اطلاعات (ISO/IEC-۲۷۰۰۶)

فصل هشتم :

راهنماهایی برای ممیزی سامانه های مدیریت امنیت اطلاعات (ISO/IEC-۲۷۰۰۷)

فصل اول

فناوری اطلاعات - فنون امنیتی- سامانه های مدیریت امنیت اطلاعات- مرور کلی و واژگان

ISO/IEC 27000

Information technology-- Security techniques
Information security management systems
Overview and vocabulary

پیش‌گفتار

استاندارد " فناوری اطلاعات- فنون امنیتی-سامانه‌های مدیریت امنیت اطلاعات- مرور کلی و واژگان" که پیش نویس آن درکمیسیون‌های مربوط توسط سازمان فناوری اطلاعات تهیه و تدوین شده و در اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده مورخ... مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت .بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

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

ISO/IEC 27000:2009, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary

۰ مقدمه

۰-۱ مرور کلی

استانداردهای ملی سامانه‌های مدیریت، به منظور فراهم آوردن مدلی برای برپایی و بهره‌برداری[1] از سامانه مدیریت تهیه شده است. این مدل دربردارنده‌ی مشخصه‌هایی است که متخصصان این حوزه در مورد آن‌ها به عنوان فناوری بین‌المللی روز به اجماع رسیده‌اند. کمیته فرعی ISO/IEC JTC 1 SC 27[2]، شامل گروهی تخصصی است که به تدوین استانداردهای سامانه‌های مدیریت بین‌المللی امنیت اطلاعات می‌پردازد. این استانداردها به‌عنوان استانداردهای خانواده سامانه مدیریت امنیت اطلاعات (ISMS)[3] شناخته می‌شوند.

سازمان‌ها می‌توانند با استفاده از استانداردهای خانواده ISMS، چارچوبی را برای مدیریت امنیت دارایی‌های اطلاعاتی خود تدوین و پیاده‌سازی کنند و برای ارزیابی[4] مستقل سامانه مدیریت امنیت اطلاعات خود، به منظور حفاظت از اطلاعاتی مانند اطلاعات مالی[5]، مالکیت معنوی[6] ، ریز اطلاعات کارکنان[7] یا اطلاعات سپرده شده به آن‌ها توسط مشتریان یا طرف سوم[8] آماده باشند.

۰-۲ استانداردهای خانواده ISMS

استانداردهای خانواده ISMS برای کمک به سازمان‌ها از هر نوع و اندازه، به منظور پیاده‌سازی و بهره‌برداری از ISMS در نظر گرفته شده است. استانداردهای خانواده ISMS شامل استانداردهای بین‌المللی زیر، با عنوان عمومی فناوری اطلاعات- فنون امنیتی است:

- ISO/IEC 27000:2009، سامانه‌های مدیریت امنیت اطلاعات- مرور کلی و واژگان
- استاندارد ملی ایران به شماره ۲۷۰۰۱، سامانه‌های مدیریت امنیت اطلاعات- الزامات
- استاندارد ملی ایران به شماره ۲۷۰۰۲، آیین کار مدیریت امنیت اطلاعات
- استاندارد ملی ایران به شماره ۲۷۰۰۳، راهنمای پیاده‌سازی سامانه مدیریت امنیت اطلاعات
- ISO/IEC 27004، مدیریت امنیت اطلاعات- سنجش
- ISO/IEC 27005:2008، مدیریت مخاطرات امنیت اطلاعات

---

1 - Operating
2 - International Organization for Standardization/ International Electro-technical Commission Joint Technical Committee
3 - Information Security Management Systems
4 - Assessment
5 - Financial Information
6 - Intellectual Property
7 - Employee Details
8 - Third Parties

- استاندارد ملی ایران به شماره ۲۷۰۰۶، الزامات نهادهای ارائه‌دهنده خدمات ممیزی و صدور گواهی سامانه‌های مدیریت امنیت اطلاعات
- ISO/IEC 27007، راهنمای ممیزی سامانه‌های مدیریت امنیت اطلاعات
- استاندارد ملی ایران به شماره ۲۷۰۱۱، راهنمای مدیریت امنیت اطلاعات برای سازمان‌های مخابراتی مبتنی بر ISO/IEC 27002

یادآوری- عنوان عمومی «فناوری اطلاعات- فنون امنیتی» نشان می‌دهد این استانداردها توسط کمیته فرعی ۲۷ با نام فنون امنیتی فناوری اطلاعات از کمیته فنی مشترک شماره یک[1] موسوم به فناوری اطلاعات، تدوین شده است.

استانداردهای بین‌المللی که تحت همین عنوان عمومی نیستند و در عین حال قسمتی از استانداردهای خانواده ISMS محسوب می‌شوند، عبارتند از:

- استاندارد ملی ایران به شماره ۱۳۲۲۰[2] انفورماتیک سلامت[3]، مدیریت امنیت اطلاعات در بهداشت با استفاده از ISO/IEC 27002

۰-۳ هدف از این استاندارد ملی

این استاندارد ملی، مرور کلی بر سامانه‌های مدیریت امنیت اطلاعات که موضوع استانداردهای خانواده ISMS را شکل می‌دهند، ارائه و اصطلاحات مرتبط را تعریف می‌کند.

یادآوری- در پیوست الف، چگونگی توصیف الزامات و/یا راهنما استانداردهای خانواده ISMS مشخص شده است.

استانداردهای خانواده ISMS شامل استانداردهایی است که:

الف) الزاماتی برای ISMS و صادرکنندگان گواهی چنین سامانه‌هایی تعریف می‌کند؛

ب) پشتیبانی مستقیم، راهنمای تفصیلی و/ یا تفسیر کلی فرآیندها و الزامات طرح- اجرا- بررسی- اقدام[4] (PDCA) را فراهم می‌کنند؛

پ) راهنمایی برای ISMS در هر بخش خاص را نشان می‌دهد؛ و

ت) به ارزیابی انطباق[5] ISMS می‌پردازد.

در خصوص اصطلاحات و تعاریف ارائه شده در این استاندارد ملی نکات زیر قابل ذکر است:

اصطلاحات و تعاریف متداول در خانواده استانداردهای ISMS را در برمی‌گیرد.

تمام اصطلاحات و تعاریف به‌کارگرفته شده در استانداردهای خانواده ISMS را در بر نمی‌گیرد.

---

1 - ISO/IEC JTC 1
2 - ISO 27799:2008
3 - Health Informatics
4 - Plan-Do-Check-Act
5 - Conformity Assessment

استانداردهای خانواده ISMS را در تعریف اصطلاحات مورد استفاده خود، محدود نمی‌کند.

استانداردهایی که فقط به پیاده‌سازی کنترل‌های استاندارد ملی ایران به شماره ۲۷۰۰۲ می‌پردازند و نه به تمام کنترل‌ها، از استانداردهای خانواده ISMS مستثنی شده‌اند.

استانداردهایی که فقط به پیاده‌سازی کنترل‌ها اشاره می‌کنند، همانند همه کنترل‌های مورد اشاره در استاندارد ملی ایران به شماره ۲۷۰۰۲، از استانداردهای خانواده ISMS مستثنی شده‌اند. به منظور بازتاب تغییر وضعیت استانداردهای خانواده ISMS، انتظار می‌رود این استاندارد ملی به طور مداوم و با تواتر بیشتر نسبت به سایر استانداردها به روز شود.

فناوری اطلاعات- فنون امنیتی- سامانه‌های مدیریت امنیت اطلاعات- مرور کلی و واژگان

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی، تعیین موارد زیر است:

الف) مرور کلی استانداردهای خانواده ISMS؛

ب) مقدمه‌ای بر سامانه‌های مدیریت امنیت اطلاعات؛

پ) توصیف مختصر فرآیند طرح- اجرا- بررسی- اقدام (PDCA)؛

ت) اصطلاحات و تعاریف مورد استفاده در استانداردهای خانواده ISMS؛

این استاندارد ملی در تمامی انواع سازمان‌ها کاربردپذیر است (مانند بنگاه‌های تجاری، دستگاه‌های دولتی، سازمان‌های غیرانتفاعی).

مراجع الزامی[۱]

۲ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌رود:

یادآوری- اصطلاحی که در تعریف یا یادآوری دیگری از این بند تعریف شده باشد به صورت برجسته به همراه شماره آن در داخل پرانتز نشان داده می شود. این اصطلاح برجسته می تواند در تعریف توسط توضیح کامل آن جایگزین گردد. برای مثال:

حمله (۲-۴) به عنوان « تلاشی جهت تخریب[۲] در معرض خطر قرار دادن[۳]، هشداردهی[۴]، ناتوان سازی[۵]، سرقت[۶] یا دسترسی غیر مجاز[۷] یا استفاده غیر مجاز یک **دارایی**[۸] (۲-۳) تعریف می‌شود»؛

دارایی (۲-۴) به عنوان « هر آنچه که برای سازمان دارای ارزش باشد تعریف می شود».

اگر اصطلاح «**دارایی**» با تعریف آن جایگزین شود:

۱- در این استاندارد ملی مراجع الزامی معرفی نشده است.

2 - Destroy
3 - Expose
4 - Alter
5 - Disable
6 - Steal
7 - Unauthorized Access
8 - Asset

آنگاه **حمله** عبارتست از: «تلاشی جهت تخریب، در معرض خطر قرار دادن، هشداردهی، ناتوان سازی، سرقت یا دسترسی غیر مجاز یا استفاده غیر مجاز هر آنچه که برای سازمان دارای ارزش باشد.

۱-۲

کنترل دسترسی

حصول اطمینان از دسترسی به **دارایی‌ها** (۲-۳) به صورت مجاز و محدود بر اساس الزامات امنیتی و الزامات کسب و کار[1]

۲-۲

پاسخ‌گویی[2]

مسؤولیت هر موجودیت[3] در قبال اقدامات و تصمیماتش

۳-۲

دارایی

هر آنچه که برای سازمان دارای ارزش باشد.

یادآوری- انواع مختلفی از دارایی‌ها وجود دارند، از جمله:

الف) **اطلاعات** (۲-۱۸)؛

ب) نرم افزار، مانند برنامه‌ی رایانه‌ای؛

پ) دارایی فیزیکی، مانند رایانه؛

ت) خدمات؛

ث) افراد، صلاحیت‌ها، مهارت‌ها و تجارب آن‌ها؛

ج) دارایی‌های نامشهود[4]، مانند وجهه[5] و شهرت.

۴-۲

حمله

تلاش جهت تخریب، افشا، دستکاری، از کار انداختن، سرقت یا دسترسی غیرمجاز یا استفاده غیرمجاز از یک **دارایی** (۲-۳)

---

1 - Business
2 - Accountability

۳ - فرهنگستان زبان و ادب فارسی واژه هستار را برای کلمه Entity پیشنهاد می نماید.

4 - Intangibles
5 - Image

۵-۲

احراز هویت[1]

تضمین صحت مشخصه ادعایی یک موجودیت

۶-۲

اصالت[2]

ویژگی که نشان می‌دهد یک موجودیت همان است که ادعا می‌کند.

۷-۲

دسترس پذیری[3]

ویژگی در دسترس و قابل استفاده بودن، به محض تقاضای یک موجودیت مجاز

۸-۲

تداوم کسب و کار[4]

فرآیندها[5] (۲-۳۱) و/ یا **روش‌های اجرایی**[6] (۲-۳۰) برای حصول اطمینان از تداوم عملیات کسب و کار

۹-۲

محرمانگی[7]

ویژگی در دسترس یا آشکار نبودن اطلاعات برای افراد، موجودیت‌ها یا **فرآیندهای** (۲-۳۱) غیرمجاز

۱۰-۲

کنترل[8]

ابزارهای مدیریت **مخاطره**[9] (۲-۳۴) شامل **خط مشی‌ها**[10] (۲-۲۸)، **روال‌ها** (۲-۳۰)، **راهنماها**[1] (۲-۱۶)، ۱۶)، اقدامات یا ساختارهای سازمانی است که می‌تواند ماهیت اداری، فنی، مدیریتی یا حقوقی داشته باشد.

---

1 - Authentication
2 - Authenticity
3 - Availability
4 - Business continuity
5 - Process
6 - Procedures
7 - Confidentiality
8 - Control
9 - Risk
10 - Policies

یادآوری- کنترل به عنوان مترادفی برای محافظت[2] یا اقدام متقابل[3] نیز استفاده می‌شود.

۲-۱۱

هدف کنترلی[4]

بیانیه‌ای که نتیجه‌ی پیاده‌سازی **کنترل‌ها** (۲-۱۰) را توصیف می‌کند.

۲-۱۲

اقدام اصلاحی[5]

اقدامی که برای از بین بردن علت یک عدم انطباق یا سایر شرایط نا مطلوب تشخیص داده شده انجام می‌گیرد.

[استاندارد ملی ایران به شماره ۹۰۰۰]

۲-۱۳

اثربخشی[6]

میزانی که فعالیت‌های برنامه ریزی شده تحقق یافته و نتایج برنامه ریزی شده به دست آمده است.

[استاندارد ملی ایران به شماره ۹۰۰۰]

۲-۱۴

کارآیی

رابطه بین نتایج حاصل و میزان مطلوبیت استفاده از منابع

۲-۱۵

رویداد[7]

وقوع مجموعه‌ای ویژه از شرایط

[ISO/IEC Guide 73:2002]

---

1 - Guidelines
2 - Safeguard
3 - Countermeasure
4 - Control Objective
5 - Corrective Action
6 - Effectiveness
7 - Event

۱۶-۲

راهنما[1]

توصیه‌ای درباره‌ی آن چه انتظار می رود، که بتوان با انجام آن به هدفی دست یافت.

۱۷-۲

اثر[2]

تغییر نامطلوب در سطح تحقق اهداف کسب و کار

۱۸-۲

دارایی اطلاعاتی[3]

دانش یا داده‌ای که برای سازمان با ارزش است.

۱۹-۲

امنیت اطلاعات[4]

حفظ محرمانگی (۲-۹)، یکپارچگی[5] (۲-۲۵) و دسترس‌پذیری اطلاعات (۲-۷)

یادآوری- علاوه بر این، سایر ویژگی‌ها، همچون **صحت** (۲-۶)، **پاسخگویی** (۲-۲)، **انکار ناپذیری**[6] (۲-۲۷)، و **قابلیت اطمینان** (۲-۳۳) را نیز می‌تواند دربرگیرد.

۲۰-۲

رویداد امنیت اطلاعات

وقوع یک حالت شناسایی شده از سامانه، خدمت یا شبکه که نشان‌گر یک نقض احتمالی از **امنیت اطلاعات** (۲-۱۹) **خط مشی** (۲-۲۸) یا شکست در **کنترل‌ها** (۲-۱۰)، یا موقعیت ناشناخته قبلی که می‌تواند مرتبط با امنیت باشد.

1 - Guideline
2 - Impact
3 - Information Asset
4 - Information Security
5 - Integrity
6 - Non-repudiation

۲-۲۱

رخداد[1] امنیت اطلاعات

یک یا مجموعه‌ای از **رویدادهای امنیت اطلاعات** (۲-۲۰) ناخواسته یا پیش‌بینی نشده که بـه احتمـال زیاد، عملیات کسب و کار را به خطر می‌اندازد و **امنیت اطلاعات** (۲-۱۹) را تهدید می‌کند.

۲-۲۲

مدیریت رخداد امنیت اطلاعات

فرآیندهایی (۲-۳۱) به منظور آشکارسازی[2]، گزارش‌دهی، ارزیابی، پاسخ‌دهی به، رسیدگی به و یادگیری از **رخدادهای امنیت اطلاعات** (۲-۲۱).

۲-۲۳

سامانه مدیریت امنیت اطلاعات (ISMS)

قسمتی از **سامانه مدیریت** (۲-۲۶) فراگیر که مبتنی بر رویکرد مخاطره کسب و کار بـوده و بـه منظـور برقراری، پیاده‌سازی، بهره‌برداری، پایش، بازبینی، نگهداری و بهبود **امنیت اطلاعات** (۲-۱۹) است.

۲-۲۴

مخاطره امنیت اطلاعات

توانایی بالقوه یک **تهدید** (۲-۴۵)، در بهره‌جویی از **آسیب‌پذیری** (۲-۴۶) یک یا گروهـی از **دارایی‌هـا** (۲-۳) و در نتیجه آسیب زدن به سازمان.

۲-۲۵

یکپارچگی

ویژگی حفاظت از صحت و تمامیت **دارایی‌ها** (۲-۳)

۲-۲۶

سامانه مدیریت

چارچوب **خط‌مشی‌ها** (۲-۲۸)، **روال‌ها** (۲-۳۰)، **راهنماها** (۲-۱۶) و منابع مرتبط به منظور دستیابی به اهداف سازمان

1 - Incident
2 - Detection

۲-۲۷

انکار ناپذیری

توانایی اثبات ادعای وقوع **رویداد** (۲-۱۵) یا اقدام و موجودیت‌های آغازکننده‌ی آن، به منظور حل اختلاف درمورد وقوع یا عدم وقوع **رویداد** (۲-۱۵) یا اقدام و دخالت موجودیت‌ها در **رویداد** (۲-۱۵)

۲-۲۸

خط مشی

نیت و جهت‌گیری کلی که به طور رسمی به وسیله مدیریت تصریح می‌شود.

۲-۲۹

اقدام پیشگیرانه[1]

اقدامی برای از بین بردن علت یک عدم انطباق بالقوه یا سایر شرایط نامطلوب بالقوه انجام می‌گیرد.

[استاندارد ملی ایران به شماره ۹۰۰۰]

۲-۳۰

روش اجرایی[2]

طریقه ی مشخص شده ای برای اجرای[3] یک فعالیت یا یک **فرایند** (۲-۳۱)

[استاندارد ملی ایران به شماره ۹۰۰۰]

۲-۳۱

فرآیند

مجموعه فعالیت‌های مرتبط با هم یا متعامل که دروندادەها را به بروندادەها تبدیل می‌کند.

[استاندارد ملی ایران به شماره ۹۰۰۰]

۲-۳۲

سابقه[4]

مدرکی که در آن نتایج بدست آمده ذکر می شود یا شواهدی را دال بر انجام فعالیت‌ها فراهم می‌آورد.

[استاندارد ملی ایران به شماره ۹۰۰۰]

---

1 - Preventive Action
2 - Procedure
3 - Carry out
4 - Record

۳۳-۲

قابلیت اطمینان[1]

ویژگی سازگاری با رفتار و نتایج مورد نظر

۳۴-۲

مخاطره

ترکیبی از احتمال وقوع یک **رویداد** (۲-۱۵) و پیامد آن

[ISO/IEC Guide 73:2002]

۳۵-۲

پذیرش مخاطره

تصمیم‌گیری در مورد پذیرش یک **مخاطره** (۲-۳۴)

[ISO/IEC Guide 73:2002]

۳۶-۲

تحلیل مخاطره

استفاده‌ی نظام‌مند از اطلاعات به منظور شناسایی منابع و برآورد **مخاطره** (۲-۳۴)

[ISO/IEC Guide 73:2002]

یادآوری- تحلیل مخاطره پایه‌ای را برای **ارزشیابی مخاطره** (۲-۴۱)، **بر طرف سازی مخاطره**[2] (۲-۴۳) و **پذیرش مخاطره** (۲-۳۵) فراهم می‌سازد.

۳۷-۲

ارزیابی مخاطره

فرآیند (۲-۳۱) کلی تحلیل مخاطره (۲-۳۶) و ارزشیابی مخاطره (۲-۴۱)

[ISO/IEC Guide 73:2002]

۳۸-۲

اطلاع‌رسانی مخاطره[3]

تبادل یا به اشتراک‌گذاری اطلاعات درباره **مخاطره** (۲-۳۴) بین تصمیم‌گیرنده و سایر ذی‌نفعان

[ISO/IEC Guide 73:2002]

---

1 - Reliability
2 - Risk treatment
3 - Risk communication

۳۹-۲

معیارهای مخاطره

شرایط مرجع که اهمیت **مخاطره** (۲-۳۴) بر اساس آن‌ها ارزیابی می‌شود.

[ISO/IEC Guide 73:2002]

۴۰-۲

برآورد مخاطره[1]

فعالیت تخصیص دادن مقدار به احتمال وقوع و پیامدهای **مخاطره** (۲-۳۴)

[ISO/IEC Guide 73:2002]

۴۱-۲

ارزشیابی مخاطره

فرآیند (۲-۳۱) مقایسه **مخاطره** (۲-۳۴) برآورد شده با **معیار مخاطره** (۲-۳۹) مفروض به منظور تعیین اهمیت **مخاطره** (۲-۳۴)

[ISO/IEC Guide 73:2002]

۴۲-۲

مدیریت مخاطره[2]

فعالیت‌های هماهنگ به منظور هدایت و کنترل سازمان با توجه به **مخاطره** (۲-۳۴)

[ISO/IEC Guide 73:2002]

یادآوری- مدیریت مخاطره به‌طور کلی شامل **ارزیابی مخاطره** (۲-۳۷)، **بر طرف سازی مخاطره** (۲-۴۳)، **پذیرش مخاطره** (۲-۳۵)، **اطلاع رسانی مخاطره** (۲-۳۸)، پایش مخاطره و بازنگری مخاطره است.

۴۳-۲

بر طرف سازی مخاطره

فرآیند (۲-۳۱) انتخاب و پیاده‌سازی اقداماتی برای تعدیل **مخاطره** (۲-۳۴)

[ISO/IEC Guide 73:2002]

1 - Risk Estimation
2 - Risk Management

۴۴-۲

بیانیه کاربست پذیری[1]

بیانیه مستندی که **اهداف کنترلی** (۲-۱۱) و **کنترل‌های** (۲-۱۰) مرتبط و کاربرد پذیر در **ISMS** (۲-۲۳) سازمان را تشریح می‌کند.

۴۵-۲

تهدید

عامل بالقوه‌ی رخدادی ناخواسته که ممکن است باعث آسیب‌رسانی به سامانه یا سازمان شود.

۴۶-۲

آسیب پذیری

ضعف یک **دارایی** (۲-۳) یا **کنترل** (۲-۱۰) که می‌تواند توسط **تهدید** (۲-۴۵)، مورد بهره‌جویی قرار گیرد.

۳ سامانه‌های مدیریت امنیت اطلاعات

۳-۱ مقدمه

سازمان‌ها از هر نوع و اندازه:

الف) مقدار زیادی اطلاعات را جمع‌آوری، پردازش، ذخیره و ارسال می‌کنند؛

ب) تشخیص می‌دهند که اطلاعات و فرآیندها، سامانه‌ها، شبکه‌ها و افراد مرتبط، دارایی‌های مهمی برای رسیدن به اهداف سازمان هستند؛

پ) با گستره‌ای از مخاطرات مواجه‌اند که ممکن است بر کارکرد دارایی‌ها اثر بگذارند؛ و

ت) با پیاده‌سازی کنترل‌های امنیت اطلاعات، مخاطرات را تعدیل می‌کنند.

تمام اطلاعات نگهداری و پردازش شده توسط سازمان، در معرض تهدیدهای حمله، خطا، عوامل طبیعی (مانند سیل یا آتش سوزی) و غیره قرار دارند و با آسیب‌پذیری‌های ذاتی در کاربرد آنها مواجه هستند. اصطلاح امنیت اطلاعات عموما مبتنی بر اطلاعاتی است که دارایی قلمداد می‌شوند و به علت ارزشی که دارند باید برای مثال در برابر از بین رفتن دسترس‌پذیری، محرمانگی و یکپارچگی، مورد حفاظت مناسب قرار گیرند. دسترسی به موقع به اطلاعات دقیق و کامل از سوی افرادی با نیاز مجاز، باعث تقویت بازدهی کسب و کار می‌شود.

1 - Statement of Applicability

حفاظت از دارایی‌های اطلاعاتی از طریق تعریف، به‌دست آوردن، نگهداری، و بهبود موثر امنیت اطلاعات، برای توانمندسازی سازمان به منظور دست یابی به اهداف و نگهداری و افزایش انطباق قانونی و وجهه‌ی آن ضروری است. این فعالیت‌های هماهنگ که پیاده‌سازی کنترل‌های مناسب را هدایت و مخاطرات امنیت اطلاعات غیر قابل قبول را بر طرف می‌کنند، عموماً اجزای مدیریت امنیت اطلاعات قلمداد می‌شوند.

نظر به اینکه مخاطرات امنیت اطلاعات و اثربخشی تغییر کنترل‌ها وابسته به تغییر وضعیت‌ها است، سازمان‌ها نیاز دارند که:

الف) اثربخشی کنترل‌ها و روال‌های پیاده‌سازی شده را پایش و ارزشیابی کنند؛

ب) مخاطرات نوظهوری را که باید بر طرف شوند، شناسایی کنند؛ و

پ) کنترل‌های مناسب مورد نیاز را برگزینند، پیاده‌سازی کنند و بهبود دهند.

به منظور مرتبط و هماهنگ نمودن این‌گونه فعالیت‌های امنیت اطلاعات، هر سازمان باید خط‌مشی و اهداف خود برای امنیت اطلاعات را تعیین نماید و با استفاده از سامانه مدیریت به طور موثری آن اهداف را بدست آورد.

۳-۲ سامانه مدیریت امنیت اطلاعات (ISMS) چیست؟

۳-۲-۱ مرور کلی و اصول

سامانه مدیریت امنیت اطلاعات (ISMS) مدلی را برای برقراری، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود حفاظت از دارایی‌های اطلاعاتی به منظور تحقق اهداف کسب و کار فراهم می‌سازد که مبتنی بر ارزیابی مخاطره و سطوح قابل قبول مخاطره سازمان برای بر طرف‌سازی و مدیریت موثر مخاطرات طراحی شده است.

تحلیل الزامات به منظور حفاظت از دارایی‌های اطلاعاتی و اعمال کنترل‌های مناسب و برای اطمینان از حفاظت لازم از این دارایی‌های اطلاعاتی، به پیاده‌سازی موفقیت‌آمیز ISMS کمک می‌کند. اصول بنیادی زیر نیز به پیاده‌سازی موفقیت‌آمیز ISMS کمک می‌کنند:

الف) آگاهی نسبت به ضرورت امنیت اطلاعات؛

ب) تخصیص مسؤولیت برای امنیت اطلاعات؛

پ) تلفیق تعهد مدیریت با منافع ذی‌نفعان؛

ت) تقویت ارزش‌های اجتماعی؛

ث) ارزیابی مخاطرات جهت اعمال کنترل‌های مناسب برای رسیدن به سطوح قابل قبول مخاطره؛

ج) امنیت لحاظ‌شده به عنوان عنصر ضروری سامانه‌ها و شبکه‌های اطلاعاتی؛

چ) پیشگیری و تشخیص فعال رخدادهای امنیت اطلاعات؛
ح) اطمینان از رویکردی جامع برای مدیریت امنیت اطلاعات؛ و
خ) ارزیابی مستمر امنیت اطلاعات و اعمال اصلاحات مناسب.

۳-۲-۲ اطلاعات

اطلاعات، دارایی است که همانند سایر دارایی‌های مهم کسب و کار برای فعالیت سازمان ضروری است و در نتیجه نیاز به حفاظت مناسب دارد. اطلاعات را می‌توان به شکل‌های بسیاری ذخیره کرد، از جمله: به شکل دیجیتالی (برای مثال داده‌های ذخیره شده در رسانه نوری یا الکترونیکی)، به شکل فیزیکی (برای مثال بر روی کاغذ) و همچنین اطلاعات نامشهود مانند دانش کارکنان. اطلاعات را می‌توان با روش‌های مختلفی برای مثال با استفاده از پیک، ارتباطات الکترونیکی یا به صورت شفاهی انتقال داد. اطلاعات، به هر شکلی که باشد، یا با هر روشی که انتقال یابد، همیشه به حفاظت مناسب نیاز دارد.

اطلاعات هر سازمان به فناوری ارتباطات و اطلاعات وابسته است. این فناوری عنصری اساسی در هر سازمان است و ایجاد، پردازش، ذخیره سازی، انتقال، حفاظت و از بین بردن اطلاعات را تسهیل می‌کند. با گسترش پیوند جهانی محیط کسب و کار حفاظت از اطلاعات ضرورت بیشتری پیدا می‌کند، زیرا اکنون اطلاعات در معرض انواع بیشتری از تهدیدها و آسیب‌ها قرار دارد.

۳-۲-۳ امنیت اطلاعات

امنیت اطلاعات دارای سه بعد اصلی است که عبارتند از محرمانگی، دسترس‌پذیری و یکپارچگی. امنیت اطلاعات با هدف اطمینان از موفقیت پایدار و تداوم کسب و کار و در جهت کمینه کردن اثرات، شامل به کارگیری و مدیریت معیارهای امنیتی مناسبی است که بازه گسترده‌ای از تهدیدات را مورد توجه قرار می‌دهد.

امنیت اطلاعات با پیاده سازی مجموعه‌ای از کنترل‌های کاربردپذیر به‌دست می‌آید که از طریق فرآیند مدیریت مخاطره انتخاب و با استفاده از ISMS مدیریت می‌شود که شامل خط مشی‌ها، فرآیندها، روال‌ها، ساختارهای سازمانی، نرم‌افزارها و سخت‌افزارها به منظور حفاظت از دارایی‌های اطلاعاتی شناسایی شده است.

به منظور اطمینان از دستیابی به اهداف معین امنیتی و کسب و کار سازمان، این کنترل‌ها باید تعیین، پیاده‌سازی، پایش، بازنگری و در صورت نیاز بهبود داده شوند. کنترل‌های مرتبط با امنیت اطلاعات باید به صورت تنگاتنگی با فرآیندهای کسب و کار سازمان یکپارچه شده باشند.

۳-۲-۴ مدیریت

مدیریت شامل فعالیت‌های هدایت، کنترل و بهبود مستمر سازمان در بستر ساختارهای مناسب می‌شود. فعالیت‌های مدیریتی شامل اقدامات، روش‌ها یا شیوه سازمان‌دهی، ساماندهی، هدایت، نظارت و کنترل منابع است. ساختارهای مدیریتی از یک فرد در سازمانی کوچک، تا سلسله مراتب مدیریتی با افرادی بسیار در سازمان‌های بزرگ، گسترش می‌یابد.

از دیدگاه ISMS، مدیریت، نظارت و تصمیم‌گیری‌های لازم برای رسیدن به اهداف کسب و کار از طریق حفاظت از دارایی‌های اطلاعاتی سازمان را در بر می‌گیرد. مدیریت امنیت اطلاعات از طریق تدوین و استفاده از خط‌مشی‌ها، استانداردها، روال‌ها و راهنماهای امنیتی اظهار می گردد که سپس توسط تمام افراد دست‌اندرکار[1] سازمان در کل سازمان اعمال می‌شود.

یادآوری- اصطلاح مدیریت گاهی به افراد اشاره دارد (برای مثال فرد یا گروهی از افراد با اختیارات و مسئولیت راهبری و کنترل سازمان). اصطلاح مدیریت در این بند به این مفهوم نیست.

۳-۲-۵ سامانه مدیریت

سامانه مدیریت برای رسیدن به اهداف سازمان چارچوبی از منابع را به کار می‌گیرد و شامل ساختار سازمانی، خط‌مشی‌ها، فعالیت‌های برنامه‌ریزی، مسؤولیت‌ها، اقدامات، روال‌ها، فرآیندها و منابع می‌شود.

سامانه مدیریت از لحاظ امنیت اطلاعات، به سازمان اجازه می‌دهد تا:

الف) نیازهای امنیتی مشتریان و سایر ذی‌نفعان را برآورده سازد.

ب) فعالیت‌ها و طرح‌های سازمان را بهبود دهد.

پ) اهداف امنیت اطلاعات سازمان را محقق سازد.

ت) با مقررات، قوانین و الزامات[2] صنفی تطبیق یابد.

ث) دارایی‌های اطلاعاتی را به صورت سازمان‌یافته‌ای مدیریت کند به طوری که بهبود مستمر و سازگاری با محیط و اهداف کنونی سازمان تسهیل شود.

۳-۳ رویکرد فرآیندی[3]

سازمان‌ها باید فعالیت‌های بسیاری را تعیین و مدیریت کنند تا کارکرد موثر و کارآمدی داشته باشند. هر فعالیتی که از منابع استفاده می‌کند، باید مدیریت شود تا تبدیل ورودی‌ها به خروجی‌ها را با به کارگیری مجموعه‌ای از فعالیتهای مرتبط و متعامل، که یک فرآیند نیز نامیده می‌شود، ممکن سازد. خروجی یک فرآیند می‌تواند به طور مستقیم ورودی فرآیند دیگری باشد و عموماً این تبدیل و در شرایط کنترل‌شده و

1 - Individual associated
2 - Mandates
3 - Process Approach

برنامه‌ریزی شده صورت می‌گیرد. به کارگیری سامانه‌ای از فرآیندها در یک سازمان، همراه با شناسایی و تعامل این فرآیندها و مدیریت آن‌ها را می‌توان «رویکرد فرآیندی» نامید.

رویکرد فرآیندی ISMS که در استانداردهای خانواده ISMS ارائه شده بر اساس اصول بهره‌برداری پذیرفته شده در استانداردهای سامانه مدیریتی ایزو معروف به فرایند طرح- اجرا- بررسی- اقدام (PDCA) پایه‌ریزی شده است.

الف) **طرح**- تعیین اهداف و طرح‌ریزی (تحلیل موقعیت سازمان، تعیین اهداف کلی و تنظیم اهداف توسعه طرح‌ها برای رسیدن به آن‌ها)؛

ب) **اجرا**- پیاده‌سازی طرح‌ها (عمل به آنچه برای اجرا برنامه‌ریزی شده است)؛

پ) **بررسی**- سنجش نتایج (سنجش/پایش میزان انطباق دست‌آوردها با اهداف برنامه‌ریزی شده)؛

ت) **اقدام**- اصلاح و بهبود فعالیت‌ها (آموختن از اشتباهات به منظور بهبود فعالیت‌ها برای رسیدن به نتایج بهتر).

۳-۴ چرا ISMS مهم است؟

مخاطرات مرتبط با دارایی‌های اطلاعاتی سازمان باید به عنوان قسمتی از ISMS سازمان، نشان داده شوند. رسیدن به امنیت اطلاعات به مدیریت مخاطره نیاز دارد و شامل مخاطرات ناشی از تهدیدهای فیزیکی، انسانی و فناوری مرتبط با تمام اشکال اطلاعات درون سازمانی و مورد استفاده سازمان می‌شوند. انتظار می‌رود پذیرش ISMS، تصمیمی راهبردی برای سازمان باشد و لازم است این تصمیم بر طبق نیازهای سازمان، کاملا یکپارچه، متناسب[1] و به روز شود.

طراحی و پیاده‌سازی ISMS سازمان، تحت تاثیر نیازها و اهداف سازمان، الزامات امنیتی، فرآیندهای کسب و کار به‌کار گرفته شده و اندازه و ساختار سازمان قرار دارد. لازم است در طراحی و بهره‌برداری از ISMS، منافع و الزامات امنیت اطلاعات همه ذی‌نفعان سازمان شامل مشتریان، تأمین‌کنندگان، شرکای تجاری، سهامداران و طرف‌های سوم منعکس شود.

در دنیای به هم پیوسته، اطلاعات و فرآیندها، سامانه‌ها و شبکه‌های مرتبط، دارایی‌های حیاتی کسب و کار را تشکیل می دهند. سازمان‌ها و سامانه‌ها و شبکه‌های اطلاعاتی آنها، با تهدیدهای امنیتی از سوی گستره‌ی وسیعی از منابع شامل تقلب رایانه‌ای[2]، جاسوسی[3]، خرابکاری[4]، تخریب[5]، آتش‌سوزی و سیل

1 - Scaled
2 - Computer assited fraud
3 - Espionage
4 - Sabotage
5 - Vandalism

روبرو می‌شوند. آسیب زدن به سامانه‌ها و شبکه‌ها اطلاعاتی به علت کدهای مخرب، رخنه‌گری رایانه‌ای و حملات انکار سرویس[1]، بیش از پیش فراگیر، جاه طلبانه‌تر و به طور فزآینده‌ای پیچیده شده است.

سامانه مدیریت امنیت اطلاعات برای کسب و کارهای هر دو بخش عمومی و خصوصی مهم است. در هر صنعتی، ISMS یک عامل توانمندساز[2] است که از کسب و کار الکترونیکی پشتیبانی می‌کند و برای فعالیت‌های مدیریت مخاطره ضروری است. اتصال متقابل شبکه‌های عمومی و خصوصی و به اشتراک‌گذاری دارایی‌های اطلاعاتی، دشواری کنترل دسترسی و ساماندهی اطلاعات را افزایش می‌دهد. به علاوه، توزیع افزاره‌های ذخیره‌سازی سیار که حاوی دارایی‌های اطلاعاتی است، می‌تواند اثر بخشی کنترل‌های مرسوم را تضعیف کند. پذیرش استانداردهای خانواده ISMS می‌تواند نشان‌دهنده‌ی توانایی سازمان در به کارگیری اصول امنیت اطلاعات قابل درک متقابل و پایدار، در برابر شرکای تجاری و سایر طرف‌های ذی‌نفع باشد.

در بسیاری موارد امنیت اطلاعات در طراحی و توسعه سامانه‌های اطلاعاتی در نظر گرفته نمی‌شود. به علاوه، امنیت اطلاعات را اغلب راهکاری فنی تلقی می‌کنند. به هر حال، امنیتی که از طریق ابزارهای فنی به دست می‌آید، محدود و ممکن است بدون پشتیبانی مدیریت و روال‌های مناسب در بستر ISMS، بی-تأثیر باشد. گنجاندن امنیت در سامانه اطلاعاتی پس از پیاده‌سازی آن، کار پرزحمت و پرهزینه‌ای است. ISMS شامل شناسایی کنترل‌های موجود است و به برنامه‌ریزی دقیق و توجه به جزئیات نیاز دارد. برای مثال، کنترل‌های دسترسی که ممکن است فنی (منطقی)، فیزیکی، اداری (مدیریتی) یا ترکیبی از این‌ها باشند، ابزارهایی را فراهم می‌آورد تا از دسترسی مجاز و محدود به دارایی‌های اطلاعاتی، مبتنی بر کسب و کار و الزامات امنیتی، اطمینان حاصل شود.

به‌کارگیری موفقیت‌آمیز ISMS برای حفاظت از دارایی‌های اطلاعاتی اهمیت دارد و به سازمان امکان می‌دهد تا:

الف) به اطمینان بیشتری دست یابد که از دارایی‌های اطلاعاتی به میزان کافی و به طور پیوسته در مقابل مخاطرات امنیت اطلاعات حفاظت می‌شود؛

ب) چارچوب ساختاریافته و فراگیری را برای شناسایی و ارزیابی مخاطرات امنیت اطلاعات، انتخاب و اعمال کنترل‌های کاربردپذیر و سنجش و بهبود اثربخشی آن‌ها داشته باشد؛

پ) محیط کنترل خود را به طور مداوم بهبود دهد؛ و

ت) به طور موثر با قوانین و مقررات تنظیم‌شده منطبق شود.

---

1 - Denial of Service (DoS)

2 - Enabler

۳-۵ برقراری، پایش، نگه‌داری و بهبود ISMS

۳-۵-۱ مرور کلی

یک سازمان برای برقراری، پایش، نگهداری و بهبود ISMS خود، نیازمند تعهد به انجام مراحل زیر است:

الف) شناسایی دارایی‌های اطلاعاتی و الزامات امنیتی مربوط به آن‌ها (طبق بند ۳-۵-۲)؛

ب) ارزیابی مخاطرات امنیت اطلاعات (طبق بند ۳-۵-۳)؛

پ) انتخاب و پیاده سازی کنترل‌های مربوطه برای مدیریت مخاطرات غیرقابل پذیرش (طبق بند ۳-۵-۴)؛

ت) پایش، نگهداری و بهبود اثربخشی کنترل‌های امنیتی مربوط به دارایی‌های اطلاعاتی سازمان (طبق بند ۳-۵-۵)؛

برای اطمینان از حفاظت موثر و مستمر ISMS از دارایی‌های اطلاعاتی سازمان ، لازم است مراحل "الف" تا "ت" به طور مداوم جهت شناسایی تغییر در مخاطرات یا در راهبردهای سازمان یا اهداف کسب و کار تکرار شود.

۳-۵-۲ شناسایی الزامات امنیت اطلاعات

الزامات امنیت اطلاعات را می‌توان در محدوده‌ی راهبرد کلی و اهداف کسب و کار سازمان، اندازه و گستره جغرافیایی آن، با درک موارد زیر شناسایی کرد:

الف) دارایی‌های اطلاعاتی شناسایی شده و ارزش آن‌ها؛

ب) نیازهای کسب وکار برای ذخیره سازی و پردازش اطلاعات؛ و

پ) الزامات قانونی، مقررات تنظیم‌شده و قراردادی.

ارزیابی روش‌مند مخاطرات مرتبط با دارایی‌های اطلاعاتی سازمان، شامل تحلیل تهدیدها علیه دارایی‌های اطلاعاتی؛ آسیب‌پذیری‌ها و احتمال تحقق تهدید در مورد دارایی‌های اطلاعاتی؛ و اثر بالقوه‌ی هر رخداد امنیت اطلاعات بر دارایی‌های اطلاعاتی است. انتظار می‌رود هزینه کنترل‌های امنیتی مربوط متناسب با اثر قابل تصور از تحقق مخاطره بر کسب و کار باشد.

۳-۵-۳ ارزیابی مخاطرات امنیت اطلاعات

مدیریت مخاطرات امنیت اطلاعات به روشی مناسب برای ارزیابی و بر طرف سازی مخاطره نیاز دارد که ممکن است شامل برآورد هزینه‌ها و منافع، الزامات قانونی، جنبه‌های اجتماعی، اقتصادی و محیطی، خواسته‌های مورد نظر ذی‌نفعان، اولویت‌ها و سایر ورودی‌ها و متغیرهای متناسب باشد. نتایج ارزیابی مخاطره امنیت اطلاعات به راهنمایی و تعیین تصمیمات مدیریتی مناسب برای برطرف سازی، به منظور انجام‌دادن و الویت‌بندی مدیریت مخاطرات امنیت اطلاعات و پیاده‌سازی کنترل‌های امنیتی مناسب برای

حفاظت در برابر این مخاطرات کمک خواهد کرد. هدایت لازم برای مدیریت مخاطره امنیت اطلاعات، شامل توصیه‌های ارزیابی مخاطره، بر طرف سازی مخاطره، پذیرش مخاطره، آگاه‌سازی مخاطره، پایش مخاطره و بازنگری مخاطره در استاندارد ملی ایران به شماره ۲۷۰۰۵ فراهم شده است.

۳-۵-۴ انتخاب و پیاده سازی کنترل‌های امنیت اطلاعات

به محض این که الزامات امنیت اطلاعات شناسایی و مخاطرات امنیت اطلاعات مربوط به دارایی‌های اطلاعاتی شناسایی شده، تعیین و ارزیابی (شامل تصمیم‌گیری در مورد بر طرف سازی مخاطرات امنیت اطلاعات) گردید، کنترل‌های مناسب را باید انتخاب و پیاده‌سازی کرد تا از کاهش مخاطرات امنیت اطلاعات به سطح قابل قبول سازمان اطمینان حاصل شود. کنترل‌ها را می‌توان از استاندارد ملی ایران به شماره ۲۷۰۰۲، سایر مجموعه‌های کنترلی مناسب یا کنترل‌های جدیدی که متناسب با نیازهای خاص طراحی شده‌اند، انتخاب کرد. انتخاب کنترل‌های امنیتی به الزامات امنیتی، پذیرش مخاطره امنیت اطلاعات، گزینه‌های بر طرف سازی مخاطره و رویکرد عمومی مورد استفاده‌ی سازمان برای مدیریت مخاطره بستگی دارد . انتخاب و پیاده‌سازی کنترل‌ها می‌تواند در قالب بیانیه کاربردپذیری مستند شود تا به تطبیق الزامات کمک کند.

کنترل‌های مشخص شده در استاندارد ملی ایران به شماره ۲۷۰۰۲ را بهترین اقدامات قابل اعمال در اکثر سازمان‌ها قلمداد می‌کنند و به آسانی با سازمان‌های دارای اندازه‌ها و پیچیدگی‌های مختلف منطبق می‌شوند. سایر استانداردهای خانواده ISMS، راهنمایی در مورد انتخاب و به کارگیری کنترل‌های امنیت اطلاعات استاندارد ملی ایران به شماره ۲۷۰۰۲ برای سامانه مدیریت (استاندارد ملی ایران به شماره ۲۷۰۰۱) فراهم می‌کنند.

۳-۵-۵ پایش، نگهداری و بهبود اثربخشی ISMS

یک سازمان نیاز به نگهداری و بهبود ISMS از طریق پایش و ارزیابی عملکرد آن براساس خط مشی و اهداف سازمان و گزارش نتایج به مدیریت جهت بازنگری ISMS دارد. این بازنگری ISMS، فراهم‌سازی شواهد اعتبارسنجی[1]، درستی‌سنجی[2] و قابلیت ردگیری اقدامات اصلاحی، پیشگیرانه و بهبوددهنده بر پایه‌ی سوابق این نواحی پایش‌شده، شامل پایش کنترل‌های امنیت اطلاعات را ممکن می‌سازد.

۳-۶ عوامل مهم موفقیت ISMS

عوامل زیادی در پیاده‌سازی موفق ISMS موثر هستند تا به سازمان اجازه رسیدن به اهداف کسب وکار خود را بدهد. نمونه‌هایی مهم این عوامل موفقیت عبارتند از:

1 - Validation
2 - Verification

الف) خط مشی امنیت اطلاعات، اهداف، و فعالیت‌های همسو با اهداف؛

ب) رویکرد و چارچوبی برای طراحی، پیاده سازی، پایش، نگهداری، و بهبود امنیت اطلاعات همساز با فرهنگ سازمانی؛

پ) پشتیبانی و پایبندی مشهود از تمامی سطوح مدیریت به خصوص مدیریت عالی؛

ت) درک الزامات حفاظت دارایی اطلاعاتی که از طریق به‌کارگیری مدیریت مخاطره امنیت اطلاعات به دست آمده است؛ (طبق استاندارد ملی ایران به شماره ۲۷۰۰۵)؛

ث) برنامه‌ی موثر آگاه‌سازی، تحصیلات دانشگاهی و مهارت‌های حرفه‌ای الزامات مندرج در خط مشی‌ها و استانداردهای امنیت اطلاعات، به منظور ارتقا سطح آگاهی کارکنان و سایر طرف‌های مرتبط و تشویق آنها به رعایت این الزامات؛

ج) فرآیند مدیریت موثر رخداد امنیت اطلاعات؛

چ) رویکرد موثر مدیریت تداوم کسب وکار؛ و

ح) سامانه سنجش جهت ارزشیابی عملکرد مدیریت امنیت اطلاعات و بازخورد پیشنهادهای بهبود عملکرد.

سامانه‌ی مدیریت امنیت اطلاعات (ISMS)، احتمال دستیابی سازمان به عوامل اصلی موفقیت مورد نیاز برای حفاظت دارایی‌های اطلاعاتی را به طور مستمر افزایش می‌دهد.

۳-۷ مزایای استانداردهای خانواده ISMS

مزایای پیاده‌سازی ISMSعمدتاً ناشی از کاهش مخاطرات امنیت اطلاعات (مانند کاهش احتمال و/یا اثر ایجاد شده توسط رخدادهای امنیت اطلاعات) است. مزایای پذیرش استانداردهای خانواده ISMS به طور اخص عبارتند از:

الف) پشتیبانی از فرآیند مشخص‌سازی، پیاده‌سازی، بهره‌برداری و نگهداری یک ISMS یکپارچه و مقرون به صرفه‌ی جامع و منظم که نیازهای سازمان را در بهره‌برداری‌ها و جایگاه‌های مختلف برآورده می‌کند؛

ب) کمک به مدیریت در ساختاربندی رویکردهای مدیریت امنیت اطلاعات در بستر همکاری مدیریت و زمامداری مخاطره، شامل کارآموزی و آموزش صاحبان سامانه و کسب و کار بر اساس مدیریت کلی‌نگر[1] امنیت اطلاعات؛

پ) ترویج اقدامات امنیت اطلاعات مطلوب و پذیرفته‌شده‌ی جهانی، با روش غیر دستوری و آزادی عمل دادن به سازمان‌ها در پذیرش و بهبود کنترل‌های متناسب با موقعیت‌های خاص آن‌ها به منظور ایستادگی در برابر تغییرات داخلی و خارجی؛ و

1 - Holistic

ت) تدارک زبان مشترک و مفاهیم پایه برای امنیت اطلاعات و ایجاد اطمینان در شرکای کسب وکار نسبت به ISMS مورد توافق، به خصوص اگر در پی دریافت گواهی رعایت استاندارد ملی ایران به شماره ۲۷۰۰۱ از نهاد معتبر صدور گواهی باشند.

۴ استانداردهای خانواده ISMS

۴-۱ اطلاعات کلی

استانداردهای خانواده ISMS شامل استانداردهای مرتبط با هم است که در گذشته منتشر شده‌اند یا در دست تدوین هستند و تعدادی از مولفه‌های ساختاری مهم را در برمی‌گیرند. این مولفه‌ها متمرکز بر استانداردهایی اجباری است که به توصیف الزامات ISMS (استاندارد ملی ایران به شماره ۲۷۰۰۰) و همچنین الزامات مرجع صدور گواهی (استاندارد ملی ایران به شماره ۲۷۰۰۶) می‌پردازند که مراجع صدور گواهی، انطباق با استاندارد ملی ایران به شماره ۲۷۰۰۱ را گواهی می‌کنند.

سایر استانداردها راهنمایی برای جنبه‌های مختلف پیاده‌سازی ISMS تاکید به فرآیند عمومی، راهنماهای مرتبط با کنترل و راهنمای بخشی خاص را فراهم می‌کند. روابط استانداردهای خانواده ISMS در شکل ۱ نشان داده شده است.

استانداردهایی که برای پشتیبانی مستقیم، تفسیر و/یا راهنمایی تفصیلی در مورد کل فرآیندها و الزامات PDCA مشخص شده در استاندارد ملی ایران به شماره ۲۷۰۰۱ (طبق بند ۴-۳-۱) ارائه شده است، عبارتند از: ISO/IEC 27000 (طبق بند۴-۲-۱)، استاندارد ملی ایران به شماره ۲۷۰۰۲ (طبق بند۴-۴-۱)، ISO/IEC 27003 (طبق بند۴-۴-۲)، استاندارد ملی ایران به شماره ۲۷۰۰۴ (طبق بند۴-۴-۳)، استاندارد ملی ایران به شماره ۲۷۰۰۵ (طبق بند۴-۴-۴) و ISO/IEC 27007 (طبق بند۴-۴-۵).

در استاندارد ملی ایران به شماره ۲۷۰۰۶ (طبق بند۴-۳-۲)، الزامات مراجع تدارک بیننده گواهینامه‌های ISMS نشان داده شده است. استاندارد ملی ایران به شماره ۲۷۰۱۱ (طبق بند۴-۵-۱) و استاندارد ملی ایران به شماره ۱۳۲۲۰ (طبق بند۴-۵-۲)، راهنماهای بخش خاص ISMS را نشان می‌دهد.

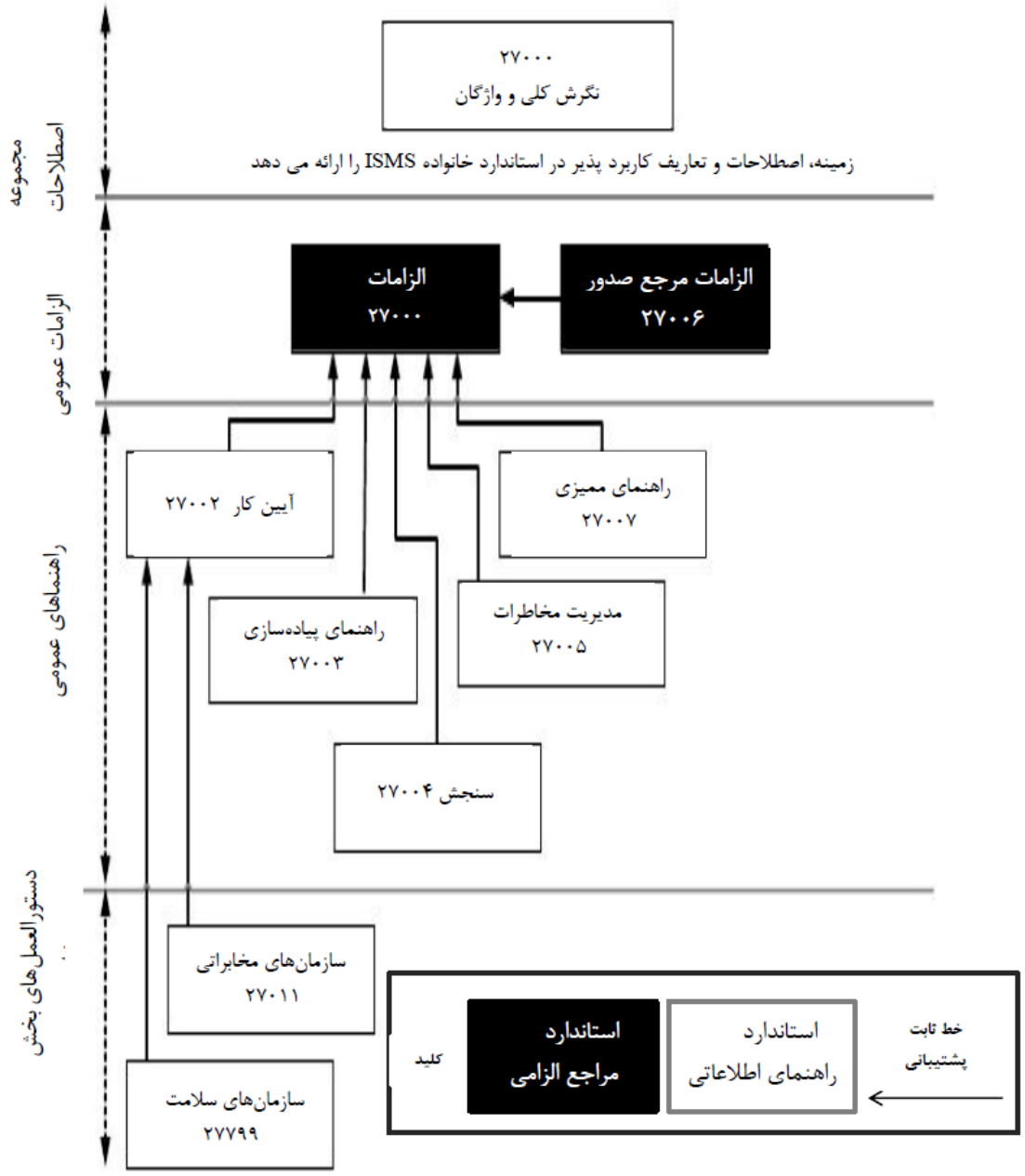
استانداردهای خانواده ISMS با بسیاری از استانداردهای دیگر ISO و ISO/IEC ارتباط دارند و به صورت زیر قابل طبقه‌بندی و توصیف هستند:

الف) استانداردهای توصیف‌کننده مرور کلی و واژگان (طبق بند۴-۲)؛

ب) استانداردهای مشخص‌کننده الزامات (طبق بند۴-۳)؛

پ) استانداردهای توصیف‌کننده راهنماهای کلی (طبق بند۴-۴)؛ یا

ت) استانداردهای توصیف‌کننده راهنماهای بخشی خاص (طبق بند۴-۵).



شکل ۱: روابط استانداردهای خانواده ISMS

۴-۲ استانداردهای توصیف کننده مرور کلی و واژگان

۴-۲-۱ ISO/IEC 27000 (سند حاضر)

فناوری اطلاعات- فنون امنیتی- سامانه‌های مدیریت امنیت اطلاعات- مرور کلی و واژگان

دامنه کاربرد: این استاندارد ملی موارد زیر را برای سازمان‌ها و افراد فراهم می‌سازد:

الف) مرور کلی بر استانداردهای خانواده ISMS؛

ب) مقدمه‌ای بر سامانه‌های مدیریت امنیت اطلاعات (ISMS)؛

پ) توصیف مختصر فرآیند طرح- اجرا- بررسی- اقدام (PDCA)؛ و
ت) اصطلاحات و تعاریف مورد استفاده در استانداردهای خانواده ISMS.
هدف: ISO/IEC 27000 مبانی سامانه‌های مدیریت امنیت اطلاعات که موضوع استانداردهای خانواده ISMS را شکل می‌دهد توصیف اصطلاحات مرتبط را تعریف می‌کند.

۴-۳ استانداردهای مشخص کننده الزامات

۴-۳-۱ استاندارد ملی ایران به شماره ۲۷۰۰۱ (ISO/IEC 27001)

فناوری اطلاعات- فنون امنیتی-سامانه‌های مدیریت امنیت اطلاعات-الزامات

دامنه کاربرد: این استاندارد ملی الزامات برقراری، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود سامانه‌های رسمی مدیریت امنیت اطلاعات (ISMS) با درنظرگرفتن محتوای مخاطرات کلی کسب و کار سازمان را مشخص می‌کند. این استاندارد همچنین الزامات پیاده‌سازی کنترل‌های امنیتی تطابق داده شده با نیازهای سازمان‌های مختلف یا بخش‌های وابسته به آن، مشخص شده است. این استاندارد ملی، تمامی انواع سازمان‌ها (مانند بنگاه‌های تجاری، موسسات دولتی، سازمان‌های غیرانتفاعی) را در برمی‌گیرد.

هدف: استاندارد ملی به شماره ۲۷۰۰۱ الزامات اجباری به منظور توسعه و بهره‌برداری از ISMS را ارائه می‌کند که شامل مجموعه کنترل‌هایی برای مهار و کاهش مخاطرات مرتبط با دارایی‌های اطلاعاتی که سازمان با کمک ISMS حفاظت می‌کند. سازمان‌های بهره‌بردار ISMS ممکن است منطبق با خود، ممیزی و گواهی کنند. اهداف کنترلی و کنترل‌های پیوست الف (استاندارد ملی ایران به شماره ۲۷۰۰۱) باید به عنوان قسمتی از این فرآیند ISMS انتخاب شوند تا الزامات شناسایی شده را به طور مناسب پوشش دهند. اهداف کنترلی و کنترل‌های فهرست شده در جدول الف-۱ (استاندارد ملی ایران به شماره ۲۷۰۰۱) به طور مستقیم از بندهای ۵ تا ۱۵ استاندارد ملی ایران به شماره ۲۷۰۰۲ استخراج شده است و تراز شده بر آن‌ها است.

۴-۳-۲ استاندارد ملی ایران به شماره ۲۷۰۰۶ (ISO/IEC 27006)

فناوری اطلاعات- فنون امنیتی – الزامات نهادهای ارائه‌دهنده خدمات ممیزی و صدور گواهی سامانه‌های مدیریت امنیت اطلاعات

دامنه کاربرد: این استاندارد ملی علاوه بر الزامات موجود در ISO/IEC 17021، الزاماتی را مشخص نموده و راهنمایی برای مراجع ارائه‌کننده‌ی ممیزی و گواهی ISMS طبق استاندارد ملی ایران به شماره ۲۷۰۰۱ را فراهم می‌کند. این استاندارد در اصل برای پشتیبانی از تایید صلاحیت نهادهای گواهی‌کننده‌ای است که گواهی ISMS را طبق استاندارد ملی ایران به شماره ۲۷۰۰۱ ارائه می‌کنند.

هدف: استاندارد ملی ایران به شماره ۲۷۰۰۶ متمم ISO/IEC 17021 است که با اعتبار سازمان‌های صدور گواهی الزامات را فراهم می‌سازد. بنابراین به این سازمان‌ها اجازه می‌دهد تا گواهی انطباق مستمر الزامات استاندارد ملی ایران به شماره ۲۷۰۰۱را ارائه دهند.

۴-۴ استانداردهای توصیف کننده راهنمای مرور کلی

۴-۴-۱ استاندارد ملی ایران به شماره ۲۷۰۰۲ (ISO/IEC 27002)

فناوری اطلاعات- فنون امنیتی- آیین کار مدیریت امنیت اطلاعات

دامنه کاربرد : این استاندارد ملی، فهرستی از اهداف کنترلی پذیرفته‌شده معمول و کنترل‌های برتر جهت استفاده به عنوان راهنمای پیاده‌سازی در زمان انتخاب و پیاده‌سازی کنترل‌ها برای رسیدن به امنیت اطلاعات را ارائه می‌دهد.

هدف: استاندارد ملی ایران به شماره ۲۷۰۰۲ راهنمایی بر پیاده‌سازی کنترل‌های امنیت اطلاعات فراهم می‌آورد. به‌خصوص توصیه‌های مختص پیاده‌سازی در بندهای ۵ تا ۱۵ و راهنمایی راجع به بهترین پشتیبانی از کنترل‌های مشخص‌شده در بندهای الف-۵ تا الف-۱۵ استاندارد ملی ایران به شماره ۲۷۰۰۱ را ارائه می‌دهد.

۴-۴-۲ استاندارد ملی ایران به شماره ۲۷۰۰۳ (ISO/IEC 27003)

فناوری اطلاعات- فنون امنیتی- راهنمای پیاده‌سازی سامانه مدیریت امنیت اطلاعات

دامنه کاربرد: این استاندارد ملی، راهنمای پیاده‌سازی عملی است و اطلاعات بیشتری برای برقراری، پیاده‌سازی، بهره‌برداری، پایش، بازنگری، نگهداری و بهبود ISMS براساس استاندارد ملی ایران به شماره ۲۷۰۰۱ را ارائه می‌دهد.

هدف: استاندارد ملی ایران به شماره ۲۷۰۰۳ رویکرد فرآیندگرا به پیاده‌سازی موفق ISMS بر اساس استاندارد ملی ایران به شماره ۲۷۰۰۱ ارائه خواهد کرد.

۴-۴-۳ استاندارد ملی ایران به شماره ۱۴۰۹۶ (ISO/IEC 27004)

فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات- سنجش

دامنه کاربرد: استاندارد ملی، راهنمایی‌ها و توصیه‌هایی راجع به تدوین و به کارگیری سنجش به منظور ارزیابی اثربخشی ISMS، اهداف کنترلی و کنترل‌های استفاده شده در پیاده سازی و مدیریت امنیت اطلاعات همانطور که در استاندارد ملی ایران به شماره ۲۷۰۰۱ مشخص شده را ارائه خواهد کرد.

هدف: استاندارد ملی ایران به شماره ۱۴۰۹۶چارچوبی برای سنجش ارائه کرده که سنجش ارزیابی اثربخشی ISMS براساس استاندارد ملی ایران به شماره ۲۷۰۰۱ را میسر خواهد کرد.

۴-۴-۴ استاندارد ملی ایران به شماره ۲۷۰۰۵ (ISO/IEC 27005)

فناوری اطلاعات- فنون امنیتی- مدیریت مخاطرات امنیت اطلاعات

دامنه کاربرد: این استاندارد ملی، راهنماهایی برای مدیریت مخاطرات امنیت اطلاعات ارائه می‌کند. رویکرد توصیف‌شده در این استاندارد ملی، مفاهیم کلی مشخص‌شده در استاندارد ملی ایران به شماره ۲۷۰۰۱را پشتیبانی می‌کند.

هدف: استاندارد ملی ایران به شماره ۲۷۰۰۵ راهنمایی بر پیاده سازی رویکرد مدیریت مخاطرات فرآیندگرا برای کمک به پیاده‌سازی رضایت‌بخش و تحقق الزامات استاندارد ملی ایران به شماره ۲۷۰۰۱ برای مدیریت مخاطره امنیت اطلاعات را ارائه می‌دهد.

۴-۴-۵ ISO/IEC 27007

فناوری اطلاعات- فنون امنیتی- راهنمای ممیزی سامانه‌های مدیریت امنیت اطلاعات

دامنه کاربرد: این استاندارد ملی، افزون بر راهنمایی ارائه شده در استاندارد ملی ایران به شماره ۱۹۰۱۱ است که به طور کلی در سامانه‌های مدیریتی کاربردپذیر است، راهنمایی را بر انجام ممیزی ISMS و نیز راهنمایی بر صلاحیت ممیزان سامانه مدیریت امنیت اطلاعات ارائه خواهد داد.

هدف: ISO/IEC 27007 راهنمایی برای سازمان‌هایی که نیاز به انجام ممیزی داخلی یا خارجی ISMS دارند یا برنامه ممیزی ISMS را در برابر الزامات مشخص شده در استاندارد ملی ایران به شماره ۲۷۰۰۱ مدیریت می‌کنند، فراهم خواهد کرد.

۴-۵ استانداردهای توصیف کننده راهنماهای بخش خاص

۴-۵-۱ استاندارد ملی ایران به شماره ۲۷۰۱۱ (ISO/IEC 27011)

فناوری اطلاعات- فنون امنیتی- راهنماهای مدیریت امنیت اطلاعات برای سازمان‌های مخابراتی بر پایه استاندارد ملی ایران به شماره ۲۷۰۰۲

دامنه کاربرد: این استاندارد ملی، راهنماهای پشتیبانی‌کننده از پیاده‌سازی مدیریت امنیت اطلاعات (ISM) در سازمان‌های مخابراتی را ارائه می‌کند.

هدف: استاندارد ملی ایران به شماره ۲۷۰۱۱، برای سازمان‌های مخابراتی، با پذیرش راهنماهای منحصر به فرد استاندارد ملی ایران به شماره ۲۷۰۰۲ در بخش صنعت آن‌ها که افزون بر راهنمای ارائه شده نسبت به تحقق الزامات پیوست الف استاندارد ملی ایران به شماره ۲۷۰۰۱ است را ارائه می‌کند.

۴-۵-۲ استاندارد ملی ایران به شماره ۱۳۲۲۰ (ISO 27799)

انفورماتیک سلامت- مدیریت امنیت اطلاعات در سلامت با استفاده از استاندارد ملی ایران به شماره ۲۷۰۰۲

دامنه کاربرد: این استاندارد ملی، راهنماهای پشتیبانی کننده از پیاده‌سازی مدیریت امنیت اطلاعات (ISM) در سازمان‌های بهداشت را ارائه می‌کند.

هدف: استاندارد ملی ایران به شماره ۱۳۲۲۰، برای سازمان‌های سلامت، با پذیرش راهنماهای منحصر به فرد استاندارد ملی ایران به شماره ۲۷۰۰۲ در بخش صنعت آن‌ها که افزون بر راهنمای ارائه شده نسبت به تحقق الزامات پیوست الف استاندارد ملی ایران به شماره ۲۷۰۰۱ است را ارائه می‌کند.

پیوست الف

(اطلاعاتی)

اصطلاحات فعلی بیان شرط

هر کدام از مستندات استانداردهای خانواده ISMS به خودی خود تعهدی برای کسی ایجاد نمی‌کند. اما چنین تعهدی برای مثال ممکن است توسط مقررات یا قراردادی ایجاد شود. برای آن که کاربری بتواند ادعای انطباق با سندی را داشته باشد، باید الزامات را شناسایی کند. همچنین در مواردی که آزادی انتخاب وجود دارد، کاربر باید بتواند این الزامات را از سایر توصیه‌ها تشخیص دهد.

جدول زیر چگونگی تفسیر اصطلاح بیان کلامی که می‌تواند الزامات و/یا توصیه‌ها برای مستندات استانداردهای خانواده‌ی ISMS باشد را تصریح می‌کند.

نشانه	شرح
الزامات	اصطلاحات «باید» و «نباید» دلالت بر الزاماتی دارد که به شدت دنبال می‌شوند تا مطابق با سند باشد و انحراف از آن مجاز نیست.
توصیه	اصطلاحات «توصیه می‌شود» و «توصیه نمی‌شود» نشان دهنده این است که از میان چندین مورد محتمل، یک مورد خصوصا، مناسب است، بدون آن که به گزینه‌های دیگر اشاره یا آن‌ها را مستثنی کند یا این که عمل معینی برتری داده شود ولی نه لزوماً الزامی بوده یا که (به شکل منفی آن) احتمال یا عمل معینی ناچیز انگاشته شود ولی منع نشود.
اجازه	اصطلاح «مجاز است» و «نیازی نیست» نشان می‌دهد که یک عمل در محدوده سند مجاز است.
امکان	اصطلاح «می‌توان» و «نمی‌توان» نشان دهنده احتمال وقوع چیزی است.

پیوست ب

(اطلاعاتی)

اصطلاحات دسته‌بندی‌شده

ب-۱ اصطلاحات مربوط به امنیت اطلاعات

۲-۲ پاسخ‌گویی accountability

۲-۵ احراز هویت authentication

۲-۶ صحت authenticity

۲-۷ دسترس‌پذیری availability

۲-۹ محرمانگی confidentiality

۲-۱۹ امنیت اطلاعات information security

۲-۲۵ یکپارچگی integrity

۲-۲۷ انکار ناپذیری non-repudiation

۲-۳۳ قابلیت اطمینان reliability

ب-۲ عبارات مربوط به مدیریت

۲-۸ تداوم کسب وکار business continuity

۲-۱۲ اقدام اصلاحی corrective action

۲-۱۳ اثربخشی effectiveness

۲-۱۴ کارایی efficiency

۲-۱۶ راهنما guideline

۲-۲۳ سامانه مدیریت امنیت اطلاعات (ISMS) information security management system (ISMS)

۲-۲۶ سامانه مدیریت management system

۲-۲۸ خط مشی policy

۲-۲۹ اقدام پیشگیرانه preventive action

۲-۳۱ فرآیند process

ب-۳ عبارات مربوط به مخاطره امنیت اطلاعات

۲-۱ کنترل دسترسی access control

۲-۳ دارایی asset

۲-۴ حمله attack

control	۲-۱۰ کنترل
control objective	۲-۱۱ هدف کنترلی
event	۲-۱۵ رویداد
impact	۲-۱۷ اثر
information asset	۲-۱۸ دارایی اطلاعاتی
information security event	۲-۲۰ رویداد امنیت اطلاعات
information security incident	۲-۲۱ رخداد امنیت اطلاعات
information security incident management	۲-۲۲ مدیریت رخداد امنیت اطلاعات
information security risk	۲-۲۴ مخاطره امنیت اطلاعات
risk	۲-۳۴ مخاطره
risk acceptance	۲-۳۵ پذیرش مخاطره
risk analysis	۲-۳۶ تحلیل مخاطره
risk assessment	۲-۳۷ ارزیابی مخاطره
risk communication	۲-۳۸ اطلاع رسانی مخاطره
risk criteria	۲-۳۹ معیارهای مخاطره
risk estimation	۲-۴۰ برآورد مخاطره
risk evaluation	۲-۴۱ ارزشیابی مخاطره
risk management	۲-۴۲ مدیریت مخاطره
risk treatment	۲-۴۳ بر طرف سازی مخاطره
threat	۲-۴۵ تهدید
vulnerability	۲-۴۶ آسیب پذیری
	ب-۴ عبارات مربوط به مستندسازی
procedure	۲-۳۰ روش اجرایی
record	۲-۳۲ سابقه
statement of applicability	۲-۴۴ بیانیه کاربست پذیری

کتابنامه

[1] ISO/IEC 17021:2006, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*

[2] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

[3] ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*

[4] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

[5] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

[6] ISO/IEC 270034), *Information technology — Security techniques — Information security management system implementation guidance*

[7] ISO/IEC 270045), *Information technology — Security techniques — Information security management —Measurement*

[8] ISO/IEC 27005:2008, *Information technology — Security techniques — Information security risk management*

[9] ISO/IEC 27006:2007, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

[10] ISO/IEC 270076), *Information technology — Security techniques — Guidelines for information security management systems auditing*

[11] ISO/IEC 270117), *Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

[12] ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

[13] ISO/IEC Guide 73:2002, *Risk Management — Vocabulary — Guidelines for use in standards*

فصل دوم

فناوری اطلاعات - فنون امنیتی- سیستم های مدیریت امنیت اطلاعات- الزامات

ISO/IEC 27001

Information technology-- Security techniques
Information security management systems
Requirements

پیش گفتار

استاندارد " فن‌آوری اطلاعات- فنون امنیتی- سیستم‌های مدیریت امنیت اطلاعات - الزامات" که پیش نویس آن درکمیسیون های مربوط توسط مؤسسهٔ استاندارد و تحقیقات صنعتی ایران تهیه و تدوین شده و در شصت و یکمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده ها مورخ ۸۷/۱۰/۱۵ مورد تصویب قرارگرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینهٔ صنایع، علوم و خـدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارایه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفـت. بنـابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

این استاندارد ملی برمبنای استاندارد بین المللی زیر تدوین شده و معادل آن به زبان فارسی است:

1- ISO/IEC 27001:2005, 1st Ed.: Information technology - Security techniques - Information security management systems – Requirements

۲- خراسانی‌راد، ایمان. حسین‌آبادی، حسن. امیـرزاده، رامـین. اسـتاندارد ISO/IEC 27001:2005 ، تهـران: شرکت مشارکتی اِر-و-توف ایران(عضو گروه توف نورد)، زمستان ۱۳۷۵.

۰ مقدمه

۰-۱ کلیات

این استاندارد ملی، به منظور فراهم آوردن مدلی برای ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری و بهبود یک سیستم مدیریت امنیت اطلاعات، تهیه شده است. توصیه می شود پذیرش یک سیستم مدیریت امنیت اطلاعات، یک تصمیم راهبردی برای سازمان باشد. طراحی و پیاده‌سازی سیستم مدیریت امنیت اطلاعات یک سازمان، تحت تاثیرنیازها واهداف، الزامات امنیتی، فرآیند های بکار گرفته شده و اندازه و ساختار سازمان، قرار دارد. انتظار می‌رود عوامل مذکور و سیستم‌های پشتیبان آنها، به مرور زمان، دچار تغییر شوند. انتظار می‌رود پیاده‌سازی یک سیستم مدیریت امنیت اطلاعات، با نیازهای سازمان متناسب شود. به عنوان مثال، یک وضعیت ساده، نیازمند یک راه کار ساده سیستم مدیریت امنیت اطلاعات است.

این استاندارد ملی می‌تواند توسط طرف‌های ذینفع[1] درونی و برونی، به منظور ارزیابی انطباق، مورد استفاده قرار گیرد.

۰-۲ دیدگاه فرآیند گرا[2]

این استاندار ملی، برای ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات سازمان، دیدگاه فرآیند گرا را بر می‌گزیند.

برای این‌که سازمانی به طرز اثربخش عمل نماید، نیاز دارد فعالیت‌های متعددی را شناسایی و مدیریت نماید. هر فعالیتی که منابعی را به خدمت می‌گیرد وآن را به منظور تبدیل ورودی‌ها به خرجی‌ها، مدیریت می‌نماید، می‌تواند یک فرآیند در نظر گرفته شود. اغلب، خروجی یک فرآیند ، مستقیماً ورودی فرآیند بعدی را شکل می‌دهد.

بکارگیری سیستمی از فرآیند های درون سازمان، همراه با شناسایی و تعیین ارتباط متقابل این فرآیند ها و همچنین مدیریت آنها، «دیدگاه فرآیندگرا» نامیده می‌شود.

دیدگاه فرآیند گرایی که در این استاندارد ملی برای مدیریت امنیت اطلاعات ارایه شده، کاربرانش را ترغیب می‌کند که اهمیت موارد ذیل را مدنظر قرار دهند:

الف) درک الزامات امنیت اطلاعات سازمان و لزوم ایجاد خط‌مشی و اهداف برای امنیت اطلاعات.

ب) پیاده سازی واجرای کنترل‌ها برای مدیریت ریسک امنیت اطلاعات یک سازمان در خصوص ریسک‌های کلان کسب وکار سازمان.

ج) پایش و بازنگری عملکرد و اثربخشی سیستم مدیریت امنیت اطلاعات، و

د) بهبود مستمر برپایه اندازه‌گیری اهداف.

این استاندارد ملی، مدل«طرح- اجرا- بررسی- اقدام(PDCA)»، که در ساختار تمامی فرآیند های سیستم مدیریت امنیت اطلاعات به کار گرفته می‌شود را برگزیده است. شکل ۱، نشان می‌دهد که چگونه یک

1- Interested parties
2- Process approach

سیستم مدیریت امنیت اطلاعات، الزامات امنیت اطلاعات و انتظارات طرف‌های ذینفع را به عنوان ورودی دریافت کرده و از طریق اقدامات و فرآیند های لازم، خروجی‌های امنیت اطلاعاتی را که با انتظارات و الزامات آنها مطابقت دارد، ایجاد می‌کند. شکل۱، ارتباط بین فرآیند های مطرح شده در بندهای ۴، ۵، ۶، ۷ و ۸ را نیز نشان می‌دهد.

پذیرش مدل PDCA، همچنین منعکس کننده اصول بیان شده در راهنماهای OECD(2002)[1] که حاکم بر امنیت شبکه‌ها و سیستم‌های اطلاعاتی است، است. این استاندارد ملی، یک مدل قوی برای پیاده‌سازی اصول راهنماهای مذکور که حاکم بر برآورد ریسک، طراحی و پیاده‌سازی امنیت، مدیریت و ارزیابی مجدد امنیت می‌باشند، فراهم کرده است.

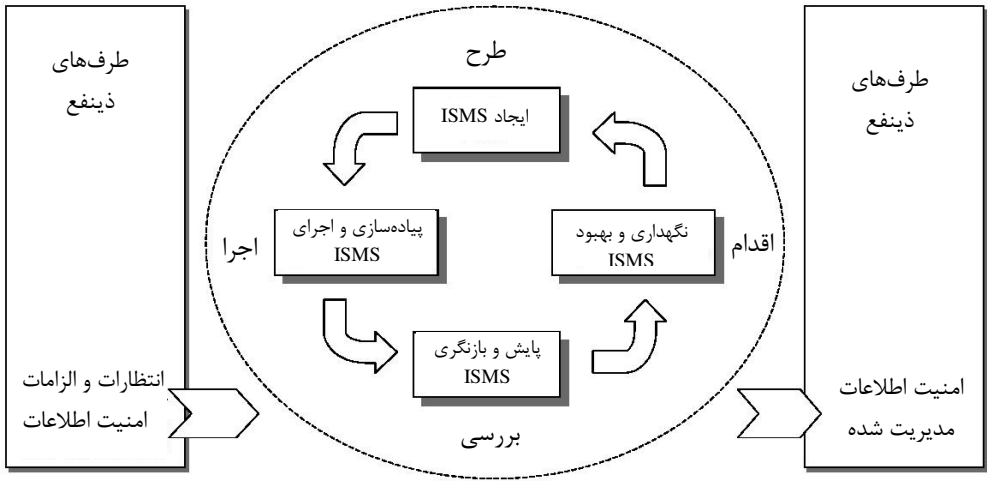
مثال ۱:

می‌تواند الزامی وجود داشته باشد که نقص‌های امنیت اطلاعات[2]، موجب زیان مالی جدی و/ یا برآشفتگی[3] سازمان نشوند.

مثال ۲:

می‌توان انتظار داشت، در صورت بروز یک حادثه خطرناک(مانند هک کردن وب سایت تجارت الکترونیکی یک سازمان)، افرادی که مطابق با روش‌های اجرایی مناسب، آموزش‌های کافی دیده‌اند، برای به حداقل رساندن آسیب، می بایست وجود داشته باشند.

شکل۱- مدل PDCA به کار رفته در فرآیند های سیستم مدیریت امنیت اطلاعات



۱- راهنمای OECD برای امنیت سیستم‌های اطلاعاتی و شبکه ها- به سوی فرهنگ امنیت- پاریس OECD، جولای ۲۰۰۲، www.oecd.org

2- Breaches of Information Security

3- Embarrassment

طرح (ایجاد سیستم مدیریت امنیت اطلاعات)	ایجاد خط‌مشی، اهداف، فرآیندها و روش‌های اجرایی سیستم مدیریت امنیت اطلاعات، مرتبط با مدیریت مخاطرات و بهبود امنیت اطلاعات، به منظور حصول نتایجی مطابق با خط‌مشی‌ها و اهداف کلان یک سازمان.
اجرا (پیاده‌سازی و اجرای سیستم مدیریت امنیت اطلاعات)	پیاده‌سازی و اجرای خط‌مشی، کنترل‌ها، فرآیندها و روش‌های اجرایی سیستم مدیریت امنیت اطلاعات.
بررسی (پایش و بازنگری سیستم مدیریت امنیت اطلاعات)	ارزیابی، و در موارد مقتضی، سنجش عملکرد فرآیند، مطابق با خط مشی، اهداف و تجارب علمی امنیتی سیستم مدیریت امنیت اطلاعات و گزارش نتایج به مدیریت به منظور بازنگری.
اقدام (نگهداری و بهبود سیستم مدیریت امنیت اطلاعات)	انجام اقدامات اصلاحی و پیشگیرانه بر مبنای نتایج ممیزی داخلی سیستم مدیریت امنیت اطلاعات و بازنگری مدیریت یا سایر اطلاعات مرتبط، به منظور دستیابی به بهبود مستمر سیستم مدیریت امنیت اطلاعات

۰-۳ سازگاری با سایر سیستم‌های مدیریتی

این استاندارد با استاندارد ملی ایران ایزو ۹۰۰۱: سال ۱۳۸۰[1] و ISO 14001:2004 به منظور پشتیبانی از پیاده‌سازی و اجرای یکپارچه و سازگار با استانداردهای مدیریتی مرتبط، تطبیق داده شده است. یک سیستم مدیریتی که به گونه‌ای مناسب طراحی شده، می‌تواند الزامات تمامی این استانداردها را برآورده سازد.

جدول پ-۱، ارتباط بین بندهای این استاندارد ملی با استاندارد ملی ایران ایزو ۹۰۰۱: سال ۱۳۸۰ و ISO 14001:2004 را نشان می‌دهد.

این استاندارد ملی به گونه‌ای طراحی شده، تا یک سازمان قادر باشد سیستم مدیریت امنیت اطلاعات خود را با الزامات سیستم مدیریتی مرتبط، یکپارچه نموده یا تطبیق دهد.

۱- منظور استاندارد ملی معادل استاندارد بین‌المللی ISO 9001:2000 می باشد.

فن‌آوری اطلاعات- فنون امنیتی- سیستم‌های مدیریت امنیت اطلاعات- الزامات

مهم- این نسخه منتشر شده، ادعا نمی‌کند که شامل تمامی شرایطی لازم برای یک قرارداد است. استفاده کنندگان، مسوول استفاده صحیح از آن می‌باشند. انطباق با یک استاندارد ملی، به تنهایی، اعطای مصونیت در برابر تعهدات قانونی نیست.

۱ هدف و دامنه کاربرد

۱-۱ کلیات

هدف از تدوین این استاندارد ملی، مشخص کردن الزامی برای ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری و بهبود یک سیستم مدیریت امنیت اطلاعات مستند شده، با در نظر گرفتن مفهوم ریسک‌های کلان کسب‌وکار سازمان است. این استاندارد ملی، الزاماتی را برای پیاده‌سازی کنترل‌های امنیتی تطابق داده شده با نیازهای سازمان‌های مختلف یا بخش‌های وابسته به آن، مشخص می‌کند. این استاندار ملی، همه انواع سازمان‌ها را پوشش می‌دهد (به عنوان مثال بنگاه‌های تجاری[1]، موسسات دولتی، سازمان‌های غیرانتفاعی[2]).
سیستم مدیریت امنیت اطلاعات، به منظور حصول اطمینان از گزینش کنترل‌های امنیتی کافی و مناسبی که از اموال اطلاعاتی حفاظت کنند و به طرف‌های ذینفع اطمینان بخشند، طراحی شده است.

یادآوری۱- اشاره به «کسب وکار» در این استاندارد ملی توصیه می شود به مفهوم وسیع کلمه، به معنای آن دسته از فعالیت‌هایی که برای مقاصد وجودی سازمان، اصلی به شمار می‌روند، تفسیر شود.

یادآوری۲- ISO/IEC 17799 راهنمایی برای پیاده‌سازی فراهم آورده، که می‌تواند در هنگام طراحی کنترل‌ها، مورد استفاده قرار گیرد.

۱-۲ کاربرد

الزامات بیان شده در این استاندارد ملی، عمومی بوده و قصد آن است که در کلیه سازمان‌ها، صرف‌نظر از نوع، اندازه وماهیت، قابل اعمال باشند. کنارگذاری هر یک از الزامات مشخص شده در بندهای۴، ۵، ۶، ۷ و۸، هنگامی‌که یک سازمان ادعای تطابق با این استاندارد ملی را دارد، قابل پذیرش نیست .
کنارگذاری هر یک از کنترل‌هایی که برای برآورده‌سازی معیار پذیرش ریسک لازمند، نیازمند توجیه و فراهم‌آوری شواهدی که ریسک‌های مربوطه، توسط افراد پاسخگو، پذیرفته شده باشند. هرجا کنترلی کنار گذاشته شود، ادعای تطابق با این استاندارد ملی پذیرفتنی نیست، مگر آنکه اینگونه موارد، توانایی و/ یا مسوولیت سازمان در قبال فراهم‌آوری امنیت اطلاعاتی که الزامات امنیتی مشخص شده به وسیله برآورد ریسک و الزامات قانونی یا آیین‌نامه مقتضی برآورده می‌سازد، را تحت تاثیر قرار ندهد.

1- Enterprises
2- Non-profit organizations

یادآوری- اگر سازمانی، یک سیستم مدیریت فرآیند کسب‌وکار اجرا شده[1] دارد، (به عنوان مثال مرتبط با استاندارد ملی ایران ایزو ۹۰۰۱ یا ISO 14001)، در بیشتر موارد، برآورده‌سازی الزامات این استاندارد ملی، در داخل سیستم مدیریتی موجود، ترجیح دارد.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی هستند که در متن این استاندارد به آنها ارجاع شده است، و به این ترتیب جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن موردنظر این استاندارد نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آنها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آنها مورد نظر است. استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 17799:2005, Information technology - Security techniques - Code of practice for information security management

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌رود.

۳-۱

دارایی[2]

هر چیزی که برای سازمان دارای ارزش است .

[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

۳-۲

دسترس پذیری[3]

ویژگی در دسترس و قابل استفاده بودن، به محض تقاضای یک موجودیت مجاز شده[4].

[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

۳-۳

محرمانگی[5]

ویژگی که اطلاعات در دسترس افراد، موجودیت‌ها یا فرآیند های غیرمجاز قرار نگرفته یا فاش نشود.

[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

1- Operative business process management system
2- Asset
3- Availibility
4- Authorized entity
5- Confidentiality

۴-۳

امنیت اطلاعات[1]

حفـظ محرمـانگی، یکپـارچگی و دسـترس‌پـذیری اطلاعـات. همچنـین، ویژگـی‌هـایی از قبیـل سـندیت[2]، پاسخگویی[3]، انکارناپذیری[4] و قابلیت اطمینان[5]، می‌تواند لحاظ شوند.

[ISO/IEC 17799-1:2005]

۵-۳

رویداد امنیت اطلاعات[6]

رخداد[7] شناسایی شده یک سیستم، سرویس یا شبکه، که دلالت برنقض احتمالی خط‌مشی امنیت اطلاعات یا یا نقص حفاظتی، یا وضعیتی که ممکن است با امنیت مرتبط بوده و قبلا شناخته نشده، دارد.

[ISO/IEC TR 18044:2004]

۶-۳

حادثه امنیت اطلاعات[8]

یک یا مجموعه‌ای از رویدادهای امنیت اطلاعات ناخواسته یا پیش‌بینی نشده که بـه احتمـال زیـاد، عملیـات کسب وکار را به خطر انداخته و امنیت اطلاعات را تهدید کنند.

[ISO/IEC TR 18044:2004]

۷-۳

سیستم مدیریت امنیت اطلاعات[9] (ISMS)

قسمتی از سیستم مدیریت کلان، بنا شده بر دیدگاه ریسک‌های کسب‌وکار، به منظـور ایجـاد، پیـاده‌سـازی، اجرا، پایش، بازنگری، نگهداری و بهبود امنیت اطلاعات.

یادآوری: سیستم مدیریتی، شامل ساختار سازمانی، خط‌مشی‌ها، طرح‌ریزی فعالیت‌ها، مسوولیت‌هـا، تجـارب، روش‌های اجرایی، فرآیند ها و منابع است.

۸-۳

یکپارچگی[10]

ویژگی حفظ صحت[11] و تمامیت[12] دارایی‌ها.

[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

1- Information security
2- Authenticity
3- Accountibility
4- Non-Repudiation
5- Reliability
6- Information security event
7- Occurence
8- Information security incident
9- Information Security Management System
10- Integrity
11- Accuracy
12- Completeness

۹-۳

ریسک باقیمانده[1]

ریسک باقیمانده پس از برطرف سازی ریسک.
[ISO/IEC Guide 73:2002]

۱۰-۳

پذیرش ریسک[2]

تصمیم برای پذیرش یک مخاطره.
[ISO/IEC Guide 73:2002]

۱۱-۳

تحلیل ریسک[3]

استفاده نظام‌مند[4] از اطلاعات به منظور شناسایی منابع و تخمین ریسک[5].
[ISO/IEC Guide 73:2002]

۱۲-۳

برآورد ریسک[6]

فرآیند کلی تحلیل و ارزیابی ریسک.
[ISO/IEC Guide 73:2002]

۱۳-۳

ارزیابی ریسک[7]

فرآیند مقایسه ریسک تخمین زده شده، با معیار ریسک ارایه شده، به منظور تعیین اهمیت ریسک.
[ISO/IEC Guide 73:2002]

۱۴-۳

مدیریت ریسک[8]

فعالیت‌های هماهنگ شده برای هدایت و کنترل یک سازمان با توجه به ریسک.
[ISO/IEC Guide 73:2002]

1- Residual risk
2- Risk acceptance
3- Risk analysis
4- Systematic
5- Risk estimate
6- Risk assesment
7- Risk evaluation
8- Risk management

۱۵-۳

برطرف‌سازی ریسک[1]

فرآیند انتخاب و پیاده‌سازی معیارهایی برای تعدیل ریسک.
[ISO/IEC Guide 73:2002]

یادآوری- در این استاندارد ملی، واژه «کنترل» به عنوان مترادف «تمهید»[2] بکار رفته است.

۱۶-۳

بیانیه کاربست‌پذیری[3]

بیانیه مستند شده‌ای که اهداف کنترلی و کنترل‌های وابسته و بکار برده شده در سیستم مدیریت امنیت اطلاعات سازمان را تشریح می‌کند.

یادآوری- اهداف کنترلی و کنترل‌ها، برمبنای نتایج و استنتاج از فرآیند های برآورد و برطرف‌سازی ریسک، الزامات قانونی یا آیین‌نامه‌ای، تعهدات قراردادی و الزامات کسب وکار سازمان برای امنیت اطلاعات، پایه‌ریزی می‌شوند.

۴ سیستم مدیریت امنیت اطلاعات

۴-۱- الزامات عمومی

سازمان باید سیستم مدیریت امنیت اطلاعات مستند شده‌ای را در چهارچوب تمامی فعالیت‌های کلان کسب‌وکار سازمان و ریسک‌هایی که با آن مواجه است، ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری نموده و بهبود دهد. در راستای مقاصد این استاندارد ملی، فرآیند ها بر پایه مدل PDCA که در شکل۱، نشان داده شده است، بکار گرفته می‌شوند.

۴-۲ ایجاد و مدیریت سیستم امنیت اطلاعات

۴-۲-۱ ایجاد سیستم مدیریت امنیت اطلاعات

سازمان باید موارد ذیل را انجام دهد:

الف- تعریف دامنه و مرزهای سیستم مدیریت امنیت اطلاعات، بر مبنای ویژگی‌های کسب‌وکار، سازمان‌ها، مکان، دارایی‌ها و فن‌آوری آن، و مشتمل بر جزئیات و توجیه برای کنارگذاری هرچیزی از دامنه. (به بند ۱-۲ رجوع کنید.)

ب- تعریف یک خط‌مشی سیستم مدیریت امنیت اطلاعات برمبنای ویژگی‌های کسب وکار، سازمان‌ها، مکان، دارایی‌ها و فن‌آوری آن که:

1- Risk treatment
2- Meaure
3- Statement of applicability

۱- مشتمل بر چهارچوبی برای تعیین اهداف و ایجاد یک درک کلان از مسیر و مبانی برای اقدام، با توجه به امنیت اطلاعات باشد.

۲- در برگیرنده کسب وکار، الزامات قانونی یا آیین‌نامه‌ای و تعهدات امنیتی قراردادی باشد.

۳- با مفاد مدیریت ریسک راهبردی سازمان که در ایجاد و نگهداری سیستم مدیریت امنیت اطلاعات لحاظ خواهد شد، هماهنگ شود.

۴- معیاری ایجاد کند که مطابق آن، ریسک ارزیابی خواهند شد(به بند۴-۲-۱-پ رجوع کنید.)، و

۵- توسط مدیریت تصویب شود.

یادآوری- برای مقاصد این استاندارد ملی، خط‌مشی سیستم مدیریت امنیت اطلاعات، به عنوان مجموعه بالاسری[1] خط‌مشی امنیت اطلاعات در نظر گرفته شده است. این خط‌مشی‌ها می‌توانند در یک مستند شرح داده شوند.

پ- تعریف رویکرد برآورد ریسک سازمان.

۱- شناسایی یک روش‌شناسی[2] برآورد ریسک که برای سیستم مدیریت امنیت اطلاعات و امنیت اطلاعات شناسایی شده کسب وکار، الزامات قانونی و آیین‌نامه‌ای، متناسب باشد.

۲- ایجادمعیاری برای پذیرش ریسک وشناسایی سطوح قابل قبول ریسک (به بند ۵-۱-و رجوع کنید).

روش‌شناسی برآورد ریسک انتخاب شده، باید اطمینان دهد که برآورد ریسک، نتایجی قابل قیاس[3] و تجدیدپذیر[4]، ارایه می‌کند.

یادآوری- روش‌شناسی های مختلفی برای برآورد ریسک وجود دارند. نمونه‌هایی از روش‌شناسی‌های برآورد ریسک در ISO/IEC TR 13335-3 (فن‌آوری اطلاعات- خطوط راهنما برای مدیریت امنیت فن‌آوری اطلاعات- فنونی برای مدیریت فن‌آوری اطلاعات) مطرح شده‌اند.

ت- شناسایی ریسک.

۱- شناسایی دارایی‌های واقع در دامنه سیستم مدیریت امنیت اطلاعات و مالکان[5] آنها.

۲- شناسایی تهدیدهای متوجه آن دارایی‌ها.

۳- شناسایی آسیب‌هایی که ممکن است با از دست دادن محرمانگی، یکپارچگی و دسترس‌پذیری، متوجه دارایی‌ها شوند.

ث- تحلیل و ارزیابی ریسک .

۱- برآورد تاثیرات کسب‌وکار، که ممکن است از نقیصه‌های امنیتی[6] حاصل شوند، بر سازمان، با توجه به پیامدهای از دست دادن محرمانگی، یکپارچگی یا دسترس‌پذیری دارایی‌ها.

1- Superset
2- Methodology
3- Compareable
4- Reproducible
5- Owners
6- Security failure

۲- برآورد واقع‌گرایانه احتمال بروز نقصیه‌های امنیتی، با در نظر گرفتن تهدیدها و آسیب‌پذیری‌های متداول، و آسیب‌های وابسته به این دارایی‌ها، و کنترل‌هایی که در حال حاضر پیاده‌سازی شده‌اند.

۳- تخمین سطوح ریسک .

۴- تعیین این‌که ریسک در حد قابل قبول هست یا نیازمند بر طرف‌سازی، با استفاده از معیارهای پذیرش ریسک ایجاد شده در۴-۲-۱-پ)۲ است.

ج- شناسایی و ارزیابی گزینه‌هایی برای برطرف‌سازی ریسک .

اقدامات ممکن شامل:

۱- به کار گرفتن کنترل‌های مناسب.

۲- پذیرش ریسک به صورت آگاهانه و هدفمند، مشروط براین‌که به وضوح، خط‌مشی‌های سازمان و معیار پذیرش ریسک را برآورده سازند(به بند۴-۲-۱-پ) ۲ رجوع کنید).

۳- اجتناب از ریسک[1] ، و

۴- انتقال[2] ریسک کسب‌وکار به طرف‌های دیگر، به عنوان مثال بیمه‌گزاران[3]، تامین کنندگان[4].

چ- گزینش اهداف کنترلی و کنترل‌ها برای برطرف‌سازی ریسک .

باید اهداف کنترلی و کنترل‌هایی به منظور برآورده‌سازی الزامات شناسایی شده به‌وسیله برآورد ریسک و فرآیند برطرف‌سازی ریسک ، برگزیده و پیاده‌سازی شوند. این گزینش باید با توجه به معیار پذیرش ریسک (به بند۴-۲-۱-پ-۲ رجوع کنید)، به علاوه الزامات قانونی، آیین‌نامه‌ای و قراردادی صورت پذیرد.

اهداف کنترلی و کنترل‌هایی از پیوست الف باید انتخاب شوند، که به عنوان بخشی از این فرآیند ، الزامات شناسایی شده را به طور مناسب پوشش دهند.

اهداف کنترلی و کنترل‌هایی که در پیوست الف فهرست شده‌اند، فراگیر نبوده و اهداف کنترلی و کنترل‌های اضافی نیز ممکن است انتخاب شوند.

یادآوری- پیوست الف، حاوی فهرست جامعی از اهداف کنترلی و کنترل‌هایی است که به طور معمول در ارتباط با سازمان‌ها یافت می‌شوند. استفاده کنندگان این استاندارد ملی، برای حصول اطمینان از این‌که هیچ گزینه کنترلی مهمی چشم‌پوشی نشده، به عنوان یک نقطه شروع برای انتخاب کنترل، به پیوست الف هدایت شده‌اند.

ح- دریافت مصوبه مدیریت برای ریسک‌های باقیمانده پیشنهاد شده.

خ- دریافت مجوز مدیریت برای پیاده‌سازی و اجرای سیستم مدیریت امنیت اطلاعات.

د- تهیه بیانیه کاربست‌پذیری.

باید یک بیانیه کاربست‌پذیری، شامل موارد ذیل تهیه شود:

۱- اهداف کنترلی و کنترل‌هایی برگزیده از (۴-۲-۱-چ) و دلایل انتخاب آنها.

1- Avoiding risk
2- Transfering
3- Insuerers
4- Suppliers

۲- اهداف کنترلی و کنترل‌هایی که در حال حاضر پیاده‌سازی شده‌اند(به بند۴-۲-۱-ث-۲ رجوع کنید). و
۳- کنارگذاری هر یک از اهداف کنترلی و کنترل‌های پیوست الف و توجیه کنارگذاری آنها.

یادآوری- بیانیه کاربست پذیری، از تصمیمات اتخاذ شده در خصوص برطرف‌سازی ریسک، یک جمع‌بندی ارایه می‌دهد. توجیهات کنارگذاری، بررسی مضاعفی را فراهم می‌کند که هیچ کنترلی، سهواً از قلم نیافتاده باشد.

۴-۲-۲ پیاده‌سازی و اجرای سیستم مدیریت امنیت اطلاعات

سازمان باید موارد ذیل را انجام دهد:

الف- قاعده‌مند کردن[1] یک طرح برطرف‌سازی ریسک، به منظور مدیریت کردن ریسک امنیت اطلاعات، که اقدام مدیریتی مناسب، منابع، مسوولیت‌ها و اولویت‌ها را شناسایی کند(به بند ۵ رجوع کنید).

ب- پیاده‌سازی طرح برطرف‌سازی ریسک به منظور دستیابی به اهداف کنترلی شناسایی شده، که دربرگیرنده ملاحظات مالی و تخصیص نقش‌ها و مسوولیت‌ها باشد.

پ- پیاده‌سازی کنترل‌های برگزیده شده در(۴-۲-۱-چ)، به منظور برآورد سازی اهداف کنترلی.

ت- تعریف چگونگی سنجش اثربخشی کنترل‌ها یا گروهی از کنترل‌های انتخاب شده و تعیین این‌که این اندازه‌گیری‌ها، چگونه برای برآورد اثربخشی کنترل‌ها، به منظور ارایه نتایج قابل قیاس و تجدیدپذیر، مورد استفاده قرار گرفته‌اند(به بند۴-۲-۳-پ) رجوع کنید).

یادآوری- اندازه‌گیری اثربخشی کنترل‌ها، به مدیران و کارکنان اجازه می‌دهد تا تعیین کنند که کنترل‌ها، تا چه اندازه اهداف کنترلی طرح‌ریزی شده را حاصل می‌نمایند.

ث- پیاده‌سازی برنامه‌های آموزشی و آگاه‌سازی(به بند ۵-۲-۲ رجوع کنید).

ج- مدیریت عملیات سیستم مدیریت امنیت اطلاعات.

چ- مدیریت منابع برای سیستم مدیریت امنیت اطلاعات(به بند ۵-۲ رجوع کنید).

ح- پیاده‌سازی روش‌های اجرایی و دیگر کنترل‌هایی که قادر به توانمند شاختن آشکارسازی سریع رخدادهای امنیتی و پاسخ‌دهی و حوادث امنیتی باشند.(به بند۴-۲-۳-الف رجوع کنید).

۴-۲-۳ پایش و بازنگری سیستم مدیریت امنیت اطلاعات

سازمان باید موارد ذیل را انجام دهد:

الف- اجرای روش‌های اجرای پایش و دیگر کنترل‌ها به منظور:
۱- تشخیص سریع خطاها در نتایج پردازش.
۲- شناسایی سریع نقض‌ها و حوادث امنیتی موفق و ناتمام.
۳- قادر ساختن مدیریت در تشخیص این‌که فعالیت‌های امنیتی سپرده شده به افراد یا پیاده‌سازی شده به‌وسیله فن‌آوری اطلاعات، آن‌گونه که انتظار می‌رود، انجام می‌شوند.

1- Formulate

۴- کمک در تشخیص رخدادهای امنیتی و از آن طریق، پیشگیری از حوادث امنیتی به‌وسیله استفاده از نشانگرها[1]، و

۵- تعیین این‌که اقدامات صورت گرفته برای رفع نقض امنیتی، موثر بوده است.

ب- تعهد بازنگری منظم[2] اثربخشی سیستم مدیریت امنیت اطلاعات(شامل برآوردسازی خط‌مشی واهداف سیستم مدیریت امنیت اطلاعات، وبازنگری کنترل‌های امنیتی)، با توجه به نتایج ممیزی‌های امنیتی، حوادث، نتایج اندازه‌گیری‌های اثربخشی، پیشنهادها و بازخورهای تمامی طرف‌های ذینفع.

پ- سنجش اثربخشی کنترل‌ها به منظور تصدیق این‌که الزامات امنیتی، برآورده شده‌اند.

ت- بازنگری برآوردهای ریسک در فواصل زمانی طرح‌ریزی شده و بازنگری ریسک باقیمانده و شناسایی سطح قابل قبول ریسک، با توجه به تغییرات در:

۱- سازمان.

۲- فن‌آوری.

۳- اهداف و فرآیند های کسب وکار.

۴- تهدیدهای شناسایی شده.

۵- اثربخشی کنترل‌های پیاده‌سازی شده، و

۶- رویدادهای برونی همانند تغییرات در فضای قانونی یا آیین‌نامه‌ای[3]، تغییر در تعهدات قراردادی[4]، و تغییرات در شرایط اجتماعی[5].

ث- انجام ممیزی‌های داخلی سیستم مدیریت امنیت اطلاعات در فواصل زمانی طرح‌ریزی شده(به بند ۶ رجوع کنید).

یادآوری- ممیزی‌های داخلی که گاهی اوقات ممیزی شخص اول نامیده می‌شوند، توسط خود سازمان یا به نیابت از سازمان، برای مقاصد داخلی، انجام می‌گیرند.

ج- تعهد به بازنگری مدیریت قاعده‌مند سیستم مدیریت امنیت اطلاعات، به منظور حصول اطمینان از متناسب باقی ماندن دامنه و این‌که بهبودها در فرآیند سیستم مدیریت امنیت اطلاعات، شناسایی شده‌اند.(به بند۷-۱ رجوع کنید).

چ- ه روزآوری[6] طرح‌های امنیتی با در نظر گرفتن یافته‌های فعالیت‌های پایش و بازنگری.

ح- ثبت اقدامات و وقایعی که می‌توانند براثربخشی یا کارآیی سیستم مدیریت امنیت اطلاعات،تاثیر شدید بگذارند.(به بند۴-۳-۳ رجوع کنید).

1- Indicators
2- Regular
3- Legal or regular environment
4- Contactual obligation
5- Social climate
6- Update

۴-۲-۴ نگهداری و بهبود سیستم مدیریت امنیت اطلاعات

سازمان باید به صورت منظم، موارد ذیل را انجام دهد:

الف- پیاده‌سازی بهبودهای شناسایی شده در سیستم مدیریت امنیت اطلاعات.

ب- انجام اقدامات اصلاحی و پیشگیرانه مناسب، مطابق با بندهای ۸-۲و ۸-۳. ه کار بستن دروس آموخته شده از تجارب امنیتی دیگر سازمان‌ها و خود سازمان.

پ- انتقال اطلاعات مربوط به اقدامات و بهبودها، به تمامی طرف‌های ذینفع، یا سطحی از جزئیات مناسب با شرایط محیطی و در صورت لزوم، توافق در مورد چگونگی ادامه کار.

ت- اطمینان از این‌که بهبودها، اهداف مورد نظرشان را حاصل می‌کنند.

۴-۳ الزامات مستندسازی

۴-۳-۱ کلیات

مستندسازی باید شامل سوابق تصمیمات مدیریتی بوده، اطمینان دهد که اقدامات، قابل ردیابی تا تصمیمات مدیریتی وخط‌مشی ها هستند، وازاین‌که نتایج ثبت شده، تجدیدپذیر هستند، اطمینان حاصل نمایند.

مهم است که بتوان ارتباط بین کنترل‌های انتخاب شده و نتایج حاصل از برآورد و ریسک و فرآیند برطرف‌سازی ریسک ، و متعاقباً ارتباط با اهداف و خط‌مشی سیستم مدیریت امنیت اطلاعات را نشان داد.

مستندسازی سیستم مدیریت امنیت اطلاعات باید شامل موارد ذیل باشد:

الف- بیانیه مدون شده خط‌مشی سیستم مدیریت امنیت اطلاعات(به بند۴-۲-۱-ب رجوع کنید) و اهداف.

ب- دامنه سیستم مدیریت امنیت اطلاعات(به بند ۴-۲-۱-الف رجوع کنید).

پ- روش‌های اجرایی و کنترل‌هایی در پشتیبانی از سیستم مدیریت امنیت اطلاعات.

ت- تشریح روش‌شناسی برآورد ریسک (به بند ۴-۲-۱-ج رجوع کنید).

ث- گزارش برآورد ریسک (به بند ۴-۲-۱-ج تا ۴-۲-۱- ز رجوع کنید).

ج- طرح برطرف‌سازی ریسک (به بند ۴-۲-۱-ب رجوع کنید).

چ- روش‌های اجرایی مدون شده مورد نیاز سازمان، برای حصول اطمینان از موثربودن طرح‌ریزی، اجرا و کنترل فرآیند های امنیت اطلاعات و تشریح چگونگی سنجش اثربخشی کنترل‌ها(به بند ۴-۲-۳-ج) مراجعه شود).

ح- سوابقی که توسط این استاندارد ملی الزام شده‌اند(به بند ۴-۳-۳ رجوع کنید)،و

خ- بیانیه کاربست‌پذیری.

یادآوری۱- در این استاندارد ملی، آنجا که از عبارت «روش اجرایی مدون[1]» استفاده می‌شود، منظور روش اجرایی است که ایجاد شده، مدون گشته، پیاده‌سازی شده و نگهداری می‌شود.

1- Documented

یادآوری۲- گستره مدون سازی سیستم مدیریت امنیت اطلاعات، از یک سازمان تا سازمان دیگر، می‌تواند به دلایل ذیل متفاوت باشد:

- اندازه سازمان و نوع فعالیت‌های آن، و
- دامنه پیچیدگی الزامات امنیتی و سیستمی که تحت مدیریت قرار دارد.

یادآوری۳- مدارک و سوابق می‌توانند در هر شکل یا نوعی از واسطه‌های اطلاعاتی باشند.

۴-۳-۲ کنترل مدارک

مدارکی که در سیستم مدیریت امنیت اطلاعات الزام شده‌اند، باید حفاظت شده و تحت کنترل باشند. یک روش اجرایی مدون برای تعریف اقدامات مدیریتی مورد نیاز ذیل، باید ایجاد شود:

الف- تصویب مدارک از نظر تناسب آنها، پیش از انتظار.

ب- بازنگری و به‌روزآوری مدارک، برحسب نیاز، و تصویب مجدد مدارک.

پ- حصول اطمینان از این‌که تغییرات و وضعیت ویرایش جاری مدارک، مشخص شده‌اند.

ت- حصول اطمینان از این‌که ویرایش‌های معتبر مدارک قابل اجرا، در مکان استفاده، در دسترس هستند.

ث- حصول اطمینان از این‌که مدارک خوانا، و به سهولت قابل تشخیص باقی می مانند.

ج- حصول اطمینان از این‌که مدارک در دسترس کسانی است که به آنها نیاز دارند، و با توجه به روش‌های اجرایی بکار گرفته شده برای طبقه‌بندی آنها، منتقل، ذخیره و نهایتاً امحاء[1] می‌شوند.

چ- حصول اطمینان از این‌که مدارک با منشاء برون سازمانی، شناسایی شده‌اند.

ح- حصول اطمینان از این‌که توزیع مدارک، تحت کنترل است.

ط- پیشگیری از استفاده ناخواسته از مدارک منسوخ، و

ی- در صورتیکه به هر دلیلی گردآوری شوند، به نحو مناسبی مورد شناسایی قرار می‌گیرند.

۴-۳-۳ کنترل سوابق

سوابق باید ایجاد و نگهداری شده تا شواهد انطباق با الزامات و نیز اجرای موثر سیستم مدیریت امنیت اطلاعات، فراهم شود. آنها باید محافظت شده و تحت کنترل باشند. سیستم مدیریت امنیت اطلاعات باید به تمامی الزامات قانونی یا آیین‌نامه‌ای و تعهدات قراردادی مرتبط، توجه داشته باشد. سوابق باید خوانا و به سهولت قابل شناسایی و بازیابی باقی بمانند. کنترل‌های مورد نیاز شناسایی، انبارش، حفاظت، بازیابی، مدت نگهداری و امحای سوابق، باید مدون و پیاده‌سازی شوند.

سوابق کارآیی فرآیندها، آن‌گونه که در بند ۴-۲ طرح شده و کلیه حوادث امنیتی بارز مرتبط با سیستم مدیریت امنیت اطلاعات، باید نگهداری شوند.

مثال :

دفتر بازدید کنندگان، گزارش‌های ممیزی و فرم‌های تکمیل شده مجازسازی دسترسی، مثال‌هایی از سوابق هستند.

1- Dispose

۵ مسوولیت مدیریت

۵-۱ تعهد مدیریت

مدیریت باید شواهدی مبنی بر تعهد وی نسبت به ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات را از طریق موارد ذیل فراهم آورد:

الف- ایجاد یک خط‌مشی سیستم مدیریت امنیت اطلاعات.

ب- حصول اطمینان از این‌که اهداف و طرح‌های سیستم مدیریت امنیت اطلاعات، ایجاد شده‌اند.

پ- ایجاد نقش‌ها و مسوولیت‌ها برای امنیت اطلاعات.

ت- ارایه اطلاعات لازم به سازمان درباره اهمیت برآورده‌سازی اهداف امنیت اطلاعات و تطابق با خط‌مشی امنیت اطلاعات، مسوولیت‌هایش در قبال قانون و نیاز به بهبود مستمر.

ث- فراهم‌آوری منابع کافی برای ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات(به بند ۵-۲-۱ رجوع کنید).

ج- تصمیم‌گیری درباره معیاری برای پذیرش ریسک و سطوح قابل قبول ریسک .

چ- حصول اطمینان از این‌که ممیزی‌های داخلی سیستم مدیریت امنیت اطلاعات، انجام می‌شوند (به بند ۶ رجوع کنید)، و

ح- انجام بازنگری‌های مدیریت سیستم مدیریت امنیت اطلاعات (به بند ۷ رجوع کنید).

۵-۲ مدیریت منابع

۵-۲-۱ فراهم‌آوری منابع

سازمان باید منابع لازم برای موارد ذیل را تعیین و فراهم نماید:

الف- ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات.

ب- حصول اطمینان از این‌که روش‌های اجرایی امنیت اطلاعات، الزامات کسب وکار را پشتیبانی می‌کنند.

پ- شناسایی و نشان‌دهی الزامات قانونی و آیین‌نامه‌ای و تعهدات امنیتی قراردادی.

ت- نگهداری امنیت در سطح مناسب، از طریق بکارگیری صحیح تمامی کنترل‌های پیاده‌سازی شده.

ث- انجام بازنگری‌ها در صورت لزوم و واکنش مناسب به نتایج این بازنگری‌ها، و

ج- آنجا که لازم است، بهبود اثربخشی سیستم مدیریت امنیت اطلاعات.

۵-۲-۲ آموزش، آگاه‌سازی و صلاحیت

سازمان باید از طریق موارد ذیل اطمینان حاصل نماید که تمام کارکنانی که مسوولیت‌هایی در سیستم مدیریت امنیت اطلاعات به آنها محول شده، صلاحیت انجام کارهای لازم را دارند:

الف- تعیین صلاحیت‌های لازم برای کارکنانی که کارهای تاثیرگذار بر سیستم مدیریت امنیت اطلاعات انجام می‌دهند.

ب- فراهم‌آوری آموزش یا انجام فعالیت‌های دیگر (همانند استخدام افراد شایسته) به منظور برآورده‌سازی این نیازها.

پ- ارزیابی اثربخشی اقدامات انجام شده، و

ت- نگهداری سوابق مربوط به تحصیلات، آموزش، مهارت‌ها، تجارب و شایستگی‌ها (به بند ۴-۳-۳ رجوع کنید).

سازمان همچنین باید اطمینان حاصل نماید که تمامی کارکنان مرتبط، نسبت به ارتباط و اهمیت فعالیت‌های امنیت اطلاعات خود و نحوه مشارکت در دستیابی به اهداف سیستم مدیریت امنیت اطلاعات، آگاه هستند.

۶ ممیزی داخلی سیستم مدیریت امنیت اطلاعات

سازمان باید ممیزی‌های داخلی سیستم امنیت اطلاعات را در فواصل زمانی طرح‌ریزی شده انجام دهد تا معین کند که آیا اهداف کنترلی، کنترل‌ها، فرآیند ها و روش‌های اجرایی سیستم مدیریت امنیت اطلاعات:

الف- با الزامات این استاندارد و مقررات و قوانین مرتبط انطباق دارند.

ب- با الزامات شناسایی شده امنیت اطلاعات، انطباق دارند.

پ- به طرز اثربخشی پیاده‌سازی شده و نگهداری می‌شوند، و

ت- آن‌گونه که انتظار می‌رود، اجرا می‌شوند.

یک برنامه ممیزی، با در نظر گرفتن وضعیت و اهمیت فرآیند ها و حیطه‌های مورد ممیزی و همچنین نتایج ممیزی‌های قبلی، باید طرح‌ریزی شود. معیار، دامنه، تواتر[1] و روش‌های ممیزی باید تعریف شوند. انتخاب ممیزان و انجام ممیزی‌ها، باید واقع‌بینی[2] و بی‌طرفی[3] فرآیند ممیزی را تضمین نماید. ممیزان نباید کار خودشان را ممیزی نمایند.

مسوولیت‌ها و الزامات برای طرح‌ریزی و انجام ممیزی‌ها، وگزارش نتایج و نگهداری سوابق (به بند ۴-۳- ۳ رجوع کنید)، باید در یک روش اجرایی مدون تعریف شده باشند.

مدیر مسوول حیطه‌ای که مورد ممیزی قرار می‌گیرد، باید از این بابت که اقدامات لازم برای رفع عدم انطباق‌های یافته شده و علل آنها، بدون تاخیر بی‌مورد انجام می‌شوند، اطمینان حاصل نماید. فعالیت‌های پیگیری[4] باید شامل تصدیق اقدامات انجام شده و گزارش‌دهی نتایج تصدیق باشد. (به بند ۸ رجوع کنید).

یادآوری- استاندارد ملی ایران ایزو ۱۹۰۱۱: سال ۱۳۸۶[5] (رهنمودهایی[6] برای ممیزی سیستم‌های مدیریت کیفیت و/ یا زیست محیطی)، می‌تواند راهنمای مفیدی برای اجرای ممیزی‌های داخلی فراهم نماید.

1- Frequency
2- Objectivity
3- Impartiality
4- Follow-up Activities

۵- منظور استاندارد ملی معادل استاندارد بین المللی ISO 19011:2002 می باشد.

6- Guidelines

۷ بازنگری مدیریت سیستم مدیریت امنیت اطلاعات

۷-۱ کلیات

مدیریت باید مدیریت امنیت اطلاعات سازمان در فواصل زمانی طرح‌ریزی شده(حداقل یک بار درسال)، مورد بازنگری قرار دهد تا از تداوم تناسب، کفایت و اثربخشی آن، اطمینان حاصل نماید. این بازنگری باید بررسی موقعیت‌های بهبود ونیاز به اعمال تغییرات در سیستم مدیریت امنیت اطلاعات، از جمله خط‌مشی و اهداف امنیت اطلاعات را شامل شود. نتایج بازنگری‌ها باید به وضوح مدون شده و سوابق آن نگهداری شوند (به بند ۴-۳-۳ رجوع کنید).

۷-۲ ورودی‌های بازنگری

ورودی‌های بازنگری مدیریت، باید شامل موارد ذیل باشند:

الف- نتایج ممیزی‌ها و بازنگری‌های سیستم مدیریت امنیت اطلاعات.

ب- بازخورهای طرف‌های ذینفع.

پ- فنون، محصولات یا روش‌های اجرایی که می‌توانند برای بهبود اثربخشی و کارآیی سیستم مدیریت امنیت اطلاعات در سازمان، مورد استفاده قرار گیرند.

ت- وضعیت اقدامات اصلاحی و پیشگیرانه.

ث- آسیب‌پذیری‌ها یا تهدیداتی که در برآورد ریسک قبلی، به طور مناسب نشانی‌دهی نشده‌اند.

ج- نتایج حاصل از اندازه‌گیری‌های اثربخشی.

چ- اقدامات پیگیرانه از بازنگری‌های قبلی مدیریت.

ح- کلیه تغییراتی که می‌توانند سیستم مدیریت امنیت اطلاعات را تحت تاثیر قرار دهند، و

خ- توصیه‌هایی برای بهبود.

۷-۳ خروجی‌های بازنگری

خروجی‌های بازنگری مدیریت، باید دربرگیرنده تمامی تصمیمات و اقدامات مربوط به موارد ذیل باشد.

الف- بهبود اثربخشی سیستم مدیریت اطلاعات.

ب- ه روزآوری برآورد ریسک و طرح‌های برطرف‌سازی ریسک.

پ- اصلاح روش‌های اجرایی و کنترل‌هایی که برامنیت اطلاعات اثر می‌گذارند، در صورت لزوم پاسخ به رویدادهای درونی و بیرونی که ممکن است به سیستم مدیریت امنیت اطلاعات آسیب برسانند، شامل تغییرات در موارد ذیل:

۱- الزامات کسب وکار.

۲- الزامات امنیتی.

۳- فرآیند های کسب وکار موثر در الزامات موجود در کسب وکار.

۴- الزامات آیین‌نامه‌ای یا قانونی.

۵- تعهدات قراردادی، و

۶- سطوح ریسک و/ یا معیاری برای پذیرش ریسک.

ت- نیاز به منافع.
ث- بهبود این‌که چگونه اثر بخشی کنترل‌ها اندازه‌گیری شده‌اند.

۸ بهبود سیستم مدیریت امنیت اطلاعات

۸-۱ بهبود مستمر

سازمان باید بطور مستمر، اثربخشی سیستم مدیریت امنیت اطلاعات را از طریق بکارگیری خط‌مشی امنیت اطلاعات، اهداف امنیت اطلاعات، نتایج ممیزی، تجزیه و تحلیل رویدادهای پایش شده، اقدامات اصلاحی و پیشگیرانه و بازنگری مدیریت، بهبود بخشد (به بند۷ رجوع کنید).

۸-۲ اقدام اصلاحی

سازمان باید اقدامی را برای رفع علت عدم انطباق‌ها با الزامات سیستم مدیریت امنیت اطلاعات، به منظور پیشگیری از رخداد مجدد آنها، به عمل آورد. روش‌اجرایی مدون برای اقدام اصلاحی، باید الزامات ذیل را تعریف نمایند:
الف- شناسایی عدم انطباق‌ها.
ب- تعیین علل عدم انطباق‌ها.
پ- ارزیابی نیاز به اقداماتی که اطمینان دهند، عدم انطباق‌ها، دوباره رخ نمی‌دهند.
ت- تعیین و انجام اقدام اصلاحی مورد نیاز.
ث- ثبت سوابق نتایج اقدام انجام شده(به بند۴-۳-۳ رجوع کنید)، و
ج- بازنگری اقدام اصلاحی انجام شده.

۸-۳ اقدام پیشگیرانه

سازمان باید اقدامی را برای رفع علت عدم انطباق‌های بالقوه با الزامات سیستم مدیریت امنیت اطلاعات، به منظور پیشگیری از رخداد آنها، تعیین کند. اقدامات پیشگیرانه باید متناسب با تاثیر مشکلات بالقوه باشند.
روش اجرایی مدون برای اقدام پیشگیرانه، باید الزامات ذیل را تعریف نماید:
الف- شناسایی عدم انطباق‌های بالقوه و علل آنها.
ب- ارزیابی نیاز به اقدامی که از رخداد عدم انطباق‌ها، پیشگیری می‌کند.
پ- تعیین و پیاده‌سازی اقدام پیشگیرانه مورد نیاز.
ت- ثبت سوابق نتایج اقدام انجام شده(به بند۴-۳-۳ رجوع کنید)، و
ث- بازنگری اقدام پیشگیرانه انجام شده.
سازمان باید ریسک تغییر یافته و الزامات اقدام پیشگیرانه معطوف به ریسکی که به صورت بارز تغییر یافته‌اند را شناسایی نماید.
اولویت اقدامات پیشگیرانه باید براساس نتایج برآورد ریسک تعیین شود.

یادآوری- اقدام برای پیشگیری از عدم انطباق، اغلب با ارزش‌تر و موثرتر از اقدام اصلاحی است.

پیوست الف

(الزامی)

اهداف کنترلی و کنترل‌ها

اهداف کنترلی و کنترل‌های فهرست شده در جدول الف-۱ به طور مستقیم از بندهای ۵ تا ۱۵ استاندارد ISO/IEC 17799:2005 و منطبق با آنها برگرفته شده است. موارد فهرست شده در جدول الف-۱ فراگیر نبوده و سازمان می‌تواند اهداف کنترلی و کنترل‌های اضافی مورد نیازش را لحاظ نماید. اهداف کنترلی و کنترل‌های مندرج در این جدول، باید به عنوان بخشی از فرآیند سیستم مدیریت امنیت اطلاعات مشخص شده در بند ۴-۲-۱ انتخاب شوند.

بندهای ۵ تا ۱۵ استاندارد ISO/IEC 17799:2005 توصیه و رهنمودهایی برای پیاده سازی براساس بهترین تجارب در پشتیبانی از کنترل‌های الف-۵ الی الف-۱۵ فراهم آورده است.

جدول الف-۱- اهداف کنترلی

الف-۵ خط‌مشی امنیتی		
الف-۵-۱ خط‌مشی امنیتی		
هدف: فراهم آوری جهت گیری و حمایت مدیریت برای امنیت اطلاعات با توجه به الزامات کسب‌وکار و قوانین و آیین‌نامه‌های مرتبط.		
الف-۵-۱-۱	سند خط‌مشی امنیت اطلاعات	*کنترل* یک سند خط‌مشی امنیت اطلاعات، باید توسط مدیریت تصویب، و منتشر و به اطلاع همه کارکنان و طرف های مرتبط بیرونی برسد.
الف-۵-۱-۲	بازنگری خط‌مشی امنیت اطلاعات	*کنترل* خط‌مشی امنیت اطلاعات، باید در فواصل زمانی طرح‌ریزی شده یا در صورتیکه تغییرات بارزی رخ دهد، به منظور حصول اطمینان از تداوم تناسب، کفایت و اثربخشی آن، بازنگری شود.
الف-۶ سازمان امنیت اطلاعات		
الف-۶-۱ سازمان داخلی		
هدف: مدیریت کردن امنیت اطلاعات در درون سازمان.		
الف-۶-۱-۱	تعهد مدیریت به امنیت اطلاعات	*کنترل* مدیریت باید فعالانه، امنیت را در درون سازمان از طریق جهت گیری شفاف، تعهد اثبات شده، مکلف کردن به صورت صریح و اعلام مسوولیت های امنیت اطلاعات، حمایت نماید.
الف-۶-۱-۲	هماهنگی امنیت اطلاعات	*کنترل* فعالیت های امنیت اطلاعات، باید توسط نمایندگانی از بخش های مختلف سازمانی با نقش ها و کارکردهای شغلی مرتبط، هماهنگ شوند.

جدول الف-۱-ادامه

الف-۶-۱-۳	تخصیص مسوولیت های امنیت اطلاعات	*کنترل* تمامی مسوولیت‌های امنیت اطلاعات، باید به وضوح تعریف شوند.
الف-۶-۱-۴	فرآیند مجاز سازی[1] برای امکانات پردازش اطلاعات	*کنترل* یک فرآیند مجازسازی مدیریتی برای امکانات جدید پردازش اطلاعات باید تعریف و پیاده سازی شود.
الف-۶-۱-۵	توافق‌نامه‌های محرمانگی[2]	*کنترل* الزاماتی برای توافق‌نامه‌های محرمانگی یا عدم افشاء که منعکس کننده نیازهای سازمان به حفاظت از اطلاعات می باشد، باید شناسایی و به طور منظم بازنگری شود.
الف-۶-۱-۶	برقراری ارتباط با اولیای امور[3]	*کنترل* باید ارتباطات مناسبی با اولیای امور مرتبط، برقرار و حفظ شود.
الف-۶-۱-۷	برقراری ارتباط با گروه های دارای گرایش خاص	*کنترل* باید ارتباطات مناسبی با گروه های دارای گرایش خاص یا سایر انجمن های امنیتی متخصص و انجمن های حرفه ای، برقرار و حفظ شود.
الف-۶-۱-۸	بازنگری مستقل امنیت اطلاعات	*کنترل* رویکرد سازمان به مدیریت امنیت اطلاعات و پیاده سازی آن (به عنوان مثال اهداف کنترلی،کنترل‌ها،خط‌مشی ها، فرآیند ها و روش های اجرایی امنیت اطلاعات) ، باید در فواصل زمانی طرح‌ریزی شده یا هنگامی‌که تغییرات عمده ای در پیاده سازی امنیت اطلاعات رخ دهد، مستقلاً بازنگری شود.
الف-۶-۲ طرف های بیرونی *هدف:* حفظ و نگهداری امنیت اطلاعات وامکانات پردازش اطلاعات سازمان که در دسترس طرف های بیرونی قرار داشته یا توسط ایشان پردازش یا مدیریت شده یا با آنها مبادله می‌شوند.		
الف-۶-۲-۱	شناسایی ریسک مرتبط با طرف های بیرونی	*کنترل* ریسک اطلاعات و امکانات پردازش اطلاعات سازمان ناشی از فرآیند های کسب‌وکار مرتبط با طرف های بیرونی، باید پیش از اعطای دسترسی، شناسایی شده و کنترل های مناسب، پیاده سازی شوند.
الف-۶-۲-۲	نشانی دهی[4] امنیت هنگام سرو کار داشتن با مشتریان	*کنترل* تمام الزامات امنیتی شناسایی شده، پیش از اعطای دسترسی اطلاعات یا اموال سازمان به مشتری، باید نشانی دهی شوند.
الف-۶-۲-۳	نشانی دهی امنیت در توافق‌نامه‌های طرف ثالث[5]	*کنترل* توافق‌نامه‌های منعقده با اشخاص ثالثی که با اعطای دسترسی، پردازش کردن، تبادل یا مدیریت کردن اطلاعات یا امکانات پردازش اطلاعات سازمان، یا اضافه کردن محصولات یا خدمات به امکانات پردازش اطلاعات، سرو کار دارند، باید تمامی الزامات امنیتی مرتبط را پوشش دهند.

جدول الف-۱-ادامه

1- Best practices
2- Confidentiality agreement
3- Authorities
4- Addressing
5- Third Party

الف-۷ مدیریت دارایی		
الف-۷-۱ مسوولیت دارایی ها		
هدف: دستیابی و نگهداری حفاظت مناسب از دارایی های سازمانی.		
الف-۷-۱-۱	لیست[1] اموال	*کنترل* تمامی دارایی ها باید به وضوح شناسایی شده و سیاهه‌ای از تمام دارایی های مهم، تنظیم و نگهداری شود.
الف-۷-۱-۲	مالکیت دارایی ها	*کنترل* تمامی اطلاعات و دارایی ها مرتبط با امکانات پردازش اطلاعات، باید در تملک بخش معینی از سازمان باشد.
الف-۷-۱-۳	استفاده پسندیده از دارایی ها	*کنترل* باید قواعدی برای استفاده پسندیده از اطلاعات و دارایی های مرتبط با امکانات پردازش اطلاعات، شناسایی، مدون و پیاده سازی شوند.
الف-۷-۲ طبقه‌بندی اطلاعات		
هدف: حصول اطمینان از این‌که اطلاعات، به سطح حفاظتی مناسبی رسیده اند.		
الف-۷-۲-۱	خطوط راهنمای طبقه‌بندی	*کنترل* اطلاعات باید با توجه به ارزش آن،الزامات قانونی، حساسیت و بحرانی بودن برای سازمان، طبقه‌بندی شوند.
الف-۷-۲-۲	برچسب گذاری[2] و اداره کردن اطلاعات	*کنترل* برای علامت گذاری و اداره کردن اطلاعات، باید مجموعه مناسبی از روش های اجرایی با توجه به طرح طبقه‌بندی پذیرفته شده سازمان،ایجاد و پیاده سازی شوند.
الف-۸ امنیت منابع انسانی		
الف-۸-۱ پیش از اشتغال[3]		
مقصود: حصول اطمینان از این‌که کارکنان، پیمانکاران و کاربران طرف ثالث، مسوولیت هایشان را درک کرده و برای نقش های در نظر گرفته شده برای ایشان مناسب هستند، و به منظور کاهش ریسک سرقت، سوء استفاده یا استفاده نابجا از امکانات.		
الف-۸-۱-۱	نقش ها و مسوولیت ها	*کنترل* نقش ها و مسوولیت های امنیتی کارکنان، پیمانکاران و کاربران طرف ثالث، باید با توجه به خط‌مشی امنیت اطلاعات سازمان، تعریف و مدون شوند.
الف-۸-۱-۲	گزینش[4]	*کنترل* برای تصدیق سوابق تمامی داوطلبین استخدام، پیمانکاران، و کاربران طرف ثالث، باید بررسی هایی با توجه به قوانین، آیین‌نامه ها و اصول اخلاقی مرتب، و متناسب با الزامات کسب‌وکار،طبقه‌بندی اطلاعاتی که در دسترس قرار می گیرند و ریسک دیده شده، انجام شوند.

جدول الف-۱-ادامه

1- Inventory
2- Labeling
۳- توضیح: واژه اشتغال در اینجا معنای تمامی موارد مختلف ذیل را پوشش می دهد: استخدام کارکنان (موقت یا بلند مدت)، انتصاب نقشهای شغلی، تغییر نقشهای شغلی، تفویض قراردادها و خاتمه هر کدام از این توافقات.
4- Screening

الف-۸-۱-۳	ضوابط و شرایط استخدام	*کنترل* کارکنان، پیمانکاران و کاربران طرف ثالث، باید به عنوان بخشی از تعهد قراردادی شان، شرایط و ضوابط قراداد استخدامیشان را کـه بایـد بـیـانگر مسـوولیت هـای ایشان و سازمان در قبال امنیت اطلاعات باشد، قبول و امضاء نمایند.
الف-۸-۲ حین خدمت		
هدف: حصول اطمینان از این‌که تمامی کارکنان، پیمانکاران و کاربران طرف ثالث، از تهدید ها و نگرانی های امنیت اطلاعات، مسوولیت ها و تعهداتشان آگاه بوده و در انجام کارهای روزمره خود و به منظور کاهش ریسک ناشی از خطای انسانی، برای پشتیبانی از خط‌مشی امنیتی سازمان، آماده شده اند.		
الف-۸-۲-۱	مسوولیت های مدیریت	*کنترل* مدیریت باید کارکنان، پیمانکاران کاربران طرف ثالث را به بکارگیری امنیـت، بـا توجه به خط‌مشی ها و روش های اجرایی ایجاد شده سازمان ، الزام نماید.
الف-۸-۲-۲	آگاه سازی، تحصیل و آموزش امنیت اطلاعات	*کنترل* تمامی کارکنان سازمان و در صورت لزوم، پیمانکاران و کاربران طرف ثالث، آنجـا که به کارکرد شغلی ایشان مرتبط باشد، باید در خصوص خـط‌مشـی هـا و روش های اجرایی سازمان، به صورت مناسب، آموزش آگاه سازانه دیده و به طور منظم، به‌روز شوند.
الف-۸-۲-۳	فرآیند انضباطی	*کنترل* یک فرآیند انضباطی رسمی، باید بـرای کارکنـان کـه مرتکـب یـک نقـض امنیتی می‌شوند، وجود داشته باشد.
الف-۸-۳ خاتمه استخدام یا تغییر در شغل		
هدف: حصول اطمینان از این‌که کارکنان، پیمانکاران و کاربران طرف ثالث، به روشی ضابطه مند[1] سازمان را ترک یا تغییر شغل می دهند.		
الف-۸-۳-۱	مسوولیت های خاتمه خدمت	*کنترل* برای خاتمه دادن به خدمت یا تغییر شغل، باید مسوولیت هایی به وضـوح تعریـف و تخصیص داده شوند.
الف-۸-۳-۲	عودت دارایی ها	*کنترل* تمامی کارکنان، پیمانکاران و کاربران طرف ثالث، باید تمامی دارایی های سازمان را که در اختیارشان می باشد، به محض خاتمه استخدام، قـرارداد یـا توافـق‌نامـه شان، به سازمان عودت دهند.
الف-۸-۳-۳	حذف حقوق دسترسی	*کنترل* حقوق دسترسی تمامی کارکنان، پیمانکاران و کاربران طرف ثالث به اطلاعات و امکانات پردازش اطلاعات، باید به محض خاتمه استخدام، قرارداد یا توافق‌نامه‌شان، حذف شده یا به محض تغییر شغل، تنظیم شود.

جدول الف-۱-ادامه

الف-۹ امنیت فیزیکی و محیطی

1- Orderly manner

الف-۹-۱ نواحی امن		
هدف: پیشگیری از دسترسی فیزیکی غیر مجاز، خسارت و تعارض به ابنیه[1] و اطلاعات سازمان.		
الف-۹-۱-۱	حصار امنیت فیزیکی	*کنترل* حصارهای امنیتی (موانعی از قبیل دیوارها، درهای ورودی کنترل شده با کارت یا میزهای پذیرش با خدمه) باید برای حفاظت نواحی حاوی اطلاعات و امکانات پردازش اطلاعات، استفاده شوند.
الف-۹-۱-۲	کنترل های مداخل فیزیکی	*کنترل* نواحی امن، به منظور حصول اطمینان از این‌که فقط کارکنان مجاز، اجازه دسترسی دارند، باید توسط کنترل های ورودی مناسب، حفاظت شوند.
الف-۹-۱-۳	امن سازی دفاتر، اتاق ها و امکانات	*کنترل* امنیت فیزیکی برای دفاتر، اتاق ها و امکانات، باید طراحی و بکار گرفته شود.
الف-۹-۱-۴	محافظت در برابر تهدیدهای بیرونی و محیطی	*کنترل* برای مقابله با خسارت ناشی ازآتش، سیل، زمین لرزه، انفجار، آشوب داخلی، و شکل های دیگری از حوادث طبیعی یا مصنوعی، باید حفاظت فیزیکی طراحی و بکار گرفته شود.
الف-۹-۱-۵	کار در نواحی امن	*کنترل* برای کار در نواحی امن، باید حفاظت فیزیکی و خطوط راهنما، طراحی و بکار گرفته شوند.
الف-۹-۱-۶	دسترسی عمومی، نواحی تحویل و بارگیری	*کنترل* نقاط دسترسی از قبیل نواحی تحویل و بارگیری و سایر نقاطی که افراد غیر مجاز ممکن است وارد ساختمان ها شوند، باید تحت کنترل قرار گرفته و در صورت امکان، برای جلوگیری از دسترسی غیر مجاز، از امکانات پردازش اطلاعات،مجزا شوند.
الف-۹-۲ امنیت تجهیزات		
هدف: پیشگیری از اتلاف، زیان، سرقت یا به خطر افتادن دارایی ها و ایجاد وقفه در فعالیت های سازمان.		
الف-۹-۲-۱	استقرار و حفاظت تجهیزات	*کنترل* تجهیزات باید (در مکان مناسب) مستقر یا محافظت شوند تا ریسک ناشب از تهدیدها و خطرات محیطی و فرصت های دسترسی غیر مجاز، کاهش یابند.
الف-۹-۲-۲	امکانات پشتیبانی[2]	*کنترل* تجهیزات باید در برابر قطع برق و سایر اختلالات ناشی از نقص‌های امکانات پشتیبانی، محافظت شوند.
الف-۹-۲-۳	امنیت کابل کشی	*کنترل* کابل کشی های برق و ارتباطات مورد استفاده برای انتقال داده یا پشتیبانی از خدمات اطلاعاتی، باید در برابر قطع شدن یا وارد آمدن خسارت، محافظت شوند.

جدول الف-۱-ادامه

الف-۹-۲-۴	نگهداری تجهیزات	*کنترل* تجهیزات باید به منظور حصول اطمینان از تداوم دسترس پذیری و

1- Premises
2- Supporting utilities

		یکپارچگی‌شان، به درستی نگهداری شوند.
الف-۹-۲-۵	امنیت تجهیزات خارج از ابینه	*کنترل* برای تجهیزات خارج از محوطه، باید با توجه به ریسک ناشی از انجام کار در خارج از ابینه های سازمان، امن ت برقرار شود.
الف-۹-۲-۶	امحاء یا استفاده مجدد از تجهیزات به صورت امن	*کنترل* تمام اجزای تجهیزاتی که دارای رسانه ذخیره سازی می باشند، باید به منظور حصول اطمینان از این‌که هر داده حساس و نرم افزاری دارای حق امتیاز، پیش از امحاء حذف شده یا به شیوه امنی جانویسی شده[1]، بررسی شوند.
الف-۹-۲-۷	خروج دارایی	*کنترل* تجهیزات، اطلاعات یا نرم افزار، نباید بدون مجوز قبلی، از محوطه خارج شوند.
الف-۱۰ مدیریت ارتباطات و عملیات		
الف-۱۰-۱ روش های اجرایی عملیاتی و مسوولیت ها		
هدف: حصول اطمینان از کارکرد صحیح و امن امکانات پردازش اطلاعات.		
الف-۱۰-۱-۱	روش های اجرایی عملیاتی مدون	*کنترل* روش های عملیاتی، باید مدون شده، نگهداری شوند و در دسترس تمام کاربرانی که به آنها نیاز دارند، قرار بگیرند.
الف-۱۰-۱-۲	مدیریت تغییر	*کنترل* تغییر در امکانات و سیستم‌های پردازش اطلاعات، باید تحت کنترل باشد.
الف-۱۰-۱-۳	تفکیک وظایف	*کنترل* به منظور کاهش فرصت های دستکاری[2] غیر عمد یا غیر مجاز، یا استفاده نابجا از دارایی های سازمان، باید وظایف و حدود مسوولیت‌ها، تفکیک شوند.
الف-۱۰-۱-۴	جداسازی امکانات توسعه، آزمایش و اجرا	*کنترل* امکانات توسعه، آزمایش و اجرا، باید به منظور کاهش ریسک ناشی از دسترسی غیر مجاز یا تغییرات در سیستم عملیاتی تفکیک شوند.
الف-۱۰-۲ مدیریت تحویل خدمت طرف ثالث		
هدف: پیاده سازی و نگهداری سطح مناسب امنیت اطلاعات و تحویل خدمت، در راستای توافق‌نامه‌های تحویل خدمت طرف ثالث.		
الف-۱۰-۲-۱	تحویل خدمت	*کنترل* باید اطمینان حاصل شود که کنترل های امنیتی، تعاریف خدمت و سطوح تحویل مندرج در توافق‌نامه تحویل خدمت طرف ثالث، پیاده سازی و اجرا شده و توسط طرف ثالث نگهداری می‌شوند.

جدول الف-۱-ادامه

الف-۱۰-۲-۲	پایش و بازنگری خدمات طرف ثالث	*کنترل* خدمات، گزارش ها و سوابق تهیه شده توسط طرف ثالث، باید به صورت منظم

1- Overwritten
2- Modification

		پایش و بازنگری شده، و مم زی ها باید به صورت منظم انجام شوند.
الف-۱۰-۲-۳	مدیریت تغییرات در خدمات طرف ثالث	*کنترل* تغییرات در ارایه خدمات، شامل نگهداری و بهبود خط‌مشی های امنیت اطلاعات، روش های اجرایی و کنترل های موجود، باید با توجه به میزان بحرانی بودن سیستم‌های کسب‌وکار و فرآیند های مرتبط و برآورد مجدد ریسک ، مدیریت شوند.
الف-۱۰-۳ طرح‌ریزی و پذیرش سیستم		
هدف: کمینه کردن ریسک ناشی از نقائص سیستم‌ها.		
الف-۱۰-۳-۱	مدیریت ظرفیت	*کنترل* استفاده از منابع باید پایش شده،تنظیم شده، و ظرفیت مورد نیاز در آینده به گونه ای پیش‌بینی شود که از کارآیی مورد نیاز سیستم، اطمینان حاصل شود.
الف-۱۰-۳-۲	پذیرش سیستم	*کنترل* معیار پذیرش سیستم‌های اطلاعاتی جدید، ویرایش های ارتقاء یافته و جدید، باید ایجاد شده و در حین توسعه و پیش از پذیرش سیستم، آزمایش های مناسب انجام پذیرند.
الف-۱۰-۴ حفاظت در برابر کدهای مخرب و سیار		
هدف: حفاظت از یکپارچگی نرم افزار و اطلاعات.		
الف-۱۰-۴-۱	کنترل هایی در برابر کدهای مخرب	*کنترل* کنترل های لازم برای تشخیص، پیشگیری و ترمیم به منظور حفاظت در برابر کدهای مخرب، و روش های اجرایی مناسب برای آگاه سازی کاربران، باید پیاده‌سازی شوند.
الف-۱۰-۴-۲	کنترل هایی در برابر کدهای سیار	*کنترل* جایی‌که استفاده از کدهای سیار، مجاز شده، پیکربندی باید اطمینان دهد که کد سیار مجاز شده ، با توجه به خط‌مشی امنیتی‌ای که به صورت شفاف تعریف شده، عمل می کند، و از اجرای کد سیار غیر مجاز نیز باید پیشگیری شود.
الف-۱۰-۵ نسخ پشتیبان		
هدف: حفظ یکپارچگی و دسترس پذیری اطلاعات و امکانات پردازش اطلاعات.		
الف-۱۰-۵-۱	ایجاد پشتیبان از اطلاعات	*کنترل* نسخه‌های پشتیبان از اطلاعات و نرم افزار، باید با توجه به خط‌مشی های توافق شده نسخه‌های پشتیبان، به صورت منظم تهیه و آزمایش شوند.

جدول الف-۱-ادامه

الف-۱۰-۶ مدیریت امنیت شبکه
هدف: حصول اطمینان از حفاظت اطلاعات در شبکه ها و حفاظت از زیر ساخت پشتیبانی کننده.

الف-۱۰-۶-۱	کنترل های شبکه	*کنترل* شبکه ها باید به منظور حفاظت در برابر تهدیدها و برای نگهداری امنیت سیستم‌ها و برنامه های کاربردی که از شبکه استفاده می کنند (شامل اطلاعات در گردش) ، به میزان کافی، مدیریت و کنترل شوند.
الف-۱۰-۶-۲	امنیت خدمات شبکه	*کنترل* ویژگی های امنیتی، سطوح خدمت، و الزامات مدیریتی تمامی خدمات شبکه ، باید شناسایی شده و در هر توافق‌نامه خدمات شبکه، اعم از این‌که این خدمات در داخل مهیا شده یا برون‌سپاری شده اند، لحاظ شوند.
الف-۱۰-۷ اداره کرده محیط های ذخیره سازی		
هدف: پیشگیری از افشاء دستکاری، خروج یا تخریب غیر مجاز دارایی ها و وقفه در فعالیت های کسب‌وکار.		
الف-۱۰-۷-۱	مدیریت محیط های ذخیره سازی قابل جابجایی	*کنترل* برای مدیریت محیط های ذخیره سازی قابل جابجایی، باید روش های اجرایی ایجاد شوند.
الف-۱۰-۷-۲	امحای محیط های ذخیره سازی	*کنترل* محیط های ذخیره سازی که دیگر مورد نیاز نیستند، باید با بکارگیری روش های اجرایی رسمی، به صورت امن و محافظت شده، امحاء شوند.
الف-۱۰-۷-۳	روش های اجرایی جابجایی اطلاعات	*کنترل* باید روش های اجرایی جابجایی و انبارش اطلاعات، برای حفاظت این اطلاعات در برابر افشای غیر مجاز یا استفاده نابجا، ایجاد شوند.
الف-۱۰-۷-۴	امنیت مستندات س ستم	*کنترل* مستندات س ستم باید در برابر دسترسی غ ر مجاز، حفاظت شوند.
الف-۱۰-۸ تبادل اطلاعات		
هدف: حفظ امنیت اطلاعات و نرم افزار مبادله شده در درون یک سازمان و با هر موجودیت بیرونی.		
الف-۱۰-۸-۱	خط‌مشی ها و روش‌های اجرایی تبادل اطلاعات	*کنترل* برای حفاظت تبادل اطلاعات بواسطه استفاده از تمام انواع امکانات ارتباطی، باید خط‌مشی ها، روش های اجرایی و کنترل های تبادل رسمی ایجاد شوند.
الف-۱۰-۸-۲	توافق‌نامه‌های تبادل	*کنترل* برای تبادل اطلاعات و نرم افزار مابین سازمان و طرف های بیرونی، باید توافق‌نامه‌هایی ایجاد شوند.
الف-۱۰-۸-۳	محیط های ذخیرسازی فیزیکی، حین حمل‌ونقل	*کنترل* محیط های ذخیره سازی حاوی اطلاعات باید در هنگام حمل و نقل خارج از مرزهای فیزیکی سازمان، در برابر دسترسی غیر مجاز، استفاده نابجا یا صدمه، محافظت شوند.

جدول الف-۱-ادامه

الف-۱۰-۸-۴	پیام رسانی الکترونیکی	*کنترل* اطلاعات مورد بحث در پیام رسانی الکترونیکی باید به صورت مناسبی حفاظت شوند.
الف-۱۰-۸-۵	سیستم‌های اطلاعاتی	*کنترل*

	کسب‌وکار	به منظور حفاظت اطلاعات مربوط به اتصالات درونی سیستم‌های اطلاعاتی کسب‌وکار، خط‌مشی ها و روش های اجرایی باید ایجاد و پیاده سازی شوند.
الف-۱۰-۹ خدمات تجارت الکترونیکی		
هدف: حصول اطمینان از امنیت خدمات تجارت الکترونیکی و استفاده امن از آنها.		
الف-۱۰-۹-۱	تجارت الکترونیک	*کنترل* اطلاعات مورد بحث در تجارت الکترونیک که از شبکه های عمومی عبور می‌کنند، باید در برابر فعالیت های کلاه برداری، مناقشات در قرارداد، و افشاء و دستکاری غیر مجاز، محافظت شوند.
الف-۱۰-۹-۲	داد و ستدهای بر خط[1] (متصل و مستقیم)	*کنترل* اطلاعات مورد بحث در داد و ستدهای بر خط (متصل و مستقیم) ، باید به منظور پیشگیری از انتقال ناقص، مسیریابی اشتباه[2]، تغییر یافتن غیر مجاز پیغام، افشای غیر مجاز، بازگرداندن یا تکرار غیر مجاز پیغام، حفاظت شوند.
الف-۱۰-۹-۳	اطلاعات در دسترس عموم	*کنترل* یکپارچگی اطلاعاتی که در یک سیستم در دسترس عموم، قابل حصول است، باید به منظور پیشگیری از دستکاری غیر مجاز، محافظت شود.
الف-۱۰-۱۰ پایش[3]		
هدف: تشخیص فعالیت های غیر مجاز پردازش اطلاعات.		
الف-۱۰-۱۰-۱	واقعه نگاری ممیزی[4]	*کنترل* سوابق وقایع[5] ممیزی مشتمل بر فعالیت های کاربر، استثناءها و وقایع امنیت اطلاعات، باید برای یک بازه زمانی توافق شده،ایجاد و نگهداری شوند تا در رسیدگی های آتی و پایش کنترل دسترسی، کمک نماید.
الف-۱۰-۱۰-۲	پایش کاربرد سیستم	*کنترل* روش های اجرایی برای پایش کاربرد امکانات پردازش اطلاعات، باید ایجاد شده و نتایج فعالیت های پایش، به طور منظم بازنگری شوند.
الف-۱۰-۱۰-۳	حفاظت از اطلاعات ثبت شده وقایع	*کنترل* امکانات واقعه نگاری و اطلاعات ثبت شده وقایع، باید در برابر دسترسی پنهانی و غیر مجاز، حفاظت شوند.

جدول الف-۱-ادامه

الف-۱۰-۱۰-۴	ثبت وقایع متولی سیستم[6] و متصدی[7]	*کنترل* وقایع فعالیت های متولی سیستم و متصدی سیستم باید ثبت شوند.
الف-۱۰-۱۰-۵	واقعه نگاری خرابی[8]	*کنترل*

1- On-line
2- Misrouting
3- Monitoring
4- Audit logging
5- Logs
1- Administrator
2- Operator
3- Fault logging

		وقایع خرابی ها باید ثبت شده، تحلیل شده و اقدام مناسبی انجام شود.
الف-۱۰-۱۰-۶	همزمان سازی ساعت‌ها	*کنترل* ساعت‌های تمامی سیستم‌های پردازش اطلاعات مرتبط در درون یک سازمان یـا دامنه امنیتی، باید با یک مبنع زمانی دقیق توافق شده، همزمان شوند.
الف-۱۱ کنترل دسترسی		
الف-۱۱-۱ الزمات کسب‌وکار برای کنترل دسترسی		
هدف: کنترل دسترسی به اطلاعات.		
الف-۱۱-۱-۱	خط‌مشی کنترل دسترسی	*کنترل* یک خط‌مشی کنترل دسترسی باید بر مبنای الزامات کسب‌وکار و الزامات امنیتی در خصوص دسترسی، ایجاد، مدون و بازنگری شود.
الف-۱۱-۲ مدیریت دسترسی کاربر		
هدف: حصول اطمینان از دسترسی کاربر مجاز شده و پ شگ ری از دسترسی غ ر مجاز به سیستم‌های اطلاعاتی.		
الف-۱۱-۲-۱	ثبت کاربر	*کنترل* رای اعطاء یا لغو دسترسی به سیستم‌ها و خدمات اطلاعاتی، باید یک روش اجرایی رسمی ثبت و حذف کاربر وجود داشته باشد.
الف-۱۱-۲-۲	مدیریت اختیارات ویژه[1]	*کنترل* تخصیص و بکارگیری اختیارات ویژه، باید محدود و کنترل شده باشد.
الف-۱۱-۲-۳	مدیریت کلمه عبور کاربر	*کنترل* تخصیص کلمات عبور، باید از طریق یک فرآیند مدیریتی رسمی، کنترل شود.
الف-۱۱-۲-۴	بازنگری حقوق دسترسی کاربر	*کنترل* مدیریت باید با استفاده از یک فرآیند رسمی، حقوق دسترسی کاربران را در فواصل زمانی منظم، بازنگری کند.
الف-۱۱-۳ مسوولیت های کاربر		
هدف: پیشگیری از دسترسی کاربر غیر مجاز، و به خطر افتادن یا سرقت اطلاعات وامکانات پردازش اطلاعات.		
الف-۱۱-۳-۱	استفاده از کلمه عبور	*کنترل* کاربران باید در انتخاب و بکارگیری کلمه عبور، به تبعیت از شیوه های امنیتی صحیح، ملزم شوند.

جدول الف-۱-ادامه

الف-۱۱-۳-۲	تجهیزات بدون مراقبت کاربر	*کنترل* کاربران اید اطمینان داشته باشند که تجهیزات بدون متصدی، حفاظت مناسبی دارند.
الف-۱۱-۳-۳	خط‌مشی میز پاک و صفحه پاک	*کنترل* یک خط‌مشی میز پاک برای کاغذها و محیط های ذخیره سازی قابل جابجایی و یک خط‌مشی صفحه پاک برای امکانات پردازش اطلاعات، باید مورد پذیرش واقع شوند.

4- Privilege management

الف-۱۱-۴ کنترل دسترسی به شبکه		
هدف: پیشگیری از دسترسی غیر مجاز به خدماتی که تحت شبکه ارایه می‌شوند.		
الف-۱۱-۴-۱	خط‌مشی استفاده از خدمات شبکه	*کنترل* کاربران باید تنها به خدماتی که مشخصاً استفاده از آنها برایشان مجاز شده، دسترسی داشته باشند.
الف-۱۱-۴-۲	احراز اصالت کاربر برای اتصالات بیرونی	*کنترل* برای کنترل دسترسی کاربران راه دور، باید روش های مناسب احراز اصالت بکار گرفته شوند.
الف-۱۱-۴-۳	شناسایی تجهیزات در شبکه‌ها	*کنترل* شناسایی خودکار تجهیزات، باید به عنوان وسیله ای برای احراز اصالت اتصالات از مکان ها و تجهیزات مشخص، در نظر گرفته شود.
الف-۱۱-۴-۴	حفاظت از درگاه عیب یابی[1] و پیکربندی راه دور[2]	*کنترل* دسترسی فیزیکی و منطقی به درگاه های عیب یابی و پیکربندی، باید تحت کنترل باشد.
الف-۱۱-۴-۵	تفکیک در شبکه ها	*کنترل* گروه های خدمات اطلاعاتی، کاربران و سیستم‌های اطلاعاتی، باید در شبکه ها تفکیک شوند.
الف-۱۱-۴-۶	کنترل اتصال به شبکه	*کنترل* برای شبکه های اشتراکی، به ویژه آنهایی که در محدوده های سازمان، گسترش می یابند، قابلیت کاربران برای اتصال به شبکه، باید در راستای خط‌مشی کنترل دسترسی و الزامات برنامه های کاربردی کسب‌وکار، محدود شود.
الف-۱۱-۴-۷	کنترل مسیریابی در شبکه	*کنترل* باید کنترل های مسیریابی برای شبکه ها پیاده سازی شوند، تا اطمینان حاصل شود که اتصالات رایانه ای و جریان اطلاعاتی، خط‌مشی کنترل دسترسی به برنامه های کاربردی کسب‌وکار را نقض نمی کنند.
الف-۱۱-۵ کنترل دسترسی به سیستم عامل		
هدف: پیشگیری از دسترسی غیر مجاز به سیستم‌های عامل.		

جدول الف-۱-ادامه

الف-۱۱-۵-۱	روش های اجرایی ورود امن به سیستم	*کنترل* دسترسی به سیستم عامل، باید از طریق یک روش اجرایی ورود امن به سیستم، کنترل شود.
الف-۱۱-۵-۲	شناسایی و احراز اصالت کاربر	*کنترل* تمامی کاربران باید یک شناسه یکتا (شناسه کاربر) برای استفاده شخصی خودشان داشته باشند و یک فن مناسب احراز اصالت، به منظور اثبات هویت ادعا شده یک کاربر، باید انتخاب شود.

1- Remote diagnostic
2- Remote configuration

الف-۱۱-۵-۳	سیستم مدیریت کلمه عبور	*کنترل* سیستم‌های مدیریت کلمات عبور، باید تعاملی بوده و کیفیت کلمات عبور را تضمین نمایند.
الف-۱۱-۵-۴	استفاده از برنامه های کمکی سیستم	*کنترل* استفاده از برنامه های کمکی سیستم که ممکن است قادر به ابطال کنترل های سیستم و برنامه کاربردی باشند، باید محدود و به شدت کنترل شوند.
الف-۱۱-۵-۵	خروج زمانی از جلسه[1]	*کنترل* جلسه غیر فعال باید پس از یک بازه زمانی تعریف شده برای غیر فعال بودن، بسته و قطع شوند.
الف-۱۱-۵-۶	محدود سازی زمان اتصال	*کنترل* به منظور فراهم آوری امنیت بیشتر برای برنامه های کاربردی پرمخاطره، باید محدودیت‌هایی در زمان اتصال اعمال شود.
الف-۱۱-۶ کنترل دسترسی به برنامه های کاربردی و اطلاعات *هدف:* پیشگیری از دسترسی غیر مجاز به اطلاعات نگهداری شده در سیستم‌های کاربردی.		
الف-۱۱-۶-۱	محدود سازی دسترسی به اطلاعات	*کنترل* مطابق با خط‌مشی کنترل دسترسی تعریف شده، باید دسترسی کاربران و کارکنان پشتیبانی کننده به اطلاعات و کارکردهای سیستم کاربردی، محدود شود.
الف-۱۱-۶-۲	جداسازی سیستم‌های حساس	*کنترل* سیستم‌های حساس باید یک محیط محاسباتی اختصاصی (مجزا)، داشته باشند.
الف-۱۱-۷ محاسبه سیار و کار از راه دور *هدف:* حصول اطمینان از امنیت اطلاعات در هنگام استفاده از امکانات محاسبه سیار و کار از راه دور.		
الف-۱۱-۷-۱	محاسبه و ارتباطات سیار	*کنترل* به منظور حفاظت در برابر ریسک بکارگیری امکانات محاسبه و ارتباطات سیار، باید یک خط‌مشی رسمی و معیارهای امنیتی مناسبی اختیار شوند.
الف-۱۱-۷-۲	کار از راه دور	*کنترل* برای فعالیت های کار ار راه دور، باید یک خط‌مشی، طرح های عملیاتی و روش‌های اجرایی، ایجاد و پیاده سازی شوند.

جدول الف-۱-ادامه

الف-۱۲ اکتساب، توسعه و نگهداری سیستم‌های اطلاعاتی		
الف-۱۲-۱ الزامات امنیتی سیستم‌های اطلاعاتی *هدف:* حصول اطمینان از این‌که امنیت، یک جزء جدائی ناپذیر از سیستم‌های اطلاعاتی است.		
الف-۱۲-۱-۱	تحلیل و تعیین الزامات امنیتی	*کنترل* بیان نیازهای سازمان به سیستم‌های اطلاعاتی جدید یا گسترش سیستم‌های اطلاعاتی موجود، باید الزاماتی را به منظور اعمال کنترل‌های امنیتی، مشخص کند.

1- Session Time-out

الف-۱۲-۲ پردازش صحیح در برنامه های کاربردی		
هدف: پیشگیری از خطاها، گم شدن، دستکاری غیر مجاز یا استفاده نابجا از اطلاعات در برنامه های کاربردی.		
الف-۱۲-۲-۱	صحه گذاری[1] داده های ورودی	*کنترل* باید داده های ورودی به برنامه های کاربردی، صحه‌گذاری شوند تا از صحت و تناسب این داده‌ها اطمینان حاصل شود.
الف-۱۲-۲-۲	کنترل پردازش های درونی	*کنترل* به منظور تشخیص هر نوع خرابی اطلاعات ناشی از خطاهای پردازشی یا اقدامات عمدی، باید در برنامه های کاربردی، بررسی هایی برای صحه‌گذاری صورت پذیرند.
الف-۱۲-۲-۳	یکپارچگی پیغام	*کنترل* الزاماتی برای اطمینان از سندیت و حفاظت از یکپارچگی پیغام در برنامه های کاربردی، باید شناسایی شده و کنترل های مناسبی شناسایی و پیاده سازی شوند.
الف-۱۲-۲-۴	صحه گذاری داده های خروجی	*کنترل* به منظور حصول اطمینان از این‌که پردازش اطلاعات ذخیره شده، صحیح بوده و شرایط مناسبی دارد، داده های خروجی برنامه های کاربردی، باید صحه‌گذاری شوند.
الف-۱۲-۳ کنترل های رمز نگاری		
هدف: جفاظت از محرمانگی، سندیت یا یکپارچگی اطلاعات، توسط مفاهیم رمز نگاری.		
الف-۱۲-۳-۱	خط‌مشی استفاده از کنترل‌های رمزنگاری	*کنترل* برای حفاظت از اطلاعات، باید یک خط‌مشی استفاده از کنترل های رمزنگاری، ایجاد و پیاده‌سازی شود.
الف-۱۲-۳-۲	مدیریت کلید	*کنترل* به منظور پشتیبانی استفاده سازمان از فنون رمز نگاری، باید یک سیستم مدیریت کلید ایجاد شود.
الف-۱۲-۴ امنیت پرونده های سیستم		
هدف: حصول اطمینان از امنیت پرونده های سیستم.		

جدول الف-۱-ادامه

الف-۱۲-۴-۱	کنترل نرم افزارهای عملیاتی	*کنترل* به منظور کنترل نصب نرم افزار بر روی سیستم‌های عملیاتی، روش‌های اجرایی باید ایجاد شوند.
الف-۱۲-۴-۲	حفاظت از داده های آزمایشی سیستم	*کنترل* داده های آزمایشی، باید به دقت انتخاب شده، و محافظت و کنترل شوند.
الف-۱۲-۴-۳	کنترل دسترسی به کد منبع برنامه	*کنترل* دسترسی به کد منبع برنامه، باید محدود شود.

1- Validation

الف-۱۲-۵ امنیت در فرآیند های توسعه و پشتیبانی		
هدف: حفظ امنیت نرم افزار و اطلاعات سیستم کاربردی.		
الف-۱۲-۵-۱	روش های اجرایی کنترل تغییر	*کنترل* با استفاده از روش های اجرایی رسمی کنترل تغییر، پیاده سازی تغییرات باید کنترل شوند.
الف-۱۲-۵-۲	بازنگری فنی نرم‌افزارهای کاربردی پس از تغییرات سیستم	*کنترل* در هنگام تغییر سیستم‌های عامل، به منظور حصول اطمینان ازعدم وجود تاثیر سوء بر عملیات یا امنیت سازمانی، نرم افزارهای کاربردی حیاتی کسب‌وکار باید بازنگری و آزمایش شوند.
الف-۱۲-۵-۳	محدود سازی در اعمال تغییرات در بسته های نرم‌افزاری	*کنترل* باید از دستکاری در بسته های نرم افزاری، اجتناب شده، محدود به تغییرات ضروری باشد، و تمامی تغییرات باید به شدت کنترل شوند.
الف-۱۲-۵-۴	نشت اطلاعات	*کنترل* باید از فرصت های نشت اطلاعات، پیشگیری شود.
الف-۱۲-۵-۵	توسعه نرم افزار برون‌سپاری‌شده	*کنترل* توسعه نرم افزار برون‌سپاری شده، باید توسط سازمان، نظارت و پایش شود.
الف-۱۲-۶ مدیریت آسیب پذیری فنی		
هدف: کاهش ریسک منتج از سوء استفاده از آسیب پذیری های فنی منتشر شده.		
الف-۱۲-۶-۱	کنترل آسیب‌پذیری‌های فنی	*کنترل* اطلاعات بهنگام در خصوص آسیب پذیری های فنی سیستم‌های اطلاعاتی مورد استفاده، باید کسب شده، قرار گرفتن سازمان در معرض چنین آسیب پذیری هایی ارزیابی شده، و معیارهای مناسبی برای نشانی دهی ریسک مربوطه، برگزیده شوند.
الف-۱۳ مدیریت حوادث امنیت اطلاعات		
الف-۱۳-۱ گزارش دهی رویدادها و ضعف های امنیت اطلاعات		
هدف: حصول اطمینان از این‌که حوادث و ضعف های امنیت اطلاعات مربوط به سیستم‌های اطلاعاتی، به شیوه ای به اطلاع برسد که اجازه اقدام اصلاحی بهنگام را بدهد.		

جدول الف-۱-ادامه

الف-۱۳-۱-۱	گزارش دهی رویدادهای امنیت اطلاعات	*کنترل* رویدادهای امنیت اطلاعات باید در کوتاه‌ترین زمان ممکن، از طریق مجاری مدیریتی مناسب، گزارش شوند.
الف-۱۳-۱-۲	گزارش دهی ضعف های امنیتی	*کنترل* تمامی کارکنان، پیمانکاران و کاربران طرف ثالث سیستم‌ها و خدمات اطلاعاتی، باید نسبت به یادداشت و گزارش دهی هر ضعف امنیتی مشاهده شده یا مورد سوء ظن در سیستم‌ها یا خدمات، ملزم شوند.

الف-۱۳-۲ مدیریت حوادث و بهبودها و ضعفهای امنیت اطلاعات		
هدف: حصول اطمینان از این‌که رویکردی استوار و موثر برای مدیریت حوادث امنیت اطلاعات، بکار گرفته شده است.		
الف-۱۳-۲-۱	مسوولیت ها و روش‌های اجرایی	*کنترل* به منظور حصول اطمینان از یک پاسخ سریع، موثر و منظم به حوادث امنیت اطلاعات، مسوولیت های مدیریتی و روش های اجرایی باید ایجاد شوند.
الف-۱۳-۲-۲	یادگیری از حوادث امنیت اطلاعات	*کنترل* برای این‌که نوع، حجم و هزینه های حوادث امنیتی، قابل اندازه گیری و پایش باشند، باید ساز و کارهای لازم ایجاد شوند.
الف-۱۳-۲-۳	گرد آوری شواهد	*کنترل* هنگامی‌که پیگرد علیه یک فرد یا سازمان، پس از یک حادثه امنیت اطلاعات، منجر به اقدام قانونی (اعم از مدنی یا جنایی) می‌شود، شواهد باید منطبق با قواعد اقامه شواهد در حوزه(ها)ی قضایی مرتبط، گردآوری، نگهداری و ارایه شوند.
الف-۱۴ مدیریت تداوم کسب‌وکار		
الف-۱۴-۱ جنبه های امنیت اطلاعات مدیریت تداوم کسب‌وکار		
هدف: خنثی کردن وقفه های فعالیت های کسب‌وکار و حفاظت از فرآیند های بحرانی کسب‌وکار در برابر اثرات ناشی از خرابی های عمده سیستم‌های اطلاعاتی یا سوانح و حصول اطمینان از، ازسرگیری به موقع آنها.		
الف-۱۴-۱-۱	لحاظ کردن امنیت اطلاعات در فرآیند مدیریت تداوم کسب‌وکار	*کنترل* باید فرآیند مدیریت شده ای به منظور تداوم کسب‌وکار در سراسر سازمان، ایجاد و نگهداری شود که الزامات امنیت اطلاعات مورد نیاز تداوم کسب‌وکار سازمان را نشانی دهی کند.
الف-۱۴-۱-۲	تداوم کسب‌وکار و برآورد ریسک	*کنترل* وقایعی که می‌توانند موجب وقفه در فرآیند های کسب‌وکار شوند، باید با توجه به احتمال بروز و آسیب ناشی از چنین وقفه هایی و پیامدهای آنها بر امنیت اطلاعات، شناسایی شوند.
الف-۱۴-۱-۳	ایجاد و پیاده سازی طرحهای تداوم در رگیرنده امنیت اطلاعات	*کنترل* در پی ایجاد وقفه یا بروز نقص در فرآیند های بحرانی کسب وکار، به منظور نگهداری یا از سرگیری عملیات و اطمینان از دسترس پذیری اطلاعات در سطح و مقیاس های زمانی مورد نیاز، باید طرح هایی ایجاد و پیاده سازی شوند.

جدول الف-۱-ادامه

الف-۱۴-۱-۴	چهارچوب طرح‌ریزی تداوم کسب‌وکار	*کنترل* به منظور حصول اطمینان از سازگار بودن تمامی طرح ها، نشانی دهی بدون تناقض الزامات امنیت اطلاعات، و شناسایی اولویت های آزمایش و نگهداری، یک چهارچوب واحد از طرح های تداوم کسب وکار باید ایجاد و نگهداری شود.
الف-۱۴-۱-۵	آزمایش، نگهداری و ارزیابی مجدد طرح های تداوم کسب‌وکار	*کنترل* طرح های تداوم کسب‌وکار، به منظور حصول اطمینان از این‌که به‌روز و موثر هستند، باید به طور منظم مورد آزمایش قرار گرفته و بهنگام شوند.

الف-۱۵ انطباق		
الف-۱۵-۱ انطباق با الزامات قانونی		
هدف: پرهیز از نقض هر نوع قانون، مقررات تعهدات آیین‌نامه ای یا قراردادی و هر الزام امنیتی.		
الف-۱۵-۱-۱	شناسایی قوانین قابل‌اجرا	*کنترل* تمامی مقررات، الزامات آیین‌نامه ای و قراردادی مرتبط و رویکرد سازمان نسبت به برآورده سازی این الزامات، باید برای هر سیستم اطلاعاتی و سازمان، به وضوح تعریف شده و به‌روز نگهداشته شوند.
الف-۱۵-۱-۲	حقوق مالکیت معنوی (IPR)	*کنترل* به منظور حصول اطمینان از انطباق با الزامات قانون گزار، الزامات آیین‌نامه ای و قراردادی در استفاده از کالایی که ممکن است دارای حقوق مالکیت معنوی باشد، و در هنگام استفاده از محصولات نرم افزاری دارای حقوق تجاری، روش های اجرایی مناسب، باید پیاده سازی شوند.
الف-۱۵-۱-۳	حفاظت از سوابق سازمانی	*کنترل* سوابق مهم، باید با توجه به مقررات، الزامات آیین‌نامه ای، قراردادی و کسب‌وکار، در برابرگم‌شدن[1]، تخریب[2] و تحریف[3]، محافظت شوند.
الف-۱۵-۱-۴	حفاظت داده ها و حریم‌خصوصی اطلاعات شخصی	*کنترل* حفاظت داده ها و حریم خصوصی باید آن‌گونه که در قوانین و آیین‌نامه های مرتبط، و در صورت قابلیت اعمال، شرایط قراردادی الزام شده، تضمین شود.
الف-۱۵-۱-۵	پیشگیری از استفاده نابجا از امکانات پردازش اطلاعات	*کنترل* کاربران باید از بکارگیری امکانات پردازش اطلاعات برای مقاصد غیرمجاز، بازداشته شوند.
الف-۱۵-۱-۶	قواعد کنترل های رمزنگاری	*کنترل* کنترل های رمز نگاری در انطباق با تمامی‌توافق‌نامه‌ها و قوانین و آیین‌نامه های مرتبط، باید بکار گرفته شوند.
الف-۱۵-۲ انطباق با خط‌مشی ها و استانداردهای امنیتی، و انطباق فنی		
هدف: حصول اطمینان از انطباق سیستم‌ها با خط‌مشی ها و استانداردهای امنیتی سازمانی.		

جدول الف-۱-ادامه

الف-۱۵-۲-۱	انطباق خط‌مشی ها و استانداردهای امنیتی	*کنترل* برای حصول انطباق با خط‌مشی ها و استانداردهای امنیتی، مدیران باید از این‌که تمامی روش های اجرایی امنیتی، در حیطه مسوولیتشان، به درستی اجرا می‌شوند، اطمینان حاصل نمایند.
الف-۱۵-۲-۲	بررسی انطباق فنی	*کنترل* به منظور انطباق با استانداردهای پیاده سازی امنیت، باید سیستم‌های اطلاعاتی به طور منظم بررسی شوند.

1- Loss
2- Destruction
3- Falsification

الف-۱۵-۳ ملاحظات ممیزی سیستم‌های اطلاعاتی		
هدف: پیشینه کردن اثربخشی و کمینه کردن اختلال در فرآیند ممیزی سیستم‌های اطلاعاتی.		
الف-۱۵-۳-۱	کنترل های ممیزی سیستم‌های اطلاعاتی	*کنترل* الزامات و فعالیت های ممیزی مرتبط با بررسی های سیستم‌های عملیاتی، باید به دقت طرح‌ریزی ومورد توافق قرار گیرند تا ریسک ناشی از توقف در فرآیند هـای کسب‌وکار، کمینه شوند.
الف-۱۵-۳-۲	حفاظت از ابزارهای ممیزی سیستم‌های اطلاعاتی	*کنترل* به منظور پیشگیری از هر گونه استفاده نابجا یا به خطر افتادن محتمل، دسترسی به ابزارهای ممیزی سیستم‌های اطلاعاتی، باید محافظت شده باشد.

پیوست ب
(اطلاعاتی)
اصول OECD[1] و این استاندارد ملی

اصول ارایه شده در راهنماهای OECD (سازمان همکاری و توسعه اقتصادی) برای امنیت سیستم‌های اطلاعاتی و شبکه‌ها، در تمامی خط‌مشی و لایه‌های عملیاتی که حاکم بر امنیت سیستم‌های اطلاعاتی و شبکه‌ها هستند، بکار گرفته می‌شوند. این استاندارد ملی، برای پیاده‌سازی بعضی از اصول OECD بکار رفته در مدل PDCA و فرآیند های تشریح شده در بندهای ۴، ۵، ۶ و۸، یک چهارچوب سیستم مدیریت امنیت اطلاعات، آن‌گونه که در جدول ب-۱ بیان شده، ارایه می‌کند.

جدول ب-۱- اصول OECD و مدل PDCA

اصل OECD	فرآیند متناظر سیستم مدیریت امنیت اطلاعات و مرحله PDCA
آگاه سازی[2] توصیه می شود شرکت کنندگان از نیازهای امنیت سیستم‌های اطلاعاتی و شبکه‌ها و آنچه که می‌توانند برای افزایش امنیت انجام دهند، آگاه باشند.	این فعالیت قسمتی از مرحله اجرا است (به بندهای ۴-۲-۲ و۵-۲-۲ رجوع کنید).
مسوولیت تمام شرکت کنندگان در قبال امنیت سیستم‌های اطلاعاتی و شبکه‌ها، مسوول هستند.	این فعالیت قسمتی از مرحله اجرا است (به بندهای ۴-۲-۲ و ۵-۱ رجوع کنید).
پاسخ توصیه می شود شرکت کنندگان به منظور پیشگیری، تشخیص و پاسخ به حوادث امنیتی، به موقع و همکارانه، عمل نمایند.	این قسمتی از مرحله بررسی در فعالیت پایش(به بندهای ۴-۲-۳ و ۶ تا ۷-۳ رجوع کنید) و مرحله اقدام در فعالیت پاسخ‌دهی (به بندهای ۴-۲-۲ و ۸-۱ تا ۸-۳ رجوع کنید) است. این همچنین به‌وسیله برخی از جنبه‌های مراحل طرح و بررسی، پوشش داده می‌شود.
برآورد مخاطب توصیه می شود شرکت کنندگان برآوردهای ریسک را هدایت نمایند.	این فعالیت قسمتی از مرحله طرح (به بندهای ۴-۲-۱ رجوع کنید) و برآورد مجدد ریسک قسمتی از مرحله بررسی (به بندهای ۴-۲-۳و ۶ تا ۷-۳ رجوع کنید) است.
طراحی و پیاده‌سازی امنیت توصیه می شود شرکت کنندگان امنیت را به عنوان یک جزء ضروری از سیستم‌های اطلاعاتی و شبکه‌ها، دخیل نمایند.	هنگامی‌که یک برآورد ریسک کامل می‌شود، به عنوان قسمتی از مرحله طرح، کنترل‌ها برای برطرف سازی ریسک انتخاب می‌شوند (به بندهای ۴-۲-۱ رجوع کنید). سپس مرحله اجرا (به بندهای ۴-۲-۲ و ۵-۲ رجوع کنید) پیاده سازی و استفاده علنی از این کنترل‌ها را پوشش می‌دهد.

جدول ب-۱-ادامه

1- Organization for Economic Co-operation and Development
2- Awareness

مدیریت امنیت توصیه می شود شرکت کنندگان یک رویکرد جامع به مدیریت امنیت را برگزینند.	مدیریت ریسک ، فرآیند ی مشتمل بر پیشگیری، تشخیص و پاسخ به حوادث، نگهداری مداوم، بازنگری و ممیزی است. مراحل طرح، اجرا، بررسی و اقدام، دربرگیرنده تمامی این جنبه‌ها می‌باشند.
برآورد مجدد توصیه می شود شرکت کنندگان، امنیت سیستم‌های اطلاعاتی و شبکه‌ها را بازنگری و برآورد مجدد نموده، و تصحیحات مناسب برای خط‌مشی‌های امنیتی، تجارب، معیارها و روش‌های اجرایی اتخاذ نمایند.	برآورد مجدد امنیت اطلاعات، قسمتی از مرحله بررسی است (به بندهای ۴-۲-۳ و ۶ تا ۷-۳ رجوع کنید) آنجا که بازنگری‌های منظم، توصیه می شود به منظور بررسی اثر بخشی سیستم مدیریت امنیت اطلاعات، و بهبود امنیت به عنوان قسمتی از مرحله اقدام (به بندهای ۴-۲-۴ و ۸-۱ تا ۸-۳ رجوع کنید) برعهده گرفته شود.

پیوست پ
(اطلاعاتی)
تناظر بین استاندارد ملی ایران ایزو ۹۰۰۱: سال ۱۳۸۰ ، ISO 14001:2004 و این استاندارد ملی

جدول پ-۱ تناظر بین استاندارد ملی ایران ایزو ۹۰۰۱: سال ۱۳۸۰ ، ISO 14001:2004 و این استاندارد ملی را نشان می‌دهد.

جدول پ-۱- تناظر بین استاندارد ملی ایران ایزو ۹۰۰۱: سال ۱۳۸۰ ، ISO 14001:2004 و این استاندارد ملی

این استاندارد ملی	استاندارد ملی ایران ایزو ۹۰۰۱ : سال ۱۳۸۰	ISO 14001:2004
۰ مقدمه ۰-۱ کلیات ۰-۲ دیدگاه فرآیند گرا ۰-۳ سازگاری با سایر سیستم‌های مدیریتی	**۰ مقدمه** ۰-۱ کلیات ۰-۲ دیدگاه فرآیند گرا ۰-۳ ارتباط ISO 9004 ۰-۴ سازگاری با سایر سیستم‌های مدیریتی	**مقدمه**
۱ دامنه ۱-۱ کلیات ۱-۲ کاربرد	**۱ دامنه** ۱-۱ کلیات ۱-۲ کاربرد	**۱ دامنه**
۲ مراجع اصلی	**۲ مراجع اصلی**	**۲ مراجع اصلی**
۳ واژگان و تعاریف	**۳ واژگان و تعاریف**	**۳ واژگان و تعاریف**
۴ سیستم مدیریت امنیت اطلاعات ۴-۱ الزامات عمومی ۴-۲ ایجاد و مدیریت سیستم مدیریت امنیت اطلاعات ۴-۲- ۱ ایجاد سیستم مدیریت امنیت اطلاعات ۴-۲-۲ پیاده‌سازی و اجرای سیستم مدیریت امنیت اطلاعات ۴-۲-۳ پایش و بازنگری سیستم مدیریت امنیت اطلاعات ۴-۲-۴ نگهداری و بهبود سیستم مدیریت امنیت اطلاعات	**۴ سیستم مدیریت کیفیت** ۴-۱ الزامات عمومی ۸-۲-۳پایش و اندازه‌گیری فرآیند ها ۸-۲-۴-پایش و اندازه‌گیری محصول	**۴ الزامات سیستم مدیریت زیست‌محیطی** ۴-۱ الزامات عمومی ۴-۴ پیاده‌سازی و اجرا ۴-۵-۱پایش و اندازه‌گیری

۴-۳ الزامات مستندسازی	۴-۲ الزامات مستندسازی	
۴-۳-۱ کلیات	۴-۲-۱کلیات	
	۴-۲-۲ نظامنامه کیفیت	
۴-۳-۲ کنترل مدارک	۴-۲-۳کنترل مدارک	۴-۴-۵ کنترل مستندات
۴-۳-۳ کنترل سوابق	۴-۲-۴ کنترل سوابق	۴-۵-۴ کنترل سوابق

جدول پ-۱-ادامه

۵ مسوولیت مدیریت	**۵ مسوولیت مدیریت**	
۵-۱ تعهد مدیریت	۵-۱ تعهد مدیریت	
	۵-۲ تمرکز بر مشتری	
	۵-۳ خطمشی کیفیت	۴-۲ خطمشی زیست محیطی
	۵-۴ طرحریزی	۴-۳ طرحریزی
	۵-۵ مسوولیت، اختیار و ارتباطات	
۵-۲ مدیریت منابع	**۶ مدیریت منابع**	
۵-۲-۱ فراهمآوری منابع	۶-۱ فراهمآوری منابع	
	۶-۲ منابع انسانی	
۵-۲-۲ آموزش، آگاهسازی و صلاحیت	۶-۲-۲ صلاحیت، آگاهسازی و آموزش	۴-۲-۲ صلاحیت، آموزش و آگاهسازی
	۶-۳ زیرساخت	
	۶-۴ محیط کار	
۶ ممیزی داخلی سیستم مدیریت امنیت اطلاعات	۸-۲-۲ ممیزی داخلی	۴-۵-۵ ممیزی داخلی
۷ بازنگری مدیریت سیستم مدیریت امنیت اطلاعات	**۶-۵ بازنگری مدیریت**	**۶-۴ بازنگری مدیریت**
۷-۱ کلیات	۶-۵-۱ کلیات	
۷-۲ ورودیهای بازنگری	۶-۵-۲ ورودیهای بازنگری	
۷-۳ خروجیهای بازنگری	۶-۵-۳ خروجیهای بازنگری	
۸ بهبود سیستم مدیریت امنیت اطلاعات	**۸-۵ بهبود**	
۸-۱ بهبود مستمر	۸-۵-۱ بهبود مستمر	
۸-۲ اقدام اصلاحی	۸-۵-۳ اقدامات اصلاحی	۴-۵-۳ عدم تطابق، اقدام اصلاحی و اقدام پیشگیرانه
۸-۳ اقدام پیشگیرانه	۸-۵-۴ اقدامات پیشگیرانه	

پیوست الف- اهداف کنترلی وکنترل‌ها پیوست ب- اصول OECD و این استاندارد ملی پیوست پ- تناظر بین استاندارد ملی ایران ایزو ۹۰۰۱: سال ۱۳۸۰ و ISO 14001:2004 و این استاندارد ملی	پیوست الف- تناظر بین استاندارد ملی ایران ایزو ۹۰۰۱: سال ۱۳۸۰ و ISO 14001:1996	پیوست الف- راهنمای کاربرد این استاندارد ملی پیوست ب- تناظر بین ISO 9001:2004 و ISO 14001:2000

کتابنامه

انتشارات استانداردها

۱- استاندارد ملی ایران ایزو ۹۰۰۱: سال ۱۳۸۰ ، سیستم‌های مدیریت کیفیت - الزامات

۲- استاندارد ملی ایران ۱-۹۹۷۰: سال ۱۳۸۶ ، فن‌آوری اطلاعات - تکنیک‌های امنیت - مدیریت امنیت تکنولوژی ارتباطات و اطلاعات – قسمت اول: مفاهیم و مدل‌های مدیریت امنیت تکنولوژی ارتباطات و اطلاعات

۳ استاندارد ملی ایران ایزو ۱۹۰۱۱: سال ۱۳۸۶ ، رهنمودهایی برای ممیزی سیستم‌های مدیریت کیفیت و/یا زیست محیطی

4- ISO/IEC TR 13335-3:1998, Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT security

5- ISO/IEC TR 13335-4:2000, Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards

6- ISO 14001:2004, Environmental management systems - Requirements with guidance for use

7- ISO/IEC TR 18044:2004, Information technology - Security techniques - Information security incident management

8- ISO/IEC Guide 62:1996, General requirements for bodies operating assessment and certification/registration of quality systems

9- ISO/IEC Guide 73:2002, Risk management - Vocabulary - Guidelines for use in standards

سایر انتشارات

1- OECD, Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

2- NIST SP 800-30, Risk Management Guide for Information Technology Systems

3- Deming W.E., Out of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 1986

فصل سوم

فناوری اطلاعات - فنون امنیتی- آئین کار مدیریت امنیت اطلاعات

ISO/IEC 27002

Information technology-- Security techniques Code of practice for Information security management

پیش گفتار

استاندارد "فن‌آوری اطلاعات - فنون امنیتی- آیین‌کار مدیریت امنیت اطلاعات" که پیش نویس آن در کمیسیون های مربوط توسط مؤسسهٔ استاندارد و تحقیقات صنعتی ایران تهیه و تدوین شده و در پنجاه و پنجمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۸۷/۸/۱۲ مورد تصویب قرارگرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارایه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت.بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

این استاندارد ملی بر مبنای استاندارد بین المللی زیر تدوین شده و معادل آن به زبان فارسی است:

1- ISO/IEC 27002:2005, 2nd Ed.: Information technology — Security techniques — Code of practice for information security management

۲ - کلیه واژگان مصوب فرهنگستان علوم, سایت اینترنتی فرهنگستان زبان و ادبیات پارسی
http://www.persianacademy.ir/

۰ مقدمه

۰-۱ امنیت اطلاعات چیست ؟

اطلاعات، دارایی است همانند سایر دارایی‌های مهم کسب وکار که برای کسب وکار سازمان دارای اهمیت است، و درنتیجه باید بگونه ای مناسب محافظت شود. این موضوع مخصوصاً در محیطی که تعاملات کسب وکار رو به رشد است، از اهمیت بیشتری برخوردار است. در نتیجه این افزایش تعامل، اطلاعات در معرض تعداد بیشتر و انواع گوناگون تری از تهدیدات و آسیب پذیریها قرار گرفته است.(همچنین رهنمودهای OECD[1] (سازمان همکاری و توسعه اقتصادی) برای امنیت اطلاعات سامانه ها و شبکه ها می باشد، ملاحظه نمایید).

اطلاعات می‌تواند به اشکال گوناگون وجود داشته باشد. می‌تواند چاپ شده یا نوشته شده بر روی کاغذ، ذخیره شده الکترونیکی باشد، با پست یا وسایل الکترونیکی ارسال شود، از طریق فیلم به نمایش درآید، یا در مکالمات بیان شود. توصیه می‌شود، همیشه هر شکلی که اطلاعات دارد، یا به هر وسیله ای که به اشتراک گذاشته می‌شود، بگونه ای مناسب محافظت شود.

امنیت اطلاعات، محافظت از اطلاعات در برابر طیف گسترده ای از تهدیدات است که به منظور اطمینان از استمرار کسب وکار، کمینه کردن ریسک کسب وکار، حداکثر کردن آورده و فرصتهای کسب وکار است.

دستیابی به امنیت اطلاعات، با پیاده سازی مجموعه ای از کنترل‌های مناسب از جمله خط مشی ها، فرایندها، رویه ها، ساختارهای سازمانی و فعالیتهای نرم‌افزاری و سخت افزاری میسر می‌شود. این کنترل‌ها در موارد لازم باید مستقر، پیاده سازی، پایش، بازبینی و اصلاح شده تا از برآورده شدن اهداف خاص امنیتی و کسب وکار در سازمان اطمینان حاصل شود. توصیه می‌شود این موارد در راستای سایر فرایندهای مدیریت کسب وکار انجام شود.

۰-۲ چرا امنیت اطلاعات لازم است ؟

اطلاعات، فرایندهای پشتیبانی، سیستم‌ها و شبکه ها دارایی‌های مهم کسب وکار هستند. تعریف، دستیابی، نگهداری و توسعه امنیت اطلاعات می‌تواند تاثیر بسزایی بر ماندگاری در عرصه رقابت، گردش مالی، سودآوری، انطباق با قانون و تصویر کسب وکار داشته باشد.

سازمانها و سیستم‌های اطلاعاتی و شبکه های با تهدیدات امنیتی از منابع گسترده و گوناگون مواجه می‌شوند، که شامل سوء استفاده رایانه ای، جاسوسی، خرابکاری، تخریب، آتش سوزی و سیل است. دلایل بروز ایراد از قبیل کد مخرب، دستیابی غیر مجاز رایانه ای، حملات ممانعت از ارایه خدمات متداول تر، زیاده خواهانه تر[2] و پیچیده تر شده اند.

امنیت اطلاعات برای کسب وکار بخشهای خصوصی و عمومی و همچنین محافظت از زیرساختارهای حیاتی اهمیت دارد. در این دو بخش، امنیت اطلاعات بعنوان توانمندساز عمل خواهد کرد، بعنوان مثال برای دستیابی به دولت الکترونیکی یا کسب وکار الکترونیکی و اجتناب یا کاهش ریسک‌های مرتبط است. تعامل شبکه های عمومی و خصوصی و به اشتراک گذاشتن منابع اطلاعاتی، موجب افزایش دشواری در کنترل دسترسی می‌شود.

1- Organisation for Economic Co-operation and Development (OECD)

2- Ambitious

بسیاری از سیستم‌های اطلاعاتی بگونه ای طراحی نشده اند که بتوان آنها را امن کرد.امنیتی که از طریق ابزار فنی بدست می‌آید، محدود بوده و توصیه می‌شود از طریق رویه ها و مدیریت مناسب پشتیبانی شود. شناسایی کنترل‌های مناسب، نیازمند برنامه ریزی دقیق و توجه به جزئیات است. مدیریت امنیت اطلاعات دست کم نیازمند مشارکت تمامی افراد سازمان است. همچنین ممکن است به مشارکت سهامداران، تامین کنندگان، اشخاص ثالث، مشتریان و سایر اشخاص بیرونی نیاز باشد. هچنین ممکن است به دریافت مشاوره از متخصصین در خارج سازمان نیاز باشد.

۰-۳ چگونه نیازهای امنیت شناسایی می‌شوند ؟

ضروری است سازمان نیازهای امنیتی خود را شناسایی نماید. سه منبع اصلی برای نیازمندیهای امنیت وجود دارد.

۱- یکی از منابع، از برآورد ریسک سازمان منتج می‌شود، که با در نظر گرفتن اهداف و راهبردهای کلان کسب وکار سازمان میسر می باشد. از طریق برآورد ریسک، تهدیدات داراییها شناسایی شده، آسیب‌پذیری و احتمال رخداد آن ارزیابی شده و میزان پیامد بالقوه حاصل از آن تخمین زده می‌شود.
۲- منبع دیگر، شامل قوانین، مقررات، حقوق مدنی و الزامات قراردادی بوده که سازمان با شرکای کسب‌وکار، پیمانکاران و خدمت دهندگان خود داشته و همچنین فضای فرهنگی جامعه آنها است.
۳- منبع دیگر، مجموعه ای خاص از اصول، اهداف و الزامات کسب وکار برای پردازش اطلاعات بوده که سازمان آنها را برای پشتیبانی از عملیات خود توسعه داده است.

۰-۴ برآورد ریسک‌های امنیت

نیازهای امنیتی از طریق برآورد روش‌مند ریسک‌های امنیت، شناسایی می‌شود. هزینه های صرف شده برای کنترل‌ها باید به گونه‌ای آسیب احتمالی رسیده به کسب وکار که ناشی از خطاهای امنیتی است را تعدیل نماید.
نتیجه برآورد ریسک به راهنمایی و تعیین اقدام مدیریتی مناسب و اولویت دهی برای مدیریت ریسک‌های امنیت اطلاعات و پیاده سازی کنترل‌های انتخاب شده برای مقابله با این ریسک‌ها، کمک خواهد کرد.
توصیه می‌شود، برآورد ریسک در بازه های زمانی تکرار شود تا هر تغییری که ممکن است بر نتایج برآورد ریسک تاثیر گذار باشد را لحاظ نماید.
اطلاعات بیشتر درباره برآورد ریسک‌های امنیت را می‌توان در بند ۴-۱ " برآورد ریسک‌های امنیت" یافت.

۰-۵ انتخاب کنترل‌ها

پس از اینکه نیازهای امنیتی و ریسک‌ها، شناسایی شدند و تصمیم برای برطرف سازی ریسک‌ها اتخاذ گردید، کنترل‌های مناسب باید به نحوی انتخاب و بکار گرفته شوند، تا از کاهش ریسک‌ها و رسیدن آنها به حدقابل قبول، اطمینان حاصل شود.کنترل‌ها را می‌توان از این استاندارد یا دیگر مجموعه های کنترلی، یا از کنترل‌های جدید که به منظور برآورده ساختن نیازهای خاص طراحی شده اند، به فرا خور حال، انتخاب نمود. انتخاب کنترل‌های امنیتی، بستگی به تصمیمات سازمان دارد که بر اساس، معیار پذیرش ریسک، گزینه های برطرف

سازی ریسک و رویکرد اتخاذ شده مدیریت ریسک در سازمان و همچنین کلیه قوانین و مقررات ملی و بین المللی که باید مدنظر قرار گیرد، اتخاذ می‌شود.
تعدادی از این کنترل‌ها در این استاندارد می‌تواند بعنوان اصول راهنما برای مدیریت امنیت اطلاعات، در نظر گرفته شود که در بیشتر سازمانها قابل بکارگیری هستند. جزئیات بیشتر در این باره در زیر و تحت عنوان "نقطه آغازین امنیت اطلاعات" تشریح شده است.
اطلاعات بیشتر درباره انتخاب کنترل‌ها و سایر گزینه‌های برطرف‌سازی ریسک را می‌توان در بند ۴-۲ "برطرف‌سازی ریسک‌های امنیت" پیدا کرد.

۶-۰ نقطه آغازین امنیت اطلاعات

تعدادی از کنترل‌ها را می‌توان به عنوان نقطه شروع مناسبی برای پیاده سازی امنیت اطلاعات در نظر گرفت. این کنترل‌ها یا بر اساس الزامات قانونی ضروری هستند و یا تجربیات مشترک[1] امنیت اطلاعات.
کنترل‌های در نظر گرفته شده که برای هر سازمان از منظر قانونی ضروری بوده بسته به قابل اجرا بودن قوانین، شامل :

الف- حفاظت از داده‌ها و حریم خصوصی افراد (رجوع کنید به بند ۱۵-۱-۴)
ب- حفاظت از سوابق سازمانی (رجوع کنید به بند ۱۵-۱-۳)
پ- حقوق مالکیت فکری (رجوع کنید به بند ۱۵-۱-۲)

کنترل‌های در نظر گرفته شده که حاصل تجربیات مشترک امنیت اطلاعات هستند، شامل:

الف- مستند خط مشی امنیت اطلاعات (رجوع کنید به بند ۵-۱-۱)
ب- تخصیص مسوولیت‌های امنیت اطلاعات (رجوع کنید به بند ۶-۱-۳)
پ- یادگیری، آموزش و آگاه سازی امنیت اطلاعات (رجوع کنید به بند ۸-۲-۲)
ت- اصلاح پردازش برنامه های کاربردی (رجوع کنید به بند ۱۲-۲)
ث- مدیریت آسیب پذیری فنی (رجوع کنید به بند ۱۲-۶)
ج- مدیریت استمرار کسب وکار (رجوع کنید به بند ۱۴)
چ- مدیریت رخدادهای[2] امنیت اطلاعات و بهبودها (رجوع کنید به بند ۱۳-۲)

این کنترل‌ها به اکثر سازمانها و محیط‌ها اعمال می‌شوند.
لازم به ذکر است که همه کنترل‌های این استاندارد مهم بوده و توصیه می‌شود در نظر گرفته شوند، ارتباط هر کنترل از لحاظ مواجهه با ریسک‌های مشخص سازمان باید در نظر گرفته شود. از اینرو، هر چند که رویکرد در نظر گرفته شده در بالا نقطه شروع مناسبی است، ولی نمی‌تواند جایگزین انتخاب کنترل‌ها بر اساس برآورد ریسک شود.

1- Common Paracticed
2- Incident

۰-۷ عوامل حیاتی موفقیت

تجربه نشان داده است، که عوامل زیر معمولاً نقش اساسی را در پیاده سازی موفق امنیت اطلاعات در سازمان بر عهده دارند :

الف - خط‌مشی امنیت اطلاعات، اهداف و فعالیتهایی که منعکس کننده اهداف کسب‌وکار هستند؛

ب – یک رویکرد و چارچوب برای پیاده سازی، پایش و اصلاح امنیت اطلاعات که با فرهنگ سازمانی سازگار است؛

پ - پشتیبانی صریح و تعهد کلیه سطوح مدیریتی؛

ت - درک مناسب از الزامات امنیت اطلاعات، برآورد ریسک و مدیریت ریسک؛

ث - بازاریابی اثربخش از امنیت اطلاعات به تمام مدیران، کارکنان و سایر افراد بمنظور آگاه‌سازی آنها؛

ج - انتشار راهنما برای خط‌مشی و استانداردهای امنیت اطلاعات برای کلیه مدیران، کارکنان و سایر افراد؛

چ - تامین منابع مالی برای فعالیتهای مدیریت امنیت اطلاعات؛

ح - آگاه‌سازی، تعلیم و آموزش مناسب؛

خ - تدوین فرایند اثربخش مدیریت رخدادهای امنیت اطلاعات؛

د - پیاده سازی سامانه ای قابل اندازه گیری[1] که برای ارزیابی عملکرد مدیریت امنیت اطلاعات و ارایه بازخورد برای بهبود بکار رود.

۰-۸ توسعه رهنمودهای مربوط به خود

این راهنمای پیاده سازی ممکن است به عنوان نقطه شروعی برای توسعه دستورالعمل‌های اختصاصی رهنمود برای سازمان بکار گرفته شود. ممکن است همه بخشهای این راهنمای پیاده سازی و کنترل‌ها قابل استفاده نباشند. از این گذشته ممکن است رهنمودها و کنترل‌های تکمیلی، که در این استاندارد نیامده است، مورد نیاز باشند. هنگامی که مستندات توسعه داده می‌شوند، این مستندات شامل کنترل‌ها و خطوط راهنمای تکمیلی هستند، که ممکن است شامل ارجاعات- متقاطع[2] به بندهای این استاندارد، در موارد مقتضی، جهت سهولت در بررسی انطباق بوسیله ممیزین و شرکا کسب وکار، باشد.

۱- توجه شود که اندازه گیری‌های مدیریت امنیت اطلاعات خارج از هدف و دامنه کاربرد این استاندارد می باشد.

2- Cross-Reference

فن‌آوری اطلاعات – فنون امنیتی – آیین کار مدیریت امنیت اطلاعات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی، برقرار کردن خطوط راهنما و اصول کلی برای راه اندازی، پیاده سازی، نگهداری و توسعه مدیریت امنیت اطلاعات در یک سازمان است. اهداف آورده شده در این استاندارد ملی، راهنمایی عمومی برای اهداف عرفاً مورد قبول مدیریت امنیت اطلاعات است.

اهداف کنترلی و کنترل‌های این استاندارد ملی برای برآورده ساختن الزامات شناساییِ داده شده بوسیله ارزیابی ریسک، پیاده سازی می‌شوند. این استاندارد ملی ممکن است بعنوان رهنمود پیاده سازی برای توسعه استانداردهای امنیت سازمانی، تجارب مدیریت امنیت اثربخش و کمک به ایجاد اطمینان در فعالیتهای درون سازمانی بکار رود.

این استاندارد معادل استاندارد بین‌المللی ISO/IEC 27002:2005 می‌باشد؛ و ساختار، بندها، ارجاعات، مفاهیم و شماره این استاندارد ملی هماهنگ با استاندارد بین‌المللی معادل می‌باشد. این استاندارد ملیِ معادل به صورت زیر شناخته می‌شود:

استاندارد ملی ایران ایزو-آی ای سی به شماره ۲۷۰۰۲: سال ۱۳۸۷

۲ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر بکار می رود.

۱-۲

دارایی[1]

هر چیزی که برای سازمان دارای ارزش است.

[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

۲-۲

کنترل[2]

ابزار مدیریت کردن ریسک، شامل خط‌مشی ها، رویه ها، رهنمودها، دستورالعمل‌ها یا ساختارهای سازمانی، که می‌تواند ماهیتی اجرایی، فنی، مدیریتی یا قانونی داشته باشند.

یادآوری : کنترل همچنین بعنوان مترادفی برای محافظ یا اقدام متقابل است.

۳-۲

خطوط راهنما[3]

توصیفی که روشن می‌کند، چه چیزی و چطور برای انجام توصیه می‌شود، تا اهداف تعیین شده در خط‌مشی بدست آید.

1- Asset
2- Control
3- Guideline : خطوط راهنما، رهنمود

۴-۲

تجهیزات پردازش اطلاعات[1]

هر سامانهٔ پردازش اطلاعات، خدمت[2] یا زیر ساخت یا مکانهای فیزیکی که در آن قرار دارند.

۵-۲

امنیت اطلاعات[3]

حفظ محرمانگی، یکپارچگی و در دسترس پذیری اطلاعات. همچنین ویژگیهایی از قبیل سندیت، پاسخگویی، انکارناپذیری و قابلیت اطمینان، را نیز می‌تواند شامل شود.

۶-۲

رویداد امنیت اطلاعات[4]

رویداد امنیت اطلاعات، رویداد شناسایی شده یک سیستم، خدمت یا شبکه است که دلالت بر نقض احتمالی خط‌مشی امنیت اطلاعات یا نقص حفاظتی، یا وضعیت ناشناخته قبلی که ممکن است با امنیت مرتبط باشد، دارد.
[ISO/IEC TR 18044:2004]

۷-۲

رخداد امنیت اطلاعات[5]

یک رخداد امنیت اطلاعات، با یک یا مجموعه ای از رویدادهای امنیت اطلاعات ناخواسته یا پیش بینی نشده که به احتمال زیاد، عملیات کسب‌وکار را به خطر انداخته و امنیت اطلاعات را تهدید می‌کند، معین می‌شوند.
[ISO/IEC TR 18044:2004]

۸-۲

خط‌مشی[6]

قصد و جهت‌گیری کلی که بطور رسمی‌توسط مدیریت بیان می‌شود.

1- Information processing facilities
2- Service
3- Information security
4- Information security event
5- Information security incident
6- Policy

۹-۲

ریسک[1]

ترکیب احتمال یک رویداد و میزان پیامدهای آن.
[ISO/IEC Guide 73:2002]

۱۰-۲

تحلیل ریسک[2]

استفاده نظام مند از اطلاعات به منظور شناسایی منابع و تخمین ریسک
[ISO/IEC Guide 73:2002]

۱۱-۲

برآورد ریسک[3]

فرایند کلی تحلیل و ارزیابی ریسک
[ISO/IEC Guide 73:2002]

۱۲-۲

ارزیابی ریسک[4]

فرایند مقایسه ریسک تخمین زده شده با معیار ریسک ارایه شده، به منظور تعیین اهمیت ریسک
[ISO/IEC Guide 73:2002]

۱۳-۲

مدیریت ریسک[5]

فعالیتهای هماهنگ شده برای هدایت و کنترل یک سازمان با توجه به ریسک.

یادآوری : مدیریت ریسک بطور معمول شامل ارزیابی ریسک، برطرف سازی ریسک، پذیرش ریسک و ارتباط با ریسک است.
[ISO/IEC Guide 73:2002]

۱۴-۲

برطرف سازی ریسک[6]

فرایند انتخاب و پیاده سازی تمهیداتی برای اصلاح ریسک
[ISO/IEC Guide 73:2002]

1- Risk
2- Risk analysis
3- Risk assessment
4- Risk evaluation
5- Risk management
6- Risk treatment

۱۵-۲

شخص سوم[1]

شخص یا نهادی که مستقل از اشخاص درگیر به موضوع مورد بحث، شناخته می‌شود.

۱۶-۲

تهدید[2]

دلیل بالقوه یک رخداد ناخواسته، که ممکن است نتیجه آن خسارت به سازمان یا سامانه باشد.
[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

۱۷-۲

آسیب پذیری[3]

یک ضعف در یک دارایی یا مجموعه ای از دارایی‌ها که می‌تواند بوسیله یک یا چند تهدید مورد بهره برداری قرار گیرد.
[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

1- Third party
2- Threat
3- Vulnerability

۳ ساختار این استاندارد

این استاندارد شامل ۱۱ بند کنترل امنیت، که در کل مشتمل بر ۳۹ طبقه اصلی امنیتی و یک بند مقدماتی از جمله برآورد و برطرف سازی ریسک، است.

۳-۱ بندها

هر بند شامل تعدادی طبقه امنیتی عمده است. این یازده بند (که با تعدادی از طبقات امنیتی عمده همراه است که در هر بند گنجانده شده اند) عبارتند از:

الف - خط مشی امنیت (۱)؛

ب - سازمان امنیت اطلاعات (۲)؛

پ - مدیریت دارایی (۲)؛

ت - امنیت منابع انسانی (۳)؛

ث - امنیت فیزیکی و محیطی (۲)؛

ج - مدیریت ارتباطات و عملیات (۱۰)؛

چ - کنترل دسترسی (۷)؛

ح - اکتساب، توسعه و نگهداری سیستم‌های عملیاتی (۶)؛

خ - مدیریت رخداد امنیت اطلاعات (۲)؛

د - مدیریت استمرارکسب وکار (۱)؛

ذ - انطباق (۳)؛

یادآوری: ترتیب بندها در این استاندارد به معنای اهمیت آنها نیست. بسته به شرایط، تمام بندها ممکن است مهم باشند. بنابراین توصیه می‌شود، هر سازمانی که این استاندارد را به کار می‌گیرد، بندهای قابل استفاده، اهمیت آنها و کاربردشان را برای فرایندهای کسب وکار خود شناسایی کند. همچنین، تمام این فهرست ها در این استاندارد به ترتیب اولویت نیستند مگر در مواردی که ذکر شده باشد.

۳-۲ طبقه های امنیتی عمده

هرطبقه امنیتی عمده شامل موارد زیر است:

الف - یک هدف کنترلی که نشان می دهد چه چیزی باید به دست آید؛ و

ب - یک یا چند کنترل که می‌توان آن برای دستیابی به هدف کنترل پیاده سازی کرد؛

شرح کنترل ها به قرار زیر است:

کنترل

بیانیه کنترل خاصی را برای برآورده سازی هدف کنترل، تعریف می‌کند.

راهنمای پیاده سازی

اطلاعات مفصل تری برای پشتیبانی از پیاده سازی کنترل و دستیابی به هدف کنترل، بدست می دهد. بعضی از این راهنمایی‌ها ممکن است در تمام موارد مناسب نباشند و بنابراین دیگر راههای پیاده سازی کنترل ممکن است مناسب تر باشند.

سایر اطلاعات

اطلاعات بیشتری ارایه می دهد که ممکن است لازم باشد در نظر گرفته شود، مثلا ملاحظات قانونی و اشاره به استانداردهای دیگر.

۴ برآورد و برطرف سازی ریسک

۴-۱ برآورد ریسک های امنیتی

برآورد ریسک باید ریسک‌ها را در مقایسه با معیارهای قابل قبول ریسک و اهداف مربوط به سازمان، شناسایی، مقدار دهی کمی و اولویت بندی نماید. توصیه می‌شود، نتایج اقدام مناسب مدیریت و اولویت های مدیریت ریسک‌ها امنیت اطلاعات برای پیاده سازی کنترل های انتخاب شده جهت محافظت در برابر این ریسک‌ها را، تعیین و راهنمایی کند. ممکن است نیاز باشد، فرایند برآورد ریسک‌ها و انتخاب کنترل ها چند بار انجام شود تا بخش های مختلف سازمان یا سامانه های اطلاعات فردی را پوشش دهد.

توصیه می‌شود برآورد ریسک شامل رویکرد نظام مند برای تخمین شدت ریسک و فرایند مقایسه ریسک تخمین زده شده در مقایسه با معیارهای ریسک باشد، تا اهمیت ریسک‌ها را تعیین نماید (ارزیابی ریسک)

توصیه می‌شود برآورد های ریسک همچنین به طور دوره ای انجام شود تا تغییرات در الزامات امنیتی و در شرایط ریسک، بعنوان مثال در دارایی‌ها، تهدیدها، آسیب پذیری ها، پیامدها، اریابی ریسک، و زمانی که تغییرات مهم رخ می دهد، را نیز لحاظ کند. توصیه می‌شود این ارزیابی های ریسک به گونه ای روش مند[1] به کار گرفته شوند تا نتایج تکرارپذیر و قابل قیاس ارایه دهد.

توصیه می‌شود، برآورد ریسک امنیت اطلاعات دارای یک هدف و دامنه کاربرد تعریف مشخص باشد، تا اثربخش باشد و همچنین توصیه می‌شود شامل روابط برآورد های ریسک در زمینه های دیگر، به شرط تناسب، نیز باشد.

هدف و دامنه کاربرد ریسک می‌تواند در کل سازمان، بخش هایی از سازمان، یک سامانه اطلاعات فردی، اجزا سیستم خاص، یا خدمات، در جاییکه که قابل اجرا است، واقع گرایانه و مفید باشد. مثال های روش شناسی های برآورد ریسک در ISO/IEC TR 13335-3 (رهنمودهای مدیریت امنیت فن‌آوری اطلاعات: روشهایی برای مدیریت امنیت فن‌آوری اطلاعات)

۴-۲ برطرف سازی ریسک‌های امنیتی

توصیه می‌شود قبل از در نظر گرفتن برطرف سازی ریسک، سازمان معیارهایی برای تعیین این که آیا ریسک را می‌توان پذیرفت یا نه تعیین کند. مثلا اگر برآورد شود که ریسک پایین است یا هزینه برطرف سازی آن برای سازمان مقرون به صرفه نیست ریسک‌ها مجاز است پذیرفته شوند. توصیه می‌شود این تصمیمات ثبت شوند.

برای هر یک از ریسک‌های که شناسایی شده پس از برآورد ریسک یک تصمیم برای برطرف سازی ریسک باید اتخاذ شود. گزینه های ممکن برای برطرف سازی ریسک عبارتند از:

الف - اعمال کنترل های مناسب برای کاهش ریسک‌ها

ب - پذیرش آگاهانه و هدفمند ریسک‌ها، به شرط آن که آنها به روشنی خط مشی و معیارهای سازمان را برای پذیرش ریسک رعایت کنند.

پ - اجتناب از ریسک با اجازه ندادن به فعالیت هایی که باعث رخ دادن ریسک می‌شوند.

ت - انتقال ریسک‌ها مربوطه به اشخاص دیگر، مثلا بیمه گران و تامین کنندگان.

1- Methodological

برای ریسک‌هایی که در برطرف سازی ریسک تصمیم به اعمال کنترل های مناسب گرفته شده است، توصیه می‌شود این کنترل ها انتخاب و برای برآورده ساختن الزامات شناسایی شده در برآورد ریسک، پیاده سازی شوند. توصیه می‌شود کنترل ها تضمین کنند که ریسک‌ها با احتساب موارد زیر تا حد قابل قبولی کاهش یافته است:

الف - الزامات و محدودیت های قوانین و مقررات ملی و بین المللی

ب - اهداف سازمانی

پ - الزامات و محدودیت های عملیاتی؛

ت - هزینه اجرا، و عملیات در رابطه با ریسک‌های که کاهش می یابند و نسبت ریسک باقیمانده با الزامات و محدودیت های سازمان؛

ث - نیاز به تعدیل سرمایه گذاری در پیاده سازی و عملیات کنترل ها در مقابل آسیبی که ممکن است از نارسایی های امنیتی حاصل شود؛

کنترل ها را می‌توان از این استاندارد یا از هر مجموعه کنترلی دیگر انتخاب کرد یا کنترل های جدید را می‌توان برای برآورده ساختن نیازهای خاص سازمان طراحی کرد. لازم به یادآوری است که بعضی از کنترل ها ممکن است در هر سامانه یا محیط اطلاعاتی قابل استفاده نبوده و ممکن است برای تمام سازمان ها قابل اجرا نباشد. مثلا، ۱۰-۱-۳ بیان می‌کند که وظایف چگونه برای جلوگیری از سوء استفاده و خطا تفکیک می‌شوند. ممکن است برای سازمان های کوچک تر امکانپذیر نباشد که تمام وظایف را تفکیک کنند و دیگر راه های دستیابی به یک هدف کنترلی ممکن است لازم باشند. در یک مثال دیگر، ۱۰-۱۰ بیان می‌کند که استفاده از سیستم را چگونه می‌توان پایش کرد و شواهد را جمع آوری کرد. کنترل های بیان شده مثلا ثبت وقایع، ممکن است با مقررات قابل قبول، نظیر محافظت از حریم خصوصی مشتریان یا محیط کار تناقض داشته باشند.

توصیه می‌شود کنترل های امنیت اطلاعات، در مرحله تعیین الزامات طراحی و خصوصیات پروژه ها و سیستم‌ها در نظر گرفته شود. قصور در انجام این کار ممکن است منجر به هزینه های اضافه و راه حلهایی با اثربخشی کمتر شود و شاید در بدترین شرایط منجر به ناتوانی در دستیابی به امنیت کافی شود.

توصیه می‌شود که به خاطر داشت؛ هیچ مجموعه ای از کنترل ها نمی‌توانند امنیت کامل را بدست دهند و توصیه می‌شود اقدام تکمیلی مدیریتی برای پایش، ارزیابی، و بهبود بازدهی و اثربخشی کنترل‌های امنیتی برای پشتیبانی از دستیابی به اهداف سازمان پیاده سازی شوند.

۵ خط‌مشی امنیتی

۵-۱ خط‌مشی امنیتی

هدف : فراهم آوری جهت‌گیری و حمایت مدیریت برای امنیت اطلاعات مطابق با الزامات کسب‌وکار و قوانین و مقررات مرتبط. توصیه می‌شود، مدیریت، خط مشی روشنی در ارتباط با اهداف کسب‌وکار اتخاذ نماید و حمایت و تعهد خود را به امنیت اطلاعات از این طریق صدور و نگهداری از خط‌مشی امنیت اطلاعات در سرتاسر سازمان به اثبات برساند.

۵-۱-۱ *مدرک خط‌مشی امنیت اطلاعات*

کنترل

توصیه می‌شود، یک سند خط‌مشی امنیت اطلاعات، توسط مدیریت تصویب و منتشر و به اطلاع همه کارکنان و اشخاص مرتبط بیرونی برسد.

راهنمای پیاده سازی

توصیه می‌شود، سند خط‌مشی امنیت اطلاعات تعهد مدیریت را بیان نماید و رویکرد سازمان به مدیریت امنیت اطلاعات را تعیین کند.

توصیه می‌شود، سند خط‌مشی محتوی بیانیه ای باشد که موارد زیر را شامل شود :

الف - تعریفی از امنیت اطلاعات، اهداف کلی آن، و دامنه کاربرد و اهمیت امنیت بعنوان ساز وکاری برای به اشتراک گذاشتن اطلاعات (رجوع کنید به مقدمه)؛

ب – بیانیه نیت مدیریت برای پشتیبانی از اهداف و اصول امنیت اطلاعات در راستای راهبرد و اهداف کسب‌وکار؛

پ - یک چارچوبی برای انتخاب کنترل‌ها و اهداف کنترلی، از جمله ساختار مدیریت و برآورد ریسک؛

ت - تشریح مختصری از خط مشی‌های امنیت، اصول، استانداردها و انطباق های قانونی مورد نظر سازمان از جمله :

۱- انطباق با قوانین و مقررات و الزامات قراردادی؛

۲- نیازمندیهای آگاه‌سازی، یادگیری و آموزش امنیت؛

۳- مدیریت استمرارکسب‌وکار؛

۴- پیامدهای حاصل از خطاهای خط‌مشی امنیت اطلاعات؛

ث - تعریفی از مسوولیت‌های عمومی و تخصصی مدیریت امنیت اطلاعات، از جمله گزارش رخدادهای امنیت اطلاعات؛

ج - ارجاع به مستنداتی که ممکن است خط‌مشی را پشتیبانی کند، از جمله برای یک سیستم اطلاعاتی خاص کدام یک از رویه ها و خط‌مشی‌های امنیتی مطابقت دارد یا توصیه می‌شود هر کاربری چه قواعدی را رعایت نماید.

توصیه می‌شود این خط مشی امنیت اطلاعات به نحوی که برای کلیه افراد قابل فهم باشد از طریق سازمان برای افراد تهیه شده و در دسترس افراد مربوطه قرار گیرد.

سایر اطلاعات

خط‌مشی امنیت اطلاعات ممکن است بعنوان بخشی از سند خط‌مشی عمومی باشد. اگر خط‌مشی امنیت اطلاعات به خارج از سازمان انتشار یابد، توصیه می‌شود مراقب بود اطلاعات حساس سازمان را فاش نکند. اطلاعات بیشتر را می‌توان در استاندارد ملی ایران به شماره ۱-۹۹۷۰ پیدا کرد.

۵-۱-۲ بازبینی خط‌مشی امنیت اطلاعات

کنترل

توصیه می‌شود خط‌مشی امنیت اطلاعات در بازه‌های زمانی برنامه ریزی شده بازبینی شود، یا اگر تغییرات معناداری رخ داد، تا همواره از مناسبت، کفایت و اثربخشی آن اطمینان حاصل شود.

راهنمای پیاده سازی

توصیه می‌شود، خط‌مشی دارای یک مالک باشد که از سوی مدیریت مسوولیت توسعه، بازبینی و ارزیابی خط‌مشی امنیت را برعهده گرفته است.توصیه می‌شود بازبینی شامل برآورد فرصت هایی برای بهبود در خط مشی امنیتی سازمان و رویکرد به مدیریت امنیت اطلاعات در واکنش به تغییرات در محیط سازمانی، رویدادهای کسب وکار، شرایط قانونی، یا محیط فنی، باشد.

توصیه می‌شود بازبینی خط مشی امنیت اطلاعات نتایج بررسی های مدیریت را مد نظر قرار دهد. توصیه می‌شود، رویه هایی تعریف شده برای بازبینی مدیریت، از جمله یک جدول زمان بندی یا دوره بازبینی وجود داشته باشند.

توصیه می‌شود ورودی بازبینی مدیریت شامل اطلاعاتی درباره موارد زیر باشد:

الف - بازخورد اشخاص ذینفع

ب - نتایج بازبینی های مستقل (رجوع کنید به ۶-۱-۸)

پ - وضعیت اقدام های اصلاحی و پیشگیرانه (رجوع کنید به ۶-۱-۸ و ۱۵-۲-۱)

ت - نتایج بازبینی های پیشین مدیریت

ث - انطباق با خط مشی امنیت اطلاعات و عملکرد فرایند

ج - تغییراتی که ممکن است بر رویکرد سازمان به مدیریت امنیت اطلاعات تاثیر بگذارد؛ از جمله تغییرات درمحیط سازمانی، شرایط کسب وکار، دسترسی به منابع، شرایط قراردادی، قانونی و حقوقی، یا محیط فنی؛

چ - روندهای مربوط به تهدیدها و آسیب پذیری ها؛

ح - رخدادهای گزارش شده امنیت اطلاعات (رجوع کنید به ۱۳-۱)؛

خ - پیشنهادات ارایه شده توسط مراجع مربوطه (رجوع کنید به ۶-۱-۶)؛

توصیه می‌شود خروجی بازبینی مدیریت شامل هر تصمیم و اقدامی درباره موارد زیر باشد:

الف - بهبود رویکرد سازمان در مدیریت امنیت اطلاعات و فرایندهای آن؛

ب - بهبود اهداف کنترلی و کنترل ها؛

پ - بهبود تخصیص منابع و/ یا مسوولیت ها.

توصیه می‌شود سابقه ای از بازبینی مدیریت نگهداری شود.

توصیه می‌شود تایید مدیریت برای خط مشی بازبینی شده اخذ شود.

۶ سازمان امنیت اطلاعات

۶-۱ سازمان داخلی

هدف : مدیریت امنیت اطلاعات در درون سازمان.
توصیه می‌شود یک چارچوب مدیریتی برای بنیان نهادن و کنترل نمودن پیاده سازی امنیت اطلاعات در درون سازمان تدوین شود.
توصیه می‌شود مدیریت خط‌مشی امنیت اطلاعات را تصویب و نقشهای امنیتی را تکلیف کند و پیاده سازی امنیت در سازمان را هماهنگ و بازبینی نماید.
توصیه می‌شود در صورت لزوم، یک منبع مشاوره تخصصی امنیت اطلاعات ایجاد و در دسترس سازمان قرار گیرد.
برقراری ارتباط با مشاوران خارج از سازمان برای آگاهی از وضعیت رویکردهای صنعتی، پایش استانداردها و روشهای ارزیابی و ارتباطات مناسب برای زمان وقوع رخدادهای امنیتی، گسترش داده می‌شود.
توصیه می‌شود رویکردی چند جانبه انظباطی برای امنیت اطلاعات ایجاد شود

۶-۱-۱ *تعهد مدیریت به امنیت اطلاعات*

کنترل
توصیه می‌شود مدیریت فعالانه، امنیت را در درون سازمان از طریق جهت‌گیری شفاف، تعهد اثبات شده، مکلف کردن به صورت صریح و اعلام مسوولیت‌های امنیت اطلاعات، حمایت نماید.
راهنمای پیاده سازی
توصیه می‌شود مدیریت:

الف - اطمینان حاصل کند که اهداف امنیت اطلاعات شناسایی می‌شوند، الزامات سازمان را برآورده می سازند و به صورت فرایندهای مرتبط یکپارچه شده اند؛
ب - خط‌مشی امنیت اطلاعات را قاعده سازی، بازبینی و تصویب کند؛
پ – اثربخشی اجرای خط‌مشی امنیت اطلاعات را بازبینی نماید؛
ت – جهت‌گیری مشخص و حمایت های مدیریتی مشهود برای طرحهای ابتکاری امنیت را فراهم آورد؛
ث - منابع لازم برای امنیت اطلاعات را تامین کند؛
ج – تخصیص نقش ها و مسوولیت های مشخص برای امنیت اطلاعات در سراسر سازمان را تایید نماید؛
چ - طرحها و برنامه هایی بمنظور آگاه سازی ازامنیت اطلاعات ایجاد نماید؛
ح - اطمینان حاصل کند که پیاده سازی کنترل‌های امنیت در سراسر سازمان هماهنگ شده اند؛

توصیه می‌شود مدیریت نیاز به مشاوره متخصصین داخلی و خارجی را شناسایی و نتایج مشورتی را در سراسر سازمان بازبینی نموده و هماهنگی های لازم را انجام دهد.
بر اساس اندازه سازمان، چنین مسوولیت‌هایی می‌توانست توسط یک مجمع مدیریتی اختصاصی یا بوسیله نهاد مدیریتی موجود، همچون هیات مدیره انجام شود.

سایر اطلاعات

اطلاعات بیشتر در استاندارد ملی ایران به شماره ۱-۹۹۷۰ وجود دارد.

۶-۱-۲ هماهنگی امنیت اطلاعات

کنترل

توصیه می‌شود فعالیتهای امنیت اطلاعات، توسط نمایندگانی از بخش‌های مختلف سازمان با نقش ها و کارکردهای شغلی مرتبط، هماهنگ شوند.

راهنمای پیاده سازی

به طور معمول، توصیه می‌شود هماهنگی امنیت اطلاعات شامل تعامل و همکاری مدیران، کاربران، راهبران[1]، طراحان برنامه های کاربردی، ممیزین، کارکنان امنیت و مهارت متخصصین این حوزه ها از جمله بیمه، موارد قانونی، منابع انسانی، فن‌آوری اطلاعات[2] یا مدیریت ریسک باشد.

توصیه می‌شود این فعالیت:

الف - تضمین نماید فعالیتهای امنیت، مطابق با خط‌مشی امنیت اطلاعات اجرا می‌شوند؛

ب - تعیین نماید چگونه با عدم انطباقها برخورد می‌شود؛

پ - روش شناسی و فرایندهایی برای امنیت اطلاعات، از جمله برآورد ریسک، طبقه‌بندی اطلاعات را تصویب کند؛

ت - تغییرات معنی دار در تهدید و در معرض تهدید قرار گرفتن اطلاعات و امکانات پردازش اطلاعات را شناسایی کند.

ث - کفایت هماهنگی در پیاده سازی کنترل‌های امنیت اطلاعات را ارزیابی کند.

ج - تحصیل، یادگیری و آگاه‌سازی امنیت اطلاعات در سراسر سازمان را بگونه ای اثربخش ارتقا دهد.

چ - اطلاعات حاصل از پایش و بازبینی رخدادهای امنیت اطلاعات را ارزیابی نموده و اقدامات مناسب را در پاسخ به رخدادهای شناسایی شدهٔ امنیت اطلاعات پیشنهاد نماید.

اگر سازمان از گروهی با عملکرد متقاطع[3] جداگانه استفاده نمی‌کند، برای مثال به این دلیل که این گروه برای اندازه سازمان مناسب نیست، توصیه می‌شود این اقدامات به نهاد مدیریتی مناسب و یا حتی مدیری مناسب سپرده شود.

۶-۱-۳ تخصیص مسوولیت‌های امنیت اطلاعات

کنترل

توصیه می‌شود تمامی مسوولیت‌های امنیت اطلاعات، به وضوح تعریف شوند.

راهنمای پیاده سازی

توصیه می‌شود تخصیص مسوولیت‌های امنیت اطلاعات مطابق با خط‌مشی امنیت اطلاعات (به بند ۴ رجوع شود) صورت پذیرد. توصیه می‌شود برای محافظت از تک تک داراییها و انجام فرایندهای امنیتی خاص، مسوولیت‌ها به

1- Administrators
2- Information Technology (IT)
3- Cross-Functional

گونه ای شفاف تعریف شوند. توصیه می‌شود این مسوولیت در صورت لزوم برای سایتهای خاص و امکانات پردازش اطلاعات با راهنمای جزیی‌تری تکمیل شود. توصیه می‌شود مسوولیت‌های محلی برای محافظت از داراییها و انجام فرایندهای خاص امنیتی، از قبیل طرح‌ریزی استمرار کسب‌وکار، بگونه ای شفاف تعریف شوند.
افراد با مسوولیت‌های امنیت تخصیص داده شده ممکن است وظیفه های امنیتی را به دیگران محول نمایند. با این حال، آنها همچنان مسوول بوده و توصیه می‌شود تعیین کنند وظایف محول شده به درستی انجام می‌شوند.
توصیه می‌شود محدودهٔ مسوولیت افراد بگونه ای شفاف بیان شود؛ بطور خاص موارد زیر باید رخ دهند :

الف – توصیه می‌شود دارایی‌ها و فرایندهای امنیتی مربوط به هر سیستم خاص شناسایی و به‌گونه ای شفاف تعریف شود؛

ب – توصیه می‌شود موجودیت مسوول در قبال هر دارایی یا فرایند امنیتی گماشته شده و جزئیات این مسوولیت مستند شود. (رجوع کنید به ۷-۱-۲)؛

پ – توصیه می‌شود سطوح اختیارات بطور شفاف تعریف گردیده و مستند شود؛

سایر اطلاعات

در بسیاری از سازمانها یک مدیر امنیت اطلاعات برای برعهده گیری مسوولیت کلان توسعه و پیاده سازی امنیت و پشتیبانی از کنترل‌های شناسایی شده منصوب خواهد شد.
با این وجود، مسوولیت تامین منابع و پیاده سازی کنترل‌ها اغلب بر عهده مدیران مختلف باقی خواهد ماند. یک تجربه مشترک این است که برای هر دارایی یک مالک مشخص شود که از آن به بعد مسوول محافظت روزانه از آن دارایی است.

۶-۱-۴ *فرایند مجوزدهی برای امکانات پردازش اطلاعات*

کنترل

توصیه می‌شود یک فرایند مجوزدهی مدیریتی برای امکانات جدید پردازش اطلاعات، تعریف و پیاده سازی شود.

راهنمای پیاده سازی

توصیه می‌شود خطوط راهنمای زیر برای فرایند مجوزدهی مد نظر قرار گیرند :

الف – توصیه می‌شود تجهیزات جدید دارای مجوزدهی مدیریت کاربری، مجوزدهی روش استفاده و دلیل استفاده، باشند. همچنین توصیه می‌شود، مجوز دهی از سوی مدیری که مسوول حفظ فضای امنیت سیستم اطلاعاتی محلی است، اخذ شود تا اطمینان حاصل شود کلیهٔ الزامات خط‌مشی های امنیت اطلاعات برآورده می‌شوند.

ب - هر جا که نیاز است، توصیه می‌شود نرم‌افزار و سخت افزار مورد بررسی قرار گیرد تا از سازگاری آنها با اجزا دیگر سیستم اطمینان حاصل شود.

پ - استفاده از امکانات پردازش اطلاعات شخصی یا خصوصی به عنوان مثال رایانه های قابل حمل، رایانه های خانگی یا وسایل قابل حمل، برای پردازش اطلاعات کسب وکار ممکن است خود باعث افزایش آسیب پذیری شود و بنابراین توصیه می‌شود کنترل‌های ضروری شناسایی و پیاده سازی شوند.

۶-۱-۵ توافق‌نامه‌های محرمانگی

کنترل

توصیه می‌شود الزاماتی برای قراردادهای محرمانگی یا عدم افشا که منعکس کننده نیازهای سازمان به حفاظت از اطلاعات است، شناسایی و بطور منظم بازبینی شوند.

راهنمای پیاده سازی

توصیه می‌شود قراردادهای محرمانگی یا عدم افشا به نیازمندیهای محافظت از اطلاعات محرمانه از طریق بکارگیری واژه های لازم الاجرای قانونی، اشاره کند. توصیه می‌شود برای شناسایی الزامات قراردادهای محرمانگی یا عدم افشا عناصر زیر مد نظر قرار گیرند :

الف – تعریفی از اطلاعاتی که باید محافظت شوند.(بعنوان مثال اطلاعات محرمانگی)؛

ب – طول مدت مورد انتظار برای یک قرارداد، دربرگیرنده مواردی که محرمانگی باید بطور نامحدود رعایت شود؛

پ - اقدامات مورد نیاز هنگامی که قرارداد خاتمه می پذیرد؛

ت - مسوولیت‌ها و اقدامات امضاکنندگان برای اجتناب از افشا اطلاعات غیر مجاز(مانند، "نیاز است که بداند")؛

ث - مالک اطلاعات، اطلاعات محرمانه تجاری و مالکیت معنوی و اینکه چگونه این با حفاظت از اطلاعات محرمانه مرتبط است؛

ج – اجازهٔ استفاده از اطلاعات محرمانه، و حق امضا استفاده از اطلاعات؛

چ - حق فعالیت‌های ممیزی و پایشی که شامل اطلاعات محرمانه می‌شوند.

ح - فرایندی برای اخطار و گزارش دهی افشا غیر مجاز یا رخنه در اطلاعات محرمانه؛

خ - مفادی[1] برای اطلاعاتی که باید در زمان خاتمه قرارداد عودت داده شوند یا از بین روند، و

د - اقدامات مورد انتظاری که در صورت تخطی از این قرارداد انجام می‌گیرند.

بر اساس الزامات امنیت سازمان، موارد دیگری ممکن است در باره قرارداد محرمانگی یا عدم افشا مورد نیاز باشد.

توصیه می‌شود قرارداد محرمانگی و عدم افشا، مطابق با قوانین و مقررات قابل اجرا برای حوزهٔ قضایی که در آن اجرا می‌شود، باشد. (رجوع کنید به ۱۵-۱-۱).

توصیه می‌شود الزامات قراردادهای محرمانگی و عدم افشا در بازه‌های زمانی منظم و هنگامی که تغییری روی داده که این الزامات را متاثر می‌کند، بازبینی شوند.

سایر اطلاعات

قراردادهای محرمانگی و عدم افشا، اطلاعات سازمانی را محافظت نموده و مسوولیت امضا کنندگان را برای حفظ، بکارگیری و افشا اطلاعات به شیوه‌ای مسوولانه و تفویضی، گوشزد می‌کند.

ممکن است یک سازمان نیازمند نمونه های مختلفی از قراردادهای محرمانگی و عدم افشا در شرایط مختلف باشد.

1- Terms

۶-۱-۶ برقراری ارتباط با مراجع دارای اختیار

کنترل

توصیه می‌شود ارتباطات مناسب با مراجع دارای اختیار مرتبط، حفظ شود.

راهنمای پیاده سازی

توصیه می‌شود سازمانها رویه هایی در اختیار داشته باشند که مشخص می‌کند در چه زمانی و با کدام یک از مراجع دارای اختیار (به عنوان مثال مجریان قانون، آتش نشانی، مراجع دارای اختیار نظارتی) تماس داشته باشند و چگونه توصیه می‌شود رخدادهای امنیت اطلاعات شناسایی شده در زمان مناسب گزارش دهی شوند، اگر این تردید وجود دارد که قانونی نقض شده است.

سازمانهای تحت شرایط حمله از طریق اینترنت ممکن است نیاز به شخص سوم بیرونی (به عنوان مثال یک ارایه کننده خدمت اینترنتی[1] یا اپراتور ارتباطاتی) برای اقدام در مقابل منبع حمله داشته باشند.

سایر اطلاعات

حفظ چنین ارتباطاتی ممکن است از ملزومات پشتیبانی از مدیریت رخدادهای امنیت اطلاعات (رجوع کنید به بخش ۱۳-۲) یا فرایند طرح‌ریزی استمرار کسب‌وکار و احتیاطی[2] (بخش ۱۴) ضروری باشد. همچنین تماس با نهادهای تنظیم مقررات[3]، برای پیش بینی و آمادگی برای تغییرات آتی در قوانین یا مقرراتی که توسط سازمان باید رعایت شوند، مفید است. تماس با دیگر مراجع دارای اختیار، شامل شرکت های خدماتی دولتی، خدمات اضطراری، و سلامت و ایمنی به عنوان مثال آتش نشانی (در رابطه با استمرار کسب وکار)، تامین کنندگان ارتباطاتی (در رابطه با مسیریابی خط و در دسترس پذیری)، تامین کنندگان آب (در رابطه با امکانات خنک‌کننده برای تجهیزات) می‌شود.

۶-۱-۷ برقراری ارتباط با گروههای بامنافع خاص

کنترل

توصیه می‌شود ارتباطات مناسب با گروه‌های دارای گرایش خاص یا سایر مجمع‌های[4] امنیتی تخصصی و انجمن‌های حرفه ای، حفظ شود.

راهنمای پیاده سازی

توصیه می‌شود، عضویت در گروه‌های دارای گرایش خاص یا مجمع ها به منظور زیر در نظر گرفته شود :

الف - توسعه دانش دربارهٔ بهترین تجربیات و بروز نگهداشتن اطلاعات مرتبط با امنیت اطلاعات؛

ب - اطمینان از اینکه درک از محیط امنیت اطلاعات کنونی[5] و کامل است؛

پ – دریافت پیش از موعد هشدارهای آماده‌باش[6]، توصیه‌ها و وصله[7]های مربوط به حملات و آسیب‌پذیری‌ها؛

1- Internet Service Provider
2- Contingency
3- Regulatory Bodies
4- Forums
5- Current
6- Alerts
7- Patch

ت - دسترسی به توصیه های تخصصی امنیت اطلاعات؛

ث - به اشتراک گذاری و تبادل اطلاعات درباره فن‌آوری ها، محصولات، تهدیدات یا آسیب پذیری های جدید؛

ج - تدارک نقاط ارتباطی مناسب در هنگام برخورد با رخدادهای امنیت اطلاعات (همچنین رجوع کنید به بند ۱۳- ۲-۱)؛

سایر اطلاعات

قراردادهای به اشتراک گذاری اطلاعات می‌تواند به منظور بهبود همکاری و هماهنگی در موضوعات امنیتی تدوین شوند. توصیه می‌شود این قبیل قراردادها نیازمندیهای محافظت از اطلاعات حساس را شناسایی نمایند.

۸-۱-۶ *بازنگری مستقل امنیت اطلاعات*

کنترل

توصیه می‌شود، رویکرد سازمان به امنیت اطلاعات و پیاده سازی آن (به عبارت دیگر اهداف کنترل، کنترل‌ها، خط‌مشی ها، فرایندها و رویه ها برای امنیت اطلاعات)، در فواصل زمانی طرح‌ریزی شده یا هنگامیکه تغییرات عمده ای در پیاده سازی امنیت اطلاعات رخ داد، مستقلاً بازبینی شود.

راهنمای پیاده سازی

توصیه می‌شود بازبینی مستقل توسط مدیریت آغاز شود. چنین بازبینی مستقلی برای اطمینان از تداوم مناسب بودن، کفایت و اثربخشی رویکرد سازمان به مدیریت امتیت اطلاعات ضروری است. توصیه می‌شود بازبینی شامل ارزیابی فرصتهای بهبود و نیاز به تغییرات رویکردی در امنیت که شامل خط‌مشی و اهداف کنترلی می‌شود، باشد. توصیه می‌شود این بازبینی توسط افرادی مستقل از حیطه بازبینی بعنوان مثال فعالیت ممیزی داخلی، یک مدیر مستقل یا سازمان ثالث متخصص در چنین بازبینی هایی انجام شود. افرادی که اینگونه بازبینی ها را انجام می‌دهند توصیه می‌شود از مهارت و تجربه مناسب برخوردار باشند.

توصیه می‌شود نتایج بازبینی های مستقل ثبت شده و به مدیریتی که آغازگر این بازبینی ها بوده است، گزارش شود. توصیه می‌شود این سوابق نگهداری شوند.

اگر بازبینی‌های مستقل نشان دهند که رویکرد سازمان و اجرای مدیریت امنیت اطلاعات کافی نبوده و یا با جهت‌گیری بیان شده در سند خط‌مشی امنیت اطلاعات منطبق نیست (رجوع کنید به بند ۵-۱-۱)، توصیه می‌شود مدیریت اقدامهای اصلاحی را در این موارد مد نظر قرار دهد.

سایر اطلاعات

حوزه‌ای که توصیه می‌شود مدیران بصورت منظم بازبینی کنند (رجوع کنید به بند ۱۵-۲-۱)، ممکن است مستقلاً بازبینی شود. روشهای بازبینی ممکن است شامل مصاحبه با مدیران، بررسی سوابق یا بازبینی اسناد خط‌مشی امنیت باشد. استاندارد ملی ایران ایزو ۱۹۰۱۱: سال ۱۳۸۶[1]، رهنمودهایی برای ممیزی سیستم‌های مدیریت کیفیت و / یا زیست محیطی بوده و ممکن است همچنین برای انجام بازبینی مستقل، که شامل تدوین و

---

[1]- منظور استاندارد ملی معادل استاندارد بین المللی ISO 19011:2002 می باشد.

پیاده‌سازی برنامه بازبینی است، راهنمای مفیدی را ارایه نماید. بخش ۱۵-۳ کنترل‌های مرتبط با بازبینی مستقل برای سیستم‌های اطلاعات عملیاتی و بکارگیری ابزارهای ممیزی سیستم را معین می‌کند.

۶-۲ اشخاص بیرونی

هدف : حفظ و نگهداری امنیت اطلاعات و امکانات پردازش اطلاعات سازمان که در دسترس طرفهای بیرونی قرار داشته یا توسط ایشان پردازش یا مدیریت شده یا با آنها مبادله می‌شوند.
توصیه می‌شود امنیت اطلاعات سازمانی و تجهیزات پردازش اطلاعات با ورود محصولات یا خدمات طرفهای بیرونی کاهش نیابد.
توصیه می‌شود هر دسترسی به امکانات پردازش اطلاعات سازمان و پردازش و ارتباط اطلاعاتی بوسیله طرف‌های بیرونی کنترل شود.
در جایی که نیاز کسب‌وکار،کارکردن با طرفهای بیرونی را بطلبد،که ممکن است نیاز به دسترسی اطلاعات سازمانی و امکانات پردازش اطلاعات، یا بدست آوردن یا تامین محصول یا خدمت از یا برای طرف بیرونی باشد، توصیه می‌شود برآورد ریسکی بمنظور تعیین عواقب امنیتی و الزامات کنترلی انجام شود. توصیه می‌شود، کنترل‌ها با طرف بیرونی مورد توافق قرار گرفته و در قراردادی با آنها تعریف شود.

۶-۲-۱ *شناسایی ریسک‌های مرتبط با اشخاص بیرونی*

کنترل

توصیه می‌شود ریسک‌های اطلاعات و امکانات پردازش اطلاعات سازمان ناشی از فرایندهای کسب‌وکار مرتبط با اشخاص بیرونی شناسایی شده و پیش از اعطای دسترسی، کنترل‌های مناسب پیاده سازی شوند.

راهنمای پیاده سازی

در جایی که نیاز به اجازه دسترسی شخص بیرونی به امکانات پردازش اطلاعات یا اطلاعات یک سازمان است، توصیه می‌شود برآورد ریسک (همچنین رجوع کنید به بخش ۴) بمنظور شناسایی هرگونه الزاماتی از کنترل‌های خاص صورت پذیرد. توصیه می‌شود شناسایی ریسک‌های مرتبط به دسترسی شخص بیرونی در زمینه های زیر مد نظر قرار گیرد :

الف - امکانات پردازش اطلاعاتی که نیاز است شخص بیرونی به آنها دسترسی داشته باشد؛

ب - نوع دسترسی که شخص بیرونی به تجهیزات پردازش اطلاعات خواهد داشت، به عنوان مثال :

۱ - دسترسی فیزیکی به عنوان مثال به دفاتر، اتاق‌های رایانه، کشوهای بایگانی[1]؛

۲ - دسترسی منطقی به عنوان مثال به پایگاه داده‌های سازمانی، سیستم‌های اطلاعاتی؛

۳ - شبکه ارتباطی بین سازمان و شبکه شخص بیرونی به عنوان مثال ارتباط دائم یا دسترسی از راه دور؛

۴ – آیا دسترسی از درون یا بیرون محیط کار اتفاق می افتد.

پ- ارزش و حساسیت اطلاعات و میزان حیاتی بودن آنها برای عملیات کسب‌وکار؛

1- Filing cabinets

ت - کنترل‌های لازم برای محافظت از اطلاعاتی که قرار نیست اشخاص بیرونی به آنها دسترسی داشته باشند؛

ث - کارکنان شخص بیرونی که با اطلاعات سازمانی سر و کار دارند.

ج - چگونه سازمان یا کارکنانی که مجاز به دسترسی، شناسایی می‌شوند، مجوزها چگونه تصدیق می‌شوند، چند وقت به چند وقت این نیازها مجدداً تایید می‌شوند.

چ - ابزارهای متفاوت و کنترل های به کار گرفته شده توسط شخص بیرونی در زمان ذخیره، پردازش، انتقال، اشتراک و تبادل اطلاعات؛

ح - پیامد دسترسی به شخص بیرونی که در زمان لازم در دسترس نباشد و شخص بیرونی که اطلاعات گمراه کننده یا غیردقیق را وارد یا دریافت می‌کند؛

خ - اقدامات و رویه های پرداختن به رخدادهای امنیت اطلاعات و آسیب های بالقوه و مفاد و شرایط استمرار دسترسی شخص بیرونی در صورت بروز یک رخداد امنیت اطلاعات؛

د - الزامات قانونی و مقرراتی و دیگر تعهدات قراردادی در رابطه با شخص بیرونی که توصیه می‌شود لحاظ شوند؛

ذ - این که منافع هر یک از ذینفعان دیگر ممکن است چگونه تحت تاثیر توافقات قرار می‌گیرد؛

توصیه می‌شود دسترسی اشخاص بیرونی به اطلاعات سازمان تا زمانی که کنترل های مناسب اجرا نشده‌اند و یا در صورت امکان تا زمانی که قراردادی که مفاد و شرایط ارتباط یا دسترسی را تعریف می‌کند، امضا نشده است، فراهم نشود. بطور کلی، توصیه می‌شود تمام الزامات امنیت اطلاعات که از کار با اشخاص بیرونی یا کنترل‌های داخلی ناشی می‌شوند از طریق قرارداد با شخص بیرونی منعکس شود (همچنین رجوع کنید به ۶-۲-۲ و۶-۲-۳). توصیه می‌شود از اینکه که شخص بیرونی از تعهداتش[1] آگاه است و مسوولیت ها و تعهدات[2] مربوط به دسترسی، پردازش، انتقال، یا مدیریت اطلاعات سازمان و تجهیزات پردازش اطلاعات را می پذیرد، اطمینان حاصل شود.

سایر اطلاعات

اطلاعات ممکن است توسط اشخاص بیرونی با مدیریت نامناسب امنیت به خطر بیفتد. توصیه می‌شود کنترل‌ها شناسایی شوند و برای ایجاد امکان دسترسی شخص بیرونی به تجهیزات پردازش اطلاعات به کار گرفته شوند. برای مثال، اگر نیاز خاصی به محرمانه بودن اطلاعات وجود دارد، می‌توان از قراردادهای عدم افشا استفاده کرد.

اگر بیشتر نیازها به منابع از خارج تامین شود، یا در جایی که چندین شخص خارجی نقش دارند، سازمان ها ممکن است با ریسک‌های مرتبط با فرایندها، مدیریت، و ارتباطات بین سازمانی روبرو شوند.

کنترل های ۶-۲-۲ و ۶-۲-۳ چیدمان‌های متفاوت توافقات شخص بیرونی را پوشش می دهند از جمله:

الف - ارایه دهندگان خدمات، نظیر ارایه دهندگان خدمات اینترنتی، ارایه کنندگان خدمات شبکه، خدمات تلفن، خدمات نگهداری و پشتیبانی

ب - خدمات امنیت مدیریت شده

پ - مشتریان

1- Obligations
2- Liabilty

ت – برون‌سپاری امکانات یا عملیات، به عنوان مثال سامانه های فن‌آوری اطلاعات، خدمات جمع آوری داده، عملیات مرکز تماس

ث - مشاوران مدیریت و بازرگانی، و ممیزان

ج - توسعه دهندگان و تامین کنندگان؛ به عنوان مثال تهیه‌کنندگان محصولات نرم‌افزاری و سیستم‌های فن‌آوری اطلاعات.

چ - نظافت، تدارکات[1] و سایر خدمات پشتیبانی برون سپاری شده.

ح - کارکنان موقت، جابجایی کارآموزان و دیگر انتصابات کوتاه مدت

این قراردادها می‌توانند به کاهش ریسک های مربوط به اشخاص بیرونی کمک کنند.

۶-۲-۲ *نشانی دهی امنیت هنگام سروکار داشتن با مشتریان*

کنترل

توصیه می‌شود، تمام الزامات امنیتی شناسایی شده، پیش از اعطای دسترسی به اطلاعات یا اموال سازمان به مشتری، مورد نشانی دهی شوند.

راهنمای پیاده سازی

توصیه می‌شود مفاد زیر برای پرداختن به امنیت قبل از ایجاد دسترسی به هر یک از دارایی‌های سازمان برای مشتریان در نظر گرفته شوند (بسته به نوع و وسعت دسترسی داده شده، ممکن همه آنها اعمال نشوند):

الف - محافظت از دارایی، شامل:

۱ - رویه هایی برای محافظت از دارایی‌های سازمان از جمله اطلاعات و نرم‌افزار و مدیریت آسیب پذیری های شناخته شده

۲- رویه هایی برای تعیین این که آیا خدشه ای به دارایی‌ها، به عنوان مثال از دست دادن یا تغییر داده‌ها رخ داده است یا نه.

۳- یکپارچگی

۴- محدودیت هایی درباره تکثیر و افشا اطلاعات

ب - توصیف محصول یا خدماتی که ارایه می‌شود

پ - دلایل، الزامات، و منافع متفاوت برای دسترسی مشتریان

ت - خط مشی کنترل دسترسی، پوشش دهنده:

۱- روش های دسترسی مجاز، و کنترل و استفاده از شناسه های منحصربه فردی نظیر شناسه کاربری و کلمه عبور

۲- یک فرایند مجوزدهی برای دسترسی کاربر و اختیارات ویژه

۳- بیانیه ای که تمام دسترسی هایی که صراحتاً مجوزدهی نشده اند، ممنوع هستند.

۴- فرایندی برای سلب حقوق دسترسی یا قطع ارتباط بین سیستم‌ها

1- Catering

ث - توافقاتی برای گزارش، اعلام، و بازرسی عدم دقت در اطلاعات(به عنوان مثال جزئیات شخصی)، رخدادهای امنیت اطلاعات و رخنه های امنیتی[1]

ج - شرح هر خدمتی که باید در دسترس قرار گیرد

چ - سطح مورد نظر[2] خدمت و سطوح غیر قابل قبول خدمات

ح - حق پایش، ابطال[3]، هر فعالیتی در رابطه با دارایی‌های سازمان

خ - ارتباطات بین هر سازمان و مشتری

د - مسوولیت هایی در رابطه با مورد قانونی و این که چگونه اطمینان حاصل می‌شود که الزامات قانونی برآورده می‌شوند؛ به عنوان مثال قوانین محافظت از داده‌ها، به خصوص احتساب سیستم‌های قانونی ملی متفاوت در صورتی که قرارداد دربرگیرنده همکاری با مشتریان در دیگر کشورها باشد. (همچنین رجوع کنید به ۱۵-۱)

ذ - حقوق مالکیت فکری و واگذاری حق تکثیر (رجوع کنید به ۱۵-۱-۲) و محافظت از هر کار مشترک (همچنین رجوع کنید به ۶-۱-۵)

سایر اطلاعات

الزامات امنیت اطلاعات در رابطه با دسترسی مشتریان به دارایی‌های سازمانی ممکن است بسته به امکانات پردازش اطلاعات و اطلاعاتی که مورد دسترسی قرار می‌گیرد، متفاوت باشد. این الزامات امنیتی را می‌توان با استفاده از قراردادهای مشتری که حاوی تمام ریسک های شناخته شده و الزامات امنیتی است، نشانی دهی کرد. (رجوع کنید به ۶-۲-۱)

قرارداد با اشخاص بیرونی، ممکن است همچنین دربرگیرنده اشخاص دیگر باشد. توصیه می‌شود، قراردادهایی که به شخص بیرونی امکان دسترسی می دهند شامل اجازه هایی برای تعیین دیگر اشخاص مجاز و شرایط برای دسترسی و مشارکت آنها باشند.

۶-۲-۳ *نشانی‌دهی امنیت در توافق‌های شخص‌سوم*

کنترل

توصیه می‌شود، توافق‌نامه های منعقده با اشخاص ثالثی که شامل اعطای دسترسی، پردازش، تبادل یا مدیریت اطلاعات یا امکانات پردازش اطلاعات سازمان، یا اضافه کردن محصولات یا خدمات به امکانات پردازش اطلاعات هستند، تمامی الزامات امنیتی مرتبط را پوشش دهند.

راهنمای پیاده سازی

توصیه می‌شود، قرارداد از اینکه که هیچ گونه سوء تفاهمی بین سازمان و شخص سوم وجود ندارد، اطمینان دهد.

توصیه می‌شود، سازمان ها خسارت خود را از شخص سوم به طور کامل اخذ نمایند.

توصیه می‌شود، مفاد زیر در قرارداد همکاری گنجانده شوند تا الزامات امنیتی شناخته شده را برآورده کنند. (رجوع کنید به ۶-۲-۱)

الف - خط مشی امنیت اطلاعات

1- Security Breaches
2- Target
3- Revoke

ب - کنترل هایی برای حصول اطمینان از محافظت از دارایی‌ها از جمله:

۱- رویه هایی برای محافظت از دارایی‌های سازمانی از جمله اطلاعات، نرم‌افزار، و سخت افزار

۲- هر گونه کنترل و سازوکار محافظت فیزیکی مورد نیاز

۳- کنترل‌هایی برای حصول اطمینان از محافظت در برابر نرم‌افزار مخرب (رجوع کنید به۱۰-۴-۱)

۴- رویه هایی برای تعیین این که آیا هیچگونه آسیب و خدشه ای به دارایی‌ها، از جمله از دست رفتن یا تغییر اطلاعات، نرم‌افزار، و سخت افزار وارد آمده است یا نه.

۵- کنترل هایی برای حصول اطمینان از بازگرداندن یا امحا اطلاعات و دارایی‌ها در پایان یا در یک زمان مورد توافق در طول زمان قرارداد.

۶- محرمانگی، یکپارچگی، در دسترس پذیری و هر گونه مالکیت مرتبط با دارایی‌ها (رجوع کنید به ۲-۱-۵)

۷- محدودیت هایی در رابطه با تکثیر و افشای اطلاعات و استفاده از قراردادهای محرمانه (رجوع کنید به ۶-۱-۵)

پ - آموزش کاربر و سرپرست درباره روش ها، رویه ها و امنیت

ت - حصول اطمینان از آگاهی کاربر از مسوولیت ها و مسائل امنیت اطلاعات

ث - تمهیداتی برای انتقال کارکنان در موارد مقتضی

ج - مسوولیت هایی در رابطه با نصب و نگهداری سخت افزار، و نرم‌افزار

چ - یک ساختار گزارش دهی واضح و قالب های گزارش دهی مورد توافق

ح - یک فرایند روشن و مشخص از مدیریت تغییر

خ - خط مشی کنترل دسترسی که موارد زیر را پوشش دهد:

۱- دلایل، الزامات، و منافع متفاوتی که دسترسی شخص سوم را ضروری می نماید.

۲- روش های دسترسی مجاز و کنترل و استفاده از شناسه های منحصربه فرد نظیر شناسه‌های کاربری و کلمات عبور.

۳- یک فرایند مجوزدهی برای دسترسی و اختیارات ویژه کاربران.

۴- یکی از الزامات برای حفظ فهرستی از افراد مجاز برای استفاده از خدماتی که در دسترس قرار می‌گیرد و این که حقوق و مزایای آنها در رابطه با این استفاده کدام است.

۵- بیانیه ای که تمام‌دسترسی هایی که صراحتاً مجوزدهی نشده اند، ممنوع هستند.

۶- فرایندی برای بازپس گیری حقوق دسترسی یا قطع ارتباط بین سیستم‌ها

د - هماهنگی هایی برای گزارش دهی، اطلاع، و بررسی رخدادهای امنیت اطلاعات و رخنه امنیتی و نیز تخلفات از الزامات بیان شده در قرارداد؛

ذ - توصیفی از محصول یا خدمتی که ارایه خواهد شد، و توصیفی از اطلاعاتی که در کنار این طبقه بندی امنیتی در دسترس قرار می‌گیرد(رجوع کنید به ۷-۲-۱)

ر - سطح هدف خدمات و سطوح غیرقابل قبول خدمات

ز - تعریف معیارهای عملکرد قابل تصدیق، پایش و گزارش دهی آنها

ژ - حق پایش، و ابطال هر فعالیت مربوط به دارایی‌های سازمان

س - حق ممیزی مسوولیت های تعریف شده در قرارداد، برای انجام این ممیزی ها توسط یک شخص سوم و لحاظ کردن حقوق آئین نامه ای ممیزان

ش – گنجاندن ماده ای برای فرایند حل مشکلات

ص - الزامات استمرار خدمات از جمله اقداماتی برای دسترسی و اطمینان پذیری در رابطه با اولویت های کسب وکار سازمان

ض - مسوولیت های مربوطه طرفین، نسبت به قرارداد

ط - مسوولیت هایی در رابطه با موضوعات قانونی و نحوه تضمین این که الزامات قانونی رعایت می‌شوند، مثلا قوانین محافظت از داده‌ها، به خصوص به حساب آوردن سیستم‌های قانونی ملی متفاوت در صورتی که قرارداد دربرگیرنده همکاری با سازمان های کشورهای دیگر است(همچنین رجوع کنید به ۱۵-۱)

ظ - حقوق مالکیت فکری و حق تکثیر(رجوع کنید به ۱۵-۱-۲) و محافظت از هر کار مشترک (همچنین رجوع کنید به ۶-۱-۵)

ع - مشارکت شخص سوم با پیمانکاران فرعی و کنترل های امنیتی که این پیمانکاران فرعی باید اجرا کنند.

غ - شرایطی برای مذاکره مجدد/خاتمه قراردادها

۱- توصیه می‌شود، در صورتی که هر یک از طرفین بخواهد رابطه را قبل از پایان قراردادها به پایان برساند برنامه احتیاطی، در نظر گرفته شود

۲- مذاکره مجدد درباره قراردادها در صورتی که الزامات امنیتی سازمان تغییر کند

۳- مستندسازی از فهرست دارایی‌ها، پروانه ها، قراردادهای حال حاضر یا حقوق مربوط به آنها

سایر اطلاعات

قراردادها ممکن است برای سازمان های متفاوت و در میان انواع مختلف اشخاص ثالث، متفاوت باشند. بنابراین، توصیه می‌شود که مراقب بود تمام ریسک‌ها شناخته شده و الزامات امنیتی در قراردادها گنجانده شوند (همچنین رجوع کنید به ۶-۲-۱). در صورت لزوم، کنترل ها و رویه های مورد نیاز را می‌توان در یک برنامه مدیریت امنیت گسترش داد.

توصیه می‌شود، اگر مدیریت امنیت اطلاعات برونسپاری شود، قرارداد به این بپردازد که شخص سوم چگونه تضمین خواهد کرد که امنیت مناسب همان طور که در برآورد ریسک تعریف شده است حفظ خواهد شد و امنیت چگونه برای شناسایی و پرداختن به ریسک‌ها رعایت خواهد شد.

بعضی از تفاوت های بین تامین منابع از بیرون و دیگر شکل های تامین خدمات توسط شخص سوم، شامل سوال درباره مسوولیت، طرح‌ریزی، دوره گذر و اختلال بالقوه در عملیات در طول آن دوره، برنامه ریزی سازگاری، هماهنگی ها و گزارش ها و جمع آوری و مدیریت اطلاعات درباره رخدادهای امنیتی می باشند. بنابراین مهم است که سازمان گذر به یک توافق برون سپاری شده را طرح‌ریزی ریزی و مدیریت کند و فرایند مناسبی را برای مدیریت تغییرات و مذاکره مجدد/خاتمه قراردادها داشته باشد.

رویه هایی برای استمرار پردازش در صورتی که شخص سوم از تامین خدماتش ناتوان باشد باید در قرارداد در نظر گرفته شود تا از هر گونه تاخیر در هماهنگ کردن خدمات جایگزینی اجتناب شود.

قرارداد با اشخاص ثالث ممکن است همچنین دربرگیرنده اشخاص ثالث دیگر نیز باشد. توصیه می‌شود، قراردادهایی که به اشخاص ثالث امکان دسترسی می دهد، شامل اجازه برای تعیین دیگر اشخاص مجاز و شرایطی برای دسترسی و مشارکت آنها باشد.

عموما، قراردادها توسط سازمان تدوین می‌شوند. ممکن است در بعضی مواقعی قراردادی طراحی شود و توسط یک شخص سوم به سازمان تحمیل شود. سازمان باید تضمین کند که امنیت تحت تاثیر الزامات قراردادهای تدوین شده شخص سوم، قرار نمی‌گیرد.

۷ مدیریت دارایی

۷-۱ مسوولیت داراییها

هدف: دستیابی به حفاظت مناسب از دارایی های سازمانی و ادامه دادن این کار.

توصیه می‌شود که برای همهٔ دارایی ها مالک مشخص شود و این دارایی ها برای مالک شمارش شوند.

توصیه می‌شود که مالکین برای همهٔ دارایی ها مشخص شده باشند و توصیه می‌شود که مسوولیت نگهداری کنترل‌های مناسب، واگذار شود. اجرای کنترل های خاص ممکن است توسط مالک (به یک شخص یا سازمان دیگر) محول شود، اما مالک، مسوول محافظت مناسب از دارایی ها باقی می ماند.

۷-۱-۱ *لیست موجودی اموال*

کنترل

توصیه می‌شود که تمام دارایی‌ها به وضوح شناسایی شوند و لیست موجودیی از تمام دارایی‌های مهم، تنظیم و نگهداری شود.

راهنمای پیاده سازی

توصیه می‌شود که سازمان تمام دارایی‌ها را شناسایی کرده و اهمیت این دارایی‌ها را مستند کند. توصیه می‌شود که این فهرست دارایی‌ها تمام اطلاعات لازم برای بازیابی پس از حادثه، از جمله نوع دارایی، قالب، محل، اطلاعات پشتیبان، اطلاعات گواهی، و یک ارزش تجاری را شامل باشد. توصیه می‌شود که لیست موجودی اموال، نسخه دوم از دیگر فهرست های غیرضروری نباشد، اما توصیه می‌شود که از به جا بودن محتوای آن، اطمینان حاصل شود.

به علاوه، توصیه می‌شود که مالکیت (رجوع کنید به ۷-۱-۲) و طبقه بندی اطلاعات (رجوع کنید به ۷-۲)، مورد توافق قرار گیرد و برای هر یک از دارایی‌ها، مستند شود. توصیه می‌شود که بر اساس اهمیت دارایی، ارزش تجاری آن و طبقه بندی امنیتی آن، سطوح محافظت متناسب با اهمیت دارایی‌ها، شناسایی شوند (اطلاعات بیشتر درباره نحوه ارزش گذاری دارایی‌ها با هدف بیان اهمیت آنها، در ISO/IEC 13335-3 قابل مشاهده است).

سایر اطلاعات

دارایی‌ها انواع بسیاری دارند، از جمله موارد زیر:

الف - اطلاعات: بانک‌های اطلاعاتی و فایل های داده، قراردادها و توافق‌نامه‌ها، مستندات سیستم، اطلاعات تحقیق، راهنماهای کاربر، محتوای آموزشی، رویه‌های عملیاتی یا پشتیبانی، طرح‌های استمرار کسب وکار، تفاهم نامه‌های پشتیبانی، گزارش‌های ممیزی، و اطلاعات کسب شده؛

ب – دارایی‌های نرم‌افزاری: نرم‌افزارهای کاربردی، نرم‌افزار سامانه، ابزارهای توسعه، و نرم‌افزارهای کمکی؛

پ – دارایی‌های فیزیکی: تجهیزات رایانه‌ای، تجهیزات ارتباطی، رسانه‌های قابل جابجایی، و سایر تجهیزات؛

ت - خدمات: خدمات محاسبه ای و ارتباطی، تجهیزات عمومی؛ مانند گرمایش، نور، برق و تهویه هوا

ث - افراد و صلاحیت، مهارت ها و تجربه های آنها؛

ج - موارد ناملموس مانند اعتبار و خوشنامی سازمان

فهرست دارایی‌ها کمک می‌کند تا این اطمینان ایجاد شود که از دارایی‌ها به نحو موثر محافظت می‌شود، و همچنین ممکن است برای دیگر اهداف تجاری نظیر سلامت و امنیت، بیمه یا دلایل مالی (مدیریت دارایی) لازم باشد. فرایند تدوین یک فهرست از دارایی‌ها، یک پیش نیاز مهم از مدیریت ریسک است (رجوع به بخش ۴).

۷-۱-۲ *مالکیت دارایی‌ها*

کنترل

توصیه می‌شود که تمام اطلاعات و دارایی‌های مرتبط با امکانات پردازش اطلاعات، در تملک[1] بخش معینی از سازمان باشند.

راهنمای پیاده سازی

توصیه می‌شود که مالک دارایی مسوول موارد زیر باشد:

الف - تضمین این‌که اطلاعات و دارایی‌های مربوط به تجهیزات پردازش اطلاعات به‌طور مناسب طبقه بندی شده‌اند.

ب - تعریف و بازنگری دوره‌ای محدودیت های دسترسی و طبقه‌بندی‌ها، به حساب آوردن خط‌مشی‌های کنترل دسترسی.

مالکیت ممکن است به موارد زیر اختصاص داده شود:

الف - یک فرایند تجاری؛

ب - مجموعه تعریف شده ای از فعالیت ها؛

پ - یک نرم‌افزار کاربردی؛ یا

ت – یک مجموعه تعریف شده از داده‌ها.

سایر اطلاعات

وظایف متداول را می‌توان واگذار کرد، مثلا به یک نگهبان که بصورت روزانه مراقب دارایی‌ها است، ولی مسوولیت به عهده مالک دارایی است.

۱- واژه "مالک" بعنوان موجودیت یا شخصی شناخته می‌شود که مسوولیت‌های تایید شده مدیریت را برای کنترل محصول، بهبود، حفظ و تگهداری، استفاده و امنیت داراییی ها، را دارد. واژه "مالک" به معنی شخصی که عملا حقوق مالکیت بر دارایی را دارد، نیست.

در سامانه های اطلاعاتی پیچیده، معین کردن گروه هایی از دارایی‌ها که با یکدیگر عمل می‌کنند تا یک وظیفه خاص تحت عنوان "خدمات" را ارایه کنند، ممکن است مفید باشد. در این نمونه، مسوولیت تحویل خدمت که شامل عملکرد دارایی‌های فراهم کننده آن خدمت نیز می باشد، بر عهده مالک خدمت است.

۷-۱-۳ *استفاده قابل قبول از دارایی‌ها*

کنترل

توصیه می‌شود که قوانینی برای استفادهٔ قابل قبول از اطلاعات و دارایی‌های مرتبط با امکانات پردازش اطلاعات، مشخص و مستندسازی و پیاده سازی شوند.

راهنمای پیاده سازی

توصیه می‌شود که تمام کارمندان، پیمانکاران، و کاربران شخص سوم از قوانین استفاده قابل قبول از اطلاعات و دارایی‌های مرتبط با تجهیزات پردازش اطلاعات، پیروی کنند. این قوانین شامل موارد زیر هستند:

الف - قوانین پست الکترونیک و استفاده از اینترنت (رجوع کنید به ۱۰-۸)

ب –رهنمودهای استفاده از دستگاه های متحرک/سیار به خصوص برای استفاده خارج از محوطه‌های سازمان (رجوع کنید به ۱۱-۷-۱)

توصیه می‌شود که قوانین خاص یا راهنمایی‌هایی توسط مدیریت، کارفرمایان و پیمانکاران مربوطه فراهم شوند.

توصیه می‌شود که کاربران اشخاص ثالثی که از دارایی‌های سازمان استفاده می‌کنند یا به آن دسترسی دارند، از محدودیت های موجود برای استفاده آنها از اطلاعات و دارایی‌های سازمان در رابطه با تجهیزات پردازش اطلاعات و منابع، آگاه باشند. توصیه می‌شود که این اشخاص برای استفاده خود از منابع پردازش اطلاعات و هر گونه کاربری انجام شده با مسوولیت آنها، مسوول شناخته شوند.

۷-۲ طبقه بندی اطلاعات

هدف: حصول اطمینان نسبت به اینکه، اطلاعات به سطح حفاظتی مناسبی رسیده اند.

توصیه می‌شود که اطلاعات برای نشان دادن نیاز، اولویت ها، و میزان محافظت مورد انتظار در زمان اداره اطلاعات، طبقه بندی شوند.

اطلاعات دارای درجه های حساسیت و بحرانی بودن متفاوتی هستند. بعضی موارد ممکن است نیازمند یک سطح محافظت اضافه یا اداره بصورت ویژه باشند. توصیه می‌شود که از یک طرح طبقه بندی اطلاعات برای تعریف مجموعه مناسبی از سطوح محافظت و تبادل اطلاعات مورد نیاز برای رسیدگی به موارد خاص، استفاده شود.

۷-۲-۱ *رهنمودهای طبقه بندی*

کنترل

توصیه می‌شود که اطلاعات باید با توجه به ارزش، الزامات قانونی، حساسیت و بحرانی بودن آن برای سازمان، طبقه بندی شوند.

راهنمای پیاده سازی

توصیه می‌شود که طبقه بندی ها و کنترل های حفاظتی مربوطه به اطلاعات، نیازهای تجاری برای اشتراک یا محدود کردن اطلاعات و پیامدهای تجاری مربوط به این نیازها را به حساب آورند.
توصیه می‌شود که رهنمود طبقه بندی، مفادی برای طبقه بندی مقدماتی و طبقه بندی مجدد با گذشت زمان؛ مطابق با خط مشی کنترل دسترسی از پیش تعیین شده (رجوع کنید به ۱۱-۱-۱) را شامل باشند.
توصیه می‌شود که تعریف طبقه بندی یک دارایی، مرور دوره ای آن و تضمین به روز بودن و در سطح مناسب نگهداری شدن آن، به عهده مالک دارایی باشد (رجوع کنید به ۷-۱-۲). توصیه می‌شود که طبقه بندی، تاثیر تجمع ذکر شده در ۱۰-۷-۲ را لحاظ کند.
توصیه می‌شود که تعداد گروه های طبقه بندی و منافعی که از به کار بردن آنها به دست می‌آید، مورد توجه قرار گیرند. استفاده از طرح های بیش از حد پیچیده، ممکن است طاقت فرسا و غیر اقتصادی باشد و یا اثبات شود که این طرح ها غیرعملی هستند. توصیه می‌شود که در تفسیر برچسب های طبقه بندی روی اسناد دریافتی از سایر سازمان ها دقت شود، زیرا ممکن است تعریف های متفاوتی برای برچسب های نامگذاری شده مشابه، داشته باشند.

سایر اطلاعات

سطح محافظت را می‌توان با تحلیل محرمانگی، یکپارچگی، و دردسترس پذیری و هر گونه الزامات دیگر برای اطلاعات مورد توجه، ارزیابی کرد.
اطلاعات اغلب پس از یک دوره زمانی، دیگر حساس و حیاتی قلمداد نمی‌شوند، مثلا هنگامی که اطلاعات در معرض دید عموم قرار داده شده باشند. توصیه می‌شود که این جنبه ها به حساب آورده شوند، چون طبقه بندی بیش از حد، ممکن است منجر به پیاده سازی کنترل های غیرضروری شود که به هزینه های اضافی منجر می‌شوند.
در هنگام تعیین کردن سطوح طبقه بندی، رسیدگی کردن به اسنادی که الزامات امنیتی مشابهی دارند همراه با هم، ممکن است به تسهیل کار طبقه بندی کمک کند.
به طور کلی، طبقه بندی اعطا شده به اطلاعات راهی اختصاری برای تعیین نحوه استفاده و محافظت از این اطلاعات است.

۷-۲-۲ برچسب‌گذاری و اداره‌کردن اطلاعات

کنترل

توصیه می‌شود که یک مجموعهٔ مناسب از رویه ها برای علامت‌گذاری و اداره‌کردن اطلاعات مطابق با طرح طبقه بندی اتخاذ شده توسط سازمان، توسعه یافته و پیاده سازی شود.

راهنمای پیاده سازی

رویه های برچسب زنی اطلاعات باید دارایی‌های اطلاعاتی را در قالب های فیزیکی و الکترونیکی پوشش دهند.
توصیه می‌شود که خروجی سیستم‌هایی که حاوی اطلاعاتی است که حساس یا حیاتی قلمداد می‌شوند، حامل یک برچسب مناسب طبقه بندی باشند (در خروجی). توصیه می‌شود که برچسب زدن، طبقه بندی را مطابق با قوانین تثبیت شده در ۷-۲-۱، انعکاس دهد. موارد قابل ملاحظه، شامل گزارش های چاپ شده، نمایش دهنده

های روی صفحه، رسانه‌های ضبط شده (مانند نوارها، دیسک ها، و سی دی ها)، پیام های الکترونیکی، و انتقال های فایل هستند.

توصیه می‌شود که برای هر سطح از طبقه بندی، رویه هایی از جمله پردازش امن، ذخیره، انتقال، برداشتن طبقه بندی، و تخریب، تعریف شود. توصیه می‌شود که رویه‌هایی برای کنترل دسترسی واقعه نگاری هر رویداد امنیتی مربوطه، نیز برای هر سطح از طبقه بندی در نظر گرفته شوند.

توصیه می‌شود که توافق نامه های منعقد شده با سازمان‌های دیگر که شامل اشتراک اطلاعات می‌باشند، رویه هایی برای شناسایی طبقه‌بندی آن اطلاعات و تفسیر برچسب‌های طبقه‌بندی دریافت شده از سازمان های دیگر را شامل باشند.

سایر اطلاعات

برچسب زدن و اداره امن اطلاعات طبقه بندی شده، یک الزام کلیدی برای هماهنگی های اشتراک اطلاعات است. برچسب های فیزیکی، نوع متداولی از برچسب زنی هستند. به هر حال، بعضی از دارایی‌های اطلاعاتی نظیر مستندات در شکل الکترونیکی را نمی‌توان به طور فیزیکی برچسب زنی کرد و باید از روش های برچسب زنی الکترونیکی استفاده شود. مثلا، برچسب زنی هشدار، ممکن است روی پرده یا صفحه نمایش ظاهر شود.

در جایی که برچسب زنی امکان پذیر نباشد می‌توان از دیگر ابزارهای نمایش طبقه بندی اطلاعات استفاده کرد، مثلا از طریق رویه ها یا فرا- داده[1].

1- Meta-Data

۸ امنیت منابع انسانی

۸-۱ پیش از اشتغال[۱]

هدف: اطمینان یافتن از این که کارکنان، پیمانکاران، و کاربران شخص ثالث، مسوولیت های خود را می دانند و برای نقش هایی که برای آنها در نظر گرفته شده اند و نیز برای کاهش خطر سرقت، تقلب و سوء استفاده از امکانات، مناسب هستند.

توصیه می‌شود که مسوولیت های امنیتی، قبل از استخدام در تشریح مشاغل به اندازه کافی و در اصطلاحات و شرایط استخدام، عنوان شوند.

توصیه می‌شود که تمام نامزدهای استخدام، پیمانکاران و کاربران شخص ثالث، به اندازه کافی - به خصوص در مشاغل حساس - کنترل شوند.

توصیه می‌شود که کارکنان، پیمانکاران، و کاربران شخص ثالث امکانات پردازش اطلاعات، توافق نامه ای درباره نقش‌ها و مسوولیت های امنیتی خود امضا کنند.

۸-۱-۱ *نقش ها و مسوولیت‌ها*

کنترل

توصیه می‌شود که نقش ها و مسوولیت‌های امنیتی کارکنان، پیمانکاران و کاربران شخص سوم، با توجه به خط‌مشی امنیت اطلاعات سازمان، تعریف و مستندسازی شوند.

راهنمای پیاده سازی

توصیه می‌شود که نقش ها و مسوولیت‌های امنیتی شامل الزاماتی باشند تا:

الف - مطابق با خط‌مشی های امنیت اطلاعات سازمان، پیاده سازی شده و اقدام کنند (رجوع کنید به ۱.۵)؛

ب - از دارایی‌ها دربرابر دسترسی غیرمجاز، افشا، تغییر، تخریب یا دخالت محافظت کنند؛

پ - فرایندها یا فعالیت های خاص امنیتی را اجرا کنند؛

ت - اطمینان دهند که مسوولیت اعمال انجام شده، به فردی که آنها را انجام داده است واگذار شده است؛

ث - رویدادهای امنیتی، یا رویدادهای بالقوه یا دیگر ریسک های امنیتی سازمان را گزارش کنند؛

توصیه می‌شود که نقش ها و مسوولیت‌های امنیتی در طول فرایند قبل از استخدام، تعریف شده و به طور واضح به نامزدهای مشاغل تفهیم شوند.

سایر اطلاعات

شرح مشاغل را می‌توان برای مستندسازی نقش ها و مسوولیت‌های امنیتی مورد استفاده قرار داد. توصیه می‌شود که نقش ها و مسوولیت‌های امنیتی برای افرادی که از طریق فرایند استخدام سازمان مشغول به کار نشده اند، مثلا از طریق یک سازمان شخص سوم به کار گرفته شده اند، نیز به طور واضح تعریف و تفویض شود.

۱- توضیح: کلمه "اشتغال" در اینجا به این صورت معنی شده است که همه وضعیت‌های مختلف ذیل را پوشش می دهد:
اشتغال افراد(موقت یا طولانی مدت)، انتصاب سمت‌های شغلی، تغییر سمت‌های شغلی، واگذار کردن قرارداد، و خاتمه دادن به هر یک از این توافق‌نامه‌ها

۸-۱-۲ *گزینش*

کنترل

توصیه می‌شود که پیشینه تمامی داوطلبن استخدام، پیمانکاران، و کاربران شخص سوم، با توجه به قوانین، مقررات و اصول اخلاقی مربوطه، و متناسب با الزامات کسب وکار، طبقه بندی اطلاعات مورد دسترسی و ریسک‌های مشاهده شده، تصدیق شود.

راهنمای پیاده سازی

توصیه می‌شود که بررسی های تصدیقی[1] درباره همه موارد مرتبط با حریم خصوصی انجام شود، محافظت از داده‌های شخصی و/یا قانون گذاری مبتنی بر استخدام را به حساب بیاورند و توصیه می‌شود که در جایی که اجازه داده می‌شود، شامل موارد زیر باشند:

الف - در دسترس بودن منابع کاراکتری رضایتبخش، به عنوان مثال یک تجاری و یک شخصی؛

ب - یک بررسی (برای کامل بودن و دقت) رزومهٔ فرد متقاضی؛

پ - تایید صلاحیت های حرفه ای و دانشگاهی ادعا شده؛

ت - بررسی مستقل هویت (گذرنامه یا سند مشابه)؛

ث - بررسی های جزئی تر نظیر بررسی‌های اعتبار یا بررسی‌های سوابق کیفری.

هنگامی که یک شغل، خواه در زمان انتصاب اولیه یا در زمان ترفیع، مستلزم دسترسی شخص به تجهیزات پردازش اطلاعات است و به خصوص اگر این تجهیزات، اطلاعات حساس را اداره می‌کنند، مانند اطلاعات مالی یا اطلاعات خیلی محرمانه، توصیه می‌شود که سازمان نیز بررسی‌هایی با جزئیات بیشتر را در نظر بگیرد.

توصیه می‌شود که رویه‌ها برای بررسی‌های تصدیق و صحه‌گذاری، معیارها و محدودیت‌هایی را تعریف کنند، مثلا این که چه کسی برای زیر نظر گرفتن افراد، واجد شرایط است، و چگونه، چه موقع و چرا بررسی‌های تصدیقی انجام می‌شوند.

توصیه می‌شود که یک فرایند کنترل برای پیمانکاران، و کاربران شخص سوم انجام شود. هنگامی که پیمانکاران از طریق یک آژانس تامین می‌شوند، توصیه می‌شود که قرارداد با آژانس به طور شفاف مسوولیت‌های آژانس را برای گزینش و رویه هایی آگاه سازی که در صورت کامل نشدن گزینش یا در صورتی‌که نتایج سبب شک و نگرانی شوند، پیمانکاران باید از آنها پیروی کنند را مشخص کند. به طریق مشابه توصیه می‌شود که قرارداد با شخص سوم (همچنین رجوع کنید به ۶-۲-۳)، به طور شفاف تمام مسوولیت‌ها و رویه‌های آگاه‌سازی را برای گزینش مشخص کند.

توصیه می‌شود که اطلاعات درباره تمام نامزدهایی که برای پست ها در سازمان در نظر گرفته می‌شوند، مطابق با هر یک از قوانین وضع شده مناسب موجود در حوزه قضایی مربوطه، جمع آوری شده و مورد استفاده قرار گیرند. توصیه می‌شود که بر حسب قوانین وضع شده و کاربردی، نامزدها از قبل درباره فعالیت های گزینشی آگاه شوند.

۸-۱-۳ *ضوابط و شرایط استخدام*

کنترل

توصیه می‌شود که کارکنان، پیمانکاران و کاربران شخص سوم، به عنوان بخشی از تعهد قراردادی خود، ضوابط و شرایط قرارداد استخدامی خود را قبول کرده و امضا کنند؛ توصیه می‌شود که این تعهد قراردادی، مسوولیت‌های کارکنان، پیمانکاران و کاربران شخص سوم، و سازمان در قبال امنیت اطلاعات را تعیین کند.

1- Verification checks

راهنمای پیاده سازی

توصیه می‌شود که مفاد و شرایط استخدام، علاوه بر منعکس کردن خط مشی امنیتی سازمان، موارد زیر را نیز تعیین کرده و توضیح دهند:

الف - این که تمام کارکنان، پیمانکاران و کاربران شخص سوم که به اطلاعات حساس دسترسی دارند، توصیه می‌شود که یک توافق نامه محرمانگی یا عدم افشا را قبل از دسترسی به امکانات پردازش اطلاعات، امضا کنند؛

ب - مسوولیت ها و حقوق قانونی کارکنان، پیمانکاران، و هر یک از کاربران دیگر، برای مثال در موضوع قوانین مالکیت معنوی یا قوانین وضع شده حفاظت از داده (همچنین رجوع کنید به ۱۵-۱-۱ و ۱۵-۱-۲)؛

پ - مسوولیت ها برای طبقه بندی اطلاعات و مدیریت دارایی‌های سازمانی مربوط به سیستم‌های اطلاعاتی و خدمات انجام شده توسط کارمند، پیمانکار، یا کاربر شخص سوم (همچنین رجوع کنید به ۷-۲-۱ و ۱۰-۷-۳)؛

ت - مسوولیت های کارمند، پیمانکار یا کاربر شخص سوم برای کار با اطلاعات دریافتی از سایر شرکت ها یا اشخاص بیرونی؛

ث - مسوولیت های سازمان برای کار با اطلاعات شخصی، شامل اطلاعات شخصی که در نتیجه یا در زمان همکاری با سازمان ایجاد شده است (همچنین رجوع کنید به ۱۵-۱-۴)؛

ج - مسوولیت هایی که به خارج از محوطه های سازمان و خارج از ساعات کار معمولی، توسعه داده می‌شوند، مثلا در مورد کار در خانه (همچنین رجوع کنید به ۹-۲-۵ و ۱۱-۷-۱)؛

چ - اقداماتی که در هنگام نادیده گرفتن الزامات امنیتی سازمان توسط کارکنان، پیمانکاران یا کاربران شخص سوم، انجام خواهند شد (همچنین رجوع کنید به ۸-۲-۳)؛

توصیه می‌شود که سازمان از موافق بودن کارکنان، پیمانکاران و کاربران شخص سوم با مفاد و شرایط مربوط به امنیت اطلاعات، متناسب با ماهیت و میزان دسترسی که به دارایی‌های سازمان در رابطه با سیستم‌های اطلاعاتی و خدمات خواهند داشت، اطمینان یابد.

توصیه می‌شود که در جای مناسب، مسوولیت های موجود در مفاد و شرایط استخدامی برای یک دوره تعیین شده پس از پایان استخدام، ادامه داده شوند. (همچنین رجوع کنید به ۸-۳)

سایر اطلاعات

می‌توان از یک کد رفتار برای پوشش دادن مسوولیت های کارمند، پیمانکار، یا شخص سوم در رابطه با محرمانگی، حفاظت از داده، اخلاقیات، استفاده مناسب از تجهیزات و امکانات سازمان، و نیز عملکردهای مربوط به خوش‌نامی سازمان - که مورد انتظار هستند - استفاده کرد. پیمانکار یا کاربران شخص سوم ممکن است با سازمانی بیرونی در ارتباط باشند، ممکن است لازم باشد که این سازمانی بیرونی نیز به نوبه خود در توافقات مربوط به قرارداد، به نمایندگی از طرف فرد دارای قرارداد، وارد شود.

۸-۲ حین خدمت

هدف: حصول اطمینان از اینکه کارکنان، پیمانکاران و کاربران شخص ثالث، از تهدیدها و نگرانی های امنیت اطلاعات و مسوولیت‌ها و تعهدات خود آگاه بوده و برای پشتیبانی از خط‌مشی امنیتی سازمان در انجام کارهای روزمره خود و کاهش ریسک ناشی از خطای انسانی، آماده شده اند.

توصیه می‌شود که مسوولیت‌های مدیریت تعریف شوند تا اطمینان حاصل شود که امنیت در سراسر مدت استخدام یک فرد در سازمان، اجرا می‌شود.

توصیه می‌شود که یک سطح کافی از آگاهی، آموزش، و پرورش در رویه های امنیتی و استفاده صحیح از امکانات پردازش اطلاعات، برای تمام کارکنان، پیمانکاران و کاربران شخص ثالث فراهم شود تا احتمال ریسک های امنیتی به حداقل برسد. توصیه می‌شود که یک فرایند انضباطی رسمی برای رسیدگی به رخنه های امنیتی، برقرار شود.

۸-۲-۱ *مسوولیت‌های مدیریت*

کنترل

توصیه می‌شود که مدیریت، اجرای امنیت مطابق با خط‌مشی ها و رویه های برقرار شدهٔ سازمان را برای کارکنان، پیمانکاران و کاربران شخص سوم الزامی‌کند.

راهنمای پیاده سازی

توصیه می‌شود که مسوولیت‌های مدیریت شامل حصول اطمینان از موارد زیر درباره کارکنان، پیمانکاران و کاربران شخص سوم، باشد:

الف - درباره نقش ها و مسوولیت‌های امنیت اطلاعات خود پیش از اعطای مجوز دسترسی به اطلاعات حساس یا سیستم‌های اطلاعاتی به طور مناسب توجیه شده اند؛

ب - رهنمودهایی برای تعیین انتظارات امنیتی از نقش خود در سازمان دریافت کرده اند؛

پ - برای رعایت سیاست های امنیتی سازمان، انگیزه مند شوند؛

ت - به سطحی از آگاهی درباره امنیت مرتبط با نقش ها و مسوولیت‌های خود در سازمان برسند (همچنین رجوع کنید به ۸-۲-۲)؛

ث - از مفاد و شرایط استخدام که شامل خط‌مشی امنیت اطلاعات سازمان و روش های مناسب کار می باشند، پیروی کنند؛

ج - همچنان به کسب مهارت ها و ویژگی های مناسب ادامه دهند.

سایر اطلاعات

اگر کارکنان، پیمانکاران، و کاربران شخص سوم از مسوولیت‌های امنیتی خود آگاه نشوند، می‌توانند باعث وارد شدن آسیب جدی به یک سازمان آسیب شوند. پرسنل دارای انگیزه، بیشتر قابل اطمینان هستند و رخدادهای امنیتی کمتری را سبب می‌شوند.

مدیریت ضعیف، ممکن است باعث شود تا پرسنل احساس کنند که سازمان کمتر از میزان لازم برای آنها ارزش قائل می‌شود و این مساله منجر به پیامد امنیتی منفی بر سازمان می‌شود. مثلا، مدیریت ضعیف ممکن است منجر به نادیده گرفته شدن امنیت یا سوء استفاده بالقوه از دارایی‌های سازمان شود.

۸-۲-۲ آگاهی رسانی، تحصیل و آموزش امنیت اطلاعات

کنترل

تمامی کارکنان سازمان و، در هنگام لزوم، پیمانکاران و کاربران شخص سوم، بایستی آموزش آگاه سازی مناسب و به روز رسانی قاعده مند خط‌مشی ها و رویه های سازمانی را دریافت کنند، آنگونه که به وظایف شغلی آنها مربوط است.

راهنمای پیاده سازی

توصیه می‌شود که آموزش آگاه سازی با یک فرایند مقدماتی رسمی آغاز شود که برای معرفی خط‌مشی های امنیتی سازمان و انتظارات، قبل از اعطای اجازه دسترسی به اطلاعات یا خدمات طراحی شده است.

توصیه می‌شود که آموزش مستمر دربرگیرنده الزامات امنیتی، مسوولیت‌های حقوقی و کنترل های تجاری و نیز آموزش استفاده صحیح از تجهیزات پردازش اطلاعات مانند رویه برقراری ارتباط با سیستم، استفاده از بسته های نرم‌افزاری و اطلاعات بر اساس فرایند انضباتی باشد (رجوع کنید به ۸-۲-۳).

اطلاعات دیگر

توصیه می‌شود که فعالیت های آگاه‌سازی، آموزش و تعلیم امنیت، با نقش، مسوولیت‌ها و مهارت های شخص متناسب و مرتبط باشد و توصیه می‌شود که شامل اطلاعاتی درباره تهدیدهای شناخته شده، فردی که برای دریافت مشاوره امنیتی بیشتر باید با او تماس گرفته شود و کانال های مناسب برای گزارش رخدادهای امنیت اطلاعات باشد (همچنین رجوع کنید به ۱۳-۱).

هدف از آموزش ارتقای آگاهی، این است که به افراد امکان داده شود تا مشکلات و رخدادهای امنیت اطلاعات را بشناسند و مطابق با نیازهای نقش کاری خود واکنش نشان دهند.

۸-۲-۳ فرایند انضباطی

کنترل

توصیه می‌شود که یک فرایند انضباطی رسمی برای کارکنانی که مرتکب یک نقض پیمان رخنه امنیتی می‌شوند، وجود داشته باشد.

راهنمای پیاده سازی

فرایند انضباطی نبایستی بدون تصدیق قبلی اینکه نقض پیمان امنیتی صورت گرفته است، آغاز شود. (برای مجموعه شواهد، همچنین رجوع کنید به ۱۳-۲-۳).

فرایند انضباطی رسمی بایستی اطمینان دهد که با کارکنانی که مظنون به ارتکاب نقض پیمان امنیتی هستند، برخوردی صحیح و عادلانه انجام می‌شود. فرایند انضباطی رسمی بایستی برای یک پاسخ آگاهانه که عواملی نظیر طبیعت و شدت نقض پیمان و پیامد آن بر کسب وکار، آیا این تخلف برای اولین بار اتفاق می افتد یا تکراری است، آیا نقض کننده به اندازه کافی آموزش دیده است یا خیر، قانون گذاری مرتبط، قراردادهای تجاری و دیگر عوامل مورد نیاز، آماده شوند. در موارد جدی سوء رفتار، این فرایند بایستی امکان حذف مستقیم وظایف، حقوق دسترسی و مجوزها، و اقدام سریع نگهبان برای همراهی فرد به خارج از محل را امکان پذیر سازد.

اطلاعات دیگر

فرایند انضباتی همچنین بایستی به عنوان عاملی برای بازداشتن کارکنان، پیمانکاران و کاربران شخص سوم از نقض خط‌مشی ها و رویه های امنیت سازمانی و هر نقض پیمان امنیتی دیگر، مورد استفاده قرار گیرد.

۸-۳ خاتمه استخدام یا تغییر شغل

هدف: حصول اطمینان از اینکه کارکنان، پیمانکاران و کاربران شخص ثالث، به روشی ضابطه مند سازمان را ترک کرده یا تغییر شغل می دهند.
توصیه می‌شود که مسوولیت‌هایی برای حصول اطمینان از اینکه خروج کارمند، پیمانکار یا کاربر شخص ثالث از سازمان، مدیریت می‌شود و اینکه بازگرداندن تمام تجهیزات و حذف تمام حقوق دسترسی، کامل می‌شود، در نظر گرفته شوند.
تغییر مسوولیت‌ها و استخدام ها در یک سازمان بایستی به عنوان خاتمه مسوولیت مربوطه یا استخدام، مطابق این بخش مدیریت شوند و هر گونه استخدام بایستی آنگونه که در بند ۱،۸ شرح داده شده است، مدیریت شود.

۸-۳-۱ *مسوولیت‌های خاتمه خدمت*

کنترل
مسوولیت های مربوط به اجرای خاتمه خدمت یا تغییر شغل، بایستی به وضوح تعریف شده و تخصیص داده شوند.

راهنمای پیاده سازی
ارتباطات مسوولیت‌های خاتمه توصیه می‌شود الزامات امنیتی جاری و مسوولیت‌های حقوقی و، در زمان مناسب، مسوولیت‌های موجود در هر توافق‌نامه محرمانگی (رجوع کنید به ۶-۱-۵) و مفاد و شرایط استخدام (رجوع کنید به ۸-۱-۳) را برای یک دوره تعیین شده پس از خاتمه استخدام کارکنان، پیمانکاران و کاربران شخص سوم ادامه می‌یابد، شامل باشد.
مسوولیت‌ها و وظایفی که پس از خاتمه خدمت همچنان معتبر هستند، بایستی در قراردادهای کارمند، پیمانکار یا کاربر شخص سوم گنجانده شوند.
تغییرات مسوولیت، یا استخدام بایستی به عنوان خاتمه مسوولیت یا استخدام مربوطه مدیریت شوند، و مسوولیت یا استخدام جدید بایستی آن‌گونه که در بند ۸-۱ شرح داده شده است، کنترل شود.

سایر اطلاعات
بخش منابع انسانی عموما مسوول کل فرایند خاتمه استخدام است و با مدیر سرپرست شخصی که سازمان را ترک می‌کند، همکاری می نماید تا جنبه های امنیتی رویه های مرتبط را مدیریت کند. در مورد یک پیمانکار، این فرایند مسوولیت خاتمه ممکن است توسط یک آژانس که مسوول پیمانکار است تقبل شود و در صورت وجود یک کاربر دیگر، این کار ممکن است توسط سازمان آنها انجام شود.
ممکن است لازم باشد که کارکنان، مشتریان، پیمانکاران یا کاربران شخص سوم از تغییرات در پرسنل و توافقات عملیاتی مطلع شوند.

۸-۳-۲ *عودت دارایی‌ها*

کنترل
تمامی کارکنان، پیمانکاران و کاربران شخص سوم بایستی به محض خاتمه استخدام قرارداد یا توافق‌نامه خود، تمامی دارایی‌های سازمان را که در اختیار آنها است، به سازمان عودت دهند.

راهنمای پیاده سازی

فرایند خاتمه بایستی رسمی‌شود تا بازگرداندن تمام نرم‌افزارهای ثبت شده، اسناد شرکتی، و تجهیزات را شامل شود. دیگر دارایی‌های سازمانی نظیر دستگاه‌های محاسبه سیار، کارت‌های اعتباری، کارت‌های دسترسی، نرم‌افزار، راهنماها، و اطلاعات ذخیره شده در رسانه های الکترونیکی نیز باید بازگردانده شوند.

در مواردی که یک کارمند، پیمانکار یا کاربر شخص سوم، تجهیزات سازمان را خریداری کند یا از تجهیزات شخصی خودش استفاده کند، بایستی رویه هایی دنبال شود تا اطمینان حاصل شود که تمام اطلاعات مرتبط به سازمان منتقل شده و به طور امن از تجهیزات پاک شده است (همچنین رجوع کنید به ۱۰-۷-۱).

در مواردی که یک کارمند، پیمانکار یا کاربر شخص سوم، دانشی دارد که برای انجام عملیات جاری مهم است، آن دانش بایستی مستندسازی شده و به سازمان منتقل شود.

۸-۳-۳ حذف حقوق دسترسی

کنترل

حقوق دسترسی تمام کارکنان، پیمانکاران و کاربران شخص سوم به اطلاعات و امکانات پردازش اطلاعات، بایستی به محض خاتمه استخدام، قرارداد یا توافق نامه آنها، حذف شده یا با تغییرات تطبیق داده شود.

راهنمای پیاده سازی

به محض خاتمه استخدام، بایستی حقوق دسترسی یک فرد به دارایی‌های مربوط به سیستم‌های اطلاعات و خدمات، مورد بازنگری قرار گیرد. این کار تعیین خواهد کرد که آیا لازم است تا حقوق دسترسی حذف شوند یا خیر. تغییرات یک استخدام بایستی در حذف تمام حقوق دسترسی که برای شغل جدید تایید نشده‌اند، انعکاس یابد. حقوق دسترسی که بایستی حذف یا تغییر داده شوند، شامل دسترسی فیزیکی و منطقی، کلیدها، کارت های شناسایی، تجهیزات پردازش اطلاعات (همچنین رجوع کنید به ۱۱-۲-۴)، تعهدات اشتراک و حذف تمام مستنداتی که این افراد یا پیمانکاران را به عنوان یک عضو جاری سازمان معرفی می‌کند، است. اگر کارمند، پیمانکار یا کاربر شخص سومی که در حال ترک شرکت است، کلمه های عبور حساب های کاربری که فعال باقی مانده اند را بداند، این کلمه های عبور بایستی به محض تغییر پست یا خاتمه قرارداد، تغییر داده شوند.

حقوق دسترسی برای دارایی‌های اطلاعاتی و تجهیزات پردازش اطلاعات، بایستی با توجه به ارزیابی عوامل ریسک، قبل از خاتمه یا تغییرات استخدام کاهش یافته یا حذف شوند. مانند:

الف - این که آیا خاتمه خدمت یا تغییر توسط کارمند، پیمانکار یا کاربر شخص سوم انجام شده است یا توسط مدیریت و نیز بیان دلیل خاتمه خدمت؛

ب - مسوولیت‌های فعلی کارمند، پیمانکار یا هر کاربر دیگر؛

پ - ارزش دارایی‌هایی که در حال حاضر در دسترس هستند.

اطلاعات دیگر

در شرایط خاص، ممکن است حقوق دسترسی برای دسترسی افراد دیگری غیر از کارمند، پیمانکار یا کاربر شخص سوم ترک کننده، نیز اختصاص داده شده باشند، مثلا، کارت های شناسایی گروهی. در چنین شرایطی، افراد ترک کننده بایستی از همه فهرست های دسترسی گروهی حذف شوند و بایستی تمهیداتی انجام شود تا به تمام کارکنان،

پیمانکاران و کاربران شخص سوم مربوط توصیه شود که این اطلاعات را بیش از این با شخصی که در حال ترک سازمان است، به اشتراک نگذارند.

در صورت خاتمه قرارداد توسط مدیریت، کارکنان، پیمانکاران و کاربران شخص سوم عزل شده، ممکن است عمدا اطلاعات را خراب کنند یا تجهیزات پردازش اطلاعات را منهدم کنند. در صورت استعفای افراد، آنها ممکن است وسوسه شوند تا اطلاعات را برای استفاده در آینده جمع آوری کنند.

۹ امنیت فیزیکی و محیطی

۹-۱ نواحی امن

هدف : پ یشگیری از دسترسی فیزیکی غیر مجاز، خسارت و تعرض به ابنیه و اطلاعات سازمان.
توصیه می‌شود تجهیزات پردازش اطلاعات حیاتی یا حساس در نواحی امن نگهداری شوند و حفاظ‌های امنیتی مناسب و کنترل های تردد درباره آنها صورت گیرد. توصیه می‌شود آنها از نظر فیزیکی در برابر دسترسی غیرمجاز، آسیب، و مداخله محافظت شوند.
توصیه می‌شود محافظت انجام شده، با ریسک های شناسایی شده متناسب باشد.

۹-۱-۱ *حصار امنیت فیزیکی*

کنترل
توصیه می‌شود حفاظ‌های امنیتی (موانعی از قبیل حایل‌ها،دیوارها، درهای ورودی کنترل شده توسط کارت یا میزهای پذیرش)، برای حفاظت نواحی حاوی اطلاعات و امکانات پردازش اطلاعات، استفاده شوند.
راهنمای پیاده سازی
توصیه می‌شود دستورالعمل های زیر در هنگام لزوم برای حفاظ‌های امنیت فیزیکی در نظر گرفته شده و اجرا شوند.

الف - توصیه می‌شود حفاظ‌های امنیتی به دقت تعریف شوند و محل قرارگیری و توانایی هر یک از حفاظ‌ها باید متناسب با نیازهای امنیتی دارایی‌های آن محیط و نتایج ارزیابی ریسک آنها باشد.

ب - توصیه می‌شود فضای ساختمان یا سایت حاوی تجهیزات پردازش اطلاعات، از نظر فیزیکی مناسب باشد (به عبارت دیگر، توصیه می‌شود هیچ شکافی در حفاظ‌ها یا نواحی که ورود غیرقانونی بتواند اتفاق بیافتد، وجود نداشته باشد)؛ توصیه می‌شود دیوارهای بیرونی سایت استحکام مناسبی داشته باشند و توصیه می‌شود تمام درب ها به طور مناسب در برابر دسترسی غیرمجاز با مکانیسم های کنترل از جمله موانع، سیستم‌های هشدار دهنده، قفل ها و غیره محافظت شوند؛ توصیه می‌شود درب ها و پنجره ها زمانی که نیاز به محاظت بیرونی و کنترل‌های عدم حضور وجود دارد قفل شوند بخصوص برای پنجره هایی که در طبقات همکف قرار دارند.

پ - توصیه می‌شود یک ناحیه پذیرش یا هر ابزار مشابه دیگری برای کنترل دسترسی فیزیکی به سایت یا ساختمان‌ها در نظر گرفته شود؛ توصیه می‌شود دسترسی به سایت‌ها و ساختمان ها فقط محدود به کارکنان مجاز شود؛

ت - توصیه می‌شود موانع فیزیکی در صورت امکان ایجاد شوند تا از دسترسی فیزیکی غیرمجاز و آلودگی‌های محیطی جلوگیری شود

ث - توصیه می‌شود تمام درب های خروج اضطراری، موجود در حفاظ‌های امنیتی مجهز به سیستم هشدار دهنده و دوربین‌های کنترلی باشند و در ترکیب با دیوارها بررسی شوند تا سطح مقاومت مورد نیاز را مطابق با استانداردهای مناسب منطقه ای، ملی و بین المللی فراهم کنند؛ توصیه می‌شود آنها مطابق با استانداردهای محلی مقابله با حریق به گونه ای بی اشتباه عمل کنند؛

ج - توصیه می‌شود سیستم‌های کشف ورود غیرمجاز مطابق با استانداردهای ملی، منطقه ای و بین المللی نصب شوند و به طور منظم مورد آزمایش قرار گیرند تا تمام درب های بیرونی و پنجره ها را پوشش دهند. توصیه می‌شود فضاهای خالی همواره باید توسط سیستم هشدار دهنده کنترل شوند؛ همچنین توصیه می‌شود این پوشش برای فضاهای دیگر مانند اتاق رایانه یا اتاق های ارتباطات تامین گردد.

چ - توصیه می‌شود تجهیزات پردازش اطلاعات که توسط سازمان مدیریت می‌شوند از نظر فیزیکی از تجهیزاتی که توسط اشخاص ثالث دیگر مدیریت می‌شوند تفکیک شوند؛

اطلاعات دیگر

محافظت فیزیکی می‌تواند از طریق ایجاد یک یا چند مانع فیزیکی در اطراف ابنیه سازمان و تجهیزات پردازش اطلاعات آن حاصل شود؛ استفاده از چندین مانع امنیت بیشتری را فراهم می‌کند، و در صورت عمل نکردن یکی از موانع امنیت فیزیکی دچار اختلال نمی‌شود؛

یک ناحیه امن ممکن است یک دفتر کار قابل قفل شدن یا چندین اتاق باشد که توسط یک مانع فیزیکی داخلی یکپارچه احاطه شده است؛ موانع و حفاظهای دیگری برای کنترل دسترسی فیزیکی ممکن است بین نواحی داخلی با نیازهای امنیتی متفاوت مورد نیاز باشد.

توصیه می‌شود ملاحظات خاصی در راستای امنیت دسترسی فیزیکی برای ساختمان هایی که چندین سازمان مختلف در آن قرار دارند در نظر گرفته شود.

۹-۱-۲ کنترل‌های مداخل فیزیکی ورودی

کنترل

توصیه می‌شود نواحی امن، به منظور حصول اطمینان از اینکه فقط کارکنان مجاز، اجازه دسترسی دارند، توسط سیستم‌های کنترل ورودی مناسب، حفاظت شوند.

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر مدنظر قرار گیرند:

الف - توصیه می‌شود تاریخ و زمان ورود و خروج بازدیدکنندگان ثبت شود و توصیه می‌شود تمام مراجعه کنندگان تحت نظارت باشند مگر این که دسترسی آنها قبلا تایید شده باشد؛ توصیه می‌شود آنها فقط دسترسی برای اهداف خاص و مجاز را داشته باشند و دستورالعمل هایی در زمینه الزامات ایمنی ناحیه و رویه های مربوط به شرایط اضطراری به آنها اعلام شود.

ب - توصیه می‌شود دسترسی به نواحی که در آنجا، اطلاعات حساس مورد پردازش قرار می‌گیرد یا ذخیره می‌شود کنترل و برای افراد مجاز محدود شود؛ کنترل های دسترسی مانند کارت کنترل دسترسی باید برای مجاز و معتبر کردن تمام دسترسی ها مورد استفاده قرار گیرد؛ یک گزارش ممیزی از تمام دسترسی ها باید در محل امنی نگهداری شود.

پ - از تمام کارکنان، پیمانکاران و کاربران شخص ثالث و تمام بازدیدکنندگان باید خواسته شود تا نوعی علامت شناسایی قابل رویت را به لباس خود نصب کنند و در صورت مواجهه با بازدیدکنندگان بدون همراه و یا بدون علامت شناسایی توصیه می‌شود بلافاصله کارکنان امنیتی را مطلع کنند.

ت - توصیه می‌شود کارکنان خدمات پشتیبانی شخص ثالث امکان دسترسی محدود به نواحی امن یا تجهیزات پردازش اطلاعات حساس را فقط در صورت ضرورت داشته باشند؛ توصیه می‌شود این دسترسی مجاز و کنترل شده باشد؛

ث - توصیه می‌شود حقوق دسترسی به نواحی امن، به طور منظم بررسی و روزآمد شوند و در زمان لازم باطل شوند (رجوع کنید به ۸-۳-۳)؛

۹-۱-۳ ایمن‌سازی دفاتر، اتاق‌ها و امکانات

کنترل

توصیه می‌شود امنیت فیزیکی برای دفاتر، اتاق‌ها و امکانات، طراحی و بکار گرفته شود.

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر برای تضمین امنیت دفاتر، اتاق ها و امکانات در نظر گرفته شود:

الف - توصیه می‌شود از مقررات سلامت و ایمنی مربوطه و استانداردها گزارشی تهیه شود؛

ب - توصیه می‌شود تجهیزات کلیدی از دسترس همگان دور نگه داشته شوند

پ - توصیه می‌شود در صورت امکان، ساختمان ها غیرقابل نفوذ باشند و حداقل نشانه ای از کاربردشان ارایه دهند و هیچ علایم واضحی خارج یا داخل ساختمان وجود نداشته باشد که وجود فعالیت های پردازش اطلاعات در آن را مشخص سازد؛

ت – راهنمای ساختمان و دفاتر تلفنی که محل قرارگیری تجهیزات پردازش اطلاعات حساس را نشان می‌دهند، توصیه می‌شود به سادگی در دسترس همگان قرار نداشته باشند؛

۹-۱-۴ محافظت در برابر تهدیدهای بیرونی و محیطی

کنترل

توصیه می‌شود برای مقابله با خسارت ناشی از آتش، سیل، زمین لرزه، انفجار، آشوب داخلی، و شکل های دیگری از حوادث طبیعی یا انسانی، حفاظت فیزیکی مناسب طراحی و بکار گرفته شود.

راهنمای پیاده سازی

توصیه می‌شود درمورد هر یک از تهدیدهای امنیتی که توسط اماکن مجاور متوجه ما می‌شود مانند آتش سوزی در ساختمان همسایه، نشت آب از سقف یا کف طبقات همکف یا انفجار در خیابان، ملاحظاتی صورت گیرد.

توصیه می‌شود رهنمودهای زیر برای اجتناب از آسیب در برابر آتش سوزی، سیل، زلزله، انفجار، شورش، و شکل‌های دیگر بلایای طبیعی یا انسانی به کار گرفته شود:

الف - توصیه می‌شود مواد خطرناک یا قابل اشتعال در فاصله ای مطمئن از نواحی امن نگه داشته شوند؛ توصیه می‌شود تجهیزات فله و باز در نواحی امن نگه داری نشوند

ب - توصیه می‌شود تجهیزات تهیه فایل‌های پشتیبان و محیط‌های ذخیره فایل‌های پشتیبان، در فاصله ای امن قرار گیرند تا از آسیب فجایعی که بر سایت اصلی تاثیر می گذارد در امان بمانند.

پ - توصیه می‌شود تجهیزات آتش نشانی مناسب فراهم و در محل مناسب قرار داده شود.

۹-۱-۵ کار در نواحی امن

کنترل

توصیه می‌شود برای کار در نواحی امن، حفاظت فیزیکی و رهنمودها، طراحی و بکار گرفته شوند.

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر مدنظر قرار گیرند.

الف - توصیه می‌شود کارکنان فقط در صورت لزوم، از وجود یا فعالیت های نواحی امن مطلع گردند.

ب - توصیه می‌شود از کارکردن بدون نظارت در نواحی امن به دلایل ایمنی و به منظور پیشگیری از فرصت انجام اقدامات خرابکارانه اجتناب شود.

پ - توصیه می‌شود نواحی امن خالی و بدون استفاده از نظر فیزیکی قفل شوند و به طور منظم بازدید شوند؛

ت - توصیه می‌شود تجهیزات عکس برداری، فیلم‌برداری، ضبط صوت یا دیگر تجهیزات ضبط کننده نظیر دوربین تلفن همراه، نباید اجازه ورود داشته باشند مگر این که برای آنها مجوز ورود صادر شود،

ملاحظات مربوط به کار در نواحی امن شامل کنترل هایی برای کارکنان، پیمانکاران و کاربران شخص ثالث و نیز فعالیت های سایر اشخاص، باید تهیه شود.

۹-۱-۶ نواحی دسترسی عمومی، نواحی تحویل و بارگیری

کنترل

توصیه می‌شود نقاط دسترسی از قبیل نواحی تحویل و بارگیری و سایر نقاطی که افراد غیر مجاز ممکن است وارد ساختمان ها شوند، تحت کنترل قرار گرفته و در صورت امکان، برای جلوگیری از دسترسی غیر مجاز، از امکانات پردازش اطلاعات، مجزا شوند.

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر، لحاظ شوند:

الف - توصیه می‌شود دسترسی به نواحی تحویل و بارگیری از خارج از ساختمان، محدود به اشخاص شناخته شده و مجاز باشد.

ب - توصیه می‌شود منطقه تحویل و بارگیری به گونه ای طراحی شود که بتوان بار را بدون دسترسی کارکنان تحویل به بخش های دیگر ساختمان تخلیه کرد؛

پ - توصیه می‌شود درب های خارجی نواحی تحویل و بارگیری، در زمانی که درب های داخلی باز می‌شوند ایمن شوند؛

ت - توصیه می‌شود مواد ورودی قبل از این که از منطقه تحویل و بارگیری به نقطه مورد استفاده انتقال داده شوند برای تهدیدهای احتمالی وارسی شوند (رجوع شود به ۹-۲-۱ مورد ت).

ث - توصیه می‌شود مواد ورودی مطابق با رویه های مدیریت دارایی در زمان ورود به محل ثبت شوند. (همچنین رجوع کنید به ۷-۱-۱)

ج - توصیه می‌شود محموله های ورودی و خروجی تا جایی که ممکن است، بصورت فیزیکی تفکیک شده باشند.

۹-۲ امنیت تجهیزات

هدف : پ شگیری از اتلاف، زیان، سرقت ی به خطر افتادن دارایی‌ها و ایجاد وقفه در فعال ت های سازمان.
توصیه می‌شود تجهیزات دربرابر تهدیدهای فیزیکی و محیطی محافظت شوند؛
محافظت از تجهیزات برای کاهش ریسک دسترسی غیرمجاز به اطلاعات و محافظت دربرابر آسیب یا خسارت ضروری است. توصیه می‌شود این ملاحظات، محل قرارگیری و تخلیه تجهیزات را هم در نظر بگیرد. کنترل های خاص ممکن است برای محافظت دربرابر تهدیدهای فیزیکی و محافظت از تجهیزات پشتیبان نظیر منبع برق و زیرساختار کابل کشی لازم باشد..

۹-۲-۱ *استقرار و حفاظت تجهیزات*

کنترل

توصیه می‌شود تجهیزات (در مکان مناسب) مستقر و محافظت شوند تا ریسک‌ها ناشی از تهدیدها و خطرات محیطی و فرصت‌های دسترسی غیر مجاز، کاهش یابند.

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر برای محافظت از تجهیزات مورد توجه قرا رگیرند:

الف - توصیه می‌شود تجهیزات به نحوی قرار گیرند که دسترسی غیرضروری به نواحی کاری به حداقل کاهش یابد؛

ب - توصیه می‌شود تجهیزات پردازش اطلاعات که با داده‌های حساس سروکار دارند، با زاویه دید محدود قرار گیرند تا ریسک رویت اطلاعات توسط اشخاص غیرمجاز در زمان استفاده کاهش یابد و تجهیزات دخیره اطلاعات برای جلوگیری از دسترسی غیر مجاز در جای امن قرار گیرند.؛

پ - توصیه می‌شود اجزایی که به محافظت خاص نیاز دارند جدا از سایر اقلام قرار گیرند تا سطح کلی محافظت مورد نیاز کاهش یابد

ت - توصیه می‌شود کنترل هایی برای کاهش ریسک تهدیدهای فیزیکی بالقوه مانند سرقت، آتش سوزی، انفجار، دود، آب، گرد و غبار، لرزش، تاثیرات شیمیایی، تداخل منابع برق، تداخل ارتباطات، تابش الکترومغناطیسی و دستکاری اتخاذ شود.

ث - توصیه می‌شود دستورالعمل های منع خوردن، آشامیدن، و سیگار کشیدن در نزدیکی تجهیزات پردازش اطلاعات تهیه شود.

ج - توصیه می‌شود شرایط محیطی نظیر دما و رطوبت برای شرایطی که ممکن است تاثیر منفی بر استفاده از تجهیزات اطلاعات بگذارند کنترل شوند

چ - توصیه می‌شود محافظت از اشتعال در تمام ساختمان ها به کار گرفته شود و توصیه می‌شود فیلترهایی برای حفاظت اشتعال در ورودی تمام خطوط ارتباطی و برق در نظر گرفته شود.

ح - توصیه می‌شود استفاده از روش های محافظت خاص، نظیر غشاهای صفحه کلید، برای تجهیزات مورد استفاده در محیط های صنعتی در نظر گرفته شوند؛

خ - توصیه می‌شود تجهیزاتی که اطلاعات حساس را پردازش می‌کنند محافظت شوند تا ریسک نشت اطلاعات در اثر سهل‌انگاری به حداقل برسد.

۹-۲-۲ امکانات و پشتیبانی

کنترل

توصیه می‌شود تجهیزات در برابر قطع برق و سایر اختلالات ناشی از نقص های امکانات پشتیبانی، محافظت شوند.

راهنمای پیاده سازی

توصیه می‌شود تمام امکانات پشتیبانی نظیر برق، آب، فاضلاب، گرمایش/تهویه و هواسازی برای سیستم‌هایی که مورد پوشش آنها قرار دارند بصورت مناسب فراهم شوند. توصیه می‌شود امکانات پشتیبانی به طور منظم بررسی و تست شوند تا عملکرد مناسب آنها تضمین شود و هر ریسکی ناشی از کارکرد نامناسب آنها کاهش یابد. توصیه می‌شود یک منبع برق مناسب تهیه شود که با مشخصات تولیدکننده تجهیزات تطابق داشته باشد.

یک منبع برق غیرقابل قطع[1]، برای تامین برق برای تجهیزاتی که عملیات حیاتی را پشتیبانی می‌کنند پیشنهاد می‌شود. توصیه می‌شود طرح‌های پیش‌آمدهای احتمالی مرتبط با برق، در زمان خرابی منبع برق غیرقابل قطع لحاظ شود. توصیه می‌شود یک ژنراتور پشتیبان، در صورتی که برای ادامه کار، تداوم پردازش اطلاعات لازم باشد در نظر گرفته شود. توصیه می‌شود یک منبع کافی سوخت در دسترس باشد تا تضمین نماید که ژنراتور می‌تواند برای دوره ای طولانی فعالیت کند. توصیه می‌شود تجهیزات منبع برق غیرقابل قطع و ژنراتورها به طور منظم بررسی شوند تا اطمینان حاصل شود که ظرفیت کافی را دارند و همچنین مطابق با پیشنهادات تولید کننده تست شوند. علاوه بر این، توصیه می‌شود چندین منبع برق مختلف تهیه شود یا اگر سایت بزرگ است یک ایستگاه برق جداگانه در نظر گرفته شود.

توصیه می‌شود کلیدهای قطع برق اضطراری در نزدیکی خروجی های اضطراری اتاق های تجهیزات قرار داده شوند تا قطع برق به سرعت در صورت وقوع شرایط اضطراری امکان‌پذیر شود. توصیه می‌شود روشنایی اضطراری برای مواقع قطع برق اصلی باید فراهم شود.

توصیه می‌شود منبع آب پایدار بوده و برای تامین آب سیستم‌های تهویه، تجهیزات مرطوب کننده، و اطفا حریق کافی باشد. نقص در سیستم تامین آب ممکن است به تجهیزات آسیب برساند یا از عملکرد مناسب سیستم اطفا حریق جلوگیری نماید. توصیه می‌شود یک سیستم هشدار دهنده برای کشف خرابی ها در امکانات پشتبانی تهیه و در صورت لزوم نصب شود.

توصیه می‌شود تجهیزات مخابرات حداقل توسط دو مسیر مختلف به ارایه دهنده خدمات متصل شوند تا خرابی در یک مسیر ارتباطات صوتی را دچار اختلال نکند. توصیه می‌شود خدمات صوتی حداقل نیازهای استانداردهای محلی را برای ارتباطات اضطراری برآورده سازد.

اطلاعات دیگر

گزینه‌هایی جهت دستیابی به منبع برق مستمر شامل استفاده از چندین منبع تغذیه برای اجتناب از وقوع قطعی در جریان برق..

۹-۲-۳ امنیت کابل کشی

کنترل

توصیه می‌شود کابل کشی های برق و ارتباطات مورد استفاده برای انتقال داده یا پشتیبانی از خدمات اطلاع رسانی، در برابر شنود، قطع شدن یا وارد آمدن خسارت، محافظت شوند.

1- Uninterruptible Power Supply (UPS)

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر برای امنیت کابل کشی مد نظر قرار گیرند:

الف - توصیه می‌شود خطوط برق و مخابرات متصل به تجهیزات پردازش اطلاعات در صورت امکان از زیرزمین انتقال یابد یا از روش‌های مناسب دیگر از آنها محافظت به عمل آید.

ب - توصیه می‌شود کابل کشی شبکه، از مداخله غیرمجاز یا آسیب محافظت شود، مثلا با عبور از کانال و اجتناب از عبور از محل‌های عمومی

پ - توصیه می‌شود سیم های برق از سیم های مخابرات جدا شود تا از تداخل جلوگیری شود

ت - توصیه می‌شود از کابل هایی که به راحتی قابل تمایز است و از علایم مناسب استفاده شود تا خطاهای انسانی نظیر اتصال اشتباه کابل‌ها به حداقل برسد.

ث - توصیه می‌شود لیست مستند اتصالات برای کاهش احتمال خطا مورد استفاده قرار گیرد

ج - برای سیستم‌های حساس یا حیاتی کنترل های بیشتری لحاظ شود که عبارتند از:

۱- نصب مسیر های دارای حفاظ یا اتاق ها یا جعبه های قفل شده در نقاط بازرسی و ترمینال‌ها

۲ - استفاده از مسیرها و / یا رسانه های انتقال جایگزین جهت تامین امنیت مناسب

۳ - استفاده از کابل فیبر نوری

۴ - استفاده از محافظ های تداخل الکترو مغناطیسی برای محافظت از کابل ها

۵ - آغاز بررسی های فنی و فیزیکی برای یافتن تجهیزاتی که بصورت غیرمجاز به کابل ها وصل شده‌اند

۶ - کنترل دسترسی به پانل های اتصال و اتاق های اتصالات کابل ها

۹-۲-۴ *نگهداری تجهیزات*

کنترل

توصیه می‌شود تجهیزات به منظور حصول اطمینان از تداوم در دسترس بودن و حفظ اصالت آنها، به درستی نگهداری شوند.

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر برای نگهداری از تجهیزات در نظر گرفته شود:

الف - توصیه می‌شود تجهیزات مطابق با فواصل زمانی و مشخصات فنی پیشنهادی تامین کننده نگهداری شوند

ب – تعمیر و سرویس تجهیزات باید فقط توسط کارکنان مجاز بخش نگهداری انجام شود

پ - توصیه می‌شود گزارش هایی از تمام خطاهای واقعی یا مشکوک و تمامی اقدامات نگهداری اصلاحی و پیشگیرانه نگهداری شود

ت - توصیه می‌شود کنترل های مناسب در زمان برنامه ریزی شده برای سرویس تجهیزات اجرا شود و به این مساله توجه شود که آیا این سرویس توسط کارکنان در داخل یا خارج از سازمان انجام می‌شود. همچنین در مواقع لازم، توصیه می‌شود اطلاعات حساس از تجهیزات پاک شود، یا کارکنان سرویس و نگهداری تجهیزات بازرسی بدنی شوند.

ث - توصیه می‌شود تمام تعهدات قید شده در بیمه نامه ها رعایت شوند.

۹-۲-۵ امنیت تجهیزات خارج از ابنیه اماکن سازمان

کنترل

توصیه می‌شود برای تجهیزات خارج از سایت، با توجه به ریسک‌ها مختلف ناشی از انجام کار در خارج از اماکن سازمان، ملاحظات امنیتی لازم بعمل آید..

راهنمای پیاده سازی

توصیه می‌شود صرف نظر از مالکیت تجهیزات، اجازه استفاده از تجهیزات پردازش اطلاعات در خارج از محوطه سازمان توسط مدیریت صادر شود.

توصیه می‌شود رهنمودهای زیر برای محافظت از تجهیزات خارج از سازمان رعایت شوند:

الف - توصیه می‌شود تجهیزات و رسانه هایی که به خارج از محوطه سازمان برده می‌شوند بدون حضور فرد مذکور در محل های عمومی نشوند؛ توصیه می‌شود رایانه‌های قابل حمل به عنوان کیف دستی حمل شوند و در صورت امکان پنهان شوند

ب - توصیه می‌شود دستورالعمل های تولید کننده برای محافظت از تجهیزات همواره مورد توجه قرار گیرد؛ مثلا محافظت دربرابر قرارگرفتن در معرض میدان های الکترومغناطیسی قوی؛

پ - توصیه می‌شود کنترل های مربوط به کار در خانه توسط ارزیابی ریسک های مربوطه تهیه و در زمان مناسب اعمال شوند؛ مثلا قفسه‌هاب بایگانی قابل قفل شدن، سیاست میز پاک، کنترل دسترسی به رایانه‌ها و امنیت ارتباط با شبکه اداره

ت - توصیه می‌شود پوشش بیمه ای کافی برای محافظت از تجهیزات خارج از سایت تهیه گردد.

ریسک‌های امنیتی مانند آسیب، سرقت یا شنود ممکن است بین محل های مختلف متفاوت باشد لذا توصیه می‌شود مناسب ترین کنترل ها مورد استفاده قرار گیرد.

اطلاعات دیگر

تجهیزات ذخیره‌سازی و پردازش اطلاعات شامل انواع رایانه‌های شخصی، سازمان دهنده ها، تلفن های همراه، کارت های هوشمند، کاغذ یا سایر اشکال که برای کار در خانه یا انتقال به سایر نقاط دور از محل کار استفاده می‌شوند

اطلاعات بیشتر درباره جنبه های دیگر محافظت از تجهیزات متحرک را می‌توانید در ۱۱-۷-۱ پیدا کنید.

۹-۲-۶ امحا یا استفاده مجدد از تجهیزات به صورت ایمن

کنترل

توصیه می‌شود تمام اجزای تجهیزاتی که دارای رسانهٔ ذخیره‌سازی می باشند، پیش از امحا به منظور حصول اطمینان از اینکه هر دادهٔ حساس و نرم‌افزار دارای حق امتیاز روی آنها، حذف شده یا به شیوهٔ امنی دوباره نویسی شده اند، بررسی شوند.

راهنمای پیاده سازی

پیش از امحا دستگاه هایی که حاوی اطلاعات حساس هستند، توصیه می‌شود آنها از نظر فیزیکی تخریب شوند یا اطلاعات روی آنها توسط تکنیک هایی خراب، پاک یا حذف شود تا اطلاعات اصلی غیرقابل بازیابی باشد و هرگز نباید از عملکرد "حذف کردن[1]" یا "قالب بندی[1]" استاندارد استفاده کرد.

1- Delete

اطلاعات دیگر

در مورد دستگاه های آسیب دیده که حاوی داده‌های حساس هستند توصیه می‌شود ارزیابی ریسک بعمل آید تا تعیین شود که آیا لازم است که آنها را به جای ارسال برای تعمیر، بصورت فیزیکی نابود کرد یا خیر.

اطلاعات ممکن است از طریق دور ریختن بی دقت یا استفاده مجدد از تجهیزات، مورد دسترسی غیرمجاز قرار گیرد. (همچنین رجوع کنید به ۱۰-۷-۲)

۹-۲-۷ خروج اموال

کنترل

توصیه می‌شود تجهیزات، اطلاعات یا نرم‌افزار، بدون مجوز قبلی، از محوطه خارج نشوند.

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر در نظر گرفته شوند:

الف - توصیه می‌شود تجهیزات، اطلاعات یا نرم‌افزارها بدون اجازه قبلی خارج نشوند

ب - توصیه می‌شود کارکنان، پیمانکاران، و کاربران شخص ثالث که حق دارند اجازه خروج اموال را صادر کنند، به روشنی مشخص شوند

پ - توصیه می‌شود محدودیت های زمانی برای بازگرداندن تجهیزات تعیین و تاریخ بازگشت کنترل شود.

ت - توصیه می‌شود در صورت امکان و لزوم تجهیزات در زمان خروج و بازگشت ثبت شوند.

اطلاعات دیگر

بازدیدهای سریع محلی که عهده‌دار آشکار کردن خروج غیر مجاز اموال است، ممکن است برای آشکار کردن تجهیزات ضبط غیرمجاز، سلاح و غیره نیز بعمل آید و از ورود آنها به سایت جلوگیری شود.

چنین بازدیدهای سریع محلی باید منطبق با ضوابط و قوانین باشد. افراد باید از وجود چنین بازدیدهای سریع محلی آگاه بوده و کنترل‌ها باید با مجوزهای مناسب صورت پذیرد تا با نیازهای قانونی و حقوقی منطبق باشد.

۱۰ مدیریت ارتباطات و عملکرد

۱-۱۰ روش‌های اجرایی عملیاتی و مسوولیت‌ها

هدف : حصول اطمینان از عملکرد صحیح و امن امکانات پردازش اطلاعات توصیه می‌شود مسوولیت‌ها و رویه های مدیریت و اجرای تمام تجهیزات پردازش اطلاعات تثبیت شود. این شامل توسعه رویه های عملیاتی مناسب می‌باشد. توصیه می‌شود تفکیک وظایف در زمان ممکن اجرا شود تا مخاطره سوء استفاده سهوی یا عمدی از سیستم کاهش یابد.

۱۰-۱-۱ *روش‌های اجرایی عملیاتی مستند شده*

کنترل

توصیه می‌شود روش‌های اجرایی عملیاتی، مدون شده، نگهداری شوند و در دسترس تمام کاربرانی که به آنها نیاز دارند قرار گیرند.

راهنمای پیاده سازی

توصیه می‌شود روش‌های اجرایی مستند برای فعالیت‌های سیستم در رابطه با تجهیزات پردازش اطلاعات و ارتباطات نظیر رویه‌های روشن و خاموش کردن رایانه‌ها، تهیه فایل پشتیبان، نگهداری از تجهیزات، کار با محیط‌های ذخیره‌سازی اطلاعات، کنترل کار با رایانه‌ها و اتاق رایانه و ایمنی تهیه شود.

توصیه می‌شود رویه‌های عملیاتی دستورالعمل‌هایی را با جزییات کامل برای انجام وظایف هر شغل مشخص کنند از جمله:

الف - پردازش و کار با اطلاعات

ب – تهیه فایل‌های پشتیبان (رجوع کنید به ۱۰-۵)

پ - الزامات زمان‌بندی از جمله وابستگی‌های متقابل با سیستم‌های دیگر، زمان شروع اولین و خاتمه آخرین کار

ت - دستورالعمل‌هایی برای کنترل خطاها یا دیگر شرایط استثنایی که ممکن است در طول اجرای کار رخ دهد از جمله محدودیت‌های استفاده از امکانات سیستم‌ها (رجوع کنید به ۱۱-۵-۴)

ث – شماره تماس‌های پرسنل پشتیبانی در صورت بروز مشکلات فنی و عملیاتی

ج - خروجی خاص و دستورالعمل‌های کار با محیط‌های ذخیره‌سازی اطلاعات نظیر استفاده از محل خاص یا مدیریت خروجی‌های محرمانه شامل رویه‌هایی برای دور ریز ایمن خروجی از کارهایی که با مشکل مواجه شده اند. (رجوع کنید به ۱۰-۷-۲ و ۱۰-۷-۳)

چ - آغاز مجدد سیستم و رویه‌هایی بازگردانی در صورت نقص در عملکرد سیستم؛

ح – مدیریت ممیزی سیستم و اطلاعات وارده به آن(رجوع کنید به ۱۰-۱۰)

توصیه می‌شود رویه‌های عملیاتی و رویه‌های مستند برای فعالیت‌های سیستم به عنوان اسناد رسمی در نظر گرفته شوند و تغییرات آنها فقط با مجوز مدیریت انجام پذیرد. هر زمان که از نظر فنی امکان پذیر باشد، توصیه می‌شود سیستم‌های اطلاعات با استفاده از رویه‌ها، ابزارها و کاربردهای یکسان و به طور سازگار مدیریت شوند.

۱۰-۱-۲ مدیریت تغییر

کنترل

توصیه می‌شود تغییر در امکانات و سیستم‌های پردازش اطلاعات، تحت کنترل باشد.

راهنمای پیاده سازی

توصیه می‌شود سیستم‌های عملیاتی و نرم‌افزارها از نظر تغییرات تحت مدیریت کنترل شدید قرار گیرند.

به خصوص، موارد زیر توصیه می‌شود مد نظر قرار گیرد:

الف - شناسایی و ثبت تغییرات مهم

ب - برنامه ریزی و آزمون تغییرات مهم

پ- ارزیابی تاثیرات بالقوه، از جمله تاثیرات ایمنی این تغییرات؛

ت - رویه تایید رسمی برای انجام تغییرات پیشنهادی

ث – تبادل جزییات تغییرات با افراد مرتبط

ج - رویه‌های برگشت از تغییرات از جمله رویه‌ها و مسوولیت‌های توقف و بازگردانی موفق به حالت قبل از تغییرات در صورت وقوع وقایع پیش بینی نشده

توصیه می‌شود مسوولیت‌ها و رویه‌های مدیریت رسمی برای تضمین کنترل رضایت بخش تمام تغییرات در تجهیزات، نرم‌افزار یا رویه‌ها تعیین شود. زمانی که تغیرات انجام شد، توصیه می‌شود یک حساب ممیزی حاوی تمام اطلاعات مرتبط حفظ شود.

سایر اطلاعات

کنترل ناکافی تغییرات در تجهیزات و سیستم‌های پردازش اطلاعات، یکی از دلایل متداول ناکامی‌های سیستم یا امنیت است. قرار دادن یک سیستم در محیط عملیاتی به خصوص در زمان انتقال یک سیستم از مرحله توسعه به مرحله عملیاتی ممکن است بر قابلیت اطمینان برنامه‌های کاربردی تاثیر بگذارد. (همچنین رجوع کنید به ۱۲-۵-۱)

توصیه می‌شود تغییرات در سیستم‌های عملیاتی فقط زمانی انجام شود که دلیل کسب وکار معتبری برای انجام این کار وجود داشته باشد. مثلا افزایش ریسک سیستم. به روز رسانی سیستم‌ها با جدیدترین نسخه‌های سیستم‌های عامل همیشه از نظر کسب وکار به صرفه نیست زیرا ممکن است آسیب پذیری‌ها و ناپایداری بیشتری را در مقایسه با نسخه فعلی به همراه داشته باشد. همچنین ممکن است نیاز به آموزش تکمیلی و هزینه‌های دریافت مجوز استفاده، پشتیبانی، نگهداری و هزینه‌های بالاسری اجرا و سخت افزار جدید به خصوص در زمان انتقال وجود داشته باشد.

۱۰-۱-۳ تفکیک وظایف

کنترل

به منظور کاهش فرصت‌های دستکاری غیر عمد یا غیر مجاز، یا استفاده نابجا از دارایی‌های سازمان، توصیه می‌شود وظایف و حدود اختیارات تفکیک شوند.

راهنمای پیاده سازی

تفکیک وظایف روشی برای کاهش ریسک مربوط به سوء استفاده تصادفی یا عمدی از سیستم است. توصیه می‌شود مراقبت‌های لازم جهت کنترل دسترسی به دارایی‌ها و اصلاح، یا استفاده هر یک از افراد، بدون اطلاع و هماهنگی و یا

تشخیص بعمل آید. توصیه می‌شود انجام هر امری از مجوز انجام آن مجزا باشد. توصیه می‌شود احتمال تبانی در طراحی کنترل‌ها در نظر گرفته شود.
سازمان‌های کوچک ممکن است انجام تفکیک وظایف را دشوار بدانند اما توصیه می‌شود این اصل همیشه تا حد امکان و به هر میزان که ممکن است رعایت شود. هر زمان که تفکیک وظایف دشوار باشد، توصیه می‌شود کنترل‌های دیگر نظیر کنترل فعالیت‌ها، ممیزی امور و نظارت‌های مدیریتی بکار برده شود. آنچه مهم است مستقل بودن ممیزی امنیت است.

۱۰-۱-۴ جداسازی امکانات توسعه، آزمون و عملیاتی

کنترل

توصیه می‌شود امکانات مربوط به سیستم‌های درحال توسعه، تحت آزمایش و عملیاتی، به منظور کاهش ریسک ناشی از دسترسی غیر مجاز یا تغییرات در سیستم‌های عملیاتی، تفکیک شوند.

راهنمای پیاده سازی

توصیه می‌شود سطح تفکیک بین محیط‌های عملیاتی، تحت آزمایش و درحال توسعه که برای پیشگیری از مشکلات عملیاتی لازم است، توصیه می‌شود که شناسایی شده و کنترل‌های مناسب اعمال شود.
توصیه می‌شود موارد زیر مد نظر قرار گیرد:

الف - توصیه می‌شود قوانین انتقال نرم‌افزار از حالت توسعه به حالت عملیاتی، تعریف و مستند شود.

ب - توصیه می‌شود نرم‌افزارهای تحت توسعه و عملیاتی، روی رایانه‌های متفاوت و یا پردازشگرهای متفاوت یک رایانه و از دامنه و پوشه‌های مختلف اجرا شوند.

پ - توصیه می‌شود همگردان‌ها[1]، ویراستارها و دیگر ابزار توسعه از سیستم‌های عملیاتی در زمانی‌که لازم نیستند قابل دسترسی نباشند.

ت - توصیه می‌شود محیط سیستم‌های تحت آزمایش تا حد امکان با محیط عملیاتی شباهت داشته باشد.

ث - توصیه می‌شود کاربران از نمایه‌های کاربری متفاوتی برای کار در محیط سیستم‌های تحت آزمایش و عملیاتی استفاده کنند و توصیه می‌شود تا منوهایی برای کاهش ریسک خطا، نمایه کاربری مورد استفاده را نمایش دهند.

ج - توصیه می‌شود داده‌های حساس، به محیط سیستم، تحت آزمایش کپی نشوند. (رجوع کنید به ۱۲-۴-۲)

اطلاعات دیگر

فعالیت‌های تست و توسعه می‌توانند باعث بروز مشکلات جدی مانند تغییر ناخواسته ی فایل‌ها یا محیط سیستم و یا خرابی سیستم شوند. در این صورت، باید محیط شناخته شده و پایداری حفظ شود که در آن، تست معنا دار انجام شود و از دسترسی نامناسب توسعه دهند نرم‌افزاری جلوگیری به عمل آید.
در جایی که کاربران سیستم‌های تحت توسعه و یا آزمون به سیستم‌های عملیاتی و اطلاعات آن دسترسی دارند، ممکن است باعث اعمال کد غیرمجاز و تست نشده‌ای شده و یا داده‌های عملیاتی را تغییر دهند. در بعضی از سیستم‌ها، این قابلیت ممکن است باعث سوءاستفاده شده یا کد غیرمجازی وارد شود که باعث مشکلات عملیاتی مهمی شود.

1- Compilers

کاربران توسعه و آزمون سیستم‌ها برای محرمانگی اطلاعات سیستم‌های عملیاتی تهدید یک به حساب می‌آیند. اگرفعالیت‌های توسعه و آزمون سیستم‌ها در محیط محاسباتی مشترکی انجام شود ممکن است تغییرات ناخواسته‌ای را برای نرم‌افزار یا اطلاعات ایجاد کند. بنابراین تفکیک تجهیزات محیط‌های عملیاتی، تحت توسعه و آزمون برای کاهش ریسک تغییرات تصادفی یا دسترسی غیرمجاز به نرم‌افزار عملیاتی و داده‌های کسب وکار ضروری است. (برای حفاظت از داده‌های آزمون، همچنین رجوع کنید به ۱۲-۴-۲)

۱۰-۲ مدیریت تحویل خدمت شخص سوم

هدف : پیاده سازی و نگهداری سطح مناسب امنیت اطلاعات و تحویل خدمت، در راستای توافق‌نامه‌های تحویل خدمت شخص ثالث. توصیه می‌شود سازمان اجرای توافقات را بررسی نماید، مطابقت با توافقات را کنترل نماید و تغییرات را مدیریت نماید تا تضمین شود که خدمات ارایه شده تمام الزامات توافق شده با شخص ثالث را برآورده می سازد.

۱۰-۲-۱ *تحویل خدمت*

کنترل

توصیه می‌شود از پیاده‌سازی، عملیاتی شدن و نگهداری کنترل‌های امنیتی، تعاریف خدمت و سطوح تحویل مندرج در توافق‌نامه تحویل خدمت اشخاص ثالث،اطمینان حاصل شود.

راهنمای پیاده سازی

وصیه می‌شود توافقنامه ارایه خدمات اشخاص ثالث باید دربرگیرنده قراردادهای امنیتی توافق شده، تعاریف خدمات و جنبه‌های مدیریت خدمات باشد. در صورت واگذاری خدمات به بیرون از سازمان، توصیه می‌شود سازمان مراحل انتقال (اطلاعات، تجهیزات پردازش اطلاعات و سایر امکانات دیگر) به داخل سازمان را تعریف نموده و توصیه می‌شود تضمین نماید که امنیت اطلاعات درزمان سراسر زمان انتقال حفظ می‌شود.

توصیه می‌شود سازمان از توانایی اشخاص ثالث در ارایه خدمات با کیفیت مطلوب و داشتن برنامه کاری مناسب جهت تداوم ارایه سطح خدمات لازم و عدم وقوع وقفه در ارایه خدمات حساس اطمینان حاصل نماید.(رجوع کنید به۱۴-۱)

۱۰-۲-۲ *پایش و بازبینی خدمات شخص سوم*

کنترل

وصیه می‌شود خدمات، گزارشات و سوابق تهیه شده توسط اشخاص ثالث، به صورت قاعده مند پایش و بازبینی شده، و توصیه می‌شود ممیزی‌ها به صورت منظم انجام شوند.

راهنمای پیاده سازی

توصیه می‌شود کنترل و بررسی خدمات ارایه شده اشخاص ثالث تضمینی بر رعایت مفاد و شرایط مربوط به امنیت اطلاعات در قراردادها و مدیریت مطلوب حوادث و مشکلات امنیت اطلاعات است. توصیه می‌شود این موضوع دربرگیرنده رابطه و فرایند مدیریت خدمات بین سازمان و اشخاص ثالث باشد تا:

الف - سطوح ارایه خدمات را جهت کنترل رعایت مفاد قرارداد بررسی نماید؛

ب - گزارش‌های خدمات ارایه شده توسط اشخاص ثالث را بررسی نماید و جلسات منظمی را برای بررسی تطابق روند پیشرفت کار با مفاد قرارداد ترتیب دهد.

پ - اطلاعاتی در رابطه با حوادث امنیت اطلاعات ارایه دهد و این اطلاعات را جهت بررسی توسط شخص ثالث و سازمان در صورتی که در قرارداد یا هر یک از دستورالعمل‌ها و رویه‌ها ذکر شده باشد در اختیار آنها قرار دهد.

ت - گزارش‌های ممیزی شخص ثالث و گزارش‌های حوادث امنیتی، مشکلات عملیاتی ناکامی‌ها و ردیابی تقصیرات و اختلالات در رابطه با خدمات ارایه شده را بررسی کند.

ث - هر مشکل تشخیص داده شده ای را حل و مدیریت کند.

توصیه می‌شود مسوولیت مدیریت روابط با با اشخاص ثالث به یک فرد منصوب شده یا تیم مدیریت خدمات سپرده شود. به علاوه، توصیه می‌شود سازمان باید از واگذاری مسوولیت امکان بررسی رعایت مفاد قرارداد توسط اشخاص ثالث اطمینان حاصل نماید. توصیه می‌شود مهارت و منابع فنی کافی در دسترس قرار گیرد تا رعایت الزامات قرارداد به خصوص الزامات امنیت اطلاعات کنترل شوند(رجوع کنید به ۶-۲-۳). توصیه می‌شود اقدامات لازم زمانی که نقصی در ارایه خدمات مشاهده شد صورت گیرد.

توصیه می‌شود سازمان در تمام جنبه‌های مربوط به اطلاعات حساس و حیاتی یا تجهیزات پردازش اطلاعات که مورد دسترسی یا مدیریت اشخاص ثالث قرار دارند، ابزارهای کنترلی خود را حفظ نموده و اطمینان حاصل کند که امکان پایش را در فعالیت‌های امنیتی نظیر مدیریت تغییرات، شناسایی آسیب پذیری‌ها و حوادث امنیت اطلاعات از طریق دریافت گزارشات تعریف شده با ساختار و شکل مشخص دارا می‌باشد.

اطلاعات دیگر

در صورت واگذاری خدمات به بیرون، سازمان باید آگاه باشد که هنوز مسوولیت نهایی اطلاعات پردازش شده به عهده سازمان است.

۱۰-۲-۳ مدیریت تغییرات در خدمات شخص سوم

کنترل

توصیه می‌شود تغییرات در ارایه خدمات شامل نگهداری و بهبود خط‌مشی‌های امنیت اطلاعات، روش‌های اجرایی و کنترل‌های موجود، توصیه می‌شود با توجه به میزان بحرانی بودن سیستم‌های کسب‌وکار و فرایندهای مرتبط و برآورد مجدد ریسک‌ها، مدیریت شوند.

راهنمای پیاده سازی

در فرایند مدیریت تغییرات خدمات اشخاص ثالث باید موارد زیر در نظر گرفته شود:

الف - تغییرات ایجاد شده توسط سازمان:

۱-بهبود هر یک از کاربردها و سیستم‌های جاری

۲-توسعه هر یک از کاربردها و سیستم‌های جدید؛

۳- اصلاحات یا ارتقای خط مشی‌ها و رویه‌های سازمان

۴- کنترل‌های جدید برای حل حوادث امنیت اطلاعات و بهبود امنیت

ب - تغییرات در خدمات اشخاص ثالث:

۱-تغییر و بهبود شبکه

۲-استفاده از فن‌آوری‌های جدید
۳- استفاده از محصولات جدید یا مدل‌ها و نسخه‌های جدیدتر محصول
۴- ابزارها و محیط جدید توسعه
۵- تغییرات در محل فیزیکی تجهیزات خدمات
۶- تغییر محصول

۱۰-۳ طرح‌ریزی و پذیرش سیستم

هدف : کمینه کردن مخاطرات ناشی از خرابی سیستم‌ها.
برنامه ریزی و آماده سازی پیشرفته ای برای تضمین دسترسی به ظرفیت و منابع کافی برای ارائه عملکرد مورد نیاز سیستم لازم است.
پیش بینی لازم در مورد ظرفیت مورد نیاز آینده به عمل آید تا مخاطره تحمیل بار زیادی به سیستم کاهش یابد.
توصیه می‌شود نیازهای عملیاتی سیستم‌های جدید در نظر گرفته و مستند شود و قبل از پذیرش و استفاده از آنها تست شود.

۱۰-۳-۱ *مدیریت ظرفیت*

کنترل
توصیه می‌شود استفاده از منابع پایش و تنظیم شده و ظرفیت مورد نیاز در آینده به گونه ای پیش بینی شود که از کارایی مورد نیاز سیستم، اطمینان حاصل شود.
راهنمای پیاده سازی
توصیه می‌شود برای هر فعالیت جدید و جاری، توصیه می‌شود نیازهای ظرفیتی شناسایی شود. توصیه می‌شود سیستم‌ها تنظیم و پایش شوند تا از تداوم عملکرد و مطلوبیت کارایی آنها در هنگام نیاز اطمینان حال شود و در صورت لزوم بهبود یابد. توصیه می‌شود از کنترل‌های شناسایی استفاده شود تا مشکلات در زمان مناسب تشخیص داده شوند. توصیه می‌شود پیش بینی الزامات ظرفیتی آینده، الزامات کسب وکار و سیستمی جدید و گرایش‌های جاری و پیش بینی شده را در قابلیت‌های پردازش اطلاعات سازمان در نظر بگیرد.
باید توجه خاصی به منابعی که زمان طولانی یا هزینه بالایی جهت تهیه دارند نمود. بنابراین توصیه می‌شود مدیران نحوه استفاده از منابع کلیدی سیستم‌ها را زیرنظر بگیرند. توصیه می‌شود آنها باید روند استفاده را به خصوص در رابطه با کاربردهای کسب وکار یا ابزارهای سیستم اطلاعات مدیریت بررسی کنند.
توصیه می‌شود مدیران از این اطلاعات برای شناسایی و اجتناب از تنگناهای احتمالی و وابستگی به کارکنان کلیدی که ممکن است برای امنیت سیستم یا خدمات تهدید به حساب آیند استفاده کرده و اقدامات مناسب را برنامه ریزی نمایند.

۱۰-۳-۲ *پذیرش سیستم*

کنترل

توصیه می‌شود معیار پذیرش برای سیستم‌های اطلاعاتی جدید، ارتقا سیستم‌های جاری و نسخه‌های جدید ایجاد شده و در حین توسعه و پیش از پذیرش سیستم، آزمایش‌های مناسب انجام پذیرند.

راهنمای پیاده سازی

توصیه می‌شود مدیران مطمئن شوند که الزامات و معیارهای پذیرش سیستم‌های جدید به طور شفاف تعریف شده، مورد توافق قرار گرفته، مستند و تست می‌شوند. توصیه می‌شود عملیاتی شدن سیستم‌های اطلاعاتی جدید، به روز رسانی سیستم‌های جاری و استفاده از نسخه جدید سیستم‌ها پس از پذیرش رسمی آن صورت پذیرد.

توصیه می‌شود موارد زیر قبل از پذیرش رسمی سیستم‌ها مورد توجه قرار گیرد:

الف - نیازهای ظرفیتی و کارایی رایانه‌ها

ب - رویه‌های بازیابی خطا و آغاز مجدد و برنامه‌های همسوسازی

پ - آماده سازی و تست رویه‌های عملیاتی متداول با استانداردهای تعریف شده

ت - مجموعه کنترل‌های امنیتی تایید شده

ث – روش‌های اجرایی دستی موثر

ج - هماهنگی‌های استمرار تجارت(رجوع کنید به ۱۴-۱)

چ - شواهدی که نشان می دهند نصب سیستم جدید تاثیری منفی بر سیستم‌های فعلی به خصوص در زمان‌های اوج پردازش نظیر پایان ماه نخواهد داشت.

ح - شواهدی که نشان می دهد به تاثیر سیستم جدید بر کل امنیت سازمان توجه کافی شده است.

خ - آموزش بهره بردار ی و استفاده از سیستم‌های جدید

د - سهولت استفاده؛ زیرا بر عملکرد کاربر تاثیر گذاشته و از خطای انسانی جلوگیری می‌کند.

برای توسعه سیستم‌های مهم و جدید، توصیه می‌شود توابع عملیاتی و کاربران در مراحل مختلف فرایند توسعه مورد مشاوره قرار گیرند تا از بازدهی طراحی سیستم پیشنهادی اطمینان حاصل شود. توصیه می‌شود تست‌های مناسب برای تایید رعایت کامل تمام معیارهای پذیرش انجام شود.

اطلاعات دیگر

پذیرش ممکن است شامل یک فرایند صدور گواهی و تایید صلاحیت برای تصدیق رعایت الزامات امنیتی باشد.

۱۰-۴ حفاظت در برابر کدهای مخرب و سیار

هدف : حفاظت از یکپارچگی نرم افزارها و اطلاعات

برای جلوگیری از ورود وکشف کدهای بدخواهانه و سیار غیرمجاز باید ملاحظات احتیاطی لازم بعمل آید.

نرم‌افزارها و تجهیزات پردازش اطلاعات نسبت به ورود کد بدخواهانه، مانند ویروس‌های کامپیوتری، کرم‌های شبکه، اسب‌های تروجان و بمب‌های منطقی آسیب‌پذیر هستند. توصیه می‌شود به کاربران در مورد خطرات کدهای بدخواهانه هشدار داده شود. توصیه می‌شود مدیران در زمان مناسب کنترل‌هایی را برای جلوگیری، کشف و رفع کدهای بدخواهانه و کنترل کدهای سیار، در نظر بگیرند.

۱۰-۴-۱ *کنترل هایی در برابر کدهای مخرب*

کنترل

توصیه می‌شود کنترل‌های لازم برای تشخیص کدهای مخرب، پیشگیری و ترمیم در برابر آنها، و روش‌های اجرایی مناسب برای آگاه‌سازی کاربران بکار برده شود.

راهنمای پیاده سازی

توصیه می‌شود محافظت دربرابر کدهای مخرب بر اساس نوع کد کشف شده و نرم‌افزار مقابله با آن، آگاهی‌های امنیتی، و راهکارهای دسترسی مناسب به سیستم و کنترل مدیریت تغییرات باشد.

توصیه می‌شودرهنمودهای زیر در نظر گرفته شود:

الف – تدوین یک خط‌مشی رسمی برای جلوگیری از استفاده از نرم‌افزارهای غیرمجاز (رجوع کنید به ۱۵-۱-۲)

ب - تدوین یک خط‌مشی رسمی برای محافظت در برابر ریسک‌های مربوط به دستیابی به فایل‌ها و نرم‌افزارها از طریق شبکه‌های بیرونی یا هر رسانه دیگر که نشان دهنده روش‌های پیشگیری مورد اتخاذ هم باشد.

پ - انجام بررسی‌های منظم نرم‌افزارها و محتوای اطلاعات سیستم‌هایی که فرایندهای حیاتی کسب وکار را پشتیبانی می‌کنند؛ توصیه می‌شود حضور هر فایل تایید نشده یا تغییر غیرمجاز رسما بررسی شود.

ت - نصب و به روز رسانی منظم نرم‌افزارهای کشف و ترمیم کدهای مخرب برای اسکن رایانه‌ها و رسانه‌ها به عنوان یک کنترل احتیاطی توصیه می‌شود کنترل‌های انجام شده شامل موارد زیر باشد:

۱- بررسی هر فایل روی رسانه‌های الکترونیکی یا نوری و فایل‌های دریافت شده از طریق شبکه‌ها برای کنترل وجود کدهای مخرب قبل از استفاده.

۲- کنترل ضمیمه‌های نامه‌های الکترونیکی برای کنترل کدهای مخرب قبل از استفاده؛ توصیه می‌شود این بررسی در محل‌های مختلف مثلا در سرویسگرهای پست الکترونیکی، رایانه‌های رومیزی، و در زمان ورود به شبکه سازمان انجام شود؛

۳- بررسی صفحات وب برای کد مخرب

ث - تعریف رویه‌ها و مسوولیت‌های مدیریت جهت محافظت سیستم‌ها در مقابل کدهای مخرب، آموزش استفاده از آنها، گزارش و بازیابی اطلاعات پس از وقوع حملات کدهای مخرب (رجوع کنید به۱۳-۱ و ۱۳-۲)

ج - آماده سازی برنامه‌های استمرار کسب وکار مناسب برای بازیابی اطلاعات پس از وقوع حملات کدهای مخرب از جمله تمام داده‌ها و نرم‌افزارها و فایل‌های پشتیبان (رجوع کنید به بند ۱۴)

چ - پیاده‌سازی روش‌های اجرایی برای جمع‌آوری منظم اطلاعات، مانند درخواست اشتراک در لیست‌های ارسال نامه و/ یا بررسی سایت‌های اینترنتی که اطلاعاتی درباره کدهای مخرب می‌دهد

ح - اجرای رویه‌هایی برای بررسی صحت اطلاعات مربوط به کدهای مخرب و تضمین این که اطلاعات بولتن‌های هشدار دهنده، دقیق و جامع هستند؛ مدیران باید تضمین کنند که منابع واجد شرایط، مانند مجلات معتبر، سایت‌های اینترنتی قابل اطمینان، یا تامین کنندگانی که نرم‌افزارهایی تولید می‌کنند که در برابر کدهای مخرب محافظت می‌کند، برای تمایز بین توهمات و کدهای مخرب واقعی مورد استفاده قرار می‌گیرند. توصیه می‌شود تمام کاربران از مساله توهمات و این که در زمان دریافت آنها چه کار باید انجام دهند مطلع شوند.

اطلاعات دیگر:

استفاده از دو یا چند محصول نرم‌افزاری از شرکت‌های متفاوت که در برابر کدهای مخرب، محیط پردازش اطلاعات را محافظت می‌کنند می‌تواند تاثیر محافظت در برابر کدهای مخرب را بهبود بخشند.
نرم‌افزارهای محافظت در برابر کدهای مخرب را می‌توان به گونه ای نصب کرد که بصورت اتوماتیک فایل‌های تعریف و موتور بررسی خود را به‌روز رسانی کند تا از به روز بودن آن اطمینان حاصل شود. به علاوه، این نرم‌افزارها را می‌توان روی هر رایانه‌ای نصب نمود تا کنترل‌ها بصورت اتوماتیک انجام شود.
در زمان تعمیرات یا انجام روال‌های اضطراری که کنترل‌های معمول مراقبت در مقابل کدهای مخرب معلق می‌شوند در مقابل ورود کدهای مخرب باید مراقب بود.

۱۰-۴-۲ *کنترل هایی در برابر کدهای سیار*

کنترل

توصیه می‌شود جایی‌که استفاده از کدهای سیار مجاز است، پیکربندی به نحوی باشد که از انطباق عملکرد کد سیار، با خط‌مشی امنیتی ای که به صورت شفاف تعریف شده، بتوان اطمینان حاصل نمود، و توصیه می‌شود از اجرای کد سیار غیر مجاز نیز پیشگیری شود.

راهنمای پیاده سازی

توصیه می‌شود ملاحظات زیر برای محافظت در برابر انجام فعالیت‌های غیرمجاز کدهای سیار در نظر گرفته شود:

الف - اجرای کد سیار در یک محیط مجزا
ب - جلوگیری از استفاده از هر گونه کد سیار
پ - جلوگیری از دریافت کد سیار
ت - استفاده از تمهیدات فنی موجود در یک سیستم خاص برای مدیریت کدهای سیار
ث - کنتر ل منابع قابل دسترسی توسط کد سیار
ج -استفاده از روش‌های رمزنگاری برای احراز هویت کدهای سیار

اطلاعات دیگر

کد سیارکدی نرم‌افزاری است که از یک رایانه به رایانه دیگر حرکت می‌کند و سپس به طور اتوماتیک عملکرد خاصی را بدون تعامل کاربر اجرا می‌کند. کد سیار با تعدادی از خدمات واسط در ارتباط است.
علاوه بر کسب اطمینان از این که کدهای سیار حاوی کدهای مخرب نیستند، کنترل کد سیار آنها برای اجتناب از استفاده غیرمجاز یا اختلال در سیستم، شبکه، یا سایر منابع و دیگر نقض‌های امنیت اطلاعات حیاتی است.

۱۰-۵ نسخه‌های پشتیبان

هدف : حفظ یکپارچگی و در دسترس بودن به اطلاعات و امکانات پردازش اطلاعات
توصیه می‌شود رویه‌های منظم برای اجرای خط‌مشی و راهبردهای تهیه فایل پشتیبان به منظور داشتن نسخه‌های پشتیبان از داده‌ها و ذخیره به موقع آنها تهیه شود.(همچنین رجوع کنید به ۱۴-۱)

۱۰-۵-۱ *ایجاد پشتیبان از اطلاعات*

کنترل

توصیه می‌شود تهیه فایل پشتیبان از اطلاعات و نرم‌افزارها، با توجه به خط‌مشی توافق شده نسخه‌های پشتیبان، به صورت منظم انجام و آزمایش شوند.

راهنمای پیاده سازی

توصیه می‌شود تجهیزات لازم برای تهیه فایل پشتیبان و بازیابی آن، فراهم شود تا تضمین شود که تمام اطلاعات ضروری و نرم‌افزارها را می‌توان پس از یک حادثه یا خرابی رسانه‌ها بازیابی نمود.

توصیه می‌شود موارد زیر برای تهیه فایل پشتیبان از اطلاعات در نظر گرفته شود:

الف - اطلاعاتی که باید از آنها فایل پشتیبان تهیه شود مشخص شوند.

ب - توصیه می‌شود سوابق دقیق و کامل از فایل‌های پشتیبان و مستندات مربوط به نحوه بازگردانی آنها تهیه شود.

پ - توصیه می‌شود نوع و فواصل زمانی تهیه فایل پشتیبان بر اساس الزامات کسب وکار سازمان، میزان حساسیت و حیاتی بودن اطلاعات برای فعالیت‌های سازمان باشد.

ت - توصیه می‌شود فایل‌های پشتیبان در یک محل دیگر و با فاصله کافی از سایت اصلی برای اجتناب از هر گونه آسیب ناشی از وقوع حادثه در سایت اصلی ذخیره شوند.

ث - توصیه می‌شود فایل‌های پشتیبان باید دارای سطح مناسبی از محافظت فیزیکی و محیطی باشند که با استانداردهای مربوطه همخوانی داشته باشد. توصیه می‌شود کنترل‌های حفاظتی استفاده شده در مورد رسانه‌های سایت اصلی در سایت پشتیبان هم به کار برده شوند(رجوع کنید به بند ۹)

ج - توصیه می‌شود رسانه‌های ذخیره فایل‌های پشتیبان به طور منظم تست شوند تا اطمینان حاصل شود که میتوان برای استفاده اضطراری در زمان لازم به آنها تکیه کرد

چ - توصیه می‌شود رویه‌های بازیابی اطلاعات به طور منظم بررسی و تست شود تا تضمین شود که آنها قابل استفاده بوده و از طریق آنها طی زمان مشخص شده در سیاست‌های امنیتی اطلاعات قابل بازگردانی هستند.

ح - توصیه می‌شود در شرایطی که محرمانگی اطلاعات اهمیت دارد، فایل‌های پشتیبان بصورت رمز نگهداری شوند.

توصیه می‌شود تهیه فایل پشتیبان برای تک تک سیستم‌ها به طور منظم تست شود تا تضمین شود که آنها الزامات برنامه‌های استمرار کسب وکار را برآورده می سازند(رجوع کنید به بند ۱۴). توصیه می‌شود برای سیستم‌های حیاتی،از تمام اطلاعات، کاربردها، و داده‌هاکه برای بازگردانی کامل سیستم در صورت بروز حادثه به آنها نیاز است، فایل پشتیبان تهیه شود.

توصیه می‌شود زمان نگهداری اطلاعات حیاتی کسب وکار و نیز هر الزام دیگری که برای نگهداری مناسب کپی‌های آرشیو لازم است تعیین شود. (رجوع کنید به ۱۵-۱-۳)

اطلاعات دیگر

تهیه فایل پشتیبان را می‌توان اتوماتیک نمود تا فرایند تهیه فایل پشتیبان و بازیابی آن تسهیل شود. توصیه می‌شود عملکرد این راه حل‌های اتوماتیک قبل از اجرا و در فواصل منظم تست شوند.

۱۰-۶ مدیریت امنیت شبکه

هدف : حصول اطم ـنان از حفاظت اطلاعات در شبکه‌ها و زیر ساختارهای پشتیبانی کننده آنها.
مدیریت امن شبکه‌ها که ممکن است مرزهای سازمانی را در نوردد نیازمند ملاحظه دقیق جریان داده، آثار حقوقی، کنترل و محافظت آن می‌باشد. کنترل‌های تکمیلی ممکن است برای محافظت از عبور اطلاعات حساس در شبکه‌های همگانی لازم باشد.

۱۰-۶-۱ *کنترل های شبکه*

کنترل

توصیه می‌شود شبکه‌ها به منظور حفاظت در برابر تهدیدها و برای حفظ امنیت سیستم‌ها و برنامه‌های کاربردی که از شبکه استفاده می‌کنند (شامل اطلاعات در گردش)، به میزان کفایت، مدیریت و کنترل شوند.

راهنمای پیاده سازی

توصیه می‌شود مدیران شبکه‌ها کنترل‌هایی را اجرا کنند تا امنیت اطلاعات در شبکه‌ها تضمین شده و خدمات شبکه در قبال دسترسی غیر مجاز حفظ شوند. به خصوص، توصیه می‌شود موارد زیر در نظر گرفته شود:

الف - توصیه می‌شود مسوول عملیاتی شبکه‌ها هر جا که ممکن بود از مسوول عملیاتی رایانه‌ها تفکیک شود. (رجوع کنید به ۱۰-۱-۳)

ب - مسوولیت‌ها و رویه‌های مدیریت تجهیزات راه دور از جمله تجهیزاتی که توسط کاربر مورد استفاده قرار می‌گیرد توصیه می‌شود تدوین و اجرا شود

پ - توصیه می‌شود کنترل‌های خاصی برای محافظت از محرمانگی و یکپارچگی داده‌هایی که از شبکه‌های همگانی یا شبکه‌های بی سیم عبور می‌کند پیش بینی شود و از سیستم‌ها و کاربردهای مرتبط محافظت شود؛ کنترل‌های خاصی نیز ممکن است برای حفظ دسترسی به خدمات شبکه و رایانه‌های متصل لازم باشد(رجوع کنید به ۱۱-۴ و ۱۲-۳)

ت - توصیه می‌شود از ابزار مشاهده و ثبت وقایع مناسب استفاده شود تا ثبت وقایع امنیتی امکان‌پذیر شود.

ث - توصیه می‌شود فعالیت‌های مدیریتی به‌دقت هماهنگ شود تا خدمات مربوط به سازمان بهینه شده و همچنین از بکار گیری مناسب کنترل‌ها در زیرساختار پردازش اطلاعات اطمینان حاصل شود.

اطلاعات دیگر

اطلاعات تکمیلی درباره امنیت شبکه را می‌توانید در ISO/IEC 18028T، روش‌های امنیت فن‌آوری اطلاعات- امنیت شبکه IT، مطالعه فرمایید.

۱۰-۶-۲ *امنیت خدمات شبکه*

کنترل

توصیه می‌شود ویژگی‌های امنیتی، سطوح خدمات، و الزامات مدیریتی تمامی خدمات شبکه، شناسایی شده و در هر توافق‌نامهٔ خدمات شبکه، اعم از اینکه این خدمات در داخل انجام یا برون سپاری می‌شود، لحاظ شود.

راهنمای پیاده سازی

توصیه می‌شود توانایی‌های ارایه کننده خدمات شبکه در مدیریت خدمات موردتوافق به گونه ای مطمئن، تعیین شود و به طور منظم مورد نظارت قرار گیرد و توصیه می‌شود حق ممیزی برای کارفرما مورد تاکید قرار گیرد.
توصیه می‌شود هماهنگی‌های امنیتی مورد نیاز برای خدات خاص مانند ویژگی‌های امنیتی، سطوح خدمات، و الزامات مدیریت شناسایی شوند. توصیه می‌شود سازمان اطمینان حاصل کند که ارایه کنندگان خدمات شبکه توانایی انجام این خدمات را دارند.

اطلاعات دیگر

خدمات شبکه می‌تواند شامل پیش‌بینی و تامین ارتباطات، خدمات شبکه خصوصی، شبکه‌های ارزش افزوده و راه‌حل‌های امنیت شبکه نظیر دیوارهای آتش و سیستم‌های کشف ورود غیرمجاز باشد.
این خدمات ممکن است از ارایه عرض باند مدیریت نشده ساده تا خدمات ارزش افزوده پیچیده متغیر باشد.
ویژگی‌های امنیتی خدمات شبکه می‌تواند شامل موارد زیر باشد:

الف - فن‌آوری به کار رفته برای امنیت خدمات شبکه نظیر مجوز دهی، رمزنگاری و کنترل‌های امنیت شبکه
ب - پارامترهای فنی موردنیاز برای ارتباط امن با خدمات شبکه مطابق با قوانین ارتباطات شبکه و امنیت
پ - رویه‌هایی برای استفاده از خدمات شبکه جهت محدود کردن دسترسی به خدمات یا کاربردهای شبکه در صورت لزوم

۱۰-۷ اداره‌کردن محیطهای ذخیره‌سازی

هدف : پ یشگیری از افشاء، دستکاری، خروج یا تخریب غیر مجاز دارایی‌ها و وقفه در فعالیتهای کسب‌وکار.
توصیه می‌شود محیطهای ذخیره‌سازی اطلاعات کنترل و بصورت فیزیکی محافظت شوند.
توصیه می‌شود روش‌های اجرایی عملیاتی مناسب برقرار بکار برده شود تا از مدارک و محیطهای ذخیره‌سازی (برای مثال، نوارها، دیسک‌ها)، داده های ورودی/خروجی و مستندات سیستم در برابر افشاء، تغییر، حذف و جابجایی غیرمجاز حفاظت بعمل آید.

۱۰-۷-۱ *مدیریت محیطهای ذخیره‌سازی قابل جابجایی*

کنترل

توصیه می‌شود برای مدیریت محیط‌های ذخیره‌سازی قابل جابجایی، روش‌های اجرایی اتخاذ شود.

راهنمای پیاده سازی

توصیه می‌شود رهنمودهای زیر برای مدیریت رسانه های قابل انتقال در نظر گرفته شود:

الف - توصیه می‌شود محتوای هر یک از رسانه‌های چندبار مصرف که مورد نیاز نیستند و باید از سازمان دور ریخته شوند. توصیه می‌شود به نحوی از روی رسانه پاک شوند که دیگرقابل بازیابی نباشند
ب - هر زمان که لازم و امکان پذیر باشد، توصیه می‌شود دور ریختن رسانه‌ها و محیط‌های ذخیره اطلاعات با اخذ مجوز انجام پذیرد و یک نسخه از آن مجوز در سوابق و مستندات حفظ شود.
پ - توصیه می‌شود تمام رسانه‌ها و محیط‌های ذخیره اطلاعات در یک محیط امن و ایمن مطابق با مشخصات تولید کننده نگهداری شوند.

ت - توصیه می‌شود اطلاعات ذخیره شده در رسانه‌ها که باید بیش از طول عمر رسانه در دسترس باقی بمانند (مطابق با مشخصات سازندگان) توصیه می‌شود در جای دیگری نیز نگهداری شوند تا از آسیب به اطلاعات به دلیل خرابی رسانه جلوگیری شود

ث - توصیه می‌شود تعداد و مشخصات محیط‌های ذخیره اطلاعات که قابل انتقال هستند در محلی ثبت شود تا احتمال از دست رفتن اطلاعات به دلیل انتقال آنها به محل دیگر کاهش یابد.

ج - توصیه می‌شود درایوهای مربوط به محیط‌های ذخیره اطلاعات قابل انتقال فقط زمانی فعال باشند که دلیل خاصی در کسب وکار برای آن وجود داشته باشد.

توصیه می‌شود تمام رویه ها و سطوح ارابه مجوز به طور شفاف مستند شود.

اطلاعات دیگر

رسانه‌های قابل انتقال شامل نوارها، دیسک‌ها، حافظه‌های کوچک، دیسک‌های سخت قابل انتقال، سی دی‌ها، دی وی دی‌ها و رسانه‌های چاپی هستند.

۱۰-۷-۲ امحای محیطهای ذخیره‌سازی

کنترل

محیط‌های ذخیره‌سازی که دیگر مورد نیاز نیستند، توصیه می‌شود با بکارگیری روش‌های اجرایی رسمی، به صورت امن و محافظت شده، امحا شوند.

راهنمای پیاده سازی

توصیه می‌شود با بکارگیری رویه‌های رسمی برای دور ریختن امن رسانه‌ها، خطر نشت اطلاعات حساس به افراد غیرمجاز را کاهش دهید. رویه‌های مورد استفاده برای دور ریز امن رسانه‌هایی که حاوی اطلاعات حساس هستند، توصیه می‌شود باید با میزان حساسیت این اطلاعات همخوانی داشته باشد. توصیه می‌شود موارد زیر در نظر گرفته شود:

الف - توصیه می‌شود رسانه‌هایی که حاوی اطلاعات حساس هستند، به گونه ای امن و ایمن نگهداری و یا دور ریخته شوند؛ برای مثال بوسیله سوزاندن یا تکه تکه کردن، یا پاک کردن کامل داده‌ها برای استفاده در کاربرد دیگری در داخل سازمان

ب - توصیه می‌شود رویه‌هایی برای شناسایی مواردی که ممکن است به دورریز امن نیاز داشته باشند در نظر گرفته شود.

پ - ممکن است جمع آوری و امحاء امن و مطمئن و دسته جمعی تمام رسانه‌هایی که باید دور ریخته شوند راحت تر از جدا سازی رسانه‌های حاوی اطلاعات حساس و امحاء جداگانه آنها باشد.

ت - بسیاری از سازمان‌ها خدمات جمع آوری و دور ریز رسانه‌های کاغذی خود را به پیمانکاران خارج از سازمان واگذار می‌کنند؛ توصیه می‌شود در انتخاب پیمانکار مناسب و با تجربه کافی، دقت لازم به عمل آید.

ث - توصیه می‌شود در صورت امکان دورریختن موارد حساس ثبت شود تا سوابق آنها وجود داشته باشد.

در زمان انباشته کردن اطلاعات برای دورریختن، توصیه می‌شود ملاحظات کافی در مورد تاثیر تجمعی آن بعمل آید تا حجم زیاد اطلاعات غیر حساس به اطلاعات حساس تبدیل نشوند.

اطلاعات دیگر

اطلاعات حساس ممکن است بواسطه دور ریختن بی دقت رسانه‌ها افشا شوند (برای کسب اطلاعات درباره دور ریختن تجهیزات، رجوع کنید به ۹-۲-۶)

۱۰-۷-۳ روش‌های اجرایی جابجایی اطلاعات

کنترل

توصیه می‌شود روش‌های اجرایی انتقال و انبارش اطلاعات، برای حفاظت این اطلاعات در برابر افشای غیر مجاز یا استفاده نابجا، تدوین شوند.

راهنمای پیاده سازی

توصیه می‌شود رویه‌هایی برای رفتار، پردازش، ذخیره، و انتقال اطلاعات مطابق با طبقه‌بندی آنها در نظر گرفته شود (رجوع کنید به ۷-۲). توصیه می‌شود موارد زیر مورد توجه قرار گیرد:

الف - برچسب زدن و رفتار با تمام رسانه‌ها بر اساس سطح طبقه‌بندی آنها.

ب – اعمال محدودیت‌های دسترسی برای پیشگیری از دسترسی کارکنان غیرمجاز

پ - نگهداری سوابق رسمی رسید داده‌ها بصورت مجاز

ت - اطمینان از ورود کامل داده‌ها و تکمیل پردازش به طور مناسب و سنجش صحت داده‌های خروجی.

ث - محافظت از داده‌های خاص که منتظر ورود به سطحی سازگارتر با حساسیت خود هستند.

ج - نگهداری از رسانه‌ها مطابق با مشخصات تولید کنندگان

چ - حفظ توزیع داده‌ها در سطح حداقل ممکن

ح - علامت گذاری واضح تمام نسخ رسانه‌ها برای توجه دریافت کننده مجاز

خ - بررسی فهرست‌های توزیع کنندگان و دریافت کنندگان مجاز در فواصل زمانی منظم

اطلاعات دیگر

این رویه‌ها در مورد اطلاعات مستند، سیستم‌های رایانه‌ی، شبکه‌ها، تجهیزات محاسبه متحرک، تجهیزات ارتباطی متحرک، نامه‌ها، ارتباطات صوتی به هر شکل آن، خدمات چند رسانه‌ای، امکانات و خدمات پستی، استفاده از دستگاه‌های نمابر و هر مورد حساس دیگر مانند چک‌های بانکی و فاکتورها به کار می روند.

۱۰-۷-۴ امنیت مستندات سیستم

کنترل

توصیه می‌شود مستندات سیستم در برابر دسترسی غیر مجاز، حفاظت شوند.

راهنمای پیاده سازی

برای ایمن سازی مستندسازی سیستم‌ها توصیه می‌شود موارد زیر مدنظر قرار گیرد:

الف - توصیه می‌شود مستندات سیستم‌ها به صورت مطمئن نگهداری شوند.

ب - توصیه می‌شود فهرستی حداقلی از افراد مجاز دارای دسترسی به مستندات سیستم‌ها توسط مالک آن برنامه کاربردی تهیه شود.

پ - توصیه می‌شود مستندات سیستم‌هایی که در شبکه‌های عمومی نگه داشته می‌شوند یا از طریق یک شبکه عمومی تامین می‌شوند باید به طور مناسب محافظت شوند.

اطلاعات دیگر

مستندات یک سیستم ممکن است شامل دامنه‌ای از اطلاعات حساس مانند شرح کاربردها، فرایندها، رویه‌ها، ساختارهای داده‌ها و فرایندهای مجوز دهی باشد.

۱۰-۸ تبادل اطلاعات

هدف : حفظ امنیت اطلاعات و نرم‌افزارهای قابل تبادل یک سازمان با هر موجودیت بیرونی.
توصیه می‌شود مبادلات اطلاعات و نرم‌افزارها بین سازمان‌ها براساس خط‌مشی رسمی مبادلات باشد، که هم‌راستا با توافق‌نامه‌های مبادله بوده و با قوانین حقوقی تطابق دارد (به بند ۱۵ رجوع کنید)
توصیه می‌شود روش‌های اجرایی و استانداردهایی برای حفاظت از اطلاعات و رسانه فیزیکی حاوی اطلاعات درحال عبور، اعمال شود.

۱۰-۸-۱ *خط‌مشی‌ها و روش‌های اجرایی تبادل اطلاعات*

کنترل

توصیه می‌شود برای حفاظت تبادل اطلاعات از طریق هر نوع محیط ارتباطی، خط‌مشی‌ها و روش‌های‌اجرایی رسمی تبادل اطلاعات تدوین شود.

راهنمای پیاده‌سازی

رویه‌ها و کنترل‌هایی که باید در زمان استفاده از تجهیزات ارتباطات الکترونیکی برای تبادل اطلاعات مورد توجه قرار گیرند عبارتند از:

الف - رویه‌های طراحی شده برای محافظت از اطلاعات در برابر دستبرد، نسخه برداری، تغییر، گمراه کردن و تخریب؛

ب - رویه‌هایی برای کشف و محافظت در برابر کدهای مخرب که ممکن است با استفاده از ارتباطات الکترونیکی منتقل شوند (رجوع کنید به بند ۱۰-۴-۱)؛

پ - رویه‌هایی برای محافظت از اطلاعات الکترونیکی حساس مبادله شده که به شکل فایل ضمیمه هستند.

ت - خط مشی یا دستورالعمل‌هایی که استفاده قابل قبول از تجهیزات ارتباطات الکترونیکی را تعریف می‌کنند (رجوع کنید به بند ۷-۱-۳).

ث – روش‌های اجرایی برای استفاده از ارتباطات بی‌سیم، با در نظر گرفتن ریسک‌های مربوطه

ج – تعیین مسوولیت، کارکنان، پیمانکاران، و هر کاربر دیگر برای این که به سازمان آسیب نرساند، مثلا از طریق بدنام کردن، آزار رسانی، جعل هویت، رد کردن نامه ای زنجیره ای، خرید غیرمجاز، و...؛

چ – استفاده از روش‌های رمزنگاری؛ برای مثال، برای حفاظت از محرمانگی، تمامیت و صحت اطلاعات (رجوع کنید به بند۱۲-۳)

ح - دستورالعمل‌های حفظ و دور ریز برای تمام مکاتبات کسب وکار از جمله پیام‌ها، مطابق با قوانین و مقررات ملی و محلی؛

خ - عدم رها کردن اطلاعات حساس در تجهیزات چاپ، مانند دستگاه تکثیر، چاپگر، و دستگاه‌های نمابر، زیرا این اطلاعات ممکن است توسط افراد غیرمجاز مورد دسترسی قرار گیرد.

د - کنترل‌ها و محدودیت‌های مربوط به هدایت امکانات ارتباطی مانند انتقال خودکار نامه الکترونیکی به نشانی‌های خارجی

ذ - یادآوری به کارکنان درباره رعایت احتیاط لازم. مثلا در حین مکالمات تلفنی اطلاعات حساس را علنی نسازند تا از دستبرد به آن توسط موارد زیر اجتناب شود:

۱ - افرادی که در نزدیکی آنها هستند به خصوص در زمان استفاده از تلفن همراه

۲ - استراق سمع و شکل‌های دیگر شنود از طریق دسترسی فیزیکی به گوشی تلفن یا خط تلفن با استفاده از تجهیزات شنود خط

۳ - افرادی که در طرف دیگر خط هستند

ر - عدم ارسال پیام‌هایی که حاوی اطلاعات حساس هستند به دستگاه‌های پاسخگو، زیرا این اطلاعات ممکن است توسط اشخاص غیرمجاز مورد دسترسی قرار گیرند و یا در سیستم‌های اشتراکی ذخیره شوند یا در اثر شماره گیری اشتباه در جای دیگری ذخیره شوند؛

ز - یادآوری به کارکنان درباره مشکلات استفاده از دستگاه‌های نمابر مخصوصا موارد ذیل :

۱ - دسترسی غیرمجاز به پیام‌های ذخیره شده و بازیابی پیام‌ها

۲ - برنامه ریزی عمدی یا تصادفی ماشین‌ها برای ارسال پیام‌ها به شماره‌های خاص

۳ - ارسال اسناد و پیام‌ها به شماره اشتباه از طریق شماره گیری اشتباه یا شماره ای که به اشتباه ذخیره شده است.

ژ - یادآوری به کارکنان درباره عدم ذخیره داده‌های مربوط به مشخصات افراد نظیر نشانی پست الکترونیکی یا دیگر اطلاعات کارکنان در هر نرم‌افزار برای اجتناب از دسترسی سایر افراد و استفاده غیرمجاز

س - یادآوری به کارکنان درباره این که ماشین‌های نمابر و تکثیر مدرن در صورت خطای کاغذی یا خطا در انتقال قابلیت ذخیره اطلاعات دارند و به محض رفع مشکل اطلاعات قابل چاپ می باشد.

ه علاوه، توصیه می‌شود به کارکنان یادآوری شود که مکالمات محرمانه خود را در مکان‌های عمومی یا اماکنی که بدون دیوار و باز هستند و در مکان‌هایی که دیوارها دارای عایق صوتی نمی‌باشند انجام ندهند.

توصیه می‌شود تجهیزات تبادل اطلاعات، الزامات قانونی مربوطه را رعایت نمایند (رجوع کنید به بند ۱۵).

اطلاعات دیگر

تبادل اطلاعات ممکن است با استفاده از تعدادی از انواع مختلف تجهیزات تبادل اطلاعات از جمله پست الکترونیکی، خدمات صوتی، نمابر و ویدیو انجام شود.

تبادل نرم‌افزارها ممکن است از طریق تعدادی از رسانه‌های مختلف از جمله دریافت از اینترنت و خرید از فروشندگانی که این محصولات را می فروشند انجام شود.

توصیه می‌شود روال‌های قانونی و امنیتی تبادل اطلاعات الکترونیکی، تجارت الکترونیکی، و ارتباطات الکترونیکی مربوط به کسب وکار و الزامات لازم برای اعمال کنترل‌ها، تهیه و اجرا شوند.

اطلاعات ممکن است به دلیل فقدان آگاهی، خط‌مشی و روش‌های اجرایی مربوط به استفاده از تجهیزات تبادل اطلاعات مثلا شنیده شدن مکالمه با تلفن همراه در اماکن عمومی، اشتباه در ارسال نامه‌های الکترونیکی یا ارسال تصادفی نمابر به تجهیزات مقصد اشتباه، مورد دسترسی غیر مجاز قرار گیرد.
در صورت خرابی تجهیزات ارتباطی یا اعمال بار اضافه به آنها و یا وقفه در عملکرد آنها عملیات کسب وکار ممکن است مختل شده و امنیت اطلاعات به مخاطره بیفتد.(رجوع کنید به ۱۰-۳ و بند ۱۴). اطلاعات می‌توانند به‌خطر یافتند در صورتی که بوسیله کاربران غیرمجاز مورد دسترسی قرار گیرند (رجوع کنید به بند ۱۱).

۱۰-۸-۲ *توافق‌نامه‌های تبادل*

کنترل

برای تبادل اطلاعات و نرم‌افزار بین سازمان‌ها و مخاطبان بیرونی آنها، توصیه می‌شود توافق‌نامه‌هایی تهیه شود.

راهنمای پیاده‌سازی

توصیه می‌شود در قراردادهای تبادل ملاحظات امنیتی زیر لحاظ شوند:

الف - مسیولیت‌های مدیریت در زمینه کنترل و اعلام انتقال، ارسال و دریافت

ب - رویه‌هایی برای مطلع ساختن فرستنده از انتقال،ارسال و دریافت

پ - رویه‌هایی برای تضمین قابلیت پیگیری و عدم انکار

ت - حداقل استانداردهای فنی برای بسته بندی و انتقال

ث - قراردادهای وجه الضمان

ج - استانداردهای شناسایی پیک

چ - مسوولیت‌ها و تعهدات در صورت بروز حوادث امنیت اطلاعات نظیر آسیب به داده‌ها

ح - استفاده از یک سیستم برچسب زنی مورد توافق برای اطلاعات حساس یا حیاتی، و اطمینان از این که معنای برچسب بلافاصله فهمیده می‌شود و این که اطلاعات به طور مناسب مورد پشتیبانی قرار می‌گیرد.

خ - مالکیت و مسوولیت‌هایی برای محافظت از داده‌ها، حق تکثیر، رعایت پروانه‌های نرم‌افزاری و ملاحظات مشابه (رجوع کنید به بند ۱۵-۱-۲ و ۱۵-۱-۴)

د - استانداردهای فنی برای ثبت و خواندن اطلاعات و نرم‌افزارها

ذ - هر کنترل خاصی که ممکن است برای محافظت از موارد حساس نظیرکلیدهای رمزگشایی لازم باشد. (رجوع کنید به بند ۱۲-۳)

توصیه می‌شود خط مشی‌ها، رویه‌ها و استانداردهایی برای محافظت از اطلاعات و رسانه‌های فیزیکی در انتقال، ایجاد و اعمال شود (همچنین رجوع کنید به بند ۱۰-۸-۳) و توصیه می‌شود در قراردادهای تبادل به آنها اشاره شود. توصیه می‌شود محتوای امنیتی هر قرارداد نشان دهنده حساسیت اطلاعات کسب وکار مربوطه باشد.

اطلاعات دیگر

قراردادها می‌توانند الکترونیکی یا دستی و به شکل قراردادها یا مفاد استخدام رسمی باشند. توصیه می‌شود برای اطلاعات حساس مکانیسم‌های خاص به‌کار رفته برای تبادل برای تمام سازمان‌ها و انواع قراردادها یکسان باشد.

۱۰-۸-۳ محیط‌های ذخیره‌سازی (رسانه) فیزیکی، حین حمل‌ونقل

کنترل

توصیه می‌شود محیط‌های ذخیره‌سازی حاوی اطلاعات در هنگام حمل‌ونقل خارج از مرزهای فیزیکی سازمان، در برابر دسترسی غیر مجاز، استفاده نابجا یا صدمه، محافظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود دستورالعمل‌های زیر برای محافظت از رسانه‌هایی که بین سایت‌های مختلف انتقال داده می‌شوند رعایت شود:

الف - توصیه می‌شود از حمل یا پیک قابل اطمینان استفاده شود

ب - توصیه می‌شود فهرستی از پیک‌های مجاز با توافق مدیریت تهیه شود.

پ – توصیه می‌شود روش‌های اجرایی برای بررسیِ هویت پیک‌ها تدوین شود.

ت - توصیه می‌شود از بسته بندی مناسب برای محافظت از محتویات بسته‌ها دربرابر هر گونه آسیب فیزیکی احتمالی در طول حمل و مطابق با تمام مشخصات تولید کننده استفاده شود، مثلا محافظت در برابر هر فاکتور محیطی که ممکن است به محتوی رسانه‌ها خسارت وارد نماید نظیر قرار گرفتن در معرض گرما، رطوبت یا میدان‌های الکترومغناطیسی.

ث - توصیه می‌شود کنترل‌هایی در صورت امکان به کار گرفته شوند تا از اطلاعات حساس دربرابر افشا غیرمجاز یا تغییرات محافظت کنند، مثلا:

۱ - استفاده از جعبه‌های قفل‌شده

۲ - تحویل دستی

۳ - بسته بندی غیرقابل دستکاری، که هر گونه اقدامی برای دسترسی را نشان می‌دهد.

۴ - در موارد خاص، تقسیم محموله به بیش از یک محموله و ارسال از مسیرهای مختلف

اطلاعات دیگر

اطلاعات ممکن است دربرابر دسترسی غیر مجاز، سوء استفاده، یا اختلال در طول حمل فیزیکی مثلا در زمان ارسال رسانه‌ها از طریق خدمات پست یا یک پیک آسیب‌پذیر باشد.

۱۰-۸-۴ پیام‌رسانی الکترونیکی

کنترل

توصیه می‌شود اطلاعات مورد بحث در پیام‌رسانی الکترونیکی به صورت مناسبی حفاظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود ملاحظات امنیتی برای پیام‌های الکترونیکی شامل موارد زیر رعایت شود:

الف - محافظت از پیام‌ها در برابر دسترسی غیرمجاز، تغییرات، یا جلوگیری از ارایه خدمات

ب - اطمینان از آدرس‌دهی و حمل صحیح پیام،

پ - قابلیت اطمینان عمومی و دسترسی به خدمات

ت - ملاحظات حقوقی مثلا الزاماتی برای امضاهای الکترونیکی

ث - کسب مجوز قبل از استفاده از خدمات همگانی نظیر پیام سریع یا اشتراک شبکه‌ها

ج - سطوح قوی‌تر تعیین هویت جهت دسترسی به شبکه‌های عمومی

اطلاعات دیگر

انتقال پیام الکترونیکی نظیر پست الکترونیکی، تبادل اطلاعات الکترونیکی. پیام رسانی الکترونیکی نقش مهمی در تبادلات تجاری امروز دارند که البته ریسک‌های آن در مقایسه با ارتباطات کاغذی متفاوت است.

۱۰-۸-۵ سیستم‌های اطلاعاتی کسب‌وکار

کنترل

توصیه می‌شود به منظور حفاظت اطلاعات مربوط به ارتباطات داخلی سیستم‌های اطلاعاتی کسب‌وکار، خط‌مشی‌ها و روش‌های اجرایی مربوطه ایجاد و پیاده‌سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود ملاحظات مربوط به آثار امنیتی و کسب وکار ارتباط این تجهیزات شامل موارد زیر باشد:

الف - آسیب‌پذیری‌های شناخته شده در سیستم‌های اجرایی و حسابداری در جایی که اطلاعات بین بخش‌های مختلف سازمان متفاوت است؛

ب - آسیب‌پذیری‌های اطلاعات در سیستم‌های ارتباطات کسب وکار مثلا درباره تماس‌های تلفنی یا کنفرانس مکالمات، محرمانگی تماس‌ها، ذخیره نمابرها، بازکردن و توزیع نامه‌ها

پ - خط مشی و کنترل‌های مناسب برای مدیریت اشتراک اطلاعات

ت - خارج ساختن طبقاتی از اطلاعات حساس کسب وکار و اسناد طبقه بندی شده در صورتی که سیستم سطح مناسبی از محافظت را ارایه نمی‌کند. (رجوع کنید به بند ۷-۲)

ث – محدود کردن دسترسی به گزارشات روزانه افراد خاص؛ برای مثال، کارکنانی که در پروژه‌های حساس کار می‌کنند.

ج – رده‌بندی کارکنان، پیمانکاران یا شرکای کسب وکار مجاز به استفاده از سیستم و محل‌هایی که ممکن است سیستم از آنجا مورد دسترسی قرار گیرد (رجوع کنید به بند ۶-۲ و بند ۶-۳)؛

ج - محدود کردن دسترسی به اطلاعات دفتر یادداشت افراد خاص مانند کارکنانی که در پروژه‌های حساس کار می‌کنند؛

چ - شناسایی وضعیت کاربران مانند کارکنان سازمان یا پیمانکاران در دفاتر یادداشت برای استفاده کاربران دیگر

ح - حفظ و کپی‌پشتیبانی گرفتن از اطلاعاتی که در سیستم‌ها نگهداری می‌شود (رجوع کنید به بند ۱۰-۵-۱)

خ - الزامات و تنظیمات انجام مجدد (رجوع کنید به بند ۱۴)

اطلاعات دیگر

سیستم‌های اطلاعات اداری فرصت‌هایی هستند برای انتشار و اشتراک سریع تر اطلاعات کسب وکار با استفاده از ترکیبی از اسناد، رایانه‌ها، محاسبه گرهای سیار، ارتباطات سیار، پست، پیام صوتی، ارتباطات صوتی در هر شکل آن خدمات و امکانات پستی، ماشین‌های نمابر.

۱۰-۹ خدمات تجارت الکترونیک

هدف: حصول اطمینان از امن ت خدمات تجارت الکترونیکی و استفاده ایمن از آنها.
توصیه می‌شود تاثیرات امنیتی در رابطه با استفاده از خدمات تجارت الکترونیکی، از جمله تعاملات برخط، و الزامات کنترلی مربوطه، در نظر گرفته شود. همچنین توصیه می‌شود یکپارچگی و در دسترس بودن به اطلاعاتی که به صورت الکترونیکی از طریق سیستم‌های عمومی منتشر می‌شوند، در نظر گرفته شود.

۱۰-۹-۱ *تجارت الکترونیک*

کنترل

اطلاعات مورد استفاده در تجارت الکترونیکی که از شبکه‌های عمومی عبور می‌کنند، توصیه می‌شود در برابر اقدامات کلاه برداری، مناقشات در قرارداد، و افشا و دستکاری غیر مجاز، محافظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود ملاحظات امنیتی برای تجارت الکترونیکی شامل موارد زیر باشد:

الف - سطح اطمینان مورد نیاز هر یک از طرفین نسبت به هویت مورد ادعای طرف دیگر مثلا از طریق مجوز دهی.

ب - فرایند مجوز دهی در رابطه با هر کسی که ممکن است قیمت‌ها را تعیین کند و اسناد مهم کسب وکار را صادر یا امضا کند؛

پ - حصول اطمینان از این که شرکای کسب وکار کاملا از اختیارات خود مطلع هستند؛

ت - تعیین و رعایت الزامات محرمانگی، یکپارچگی، اثبات ارسال و دریافت اسناد کلیدی، و عدم دستکاری قراردادها مثلا در رابطه با فرایندهای مناقصه یا قرارداد

ث - سطح اطمینانی که در یکپارچگی لیست قیمت‌های اعلام شده لازم است

ج - محرمانگی هر یک از داده‌ها یا اطلاعات حساس

چ - محرمانگی و یکپارچگی هر یک از تعاملات، اطلاعات پرداخت، جزییات نشانی تحویل، و تایید رسیدها

ح - تعیین سطح مناسب کنترل اطلاعات پرداخت که توسط مشتری ارایه شده است.

خ - انتخاب مناسب ترین نحوه پرداخت برای محافظت در برابر تقلب و کلاه‌برداری

د - سطح محافظت مورد نیاز برای حفظ محرمانگی و یکپارچگی اطلاعات سفارش

ر - اجتناب از خرابی یا تکرار در اطلاعات تعاملات

ز - مسوولیت در قبال انجام تعاملات جعلی

ج - الزامات بیمه

بسیاری از ملاحظات فوق را می‌توان با استفاده از کنترل‌های رمزگشایی(رجوع کنید به بند ۱۲-۳) با احتساب رعایت الزامات قانونی مورد رسیدگی قرار داد (رجوع کنید به بند ۱۵-۱، مخصوصا بند ۱۵-۱-۶ برای وضع قوانین رمزنگاری). توصیه می‌شود توافقات تجارت الکترونیکی بین شرکای کسب وکار، توسط یک قرارداد مستند که هر دو طرف را به رعایت مفاد مورد توافق تجارت، از جمله جزییات اختیارات ملزم کند پشتیبانی شود (رجوع کنید به مورد ب در بالا). قراردادهای دیگری هم با ارایه دهندگان خدمات اطلاعاتی و خدمات ارزش افزوده شبکه ممکن است ضروری باشد.

توصیه می‌شود سیستم‌های تجارت همگانی، مفاد تجارت خود را به اطلاع مشتریان برسانند.
توصیه می‌شود ملاحظات لازم برای ایجاد انعطاف پذیری در سیستم در برابر حمله به سایت میزبان مورد استفاده برای تجارت الکترونیکی و الزامات امنیتی هر یک از ارتباطات متقابل شبکه که برای اجرای خدمات تجارت الکترونیکی لازم است مورد توجه قرار گیرد. (رجوع کنید به بند ۱۱-۴-۶)

اطلاعات دیگر

تجارت الکترونیکی در مقابل تعدادی از تهدیدهای شبکه ای که ممکن است منجر به کلاهبرداری، اختلاف در قرارداد، و افشا یا تغییر اطلاعات شوند آسیب‌پذیر است.
تجارت الکترونیکی، می‌تواند از روش‌های امن احراز اصالت استفاده کند. برای مثال می‌تواند از رمز نگاری کلید همگانی و امضاهای دیجیتال(رجوع کنید به بند ۱۲-۳) برای کاهش ریسک استفاده کند. همچنین از اشخاص ثالث امین می‌توان در زمانی که به این خدمات نیاز است استفاده کرد.

۱۰-۹-۲ *تراکنش های برخط*

کنترل

توصیه می‌شود اطلاعات مورد استفاده در داد و ستدهای برخط، به منظور پیشگیری از انتقال ناقص، مسیریابی اشتباه، تغییر یافتن غیر مجاز پیغام، افشای غیر مجاز، بازگرداندن یا تکرار غیر مجاز پیغام، حفاظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود ملاحظات امنیتی برای تعاملات برخط، شامل موارد زیر باشد:

الف - استفاده از امضاهای الکترونیکی توسط هر یک از طرفین دخیل در معامله

ب – رعایت تمام جنبه‌های معامله برای اطمینان حصول اطمینان از اینکه:

۱ - مدارک طرفین معتبر و تایید شده است

۲ - معامله محرمانه باقی می ماند؛ و

۳ - محرمانگی اطلاعات مربوط به تمام طرفین حفظ می‌شود

پ - مسیر ارتباطی بین تمام طرفین رمز می‌شود.

ت - پروتکل‌های به‌کار رفته برای ارتباط بین تمام طرفین ایمن است؛

ث - اطمینان از قرارگیری جزییات معامله در مکانی خارج از دسترسی عموم مثلا در یک سکوی ذخیره سازی که در اینترانت سازمان قرار دارد، و نه بر روی رسانه‌هایی که مستقیما در دسترس همگان است.

ج - در جایی که از یک مرجع مورد اطمینان استفاده می‌شود (مثلا، برای صدور و حفظ امضاهای دیجیتال و/یا گواهینامه‌های دیجیتال)، امنیت در سراسر فرایند مدیریت انتهابه‌انتهای امضا/گواهینامه، اعمال شود.

اطلاعات دیگر

میزان کنترل‌های به‌کار رفته باید با سطح ریسک‌های مربوط به هر معامله برخط تناسب داشته باشد.
تراکنش‌ها باید با قوانین، احکام و مقررات قضایی جایی که در آن ایجاد یا پردازش و یا نگهداری می‌شوند مطابقت داشته باشند.
بسیاری از شکل‌های معاملاتی وجود دارند که ممکن است به گونه ای برخط اجرا شوند مثلا قراردادی، مالی و غیره.

۱۰-۹-۳ اطلاعات قابل دسترس عموم

کنترل

توصیه می‌شود یکپارچگی اطلاعاتی که در یک سیستم در قابل دسترس عموم قرار می‌گیرد، به منظور پیشگیری از دستکاری غیر مجاز، باید محافظت شود.

راهنمای پیاده‌سازی

توصیه می‌شود نرم‌افزارها، داده‌ها، و اطلاعات دیگری که نیازمند سطح بالایی از یکپارچگی هستند و در یک سیستم قابل دسترس عموم قرار دارند توسط مکانیسم‌های مناسب مثلا امضاهای دیجیتال محافظت شوند (رجوع کنید به بند ۱۲-۳). برای سیستمی که در دسترس همگان قرار می گیرد، توصیه می‌شود قبل از ارایه دسترسی باید ضعف‌ها و مشکلات کاملا بررسی شود.

توصیه می‌شود یک فرایند تایید رسمی قبل از این که اطلاعات در معرض دید همگان قرار گیرد وجود داشته باشد. بعلاوه، توصیه می‌شود، همه ورودی‌های تامین شده از خارج از سیستم تصدیق و تایید شوند.

توصیه می‌شود سیستم‌های انتشار الکترونیکی به خصوص سیستم‌هایی که انعکاس و ورود مستقیم اطلاعات را امکان پذیر می‌کنند به دقت کنترل شوند به گونه ای که:

الف - اطلاعات مطابق با مقررات محافظت از داده‌ها به دست آید (رجوع کنید به بند ۱۵-۱-۴)؛

ب - اطلاعات ورودی به سیستم انتشار و اطلاعاتی که توسط آن پردازش می‌شود به طور کامل و دقیق و به موقع پردازش شوند؛

پ - اطلاعات حساس در طول زمان جمع آوری، پردازش، و ذخیره سازی محافظت شوند.

ت – ساختار دسترسی به سیستم انتشار، اجازه دسترسی غیر عمدی به شبکه‌هایی که سیستم به آنها متصل است را نمی‌دهد.

اطلاعات دیگر

اطلاعات روی یک سیستم قابل دسترس عموم مانند اطلاعات سرور شبکه که از طریق اینترنت قابل دسترسی است، ممکن است نیازمند رعایت قانون و مقررات حوزه قضایی محل قرارگیری سرور، یا محل انجام معاملات و یا در جایی که مالک (ها) سکونت دارند باشد. تغییر غیرمجاز اطلاعات منتشر شده ممکن است به خوش‌نامی سازمان منتشر کننده آسیب برساند.

۱۰-۱۰ پایش

هدف: تشخیص فعالیتهای غیر مجاز پردازش اطلاعات.

توصیه می‌شود بر فعالیت سیستم‌ها نظارت شده و توصیه می‌شود اتفاقات امنیت اطلاعات ضبط شود. توصیه می‌شود اطلاعات ثبت وقایع کاربر و ثبت وقایع خرابی برای اطمینان از اینکه مشکلات سیستم اطلاعاتی شناسایی شده‌اند مورد استفاده قرار گیرند.

توصیه می‌شود سازمان تمام الزامات قانونی در رابطه با نظارت و ثبت وقایع را رعایت کند.

توصیه می‌شود یک سیستم نظارت برای بررسی میزان اثربخشی کنترل های بکار رفته و تایید سهولت استفاده از مدل سیاست دسترسی، مورد استفاده قرار گیرد.

۱۰-۱۰-۱ واقعه‌نگاری ممیزی

کنترل

توصیه می‌شود سوابق ممیزی مشتمل بر فعالیت‌های کاربر، استثناها و وقایع امنیت اطلاعات، برای یک بازهٔ زمانی توافق شده، ایجاد و نگهداری شوند تا در رسیدگی‌های آتی و پایش کنترل دسترسی، مورد استفاده قرار گیرند.

راهنمای پیاده‌سازی

توصیه می‌شود گزارش‌های ممیزی شامل موارد زیر باشند:

الف - هویت کاربر

ب - تاریخ، زمان، و جزییات وقایع کلیدی، مانند ورود به/ خروج از سیستم

پ – شناسه یا محل ترمینال در صورت امکان

ت - سوابق مربوط به دسترسی‌های موفق و غیر موفق به سیستم

ث – سوابق مربوط به دسترسی‌های موفق و غیر موفق به داده‌ها و سایر منابع سیستم

ج - تغییرات در پیکربندی سیستم

چ - استفاده از حقوق دسترسی

ح - استفاده از کاربردها و امکانات سیستم

خ - فایل‌های مورد پردازش و نوع دسترسی

د - نشانی‌ها و پروتکل‌های شبکه

ذ - هشدارهای ایجادشده توسط سیستم کنترل دسترسی

ر – فعال‌سازی و غیرفعال‌سازی سیستم‌های مراقبت نظیر سیستم‌های ضد ویروس و سیستم‌های کشف مزاحمت

اطلاعات دیگر

گزارش‌های ممیزی ممکن است حاوی داده‌های شخصی افراد باشد. توصیه می‌شود اقدامات مناسب برای محافظت از محرمانگی این گزارشات به کار گرفته شود (همچنین رجوع کنید به بند ۱۵-۱-۴). توصیه می‌شود در صورت امکان، مجریان سیستم اجازه پاک کردن یا غیرفعال کردن گزارش‌های فعالیت خودشان را نداشته باشند (رجوع کنید به بند ۱۰-۱-۳).

۱۰-۱۰-۲ پایش کاربرد سیستم

توصیه می‌شود روش‌های‌اجرایی برای پایش کاربرد امکانات پردازش اطلاعات، ایجاد شده و نتایج فعالیت‌های پایش، به صورت منظم، بازبینی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود سطح مراقبت مورد نیاز برای تک تک تجهیزات از طریق ارزیابی ریسک تعیین شود. توصیه می‌شود سازمان از تمام الزامات قانونی مربوطه در مورد فعالیت‌های کنترلی اش پیروی کند. توصیه می‌شود موضوعاتی که باید مورد توجه قرار گیرند عبارتند از:

الف - دسترسی مجاز، از جمله جزییاتی نظیر

۱ - هویت کاربر

۲ - تاریخ و زمان وقایع کلیدی

۳ - نوع وقایع

۴ - فایل‌های مورد دسترسی

۵ – برنامه/امکانات استفاده شده

ب - تمام فعالیت‌های ویژه شامل :

۱ - استفاده از شناسه‌های کاربری ویژه مانند ناظر[1]، ریشه[2]، راهبر

۲ - راه اندازی و توقف سیستم

۳ - اتصال/جداکردن دستگاه I/O

پ - اقدامات دسترسی غیرمجاز نظیر:

۱ - فعالیت‌های مشکل دار یا رد شده

۲ - فعالیت‌های مشکل دار یا ردشده ای که از داده‌ها و سایر منابع استفاده می‌کنند.

۳ - تخلف از خط مشی دسترسی و هشدارهای مربوط به دروازه شبکه و دیوار آتش

۴ – هشدار از سیستم‌های کشف مزاحمت

ت - هشدارها یا خرابی‌های سیستم‌نظیر:

۱ - هشدارها یا پیام‌های کنسول

۲ - گزارش استثناها سیستم

۳ - هشدارهای مدیریت شبکه

۴ – هشدارهای ارایه شده توسط سیستم کنترل دسترسی

ث - تغییرات یا اقدام برای تغییر تنظیم سیستم امنیت و کنترل‌های آن

فواصل زمانی بررسی فعالیت‌های سیستم نظارتی باید منطبق با ریسک مرتبط با آن باشد. توصیه می‌شود عوامل ریسک در نظر گرفته شده شامل این موارد باشند:

الف - میزان حساسیت فرایندهای کاربردها

ب - ارزش، حساسیت، و حیاتی بودن اطلاعات به‌کار رفته؛

پ - تجربه گذشته نفوذ و سوء استفاده و فراوانی آسیب‌پذیری‌هایی که کشف می‌شوند؛

ت - میزان ارتباطات داخلی سیستم (بخصوص شبکه‌های عمومی)

ث - امکانات ثبت وقایع غیر فعال شده.

اطلاعات دیگر

استفاده از سیستم‌های نظارتی برای حصول اطمینان از اینکه کاربران فقط کارهایی را انجام می دهند که باید انجام دهند الزامی است.

بررسی سوابق نظارتی باعث درک تهدیدهای پیش روی سیستم و نحوه ایجاد آنها است. مثال‌های مربوط به وقایعی که ممکن است نیازمند بررسی بیشتر در صورت وقوع حوادث امنیت اطلاعات باشند در ۱۳-۱-۱ آمده است.

1- Supervisor
2- Root

۱۰-۱۰-۳ حفاظت از اطلاعات ثبت شدهٔ وقایع

کنترل

توصیه می‌شود امکانات واقعه‌نگاری و اطلاعات ثبت وقایع، در برابر دسترسی پنهانی و غیر مجاز، حفاظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود هدف کنترل‌ها، محافظت از تغییرات غیرمجاز و مشکلات عملیاتی در تجهیزات ثبت وقایع باشد که شامل موارد زیر است:

الف - تغییرات در انواع پیام‌هایی که ثبت می‌شوند؛

ب - فایل‌های ثبت شده ای که ویرایش یا حذف می‌شوند

پ – محدودیت در ظرفیت رسانه‌های ثبت وقایع، که منجر به ناکامی در ثبت وقایع یا دوباره کاری وقایع ثبت شده در گذشته می‌شود.

بعضی از گزارش‌های ممیزی ممکن است به عنوان بخشی از خط‌مشی نگهداری گزارش وقایع یا به دلیل الزامات خاص، جمع آوری و بایگانی شوند. (همچنین رجوع کنید به بند ۱۳-۲-۳)

اطلاعات دیگر

گزارش‌های سیستم حاوی حجم وسیعی از اطلاعات است که بسیاری از آن برای کنترل امنیت، استفاده ای نداشته باشد. توصیه می‌شود برای کمک به شناسایی وقایع مهم کنترل امنیت، پیام‌های مربوط بصورت اتوماتیک به یک گزارش دیگر کپی شوند و/یا از ابزارهای ممیزی مناسب که فایل را بررسی و وقایع مهم را جدا می‌کنند استفاده شود. گزارشات ثبت وقایع سیستم باید محافظت شود زیرا اگر داده‌ها را بتوان تغییر داده و یا حذف نمود، وجود آنها ممکن است احساس نادرستی از امنیت ایجاد کند.

۱۰-۱۰-۴ اطلاعات ثبت‌شده وقایع مربوط‌به راهبر و اپراتور سیستم

کنترل

توصیه می‌شود وقایع فعالیت‌های راهبر و اپراتور سیستم ثبت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود گزارش‌ها شامل موارد زیر باشد:

الف - زمان وقوع حادثه

ب - اطلاعات مربوط به واقعه (فایل‌های مورد استفاده قرار گرفته) یا ناکامی (خطای اتفاق افتاده و اقدامات اصلاحی)

پ - کدام شناسه‌های کاربری، راهبر و اپراتور شرکت داشته اند.

ت - کدام فرایندها نقش داشتند

توصیه می‌شود گزارش‌های راهبر و اپراتور سیستم به صورت منظم بررسی شوند.

اطلاعات دیگر

یک سیستم کشف مزاحمت که خارج از کنترل راهبران سیستم و شبکه مدیریت می‌شود، را می‌توان برای کنترل فعالیت‌های راهبر شبکه و سیستم مورد استفاده قرار داد.

۱۰-۱۰-۵ واقعه‌نگاری خرابی

کنترل

توصیه می‌شود وقایع خرابی‌ها ثبت و تحلیل شده و اقدام مناسبی در رفع آنها انجام شود.

راهنمای پیاده‌سازی

توصیه می‌شود خطاهای گزارش شده توسط کاربران یا توسط برنامه‌های سیستم در رابطه با مشکلات پردازش اطلاعات یا سیستم‌های ارتباطات، ثبت شوند. توصیه می‌شود قوانین روشنی برای رسیدگی به خطاها وجود داشته باشد از جمله:

الف - بررسی گزارش‌های خطا برای تضمین این که خطاها به صورت رضایت بخش حل شده اند

ب - بررسی اقدامات اصلاحی برای تضمین این که کنترل‌ها نادرست نبوده اند و اینکه اقدام انجام شده کاملا مجاز است

اگر این امکان در سیستم وجود دارد باید از فعال بودن سیستم ثبت خطاها اطمینان حاصل نمود.

اطلاعات دیگر

ثبت خطاها و اشکالات ممکن است بر عملکرد یک سیستم تاثیر بگذارد. توصیه می‌شود این ثبت توسط کارکنان ذی‌صلاح انجام شود و سطح ثبت مورد نیاز برای تک تک سیستم‌ها توصیه می‌شود توسط یک ارزیابی ریسک با احتساب کاهش سطح عملکرد تعیین شود.

۱۰-۱۰-۶ همزمان‌سازی ساعت‌ها

کنترل

توصیه می‌شود ساعت‌های تمامی سیستم‌های پردازش اطلاعات مرتبط در درون یک سازمان یا دامنهٔ امنیتی، توصیه می‌شود با یک منبع زمانی دقیق توافق شده، همزمان شوند.

راهنمای پیاده‌سازی

در جایی که یک رایانه یا دستگاه ارتباطی قابلیت راه اندازی یک ساعت زمان واقعی را داشته باشد، توصیه می‌شود این ساعت، مطابق با یک استاندارد مورد توافق مثلا زمان جهانی هماهنگ[1]. یا زمان استاندارد محلی تنظیم شود، همانطور که بعضی از ساعت‌ها با زمان تغییر می‌کنند توصیه می‌شود رویه‌ای باشد که هر گونه تغییرمهم را اصلاح کند.

تفسیر صحیح فورمت تاریخ زمان، برای تضمین این که ثبت کننده زمان نشان دهنده زمان واقعی است، مهم است. توصیه می‌شود تغییرات ساعت تا ستانی مد نظر قرار گیرد.

اطلاعات دیگر

تنظیم صحیح ساعت‌رایانه‌ها برای تضمین دقت گزارش‌های ممیزی مهم است و نشان دهنده دقت گزارش است و ممکن است لازم باشد در تحقیقات و یا دادگاه به آن استناد شود.

گزارش‌های ممیزی غیردقیق، ممکن است مانع از این بررسی‌ها شود و به اعتبار این شواهد خدشه وارد کند. ساعتی که با ساعت یک فرستنده رادیویی مرتبط به ساعت اتمی ملی همزمان است، می‌تواند به عنوان یک ساعت اصلی برای سیستم‌های ثبت کننده مورد استفاده قرار گیرد. یک پروتکل زمان شبکه را می‌توان برای حفظ تمام سرورها به صورت همزمان با ساعت اصلی مورد استفاده قرار داد.

1- Coordinated Universal Time (UTC)

۱۱ کنترل دسترسی

۱-۱۱ الزامات کسب‌وکار برای کنترل دسترسی

هدف: کنترل دسترسی به اطلاعات. توصیه می‌شود دسترسی به اطلاعات، امکانات پردازش اطلاعات و پردازش‌های تجاری براساس الزامات امنیتی و تجاری کنترل شود. توصیه می‌شود در قوانین کنترل دسترسی خط مشی های مربوط به انتشار و تایید اطلاعات لحاظ شوند.

۱-۱-۱۱ خط‌مشی کنترل دسترسی

کنترل

توصیه می‌شود یک خط‌مشی کنترل دسترسی بر مبنای الزامات کسب‌وکار و الزامات امنیتی در خصوص دسترسی، ایجاد، مدون و بازنگری شود.

راهنمای پیاده‌سازی

توصیه می‌شود قوانین و مقررات کنترل دسترسی برای هر کاربر یا گروه کاربران، به روشنی در یک خط‌مشی کنترل دسترسی بیان شود. کنترل‌های دسترسی هم منطقی و هم فیزیکی هستند(همچنین رجوع کنید به بخش ۹) و توصیه می‌شود اینها با هم در نظر گرفته شوند. توصیه می‌شود کاربران و ارایه کنندگان خدمات یانیه روشنی از الزامات کسب و کار توسط کنترل‌های دسترسی رعایت شوند دریافت کنند.

توصیه می‌شود در خط مشی موارد زیر لحاظ شود:

الف - الزامات امنیتی هر یک از برنامه های کاربردی تجاری

ب - شناسایی تمام اطلاعات مربوط به برنامه های کاربردی تجاری و ریسک‌هایی که اطلاعات با آنها مواجه خواهند بود.

پ - خط‌مشی هایی برای انتشار و تایید اطلاعات مانند قاعده نیاز به دانستن، و سطوح امنیتی و طبقه بندی اطلاعات (رجوع کنید به بند ۷-۲)

ت - سازگاری بین کنترل دسترسی و خط‌مشی های طبقه بندی اطلاعات سیستم‌ها و شبکه‌های مختلف

ث - قوانین مربوطه و هر یک از الزامات قراردادی درباره محافظت از دسترسی به داده‌ها یا خدمات (رجوع کنید به بند ۱۵-۱)

ج - شرح حال‌های دسترسی کاربر استاندارد برای قوانین شغل متعارف در سازمان

چ - مدیریت حقوق دسترسی در یک محیط توزیع شده و شبکه ای که تمام انواع اتصالات موجود را به رسمیت می شناسد.

ح - تفکیک نقش‌های کنترل دسترسی مانند، تقاضای دسترسی، تایید دسترسی، اجرای دسترسی

خ - الزامات مجوز دهی رسمی تقاضاهای دسترسی (رجوع کنید به بند ۱۱-۲-۱)

د - الزامات بررسی دوره ای کنترل‌های دسترسی (رجوع کنید به بند ۱۱-۲-۴)

ذ - از بین بردن حقوق دسترسی (رجوع کنید به بند ۸-۳-۳)

اطلاعات دیگر

توصیه می‌شود در زمان تعیین قوانین کنترل دسترسی موارد زیر لحاظ گردند:

الف - تمایز قائل شدن بین قوانینی که باید همیشه اجرا شوند و رهنمودهایی که اختیاری یا مشروط هستند؛
ب - تثبیت قوانین بر اساس این فرض "هر چیزی به طور کلی ممنوع است مگر این که صریحا اجازه داده شود" به جای این فرض که "هر چیزی عموما مجاز است مگر این که صریحا ممنوع شود"
پ - تغییرات در برچسب‌های اطلاعات(رجوع کنید به بند ۷-۲) که به طور خودکار توسط تجهیزات پردازش اطلاعات ایجاد می‌شوند و آنهایی که به اختیار کاربر ایجاد می‌شوند؛
ت – تغییراتِ مجوزهای کاربر که بطور خودکار توسط سیستم اطلاعاتی ایجاد می‌شود و آنهایی که بوسیله راهبر سیستم ایجاد می‌شود.
ث - قوانینی که نیازمند تایید ویژه قبل از اعمال می‌باشند و قوانینی که نیازمند تایید ویژه قبل از اعمال نمی‌باشند.

توصیه می‌شود قوانین کنترل دسترسی توسط روش‌های اجرایی رسمی و مسوولیت‌های تعیین شده پشتیبانی شوند. (برای مثال، رجوع کنید به بند ۶-۱-۳، ۱۱-۳، ۱۰-۴-۱، ۱۱-۶)

۱۱-۲ مدیریت دسترسی کاربر

هدف: حصول اطمینان از دسترسی کاربر دارای مجوز و پیشگیری از دسترسی غیر مجاز به سیستم‌های اطلاعاتی.
توصیه می‌شود روش‌های اجرایی رسمی برای کنترل تخصیص حقوق دسترسی به سیستم‌ها و خدمات اطلاعات در نظر گرفته شوند.
توصیه می‌شود روش‌های اجرایی تمام مراحل چرخه دسترسی کاربر را از ثبت اولیه کاربران جدید تا پایان ثبت نهایی کاربرانی که دیگر نیاز به دسترسی به سیستم‌ها و خدمات اطلاعاتی ندارند را پوشش دهند. توصیه می‌شود توجه خاصی در زمان مناسب به نیاز به کنترل تخصیص حقوق دسترسی برتر معطوف شود که به کاربران اجازه می‌دهد کنترل‌های سیستم را طی کنند.

۱۱-۲-۱ ثبت کاربر

کنترل

توصیه می‌شود برای اعطا یا لغو دسترسی به سیستم‌ها و خدمات اطلاعاتی، یک روش‌اجرایی رسمی ثبت و حذف کاربر وجود داشته باشد.

راهنمای پیاده‌سازی

توصیه می‌شود روش‌های اجرایی کنترل دسترسی برای ثبت و حذف کاربران شامل موارد زیر باشد:
الف - استفاده از شناسه های منحصر به فرد کاربر برای ایجاد امکان پذیرش مسوولیت فعالیت‌های کاربران توسط خود آنها؛ توصیه می‌شود استفاده از شناسه های گروهی فقط در صورتی مجاز شود که به دلایل کاری یا عملیاتی لازم باشد و توصیه می‌شود که تایید و مستند شوند.
ب - بررسی این که کاربر از مالک سیستم برای استفاده از سیستم و خدمات اطلاعات مجوز دارد؛ کسب تایید جداگانه از مدیریت برای حقوق دسترسی نیز می‌تواند مناسب باشد.

پ - بررسی این که سطح دسترسی اعطا شده متناسب با اهداف کاری (رجوع کنید به بند ۱۱-۱) و با خط‌مشی امنیت سازمانی سازگار است به عنوان مثال به تفکیک وظایف آسیب نمی‌رساند (رجوع کنید به بند ۱۰-۱-۳).

ت - ارایه یک بیانیه کتبی از حقوق دسترسی کاربران به آنها

ث - تقاضا از کاربران برای امضا بیانیه‌ای که نشان می‌دهد آنها شرایط دسترسی را درک کرده اند؛

ج - حصول اطمینان از این که ارایه کنندگان خدمات دسترسی را تا زمانی که روش‌های اجرایی مربوطه بطور کامل به انجام برسند، ارایه نمی‌کنند.

چ - حفظ مدرکی رسمی از تمام اشخاصی که برای استفاده از خدمات ثبت شده اند.

ح - حذف یا توقیف از حقوق دسترسی کاربرانی که نقش‌ها یا وظایف را تغییر داده اند یا سازمان را ترک کرده‌اند.

خ- بررسی دوره‌ای، و حذف یا مسدود کردن شناسه‌ها یا حساب‌های کاربری زائد (رجوع کنید به بند ۱۱-۲-۴)

د- حصول اطمینان از اینکه شناسه ها و حسابهای کاربری مازاد به دیگر کاربران ارایه نمی‌شود؛

اطلاعات دیگر

توصیه می‌شود به تثبیت نقش‌های دسترسی کاربر بر مبنای الزامات کسب وکار که تعدادی از حقوق دسترسی را به شرح‌های دسترسی کاربر معمولی خلاصه می‌کنند، ملاحظه زیادی شود. تقاضاها و بررسی‌های دسترسی (رجوع کنید به بند ۱۱-۲-۴) در سطح این نقش‌ها ساده تر از سطح حقوق خاص مدیریت می‌شوند.

توصیه می‌شود بعنوان ملاحظات بندهایی در قراردادهای پرسنل و بندهای خدمات گنجانده شود که در صورتی که دسترسی غیرمجاز توسط پرسنل یا عوامل خدمات سعی می‌شود محرومیت‌هایی در نظر گرفته شود. (همچنین رجوع کنید به بند ۶-۱-۵، ۸-۱-۳ و ۸-۲-۳)

۱۱-۲-۲ مدیریت اختیارات ویژه

کنترل

توصیه می‌شود تخصیص و بکارگیری اختیارات ویژه، محدود و کنترل شده باشد.

راهنمای پیاده‌سازی

توصیه می‌شود سیستم‌های چندکاربره، که نیازمند محافظت در برابر دسترسی غیر مجاز، دارای تخصیص مزایا که از طریق یک فرایند رسمی کنترل می‌شود، باشند. توصیه می‌شود مراحل زیر در نظر گرفته شود:

الف - مزایای دسترسی در رابطه با هر یک از محصولات سیستم، مانند سیستم عامل، سیستم مدیریت بانک داده و هر یک از کاربردها و کاربرانی که باید به آنها ختصاص داده شود توصیه می‌شود شناسایی شوند.

ب - توصیه می‌شود مزایایی به هر کاربر بر مبنای نیاز به استفاده و بر مبنای واقعه به واقعه در راستای خط‌مشی کنترل دسترسی؛ به عبارت دیگر حداقل الزامات نقش عملکردی آنها فقط در زمان مورد نیاز اختصاص یابد؛

پ - توصیه می‌شود یک فرایند تایید اعتبار و گزارشی از تمام مزایای اختصاص یافته، نگهداری شود. توصیه می‌شود مزایا تا زمانی که فرایند صدور مجوز به طور کامل به انجام برسد، ارایه نشود؛

ت - توصیه می‌شود توسعه و استفاده از روتین‌های سیستم ارتقا یابد تا از نیاز به اعطای مزایا به کارکنان اجتناب شود؛

ث - توصیه می‌شود توسعه و استفاده از برنامه‌هایی که از نیاز به اجرا با مزایا اجتناب می‌کنند ارتقا یابد؛

ج - توصیه می‌شود مزایایی به کاربران متفاوت در نظر گرفته شود در مقایسه با آنهایی که برای استفاده کسب وکار عادی مورد استفاده قرار گرفتند.

اطلاعات دیگر

استفاده نامناسب از مزایای اجرای سیستم (هر ویژگی یا امکانی از یک سیستم اطلاعاتی که این امکان را به کاربر می‌دهد تا کنترل‌ها را باطل کند) می‌تواند عامل موثری برای خرابی یا رخنه در سیستم‌ها باشد.

۱۱-۲-۳ مدیریت کلمهٔ عبور کاربر

کنترل

توصیه می‌شود تخصیص کلمات عبور، از طریق یک فرایند مدیریت رسمی، کنترل شود.

راهنمای پیاده‌سازی

توصیه می‌شود این فرایند شامل الزامات زیر باشد:

الف - توصیه می‌شود از کاربران خواسته شود بیانیه ای را برای محرمانه نگه داشتن کلمات عبور و حفظ کلمات عبور فقط در میان اعضای گروه امضا کنند؛ این بیانیه امضا شده را می‌توان در مفاد و شرایط استخدام گنجاند (رجوع کنید به بند ۸-۱-۳)

ب - زمانی که از کاربران خواسته می‌شود کلمات عبور خود را حفظ کنند، توصیه می‌شود ابتدا یک شماره رمز موقت و امن (رجوع کنید به بند ۱۱-۳-۱) به آنها داده شود که مجبور شوند بلافاصله کلمه عبور خود را به آن تغییر دهند.

پ - تثبیت روش‌های اجرایی برای تصدیق هویت یک کاربر قبل از ارایه کلمه عبور جدید، جابجایی یا کلمه عبور موقت؛

ت - توصیه می‌شود کلمات عبور موقت به صورتی ایمن به کاربران داده شود؛ توصیه می‌شود استفاده از پیام‌های الکترونیکی اشخاص ثالث یا محافظت نشده اجتناب شود؛

ث - توصیه می‌شود کلمات عبور برای هر فرد، منحصر به فرد باشد و توصیه می‌شود قابل حدس نباشد؛

ج - توصیه می‌شود کاربران دریافت کلمه عبور خود را اعلام کنند؛

چ - توصیه می‌شود کلمات عبور هرگز در سیستم‌های رایانه‌ی به گونه ای محافظت نشده ذخیره نشوند

ح - توصیه می‌شود کلمات عبور فروشندگان پس از نصب سیستم‌ها یا نرم‌افزار تغییر یابد.

اطلاعات دیگر

کلمات عبور ابزارهای متداولی برای تصدیق هویت یک کاربر قبل از دسترسی به یک سیستم اطلاعات یا سرویس مطابق با تایید اعتبار کاربر است. فن‌آوری‌های دیگر برای شناسایی کاربر و تایید اعتبار، نظیر زیست سنجی مانند تصدیق اثر انگشت، تصدیق امضا، و استفاده از نشانه‌های سخت افزاری، مانند کارت‌های هوشمند، موجود هستند و توصیه می‌شود در صورت مناسب بودن در نظر گرفته شوند.

۱۱-۲-۴ *بازنگری حقوق دسترسی کاربر*

کنترل

توصیه می‌شود مدیریت با استفاده از یک فرایند رسمی، حقوق دسترسی کاربران را در فواصل زمانی منظم، بازنگری کند.

راهنمای پیاده‌سازی

توصیه می‌شود در بررسی حقوق دسترسی رهنمودهای زیر مد نظر قرار گیرد :

الف - توصیه می‌شود حقوق دسترسی کاربران در فواصل منظم مثلا در دوره‌های شش ماهه، و پس از هر تغییر نظیر ارتقا، تنزل رتبه، یا خاتمه استخدام بررسی شوند(رجوع کنید به بند ۱۱-۲-۱)؛

ب - توصیه می‌شود حقوق دسترسی کاربران در زمان جابجایی از یک کارمند به کارمند دیگر در همان سازمان بررسی شود و مجددا اختصاص یابد؛

پ - اختیارات برای حقوق دسترسی دارای مزیت خاص(رجوع کنید به بند ۱۱-۲-۲)، توصیه می‌شود در فواصل کمتر مثلا به صورت ۳ ماهه بررسی شود؛

ت - تخصیص مزایا توصیه می‌شود در فواصل منظم بررسی شود تا اطمینان حاصل شود که مزایای غیر مجاز احراز نشده است؛

ث - تغییر در حساب‌های برتر توصیه می‌شود برای بررسی دوره ای ثبت شود

اطلاعات دیگر

لازم است که حقوق دسترسی کاربران برای حفظ کنترل موثر بر دسترسی به داده‌ها و خدمات اطلاعات بررسی شود.

۱۱-۳ مسوولیت‌های کاربر

هدف: پیشگیری از دسترسی کاربر غیر مجاز، و به خطر افتادن یا سرقت اطلاعات و امکانات پردازش اطلاعات.

همکاری کاربران مجاز برای امنیت موثر لازم است.

توصیه می‌شود کاربران درباره مسوولیت‌های شان برای حفظ کنترل‌های دسترسی موثر، به خصوص در رابطه با استفاده از کلمات عبور و امنیت تجهیزات کاربران آگاه شوند.

توصیه می‌شود یک خط‌مشی کنترل آشکار برای کاهش خطر دسترسی غیرمجاز یا آسیب به ورقه‌ها، رسانه ها، و تجهیزات پردازش اطلاعات اجرا شود.

۱۱-۳-۱ *استفاده از کلمهٔ عبور*

کنترل

توصیه می‌شود کاربران در انتخاب و بکارگیری کلمهٔ عبور، به تبعیت از شیوه‌های امنیتی صحیح، ملزم شوند.

راهنمای پیاده‌سازی

توصیه می‌شود به تمام کاربران توصیه شود که:

الف - کلمات عبور را محرمانه نگه دارند

ب - از نگهداری سابقه ای (مثلا، کاغذ، فایل نرم‌افزاری، یا وسیله دستی) از کلمات عبور مگر زمانی که بتوان آن را به طور ایمن ذخیره کرد و روش ذخیره بهبود مورد تأیید اجتناب کنند؛

پ - کلمات عبور را هر زمان که نشانه‌ای از سوء استفاده احتمالی از سیستم یا کلمه عبور باشد؛ تغییر دهند

ت - کلمات عبور با کیفیت را با حداقل طول انتخاب کنند که:

۱ - حفظ کردن شان ساده باشد؛

۲ - به چیزخاصی مربوط نباشد که شخص دیگری بتواند به سادگی آن را حدس بزند یا با استفاده از اطلاعات شخصی فرد آن را پیدا کند؛ مثلا، نام، شماره تلفن، و تاریخ تولد؛

۳ - نسبت به حملات واژه‌نامه آسیب‌پذیر نباشد؛ مثلا متشکل از واژگانی که در واژه‌نامه آمده است، نباشد.

۴ - از حروف مشابه، تماما عددی یا تماما الفبایی استفاده نشود.

ث - کلمات عبور را در فواصل منظم یا بر اساس تعداد دسترسی‌ها تغییر دهند (توصیه می‌شود کلمات عبور برای حساب‌های ممتاز با تکرار بیشتری نسبت به حساب‌های معمولی تغییر کنند) و از استفاده مجدد از کلمات عبور قدیمی اجتناب کنند.

ج - کلمات عبور موقت را در اولین ارتباط با سیستم تغییر دهند.

چ - کلمات عبور را در هیچ فرایندی که به طور اتوماتیک با سیستم مرتبط می‌شود قرار ندهند مثلا در کلید ماکرو ذخیره نکنند؛

ح - کلمات عبور را بین افراد به اشتراک نگذارند.

خ - از کلمه عبور مشابه برای اهداف کاری و غیر کاری استفاده نکنند.

اگر کاربران نیاز به دسترسی به چندین سرویس، سیستم یا الگو داشته باشند از آنها خواسته شود که چندین کلمه عبور جداگانه را حفظ کنند، باید به آنها توصیه شود که می‌توانند از یک کلمه عبور منفرد و باکیفیت (رجوع کنید به مورد ت) برای تمام خدمات استفاده کنند، زمانی که به کاربران اطمینان داده شد که سطح معقولی از محافظت برای ذخیره کلمه عبور در هر سرویس، سیستم یا الگو تثبیت شده است.

اطلاعات دیگر

مدیریت سیستم کمکی که به کلمات عبور گم شده یا فراموش شده می پردازد، نیازمند مراقبت خاص است زیرا این ممکن است همچنین وسیله ای برای حمله به سیستم کلمه عبور باشد.

۱۱-۳-۲ *تجهیزات بدون مراقبت کاربر*

کنترل

توصیه می‌شود کاربران اطمینان داشته باشند که تجهیزات بدون متصدی، حفاظت مناسبی دارند.

راهنمای پیاده‌سازی

توصیه می‌شود تمام کاربران از الزامات امنیتی و روش‌های اجرایی محافظت از تجهیزات رها شده و نیز مسوولیت شان برای اجرای این محافظت آگاه شوند. توصیه می‌شود به کاربران توصیه شود که:

الف - جلسات فعالی را در پایان به خاتمه برسانند مگر این که بتوان آنها را از طریق یک مکانیسم قفل مناسب مانند یک برنامه محافظ صفحه نمایش محافظت نمود.

ب - از رایانه‌های پردازنده مرکزی، سرورها، و رایانه‌های اداری در زمانی که جلسه بـه پایـان مـی رسـد، قطـع ارتباط نمایند.

پ - رایانه‌ها یا پایانه‌ها را از استفاده غیرمجاز توسط یک قفل کلیددار یا یک کنتـرل معـادل ماننـد دسترسـی توسط کلمه عبور در زمانی‌که در حال استفاده نیست محافظت کنند (همچنین رجوع کنید به بند ۱۱-۳-۳).

اطلاعات دیگر

تجهیزات نصب شده در محیط‌های کاربر، برای مثال ایستگاه‌های کاری، سرویس دهنده‌های فایل ممکن است نیازمند حفاظت خاص دربرابر دسترسی غیرمجاز وقتی که برای مدت مدیدی بدون متصدی باقی می‌مانند.

۱۱-۳-۳ خط‌مشی میز پاک و صفحهٔ پاک

کنترل

توصیه می‌شود یک خط‌مشی میز پاک برای کاغذها و محیط‌های ذخیره‌سازی قابل جابجایی و یک خط‌مشی صـفحهٔ پاک برای امکانات پردازش اطلاعات، مورد پذیرش واقع شوند.

راهنمای پیاده‌سازی

توصیه می‌شود خط‌مشی میز پاک و صفحه پاک در طبقه‌بنـدی اطلاعـات(رجـوع کنیـد بـه ۷-۲)، الزامـات قـانونی و قراردادی(رجوع کنید به ۱۵-۱)، و ریسک‌های مشابه و جنبه‌های فرهنگیِ سازمان، درنظرگرفته شود. توصیه می‌شـود رهنمودهای زیر در نظر گرفته شود:

الف – توصیه می‌شود اطلاعات کسب وکار حیاتی یا حساس، برای مثـال روی کاغـذ یـا رسـانه ذخیـره‌سـازی الکترونیکی، وقتی که به آنها نیاز نیست بطور ایده‌ال در یک گاوصندوق یا قفسه یا سایر شکل‌هـای وسـایل حفاظتی نگهداری شود، مخصوصا وقتی که اداره تعطیل است.

ب – توصیه می‌شود رایانه‌ها و پایانه‌ها بصورت قطع ارتباط یا حفاظت شده با یک ساز و کار قفل صفحه کلید و نمایش کنترل شده با کلمه عبور، کلمه رمز یا ساز و کار احراز اصالت کاربر مشابه، رها شوند وقتی که بدون متصدی هستند و توصیه می‌شود با قفل رمزی، کلمه عبور یا سـایر کنتـرل‌هـا وقتـی کـه مـورد اسـتفاده نیستند، محافظت شوند

پ – توصیه می‌شود نقاط پستی ورودی و خروجی و ماشین‌های نمابر بدون متصدی محافظت شوند.

ت – توصیه می‌شود از استفاده غیرمجاز از تجهیزات نسخه‌برداری و سایر فن‌آوری‌های تکثیـر (مـثلا اسـکنرها، دوربین‌های عکاسی) جلوگیری شود.

ث – توصیه می‌شود مدارک حاوی اطلاعات طبقه‌بندی شده و حساس سریعا از چاپگرها برداشته شوند.

اطلاعات دیگر

یک خط‌مشی میز پاک/صفحه پاک ریسک‌های دسترسی غیرمجاز، از دست دادن، یا آسیب به اطلاعات را در حـین و خارج از ساعات کاری عادی را کاهش می دهد. همچنین گاوصندوق ها یا سایر اشکال امکانات نگهـدای امـن ممکـن است از اطلاعات نگهداری شده در آنها در برابر بلاهایی مانند آتش، زمین لرزه، سیل یا انفجار حفاظت نمایند.

۱۱-۴ کنترل دسترسی به شبکه

هدف: پیشگیری از دسترسی غیر مجاز به خدماتی که تحت شبکه ارائه می‌شوند.
توصیه می‌شود دسترسی به خدمات شبکه ای درونی و بیرونی کنترل شود.
توصیه می‌شود دسترسی کاربران به شبکه‌ها و خدمات با استفاده از موارد زیر به امنیت خدمات شبکه ای آسیب نرساند:
الف - واسط های مناسب بین شبکه سازمان و شبکه‌های دیگر سازمان‌ها و شبکه‌های همگانی برقرار است.
ب - ساز و کارهای سنجش اعتبار مناسب برای کاربران و تجهیزات به کار گرفته می‌شوند:
پ - کنترل دسترسی کاربر به خدمات اطلاعات اجرا می‌شود.

۱۱-۴-۱ *خط‌مشی استفاده از خدمات شبکه*

کنترل
توصیه می‌شود کاربران تنها به خدماتی که مشخصاً استفاده از آنها برایشان مجاز شده، دسترسی داشته باشند.
راهنمای پیاده‌سازی
توصیه می‌شود یک خط‌مشی درباره استفاده از شبکه‌ها و خدمات شبکه ای تدوین شود. توصیه می‌شود این خط‌مشی دربرگیرنده موارد زیر باشد:
الف - شبکه‌ها و خدمات شبکه ای که دسترسی به آنها مجاز است؛
ب - روش‌های اجرایی مجوزدهی برای تعیین این که چه کسی مجاز است به کدام شبکه‌ها و خدمات شبکه ای دسترسی پیدا کند؛
پ - کنترل‌ها و روش‌های اجرایی مدیریتی برای محافظت از دسترسی به اتصالات شبکه و خدمات شبکه؛
ت - ابزارهای به‌کار رفته برای دسترسی به شبکه‌ها و خدمات شبکه ای (برای مثال، شرایطی برای دسترسی از طریق شماره‌گیری برای دسترسی به تامین کننده سرویس اینترنت یا سیستم راه دور)
توصیه می‌شود خط‌مشی استفاده از خدمات شبکه ای با خط‌مشی کنترل دسترسی کسب وکار همخوانی داشته باشد(رجوع کنید به بند ۱۱-۱).
اطلاعات دیگر
ارتباطات غیرمجاز و ناامن به خدمات شبکه می‌تواند بر کل سازمان تاثیر بگذارد. این کنترل به خصوص برای ارتباطات شبکه‌ها به نرم‌افزارهای کاربردی کسب وکار حساس و حیاتی یا برای کاربران در مکان‌های با ریسک بالا مانند نواحی عمومی یا بیرونی که خارج از کنترل و مدیریت سازمان است مهم است.

۱۱-۴-۲ *احراز اصالت (تصدیق هویت) کاربر برای اتصالات بیرونی*

کنترل
توصیه می‌شود برای کنترل دسترسی کاربران راه دور، روش‌های مناسب تصدیق هویت بکار گرفته شوند.

راهنمای پیاده‌سازی

تعیین اعتبار کاربران راه دور را می‌توان مثلا با استفاده از یک فن مبتنی بر رمزنگاری، نشانه‌های سخت افزاری، یا یک پروتکل چالش/پاسخ به دست آورد. اجرای مناسب این روشها را می‌توان در انواع راه حل های شبکه های خصوصی مجازی یافت. خطوط اختصاصی خصوصی را نیز می‌توان برای حصول اطمینان از منبع اتصالات مورد استفاده قرار داد. روش‌های اجرایی و کنترل‌های شماره گیری مثلا استفاده از مودم‌های شماره گیر، می‌تواند محافظتی دربرابر ارتباطات غیرمجاز و ناخواسته به تجهیزات پردازش اطلاعات یک سازمان ایجاد کند. این نوع کنترل اصالت کاربرانی را که سعی می‌کنند ارتباطی با شبکه یک سازمان از مکان‌های دور برقرار کنند احراز می‌کند. در زمان استفاده از این پروتکل، توصیه می‌شود یک سازمان از خدمات شبکه ای که شامل انتقال تماس است استفاده نکند یا اگر این کار این کار را می‌کند، توصیه می‌شود آنها استفاده از این ویژگی‌ها را برای اجتناب از ضعف‌های مربوط به انتقال تماس غیرفعال کنند. توصیه می‌شود فرایند تماس مجدد تضمین کند که قطع ارتباط واقعی در طرف سازمان رخ می‌دهد. در غیر این صورت، کاربر راه دور ممکن است خط را باز نگه دارد و وانمود کند که تصدیق تماس انجام شده است. توصیه می‌شود روش‌های اجرایی و کنترل‌های تماس عمیقا برای مقابله با این احتمال آزموده شود.

تعیین اعتبار گره، می‌تواند به عنوان یک ابزار جایگزین تعیین اعتبار گروه‌های کاربران راه دور در زمانی که به تجهیزات رایانه‌ی امن و مشترک متصل هستند عمل کند. روشهای رمزنگاری مثلا بر اساس گواهی دهی ماشینی می‌تواند برای تعیین اعتبار گره مورد استفاده قرار گیرد. این بخشی از راه حل‌های مبتنی بر شبکه خصوصی مجازی است.

توصیه می‌شود کنترل‌های اضافه تعیین اعتبار، برای کنترل دسترسی به شبکه‌های بی سیم اجرا شوند. به خصوص، در انتخاب کنترل‌هایی برای شبکه‌های بی سیم به دلیل فرصت‌های بزرگتر برای مداخله کشف نشده و واردکردن ترافیک شبکه لازم است.

اطلاعات دیگر

ارتباطات خارجی پتانسیل دسترسی غیرمجاز به اطلاعات کسب وکار را مثلا از طریق روش‌های شماره گیری ایجاد می‌کنند. انواع مختلف روش‌های سنجش اعتبار وجود دارد که بعضی از آنها سطح بالاتری از محافظت را در مقایسه با بقیه ارایه می‌کنند مثلا روش‌هایی بر اساس استفاده از روشهای رمزنگاری می‌توانند سنجش اعتباری قوی ایجاد کنند. مهم است که با یک ارزیابی ریسک، سطح محافظت لازم تعیین شود. این برای انتخاب مناسب یک روش تعیین اعتبار لازم است.

یکی از راه‌های تسهیل ارتباط با یک رایانه راه دور ممکن است راهی برای دستیابی به دسترسی غیرمجاز به یک عملکرد کسب وکار باشد. این بخصوص زمانی مهم است که اتصال از شبکه ای استفاده کند که خارج از کنترل مدیریت امنیت سازمان است.

۱۱-۴-۳ *شناسایی تجهیزات در شبکه‌ها*

کنترل

توصیه می‌شود شناسایی خودکار تجهیزات، به عنوان وسیله ای برای احراز اصالت اتصالات از مکان‌ها و تجهیزات مشخص، در نظر گرفته شود.

راهنمای پیاده‌سازی

شناسایی تجهیزات باید زمانی انجام شود که مهم باشد ارتباطات فقط می‌تواند از یک محل یا تجهیزات خاص آغاز شود. یک شناسایی کننده تجهیزات می‌تواند برای نشان دادن این که آیا تجهیزات اجازه دارد با شبکه اتصال برقرار کند یا نه مورد استفاده قرار گیرد. اگر بیش از یک شبکه وجود دارد و بخصوص اگر این شبکه‌ها حساسیت‌های متفاوت دارند. توصیه می‌شود این شناسایی کنندگان به روشنی نشان دهند که تجهیزات اجازه اتصال به کدام شبکه را دارند. ممکن است لازم باشد که محافظت فیزیکی از تجهیزات را برای حفظ امنیت شناسایی کننده تجهیزات در نظر داشته باشیم.

اطلاعات دیگر

این کنترل می‌تواند با روش‌های دیگری برای احراز اصالت کاربر تجهیزات (رجوع کنید به بند ۱۱-۴-۲) تکمیل شود. شناسایی تجهیزات می‌تواند علاوه بر تعیین اعتبار کاربر مورد استفاده قرار گیرد.

۱۱-۴-۴ حفاظت از درگاه عیب‌یابی و پیکر بندی راه دور

کنترل

توصیه می‌شود دسترسی فیزیکی و منطقی به درگاه‌های عیب‌یابی و پیکربندی، تحت کنترل باشد.

راهنمای پیاده‌سازی

دسترسی فیزیکی و منطقی به پورت های عیب یابی و پیکربندی دربرگیرنده استفاده از یک قفل و رویه روش‌های اجرایی پشتیبان برای کنترل دسترسی فیزیکی به درگاه است. مثالی از چنین روش‌های اجرایی پشتیبان، تضمین آن است که درگاه‌های عیب یابی و پیکربندی فقط توسط هماهنگی بین مدیر خدمات رایانه و پرسنل پشتیبانی نرم‌افزار/سخت افزار است که به دسترسی نیاز دارند.

درگاه‌ها، خدمات، و تجهیزات مشابهی که روی یک رایانه یا دستگاه شبکه ای نصب می‌شوند، و به طور خاص برای کارایی کسب وکار لازم نیستند، توصیه می‌شود غیرفعال شوند یا حذف شوند.

اطلاعات دیگر

بسیاری از سیستم‌های رایانه‌ی، سیستم‌های شبکه، و سیستم‌های ارتباطات، با یک تجهیزات عیب یابی و پیکربندی راه دور برای استفاده توسط مهندسان نگهداری نصب می‌شوند.

اگر این درگاه‌های عیب یابی محافظت نشده باشند، به ابزاری برای دسترسی غیرمجاز تبدیل می‌شوند.

۱۱-۴-۵ تفکیک در شبکه‌ها

کنترل

توصیه می‌شود گروه‌های خدمات اطلاعاتی، کاربران و سیستم‌های اطلاعاتی، در شبکه‌ها تفکیک شوند.

راهنمای پیاده‌سازی

یکی از روش‌های کنترل امنیت شبکه‌های بزرگ تقسیم آنها به حوزه‌های شبکه منطقی جداگانه مانند حوزه‌های شبکه داخلی یک سازمان و حوزه‌های شبکه خارجی است که هر کدام توسط یک محیط امنیتی تعریف شده محافظت می‌شوند. یک مجموعه مدرج از کنترل‌ها را می‌توان در حوزه‌های شبکه‌های منطقی مختلف برای تفکیک بیشتر محیط‌های امنیتی شبکه، مثلا سیستم‌هایی که برای همگان قابل دسترسی هستند، شبکه‌های داخلی، و دارایی‌های حیاتی مورد استفاده قرار داد. توصیه می‌شود حوزه‌ها بر اساس یک ارزیابی ریسک و الزامات مختلف امنیتی در هر یک از دوره‌ها تعریف شوند.

چنین محیط‌های شبکه را می‌توان از طریق نصب یک دروازه امن بین دو شبکه که برای کنترل دسترسی و جریان اطلاعات بین دو حوزه متصل می‌شوند اجرا کرد. توصیه می‌شود این دروازه برای فیلتر کردن ترافیک بین این حوزه‌ها (رجوع کنید به بند ۱۱-۴-۶ و ۱۱-۴-۷) و مسدود کردن دسترسی غیرمجاز مطابق با خط‌مشی کنترل دسترسی سازمان پیکربندی گردد (رجوع کنید به بند ۱۱-۱). مثالی از این نوع دروازه، چیزی به نام دیوار آتش است. روش دیگر روش حوزه‌های منطقی جداگانه محدودکردن دسترسی شبکه با استفاده از شبکه‌های خصوصی مجازی برای گروه‌های کاربر در سازمان است.

شبکه‌ها، را همچنین می‌توان با استفاده از کارایی دستگاه شبکه، مثلا با سوئیچ کردن پروتکل اینترنت[1] تفکیک کرد. حوزه‌های جداگانه را آن گاه می‌توان با کنترل جریان‌های داده‌های شبکه با استفاده از قابلیت‌های مسیریابی/ راه‌گزینی[2] نظیر فهرست‌های کنترل دسترسی اجرا کرد.

توصیه می‌شود معیارهای تفکیک شبکه ها به دامنه ها براساس خط مشی کنترل دسترسی و الزامات دسترسی باشد (رجوع کنید به ۱۰-۱)، و همچنین درنظر گرفتن هزینه مربوطه و پیامد عملکرد متحد کردن فن‌آوری دروازه یا مسیریابی مناسب شبکه (رجوع کنید به ۱۱-۴-۶ و ۱۱-۴-۷).

بعلاوه، توصیه می‌شود تفکیک شبکه ها بر اساس ارزش و طبقه‌بندیِ اطلاعات نگهداری شده یا پردازش شده در شبکه، سطوح اعتماد، یا خطوط کسب وکار برای کاهش پیامد کلی قطع سرویس.

توصیه می‌شود ملاحظاتی برای تفکیک شبکه های بی‌سیم از شبکه های داخلی و خصوصی درنظر گرفته شود. از آنجا که فضای احاطه شده توسط شبکه بی‌سیم بخوبی تعریف نشده است، توصیه می‌شود یک ارزیابی ریسک در این شرایط برای شناسایی کنترل ها انجام شود (برای مثال، احراز اصالت قوی، روش‌های رمزنگاری، و انتخاب فرکانس) تا از وضعیت مناسب تفکیک شبکه اطمینان حاصل آید.

اطلاعات دیگر

شبکه ها بطور فزاینده در حال توسعه یافتن، فراتر از مرزهای سنتی سازمانی هستند، از آنجایی که شرکای کسب وکار به صورتی شکل گرفته اند که ممکن است به اتصال میانی یا اشتراک پردازش میانی و تجهیزات شبکه نیاز داشته باشند. این توسعه ها ممکن است ریسک دسترسی غیرمجاز به سیستم‌های اطلاعاتی موجود را که از شبکه استفاده می‌کند افزایش دهد؛ تعدادی از آنها ممکن است نیاز به حفاظت در برابر کاربران شبکه های دیگر داشته باشند، بخاطر حیاتی بودن یا حساس بودن آنها.

۱۱-۴-۶ کنترل اتصال به شبکه

کنترل

برای شبکه‌های اشتراکی، به ویژه آنهایی که در محدوده‌های سازمان، گسترش می یابند، قابلیت کاربران برای اتصال به شبکه، توصیه می‌شود در راستای خط‌مشی کنترل دسترسی و الزامات برنامه‌های کاربردی کسب‌وکار، محدود شود (رجوع کنید به بند ۱۱-۱)

راهنمای پیاده‌سازی

توصیه می‌شود حقوق دسترسی کاربران به شبکه طبق نیاز خط‌مشی کنترل دسترسی حفظ و روزآمد شود. (رجوع کنید به بند ۱۱-۱-۱)

1- Internet Protocol (IP)
1- Switching/Routing

قابلیت ارتباط کاربران را می‌توان از طریق دروازه های شبکه که تردد را با استفاده از جدول‌ها یا قوانین از پیش تعیین شده فیلتر می‌کنند محدود کرد. مثال‌های کاربردهایی که توصیه می‌شود محدودیت‌ها به آنها اعمال می‌شوند شامل موارد زیر است:

الف - پیام‌رسانی؛ مثلا پست الکترونیکی

ب - انتقال فایل

پ - دسترسی تعاملی

ت - دسترسی به برنامه های کاربردی

توصیه می‌شود پیوند حقوق دسترسی شبکه به تاریخ ها یا زمان‌های خاصی از روز در نظر گرفته شود.

اطلاعات دیگر

به کارگیری کنترل‌هایی برای محدود کردن قابلیت اتصال کاربران ممکن است توسط خط‌مشی کنترل دسترسی برای شبکه‌های مشترک به خصوص شبکه‌هایی که در فراسوی مرزهای سازمانی بسط می یابند مورد نیاز باشد.

۱۱-۴-۷ کنترل مسیر یابی در شبکه

کنترل

توصیه می‌شود کنترل‌های مسیریابی برای شبکه‌ها پیاده‌سازی شوند، تا اطمینان حاصل شود که اتصالات رایانه ای و جریان‌های اطلاعاتی، خط‌مشی کنترل دسترسی به برنامه‌های کاربردی کسب‌وکار را نقض نمی‌کنند.

راهنمای پیاده‌سازی

توصیه می‌شود کنترل های مسیریابی بر ساس ساز و کار های بررسی آدرس مقصد و منبع مثبت باشد.

مداخل امنیت را می‌توان برای اعتبار بخشی نشانی‌های مقصد و منبع در نقاط کنترل شبکه داخلی و بیرونی در صورتی که میان بر و یا فن‌آوری ترجمه نشانی شبکه مورد استفاده قرار می‌گیرند. توصیه می‌شود مجریان از قدرت و نارسایی‌های هر یک از ساز و کارهای به‌کار رفته آگاه باشند. توصیه می‌شود الزامات کنترل مسیریابی شبکه بر اساس خط‌مشی دسترسی باشد. (رجوع کنید به بند ۱۱-۱)

اطلاعات دیگر

شبکه‌های مشترک، به خصوص شبکه‌هایی که ماورای مرزهای سازمانی گسترش دارند ممکن است نیازمند کنترل‌های مسیریابی اضافی باشند. این به خصوص در جایی که شبکه‌ها با کاربران شخص سوم مشترک هستند اعمال می‌شود.

۱۱-۵ کنترل دسترسی به سیستم عامل

هدف: پیشگیری از دسترسی غیر مجاز به سیستم‌های عامل.

توصیه می‌شود تجهیزات امنیتی برای محدود کردن دسترس به سیستم‌های عامل به کاربران مجاز مورد استفاده قرار گیرد. توصیه می‌شود تجهیزات قابلیت‌های زیر را داشته باشند:

الف - تصدیق اعتبار کاربران مجاز مطابق با یک خط‌مشی کنترل دسترسی تعریف شده

ب - ثبت تلاشهای موفق و ناموفق تصدیق اعتبار سیستم

پ - ثبت استفاده از مزایای ویژه سیستم

ت - صدور هشدارهایی در زمانی‌که خط مشی‌های امنیتی سیستم نقض می‌شوند

ث - ارائه ابزارهای مناسب برای تصدیق اعتبار

ج - در جای مناسب، محدود کردن زمان ارتباط کاربران

۱۱-۵-۱ *روش‌های اجرایی برقراری ارتباط امن*

کنترل

توصیه می‌شود دسترسی به سیستم‌های عامل، از طریق یک روش‌اجرایی برقراری ارتباط امن با سیستم، کنترل شود.

راهنمای پیاده‌سازی

توصیه می‌شود روش اجرایی ورود به یک سیستم عامل برای کاهش فرصت دسترسی غیرمجاز طراحی شود. بنابراین توصیه می‌شود این روش اجرایی برقراری ارتباط حداقل اطلاعات را درباره سیستم افشا کند تا از ارایه کمک غیرمجاز به یک کاربرد غیرمجاز اجتناب شود. توصیه می‌شود یک روش اجرایی خوب برای برقراری ارتباط:

الف - سیستم یا شناساننده‌های برنامه کاربردی را تا زمانی که فرایند برقراری ارتباط با موفقیت به پایان نرسیده است نشان ندهد.

ب - یک هشدار عمومی را نمایش دهد که توصیه می‌شود رایانه فقط توسط اشخاص مجاز مورد دسترسی قرار گیرد.

پ - پیام‌های کمک را در طول روش اجرایی برقراری ارتباط ارایه نکند که به کاربران غیرمجاز کمک شود.

ت - اطلاعات برقراری ارتباط را پس از تکمیل تمام داده‌های ورودی اعتبار بخشی نماید. اگر خطایی سرزند، توصیه می‌شود سیستم نشان ندهد که کدام بخش از داده‌ها صحیح و کدام بخش صحیح نیست.

ث - تعداد تلاشهای برقراری ارتباط ناموفق مجاز را محدود کند؛ مثلا به سه بار و موارد زیر را در نظر گیرد:

۱ - ثبت تلاشهای موفق و ناموفق

۲ - ایجاد یک تاخیر زمانی قبل از این که به تلاشهای برقراری ارتباط بیشتر اجازه داده شود یا هر تلاشی بدون مجوز خاص رد شود.

۳ - قطع ارتباط داده‌ها

۴ - ارسال یک پیام هشدار به مرکز فرمان سیستم اگر تعداد تلاشها برای برقراری ارتباط به میزان حد اکثر خود رسید.

۵ - تعیین تعداد (تلاشهای مکرر وارد کردن کلمه عبور در ارتباط با حداقل طول کلمه عبور و ارزش سیستمی که محافظت می‌شود

ج - حداکثر و حداقل زمان مجاز برای روش اجرایی برقراری ارتباط را محدود کند. توصیه می‌شود اگر از حد انتظار فراتر رفت، سیستم برقراری ارتباط را خاتمه دهد.

چ - اطلاعات زیر را درباره تکمیل یک برقراری ارتباط موفق نمایش دهد:

۱ - تاریخ و زمان برقراری ارتباط موفق قبلی

۲ - جزئیات هر تلاش ناموفق برای برقراری ارتباط از زمان آخرین برقراری ارتباط موفق

ح - کلمه عبوری را که وارد می‌شود نمایش ندهد یا کاراکترهای کلمه عبور را توسط نمادهایی نشان دهد.

خ - کلمات عبور را در یک متن آشکار در یک شبکه منتقل نکند

اطلاعات دیگر

اگر کلمات عبور در طول جلسه برقراری ارتباط در یک شبکه در یک متن آشکار منتقل شوند، می‌توان آنها را توسط یک برنامه کشف کننده شنود تحت شبکه در شبکه به دست آورد.

۱۱-۵-۲ *شناسایی و احراز اصالت کاربر*

کنترل

توصیه می‌شود تمامی کاربران یک شناسهٔ منحصر به فرد (شناسهٔ کاربر) برای استفاده شخصی خودشان داشته باشند و توصیه می‌شود یک فن مناسب تصدیق هویت، به منظور اثبات هویت ادعا شده توسط یک کاربر، انتخاب شود.

راهنمای پیاده‌سازی

توصیه می‌شود این کنترل برای تمام انواع کاربران به کار گرفته شود (شامل پرسنل پشتیبانی فنی، اپراتورها، راهبران شبکه، برنامه نویسان سیستم، و راهبران بانک داده)

توصیه می‌شود هویت کاربر برای ردیابی فعالیت‌ها در مورد افراد مسوول مورد استفاده قرار گیرد. توصیه می‌شود فعالیت‌های منظم کاربر از طریق حساب‌های با امتیازات ویژه انجام نشود.

در مواقع استثنایی، در جایی که منفعت کاری آشکاری وجود دارد، می‌توان از شناسه کاربری مشترک برای گروهی از کاربران یا یک شغل خاص استفاده کرد. توصیه می‌شود تایید مدیریت برای این موارد مستند شود. کنترل‌های اضافی ممکن است برای حفظ پاسخگویی لازم باشد.

توصیه می‌شود شناسه‌های عمومی برای استفاده توسط یک فرد فقط در صورتی مجاز است که یا در جایی که عملکردهای در دسترسی یا فعالیت‌های انجام شده توسط نام کاربری نیازی به ردیابی شدن ندارند (برای مثال، دسترسی فقط خواندنی)، یا در جایی که کنترل‌های دیگری در حال اجرا است مورد استفاده قرار گیرند (برای مثال، کلمه عبور برای یک شناسه کلی فقط برای یک شخص و در یک زمان و برای واقعه نگاری آن لحظه صادر می‌شود)

در جایی که احراز اصالت و تصدیق هویت قوی لازم است، توصیه می‌شود روش‌های تایید اعتبار که جایگزین کلمه عبور می‌شوند، نظیر ابزارهای رمزنگاری، کارت‌های هوشمند، علائم یا ابزارهای زیست سنجی مورد استفاده قرار گیرند.

اطلاعات دیگر

کلمات عبور (همچنین رجوع کنید به بند ۱۱-۳-۱ و بند ۱۱-۵-۳) راهی بسیار معمول برای ارایه شناسایی و اعتبار بر اساس یک رمز هستند که فقط کاربر آن را می‌داند. همین را می‌توان با ابزار رمزنگاری و پروتکل‌های تایید اعتبار به

دست آورد. توصیه می‌شود شدت شناسایی کاربر و تایید اعتبار او با حساسیت اطلاعاتی که قرار است مورد دسترسی قرار گیرد همخوانی داشته باشد.
مواردی نظیر علائم و کارتهای هوشمند، که کاربر آنها را دارد، نیز می‌توانند برای شناسایی و تعیین اعتبار مورد استفاده قرار گیرند. فن‌آوری‌های زیست سنجی تعیین اعتبار که از ویژگی‌های منحصر به فرد یا ویژگی‌های یک فرد هستند نیز می‌توانند برای احراز اصالت یک شخص مورد استفاده قرار گیرد. ترکیبی از فن‌آوری‌ها و ساز و کارهایی که پیوند محکمی با هم دارند منجر به شناسایی قوی‌تر خواهد شد.

۱۱-۵-۳ سیستم مدیریت کلمهٔ عبور

کنترل

توصیه می‌شود سیستم‌های مدیریت کلمات عبور، تعاملی بوده و توصیه می‌شود کیفیت کلمات عبور را تضمین نمایند.

راهنمای پیاده‌سازی

توصیه می‌شود یک سیستم مدیریت کلمه عبور:

الف - استفاده از هویت‌های کاربر و کلمات عبور را برای حفظ پاسخگویی اجبار کند

ب - به کاربران اجازه دهد کلمه عبور خود را انتخاب کنند و تغییر دهند، و روش اجرایی تاییدی را برای خطاهای وارده بگنجاند

پ - انتخاب کلمات عبور با کیفیت را انجام دهد. (رجوع کنید به بند ۱۱-۳-۱)

ت - تغییرات در کلمات عبور را اجبار کند (رجوع کنید به بند ۱۱-۳-۱)

ث - کاربران را وادار کند کلمات عبور موقت را در اولین برقراری ارتباط تغییر دهند. (رجوع کنید به بند ۱۱-۳-۲)

ج - سابقه ای از کلمات عبور پیشین را نگهداری کند و از استفاده مجدد آنها جلوگیری کند؛

چ - کلمات عبور را در زمان وارد شدن روی صفحه نشان ندهد.

ح - فایل‌های کلمات عبور را جدا از دیگر داده‌های سیستم کاربردی ذخیره کند.

خ - کلمات عبور را در فرم‌های محافظت شده ذخیره کند یا منتقل کند.

اطلاعات دیگر

کلمات عبور یکی از ابزارهای اساسی اعتباربخشی مجوز کاربران در دسترسی به یک سرویس رایانه‌ی هستند.
بعضی از برنامه های کاربردی نیازمند کلمات عبور هستند که توسط مراجع مستقل تعیین می‌شوند؛ در چنین مواردی نکات ب، ت، و ث از راهنمای فوق به‌کار نمی‌روند. در اکثر موارد کلمات عبور توسط کاربران انتخاب و حفظ می‌شوند.
بخش ۱۱-۳-۱ را برای راهنمای درباره استفاده از شبکه‌ها ببینید.

۱۱-۵-۴ استفاده از برنامه‌های کمکی سیستم

کنترل

توصیه می‌شود استفاده از برنامه‌های کمکی سیستم که ممکن است قادر به ابطال کنترل‌های سیستم و برنامهٔ کاربردی باشند، محدود و به شدت کنترل شوند.

راهنمای پیاده‌سازی

توصیه می‌شود رهنمودهای زیر برای استفاده از برنامه های کاربردی سیستم در نظر گرفته شود:

الف - استفاده از روش‌های اجرایی شناسایی، احراز اصالت، و مجوز دهی برای برنامه های کمکی سیستم
ب - تفکیک برنامه های کمکی سیستم از نرم‌افزارهای کاربردی
پ - محدودکردن استفاده از برنامه های کمکی سیستم به حداقل تعداد کاربردی کاربران مجاز و مورد اطمینان(رجوع کنید به بند ۱۱-۲-۲)
ت – اجازه برای استفاده تک کاره از ابزارهای سیستم‌ها
ث - محدودکردن دسترسی به سطوح تایید مجوز برای کاربردهای سیستم
ج – واقعه نگاریِ همه استفاده ها از ابزارهای سیستم.
چ – محدودسازی دسترسی به ابزارهای کمکی سیستم، برای مثال برای دوره از یک تغییر مجاز
ح - از بین بردن با غیرفعال کردن نرم‌افزارهای غیرضروری بر اساس برنامه های کمکی و نرم‌افزار سیستمی
خ - عدم اجازه دسترسی به کاربرانی که به برنامه های کمکی در یک سیستم دسترسی دارند در زمانی که تفکیک وظایف لازم است.

اطلاعات دیگر

اکثر نصب‌های رایانه‌ی یک یا چند برنامه کمکی سیستم دارند که ممکن است منجر به ابطال کنترل‌های سیستم و برنامه های کاربردی شوند.

۱۱-۵-۵ خروج زمانی از لایه ارتباطی

کنترل

توصیه می‌شود لایه‌های ارتباطی غیر فعال پس از یک بازهٔ زمانی تعریف شده برای غیر فعال بودن، بسته و قطع شوند.

راهنمای پیاده‌سازی

توصیه می‌شود یک دستگاه اتمام وقت صفحه جلسه را روشن کند و احتمالا بعدا، هر دو عملکرد و جلسات شبکه را پس از یک دوره تعریف شده عدم فعالیت ببندد. توصیه می‌شود تاخیر اتمام وقت، نشانگر ریسک های امنیتی منطقه، طبقه بندی اطلاعاتی که مورد استفاده قرار می‌گیرند و کاربردهای مورد استفاده و ریسک های مربوط به تجهیزات باشد.

شکل محدودی از تجهیزات اتمام وقت را می‌توان برای بعضی از سیستم‌ها ارایه کرد که صفحه را روشن می‌کند و از دسترسی غیرمجاز جلوگیری می‌کند اما کارایی یا جلسات شبکه را نمی بندد.

اطلاعات دیگر

کنترل به خصوص در محل‌هایی که ریسک بالایی دارند مهم است، که شامل مناطق همگانی یا بیرونی خارج از مدیریت امنیت سازمان است. توصیه می‌شود جلسات برای جلوگیری از دسترسی اشخاص غیرمجاز و جلوگیری از حمله به خدمات خاموش شود.

۱۱-۵-۶ محدودسازی زمان اتصال

کنترل

به منظور فراهم آوری امنیت بیشتر برای برنامه‌های کاربردی با ریسک بالا، توصیه می‌شود محدودیت‌هایی در زمان‌های اتصال اعمال گردد.

راهنمای پیاده‌سازی

توصیه می‌شود کنترل‌های زمان ارتباط برای برنامه‌های کاربردی رایانه‌ی حساس در نظر گرفته شود، به خصوص از محل‌های با ریسک بالا مانند مناطق عمومی یا بیرونی که خارج از مدیریت امنیت سازمان هستند. مثال‌های این محدودیت‌ها عبارتند از:

الف - استفاده از علائم زمانی از پیش تعیین شده مثلا برای انتقال یا جلسات عادی کوتاه

ب - محدودکردن زمان‌های اتصال به ساعات اداری عادی اگر الزامی برای عملیات مازاد زمان یا عملیات ساعات اضافه وجود ندارد.

پ - در نظر گرفتن تایید مجدد اعتبار در فواصل زمان بندی شده

اطلاعات دیگر

محدود کردن دوره ای که در طول آن، ارتباطات با خدمات رایانه امکان پذیر می‌شوند فرصت دسترسی غیرمجاز را کاهش می‌دهد. محدود کردن طول جلسات فعال، از برگزاری جلساتی که برای پیشگیری از تایید اعتبار مجدد باز هستند جلوگیری می‌کند.

۱۱-۶ کنترل دسترسی به برنامه‌های کاربردی و اطلاعات

هدف: پیشگیری از دسترسی غیر مجاز به اطلاعات نگهداری شده در سیستم‌های کاربردی.

توصیه می‌شود تجهیزات امنیتی برای محدودکردن دسترسی به سیستم‌های کاربرد مورد استفاده قرار گیرند.

توصیه می‌شود دسترسی منطقی به نرم‌افزار و اطلاعات محدود به کاربران مجاز باشد.

توصیه می‌شود سیستم‌های کاربرد:

الف - دسترسی کاربر را به اطلاعات و سیستم‌های کاربردی مطابق با یک خط‌مشی کنترل دسترسی تعریف شده کنترل کنند؛

ب - محافظت در برابر دسترسی غیرمجاز را توسط هر نرم افزارکمکی، نرم‌افزار سیستم عامل، و نرم‌افزار را مخربی که توانایی حذف و یا عبور از کنترلهای برنامه های کاربردی و یا سیستمی دارد را ایجاد کند.

پ - به دیگر سیستم‌هایی که منابع اطلاعاتی با آنها در ارتباط هستند، اختلال وارد نکنند.

۱۱-۶-۱ *محدودیت دسترسی به اطلاعات*

کنترل

مطابق با خط مشی کنترل دسترسی تعریف شده، توصیه می‌شود دسترسی کاربران و کارکنان پشتیبانی کننده به اطلاعات و کارکردهای سیستم کاربردی، محدود شود.

راهنمای پیاده‌سازی

توصیه می‌شود محدودیت در دسترسی بر اساس الزامات عملکرد کسب وکار فردی باشد. توصیه می‌شود خط‌مشی کنترل دسترسی همچنین با خط‌مشی دستریس سازمانی همسو باشد. (رجوع کنید به بند ۱۱-۱)

توصیه می‌شود به کارگیری رهنمودهای زیر به منظور پشتیبانی الزامات محدودیت دسترسی در نظر گرفته شود:

الف - ارایه منوهایی برای کنترل دسترسی به وظایف سیستم کاربردی

ب - کنترل حقوق دسترسی کاربران، مانند خواندن، نوشتن، حذف کردن و اجرا کردن

پ - کنترل حقوق دسترسی نرم‌افزارهای کاربردی دیگر

ت – حصول اطمینان از این که خروجی سیستم‌های کاربردی که اطلاعات حساس را اجرا می‌کنند فقط حاوی اطلاعات مرتبط برای استفاده از خروجی می‌باشند و فقط به پایانه ها و محل‌های مجاز فرستاده می‌شوند. توصیه می‌شود این شامل بررسی‌های دوره ای از این خروجی‌ها برای تضمین این باشد که اطلاعات زائد حذف می‌شود.

۱۱-۶-۲ *جداسازی سیستم‌های حساس*

کنترل

توصیه می‌شود سیستم‌های حساس یک محیط محاسباتی اختصاصی (مجزا)، داشته باشند.

راهنمای پیاده‌سازی

توصیه می‌شود نکات زیر برای جداسازی سیستم حساس در نظر گرفته شود:

الف - توصیه می‌شود حساسیت سیستم کاربردی صریحا شناسایی و توسط مالک سیستم کاربردی شناسایی و مستند شود مستند شود(رجوع کنید به بند ۷-۱-۲).

ب - زمانی که یک نرم‌افزار کاربردی حساس در حال اجرا در یک محیط مشترک است، سیستم‌های کاربردی که این نرم‌افزار دارای منابع مشترک با آنها است، توصیه می‌شود توسط مالک نرم‌افزار کاربردی حساس شناسایی و پذیرفته شوند.

اطلاعات دیگر

بعضی از سیستم‌های کاربردی، به اندازه کافی به آسیب بالقوه که نیازمند اجرای خاص هستند حساس هستند.

حساسیت ممکن است نشان دهد که سیستم کاربردی:

الف - توصیه می‌شود در یک رایانه اختصاصی اجرا شود

ب - توصیه می‌شود فقط منابع را با سیستم‌های کاربردی مورداطمینان در اشتراک داشته باشد.

جداسازی را می‌توان با استفاده از روش‌های فیزیکی یا منطقی به دست آورد. (همچنین رجوع کنید به بند ۱۱-۴-۵)

۱۱-۷ محاسبهٔ سیار و کار از راه دور

هدف: حصول اطمینان از امنیت اطلاعات در هنگام استفاده از امکانات محاسبهٔ سیار و کار از راه دور.

در زمان استفاده از محاسبه سیار، رسیک‌های کار در یک محیط محافظت نشده توصیه می‌شود (توصیه می‌شود ریسک‌های کار در یک محیط محافظت نشده) در نظر گرفته شود و توصیه می‌شود محافظت مناسب به کار گرفته شود. در مورد کار از راه دور، توصیه می‌شود سازمان از محافظت برای محل کار از راه دور استفاده کند و تضمین کند که مقررات مناسب برای این نوع کار کردن وجود دارند.

۱۱-۷-۱ *محاسبه و ارتباطات سیار*

کنترل

به منظور حفاظت در برابر ریسک‌های بکارگیری امکانات محاسبه و ارتباطات سیار، توصیه می‌شود یک خط‌مشی رسمی بکار گرفته شود و توصیه می‌شود معیارهای امنیتی مناسبی اختیار شوند.

راهنمای پیاده‌سازی

در زمان استفاده از تجهیزات محاسبه و ارتباط سیار، مانند رایانه‌های کیفی، رایانه‌های دستی، رایانه‌های روپایی، کارت‌های هوشمند، و تلفن‌های همراه توصیه می‌شود که مراقبت شود که تضمین شود اطلاعات کسب وکار مورد دستبرد قرار نمی‌گیرند. توصیه می‌شود خط‌مشی محاسبه سیار به حساب آوردند، ریسک‌های کار با تجهیزات محاسبه سیار در محیط‌های محافظت نشده را مد نظر قرار دهند.

توصیه می‌شود خط‌مشی محاسبه سیار، شامل الزاماتی برای محافظت فیزیکی، کنترل‌های دسترسی، روشهای رمزنگاری، نسخه های پشتیبان و محافظت دربرابر ویروس باشد. توصیه می‌شود خط‌مشی همچنین شامل قوانین و نکاتی درباره تجهیزات ارتباط سیار برای شبکه‌ها و راهنمایی درباه استفاده از این تجهیزات در مکان‌های عمومی باشد. توصیه می‌شود در زمان استفاده از تجهیزات محاسبه سیار در مکان‌های عمومی، اتاق‌های جلسات، و مناطق محافظت نشده خارج از حوزه‌های سازمان مراقبت شود. توصیه می‌شود محافظت برای اجتناب از دسترسی غیرمجاز یا افشای اطلاعات ذخیره شده و پردازش شده توسط تجهیزات به کار گرفته شود. برای مثال استفاده از روش‌های رمزنگاری (رجوع کنید به بند ۱۲-۳)

توصیه می‌شود کاربران تجهیزات محاسبه سیار، در مکان‌های عمومی مراقب باشند تا از ریسک دیده شدن توسط اشخاص غیرمجاز اجتناب شود. توصیه می‌شود روش‌های اجرایی دربرابر نرم‌افزارهای نامناسب در نظر گرفته شود و به‌روز شود. (رجوع کنید به بند ۱۰-۴)

توصیه می‌شود نسخه های پشتیبان اطلاعات کسب وکار حیاتی به طور منظم گرفته شود. توصیه می‌شود تجهیزات برای امکان پذیر کردن پشتیبان گیری سریع و ساده از اطلاعات در دسترس باشد. توصیه می‌شود این نسخه های پشتیبان محافظت کافی را در برابر سرقت یا آسیب به اطلاعات داشته باشند.

توصیه می‌شود محافظت مناسب در استفاده از تجهیزات سیار مرتبط با شبکه‌ها در نظر گرفته شود. توصیه می‌شود دسترسی راه دور به اطلاعات کسب وکار در سراسر شبکه همگانی با استفاده از تجهیزات محاسبه سیار فقط پس از شناسایی و مجوز دهی و با مکانیسم کنترل دسترسی مناسب رخ دهند. (رجوع کنید به بند ۱۱-۴)

توصیه می‌شود تجهیزات محاسبه سیار، همچنین از نظر فیزیکی در برابر سرقت به خصوص در زمانی که مثلا در ماشین و انواع دیگر حمل‌ونقل، اتاق‌های هتل‌ها، مراکز کنفرانس، و مکان‌های همایش محافظت شوند. توصیه می‌شود رویه ای خاص که الزامات امنیتی قانونی، بیمه و... سازمان را مد نظر قرار می‌دهد برای موارد سرقت یا آسیب به تجهیزات محاسبه سیار تثبیت شود.

توصیه می‌شود تجهیزاتی که اطلاعات حساس، مهم و یا حیاتی را حمل می‌کنند بی توجه رها نشود و در صورت امکان توصیه می‌شود از نظر فیزیکی قفل شود و توصیه می‌شود برای امنیت تجهیزات مورد استفاده قرار گیرد. (رجوع کنید به بند ۹-۲-۵)

توصیه می‌شود آموزش برای پرسنلی که از محاسبه سیار برای افزایش آگاهی آنها درباره ریسک‌های ناشی از این نوع کار و کنترل‌هایی که توصیه می‌شود اجرا شوند هماهنگ شود.

اطلاعات دیگر

اتصالات بی سیم شبکه سیار، شبیه به انواع دیگر ارتباطات شبکه است، اما تفاوت‌های مهمی دارد که توصیه می‌شود در زمان شناسایی کنترل‌ها در نظر گرفته شود.

تفاوت‌های معمول عبارتند از:

الف - بعضی از پروتکل‌های امنیتی بی سیم ناکافی هستند و ضعف‌های مشهودی دارند.

ب - اطلاعات ذخیره شده در رایانه‌های سیار را به دلیل عرض باند محدود شبکه و یا به این دلیل که تجهیزات سیار ممکن است در زمان‌هایی که پشتیبان‌گیری زمان بندی می‌شود متصل نباشند، نمی‌توان پشتیبان گرفت.

۱۱-۷-۲ کار از راه دور

کنترل

توصیه می‌شود برای عملیات‌های کار از راه دور، یک خط‌مشی، طرح‌های عملیاتی و روش‌های اجرایی، ایجاد و پیاده‌سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود سازمان‌ها فقط فعالیت‌های کار از راه دور را در صورتی که مطمئن شدند هماهنگی‌های امنیتی مناسب در حال اجرا است و این‌ها با خط‌مشی امنیت سازمان مطابقت دارد مجاز کنند.

توصیه می‌شود محافظت مناسب از محل کار از راه دور مثلا در مقابله با سرقت از تجهیزات و اطلاعات، افشای غیرمجاز اطلاعات، دسترسی راه دور غیرمجاز به سیستم‌های داخلی سازمان یا سوءاستفاده از تجهیزات در نظر گرفته شود. توصیه می‌شود فعالیت‌های کار از راه دور، توسط مدیریت مجوز داده و کنترل شود و توصیه می‌شود که از مدنظر قرار دادن هماهنگی های مناسب برای این نوع کار اطمینان حاصل شود.

توصیه می‌شود موضوعات زیر در نظر گرفته شود:

الف - امنیت فیزیکی فعلی محل کار از راه دور با احتساب امنیت فیزیکی ساختمان و محیط محلی؛

ب - محیط فیزیکی پیشنهادی کار از راه دور

پ - الزامات امنیت ارتباطات با احتساب نیاز به دسترسی راه دور به سیستم‌های داخلی سازمان، حساسیت اطلاعاتی که مورد دسترسی قرار خواهد گرفت و از لینک های ارتباطی عبور می‌کند و حساسیت سیستم داخلی؛

ت - تهدید دسترسی غیرمجاز به اطلاعات یا منابع از اشخاص دیگر از طریق اسکان، مثلا دوستان و خانواده؛

ث - استفاده از شبکه‌های خانگی و الزامات یا محدودیت‌هایی درباره پیکربندی خدمات شبکه بی سیم؛

ج - خط‌مشی‌ها و روش‌های اجرایی برای جلوگیری از اختلافات درباره حقوق مالکیت مجازی که درباره تجهیزات کاملا خصوصی

چ - دسترسی به تجهیزات خصوصی (برای بررسی امنیت ماشین یا حین یک تجسس) که ممکن است از نظر قانونی ممنوع باشد.

ح - توافقنامه های مجوزهای نرم‌افزاری که به گونه ای هستند که سازمان ممکن است مسوول تایید مجوز برای نرم‌افزارها یا ایستگاه‌های کاری کارفرما باشد که مالکیت آن با کارکنان، پیمانکاران یا کاربران شخص سوم است

خ - محافظت آنتی ویروس و الزامات دیوار آتش

توصیه می‌شود در رهنمودها و ضمائم قرارداد موارد زیر در نظر گرفته شوند:

الف - تهیه تجهیزات مناسب و منابع ذخیره برای فعالیت‌های کار از راه دور، در جایی که استفاده از تجهیزات خصوصی که تحت کنترل سازمان نیست مجاز نیست؛

ب - تعریفی از کار مجاز، ساعات کار، طبقه بندی اطلاعاتی که ممکن است در سیستم‌های داخلی نگه داشته شـود و خدماتی که کاربر راه دور مجاز به دسترسی به آنها است؛

پ - تدارک تجهیزات ارتباطی مناسب، از جمله روش‌هایی برای تامین امنیت دسترسی راه دور

ت - امنیت فیزیکی

ث - قوانین و راهنمایی برای اعضا و دسترسی بازدید کننده به تجهیزات و اطلاعات

ج - تدارک پشتیبانی و نگهداری سخت افزار و نرم‌افزار

چ - تدارک بیمه

ح - روش‌های اجرایی برای پشتیبانی گرفتن از داده‌ها و استمرار کسب وکار

خ - ممیزی و کنترل امنیت

د - پس گرفتن حقوق دسترسی و اجازه و بازگرداندن تجهیزات در زمانی که فعالیت‌های کار راه دور خاتمه می‌یابند.

اطلاعات دیگر

کار راه دور از فن‌آوری ارتباطات برای قادر ساختن پرسنل به کار از راه دور از یک محل ثابت خـارج از سـازمان آنهـا استفاده می‌کند.

۱۲ اکتساب، بهبود، حفظ و نگهداری سیستم‌های اطلاعاتی

۱-۱۲ الزامات امنیتی سیستم‌های اطلاعاتی

هدف: حصول اطمینان از اینکه امنیت، یک جزء جدائی ناپذیر از سیستم‌های اطلاعاتی است.
سیستم‌های اطلاعاتی شامل سیستم‌های عامل، زیرساخت‌ها، برنامه های کاربردی کسب و کار، محصولات در دسترس، خدمات و برنامه های کاربردی توسعه یافته توسط کاربر است. طراحی و پیاده سازی سیستم اطلاعاتی که از فرایند تجاری پشتیبانی می‌کند، می‌تواند برای امنیت حیاتی باشد. توصیه می‌شود الزامات امنیتی قبل از بهبود و/یا پیاده سازی سیستم‌های اطلاعات، شناسایی شده و مورد توافق قرار گیرند.
توصیه می‌شود تمامی الزامات امنیتی در مرحله الزامات یک پروژه شناسایی شده، و به عنوان بخشی از کل حالت کسب و کار برای یک سیستم اطلاعاتی مورد دفاع قرار گرفته، توافق شده و مستند شود.

۱-۱-۱۲ *مشخصات و تحلیل الزامات امنیتی*

کنترل

توصیه می‌شود، بیانه های الزامات کسب وکار برای سیستم‌های اطلاعاتی جدید، یا توسعه سیستم‌های اطلاعاتی موجود، الزاماتی برای کنترل های امنیتی مشخص کنند.

راهنمای پیاده‌سازی

توصیه می‌شود مشخصاتِ الزاماتِ کنترل‌ها، کنترل‌های خودکار را بصورت آمیخته شده در سیستم اطلاعاتی، و نیاز برای پشتیبانی کنترل‌های دستی، در نظر بگیرند. توصیه می‌شود ملاحظات مشابه در زمان ارزشیابی بسته‌های نرم‌افزاری، بهبود یافته یا خریداری شده، برای برنامه های کاربردی کسب وکار به کار گرفته شود.
توصیه می‌شود الزامات و کنترل‌های امنیتی منعکس کننده ارزش کسب وکار دارایی‌های اطلاعاتی درگیر (همچنین به ۷-۲ رجوع کنید)، و آسیب کسب وکار بالقوه، که ممکن است ناشی از خرابی یا فقدان امنیت باشد.
توصیه می‌شود الزامات سیستم برای امنیت اطلاعات و فرایندها برای پیاده سازی امنیت، در مراحل اولیه پروژه‌های سیستم اطلاعات گنجانده شود. کنترل های معرفی شده در مرحله طراحی بصورت قابل توجه کم ارزش تر از پیاده سازی و حفظ آن کنترل هایی هستند که در حین و پس از پیاده سازی گنجانده می‌شوند.
اگر محصولات خریداری شوند، توصیه می‌شود یک فرایند آزمون و اکتساب رسمی، دنبال شود. توصیه می‌شود قراردادها با تامین کننده به الزامات امنیتی شناخته شده اشاره داشته باشند. در جایی که عاملیت امنیت در یک محصول پیشنهادی، الزامات مشخص شده را برآورده نمی‌کند؛ توصیه می‌شود ریسک مطرح شده و کنترل های مربوط، مجددا قبل از خرید محصول، مورد ملاحظه قرار گیرد. در جایی که کارا بودن افزودنی، در جایی که عاملیت افزودنی تامین می‌شود و باعث ایجاد یک ریسک امنیتی می‌شود، توصیه می‌شود این موضوع غیرفعال شود یا توصیه می‌شود ساختار کنترل پیشنهادی مورد بازنگری قرار گیرد تا تعیین که آیا مزیت را می‌توان از عاملیت پیشرفته در دسترس به دست آورد.

اطلاعات دیگر

اگر مثلا به دلایل هزینه ای مناسب در نظر گرفته شود، مدیریت ممکن است بخواهد از محصولاتی که به طور مستقل ارزشیابی و گواهی شده‌اند، استفاده کند. اطلاعات بیشتر درباره معیارهای ارزشیابی برای محصولات امنیتی فن‌آوری

اطلاعات را می‌توان در ISO/IEC 15408 یا دیگر استانداردهای ارزشیابی یا صدور گواهی بطوری که مناسب باشد، پیدا کرد.
ISO/IEC TR 13335-3 راهنمایی‌هایی درباره استفاده از فرایندهای مدیریت ریسک برای شناسایی الزاماتِ کنترل‌های امنیتی فراهم می‌کند.

۱۲-۲ پردازش صحیح در برنامه‌های کاربردی

هدف: پیشگیری از خطاها، گم شدن، دستکاری غیر مجاز یا استفاده نابجا از اطلاعات در برنامه‌های کاربردی.
توصیه می‌شود کنترل‌های مناسب در برنامه های کاربردی از جمله برنامه های کاربردی توسعه یافته توسط کاربر، طراحی شود تا از پردازش صحیح اطمینان حاصل شود. توصیه می‌شود این کنترل‌ها شامل صحه گذاری داده ورودی، پردازش داخلی و داده خروجی باشد.
ممکن است کنترل‌های افزودنی برای سیستم‌هایی که پردازش انجام می دهند، یا پیامدی روی اطلاعات حساس، با ارزش یا حیاتی دارند، لازم باشد. توصیه می‌شود چنین کنترل هایی بر پایه الزامات امنیتی و ارزیابی ریسک تعیین شوند.

۱۲-۲-۱ *صحه‌گذاری داده ورودی*

کنترل
توصیه می‌شود داده ورودی به برنامه‌های کاربردی، اعتباردهی شوند تا از درستی و تناسب این داده اطمینان حاصل شود.
راهنمای پیاده‌سازی
توصیه می‌شود بررسی‌هایی بر روی ورودی تراکنش های کسب وکار، داده دائمی (برای مثال، نام ها و آدرس ها، محدودیت های اعتباری، شماره های ارجاع مشتری)، و جداول پارامتری(برای مثال، قیمت های فروش، نرخ های تبدیل پول رایج، نرخ های مالیات) به کار گرفته شود. توصیه می‌شود رهنمودهای زیر در نظر گرفته شود:

الف - بررسی‌های ورودی دوگانه یا ورودی دیگر، نظیر بررسی مرز یا محدود کردن میدان ها به گستره مشخصی از داده ورودی، تا خطاهای زیر آشکار شود:
۱ - ارزش‌های خارج از گستره
۲ - کاراکترهای غیرمعتبر در میدان‌های داده
۳ - داده مفقودشده یا غیرکامل
۴ - تجاوز کردن از محدوده‌های بالا و پایین حجم داده
۵ - داده کنترلی غیرمجاز یا متناقض

ب - بازنگری دوره‌ای محتوای میدان‌های کلیدی یا فایل های داده برای تایید اعتبار و تمامیت آنها

پ - بازبینی مدارک چاپی ورودی برای تغییرات غیرمجاز (توصیه می‌شود همه تغییرات به مدارک ورودی مجاز باشند)

ت – روش های اجرایی برای پاسخ به خطاهای صحه گذاری

ث - روش های اجرایی برای آزمون معقول بودن داده ورودی

ج - تعریف مسوولیت‌های تمامی پرسنل درگیر در فرایند ورود داده

چ - ایجاد اطلاعات ثبت شده وقایع از فعالیتهای درگیر در فرایند ورود داده (رجوع کنیدبه ۱۰-۱۰-۱)

اطلاعات دیگر

امتحان خودکار و صحه گذاری داده ورودی در جایی که قابل اجرا است، می‌تواند در نظر گرفته شود، تا ریسک خطا ها را کاهش دهد و از حملات استاندارد شامل سرریز حافظه میانجی و تزریق کد جلوگیری بعمل آورد.

۱۲-۲-۲ کنترل پردازش درونی

کنترل

توصیه می‌شود بررسی های صحه گذاری در برنامه های کاربردی گنجانده شود تا هر خرابی اطلاعات درحین پردازش خطاها یا اقدامات عمدی آشکار شود.

راهنمای پیاده‌سازی

توصیه می‌شود طراحی و پیاده سازی برنامه های کاربردی، اطمینان دهد که ریسک های خرابی های پردازش که منجر به از دست رفت تمامیت می‌شود، حداقل شود. نواحی مشخص که مد نظر قرار می‌گیرند عبارتند از:

الف - استفاده از توابع اضاافه کردن، تغییر دادن و حذف برای پیاده سازی تغییرات در داده

ب – روش های اجرایی برای جلوگیری از برنامه هایی که در ترتیب انجام غلط در حال اجرا هستند یا پس از خطا در پردازش قبلی اجرا می‌شوند (همچنین رجوع کنید به بند ۱۰-۱-۱)

پ - استفاده از برنامه های مناسب برای بازیابی خرابی ها بمنظور اطمینان دهی از پردازش صحیح داده

ت - حفاظت در برابر حمله‌هایی که از اجراهای بیش از حد/ سرریزهای حافظه میانجی بهره می‌گیرد.

توصیه می‌شود یک چک لیست مناسب آماده شود، فعالیت‌ها مستند شوند و توصیه می‌شود نتایج امن نگه داشته شوند. مثال‌های بررسی‌هایی که می‌توانند مورد استفاده قرار گیرند عبارتند از:

الف - جلسه یا کنترل‌های گروهی، برای سازگار کردن فایل‌های داده‌ها پس از روزآمد شدن معاملات

ب - کنترل‌های تعادلی برای بررسی تعادل‌ها در مقایسه با تعادل‌های قبلی به عبارت دیگر:

۱ - کنترل‌های اجرا به ا جرا

۲ - کل بروزرسانی فایل ها

۳ - کنترل‌های برنامه به برنامه

پ - صحه گذاری داده‌های ورودی که در سیستم تولید شده اند(رجوع کنید به بند ۱۲-۲-۱):

ت - بررسی درباره یکپارچگی، موثق بودن، یا هر گونه ویژگی امنیتی داده‌ها یا نرم‌افزارهای بارگیری‌شده، یا بارگیری شده، بین رایانه‌های مرکزی و راه دور.

ث - کل سوابق و فایل‌ها بصورت درهم

ج - بررسی‌هایی برای تضمین این که برنامه‌های کاربرد در زمان صحیح اجرا می‌شوند

چ - بررسی‌هایی برای تضمین این که برنامه‌ها با ترتیب صحیح اجرا می‌شوند و در صورت بروز خطا پایان می‌یابند و این که پردازش بیشتر تا زمانی که مشکل حل شود متوقف می‌شود.

ه - ایجاد اطلاعات ثبت شده از فعالیت‌های موجود در پردازش(رجوع کنید به بند ۱۰-۱۰-۱)

اطلاعات دیگر

داده‌هایی که به درستی وارد شده اند ممکن است از طریق خطاهای سخت افـزاری، خطاهـای پـردازش یـا از طریـق فعالیت‌های عمدی مختل شوند. بررسی‌های اعتباردهی موردنیاز به ماهیت کاربرد و پیامد کسب وکار هر گونه اختلال در داده‌ها بستگی خواهد داشت.

۱۲-۲-۳ تمامیت پیغام

کنترل

توصیه می‌شود الزاماتی برای اطمینان از سندیت و حفاظت از یکپارچگی پیغام در برنامه‌های کاربردی، شناسایی شده و کنترل‌های مناسبی شناسایی و پیاده‌سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود ارزیابی ریسک‌های امنیتی برای تعیین این که آیا یکپارچگی پیام لازم است و برای شناسایی مناسـب ترین روش اجرا انجام شود.

اطلاعات دیگر

روشهای رمزنگاری(رجوع کنید به بند ۱۲-۳) را می‌توان به عنوان ابزار مناسبی برای اجرای تعیین اعتبار پیـام مـورد استفاده قرار داد.

۱۲-۲-۴ صحه‌گذاری داده خروجی

کنترل

توصیه می‌شود به منظور حصول اطمینان از اینکه پردازش اطلاعات ذخیره شده، صحیح بوده و شرایط مناسبی دارد، داده‌های خروجی برنامه‌های کاربردی، صحه‌گذاری شوند.

راهنمای پیاده‌سازی

صحه‌گذاری خروجی ممکن است شامل موارد زیر باشد:

الف - بررسی‌های امکان پذیری برای آزمون این که آیا داده‌های خروجی معقول هستند:

ب - هماهنگ کردن حساب‌های کنترلی برای تضمین پردازش تمام داده‌ها

پ – ارایه اطلاعات کافی برای یک خواننده یا سیستم پردازش متعاقب آن برای تعیـین دقـت، کامـل بـودن، و طبقه بندی اطلاعات

ت - روش‌های اجرایی برای پاسخگویی به آزمون‌های صحه‌گذاری خروجی

ث - تعریف مسوولیت‌های تمام اشخاص دخیل در فرایند خروجی داده‌ها

ج - ایجاد اطلاعات ثبت شده از فعالیت‌ها در فرایند صحه‌گذاری خروجی داده‌ها

اطلاعات دیگر

معمولا سیستم‌ها و کاربردها با این فرض ساخته می‌شوند که پس از گذراندن صحه‌گذاری، تصـدیق، و آزمـون لازم و مناسب، نتیجه همیشه صحیح خواهد بود. به هر حال، این فرض همیشه معتبر نیست، به عبارت دیگر سیسـتم‌هـایی که آزموده شده اند ممکن است با این حال در بعضی شرایط خروجی نادرستی بدهند.

۱۲-۳ کنترل‌های رمزنگاری

هدف: حفاظت از محرمانگی، سندیت یا یکپارچگی اطلاعات، توسط مفاهیم رمزنگاری.
توصیه می‌شود یک خط‌مشی درباره استفاده از کنترل‌های رمزنگاری طراحی شود. توصیه می‌شود مدیریت کلیدی برای پشتیبانی از استفاده از روشهای رمزنگاری به کار گرفته شود.

۱۲-۳-۱ خط‌مشی استفاده از کنترل‌های رمزنگاری

کنترل

توصیه می‌شود برای حفاظت از اطلاعات، یک خط‌مشی استفاده از کنترل‌های رمزنگاری، ایجاد و پیاده‌سازی شود.

راهنمای پیاده‌سازی

توصیه می‌شود در زمان توسعه یک خط‌مشی رمز نگاری موارد زیر در نظر گرفته شود:

الف - رویکرد مدیریت در قبال استفاده از کنترل‌های رمزنگاری در سازمان، از جمله اصول کلی که توصیه می‌شود اطلاعات کسب وکار تحت آن محافظت شود(همچنین رجوع کنید به بند ۵-۱-۱)

ب - بر اساس یک ارزیابی ریسک، توصیه می‌شود سطح مورد نیاز محافظت با احتساب نوع، مقاومت، و کیفیت الگوریتم رمزنگاری مورد نیاز شناسایی شود.

پ - استفاده از رمزنگاری برای محافظت از اطلاعات حساس که توسط رسانه‌های سیار یا قابل جابجایی، دستگاه‌ها یا خطوط ارتباطی حمل می‌شود.

ت - رویکرد در قبال مدیریت کلیدی، از جمله روش‌هایی برای پرداختن به محافظت از کلیدهای رمزنگاری و بازیابی اطلاعات رمزنگاری شده در صورت آسیب، خدشه یا صدمه

ث - نقش‌ها و مسوولیت‌ها مثلا این که چه کسی مسوول موارد زیر است:

۱ - اجرای خط‌مشی

۲ - مدیریت کلیدی از جمله تولید کلید (همچنین رجوع کنید به بند ۱۲-۳-۲)

ج - استانداردهایی که باید برای اجرای موثر در تمام سازمان مورداستفاده قرار گیرد. (که چه راه حلی برای چه فرایندهای کسب وکار استفاده می‌شود)

چ –پیامد استفاده از اطلاعات رمزنگاری شده درکنترل‌هایی که بر بررسی محتوا تکیه دارند. (برای مثال، آشکارسازی ویروس)

توصیه می‌شود در زمان اجرای خط مشی رمزنگاری سازمان، به مقررات و محدودیت‌های ملی که ممکن است در مورد استفاده از روشهای رمزنگاری در بخش‌های مختلف جهان اعمال شود و نیز به مسائل جریان گسترده اطلاعات رمزنگاری شده ملاحظه شود(همچنین رجوع کنید به بند ۱۵-۱-۶).

کنترل‌های رمزنگاری را می‌توان برای دستیابی به اهداف امنیت اطلاعات مورد استفاده قرار داد مثلا:

الف- محرمانگی: استفاده از رمزنگاری اطلاعات برای محافظت از اطلاعات حساس و حیاتی خواه ذخیره شده خواه منتقل شده؛

ب - یکپارچگی/موثق بودن: استفاده از امضاهای دیجیتال یا کدهای تایید پیام برای محافظت از موثق بودن و یکپارچگی اطلاعات حساس یا حیاتی ذخیره شده یا منتقل شده؛

پ - عدم انکار: استفاده از روش‌های رمز نگاری برای به دست آوردن شاهدی بر وقوع یا عدم وقوع یک واقعه یا فعالیت

اطلاعات دیگر

توصیه می‌شود تصمیم گیری درباره این که آیا راه حل رمزنگاری مناسب است، به عنوان بخشی از فرایند گسترده تر ارزیابی خطر و انتخاب کنترل‌ها در نظر گرفته شوند. این ارزیابی را سپس می‌توان برای تعیین این که آیا کنترل رمزنگاری مناسب است یا نه، چه نوع کنترلی توصیه می‌شود که به کار گرفته شود و برای کدام اهداف و فرایندهای کسب وکار به کار گرفته شود انجام داد.

سیاستی درباره استفاده از کنترل‌های رمزنگاری برای افزایش منافع و کاهش ریسک‌ها استفاده از روشهای رمزنگاری و اجتناب از استفاده نامناسب یا غیرصحیح لازم است. توصیه می‌شود در زمان استفاده از امضاهای دیجیتال به هر گونه قوانین مربوطه به خصوص قوانینی که شرایطی را توصیف می‌کنند که تحت آن، امضای دیجیتال قانونا الزام آور است ملاحظه شود(رجوع کنید به بند ۱۵-۱).

توصیه می‌شود مشاوره تخصصی برای شناسایی سطح مناسب محافظت و تعریف مشخصات مناسبی که محافظت مورد نیاز را ارایه خواهند کرد و اجرای یک سیستم مدیریت کلیدی ایمن را پشتیبانی خواهندکرد انجام شود.

ISO/IEC JTC1 SC27 چندین استاندارد را در رابطه با کنترل‌های رمزنگاری طراحی کرده است. اطلاعات بیشتر را همچنین می‌توانید در IEEE P1363 و رهنمودهای OECD در باره رمزنگاری پیدا کنید. (همچنین رجوع کنید به بند ۱۲-۳-۲)

۱۲-۳-۲ مدیریت کلید

کنترل

توصیه می‌شود به منظور پشتیبانی استفاده سازمان از فنون رمزنگاری، یک سیستم مدیریت کلید ایجاد شود.

راهنمای پیاده‌سازی

توصیه می‌شود تمام کلیدهای رمزنگاری در مقابل تغییر، آسیب و خرابی محافظت شوند. به علاوه، کلیدهای رمزی و خصوصی نیازمند محافظت در برابر دسترسی غیرمجاز دارند. توصیه می‌شود تجهیزات به‌کار رفته برای تولید ذخیره، و بایگانی کلیدها از نظر فیزیکی محافظت شود.

توصیه می‌شود یک سیستم مدیریت کلیدی بر اساس مجموعه مورد توافق استانداردها، رویه‌ها و روش‌های امن باشد برای:

الف - تولید کلید برای سیستم‌های رمزنگاری مختلف و کاربردهای مختلف

ب - تولید و به دست آوردن گواهینامه های کلیدی همگانی

پ - توزیع کلیدها بین کاربرهای مورد نظر از جمله این که توصیه می‌شود کلیدها چگونه در زمان دریافت فعال شوند؛

ت - ذخیره کلیدها از جمله این که چگونه کاربران مجاز به کلیدها دسترسی پیدا می‌کنند؛

ث - تغییر یا روزآمد کردن کلیدها از جمله نقش‌ها درباره این که توصیه می‌شود چه زمانی کلیدها تغییر کنند و این کار چگونه باید انجام شود.

ج - رسیدگی به کلیدهای خدشه واردشده

چ - پس گرفته کلیدها از جمله این که توصیه می‌شود چگونه کلیدها مسترد شوند یا غیرفعال شوند، مثلا زمانی که کلیده‌ها مورد آسیب قرار گرفته اند یا زمانی که یک کاربر از سازمان می رود. (در چه حالتی توصیه می‌شود که کلیدها بایگانی شوند)

ح - بازیابی کلیدهایی که گم می‌شوند یا مختل می‌شوند به عنوان بخشی از مدیریت استمرار کسب وکار مثلا برای بهبود اطلاعات رمزنگاری شده

خ - بایگانی کلیدها مثلا برای اطلاعات بایگانی شده یا کپی پشتیبان گرفته شده

د - تخریب کلیدها

ذ - واقعه نگاری و ممیزی فعالیت‌های مرتبط با مدیریت کلید

توصیه می‌شود به منظور کاهش احتمال آسیب، فعالی سازی و غیرفعال سازی، تاریخ‌هایی برای کلیدها تعریف شوند تا کلیدها را فقط بتوان برای دوره محدودی از زمان مورد استفاده قرار داد. توصیه می‌شود دوره زمان وابسته به شرایطی باشد که کنترل رمزنگاری تحت آن مورد استفاده قرار می‌گیرد.

علاوه بر مدیریت مطمئن کلیدهای خصوصی و رمزی، توصیه می‌شود اصیل بودن کلیدهای عمومی نیز در نظر گرفته شود. این فرایند احراز اصالت می‌تواند با استفاده از گواهینامه های کلید عمومی که معمولا توسط یک مرجع دارای اختیار صدور گواهی صادر می‌شود، -که توصیه می‌شود یک نهاد به رسمیت شناخته شده با کنترل ها و روش های اجرایی مناسب و بجا برای تامین درجه اطمینان مورد نیاز باشد-؛ انجام شود.

توصیه می‌شود محتوای قراردادها یا توافق‌نامه های سطح خدمات با تامین کنندگان بیرونی خدمات رمزنگاری - مثلا با یک مرجع دارای اختیار صدور گواهی-، موضوعات مسوولیت، اطمینانِ از خدمات، و زمان های پاسخ برای فراهم کردن خدمات را پوشش دهد(رجوع کنید به بند ۶-۲-۳).

اطلاعات دیگر

مدیریت کلیدهای رمزنگاری برای استفاده موثر از روشهای رمزنگاری لازم است.

ISO/IEC 11770 اطلاعات بیشتری را درباره مدیریت کلید ارایه می‌کند. دو نوع تکنیک رمزنگاری عبارتند از:

الف - روشهای کلید رمزی، در جایی که دو یا چند طرف، یک کلید را در اشتراک دارند و این کلید هم برای رمزنگاری و هم برای رمزگشای اطلاعات مورد استفاده قرار می‌گیرد. این کلید باید سری نگه داشته شود زیرا هر کسی که به کلید دسترسی داشته باشد می‌تواند تمام اطلاعاتی را که با آن کلید رمزنگاری می‌شود رمزگشایی کند یا اطلاعات غیرمجاز را با استفاده از کلید عرضه کند:

ب - روشهای کلید همگانی که در آن هر کاربر یک جفت کلید دارد؛ یک کلید همگانی و یک کلید خصوصی(که باید محرمانه نگهداری شود)؛ روشهای کلید همگانی را می‌توان برای رمزنگاری و تولید امضاهای دیجیتال مورد استفاده قرار داد (همچنین رجوع کنید به ISO/IEC 9796 و ISO/IEC 14888)

تهدید جعل یک امضای دیجیتال با جایگزین کردن یک کلید همگانی کاربر وجود دارد. این مشکل با استفاده از یک گواهینامه کلید همگانی مورد رسیدگی قرار می‌گیرد.

روشهای رمزنگاری را همچنین می‌توان برای محافظت از کلیدهای رمزنگاری مورد استفاده قرار داد. روش‌های اجرایی ممکن است برای پرداختن به تقاضاهای دسترسی به کلیدهای رمزنگاری وجود داشته باشد مثلا ممکن است لازم باشد اطلاعات رمزنگاری شده به شکلی رمزنگاری نشده مانند مدرکی در یک دادگاه در دسترس قرار گیرند.

۱۲-۴ امنیت فایل های سیستم

هدف: حصول اطمینان از امنیت پرونده‌های سیستم.
توصیه می‌شود دسترسی به فایل‌های سیستم و کد منبع برنامه کنترل شوند و پروژه‌های فن‌آوری اطلاعات و فعالیت‌های پشتیبانی به گونه‌ای ایمن انجام شوند. توصیه می‌شود مراقبت شود که از قرارگرفتن داده حساس در محیط‌های آزمون اجتناب شود.

۱۲-۴-۱ کنترل نرم‌افزار عملیاتی

کنترل
توصیه می‌شود به منظور کنترل نصب نرم‌افزار بر روی سیستم‌های عملیاتی، روش‌های اجرایی ایجاد شوند.
راهنمای پیاده‌سازی
توصیه می‌شود به منظور کاهش خطر اختلال در سیستم‌های عملیاتی رهنمودهای زیر، برای کنترل تغییرات در نظر گرفته شوند:

الف - توصیه می‌شود روزآمدسازی نرم‌افزار عملیاتی، عملکردها، و کتابخانه‌های برنامه فقط توسط مجریان آموزش دیده پس از تایید مدیریتی مناسب انجام شود(رجوع کنید به بند ۱۲-۴-۳)

ب - توصیه می‌شود سیستم‌های عملیاتی فقط کد قابل‌اجرای تایید شده را در اختیار بگیرند و نه کد توسعه یا همگردان‌ها را.

پ- توصیه می‌شود برنامه های کاربردی و نرم‌افزار سیستم عامل فقط پس از آزمون گسترده و موفقیت آمیز اجرا شود؛ توصیه می‌شود آزمون‌ها شامل آزمون‌هایی درباره قابل استفاده بودن، امنیت، تاثیرات بر دیگر سیستم‌ها و مناسب نبودن برای کاربر باشند و توصیه می‌شود درباره سیستم‌های جداگانه انجام شوند(رجوع کنید به بند ۱۰-۱-۴)؛ توصیه می‌شود تضمین شود که تمام کتابخانه‌های منبع برنامه متناظر روزآمد شده اند؛

ت - توصیه می‌شود سیستم کنترل پیکربندی برای حفظ کنترل تمام نرم‌افزارهای اجرا شده و نیز مستندات سیستم مورد استفاده قرار گیرند.

ث - توصیه می‌شود یک راهبرد کاهنده قبل از اجرای تغییرات در نظر گرفته شود.

ج - توصیه می‌شود اطلاعات ثبت شده حسابرسی از تمام روزآمدسازی‌های کتابخانه‌های برنامه عملیاتی نگهداری شود

چ - توصیه می‌شود نسخه‌های قبلی نرم‌افزار عملکرد، به عنوان یک اقدام همسوسازی حفظ شود.

ح - توصیه می‌شود نسخه‌های قدیمی نرم‌افزار، به همراه اطلاعات مورد نیاز و پارامترها، رویه‌ها، جزئیات پیکربندی، و نرم‌افزار پشتیبان برای مدت زمانی که داده‌ها در آرشیو نگهداری می‌شوند ذخیره شوند.

توصیه می‌شود نرم‌افزارهای تامین شده توسط فروشندگان که در سیستم‌های عملیاتی مورد استفاده قرار گرفتند، در سطح پشتیبانی شده توسط تامین کننده نگهداری شوند. با گذشت زمان، فروشندگان نرم‌افزار نسخه‌های قدیمی تر نرم‌افزار را پشتیبانی نمی‌کنند. توصیه می‌شود سازمان ریسک‌ها تکیه بر نرم‌افزار پشتیبانی نشده را در نظر بگیرد.

توصیه می‌شود هر تصمیمی برای روزآمدسازی به یک نسخه جدید الزامات کسب وکار را برای تغییر و امنیت نسخه جدید به حساب آورد، به عبارت دیگر معرفه یک کارایی جدید امنیتی یا تعداد و شدت مشکلات امنیتی که بر این مدل تاثیر می گذارند. توصیه می‌شود بسته‌های نرم‌افزاری در زمانی که می‌توانند به از بین بردن یا کاهش ضعف‌های امنیتی کمک کنند به کار گرفته شوند(همچنین رجوع کنید به بند ۱۲-۶-۱).

توصیه می‌شود دسترسی فیزیکی یا منطقی فقط به تامین کنندگان برای اهداف پشتیبانی در زمان لازم و با تایید مدیریت داده شود. توصیه می‌شود فعالیت‌های تامین کننده کنترل شوند.

نرم‌افزار رایانه‌ی ممکن است بر نرم‌افزارو مدول‌های ارایه شده از خارج تکیه داشته باشند که توصیه می‌شود برای اجتناب از تغییرات غیرمجازکه ممکن است ضعف‌های امنیتی ایجاد کند کنترل شوند.

اطلاعات دیگر

توصیه می‌شود سیستم‌های عامل فقط زمانی که لازم است روزآمد شوند مثلا اگر نسخه فعلی سیستم عامل دیگر الزامات کسب وکار را پشتیبانی نمی‌کند. توصیه می‌شود روزآمدسازی‌ها فقط به این دلیل که نسخه جدیدی از سیستم عامل موجود است رخ ندهند. نسخه‌های جدید سیستم‌های عامل ممکن است امنیت کمتری داشته باشندو کمتر از سیستم‌های فعلی درک شوند.

۱۲-۴-۲ *حفاظت از داده‌های آزمون سیستم*

کنترل

توصیه می‌شود داده‌های آزمون، به دقت انتخاب شده، محافظت و کنترل شوند.

راهنمای پیاده‌سازی

توصیه می‌شود استفاده از بانک‌های داده عملیاتی که حاوی اطلاعات شخصی است یا هر اطلاعات حساس دیگر برای اهداف آزمون اجتناب شود. اگر اطلاعات شخصی یا به هر جهت حساس برای اهداف تست(آزمون) مورد استفاده قرار گیرد، توصیه می‌شود تمام جزئیات حساس و محتوای حساس قبل از استفاده حذف شوند یا تغییر کنند. توصیه می‌شود رهنمودهای زیر برای محافظت از داده‌های عملیاتی زمانی که برای اهداف آزمونی له کار می روند به کار گرفته شود:

الف - رویه‌های کنترل دسترسی که در سیستم‌های کاربرد عملیاتی مورد استفاده قرار می‌گیرند نیز توصیه می‌شود در سیستم‌های آزمون عملکرد قرار گیرند.

ب - توصیه می‌شود هر زمان که اطلاعات عملیاتی روی یک سیستم عملیاتی آزمون کپی می‌شود مجوز جداگانه ای لازم باشد

پ - توصیه می‌شود اطلاعات عملیاتی از یک سیستم عملیاتی آزمون بلافاصله پس از کامل شدن آزمون حذف شوند.

ت - توصیه می‌شود کپی کردن و استفاده از اطلاعات عملیاتی واقعه‌نگاری شود تا بعنوان داده ممیزی در دسترس قرار گیرد.

اطلاعات دیگر

آزمون پذیرش و سیستم معمولا نیازمند حجم‌های مهمی از داده‌های آزموده هستند که تا حد امکان به داده‌های عملیاتی نزدیک هستند.

۱۲-۴-۳ کنترل دسترسی به کد منبع برنامه

کنترل

توصیه می‌شود دسترسی به کد منبع برنامه، محدود شود.

راهنمای پیاده‌سازی

توصیه می‌شود دسترسی به کد منبع برنامه و موارد مربوطه (مانند طراحی ها، مشخصات، طرح های تصدیق، طرح های صحه گذاری)، شدیدا کنترل شود تا از امکان کارایی غیرمجاز جلوگیری شود و از تغییرات غیرعمدی اجتناب شود. برای کد منبع برنامه، این را می‌توان از طریق ذخره مرکزی کنترل شده این کد، ترجیحا در کتاب‌خانه‌های منبع برنامه به دست آورد. رهنمودهای زیر، باید برای کنترل دسترسی به این کتابخانه‌های منبع برنامه به منظور کاهش پتانسیل اختلال برنامه‌های رایانه‌ی در نظر گرفته شوند(همچنین رجوع کنید به ۱۱):

الف - توصیه می‌شود در هر جایی که ممکن باشد، کتابخانه‌های منبع برنامه در سیستم‌های عملیاتی نگهداری نشوند

ب - توصیه می‌شود کد منبع برنامه و کتابخانه‌های منبع برنامه مطابق با رویه‌های تثبیت شده مدیریت شوند

پ - توصیه می‌شود پرسنل پشتیبانی دسترسی نامحدود به کتابخانه‌های منبع برنامه نداشته باشند.

ت - توصیه می‌شود روزآمدسازی کتابخانه‌های منبع برنامه و زمان‌های مربوطه، و صدور منابع برنامه برای برنامه ریزها فقط پس از دریافت تایید مناسب انجام شوند.

ث - توصیه می‌شود فهرست‌های برنامه در یک محیط ایمن نگهداری شوند. (رجوع کنید به بند ۱۰-۷-۴)

ج - توصیه می‌شود اطلاعات ثبت شده حسابرسی از تمام دسترسی‌ها به کتابخانه‌های منبع برنامه نگهداری شوند

چ - توصیه می‌شود نگهداری و کپی کتابخانه‌های منبع برنامه منوط به رویه‌های شدید کنترل تغییر باشد(رجوع کنید به بند ۱۲-۵-۱)

اطلاعات دیگر

کد منبع برنامه کدی است که توسط برنامه نویس‌ها نوشته می‌شود و برای ایجاد موارد قابل‌اجرا تدوین (و پیوند) می‌شود. زبان‌های برنامه نویسی خاص به طور رسمی بین کد منبع و موارد قابل‌اجرا تمایز قائل نمی‌شوند زیرا قابل‌اجراها در زمانی که فعال می‌شوند ایجاد می‌شوند.

استانداردهای ISO10007 و ISO/IEC 12207 اطلاعات بیشتری را درباره مدیریت پیکربندی و فرایند چرخه نرم‌افزار ارایه می‌کنند.

۱۲-۵ امنیت در فرایندهای بهبود و پشتیبانی

هدف: حفظ امنیت نرم‌افزار و اطلاعات سیستم کاربردی.

توصیه می‌شود محیط‌های پروژه و پشتیبانی شدیدا کنترل شوند.

توصیه می‌شود مدیرانی که مسئول سیستم‌های کاربرد هستند مسوول امنیت پروژه یا محیط پشتیبانی باشند.

توصیه می‌شود آنها تضمین کنند که تمام تغییرات سیستم‌های پیشنهادی بررسی می‌شوند تا بررسی شود که آنها به امنیت سیستم یا محیط عملکرد خدشه وارد نمی‌کنند.

۱۲-۵-۱ روش‌های اجرایی کنترل تغییر

کنترل

توصیه می‌شود با استفاده از روش‌های اجرایی رسمی کنترل تغییر، پیاده‌سازی تغییرات کنترل شوند.

راهنمای پیاده‌سازی

توصیه می‌شود رویه‌های کنترل تغییرات رسمی به منظور کاهش اختلال سیستم‌های اطلاعاتی مستند و اجرا شوند.

توصیه می‌شود عرضه سیستم‌های جدید و تغییرات عمده در سیستم‌های فعلی یک فرایند رسمی مستندسازی، مشخص سازی، آزمون، کنترل کیفیت و اجرای مدیریت شده را دنبال کند.

توصیه می‌شود این فرایند شامل یک ارزیابی ریسک، تحلیل پیامدهای تغییرات، و مشخصات کنترل‌های امنیتی موردنیاز باشد. توصیه می‌شود این فرایند همچنین تضمین نماید که رویه‌های فعلی امنیت و کنترل، مختل نمی‌شوند و برنامه نویس‌ها دسترسی را فقط به بخش‌هایی از سیستم دارند که برای کارشان لازم است و این که قرارداد و تایید رسمی برای هر تغییر کسب می‌شود.

توصیه می‌شود در صورت امکان، رویه‌های تغییر عملیاتی و عملکرد یکپارچه باشند(همچنین رجوع کنید به بند ۱۰-۱-۲). توصیه می‌شود رویه‌های تغییرات شامل موارد زیر باشند:

الف - حفظ گزارشی از سطوح تایید مورد توافق

ب - تضمین تغییرات توسط کاربران مجاز ارایه می‌شوند.

پ - بررسی کنترل‌ها و رویه‌های یکپارچگی برای تضمین این که آنها بواسطه تغییرات مختل نخواهند شد.

ت- شناسایی همه نرم‌افزارها، اطلاعات، موجودیت های بانک داده، و سخت افزار که اصلاحاتی را نیاز دارند.

ث - به دست آوردن تایید رسمی برای پیشنهادهای مفصل قبل از آغاز کار

ج - تضمین این که کاربران مجاز تغییرات را قبل از اجرای آنها می پذیرند.

چ - تضمین این که مجموعه مستندسازی سیستم پس از تکمیل هر تغییر روزآمد می‌شود و این که مستندسازی بایگانی می‌شود یا دور ریخته می‌شود

ح - حفظ یک نسخه کنترل برای تمام روزآمدسازی‌های نرم‌افزار

خ - حفظ یک گزارش ممیزی از تمام تقاضاهای تغییرات

د - تضمین این که مستندسازی عملیات(رجوع کنید به بند ۱۰-۱-۱) و رویه‌های کاربر در زمان لازم تغییر می‌کنند تا مناسب باقی بمانند.

ذ - تضمین این که اجرای تغییرات در زمان صحیح رخ می‌دهد و فرایندهای کسب وکار مربوطه را مختل نمی‌کند

اطلاعات دیگر

تغییر نرم‌افزار می‌تواند بر محیط عملیاتی تاثیر بگذارد.

عملکرد خوب شامل آزمون نرم‌افزار جدید در محیطی است که هم از محیط تولید و هم از محیط توسعه جدا شده باشد(همچنین رجوع کنید به بند ۱۰-۱-۴). این ابزاری برای کنترل بر نرم‌افزار جدید و ایجاد محافظت اضافه اطلاعات عملیاتی که برای اهداف آزمون مورد استفاده قرار می‌گیرد ایجاد می‌کند. توصیه می‌شود این شامل بسته‌های خدمات، و دیگر روزآمدسازی‌ها باشد. توصیه می‌شود روزآمدسازی‌های اتوماتیک در سیستم‌های حیاتی انجام نشوند زیرا بعضی روزآمدسازی‌ها ممکن است باعث ایجاد مشکل در کاربردهای حیاتی شوند (رجوع کنید به بند ۱۲-۶)

۱۲-۵-۲ بازنگری فنی نرم‌افزارهای کاربردی پس از تغییرات سیستم عامل

کنترل

توصیه می‌شود در هنگام تغییر سیستم‌های عامل، به منظورحصول اطمینان از عدم وجود پیامد سوء بر عملیات یا امنیت سازمانی، نرم‌افزارهای کاربردی حیاتی کسب‌وکار بازنگری و آزموده شوند.

راهنمای پیاده‌سازی

توصیه می‌شود این فرایند موارد زیر را پوشش دهد:

الف - بررسی کنترل کاربرد و رویه‌های یکپارچگی برای تضمین این که آنها از طریق تغییرات در سیستم عامل مختل نشده‌اند.

ب - تضمین این که برنامه و بودجه پشتیبانی سالانه بررسی‌ها و آزمون سیستم را که از تغییرات سیستم عامل ناشی می‌شوند پوشش خواهد داد.

ت - تضمین این که اعلام تغییرات سیستم عامل به موقع انجام می‌شود تا آزمون‌ها و بررسی‌های مناسب قبل از اجرا امکان پذیر شوند.

ث - تضمین این که تغییرات مناسب در برنامه‌های استمرار کسب وکار انجام می‌شوند(رجوع کنید به بند ۱۴).

توصیه می‌شود یک گروه یا فرد خاص مسوولیت کنترل آسیب‌پذیری‌ها و پخش بسته‌ها توسط فروشنده را به عهده داشته باشد (رجوع کنید به بند ۱۲-۶).

۱۲-۵-۳ محدودسازی در اعمال تغییرات در بسته‌های نرم‌افزاری

کنترل

توصیه می‌شود از دستکاری در بسته‌های نرم‌افزاری، اجتناب شده، محدود به تغییرات ضروری باشد، و توصیه می‌شود تمامی تغییرات به شدت کنترل شوند.

راهنمای پیاده‌سازی

توصیه می‌شود تا حد امکان بسته‌های نرم‌افزاری تهیه شده توسط فروشندگان بدون تغییر مورد استفاده قرار گیرد.

توصیه می‌شود هر زمان که یک بسته نرم‌افزاری تغییر کند، نکات زیر باید رعایت شود:

الف - خطر کنترل‌های درونی و فرایندهای یکپارچه ای که مختل می‌شوند

ب - توصیه می‌شود این که آیا رضایت فروشنده کسب شود یا نه

پ - احتمال دریافت تغییرات لازم از فروشنده به صورت روزآمدسازی‌های برنامه استاندارد

ت –پیامد این که اگر سازمان مسوول نگهداری نرم‌افزار در نتیجه تغییر در آینده شود

اگر تغییرات لازم باشد توصیه می‌شود نرم‌افزار اصلی تهیه شود و تغییرات به یک نسخه ای که کاملا شناسایی شده است اعمال شود. یک فرآیند مدیریت روزآمدسازی نرم‌افزار، توصیه می‌شود برای تضمین این که روزآمدترین بسته‌های تایید شده و روزآمدسازی‌های کاربرد برای تمام نرم‌افزار مجاز نصب می‌شوند اجرا شود(رجوع کنید به بند ۱۲-۶). توصیه می‌شود تمام تغییرات به طور کامل آزموده و مستند شود به گونه ای که آنها را بتوان در صورت لزوم در روزآمدسازی‌های نرم‌افزاری آینده مجددا به کار برد. در صورت لزوم، توصیه می‌شود تغییرات توسط یک نهاد ارزیابی مستقل آزموده و اعتبار بخشی شود.

۱۲-۵-۴ نشت اطلاعات

کنترل

توصیه می‌شود از فرصتهای نشت اطلاعات، پیشگیری شود.

راهنمای پیاده‌سازی

توصیه می‌شود موارد زیر برای محدود کردن ریسک نشت اطلاعات مثلا از طریق استفاده از کانال‌های مخفی در نظر گرفته شود:

الف - جستجوی رسانه‌ها و ارتباطات خارج از باند برای اطلاعات مخفی

ب – پنهان کردن و مدوله کردن سیستم و رفتار ارتباطات برای کاهش احتمال این که یک شخص سوم بتواند اطلاعات را از چنین رفتاری استنباط کند

پ - استفاده از سیستم‌ها و نرم‌افزاری که یکپارچگی بالایی دارند مثلا استفاده از محصولات ارزیابی شده (رجوع کنید به بند ISO/IEC 15408)

ت - کنترل منظم فعالیت‌های پرسنل و سیستم در صورت مجاز بودن تحت مقررات موجود

ث - کنترل استفاده از منابع در سیستم‌های رایانه‌ی

اطلاعات دیگر

کانال‌های پنهان مسیرهایی هستند که هدف از ایجادشان هدایت جریان اطلاعات ناست اما ممکنم است با این حال در یک سیستم یا یک شبکه وجود داشته باشند. مثلا دستکاری بیت‌ها در بسته‌های پروتکل ارتباطات را می‌توان به عنوان روشی مخفی برای سیگنال دهی مورد استفاده قرار داد. به دلیل ماهیت شان، پیشگیری از وجود تمام کانال‌های پنهان اگر غیرممکن نباشد مشکل خواهد بود. به هر حال استفاده از این کانال‌ها اغلب توسط کد تروجان انجام می‌شود(همچنین رجوع کنید به بند ۱۰-۴-۱). بنابراین اقداماتی برای محافظت از کد تروجان ریسک استفاده از کانال‌های پنهان را کاهش می‌دهد.

پیشگیری از دسترسی غیرمجاز به شبکه(۱۱-۴) و نیز سیاست‌ها و رویه‌های جلوگیری از سوء استفاده از خدمات اطلاعات توسط پرسنل(۱۵-۱-۵) به محافظت دربرابر کانال‌های پنهان کمک می‌کند.

۱۲-۵-۵ بهبود نرم‌افزار برون‌سپاری شده

کنترل

توصیه می‌شود توسعهٔ نرم‌افزار برون‌سپاری شده، توسط سازمان، نظارت و پایش شود.

راهنمای پیاده‌سازی

در جایی که توسعه نرم‌افزار از بیرون تامین می‌شود، توصیه می‌شود نکات زیر مد نظر قرار گیرد:

الف - تایید قراردادها، مالکیت کد، و حقوق مالکیت فکری (رجوع کنید به بند ۱۵-۱-۲)

ب – گواهی کردن کیفیت و دقت و صحت کار انجام شده

پ - مدیریت وجه الضمان‌ها در صورت کوتاهی شخص سوم

ت - حقوق دسترسی برای ممیزی کیفیت و دقت کار انجام شده

ث - الزامات قراردادی برای کارایی کیفیت و امنیت کد

ج - آزمون قبل از نصب برای کشف کد نامناسب و تروجان

۱۲-۶ مدیریت آسیب‌پذیری فنی

هدف: کاهش مخاطرات منتج از سوء استفاده از آسیب‌پذیری‌های فنی منتشر شده.
توصیه می‌شود مدیریت آسیب‌پذیری فنی به گونه ای موثر، سیستماتیک و قابل تکرار با اقدامات انجام شده در جهت تایید تاثیر آن انجام شود. توصیه می‌شود این ملاحظات شامل سیستم‌های عامل، و هر کاربرد دیگری که در حال استفاده است باشند.

۱۲-۶-۱ کنترل آسیب‌پذیری‌های فنی

کنترل

اطلاعات بهنگام در خصوص آسیب پذیری‌های فنی سیستم‌های اطلاعاتی مورد استفاده، توصیه می‌شود که کسب شده، قرار گرفتن سازمان در معرض چنین آسیب‌پذیری‌هایی ارزیابی شده، و معیارهای مناسبی برای نشان دهی ریسک‌ها مربوطه، برگزیده شوند.

راهنمای پیاده‌سازی

یک لیست موجودی جدید و کامل از دارایی‌ها(رجوع کنید به بند ۷-۱) پیش نیاز مدیریت موثر آسیب‌پذیری فنی است. اطلاعات خاص مورد نیاز برای پشتیبانی مدیریت آسیب‌پذیری فنی شامل فروشنده نرم‌افزار، تعداد نسخه‌ها، وضعیت فعلی استقرار (برای مثال چه نرم‌افزاری روی چه سیستمی نصب می‌شود)، و شخص یا اشخاص دخیل در سازمان که مسوول نرم‌افزار هستند است.

توصیه می‌شود فعالیت مناسب و به موقع در پاسخ به شناسایی آسیب پریری‌های فنی بالقوه صورت گیرد. توصیه می‌شود راهنمایی‌های زیر برای تثبیت یک فرایند مدیریت موثر برای آسیب‌پذیری‌های فنی دنبال شوند:

الف - توصیه می‌شود سازمان نقش‌ها و مسوولیت‌های مربوط به مدیریت آسیب‌پذیری فنی از جمله کنترل آسیب‌پذیری، ارزیابی ریسک آسیب‌پذیری، بسته بندی، ردیابی دارایی‌ها، و هر هماهنگی مورد نیاز را تعریف و ایجاد کند.

ب - منابع اطلاعات که برای شناسایی آسیب‌پذیری‌های فنی مربوطه و حفظ آگاهی درباره آنها مورد استفاده قرار خواهد گرفت توصیه می‌شود برای نرم‌افزار و فن‌آوری دیگر شناسایی شود. (بر اساس لیست موجودی دارایی‌ها، رجوع کنید به بند ۷-۱-۱)؛ توصیه می‌شود این منابع اطلاعات بر اساس تغییرات در لیست موجودی یا در زمانی که منابع جدید یا مفیدی پیدا می‌شوند روزآمد شوند.

پ - توصیه می‌شود برای واکنش به اعلام آسیب‌پذیری‌های فنی مربوطه یک زمان بندی تعریف شود

ت - به محض این که یک آسیب‌پذیری فنی بالقوه شناسایی شد، توصیه می‌شود سازمان ریسک‌های مربوطه و فعالیت‌های مورد نیاز را شناسایی کند. این فعالیت‌ها ممکن است دربرگیرنده دسته بندی گروه‌های آسیب‌پذیر و یا به کارگیرِ کنترل‌های دیگر باشد

ث - با توجه به این که یک آسیب‌پذیری فنی با چه اولویتی باید مورد رسیدگی قرار گیرد، توصیه می‌شود فعالیت‌های انجام شده مطابق با کنترل‌های مربوط به مدیریت تغییر (رجوع کنید به بند ۱۲-۵-۱) یا با پیروی از رویه‌های واکنش به رخدادهای امنیتی اطلاعات انجام شوند (رجوع کنید به بند ۱۳-۲).

ج - اگر یک وصله[1] در دسترس باشد، توصیه می‌شود ریسک‌های مربوط به نصب دسته‌های جدید ارزیابی شود (برای مثال، توصیه می‌شود ریسک‌های مطرح شده بوسیله آسیب پذیری سیستم با ریسک‌های نصب وصله مقایسه شود)

چ - توصیه می‌شود دسته‌ها قبل از این که نصب شوند آزموده و ارزیابی شوند تا تضمین شود که آنها موثر هستند و منجر به عوارض جانبی غیرقابل تحمل نمی‌شود. اگر هیچ دسته ای موجود نباشد، توصیه می‌شود کنترل‌های دیگر در نظر گرفته شود نظیر:

۱ - متوقف کردن خدمات یا قابلیت‌های مربوط به آسیب‌پذیری

۲ - استفاده یا اضافه کردن کنترل‌های دسترسی مانند دیوارهای آتش در مرزهای شبکه(رجوع کنید به بند ۱۱-۴-۵)

۳ - افزایش نظارت برای کشف یا پیشگیری از حملات واقعی

۴ - افزایش آگاهی از آسیب‌پذیری

ح - توصیه می‌شود اطلاعات ثبت شده حسابرسی برای تمام رویه‌های مورد نظر نگهداری شود

خ - توصیه می‌شود فرایند مدیریت آسیب‌پذیری فنی به طور منظم نظارت شود و به منظور تضمین تاثیر و بازدهی اش ارزیابی شود.

د - توصیه می‌شود سیستم‌هایی که در معرض ریسک بالا قرار دارند ابتدا مورد رسیدگی قرار گیرند.

اطلاعات دیگر

عملکرد صحیح یک فرایند مدیریت آسیب‌پذیری فنی سازمان برای بسیاری از سازمان‌ها حیاتی است و بنابراین توصیه می‌شود به طور منظم کنترل شود. یک لیست موجودی دقیق برای تضمین این که آسیب‌پذیری‌های فنی مربوطه شناسایی می‌شوند لازم است.

مدیریت آسیب‌پذیری فنی را می‌توان به عنوان یک عملکرد فرعی مدیریت تغییر دانست و بدین ترتیب می‌تواند از مزیت فرایندها و رویه‌های مدیریت تغییر استفاده کند(رجوع کنید به بند ۱۰-۱-۲ و ۱۲-۵-۱)

فروشندگان اغلب زیر فشار زیادی برای پخش بسته‌ها در سریع ترین زمان ممکن قرار دارند. بنابراین، یک دسته نمی‌تواند به مشکل به اندازه کافی برسد و ممکن است تاثیرات جانبی منفی داشته باشد. همچنین در بعضی موارد، برداشتن یک دسته ممکن است به سادگی به محض استفاده از دسته امکان پذیر نباشد.

اگر آزمون کافی از دسته‌ها ممکن نباشد، مثلا به دلیل هزینه یا نبود منابع، تاخیری در دسته بندی را می‌توان برای ارزیابی ریسک‌های مربوطه بر اساس تجربه گزارش شده توسط کاربران دیگر در نظر گرفت.

1- Patch

۱۳ مدیریت رخدادهای امنیت اطلاعات

۱-۱۳ گزارش‌دهی وقایع و ضعف‌های امنیت اطلاعات

هدف: حصول اطمینان از اینکه وقایع و ضعف‌های امنیت اطلاعات مربوط به سیستم‌های اطلاعاتی، به شیوه ای به اطلاع برسد که اجازهٔ اقدام اصلاحی بهنگام را بدهد.

توصیه می‌شود گزارش رسمی وقایع و رویه‌های افزایشی به کار گرفته شود. توصیه می‌شود تمام کارکنان، پیمانکاران، و کاربران شخص ثالث از رویه‌های گزارش انواع مختلف وقایع و ضعف‌هایی که ممکن است بر امنیت دارایی‌های سازمان تاثیر بگذارند مطلع شوند. توصیه می‌شود از آنها خواسته شود هر واقعه و ضعف امنیت اطلاعات را در اسرع وقت به نقطه تماس تعیین شده گزارش کنند.

۱-۱-۱۳ گزارش‌دهی وقایع امنیت اطلاعات

کنترل

توصیه می‌شود وقایع امنیت اطلاعات در کوتاهترین زمان ممکن، از طریق مجاری مدیریتی مناسب، گزارش شوند.

راهنمای پیاده‌سازی

توصیه می‌شود یک رویه گزارش رسمی وقایع امنیت اطلاعات ایجاد شود و رویه ای برای واکنش به رخدادها نیز باید ایجاد شود که فعالیت‌هایی را که باید در زمان دریافت گزارشی مبنی بر یک واقعه امنیت اطلاعات انجام شود تعریف می‌کند. توصیه می‌شود یک محل گزارش‌دهی برای گزارش وقایع امنیت اطلاعات ایجاد شود. توصیه می‌شود که تضمین شود که این محل گزارش‌دهی در سراسر سازمان، شناخته شده است و همیشه در دسترس بوده و توانایی ارایه واکنش کافی و به موقع را دارد.

توصیه می‌شود تمام کارکنان، پیمانکاران، و کاربران شخص سوم از مسوولیت شان در گزارش هر واقعه امنیت اطلاعات در اسرع وقع آگاه باشند. توصیه می‌شود آنها از رویه گزارش وقایع امنیت اطلاعات و محل گزارش‌دهی آگاه باشند. توصیه می‌شود رویه‌های گزارش شامل موارد زیر باشد:

الف - فرآیندهای انعکاس مناسب برای تضمین این که کسانی که وقایع امنیت اطلاعات را گزارش می‌کنند از نتایج پس از رسیدگی به مساله آگاه هستند

ب - فرم‌های گزارش وقایع امنیت اطلاعات برای پشتیبانی فعالیت گزارش و برای کمک به شخص گزارش کننده برای به یاد داشتن تمام فعالیت‌های لازم در صورت وقوع حادثه امنیت اطلاعات

پ - رفتار صحیح که باید در صورتی که یک حادثه امنیت اطلاعات رخ داد؛ انجام شود

۱ - اعلام فوری تمام جزئیات مهم (برای مثال، نوع عدم انطباق یا نقض، پدیدآمدن عیب فنی، پیغام های روی صفحه نمایش، رفتار عجیب)

۲ - عدم انجام هر گونه فعالیت خودسرانه اما گزارش آنی آن به محل گزارش‌دهی

ت - اشاره به فرآیند انضباطی رسمی تثبیت شده برای برخورد با کارکنان، پیمانکاران، یا کاربران شخص سومی که مرتکب رخنه امنیتی شده اند.

در محیط‌های پر خطر، یک هشدار اجباری ممکن است ارایه شود تا از طریق آن، شخص، تحت اجبار بتواند این مشکلات را نشان دهد. توصیه می‌شود رویه‌هایی پاسخگویی به هشدارهای اجبار نشان دهنده شرایط پرخطری باشد که این هشدارها نشان می‌دهند.

اطلاعات دیگر

مثال‌های رخدادهای امنیت اطلاعات عبارتند از:

الف - آسیب به خدمات، تجهیزات یا تاسیسات

ب - عملکرد نامناسب یا سرریز کردن سیستم

پ - خطاهای انسانی

ت - عدم انطباق با خط‌مشی‌ها و رهنمودها

ث - نقض هماهنگی‌های امنیت فیزیکی

ج - تغییرات کنترل نشده سیستم

چ - عملکرد نامناسب نرم‌افزار یا سخت افزار

ح - نقض دسترسی

با مراقبت مناسب از جنبه‌های محرمانگی، رخدادهای امنیت اطلاعات را می‌توان در آموزش آگاهانه کاربران به کاربرد(رجوع کنید به بند ۸-۲-۲)، مثلا در آموزش آنچه که ممکن است رخ دهد، نحوه واکنش به این رخدادها و نحوه اجتناب از آنها در آینده است. برای ایجاد امکان پرداختن به رخدادهای امنیت اطلاعات به طور مناسب، ممکن است لازم باشد که شواهد در اسرع وقت پس از وقوع جمع آوری شوند. (رجوع کنید به بند ۱۳-۲-۳)

عملکرد نامناسب یا دیگر رفتارهای نامناسب سیستم ممکن است نشان دهنده یک حمله امنیتی یا رخنه امنیتی باشد و بنابراین توصیه می‌شود همیشه به عنوان واقعه امنیت اطلاعات گزارش شود.

اطلاعات بیشتر درباره گزارش رخدادهای امنیت اطلاعات و مدیریت وقایع امنیت اطلاعات را می‌توان در ISO/IECTR 18044 پیدا کرد.

۱۳-۱-۲ گزارش‌دهی ضعف‌های امنیتی

کنترل

توصیه می‌شود تمامی کارکنان، پیمانکاران و کاربران شخص سوم سیستم‌ها و خدمات اطلاعاتی، نسبت به یادداشت و گزارش‌دهی هر ضعف امنیتی مشاهده شده یا مورد سوء ظن در سیستم‌ها یا خدمات، ملزم شوند.

راهنمای پیاده‌سازی

توصیه می‌شود تمام کارمندان، پیمانکاران و کابران شخص سوم این موضوعات را در اولین فرصت ممکن یا به مدیران‌شان و یا به بطور مستقیم به تامین کننده سرویس‌شان گزارش کنند تا از ریسک‌های رخدادهای امنیت اطلاعات جلوگیری شود. توصیه می‌شود ساز و کار گزارش، ساده و تا حد امکان قابل دسترسی باشد. همچنین توصیه می‌شود آنها مطلع شوند که در هیچ شرایطی سعی نکنند یک ضعف مشکوک را به اثبات برسانند.

اطلاعات دیگر

به کارکنان، پیمانکاران و کاربران شخص سوم باید توصیه شود سعی نکنند ضعف‌های امنیتی مشکوک را اثبات کنند. آزمون ضعیف ممکن است به عنوان سوء استفاده احتمالی از سیستم تلقی شود و همچنین ممکن است باعث آسیب به سیستم اطلاعات یا خدمات شود و منجر به ایجاد مسوولیت قانونی برای شخصی شود که آزمون را انجام می‌دهد.

۱۳-۲ مدیریت رخدادها و بهبودهای امنیت اطلاعات

هدف: حصول اطمینان از اینکه رویکردی استوار و موثر برای مدیریت رخدادهای امنیت اطلاعات، بکار گرفته شده است.

توصیه می‌شود مسوولیت‌ها و رویه‌هایی برای پرداختن به وقایع و ضعف‌های امنیت اطلاعات به محض این که گزارش شدند در نظر گرفته شود. توصیه می‌شود یک فرآیند بهبود مداوم برای واکنش، کنترل، ارزیابی و مدیریت رخدادهای امنیت اطلاعات به کار گرفته شود.

توصیه می‌شود هر زمان که شواهدی لازم است، جمع آوری شود تا انطباق با الزامات قانونی تضمین شود

۱۳-۲-۱ مسوولیت‌ها و روش‌های اجرایی

کنترل

توصیه می‌شود به منظور حصول اطمینان از یک پاسخ سریع، موثر و منظم به رخدادهای امنیت اطلاعات، مسوولیت‌های مدیریتی و روش‌های اجرایی ایجاد شوند.

راهنمای پیاده‌سازی

علاوه بر گزارش رخدادها و ضعف‌های امنیت اطلاعات (همچنین رجوع کنید به بند ۱۳-۱)، توصیه می‌شود کنترل سیستم‌ها، هشدارها، و آسیب‌پذیری‌ها (۱۰-۱۰-۲) برای کشف رخدادهای امنیت اطلاعات مورد استفاده قرار گیرند.

توصیه می‌شود رهنمودهای زیر برای اجرای رویه‌های مدیریت وقایع امنیت اطلاعات در نظر گرفته شوند:

الف - توصیه می‌شود رویه‌هایی برای رسیدگی به انواع مختلف رخدادهای امنیت اطلاعات تثبیت شود که شامل موارد زیر است:

۱ - خرابی‌های سیستم اطلاعات و آسیب به خدمات

۲ - کد نامناسب (رجوع کنید به بند ۱۰-۴-۱)

۳ - انکار خدمات

۴ - خطاهایی که از داده‌های کسب وکار ناقص یا غیردقیق ناشی می‌شوند.

۵ - رخنه در محرمانگی و یکپارچگی

۶ - سوء استفاده از سیستم‌های اطلاعات

ب - علاوه بر برنامه‌های عادی(رجوع کنید به بند ۱۴-۱-۳)، توصیه می‌شود رویه‌هایی موارد زیر را پوشش دهند(همچنین رجوع کنید به بند ۱۳-۲-۲):

۱ - تحلیل و شناسایی علت دقیق رخداد

۲ - محدودسازی

۳ - برنامه ریزی و اجرای فعالیت اصلاحی برای پیشگیری از وقوع مجدد در صورت لزوم؛

۴ - ارتباط با آنهایی که تحت تاثیر رخداد قرار دارند یا در آن مشارکت دارند

۵ - گزارش فعالیت به مرجع مناسب

پ - توصیه می‌شود گزارش‌های ممیزی و شواهد مشابه جمع آوری شوند (رجوع کنید به بند ۱۳-۲-۳) و امنیت شان تامین شود که برای موارد زیر مناسب باشند:

۱- تحلیل مسایل داخلی
۲ - استفاده به عنوان شواهد دادگاهی در رابطه با نقض احتمالی قرارداد یا الزامات قانونی یا در واقعه غیرنظامی یا اقدامات جنایی مثلا در شرایط سوء استفاده از رایانه یا قوانین محافظت از داده‌ها
۳ - مذاکره برای دریافت خسارت از تامین کنندگان نرم‌افزار و خدمات

ت - توصیه می‌شود فعالیت‌هایی برای نجات از رخنه های امنیتی و اصلاح خطاهای سیستم با دقت و به طور رسمی‌کنترل شود. توصیه می‌شود این رویه‌ها تضمین کنند که:

۱ - فقط کارکنانی که شناخته شده و مجاز هستند اجازه دسترسی به سیستم‌های زنده و داده‌ها را دارند(همچنین برای دسترسی خارجی، رجوع کنید به بند ۶-۲)
۲ - تمام فعالیت‌های اضطراری به طور مفصل مستند می‌شوند
۳ - فعالیت اضطراری به مدیریت گزارش می‌شود و به صورت منظم بررسی می‌شود
۴ - یکپارچگی سیستم‌های کسب وکار و کنترل‌ها با حداقل تاخیر تایید می‌شود.

توصیه می‌شود اهداف مدیریت رخدادهای امنیت اطلاعات با مدیریت مورد توافق قرار گیرد و توصیه می‌شود که تضمین شود که کسانی که مسوول مدیریت رخدادهای امنیت اطلاعات هستند اولویت‌های سازمان را برای پرداختن به رخدادهای امنیت اطلاعات درک می‌کنند.

اطلاعات دیگر

رخدادهای امنیت اطلاعات ممکن است از مرزهای سازمانی و ملی فرا رود. به منظور واکنش به این رخدادها نیاز فزاینده ای به هماهنگ کردن در ارایه عکس‌العمل و اشتراک اطلاعات درباره این رخدادها با سازمان‌های بیرونی در زمان مناسب وجود دارد.

۱۳-۲-۲ یادگیری از رخدادهای امنیت اطلاعات

کنترل

توصیه می‌شود برای اینکه نوع، حجم و هزینه‌های رخدادهای امنیتی، قابل اندازه گیری و پایش باشند، ساز و کارهای لازم ایجاد شوند.

راهنمای پیاده‌سازی

توصیه می‌شود اطلاعات به دست آمده از ارزیابی رخدادهای امنیت اطلاعات برای شناسایی رخدادهای پرتکرار یا با تاثیر زیاد مورد استفاده قرار گیرد. (رجوع کنید به بند ۵-۱-۲)

اطلاعات دیگر

ارزیابی اطلاعات رخدادهای امنیت اطلاعات ممکن است نشان دهنده نیاز به افزایش کنترل برای محدود کردن فراوانی، آسیب، و هزینه وقایع آینده یا در نظر گرفته شدن در فرآیند بررسی خط‌مشی امنیت باشد.

۱۳-۲-۳ گردآوری شواهد

کنترل

هنگامی‌که پیگرد علیه یک فرد یا سازمان، پس از یک رخداد امنیت اطلاعات، منجر به اقدام قانونی (اعم از مدنی یا جنایی) می‌شود، توصیه می‌شود شواهد منطبق با قواعد اقامهٔ شواهد در حوزه‌های قضایی مرتبط، گردآوری، نگهداری و ارایه شوند.

راهنمای پیاده‌سازی

توصیه می‌شود رویه‌های داخلی توسعه یابند و در زمان جمع آوری و ارایه شواهد برای اهداف فعالیت انضباطی در یک سازمان دنبال شوند.

به طور کلی، قوانین شواهد موارد زیر را پوشش می‌دهند:

الف - قابل پذیرش بودن شواهد: این که آیا شواهد را می‌توان در دادگاه مورد استفاده قرار داد؛

ب - وزن شواهد: کیفیت و کامل بودن شواهد

توصیه می‌شود به منظور دستیابی به شواهد قابل قبول، سازمان تضمین نماید که سیستم‌های اطلاعاتی آنها با هر استاندارد منتشر شده یا آئین نامه تولید شواهد قابل پذیرش، مطابقت دارد.

توصیه می‌شود وزن شواهد ارایه شده با تمام الزامات موجود مطابقت داشته باشد. به منظور دستیابی به شواهد معتبر، توصیه می‌شود کیفیت و کامل بودن کنترل‌های به‌کار رفته برای محافظت صحیح و مستمر از شواهد (به عبارت دیگر شواهد کنترل فرآیند) در سراسر دوره ای که شواهد بازیابی، ذخیره و پردازش می‌شوند، با شواهدی قوی نشان داده شود. به طور کلی، این گزارش قوی باید تحت شرایط زیر ایجاد شود:

الف - برای اسناد کاغذی: نسخه اصل به طور ایمن با سوابقی از فردی که سند را پیدا کرده، محل پیدا شدن سند، زمان پیدا شدن سند، و کسی که شاهد این پیدا شدن است نگهداری می‌شود؛ توصیه می‌شود هر گونه بررسی که تضمین می‌کند نسخه‌های اصل مشکل پیدا نمی‌کنند؛ در نظر گرفته شود

ب - برای اطلاعات موجود در رسانه‌های رایانه‌ی؛ توصیه می‌شود تصاویر برابر اصل یا نسخه‌برداری (بسته به الزامات قابل کاربردی) از هر یک از رسانه‌های قابل جابجایی، اطلاعات موجد در دیسک‌های سخت یا در حافظه برای تضمین امنیت موجود باشند. توصیه می‌شود اطلاعات ثبت شده تمام فعالیت‌ها در زمان فرآیند نسخه‌برداری نگهداری شود و فرآیند مشاهده شود؛ توصیه می‌شود رسانه‌های اصل و اطلاعات ثبت شده (اگر این ممکن نیست، حداقل یک تصویر برابر اصل یا کپی) به طور ایمن و دست نخورده نگه داشته شوند.

توصیه می‌شود هر گونه کار کارشناسی فقط روی نسخه‌های کپی انجام شود. توصیه می‌شود یکپارچگی تمام مطالب موجود در مدارک محافظت شود. توصیه می‌شود نسخه برداری از شواهد توسط کارکنان قابل اعتماد نظارت شود و اطلاعات درباره مکان و زمان انجام نسخه برداری فردی که فعالیت‌های نسخه برداری را انجام می‌دهد و ابزارها و برنامه‌هایی که مورد استفاده قرار گرفته اند ثبت شود.

اطلاعات دیگر

زمانی که یک واقعه امنیت اطلاعات برای نخستین بار کشف می‌شود، ممکن است دقیقا معلوم نباشد که آیا این حادثه منجر به اقدام دادگاهی شود. بنابراین این خطر وجود دارد که شواهد لازم عمدا یا تصادفا قبل از تشخیص جدی بودن رخداد خراب شود. توصیه می‌شود از یک وکیل یا پلیس در مراحل اولیه هر اقدام حقوقی مشورت خواسته شود و توصیه‌های او اجرا شود.

شواهد ممکن است از مرزهای سازمان یا حوزه قضایی فراتر روند. در این موارد، توصیه می‌شود که تضمین شود سازمان حق دارد اطلاعات لازم را به عنوان شاهد جمع آوری کند. توصیه می‌شود الزامات حوزه‌های قضایی مختلف نیز برای افزایش شانس پذیرش فراسوی مرزهای قضایی مربوطه در نظر گرفته شود.

۱۴ مدیریت استمرار کسب‌وکار

۱۴-۱ جنبه‌های امنیت اطلاعات مدیریت استمرار کسب‌وکار

هدف : خنثی کردن وقفه های فعالیتهای کسب و کار و حفاظت از فرآیندهای بحرانی کسب و کار در برابر اثرات ناشی از خرابی های عمدهٔ سیستم‌های اطلاعاتی یا سوانح و حصول اطمینان به از سرگیری به موقع آنها.
توصیه می‌شود یک فرآیند مداوم مدیریت استمرار کسب و کار برای کاهش پیامد بر سازمان و بازیابی از آسیب به دارایی های اطلاعاتی که میتوانند ناشی از حوادث طبیعی، نقایص فیزیکی سخت افزارها و یا خسارتهای عمدی باشند تا سطح مطلوبی از طریق آمیزه ای از کنترل های پیشگیرانه و بازیابی انجام شود. توصیه می‌شود، این فرآیند فرآیندهای تجاری مهم را شناسایی کند و الزامات مدیریت امنیت اطلاعات استمرار کسب و کار را با دیگر الزامات مربوط به جنبه هایی از جمله عملیات، استخدام، تجهیزات، حمل و نقل و امکانات یکپارچه سازد.
پیامدهای فجایع، اختلالات امنیتی، آسیب به خدمات و دسترسی به خدمات باید تابع یک روش تحلیل آسیب‌های کسب و کار قرار گیرند. توصیه می‌شود برنامه های استمرارکسب و کار طراحی شوند و برای تضمین از سرگیری به موقع عملیات حیاتی اجرا شوند. توصیه می‌شود امنیت اطلاعات جزء لاینفک یک فرآیند تداوم تجاری و دیگر فرآیندهای مدیریتی در سازمان باشد.
توصیه می‌شود مدیریت استمرار کسب و کار شامل کنترل هایی برای شناسایی و کاهش ریسک ها به علاوه فرآیند ارزیابی ریسک های کلی باشد، پیامدهای رخدادهای آسیب رسان را محدود کند و تضمین کند که اطلاعات مورد نیاز برای فرآیندهای کسب و کار به سادگی در دسترس است.

۱۴-۱-۱ لحاظ کردن امنیت اطلاعات در فرایند مدیریت استمرار کسب‌وکار

کنترل

توصیه می‌شود فرآیند مدیریت شده ای به منظور استمرار کسب وکار در سراسر سازمان، ایجاد و پیاده سازی شود که الزامات امنیت اطلاعات مورد نیاز استمرار کسب وکار سازمان را نشانی دهی کند.

راهنمای پیاده‌سازی

توصیه می‌شود این فرآیند ارکان مهم مدیریت استمرار کسب و کار شامل موارد زیر را در کنار هم داشته باشد:

الف - درک ریسک هایی که یک سازمان با آن روبرو است، از نظر احتمال رخداد و میزان پیامد آنها در زمان شامل شناسایی و اولویت بندی فرآیندهای کسب و کار مهم (رجوع کنید به بند ۱۴-۱-۲)

ب - شناسایی تمام داراییهای موجود در فرآیندهای حیاتی کسب و کار (رجوع کنید به بند ۷-۱-۱)

پ - درک پیامدی که اختلالات رخدادهای امنیت اطلاعات احتمالا بر کسب و کار، تثبیت اهداف کسب وکار و تجهیزات پردازش اطلاعات ایجاد کردند (این موضوع مهم است که راه حل هایی پیدا شود تا رخدادهای منجر به پیامدهای کوچکتر را اداره کنند، به اندازه رخدادهای جدی که می‌تواند دوام سازمان را تهدید کند)

ت - در نظر گرفتن بیمه مناسب که ممکن است بخشی از فرآیند استمرار کسب و کار و نیز بخشی از مدیریت عملیاتی ریسک باشد.
ث - شناسایی و در نظر گرفتن کنترل های پیشگیرانه و اصلاحی اضافی
ج - شناسایی منابع مالی، سازمانی، فنی، و زیست محیطی برای اشاره به الزامات شناخته شده امنیت اطلاعات.
چ - تضمین ایمنی کارکنان و محافظت از تجهیزات پردازش اطلاعات و اموال سازمانی
ح - فرمول بندی و مستندسازی برنامه های استمرار کسب و کار که به الزامات امنیت اطلاعات در راستای راهبرد استمرار کسب و کار مورد توافق اشاره دارد (رجوع کنید به بند ۱۴-۱-۳)
خ - آزمون و بروزسازی منظم برنامه ها و فرآیندهای پیاده سازی شده (رجوع کنید به بند ۱۴-۱-۵)
د - تضمین این که مدیریت استمرار کسب و کار در فرآیندها و ساختار سازمان به کار گرفته می‌شود، توصیه می‌شود مسوولیت فرآیند مدیریت استمرار کسب وکار در سطح مناسب در سازمان تعیین شود. (رجوع کنید به بند ۶-۱-۱)

۱۴-۱-۲ استمرار کسب‌وکار و ارزیابی ریسک

کنترل

توصیه می‌شود وقایعی که می‌توانند موجب وقفه در فرآیندهای کسب وکار شوند، با توجه به احتمال بروز و آسیب ناشی از چنین وقفه هایی و پیامدهای آنها بر امنیت اطلاعات، شناسایی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود جنبه های امنیت اطلاعات استمرار کسب و کار بر اساس شناسایی حوادثی باشد که باعث اختلال در فرآیندهای کسب وکار سازمان ها می‌شود، مثلا خرابی تجهیزات، خطاهای انسانی، سرقت، آتش سوزی، بلایای طبیعی، و اقدامات تروریستی. توصیه می‌شود این فعالیت‌ها با یک فرآیند ارزیابی ریسک به منظور تعیین احتمال و پیامد این اختلالات از نظر زمانی، میزان آسیب و دوره از سر گیری فرآیند دنبال شود.

توصیه می‌شود ارزیابی ریسک استمرار کسب و کار با مشارکت کامل تمام مالکان منابع و فرآیندهای تجاری انجام شود. توصیه می‌شود این ارزیابی تمام فرآیندهای کسب وکار را در برگیرد و به تجهیزات پردازش اطلاعات محدود نباشد، لیکن باید شامل نتایج خاص امنیت اطلاعات باشد. مهم است که جنبه های مختلف به هم پیوند داده شوند تا تصویر کاملی از الزامات استمرار کسب و کار سازمان به دست آید. توصیه می‌شود ارزیابی ریسک ها را در مقایسه با معیارها و اهداف مربوط به سازمان از جمله، منابع مهم، پیامدهای اختلالات، زمان های مجاز قطعی سرویس و اولویت های بازیابی؛ شناسایی، سنجش و اولویت بندی کند.

بسته به نتایج ارزیابی ریسک، توصیه می‌شود یک راهبرد استمرار کسب و کار برای تعیین رویکرد کلی در قبال استمرار کسب و کار در نظر گرفته شود. پس از ایجاد این راهبرد، لازم است مدیریت سازمان آن را تایید نموده و به گونه‌ای برنامه‌ریزی نماید تا این راهبرد اجرا شود.

۱۴-۱-۳ ایجاد و پیاده‌سازی طرح‌های استمرار دربرگیرندهٔ امنیت اطلاعات

کنترل

در پی وقفه و یا بروز نقص در فرآیندهای بحرانی کسب وکار، به منظور نگهداری یا از سرگیری عملیـات و اطمینـان از دسترس پذیری اطلاعات در سطح و دوره زمانی قابل قبول، توصیه می‌شود طرح هایی ایجاد و پیاده سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود فرآیند برنامه ریزی استمرار کسب و کار موارد زیر را در نظر گیرد:

الف - شناسایی و توافق درباره مسوولیت ها و رویه های استمرار کسب و کار

ب- شناسایی حد قابل قبول آسیب به اطلاعات و خدمات

پ- اجرای رویه هایی برای امکان پذیر کردن بازیابی و نگهداری عملیات کسب وکار و دسترسی به اطلاعات در مقیاسهای زمانی مورد نیاز؛ توجه خاصی باید به ارزیابی وابستگی های داخلی و خارجی کسب و کار و قراردادهای موجود شود؛

ت- رویه های عملیاتی به منظور پیگیری تکمیل بازیابی و ذخیره سازی در آینده؛

ث- مستندسازی رویه ها و فرآیندهای مورد توافق

ج- آموزش مناسب کارکنان درخصوص رویه ها و فرآیندهای مورد توافق از جمله مدیریت بحران

چ- تست و ارتقاء برنامه ها

توصیه می‌شود فرآیند برنامه ریزی بر اهداف کسب وکار از جمله حفظ خدمات ارتباطی خاص مشتریان در زمان قابل قبول تاکید کند. همچنین توصیه می‌شود خدمات و منابعی که این امر را تسهیل می‌کنند شناسایی شوند که از آن جمله می‌توان به استخدام، منابع پردازش غیراطلاعاتی، و نیز هماهنگی های پشتیبانی برای تجهیزات پردازش اطلاعات اشاره کرد. این فعالیت‌ها ممکن است شامل هماهنگی با شخص های ثالث به شکل قراردادهای دوجانبه یا خدمات اشتراک کسب وکار باشد.

توصیه می‌شود برنامه های تداوم کسب و کار به آسیب پذیری های سازمانی اشاره کنند و بنابراین ممکن است شامل اطلاعات حساسی باشند که باید به طور مناسب محافظت شوند. توصیه می‌شود نسخه های برنامه های استمرار کسب و کار در محلی دیگر با فاصله کافی برای جلوگیری از هر گونه آسیب ناشی از حوادث قرار داده شوند. توصیه می‌شود مدیریت تضمین کند که نسخه های برنامه های استمرار کسب وکار به روز هستند و با سطح مشابه امنیت به کار رفته در محل اصلی محافظت می‌شوند. موارد دیگری که برای اجرای برنامه های استمرار کسب و کار لازم هستند توصیه می‌شود در محلی دور ذخیره شوند.

اگر محل های موقت جایگزین مورد استفاده قرار می‌گیرند، توصیه می‌شود سطح کنترل های امنیتی اجرا شده در این محل ها مشابه محل اصلی باشد.

اطلاعات دیگر

باید اشاره شود که برنامه ها و فعالیت های مدیریت بحران ممکن است با مدیریت استمرار کسب و کار متفاوت باشد؛ به عبارت دیگر ممکن است بحرانی رخ دهد که بتوان آن را با رویه های مدیریتی رفع کرد

۴-۱-۱۴ چارچوب طرح‌ریزی استمرار کسب‌وکار

کنترل

به منظور حصول اطمینان از سازگاربودن تمامی طرح ها، نشان دهی بدون تناقض الزامات امنیت اطلاعات، و شناسایی اولویت های آزمون و نگهداری، توصیه می‌شود یک چارچوب واحد از طرح های استمرار کسب وکار ایجاد و نگهداری شود.

راهنمای پیاده‌سازی

توصیه می‌شود هر برنامه استمرار کسب و کار رویکرد استمرار را مثلا رویکرد تضمین اطلاعات یا دسترسی و امنیت سیستم اطلاعات را بیان کند. توصیه می‌شود هر برنامه همچنین یک برنامه برای موارد اضطراری را مشخص و شرایط فعال سازی آن را تعیین کند، و نیز افراد مسوول اجرای هر جزء از برنامه را مشخص شوند. زمانی که الزامات جدید شناسایی شدند، توصیه می‌شود هر گونه رویه اضطراری[1] موجود مثلا، برنامه های تخلیه محل[2] به طور مناسب اصلاح شوند. توصیه می‌شود رویه هایی در برنامه مدیریت تغییر سازمان گنجانده شوند تا تضمین شود که موضوعات استمرار همیشه به طور مناسب مورد اشاره و رسیدگی قرار می‌گیرند.

توصیه می‌شود هر برنامه یک مالک خاص داشته باشد. توصیه می‌شود رویه های اضطراری، برنامه هایی با اجرای دستی برای شرایط اضطرار[3]، و برنامه های از سرگیری[4] در حوزه مسوولیت مالک منابع یا فرآیندهای کسب وکار مربوطه باشند. توصیه می‌شود قراردادهای پشتیبانی برای خدمات فنی جایگزین، نظیر تجهیزات پردزاش اطلاعات و ارتباطات معمولا در حیطه مسوولیت ارایه کنندگان خدمات باشد.

توصیه می‌شود یک چارچوب برنامه ریزی استمرار کسب و کار الزامات امنیت اطلاعات شناسایی شده را مورد اشاره قرار دهد و موارد زیر را در نظر گیرد:

الف - شرایط فعال سازی برنامه هایی که باید قبل از فعال سازی آنها فرآیندی اجرا شود(برای مثال چگونگی ارزیابی موقعیت، اینکه چه کسانی در برنامه دخیل هستند)؛ بیان می‌کند.

ب - رویه های اضطراری که توصیف کننده فعالیت هایی هستند که باید پس از وقوع یک رخداد که عملیات کسب وکار را به خطر می اندازد؛ اجرا گردند

پ - رویه های پشتیبانی که فعالیت هایی را که برای انجام فعالیت های کسب وکار مهم یا حمایت از خدمات پشتیبانی جایگزین باید در نظر گرفته شوند بیان می‌کند و فرآیندها را عملیاتی می‌کنند.

ت - رویه های عملیاتی موقت برای تکمیل فرآیند ذخیره و بازیابی

ث - رویه های از سر گیری که فعالیت هایی را که برای بازگشتن به عملیات عادی کسب و کار اتخاذ شوند را بیان می‌کنند

ج - یک برنامه زمانبندی نگهداری که مشخص می‌کند چگونه و در چه موقعی برنامه و فرآیند نگهداری از برنامه باید آزموده شود.

چ - فعالیت های آگاه‌سازی، آموزش، و تعلیم که برای ایجاد درکی از فرآیندهای استمرار کسب و کار و تضمین این که فرآیند همچنان موثر خواهند بود نیاز می‌باشند

ح - مسوولیت‌های افراد به گونه ای که بیان کند چه کسی مسوول اجرای چه جزئی از برنامه است. توصیه می‌شود گزینه‌ها بر حسب نیاز در نظر گرفته شوند؛

1- Escalation plan
2- Evacuation plan
3- Manual fallback plans
4- Resumption plans

خ - دارایی‌های حیاتی و منابع مورد نیاز برای انجام رویه های اضطراری، پشتیبانی و از سر گیری

۱۴-۱-۵ حفظ و نگهداری آزمون و ارزیابی مجدد طرح‌های استمرار کسب‌وکار

کنترل

توصیه می‌شود طرح های استمرار کسب وکار، به منظور حصول اطمینان از اینکه به روز و موثر هستند، به طورمنظم مورد آزمون قرار گرفته و بهنگام شوند.

راهنمای پیاده‌سازی

توصیه می‌شود آزمون‌های برنامه استمرار کسب و کار تضمین کنند که اعضاء تیم بازیابی و دیگر کارکنان مربوطه از برنامه ها و مسوولیت شان برای استمرار کسب و کار و امنیت اطلاعات آگاهند و نقش خود را در زمان هر پیشامد می‌دانند.

توصیه می‌شود جدول آزمون برای برنامه (های) استمرار کسب و کار نشان دهد که توصیه می‌شود چگونه و چه موقع هر جزء از برنامه آزموده شود. توصیه می‌شود هر جزء برنامه (ها) به کرات آزموده شود.

توصیه می‌شود انواع تکنیک ها به منظور تضمین اینکه برنامه ها در محیط واقعی عملیاتی می‌شوند مورد استفاده قرار گیرند. توصیه می‌شود موارد زیر شامل شوند:

الف - آزمون به موقع سناریوهای مختلف (مطرح کردن تمهیدات بازسازی کسب وکار با بکار بردن وقفه‌های نمونه)

ب - شبیه سازی‌ها (بطور مشخص برای آموزش افراد در نقش های مدیریتی بحران/ رخدادها در آینده)

پ - آزمون بازیابی فنی (اطمینان از اینکه سیستم‌های عملیات بازیابی اطلاعات بطور موثر بازیابی شوند)

ت - بازیابی آزمون در محل‌های متفاوت (اجرای فرایندهای کسب وکار همزمان با عملیات بازیابی، جدا از سایت اصلی)

ث - آزمون‌های تجهیزات و خدمات تامین کننده (اطمینان از اینکه سرویس ها و محصولات تامین شده خارجی، تعهدات قراردادی را برآورده می‌کنند)

ج - تست‌های سازگاری (آزمون اینکه سازمان، کارکنان، تجهیزات، امکانات و فرایندها می‌توانند بر وقفه ها فائق آیند)

این تکنیک ها را می‌توان در هر سازمانی مورد استفاده قرار داد. توصیه می‌شود آنها به گونه ای به کار گرفته شوند که مرتبط با برنامه بازیابی خاصی باشد. توصیه می‌شود نتایج آزمون‌ها ثبت شود و اقداماتی برای بهبود برنامه ها در صورت لزوم باید اتخاذ شود.

توصیه می‌شود مسوولیت‌ها برای بررسی های منظم هر برنامه استمرار کسب و کار تعیین شود. توصیه می‌شود شناسایی تغییرات در محیط های کسب وکار که تا به حال در برنامه های استمرار کسب و کار منعکس نشده اند از طریق روزآمدسازی مناسب برنامه دنبال شود. همچنین توصیه می‌شود این فرآیند کنترل تغییر رسمی تضمین کند که برنامه های روزآمد شده از طریق بررسی های منظم توزیع و تقویت شده اند.

مثال هایی از تغییراتی که بروزسازی برنامه های استمرار کسب و کار در نظر میگیرند عبارتند از دستیابی به تجهیزات جدید، بروزسازی سیستم‌ها و تغییرات در موارد زیر است:

الف - کارکنان

ب - نشانی‌ها و شماره‌های تماس

پ - راهبرد کسب وکار
ت - محل، تجهیزات و منابع
ث - مقررات
ج - قراردادها، تامین کننده‌ها و مشتریان کلیدی
چ - فرایندها یا فرایندهای جدید یا کنارگذاشته شده
خ - ریسک (عملیاتی و مالی)

۱۵ انطباق

۱۵-۱ انطباق با الزامات قانونی

هدف : پرهیز از نقض هر نوع قانون، مقررات، تعهدات آیین نامه ای یا قراردادی و هر الزام امنیتی.
طراحی، عملکرد، استفاده و مدیریت سیستم‌های اطلاعات ممکن است منوط به الزامات آئین نامه ای، مقرراتی، و قراردادی باشد.
توصیه می‌شود الزامات قانونی خاص از مشاوران حقوقی سازمان یا دست اندرکاران حقوقی خاص و واجد شرایط درخواست شود. الزامات قانونی در کشورهای مختلف متفاوتند و ممکن است برای اطلاعات ایجاد شده در یک کشور که به کشور دیگر منتقل می‌شود تغییر کنند. (بعبارت دیگر جریان داده عبوری از مرز)

۱۵-۱-۱ شناسایی قوانین قابل اجرا

کنترل

تمامی مقررات، الزامات آیین نامه ای و قراردادی مرتبط و رویکرد سازمان نسبت به برآورده سازی این الزامات، باید برای هر سیستم اطلاعاتی و سازمان، به وضوح تعریف شده، مدون شده و به روز نگه داشته شوند.

راهنمای پیاده‌سازی

توصیه می‌شود کنترل های خاص و مسوولیت های فردی برای رعایت این الزامات تعریف و مستند شود.

۱۵-۱-۲ حقوق مالکیت فکری[1]

توصیه می‌شود به منظور حصول اطمینان از انطباق با الزامات قانون گزار، الزامات آیین نامه ای و قراردادی در استفاده از کالاهایی که ممکن است دارای حقوق مالکیت فکری باشد، و در هنگام استفاده از محصولات نرم‌افزاری دارای حقوق انحصاری، روشهای اجرایی مناسب، پیاده سازی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود رهنمودهای زیر برای محافظت از هر کالائی که ممکن است مالکیت فکری در نظر گرفته شود رعایت شود:

الف - انتشار خط مشی انطباق با حقوق مالکیت فکری که استفاده قانونی از محصولات نرم‌افزاری و اطلاعاتی را تعریف می‌کند

ب - دستیابی به نرم‌افزار فقط از طریق منابع شناخته شده و معتبر برای تضمین این که حق تکثیر نقض نمی‌شود.

پ - حفظ و آگاهی از خط مشی ها به منظور محافظت از حقوق مالکیت فکری و دادن اطلاعیه درباره برخورد انضباطی در برابر نقض آنها.

ت - نگهداری گزارش های مناسب از دارایی‌ها و شناسایی تمام آنها با الزامات مرتبط به منظور محافظت از حقوق مالکیت فکری

ث - حفظ شواهد و مدارک مالکیت گواهی‌ها و پروانه‌ها، دیسک‌های اصلی و راهنماها

1- Intellectual property rights (IPR)

ج - اجرای کنترل هایی برای تضمین این که حداکثر استفاده کنندگان مجاز از حد خاصی فراتر نمی رود.
چ - انجام بررسی هایی که فقط نرم‌افزارهای مجاز و محصولات دارای مجوز نصب می‌شوند
ح - ارایه خط مشی برای حفظ شرایط مناسب گواهی
خ - ارایه خط مشی برای دور ریز یا انتقال نرم‌افزار به دیگران
د - استفاده از ابزارهای مناسب ممیزی
ذ –مطابقت مفاد و شرایط نرم‌افزار و اطلاعات به دست آمده از شبکه‌های همگانی
ر - عدم تکثیر، تبدیل به قالب دیگر یا چکیده گرفتن غیر از مواردی که در قانون حق تکثیر مجاز دانسته شده‌اند
ز - عدم کپی برداری کامل یا جزئی از کتاب ها، مقالات، گزارش ها و دیگر مستندات غیر از مواردی که در قانون حق تکثیر مجاز دانسته شده اند..

اطلاعات دیگر

حقوق مالکیت فکری شامل حق تکثیر نرم‌افزار یا مستندات، حقوق طراحی، علائم تجاری، حق انحصاری، و گواهی های کد منبع است.

محصولات نرم‌افزاری اختصاصی معمولا در قالب یک قرارداد دارای مجوز تامین می‌شوند که مفاد و شرایط گواهی را مثلا برای محدود کردن استفاده از محصولات در ماشین های خاص یا محدود کردن کپی برداری برای ایجاد نسخه های پشتیبان مشخص می‌کند. شرایط حقوق مالکیت معنوی یک نرم‌افزار که توسط سازمان طراحی شده است باید برای کارکنان روشن شود.

الزامات قانونی، مقرراتی و قراردادی ممکن است محدودیت‌هایی در تکثیر مطالب اختصاصی ایجاد کند. به خصوص، ممکن است آنها این گونه حکم کنند که فقط مطالبی که توسط سازمان طراحی شده است یا توسط سازنده طی یک مجوز به سازمان داده شده است می‌تواند مورد استفاده قرار گیرد. نقض حق تکثیر ممکن است منجر به اقدام حقوقی شود که دربرگیرنده محاکمه کیفری است.

۱۵-۱-۳ حفاظت از سوابق سازمانی

کنترل

توصیه می‌شود سوابق مهم، با توجه به مقررات، الزامات آئین نامه ای، قراردادی و کسب وکار، در برابر گم شدن، تخریب و تحریف، محافظت شوند.

راهنمای پیاده‌سازی

توصیه می‌شود گزارش ها در بخش‌های مختلف گروه بندی شوند بعنوان مثال گزارش های حسابداری، گزارش های پایگاه داده‌ها، اطلاعات ثبت شده معاملات، اطلاعات ثبت شده ممیزی و رویه های عملیاتی که هر کدام جزئیاتی از دوره نگهداری و نوع رسانه ذخیره مثلا، کاغذ، میکروفیلم، مغناطیسی یا نوری را نشان می دهند. هر گونه مطلب و برنامه رمزنگاری و نسخه برداری مربوطه در رابطه با بایگانی های نسخه برداری شده یا امضاهای دیجیتال (رجوع کنید به ۱۲-۳) همچنین توصیه می‌شود برای ایجاد امکان رمزگشایی از گزارش‌ها برای طول دوره زمانی که گزارش‌ها نگهداری می‌شوند ذخیره شوند.

توصیه می‌شود درباره احتمال خرابی رسانه های به کار رفته به منظور ذخیره گزارش ها تمهیداتی اندیشیده شود. توصیه می‌شود رویه های ذخیره و استفاده، مطابق با پیشنهادات تولیدکننده اجرا شوند. توصیه می‌شود برای ذخیره بلندمدت، استفاده از کاغذ و میکروفیلم در نظر گرفته شود.

در جایی که رسانه های ذخیره‌سازی الکترونیکی انتخاب می‌شوند، توصیه می‌شود رویه هایی برای تضمین توانایی دسترسی به داده‌ها در سراسر دوره نگهداری گنجانده شود تا در برابر آسیب به دلیل تغییر فن‌آوری در آینده محافظت شود.

توصیه می‌شود سیستم‌های ذخیره‌سازی داده‌ها به گونه ای انتخاب شود که داده‌های مورد نیاز را بتوان در یک شکل و بازه زمانی قابل قبول با توجه به الزامات موجود نگهداری کرد.

توصیه می‌شود سیستم ذخیره اطلاعات کار شناسایی دقیق اسناد و دوره های حفظ آنها را به گونه ای که در مقررات یا قوانین ملی و منطقه ای تعریف شده است تضمین کند. این سیستم باید تخریب مناسب گزارش ها را پس از آن دوره در صورتی که سازمان به آنها نیاز ندارد مجاز شمارد.

به منظور رعایت این اهداف محافظتی، توصیه می‌شود مراحل زیر در یک سازمان انجام شوند:

الف – توصیه می‌شود رهنمود هایی درباره حفظ، ذخیره و کار و دور ریز گزارش‌ها و اطلاعات صادر شود.

ب - توصیه می‌شود یک جدول زمانی نگهداری برای شناسایی گزارش‌ها و دوره زمانی که برای آن نگهداری شده اند تهیه شود.

پ - توصیه می‌شود لیست موجودی از منابع اطلاعات کلیدی نگهداری شود

ت - توصیه می‌شود کنترل‌های مناسبی برای محافظت از گزارش‌ها و اطلاعات در برابر آسیب، تخریب، و تقلب اجرا شود.

اطلاعات دیگر

بعضی گزارش ها ممکن است نیازمند این باشند که به گونه ای امن حفظ شوند تا الزامات آئین نامه ای، مقرراتی یا قراردادی رعایت شوند و نیز فعالیت های ضروری کسب و کار پشتیبانی شوند.

به عنوان مثال گزارش هایی هستند که ممکن است به عنوان شواهدی که یک سازمان در چارچوب قوانین عمل می‌کند مورد نیاز باشند تا دفاع کافی دربرابر اقدامات غیر حقوقی یا حقوقی یا تایید وضعیت مالی یک سازمان در قبال سهام داران، اشخاص بیرونی، و حسابرسان تضمین شود. دوره زمانی و محتوای داده‌ها برای حفظ اطلاعات ممکن است توسط قوانین و مقررات ملی تعیین شوند.

اطلاعات بیشتر درباره مدیریت گزارش‌های سازمانی را می‌توانید در ISO 15489-1 بیابید.

۱۵-۱-۴ حفاظت داده‌ها و حریم خصوصی اطلاعات شخصی

کنترل

توصیه می‌شود حفاظت داده‌ها و حریم خصوصی آنگونه که در مقرارت و آئین نامه های مرتبط، و در صورت قابلیت اعمال، شرایط قراردادی، الزام شده، تضمین شود.

راهنمای پیاده‌سازی

توصیه می‌شود یک خط مشی سازمانی محافظت از داده‌ها طراحی و حریم خصوصی اجرا شود. توصیه می‌شود این خط مشی به تمام اشخاصی که در پردازش اطلاعات شخصی نقش دارند اطلاع داده شود.

انطباق با این خط مشی و تمام قوانین محافظت از داده‌های مربوطه و مقررات نیازمند ساختار و کنترل مدیریتی مناسب می باشند. اغلب این امر به بهترین نحو توسط انتصاب یک شخص مسوول مانند یک مامور محافظت از داده‌ها انجام می‌شود که توصیه می‌شود این شخص راهنمایی را برای مدیران، کاربران، و ارایه کنندگان خدمات درباره مسوولیت فردی و رویه های خاصی که توصیه می‌شود دنبال شود ارایه کند. توصیه می‌شود مسوولیت کار با اطلاعات شخصی و تضمین آگاهی از اصول مراقبت از داده‌ها مطابق با قوانین و مقررات مربوطه مورد توجه قرار گیرد. توصیه می‌شود اقدامات فنی و سازمانی مناسب برای محافظت از اطلاعات شخصی اجرا شود.

اطلاعات دیگر

تعدادی از کشورها مقرراتی دارند که کنترل هایی را درباره جمع آوری، پردازش و انتقال داده‌های شخصی اعمال می‌کند. با توجه به مقررات ملی مربوطه این کنترل ها ممکن است وظایفی را برای افراد جمع آوری کننده، پردازش کننده و منتشر کننده اطلاعات شخصی ایجاد کند و ممکن است امکان انتقال داده‌ها را به کشورهای دیگر محدود کند.

۱۵-۱-۵ پیشگیری از استفاده نابجا از امکانات پردازش اطلاعات

کنترل

توصیه می‌شود کاربران از بکارگیری امکانات پردازش اطلاعات برای مقاصد غیر مجاز، بازداشته شوند.

راهنمای پیاده‌سازی

توصیه می‌شود مدیریت استفاده از تجهیزات پردازش اطلاعات را تایید کند. هر گونه استفاده از این تجهیزات برای اهداف غیرکسب وکار بدون تایید مدیریت (رجوع کنید به بند ۶-۱-۴) یا برای هر گونه هدف غیرمجاز توصیه می‌شود به عنوان استفاده غیرمجاز از تجهیزات قلمداد شود. اگر هر فعالیت غیرمجازی از طریق کنترل یا طرق دیگر شناسایی شود، توصیه می‌شود این فعالیت به اطلاع مدیر خاص مربوطه برای بررسی اقدام حقوقی و یا انضباطی مناسب، برسد.

توصیه می‌شود مشاوره قانونی قبل از اجرای رویه های کنترل مورد استفاده قرار گیرد.

توصیه می‌شود تمام کاربران از هدف و دامنه کاربرد دقیق دسترسی مجازشان و کنترل‌های موجود برای کشف استفاده غیرمجاز آگاه باشند. این امر ممکن است از طریق اجازه دادن کتبی به کاربران، که توصیه می‌شود نسخه ای از آن توسط کاربر امضا شود و در اختیار سازمان باشد انجام شود. توصیه می‌شود که به کارکنان یک سازمان، پیمانکاران و کاربران شخص ثالث یادآوری شود که فقط دسترسی مجاز امکان پذیر است.

در زمان برقراری ارتباط با یک سیستم، توصیه می‌شود یک پیام هشدار ارایه شود که نشان می دهد که تجهیزات پردازش اطلاعاتی که کاربر وارد آن شده است متعلق به سازمان است و این که دسترسی غیرمجاز ممکن نیست. توصیه می‌شود کاربر اظهار کند که پیام را مشاهده کرده است تا بتواند در فرآیند برقراری ارتباط به کار خود ادامه دهد. (رجوع کنید به بند ۱۱-۵-۱).

اطلاعات دیگر

تجهیزات پردازش اطلاعات، یک سازمان عمدتا و منحصرا برای اهداف کسب وکار می باشد. کشف ورود غیرمجاز، بررسی محتوا و دیگر ابزارهای کنترلی می‌توانند به پیشگیری و کشف سوء استفاده از تجهیزات پردازش اطلاعات کمک کنند.

بسیاری از کشورها مقرراتی برای محافظت دربرابر سوء استفاده از رایانه دارند. استفاده از یک رایانه برای اهداف غیرمجاز ممکن است یک تخلف کیفری محسوب شود.
قانونی بودن کنترل استفاده در کشورهای مختلف متفاوت است و ممکن است نیازمند این باشد که مدیریت به تمام کاربران این کنترل را اطلاعات دهد و موافقت آنها را کسب کند.
در جایی که سیستم مورد استفاده برای دسترسی همگانی مورد استفاده قرار می‌گیرد (برای مثال، یک سرویس دهنده عمومی وب)، و در معرض کنترل امنیتی است باید پیامی روی صفحه ظاهر شود و این را نشان دهد.

۱۵-۱-۶ مقرارت کنترل‌های رمزنگاری

کنترل

توصیه می‌شود کنترل‌های رمزنگاری در انطباق با تمامی‌توافق نامه ها، قوانین و مقررات مرتبط، بکارگرفته شوند.

راهنمای پیاده‌سازی

توصیه می‌شود موارد زیر برای انطباق با قراردادها، قوانین، و مقررات مربوطه در نظر گرفته شود:

الف - محدودیت‌های ورود و/یا صدور سخت افزار و نرم‌افزار رایانه برای اجرای عملکردهای رمزنگاری

ب - محدودیت‌هایی درباره ورود یا خروج نرم‌افزار و سخت افزار رایانه‌ی که برای اضافه شدن کارایی رمزنگاری طراحی شده اند.

پ - محدودیت‌هایی درباره استفاده از رمزنگاری

ت - روش های اجباری یا اختیاری دسترسی به اطلاعات رمزنگاری شده توسط سخت افزار یا نرم‌افزار برای تضمین محرمانگی محتوا

توصیه می‌شود مشاوره قانونی برای تضمین انطباق با قوانین و مقررات ملی انجام شود. قبل از این که اطلاعات رمزنگاری شده یا کنترل های رمزنگاری به کشور دیگری منتقل شود توصیه می‌شود مشاوره قانونی انجام شود.

۱۵-۲ انطباق با خط‌مشی‌ها و استانداردهای امنیتی، و انطباق فنی

هدف : حصول اطمینان از انطباق سیستم‌ها با خط مشی ها و استانداردهای امنیتی سازمانی.
توصیه می‌شود امنیت سیستم‌های اطلاعات به طور منظم بررسی شود.
توصیه می‌شود این بررسی ها در قبال خط مشی های امنیتی مناسب و الگوهای فنی انجام شوند و توصیه می‌شود سیستم‌های اطلاعات برای انطباق با استانداردهای امنیتی حاکم و کنترل های امنیتی مستند مورد ممیزی قرار گیرند.

۱۵-۲-۱ انطباق با خط‌مشی‌ها و استانداردهای امنیتی

کنترل

برای حصول انطباق با خط مشی ها و استانداردهای امنیتی، توصیه می‌شود مدیران از اینکه تمامی روش‌های اجرایی امنیتی، در حیطهٔ مسوولیت شان، به درستی اجرا می‌شوند، اطمینان حاصل نمایند.

راهنمای پیاده‌سازی

توصیه می‌شود مدیران انطباق پردازش اطلاعات را در حوزه مسوولیت خود با خط مشی ها، استانداردها و دیگر الزامات امنیتی مناسب بررسی کنند.

اگر هر گونه عدم انطباق در نتیجه بررسی مشاهده شود، توصیه می‌شود مدیران:

الف - علل عدم انطباق را تعیین کنند

ب – ارزشیابی نیاز به اقداماتی برای اطمینان از عدم وقوع مجدد عدم انطباق

پ - اقدام اصلاحی مناسب را تعیین واجرا کنند

ت - اقدامات اصلاحی انجام شده را بررسی کنند.

توصیه می‌شود نتایج بررسی ها و اقدامات اصلاحی انجام شده توسط مدیران ثبت شود و توصیه می‌شود این گزارش ها نگهداری شوند. توصیه می‌شود مدیران نتایج را به اشخاصی که بررسی های مستقل (رجوع کنید به بند ۶-۱-۸) را انجام می دهند در زمانی که بررسی های مستقل در حوزه مسوولیت شان انجام می‌شود گزارش کنند.

اطلاعات دیگر

کنترل عملیاتی استفاده از سیستم در ۱۰-۱۰ آمده است.

۱۵-۲-۲ بررسی انطباق فنی

کنترل

توصیه می‌شود به منظور انطباق با استانداردهای پیاده سازی امنیت، سیستم‌های اطلاعاتی به طور منظم بررسی شوند.

راهنمای پیاده‌سازی

توصیه می‌شود بررسی انطباق فنی یا به طور دستی (اگر لازم باشد، پشتیبانی شده بوسیله ابزارهای نرم‌افزاری مناسب)توسط یک مهندس با تجربه سیستم و/یا با کمک ابزارهای اتوماتیک که گزارش فنی را برای تفسیر متعاقب توسسط یک متخصص فنی آماده می‌کند انجام شوند.

اگر آزمون‌های نفوذ یا ارزیابی‌های آسیب‌پذیری مورد استفاده قرار می‌گیرند، توصیه می‌شود احتیاط شود زیرا این فعالیت‌ها ممکن است منجر به نقض امنیت سیستم شوند. توصیه می‌شود این آزمون‌ها برنامه ریزی شده، مستند و قابل تکرار باشند.

توصیه می‌شود هر بررسی انطباق فنی فقط بوسیله اشخاص مجاز وشایسته انجام شود، یا تحت نظارت چنین افرادی صورت گیرد.

اطلاعات دیگر

بررسی انطباق فنی دربرگیرنده بررسی سیستم‌های عملیاتی برای تضمین این است که کنترل‌های سخت افزاری و نرم‌افزاری به طور صحیح اجرا شده اند. این نوع بررسی‌های انطباق نیازمند تخصص فنی یک متخصص است.

بررسی انطباق همچنین مثلا آزمون نفوذ و ارزیابی‌های آسیب‌پذیری را شامل می‌شود که ممکن است توسط کارشناسان مستقلی که به طور خاص برای این منظور در نظر گرفته شده اند انجام شود. این ممکن است در کشف آسیب‌پذیری‌ها در سیستم و برای بررسی این که کنترل‌ها در پیشگیری از دسترسی غیرمجاز به دلیل این آسیب‌پذیری‌ها تا چه حد موثر هستند مفید باشد.

آزمون نفوذ و ارزیابی‌های آسیب‌پذیری مجرایی برای یک سیستم در زمان خاص ایجاد می‌کنند. این محدود به بخش‌هایی از سیستم است که در واقع در طول اقدامات نفوذ آزموده می‌شوند. آزمون نفوذ و ارزیابی‌های آسیب‌پذیری جایگزین ارزیابی ریسک نیستند.

۱۵-۳ ملاحظات ممیزی سیستم‌های اطلاعاتی

هدف : بیشینه کردن اثربخشی و کمینه کردن اختلال در فرآیند ممیزی سیستم‌های اطلاعاتی.
توصیه می‌شود برای محافظت از سیستم‌های عملیاتی و ابزارهای بازرسی در طول بازرسی سیستم‌های اطلاعات کنترل هایی موجود باشد.
محافظت همچنین برای حفظ یکپارچگی و پیشگیری از سوء استفاده از ابزارهای ممیزی لازم است.

۱۵-۳-۱ کنترل‌های ممیزی سیستم‌های اطلاعاتی

کنترل
توصیه می‌شود الزامات و فعالیت های ممیزی مرتبط با بررسی های سیستم‌های عملیاتی، به دقت طرح‌ریزی و مورد توافق قرار گیرند تا ریسک‌های ناشی از توقف در فرآیندهای کسب وکار، کمینه شوند.
راهنمای پیاده‌سازی
توصیه می‌شود رهنمودهای زیر رعایت شوند:

الف - توصیه می‌شود الزامات بازرسی با مدیریت مناسب مورد توافق قرار گیرند.
ب - توصیه می‌شود هدف و دامنه کاربرد بررسی‌ها مورد توافق قرار گرفته و کنترل شود.
پ - توصیه می‌شود بررسی‌ها محدود به دسترسی فقط خواندنی به نرم‌افزار یا داده‌ها باشد
ت - توصیه می‌شود دسترسی غیر از فقط خواندنی فقط برای نسخه‌های جدا شده فایل‌های سیستم، مجاز شوند که توصیه می‌شود در زمانی که بازرسی کامل می‌شود پاک شوند. یا در صورتی که الزامی به حفظ این فایل‌ها تحت شرایط مستندسازی بازرسی وجود دارد محافظت مناسب از آنها به عمل آید.
ث - توصیه می‌شود منابع مورد نیاز جهت اجرای بررسی ها صریحا شناسایی شده و در دسترس قرار گیرد.
ج - توصیه می‌شود الزامات پردازش اضافه، شناسایی شده مورد توافق قرار گیرد
چ - توصیه می‌شود تمام دسترسی کنترل و ثبت شود تا یک گزارش مرجع موجود باشد؛ استفاده از گزارش‌های ممهور باید برای اطلاعات یا سیستم‌های حیاتی در نظر گرفته شود.
ح - توصیه می‌شود تمام رویه‌ها، الزامات و مسوولیت‌ها مستند شوند
خ - توصیه می‌شود شخص یا اشخاصی که بازرسی را انجام می‌دهند از فعالیت‌های مورد بازرسی مستقل باشد.

۱۵-۳-۲ حفاظت از ابزارهای ممیزی سیستم‌های اطلاعاتی

کنترل
توصیه می‌شود به منظور پیشگیری از هرگونه استفادهٔ نابجا یا به خطر افتادن احتمالی، دسترسی به ابزارهای ممیزی سیستم‌های اطلاعاتی، محافظت شده باشد.
راهنمای پیاده‌سازی
توصیه می‌شود ابزارهای کنترل سیستم‌های اطلاعات مانند نرم‌افزارها یا فایل های داده‌ها، از سیستم‌های توسعه و عملیاتی تفکیک شوند و در کتابخانه های نوار یا مناطق کاربر نگهداری نشوند مگر این که سطح مناسبی از محافظت اضافه را دریافت کنند.

اطلاعات دیگر

اگر اشخاص ثالث در بازرسی شرکت دارند، ممکن است خطر سوء استفاده از ابزارهای حسابرسی توسط این اشخاص ثالث وجود داشته باشد، و اطلاعات توسط این سازمان شخص سوم مورد دسترسی قرار گیرد. توصیه می‌شود کنترل هایی نظیر ۶-۲-۱ (برای ارزیابی ریسک ها) و ۹-۱-۲ (برای محدودسازی دسترسی فیزیکی) را می‌توان برای پرداختن به ریسک و هر گونه پیامد آن نظیر کلمات عبوری که فورا تغییر می‌کنند و در معرض دید بازرسی کننده ها قرار دارند باید در نظر گرفته شود.

کتابنامه

۱- استاندارد ملی ایران ۱-۹۹۷۰: سال ۱۳۸۶، فن‌آوری اطلاعات - تکنیک‌های امنیت - مدیریت امنیت تکنولوژی ارتباطات و اطلاعات – قسمت اول: مفاهیم و مدل‌های مدیریت امنیت تکنولوژی ارتباطات و اطلاعات

۲- استاندارد ملی ایران ایزو ۱۹۰۱۱: سال ۱۳۸۶، رهنمودهایی برای ممیزی سیستم‌های مدیریت کیفیت و/یا زیست محیطی

3- ISO/IEC Guide 2:1996, Standardization and related activities – General vocabulary

4- ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards

5- ISO/IEC TR 13335-3:1998, Information technology – Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT Security

6- ISO/IEC 13888-1: 1997, Information technology – Security techniques – Non-repudiation – Part 1: General

7- ISO/IEC 11770-1:1996 Information technology – Security techniques – Key management – Part 1: Framework

8- ISO/IEC 9796-2:2002 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms

9- ISO/IEC 9796-3:2000 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms

10- ISO/IEC 14888-1:1998 Information technology – Security techniques – Digital signatures with appendix – Part 1: General

11- ISO/IEC 15408-1:1999 Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model

12- ISO/IEC 14516:2002 Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services

13- ISO 15489-1:2001 Information and documentation – Records management – Part 1: General

14- ISO 10007:2003 Quality management systems – Guidelines for configuration management

15- ISO/IEC 12207:1995 Information technology – Software life cycle processes

16- OECD Guidelines for the Security of Information Systems and Networks: ‘Towards a Culture of Security’, 2002

17- OECD Guidelines for Cryptography Policy, 1997

18- IEEE P1363-2000: Standard Specifications for Public-Key Cryptography

19- ISO/IEC 18028-4 Information technology – Security techniques – IT Network security – Part 4: Securing remote access

20- ISO/IEC TR 18044 Information technology – Security techniques – Information security incident

فصل چهارم

فناوری اطلاعات - فنون امنیتی- راهنمای اجرای سامانه مدیریت امنیت اطلاعات

ISO/IEC 27003

Information technology-- Security techniques Information security management system implementation guidance

پیش گفتار

استاندارد "فناوری اطلاعات- فنون امنیتی – راهنمای اجرای سامانه مدیریت امنیت اطلاعات" که پیش نویس آن در کمیسیون فنی مربوط ،توسط .....سازمان استاندارد، بر مبنای روش تنفیذ مورد اشاره در راهنمای ISO/IEC Guide21-1 (پذیرش منطقه ای یا ملی استاندارد های " بین المللی/ منطقه ای" و دیگر مدارک استاندارد) به عنوان استاندارد ملی ایران ، تهیه شده ودر یک صد و سی هفتمین اجلاسیه کمیته ملی استانداردرایانه و فر آوری داده.مورخ .۱۳۸۹/۱۲/۲۴.مورد تصویب قرارگرفته است اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱،به عنوان استانداردملی ایران منتشر می گردد.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفتهای ملی و جهانی در زمینه صنایع ،علوم وخدمات ،استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهدشدو هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود،در هنگام تجدیدنظردرکمیسیون فنی مربوط،موردتوجه قرارخواهدگرفت.بنابراین همواره از آخرین تجدیدنظرآنها استفاده خواهدشد.

این استاندارد ملی بر اساس پذیرش استاندارد" بین المللی " به شرح زیر است:

ISO/IEC 27003: 2010, Information technology – security techniques – information security management implementation guidance

فناوری اطلاعات ـ فنون امنیتی ـ راهنمای اجرای سامانه مدیریت امنیت اطلاعات

۱ هدف و دامنه کاربرد

این استاندارد ملی، براساس پذیرش استاندارد بین المللی ISO/IEC 27003:2010 تدوین شده است.

هدف از تدوین این استانداردتمرکز بر روی جنبه های حیاتی مورد نیاز برای طراحی و اجرای یک سامانه مدیریت امنیت اطلاعاتی۱ (ISMS) هماهنگ با استاندارد ملی ایران – ایزو آی ای سی ۲۷۰۰۱ : سال ۸۷ است.

این استاندارد فرآیند ویژگی سیستم مدیریت امنیت اطلاعات و طراحی آن از ابتدا تا تولید طرحهای اجرایی را توصیف می کند. این استاندارد فرآیند دستیابی به تایید مدیریت جهت اجرای سیستم مدیریت امنیت اطلاعات، معرف پروژه ای جهت اجرای سامانه مدیریت امنیت اطلاعات (که در این استاندارد ملی به عنوان پروژه ISMS بیان شده است.) و راهنمایی جهت طرح ریزی پروژه ISMS فراهم می کند که منجر به طرح نهایی اجرای پروژه ISMS می شود.

این استاندارد ملی مخصوص در سازمان های اجرا کننده ISMS است. این استاندارد قابلیت کاربرد برای تمام انواع سازمان ها در تمامی ابعاد را دارا می باشد (برای مثال بنگاههای اقتصادی تجاری ، ارگان های دولتی،سازمان های غیرانتفاعی) . پیچیدگی هر سازمان و ریسک هایش منحصر بفرد می باشد و الزامات ویژه آن منجر به اجرای ISMS می شود. سازمانهای کوچکتر فعالیتهای ذکرشده در این استاندارد ملی را برای خود، کاربردی میدانند و میتوانند آن را ساده سازی کنند. سازمانهای با مقیاس بزرگترو پیچیده متوجه می شوند که سازمان با لایه های ساختاری یا سامانه مدیریت ، برای مدیریت فعالیتهای این استاندارد ملی به صورت اثر بخش مورد نیاز می باشد. اگرچه، در دو حالت ذکرشده ، میتوانند فعالیتهای مرتبطی برای کاربرد این استاندارد ملی طرح ریزی شود.

این استاندارد ملی توضیحات و توصیه هایی ارائه می دهد که تعیین کننده هیچ گونه الزاماتی نمی باشد . این استاندارد به منظور استفاده مقارن با استاندارد ملی ایران–ایزو آی ای سی ۲۷۰۰۲ : سال ۸۷ ایجاد شده است ، اما قصد اصلاح و/یا کم کردن الزامات مشخص شده در استاندارد ملی ایران– ایزو آی ای سی ۲۷۰۰۱ و یا توصیه های فراهم شده در استاندارد ملی ایران– ایزو آی ای سی ۲۷۰۰۲ : سال ۸۷ را ندارد . ادعای تطابق با این استاندارد ملی صحیح نمی باشد .

۲ مراجع الزامی

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

در صورتی که با مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه هـا و تجدیـد نظرهـای بعدی آن مورد نظر این استاندارد ملی نیست. در مورد مدارکی بدون ذکر تـاریخ انتشـار بـه آن هـا ارجاع داده شده است،همواره آخرین تاریخ تجدید نظر و اصلاحیه های بعدی آن ها مورد نظر است . استفاده از مراجع زیر برای این استاندارد الزامی است :

2-1 ISO/IEC 27000:2009 Information technology – security techniques – information security management system – overview and vocabulary

۲-۲ استاندارد ملی ایران – ایزو آی ای سی ۲۷۰۰۱ : سال ۸۷، فن آوری اطلاعات ،فنون امنیتی – سیستم های مدیریت امنیت اطلاعات – الزامات

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف تعریف شده در استاندارد ایران– ایزو آی ای سی ۲۷۰۰۱ : سال ۸۷ و استاندارد ISO/IEC 27000:2009 کاربرد دارد .

کلیه بندهای استاندارد بین المللی ISO/IEC 27003: 2010 در مورد این استاندارد معتبر و الزامی است.

فصل پنجم

فناوری اطلاعات- فنون امنیتی-مدیریت امنیت اطلاعات - سنجش

ISO/IEC 27004(14096)

Information technology-- Security techniques
Information security management
Measurement

پیش‌گفتار

استاندارد" فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات-سنجش" که پیش نویس آن درکمیسیون‌های مربوط توسط سازمان استاندارد و تحقیقات صنعتی ایران تهیه و تدوین شده و دریکصد و سی و دومین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۸۹/۱۲/۱۶ مورد تصویب قرار گرفته است ، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ ، به عنوان استاندارد ملی ایران منتشر می‌شود .

برای حفظ همگامی‌و هماهنگی با تحولات و بهبودهای ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

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

ISO/IEC27004- Information technology-Security techniques-Information Security management-Measurement

۰ مقدمه

۰-۱ عمومی

این استاندارد ملی راهنمایی‌هایی در مورد توسعه و استفاده از سنجه‌ها و سنجش به منظور ارزیابی تاثیر گذاری یک سامانه مدیریت امنیتی اطلاعات پیاده سازی شده (ISMS)[1] و کنترل‌ها یا گروه‌هایی از کنترل‌های مشخص شده در ISO/IEC 27001 فراهم می‌آورد.

این شامل سیاست، مدیریت ریسک امنیت اطلاعات، اهداف کنترلی، کنترل‌ها، فرآیندها وزیر رویه‌ها می‌شود، و فرآیند بازبینی آن‌ها را پشتیبانی می‌کند، و به مشخص کردن این که آیا هیچیک از فرآیندهای ISMS یا کنترل نیاز به تغییر یا بهبود بخشیدن دارند یا نه، کمک می‌کند. نیاز است به خاطر سپرده شود که هیچ‌یک از سنجش کنترل‌ها نمی‌توانند امنیت کامل را تضمین کنند.

پیاده سازی این رویکرد یک برنامه‌ی سنجش امنیت اطلاعات را تشکیل می‌دهد. برنامه‌ی سنجش امنیت اطلاعات با مدیریت، در شناسایی و ارزیابی فرآیندهای ISMS، ناسازگار و غیر موثر و کنترل‌ها با اولویت بندی اعمال مرتبط با بهبود، یا تغییر این فرآیندها و/ یا کنترل‌ها، همکاری خواهد کرد. و همچنین مجاز است که در اثبات انطباق ISO/IEC 27001 با سازمان همکاری کند و مدارک اضافی برای بازبینی مدیریت و فرآیندهای مدیریت ریسک امنیت اطلاعات فراهم آورد.

این استاندارد ملی فرض می‌کند که نقطه‌ی شروع برای توسعه‌ی سنجه‌ها و سنجش‌ها یک فهم دقیق از ریسک امنیت اطلاعات که‌یک سازمان با آن مواجه می‌شود، و این که فعالیت‌های ارزیابی ریسک یک سازمان به درستی اجرا شده‌اند (یعنی براساس ISO/IEC 27005)، همانطورکه با ISO/IEC 27001 الزام شده است. برنامه‌ی سنجش امنیت اطلاعات یک سازمان را به فراهم آوردن اطلاعات قابل اعتماد برای سهام‌داران مربوطه درباره‌ی ریسک‌های امنیت اطلاعات آن و وضعیت ISMS پیاده‌سازی شده‌ی آن، به منظور مدیریت این ریسک‌ها، تشویق می‌کند.

برنامه‌ی امنیت اطلاعات که به طور موثر پیاده سازی شده است، اطمینان سهام‌داران را در نتیجه‌ها سنجش‌ها بهبود می‌بخشد، و سهام‌داران را قادر به استفاده از این سنجه‌ها برای اجرای بهبود پی در پی امنیت اطلاعات و ISMS، می‌سازد.

نتیجه‌ها ذخیره سازی شده‌ی سنجش‌ها اجازه مقایسه‌ی بهبود در دستیابی به هدف‌ها امنیت اطلاعات را در طی یک دوره‌ی زمانی، به عنوان بخشی از یک فرآیند بهبود مستمر ISMS یک سازمان، خواهد داد.

۰-۲ مرور کلی بر مدیریت

ISO/IEC 27001 سازمان را مستلزم «انجام بررسی‌های منظم اثربخشی نتیجه‌ها به اجرای ISMS از سنجش موثر» و «سنجش اثر بخشی کنترل‌ها، برای اثبات این که الزامات امنیتی برآورده شده‌اند » می‌کند. ISO/IEC 27001 همچنین سازمان را مستلزم «تعریف کردن این که چگونه اثر بخشی کنترل‌ها یا گروه‌های کنترل‌های

1- information security management system

مشخص شده سنجش شوند و مشخص کردن این که چگونه این سنجه‌ها قرار است برای ارزیابی اثر بخشی کنترل به منظور تولید نتیجه‌ها قابل مقایسه و تجدید پذیر مورد استفاده قرار می‌گیرند» می‌کند.

رویکرد اتخاذ شده از سوی یک سازمان به منظور تحقق الزامات سنجش که در ISO/IEC 27001 مشخص شده، براساس تعدادی از عوامل قابل توجه متغیر خواهد بود، که شامل ریسک‌های امنیت اطلاعاتی که سازمان با آن مواجه است، اندازه‌ی سازمانی آن، منابع در دسترس، و برنامه قانون کاربردی[1]، الزامات تنظیمیو قراردادی، می‌شود. انتخاب و توجیه دقیق روش مورد استفاده برای برآوردن الزامات سنجش برای اطمینان حاصل کردن از این که به ضرر دیگران، منابع بیش از اندازه به این فعالیت‌های ISMS اختصاص داده نشده‌اند مهم هستند. به طور ایده‌آل، فعالیت‌های در حال انجام سنجش به صورت عملیات منظم سازمان‌ها با حداقل الزامات منابع اضافی، تکمیل خواهند شد.

این استاندارد ملی توصیه‌هایی درباره‌ی فعالیت‌های ذیل به عنوان یک مبنا برای یک سازمان، به منظور برآوردن الزامات سنجش مشخص شده در ISO/IEC 27001 می‌کند:

الف) توسعه‌ی سنجه‌ها (به عنوان مثال سنجه‌های پایه، سنجه‌های مشتق و شاخص‌ها)

ب) پیاده سازی و اداره کردن یک برنامه سنجش امنیت اطلاعات

پ) جمع آوری و تحلیل داده

ت) توسعه‌ی نتیجه‌ها سنجش‌ها

ث) ارتباط دادن نتیجه‌ها توسعه‌یافته‌ی سنجش به سهام‌داران مربوطه

ج) استفاده از نتیجه‌ها سنجش‌ها به عنوان عوامل ارائه‌ی تصمیمات مربوط به ISMS

چ) استفاده از نتیجه‌ها سنجش‌ها به منظور شناسایی نیازها برای بهبود بخشیدن به ISMS پیاده سازی شده، شامل دامنه‌ی کاربرد، سیاست‌ها، هدف‌ها، کنترل‌ها، فرآیندها و زیر رویه‌ها،

ح) تسهیل بهبود پی در پی برنامه‌ی سنجش امنیت اطلاعات.

یکی از عواملی که توانایی سازمان برای دستیابی به سنجش را تحت فشار قرار می‌دهد، اندازه‌ی آن است. به طور کلی اندازه و پیچیده گی تجارت در ترکیب با اهمیت امنیت اطلاعات، اندازه‌ی سنجش‌های مورد نیاز را هم از نظر تعداد و هم از نظر سنجه‌هایی که انتخاب می‌شوند و تناوب جمع آوری و تحلیل داده، تحت تاثیر قرار می‌دهند. برای SME‌ها[2] (سرمایه گذاری‌های کوچک و متوسط) یک برنامه‌ی سنجش امنیت اطلاعات که کمتر جامع است کافی خواهد بود، در حالی که سرمایه گذاری‌های بزرگ برنامه‌های چند گانه‌ی سنجش امنیت اطلاعات را پیاده سازی و اداره خواهند کرد.

یک برنامه‌ی واحد سنجش امنیت اطلاعات ممکن است برای سازمان‌های کوچک کافی باشد، در حالی که برای سرمایه گذاری‌های بزرگ نیاز به برنامه‌های سنجش امنیت اطلاعات چند گانه مجاز است وجود داشته باشد.

رهنمود فراهم آمده با این استاندارد ملی منجر به تولید مستنداتی می‌شود که برای اثبات این که اثر بخشی کنترل، مورد ارزیابی و سنجش قرار می‌گیرد، خواهد شد.

1- applicable legal

2- Small and Medium Enterprises

فناوری اطلاعات- فنون امنیت- مدیریت امنیت اطلاعات- سنجش

۱ هدف و دامنه‌ی کاربرد

هدف از تدوین این استاندارد ملی تعیین رهنمودهایی برای توسعه و استفاده‌ی سنجه‌ها[۱] و سنجش[۲] به منظور ارزیابی اثربخشی یک سامانه مدیریت امنیت اطلاعات پیاده سازی شده (ISMS) و کنترل‌ها یا گروهی از کنترل‌ها، همانطور که در استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ مشخص شده، فراهم می‌آورد.
این استاندارد ملی برای همه انواع و اندازه‌های سازمان قابل اجراست.

یادآوری- - این استاندارد برای بیان ماده قانون‌ها از شکل‌های گفتاری استفاده می‌کند (به عنوان مثال " باید[۳] " ، " نباید[۴] " ، " توصیه می‌شود[۵] " ، " توصیه نمی‌شود[۶] "، " مجاز است[۷] " ، " نیازی نیست[۸] "، " می‌توان[۹] " و " نمی‌توان[۱۰] ") که در رهنمودهای استانداردملی ایران شماره ۵ سال ۱۳۸۶، پیوست ح مشخص شده‌اند . همچنین ISO/IEC 27000:2009 ، پیوست A نیز مشاهده شود.

۲مراجع 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 می‌شود. 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 و انتشار به آنها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آنها مورد نظر است.استفاده از مرجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 27000:2009, Information technology — Security techniques — Information security management systems — Overview and vocabulary

۲- ۲ استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ ، فناوری اطلاعات - فنون امنیتی- سامانه‌های مدیریت امنیت اطلاعات – الزامات

1- Measures
2- Measurment
3- Shall
4 - shall not
5 - should
6 - should not
7 - may
8 - need not
9 - can
10 - cannot

۳اصلاحات و تعاریف

در این استاندارد علاوه بر اصطلاحات و تعاریف تعیین شده در ISO/IEC 27000، اصطلاحات و تعاریف زیر نیز به کار می‌رود:

۳-۱ مدل تحلیلی[1]

الگوریتم یا ترکیب محاسباتی یک یا بیشتر، پایه‌ها سنجه‌های مبنا و یا مشتق به همراه معیار تصمیم آن.

[استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷[2]]

۳-۲ صفت[3]

صفت[4] یا مشخصه[5]ی یک شیء[6] که می‌تواند به طور کمی‌یا کیفی با انسان یا به طور خودکار تشخیص داده شود.

[استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷]

۳-۳ سنجه‌ی مبنا[7]

سنجه‌ی تعریف شده در چهار چوب یک صفت و روشی برای تعیین کمیت آن است.

[استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷]

یادآوری- - یک سنجه‌ی مبنا در عمل مستقل از سایر سنجه‌هاست.

۳-۴داده

مجموعه‌ی مقادیر اختصاص داده شده به سنجه‌های مبنا، سنجه‌های مشتق و/یا شاخص‌ها است.

[استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷]

۳-۵معیار تصمیم[8]

آستانه‌ها، هدف‌ها، یا الگوهای استفاده شده به منظور تعیین نیاز برای اقدام یا تحقیق بیشتر، یا برای توصیف میزان اطمینان در یک نتیجه‌ی داده شده، استفاده می‌شود.

[استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷]

۳-۶ سنجه‌ی مشتق[9]

سنجه‌ای که به عنوان یک تابع از مقادیر دو یا بیشتر از سنجه‌ی مبنا تعریف شده است.

[استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷]

۳-۷ شاخص[10]

1- analytical model
2- ISO/IEC 15939:2007
3- attribute
4- property
5- characteristic
6- object
7- base measure
8- decision criteria
9- derived measure
10- indicator

سنجه‌ای که، ارزیابی یا تخمینی از صفات مشخص شده‌ی مشتق از یک مدل تحلیلی را با توجه به نیازهای اطلاعاتی تعریف شده فراهم می‌آورد.

۳-۸ نیاز اطلاعاتی

بینش ضروری برای مدیریت بر مقاصد، هدف‌ها، ریسک‌ها و مشکلات
[استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷]

۳-۹ سنجه

متغیری که به آن مقداری به عنوان نتیجه‌ی یک سنجش اختصاص داده می‌شود
[استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷]

یادآوری- – واژه‌ی " سنجه‌ها " به طور جمعی برای ارجاع به سنجه‌های مبنا، سنجه‌های مشتق، و شاخص‌ها مورد استفاده قرار می‌گیرد.

مثال– مقایسه‌ی یک نرخ نقص اندازه گیری شده با نرخ نقص برنامه ریزی شده همراه با یک ارزیابی از اینکه آیا تفاوت یک مشکل را نشان می‌دهد یا خیر.

۳-۱۰سنجش

فرآیند به‌دست آوردن اطلاعات در مورد اثر بخشی ISMS و کنترل‌ها با استفاده از یک روش سنجش، یک تابع سنجش، یک مدل تحلیلی، و معیار تصمیم، است.

۳-۱۱ تابع سنجش

الگوریتم یا محاسبه‌ی انجام شده به منظور ترکیب دو یا بیشتر از سنجه‌های مبنا است.
[استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷]

۳-۱۲ روش سنجش

دنباله‌ای منطقی از عملیات، تعریف شده به طور عمومی، که در تعیین کمیت یک صفت با توجه به‌یک مقیاس مشخص شده مورد استفاده قرار می‌گیرد.
[استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷]

یادآوری- نوع روش سنجش به ماهیت عملیات که برای تعیین کمیت یک صفت استفاده می‌شوند بستگی دارد. دو نوع مشخص می‌شود:

- درونی: اندازه گیری شامل رای انسانی
- برونی: اندازه گیری براساس قوانین عددی.

۳-۱۳ نتیجه‌های سنجش

یک یا بیشتر از شاخص‌ها و تفسیرهای وابسته‌ی آن‌ها که به‌یک نیاز اطلاعاتی را نشان می‌دهد.

۳-۱۴ شیء

قلم مشخص شده از طریق سنجش صفت‌های آن، است.

۳-۱۵ مقیاس

مجموعه ای از مقادیر منظم، به صورت پیوسته یا مجزا، یا مجموعه ای از رده‌ها که صفت به آن‌ها ترسیم می‌شود.

[استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷]

یادآوری- نوع مقیاس بستگی دارد به ماهیت ارتباط بین مقادیر در آن مقیاس. عموما چهار نوع از مقیاس‌ها تعریف شده‌اند :

صوری: مقادیر سنجش مطلق هستند

ترتیبی: مقادیر سنجش رتبه بندی هستند

وقفه: مقادیر سنجش متناظر با کمیت‌های مساوی از صفت، فواصل مساوی دارند

نسبت: مقادیر سنجش متناظر با کمیت‌های مساوی از صفت فواصل مساوی دارند، جایی که مقدار صفر متناظر با هیچیک از صفات نیست.

این‌ها فقط مثال‌هایی از انواع مقیاس هستند.

۳-۱۶ واحد سنجش

کمیتی خاص، تعریف شده و برگزیده شده با قرارداد، که با آن سایر کمیت‌ها از همان نوع به منظور بیان قدر نسبت آن‌ها با آن کمیت، مقایسه می‌شوند

[استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷]

۳-۱۷ اعتبار

تاییدی است از طریق تهیه‌ی شاهد عینی، به طوری که الزامات برای یک کاربرد یا استفاده‌ی خاص از قبل در نظر گرفته شده، برآورده شده‌اند .

۳-۱۸تصدیق

تایید از طریق تهیه‌ی شواهد عینی، که الزامات مشخص شده به خوبی، برآورده شده است.

[استاندارد ایران- ایزو ۹۰۰۰-سال ۸۷[1]]

یادآوری- این می‌تواند آزمون انطباق نیز نامیده شود.

۴ساختار این استاندارد ملی

این استاندارد ملی توضیح عمل سنجه‌ها و سنجش‌های مورد نیاز برای ارزیابی اثر بخشی الزامات ISMS برای مدیریت کنترل‌های امنیتی کافی و متناسب، که در بند ۴-۲ از استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷، الزام شده است، فراهم می‌آورد.

این استاندارد ملی به صورت ذیر ساخت یافته است:

- مرور کلی بر برنامه‌ی سنجش امنیت اطلاعات و مدل سنجش امنیت اطلاعات (بند۵)
- مسئولیت‌های مدیریت برای سنجش‌های امنیت اطلاعات (بند۶)

1- ISO 9000:2005

- طرح‌ریزی‌های سنجش و فرآیندها (به عنوان مثال طرح و توسعه‌ی، پیاده سازی و عملکرد، و بهبود بخشیدن سنجش‌ها: برقراری ارتباط با نتیجه‌های سنجش‌ها) برای اینکه در برنامه‌ی سنجش امنیت اطلاعات پیاده‌سازی شوند (بندهای ۷ تا ۱۰).

به علاوه، پیوست الف یک الگوی مثال برای طرح‌ریزی سنجش که درآن اجزاء سازنده عنصرهای مدل سنجش امنیت اطلاعات هستند، فراهم می‌آورد (به بند ۷ مراجعه شود). پیوست ب مثال‌های طرح‌ریزی سنجش را برای کنترل‌های خاص یا فرآیندهای یک ISMS ، با استفاده از الگوی تهیه شده در پیوست الف فراهم می‌آورد.

این مثال‌ها برای کمک به‌یک سازمان در مورد چگونگی پیاده سازی سنجش امنیت اطلاعات و چگونگی ضبط فعالیت‌های سنجش و خروجی‌های آن‌ها، در نظر گرفته شده‌اند .

۵مرور کلی بر سنجش امنیت اطلاعات

۵-۱ هدف‌ها سنجش امنیت اطلاعات

هدف‌های سنجش امنیت اطلاعات در متن یک ISMS شامل:

الف) ارزیابی اثر بخشی کنترل‌های پیاده سازی شده‌یا گروه‌های کنترل‌ها (به ۴-۲-۲ د در شکل ۱ مراجعه شود.)

ب) ارزیابی اثر بخشی ISMS پیاده سازی شده (به ۴-۲-۳ ب در شکل ۱ مراجعه شود.)

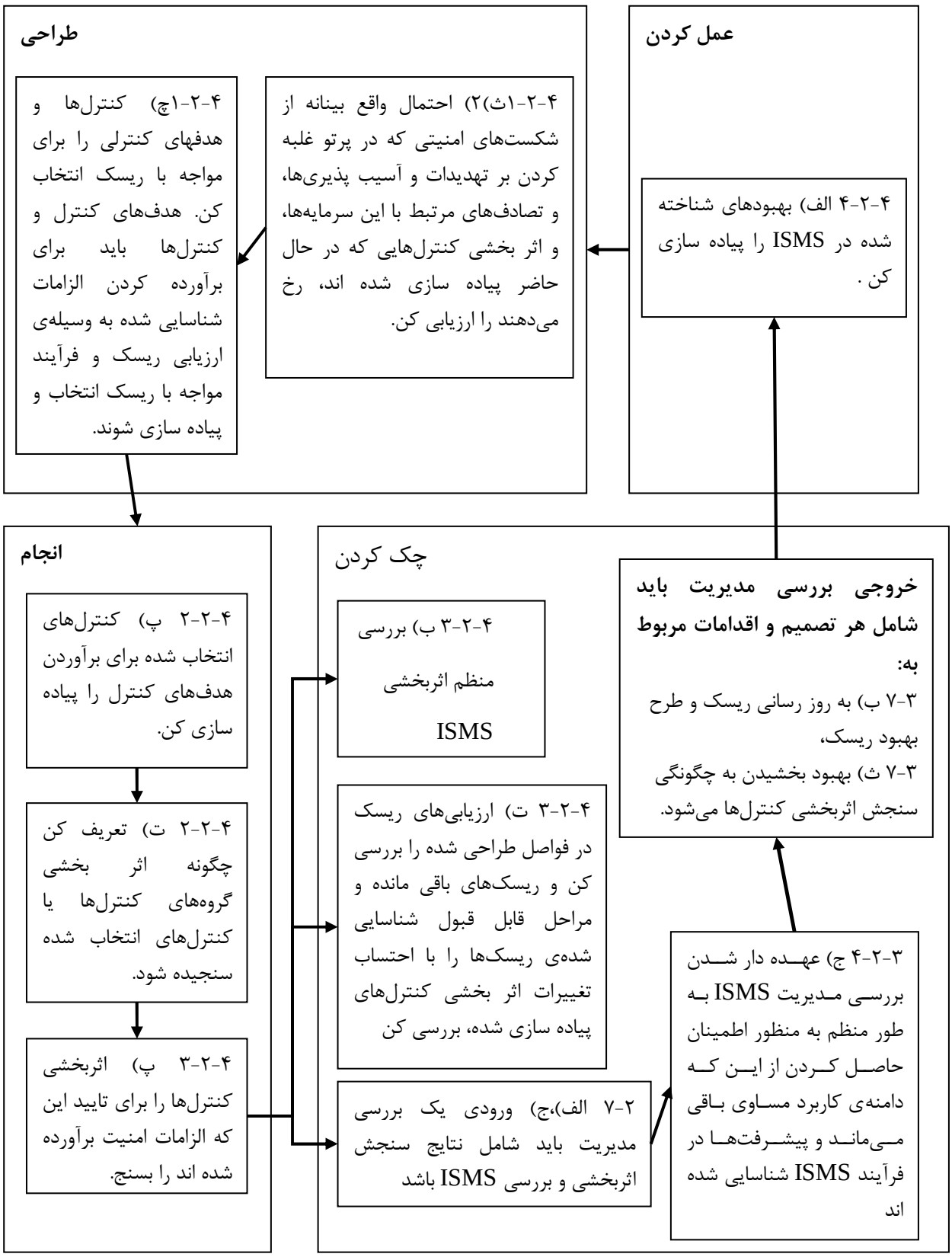
پ) تایید اندازه‌ی برآورده شدن الزامات امنیتی شناخته شده(به ۴-۲-۳ پ در شکل ۱ مراجعه شود.)

ت) تسهیل بهبود کارایی امنیت اطلاعات از نظر ریسک‌های تجاری کلی سازمان

ث) فراهم آوردن ورودی برای بررسی مدیریت به منظور تسهیل تصمیم گیری‌های مربوط به ISMS و توجیه بهبودهای لازم ISMS پیاده سازی شده.

شکل ۱ ارتباط ورودی خروجی ادواری از فعالیت‌های سنجش در ارتباط با چرخه‌ی (PDCA)[1] طراحی- انجام- چک کردن- عمل کردن مشخص شده در ISO/IEC 27001 را نشان می‌دهد. شماره‌های درون هر شکل نشان دهنده‌ی زیر بندهای مربوط به استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ می‌باشد.

1- Plan-Do-Check-Act


طراحی
۴-۲-۱ث)۲) احتمال واقع بینانه از شکست‌های امنیتی که در پرتو غلبه کردن بر تهدیدات و آسیب پذیری‌ها، و تصادف‌های مرتبط با این سرمایه‌ها، و اثر بخشی کنترل‌هایی که در حال حاضر پیاده سازی شده اند، رخ می‌دهند را ارزیابی کن.
۴-۲-۱چ) کنترل‌ها و هدفهای کنترلی را برای مواجه با ریسک انتخاب کن. هدف‌های کنترل و کنترل‌ها باید برای برآورده کردن الزامات شناسایی شده به وسیله‌ی ارزیابی ریسک و فرآیند مواجه با ریسک انتخاب و پیاده سازی شوند.
عمل کردن
۴-۲-۴ الف) بهبودهای شناخته شده در ISMS را پیاده سازی کن .
خروجی بررسی مدیریت باید شامل هر تصمیم و اقدامات مربوط به:
۳-۷ ب) به روز رسانی ریسک و طرح بهبود ریسک،
۳-۷ ث) بهبود بخشیدن به چگونگی سنجش اثربخشی کنترل‌ها می‌شود.
چک کردن
۴-۲-۳ ب) بررسی منظم اثربخشی ISMS
۴-۲-۳ ت) ارزیابی‌های ریسک در فواصل طراحی شده را بررسی کن و ریسک‌های باقی مانده و مراحل قابل قبول شناسایی شده‌ی ریسک‌ها را با احتساب تغییرات اثر بخشی کنترل‌های پیاده سازی شده، بررسی کن
۷-۲ الف)،ج) ورودی یک بررسی مدیریت باید شامل نتایج سنجش اثربخشی و بررسی ISMS باشد
۴-۲-۳ ج) عهده دار شدن بررسی مدیریت ISMS به طور منظم به منظور اطمینان حاصل کردن از این که دامنه‌ی کاربرد مساوی باقی می‌ماند و پیشرفت‌ها در فرآیند ISMS شناسایی شده اند
انجام
۴-۲-۲ پ) کنترل‌های انتخاب شده برای برآوردن هدف‌های کنترل را پیاده سازی کن.
۴-۲-۲ ت) تعریف کن چگونه اثر بخشی گروه‌های کنترل‌ها یا کنترل‌های انتخاب شده سنجیده شود.
۴-۲-۳ پ) اثربخشی کنترل‌ها را برای تایید این که الزامات امنیت برآورده شده اند را بسنج.

شکل ۱- ورودی‌ها و خروجی‌های در چرخه‌ی ISMS PDCA مدیریت امنیت اطلاعات

سازمان باید هدف‌ها سنجش را براساس تعدادی از ملاحظات، شامل:

الف) نقش امنیت اطلاعات در پشتیبانی فعالیت‌های تجاری سراسری سازمان و ریسک‌هایی که با آن مواجه است

ب) برنامه کاربردی قانونی، الزامات تنظیمی، و قراردادی

پ) ساختار سازمانی

ت) هزینه‌ها و مزایای پیاده سازی سنجه‌های امنیتی اطلاعات

ث) معیار پذیرش ریسک برای سازمان

ج) نیاز به مقایسه‌ی چندین ISMS در همان سازمان

بسازد.

۵-۲ برنامه‌ی سنجش امنیت اطلاعات

یک سازمان باید یک برنامه‌ی سنجش امنیت اطلاعات را به منظور به دست آوردن هدف‌ها سنجش ساخته شده بسازد و اداره کند و مدل PDCA را در درون فعالیت‌های سراسری سنجش سازمان برگزینند. همچنین یک سازمان باید طرح‌ریزی‌های سنجش را به منظور به دست آوردن نتیجه‌ها قابل تکرار، عینی و مفید سنجش بر پایه‌ی مدل سنجش امنیت اطلاعات توسعه دهد و پیاده سازی کند (به بند ۴-۵ مراجعه شود.).

برنامه‌ی سنجش امنیت اطلاعات و طرح‌ریزی سنجش توسعه‌یافته باید اطمینان حاصل کند که‌یک سازمان به طور موثر به هدف‌ها و سنجش‌های قابل تکرار دست می‌یابد و نتیجه‌ها سنجش برای سهام‌داران مربوطه را به منظور شناسایی نیازها برای بهبود بخشیدن به ISMS پیاده سازی شده، شامل دامنه‌ی کاربرد آن، سیاست‌ها، هدف‌ها، کنترل‌ها، فرآیندها و رویه‌ها فراهم می‌آورد.

یک برنامه‌ی سنجش امنیت اطلاعات باید شامل فرآیندهای ذیل باشد:

الف) توسعه‌ی سنجش‌ها و سنجه‌ها (به بند ۷ مراجعه شود.)

ب) عملیات سنجش (به بند ۸ مراجعه شود.)

پ) تحلیل داده و گزارش نتیجه‌ها سنجش (به بند ۹ مراجعه شود.) و

ت) ارزیابی و بهبود برنامه‌ی سنجش امنیت اطلاعات (به بند ۱۰ مراجعه شود.)

ساختار سازمانی و عملیاتی یک برنامه‌ی سنجش امنیت اطلاعاتی باید با احتساب مقیاس و پیچیدگی ISMS که بخشی از آن است تعیین شود. در تمام موارد، نقش‌ها و مسئولیت‌های برنامه‌ی سنجش امنیت اطلاعات باید با صراحت به کارمندان شایسته واگذار شوند (۸-۵-۷ مشاهده شود).

سنجه‌های انتخاب شده و پیاده سازی شده با برنامه‌ی سنجش امنیت اطلاعات باید به طور مستقیم مربوط به عملیات یک ISMS باشند، سایر سنجه‌ها، همانند فرآیند تجاری سازمان.

سنجش می‌تواند در فعالیت‌های عملیاتی منظم ادغام شود یا در فواصل منظم مشخص شده با مدیریت ISMS اجرا شود.

۵-۳ عوامل موفقیت

در ذیل برخی از عوامل کمک کننده به موفقیت برنامه‌ی سنجش امنیت اطلاعات در جهت تسهیل بهبود پیوسته‌ی ISMS وجود دارد:

الف) تعهد مدیریت که با منابع مناسب پشتیبانی می‌شود

ب) وجود فرآیندها و رویه‌های ISMS

پ) یک فرآیند قابل تکرار با توانایی دریافت و گزارش داده‌ی با معنا برای فراهم آوردن گرایش‌های معمول در طی یک دوره‌ی زمانی،

ت) سنجه‌هایی براساس هدف‌ها ISMS که قابل تعیین کمیت هستند.

ث) داده‌ی به سادگی قابل دریافت، که می‌تواند برای سنجش‌ها استفاده شود.

ج) ارزیابی اثر بخشی برنامه‌ی سنجش امنیت اطلاعات و پیاده سازی بهبودهای شناسایی شده،

چ) مجموعه‌ی دوره‌ای سازگار، تحلیل، و گزارش از داده‌ی سنجش به طوری که معنی دار است

ح) استفاده از نتیجه‌ها سنجش با سهام‌داران مربوطه به منظور شناسایی نیازها برای بهبود بخشیدن به ISMSهای پیاده سازی شده، شامل دامنه‌ی کاربرد آن، سیاست‌ها، هدف‌ها، کنترل‌ها، فرآیندها و رویه‌ها

خ) پذیرفتن بازخورد بر نتیجه‌ها سنجش از سهام‌داران مربوطه،

د) ارزیابی‌هایی از مفید بودن نتیجه‌ها سنجش‌ها و پیاده سازی بهبودهای شناسایی شده.

یک برنامه‌ی سنجش امنیت اطلاعات که‌یک بار به طور موفقیت آمیزی پیاده سازی شده می‌تواند:

۱- باید انطباق سازمان را با برنامه کاربردی قانونی یا الزامات تنظیمی و تعهد قرار دادی نشان دهد.

۲- پشتیبانی موضوعات امنیت اطلاعات، که ناشناخته یا از اقبل شناسایی نشده هستند.

۳- کمک در تامین نیازهای گزارشی مدیریتی، در هنگام بیان سنجه‌ها، برای بیشینه فعالیت‌های جاری.

۴- به عنوان ورودی در فرآیند مدیریت ریسک امنیت اطلاعات، ممیزی‌های داخلی ISMS و بررسی‌های مدیریت، مورد استفاده قرار گیرد.

۵-۴ مدل سنجش امنیت اطلاعات

یادآوری- مفاهیم مدل سنجش امنیت اطلاعات و طرح‌ریزی‌های سنجش برگزیده شده در این استاندارد ملی براساس استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷ هستند. اصطلاح "محصول اطلاعاتی[1]" استفاده شده در استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷ با " نتیجه‌های سنجش[2] " در این استاندارد ملی هم معنی است و " فرآیند سنجش[3] " استفاده شده در استاندارد ملی ایران ۱۲۷۵۵: سال ۸۷با " برنامه سنجش[4] " در این استاندارد ملی هم معنی است.

1- Information product

2 -Measurment result

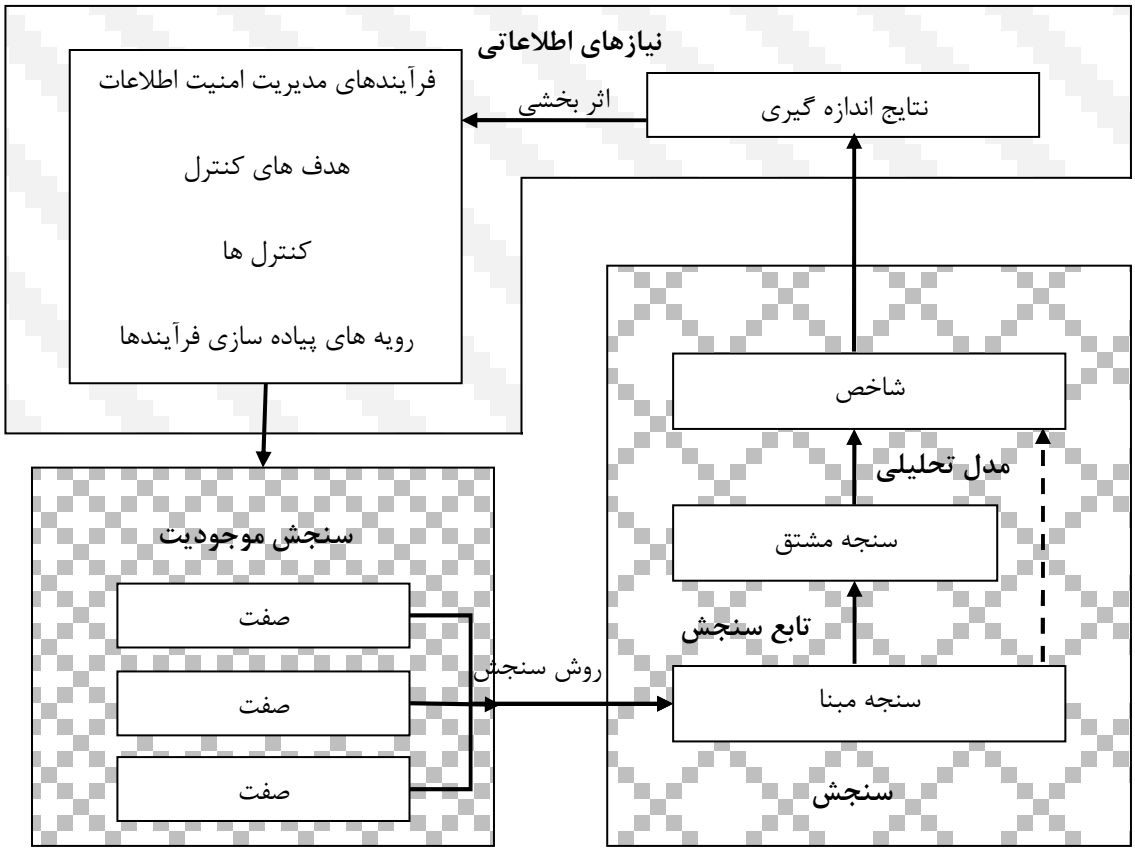
3- Measurment process

4 -Measurment Programme

۵-۴-۱ مرور کلی

مدل سنجش امنیت اطلاعات یک ساختار است که‌یک نیاز اطلاعاتی را به موضوع‌های مربوط به سنجش و صفات آن‌ها پیوند می‌دهد. موضوعات سنجش ممکن است شامل فرآیندها، رویه‌ها، پروژه‌ها و منبع‌های طراحی شده یا پیاده سازی شده باشند.

مدل سنجش امنیت اطلاعات توضیح می‌دهد که چگونه صفت‌های مربوطه، تعیین کمیت شده و به شاخص‌هایی که بنایی برای تصمیم‌گیری فراهم می‌آورند، تبدیل می‌شوند. شکل ۲ مدل سنجش امنیت اطلاعات را نشان می‌دهد.



شکل ۲- مدل سنجش امنیت اطلاعات

یادآوری- بند ۷ اطلاعات دقیقی را در مورد عنصرها منحصر به فرد مدل سنجش امنیت اطلاعات، فراهم می‌آورد.

زیر بندهای بعدی عنصرهای منحصر به فرد مدل را معرفی می‌کنند. همچنین آن‌ها مثال‌هایی از چگونگی استفاده از این عنصرهای منحصر به فرد را فراهم می‌آورند.

نیازهای اطلاعاتی یا هدف سنجش، استفاده شده در مثال‌هایی که جدول‌های ۱ تا ۴ از زیر بندهای بعدی دارند برای ارزیابی وضعیت آگاهی از انطباق با سیاست امنیت سازمان در میان کارمندان مربوطه است (هدف کنترل

الف-۲-۸[1] ، و کنترل‌ها الف-۱-۲-۸ و الف-۲-۲-۸ از استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷).

۵-۴-۲ مدل پایه ای سنجش و سنجه

یک سنجه‌ی مبنا ساده ترین سنجه است که می‌توان فراهم کرد. یک سنجه‌ی مبنا از به کار بردن روش سنجش برای صفات انتخاب شده از یک شیء سنجش حاصل می‌شود. شیء سنجش مجاز است صفات فراوانی داشته باشد که فقط برخی از آن‌ها مقادیر مناسبی را جهت اختصاص به سنجه‌ی مبنا فراهم می‌آورند. یک صفت داده شده مجاز است که برای چندین سنجه‌ی مبنای گوناگون مورد استفاده قرار گیرد.

یک روش سنجش یک دنباله منطقی از عملیات مورد استفاده در تعیین کمیت یک صفت با توجه به‌یک مقیاس مشخص شده می‌باشد. این عملیات مجاز است شامل فعالیت‌هایی مانند شمارش رخدادها یا مشاهده‌ی گذر زمان باشد.

یک روش سنجش می‌تواند صفات را برای یک شیء سنجش به کار ببرد. مثال‌هایی از یک شیء سنجش شامل موارد ذیل می‌شود ولی به آن‌ها محدود نمی‌شود:

- عملکرد کنترل‌های پیاده سازی شده در ISMS
- وضعیت سرمایه‌های اطلاعاتی حفاظت شده با کنترل‌ها
- عملکرد فرآیندهای پیاده سازی شده در ISMS
- رفتار اشخاصی که مسئول ISMS پیاده سازی شده هستند
- فعالیت‌های واحدهای سازمانی مسئول امنیت اطلاعات و
- میزان رضایت گروه‌های ذینفع

یک روش سنجش مجاز است از اشیاء سنجش و صفات مربوط به منبع‌های گوناگون برای سنجش استفاده کند، مانند:

- تحلیل ریسک و ارزیابی نتیجه‌های ریسک
- پرسشنامه‌ها و مصاحبه‌های کارمندان
- گزارشات داخلی و/یا خارجی ممیزی
- ثبت پیشامدها، مانند دفتر گزارشات[2]، آمارهای گزارش و رد گیری‌های ممیزی
- گزارشات پیشامدهای ناخوشایند، به خصوص آن‌هایی که منجر به وقوع یک ضربه می‌شود
- نتیجه‌ها آزمون به عنوان مثال از آزمون نفوذ، مهندسی اجتماعی، ابزارهای انطباق، و ابزارهای ممیزی امنیت

رکوردهایی از رویه‌ها و برنامه‌های مربوط به امنیت اطلاعات سازمان، به عنوان مثال نتیجه‌ها آموزش آگاهی امنیت اطلاعات.

جدول‌های ۱ تا ۴ در ذیر کاربرد مدل امنیت اطلاعات را برای کنترل‌های زیر ارائه می‌دهند:

---

[1] - پیوست الف-۸-۲ و پیوست الف-۸-۲-۱ و پیوست الف-۲-۲

[2]- Log

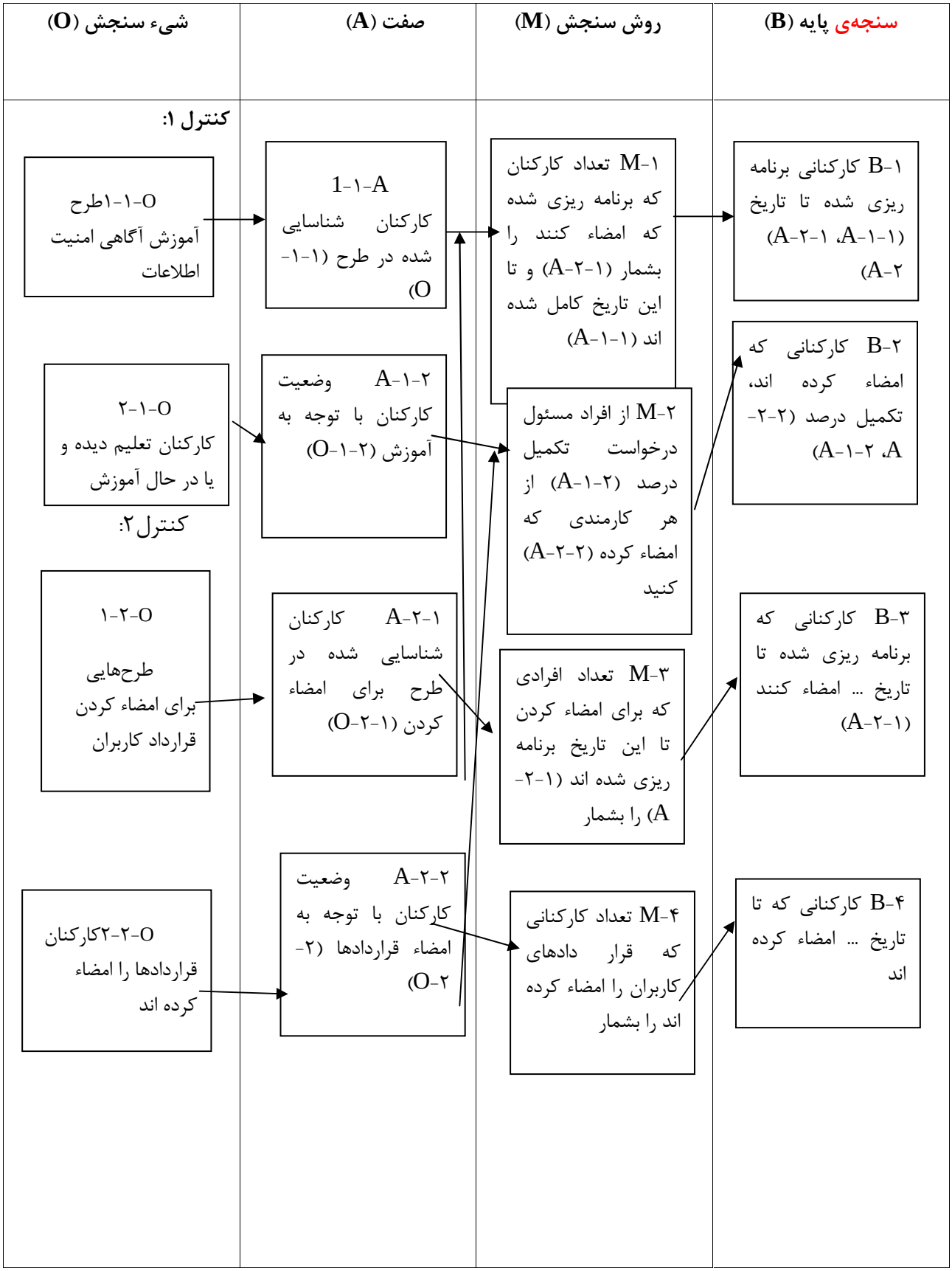
- «کنترل ۲» به مدیریت مسئولیت کنترل ۱-۲-۸-الف در استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ - سال ۸۷ اشاره می‌کند («مدیریت باید مستخدمین، پیمان کاران و کاربران شخص ثالث را مستلزم به کار بردن امنیت مطابق با سیاست‌های اتخاذ شده و رویه‌های سازمان کند»)، که به صورت زیر پیاده سازی شده: «تمام کارمندان مربوط به ISMS باید توافق‌های کاربر را قبل از این که اجازه دسترسی به‌یک سامانه اطلاعات داده شود، امضاء کنند.»

- «کنترل ۱ » به کنترل الف-۸-۲-۲ «آگاهی امنیت اطلاعات، آموزش و تعلیم» از استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ اشاره می‌کند («تمام کارمندان سازمان و، در جایی که مربوط است، پیمان کاران و کاربران شخص ثالث باید آموزش آگاهی مناسب ببینند و با به روز رسانی‌های منظم در سیاست‌های سازمانی و رویه‌های مربوط به کارکرد شغلی شان را دریافت کنند»)، که به صورت زیر پیاده سازی شده: «تمام کارمندان مربوط به ISMS باید قبل از این که اجازه‌ی دسترسی به‌یک سامانه اطلاعات داده شود، آموزش آگاهی امنیت اطلاعات ببینند».

طرح‌ریزی‌های متناظر سنجش در ب-۱ متضمن شده‌اند .

یادآوری- جدول ۱ تا ۴ شامل ستون‌های گوناگونی می‌شود (جدول ۱، چهار ستون، جدول۲ تا ۴، سه ستون) که به هر کدام از آن‌ها یک شناسه‌ی حرفی اختصاص داده شده. به هر خانه درون ستون‌های منحصر به فرد تعدادی شناسه اختصاص داده شده. ترکیب حروف و شناسه اعداد در خانه‌های بعدی برای اشاره به خانه‌های قبلی مورد استفاده قرار گرفته اند. پیکان‌ها جریان‌های داده بین عنصرهای منحصر به فرد مدل سنجش امنیت اطلاعات را با مثال‌های معین، تعیین می‌کنند.

جدول۱ شامل یک مثال از روابط میان شیء سنجش، صفت، روش سنجش و سنجه‌ی مبنا برای سنجش اشیاء ساخته شده برای کنترل‌های پیاده سازی شده‌ی توصیف شده در بالا، می‌شود.



جدول۱- مثال برای سنجه‌ی پایه و روش سنجش

۵-۴-۳ سنجه مشتق و تابع سنجش

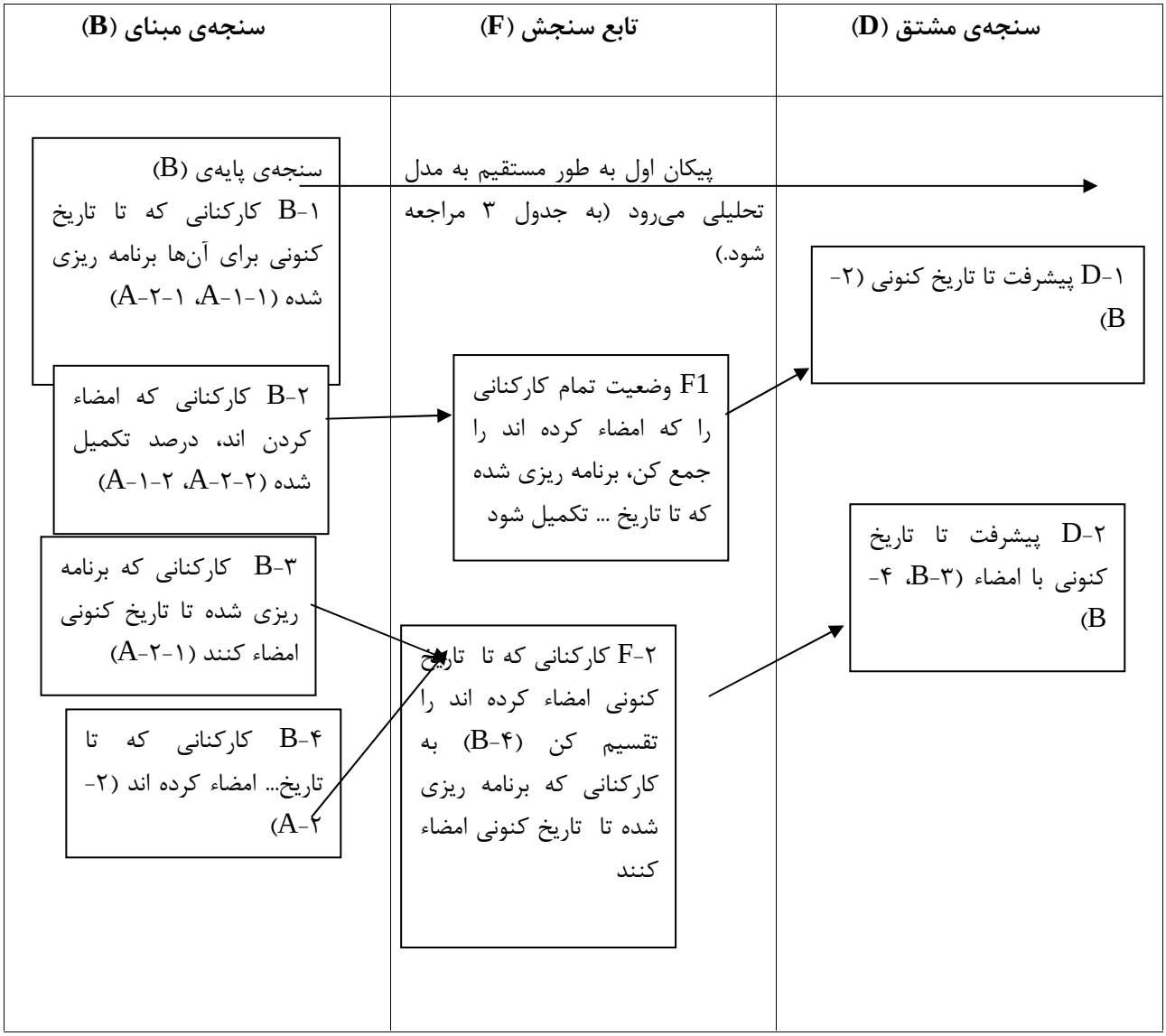
سنجه‌ی مشتق مجموع دو یا بیشتر از سنجه‌های مبنا است. یک سنجه‌ی مبنای داده شده مجاز است که به عنوان ورودی برای چندین سنجه‌ی مشتق به کار رود.

یک تابع سنجش، محاسباتی است که برای ترکیب سنجه‌های مبنا با هم به منظور به وجود آوردن یک سنجه‌ی مشتق مورد استفاده قرار می‌گیرد.

مقیاس و واحد سنجه‌ی مشتق به مقیاس‌ها و واحدها ی سنجه‌ها ی پایه ای بستگی دارد که از آن‌ها مرکب است و همچنین به این که چگونه با تابع سنجش ترکیب می‌شوند.

تابع سنجش مجاز است که فنون گوناگونی، مانند محاسبه‌ی سنجه‌ی پایه، به کار بردن وزن برای سنجه‌های پایه، یا اختصاص دادن مقادیر کیفی به سنجه‌های پایه، را در بر بگیرد. تابع سنجش مجاز است که سنجه‌های مبنا را با استفاده از مقیاس‌های گوناگون، مانند نتیجه‌ها ارزیابی کیفی و درصدی، ترکیب کند.

یک مثال از رابطه‌ی عنصرهای بعدی از کاربرد مدل سنجش امنیت اطلاعات، به عنوان مثال سنجه‌ی پایه، تابع سنجش و سنجه‌ی مشتق، در جدول ۲ ارائه شده است.

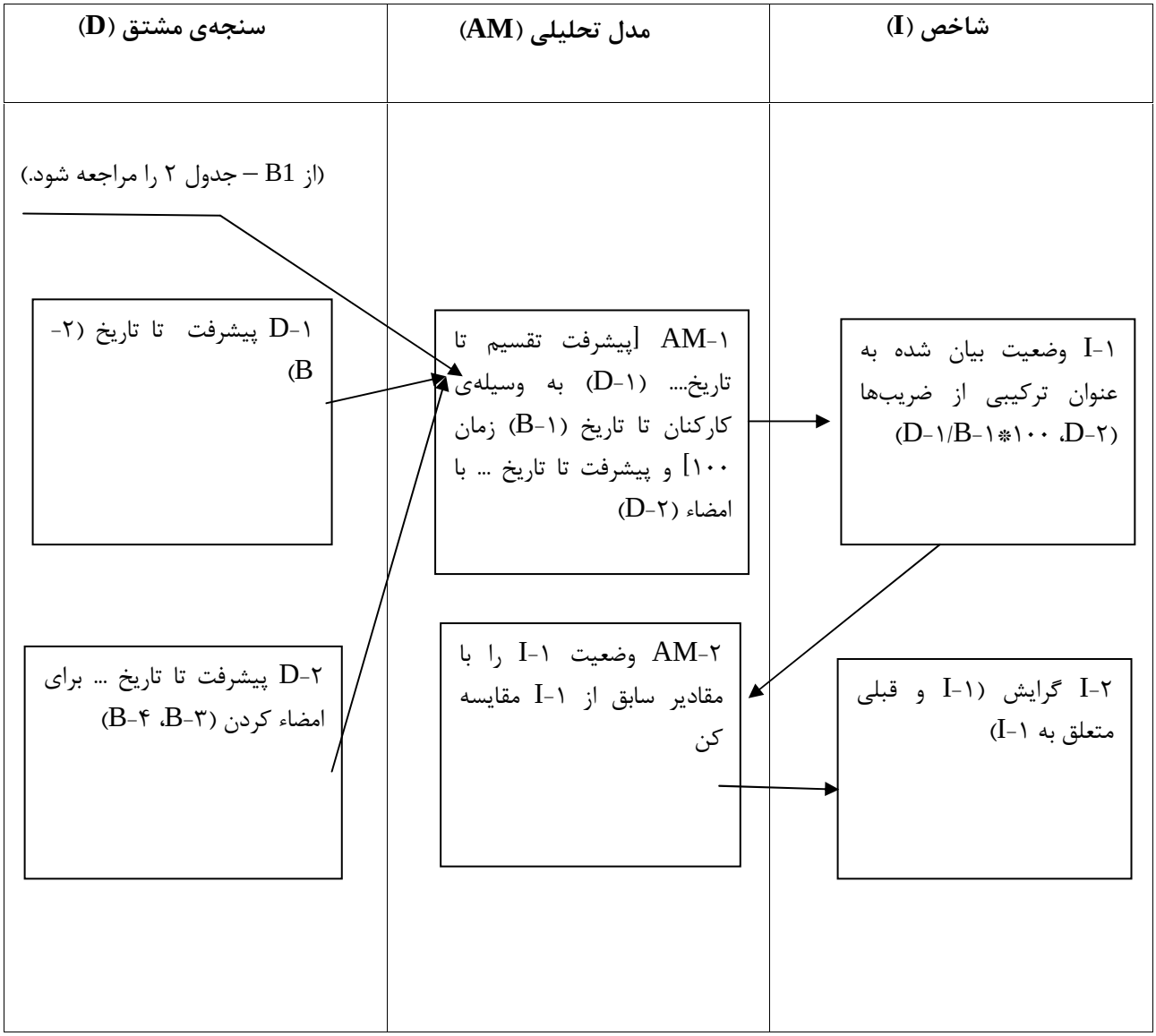


جدول ۲- مثالی از سنجه‌ی مشتق و تابع سنجش

۴-۴-۵ شاخص‌ها و مدل تحلیلی

یک شاخص یک سنجه است که‌یک تخمین یا ارزیابی از صفت‌های مشخص شده‌ی مشتق شده از مدل تحلیلی را با توجه به نیاز به اطلاعات تعریف شده فراهم می‌آورد. شاخص‌ها با اجرای یک مدل تحلیلی بر یک سنجه‌ی پایه و/یا سنجه‌ی مشتق و ترکیب آن‌ها با معیارهای تصمیم، فراهم می‌شوند. مقیاس و روش سنجش بر انتخاب روش‌های تحلیلی مورد استفاده برای تولید شاخص تاثیر می‌گذارد.

یک مثال از روابط بین سنجه‌های مشتق، مدل تحلیلی و شاخص‌ها برای کاربرد مدل سنجش امنیت اطلاعات در جدول ۳ نشان داده شده است.



جدول ۳- مثال برای شاخص و مدل تحلیلی

یادآوری- اگر یک شاخص در یک شکل نگاره‌ای[1] نشان داده شده، باید با کاربرانی که اختلال بینایی دارند، یا زمان استفاده کپی‌های تک رنگ استفاده می‌شود، قابل استفاده باشد. برای امکان پذیر کردن این امر، توصیف شاخص باید شامل رنگ‌ها، سایه‌ها، فونت‌ها یا سایر روش‌های بصری باشد.

۵-۴-۵ نتیجه‌ها سنجش و معیار تصمیم

نتیجه‌ها سنجش با تفسیر شاخص‌های قابل اجرای مبتنی بر معیار تصمیم تعریف شده، توسعه‌یافته اند و بهتر است در متن سنجش کلی اشیاء از ارزیابی اثر بخشی ISMS در نظر گرفته شوند. معیار تصمیم برای مشخص

1- Graphical

کردن نیاز به عمل یا تحقیق بیشتر، همچون توصیف سطح اطمینان در نتیجه‌ها سنجش، مورد استفاده قرار می‌گیرد. معیار تصمیم ممکن است بر یک سری از شاخص‌ها اعمال شود، به عنوان مثال برای هدایت تحلیل گرایش مبتنی بر شاخص‌های دریافت شده در نقاط مختلفی از زمان.

هدف‌ها مشخصات کارایی دقیق قابل اجرا برای سازمان یا قسمت‌های وابسته، مشتق شده از اشیاء امنیت اطلاعات مانند اشیاء ISMS و اشیاء کنترلی، و این که برای بدست آوردن آن اشیاء نیاز است که تنظیم و برآورده شوند را فراهم می‌آورند.

یک مثال از ارتباط عنصرهای نهایی کاربرد مدل سنجش امنیت اطلاعات (به عنوان مثال شاخص، معیار تصمیم و نتیجه‌ها سنجش) در جدول ۴ نشان داده شده است.

نتیجه‌های سنجش	معیار تصمیم (DC)	شاخص (I)
تفسیر برای I-۱: معیار سازمان برای انطباق با سیاست آگاهی امنیت سازمان به طور موثر برآورده شده اگر: ۰.۹≤D.۱/B.۱ ≤ ۱.۱ و ۰.۹۹≤D۲≤۱.۰۱؛ معیار سازمان به طور موثر برآورده نشده اگر D.۱/B.۱<۰.۹ یا [D.۱/B.۱ >۱.۱ اول و ۰.۹۹≤D.۲≤۱.۰۱ ؛ معیار سازمان برآورده نشده اگر D.۲<۰.۹۹ یا D.۲> ۱.۰۱]	DC.۱ ضرایب نتیجه (I.۱ – D.۱/B.۱، D.۲) توصیه می‌شود به ترتیب بین ۰.۹ و ۱.۱ و بین ۰.۹۹ و ۱.۰۱ به منظور نتیجه گیری از دستیابی اشیاء کنترل کاهش یابند؛ در غیر این صورت یک اقدام مدیریت مورد نیاز است DC-۲ توصیه می‌شود گرایش (I.۲) رو به بالا یا ثابت باشد؛ در غیر این صورت یک اقدام مدیریت نیاز است	شاخص (I) I.۱ وضعیت بیان شده به عنوان یک ترکیب از ضرایب (D-۱/B-۱*۱۰۰،D-۲) I.۲ گرایش (I.۱ و برای I.۱ قبلی)

جدول ۴- مثال نتیجه‌ها سنجش و مدل تحلیلی

۶ مسئولیت‌های مدیریت

۶-۱ مرور کلی

مدیریت برای ساختن برنامه‌ی سنجش امنیت اطلاعات با درگیر کردن سهام‌داران مربوطه (به بند ۸-۵-۷ مراجعه شود.) در فعالیت‌های سنجش، قبول نتیجه‌ها سنجش به عنوان ورودی در بررسی مدیریت و با استفاده از نتیجه‌ها سنجش در فعالیت‌های بهبود در درون ISMS، مسئول است.

برای دست یافتن به این، مدیریت باید:

الف) اشیاء را برای برنامه‌ی سنجش امنیت اطلاعات بسازد؛

ب) سیاستی برای برنامه‌ی سنجش امنیت اطلاعات بسازد؛

پ) نقش‌ها و مسئولیت‌ها را برای برنامه‌ی سنجش امنیت اطلاعات بسازد؛

ت) منابع کافی برای انجام سنجش، شامل کارمندان، سرمایه، ابزارها و زیر ساخت فراهم آورد؛

ث) اطمینان حاصل کند که اشیاء برنامه‌ی سنجش امنیت اطلاعات به دست آمده اند؛

ج) اطمینان حاصل کند که ابزارها و تجهیزات مورد استفاده برای جمع آوری داده به درستی پشتیبانی می‌شوند؛

چ) هدف سنجش را برای هر طرح‌ریزی سنجش بسازد؛

ح) اطمینان حاصل کند که سنجش اطلاعات کافی را برای سهام‌داران مربوطه با توجه به اثر بخشی ISMS و نیازها برای بهبود ISMS پیاده سازی شده، شامل دامنه‌ی کاربرد خودش، سیاست‌ها، هدف‌ها، کنترل‌ها، فرآیندها و رویه‌ها فراهم آورد؛ و

خ) اطمینان حاصل کند که سنجش اطلاعات کافی را برای سهام‌داران مربوطه با توجه به اثربخشی کنترل‌ها یا گروهی از کنترل‌ها و نیاز به بهبود بخشیدن کنترل‌های پیاده سازی شده، فراهم می‌آورد.

از طریق واگذاری مناسب مسئولیت‌ها و نقش‌های سنجش، مدیریت باید اطمینان حاصل کند که نتیجه‌ها سنجش متاثر از صاحبان اطلاعات قرار نمی‌گیرد (به بند ۸-۵-۷ را مراجعه شود.). این ممکن است از طریق تفکیک وظایف یا، اگر این ممکن نیست، از طریق استفاده از مستند سازی دقیق که اجازه‌ی بررسی‌های مستقل را می‌دهد حصول شود.

۶-۲ مدیریت منابع

مدیریت باید منابع را برای پشتیبانی از فعالیت‌های اساسی سنجش، مانند جمع آوری داده، تحلیل، ذخیره سازی، گزارش کردن، و توزیع فراهم و واگذاری کند. تخصیص منبع باید شامل واگذاری:

الف) افراد، با مسئولیت برای تمام جنبه‌های برنامه‌ی سنجش امنیت اطلاعات؛

ب) پشتیبانی مالی مناسب؛ و

پ) پشتیبانی زیر ساختی مناسب، مانند زیرساخت فیزیکی و ابزارهای استفاده شده برای انجام فرآیند سنجش باشد.

یادآوری- بند ۱-۲-۵ از استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ الزامات تهیه‌ی منابع برای پیاده سازی و عملکرد یک ISMS را مشخص می‌کند.

۶-۳ آموزش سنجش، آگاهی، و صلاحیت

مدیریت باید اطمینان یابد که:

الف) سهام‌داران (به بند ۸-۵-۷ را مراجعه شود.) به اندازه‌ی کافی برای بدست آوردن نقش و مسئولیت‌هایشان در برنامه‌ی پیاده سازی شده‌ی سنجش امنیت اطلاعات، آموزش دیده‌اند و تا حد مناسبی برای ایفای نقش و مسئولیت‌هایشان واجد شرایط هستند؛

ب) سهام‌داران متوجه وظایف شان، شامل پیشنهاد دادن برای بهبود در برنامه‌ی پیاده سازی شده‌ی سنجش امنیت اطلاعات، هستند.

۷ توسعه‌ی سنجه و سنجش

۷-۱ مرور کلی

این بند رهنمون‌هایی در مورد چگونگی توسعه‌ی سنجه‌ها و سنجش‌ها برای هدف ارزیابی اثربخشی ISMS پیاده سازی شده و کنترل‌ها یا گروه کنترل‌ها، و شناسایی مجموعه‌های مخصوص سازمان طرح‌ریزی‌های سنجش، فراهم می‌آورد. فعالیت‌های مورد نیاز برای توسعه‌ی سنجه‌ها و سنجش باید ساخته شده و مستند و شامل موارد ذیل باشد:

الف) تعریف کردن دامنه‌ی کاربرد سنجش (به بند ۷-۲مراجعه شود.)؛

ب) شناسایی یک نیاز اطلاعاتی (به بند ۷-۳ مراجعه شود.)؛

پ) انتخاب شیء سنجش و صفات آن (به بند ۷-۴ مراجعه شود.)؛

ت) توسعه‌ی طرح‌ریزی‌های سنجش (به بند ۷-۵ مراجعه شود.)؛

ث) استفاده از طرح‌ریزی‌های سنجش (به بند ۷-۶ مراجعه شود.)؛

ج) واگذاری جمع آوری داده و فرآیند تحلیل و ابزارها (به بند ۷-۷ مراجعه شود.)، و

چ) واگذاری رویکرد و مستند سازی پیاده سازی سنجش (به بند ۷-۸ مراجعه شود.).

در هنگام واگذاری این فعالیت‌ها، سازمان باید منابع مالی، انسانی، زیرساختی (فیزیکی یا ابزاری) را به حساب بیاورد.

۷-۲ تعریف دامنه‌ی کاربرد سنجش

بسته به منابع و توانایی‌های یک سازمان، دامنه‌ی کاربرد اولیه فعالیت‌های سنجش یک سازمان به عنصرهایی چون کنترل‌های خاص، سرمایه‌های اطلاعاتی حفاظت شده با کنترل‌های خاص، فعالیت‌های خاص برای امنیت اطلاعات که با مدیریت بیشترین اولویت به آن‌ها داده شده، محدود خواهند شد. در طول زمان، دامنه‌ی کاربرد فعالیت‌های سنجش به منظور پرداختن به عنصرهای بیشتر از ISMS پیاده سازی شده و کنترل‌ها و گروهی از کنترل‌ها، با در نظر گرفتن اولویت‌های سهام‌داران، گسترش خواهند یافت. سهام‌داران مربوطه باید شناسایی شده باشند و در تعریف دامنه‌ی کاربرد سنجش شرکت کنند. سهام‌داران مربوطه ممکن است داخل یا خارج از واحدهای سازمانی، همچون مدیران پروژه، مدیران سامانه اطلاعاتی، یا تصمیم گیرندگان امنیت اطلاعات، باشند.

نتیجه‌ها سنجش خاص که به اثربخشی کنترل‌های منحصر به فرد یا گروهی از کنترل‌ها می‌پردازند، باید برای سهام‌داران مربوطه تعریف و ابلاغ شوند.
سازمان مجاز است که محدود کردن تعداد نتیجه‌های که به تصمیم گیرنده گان گزارش می‌شود را در طول زمان داده شده، به منظور اطمینان یافتن از توانایی شان در تاثیر گذاردن بر بهبودهای مبتنی بر نتیجه‌ها سنجش گزارش شده‌ی ISMS ، ملاحظه کند. تعداد بیش از حد نتیجه‌ها سنجش گزارش شده به توانایی تصمیم گیرنده برای تمرکز بر تلاش‌ها و اولویت بندی بیشتر فعالیت‌های بهبود، ضربه می‌زند. نتیجه‌ها سنجش باید براساس اهمیت نیاز اطلاعات متناظر و اشیاء ISMS مربوطه، اولویت بندی شوند.

یادآوری– دامنه‌ی کاربرد سنجش مربوط به دامنه‌ی کاربرد ISMS ساخته شد ه مطابق با ۱-۲-۴ الف) از استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷.

۷-۳ شناسایی نیاز اطلاعات

هر طرح‌ریزی‌ی سنجش باید حداقل متناظر با یک نیاز اطلاعاتی باشد. یک مثال از نیاز اطلاعات، که در نقطه‌ی شروع به عنوان هدف سنجش توصیف می‌شود و با معیارهای تصمیم مربوطه پایان می‌یابد، در پیوست الف نشان داده شده است.
فعالیت‌های ذیل باید برای شناسایی نیازهای اطلاعاتی انجام شوند:
الف) امتحان کردن ISMS و فرآیندهای آن مانند:
سیاست و هدف‌ها ISMS ، هدف‌ها کنترل و کنترل‌ها؛
الزامات قانونی، تنظیمی، قراردادی، و سازمانی برای امنیت اطلاعات؛
نتیجه‌ها فرآیند مدیریت ریسک امنیت اطلاعات، همانطور که در ISO/IEC 27001 توضیح داده شده.
ب) اولویت بندی کردن نیازهای اطلاعاتی شناسایی شده براساس معیار، مانند:
اولویت بندی‌های بهبود ریسک؛
منابع و توانایی‌های سازمان
سود سهام‌داران؛
سیاست امنیت اطلاعات؛
اطلاعات لازم برای برآوردن الزامات قانونی، تنظیمی، و قراردادی؛
ارزش اطلاعات در ارتباط با هزینه‌ی سنجش؛
پ) انتخاب یک زیر مجموعه از اطلاعات مورد نیاز که قرار است در فعالیت‌های سنجش از لیست اولویت بندی شده، به آن‌ها پرداخته شود؛ و
ت) مستند و ارتباطی که اطلاعات انتخاب شده برای تمام سهام‌داران مربوطه نیاز دارند.
تمام سنجه‌های به کار برده شده در یک ISMS پیاده سازی شده، کنترل‌ها یا گروه‌هایی از کنترل‌ها باید مبتنی بر نیازهای اطلاعاتی انتخاب شده پیاده سازی شوند.

۷-۴ انتخاب صفت و شیء

یک شیء سنجش و صفات آن باید در سراسر متن و دامنه‌ی کاربرد یک ISMS شناسایی شوند. باید یادآوری- کرد که‌یک شیء سنجش می‌تواند چندین صفت قابل اجرا داشته باشد.

شیء و صفات آن که قرار است با سنجش مورد استفاده قرار گیرند، باید براساس اولویت نیازهای متناظر اطلاعات انتخاب شوند.

مقادیری که قرار است به‌یک سنجه‌ی مبنای مربوط اختصاص داده شوند، با به کار بردن یک روش سنجش مناسب برای صفات انتخاب شده، به دست می‌آیند. همچنین این انتخاب باید این اطمینان را بدهد که:

- سنجه‌ی پایه مربوطه و یک روش سنجش مناسب می‌تواند شناسایی شود؛ و
- سنجش معنی دار می‌تواند براساس مقادیر بدست آمده و سنجه‌های توسعه‌یافته، توسعه‌یابد.

مشخصه‌های صفات انتخاب شده تعیین می‌کنند که کدام نوع روش سنجش نیاز به استفاده به منظور به دست آوردن مقادیر برای اختصاص دادن به سنجه‌های مبنا دارند (به عنوان مثال کمی‌و کیفی).

شیء و صفات انتخاب شده باید همراه با منطق انتخاب مستند سازی شوند. داده‌هایی که شیء سنجش و صفات متناظر را توصیف می‌کند، باید به عنوان مقادیری که قرار است به سنجه‌ی پایه اختصاص داده شوند، مورد استفاده قرار گیرد. مثال‌های یک شیء سنجش شامل موارد زیر می‌شود ولی محدود به آن‌ها نمی‌شود:

- محصولات و خدمت‌ها؛
- فرآیندها؛
- سرمایه‌های مناسبی مانند سهولت، کاربردها، و سامانه‌های اطلاعات همانطور که در استاندارد ملی ایران - ایزو- آی ای سی ۲۷۰۰۱ -سال ۸۷ (فهرست اموال و سرمایه‌ها، الف-۷-۱-۱) تعریف شده؛
- واحدهای تجاری؛
- موقعیت‌های جغرافیایی؛ و
- خدمت‌های شخص ثالث.

صفات باید بررسی شوند تا اطمینان حاصل شود که:

الف) صفات مناسب برای سنجش انتخاب شده‌اند ؛ و

ب) جمع آوری داده تعریف شده تا اطمینان حاصل شود که تعداد کافی صفات برای اجازه دادن به سنجش اثر بخش، موجود است.

فقط صفاتی که مربوط به سنجه‌های پایه‌ی متناظر هستند باید انتخاب شوند. گرچه انتخاب صفات باید درجه‌ی سختی را در به دست آوردن صفات برای سنجه مورد توجه قرار دهد، نباید منحصرا برروی داده ای که به سادگی قابل به دست آوردن است یا صفتی که سنجش آن ساده است، ساخته شود.

۷-۵ توسعه‌ی طرح‌ریزی‌ی سنجش

۷-۵-۱ مرور کلی

این زیر بند (۷-۵) به توسعه‌ی طرح‌ریزی‌ی سنجش از ۷-۵-۲ (انتخاب سنجه) تا ۷-۵-۸ (سهام‌داران) می‌پردازد.

۷-۵-۲ انتخاب سنجه

سنجه‌هایی که به طور بالقوه می‌توانند نیازهای اطلاعاتی انتخاب شده را برآورده کنند، باید شناسایی شوند. سنجه‌های شناسایی شده باید با جزئیات کامل تعریف شوند تا اجازه‌ی انتخاب سنجه‌هایی که در آینده پیاده سازی خواهند شد را بدهند. سنجه‌هایی که به تازگی شناسایی شده‌اند مجاز به در برداشتن یک انطباق از سنجه‌ی موجود هستند.

یادآوری- شناسایی سنجه‌های مبنا با شناسایی اشیاء سنجش و صفات آن‌ها ارتباط نزدیک دارد.

بهتر است سنجه‌های شناسایی شده که می‌توانند به طور بالقوه نیاز به اطلاعات انتخاب شده را برطرف کنند، انتخاب شوند. همچنین اطلاعات متن ضروری برای تفسیر یا به هنجار سازی سنجه‌ها بهتر است در نظر گرفته شوند.

یادآوری- تعداد زیادی از ترکیب‌های سنجه‌ها (به عنوان مثال سنجه‌های پایه، سنجه‌های مشتق، و شاخص‌ها) ممکن است برای پرداختن به‌یک نیاز اطلاعاتی خاص، انتخاب شوند.

سنجه‌های انتخاب شده باید اولویت نیازهای اطلاعاتی را منعکس کنند. مثال‌های بیشتر از معیارها که مجاز هستند برای انتخاب سنجه‌ها استفاده شوند شامل:

- سادگی جمع آوری داده؛
- دسترس پذیری منابع انسانی برای جمع آوری و مدیریت داده؛
- دسترس پذیری ابزارهای مناسب؛
- تعداد شاخص‌های مربوط بالقوه که با سنجه‌ی پایه پشتیبانی می‌شوند؛
- سادگی تفسیر؛
- تعداد کاربران نتیجه‌ها سنجش توسعه‌یافته؛
- شواهدی مثل سازگاری سنجه برای هدف یا نیاز اطلاعاتی؛ و
- هزینه‌های جمع آوری، مدیریت، و تحلیل داده

هستند.

۷-۵-۳ روش سنجش

برای هر سنجه‌ی مبنای منحصر به فرد باید یک روش سنجش تعریف شود. این روش سنجش برای تعیین کمیت یک شیء سنجش از طریق تبدیل صفات به مقداری که قرار است به سنجه‌ی پایه اختصاص داده شود، مورد استفاده قرار می‌گیرد.

یک روش سنجش ممکن است عینی یا ذهنی باشد. روش‌های ذهنی بر تعیین کمیت شامل رای انسانی تکیه دارند، در حالی که روش‌های عینی از تعیین کمیت مبتنی بر قوانین عددی همچون شمارش که ممکن است از طریق انسان یا اتوماسیون پیاده سازی شود، استفاده می‌کنند.

روش سنجش، صفات را، با به کار بردن یک مقیاس مناسب، به مقادیر، تعیین کمیت می‌کند. هر مقیاس از واحدهای اندازه گیری استفاده می‌کند. فقط کمیت‌های بیان شده در همان واحد سنجش به طور مستقیم قابل مقایسه هستند.

برای هر روش ارزیابی، فرآیند تصدیق باید ایجاد و مستند سازی شود. این تصدیق باید یک سطح اطمینان را در مقداری که قرار است با به کار بردن یک روش سنجش به‌یک صفت از شیء سنجش، و اختصاص به‌یک سنجه‌ی پایه به دست آید را تضمین کند. جایی که معلوم کردن مقدار معتبر ضروری است، ابزارهای مورد استفاده برای به دست آوردن صفات باید در فواصل مشخص استاندارد سازی و تایید شوند.

دقت روش سنجش باید به حساب آورده شود و انحراف مرتبط یا واریانس باید ضبط شود.

یک روش سنجش باید در طول زمان سازگار باشد به طوری که مقادیر اختصاص داده شده به‌یک سنجه‌ی پایه گرفته شده در زمان‌های گوناگون قابل مقایسه هستند و این که مقادیر اختصاص داده شده به‌یک سنجه‌ی مشتق و یک شاخص نیز قابل مقایسه هستند.

۷-۵-۴ تابع سنجش

برای هر سنجه‌ی مشتق منحصر به فرد یک تابع سنجش باید تعریف شود که برای مقادیر دو یا بیشتر اختصاص داده شده به سنجه‌های مبنا به کار برده می‌شود. این تابع سنجش برای تبدیل مقادیر اختصاص داده شده به‌یک یا بیشتر از سنجه‌های پایه، به مقداری که قرار است به سنجه‌ی مشتق اختصاص داده شود، مورد استفاده قرار می‌گیرد. در بعضی موارد، یک سنجه‌ی پایه ممکن است به طور مستقیم علاوه بر به مدل تحلیلی به‌یک سنجه‌ی مشتق کمک کند.

یک تابع سنجش (به عنوان مثال محاسبات) ممکن است در بر گیرنده‌ی فنون گوناگونی مانند میانگین‌گیری از تمام مقادیر اختصاص داده شده به سنجه‌ی پایه، به کار بردن وزن برای مقادیر اختصاص یافته به سنجه‌ی پایه، یا اختصاص دادن مقادیر کمی‌به مقادیر اختصاص یافته به سنجه‌های مبنا قبل از جمع کردن آن‌ها با مقداری که قرار است به‌یک سنجه‌ی مشتق اختصاص داده شوند، باشد. تابع سنجش مجاز است مقادیر اختصاص داده شده به سنجه‌های مبنا را با استفاده از مقیاس‌های گوناگون، همچون درصد و نتیجه‌ها ارزیابی کیفی، ترکیب کند.

۷-۵-۵ مدل تحلیلی

برای هر شاخص، باید یک مدل تحلیلی برای هدف تبدیل مقادیر یک یا بیشتر اختصاص یافته به‌یک سنجه‌ی پایه و/یا مشتق به مقداری که قرار است به‌یک شاخص اختصاص یابد، تعریف شود.

مدل تحلیلی سنجه‌های مربوطه را به نحوی ترکیب می‌کند که‌یک خروجی که برای سهام‌داران با معنی است را تولید می‌کند.

همچنین معیار تصمیم که در یک شاخص به کار می‌روند باید وقتی که مدل تحلیلی تعریف می‌شود در نظر گرفته شوند.

گاهی اوقات یک مدل تحلیلی ممکن است به سادگی تبدیل یک مقدار منحصر به فرد اختصاص یافته به‌یک سنجه‌ی مشتق، به مقداری که قرار است به‌یک شاخص اختصاص یابد باشد.

۷-۵-۶ شاخص‌ها

مقادیری که قرار است که به شاخص‌ها اختصاص یابند با جمع کردن مقادیر اختصاص یافته به سنجه‌ی مشتق و تفسیر این مقادیر بر مبنای معیار تصمیم ساخته می‌شوند. برای هر شاخص که به مشتری گزارش خواهد شد باید یک قالب برای ارائه‌ی شاخص به عنوان یک بخش از قالب‌های گزارش شده(به بند ۷-۷ مراجعه شود.)، تعریف شود.

قالب‌های ارائه‌ی شاخص به طور عینی سنجه‌ها را نمایش می‌دهند و یک توضیح زبانی از شاخص‌ها را فراهم می‌آورند. قالب‌های ارائه‌ی شاخص باید سفارشی باشند تا نیاز به اطلاعات مشتری را برآورده کنند.

۷-۵-۷ معیار تصمیم

معیار تصمیم متناظر با هر شاخص باید براساس هدف‌ها امنیت اطلاعات تعریف و مستند سازی شود، تا راهنمایی قابل تعقیب قانونی برای سهام‌داران فراهم شود. این راهنمایی باید به انتظارات برای بهبود و آستانه‌ها برای شروع بهبود اقدامات براساس شاخص، به‌پردازد.

معیار تصمیم هدفی را می‌سازد که با آن موفقیت سنجش می‌شود (به بند ۳-۵ مراجعه شود.) و راهنمایی در مورد تفسیر شاخص در ارتباط با نزدیکی آن به هدف را فراهم می‌آورد.

نیاز است که هدف‌ها برای هر بخش با چشم پوشی از عملکرد فرآیندهای ISMS و کنترل‌ها، دست یابی به هدف‌ها، و برای اثربخشی ISMS که قرار است ارزیابی شود، تنظیم شوند.

مدیریت ممکن است تصمیم بگیرد که هدف‌ها را تا هنگامی‌که داده اولیه جمع آوری می‌شود برای شاخص‌ها تنظیم نکند. هر وقت که اقدامات اصلاحی براساس داده‌ی اولیه شناسایی شدند، معیار تصمیم مناسب و نقاط برجسته پروژه[1] پیاده‌سازی که برای یک ISMS خاص واقع بینانه هستند، می‌توانند تعریف شوند. اگر معیار تصمیم در آن نقطه نمی‌تواند ساخته شود، مدیریت باید ارزیابی کند که آیا شیء سنجش و سنجه‌های متناظر مقدار مورد انتظار برای سازمان را فراهم می‌آورد یا نه.

ساخت معیار تصمیم می‌تواند اگر داده‌ی تاریخی که به سنجه‌های توسعه‌یافته‌یا انتخاب شده در دسترس وابسته است، تسهیل یابد. گرایش‌های مشاهده شده در گذشته بینش در محدوده‌ی کارایی که قبلا وجود داشته را فراهم خواهند آورد و خلق معیار تصمیم واقع گرایانه را راهنمایی می‌کنند. معیار تصمیم ممکن است براساس یک فهم ادراکی از رفتار مورد توقع، محاسبه شود. معیار تصمیم ممکن است از داده، طرح‌ها، و اکتشافات تاریخی مشتق شده باشد، یا به عنوان محدودیت‌های کنترل آماری یا محدودیت‌های اطمینان آماری محاسبه شود.

۷-۵-۸ سهام‌داران

برای هر سنجه‌ی پایه و/یا مشتق بهتر است سهام‌داران مناسب شناسایی و مستند سازی شوند.

سهام‌داران مجاز هستند که شامل موارد ذیل باشند:

الف) مشتری برای سنجش: مدیریت یا سایر گروه‌های ذینفع که خواستار یا مستلزم اطلاعات در مورد اثربخشی یک ISMS، کنترل‌ها یا گروهی از کنترل‌ها؛

---

[1]- milestone

ب) بازبین برای سنجش: شخص یا واحد سازمانی که طرح‌ریزی‌های سنجش توسعه‌یافته که برای ارزیابی اثربخشی یک ISMS، کنترل‌ها یا گروه کنترل‌ها مناسب هستند، را معتبر می‌سازد؛
پ) صاحب اطلاعات: شخص یا واحد سازمانی که صاحب اطلاعات راجع به شیء سنجش و صفات هستند و برای سنجش مسئول هستند؛
ت) جمع آوری کننده‌ی اطلاعات: شخص یا واحد سازمانی مسئول جمع آوری، ثبت و ذخیره سازی داده؛ و
ث) شخص در تماس با اطلاعات: شخص یا واحد سازمانی مسئول برای تحلیل داده و نتیجه‌ها سنجش ارتباط.

۷-۶ طرح‌ریزی سنجش

به عنوان یک حداقل، مشخصات طرح‌ریزی‌ی سنجش بهتر است شامل اطلاعات ذیل باشد:
الف) هدف سنجش؛
ب) هدف کنترل که قرار است با کنترل‌ها، و کنترل‌های خاص، گروه کنترل‌ها و فرآیند ISMS که قرار است سنجش شوند، به دست آید؛
پ) شیء سنجش؛
ت) داده ای که قرار است جمع آوری و استفاده شود؛
ث) فرآیندهایی برای جمع آوری و تحلیل داده؛
ج) فرآیندی برای گزارش کردن نتیجه‌ها سنجش، شامل قالب‌های گزارش؛
چ) نقش‌ها و مسئولیت‌های سهام‌داران مربوط؛ و
ح) یک چرخه برای بازبینی سنجش برای اطمینان از مفید بودن آن‌ها در ارتباط با یک نیاز اطلاعات.
پیوست الف یک مثال از طرح‌ریزی‌ی سنجش کلی که الف تا ح را ترکیب می‌کند، را فراهم می‌آورد. پیوست ب مثال‌های طرح‌ریزی سنجش به کار برده شده برای سنجش فرآیندها و کنترل‌های ISMS را فراهم می‌آورد.

۷-۷ جمع آوری داده، تحلیل و گزارش

رویه‌ها برای جمع آوری و تحلیل داده، و فرآیندها برای گزارش نتیجه‌ها سنجش توسعه‌یافته بهتر است ساخته شوند. ابزارهای پشتیبانی، تجهیزات و فناوری‌های سنجش نیز بهتر است در صورت نیاز ساخته شوند. این رویه‌ها، ابزارها، تجهیزات و فناوری سنجش به فعالیت‌های ذیل خواهند پرداخت:
الف) جمع آوری داده، شامل ذخیره و تایید داده (به بند ۸-۳ مراجعه شود). رویه‌ها بهتر است شناسایی کنند که همانند چگونگی و کجا بودن محل ذخیره‌ی تمام داده‌ها با هر اطلاعات متنی ضروری برای فهمیدن و تایید داده، چگونه داده‌ها قرار است با استفاده از روش سنجش، تابع سنجش و مدل تحلیلی، جمع آوری شوند. تایید داده می‌تواند با بازرسی داده با یک چک لیست که برای تایید این که داده‌ی گم شده حداقل هستند، و این که مقداری که قرار است به هر سنجه اختصاص یابد معتبر است، ساخته شده، اجرا شود.

یادآوری- تایید مقادیری که قرار است به سنجه‌های مبنا اختصاص یابند با تایید روش سنجش رابطه نزدیک دارد (به بند۷-۵-۳ مراجعه شود.).

ب) تحلیل داده و گزارش نتیجه‌ها سنجش توسعه‌یافته. رویه‌ها بهتر است فنون تحلیل داده (به بند ۹-۲ مراجعه شود.)، و تناوب، روش‌ها و قالب‌ها برای گزارش نتیجه‌ها سنجش را مشخص کنند. محدوده‌ی ابزارها که ممکن است برای اجرای تحلیل داده مورد نیاز باشند، بهتر است شناسایی شوند.

مثال‌هایی از قالب‌های گزارش شامل:

-کارت شمارش امتیاز برای فراهم آوردن اطلاعات استراتژیک با جمع کردن شاخص‌های سطح بالا؛

-داش‌بورد[1] اجرایی و عملیاتی که کمتر بر هدف‌ها استراتژیک تمرکز دارند و بیشتر به اثربخشی کنترل‌ها و فرآیندهای خاص گره خورده اند؛

-گزارشات، با ماهیت‌های ساده و ایستا، مانند یک فهرست از سنجه‌ها برای یک بازه‌ی زمانی داده شده، به گزارشات پیچیده تر Cross-tab با گروه بندی‌های تو در تو، خلاصه‌های هموار[2]، و پیوندها یا Drill-through پویا. گزارشات بیشتر در هنگامی‌که کاربر نیاز دارد که در یک قالب آسان برای خواندن به داده‌ی خام نگاه کند، استفاده می‌شوند؛ و

-اندازه‌ها برای معرفی مقادیر پویا شامل اعلام خطرها، عنصرهای اضافی گرافیکی و برچسب گذاری نقاط پایان. می‌شوند.

۷-۸ پیاده سازی و مستند سازی سنجش

رویکرد کلی برای سنجش بهتر است در یک طرح پیاده سازی شده، مستند شود. طرح پیاده سازی بهتر است حداقل شامل اطلاعات ذیل باشد:

الف) پیاده سازی برنامه سنجش امنیت اطلاعات برای سازمان؛

ب) مشخصات سنجش به شرح زیر هستند:

۱)طرح‌ریزی‌ی سنجش کلی سازمان؛

۲)طرح‌ریزی‌های سنجش منحصر به فرد سازمان؛ و

۳)تعریف محدوده و رویه‌ها برای جمع آوری داده و تحلیل داده؛

پ) طرح تقویم برای انجام فعالیت‌های سنجش؛

ت) رکوردهای ایجاد شده از طریق انجام فعالیت‌های سنجش، شامل داده‌ی جمع آوری شده و تحلیل رکوردها؛ و

ث) قالب‌های گزارش شده برای نتیجه‌ها سنجشی که قرار است به مدیریت/ سهام‌داران گزارش شوند (استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ بند ۷ «بازبینی مدیریت» مشاهده شود).

---

[1]- Dashboardپ

[2]- rolling

۸ عملکرد سنجش

۸-۱ مرور کلی

عملکرد سنجش امنیت اطلاعات شامل فعالیت‌هایی است که برای اطمینان حاصل کردن از این که نتیجه‌ها سنجش توسعه‌یافته، اطلاعات دقیقی با در نظر گرفتن اثربخشی یک ISMS پیاده سازی شده، کنترل‌ها یا گروه کنترل‌ها و نیازهایی برای اقدامات بهبود مناسب فراهم می‌آورند، ضروری می‌باشند.

این فعالیت شامل موارد ذیل می‌شود:

الف) ادغام کردن رویه‌های سنجش با عملکرد کلی ISMS.

ب) جمع آوری، ذخیره سازی و تایید داده.

۸-۲ یکپارچه‌سازی رویه

برنامه‌ی سنجش امنیت اطلاعات بهتر است به طور کامل با ISMS ادغام و با آن استفاده شود. رویه‌های سنجش بهتر است با عملکرد ISMS شامل:

الف) تعریف و مستند سازی نقش‌ها، قدرت و مسئولیت، در مورد بهبود، پیاده سازی، و پشتیبانی سنجش امنیت اطلاعات؛

ب) جمع آوری داده، و، در جای مورد نیاز، تغییر دادن عملکرد جاری ISMS برای جا دادن فعالیت‌های تولید و جمع آوری داده؛

پ) ارتباط تغییرات در جمع آوری فعالیت‌های داده برای سهامداران مربوط؛

ت) پشتیبانی از جمع آوری کننده گان داده، صلاحیت و فهم انواع داده‌ی لازم، ابزار جمع آوری داده، و رویه‌های جمع آوری داده؛

ث) توسعه‌ی سیاست‌ها و رویه‌های تعریف کننده‌ی استفاده‌ی سنجش در درون سازمان، انتشار اطلاعات سنجش، ممیزی و بازبینی برنامه‌ی سنجش امنیت اطلاعات؛

ج) ادغام تحلیل و گزارش داده با فرآیندهای مربوط برای حصول اطمینان از کارایی منظم آن‌ها؛

چ) نظارت، بازبینی و ارزیابی نتیجه‌ها سنجش؛

ح) تشکیل یک فرآیند برای فاز بندی سنجه‌ها و اضافه کردن سنجه‌های جدید برای حصول اطمینان از این که آن‌ها با سازمان تکامل می‌یابند؛ و

خ) تشکیل یک فرآیند برای تعیین عمر مفید داده‌ی تاریخی برای تحلیل گرایش
متناسب باشد.

۸-۳ جمع آوری، ذخیره سازی و تایید داده

جمع آوری، ذخیره سازی و تایید فعالیت‌های تایید داده شامل موارد ذیل می‌شوند:

الف) جمع آوری داده‌ی مورد نیاز در فواصل معین با استفاده از یک روش سنجش تعیین شده است؛

ب) مستند سازی جمع آوری داده شامل:

۱) تاریخ، زمان ، و محل جمع آوری داده؛

۲) جمع آوری کننده‌ی اطلاعات؛

۳) صاحب اطلاعات؛
۴) هر موضوعی که در حین جمع آوری داده که ممکن است مفید باشد رخ داده است؛
۵) اطلاعات برای تایید داده و تایید مدیریت؛ و
۶)تایید داده‌ی جمع آوری شده بر خلاف معیار انتخاب سنجه و معیار اعتبار طرح‌ریزی‌های سنجش.
۷)داده‌ی جمع آوری شده و هر اطلاعات متن ضروری بهتر است در یک قالب ثبت مساعد برای تحلیل داده، تحکیم و ذخیره سازی شود.

۹ تحلیل داده و گزارش نتیجه‌ها سنجش

۹-۱ مرور کلی

داده‌ی جمع آوری شده باید برای توسعه‌ی نتیجه‌ها سنجش تحلیل شود، و نتیجه‌ها توسعه‌یافته‌ی سنجش بهتر است ابلاغ شوند.
این فعالیت شامل موارد ذیل می‌شود:
الف) تحلیل داده و توسعه‌ی نتیجه‌ها سنجش؛ و
ب) برقراری ارتباط میان نتیجه‌ها سنجش و سهام‌داران مربوطه.

۹-۲ تحلیل داده و توسعه‌ی نتیجه‌ها سنجش

داده‌ی جمع آوری شده باید از نظر معیار تصمیم، تحلیل و تفسیر شود. داده مجاز است قبل از تحلیل مجموع، تبدیل یافته، یا کد دهی مجدد شده باشد. در حین این وظیفه، داده باید برای تولید شاخص‌ها، فرآیند شود. تعدادی از فنون تحلیل می‌توانند بکار روند. عمق تحلیل باید با ماهیت داده و نیاز اطلاعاتی تعیین شود.

یادآوری- راهنمایی برای انجام تحلیل آماری ممکن است در ISO/TR 10017 (راهنمای فنون آماری برای ISO 9001) یافت شود.

نتیجه‌ها تحلیل داده بهتر است تفسیر شوند. شخصی که نتیجه را تحلیل می‌کند (ارتباط برقرار کننده) بهتر است قادر به بیرون کشیدن مقداری از جمع بندی‌های اولیه مبتنی بر نتیجه‌ها باشد. اگر چه، از آن جایی که ارتباط برقرار کننده (ها) ممکن است به طور مستقیم در فرآیند ساز و کار و مدیریتی در گیر نشوند، چنین جمع بندی‌هایی نیاز به بازبینی با سایر سهام‌داران دارند. تمام تفسیرها بهتر است متن سنجه‌ها را به حساب بیاورند.
تحلیل داده بهتر است شکاف بین نتیجه‌ها سنجش مورد انتظار و واقعی یک ISMS پیاده سازی شده، کنترل‌ها یا گروه‌هایی از کنترل‌ها را شناسایی کند. شکاف‌های شناسایی شده به نیازها برای بهبود بخشیدن به ISMS پیاده سازی شده، شامل دامنه‌ی کاربرد آن، سیاست‌ها، هدف‌ها، کنترل‌ها، فرآیندها و روال‌ها اشاره خواهند کرد.
آن شاخص‌ها که عدم انطباق یا عملکرد ضعیف را نشان می‌دهند بهتر است که شناسایی و شاید به شیوه‌ی زیر دسته بندی شوند:
الف) شکست طرح بهبود ریسک برای پیاده سازی یا پیاده سازی کافی، عمل کردن، و مدیریت کنترل‌ها یا فرآیندهای ISMS (به عنوان مثال، کنترل‌ها و فرآیندهای ISMS می‌توانند با تهدیدات دور زده شوند)؛
ب) شکست ارزیابی ریسک:

۱) کنترل‌ها یا فرآیندهای ISMS غیر موثرند زیرا آن‌ها هم برای شمارنده و هم برای تهدیدات تخمین زده شده کافی نیستند (به عنوان مثال احتمال تهدیدها ناچیز شمرده شده بود)؛ یا شمارنده‌ی تهدیدات جدید؛
۲) فرآیندهای ISMS یا کنترل‌ها به خاطر تهدیدات نادیده گرفته شده، پیاده سازی نشده‌اند .
گزارشاتی که برای ارتباط برقرار کردن نتیجه‌ها سنجش با سهام‌داران مربوطه مورد استفاده قرار می‌گیرند، باید با استفاده از گزارش فرمت‌های مناسب مطابق با طرح پیاده سازی برنامه‌ی سنجش امنیت اطلاعات آماده شوند (به بند ۷-۷ مراجعه شود.).
بهتر است مجموع تحلیل‌ها با سهام‌داران مربوطه برای اطمینان از تفسیر درست داده، بازبینی شوند. نتیجه‌ها تحلیل داده بهتر است برای ارتباط با سهام‌داران مستند سازی شوند.

۹-۳ ارتباط نتیجه‌ها سنجش

ارتباط برقرار کننده بهتر است چگونگی ارتباط با نتیجه‌های سنجش امنیت اطلاعات مانند موارد زیر را تعیین کند:
-کدامیک از نتیجه‌ها سنجش قرار است که به طور داخلی و خارجی گزارش شوند؛
- لیست کردن سنجه‌ها متناظر با سهام‌داران منحصر به فرد، و گروه‌های ذینفع؛
- نتیجه‌های خاص سنجش که قرار است فراهم شوند، و نوع ارائه، مناسب سازی شده برای نیازهای هر گروه؛ و
- وسایلی برای به دست آوردن بازخورد از سهام‌داران که قرار است برای ارزیابی میزان مفید بودن نتیجه‌ها سنجش و اثربخشی برنامه‌ی سنجش امنیت اطلاعات استفاده شوند.
- بهتر است نتیجه‌ها سنجش با سهام‌داران داخلی گوناگونی ارتباط برقرار کنند، که شامل موارد زیر می‌شوند اما به آن‌ها محدود نمی‌شوند:
- مشتری برای سنجش (به بند ۷-۵-۸ مراجعه شود.)
- صاحبان اطلاعات (به بند ۷-۵-۸ مراجعه شود.)
-کارمندان مسئول مدیریت ریسک امنیت اطلاعات، مخصوصا جایی که شکست‌های ارزیابی ریسک شناسایی شده‌اند ؛ و
-کارمندانی که مسئول نواحی شناخته شده که نیاز به بهبود دارند، هستند.
سازمان ممکن است در برخی از موارد به جهت توزیع گزارشات نتیجه‌ها سنجش به گروه‌های خارجی، شامل قدرت‌های تنظیمی، سهام‌داران، مشتریان، و تهیه کننده گان، مورد درخواست قرار گیرد. توصیه شده که گزارش نتیجه‌ها سنجش که قرار است به طور خارجی توزیع شوند فقط دربرگیرنده‌ی داده‌ی مناسب برای انتشار خارجی باشد و با مدیریت و سهام‌داران مربوطه قبل از انتشار تایید شود.

۱۰ ارزیابی و بهبود برنامه‌ی سنجش امنیت اطلاعات

۱۰-۱ مرور کلی

بهتر است سازمان در فواصل طرح ریزی شده موارد زیر را ارزیابی کند :
الف) اثربخشی برنامه‌ی مدیریت امنیت اطلاعات پیاده سازی شده، برای حصول اطمینان از:

۱)نتیجه‌ها سنجش را به شیوه موثر تولید می‌کند؛
۲)همان طور که طرح ریزی شده اجرا می‌شود؛
۳) تغییرات در ISMS پیاده سازی شده و/یا کنترل‌ها را نشان می‌دهد؛
۴) تغییرات محیطی را نشان می‌دهد
ب) مفید بودن نتیجه‌ها سنجش توسعه‌یافته برای حصول اطمینان از این که آن‌ها نیازهای اطلاعاتی مربوطه را برآورده می‌کنند.
مدیریت باید تکرار چنین ارزیابی‌هایی را مشخص کند، طراحی بازبینی دوره ای و ساختن ساز و کارها برای امکان پذیر کردن بازبینی (بند۲-۷ از استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ مراجعه شود.).
فعالیت‌های مربوط بهتر است مانند موارد زیر باشد:
۱) برای شناسایی معیار ارزیابی برای برنامه‌ی سنجش امنیت اطلاعات (به بند ۱۰-۲ مراجعه شود.)؛
۲) برای نظارت، بازبینی، و ارزیابی سنجش (به بند ۱۰-۳ مراجعه شود.)؛ و
۳) برای پیاده سازی بهبود (به بند ۱۰-۴ مراجعه شود.).

۱۰-۲ شناسایی معیار ارزیابی برای برنامه‌ی سنجش امنیت اطلاعات

سازمان باید برای ارزیابی اثربخشی برنامه‌ی سنجش امنیت اطلاعات همچون مفید بودن نتیجه‌ها سنجش توسعه‌یافته، معیار تعریف کند. معیار بهتر است در آغاز پیاده سازی برنامه‌ی سنجش امنیت اطلاعات، با احتساب متن هدف‌ها فنی و تجاری سازمان تعریف شود.
محتمل ترین معیار وقتی که سازمان‌ها توصیه می‌شود که برنامه‌ی ارزیابی امنیت اطلاعات را ارزیابی کنند و بهبود بخشند موارد ذیل هستند:
- تغییرات در هدف‌ها تجاری سازمان
- تغییرات در الزامات قانونی یا تنظیمیو تعهدات پیمانی روی امنیت اطلاعات؛
- تغییرات در الزامات سازمان بر امنیت اطلاعات؛
- تغییرات در ریسک‌های امنیت اطلاعات در سازمان‌ها؛
- افزایش دسترسی به داده و/یا روش‌های تصفیه شده‌یا مناسب بیشتر برای جمع آوری داده برای ارزیابی هدف‌ها؛ و
- تغییرات شیء سنجش و/یا صفات آن؛
معیارهای زیر ممکن است برای ارزیابی نتیجه‌ها سنجش توسعه‌یافته به کار برده شوند:
الف) نتیجه‌ها ارزیابی:
۱) به راحتی قابل فهم بودن؛
۲) به طور به موقعی ارتباط دارند؛ و
۳)عینی، قابل مقایسه و قابل تولید مجدد
هستند.
ب) فرآیندهای ساخته شده برای توسعه‌ی نتیجه‌ها سنجش:

۱) به خوبی تعریف شده باشند؛
۲) به سادگی عمل می‌کنند؛ و
۳) به طور مناسب دنبال می‌شوند.
هستند.
پ) نتیجه‌ها سنجش برای بهبود بخشیدن به امنیت اطلاعات مفید هستند.
ت) نتیجه‌ها سنجش به نیازهای متناظر اطلاعات می‌پردازند.

۱۰-۳ نظارت، بررسی، و ارزیابی برنامه‌ی سنجش امنیت اطلاعات

سازمان باید برنامه‌ی سنجش امنیت اطلاعاتش را در برابر معیار ساخته شده نظارت، بررسی، و ارزیابی کند. (به بند ۱۰-۲ را مراجعه شود.).
سازمان باید نیازهای بالقوه را برای بهبود برنامه‌ی سنجش امنیت اطلاعات شناسایی کند، [که این نیازها] شامل:
الف) بازبینی یا برداشتن طرح‌ریزی‌های سنجش پذیرفته که دیگر مناسب نیستند؛ و
ب) تخصیص مجدد منبع‌ها برای پشتیبانی برنامه‌ی امنیت اطلاعات
هستند.
همچنین سازمان باید نیازهای بالقوه را برای بهبود بخشیدن به ISMS پیاده سازی شده، شامل دامنه‌ی کاربرد آن، سیاست‌های آن، هدف‌ها آن، کنترل‌ها، فرآیندها و رویه‌ها شناسایی کند؛ و تصمیمات مدیریت را برای اجازه دادن به مقایسه و تحلیل گرایش در حین بررسی‌های متوالی، مستند سازی کند.
نتیجه‌ها این ارزیابی و نیازهای بالقوه‌ی شناسایی شده برای بهبود باید با سهام‌داران مربوطه مرتبط شوند تا اجازه‌ی تصمیم گیری در مورد بهبودهای ضروری را بدهند.
سازمان باید مطمئن شود که بازخورد از سهام‌داران در مورد نتیجه‌ها این ارزیابی و نیازهای شناسایی شده‌ی بالقوه برای بهبود مطلوب است. سازمان باید بداند که بازخورد یکی از ورودی‌ها در مورد اثربخشی برنامه‌ی سنجش امنیت اطلاعات است.

۱۰-۴ پیاده سازی بهبودها

سازمان باید اطمینان حاصل کند که سهام‌داران مربوطه بهبودهای مورد نیاز از برنامه‌ی سنجش امنیت اطلاعات را شناسایی کرده اند (بند ۳-۷ ث از استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ را مراجعه شود.). بهبودهای شناسایی شده بهتر است با مدیریت تایید شوند. طرح‌های تایید شده بهتر است به سهام‌داران مناسب مستند سازی و ارتباط دهی شوند.
سازمان باید اطمینان حاصل کند که بهبودهای تایید شده برنامه‌ی سنجش امنیت اطلاعات همانطور که طرح ریزی شده، پیاده سازی شده.
سازمان مجاز است فنون مدیریت پروژه را برای به کامل انجام رساندن بهبود، تایید کند.

پیوست الف

(اطلاعاتی)

الگوی طرح ریزی سنجش امنیت اطلاعات

پیوست الف نمونه ای از الگوی طرح ریزی سنجش امنیت اطلاعات را که شامل تمام مولفه‌های شناسایی شده در ۵-۷ که در ۵-۴ شرح داده شده‌اند را ارائه می‌دهد. سازمان‌ها می‌توانند الگو را مطابق با الزامات خود تغییر دهند.

شناسایی طرح ریزی سنجش	
سنجش طرح‌ریزی نام	نام سنجش
شناسه عددی	شناسه عددی منحصر به فرد مخصوص به سازمان.
هدف طرح ریزی سنجش	دلایل معرفی سنجش را شرح می‌دهد.
هدف کنترل/فرآیند	هدف کنترل/فرآیند تحت سنجش (برنامه ریزی شده‌یا اجرا شده).
کنترل (۱)/ فرآیند (۱)	کنترل/فرآیند تحت سنجش
کنترل (۲)/ فرآیند (۲)	اختیاری: درصورت قابلیت اجرا، کنترل/ فرآیند بیشتر در دسته بندی که در سنجه مشابه قرار دارد (برنامه ریزی شده‌یا اجرا شده).
موضوع سنجش و صفت‌ها	
موضوع سنجش	موضوع (نهاد) که از طریق سنجش صفات مشخص می‌شود. یک موضوع می‌تواند شامل فرآیندها، طرح‌ها، پروژه‌ها، منبع‌ها و سامانه‌ها یا مولفه‌های سامانه شود.
صفت	مشخصه‌یا خصوصیت یک موضوع سنجش که می‌تواند به صورت کیفی یا کمی‌توسط انسان یا ابزارهای خودکار مشخص شوند.
صفت سنجه مبنا (برای هر سنجه مبنا [1…n]	
سنجه مبنا	یک سنجه مبنا از نظر یک صفت و روش سنجش جهت تعیین کمیت آن تعریف می‌شود (برای

	مثال، عدد کارمندان آموزش دیده، تعداد محل‌ها و هزینه کل تا آن تاریخ). با جمع آوری داده، یک مقدار برای یک سنجه مبنا تعیین می‌شود.
روش سنجش	ترتیب منطقی عملیات‌های مورد استفاده در تعیین کمیت یک صفت با توجه به یک مقیاس مشخص شده.
نوع روش سنجش	بسته به ماهیت عملیات‌های مورد استفاده جهت تعیین کمیت یک صفت، دو روش ممکن است مشخص شود: ذهنی: تعیین کمیت با رای انسانی عینی: تعیین کمیت مبتنی بر قوانین عددی شامل محاسبه
مقیاس	مجموعه منظمی‌از مقادر یا طبقات که صفت سنجه مبنا برای آن رسم می‌شود
نوع مقیاس	بسته به ماهیت روابط میان مقادیر در مقیاس، چهار نوع مقیاس معمولا تعریف می‌شوند: اسمی، ترتیبی، مدت و نسبت.
واحد سنجش	کمیتی خاص، تعریف شده و برگزیده شده با قرارداد، که با آن سایر کمیت‌ها از همان نوع به منظور بیان قدر نسبت آن‌ها با آن کمیت، مقایسه می‌شوند.
صفت سنجه مشتق شده	
سنجه مشتق شده	یک سنجه که به عنوان یک تابع برای دو یا چند سنجه مبنا مشتق می‌شود.
عملکرد سنجش	الگوریتم یا محاسبه انجام شده جهت ترکیب دو یا چند سنجه مبنا. مقیاس و واحد سنجه مشتق شده بسته به مقیاس‌ها و واحدهای سنجه‌های مبنا که مرکب از آن است و همچنین چگونگی ترکیب آنها به وسیله این تابع است.
صفت شاخص	
شاخص	سنجه‌ای که، ارزیابی یا تخمینی از صفات مشخص شده‌ی مشتق از یک مدل تحلیلی را با توجه به نیازهای اطلاعاتی تعریف شده فراهم می‌آورد.
مدل تحلیلی	الگوریتم یا محاسبه ترکیب کننده‌یک یا بیشتر نسخه‌های مبنا و یا سنجه‌های مشتق شده با معیار تصمیم آن است. این مدل مبتنی بر درک یا فرضیات درمورد ارتباط مورد انتظار بین سنجه مبنا و یا سنجه مشتق شده و یا رفتار آنها در طول زمان است. یک مدل تحلیلی تخمین‌ها یا ارزیابی‌های مرتبط با یک نیاز اطلاعاتی تعریف شده را ایجاد می‌کند.

صفت معیار تصمیم	
معیار تصمیم	آستانه‌ها، هدف‌ها یا الگوهای مورد استفاده جهت تعیین نیاز به اقدام یا بررسی بیشتر یا تعریف سطح اطمینان به‌یک نتیجه معین. معیار تصمیم به تفسیر نتیجه‌ها سنجش کمک می‌کند.
نتیجه‌های سنجش	
تفسیر شاخص	شرح چگونگی شاخص نمونه (به عدد نمونه در شرح شاخص مراجعه شود) باید تفسیر شود.
قالب‌های گزارش دهی	قالب‌های گزارش دهی باید شناسایی و مستند شوند. مشاهداتی که سازمان یا صاحب اطلاعات ممکن است درمورد سابقه بخواهد را شرح می‌دهد. قالب‌های گزارش دهی به صورت بصری سنجه‌ها را نمایش می‌دهد و تعریفی کلامی‌را در مورد شاخص‌ها ارائه می‌دهد. قالب‌های گزارش دهی باید با نیاز خریدار اطلاعات مطابقت داده شود.
سهام‌داران	
کارگزار سنجش	مدیریت یا دیگر طرف‌های ذینفع درخواست دهنده‌یا نیازمند اطلاعات درمورد کارایی ISMS، کنترل‌ها یا مجموعه گروه‌ها.
بررسی کننده سنجش	شخص یا واحد سازمانی که تصدیق می‌کند که طرح ریزی‌های سنجش توسعه داده شده برای ارزیابی کارایی ISMS، کنترل‌ها یا مجموعه کنترل‌ها مناسب هستند.
صاحب اطلاعات	شخص یا واحد سازمانی که مالکیت اطلاعات درمورد یک موضوع سنجش و صفت‌ها را در اختیار دارد و مسئول سنجش است.
جمع آورنده اطلاعات	شخص یا واحد سازمانی که مسئول جمع آوری، ثبت و ذخیره داده است.
برقرار کننده ارتباط	شخص یا واحد سازمانی مسئول تحلیل داده و محاسبه نتیجه‌های سنجش.
تناوب/دوره	
تناوب مجموعه داده	چند وقت به چند وقت داده جمع آوری می‌شود
تناوب تحلیل داده	چند وقت به چند وقت داده تحلیل می‌شود.
تناوب گزارش دهی	چند وقت به چند وقت نتیجه‌ها سنجش گزارش داده می‌شوند (می‌تواند نسبت به جمع آوری داده

نتیجه‌های سنجش	دفعات کمتری داشته باشد).
بررسی سنجش	داده بازبینی سنجش (انقضاء یا تجدید اعتبار سنجش)
دوره سنجش	دوره زمانی سنجش را تعریف می‌کند.

پیوست ب

(اطلاعاتی)

مثال‌های طرح ریزی سنجش

بندهای زیر مثال‌های از طرح‌ریزی‌های سنجش را ارائه می‌دهد. این مثال‌ها جهت نشان دادن چگونگی اجرای این استاندارد با استفاده از الگوی ارائه شده در پیوست الف بیان شده‌اند .

فهرست مطالب

فرآیندها و کنترل‌های مربوطه (بند استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ یا شماره کنترل در پیوست الف)	مثال‌های طرح ریزی سنجش مربوطه (ارجاع به این پیوست)	نام‌های مثال طرح ریزی سنجش
بند ۴-۲-۲ ح)	ب-۴-۱	اثربخشی مدیریت حادثه امنیت اطلاعات
بند ۵-۲-۲ د)	ب-۱-۱	کارمندان آموزش دیده ISMS

بند ۸-۲	ب-۴-۲	اجرای اقدام اصلاحی
کنترل الف-۶-۱-۸	ب-۳	فرآیند بررسی ISMS
کنترل الف-۶-۱-۱ و الف-۶-۱-۲	ب-۵	تعهد مدیریتی
کنترل الف-۶-۲-۳	ب-۱۰	امنیت در توافق نامه‌های شخص ثالث
کنترل الف-۸-۲ و الف-۸-۲-۲	ب-۱-۲	آموزش امنیت اطلاعات
کنترل الف-۸-۲ و الف-۸-۲-۲	ب-۱-۳	تطبیق آگاهی امنیت اطلاعات
کنترل الف-۹-۱-۲	ب-۷	کنترل فیزیکی ورود
کنترل الف-۹-۲-۴	ب-۹	مدیریت نگهداری دوره ای
کنترل الف-۱۰-۴-۱	ب-۶	حفاظت دربرابر کد مخرب
کنترل الف-۱۰-۱۰-۱ و الف-۱۰-۱۰-۲	ب-۸	بررسی فایل‌های ثبت وقایع
کنترل الف-۱۱-۳-۱	ب-۲-۱	کیفیت کلمه عبور- دستی
کنترل الف-۱۱-۳-۱	ب-۲-۲	کیفیت کلمه عبور- خودکار

ب- ۱ آموزش ISMS

ب-۱-۱ کارمندان آموزش دیده ISMS

شناسایی طرح ریزی سنجش	
سنجش طرح‌ریزی نام	کارمندان آموزش دیده ISMS
شناسه عددی	مخصوص به سازمان.
هدف طرح ریزی سنجش	برقراری تطبیق کنترل با خط مشی امنیت اطلاعات سازمان
هدف کنترل/فرآیند	بند ۵-۲-۲ { استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ } آموزش، آگاهی و صلاحیت.
کنترل (۱) / فرآیند (۱)	بند ۵-۲-۲ {استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷} آموزش، آگاهی و صلاحیت. سازمان باید به وسیله: د) نگهداری از سوابق تحصیلی، آموزش، مهارت‌ها، تجربه و شایستگی‌ها تضمین کند که تمام کارمندانی که به آن مسئولیت‌هایی که در ISMS تعریف شده، اختصاص داده شده است صلاحیت اجرای وظایف مورد نیاز را دارند.
کنترل (۲) / فرآیند (۲)	اختیاری: درصورت قابلیت اجرا، کنترل/ فرآیند بیشتر در دسته بندی که در سنجه مشابه قرار دارد (برنامه ریزی شده‌یا اجرا شده).
موضوع سنجش و صفت‌ها	
موضوع سنجش	پایگاه داده کارمند
صفت	سوابق آموزش
صفت سنجه مبنا (۱)	
سنجه مبنا	تعداد کارمندانی که مطابق با برنامه آموزش سالانه ISMS آموزش ISMS دیده‌اند. تعداد کارمندانی که باید آموزش ISMS ببینند.

روش سنجش	شمارش ثبت وقایع/ثبت با پرکننده رشته/ردیف آموزش ISMS پس از "آموزش دیدن"
نوع روش سنجش	عینی
مقیاس	عددی
نوع مقیاس	نسبت
واحد سنجش	کارمند
صفت سنجه مشتق شده	
سنجه مشتق شده	درصد کارمندان آموزش دیده ISMS
عملکرد سنجش	تعداد کارمندانی که آموزش ISMS می‌بینند/تعداد کارمندانی که باید آموزش ISMS ببینند× ۱۰۰
صفت شاخص	
شاخص	استفاده از کد گذاری رنگی با استفاده از شاخص‌های رنگی. نمودار میله ای نمایش دهنده تطبیق چندین دوره گزارش دهی در ارتباط با آستانه‌های (قرمز، زرد، سبز) که به وسیله مدل تحلیلی تعریف می‌شوند. تعداد دوره‌های گزارش دهی برای استفاده در نمودار باید به وسیله سازمان تعریف شود.
مدل تحلیلی	۰-۶۰٪- قرمز؛ ۶۰-۹۰٪- زرد؛ ۹۰-۱۰۰٪- سبز. در مورد زرد، اگر پیشروی حداقل ۱۰ درصد به ازای هر یک چهارم بدست نیاید، درجه به صورت خودکار قرمز می‌شود.
صفت معیار تصمیم	
معیار تصمیم	قرمز- مداخله ضروری است، تحلیل علت و معلول باید جهت تعیین دلایل عدم تطبیق و عملکرد ضعیف اجرا شود. زرد- لازم است برای افت احتمالی به سمت قرمز نظارت بر شاخص به صورت نزدیک انجام شود. سبز- هیچ اقدامی‌لازم نیست.
نتیجه‌های سنجش	
تفسیر شاخص	مخصوص به سازمان
قالب‌های گزارش دهی	نمودار میله ای دارای میله‌های به صورت رنگی کد گذاری شده مبتنی بر معیارهای تصمیم گیری. لازم است خلاصه کوتاهی درمورد معنای سنجه و اقدامات مدیریتی احتمالی به نمودار میله ای الحاق شود.
سهام‌داران	
مشتری سنجش	مدیران مسئول ISMS
بررسی کننده سنجش	مدیران مسئول ISMS
صاحب اطلاعات	مدیرآموزش- منابع انسانی
جمع آورنده اطلاعات	مدیریت آموزش- بخش منابع انسانی
برقرار کننده اطلاعات	مدیران مسئول ISMS

تناوب/دوره	
تناوب مجموعه داده	ماهانه، اولین روز کاری ماه
تناوب تحلیل داده	سه ماهه
تناوب گزارش دهی نتیجه‌ها سنجش	سه ماهه
بازبینی سنجش	بررسی سالانه
دوره سنجش	سالانه

ب-۱-۲ آموزش امنیت اطلاعات

شناسایی طرح ریزی سنجش	
سنجش طرح‌ریزی نام	آموزش امنیت اطلاعات
شناسه عددی	ویژه سازمان.
هدف طرح ریزی سنجش	ارزیابی تطبیق با الزامات آموزش آگاهی امنیت اطلاعات سالانه.
هدف کنترل/فرآیند	الف.۸.۲ درجریان استخدام هدف: تضمین اینکه تمام کارمندان، پیمانکاران و کاربران شخص ثالث از تهدیدات و نگرانی‌های امنیت اطلاعات، مسئولیت‌ها و التزام‌ها آگاهی دارند و برای پشتیبانی از خط مشی امنیت سازمانی در دوره معمول کاریشان و کاهش خطر خطاهای انسانی تجهیز هستند.
کنترل (۱) / فرآیند (۱)	الف-۸-۲-۲ { استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ } آگاهی، تعلیم و آموزش امنیت اطلاعات. تمام کارمندان سازمان و در موقعیت مربوطه، پیمانکاران و کاربران شخص ثالث باید آموزش آگاهی و به روزرسانی‌های متداول خط مشی و دستورالعمل‌های سازمانی که به عملکرد شغلی آنها مربوط است، را دریافت کنند.
موضوع سنجش و صفت‌ها	
موضوع سنجش	پایگاه داده کارمند
صفت	سوابق آموزش
صفت سنجه مبنا (۱)	
سنجه مبنا	تعداد کارمندانی که آموزش آگاهی امنیت اطلاعات سالانه می‌بینند. تعداد کارمندانی که به آموزش آگاهی امنیت اطلاعات سالانه نیاز دارند.
روش سنجش	شمارش ثبت وقایع/ثبت با پرکننده رشته/ردیف آموزش ISMS پس از "آموزش دیدن"
نوع روش سنجش	عینی
مقیاس	عددی
نوع مقیاس	نسبت
واحد سنجش	کارمند

صفت سنجه مشتق شده	
سنجه مشتق شده	درصد کارمندانی که آموزش آگاهی امنیت اطلاعات سالانه را دریافت کرده اند.
عملکرد سنجش	تعداد کارمندانی که آموزش آگاهی امنیت اطلاعات سالانه را می‌بینند/ تعداد کارمندانی که به آموزش آگاهی امنیت اطلاعات سالانه نیاز دارند*۱۰۰.
صفت شاخص	
شاخص	نمودار میله ای نمایش دهنده تطبیق با چندین دوره گزارش دهی در ارتباط با آستانه‌های (قرمز، زرد، سبز با شناساگرهای رنگی) که به وسیله مدل تحلیلی تعریف می‌شوند. تعداد دوره‌های گزارش دهنی برای استفاده در نمودار باید توسط سازمان تعریف شوند.
مدل تحلیلی	۰-۶۰٪- قرمز؛ ۶۰-۹۰٪- زرد؛ ۹۰-۱۰۰٪- سبز. در مورد زرد، اگر پیشروی حداقل ۱۰ درصد به ازای هر یک چهارم بدست نیاید، درجه به صورت خودکار قرمز می‌شود.
صفت معیار تصمیم	
معیار تصمیم	قرمز- مداخله ضروری است، تحلیل علت و معلول باید جهت تعیین دلایل عدم تطبیق و عملکرد ضعیف اجرا شود. زرد- لازم است برای افت احتمالی به سمت قرمز نظارت بر شاخص به صورت نزدیک انجام شود. سبز- هیچ اقدامی‌لازم نیست.
نتیجه‌های سنجش	
تفسیر شاخص	مخصوص به سازمان
قالب‌های گزارش دهی	نمودار میله ای دارای میله‌های به صورت رنگی کد گذاری شده مبتنی بر معیارهای تصمیم گیری. لازم است خلاصه کوتاهی درمورد معنای سنجه و اقدامات مدیریتی احتمالی به نمودار میله ای الحاق شود.
سهام‌داران	
مشتری سنجش	مدیران مسئول ISMS. مدیریت امنیت. مدیریت آموزش
بررسی کننده سنجش	مدیر امنیت
صاحب اطلاعات	مأمور امنیت اطلاعات و مدیر آموزش
جمع آورنده اطلاعات	مدیریت آموزش- بخش منابع انسانی
بیانگر اطلاعات	مدیران مسئول ISMS
تناوب/دوره	
تناوب مجموعه داده	ماهانه، اولین روز کاری ماه
تناوب تحلیل داده	سه ماهه
تناوب گزارش دهی نتیجه‌ها سنجش	سه ماهه
بازبینی سنجش	بررسی سالانه
دوره سنجش	سالانه

ب-۱-۳ تطبیق آگاهی امنیت اطلاعات

شناسایی طرح ریزی سنجش	
سنجش طرح‌ریزی نام	تطبیق خط مشی آگاهی امنیت اطلاعات
شناسه عددی	مخصوص به سازمان.
هدف طرح ریزی سنجش	ارزیابی وضعیت تطبیق با خط مشی آگاهی امنیت اطلاعات میان کارمندان مربوطه
شناسایی طرح ریزی سنجش	الف-۸-۲ درجریان استخدام تضمین اینکه تمام کارمندان، پیمانکاران و کاربران شخص ثالث از تهدیدات و نگرانی‌های امنیت اطلاعات، مسئولیت‌ها و التزام‌ها آگاهی دارند و برای پشتیبانی از خط مشی امنیت سازمانی در دوره معمول کاریشان و کاهش خطر خطاهای انسانی تجهیز هستند.
کنترل (۱)/ فرآیند (۱)	الف-۸-۲-۲ تمام کارمندان سازمان و در موقعیت مربوطه، پیمانکاران و کاربران شخص ثالث باید آموزش آگاهی و به روزرسانی‌های متداول خط مشی و دستورالعمل‌های سازمانی که به عملکرد شغلی آنها مربوط است، را دریافت کنند. (اجرا) تمام کارمندان مربوط به ISMS باید پیش از موافقت با دستیابی آنها به سامانه اطلاعاتی، آموزش آگاهی امنیت اطلاعات ببینند. آموزش شامل...
کنترل (۲)/ فرآیند (۲)	الف-۸-۲-۱ مدیریت جهت اجرای امنیت مطابق با خط مشی‌ها و دستورالعمل‌های امنیتی که توسط سازمان برقرار شده‌اند به کارمندان، پیمانکاران و کاربران شخص ثالث نیاز دارند. (اجرا) تمام کارمندان مربوط به ISMS باید پیش از موافقت با دستیابی آنها به سامانه اطلاعاتی، توافقنامه‌های کاربری را امضا کنند.
موضوع سنجش و صفت‌ها	
موضوع سنجش	۱-۱ برنامه زمانبندی/طرح آموزش آگاهی امنیت اطلاعات ۱-۲ کارمندانی که آموزش را کامل کرده اند یا درحال آموزش دیدن هستند ۲-۱ طرح امضای برنامه زمانبندی/توافقنامه‌های کاربری ۲-۲ کارمندانی که توافقنامه امضا کرده اند
صفت	۱-۱ کارمندان شناسایی شده در طرح ۱-۲ وضعیت کارمندان با توجه به آموزش ۲-۱ کارمندان شناسایی شده در طرح برای امضا ۲-۲ وضعیت کارمندان با توجه به امضای توافقنامه‌ها
صفت سنجه مبنا	
سنجه مبنا	۱-۱ تعداد کارمندان طرح ریزی شده تا تاریخ کنونی ۱-۲ تعداد کارمندانی که امضا کرده اند ۲-۱ تعداد کارمندانی که برای امضا تا تاریخ کنونی طرح ریزی شده‌اند

	۲-۲ تعداد کارمندانی که تا تاریخ کنونی امضا کرده اند
روش سنجش	۱-۱ شمارش تعداد کارمندانی که براساس برنامه زمانبندی باید تا تاریخ کنونی آموزش را تکمیل و امضا کنند. ۱-۲ پرسش از افراد مسئول درمورد درصد از کارمندانی که آموزش را تکمیل و امضا کرده اند. ۱-۲ شمارش تعداد کارمندانی که براساس برنامه زمانبندی شده تا این تاریخ امضا کرده اند ۲-۲ شمارش تعداد کارمندانی که توافقنامه‌های کاربری را امضا کرده اند
نوع روش سنجش	۱-۱ عینی ۱-۲ ذهنی ۱-۲ عینی ۲-۲ عینی
مقیاس	۱-۱ اعداد صحیح از صفر تا بینهایت ۱-۲ اعداد صحیح از صفر تا صد ۱-۲ اعداد صحیح از صفر تا بینهایت ۲-۲ اعداد صحیح از صفر تا بینهایت
نوع مقیاس	۱-۱ ترتیبی ۱-۲ نسبت ۱-۲ ترتیبی ۲-۲ ترتیبی
واحد سنجش	۱-۱ کارمندان ۱-۲ درصد ۱-۲ کارمندان ۲-۲ کارمندان
صفت سنجه مشتق شده	
سنجه مشتق شده	۱)پیشرفت تا تاریخ کنونی ۲)پیشرفت تا تاریخ کنونی با امضا
عملکرد سنجش	۱) افزودن وضعیت که تا تاریخ کنونی تکمیل آن طرح ریزی شده است برای تمام کارمندانی که امضا کرده اند ۲) جداکردن کارمندانی که تا تاریخ کنونی امضا کرده اند از کارمندانی که تا تاریخ کنونی امضای آنها طرح ریزی شده است.
صفت شاخص	
شاخص	الف) وضعیت بیان شده به عنوان ترکیبی از نسبت‌ها و؛ ب) روند
مدل تحلیلی	الف) [جداکردن پیشرفتتا تاریخ کنونی از (کارمندانی که تاریخ زمان ۱۰۰ طرح ریزی شده‌اند)] و پیشرفت تا تاریخ کنونی با امضا ب) مقایسه وضعیت با وضعیت‌های پیشین

صفت معیار تصمیم	
معیار تصمیم	الف) نسبت‌های حاصل شده باید به ترتیب بین ۰/۹ و ۱/۱ و بین ۰/۹۹ و ۱/۰۱ قرارگیرد تا دست یابی به کنترل هدف بدست آید؛ و ب) روند باید صعودی یا ثابت باشد.
نتیجه‌های سنجش	
تفسیر شاخص	تفسیر شاخص الف) باید به صورت زیر باشد: - معیارهای سازمان برای مطابقت با خط مشی آگاهی امنیت به طور رضایت بخشی در ۰/۹≥نسبت اول≥۱/۱ و ۰/۹۹≥نسبت دوم≥.۱/۰۱ مطابقت داده شده است؛ مطابق با نوع نوشتار (font) استاندارد. - معیارهای سازمانی به طور غیرقابل قبولی در [۰/۹≥نسبت اول≥۱/۱یا اول نسبت>۱/۱] و ۰/۹۹≥نسبت دوم≥۱.۰۱ مطابقت داده شده است؛مطابق با نوع نوشتار مایل؛ - معیارهای سازمان در [نسبت دوم<۰/۹۹ یا نسبت دوم<۱/۰۱] مطابقت نمی‌کنند؛ مطابق با نوع نوشتار bold تفسیر شاخص ب) باید به صورت زیر باشد: - روندصعودی مطابقت افزایش یافته را نشان می‌دهد،روند نزولی مطابقت روبه کاهش را نشان می‌دهد. درجه تغییر روند می‌توانند بینش‌هایی را برای کارآمدی کنترل اجرایی فراهم آورد. تغییرات سریع درهر جهتی نشان دهنده این است که کنترل اجرایی مستلزم بررسی دقیق جهت تعیین دلیل است. روندهای منفی ممکن است مستلزم مداخله مدیریت باشد. روندهای مثبت باید جهت شناسایی بهترین عمل‌های بالقوه بررسی شوند.
قالب‌های گزارش دهی	نوشتار استاندارد= معیارها به طور رضایت بخشی مطابقت می‌کنند. نوشتار مایل= معیارها به طور غیرقابل قبولی مطابقت می‌کنند. نوشتار برجسته= معیارها مطابقت نکرده اند.
سهام‌داران	
مشتری سنجش	مدیران مسئول ISMS. مدیریت امنیت. مدیریت آموزش
بررسی کننده سنجش	مدیر امنیت
صاحب اطلاعات	مأمور امنیت اطلاعات و مدیر آموزش
جمع آورنده اطلاعات	مدیریت آموزش- بخش منابع انسانی
بیانگر اطلاعات	مدیران مسئول ISMS
تناوب/دوره	
تناوب مجموعه داده	ماهانه، اولین روز کاری ماه
تناوب تحلیل داده	سه ماهه
تناوب گزارش دهی نتیجه‌ها سنجش	سه ماهه
بازبینی سنجش	بررسی سالانه

دوره سنجش	سالانه

ب-۲ خط مشی‌های کلمه عبور

ب-۲-۱ کیفیت کلمه عبور- دستی

شناسایی طرح ریزی سنجش	
سنجش طرح‌ریزی نام	کیفیت کلمه عبور
شناسه عددی	ویژه سازمان.
هدف طرح ریزی سنجش	ارزیابی کیفیت کلمه عبورهایی که توسط کاربران جهت دستیابی به سامانه‌های IT سازمان مورد استفاده قرار می‌گیرند
هدف کنترل/فرآیند	بازداشتن کاربران از انتخاب کلمه عبورهای غیرایمن.
کنترل (۱) / فرآیند (۱)	الف-۱۱-۳-۱ باید کاربران ملزم به پیروی از عملکردهای امنیتی مناسب در انتخاب و استفاده از کلمه عبور شوند. اجرا. تمام کاربران باید کلمه عبورهای قوی برای هر سامانه انتخاب کنند که: ۱) طول آن بیش از ۸ است؛ ۲) مبتنی برهرچیزی که شخص دیگری بتواند به راحتی آن را حدس بزند یا با استفاده از اطلاعات مرتبط با شخص مانند، نام، شماره تلفن، تاریخ تولد و غیره بدست آورد، نباشد؛ ۳) از کلماتی تشکیل نشوند که در دیکشنری‌ها وجود دارند؛ ۴) دارای کاراکترهای تماما عددی یا تماما حروفی یکسان متوالی نباشد. تمام حساب‌های کاربری و کلمه عبورهای سامانه‌های IT سازمان باید توسط سامانه کارمند کنترل شود.
موضوع سنجش و صفت‌ها	
موضوع سنجش	پایگاه داده کلمه عبور کاربر
صفت	کلمه عبورهای افراد
صفت سنجه مبنا (۱)	
سنجه مبنا	۱- تعداد کلمه عبورهای ثبت شده. ۲- تعداد کلمه عبورهایی که خط مشی کیفیت کلمه عبور سازمان را برای هر کاربر برآورده می‌کند.
روش سنجش	۱- شمارش تعداد کلمه عبورها در پایگاه داده کلمه عبور کاربر. ۲- پرسش از هر کاربر درمورد تعداد کلمه عبورهایی که خط مشی کلمه عبور سازمان را برآورده می‌کنند.
نوع روش سنجش	۱- عینی ۲- ذهنی
مقیاس	۱- اعداد صحیح از صفر تا بینهایت

	۲- اعداد صحیح از صفر تا بینهایت
نوع مقیاس	۱- ترتیبی ۲- ترتیبی
واحد سنجش	۱- کلمه عبورها ۲- کلمه عبورها
صفت سنجه مشتق شده	
سنجه مشتق شده	تعداد کل کلمه عبورهایی که با خط مشی کیفیت کلمه عبور سازمان مطابقت می‌کند.
عملکرد سنجش	∑ [تعداد کل کلمه عبورهایی که با خط مشی کیفیت کلمه عبور سازمان برای هر کاربر مطابقت می‌کند]
صفت شاخص	
شاخص	الف) نسبت کلمه عبورهایی که با خط مشی کیفیت کلمه عبور سازمان مطابقت دارد. ب) روندهای وضعیت مطابقت درخصوص خط مشی کیفیت کلمه عبور
مدل تحلیلی	جداسازی [تعداد کل کلمه عبورهایی که با خط مشی کیفیت کلمه عبور سازمان مطابقت دارند] از [تعداد کلمه عبورهای ثبت شده]. ب) مقایسه نسبت با نسبت گذشته.
صفت معیار تصمیم	
معیار تصمیم	هدف کنترل بدست می‌آید و درصورتی که نسبت حاصل شده بالاتر از ۰/۹ باشد هیچ اقدامی‌نیاز نیست. درصورتی که نسبت حاصل شده بین ۰/۸ و ۰/۹ باشد هدف کنترل بدست نیامده است، اما روند مثبت نشانگر بهبود است. درصورتی که نسبت کمتر از ۰/۸ باشد باید اقدام فوری صورت گیرد.
نتیجه‌ها سنجش	
تفسیر شاخص	تفسیر شاخص باید الف)باید به صورت زیر باشد: - معیارهای سازمان برای مطابقت با خط مشی کلمه عبور سازمانی به طور رضایت بخشی در ۰/۹≥نسبت مطابقت داده شده است. - معیارهای سازمانی به طور غیرقابل قبولی در [۰/۸ ≥نسبت≥۰/۹]با خط مشی کلمه عبور سازمانی مطابقت داده شده است. - معیارهای سازمان درنسبت≥۰/۸ با خط مشی کلمه عبور سازمانی مطابقت نمی‌کنند. تفسیر شاخص ب) باید به صورت زیر باشد: - روندصعودی مطابقت افزایش یافته را نشان می‌دهد،روند نزولی مطابقت روبه کاهش را نشان می‌دهد. - درجه تغییر روند می‌توانند بینش‌هایی را برای کارآمدی کنترل‌های اجرا شده فراهم آورد. - روندهای منفی ممکن است مستلزم کنترل‌های بیشتر مانند آگاهی یا ابزارهای فنی جهت الزام انتخاب کلمه عبورهای قوی یا تغییر دوره ای کلمه عبور باشد. - روندهای مثبت باید جهت تخمین اصطلاحات ضروری جهت مطابقت با خط مشی کلمه عبور از نسبت جاری باشد. تاثیر/اثر مطابقت نکردن با معیارها خطر افزایش یافته نقض قابلت اطمینان است. عوامل بالقوه انحراف شامل فقدان آگاهی امنیتی، نقص‌های اجرایی فنی و کمبود زمان برای

	اجرا در تمام سامانه‌های IT است.
قالب‌های گزارش دهی	خط روند تعداد کلمه عبورهای مطابق با خط مشی کیفیت کلمه عبور سازمان را نشان می‌دهد که به خطوط روند تولید شده طی دوره‌های گزارش دهی گذشته افزوده شده‌اند .
سهام‌داران	
مشتری سنجش	مدیران مسئول ISMS، مدیر امنیت.
بررسی کننده سنجش	مدیریت امنیت
صاحب اطلاعات	مدیر سامانه
جمع آورنده اطلاعات	کارمند امنیتی
بیانگر اطلاعات	کارمند امنیتی
تناوب/دوره	
تناوب مجموعه داده	سالیانه
تناوب تحلیل داده	سالیانه
تناوب گزارش دهی نتیجه‌ها سنجش	سالیانه
بازبینی سنجش	بررسی و به روزرسانی برای هر سال
دوره سنجش	سالانه

ب-۲-۲ کیفیت کلمه عبور-خودکار

شناسایی طرح ریزی سنجش	
سنجش طرح‌ریزی نام	کیفیت کلمه عبور
شناسه عددی	ویژه سازمان.
هدف طرح ریزی سنجش	ارزیابی کیفیت کلمه عبورهایی که توسط کاربران جهت دستیابی به سامانه‌های IT سازمان مورد استفاده قرار می‌گیرند
هدف کنترل/فرآیند	بازداشتن کاربران از انتخاب کلمه عبورهای غیرایمن.
کنترل (۱)/ فرآیند (۱	الف-۱۱-۳-۱ کاربران باید ملزم به پیروی از عملکردهای امنیتی مناسب در انتخاب و استفاده از کلمه عبور شوند. اجرا: تمام کاربران باید کلمه عبورهای قوی برای هر سامانه انتخاب کنند که: ۱) طول آن بیش از ۸ باشد؛ ۲) مبتنی برهرچیزی که شخص دیگری بتواند به راحتی آن را حدس بزند یا با استفاده از اطلاعات مرتبط با شخص مانند، نام، شماره تلفن، تاریخ تولد و غیره بدست آورد، نباشد؛ ۳) از کلماتی تشکیل نشوند که در دیکشنری‌ها وجود دارند؛ ۴) دارای کاراکترهای تماما عددی یا تماما حروفی یکسان متوالی نباشد. تمام حساب‌های کاربری و کلمه عبورهای سامانه‌های IT سازمان باید توسط سامانه کارمند

	کنترل شود. قدرت کلمه عبور باید با استفاده از یک نرم افزار کرک کلمه عبور بررسی شود.
موضوع سنجش و صفت‌ها	
موضوع سنجش	پایگاه داده حساب کاربری سامانه کارمند
صفت	کلمه عبورهای افراد که در سوابق حساب کاربری سامانه کارمند ذخیره شده است.
صفت سنجه مبنا	
سنجه مبنا	۱- تعداد کل کلمه عبورها ۲- تعداد کل کلمه عبورهای غیرقابل کرک
روش سنجش	۱- پرس و جو کردن درمورد سوابق حساب کاربری کارمند ۲- اجرای کرکر کلمه عبور در سوابق حساب کاربری سامانه کاربر با استفاده از حملات ترکیبی
نوع روش سنجش	۱- عینی ۲- عینی
مقیاس	۱- اعداد صحیح از صفر تا بینهایت ۲- اعداد صحیح از صفر تا بینهایت
نوع مقیاس	۱- ترتیبی ۲- ترتیبی
واحد سنجش	۱- کلمه عبورها ۲- کلمه عبورها
صفت سنجه مشتق شده	
سنجه مشتق شده	هیچ
عملکرد سنجش	هیچ
صفت شاخص	
شاخص	۱- نسبت کلمه عبورهای قابل کرک طی ۴ ساعت ۲- روند نسبت ۱
مدل تحلیلی	الف) جداسازی [تعداد کل کلمه عبورهایی که با خط مشی کیفیت کلمه عبور سازمان مطابقت دارند] از [تعداد کلمه عبورهای ثبت شده]. ب) مقایسه نسبت با نسبت گذشته.
صفت معیار تصمیم	
معیار تصمیم	هدف کنترل بدست می‌آید و درصورتی که نسبت حاصل شده بالاتر از ۰/۹ باشد هیچ اقدامی‌نیاز نیست. درصورتی که نسبت حاصل شده بین ۰/۸ و ۰/۹ باشد هدف کنترل بدست نیامده است، اما روند مثبت نشانگر بهبود است. درصورتی که نسبت کمتر از ۰/۸ باشد باید اقدام فوری صورت گیرد.
نتیجه‌ها سنجش	
تفسیر شاخص	تفسیر شاخص باید الف)باید به صورت زیر باشد: - معیارهای سازمان برای مطابقت با خط مشی کلمه عبور سازمانی به طور رضایت بخشی در ۰/۹≤نسبت مطابقت داده شده است. - معیارهای سازمانی به طور غیرقابل قبولی در [۰/۸ ≤نسبت≤۰/۹]با خط مشی کلمه عبور

	سازمانی مطابقت داده شده است. - معیارهای سازمان درنسبت≥۰/۸ با خط مشی کلمه عبور سازمانی مطابقت نمی‌کنند. تفسیر شاخص ب) باید به صورت زیر باشد: - روندصعودی مطابقت افزایش یافته را نشان می‌دهد،روند نزولی مطابقت روبه کاهش را نشان می‌دهد. - درجه تغییر روند می‌توانند بینش‌هایی را برای کارآمدی کنترل‌های اجرا شده فراهم آورد. - روندهای منفی ممکن است مستلزم کنترل‌های بیشتر مانند آگاهی یا ابزارهای فنی جهت الزام انتخاب کلمه عبورهای قوی یا تغییر دوره ای کلمه عبور باشد. - روندهای مثبت باید جهت تخمین اصطلاحات ضروری جهت مطابقت با خط مشی کلمه عبور از نسبت جاری باشد. تاثیر/اثر مطابقت نکردن با معیارها خطر افزایش یافته درخطر کشف افتادن کلمه عبور است که می‌تواند به دسترسی غیرمجاز به سامانه منجر شود. عوامل بالقوه انحراف شامل فقدان آگاهی امنیتی، نقص‌های اجرایی فنی و کمبود زمان برای اجرا در تمام سامانه‌های IT است.
قالب‌های گزارش دهی	خط روند که قابلیت کرک شدن کلمه عبور را برای تمام سوابق آزمایش شده نشان می‌دهد به خطوط تولید شده طی آزمایش‌های پیشین افزوده می‌شود.
سهام‌داران	
مشتری سنجش	مدیران مسئول ISMS، مدیر امنیت.
بررسی کننده سنجش	مدیریت امنیت
صاحب اطلاعات	مدیر سامانه
جمع آورنده اطلاعات	کارمند امنیتی
بیانگر اطلاعات	کارمند امنیتی
تناوب/دوره	
تناوب مجموعه داده	هفتگی
تناوب تحلیل داده	هفتگی
تناوب گزارش دهی نتیجه‌ها سنجش	هفتگی
بازبینی سنجش	بررسی و به روزرسانی برای هر سال
دوره سنجش	قابل اجرا در ۳ سال

ب-۳ فرآیند بررسی ISMS

شناسایی طرح ریزی سنجش	
سنجش طرح‌ریزی نام	فرآیند بررسی ISMS
شناسه عددی	ویژه سازمان.
هدف طرح ریزی سنجش	ارزیابی درجه بهبود بررسی مستقل امنیت اطلاعات

هدف کنترل/فرآیند	مدیریت اطلاعات در سازمان
کنترل (۱) / فرآیند (۱)	الف-۶-۱-۸ رویکرد سازمان برای مدیریت امنیت اطلاعات و اجرای آن (یعنی هدف کنترل، کنترل‌ها، خط مشی‌ها، فرآیندها و دستورالعمل‌های برای امنیت اطلاعات) باید به صورت مستقل در فاصله‌های زمانی برنامه ریزی شده‌یا زمانی که تغییرات قابل توجه برای اجرا امنیتی رخ دهد بررسی شود. (اجرا) رویکرد سازمان برای مدیریت امنیت اطلاعات و اجرای آن هر سه ماهه توسط یک مشاور امنیتی شخص ثالث بررسی می‌شود.
موضوع سنجش و صفت‌ها	
موضوع سنجش	۱- گزارش بررسی‌های شخص ثالث ۲- طرح‌های بررسی‌های شخص ثالث
صفت	۱- بررسی‌های شخص ثالث گزارش شده ۲- بررسی‌های شخص ثالث طرح ریزی شده
صفت سنجه مبنا	
سنجه مبنا	۱- تعداد بررسی‌های اجرا شده توسط شخص ثالث ۲- تعداد کل بررسی‌های شخص ثالث طرح ریزی شده
روش سنجش	۱- شمارش تعداد گزارش بررسی‌های منظم اجرا شده توسط شخص ثالث ۲- شمارش تعداد کل بررسی‌های شخص ثالث طرح ریزی شده
نوع روش سنجش	۱- عینی ۲- عینی
مقیاس	۱- اعداد صحیح از صفر تا بینهایت ۲- اعداد صحیح از صفر تا بینهایت
نوع مقیاس	۱- ترتیبی ۲- ترتیبی
واحد سنجش	۱- بررسی ۲- بررسی
صفت سنجه مشتق شده	
سنجه مشتق شده	هیچ
عملکرد سنجش	هیچ
صفت شاخص	
شاخص	بهبود نسبت بررسی‌های مستقل انجام گرفته.
مدل تحلیلی	الف) جداسازی [تعداد بررسی‌های انجام شده توسط شخص ثالث] از [تعداد کل بررسی‌های طرح ریزی شده شخص ثالث].
صفت معیار تصمیم	
معیار تصمیم	نسبت حاصل شده شاخص باید اصولا بین ۰/۸ و ۱/۱قرار گیرد تا دستیابی به هدف کنترل و no action انجام شود. و درصورتی که با شرایط ابتدایی مطابقت نکند باید بیش از ۰.۶ باشد.

نتیجه‌های سنجش	
تفسیر شاخص	تفسیر شاخص باید به صورت زیر باشد: معیارهای سازمان برای مدیریت امنیت اطلاعات در سازمان از طریق بررسی شخص ثالث به طور رضایت بخشی در ۰/۸ ≤نسبت≤۱/۱مطابقت داده شده است. معیارهای سازمانی به طور غیرقابل قبولی در [۰.۶≤نسبت≤۰/۸ یا نسبت≤۱/۱]مطابقت داده شده است. نظارت جهت تضمین اینکه بهبود مناسب صورت می‌گیرد مورد نیاز است. معیارهای سازمان در [۰≤نسبت≤۰.۶]مطابقت نمی‌کنند. مداخله فوری جهت تضمین اینکه بهبود مناسب صورت می‌گیرد ضروری است. درصورتی که در پایان سه ماهه دوم شاخص الف) غیرقابل قبول باشد، یک اقدام اصلاحی مورد نیاز است و باید به مدیریت مسئول ISMS انتقال داده شود. درصورتی که درپایان سال شاخص الف) غیرقابل قبول باشد، مدیریت ارشد باید مطلع شود و از آنها درخواست پشتیبانی شود. تاثیر/اثر مطابقت نکردن با معیار فرآیند بررسی مدیریت غیرموثر است. عوامل بالقوه انحراف شامل بودجه پایین، طرح ریزی نادرست و فقدان تعهد مدیریت/کارمندان مهم می‌شود.
قالب‌های گزارش دهی	نمودار میله ای نشان دهنده مطابقت با چندین دوره گزارش دهی در ارتباط با آستانه‌های تعریف شده به وسیله معیارهای تصمیم.
سهام‌داران	
مشتری سنجش	مدیران مسئول ISMS. مدیر سامانه کیفیت
بررسی کننده سنجش	مدیران مسئول ISMS
صاحب اطلاعات	مدیران مسئول ISMS
جمع آورنده اطلاعات	ممیزی داخلی. مدیر کیفیت
بیانگر اطلاعات	ممیزی داخلی. مدیر کیفیت. مدیران مسئول ISMS
تناوب/دوره	
تناوب مجموعه داده	سه ماهه
تناوب تحلیل داده	سه ماهه
تناوب گزارش دهی نتیجه‌ها سنجش	سه ماهه
بازبینی سنجش	بررسی و به روزرسانی برای هر ۲ سال
دوره سنجش	قابل اجرا در ۲ سال

ب-۴ بهبود پیوسته ISMS

ب-۴-۱ کارایی مدیریت حادثه امنیت اطلاعات

شناسایی طرح ریزی سنجش	
سنجش طرح‌ریزی نام	کارایی مدیریت حادثه امنیت اطلاعات

شناسه عددی	ویژه سازمان.
هدف طرح ریزی سنجش	ارزیابی کارایی مدیریت حادثه امنیت اطلاعات
هدف کنترل/فرآیند	امکان پذیر کردن کشف بی درنگ رویدادهای امنیتی و پاسخ به حوادث امنیتی
کنترل (۱) / فرآیند (۱)	بند ۴-۲-۲ ح) استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷
موضوع سنجش و صفت‌ها	
موضوع سنجش	ISMS
صفت	حادثه فردی
صفت سنجه مبنا	
سنجه مبنا	عدد آستانه از پیش تعیین شده
روش سنجش	شمارش رویدادهای حوادث امنیت اطلاعات گزارش شده تا آن تاریخ
نوع روش سنجش	عینی
مقیاس	عددی
نوع مقیاس	ترتیبی
واحد سنجش	حادثه
صفت سنجه مشتق شده	
سنجه مشتق شده	حوادث فراتر از آستانه
عملکرد سنجش	مقایسه تعداد کل حوادث با آستانه
صفت شاخص	
شاخص	نمودار خطی که خط افقی ثابت نشان دهنده اعداد آستانه در مقابل کل تعداد حوادث در چندین دوره گزارش دهی را نشان می‌دهد.
مدل تحلیلی	قرمز زمانی که کل تعداد حوادث از آستانه فراتر می‌رود (بالاتر از خط قرار می‌گیرد)؛ زرد زمانی که کل تعداد حوادث در ۱۰ درصد از آستانه قرار داشته باشد؛ سبز زمانی که کل تعداد حوادث پایین تر از آستانه به میزان ۱۰ درصد یا بیشتر باشد.
صفت معیار تصمیم	
معیار تصمیم	قرمز- بررسی سریع درمورد دلایل افزایش تعداد حوادث مورد نیاز است. زرد- باید بر اعداد به صورت نزدیک نظارت شود و درصورتی که اعداد بهبود نداشته باشند بررسی باید آغاز شود. سبز- هیچ اقدامی‌نیاز نیست.
نتیجه‌های سنجش	
تفسیر شاخص	درصورتی که قرمز در دو چرخه گزارش دهی مشاهده شود، بررسی رویکردهای مدیریت حادثه نیاز است تا رویکردهای موجود یا شناسایی رویکردهای افزوده مورد نیاز است. درصورتی که روند طی دو دوره گزارش دهی آینده معکوس نباید اقدام اصلاحی، مانند پیشنهاد بسط دامنه کاربرد ISMS نیاز است.
قالب‌های گزارش دهی	نمودار خطی
سهام‌داران	

مشتری سنجش	کمیته مدیریت ISMS مدیران مسئول ISMS مدیریت امنیت مدیریت حادثه
بررسی کننده سنجش	مدیران مسئول ISMS
صاحب اطلاعات	مدیران مسئول ISMS
جمع آورنده اطلاعات	مدیر مدیریت حادثه
بیانگر اطلاعات	کمیته مدیریت ISMS
تناوب/دوره	
تناوب مجموعه داده	ماهانه
تناوب تحلیل داده	ماهانه
تناوب گزارش دهی نتیجه‌ها سنجش	ماهانه
بازبینی سنجش	شش ماه
دوره سنجش	ماهانه

ب-۴-۲ اجرای اقدام اصلاحی

شناسایی طرح ریزی سنجش	
سنجش طرح‌ریزی نام	اجرای اقدام اصلاحی
شناسه عددی	شناسه ویژه سازمان.
هدف طرح ریزی سنجش	ارزیابی میزان کارایی اجرا اقدام اصلاحی
هدف کنترل/فرآیند	بند ۸-۲ استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ اقدام اصلاحی سازمان باید اقدامی‌اصلاحی انجام دهد تا دلیل عدم انطباق با الزامات ISMS را به منظور جلوگیری از رخداد مجدد آنها، رفع کند.
کنترل (۱) / فرآیند (۱)	رویکرد مستند شده برای اقدام اصلاحی باید الزامات را برای موارد زیر تعریف کند: الف) شناسایی عدم تطابق‌ها؛ ب) تعیین دلایل عدم تطابق‌ها؛ پ) ارزیابی نیاز به اقدامات جهت تضمین اینکه عدم تطابق‌ها رخ نمی‌دهند؛ ت) تعیین و اجرای اقدام اصلاحی مورد نیاز؛ ث) ثبت نتیجه‌ها اقدام صورت گرفته (مراجعه به ۴-۳-۳)؛ و ج) بررسی اقدام اصلاحی انجام شده. (اجرا شده) ..... سازمان اقدامات اصلاحی مورد نیاز را تعیین می‌کند و گزارش اقدام اصلاحی مستند کننده اطلاعات

	پیرامون عدم تطابق، دلیل آن و تاریخ سررسید آن را برای انجام اقدام اصلاحی منتشر می‌کند. به محض دریافت گزارش، مدیر مسئول حوزه ای که عدم تطابق درآن کشف شده است باید تضمین کند که جهت برطرف کردن عدم تطابق‌ها و دلایل آنها اقدامات بدون تاخیر بی مورد انجام می‌شوند. درصورتی که اقدام اصلاحی به صورتی که نیاز است انجام نشود، دلیل عدم اجرا و همچنین جایگزین‌ها برای اقدام اصلاحی اصلی که به عنوان اقدام مقتضی تعیین می‌شوند باید شناسایی شوند. اقدامات انجام شده با تاریخ و نتیجه‌ها مشابه باید مستند شوند. درصورتی که اقدام اصلاحی به طوری که طرح ریزی شده است اجرا نشود، دلیل و اقدام جایگزین باید مستند شود. گزارش باید در اختیار مدیریت امنیت اطلاعات قرار گیرد.
موضوع سنجش و صفت‌ها	
موضوع سنجش	گزارش‌های اقدام اصلاحی
صفت	تاریخ سررسید اقدام اصلاحی در گزارش. تاریخ اقدام اصلاحی انجام شده در ثبت گزارش. دلیل تاخیر و صورت نگرفتن اقدام.
صفت سنجه مبنا	
سنجه مبنا	۱- تعداد اقدامات اصلاحی طرح ریزی شده تا تاریخ کنونی. ۲- تعداد اقدامات اصلاحی اجرا شده که تا تاریخ کنونی طرح ریزی شده‌اند . ۳- تعداد اقدامات اصلاحی که با دلیل اجرا نشده‌اند تا تاریخ کنونی.
روش سنجش	- شمارش اقدامات اصلاحی طرح ریزی شده برای اجرا شدن تا تاریخ کنونی. - شمارش اقدامات اصلاحی که به عنوان اجرا شده در تاریخ سررسید ثبت شده‌اند . - شمارش اقدامات اصلاحی که به عنوان اقدامات طرح ریزی شده ثبت شده‌اند که به دلیلی انجام نشده‌اند .
نوع روش سنجش	۱-۳ عینی
مقیاس	۱-۳ اعداد صحیح از صفر تا بینهایت
نوع مقیاس	۱-۳ ترتیبی
واحد سنجش	۱-۳ اقدام اصلاحی
صفت سنجه مشتق شده	
سنجه مشتق شده	الف) اقدام اصلاحی که تا تاریخ کنونی اجرا نشده‌اند ب) اقدام اصلاحی اجرا نشده بدون دلیل قانونی
عملکرد سنجش	الف) تفریق [اقدامات اصلاحی طرح ریزی شده انجام شده تا تاریخ کنونی] از [اقدامات اصلاحی طرح ریزی شده تا تاریخ کنونی] ب) تفریق [اقدام اصلاحی اجرا نشده تا تاریخ کنونی] از [اقدامات اصلاحی طرح ریزی شده با دلیل انجام نشده تا تاریخ کنونی]
صفت شاخص	
شاخص	الف) وضعیت بیان شده از اقدام اصلاحی اجرا نشده به شکل نسبت. ب) وضعیت بیان شده از اقدام اصلاحی بدون دلیل اجرا نشده به شکل نسبت پ) روند وضعیت

مدل تحلیلی	الف) تقسیم [اقدام اصلاحی اجرا نشده تا تاریخ کنونی] بر [اقدامات اصلاحی طرح ریزی شده تا تاریخ کنونی] ب) تقسیم [اقدام اصلاحی بدون دلیل اجرا نشده] بر [اقدامات اصلاحی طرح ریزی شده تا تاریخ کنونی] پ) مقایسه وضعیت‌ها با وضعیت‌های گذشته.
صفت معیار تصمیم	
معیار تصمیم	به منظور دستیابی به هدف و no action نسبت‌های شاخص الف) و ب) باید به ترتیب بین ۰.۴ و ۰.۰ و بین ۰.۲ و ۰.۰ قرار گیرد و روند شاخص پ) برای دو دوره گزارش دهی آخر کاهش یابد. شاخص پ) باید در مقایسه با شاخص‌های گذشته ارائه شود از این رو روند اجرای اقدام اصلاحی باید آزمایش شود.
نتیجه‌ها سنجش	
تفسیر شاخص	تفسیر شاخص الف) و ب) باید به شکل زیر باشد: اقدامات اصلاحی طرح ریزی شده باید اجرا شود مگر اینکه اولویت‌های سازمان تغییر کند که به نیاز به اجرای اقدامات اصلاحی مختلف و تعیین جهت مجدد منابع اختصاص یافته به اجرای اقدام اصلاحی منجر می‌شود. درصورتی که بیش از ۴۰ درصد از اقدامات اصلاحی صرف نظر از دلیل اجرا نشود، اقدامات مدیریت مورد نیاز است. درصورتی که بیش از ۲۰ درصد از اقدامات اصلاحی بدون دلیل مناسب اجرا نشود، اقدام مدیریت مورد نیاز است. اقدامات اصلاحی که اجرا نشده‌اند باید برای شناسایی دلایل عدم اجرا بررسی شوند. بسته به درصد کلی اجرا نشده و دلایل عدم اجرا، ممکن است اقدامات بیشتر مورد نیاز باشد. تفسیر شاخص پ)باید به صورت زیر باشد: روند اجرای اقدام اصلاحی باید هر پسرفت کلی عملکرد یا بهبود قابل توجه در عملکرد بررسی شود. درصورتی که درصد اقدام اصلاحی انجام شده برای دو دوره گزارش دهی آخر به طور پیوسته و یکنواخت کاهش یابد، اقدام مدیریت صرف نظر از تفکیک دلایل برای عدم مطابقت مورد نیاز است. تاثیر/اثر عدم مطابقت با معیارها فقدان بالقوه بهبود مداوم ISMS است. دلایل بالقوه ممکن است شامل فقدان منابع، طرح ریزی نادرست و فقدان تعهد مدیریت و کارمندان مهم است.
قالب‌های گزارش دهی	نمودار میله ای ردیفی دارای شرح نتیجه‌ها سنجش شامل خلاصه اجرایی یافته‌ها و اقدامات مدیریتی احتمالی که تعداد کل اقدامات اصلاحی را نشان می‌دهد به اجرا شده، اجرا نشده بدون دلیل قانونی و اجرا نشده با دلیل قانونی تقسیم می‌شود.
سهام‌داران	
مشتری سنجش	مدیران مسئول ISMS. مدیر امنیت اطلاعات.
بررسی کننده سنجش	مدیران مسئول ISMS
صاحب اطلاعات	مدیران مسئول ISMS
جمع آورنده اطلاعات	مدیران مسئول ISMS
بیانگر اطلاعات	مدیران مسئول ISMS
تناوب/دوره	
تناوب مجموعه داده	سه ماهه

تناوب تحلیل داده	سه ماهه
تناوب گزارش دهی نتیجه‌ها سنجش	سه ماهه
بازبینی سنجش	بررسی سالانه
دوره سنجش	قابل اجرا در ۱ سال

ب-۵ تعهد مدیریت

شناسایی طرح ریزی سنجش	
سنجش طرح‌ریزی نام	تناوب بررسی مدیریت
شناسه عددی	ویژه سازمان.
هدف طرح ریزی سنجش	ارزیابی تعهد مدیریت و فعالیت‌های امنیت اطلاعات پیرامون فعالیت‌های بررسی مدیریتی
هدف کنترل/فرآیند	الف-۶-۱ مدیریت امنیت اطلاعات در سازمان (طرح ریزی شده). مدیریت امنیت اطلاعات در سازمان از طریق اجرای منظم بررسی‌های مدیریتی.
کنترل (۱) / فرآیند (۱)	الف-۶-۱-۱ تعهد مدیریت نسبت به امنیت اطلاعات مدیریت باید فعالانه از طریق جهت دهی شفاف، تعهد اثبات شده، انتصاب صریح و تایید امنیت اطلاعات از امنیت در سازمان پشتیبانی کند (اجرا شده). سازمان باید ماهانه نشست‌های بررسی مدیریتی را جهت پشتیبانی از امنیت در سازمان از طریق جهت دهی شفاف، تعهد اثبات شده، انتصاب صریح و تایید امنیت اطلاعات برگزار کند. بررسی مدیریت ISMS باید با بررسی مدیریت QMS ترکیب شود.
کنترل(۲) /فرآیند(۲)	الف-۶-۱-۲ هماهنگی امنیت اطلاعات فعالیت‌های امنیت اطلاعات به وسیله نماینده‌ها از بخش‌های مختلف سازمان دارای عملکردهای شغلی و نقش‌های مرتبط هماهنگ شود. (اجرا شده). نماینده‌های بخش‌های مختلف که نقش‌ها و مسئولیت‌های مرتبط دارند باید هماهنگ شوند و در بررسی مدیریت شرکت کنند.
موضوع سنجش و صفت‌ها	
موضوع سنجش	۱- طرح/برنامه زمانبندی بررسی مدیریت امنیت اطلاعات ۲- ثبت صورت جلسات بررسی مدیریت
صفت	۱-۱ تاریخ‌های جلسات بررسی مدیریت که در طرح برنامه ریزی شده است ۱-۲ مدیرانی که براساس برنامه ریزی زمان بندی در جلسات بررسی مدیریتی شرکت می‌کنند ۲-۱ تاریخ جلسات بررسی مدیریت که در صورت جلسات جلسه ثبت شده است ۲-۲ مدیرانی که شرکت کردن آن در جلسات بررسی مدیریتی ثبت شده است
صفت سنجه مبنا	
سنجه مبنا	۱-۱ تعداد جلسات بررسی مدیریتی که تا تاریخ کنونی طرح ریزی شده است ۱-۲ تعداد مدیرانی که براساس برنامه ریزی شده است تا در جلسات بررسی مدیریتی شرکت کنند ۲-۱-۱ تعداد جلسات بررسی مدیریتی طرح ریزی شده که تا تاریخ کنونی برگزار شده است

	۲-۱-۲ تعداد جلسات بررسی مدیریتی طرح ریزی نشده که تا تاریخ کنونی برگزار شده است. ۲-۱-۳ تعداد جلسات بررسی مدیریتی دوباره برنامه ریزی شده که تا تاریخ کنونی برگزار شده است ۲-۳ تعداد مدیرانی که تا تاریخ کنونی در جلسات بررسی مدیریتی شرکت کرده اند
روش سنجش	۱-۱ شمارش جلسات بررسی مدیریتی برنامه ریزی شده تا تاریخ کنونی ۱-۲ به ازای جلسات بررسی تا تاریخ کنونی، شمارش مدیرانی که شرکت آن برنامه ریزی شده است و افزودن یک ورودی جدید با مقدار قراردادی برای جلسات صورت گرفته برنامه ریزی نشده به روش موردی ۲-۱-۱ شمارش جلسات برگزار شده بررسی مدیریتی طرح ریزی شده تا تاریخ کنونی ۲-۱-۲ شمارش جلسات برگزار شده بررسی مدیریتی طرح ریزی نشده تا تاریخ کنونی ۲-۱-۳ شمارش جلسات برگزار شده بررسی مدیریتی دوباره برنامه ریزی شده تا تاریخ کنونی ۲-۲ برای تمام جلسات بررسی مدیریتی برگزارش شده، شمارش تعداد مدیرانی که شرکت کرده اند.
نوع روش سنجش	۱-۱ عینی ۱-۲ عینی یا ذهنی ۲-۱-۱ عینی ۲-۱-۲ عینی ۲-۱-۳ عینی ۲-۲ عینی
مقیاس	۱-۱ اعداد صحیح از صفر تا بینهایت ۱-۲ اعداد صحیح از صفر تا بینهایت ۲-۱-۱ اعداد صحیح از صفر تا بینهایت ۲-۱-۲ اعداد صحیح از صفر تا بینهایت ۲-۱-۳ اعداد صحیح از صفر تا بینهایت ۲-۲ اعداد صحیح از صفر تا بینهایت
نوع مقیاس	۱-۱ ترتیبی ۱-۲ ترتیبی ۲-۱-۱ ترتیبی ۲-۱-۲ ترتیبی ۲-۱-۳ ترتیبی ۲-۲ ترتیبی
واحد سنجش	۱-۱ جلسه ۱-۲ کارمندان ۲-۱-۱ جلسه ۲-۱-۲ جلسه ۲-۱-۳ جلسه ۲-۲ کارمندان
صفت سنجه مشتق شده	

سنجه مشتق شده	الف)تعداد جلسات برگزار شده بررسی مدیریتی تا تاریخ کنونی ب) میزان شرکت در جلسات برگزار شده بررسی مدیریتی تا تاریخ کنونی
عملکرد سنجش	الف) افزودن [تعداد جلسات طرح ریزی شده بررسی مدیریتی تا تاریخ کنونی] و [تعداد تعداد جلسات طرح ریزی نشده بررسی مدیریتی تا تاریخ کنونی] و [تعداد جلسات دوباره برنامه ریزی شده بررسی مدیریتی تا تاریخ کنونی] ب) برای هر جلسه بررسی مدیریتی [تعدااد مدیرانی که در جلسه بررسی مدیریتی شرکت کرده اند] بر [تعداد مدیرانی که برنامه ریزی شده است تا در جلسه بررسی مدیریتی شرکت کنند] تقسیم می‌شود.
صفت شاخص	
شاخص	الف) جلسات به پایان رسید بررسی مدیریتی تا تاریخ کنونی ب) میزان میانگین شرکت در جلسات بررسی مدیریتی تا تاریخ کنونی
مدل تحلیلی	الف) تقسیم [جلسات انجام شده بررسی مدیریتی] بر [جلسات بررسی مدیریتی برنامه ریزی شده] ب) محاسبه انحراف متوسط و استاندارد کل میزان شرکت در جلسات بررسی مدیریتی
صفت معیار تصمیم	
معیار تصمیم	نسبت شاخص حاصل شده الف) باید بین ۰.۷ و ۱/۱قرار گیرد تا هدف کنترل و no action بدست آید. حتی اگر این امر موفق نباشد، باید همچنان بالاتر از ۰.۵ قرار داشته باشد تا به حداقل بازده بدست آید. با توجه به شاخص ب)محدودیت‌های اطمینان محاسبه شده مبتنی بر انحراف استاندارد، احتمال اینکه نتیجه واقعی نزدیک به میانگین میزان شرکت کردن بدست آید را نشان می‌دهد. محدودیت‌های بسیار گسترده اطمینان انحراف به صورت بالقوه زیاد و نیاز به طرح ریزی احتمالی برای رسیدگی به این نتیجه را نشان می‌دهد.
نتیجه‌ها سنجش	
تفسیر شاخص	تفسیر شاخص الف) باید به شکل زیر باشد: معیار سازمان برای مدیریت امنیت اطلاعات در سازمان از طریق بررسی مدیریتی در ۰.۷≥نسبت≥۱/۱به صورت قابل قبولی مطابقت دارد؛ معیار سازمانی در [۰.۵≥نسبت≥۰.۷ یا نسبت≥۱/۱] به صورت غیرقابل قبولی مطابقت دارد. این نتیجه ممکن است فقدان احتمالی تعهد مدیریتی را نشان دهد و ممکن است مستلزم اقدام اصلاحی باشد. نتیجه‌ها متعاقب سنجش باید از جهت بهبود نظارت و ارزیابی شود. معیارسازمان در [۰≥نسبت≥۰.۵] مطابقت نمی‌کنند. این نتیجه فقدان تعهد مدیریتی را نشان می‌دهد و مستلزم مداخله سریع جهت اجرای اقدام اصلاحی مناسب است. مدیریت ارشد باید از نتیجه مطلع شود. نسبت نزدیک به ۰ می‌تواند فقدان تعهد مدیریت ارشد را نشان دهد. درصورتی که مدیران ISMS بررسی‌ها را به عنوان اولویت درنظر نمی‌گیرند، ممکن است تحت نفوذ مدیران ارشد قرار گیرند. تاثیر/ اثر عدم مطابقت با معیار فقدان بالقوه‌یک فرآیند بررسی مدیریتی موثر و مداوم است. دلایل بالقوه انحراف در شاخص ب) می‌تواند شامل طرح ریزی نادرست، تعهد ناکافی مدیران مسئول ISMS، اولویت‌های ناسازگار و یا کار زیاد تاثیر گذار بر مدیران ISMS باشد.
قالب‌های گزارش دهی	نمودار خطی نشان دهنده شاخص با معیار چندین مجموعه داده ای و دوره‌های گزارش دهی با توضیح نتیجه‌ها سنجش. تعداد مجموعه‌های داده و دوره‌های گزارش دهی باید توسط سازمان

	تعریف شود.
سهام‌داران	
مشتری سنجش	مدیران مسئول ISMS. مدیر سامانه کیفیت.
بررسی کننده سنجش	مرجع برنامه داخلی ممیزی ISMS
صاحب اطلاعات	مدیر سامانه کیفیت سامانه فرضی مدیریتی ترکیب شده QMS و ISMS
جمع آورنده اطلاعات	مدیر کیفیت. مدیر امنیت اطلاعات
بیانگر اطلاعات	مدیر امنیت اطلاعات. مدیر کیفیت
تناوب/دوره	
تناوب مجموعه داده	ماهانه
تناوب تحلیل داده	سه ماهه
تناوب گزارش دهی نتیجه‌ها سنجش	سه ماهه
بازبینی سنجش	بررسی و به روز رساتی هر ۲ سال
دوره سنجش	قابل اجرا در ۲ سال

ب-۶ محافظت دربرابر کد مخرب

شناسایی طرح ریزی سنجش	
سنجش طرح‌ریزی نام	حفاظت دربرابر نرم افزار مخرب
شناسه عددی	ویژه سازمان.
هدف طرح ریزی سنجش	ارزیابی کارایی سامانه حفاظتی در برابر حملات نرم افزار مخرب.
هدف کنترل/فرآیند	هدف کنترل الف ۱۰-۴ استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ حفاظت از یکپارچگی نرم افزار و اطلاعات. (طرح ریزی شده) محافظت دربرابر یکپارچگی نرم افزار و اطلاعات دربرابر نرم افزار مخرب.
کنترل (۱) / فرآیند (۱)	کنترل ۱۰-۴-۱ [2700:2005]. کنترل دربرابر کد مخرب. کنترل کشف، پیشگیری و بازیابی جهت محافظت دربرابر کد مخرب و رویکردهای مناسب آگاهی کاربر باید اجرا شود.
موضوع سنجش و صفت‌ها	
موضوع سنجش	۱- گزارش حادثه ۲- ثبت وقایع نرم افزار اقدام متقابل در برابر نرم افزار مخرب
صفت	حوادثی که به وسیله نرم افزار مخرب ایجاد می‌شوند
صفت سنجه مبنا	
سنجه مبنا	۱- تعداد حوادث امنیتی که به وسیله نرم افزار مخرب ایجاد شده است.

	۲- حملات مسدود شده که در کل به وسیله نرم افزار مخرب ایجاد شده است.
روش سنجش	۱- شمارش تعداد حوادث امنیتی در گزارش حوادث که به وسیله نرم افزار مخرب به وجود می‌آید. ۲- شمارش تعداد سوابق حملات مسدود شده
نوع روش سنجش	۱- عینی ۲- عینی
مقیاس	۱- اعداد صحیح از صفر تا بینهایت ۲- اعداد صحیح از صفر تا بینهایت
نوع مقیاس	۱- ترتیبی ۲- ترتیبی
واحد سنجش	۱- حادثه امنیتی ۲- سوابق
صفت سنجه مشتق شده	
سنجه مشتق شده	قدرت حفاظت نرم افزار مخرب
عملکرد سنجش	تعداد حوادث امنیتی که به وسیله نرم افزار مخرب ایجاد می‌شود/تعداد حملات کشف شده و مسدود شده که به وسیله نرم افزار مخرب ایجاد می‌شود.
صفت شاخص	
شاخص	روند حملات کشف شده که طی چندین دوره گزارش دهی مسدود نشده‌اند .
مدل تحلیلی	مقایسه نسبت با درصد گذشته
صفت معیار تصمیم	
معیار تصمیم	خطوط روند باید زیر عدد مشخص شده باقی بماند. روند حاصل شده باید نزولی یا ثابت باشد.
نتیجه‌ها سنجش	
تفسیر شاخص	روند صعودی نشانگر مطابقت روبه کاهش است، روند نزولی نشانگر مطابقت درحال بهبود است؛ و زمانی که روند به صورت قابل توجهی افزایش یابد، بررسی دلیل و فضا برای اقدامات متقابل بیشتر نیاز است.
قالب‌های گزارش دهی	خط روند که نسبت کشف و پیشگیری نرم افزار مخرب را با خطوط تولید شده طی دوره‌های گزارش دهی گذشته نشان می‌دهد.
سهام‌داران	
مشتری سنجش	مدیریت امنیت
بررسی کننده سنجش	مدیریت امنیت
صاحب اطلاعات	مدیر سامانه
جمع آورنده اطلاعات	مدیریت امنیت؛ مدیر سامانه؛ مدیر شبکه
بیانگر اطلاعات	هماهنگی خدمت
تناوب/دوره	
تناوب مجموعه داده	روزانه

تناوب تحلیل داده	ماهانه
تناوب گزارش دهی نتیجه‌ها سنجش	ماهانه
بازبینی سنجش	بررسی سالانه
دوره سنجش	قابل اجرا در ۱ سال

ب-۷ کنترل‌های فیزیکی ورودی

شناسایی طرح ریزی سنجش	
سنجش طرح‌ریزی نام	کنترل فیزیکی ورودی با کارت‌های دسترسی
شناسه عددی	ویژه سازمان.
هدف طرح ریزی سنجش	نمایش وجود، گسترش و کیفیت سامانه مورد استفاده برای کنترل دسترسی
هدف کنترل/فرآیند	هدف کنترل الف-۹-۱ استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ پیشگیری از دسترسی فیزیکی، تخریب و برقرار ارتباط غیر مجاز با متعلقات و اطلاعات سازمان.
کنترل (۱) / فرآیند (۱)	کنترل الف-۹-۱-۲ استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷. کنترل فیزیکی ورودی. مناطق ایمن باید به وسیله کنترل ورودی مناسب جهت تضمین اینکه تنها کارمندان مجاز اجازه دسترسی دارند حفاظت شود.
موضوع سنجش و صفت‌ها	
موضوع سنجش	مناطق ایمن
صفت	سوابق مدیریت هویت
صفت سنجه مبنا	
سنجه مبنا	کنترل فیزیکی ورودی با کارت‌های دسترسی
روش سنجش	روش سنجش وابسته که هر درجه زیرمجموعه بخشی از درجه بالاتر است. کنترل نوع سامانه کنترل ورودی و بررسی جنبه‌های زیر: - وجود سامانه کارت کنترل دسترسی - استفاده از PIN کد - عملکرد ثبت وقایع - تصدیق بیومتریک
نوع روش سنجش	ذهنی
مقیاس	۰-۵ ۰ هیچ سامانه کنترل دسترسی وجود ندارد. ۱ یک سامانه دسترسی وجود دارد که PIN کد (سامانه یک فاکتور) برای کنترل ورودی مورد استفاده می‌شود. ۲ یک سامانه کارت کنترل دسترسی وجود دارد که کارت عبور (سامانه یک فاکتور) برای کنترل ورود استفاده می‌شود. ۳ یک سامانه کارت دسترسی وجود دارد که کارت عبور و PIN کد برای کنترل ورود استفاده

	می‌شود. ۴ پیشین+ عملکرد ثبت وقایع فعال شده ۵ پیشین+ PIN کد به وسیله تصدیق بیومتریک جایگزین می‌شود (اثر انگشت، تشخیص صوت، اسکن شبکیه و غیره).
نوع مقیاس	ترتیبی
واحد سنجش	N/A
صفت سنجه مشتق شده	
سنجه مشتق شده	هیچ
عملکرد سنجش	هیچ
صفت شاخص	
شاخص	میله‌های بهبود. قرمز تا ۰و۸، سبز بین ۰/۸ و ۱.
مدل تحلیلی	تحلیل سنجه
صفت معیار تصمیم	
معیار تصمیم	مقدار۳= قابل قبول
نتیجه‌ها سنجش	
تفسیر شاخص	پایین تر از ۳ قابل قبول، که(۳- درجه واقعی=شکاف امنیتی)، اقدامات جهت صورت گرفتن مبتنی بر وسعت شکاف امنیتی است. بالاتر از ۳ با برتری قابل قبول است که درجه ممکن است بالاتر از سرمایه گذاری پیرامون موضوع سنجیده شده نشان داده شود.
قالب‌های گزارش دهی	نمودارها
سهام‌داران	
مشتری سنجش	کمیته مدیریت
بررسی کننده سنجش	ارزیاب داخلی/ارزیاب خارجی
صاحب اطلاعات	مدیر امکانات
جمع آورنده اطلاعات	ارزیاب داخلی/ارزیاب خارجی
بیانگر اطلاعات	ارزیاب داخلی و مدیریت امنیت
تناوب/دوره	
تناوب مجموعه داده	سالانه
تناوب تحلیل داده	سالانه
تناوب گزارش دهی نتیجه‌ها سنجش	سالانه
بازبینی سنجش	۱۲ ماه
دوره سنجش	قابل اجرا در ۱۲ ماه

ب-۸ بررسی فایل‌های ثبت واقعه

شناسایی طرح ریزی سنجش	
سنجش طرح‌ریزی نام	بررسی فایل‌های ثبت واقعه
شناسه عددی	شناسه عددی منحصر به فرد ویژهسازمان.
هدف طرح ریزی سنجش	ارزیابی وضعیت مطابقت بررسی منظم فایل‌های مهم ثبت واقعه سامانه
هدف کنترل/	هدف کنترل الف-۱۰-۱۰ استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ . شناسایی فعالیت‌های فرآیند اطلاعات غیر مجاز. (طرح ریزی شده) شناسایی فعالیت‌های فرآیند اطلاعات غیر مجاز سامانه‌های حساس از ثبت وقایع سامانه.
کنترل (۱)	کنترل الف ۱۰-۱۰-۲ استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ رویکردهای استفاده نظارتی از امکانات فرآیند اطلاعات باید برقرار شود و نتیجه‌ها فعالیت‌های نظارتی باید به طور منظم بررسی شود.
موضوع سنجش و صفت‌ها	
موضوع سنجش	سامانه
صفت	فایل‌های ثبت وقایع فرد
صفت سنجه مبنا (۱)	
سنجه مبنا	تعداد فایل‌های ثبت وقایع
روش سنجش	جمع تعداد کل فایل‌های ثبت وقایع فهرست شده در فهرست بررسی ثبت وقایع
نوع روش سنجش	عینی
مقیاس	اعداد صحیح از صفر تا بینهایت
نوع مقیاس	ترتیبی
واحد سنجش	فایل ثبت وقایع
صفت سنجه مبنا (۲)	
سنجه مبنا	تعداد فایل‌های ثبت وقایع بررسی شده
روش سنجش	جمع تعداد کل فایل‌های ثبت وقایع در کل سامانه در حوزه ISMS
نوع روش سنجش	عینی
مقیاس	عددی
نوع مقیاس	نسبت
واحد سنجش	فایل ثبت وقایع
صفت سنجه مبنا (۳)	
سنجه مبنا	تعداد سامانه‌ها در حوزه ISMS
روش سنجش	شناسایی تعداد فایل‌های ثبت وقایع بررسی شده

نوع روش سنجش	عینی
مقیاس	عددی
نوع مقیاس	نسبت
واحد سنجش	فایل ثبت وقایع
صفت سنجه مشتق شده	
سنجه مشتق شده	درصد فایل‌های ثبت وقایع بررسی شده ممیزی هنگامی‌که نیاز است به ازای هر دوره زمانی
عملکرد سنجش	(# فایل‌های ثبت وقایع بررسی شده در دوره زمانی مشخص شده)/(کل# فایل‌های ثبت وقایع)*۱۰۰
صفت شاخص	
شاخص	نمودار خطی یک روند در طول دوره زمانی در میزان بررسی ثبت وقایع ممیزی
مدل تحلیلی	روند صعودی به سوی ۱۰۰٪ مطلوب است.
صفت معیار تصمیم	
معیار تصمیم	نتیجه زیر ۲۰ درصد باید به دلایل تحت اجرا آزمایش شود.
نتیجه‌ها سنجش	
تفسیر شاخص	مقادیر کمتر از مقدار تعریف شده توسط غیرقابل قبول هستند درموقعیتی که (تعریف شده سازمانی- مقدار واقعی=شکاف امنیتی). اقدام مدیریتی مبتنی بر وسعت شکاف امنیتی مورد نیاز است. مقادیر بیشتر از مقدار تعریف شده توسط سازمان ممکن است هنگام سرمایه گذاری نشان داده شود مگر اینکه این مکانیزم کنترل به ازای هر ارزیابی خطر مورد نیاز باشد.
قالب‌های گزارش دهی	نمودار خطی که نشان دهنده روندی با خلاصه ای از یافته‌ها و هر اقدام مدیریتی پیشنهادی است.
سهام‌داران	
مشتری سنجش	مدیران مسئول ISMS، مدیر امنیتی
بررسی کننده سنجش	مدیر امنیت
صاحب اطلاعات	مدیر امنیت
جمع آورنده اطلاعات	کارمند امنیت
بیانگر اطلاعات	کارمند امنیت
تناوب/دوره	
تناوب مجموعه داده	ماهانه
تناوب تحلیل داده	ماهانه
تناوب گزارش دهی نتیجه‌ها سنجش	سه ماهه
بازبینی سنجش	بررسی و به روز رسانه هر ۲ سال
دوره سنجش	قابل اجرا در ۲ سال

ب-۹ مدیریت حفاظت دوره ای

شناسایی طرح ریزی سنجش

سنجش طرح‌ریزی نام	مدیریت حفاظت دوره ای
شناسه عددی	ویژه سازمان.
هدف طرح ریزی سنجش	ارزیابی مناسبت فعالیت‌های حفاظت در ارتباط با برنامه
هدف کنترل/فرآیند	هدف کنترل الف-۹-۲ استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ ممانعیت از خسارت، آسیب دیدگی، دزدی یا سوءاستفاده از دارایی‌ها و توقف فعالیت‌های سازمان. (طرح ریزی شده) ممانعیت از خسارت، آسیب دیدگی، دزدی یا سوءاستفاده از دارایی‌ها و توقف فعالیت‌های سازمان از طریق حفاظت دوره ای سامانه.
کنترل (۱) / فرآیند (۱)	کنترل الف۹-۲-۴ استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ . تجهیزات باید به درستی حفاظت شوند تا قابلیت دسترسی و یکپارچگی مداوم آن تضمین شود.
موضوع سنجش و صفت‌ها	
موضوع سنجش	۱- طرح/برنامه حفاظت سامانه ۲- سوابق حفاظت سامانه
صفت	۱- تاریخ‌های نگهداری سامانه طرح ریزی شده/برنامه ریزی شده ۲- تاریخ‌های نگهداری سامانه تکمیل شده
صفت سنجه مبنا (۱-۴)	
سنجه مبنا	۱- تاریخ‌های نگهداری برنامه ریزی شده ۲- تاریخ‌های نگهداری تکمیل شده ۳- تعداد کل رویدادهای نگهداری طرح ریزی شده ۴- تعداد کل رویدادهای نگهداری تکمیل شده
روش سنجش	۱- استخراج تاریخ‌های برنامه ریزی شده از طرح نگهداری سامانه ۲- استخراج تاریخ‌های تکمیل شده از سوابق نگهداری سامانه ۳- شمارش تعداد رویدادهای نگهداری برنامه ریزی شده در طرح نگهداری سامانه ۴- شمارش سوابق نگهداری
نوع روش سنجش	عینی
مقیاس	۱- زمان ۲- زمان ۳- عدد صحیح از صفر تا بینهایت ۴- عدد صحیح از صفر تا بینهایت
نوع مقیاس	۱- فهرست ۲- فهرست ۳- ترتیبی ۴- ترتیبی
واحد سنجش	۱- فاصله مانی ۲- فاصله زمانی ۳- رویدادهای نگهداری

	۴- رویدادهای نگهداری
صفت سنجه مشتق شده	
سنجه مشتق شده	تاخیر نگهداری به ازای هر رویداد نگهداری تکمیل شده
عملکرد سنجش	برای هر رویداد تکمیل شده، تفریق [تاریخ نگهداری واقعی] از [تاریخ نگهداری برنامه ریزی شده]
صفت شاخص	
شاخص	۱- میانگین تاخیر نگهداری ۲- نسبت رویدادهای نگهداری تکمیل شده ۳- روند میانگین تاخیر نگهداری ۴- روند نسبت رویدادهای نگهداری تکمیل شده
مدل تحلیلی	۱- تقسیم (مجموع [تاخیر نگهداری به ازای هر رویداد نگهداری تکمیل شده]) بر [تعداد رویدادهای نگهداری تکمیل شد] ۲- تقسیم [تعداد رویدادهای نگهداری تکمیل شده] بر [تعداد رویدادهای نگهداری طرح ریزی شده] ۳- مقایسه شاخص ۱ در چندین دوره زمانی ۴- مقایسه شاخص ۲ در چندین دوره زمانی
صفت معیار تصمیم	
معیار تصمیم	۱- ویژه سازمان، برای مثال، درصورتی که میانگین تاخیر به طور مداوم در بیش از ۳ روز نشان داده شده است، دلایل باید مورد آزمایش قرار گیرند. ۲- نسبت رویدادهای نگهداری تکمیل شده باید بزرگتر از ۰/۹ باشد ۳- روند باید ثابت یا نزدیک به ۰ باشد ۴- روند باید ثابت یا صعودی باشد.
نتیجه‌ها سنجش	
تفسیر شاخص	شاخص به اندازه گیری کیفیت فرآیند نگهداری تجهیزات کمک می‌کند.
قالب‌های گزارش دهی	نمودار خطی که نشان دهنده میانگین انحراف تاخیر نگهداری را نشان می‌دهد به خطوط تولید شده طی دوره‌های گذشته گزارش دهی و تعداد سامانه‌ها در حوزه اضافه می‌شود. تعریف یافته‌ها و توصیه اقدام بالقوه مدیریتی
سهام‌داران	
مشتری سنجش	مدیران مسئول ISMS، مدیر امنیت
بررسی کننده سنجش	مدیر امنیت
صاحب اطلاعات	مدیر سامانه
جمع آورنده اطلاعات	کارمند امنیتی
بیانگر اطلاعات	کارمند امنیتی
تناوب/دوره	
تناوب مجموعه داده	سالانه
تناوب تحلیل داده	سالانه
تناوب گزارش دهی	سالانه

نتیجه‌ها سنجش	
بازبینی سنجش	سالانه
دوره سنجش	سالانه

ب-۱۰ امنیت در توافقنامه‌های شخص ثالث

شناسایی طرح ریزی سنجش	
سنجش طرح‌ریزی نام	امنیت در توافقنامه‌های شخص ثالث
شناسه عددی	ویژه سازمان.
هدف طرح ریزی سنجش	ارزیابی درجه ای که در آن امنیت در توافقنامه‌های شخص ثالث فرآیند اطلاعات کارمندان مورد توجه قرار می‌گیرد.
هدف کنترل/فرآیند	هدف کنترل الف-۶-۲ استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ حفاظت از امنیت اطلاعات سازمان و امکانات فرآیند اطلاعات که بخش‌های خارجی به آنها دسترسی می‌یابند، فرآیند می‌کنند، ارتباط برقرار می‌کنند یا مدیریت می‌کنند.
کنترل (۱)/ فرآیند (۱)	کنترل الف-۶-۲-۳ استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ -سال ۸۷ توافقنامه‌ها با شخص ثالث شامل دسترسی، فرآیند، برقراری ارتباط یا مدیریت اطلاعات سازمان یا امکانات فرآیند اطلاعات، یا افزودن محصولات یا خدمات به امکانات فرآیند اطلاعات باید تمام الزامات امنیتی را پوشش دهد.
موضوع سنجش و صفت‌ها	
موضوع سنجش	توافق نامه‌های شخص ثالث
صفت	بندها یا الزامات امنیتی در هر توافقنامه شخص ثالث.
صفت سنجه مبنا (۱)	
سنجه مبنا	تعداد توافقنامه‌های شخص ثالث
روش سنجش	بررسی توافق نامه‌های شخص ثالث، شمارش تعداد توافقنامه‌ها
نوع روش سنجش	عینی
مقیاس	اعداد صحیح از صفر تا بینهایت
نوع مقیاس	ترتیبی
واحد سنجش	توافقنامه شخص ثالث
صفت سنجه مبنا (۲)	
سنجه مبنا	تعداد الزامات امنیتی استاندارد مورد نیاز برای توافقنامه‌های شخص ثالث
روش سنجش	شناسایی تعداد الزامات امنیتی که باید در هر توافقنامه به ازای هر خط مشی باید مورد توجه قرار گیرد
نوع روش سنجش	عینی
مقیاس	اعداد صحیح از صفر تا بینهایت
نوع مقیاس	ترتیبی

واحد سنجش	الزامات
صفت سنجه مبنا (۳)	
سنجه مبنا	تعداد الزامات امنیتی مورد توجه قرار گرفته در هر توافقنامه شخص ثالث
روش سنجش	بررسی توافقنامه‌های شخص ثالث، شمارش تعداد الزامات امنیتی مورد توجه قرار گرفته در هر توافقنامه
نوع روش سنجش	عینی
مقیاس	اعداد صحیح از صفر تا بینهایت
نوع مقیاس	ترتیبی
واحد سنجش	الزامات
صفت سنجه مشتق شده	
سنجه مشتق شده	درصد میانگین الزامات امنیتی مرتبط که در توافقنامه‌های شخص ثالث مورد توجه قرار گرفته است.
عملکرد سنجش	مجموع (برای هر توافقنامه (تعداد الزامات مورد نیاز- تعداد الزامات مورد توجه قرار گرفته- تعداد الزامات مورد توجه قرار گرفته))/تعداد توافقنامه‌ها
صفت شاخص	
شاخص	۱- نسبت میانگین تفاوت الزامات استاندارد جهت توجه به الزامات ۲- روند نسبت
مدل تحلیلی	۱- مجموع (برای هر توافقنامه ([الزامات امنیتی به طور کلی مورد توجه قرا رگرفته] - [کل الزامات امنیتی استاندارد]))/ [تعداد توافقنامه‌های شخص ثالث] ۲- مقایسه با شاخص پیشین ۱
صفت معیار تصمیم	
معیار تصمیم	۱- شاخص ۱ باید بیش از ۰/۹ باشد ۲- شاخص ۲ باشد ثابت یا صعودی باشد.
نتیجه‌ها سنجش	
تفسیر شاخص	این شاخص باید بینشی را درمورد توانایی عملکرد بکارگیری شرکت دیگر برای جهت تامین خدمات جهت توجه الزامات امنیتی فراهم آورد.
قالب‌های گزارش دهی	نمودار خطی که‌یک روند در چندین دوره گزارش دهی را نشان می‌دهد. خلاصه کوتاهی از یافته‌های و اقدامات مدیریتی.
سهام‌داران	
مشتری سنجش	مدیران مسئول ISMS. مدیر امنیت
بررسی کننده سنجش	مدیر امنیت
صاحب اطلاعات	دفتر قرارداد
جمع آورنده اطلاعات	کارمند امنیتی
بیانگر اطلاعات	کارمند امنیتی
تناوب/دوره	
تناوب مجموعه داده	ماهانه
تناوب تحلیل داده	سه ماهه

تناوب گزارش دهی نتیجه‌ها سنجش	سه ماهه
بازبینی سنجش	۲ سال
دوره سنجش	قابل اجرا در ۲ سال

فصل ششم

فناوری اطلاعات - فنون امنیتی- مدیریت مخاطرات امنیت اطلاعات

ISO/IEC 27005

Information technology-- Security techniques
Information security risk management

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.

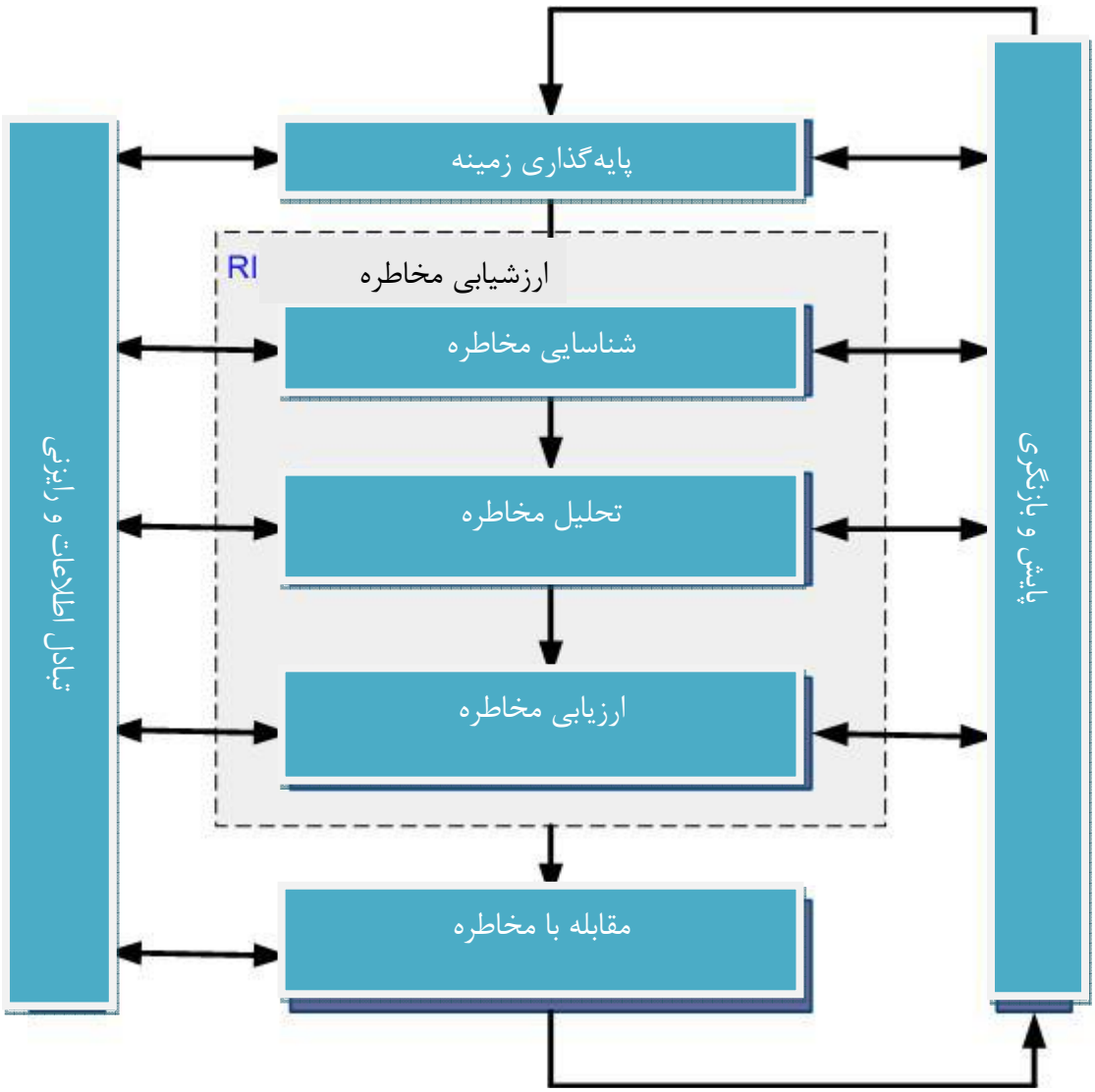
۶ مروری کلی بر فرآیند مدیریت مخاطرات امنیت اطلاعات

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

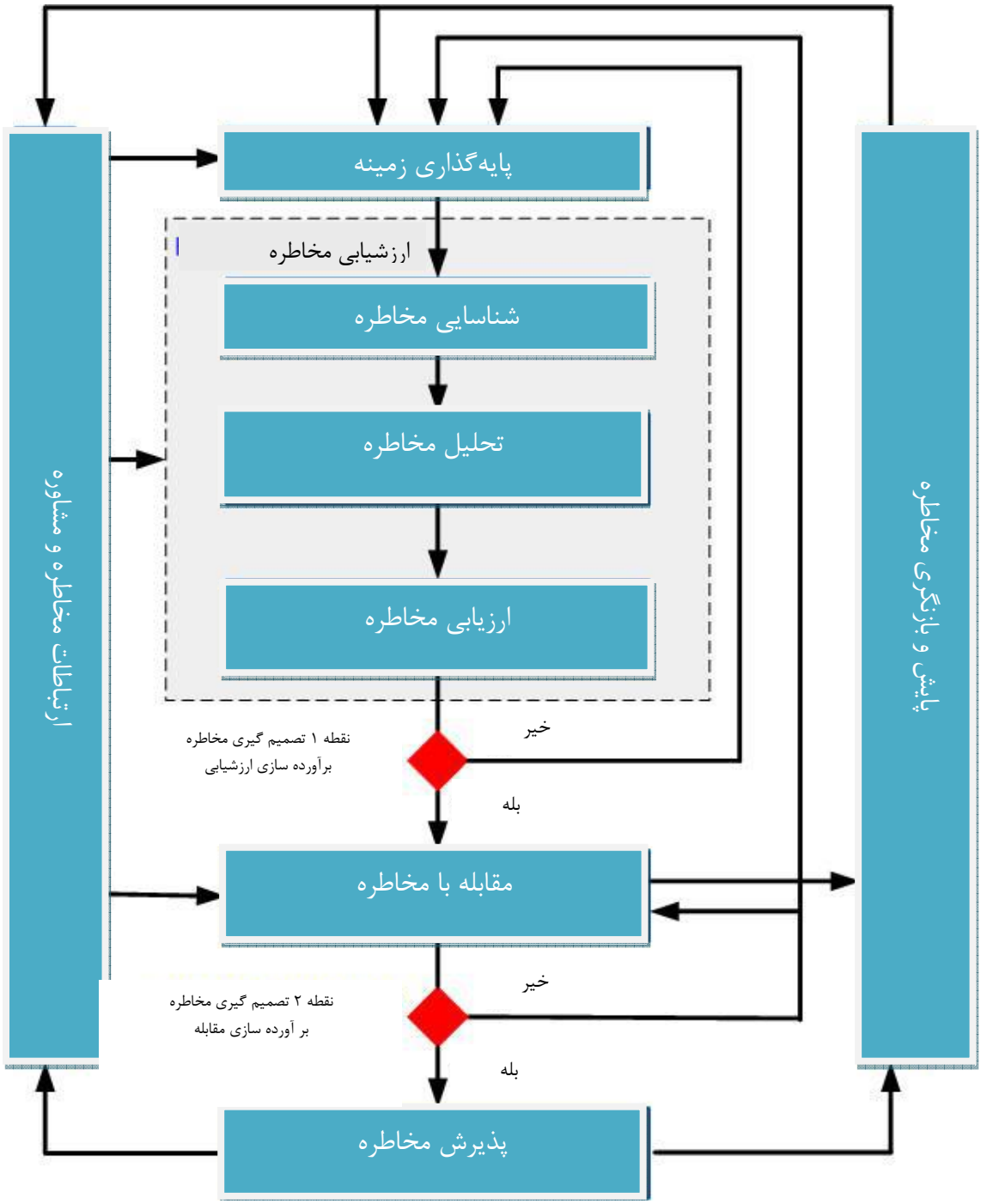
شکل ۲ نشان می‌دهد که چگونه در این استاندارد ملی فرآیند مدیریت مخاطرات اعمال می‌شود.

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.

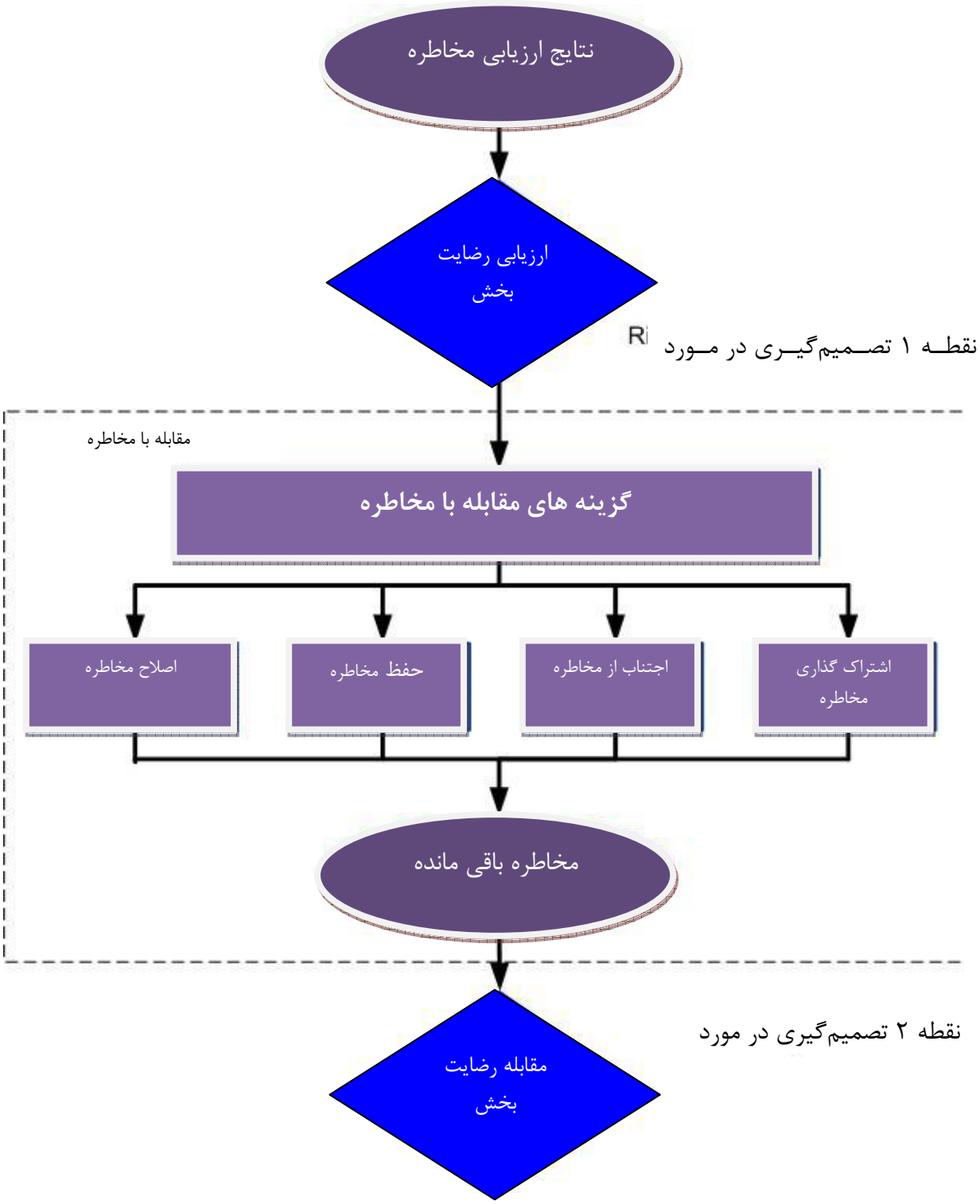
اقدام: کنترل‌هایی برای کاهش، حفظ، اجتناب نمودن یا انتقال(اشتراک) مخاطره باید انتخاب شده و طرح مقابله با مخاطره تعریف شود.

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 به طور کاملًاموثر 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

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

محدودیت‌های حاصل از فرآیندهای موجود از قبل

پروژه های کاربردی لزومًابه‌صورت همزمان توسعه نمی‌یابند. بعضی به فرآیندهای موجود از قبل بستگی دارند. با اینکه یک فرایند می‌تواند به چندین فرآیند فرعی تقسیم شود، اما فرآیند لزومًاتحت 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 کاملاًتجاری‌سازی 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 به صورت عمومی، حوزه کّلی‌تری 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 داده ای 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. **یادآوری ۳**- 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 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
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 مخـاطره پوشـش 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» جـایگزین شـده 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*

فصل هفتم

فناوری اطلاعات - فنون امنیتی- الزامات نهادهای ممیزی کننده و گواهی کننده سیستم های مدیریت امنیت اطلاعات

ISO/IEC 27006

Information technology-- Security techniques Requirements for bodies providing audit certification of Information security management

پیش گفتار

استاندارد " فن‌آوری اطلاعات - فنون امنیتی- الزامات نهادهای ممیزی‌کننده و گواهی‌کننده سیستم‌های مدیریت امنیت اطلاعات " که پیش نویس آن درکمیسیون های مربوط توسط مؤسسهٔ استاندارد و تحقیقات صنعتی ایران تهیه و تدوین شده و در پنجاه و چهارمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۸۷/۸/۱۲ مورد تصویب قرارگرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینهٔ صنایع، علوم و خـدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفـت. بنـابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

این استاندارد ملی برمبنای استاندارد بین المللی زیر تدوین شده و معادل آن به زبان فارسی است:

1- ISO/IEC 27006:2007, 1st Ed.: Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

۲ - کلیه واژگان مصوب فرهنگستان علوم, سایت اینترنتی فرهنگستان زبان و ادبیات پارسی
http://www.persianacademy.ir/

مقدمه

استاندارد ISO/IEC 17021 یک استاندارد بین‌المللی است، که معیارهایی را برای نهادهای ممیزی‌کننده[1] و گواهی‌کننده[2] در زمینه سیستم‌های مدیریت سازمان‌ها[3] تعیین می‌کند. برای آنکه چنین نهادهایی جهت ممیزی[4] و ارائه گواهی سیستم‌های مدیریت امنیت اطلاعات بر اساس استاندارد ملی ایران ایزو-آی ای سی به شماره ۲۷۰۰۱ و مطابق با استاندارد ISO/IEC 17021 تایید صلاحیت شوند، الزامات و راهنمایی تکمیلی علاوه‌بر الزامات ISO/IEC 17021 لازم است. این الزامات در این استاندارد ارائه می‌شوند.

این استاندارد معادل استاندارد بین‌المللی ISO/IEC 27006:2007 می‌باشد، و ساختار، بندها، ارجاعات، مفاهیم و شماره این استاندارد ملی هماهنگ با استاندارد بین‌المللی معادل می‌باشد. این استاندارد ملیِ معادل به صورت زیر شناخته می شود:

استاندارد ملی ایران ایزو-آی ای سی به شماره ۲۷۰۰۶: سال ۱۳۸۷.

متن این استاندارد مطابق با ساختار ISO/IEC 17021 بوده و تنها در مواردی که الزامات و راهنمایی تکمیلی مختص ISMS[5] برای بکارگیری ISO/IEC 17021 جهت صدورگواهی ISMS مطرح است، از حروف "IS" استفاده می‌شود.

به منظور روانی و شیوایی متن، سعی شده است در صورت امکان بجای عبارت "استاندارد ملی ایران ایزو-آی ای سی به شماره ۲۷۰۰۱" از عبارت "استاندارد ۲۷۰۰۱" استفاده شود.

اصطلاح «باید» در این استاندارد نشانگر ضوابط[6] اجباری دو استاندارد ISO/IEC 17021 و استاندارد ۲۷۰۰۱ ۲۷۰۰۱ است. اصطلاح «توصیه می‌شود» برای نشان دادن ضوابطی بکاربرده می‌شود که - اگرچه آنها راهنمایی برای کاربرد الزامات تعبیر می‌شوند،- انتظار می‌رود مورد قبول یک نهاد گواهی‌کننده[7] واقع شوند.

یکی از اهداف این استاندارد، قادر ساختن نهادهای تاییدصلاحیت[8] به همسان‌سازی اثربخش‌تر در بکارگیری استانداردهایشان جهت ارزیابی[9] نهادهای گواهی‌کننده است. در این زمینه هرگونه انحراف از راهنمایی[10] از سوی نهاد گواهی‌کننده به عنوان استثناء تلقی می‌شود. چنین انحرافاتی به‌صورت موردی و تنها در صورتی مجاز هستند، که نهاد گواهی‌کننده به نهاد تاییدصلاحیت اثبات کند که این استثناء به‌روشی تقریبا معادل الزامات مربوط به بندی از استاندارد ISO/IEC 17021 و استاندارد ۲۷۰۰۱ و در نتیجه هدف این استاندارد را برآورده می‌سازد.

یادآوری: در سرتاسر این استاندارد، اصطلاح«سیستم مدیریت» و « سیستم» به جای هم استفاده می‌شوند.

1- Body operating audit
2- Body operating certification
3- Organizations
4- Audit
6- Information Security Management Systems
7- Provisions
8- Certification body
9- Accreditation body
10- Assessment
11- Guidance

تعریف اصطلاح « سیستم مدیریت» در استاندارد ISO 9000:2005 موجود است. سیستم مدیریتی که در این استاندارد استفاده می‌شود نباید با انواع دیگر سیستم‌ها از جمله سیستم‌های فن‌آوری اطلاعات اشتباه گرفته شود.

در استانداردهای موضوع "سیستم‌های مدیریت امنیت اطلاعات"، توصیه می شود که در دو مبحث "سیستم مدیریت" و "فن‌آوری اطلاعات"، الزامات و موضوعات مرتبط با هر کدام بـه دقـت مـورد توجـه قـرار گیـرد.

فن‌آوری اطلاعات- فنون امنیتی[1]- الزامات نهادهای ممیزی‌کننده و گواهی‌کننده سیستم‌های مدیریت امنیت اطلاعات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد مشخص کردن الزامات و فراهم آوردن راهنمایی برای نهادهایی است که خدمات ممیزی و یا صدورگواهی سیستم مدیریت امنیت اطلاعات[2] (ISMS) را تامین می‌کنند. این الزامات افزون بر الزاماتی هستند که در استانداردهای ISO/IEC 17021 و استاندارد ۲۷۰۰۱ ارائه می‌شوند. هدف اصلی این استاندارد پشتیبانی از تاییدصلاحیتِ نهادهایِ گواهی‌کننده‌ای است که گواهی ISMS را تامین می‌کنند.

الزاماتی که در این استاندارد وجود دارند، به عنوان شاخصی برای اثبات شایستگی[3] و قابلیت اعتماد[4] هر نهاد نهاد تامین‌کننده گواهیISMS شناخته می‌شوند و راهنمایی که در این استاندارد وجود دارد، تعابیر تکمیلی از این الزامات برای هر نهاد گواهی‌کنندهISMS می‌باشد.

یادآوری: این استاندارد می‌تواند به عنوان مدرک معیار[5] جهت تاییدصلاحیت، ارزیابی همترازی[6] و یا سایر فرآیندهای ممیزی[7] ممیزی[7] مورد استفاده قرار گیرد.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی هستند که در متن این استاندارد به آنها ارجاع شده است، و به‌این ترتیب جزئی از این استاندارد محسوب می‌شوند.

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

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران ایزو- آی ای سی به شماره ۲۷۰۰۱ : سال ۱۳۸۷، فن‌آوری اطلاعات- فنون امنیتی- سیستم‌های مدیریت امنیت اطلاعات - الزامات

2-2 ISO/IEC 17021:2006, Conformity assessment - Requirements for bodies providing audit and certification of management systems.

2-3 ISO/IEC 19011, Guidelines for quality and/or environmental management systems auditing.

1- Security techniques
2- Information security management system
3- Competence
4- Reliability
5- Criteria document
6- Peer Assessment (PA)
7- Audit processes

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف ارائه شده در استانداردهای ISO/IEC 17021 و استاندارد ۲۷۰۰۱، اصطلاحات و تعاریف زیر نیز به کار می‌روند.

۳-۱

گواهینامه[1]

گواهینامه بوسیله یک نهاد گواهی‌کننده، مطابق با شرایط تاییدصلاحیت آن نهاد، صادر شده و حاوی یک نماد[2] یا بیانیه[3] تایید صلاحیت از سوی آن نهاد است.

۳-۲

نهاد گواهی‌کننده

شخص‌سومی[4] که ISMS یک سازمان مشتری را، براساس استانداردهای منتشر شده ISMS و سایر مستندات مستندات تکمیلی الزام شده سیستم، ارزیابی و گواهی می‌کند.

۳-۳

مدرک صدور گواهی[5]

مدرکی که نشان می‌دهد ISMS یک سازمان مشتری، با استانداردهای ISMS و مستندات تکمیلی الزام شده در این سیستم مطابقت دارد.

۳-۴

علامت[6]

علامت ثبت شده قانونی و یا هر نماد محافظت‌شده به‌روش‌دیگر که برطبق قوانین نهاد تاییدصلاحیت یا نهاد گواهی‌کننده صادر شده و اثبات‌کننده احراز اطمینان کافی از سیستم‌های اجرا شده توسط یک نهاد بوده و یا اینکه اجزاء[7] و یا محصولات[8] با الزامات یک استاندارد خاص مطابقت دارند.

1- Certificate
2- Symbol
3- Statement
4- Third party
5- Certification document
6- Mark
7- Individuals
8- Products

۵-۳

سازمان

شرکت، شرکت سهامی، دفتر، بنگاه تجاری، موسسه یا مرجع دارای اختیار[1]، یا قسمت یا تلفیقی[2] از قسمتهای متعلق به آن، به صورت ثبت شده و یا ثبت نشده، خصوصی و یا دولتی که دارای ساختار اداری و عملکرد مستقلی بوده و توانایی احراز نهادینه‌سازی امنیت اطلاعات را در سازمان خود دارد.

۴ اصول

اصول بند ۴ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۵ الزامات عمومی

۵-۱ موارد قانونی و قراردادی

الزامات بند ۵-۱ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۵-۲ مدیریت بی‌طرفی

الزامات بند ۵-۲ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۵-۲-۱ موارد تضاد منافع در IS 5.2

نهادهای گواهی‌کننده می‌توانند فعالیت‌های زیر را انجام دهند؛ بدون آنکه به عنوان مشاور شناخته شوند و یا موردی متضاد با منافع داشته باشند.

الف- صدورگواهی، شامل جلسات توجیهی[3]، جلسات طرح‌ریزی[4]، بررسی مدارک[5]، ممیزی(البته نه ممیزی داخلی ISMS یا بازنگری‌های امنیتی داخلی) جهت یافتن و پیگیری عدم‌انطباقات.

ب- برگزاری و شرکت در دوره‌های آموزشی مرتبط با مدیریت امنیت اطلاعات، سیستم‌های مدیریتی و یا ممیزی به عنوان مدرس[6]؛ توصیه می‌شود، نهادهای گواهی‌کننده خود را محدود به تهیه اطلاعات عام و توصیه‌هایی نمایند که آزادانه قابل دسترس عموم هستند. به‌عبارت‌دیگر توصیه نمی‌شود، آنها مختص یک شرکت توصیه‌ای[7] ارائه دهند، که این موضوع تخطی از الزامات بند پ تلقی شود.

پ- در اختیار گذاشتن یا انتشار اطلاعات درخواستی که در برگیرنده تعبیر و تفسیر نهاد گواهی‌کننده از الزامات استانداردهای ممیزی‌صدورگواهی[8] باشد.

1- Authority
2- Combination
3- Information meetings
4- Planning meetings
5- Examination of documents
6- Lecturer
7- Advice
8- Certification audit

ت- فعالیت‌های پیش از ممیزی، تنها با هدف سنجش آمادگی برای ممیزی‌صدورگواهی. با این وجود توصیه می‌شود، چنین فعالیت‌هایی منجر به تهیه پیشنهادات یا توصیه‌هایی نشوند که این بند را نقض می‌کند و توصیه‌می‌شود، نهاد گواهی‌کننده بتواند این مطلب را تایید کند که چنین فعالیت‌هایی نقض این الزامات نبوده و به عنوان توجیهی جهت چشم‌پوشی از رخدادهای حین ممیزی‌صدورگواهی بکار نرفته است.

ث- اجرای ممیزی شخص‌دوم و شخص‌سوم مطابق با استانداردها یا مقررات؛ به‌غیر از آنهایی که قسمتی از دامنه‌شمول تاییدصلاحیت هستند.

ج- ایجاد ارزش افزوده در کار در حین ممیزی‌صدورگواهی و بازدیدهای نظارتی[1]، برای‌مثال با شناسایی فرصت‌های بهبود، در زمانی‌که در حین ممیزی، جزء شواهد ممیزی می‌شوند، بدون پیشنهاد راه‌حل مشخص.

نهاد گواهی‌کننده باید از نهاد یا نهادهایی(شامل افراد نیز می‌شود) که فعالیت ممیزی داخلیِ ISMS سازمان مشتری -که موضوع گواهی است- را بر عهده دارند، مستقل باشد.

۵-۳ تعهدات مالی و پرداختها

الزامات بند ۵-۳ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۶ الزامات ساختاری

۶-۱ ساختار سازمانی و مدیریت رده بالا

الزامات بند ۶-۱ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۶-۲ کمیته ای برای رعایت طرفی

الزامات بند ۶-۲ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۷ الزامات منابع

۷-۱ شایستگی مدیران و کارکنان

الزامات بند ۷-۱ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

1- Surveillance visits

واژه "Surveillance" در معانی بازبینی، نظارتی و مراقبتی مورد استفاده قرار می‌گیرد.

۷-۱-۱ شایستگی مدیریت در IS 7.1

مولفه‌های اصلی شایستگی که برای صدورگواهی ISMS الزامی هستند، عبارتند از: انتخاب، تامین و مدیریت نیروهایی که مهارت‌ها و شایستگی آنها متناسب با فعالیت‌های مورد ممیزی و نیز سایر موارد مرتبط با امنیت اطلاعات می‌باشد.

۷-۱-۱-۱ تحلیل شایستگی و بازنگری قرارداد

نهاد گواهی‌کننده باید اطمینان حاصل‌نماید که دانش بهبود[1] در حوزه فن‌آوری و قانونی مرتبطبه ISMS سازمان‌مشتری، که مورد ارزیابی قرار می‌دهد، را دارا است.

نهاد گواهی‌کننده باید از سیستمی اثربخش[2] جهت تحلیل شایستگی‌هایی که در مدیریت امنیت اطلاعات به آنها نیاز دارد و در تمامی زمینه های فنی که در آنها فعالیت دارد، برخوردار باشد.

به ازای هر مشتری، نهاد گواهی‌کننده باید بتواند اثبات کند که تحلیلی از شایستگی‌ها (ارزیابی[3] مهارت‌ها در پاسخ به نیازهای ارزشیابی شده) در زمینه تمامی الزامات مرتبط با هر بخش، پیش از بازنگری قرارداد را انجام داده‌است. نهاد گواهی‌کننده سپس باید قرارداد را با سازمان مشتری خود، براساس نتایج این تحلیل شایستگی، بازنگری نماید. به‌صورت مشخص، نهاد گواهی‌کننده باید بتواند ثابت نماید، شایستگی انجام فعالیت‌های زیر را دارد:

الف- درک حوزه‌های فعالیت سازمان مشتری و ریسک‌های مرتبط با کسب‌وکار[4] آن.

ب- تعریف شایستگی‌های مورد نیاز در نهاد گواهی‌کننده، برای گواهی‌کردن[5] فعالیت‌های شناسایی‌شده و امنیت اطلاعات مرتبط با تهدیدات دارایی‌ها، آسیب‌پذیری‌ها و پیامدهای آن بر روی سازمان مشتری.

پ- تایید در دسترس بودن شایستگی‌های مورد نیاز.

۷-۱-۱-۲ منابع

مدیریت نهاد گواهی‌کننده باید منابع و فرآیندهای لازم برای تعیین شایسته بودن تک‌تک ممیزان در مورد فعالیت‌هایی که نیازاست در دامنه‌شمول گواهی انجام‌شود را داشته‌باشد. شایستگی ممیزان، ممکن است از طریق سابقه کاری تصدیق‌شده[6] و آموزش خاص یا جلسات توجیهی (به پیوست ب رجوع شود) اثبات شود. نهاد گواهی‌کننده باید بتواند به طور اثربخش با مشتری‌هایی که به آنها خدمت ارائه می‌کند ارتباط برقرار نماید.

1- Development
2- Effective
3- Assessment
4- Business
5- Certify
6- Verified

۷-۲ کارکنانی که در فعالیت‌های صدورگواهی دخیل هستند

الزامات بند ۷-۲ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۷-۲-۱ شایستگی کارکنان نهاد گواهی‌کننده در IS 7.2

نهادهای گواهی‌کننده باید کارکنانی را در اختیار داشته باشند، که شایستگی انجام فعالیت‌های زیر را داشته باشند:

الف- انتخاب و تصدیق[1] شایستگی ممیزان ISMS برای تیم‌های ممیزی و مناسب بودن آنها برای انجام فعالیت ممیزی.

ب- توجیه ممیزان ISMS و تدارک آموزشهای لازم برای آنها.

پ- تصمیم‌گیری در مورد اعطا[2]، حفظ‌ونگهداری[3]، ابطال[4]، تعلیق[5]، افزایش یا کاهش مدت اعتبار گواهی‌ها

ت- تنظیم و اجرای فرآیند درخواست‌های رسیدگی‌مجدد[6] و شکایات.

۷-۲-۱-۱ آموزش تیم‌های ممیزی

نهاد گواهی‌کننده باید معیارهایی را برای آموزش تیم‌های ممیزی داشته باشد، تا به این روش بتواند از موارد زیر اطمینان حاصل نماید:

الف- دانش استاندارد ISMS و سایر مدارک الزامی مرتبط.

ب- درک صحیح از امنیت اطلاعات.

پ- درک صحیح از ارزیابی‌ریسک و مدیریت ریسک از دیدگاه کسب‌وکار.

ت- دانش فنی از فعالیت مورد ممیزی.

ث- دانش کلی از الزاماتِ مقرراتیِ مرتبط با ISMS .

ج- دانش سیستم‌های مدیریتی.

چ- درک صحیح از اصول ممیزی براساس استاندارد ISO 19011 .

ح- دانش بازنگری اثربخشی[7] ISMS و اندازه‌گیری میزان اثربخشی کنترل.

این الزامات آموزشی تمامی اعضای تیم ممیزی را شامل می‌شود، به‌غیر از بند «ت»، که می‌تواند بین اعضای تیم تقسیم شود.

1- Verify
2- Granting
3- Maintaining
4- Withdrawing
5- Suspending
6- Appeals
7- Effectiveness

۷-۲-۱-۱-۱ در زمان انتخاب تیم ممیزی به‌منظور انجام ممیزی‌صدورگواهی خاص، نهاد گواهی‌کننده باید اطمینان حاصل نماید که مهارت‌های لازم برای هر کار به درستی بکار گرفته شده‌اند. تیم باید:

الف- دانش فنی مناسب از فعالیت‌های خاص در دامنه‌شمول ISMSای که صدورگواهی برای آن انجام می‌شود، داشته باشد. این دانش، در موارد مرتبط، روش‌های اجرایی[1] مرتبط و ریسک‌های امنیت اطلاعات بالقوه آنها را شامل می‌شود (کارشناسان فنی[2] که ممیز نیستند، می‌توانند این کار را انجام دهند).

ب- درک مناسبی از سازمان مشتری داشته باشد، تا یک ممیزی قابل اعتماد برای صدورگواهی ISMS در زمینه مدیریت کردن[3] امنیت اطلاعات برای فعالیت‌ها، محصولات و خدمات را انجام دهد.

پ- درک مناسبی از الزامات قانونی که در مورد ISMS سازمان مشتری کاربرد پیدا می‌کند، داشته باشد.

۷-۲-۱-۱-۲ در موارد لازم تیم ممیزی می‌تواند، با استفاده از کارشناسان فنی، که شایستگی آنها در زمینه فن‌آوری مورد ممیزی قابل اثبات است، تکمیل شود. این نکته باید در نظر گرفته شود که نمی‌توان از کارشناسان فنی بجای ممیزان ISMS استفاده کرد. بلکه آنها فقط می‌توانند به ممیزان در زمینه‌های فنی درخصوص سیستم مدیریتِ مورد ممیزی، مشاوره ارائه کنند. نهاد گواهی‌کننده باید روش اجرایی برای موارد زیر داشته باشد:

الف- انتخاب ممیزان و کارشناسان فنی براساس شایستگی، آموزش، اثبات شرایط[4] و تجربه‌شان.

ب- ارزیابی اولیه رفتارِ ممیزان[5] و کارشناسان فنی در یک ممیزی‌صدورگواهی و متعاقب آن پایش عملکرد[6] ممیزان و کارشناسان فنی.

۷-۲-۱-۲ مدیریت فرآیند تصمیم‌گیری

حوزه[7] مدیریت باید از شایستگی و قابلیتهای فنی برای مدیریت فرآیند تصمیم‌گیری، در مورد اعطا، حفظ‌ونگهداری، افزایش مدت اعتبار، کاهش مدت اعتبار، تعلیق و ابطال گواهی ISMS براساس الزامات استاندارد ۲۷۰۰۱، برخوردار باشد.

۷-۲-۱-۳ پیش‌نیازهای تحصیلی، تجربیات کاری، آموزش ممیزی و تجربه ممیزی برای ممیزانی که یک ممیزی ISMS را انجام می‌دهند.

۷-۲-۱-۳-۱معیارهای زیر باید برای هر ممیز تیم ممیزی ISMS لحاظ شود. یک ممیز باید:

الف- تحصیلات دوره متوسطه را گذرانده باشد.

1- Procedures
2- Technical experts
3- Managing
4- Qualification
5- Conduct of auditors
6- Performance
7- Function

ب- دارای حداقل ۴ سال تجربه کاری تمام‌وقت در حوزه فن‌آوری اطلاعات بوده که حداقل دو سال آن مرتبط با امنیت اطلاعات است.

پ- ۵ روز دوره آموزشی را با موفقیت گذرانده باشد که دامنه‌شمول دوره آموزشی باید ممیزی ISMS و مدیریت ممیزی را به‌نحو مناسبی دربرگیرد.

ت- پیش از آنکه مسوولیت‌های ممیزی به وی محول شود، باید در کلیه فرآیندهای ارزیابی امنیت اطلاعات تجربه کسب کرده باشد. توصیه می‌شود این تجربه از طریق شرکت در حداقل چهار ممیزی‌صدورگواهی که دست‌کم ۲۰ روز بوده و شامل بازنگری مدارک، تحلیل ریسک، ارزیابی پیاده‌سازی و گزارش‌دهی ممیزی است، به دست آمده باشد.

ث- تجربیات وی تا حد امکان جدید باشد.

ج- توانایی تصویرسازی کلی از عملیات[1] پیچیده و درک نقش‌ها واحدهای مستقل موجود در سازمان‌های بزرگ‌تر مشتری را داشته باشد.

چ- دانش و توانمندی‌های خود را در زمینه امنیت اطلاعات و ممیزی، از طریق بهبود حرفه‌ای مداوم[2]، روزآمد نماید.

کارشناسان فنی باید مطابق با معیارهای «الف»، «ب»، «ث»، و «ج» انتخاب شوند.

۷-۲-۱-۳-۲ علاوه بر الزامات بند ۷-۲-۱-۳-۱، راهبران تیم‌های ممیزی باید شرایط زیر را برآورده کنند. برآورده شدن این شرایط باید در ممیزی‌ها و مطابق با راهنمایی و تحت نظارت اثبات شود:

الف- دارا بودن دانش و خصوصیات برای مدیریت فرآیند ممیزی‌صدورگواهی.

ب- ممیز بودن در حداقل سه ممیزی کامل ISMS .

پ- اثبات کردن توانمندی[3] برای برقراری ارتباط بصورت اثربخش، به هر دو صورت کتبی و شفاهی.

۷-۳ استفاده از ممیزان بیرونی[4] مستقل و کارشناسان فنی بیرونی

الزامات بند ۷-۳ از استاندارد ۲۷۰۰۱ بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۷-۳-۱ استفاده از ممیزان بیرونی یا کارشناسان فنی بیرونی به‌عنوان قسمتی از تیم ممیزی در IS 7.3

در زمان استفاده از ممیزان بیرونی مستقل یا کارشناسان فنی بیرونی به عنوان قسمتی از تیم ممیزی، نهاد گواهی‌کننده باید اطمینان حاصل نماید که این افراد از شایستگی لازم برخوردار بوده و با ضوابط کاربردی در این استاندارد مطابقت دارند. همچنین به طور مستقیم و یا از طریق کارفرمایشان با طراحی، پیاده‌سازی و یا

1- Operation
2- Continual
3- Capability
4- External

نگهداری از ISMS یا سیستم مدیریت مرتبط با آن به‌گونه‌ای که بی‌طرف بودن ایشان نقض شود، ارتباطی نداشته باشند.

۷-۳-۱-۱ استفاده از کارشناسان فنی

کارشناسان فنی که در زمینه فرآیند و موارد مربوط به امنیت اطلاعات و قوانین تاثیرگذار بر سازمان مشتری از دانشی خاص برخوردارند، ولی همه معیارهای بند ۷-۲ را برآورده نمی‌کنند، می‌توانند قسمتی از تیم ممیزی باشند. کارشناسان فنی باید تحت نظارت یک ممیز فعالیت نمایند.

۷-۴ سوابق[1] کارکنان

الزامات بند ۷-۴ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۷-۵ برون‌سپاری

الزامات بند ۷-۵ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۸ الزامات اطلاعات

۸-۱ اطلاعات در دسترس عموم

الزامات بند ۸-۱ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۸-۱-۱ روش‌های اجرایی برای اعطا، حفظ‌ونگهداری، افزایش مدت اعتبار، کاهش مدت اعتبار، تعلیق و ابطال گواهی ISMS در IS 8.1

نهاد گواهی‌کننده باید سازمان مشتری را ملزم کند تا شواهدی دال بر یک ISMS مستند و پیاده‌سازی‌شده را، مطابق با استاندارد ۲۷۰۰۱ به همراه سایر مدارک لازم برای صدورگواهی، در اختیار وی قرار دهد.
نهاد گواهی‌کننده باید برای موارد زیر روش‌های اجرایی مدونی داشته باشد:
الف- ممیزی‌صدورگواهی اولیه ازISMS سازمان‌مشتری مطابق‌با ضوابط استانداردهای ISO 19011, ISO/IEC 17021 و سایر مدارک مرتبط.
ب- ممیزی‌های بازبینی و ممیزی‌های صدورگواهی‌مجدد ISMS سازمان‌مشتری مطابق با استانداردهای ISO 19011, ISO/IEC 17021 در بازه‌های زمانی مشخص، جهت تداوم انطباق با الزامات مرتبط و همچنین تصدیق و ثبت اینکه سازمان‌مشتری، برمبنای زمان، اقدام‌اصلاحی[2] را درجهت اصلاح تمامی عدم‌انطباق‌هایش انجام می‌دهد.

1- Records
2- Corrective action

۸-۲ مدارک صدور گواهی

الزامات بند ۸-۲ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۸-۲-۱ مدارک صدور گواهی ISMS در IS 8.2

نهاد گواهی‌کننده باید به هر سازمان مشتری خود، که ISMS آن گواهی شده است؛ مدارک صدور گواهی مانند یک نامه و یا یک گواهینامه امضاشده از سوی فردی که چنین مسوولیتی دارد، را ارائه نماید. برای هر سازمان مشتری و هر یک از سیستم‌های اطلاعاتی آن، که بوسیله گواهی پوشش داده می‌شود، این مدارک باید دامنه‌شمول گواهی اعطا شده و استانداردِ "سیستم‌های مدیریت امنیت اطلاعات" -استاندارد ۲۷۰۰۱- که ISMS بر اساس آن گواهی می‌شود را مشخص نماید. به‌علاوه توصیه می‌شود، در گواهینامه به نسخه خاصی از بیانیه کاربردپذیری[1] ارجاع داده شده باشد.

۸-۳ لیست مشتری‌های دارای گواهی

الزامات بند ۸-۳ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۸-۴ ارجاع به گواهی و استفاده از علامت

الزامات بند ۸-۴ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۸-۴-۱ کنترل علامت‌های گواهی در IS 8.4

نهاد گواهی‌کننده باید کنترل‌های مناسبی را بر مالکیت، استفاده و نمایش علامت‌های گواهی ISMS خود اعمال نماید. اگر نهاد گواهی‌کننده مجوز استفاده از علامت را جهت ثبت در گواهی ISMS صادر کرده است؛ توصیه می‌شود، نهاد گواهی‌کننده اطمینان حاصل نماید، سازمان مشتری آن علامت خاص را تنها در مواردی که از سوی نهاد گواهی‌کننده مشخص شده است استفاده کند. نهاد گواهی‌کننده نباید این حق را به سازمان مشتری بدهد که این علامت را روی یک محصول استفاده کند یا به‌گونه‌ای استفاده کند که امکان داشته باشد به‌عنوان دلیل انطباق محصول تفسیر شود.

۸-۵ محرمانگی

الزامات بند ۸-۵ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

1- Statement of applicability

۸-۵-۱ دسترسی به سوابق سازمانی در IS 8.5

پیش از ممیزی‌صدورگواهی، نهاد گواهی‌کننده باید از سازمان مشتری پرسش نماید که آیا سوابقی از ISMS در سازمان وجود دارد، که به‌دلیل حاوی اطلاعات محرمانه یا حساس بودن نمی‌تواند برای بازنگری در اختیار تیم ممیزی قرار گیرد. نهاد گواهی‌کننده باید تعیین نماید، آیا ممیزی ISMS بدون وجود این سوابق، به‌نحومناسب امکان‌پذیر است یا خیر. اگر نهاد گواهی‌کننده به این نتیجه برسد، که امکان ممیزی، به‌نحومناسب، بدون بازنگری سوابق محرمانه یا حساس وجود ندارد، سازمان مشتری باید توجیه شود که ممیزی‌صدورگواهی نمی‌تواند انجام شود؛ تازمانی‌که تمهیدات دسترسی کافی برای نهاد گواهی‌کننده فراهم شود.

۸-۶ تبادل اطلاعات بین نهاد گواهی‌کننده و مشتریانش

الزامات بند ۸-۶ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۹ الزامات فرآیندی

۹-۱ الزامات عمومی

الزامات بند ۹-۱ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۹-۱-۱ الزامات عمومی ممیزی ISMS در IS 9.1

۹-۱-۱-۱ معیارهای ممیزی صدورگواهی

معیارهایی که ISMS یک مشتری بر اساس آن مورد ممیزی قرار می‌گیرد، باید از استاندارد ۲۷۰۰۱ و سایر مدارک مورد نیاز برای صدورگواهی مرتبط با عملکرد آن سازمان، استخراج شده باشد.

اگر نیاز به توضیح درباره کاربرد این مدارک، برای یک برنامه صدورگواهی خاص وجود داشت، چنین توضیحی باید بوسیله افراد یا کمیته‌ای مرتبط و بی‌طرف که از شایستگی فنی لازم برخوردار است، داده شود و از طریق نهاد گواهی‌کننده منتشر شود.

۹-۱-۱-۲ خط‌مشی ها و روش‌های اجرایی

مستندسازی نهاد گواهی‌کننده باید شامل خط‌مشی و روش‌های‌اجرایی برای پیاده‌سازی فرآیند صدورگواهی باشد که شامل بررسی‌های استفاده و کاربرد مدارک بکاررفته در گواهیISMSها و روش‌های اجرایی برای ممیزی و صدورگواهی ISMS در سازمان مشتری می‌شود.

۹-۱-۱-۳ تیم ممیزی

تیم ممیزی باید به طور رسمی منصوب شده و مدارک کاری لازم در اختیار آن قرار گیرد. برنامه و تاریخ ممیزی باید با توافق سازمان مشتری تعیین شود. دستورات ابلاغ شده به تیم ممیزی باید به طور واضح

تعریف و به اطلاع سازمان مشتری برسد. همچنین باید تیم ممیزی ملزم شود ساختار، خط‌مشی‌ها و روش‌های اجرایی سازمان مشتری را بررسی کند و تایید نماید که، این موارد کلیه الزامات مربوط به دامنه‌شمول گواهی را برآورده می‌کنند، و روش‌های اجرایی پیاده‌سازی شده‌اند، و به‌گونه‌ای هستند که بتوان از ISMS سازمان مشتری اطمینان حاصل نمود.

۹-۱- ۲ دامنه‌شمول گواهی در IS 9.1.2

تیم ممیزی باید ISMS سازمان مشتری، مشمول دامنه‌شمول، را از جهت تمامی الزاماتِ قابل اجرا برای صدورگواهی، ممیزی کند. نهاد گواهی‌کننده باید اطمینان حاصل نماید، که دامنه‌شمول و تمامی قیود ISMS سازمان مشتری به طور واضح بر مبنای ویژگیهای[1] کسب‌وکار، سازمان، موقعیت، دارایی‌ها و فن‌آوری آن تعریف شده است. نهاد گواهی‌کننده باید تایید نماید، در دامنه‌شمول ISMS سازمان، الزامات ذکر شده در بند ۱-۲ از استاندارد ۲۷۰۰۱ لحاظ شده‌اند.

نهادهای گواهی‌کننده باید اطمینان یابند، ارزیابی‌ریسک و برطرف‌سازی‌ریسک امنیت‌اطلاعات در سازمان‌مشتری به‌نحومناسبی منعکس‌کننده فعالیت‌های آن سازمان می‌باشد و تا حدود فعالیت‌های آن سازمان وسعت پیدا می‌کند، همانطور که در استاندارد ۲۷۰۰۱ تعریف شده است.

نهادهای گواهی‌کننده باید تایید کنند، این مطلب در دامنه‌شمول ISMS انها و بیانیه کاربردپذیری سازمان مشتری منعکس شده است.

نهادهای گواهی‌کننده باید اطمینان یابند، که فصل‌های مشترک[2] با خدمات یا فعالیت‌ها که به‌طور کامل در دامنه‌شمول ISMS قرارنگرفته‌اند، در داخل ISMSِ موضوعِ‌گواهی قرارگرفته، و در ارزیابی‌ریسک امنیت‌اطلاعات سازمان مشتری قرار داده می‌شوند. مثالی از این حالت، به‌اشتراک‌گذاری تجهیزات (برای‌مثال سیستم‌های IT، سیستم‌های پایگاه داده و ارتباطی) با سازمان‌های دیگر است.

۹-۱- ۳ زمان ممیزی در IS 9.1.3

نهادهای گواهی‌کننده باید زمان کافی را برای انجام تمامی تعهدات ممیزی اولیه، ممیزی بازبینی یا ممیزی صدورگواهی‌مجدد در اختیار ممیزان قرار دهند. توصیه می‌شود، زمان تخصیص داده‌شده براساس فاکتورهای زیر تعیین شود:

الف- ابعاد دامنه‌شمول ISMS (برای‌مثال تعداد سیستم‌های اطلاعاتی استفاده شده و تعداد کارکنان)

ب- پیچیدگی ISMS. (برای‌مثال بحرانی‌بودن سیستم‌های اطلاعاتی و موقعیت ریسک ISMS) همچنین به پیوست الف مراجعه شود.

پ- نوع(انواع) کسب‌وکاری که در دامنه‌شمول ISMS ذکر شده است.

1- Characteristic

2- Interfaces

این واژه به معنی "محیط‌های واسط" نیز بیان می‌شود.

ت- وسعت و گوناگونی فن‌آوری به‌کارگرفته‌شده در پیاده‌سازی اجزای مختلف ISMS (مانند کنترل‌های پیاده‌سازی شده، مستندسازی و/ یا کنترل فرآیند، اقدام اصلاحی/ پیشگیرانه[1] و غیره)

ث- تعداد سایت‌ها.

ج- عملکرد اثبات‌شده قبلی ISMS.

چ- وسعت برون‌سپاری و هماهنگی‌های شخص‌سوم استفاده شده در دامنه‌شمول ISMS.

ح- استانداردها و مقرراتی که جهت صدور گواهی کاربرد دارند.

پیوست پ راهنمایی را برای زمان ممیزی ارائه می‌کند. نهاد گواهی‌کننده باید آماده باشد، تا مدت زمانی که برای هر ممیزی اولیه، ممیزی بازبینی یا ممیزی صدورگواهی‌مجدد استفاده می‌شود را، با دلیل‌ومدرک ثابت کند یا توجیه نماید

۹-۱- ۴ سایت‌های چندگانه در IS 9.1.4

۹-۱-۴-۱

تصمیم‌گیری براساس نمونه‌گیری از چند سایت در حوزه گواهی ISMS پیچیده‌تر از تصمیم‌گیری درباره سیستم‌های مدیریت کیفیت است. جایی‌که سازمان مشتری چندین سایت دارد که معیارهای الف تا پ، که در زیر به آنها اشاره می‌شود، را برآورده می‌کنند، نهادهای گواهی‌کننده مجازند از رویکرد مبتنی بر نمونه‌گیری[2] برای ممیزی‌صدورگواهی چند سایتی استفاده نمایند:

الف- تمامی سایت‌ها تحت یک ISMS، که به طور مرکزی مدیریت و ممیزی شده و تحت بازنگری مدیریتی مرکزی قرار دارند، کار می‌کنند.

ب- تمامی سایت‌ها در برنامه ممیزی داخلی ISMS سازمان مشتری قرار دارند.

پ- تمامی سایت‌ها در برنامه بازنگری مدیریتی ISMS سازمان مشتری قرار دارند.

۹-۱-۴-۲

نهاد گواهی‌کننده، که تصمیم دارد از رویکرد مبتنی بر نمونه‌گیری استفاده نماید، باید روش‌های اجرایی مناسب و به‌جا برای اطمینان از موارد زیر داشته باشد:

الف- بازنگری اولیه قرارداد، تفاوت میان سایت‌ها را تا حد امکان به‌گونه‌ای مشخص‌کرده‌باشد که سطح مناسب نمونه‌گیری را بتوان تعیین نمود.

ب- ازسوی نهادگواهی‌کننده،تعدادی از سایت‌های‌معرف بادرنظرگرفتن مواردزیر به‌عنوان‌نمونه تعیین‌می‌شوند:

۱- نتایج ممیزی داخلی دفتر مرکزی[3] و سایت‌ها.

۲- نتایج بازنگری مدیریتی.

3- Preventive action
1- Sample-based approach
2- Head office

۳- تغییرات در ابعاد سایت‌ها.
۴- تغییرات در اهداف کسب‌وکار سایت‌ها.
۵- پیچیدگی ISMS .
۶- پیچیدگی سیستم‌های اطلاعاتی در سایت‌های مختلف.
۷- تغییرات در رویه‌های کاری.
۸- تغییرات در تعهدات کاری.
۹- تعاملات بالقوه با سیستم‌های اطلاعاتی حیاتی و یا سیستم‌های اطلاعاتی که اطلاعات حساس را پردازش می‌کنند.
۱۰- هر تفاوتی در الزامات قانونی.

پ- سایت نمونه معرف از میان تمامی سایت‌های موجود در دامنه‌شمول ISMS سازمان‌مشتری انتخاب می‌شود. توصیه می‌شود، این انتخاب به‌گونه‌ای حساب شده انجام شود تا در عین دربرداشتن عوامل ذکر شده در ماده ب این بند، مولفه تصادفی بودن را نیز تامین نمایند.

ت- هر سایت که در ISMS قرار دارد و از ریسک‌های مهمی برخوردار است، پیش از صدورگواهی توسط نهاد گواهی‌کننده ممیزی می‌شود.

ث- برنامه بازبینی با توجه به الزامات بالا انجام شده و تمامی سایت‌ها و یا آنهایی‌که در دامنه‌شمول گواهی ISMS سازمان مشتری هستند را در مدت زمان معقولی پوشش دهد.

ج- زمانی‌که عدم‌انطباقی[1] مشاهده شود، چه در دفتر مرکزی و چه در یک سایت دیگر، روش‌اجرایی اقدام اصلاحی به دفتر مرکزی و تمامی سایت‌های تحت پوشش گواهینامه اعمال می‌شود.

ممیزی که در بخش IS 9.1.5 به آن اشاره می‌شود باید فعالیت‌های دفتر مرکزی سازمان مشتری را مدنظر قرار دهد تا اطمینان حاصل‌نماید که یک ISMS منفرد به تمامی سایت‌ها اعمال شده و مدیریت مرکزی تا سطح عملیاتی[2] تسری پیدا می‌کند. ممیزی باید تمام مواردی که در بالا به آنها اشاره شد، را مدنظر قراردهد.

۹-۱- ۵ روش‌شناسی ممیزی در IS 9.1.5

نهاد گواهی‌کننده باید روش‌های اجرایی داشته باشد، که سازمان مشتری را ملزم نماید تا بتواند اثبات کند که ممیزی‌های داخلی ISMS در آن سازمان دارای برنامه زمان‌بندی بوده، و برنامه‌ها و روش‌های اجرایی عملیاتی هستند و این عملیاتی شدن می‌تواند قابل مشاهده باشد.

توصیه نمی‌شود، روش‌های‌اجرایی نهاد گواهی‌کننده شامل پیش‌فرض‌هایی درباره شیوه‌خاصی از پیاده‌سازی ISMS یا شیوه‌خاصی در مستندسازی و حفظ سوابق باشد. روش‌های‌اجرایی صدورگواهی باید تنها متمرکز بر برآورده‌سازی الزامات استاندارد ۲۷۰۰۱ و خط‌مشی‌ها و اهداف سازمان مشتری در ISMS سازمان باشد.

توصیه می‌شود، طرح ممیزی[3]، روش‌های ممیزی شبکه‌ای[1] را که در حین ممیزی در زمان مناسب استفاده خواهند شد، شناسایی نماید.

1- Nonconformity
2- Operational level
3- Audit plan

یادآوری: روش‌های ممیزی شبکه‌ای می‌تواند شامل تله‌کنفرانس، ملاقات از طریق وب، ارتباط تعاملی مبتنی بر وب و دسترسی الکترونیکی از فاصله دور به مستندات ISMS و فرآیندهای آن باشد. توصیه می‌شود، هدف و تمرکز اصلی این شیوه‌ها بالا بردن اثربخشی و کارآیی[۲] ممیزی بوده و درعین حال یکپارچگی فرآیند ممیزی را نیز حمایت نماید.

۹-۱- ۶ گزارش ممیزی‌صدورگواهی در IS 9.1.6

۹-۱-۶-۱ نهاد گواهی‌کننده مجاز است روش‌های اجرایی گزارش‌دهی را با توجه به نیازهای خود اتخاذ کند؛ ولی این روش‌های اجرایی باید دست‌کم بتوانند آن سازمان را از موارد زیر مطمئن کنند:

الف- یک جلسه با حضور تیم ممیزی و مدیریت سازمان مشتری پیش از ترک مکان سازمان مشتری تشکیل شود که در آن تیم ممیزی موارد زیر را ارائه دهد:

۱- یک گزارش شفاهی یا کتبی راجع به انطباق ISMS سازمان مشتری با الزاماتِ خاصِ صدورگواهی.

۲- فرصتی به سازمان مشتری برای پرسیدن سوالاتی درباره یافته‌ها و پایه و اساس آنها.

ب- تیم ممیزی یافته‌هایش راجع به انطباق ISMS سازمان‌مشتری به‌همراه تمامی الزاماتِ صدورگواهی را بصورت یک گزارش‌ممیزی در اختیار نهاد گواهی‌کننده قرار می‌دهد.

۹-۱-۶-۲ توصیه می‌شود، گزارش ممیزی شامل اطلاعات زیر باشد:

الف- گزارشی از ممیزی شامل خلاصه‌ای از بازنگری مدارک.

ب- گزارشی از ممیزی‌صدورگواهی تحلیل ریسک امنیت اطلاعات سازمان مشتری.

پ- کل‌زمان ممیزی صرف‌شده و مشخصات جزئی[۳] زمان گذرانده‌شده برای بازنگری مدارک، ارزیابی تحلیل ریسک، ممیزی در محل و تهیه گزارش ممیزی.

ت- پرسش‌های ممیزی[۴] که پیگیری‌شده‌اند، دلایل انتخاب آنها و روش‌شناسی بکار گرفته شده.

۹-۱-۶-۳ گزارش ممیزی از یافته‌ها، که به نهاد گواهی‌کننده تحویل می‌شود، باید از جزئیات کافی جهت تسهیل و پشتیبانی از تصمیم‌گیری برای صدورگواهی برخوردار بوده و شامل موارد زیر باشد:

الف- موضوعاتی که بوسیله ممیزی پوشش داده شده‌اند. (برای‌مثال الزاماتِ صدورگواهی و محلهایی که ممیزی شده‌اند.) شامل: داده‌های ممیزی مهم[۵] پیگیری‌شده و روش‌شناسی‌های ممیزی استفاده شده (رجوع شود به IS 9.1.5).

ب- مشاهدات انجام گرفته چه مثبت(برای‌مثال نکات برجسته) و چه منفی(برای‌مثال عدم‌انطباقات بالقوه).

4- Network-assisted
5- Efficiency
1- Detailed specification
2- Audit enquiries
3- Significant audit trails

پ- جزئیات هر عدم‌انطباق شناسایی شده، که با استفاده از شواهد عینی[1] و ارجاع این عدم‌انطباقات به الزامات استانداردِ "سیستم‌های مدیریت امنیت اطلاعات" استاندارد ۲۷۰۰۱ یا سایر مدارک لازم برای صدور گواهی پشتیبانی می‌شوند.

ت- اعلام‌نظر درباره انطباق ISMS سازمان مشتری با الزاماتِ صدورگواهی، به همراه بیانیه شفاف درباره عدم‌انطباقات، ارجاع به نسخه بیانیه کاربردپذیری و درجایی‌که امکان‌پذیر است، مقایسه سودمند با نتایج پیشین ممیزی‌های صدورگواهی سازمان مشتری.

پرسشنامه‌های تکمیل شده، چک‌لیست‌ها[2]، مشاهدات، اطلاعات ثبت‌شده وقایع[3]، یا یادداشت‌های ممیز، می‌توانند جزء لاینفک گزارش ممیزی باشند. اگر چنین روش‌هایی بکارگرفته می‌شوند، این مدارک باید به عنوان شواهد پشتیبان در تصمیم‌گیری برای صدورگواهی در اختیار نهاد گواهی‌کننده قرارداده‌شوند. توصیه می‌شود، اطلاعات درباره نمونه‌هایی که در حین ممیزی ارزشیابی شده‌اند نیز در گزارش‌ممیزی یا در دیگر مستندات صدور گواهی، آورده شوند. گزارش باید شایستگی سازمان داخلی و روش‌های اجرایی پذیرفته‌شده بوسیله سازمان مشتری جهت اطمینان از اینکه ISMS ایجاد شده است، را مد نظر قرار دهد.

علاوه بر الزاماتی که در بند ۹-۱-۱۰ از استاندارد ۲۷۰۰۱ برای گزارش‌دهی آورده شده است، توصیه می‌شود، گزارش موارد زیر را نیز پوشش دهد:

- درجه اعتمادی که می‌توان به ممیزی‌های داخلی ISMS و بازنگری‌های مدیریت داشت.
- خلاصه‌ای از مهمترین مشاهدات، چه مثبت و چه منفی، از اثربخشی و پیاده‌سازی ISMS.
- پیشنهاد تیم ممیزی که آیا گواهی برای ISMS سازمان مشتری صادر شود یا خیر و اطلاعاتی که این پیشنهاد را تایید و اثبات نماید.

۹-۲ ممیزی اولیه و صدورگواهی

الزامات بند ۹-۲ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۹-۲-۱ شایستگی تیم ممیزی در IS 9.2.1

علاوه بر الزاماتی که در بند ۷-۲ آورده شده است، الزامات زیر نیز در ارزیابی صدورگواهی لحاظ می‌شوند. در فعالیت‌های بازبینی صرفاً الزاماتی که به برنامه زمان‌بندی آن فعالیت مرتبط هستند کاربرد دارند.

الزامات زیر به کل تیم ممیزی اعمال می‌شود:

الف- در هریک از زمینه های زیر، دست‌کم یکی از اعضای تیم ممیزی باید معیارهای نهاد گواهی‌کننده را، جهت برعهده‌گیری مسوولیت، برآورده نماید:

۱- مدیریت تیم.

۲- سیستم‌های مدیریتی و فرآیند بکار گرفتن آن در مورد ISMS.

4- Objective evidence
1- Checklists
2- Logs

۳- دانش درباره الزامات قانون‌گذاری و مقرارت، بویژه در حوزه امنیت اطلاعات.
۴- شناسایی تهدیدات و روند رخدادهای امنیتی مرتبط با امنیت اطلاعات.
۵- شناسایی آسیب‌پذیری‌های سازمان مشتری و درک احتمال سوء استفاده از آنها، پیامد و چگونگی کاهش[1] و کنترل این پیامدها.
۶- دانش درباره کنترل‌های ISMS و پیاده‌سازی آنها.
۷- دانش درباره بازنگری اثربخشی ISMS و اندازه‌گیری کنترل‌ها.
۸- استانداردهای مرتبط و یا مربوطبه ISMS، بهترین تجربیات عملی، روش‌های اجرایی و خط‌مشی‌های امنیتی.
۹- دانش درباره روش‌های رسیدگی به رخدادهای امنیتی[2] و استمرار[3] کسب‌وکار.
۱۰- دانش درباره دارایی‌های اطلاعاتی ملموس و غیر ملموس و تحلیل پیامدها.
۱۱- دانش درباره فن‌آوری حال حاضر که ممکن است به امنیت مربوط بوده یا موضوع آن باشد.
۱۲- دانش درباره فرآیندها و روش‌های مدیریت ریسک.

ب- تیم ممیزی باید برای دنبال کردن نشانه های یک رخداد امنیتی در ISMS سازمان مشتری را تا رسیدن به مولفه‌های ISMS مربوط به آن، شایسته باشد.

پ- تیم ممیزی باید تجربه کاری و کاربرد عملی مناسبی از موارد فوق داشته باشد (این به‌معنای آن نیست که یک ممیز نیاز دارد گستره وسیعی از تجربیات در همه زمینه‌های امنیت اطلاعات داشته باشد. ولی توصیه می‌شود، تیم ممیزی به‌طور کل، از تجربه کافی برای پوشش دامنه‌شمول ISMS ممیزی شونده برخوردار باشد)

یک تیم ممیزی می‌تواند شامل یک نفر باشد به شرط آنکه وی تمامی معیارهای بخش الف را برآورده سازد.

۹-۲-۱-۱ اثبات شایستگی ممیز در IS 9.2.1.1

ممیزان باید بتوانند دانش و تجربه خود را، همان‌گونه که در بالا اشاره شد، اثبات کنند برای مثال از طریق:

الف- اثبات شرایط به‌رسمیت شناخته‌شده و مختص ISMS.
ب- ثبت نام به عنوان ممیز.
پ- دوره‌های آموزشی تایید شده ISMS .
ت- سوابق روزآمد از بهبود حرفه‌ای مستمر.
ث- تجربیات عملی کسب‌شده از مشاهده کار ممیزان با حضور در فرآیند واقعی ممیزی سیستم‌های مشتری.

1- Mitigation
2- Incident handling
3- Continuity

۹-۲- ۲ تدارکات عمومی برای ممیزی اولیه در IS 9.2.2

نهاد گواهی‌کننده باید از سازمان مشتری بخواهد تا تمامی تدارکات مورد نیاز برای اجرای ممیزی‌صدورگواهی، شامل فراهم کردن شرایط بررسی مستندات و دسترسی به تمامی نواحی، سوابق(شامل گزارشات ممیزی‌های داخلی و گزارشات بازنگری‌های مستقل امنیت اطلاعات) و کارکنان با اهداف ممیزی‌صدورگواهی، ممیزی‌صدورگواهی مجدد و رسیدگی به شکایات را ایجاد کند.

دست‌کم اطلاعات زیر باید پیش از ممیزی‌صدورگواهی درمحل سازمان از سوی مشتری در اختیار مرجع صدورگواهی قرار گیرد:

الف- اطلاعات کلی درباره ISMS و فعالیت‌هایی که پوشش می‌دهد.

ب- یک رونوشت از مستندات مورد نیاز ISMS که در بند ۴-۳-۱ از استاندارد ۲۷۰۰۱ تعیین شده‌اند؛ همچنین مستندات مرتبط در صورت لزوم.

۹-۲- ۳ ممیزی اولیه صدورگواهی در IS 9.2.3

۹-۲-۳-۱ ممیزی مرحله اول[1] در IS 9.2.3.1

در این مرحله از ممیزی، نهاد گواهی‌کننده باید مستندات طراحی ISMS را که پوشش‌دهنده مستندات الزامی در بند ۴-۳-۱ از استاندارد ۲۷۰۰۱ است، دریافت نماید.

هدف از ممیزی مرحله اول، تعیین نقطه تمرکز برای طرح‌ریزی ممیزی مرحله دوم با بدست آوردن درکی از ISMS، در قالب اهداف و خط‌مشیِ ISMS سازمان مشتری و به طور خاص، وضعیت حال حاضر سازمان مشتری و میزان آمادگی آن برای ممیزی است.

ممیزی مرحله اول شامل بازنگری مدارک می‌شود. ولی توصیه می‌شود که محدود به آن نباشد. نهاد گواهی‌کننده باید در این مورد که مدارک کی‌وکجا مورد بازنگری قرار گیرند با سازمان مشتری توافق کند. در هر حال بازنگری مدارک باید پیش از آغاز ممیزی مرحله دوم انجام شود.

نتایج ممیزی مرحله اول باید به صورت مکتوب مدون شوند. نهاد گواهی‌کننده باید پیش از تصمیم بر ادامه کار و رفتن به ممیزی مرحله دوم و همچنین انتخاب تیم ممیزی و تعیین شایستگی آنها، گزارش ممیزی مرحله اول را بازنگری نماید.

نهاد گواهی‌کننده باید سازمان مشتری را از نوع اطلاعات و سوابق بیشتری که ممکن است در ممیزی مرحله دوم برای بررسی‌های دقیق‌تر به آنها نیاز باشد، آگاه کند.

1- Stage 1 audit

منظور از ممیزی مرحله اول، مرحله اول از مراحل انجام ممیزی می باشد.

۹-۲-۳-۲ ممیزی مرحله دوم در IS 9.2.3.2

۹-۲-۳-۲-۱ممیزی مرحله دوم همیشه در محل(های) سازمان مشتری انجام می‌شود. بر اساس یافته‌های موجود در مدارک گزارش ممیزی مرحله اول، نهاد گواهی‌کننده یک طرح ممیزی را برای انجام ممیزی مرحله دوم تهیه می‌نماید. اهداف ممیزی مرحله دوم عبارتند از:

الف- تایید این امر که سازمان مشتری به خط‌مشی ها، اهداف و روش‌های اجرایی‌اش پایبند است.

ب- تایید این امر که ISMS با تمامی الزامات استاندارد الزامی ISMS - استاندارد ۲۷۰۰۱- مطابقت داشته و اهداف خط‌مشی سازمان مشتری را تامین می‌نماید.

۹-۲-۳-۲-۲ جهت دستیابی به این مهم، ممیزی باید تمرکز خود را معطوف موارد زیر از سازمان مشتری نماید:

الف- ارزیابی‌ریسک‌های مرتبط با امنیت اطلاعات و اینکه ارزیابی‌ها نتایج قابل‌قیاس و تجدیدپذیری را بدست دهد.

ب- الزامات مستندسازی ذکر شده در بند ۴-۳-۱ از استاندارد ۲۷۰۰۱.

پ- انتخاب اهداف کنترلی و کنترل‌ها براساس ارزیابی‌ریسک و فرآیندهای برطرف‌سازی ریسک.

ت- بازنگری‌های اثربخشی ISMS و اندازه‌گیری اثربخشی کنترل‌های امنیت اطلاعات، گزارش‌ها و بازنگری‌های اهداف ISMS.

ث- بازنگری‌های مدیریتی و ممیزی‌های داخلی ISMS .

ج- مسوولیت مدیریت در خط‌مشی امنیت اطلاعات.

چ- تطابق بین کنترل‌های انتخابی و کنترل‌های پیاده‌سازی شده، بیانیه کاربردپذیری و نتایج ارزیابی‌ریسک و فرآیند برطرف‌سازی ریسک و خط‌مشی و اهداف ISMS .

ح- پیاده‌سازی کنترل‌ها (به پیوست ت رجوع شود)، با در نظر گرفتن اندازه‌گیری‌های انجام‌شده از سوی سازمان، از میزان اثربخشی کنترل‌ها (بند ت)، جهت تعیین اینکه آیا کنترل‌ها پیاده‌سازی شده و از اثربخشی لازم برای نیل به اهداف بیان‌شده برخوردار هستند یا خیر.

خ- برنامه‌ها، فرآیندها، روش‌های اجرایی، سوابق، ممیزی‌های داخلی، و بازنگری‌های اثربخشی ISMS جهت اطمینان از اینکه این موارد تا تصمیمات مدیریتی، خط‌مشی و اهداف ISMS قابل‌ردیابی[1] هستند.

۹-۲-۳-۳ مولفه‌های مختص ممیزی ISMS در IS 9.2.3.3

نقش نهاد گواهی‌کننده این است که تعیین کند، سازمان‌های مشتری در ایجاد و حفظونگهداری روش‌های اجرایی‌شان برای شناسایی، بررسی و ارزشیابی[2] آسیب‌پذیری‌ها و تهدیداتِ دارایی‌های (تهدیدات مرتبط با امنیت اطلاعات) و پیامدهای آن برای سازمان خود پایبند هستند. نهادهای گواهی‌کننده باید:

1- Traceable
2- Evaluation

الف- سازمان مشتری را ملزم کنند تا اثبات کند که تحلیل امنیتی تهدیدات، کافی و در عین حال مرتبط با عملکرد سازمان مشتری است.

یادآوری- سازمان مشتری مسوول تعریف معیارهایی است، که به کمک آن ریسک‌های مرتبط با امنیت اطلاعات در سازمان مشتری را تحت عنوان «مهم[1]» شناسایی نموده و برای انجام آن روش‌های اجرایی تدوین نماید.

ب- تعیین کند، که آیا روش‌های اجرایی سازمان مشتری برای شناسایی، بررسی و همچنین ارزشیابی تهدیداتِ دارایی‌ها (تهدیدات مرتبط با امنیت اطلاعات)، آسیب‌پذیری‌ها و پیامدها، و نتایج به کار گرفتن آنها در راستای اهداف، خط‌مشی و مقاصد سازمان مشتری قرار دارد یا خیر.

نهاد گواهی‌کننده همچنین باید تعیین کند که آیا روش‌های اجرایی بکارگرفته شده در تحلیل میزان اهمیت[2] بی‌عیب هستند و به‌طور صحیح پیاده‌سازی شده‌اند. اگر یک تهدید دارایی‌ها (تهدید مرتبط با امنیت اطلاعات)، یک آسیب‌پذیری، یا یک پیامد بر سازمان مشتری، مهم تشخیص داده شود، باید در ISMS به آن پرداخته شود.

۹-۲-۳-۳-۱ انطباق با قوانین و مقررات

نگهداری و ارزشیابی تطابق و پیروی از قوانین و مقررات برعهده سازمان مشتری است. نهاد گواهی‌کننده باید خود را تنها به بررسی و نمونه برداری جهت اطمینان از عملکرد سازمان مشتری در این زمینه محدود کند. نهاد گواهی‌کننده باید برخوردار بودن سازمان مشتری را، از یک سیستم مدیریت برای دستیابی به انطباق با قوانین و مقررات قابل‌اجرا درمورد ریسک‌های امنیت اطلاعات و پیامدهای آن، تصدیق کند.

۹-۲-۳-۳-۲ یکپارچه سازی مستندات ISMS با سایر مستندات سیستم‌های مدیریتی

سازمان مشتری می‌تواند مستندات ISMS و سایر سیستم‌های مدیریتی (مانند: کیفیت، بهداشت و ایمنی، و محیط زیست) را با یکدیگر تلفیق کند تا جایی‌که ISMS به وضوح به همراه فصل‌های مشترک مناسب با سایر سیستم‌ها قابل تمیز باشد.

۹-۲-۳-۳-۳ تلفیق ممیزی‌های سیستم مدیریت

یک نهاد گواهی‌کننده مجاز است صدورگواهی سایر سیستم‌های مدیریتی را همراه با صدورگواهی ISMS عرضه کند و یا فقط صدورگواهی ISMS را عرضه کند.

ممیزی ISMS می‌تواند به صورت تلفیقی با ممیزی سایر سیستم‌های مدیریتی انجام شود. این تلفیق به‌شرطی امکان‌پذیر خواهد بود، که بتوان اثبات کرد تمامی الزامات صدورگواهی ISMS برآورده شده‌اند. تمامی مولفه‌های دارای اهمیت برای ISMS باید در گزارشات ممیزی به طور شفاف قابل مشاهده و به سادگی قابل تشخیص باشند. کیفیت ممیزی نباید به هیچ عنوان تحت تاثیر تلفیق ممیزی‌ها قرار گیرد.

3- Significant

1- Analysis of significance

یادآوری- استاندارد ISO19011 راهنمایی جهت انجام ممیزی تلفیقی[1] سیستم مدیریت ارائه می‌کند.

۹-۲- ۴ اطلاعات لازم برای اعطای گواهی اولیه در IS 9.2.4

جهت دستیابی به مبنایی برای، تصمیم‌گیری برای صدورگواهی، نهاد گواهی‌کننده باید گزارشاتی شفاف، که اطلاعات کافی جهت تصمیم‌گیری را در اختیار وی قرار دهد، درخواست نماید.

گزارش‌دهی توسط تیم ممیزی به نهاد گواهی‌کننده در مراحل مختلف فرآیند ممیزی‌صدورگواهی الزامی است.

توصیه می‌شود، علاوه بر اطلاعاتی که در فایل موجود هستند، این گزارشات دست‌کم شامل الزامات ذکر شده در بند IS 9.1.6 باشند.

۹-۲- ۵ تصمیم‌گیری برای صدورگواهی در IS 9.2.5

توصیه می‌شود، موجودیتی[2]- که ممکن است یک فرد باشد- که در نهاد گواهی‌کننده درباره اعطا/ ابطال یک گواهی تصمیم‌گیری می‌کند، شالوده‌ای از دانش‌ها و تجربیات در تمامی زمینه ها باشد، که برای ارزشیابی فرآیندهای ممیزی و همچنین پیشنهادات مرتبط با آن، که توسط تیم ممیزی انجام شده است، مناسب است.

تصمیم صدور یا عدم صدورگواهی برای یک سازمان مشتری باید توسط نهاد گواهی‌کننده و براساس اطلاعات جمع‌آوری شده در فرآیند صدورگواهی و همچنین سایر اطلاعات مرتبط انجام پذیرد.

کسانی که در مورد صدورگواهی، تصمیم‌گیری می‌کنند، نباید در تیم ممیزی حضور داشته باشند. این تصمیم باید براساس یافته‌ها و پیشنهادات تیم ممیزی که در گزارش ممیزی‌صدورگواهی ایشان (رجوع شود به بخش IS 9.1.6) آورده شده است و یا هر اطلاعات مرتبطی که قابل دسترس نهاد گواهی‌کننده است، انجام پذیرد.

معمولاً توصیه نمی‌شود، موجودیتی که درباره اعطای‌گواهی تصمیم‌گیری می‌کند، مخالف نظرات منفی تیم ممیزی تصمیم‌گیری نماید. اگر چنین اتفاقی رخ دهد، نهاد گواهی‌کننده باید دلایل مخالفت با توصیه را مستند و توجیه نماید.

در مورد تصمیم‌گیری درباره صدورگواهی، استاندارد ISO/IEC 17021 هیچ مدت زمان مشخصی را که در آن دست‌کم باید یک ممیزی داخلی کامل ISMS و یک بازنگری مدیریتی در سازمان مشتری انجام شود، مشخص نمی‌کند. نهاد گواهی‌کننده می‌تواند چنین مدت زمانی را تعیین کند. صرف‌نظر از اینکه نهاد گواهی‌کننده جهت انتخاب یک حداقل تناوب[3] تعیین شده است یا نه، اقداماتی از سوی نهاد گواهی‌کننده باید برای اطمینان از اثربخشی فرآیندهای ممیزی داخلی ISMS و بازنگری‌های مدیریتی سازمان مشتری، تعیین شود.

2- Combined audit
1- Entity
2- Minimum Frequency

گواهی نباید به سازمان مشتری اعطا شود، تا زمانی‌که شواهد کافی دال بر این مطلب وجود داشته باشد که: تمهیدات لازم که برای بازنگری‌های مدیریتی و ممیزی‌های داخلی ISMS پیاده‌سازی شده‌اند، اثربخش هستند و به خوبی نگهداری خواهند شد.

۹-۳ فعالیت‌های بازبینی

الزامات بند ۹-۳ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۹-۳-۱ ممیزی‌های بازبینی در IS 9.3

۹-۳-۱-۱ روش‌های اجرایی ممیزی بازبینی باید با روش‌های اجرایی ممیزی‌صدورگواهی ISMS سازمان مشتری، همان‌گونه که در این استاندارد به آنها اشاره شد، هماهنگ باشد.

هدف از بازبینی؛ تصدیق این امر است که ISMSای که قبلاً تاییدشده، همچنان استقرار دارد؛ مدنظر قرار دادن دلایل ضمنی ایجاد تغییرات در سیستم ISMS به‌دلیل تغییراتِ عملکردِ سازمانِ مشتری؛ و تایید تداوم انطباق با الزامات صدور گواهی است. توصیه می‌شود، برنامه‌های بازبینی به‌طورعادی موارد زیر را پوشش دهد:

الف- مولفه‌های نگهداری سیستم شامل: ممیزی‌داخلی ISMS، بازنگری‌مدیریت و اقدام پیشگیرانه و اصلاحی.

ب- ارتباطات اشخاص بیرونی، همان‌گونه که در استاندارد ۲۷۰۰۱ و سایر مدارک لازم برای صدورگواهی الزام شده است.

پ- تغییرات سیستم مستندسازی.

ت- حوزه‌های مورد تغییر قرارگرفته.

ث- مولفه‌های انتخابی از استاندارد ۲۷۰۰۱.

ج- سایر حوزه‌های انتخابی در موارد مقتضی.

۹-۳-۱-۲ بازبینی که از سوی نهاد گواهی‌کننده انجام می‌شود، باید دست‌کم موارد زیر را مورد بازنگری قرار دهد:

الف- اثربخشی ISMS با توجه به دستیابی به اهداف خط‌مشی امنیت اطلاعات سازمان مشتری.

ب- عملکرد صحیح روش‌های اجرایی در ارزشیابی دوره‌ای و بازنگری مطابقت با قوانین و مقرارت مرتبط با امنیت اطلاعات.

پ- اقدامات انجام شده در راستای از بین بردن عدم‌انطباقات شناسایی شده در آخرین ممیزی.

۹-۳-۱-۳ توصیه می‌شود، بازبینی که از سوی نهاد گواهی‌کننده انجام می‌شود، دست‌کم نکات الزامی ممیزی بازبینی را که در استاندارد ISO/IEC 17021 به آنها اشاره شده است، پوشش دهند. به‌علاوه، توصیه می‌شود، موارد زیر نیز در نظر گرفته شوند:

الف- توصیه می‌شود، نهاد گواهی‌کننده بتواند برنامه بازبینی خود را با موارد امنیت اطلاعات، مرتبط با تهدیداتِ دارایی‌ها، آسیب‌پذیری‌ها و پیامدها، برای سازمان مشتری وفق داده و این برنامه را توجیه کند.

ب- توصیه می‌شود، برنامه بازبینی نهاد گواهی‌کننده، بوسیله نهاد گواهی‌کننده تعیین شود. زمان‌های مشخص بازدید می‌تواند با توافق سازمان مشتری تعیین شود.

پ- ممیزهای بازبینی می‌تواند به صورت تلفیقی با ممیزی‌های سایر سیستم‌های مدیریتی انجام پذیرد. در گزارش باید به طور شفاف موارد مربوط به هر سیستم مدیریتی مشخص باشد.

ت- نظارت نهاد گواهی‌کننده بر نحوه استفاده از گواهینامه الزامی است.

در حین ممیزی‌های بازبینی، نهادهای گواهی‌کننده باید سوابق درخواست‌هایِ رسیدگی‌مجدد و شکایاتِ ازپیش‌ارائه‌شده به نهادگواهی‌دهنده را، در مواردی‌که عدم‌انطباق یا مردودی در الزامات صدور گواهی مشاهده شده است، بررسی نمایند و همچنین تحقیق کنند، آیا ISMS سازمان مشتری روش‌های اجرایی خود را بررسی و اقدام اصلاحی لازم را انجام داده است یا خیر.

یک گزارش بازبینی به طور خاص باید شامل اطلاعاتی مبنی بر برطرف سازی عدم‌انطباقات گزارش شده قبلی باشد. توصیه می‌شود، گزارشاتی که در بازبینی تهیه می‌شوند، دست‌کم تمامی الزامات ذکر شده در بند الف را پوشش دهند.

۹-۴ صدورگواهی مجدد

الزامات بند ۹-۴ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۹-۴-۱ ممیزی صدورگواهی مجدد در IS 9.4

روش‌های اجرایی ممیزی‌صدورگواهی‌مجدد باید با روش‌های اجرایی ممیزی‌صدورگواهی ISMS سازمان مشتری ذکر شده در این استاندارد همخوانی داشته باشد.

نهادهای گواهی‌کننده باید روش‌های اجرایی مشخص و شفاف جهت تبیین شرایط و موقعیت‌هایی که منجر به حفظ گواهی سازمان مشتری می‌شود، داشته باشد. اگر در ممیزی بازبینی یا ممیزی صدورگواهی‌مجدد عدم‌انطباقاتی یافت شود، این عدم‌انطباقات باید به صورت اثربخش و در زمان توافق شده با نهاد گواهی‌کننده اصلاح شوند. اگر این اصلاح در زمان توافق شده انجام نشود، دامنه‌شمول گواهی باید کوچکتر شود یا گواهینامه به حالت تعلیق درآید و یا ابطال شود. توصیه می‌شود، مدت زمانی‌که جهت انجام اقدام‌اصلاحی در اختیار سازمان‌مشتری قرار می‌گیرد با میزان اهمیت عدم‌انطباق و ریسکِ اطمینان ازاین‌که محصولات و خدمات سازمان مشتری الزامات خاصی را رعایت می‌کنند، هم‌خوانی داشته باشد.

۹-۵ ممیزی‌های خاص

الزامات بند ۹-۵ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۹-۵-۱ حالتهای خاص در IS 9.5

فعالیت‌های بازبینی باید تحت ضوابط خاصی قرار گیرند، اگر یک سازمان مشتری که دارای گواهی ISMS است، تغییرات عمده‌ای در سیستم‌اش دهد یا تغییرات دیگری اتفاق بیافتد که بتواند اساس گواهی آن سازمان را تحت تاثیر قرار می‌دهد.

۹-۶ تعلیق، ابطال یا کوچک کردن دامنه‌شمول گواهی

الزامات بند ۹-۶ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۹-۷ درخواست‌های رسیدگی‌مجدد

الزامات بند ۹-۷ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۹-۸ شکایات

الزامات بند ۹-۸ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۹-۸-۱ شکایات در IS 9.8

شکایات بعنوان یک منبع اطلاعات برای نشان دادن عدم‌انطباق احتمالی عمل می‌کنند. توصیه می‌شود، نهاد گواهی‌کننده سازمان مشتری صاحب گواهی را ملزم کند تا در زمان دریافت شکایت، دلیل شکایت را مدون و در زمان مناسب آن را گزارش دهد. این گزارش شامل هر مورد از پیش تعیین شده (یا قبلاً ارائه شده) در ISMS سازمان مشتری است.

توصیه می‌شود، نهاد گواهی‌کننده این‌گونه تعبیر نماید که سازمان مشتری با استفاده از این بررسی‌ها قصد دارد اقدام جبرانی[1]/ اصلاحی را انجام دهد. توصیه می‌شود این امر شامل اقداماتی[2] برای موارد زیر باشد:

الف- مطلع ساختن مراجع دارای اختیار مناسب، درصورتی‌که این‌کار براساس مقررات الزام شده است.

ب- انطباق ترمیمی[3].

پ- اجتناب از وقوع مجدد.

ت- ارزشیابی و کاهش رخدادهای امنیتی مخرب و کاهش پیامدهای آنها.

ث- اطمینان از تعامل رضایت بخش با سایر اجزای ISMS .

ج- ارزیابی اثربخشی اقدامات جبرانی/ اصلاحی اختیار شده.

1- Remedial action
2- Measures
3- Restoring Conformity

نهاد گواهی‌کننده باید هر سازمان مشتری که ISMS آن گواهی شده است، را ملزم کند تا سوابق تمامی شکایات و اقدام اصلاحی انجام پذیرفته در راستای تطابق با الزامات استاندارد ملی ایران ایزو-آی ای سی به شماره ۲۷۰۰۱ را، بنا به درخواست، در اختیار نهاد گواهی‌کننده قرار دهد.

۹-۹ سوابق متقاضیان و مشتریان

الزامات بند ۹-۹ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۱۰ الزامات سیستم مدیریتی برای نهادهای گواهی‌کننده

۱۰-۱ گزینه ها

الزامات بند ۱۰-۱ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۱۰-۲ گزینه ۱- الزامات سیستم مدیریتی مطابق با ISO9001

الزامات بند ۱۰-۲ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۱۰-۳ گزینه ۲- الزامات عمومی سیستم مدیریت

الزامات بند ۱۰-۳ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۱۰-۳-۱ پیاده‌سازی ISMS در IS 10.3

توصیه می‌شود، نهادهای گواهی‌کننده ISMS را مطابق با استاندارد ۲۷۰۰۱ پیاده‌سازی کنند.

پیوست الف

(اطلاعاتی)

تحلیل پیچیدگی سازمان‌های مشتری و موارد مختص بخش

الف- ۱ ریسک بالقوه سازمان

پیچیدگی دامنه‌شمول ISMS باید در زمان تعیین زمان ممیزی یا شایستگی ممیزان در نظر گرفته شود. این پیوست مثالی از تحلیل پیچیدگی یک سازمان مشتری را برای این منظور ارائه می‌کند.

رده‌ی پیچیدگی که به دامنه‌شمول ISMS اختصاص داده می‌شود می‌تواند برای تصمیم‌گیری در موارد زیر استفاده شود:

الف- الزامات شایستگی ممیزان برای ممیزی ISMS (مثالی از آن در پیوست ب شرح داده شده است).

ب- الزامات زمان ممیزی برای ممیزی ISMS (مثالی از آن در پیوست پ شرح داده شده است).

جدول الف-۱ نمایشی کلی از عوامل ممکن که برای تعیین پیچیدگی دامنه‌شمول ISMS درنظر گرفته می‌شوند، را در بردارد. این جدول نیاز دارد برای موقعیت‌های مشخص تطبیق داده شود و یا در موارد مقتضی، فاکتورهای خاص دیگری به آن اضافه شود.

با استفاده از معیار پیچیدگی بطور مجزا (در جدول الف-۱)، جنبه‌های پیچیدگی دامنه‌شمول ISMS می‌تواند به سه رده طبقه‌بندی شود: "بالا"، "متوسط" و "پایین". این سطوح با استفاده از تعدادی عوامل متفاوت بدست می‌آیند. رده اثربخش کلی پیچیدگی می‌تواند با درنظر گرفتن بالاترین رده موجود در بین فاکتورها تعیین شود و ماحصل نیز به صورت رده خواهد بود، به‌عبارت‌دیگر «بالا»،«متوسط» یا «پایین».

جدول الف-۱ – معیارهای پیچیدگی دامنه‌شمول ISMS

عامل پیچیدگی	رده			اهمیت
	بالا	متوسط	پایین	
تعداد کارکنان + کارکنان پیمانکاران	۱۰۰۰	≥۲۰۰	<۲۰۰	ابعاد پیاده‌سازی ISMS سیستم مدیریت اطلاعات سیستم‌های تولیدی مرتبط با مدیریت سیستم‌های مرتبط با خدمات عمومی / توزیع / فروش فن‌آوری اطلاعات/ خدمات اطلاعات و سیستم‌های مرتبط ساخت و ساز/ کشتی سازی/ سیستم تاسیسات مرتبط با مهندسی
تعداد کاربران	۱میلیون	۲۰۰۰۰۰	<۲۰۰۰۰۰	سیستم‌های مالی دولتها، مدارس، سیستم‌های بیمارستانی / پزشکی

جدول الف-۱ – ادامه

عامل پیچیدگی	رده			اهمیت
	بالا	متوسط	پایین	
تعداد سایت‌ها	≥۵	≥۲	۱	مقیاس پیاده‌سازی ISMS امنیت فیزیکی و محیطی (الف-۹ از استاندارد ۲۷۰۰۱)
تعداد سرورها	≥۱۰۰	≥۱۰	<۱۰	مقیاس پیاده‌سازی ISMS امنیت فیزیکی و محیطی (الف-۹ از استاندارد ۲۷۰۰۱) کنترل دسترسی (الف-۱۱ از استاندارد ۲۷۰۰۱) مخابرات و مدیریت عمکرد (الف-۱۰ از استاندارد ۲۷۰۰۱)
تعداد ایستگاههای کاری + رایانه های شخصی + رایانه های قابل حمل	≥۳۰۰	≥۵۰	<۵۰	کنترل دسترسی (الف-۱۱ از استاندارد ۲۷۰۰۱)
تعداد کارکنان بهبود و نگهداری برنامه کاربردی[1]	≥۱۰۰	≥۲۰	<۲۰	اکتساب، بهبود و نگهداری سیستم‌های اطلاعاتی (الف-۱۲ از استاندارد ۲۷۰۰۱)
فن‌آوری رمزنگاری و شبکه	اتصالات بیرونی/ اینترنت با رمزنگاری/ امضای دیجیتال/ الزامات زیرساخت‌کلیدهمگانی (PKI[2])	اتصالات بیرونی/ اینترنت بااستفاده از رمزنگاری موجود در تجهیزات استاندارد و بدون امضای دیجیتال/ الزامات زیرساخت‌کلیدهمگانی (PKI)	اتصالات بیرونی/ اینترنت بدون رمزنگاری/ امضای دیجیتال/ الزامات زیرساخت‌کلیدهمگانی (PKI)	مخابرات و مدیریت عملکرد (الف-۱۰ از استاندارد ۲۷۰۰۱) کنترل دسترسی (الف-۱۱ از استاندارد ۲۷۰۰۱)
اهمیت در انطباق قانونی	عدم برآورده‌سازی پیگرد قانونی دارد.	عدم برآورده‌سازی منجر به پرداخت‌تاوان‌مالی‌مهم یا خدشه‌دارشدن‌اعتبارمهم می‌شود.	عدم برآورده‌سازی منجر به پرداخت‌تاوان‌مالی‌ناچیز یا خدشه‌دارشدن‌اعتبارناچیز می‌شود.	قوانین و راهنمایی‌ها (الف-۱۵ از استاندارد ۲۷۰۰۱)

1- Application
2- Public Key Infrastructure

جدول الف-۱ – ادامه

عامل پیچیدگی	رده			اهمیت
	بالا	متوسط	پایین	
کاربردپذیری ریسک مختص بخش (برای مثال‌هایی از رده‌های‌مختص‌بخش درریسک‌امنیت‌اطلاعات به الف-۲ مراجعه شود)	قانون‌ومقررات مختص‌بخش کاربرد دارد.	قانون‌و قررات مختص‌بخش، کاربرد ندارد ولی ریسک‌مهم‌مختص‌بخش کاربرد دارد.	قانون‌ومقررات مختص‌بخش، کاربرد ندارد و ریسک‌مختص‌بخش کاربرد ندارد.	مقیاس پیاده‌سازی ISMS قوانین و راهنمایی‌ها (الف-۱۵ از استاندارد ۲۷۰۰۱)

الف-۲ رده‌های مختص بخش در ریسک امنیت اطلاعات

ریسک‌های اطلاعات ممکن است مختص به نوع اطلاعات موردنظر یا بخش فعالیت سازمان، باشد. مثال‌های زیر رده‌های متفاوتی از ریسک را نشان می دهند:

رده‌های خاص کاربردی برای همه سازمان‌ها:

- حقوقها، مستمری‌ها، بهداشت و ایمنی، سوابق سازمانی، اطلاعات درون بخشی یا بین بخشی و غیره؛
- هر اطلاعات قابل تشخیص فردی دیگر؛
- هر اطلاعات تجاری مهم/ حساس دیگر مانند: اطلاعات تحقیق و بهبود، اطلاعات طراحی، اطلاعات مشتریان، نتایج و پیش‌بینی‌های مالی، طرح کسب‌وکار، حقوق مالکیت معنوی، فرآیندهای ساخت، و غیره.

اطلاعات دولتی حساس/ مهم:

- اطلاعات همگانی؛
- برنامه‌های کاربردی دولت الکترونیک[1]؛
- اطلاعات نگهداشته شده درباره شهروندان (برای‌مثال سلامتی، منفعت، مالیات‌ها، سوابق و غیره)؛
- اطلاعاتی که توسط تامین‌کنندگان[2] و سازندگان دولت مورد استفاده قرارمی‌گیرند: مانند طراحی‌های فن‌آوری ارتباطات و اطلاعات[3]، امکانات، محصولات، خدمات و غیره.

رده‌های خاص کاربردی برای کلاس‌های سازمانی:

- اصناف[4]- شرکت‌های لیست شده (احتمالا سایر نهادهای بزرگ).

1- E-government
2- Suppliers
3- Information Communication Technology (ICT)
4- Corporate governance

رده‌های خاص کاربردی برای بخش‌های تجاری:

- بهداشت؛
- تعلیم و تربیت؛
- هوا- فضا؛
- مخابرات؛
- خدمات مالی؛
- سازمان‌های خیریه و غیرانتفاعی.

پیوست ب
(اطلاعاتی)
حوزه‌های نمونه از شایستگی ممیز

ب-۱ ملاحظات کلی شایستگی

شیوه‌های متفاوتی برای اثبات دانش و تجربه یک ممیز وجود دارد. برای مثال دانش و تجربه می‌تواند از طریق اثبات شرایط برسمیت شناخته‌شده نشان‌داده‌شود. ثبت نام ممیز، برای‌مثال در مرکز IRCA[1] یا ثبت‌نام ممیز به هر طریق برسمیت شناخته‌شده دیگر نیز، می‌تواند نشانگر تجربه و دانش لازم برای ممیز باشد. توصیه می‌شود، سطح شایستگی‌های لازم برای تیم ممیزی با درنظر گرفتن حوزه مربوط به فن‌آوری/صنعتی سازمان و عوامل پیچیدگی آن تعیین شود.

ب-۲ ملاحظات مختص شایستگی

ب-۲-۱ آگاهی از کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱

موارد زیر دانش عمومی لازم در ارتباط با ممیزی ISMS را بیان می‌کنند. علاوه بر حوزه‌های کنترلی پیوست الف از استاندارد ۲۷۰۰۱، که در جدول زیر لیست شده‌اند، توصیه می‌شود، ممیزان از مفاد سایر استانداردهای خانواده ۲۷۰۰۰ نیز آگاهی داشته باشند.

دانش و تجربه درباره خط‌مشی‌ها و الزامات کسب‌وکار برای امنیت اطلاعات	خط‌مشی امنیتی
دانش و تجربه عمومی از فرآیندهای کسب‌وکار، اعمال و ساختارهای سازمانی	سازمان امنیت اطلاعات
دانش ارزش‌گذاری دارایی‌ها، سیاهه اموال، طبقه بندی دارایی‌ها و خط‌مشی‌های قابل قبول مورد استفاده در دارایی‌ها	مدیریت دارایی
دانش و تجربه کلی از فرآیندها و روش‌های اجرایی استفاده شده در بخش‌های منابع انسانی	امنیت منابع انسانی
آگاهی از امنیت زیست‌محیطی و فیزیکی	امنیت محیطی و فیزیکی
دانش و تجربه روزآمد از استانداردها، فرآیندها، تکنیک‌ها و روش‌های بکارگرفته شده در امنیت اطلاعات شامل اقدامات مدیریتی و همچنین سطح مناسب تخصص‌های فنی. این مورد همچنین دربرگیرنده آخرین اطلاعات برخی شیوه‌های کسب‌وکار متداول نیز می‌شود.	مدیریت عملکرد و ارتباطات کنترل دسترسی اکتساب، بهبود و نگهداری سیستم‌های اطلاعاتی
دانش و تجربیات روزآمد از فرآیندها و روش‌های اجرایی مدیریت رخدادهای امنیتی	مدیریت رخدادهای امنیت اطلاعات
دانش و تجربیات روزآمد از استانداردها، فرآیندها، برنامه‌ها و روش‌های اجرایی آزمون برای تداوم کسب‌وکار	مدیریت تداوم کسب‌وکار
دانش روزآمد از موارد قراردادی تجاری و قوانین و مقررات متداول و مرتبط	انطباق

1- International Register of Certificated Auditors

با ISMS	

ب-۲-۲ دانش معمول مرتبط با ISMS

توصیه می‌شود، ممیزان درباره موضوعات ممیزی و ISMS ،که در زیر آورده شده‌اند، اطلاع و آگاهی داشته باشند:

- طرح‌ریزی و برنامه‌ریزی ممیزی،
- نوع و روش‌شناسی‌های ممیزی،
- ریسک ممیزی،
- تحلیل فرآیندهای امنیت اطلاعات،
- چرخه دمینگ[1] (PDCA[2]) برای بهبود مداوم،
- ممیزی داخلی برای امنیت اطلاعات.

توصیه می‌شود، ممیزان از الزامات قانونی و مقررات زیر اطلاع و آگاهی داشته باشند:

- مالکیت معنوی،
- محتوی، حفاظت و نگهداری از سوابق سازمانی،
- حفاظت از اطلاعات و حریم شخصی،
- مقررات کنترل‌های رمزنگاری،
- ضد تروریستی،
- تجارت الکترونیکی،
- امضای دیجیتال و الکترونیکی،
- بازبینی‌های محیط کار،
- قطع ارتباط مخابراتی و مشاهده اطلاعات (برای‌مثال پست الکترونیک)،
- سوء استفاده های رایانه‌ای،
- جمع‌آوری شواهد الکترونیکی،
- آزمون نفوذپذیری،
- الزامات ملی و بین‌المللی مختص‌بخش (برای‌مثال بانکداری).

توصیه می‌شود ممیزان از الزامات مدیریتی زیر اطلاع و آگاهی داشته باشند:

- برطرف سازی ریسک‌های امنیت اطلاعات،
- ریسک‌های امنیتی برون سپاری در فن‌آوری ارتباطات و اطلاعات،
- ریسک‌های امنیت اطلاعات در زنجیره تامین.

1- Deming cycle
2- Plan, Do, check, Act

پیوست پ
(اطلاعاتی)
زمان ممیزی

پ-۱ مقدمه

این پیوست حاوی اطلاعات بیشتری درباره بندهای ۹-۱، ۹-۲، ۹-۳ و ۹-۴ از استاندارد ۲۷۰۰۱ است. توصیه می‌شود، این پیوست به همراه بندهای IS 9.1.2، IS 9.1.3، IS 9.1.5، IS 9.1.6، IS 9.2.3.1 ، IS 9.2.3.3 و IS 9.2.3.3 از این استاندارد مطالعه شود. این پیوست راهنمایی برای نهاد گواهی‌کننده در راستای بهبود روش‌های اجرایی آنها در تعیین زمان لازم برای صدورِگواهی، برای دامنه‌شمولِISMS سازمان‌های مشتری، با اندازه و پیچیدگی‌های متفاوت و در طیف وسیعی از فعالیت‌ها، ارائه می‌کند.

نهادهای گواهی‌کننده نیاز دارند مدت زمانی را که برای ممیزی اولیه صدورگواهی، ممیزی بازبینی و ممیزی صدورگواهی مجدد برای هر مشتری و ISMS گواهی شده قبلی صرف می‌شود، تعیین نمایند. استفاده از این پیوست در فاز طرح‌ریزی ممیزی می‌تواند منجر به رویکرد باثباتی برای تعیین زمان مناسب ممیزی شود. در عین حال، راهنمایی که در این پیوست ارائه می‌شود از انعطاف پذیری بر اساس یافته‌های دوره ممیزی، بخصوص در مرحله اول و همچنین پیچیدگی دامنه‌شمول ISMS، برخوردار است.

پ-۲ روش اجرایی تعیین زمان ممیزی

تجربه نشان داده است که دامنه‌شمول ISMS، تعداد کارکنان (همان‌گونه که در جدول پ-۳ نشان داده شده است)، ابعاد، ویژگی‌ها، پیچیدگی‌ها و میزان اهمیت ریسک‌های بالقوه امنیت اطلاعات (همان‌گونه که با جزئیات در زیر تشریح شده‌اند) در میزان زمان ممیزی ISMS تعیین کننده خواهند بود. بند IS 9.1.3 و همچنین بندهای IS 9.2.3.1، IS 9.2.3.2 و IS 9.2.3.3 فهرستی از معیارهایی که توصیه می‌شود در هنگام تعیین زمان مورد نیاز برای ممیزی در نظر گرفته شوند را ارائه می‌کند. این عوامل و عوامل دیگر باید در فرآیند بازنگری قرارداد نهاد گواهی‌کننده مورد بررسی قرار گیرند، زیرا از پیامد بالقوه‌ای بر میزان زمان تخصیص داده شده برای ممیزی، برخوردار هستند.

شایان ذکر است که توصیه شود، تمامی این عوامل برای تعیین زمان ممیزی لحاظ شوند و جدول زمانی ممیز، که در پ -۳ آورده شده است، نمی‌تواند به صورت جداگانه به کار برده شود. مثالهای زیر عواملی را که می‌توانند میزان زمان ممیزی را تحت تاثیر قرار دهند نشان می‌دهد و همچنین عوامل ذکر شده در بند IS9.1.3 را شرح می‌دهند.

- عوامل مرتبط با ابعاد دامنه‌شمول ISMS (برای‌مثال تعداد سیستم‌های اطلاعاتی مورد استفاده، حجم اطلاعات پردازش‌شده، تعداد کاربران، تعداد کاربران با اختیارات ویژه، تعداد بسترهای فن‌آوری اطلاعات، تعداد شبکه‌ها و ابعاد آنها)؛

- عوامل مرتبط با پیچیدگی ISMS (برای‌مثال حیاتی‌بودن سیستم‌های اطلاعاتی، موقعیت ریسک ISMS حجم و نوع اطلاعات حساس و حیاتی که مورد استفاده قرارگرفته و پردازش می‌شوند، تعداد و نوع تراکنش‌های الکترونیکی، تعداد و ابعاد پروژه‌های بهبود، وسعت فعالیت‌های از راه‌دور، وسعت مستندات ISMS)؛
- نوع/ انواع کسب‌وکار انجام پذیرفته در دامنه‌شمول ISMS و الزامات امنیتی، قانونی، مقرراتی، قراردادی و تجاری مرتبط با آن نوع کسب‌وکار؛
- وسعت و گوناگونی فن‌آوری به‌کارگرفته شده در پیاده‌سازی اجزای مختلف ISMS (مانند کنترل‌های پیاده‌سازی شده، مستندسازی و/یا کنترل فرآیند، اقدام اصلاحی/پیشگیرانه، سیستم‌های اطلاعاتی، سیستم‌های فن‌آوری اطلاعات، شبکه‌ها، برای‌مثال آیا ثابت، متحرک، بی‌سیم، بیرونی و یا داخلی هستند.)؛
- تعداد سایت‌های موجود در دامنه‌شمول ISMS؛ تا چه اندازه این سایت‌ها مشابه یا متفاوت هستند، و آیا تمامی این سایت‌ها یا فقط یک نمونه از آنها مورد ممیزی قرار خواهند گرفت؛
- عملکرد اثبات‌شده قبلی ISMS؛
- وسعت برون‌سپاری و توافقات شخص‌سوم استفاده شده در دامنه‌شمول ISMS و همچنین وابستگی به این خدمات؛
- استانداردها، قوانین و مقرراتی که برای صدور گواهی بکار گرفته می‌شوند و هر الزامات مختصِ‌بخش که ممکن است بکار گرفته شود.

صدورگواهی ISMS به طور معمول بیشتر از صدر گواهی سیستم مدیریت کیفیت یا سیستم مدیریت محیط زیست طول می‌کشد و این به علت افزایش الزامات یک سیستم مدیریت امنیت اطلاعات به ازای یک درخواست مشخص برای ISMS است، مانند: خط‌مشی ISMS، مدیریت ریسک و کنترل‌ها و اهداف کنترلی ISMS. نهاد گواهی‌کننده لازم است:

الف- صحت و ثبات شیوه‌ای را که به وسیله آن؛ سازمان مشتری میزان اهمیت ریسک‌های امنیت اطلاعات و پیامدهای آن را تعیین می‌کند، مورد ممیزی قرار دهد؛

ب- تایید کند که سیستم طراحی شده برای دستیابی به انطباق (با همه قوانین و الزامات دیگری که در ISMS بکار گرفته می‌شوند) از قابلیت لازم برخوردار بوده و این سیستم پیاده‌سازی شده و نگهداری می‌شود؛

پ- تایید کند که اهداف کنترلی و کنترل‌ها به درستی انتخاب و پیاده‌سازی شده‌اند و میزان اثربخشی آنها اندازه‌گیری می‌شود و فرآیند دستیابی به «پیشگیری از رخدادهای‌امنیتی و پاسخ مناسب به آنها» درست و مناسب است؛

ت- تایید کند که الزامات مدارک ISMS سازمان مشتری به درستی برآورده شده‌اند؛

ث- به افزایش درخواست‌هایی که از ممیزی مرحله اول ایجاد می‌شوند واکنش نشان دهد.

پ-۳ جدول زمانی ممیز

پ-۳-۱ کلی

جدول زمانی ممیز که در زیر آورده شده است، میانگینی از تعداد روزهای ممیزی اولیه ارائه می‌کند (در اینجا و از این‌به‌بعد، این تعداد شامل روزهای ممیزی مرحله اول و ممیزی مرحله دوم می‌شود)، که تجربه نشان داده است برای دامنه‌شمول ISMS با تعداد کارکنان مشخص مناسب است. تجربه همچنین اثبات کرده است که برای دامنه‌های شمول ISMS با ابعاد مشابه برخی نیاز به زمان کمتر و برخی به زمان بیشتر نیاز دارند.

تغییرات زمانِ صرف‌شده برای صدور هر گواهی، بستگی به تعدادی از عوامل شامل ابعاد، دامنه‌شمول ممیزی، تدارکات، پیچیدگی سازمان و آمادگی آن برای انجام ممیزی دارد (همچنین به پ-۲ رجوع شود). این عوامل و عوامل دیگر لازم است در فرآیند بازنگری قرارداد نهاد گواهی‌کننده مورد بررسی قرار گیرند، زیرا از پیامد بالقوه‌ای بر میزان زمان تخصیص داده شده برای ممیزی برخوردار هستند. بنابراین جدول زمانی ممیز نمی‌تواند جدا از این عوامل مورد استفاده قرار گیرد.

جدول‌زمانی ممیز که در زیر ارائه شده‌است، چارچوبی فراهم می‌آورد، که با استفاده از تعیین یک نقطه آغاز براساس مجموع تعدادکارکنان درتمامی نوبت‌های‌کاری و تنظیم و تغییر آن براساس عوامل‌مهم‌موثر بر دامنه‌شمول ISMS موردممیزی و تخصیص یک‌وزن جمع‌شونده یا کم‌شونده جهت اصلاح عددپایه، می‌تواند در طرح‌ریزی ممیزی مورداستفاده قرارگیرد. اصطلاحات استفاده‌شده در این جدول در پ-۳-۲ ارائه شده‌اند.

جدول زمانی ممیز

تعداد کارکنان	زمان QMS[1] برای ممیزی اولیه (روزهای ممیز)	زمان ممیز EMS[2] برای ممیزی اولیه (روزهای ممیز)	زمان ممیز ISMS برای ممیزی اولیه (روزهای ممیز)	عوامل جمع‌شونده و کم‌شونده	زمان کل ممیزی
۱~۱۰	۲	۳	۵	به پیوست پ-۲ رجوع شود	
۱۱~۲۵	۳		۷	به پیوست پ-۲ رجوع شود	
۲۶~۴۵	۴	۶	۸.۵	به پیوست پ-۲ رجوع شود	
۴۶~۶۵	۵		۱۰	به پیوست پ-۲ رجوع شود	
۶۶~۸۵	۶		۱۱	به پیوست پ-۲ رجوع شود	

1- Quality Management Systems

سیستم‌های مدیریت کیفیت

2- Environmental Management Systems

سیستم‌های مدیریت زیست‌محیطی

۸۶~۱۲۵	۷	۸	۱۲	به پیوست پ-۲ رجوع شود	
۱۲۶~۱۷۵	۸		۱۳	به پیوست پ-۲ رجوع شود	

جدول زمانی ممیز- ادامه

تعداد کارکنان	زمان QMS برای ممیزی اولیه (روزهای ممیز)	زمان ممیز EMS برای ممیزی اولیه (روزهای ممیز)	زمان ممیز ISMS برای ممیزی اولیه (روزهای ممیز)	عوامل جمع‌شونده و کم‌شونده	زمان کل ممیزی
۱۷۶~۲۷۵	۹		۱۴	به پیوست پ-۲ رجوع شود	
۲۷۶~۴۲۵	۱۰		۱۵	به پیوست پ-۲ رجوع شود	
۴۲۶~۶۲۵	۱۱	۱۲	۱۶.۵	به پیوست پ-۲ رجوع شود	
۶۲۶~۸۷۵	۱۲		۱۷.۵	به پیوست پ-۲ رجوع شود	
۸۷۶~۱۱۷۵	۱۳		۱۸.۵	به پیوست پ-۲ رجوع شود	
۱۱۷۶~۱۵۵۰	۱۴		۱۹.۵	به پیوست پ-۲ رجوع شود	
۱۵۵۱~۲۰۲۵	۱۵	۱۸	۲۱	به پیوست پ-۲ رجوع شود	
۲۰۲۶~۲۶۷۵	۱۶		۲۲	به پیوست پ-۲ رجوع شود	
۲۶۷۶~۳۴۵۰	۱۷		۲۳	به پیوست پ-۲ رجوع شود	
۳۴۵۱~۴۳۵۰	۱۸		۲۴	به پیوست پ-۲ رجوع شود	
۴۳۵۱~۵۴۵۰	۱۹		۲۵	به پیوست پ-۲ رجوع شود	
۵۴۵۱~۶۸۰۰	۲۰		۲۶	به پیوست پ-۲ رجوع شود	
۶۸۰۱~۸۵۰۰	۲۱		۲۷	به پیوست پ-۲ رجوع شود	
۸۵۰۱~۱۰۷۰۰	۲۲		۲۸	به پیوست پ-۲ رجوع شود	
>۱۰۷۰۰	روند بالا ادامه یابد		روند بالا ادامه یابد	به پیوست پ-۲ رجوع شود	

پ-۳-۲ توضیح اصطلاحات

«کارکنان» که در جدول زمانی ممیز به آن ارجاع شده است، اشاره به تمامی افرادی دارد که فعالیت‌های کاری‌شان به دامنه‌شمول ISMS مرتبط است. کل تعداد کارکنان در تمامی نوبت‌های کاری نقطه آغازی برای تعیین زمان ممیزی است.

تعداد اثربخش کارکنان شامل: کارکنان غیر رسمی(فصلی، موقت و یا پیمانی) که در زمان ممیزی حضور دارند، می‌شود. توصیه می‌شود، نهاد گواهی‌کننده با سازمان مشتری ممیزی شونده بر سر زمان‌بندی ممیزی، که به بهترین وجه نمایانگر دامنه‌شمول کامل سازمان است، توافق کند. موارد توافق می‌تواند شامل فصل، ماه، روز/تاریخ و نوبت کاری برحسب مورد باشد.

توصیه می‌شود، با کارکنان نیمه وقت نیز مشابه کارکنان تمام وقت رفتار شود. این تصمیم بستگی به تعداد ساعات کاری آنها درمقایسه با کارکنان تمام وقت دارد.

«زمان ممیز» شامل زمانی است که یک ممیز یا تیم ممیزی در، ممیزی مرحله‌اول، ممیزی مرحله‌دوم و مرحله طرح‌ریزی (شامل بازنگری خارج از محل مدارک در صورت نیاز)؛ برقراری ارتباط با سازمان، کارکنان، سوابق، مستندات و فرآیند؛ و نوشتن گزارش، صرف می‌نماید. انتظار می‌رود که «زمان ممیز»، که شامل تلفیقی از زمان برای طرح‌ریزی و نوشتن گزارش است، به طور معمول، مجموع «زمان ممیز» برای حضور در محل را به کمتر از ۷۰٪ زمان نشان داده شده در جدول کاهش ندهد. در جایی که زمان بیشتری برای طرح‌ریزی و/ یا نوشتن گزارش لازم است، انجام این امور توجیه مناسبی برای کاهش میزان زمان ممیز برای حضور در محل نیست. زمان سفر ممیز در محاسبات لحاظ نمی‌شود، و به زمان ممیز که در جدول به آن اشاره شده است اضافه می‌شود.

یادآوری ۱- عدد ۷۰٪ براساس تجربیات ممیزی ISMS بدست آمده است.

اگر از روش‌های ممیزی راه‌دور مانند: همکاری تعاملی از طریق وب، جلسات از طریق وب، تله کنفرانس و/ یا تصدیق الکترونیکی فرآیندهای سازمان برای ارتباط با سازمان استفاده می‌شود؛ توصیه می‌شود، این فعالیت‌ها در طرح ممیزی (به بند IS 9.1.5 رجوع شود) شناسایی شده و می‌تواند به عنوان ملحقات جزئی «زمان ممیز برای حضور در محل» لحاظ شود.

اگر نهاد گواهی‌کننده یک طرح ممیزی را طرح‌ریزی می‌کند که در آن، فعالیت‌های ممیزی راه‌دور بیش از ۳۰٪ زمان برنامه‌ریزی شده برای حضور در محل را تشکیل می‌دهد، توصیه می‌شود نهاد گواهی‌کننده طرح ممیزی را توجیه کرده و مجوزهای خاص را از نهاد تاییدصلاحیت پیش از اجرا اخذ نماید.

یادآوری ۲- منظور از زمان ممیز برای حضور در محل، زمانی است که ممیز برای بازدید از تک‌تک سایت‌ها در محل تخصیص می‌دهد. ممیزی‌های الکترونیکی سایت‌های راه‌دور، ممیزی‌های از راه‌دور لحاظ می‌شوند، حتی اگر ممیزی‌های الکترونیکی از نظر فیزیکی در محل سازمان انجام شود.

«زمان ممیز»، همان‌گونه که در جدول نیز به آن اشاره شده است، برحسب «روزهای ممیز» که در ممیزی صرف می‌شود بیان می‌شود. «روز ممیز» به طور معمول یک روز کاری عادی کامل است.

برای چرخه ممیزی اولیه صدورگواهی، توصیه می‌شود، زمان بازبینی یک سازمان متناسب با زمان صرف شده برای ممیزی اولیه آن به همراه مجموع زمان صرف شده سالیانه برای بازبینی باشد، که در حدود ۱/۳ زمان ممیزی اولیه است. توصیه می‌شود، زمان بازبینی طرح‌ریزی‌شده هر از چندگاهی، با در نظر گرفتن تغییرات سازمان، تکامل سیستم و غیره و دست‌کم در زمان ممیزی‌صدورگواهی‌مجدد، مورد بازنگری قرار گیرد.

کل زمان صرف شده برای اجرای ممیزی‌صدورگواهی‌مجدد به یافته‌های بازنگری، که در بند IS 9.1.6 این استاندارد و بند ۹-۴ از استاندارد ISO/IEC 17021 تعریف شده‌اند، بستگی خواهد داشت. توصیه می‌شود، زمان صرف شده در ممیزی‌صدورگواهی‌مجدد متناسب با زمان ممیزی اولیه صدورگواهی برای آن سازمان بوده و توصیه می‌شود، در حدود ۲/۳ زمانی باشد که برای ممیزی اولیه صدورگواهی همان سازمان مورد نیاز بوده است. زمان ممیزی‌صدورگواهی‌مجدد بیشتر و فراتر از زمان بازبینی معمولی است، ولی زمانی‌که ممیزی‌صدورگواهی‌مجدد انجام می‌شود و همزمان با آن باید برنامه زمان‌بندی بازدید معمول نظارتی انجام گیرد، ممیزی‌صدورگواهی‌مجدد برای پوشش الزامات بازبینی کفایت می‌کند. صرف‌نظر از نتیجه‌نهایی که بدست می آید، راهنمایی موجود در IS 9.1.2 بکار گرفته می‌شود.

زمانی‌که نقطه آغاز جهت تعیین زمان لازم ممیز، برای دامنه‌شمول معمول ISMS، با استفاده از تعداد کارکنان مشخص گردید؛ به‌علت تفاوتهایی که ممکن است زمانِ واقعیِ ممیز را برای اجرای ممیزی اثربخش در یک ISMS خاصِ موردممیزی، تحت تاثیر قرار دهد؛ علاوه بر آنهایی که در پ-۲ بیان شد، برخی اصلاحات دیگر نیز نیاز است تا در این زمان‌بندی لحاظ شوند.

از عوامل نمونه که به زمان ممیز بیشتری نیاز دارند، می‌توان به موارد زیر اشاره کرد:

- تدارکات پیچیده شامل قرارداشتن بیش از یک ساختمان یا مکان در دامنه‌شمول ISMS؛
- کارکنانی که به بیش از یک زبان صحبت می‌کنند (نیاز به مترجم وجود دارد یا مانع از فعالیت مستقل ممیزان می‌شود)؛
- مقررات سطح بالا؛
- ISMS، فرآیندهای بسیار پیچیده یا تعداد زیادی فعالیت‌های نسبتاً منحصر به فرد را در بر می‌گیرد؛
- فرآیندها، شامل تلفیقی از سخت افزار، نرم افزار، فرآیند و خدمت هستند؛
- فعالیت‌هایی که نیازمند بازدید از سایت‌های موقت برای تایید فعالیت‌های سایت‌های دائمی هستند که سیستم مدیریت‌شان موضوع گواهی است (یادآوری ۳ ملاحظه شود).

از عوامل نمونه که اجازه کاهش زمان ممیز را می دهند، می‌توان به موارد زیر اشاره کرد:

- فرآیندها/ محصول با ریسک کم/ بدون ریسک؛
- دانش قبلی از سازمان(برای مثال، در صورتیکه سازمان قبلاً از سوی همین نهاد گواهی‌کننده برای استاندارد دیگری گواهی اخذ کرده باشد)؛

- آمادگی مشتری برای صدور گواهی(برای مثال، قبلاً در برنامه شخص‌سوم دیگری گواهی اخذکرده‌است یا به‌رسمیت شناخته شده است.)؛
- فرآیندها شامل یک فعالیت عمومی واحد باشد.(برای‌مثال صرفاً خدمت)؛
- تکامل سیستم مدیریت در محل؛
- درصد بالایی از کارکنان اعمال ساده و یکسانی را انجام دهند.

یادآوری ۳- در مواقعی‌که مشتری‌گواهی یا سازمان‌دارنده‌گواهی، محصولات یا خدمت خودرا در سایت‌های‌موقت عرضه‌می‌کنند، مساله ارزشیابی چنین سایت‌هایی در برنامه‌های ممیزی‌صدورگواهی یا برنامه‌های بازبینی از اهمیت زیادی برخوردارمی‌شود.

سایت‌های موقت مکان‌هایی هستند به غیر از سایت‌ها یا مکان‌هایی که در مدرک صدورگواهی مشخص شده‌اند که در آنها فعالیت‌هایی، در حوزه دامنه‌شمول گواهی، در مدت زمانی تعیین‌شده انجام می‌پذیرد. گستره این سایت‌ها از سایت‌های مهم مدیریت پروژه گرفته تا سایت‌های کم اهمیت خدمات‌رسانی یا نصب می‌تواند تغییر کند. توصیه می‌شود، نیاز به بازدید این سایت‌ها و همچنین وسعت نمونه‌گیری‌ها، براساس ارزشیابی ریسک‌هایِ‌نقصِ یک محصول یا خدمت در برآورده‌سازی نیازها/ انتظارات به‌دلیل عدم‌انطباق‌سیستم، انجام شود. توصیه می‌شود، نمونه‌های انتخابی از سایت‌ها دربرگیرنده گستره تغییرات خدمات و نیازهای تکاملی سازمان بوده و ابعاد و نوع فعالیت‌ها و همچنین مراحل مختلف پروژه‌های در حال انجام را نیز لحاظ کند.

توصیه می‌شود تمامی مشخصه‌های دامنه‌شمول ISMS، فرآیندها و محصولات/ خدمات، درنظر گرفته شده، و یک تعدیل منصفانه برای آن عوامل اعمال شود، که می‌توانند کم‌وبیش، زمان ممیز برای یک ممیزی اثربخش را توجیه کنند. عوامل جمع‌شونده ممکن است خارج از محل[1] و به همراه عوامل کم‌شونده باشند. در تمامی مواردی که تغییرات در جدول زمان‌بندی ممیز انجام می‌شود، باید شواهد و سوابق کافی که این تغییرات را توجیه می‌کنند، حفظ و نگهداری شوند.

شکل‌زیر تعاملات‌بالقوه عوامل‌جمع‌شونده و کم‌شونده در زمان‌ممیز که درجدول بالا به آنها اشاره‌شد را نشان‌می‌دهد.

\- پیچیدگی سازمان/ سیستم +

بزرگ ساده	**بزرگ پیچیده**
چند سایتی	چند سایتی
تعداد کمی فرآیند(پردازش)	فرآیندهای زیاد
فرآیندهای تکراری	دامنه‌شمول بزرگ
دامنه‌شمول کوچک	فرآیندهای منحصر به فرد
	فرآیندها و محصولات با ریسک بالا

نقطه آغاز از جدول زمان ممیز

1- Off-site

تعداد کمی فرآیند دامنه‌شمول کوچک فرآیندهای تکراری **کوچک ساده**	فرآیندهای زیاد فرآیندها و محصولات با ریسک بالا دامنه‌شمول بزرگ فرآیندهای منحصر به فرد **کوچک پیچیده**

پراکندگی سازمان + ←

- ↕

پیوست
(اطلاعاتی)
راهنمایی برای بازنگری کنترل‌های پیاده‌سازی شده
از پیوست الف استاندارد ۲۷۰۰۱

۱- هدف

این پیوست راهنمایی را برای بازنگری پیاده‌سازی کنترل‌های لیست شده در پیوست الف استاندارد ۲۷۰۰۱، و جمع‌آوری شواهد ممیزی[1] از عملکرد آنها در حین ممیزی اولیه و بازدیدهای نظارتی بعدی بدست می‌دهد. لازم است، پیاده‌سازی تمام کنترل‌های انتخابی بوسیله سازمان مشتری برای ISMS (که در بیانیه کاربردپذیری به آنها اشاره شده است) در مرحله دوم ممیزی اولیه و در طول فعالیت‌های بازبینی یا صدور مجدد گواهی مورد بازنگری قرار گیرند.

شواهد ممیزی که نهاد گواهی‌کننده جمع‌آوری می‌کند باید به‌اندازه‌ای باشد که بتوان از آنها نتیجه‌گیری نهایی نمود که آیا کنترل‌های پیاده‌سازی شده اثربخش هستند یا خیر. اینکه از یک کنترل چه عملکردی انتظار می‌رود، در روش‌های اجرایی یا خط‌مشی‌های سازمان مشتری که در بیانیه کاربردپذیری بیان‌شده یا به آنها ارجاع داده شده است مشخص می‌شود. واضح است که آن دسته از کنترل‌هایی که در خارج از دامنه‌شمول ISMS قرار دارند، ممیزی نخواهند شد.

۱-۱ شواهد ممیزی

با کیفیت ترین شواهد ممیزی از طریق مشاهدات ممیز جمع‌آوری می‌شوند. (برای‌مثال، اینکه یک درِ قفل شده، قفل است، افراد توافقهای محرمانگی امضا می‌کنند، ثبت دارایی وجود دارد و شامل اموال رویت شده می‌شود، تنظیمات سیستم‌ها کافی هستند و غیره) . شواهد می‌توانند از طریق مشاهده نتایج اجرایی یک کنترل (برای‌مثال نسخه چاپی حقوق دسترسی داده شده به افراد، که بوسیله مراجع‌دارای‌اختیار امضا شده‌اند، سوابق رسیدگی به رخدادها، فرآیند مجوزدهی‌ها، که بوسیله مراجع‌دارای‌اختیار امضا شده‌اند، صورتجلسات جلسات مدیریتی یا جلسات دیگر)، بدست می آیند. شواهد همچنین می‌توانند نتیجه آزمون مستقیم(یا اجرایِ‌مجدد) کنترل‌ها بوسیله ممیز باشند (برای‌مثال تلاش برای انجام عملی که از نظر کنترل‌ها نباید انجام شود، تعیین اینکه آیا نرم افزاری برای محافظت در برابر کدهای مخرب روی دستگاه نصب شده و به روز است یا خیر، حقوق دسترسی اعطا شده است یا خیر (البته بعد از بررسی مراجع‌دارای‌اختیار) و غیره). شواهد را می‌توان از طریق مصاحبه با کارکنان/پیمانکاران درباره فرآیندها و کنترل‌ها و تعیین صحت و سقم آنها، جمع‌آوری کرد.

1- Audit evidence

۲- چگونگی استفاده از جدول د-۱

۲-۱ ستونهای «کنترل سازمانی» و «کنترل فنی»

علامت «×» در ستون متناظر نشانگر این مطلب است که کنترل مربوطه سازمانی یا فنی است. از آنجایی‌که برخی کنترل‌ها هم سازمانی و هم فنی هستند، این علامت در هردو ستون مربوط به آن کنترل درج شده است.

شواهد اجرایی کنترل‌های سازمانی می‌توانند از طریق بازنگری سوابق اجرایی کنترل‌ها، مصاحبه، مشاهده و بازرسی فیزیکی جمع‌آوری شوند. شواهد اجرایی کنترل‌های فنی می‌توانند از طریق آزمون سیستم (بند بعد ملاحظه شود) یا با استفاده از ابزار تخصصی ممیزی/ گزارش‌دهی جمع‌آوری شوند.

۲-۲ ستون « آزمون سیستم[1]»

«آزمون سیستم» به معنی بازنگری مستقیم سیستم است (برای‌مثال بازنگری تنظیمات سیستم یا پیکربندی). سوالات ممیز ممکن است در پایانه‌نمایش‌سیستم[2] یا از طریق ارزشیابی نتایج بدست آمده از ابزار آزمون پاسخ داده شود. اگر سازمان مشتری از ابزار رایانه‌ای استفاده می‌کند که برای ممیز شناخته شده است، این موضوع می‌تواند پشتیبان ممیزی باشد یا نتایج بدست آمده از ارزشیابی انجام شده بوسیله سازمان مشتری (یا پیمانکاران فرعی آن) می‌تواند بازنگری شود.

دو رده برای بازنگری کنترل‌های فنی وجود دارند:

امکان‌پذیر: آزمون سیستم برای ارزشیابی پیاده‌سازی کنترل امکان‌پذیر است ولی معمولا لازم نیست.

پیشنهادی: آزمون سیستم معمولا لازم است.

۲-۳ ستون «بازرسی چشمی»

«بازرسی چشمی» به این معنی است که این کنترل‌ها معمولا نیازمند بازرسی چشمی در محل برای ارزشیابی اثربخشی‌شان هستند این به‌این‌معنی است که بازنگری مستندات کاغذی مربوطه یا انجام مصاحبه‌ها به تنهایی کفایت نمی‌کند - ممیز نیاز دارد که کنترل را در محلی که پیاده‌سازی می‌شود، تصدیق کند.

۲-۴ ستون «راهنمایی بازنگری ممیزی»

در جایی‌که امکان دارد وجود راهنمایی برای ممیزی یک کنترل مشخص راهگشا باشد، ستون «توضیحات» حوزه تمرکز برای ارزشیابی آن کنترل را به عنوان راهنمایی بیشتر برای ممیز بدست می‌دهد.

1- System testing
2- System console

جدول د-۱- طبقه‌بندی کنترل‌ها

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۵ خط‌مشی امنیتی					
الف-۵-۱ خط‌مشی امنیتی					
الف-۵-۱- ۱ مدرک خط‌مشی امنیت اطلاعات	×				
الف-۵-۱-۲ بازنگری خط‌مشی امنیت اطلاعات	×				صورتجلسه های بازنگری مدیریت.
الف-۶ سازمان امنیت اطلاعات					
الف-۶-۱ سازمان داخلی					
الف-۶-۱-۱ تعهد مدیریت به امنیت اطلاعات	×				صورتجلسه های جلسات مدیریت
الف-۶-۱-۲ هماهنگی امنیت اطلاعات	×				صورتجلسه های جلسات مدیریت.
الف-۶-۱-۳ تخصیص مسوولیتهای امنیت اطلاعات	×				
الف-۶-۱-۴ فرایند مجوزدهی برای امکانات پردازش اطلاعات	×				
الف-۶-۱-۵ توافق‌نامه‌های محرمانگی	×				چند کپی از فایل‌ها به عنوان نمونه برداشته شود.
الف-۶-۱-۶ برقراری ارتباط‌با مراجع‌دارای‌اختیار	×				
الف-۶-۱-۷ برقراری ارتباط با گروههای بامنافع خاص	×				
الف-۶-۱-۸ بازنگری مستقل امنیت اطلاعات	×				گزارشات خوانده شود
الف-۶-۲ اشخاص بیرونی					
الف-۶-۲-۱ شناسایی ریسک‌ها مرتبط با اشخاص بیرونی	×				
الف-۶-۲-۲ نشانی دهی امنیت هنگام سرو کار داشتن با مشتریان	×				
الف-۶-۲-۳ نشانی‌دهی امنیت در توافق‌های شخص‌سوم	×				برخی از شرایط قراردادها آزمون شود.
الف-۷ مدیریت دارایی					
الف-۷-۱ مسوولیت داراییها					
الف-۷-۱-۱ سیاهه اموال	×				دارایی‌ها شناسایی شوند
الف-۷-۱-۲ مالکیت داراییها	×				
الف-۷-۱-۳ استفاده پسندیده از داراییها	×				
الف-۷-۲ طبقه بندی اطلاعات					
الف-۷-۲-۱ راهنمایی‌های طبقه بندی	×				
الف-۷-۲-۲ برچسب‌گذاری و اداره‌کردن‌اطلاعات	×				نام‌گذاری: دایرکتوریها، فایل‌ها، گزارشات چاپ شده، رسانه های ضبط شده(برای‌مثال نوارها، دیسکها و لوحهای فشرده)، پیامهای الکترونیکی و انتقال فایل‌ها.

جدول د-۱- ادامه

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۸ امنیت منابع انسانی					چند فایل منابع انسانی به‌عنوان نمونه برداشته شود.
الف-۸-۱ پیش از اشتغال					
الف-۸-۱-۱ نقش‌ها و مسوولیتها	×				
الف-۸-۱-۲ گزینش	×				
الف-۸-۱-۳ ضوابط و شرایط استخدام	×				
الف-۸-۲ حین خدمت					
الف-۸-۲-۱ مسوولیتهای مدیریت	×				
الف-۸-۲-۲ آگاهی رسانی، تحصیل و آموزش امنیت اطلاعات	×				پرسش ازکارکنان مبنی‌براینکه آیا از مواردی‌مشخصی که توصیه‌می‌شود آگاه‌باشند، مطلع‌هستند یا خیر.
الف-۸-۲-۳ فرآیند انضباطی	×				
الف-۸-۳ خاتمه استخدام یا تغییر در شغل					
الف-۸-۳-۱ مسوولیتهای خاتمه خدمت	×				
الف-۸-۳-۲ عودت دارایی‌ها	×				
الف-۸-۳-۳ حذف حقوق دسترسی	×	×	پیشنهادی		
الف-۹ امنیت فیزیکی و محیطی					
الف-۹-۱ نواحی امن					
الف-۹-۱-۱حصار امنیت فیزیکی	×				
الف-۹-۱-۲ کنترل‌های مداخل فیزیکی	×	×	امکان‌پذیر	×	آرشیو کردن سوابق دسترسی
الف-۹-۱-۳ ایمن سازی دفاتر،اتاقها وامکانات	×			×	
الف-۹-۱-۴ محافظت در برابر تهدید های بیرونی و محیطی	×			×	
الف-۹-۱-۵ کار در نواحی امن	×			×	
الف-۹-۱-۶ دسترسی عمومی، نواحی تحویل و بارگیری	×			×	
الف-۹-۲ امنیت تجهیزات					
الف-۹-۲-۱ استقرار و حفاظت تجهیزات	×	×	امکان‌پذیر	×	
الف-۹-۲-۲ امکانات پشتیبانی	×	×	امکان‌پذیر	×	
الف-۹-۲-۳ امنیت کابل کشی	×			×	
الف-۹-۲-۴ نگهداری تجهیزات	×				
الف-۹-۲-۵ امنیت تجهیزات خارج از ابنیه	×	×	امکان‌پذیر		رمزنگاری وسایل قابل حمل
الف-۹-۲-۶ امحاء یا استفاده مجدد از تجهیزات به صورت ایمن	×	×	امکان‌پذیر	×	
الف-۹-۲-۷ از رده خارج‌کردن دارائی	×				
الف-۱۰ مدیریت ارتباطات و عملکرد					
الف-۱۰-۱ روش‌های‌اجرایی‌عملیاتی‌ومسوولیت‌ها					

جدول د-۱- ادامه

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۱۰-۱-۱روش‌های اجرایی عملیاتی مستندشده	×				
الف-۱۰-۱-۲ مدیریت تغییر	×	×	پیشنهادی		
الف-۱۰-۱-۳ تفکیک وظایف	×				
الف-۱۰-۱-۴ جداسازی امکانات بهبود، آزمون و عملیاتی	×	×	امکان‌پذیر		
الف-۱۰-۲ مدیریت تحویل خدمت شخص‌سوم					
الف-۱۰-۲-۱ تحویل خدمت	×				
الف-۱۰-۲-۲ پایش و بازنگری خدمات شخص‌سوم	×	×	امکان‌پذیر		
الف-۱۰-۲-۳ مدیریت تغییرات در خدمات شخص‌سوم	×				
الف-۱۰-۳ طرح‌ریزی و پذیرش سیستم					
الف-۱۰-۳-۱ مدیریت ظرفیت	×	×	امکان‌پذیر		
الف-۱۰-۳-۲ پذیرش سیستم	×				
الف-۱۰-۴ حفاظت در برابر کدهای مخرب‌وسیار					
الف-۱۰-۴-۱ کنترل‌هایی در برابر کدهای‌مخرب	×	×	پیشنهادی		چند نمونه از سرورها، رایانه ها و دروازه های ورود.
الف-۱۰-۴-۲ کنترل‌هایی در برابر کدهای سیار	×	×	امکان‌پذیر		
الف-۱۰-۵ نسخ پشتیبان					
الف-۱۰-۵-۱ ایجاد پشتیبان از اطلاعات	×	×	پیشنهادی		یک بار اطلاعات را بازگردانی کنید.
الف-۱۰-۶ مدیریت امنیت شبکه					
الف-۱۰-۶-۱ کنترل های شبکه	×	×	امکان‌پذیر		
الف-۱۰-۶-۲ امنیت خدمات شبکه	×				خصوصیات امنیتی، SLA ها[1]
الف-۱۰-۷ اداره کرده محیط های ذخیره سازی					
الف-۱۰-۷-۱ مدیریت محیط های ذخیره سازی قابل جابجایی	×	×	امکان‌پذیر		
الف-۱۰-۷-۲ امحای محیط های ذخیره سازی	×				
الف-۱۰-۷-۳ روش‌های‌اجرایی جابجایی‌اطلاعات	×				
الف-۱۰-۷-۴ امنیت مستندات سیستم	×	×	امکان‌پذیر	×	
الف-۱۰-۸ تبادل اطلاعات					
الف-۱۰-۸-۱ خط‌مشی ها و روش‌های اجرایی تبادل اطلاعات	×				
الف-۱۰-۸-۲ توافق‌نامه‌های تبادل	×				

1- Service Level Agreements

توافق‌نامه‌های سطح خدمات

جدول د-۱- ادامه

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۱۰-۸-۳ محیط های ذخیره سازی(رسانه) فیزیکی، حین حمل و نقل	×	×	امکان‌پذیر		حفاظتهای فیزیکی یا رمزنگاری
الف-۱۰-۸-۴ پیام رسانی الکترونیکی	×	×	امکان‌پذیر		تطابق پیامهای نمونه با خط‌مشی/ روش‌های اجرایی تایید شود.
الف-۱۰-۸-۵ سیستم‌های اطلاعاتی کسب‌وکار	×				
الف-۱۰-۹ خدمات تجارت الکترونیک					
الف-۱۰-۹-۱ تجارت الکترونیک	×	×	امکان‌پذیر		
الف-۱۰-۹-۲ تراکنش‌های برخط (متصل و مستقیم)	×	×	پیشنهادی		تمامیت و مجوزهای دسترسی بررسی شوند.
الف-۱۰-۹-۳ اطلاعات قابل‌دسترس عموم	×	×	امکان‌پذیر		
الف-۱۰-۱۰ پایش					
الف-۱۰-۱۰-۱ واقعه نگاری ممیزی	×	×	امکان‌پذیر		برخط یا چاپی
الف-۱۰-۱۰-۲ پایش کاربرد سیستم	×	×	امکان‌پذیر		
الف-۱۰-۱۰-۳ حفاظت‌از اطلاعات‌ثبت‌شده‌وقایع	×	×	امکان‌پذیر		
الف-۱۰-۱۰-۴ اطلاعات ثبت‌شده وقایع مربوط‌به متولی سیستم[1] و کاربر	×	×	امکان‌پذیر		
الف-۱۰-۱۰-۵ واقعه نگاری خرابی	×				
الف-۱۰-۱۰-۶ هم زمان سازی ساعتها		×	امکان‌پذیر		
الف-۱۱ کنترل دسترسی					
الف-۱۱-۱ الزامات کسب‌وکار برای کنترل دسترسی					
الف-۱۱-۱-۱ خط‌مشی کنترل دسترسی	×				
الف-۱۱-۲ مدیریت دسترسی کاربر					
الف-۱۱-۲-۱ ثبت کاربر	×				نمونه‌هایی از حقوق دسترسی[2] کارکنان و پیمانکاران به تمامی سیستم‌ها بررسی شود.
الف-۱۱-۲-۲ مدیریت اختیارات ویژه	×	×	امکان‌پذیر		انتقال داخلی کارکنان
الف-۱۱-۲-۳ مدیریت کلمه عبور کاربر	×				
الف-۱۱-۲-۴ بازنگری حقوق دسترسی کاربر	×				
الف-۱۱-۳ مسوولیتهای کاربر					
الف-۱۱-۳-۱ استفاده از کلمه عبور	×				تصدیق خط‌مشی/راهنمایی‌ها در محل کاربران
الف-۱۱-۳-۲ تجهیزات بدون مراقبت کاربر	×				تصدیق خط‌مشی/راهنمایی‌ها در محل کاربران
الف-۱۱-۳-۳ خط‌مشی میز پاک و صفحه پاک	×			×	

1- Administrator
2- Access Rights

جدول د-۱- ادامه

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۱۱-۴ کنترل دسترسی به شبکه					
الف-۱۱-۴-۱ خط‌مشی استفاده از خدمات شبکه	×				
الف-۱۱-۴-۲ احراز اصالت کاربر برای اتصالات بیرونی	×	×	پیشنهادی		
الف-۱۱-۴-۳ شناسایی تجهیزات در شبکه ها	×	×			
الف-۱۱-۴-۴ حفاظت از درگاه عیب یابی و پیکربندی راه‌دور	×	×	پیشنهادی		
الف-۱۱-۴-۵ تفکیک در شبکه ها	×	×	امکان‌پذیر		دیاگرام‌های شبکه: WAN,LAN, VLAN, VPN, بخش‌های شبکه، اشیاء شبکه (برای‌مثال DMZ)
الف-۱۱-۴-۶ کنترل اتصال به شبکه	×	×	پیشنهادی		شبکه‌های مشترک زیاد معمول نیست.
الف-۱۱-۴-۷ کنترل مسیریابی در شبکه	×	×	پیشنهادی		دیوارهای‌آتش،سوییچ‌ها/مسیریاب‌ها: براساس قاعده، لیست کنترل دسترسی، خط‌مشی های کنترل دسترسی
الف-۱۱-۵ کنترل دسترسی به سیستم عامل					
الف-۱۱-۵-۱روش‌های اجرایی ورود امن به سیستم	×	×	پیشنهادی		
الف-۱۱-۵-۲ شناسایی و احراز اصالت کاربر	×	×	پیشنهادی		
الف-۱۱-۵-۳ سیستم مدیریت کلمه عبور	×	×	پیشنهادی		
الف-۱۱-۵-۴ استفاده از برنامه‌های کمکی سیستم	×	×	پیشنهادی		
الف-۱۱-۵-۵ خروج زمانی از لایه ارتباطی	×	×	امکان‌پذیر		
الف-۱۱-۵-۶ محدود سازی زمان اتصال	×	×	امکان‌پذیر		
الف-۱۱-۶ کنترل دسترسی به برنامه‌های کاربردی و اطلاعات					
الف-۱۱-۶-۱ محدودیت دسترسی به اطلاعات	×	×	پیشنهادی		
الف-۱۱-۶-۲ جداسازی سیستم‌های حساس	×	×	امکان‌پذیر		
الف-۱۱-۷ محاسبه سیار و کار از راه‌دور					
الف-۱۱-۷-۱ محاسبه و ارتباطات سیار	×	×	امکان‌پذیر		
الف-۱۱-۷-۲ کار از راه‌دور	×	×	امکان‌پذیر		
الف-۱۲ اکتساب، بهبود و نگهداری سیستم‌های اطلاعاتی					
الف-۱۲-۱ الزامات امنیتی سیستم‌های اطلاعاتی					

جدول د-۱- ادامه

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۱۲-۱-۱ مشخصات و تحلیل الزامات امنیتی	×				
الف-۱۲-۲ پردازش صحیح در برنامه‌های کاربردی					
الف-۱۲-۲-۱ صحه‌گذاری داده[1] ورودی	×	×	پیشنهادی		راهنمایی‌های بهبود نرم افزاری، آزمون نرم افزار؛ در برنامه‌های نمونه کاربردی کسب‌وکار تایید می‌کند که کنترل‌های الزامی کاربران در عمل وجود دارند.
الف-۱۲-۲-۲ کنترل پردازش درونی	×	×	امکان‌پذیر		راهنمایی‌های بهبود نرم افزاری، آزمون نرم افزار؛ در برنامه‌های نمونه کاربردی کسب‌وکار تایید می‌کند که کنترل‌های الزامی کاربران در عمل وجود دارند.
الف-۱۲-۲-۳ تمامیت پیغام		×	امکان‌پذیر		
الف-۱۲-۲-۴ صحه‌گذاری داده خروجی	×	×	امکان‌پذیر		راهنمایی‌های بهبود نرم افزاری، آزمون نرم افزار؛ در برنامه‌های نمونه کاربردی کسب‌وکار تایید می‌کند که کنترل‌های الزامی کاربران در عمل وجود دارند.
الف-۱۲-۳ کنترل‌های رمزنگاری					
الف-۱۲-۳-۱خط‌مشی استفاده از کنترل‌های رمزنگاری	×	×	امکان‌پذیر		همچنین پیاده‌سازی خط‌مشی در موارد مقتضی بررسی شوند.
الف-۱۲-۳-۲ مدیریت کلید	×	×	پیشنهادی		
الف-۱۲-۴ امنیت فایل‌های سیستم					
الف-۱۲-۴-۱ کنترل نرم افزار عملیاتی	×	×	امکان‌پذیر		
الف-۱۲-۴-۲حفاظت از داده‌های آزمون سیستم	×	×	امکان‌پذیر	×	
الف-۱۲-۴-۳ کنترل دسترسی به کدمنبع برنامه	×	×	پیشنهادی		
الف-۱۲-۵ امنیت در فرایندهای بهبود و پشتیبانی					
الف-۱۲-۵-۱ روش‌های اجرایی کنترل تغییر	×				
الف-۱۲-۵-۲ بازنگری فنی نرم افزارهای کاربردی پس از تغییرات سیستم عامل	×				

1- Validation

جدول د-۱- ادامه

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۱۲-۵-۳ محدود سازی در اعمال تغییرات در بسته های نرم افزاری	×				
الف-۱۲-۵-۴ نشت اطلاعات	×	×	امکان‌پذیر		خدمات نا شناخته
الف-۱۲-۵-۵ بهبود نرم افزار برون‌سپاری‌شده	×				
الف-۱۲-۶ مدیریت آسیب پذیری فنی					
الف-۱۲-۶-۱ کنترل آسیب پذیرهای فنی	×	×	پیشنهادی		توزیع وصله های نرم افزاری
الف-۱۳ مدیریت رخدادهای امنیت اطلاعات					
الف-۱۳-۱ گزارش دهی وقایع و ضعفهای امنیت اطلاعات					
الف-۱۳-۱-۱گزارش دهی وقایع امنیت اطلاعات	×				
الف-۱۳-۱-۲ گزارش دهی ضعفهای امنیتی	×				
الف-۱۳-۲ مدیریت رخدادها و بهبودهای امنیت اطلاعات					
الف-۱۳-۲-۱ مسوولیتها و روش‌های اجرایی	×				
الف-۱۳-۲-۲یادگیری‌ازرخدادهای‌امنیت‌اطلاعات	×				
الف-۱۳-۲-۳-گرد آوری شواهد	×				
الف-۱۴ مدیریت استمرار کسب‌وکار					
الف-۱۴-۱ جنبه های امنیت اطلاعات مدیریت استمرار کسب‌وکار					صورتجلسه های بازنگری مدیریت.
الف-۱۴-۱-۱ لحاظ کردن امنیت اطلاعات در فرایند مدیریت استمرار کسب‌وکار	×				
الف-۱۴-۱-۲ استمرار کسب‌وکار و ارزیابی‌ریسک	×				
الف-۱۴-۱-۳ ایجاد و پیاده سازی طرح‌های استمرار در برگیرنده امنیت اطلاعات	×	×	امکان‌پذیر	×	بررسی سایت‌های بازیابی در مواقع بحران، فاصله این سایت‌ها براساس ارزیابی‌ریسک و الزامات قانونی و مقرراتی
الف-۱۴-۱-۴ چارچوب طرح‌ریزی استمرار کسب‌وکار	×				
الف-۱۴-۱-۵ حفظ‌ونگهداری آزمون و ارزیابی مجدد طرح های استمرار کسب‌وکار	×				
الف-۱۵ انطباق					
الف-۱۵-۱ انطباق با الزامات قانونی					
الف-۱۵-۱-۱ شناسایی قوانین قابل اجرا	×				
الف-۱۵-۱-۲ حقوق مالکیت معنوی[1]	×				
الف-۱۵-۱-۳ حفاظت از سوابق سازمانی	×	×	امکان‌پذیر		

1- Intellectual Property Rights (IPR)

جدول د-۱- ادامه

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۱۵-۱-۴ حفاظت داده‌ها و حریم خصوصی اطلاعات شخصی	×	×	امکان‌پذیر		
الف-۱۵-۱-۵ پیشگیری از استفاده نابجا از امکانات پردازش اطلاعات	×				
الف-۱۵-۱-۶ قواعد کنترل‌های رمزنگاری	×				
الف-۱۵-۲ انطباق با خط‌مشی‌ها و استانداردهای امنیتی، و انطباق فنی					
الف-۱۵-۲-۱ انطباق خط‌مشی ها واستانداردهای امنیتی	×				
الف-۱۵-۲-۲ بررسی انطباق فنی	×	×	امکان‌پذیر		فرآیند ارزیابی و پیگیری
الف-۱۵-۳ ملاحظات ممیزی سیستم‌های اطلاعاتی					
الف-۱۵-۳-۱ کنترل‌های ممیزی سیستم‌های اطلاعاتی	×				
الف-۱۵-۳-۲ حفاظت از ابزارهای ممیزی سیستم‌های اطلاعاتی	×	×	امکان‌پذیر		

فصل هشتم

فناوری اطلاعات – فنون امنیتی– راهنماهایی برای ممیزی سامانه های مدیریت امنیت اطلاعات

ISO/IEC 27007

Information technology-- Security techniques

Guidelines for information security management systems auditing

پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- راهنماهایی برای ممیزی سامانه‌های مدیریت امنیت اطلاعات» که پیش نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده و در یکصد و نود وششمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده مورخ ۹۱/۶/۲۰ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

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

ISO/IEC 27007: 2011, Information technology — Security techniques — Guidelines for information security management systems auditing

- **مقدمه**

این استاندارد ملی راهنمایی بر مدیریت برنامه ممیزی سامانه مدیریت امنیت اطلاعات (ISMS)[1] و راهبری ممیزی‌های داخلی یا خارجی مطابق با استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ ارائه می‌دهد، همچنین راهنمایی درمورد شایستگی و ارزیابی ممیزان ISMS که باید به همراه راهنمایی موجود در استاندارد ISO 19011 استفاده شود را فراهم می‌کند. این استاندارد به بیان الزامات نمی‌پردازد.

این راهنما برای تمام کاربران اعم از سازمان‌هایی با اندازه کوچک و متوسط در نظر گرفته شده است.

استاندارد ISO 19011 (راهنماهایی برای ممیزی سامانه‌های مدیریت)، راهنمایی بر مدیریت برنامه‌های ممیزی، راهبری ممیزی‌های خارجی یا داخلی سامانه‌های مدیریت، همچنین شایستگی و ارزیابی ممیزان سامانه مدیریت را فراهم می‌کند.

متن این استاندارد ملی، از ساختار استاندارد ISO 19011 پیروی می‌کند و راهنمایی اضافی خاص ISMS در کاربرد استاندارد ISO 19011 برای ممیزی ISMS با حروف IS نشان داده می‌شود.

1- Information Security Management System

فناوری اطلاعات – فنون امنیتی – راهنماهایی برای ممیزی سامانه‌های مدیریت امنیت اطلاعات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ارائه راهنمایی‌هایی در مورد راهبری برنامه ممیزی سامانه مدیریت امنیت اطلاعات (ISMS)، هدایت ممیزی‌ها و شایستگی ممیزان ISMS است که علاوه بر راهنماهای موجود در استاندارد ISO 19011 است.

این استاندارد ملی برای آن‌هایی که به درک یا راهبری ممیزی‌های داخلی یا خارجی ISMS یا مدیریت برنامه ممیزی ISMS نیاز دارند، کاربردپذیر است.

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 می‌شود.

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 الزامی‌است:

2-1 ISO 19011:2011, Guidelines for auditing management systems

۲-۲ استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سیستم‌های مدیریت امنیت اطلاعات -- الزامات

۲-۳ استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۱، فناوری اطلاعات – فنون امنیتی – سامانه‌های مدیریت امنیت اطلاعات – مرورکلی و واژگان

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف ارائه شده در استاندارد ISO 19011 و استاندارد ISO/IEC 27000 به کار می‌رود.

۴ اصول ممیزی

اصول ممیزی از استاندارد ISO 19011:2011، بند ۴، به کار گرفته می‌شود.

۵ مدیریت کردن برنامه ممیزی

۵-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۵-۱ اعمال می‌شود. علاوه بر آن راهنمای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۵-۱-۱ IS [1] ۵-۱ کلیات

برنامه ممیزی[2] ISMS باید بر اساس وضعیت مخاطره امنیت اطلاعات ممیزی‌شونده توسعه داده شود.

۵-۲ پایه‌گذاری[3] اهداف برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۲ اعمال می‌شود. علاوه بر آن راهنمای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۵-۲-۱ IS ۵-۲ پایه‌گذاری اهداف برنامه ممیزی

اهداف برنامه (های) ممیزی باید به منظور هدایت طرح‌ریزی و راهبری ممیزی و اطمینان از اینکه برنامه ممیزی به طور موثر اجرا می‌شود، پایه‌گذاری شود. این اهداف می‌تواند به موارد زیر وابسته باشد.

الف- الزامات امنیت اطلاعات شناسایی شده؛

ب- الزامات استاندارد ISO/IEC 27001؛

پ- سطح عملکرد ممیزی‌شونده همان طور که در وقوع نقائص امنیت اطلاعات، رخدادها و سنجش‌های اثربخشی‌منعکس شده است؛ و

ت- مخاطرات امنیت اطلاعات برای سازمان در حال ممیزی.

نمونه‌هایی از اهداف برنامه ممیزی ممکن است شامل موارد زیر باشد:

۱- درستی‌سنجی تطابق با الزامات قراردادی و قانونی و سایر الزامات و مفهوم[4] امنیت آن‌ها.

۲- دستیابی و حفظ اعتماد در رابطه با توانایی مدیریت مخاطرات ممیزی‌شونده.

۵-۳ پایه‌گذاری برنامه ممیزی

۵-۳-۱ نقش و مسئولیت‌های مدیر برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۳-۱ به کار گرفته می‌شود.

۵-۳-۲ شایستگی مدیر برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۳-۲ به کار گرفته می‌شود.

1- Information security

۲- در این استاندارد، هر زمان که از اصطلاح «ممیزی» استفاده شد، منظور ممیزی ISMS است.

3- Establish

4- Implication

۵-۳-۳ تعیین گستره برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۳-۳ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۵-۳-۳-۱ IS ۵-۳-۳ تعیین گستره برنامه ممیزی

گستره هر برنامه ممیزی می‌تواند متفاوت باشد. عواملی که می‌تواند بر گستره برنامه ممیزی تاثیر بگذارد، عبارتند از:

الف- اندازه ISMS ، شامل:

۱- تعداد کل کارکنان مشغول به کار در هر مکان و روابط با پیمانکاران طرف سوم که به طور منظم در محلی که باید ممیزی شود کار می‌کنند؛

۲- تعداد سامانه‌های اطلاعاتی؛

۳- تعداد پایگاه‌های[1] پوشش داده شده با ISMS.

ب- پیچیدگی ISMS (شامل تعداد و حساسیت فرآیندها و فعالیت‌ها)

پ- اهمیت مخاطرات امنیت اطلاعات شناسایی شده برای ISMS؛

ت- اهمیت اطلاعات و دارایی‌های وابسته در محدوده ISMS؛

ث- پیچیدگی سامانه‌های اطلاعاتی موجود که باید مورد ممیزی قرار گیرند، شامل پیچیدگی فناوری اطلاعات پیاده‌سازی شده؛

ج- وجود پایگاه‌های مشابه متعدد؛ و

چ- تفاوت در پیچیدگیISMS در گستره پایگاه‌های محدوده ممیزی.

ملاحظات باید در برنامه ممیزی به منظور تنظیم اولویت ها بر اساس مخاطرات امنیت اطلاعات والزامات کسب وکار در رابطه با حوزه‌های ISMS که تضمین کننده بررسی جزیی‌تر است، رعایت گردد.

اطلاعات بیشتر در مورد روش نمونه‌برداری چند پایگاهی می‌تواند در استاندارد ملی ایران شماره ۲۷۰۰۶: سال ۱۳۸۷ و IAF MD 1:2007 یافت شود (به کتابنامه مراجعه شود)، که اطلاعات این اسناد فقط مربوط به گواهی ممیزی‌ها است.

۵-۳-۴ شناسایی و ارزیابی مخاطرات برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۳-۴ به کار گرفته می‌شود.

۵-۳-۵ پایه‌گذاری روش‌های اجرایی برای برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۳-۵ به کار گرفته می‌شود.

۵-۳-۶ شناسایی منابع برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۳-۶ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

1- sites

۵-۳-۶-۱ IS ۵-۳-۶ شناسایی منابع برنامه ممیزی

به طور خاص، برای همه مخاطرات امکان پذیر برای ممیزی شونده ، باید به ممیزان برای تحقیق اثربخشی اقدام کاهش مخاطره مربوطه، زمان کافی تخصیص داده شود.

۵-۴ پیاده‌سازی برنامه ممیزی

۵-۴-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۵-۴-۱ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۵-۴-۱-۱ IS ۵-۴-۱ کلیات

هر جا که کاربردپذیر است، الزامات محرمانگی ممیزی‌شونده‌ها و سایر طرف‌های مربوطه، ازجمله الزامات قراردادی و قانونی ممکن باید در پیاده‌سازی برنامه ممیزی مشخص شوند.

۵-۴-۲ تعریف اهداف، محدوده و معیارهای یک ممیزی جداگانه

راهنماها از استاندارد ISO 19011:2011، بند ۵-۴-۲ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۵-۴-۲-۱ IS ۵-۴-۲ تعریف اهداف، محدوده و معیار برای ممیزی جداگانه

محدوده ممیزی باید مخاطرات امنیت اطلاعات ممیزی شونده، الزامات کسب وکار مربوطه و مخاطرات کسب وکار را منعکس کند.

به علاوه اهداف ممیزی ممکن است موارد زیر را دربرگیرد:

الف- ارزیابی این که آیا ISMS ، به طور مناسب الزامات امنیت اطلاعات را شناسایی و مشخص می‌کند؛

ب- ارزیابی مناسب بودن مداوم اهداف ISMS، تعریف شده توسط مدیریت؛ و

پ- ارزیابی فرآیندها برای نگهداری و بهبود موثر ISMS.

کمک‌های کاربردی- مثال‌هایی از معیارهای ممیزی

موضوعات زیر عناوینی هستند که به عنوان معیار ممیزی در نظر گرفته می‌شوند:

۱- روش ارزشیابی مخاطره امنیت اطلاعات ممیزی‌شونده و ارزشیابی مخاطره و نتایج برطرف‌سازی که این‌ها همه‌ی الزامات مرتبط را نشان می‌دهد؛

۲- نسخه‌ای از بیانیه کاربست پذیری و رابطه آن با نتایج حاصل از ارزشیابی مخاطره؛

۳- پیاده‌سازی موثر کنترل‌ها به منظور کاهش مخاطرات؛

۴- سنجش اثربخشی کنترل‌های پیاده‌سازی شده که این سنجش‌ها، مطابق تعریف اندازه‌گیری اثر بخشی کنترل‌ها به کار گرفته می شوند. (به ISO/IEC 27004[1] مراجعه کنید)؛

۵- فعالیت‌هایی برای پایش و بازنگری کنترل‌ها و فرایندهای ISMS؛

۶- ممیزی‌های داخلیISMS و بازنگری‌های مدیریت و اقدامات اصلاحی سازمان؛

۱- معادل استاندارد ISO/IEC 27004، استاندارد ملی ایران شماره ۱۴۰۹۶: سال ۱۳۸۹ موجود است.

۷- اطلاعاتی در مورد کفایت و تطابق با اهداف، خط‌مشی‌ها و روش‌های اجرایی اتخاذ شده به وسیله ممیزی شونده؛ و
۸- انطباق با الزامات قراردادی و قانونی خاص و سایر الزامات مربوط به ممیزی‌شونده و مفهوم امنیت اطلاعات آن‌ها.
تیم ممیزی باید از تعریف شفاف محدوده و قلمروهای ISMS ممیزی شونده بر مبنای ویژگی‌های کسب و کار، سازمان، مکان، دارایی‌ها و فناوری آن از جمله جزئیات و توجیه برای کنارگزاری هر چیزی از محدوده، اطمینان حاصل کند. تیم ممیزی باید تایید کند که ممیزی شونده، به الزامات بیان شده در بند ۱-۲ استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ در محدوده ISMS، توجه داشته است.
بنابراین ممیزان باید مطمئن شوند که فعالیت‌های ارزشیابی مخاطره امنیت اطلاعات و برطرف‌سازی مخاطرات ممیزی شونده به درستی منعکس شده‌اند و قلمروهای محدوده را پوشش می‌دهد. ممیزان باید تایید کنند که این موضوع در بیانیه کاربست پذیری منعکس شده است.
بنابراین ممیزان باید مطمئن شوند که واسط‌های مربوط به خدمات یا فعالیت‌هایی که به طور کامل در محدوده ISMS نیستند، در ISMS توجه شده است و در ارزیابی مخاطره امنیت اطلاعات ممیزی شونده وارد شده است. مثالی از چنین وضعیتی، به اشتراک‌گذاری تسهیلات (به عنوان مثال سامانه های فناوری اطلاعات، پایگاه‌های داده و سامانه‌های مخابراتی) با دیگر سازمان‌ها است.

۵-۴-۳ انتخاب روش‌های ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۴-۳ اعمال می‌شود. علاوه بر آن راهنمای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۵-۴-۳-۱ IS ۵-۴-۳ انتخاب روش‌های ممیزی

اگر ممیزی مشترک انجام شود، باید در خصوص عدم افشای اطلاعات در طول ممیزی توجه ویژه‌ای شود. قبل از آغاز ممیزی باید همه طرف‌های ذینفع بر سر این موضوع به توافق رسیده باشند.

۵-۴-۴ انتخاب اعضای تیم ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۴-۴ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۵-۴-۴-۱ IS ۵-۴-۴ انتخاب اعضای تیم ممیزی

شایستگی تیم ممیزی روی هم رفته باید موارد زیر را شامل شود:
الف- دانش و درک کافی از مدیریت مخاطرات امنیت اطلاعات که برای ارزیابی روش‌های استفاده شده توسط ممیزی شونده کفایت نماید؛ و
ب- دانش و درک کافی از امنیت اطلاعات و مدیریت امنیت اطلاعات که برای ارزیابی انتخاب کنترل و طرح‌ریزی، پیاده‌سازی، نگهداری واثر بخشی ISMS کفایت نماید.
در جایی که لازم است، باید دقت شود که ممیزان مجوز لازم برای دسترسی به شواهد ممیزی را بدست آورده‌اند.

۵-۴-۵ اختصاص مسئولیت برای ممیزی جداگانه به رهبر تیم ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۴-۵ به کار گرفته می‌شود.

۵-۴-۶ مدیریت دستاورد برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۴-۶ به کار گرفته می‌شود.

۵-۴-۷ مدیریت و نگهداری سوابق برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۴-۷ به کار گرفته می‌شود.

۵-۵ پایش برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۵ به کار گرفته می‌شود.

۵-۶ بازنگری و بهبود برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۶ به کار گرفته می‌شود.

۶ اجرای ممیزی

۶-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۶-۱ به کار گرفته می‌شود.

۶-۲ راه‌اندازی ممیزی

۶-۲-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۶-۲-۱ به کار گرفته می‌شود.

۶-۲-۲ برقرارکردن تماس اولیه با ممیزی‌شونده

راهنماها از استاندارد ISO 19011:2011، بند ۶-۲-۲ به کار گرفته می‌شود.

۶-۲-۳ تعیین امکان‌سنجی[1] ممیزی

راهنماها از استاندارد ISO 19011:2011، بند۶-۲-۳ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۶-۲-۳-۱ IS ۶-۲-۳ تعیین امکان‌سنجی ممیزی

قبل از شروع ممیزی، باید از ممیزی شونده پرسیده شود، که آیا سوابق ISMS برای بازنگری توسط تیم ممیزی در دسترس نیست، به عنوان مثال به دلیل اینکه آن‌ها شامل اطلاعات حساس و محرمانه است. شخص مسئول مدیریت برنامه ممیزی، باید تعیین کند که آیا ISMS می‌تواند در صورت نبود این سوابق به طور مناسب بررسی شود. اگر نتیجه این است که ممکن نیست که ، ISMS بدون بازنگری سوابق مشخص شده، به طور مناسب ممیزی شود، شخص باید ممیزی‌شونده را آگاه کند که امکان ممیزی تا

1- Feasibility

تضمین شدن مقدمات دسترسی مناسب وجود ندارد و راه‌کار جایگزین می‌تواند به/توسط ممیزی‌شونده پیشنهاد شود.

۶-۳ آماده‌سازی فعالیت‌های ممیزی

۶-۳-۱ اجرای سند خوانی[1] به منظور آماده‌سازی برای ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۳-۱ به کار گرفته می‌شود.

۶-۳-۲ آماده سازی طرح ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۳-۲ به کار گرفته می‌شود.

۶-۳-۳ اختصاص کار به تیم ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۳-۳ به کار گرفته می‌شود.

۶-۳-۴ آماده سازی اسناد کاری

راهنماها از استاندارد ISO 19011:2011، بند ۶-۳-۴ به کار گرفته می‌شود.

۶-۴ هدایت فعالیت‌های ممیزی

۶-۴-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۱ به کار گرفته می‌شود.

۶-۴-۲ برگزاری جلسه افتتاحیه[2]

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۲ به کار گرفته می‌شود.

۶-۴-۳ انجام سند خوانی در هنگام هدایت ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۳ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۶-۴-۳-۱ IS ۶-۴-۳ انجام سند خوانی در هنگام ممیزی

ممیزان باید وارسی کنند که اسناد مورد نیاز استاندارد ISO/IEC 27001 وجود دارد و مطابق با الزامات آن است.

ممیزان باید تایید کنند که کنترل‌های انتخاب شده مربوط به نتایج ارزشیابی مخاطره و فرایند برطرف‌سازی مخاطره است و در نتیجه قابل ردیابی در خط‌مشی و اهداف ISMS است.

یادآوری- پیوست الف این استاندارد راهنمایی در مورد چگونگی ممیزی فرایندها و مستندات ISMS ارائه می‌کند.

۶-۴-۴ تبادل اطلاعات[3] در حین ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۴ به کار گرفته می‌شود.

1- Document review
2- Opening meeting
3- Communicating

۶-۴-۵ اختصاص نقش‌ها و مسئولیت‌های راهنماها و ناظران[1]

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۵ به کار گرفته می‌شود.

۶-۴-۶ جمع آوری و درستی‌سنجی[2] **اطلاعات**

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۶ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۶-۴-۶-۱ IS ۶-۴-۶ گرد آوری و درستی‌سنجی اطلاعات

گردآوری اطلاعات و شواهد که نشان‌دهنده‌ی آن است که فرایندها و کنترل های ISMS پیاده‌سازی شده و قابل اجرا است، بخش مهمی از ممیزی ISMS است. روش‌های ممکن برای جمع آوری اطلاعات مربوطه در طول ممیزی عبارتند از:

الف) بازنگری دارایی‌های اطلاعاتی و فرایندهای ISMS و کنترل‌های پیاده‌سازی شده برای آن‌ها؛ و

ب) استفاده از ابزارهای خودکار ممیزی.

یادآوری- پیوست الف این استاندارد راهنمایی در مورد چگونگی ممیزی فرایندهای ISMS ارائه می‌کند.

ممیزان ISMS باید از اداره[3] مناسب همه‌ی اطلاعات دریافت شده از ممیزی‌شوندگان بر طبق توافق بین ممیزی‌شونده و تیم ممیزی اطمینان حاصل کنند.

۶-۴-۷ ایجاد یافته‌های ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۷ به کار گرفته می‌شود.

۶-۴-۸ آماده‌کردن نتایج ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۸ به کار گرفته می‌شود.

۶-۴-۹ برگزاری جلسه اختتامیه

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۹ به کار گرفته می‌شود.

۶-۵ آماده سازی و توزیع گزارش ممیزی

۶-۵-۱ آماده سازی گزارش ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۵-۱ به کار گرفته می‌شود.

۶-۵-۲ توزیع گزارش ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۵-۲ به کار گرفته می‌شود.

۶-۶ اتمام ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۶ به کار گرفته می‌شود.

1- Observer
2- Verify
3- Handling

۷-۶ انجام اقدامات پیگیری بعد از ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۷ به کار گرفته می‌شود.

۷ شایستگی و ارزیابی ممیزان

۷-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۷-۱ به کار گرفته می‌شود.

۷-۲ تعیین شایستگی ممیز به منظور رفع نیازهای برنامه ممیزی

۷-۲-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۱ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۷-۲-۱-۱ IS ۷-۲-۱ کلیات

در گزینش دانش و شایستگی‌های مناسب، موارد زیر باید در نظر گرفته شود:

الف- پیچیدگی ISMS (به عنوان مثال، حیاتی‌بودن[1] سامانه‌های اطلاعاتی، وضعیت مخاطره ISMS)

ب- ماهیت(های) کسب و کاری که در محدوده ISMS انجام شده است.

پ- وسعت و تنوع[2] فناوری مورد استفاده در پیاده‌سازی مولفه‌های مختلف ISMS (مانند کنترل‌های پیاده‌سازی شده، مستندات و/یا کنترل فرایند، اقدامات اصلاحی/پیشگیرانه و غیره)؛

ت- تعداد پایگاه‌ها؛

ث- کارایی نشان داده شده[3] قبلی ISMS؛

ج- وسعت برون سپاری و هماهنگی‌های استفاده شده با طرف سوم در محدوده ISMS؛

چ- استانداردها، الزامات قانونی و سایر الزامات مربوط به برنامه ممیزی.

۷-۲-۲ ویژگی‌های شخصی

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۲ به کار گرفته می‌شود.

۷-۲-۳ دانش و مهارت‌ها

۷-۲-۳-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۳-۱ به کار گرفته می‌شود.

۷-۲-۳-۲ دانش و مهارت‌های عمومی ممیزان سامانه مدیریت

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۳-۲ به کار گرفته می‌شود.

1- Criticality
2- Diversity
3- Demonstrated

۷-۲-۳-۳ دانش خاص حوزه[1] و بخش و مهارت‌های ممیزان سامانه مدیریت

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۳-۳ اعمال می‌شود. علاوه بـر آن راهنماهـای خـاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۷-۲-۳-۳-۱ IS ۷-۲-۳-۳ دانش خاص حوزه و بخش ومهارت‌های خاص ممی‌زان سامانه مدی‌ری‌ت

ممیزان ISMS باید دانش و مهارت‌هایی در زمینه‌های زیر داشته باشند:

الف- روش‌های مدیریت امنیت اطلاعا:، به منظور قادر ساختن ممیز برای بررسی ISMS و تولید یافته‌های ممیزی و توصیه‌های مناسب. دانش و مهارت در این زمینه باید شامل موارد زیر باشد.

۱- اصطلاحات[2] امنیت اطلاعات؛

۲- اصول مدیریت امنیت اطلاعات و کاربرد آن‌ها؛ و

۳- روش‌های مدیریت مخاطرات امنیت اطلاعات و کاربرد آن‌ها.

ب- دانش عمومی در فناوری اطلاعات و فنون امنیت اطلاعات، به صورت مقتضی (به عنوان مثال، روش‌های کنترل دسترسی فیزیکی و منطقی، حفاظت در برابر نرم افزار مخرب، روش‌های مدیریت آسیب‌پذیری) یا دسترسی به آن.

پ- تهدیدات امنیت اطلاعات موجود، آسیب‌پذیری و کنترل‌ها، به علاوه زمینه وسیع‌تر سازمانی، چارچوب قراردادی و قانونی برای ISMS (به عنوان مثال، روابط و فرایندهای در حال تغییر کسب و کار، فناوری یا قوانین)

اگر دانش خاص یا مهارت‌های اضافه‌تری مورد نیاز باشد، باید از متخصصین امنیت اطلاعـات (بـه عنـوان مثال با شایستگی بخش خاص، شایستگی در امنیت IT، یا مدیریت تداوم کسب و کار) استفاده شـود. در صورت استفاده از متخصصین، شایستگی آن‌ها باید به دقت ارزیابی شده باشد.

۷-۲-۳-۴ دانش و مهارت‌های کلی رهبر تیم ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۳-۴ به کار گرفته می‌شود.

۷-۲-۳-۵ دانش و مهارت‌ها برای ممیزی سامانه‌های مدیریت چند وجهی[3]

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۳-۵ به کار گرفته می‌شود.

۷-۲-۴ کسب شایستگی ممیز

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۴ اعمال مـی‌شـود. عـلاوه بـر آن راهنماهـای خـاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۷-۲-۴-۱ IS ۷-۲-۴ کسب شایستگی ممیز

ممیزان ISMS باید دانش و مهارت‌هایی در زمینه فناوری اطلاعات و امنیت اطلاعات، برای مثال با ارائه‌ی گواهینامه‌های مربوطه داشته باشند و همچنین باید قادر به درک نیازهـای کسـب وکـار مربوطـه باشـند.

1- Discipline
2- Terminology
3- Multiple discipline

همچنین تجربه کاری ممیزان ISMS باید به پیشرفت دانش و شایستگی‌های آن‌ها در رشته ISMS کمک کند.

۷-۲-۵ رهبر تیم ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۵ به کار گرفته می‌شود.

۷-۳ تعیین معیارهای ارزیابی ممیز

راهنماها از استاندارد ISO 19011:2011، بند ۷-۳ به کار گرفته می‌شود.

۷-۴ انتخاب روش ارزیابی ممیزِمناسب

راهنماها از استاندارد ISO 19011:2011، بند ۷-۴ به کار گرفته می‌شود.

۷-۵ هدایت ارزیابی ممیز

راهنماها از استاندارد ISO 19011:2011، بند ۷-۵ به کار گرفته می‌شود.

۷-۶ نگهداری و بهبود شایستگی ممیز

راهنماها از استاندارد ISO 19011:2011، بند ۷-۶ به کار گرفته می‌شود.

پیوست الف

(اطلاعاتی)

راهنمای عملی برای ممیزی ISMS

متن زیر راهنمایی کلی در مورد چگونگی ممیزی فرایندهای ISMS را طبق الزامات استاندارد ISO/IEC 27001 بدون توجه به الزامات مشخص ISMS که ممکن است یک سازمان مجزا داشته باشد (برای مثال، الزامات قانونی و قراردادی و دیگر الزامات مربوط به پیاده‌سازی کنترل‌های امنیت اطلاعات ویژه) ارائه می‌دهد.

این راهنما در درجه اول به منظور رجوع و استفاده به وسیله ممیزانی (داخلی یا خارجی) که ممیزی ISMS را انجام خواهند داد، می‌باشد.

استانداردهای اضافی اختیاری می‌توانند به منظور راهنمایی ممیزی شونده یا ممیز استفاده شوند. این‌ها به عنوان «استانداردهای مربوط» در جداول زیر فهرست شده‌اند. به ممیزان یادآوری می‌شود که تنها عدم انطباق‌ها، بر معیارهای ممیزی و الزامات استاندارد ISO/IEC 27001 را مبنا قرار دهند.

جدول الف-۱: راهنمای عملی ممیزی ISMS

الف-۱ محدوده ISMS، خط‌مشی و رویکرد ارزشیابی مخاطره (استاندارد ISO/IEC 27001 بند ۴-۱ و ۴-۲-۱ الف تا پ	
معیارهای ممیزی	استاندارد ISO/IEC 27001[1] بند ۴-۱، ۴-۲-۱ الف، ب و پ
استانداردهای مربوط	استاندارد ISO/IEC 17021 بند ۹-۲-۱ الف تا ت استاندارد ISO/IEC 27005 بند ۳-۱ تا ۳-۹ (استاندارد ISO/IEC Guide73) استاندارد ISO/IEC 27005 بند ۷-۱، ۷-۲، ۷-۳ و ۷-۴ استاندارد ISO/IEC 27006 بند ۳-۱، ۳-۵، ۹-۱-۲ و ۹-۱-۴-۲ ب تا ت
شواهد ممیزی	شواهد ممیزی عبارتند از: • محدوده ISMS (۴-۳-۱ ب)؛ • نمودار سازمانی؛ • راهبرد سازمان؛ • بیانیه خط‌مشی کسب و کار، فعالیت‌ها و فرایندهای کسب و کار؛ • مستندات نقش‌ها و مسئولیت‌ها؛ • پیکربندی شبکه؛ • اطلاعات پایگاه‌ها، شامل فهرستی از شعب، کسب و کار، دفاتر و تسهیلات، و نقشه طبقات آن‌ها؛ • واسطها و وابستگی‌هایی که فعالیت های انجام شده کسب و کار در محدوده ISMS با افراد بیرون از محدوده دارند؛ • قوانین مربوط، مقررات و قراردادها؛

۱- مراجع بدون تاریخ، به نسخه‌ی استاندارد که در مراجع الزامی یا کتابنامه آمده است، بر می‌گردد.

	• اطلاعات دارایی‌های اولیه؛ • مستند خط‌مشی ISMS.
راهنمای عملی ممیزی	**سامانه مدیریت امنیت اطلاعات (۴)**
	الزامات کلی (۴-۱)
	«۴-۱ الزامات کلی» در استاندارد ISO/IEC 27001 زمینه کلی از ISMS مورد نیاز استاندارد ISO/IEC 27001 را مشخص می‌کند، که همه الزامات مندرج در بندهای بعد از ۴-۱ را پوشش می‌دهد. در راهنمای ممیزی، ISMS باید تحت موارد زیر تایید شود: • سازماندهی شده و انجام شده در زمینه‌ای از فعالیت های کلی کسب و کار سازمان و مخاطراتی که سازمان با آن مواجه است؛ • مستندسازی شده به منظور برآورده‌سازی الزامات (مندرج در۴-۳). به علاوه، باید نشان داده شود که ISMS پایه‌گذاری، پیاده‌سازی، راه‌اندازی، پایش، بازنگری، نگهداری و بهبود داده شده است. به عنوان مثال، سازمان نشان می‌دهدکه قابلیت انجام این فرایندها را دارد.
	پایه‌گذاری و مدیریت ISMS (۴-۲)
	پایه‌گذاری ISMS (۴-۲-۱)
	محدوده ISMS (۴-۲-۱ الف)
	ممیز باید بازنگری و تایید کند که سازمان محدوده و قلمروهای ISMS را مشخص کرده است. محدوده ISMS باید تعیین شود تا از به حساب آمدن همه دارایی‌های مرتبط در ISMS و مدیریت مخاطرات آن اطمینان حاصل شود. به علاوه، قلمروها، واسطها و وابستگی‌ها، برای نشان‌دادن مخاطراتی که ممکن است میان آن‌ها به وجود آید، نیاز است شناسایی شود. باید تایید شود که اطلاعاتی که درباره سازمان برای تعیین زمینه‌ای که سازمان عمل می‌کند و چگونگی ارتباط سازمان به ISMS و فرایندهای مدیریت مخاطرات امنیت اطلاعات آن‌ها، به منظور تعریف محدوده و قلمروها جمع آوری شده است. ممیز باید تایید کند که سازمان، اطلاعات زیر را به منظور تعریف محدوده و قلمروها در نظر گرفته است: • راهبردهای سازمان، اهداف کسب وکار و خط‌مشی‌ها؛ • فرایندهای کسب و کار؛ • ساختار و کارکردهای سازمان؛ • الزامات قراردادی و قانونی و سایر الزامات مربوط به سازمان؛ • دارایی‌های اطلاعاتی اولیه؛ • موقعیت‌های سازمان و مشخصه‌های جغرافیایی آن‌ها؛ • محدودیت‌های تاثیرگذار بر سازمان؛ • انتظار ذینفعان؛ • محیط اجتماعی- فرهنگی؛ و • واسطها (به عنوان مثال، تبادل اطلاعات با محیط)؛ باید بازنگری و تایید شود که سازمان توجیهی برای هر مورد کنارگذاشته شده از محدوده را ارائه می‌کند. باید تایید شود که سازمان، کارکردها و عملیات اجرایی خود را دارد و به اطمینان

	از اینکه ISMS به طور مداوم طبق چرخه حیات (استاندارد ISO/IEC 27001 قسمت ۴-۱ و استاندارد ISO/IEC 27006 قسمت ۳-۵) اجرا شده است، قادر می‌باشد. راهنمایی بیشتر درباره چگونگی ممیزی محدوده ISMS در بخش ۶-۲-۳ آورده شده است.
	خط‌مشی ISMS (۴-۲-۱ ب)
•	• ممیز باید تایید کند که خط‌مشی ISMS سازمان به طور خاص در اصطلاحات مشخصه‌های کسب و کار، سازمان، محل آن، دارایی‌ها و فناوری توصیف شده است. ممیز همچنین باید تایید کند که خط‌مشی ISMS به طور واضح موارد زیر را تعیین می‌کند: • چارچوبی برای تنظیم اهداف ISMS (پیش زمینه و اساس تنظیم اهداف و در صورتی که خط‌مشی ISMS و خط‌مشی‌های امنیت اطلاعات در یک مستند توصیف شده است، اهداف)، همچنین جهت و اصول اقدامات، از نقطه نظر مدیریت؛ • الزامات کسب و کار ضروری، الزامات قراردادی و قانونی و دیگر الزامات مرتبط با ممیزی‌شونده؛ • موقعیت و واسط نحوه تنظیم مدیریت مخاطرات امنیت اطلاعات با مدیریت مخاطرات کلی سازمان شامل CSR، حاکمیت[1] داخلی، کنترل مالی و ایمنی و غیره؛ • اساس مدیریت مخاطرات، مانند اینکه چه دارایی‌هایی اولیه‌ای باید به عنوان دارایی مهم برای حفاظت در نظر گرفته شوند و کدام جنبه‌های امنیت اطلاعات، برای مثال، محرمانگی، یکپارچگی یا دسترس‌پذیری باید به طور جدی هنگام هدایت ارزشیابی مخاطره ISMS ارزیابی شود؛ و • مصوبات و تعهد مدیریت ارشد. ممیزی خط‌مشی ISMS می‌تواند به وسیله موارد زیر انجام شود: • تایید این که خط‌مشی ISMS به عنوان یک سند که شامل امضاها یا مهرهایی که نشان می دهد مدیریت ارشد خط مشی را پایه‌گذاری کرده است، ایجاد شده است؛ • تایید از طریق مستندات مربوط به روش‌های اجرایی پایه‌گذاری خط‌مشی (به عنوان مثال: چگونه خط‌مشی در سازمان مجاز یا بازنگری شده است) و قواعد برای روش‌های اجرایی تعریف شده، نقش‌ها مستند شده و روش‌ها برای کنترل مستندات مشخص شده است؛ • مصاحبه با مدیریت برای درک رویکرد و تعهد آن‌ها به ISMS سازمان؛ • ارزیابی از طریق صورت جلسات و سوابق بازنگری مدیریت، تعهد و درگیری مدیریت در پیاده‌سازی، نگهداری و بهبود خط‌مشی ISMS؛ • ارزشیابی این که آیا مدیریت به طور موثر با خط‌مشی ISMS ارتباط دارد، به عنوان مثال، با تمرکز بر مخاطبان خاص، در تمام سطوح سازمان؛ • انجام مصاحبه با کارکنان در محدوده ISMS، به منظور تایید اینکه آیا آن‌ها از اهمیت اهداف امنیت اطلاعات جلسات، پیروی خط مشی امنیت اطلاعات و وظایف امنیت اطلاعات خود آگاه هستند؛ و • مد نظر قرار دادن خط‌مشی امنیت اطلاعات (اگر در دسترس باشد) و رابطه آن با خط‌مشی ISMS . • ممیزی اهداف ISMS می‌تواند با تایید موارد زیر انجام شود:

1- Governance

	• اهداف ISMS سازمان که تعریف شده، در خط‌مشی ISMS منعکس شده و با اهداف کلان کسب و کار هم تراز[1] شده است. • فرآیندها و کنترل‌های ISMS شناسایی شده و به منظور برآوردسازی اهداف ISMS مستند شده است؛ • اهداف به طور مناسب مستند شده است؛ • اهداف ISMS به طور مناسب با همه سطوح سازمان در ارتباط هستند؛ و • سازمان، کارکنان مسئول را به عنوان منابع مورد نیاز برای دستیابی به اهداف تخصیص داده است. • توصیه می‌شود که ممیز خط‌مشی مستند شده ISMS و اهداف در مرحله ممیزی بازنگری مستند را بررسی کند. • نیاز است اهداف و خط‌مشی ISMS در پاسخ به تغییر زمینه مدیریت مخاطرات بازنگری و به روزرسانی شود. ممیز باید تایید کند که بهبودهای مداوم در زمینه محیط کسب و کار انجام شده است. • ممیز باید به خاطر داشته باشد که انطباق با خط‌مشی ISMS و تحقق اهداف می‌تواند به صورت کمی یا کیفی سنجیده شود.
	رویکرد ارزشیابی مخاطره (۴-۲-۱ پ)
	استاندارد ISO/IEC 27001 ملزم می‌کند که سازمان‌ها یک رویکرد ارزشیابی مخاطره را تعریف کنند و بند ۴-۲-۱ موارد ت تا ج مولفه‌های این رویکرد را مشخص می‌کند. استاندارد ISO/IEC 27001 بیان نکرده است چه رویکرد ارزشیابی مخاطره‌ای باید به کار گرفته شود و هر رویکرد تا زمانی قابل قبول است که مطابق با الزامات استاندارد ISO/IEC 27001 باشد. ممیز باید انطباق رویکرد ارزشیابی مخاطره، با الزامات ارزشیابی مخاطره در استاندارد ISO/IEC 27001 و مناسب بودن آن برای سازمان و مدیریت کلان مخاطرات در محل را تصدیق کند. باید تایید شود که رویکرد ارزشیابی مخاطره به منظور شناسایی مخاطرات فرآیندهای کسب وکار، فعالیت‌ها و اقدامات مناسب در مقابل مخاطرات صورت گرفته، پیاده‌سازی شده است. استاندارد ISO/IEC 27005 راهنمایی را در مورد مدیریت و ارزشیابی مخاطره فراهم می‌کند. ممیز باید آگاه باشد که روش های کیفی و کمی، یا هر ترکیبی از این دو، برای ارزیابی مخاطره وجود دارد و این بستگی به سازمان دارد که تصمیم بگیرد چه روشی را به کار برد. لازم است فرایندها و روش‌های استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ بند ۴-۲-۱-پ تا د به عنوان رویکرد ارزشیابی مخاطره مطابق بیانیه مدیریت که در خط‌مشی ISMS سازمان توصیف شده است (به عنوان مثال ۴-۲-۱ ب، ۴، معیاری که کدام مخاطره ارزیابی خواهد شد) تعریف، پیاده‌سازی و مستند شوند. رویکرد این گونه تعریف می‌شود: در برگرفتن چگونگی انطباق با الزامات قراردادی و قانونی و سایر الزامات مرتبط در ارتباط با مخاطرات و دارایی‌هایی که سازمان باید به صورت راهبردی در زمینه کسب وکار و ارزشیابی مخاطره به‌کار برد. در ممیزی باید تایید شود که رویکرد، همان طور که در استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ بند ۴-۲-۱ ب تا د مورد نیاز است، پیاده‌سازی و انجام شده است.

1- Aligned

	ممیز باید تایید کند که نتایج ارزشیابی مخاطره توسط رویکرد ارزشیابی مخاطره قابل مقایسه و تجدید پذیر هستند. به عبارت دیگر، ممیز باید تایید کند که رویکرد، افراد مختلف عهده دار ارزشیابی مخاطره را قادر می سازد بدون توجه به مکان و زمان راهبری ارزیابی مخاطره، به نتیاج یکسانی دست پیدا کنند، به شرطی که آن‌ها سطح مشخصی از شایستگی در ارزشیابی مخاطره و راهبری ارزشیابی‌ها برای دارایی‌های مشابه مطابق با فرایندها و روش‌های اجرایی تعریف شده در رویکرد دارند و اگر نتیجه مختلفی مطرح شود، آن‌ها را برای شناسایی اینکه کجا و چرا در ارزشیابی مخاطره اختلاف رخ داده قادر می سازد. همچنین برای سازمان ضروری است که دارای رویکردی با توانایی رسیدن به انتخاب یکسان کنترل های برطرف سازی مخاطره در صورت یکسان بودن مخاطرات تخمین زده شده، به عبارت دیگر با سطح مخاطره و مشخصات یکسان (دارایی ها و الزمات امنیتی) باشد. این تاییدیه باید با نمونه برداری سوابق گزارش ارزشیابی مخاطره برای ردیابی رو به جلو و عقب توالی فرایندهای ارزشیابی مخاطره، با ممیزی‌های در پایگاه، بر دارایی‌ها انجام شود. معیارهای پذیرش مخاطرات اغلب تحت تاثیر خط‌مشی‌های مدیریت سازمان، اهداف، فناوری، سرمایه‌ها، قوانین و مقررات وابسته و افراد علاقه مند هستند و آن‌ها در نهایت به وسیله سازمان تعریف می شوند. بنابراین برای ممیزان لازم است با توجه به اثربخشی معیارها بر حسب موجودیت‌های بالا را بازنگری کنند. همچنین باید تایید کنند که آن‌ها تعریف شده و وجود دارند. ممیزان ممکن است برای تفسیرهای دقیق از معیار پذیریش مخاطره به استاندارد ISO/IEC 27005 :2008 بند ۷-۲ مراجعه کنند.
الف-۲ شناسایی مخاطره، تحلیل و ارزیابی و شناسایی و ارزیابی گزینه برطرف‌سازی مخاطره (استاندارد ISO/IEC 27001 بند ۴-۲-۱ت تا ج)	
معیار ممیزی	استاندارد ISO/IEC 27001 بند ۴-۲-۱ ت، ث، ج
استانداردهای مربوط	استاندارد ISO/IEC 27005 بند ۸-۲، ۸-۳، ۹، ۱۰
شواهد ممیزی	شواهد ممیزی شامل می شوند: • فهرستی از دارایی‌ها؛ • روش ارزیابی مخاطره؛
راهنمای عملی ممیزی	**شناسایی مخاطره (بند ۴-۲-۱ ت)**
	ممیز باید فهرست دارایی را برای تایید این که همه دارایی‌های مهم مربوط در محدوده ISMS در فهرست آورده شده و صاحبان پاسخگو برای همه دارایی‌ها شناسایی شده‌اند، بازنگری کند. آن‌ها باید شناسایی تهدیدهای مربوط به دارایی ها، آسیب پذیری بهره‌جویی‌شده با تهدیدات و علت شکست امنیت به وسیله آن‌ها را بازنگری کنند برای مثال سناریوهای رخداد نشان داده شده در استاندارد ISO/IEC 27005.
	تحلیل و ارزیابی مخاطره (بند ۴-۲-۱ث)
	وارسی اینکه ارزشیابی مخاطره تمامی دارایی‌های مهم در محدوده ISMS را نشان می‌دهد و ارزشیابی تهدید/آسیب پذیری در رابطه با دارایی‌ها برای سازمان مناسب است و تنها از فهرست پیشین تهدیدات و آسیب پذیری‌ها استفاده نمی‌شود، مهم است. همچنین به دنبال گشتن مخاطراتی که اساسا اشتباه تعیین شده یا مورد کم توجهی قرار گرفته اند، به عنوان

	مثال آن‌هایی که کنترل های مربوط به آنها هزینه بر بوده یا پیاده سازی آنها سخت است یا جایی که مخاطره اشتباه برداشت شده است، دارا اهمیت می‌باشد. ممیز باید با نمونه‌برداری تایید کند که همه دارایی های مهمی که در فهرست دارایی آمده در ارزشیابی مخاطره در بر گرفته شده و نمونه های سناریوهای ارزیابی مخاطره، رخداد را برای ارزیابی این که آیا آن‌ها نیازها و اثرات کسب و کار را به طور مناسب منعکس می کنند. بازنگری کند. دسترس پذیری کارکنان شایسته برای کارکرد خوب ISMS مهم است. ممیز باید شواهدی را که مخاطره میان مدت و بلند مدت مرتبط با از دست دادن دسترس پذیری کارکنان به طور مناسب توسط سازمان ارزیابی شده و به جدیدترین نسخه بازنگری شده و کنترل‌های امنیت اطلاعات مناسب جهت افزایش انعطاف پذیری سازمان در مقابل این نقصان‌ها پیاده سازی شده، ارزشیابی کند.
	گزینه‌های برطرف‌سازی مخاطره (بند ۴-۲-۱ ج)
	ممیز باید گزینه های برطرف‌سازی مخاطره انتخاب شده سازمان را بازنگری کند. باید بازنگری شود که آیا «برطرف‌سازی» (به عنوان مثال کاهش از طریق استفاده کنترل‌ها مناسب، اجتناب از مخاطره، انتقال مخاطره به طرف‌های سوم و یا پذیرش آگاهانه مخاطرات در صورتی که در مدیریت مخاطره پذیری قرار می‌گیرند.) مناسبی برای تمامی مخاطرات شناسایی شده مشخص شده است. ممیز باید شکاف‌ها و ناهنجاری‌های دیگر را جستجو کند و وارسی کند که آیا تغییرات اخیر (به عنوان مثال سامانه‌های IT جدید یا فرآیند های کسب و کار) به طور مناسب در ارزشیابی مخاطره و تصمیم گیری های برطرف‌سازی مخاطره ثبت شده است.
الف-۳ انتخاب اهداف کنترلی و کنترل ها، مصوبات مخاطرات باقی‌مانده پیشنهاد شده، مجوز مدیریت و بیانیه کاربست پذیری (استاندارد ISO/IEC 27001 بند ۴-۲-۱ چ تا د)	
معیارهای ممیزی	استاندارد ISO/IEC 27001 بند ۴-۲-۱, چ – خ، پیوست الف
استانداردهای مربوط	استاندارد ISO/IEC 27005 بند ۹-۱، ۹-۲، ۱۰ استاندارد ISO/IEC 27006 بند ۹-۱-۲
شواهد ممیزی	شواهد ممیزی شامل موارد زیر است: • مستندات برای روش ارزشیابی مخاطره؛ • گزارش‌های ارزشیابی مخاطره؛ • مستنداتی که میزان کاهش مخاطره توسط کنترل‌های اتخاذ شده (نتایج ارزشیابی مخاطره) را توصیف می کند؛ • سوابق نشان‌دهنده مصوبات مخاطرات باقی‌مانده توسط مدیریت (به ویژه، جایی که مخاطرات باقی‌مانده بالاتر از سطح تعریف شده در معیار پذیرش مخاطرات است، توجیه آن‌ها باید شامل شود)؛ • سوابق نشان‌دهنده مجوز مدیریت در پیاده‌سازی و بهره برداری از ISMS؛ • بیانیه‌ی کاربست پذیری.
راهنمای عملی ممیزی	**انتخاب اهداف کنترلی و کنترل‌ها (بند ۴-۲-۱چ)**

برای الزامات امنیت اطلاعاتی بدست آمده از گزینه‌های ارزشیابی مخاطره و برطرف‌سازی مخاطره انتخاب شده برای الزامات، ممیز باید بازنگری کند که کنترل‌های مناسب انتخاب و اهداف کنترلی به منظور دستیابی با نمونه‌برداری مناسب طراحی می‌شوند. ممیز باید بازنگری کند که کنترل‌ها و اهداف انتخاب شده مطابق با الزامات امنیت اطلاعات در الزامات کنترلی تعریف شده در پیوست الف استاندارد ISO/IEC 27001 می باشند (برای تفسیر الزامات کنترل پیوست الف، نمونه‌های عملی برتر شرح داده شده به عنوان راهنمایی‌های پیاده‌سازی استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷می‌تواند مرجع خوبی باشد). هر اختلاف مهم در الزامات پیوست الف در انتخاب کنترل (به عنوان مثال در صورت وجود اهداف کنترلی پیوست الف و کنترل‌هایی که به وسیله سازمان مورد قبول نیستند یا اهداف اضافی و کنترل های انتخاب شده از خارج پیوست الف) باید از نظر منطقی شناسایی و بازنگری شود. به علاوه، ممیز باید وارسی کند که معمولا بهترین شیوه قابل قبول برای بخش کسب و کار وابسته در فرایند انتخاب کنترل در نظر گرفته شده است. بیان صریح همه الزامات امنیت اطلاعات به وسیله خط‌مشی سازمان، مقررات صنعت، قوانین یا قراردادها و غیره باید وارسی شود که به طور صحیح در اهداف کنترلی مستند و کنترل‌ها، وکاهش مخاطره ها به منظور شفاف سازی معیار پذیرش مخاطره منعکس شده است. باید تایید شود که برطرف‌سازی مخاطرات در صورتی که مخاطرات باقی‌مانده، معیار پذیرش مخاطره را حتی بعد از گزینش کنترل‌ها برآورده نسازند، به طور مکرر اعمال می‌شود.	
تصویب مخاطرات باقی‌مانده پیشنهادی (بند ۴-۲-۱ح) **مجوز مدیریت (بند ۴-۲-۱خ)**	
ممیز باید به طور خلاصه مخاطرات باقی‌مانده امنیت اطلاعات را ارزیابی کند و تایید کند که سازمان مصوبه مدیریت را برای مخاطرات باقی‌مانده که بعد از انتخاب کنترل های برطرف‌سازی مخاطره باقی مانده، به دست آورده است. باید وارسی شود که مدیریت به طور رسمی مخاطرات باقی‌مانده، اینکه مخاطرات در تعریف مخاطره پذیری سازمان هستند، اینکه تصمیمات پذیرش مخاطره به وسیله سطوح مجاز کافی مدیریت و نهادهای تصمیم گیری، گرفته شده اند، و اینکه هر کجا که سطوح مخاطرات باقی‌مانده نمی تواند به زیر معیارهای پذیرش کاهش داده شود، مدیریت تصمیم می گیرد به طور رسمی مخاطرات و دلایلی برای تصمیمی که ثبت شده را بپذیرد، پذیرفته و در نظر گرفته است. علاوه بر این، ممیز باید تایید کند که مدیریت مجاز به پیاده‌سازی و بهره برداری از ISMS است، برای مثال به واسطه یک شراکت نامه رسمی، تصویب پروژه، نامه پشتیبانی از مدیر عامل و غیره. باید وارسی شود که این تشریفات محض نیست و شواهدی که مدیریت واقعا ISMSرا می فهمد و حمایت می‌کند، وجود دارد.	
بیانیه کاربست پذیری[1] (۴-۲-۱ د)	
ممیز باید بیانیه کاربست پذیری سازمان را بازنگری کند که اهداف کنترل و کنترل‌ها را مستند و توجیه می‌کند، ، هم آنهایی که که قابل کاربرد است و هم آنهایی غیر قابل کاربرد است. مهم است که بیانیه کاربست پذیری اتصال بین مخاطرات شناسایی شده و اهداف کنترلی و کنترل‌هایی که برای کاهش آن‌ها انتخاب شده اند، را بیان می‌کند. همچنین مهم است که توجیهات برای کنترل‌های غیر قابل کاربرد ارائه شود. ممیز باید تایید کند که ورودی	

1- Statement of applicability

	های مناسب برای همه اهداف کنترلی و کنترل‌های فهرست‌شده در پیوست الف استاندارد ISO/IEC 27001 وجود دارند. بیانیه کاربست پذیری همچنین به دارا بودن کنترل های موجود، نیاز دارد. ضروری است که بیانیه کاربست پذیری بازنگری شده به وسیله یک سطح مدیریتی مناسب برای بازنگری با سوابق گذشته ایجاد شده، تصویب شده، بازبینی شده و به روز شده و غیره به عنوان شواهدتایید/مجاز شود.
الف-۴ انجام و عملکرد ISMS (۴-۲-۲)	
معیار ممیزی	استاندارد ISO/IEC 27001 بند ۴-۲-۲
استاندارد های مربوط	استاندارد ISO/IEC 27001 پیوست الف استاندارد ISO/IEC 27002 استاندارد ISO/IEC 27005 بند ۸-۲-۱-۴، ۹-۱
شواهد ممیزی	شواهد ممیزی موارد زیر را شامل می شوند: • طرح برطرف‌سازی مخاطره و سوابق پیشرفت پروژه‌های طرح‌ریزی • سوابق و روش‌های اجرایی مستند شده برای سنجش اثربخشی کنترل
راهنمای عملی ممیزی	ممیز باید تایید کند که سازمان طرح برطرف‌سازی مخاطره را با گزینه های برطرف‌سازی مخاطره تعریف شده تنظیم و پیاده‌سازی کرده است. این امر برای تایید موارد زیر مهم است: • طرح برطرف‌سازی مخاطره پیاده‌سازی‌شده، اولویت‌ها و مسئولیت‌ها را به حساب آورده است، طبق تعریف؛ • منابع کافی برای پشتیبانی از بهره برداری ISMS تخصیص داده شده است (به بند پ-۹ مراجعه شود)؛ • اولویت‌ها و زمان بندی برای پیاده‌سازی موثر برطرف‌سازی مخاطره به طور واضح تعریف شده است؛ • بودجه، نقش‌ها و مسئولیت‌ها برای برطرف‌سازی مخاطره به وضوح شناسایی شده است; و • طرح برطرف‌سازی مخاطره به طور فعال به عنوان یک ابزار مدیریت امنیت اطلاعات استفاده و به روز رسانی شده است. ممیز باید به وسیله نمونه‌برداری از پیاده سازی و کارایی کنترل‌ها بازنگری کند که ISMS با الزامات مستند ISMS پیاده سازی و اجرا شده است (بند ۴-۲-۱چ مراجعه شود) و پیوست الف از استاندارد ISO/IEC 27001 . لازم است شواهد مربوط به پشتیبانی یا رد ارتباط بین مخاطرات مستند و برنامه و کنترل های انجام شده جستجو کند. ممیز باید تایید کند که هدف و راه سنجش اثر بخشی کنترل‌های انتخاب شده به طور واضح تعریف شده است. توانایی وارسی این که آیا کنترل‌ها واقعا مخاطرات یا اثرات رخداد را در روش سنجش اثر بخشی کنترل‌ها کاهش می دهند، مهم است. (استاندارد ISO/IEC 27005 بند ۸-۲-۱-۴) در زمان ممیزی سنجش ISMS، توجه کنید که سنجش‌ها می توانند از روش‌های متعددی که برخی از آن‌ها پیچیده‌تر از برخی دیگر هستند، به دست آیند. ممیز باید آگاه شود که اگرچه راهنمایی در مورد سنجش ISMS وجود دارد، اما تا زمانی که معیار برای تولید نتایج قابل مقایسه و تکرارپذیر ارزشیابی اثربخشی کنترل، به وسیله مدیریت، تعریف و پذیرش می‌شود، الزامات استاندارد ISO/IEC 27001 برآورده خواهد شد. همچنین مهم است با در نظر گرفتن نتایج ارزیابی و مخاطره و فرآیندهای بر طرف سازی اطمینان حاصل شود که

	سنجش ISMS، الزامات کسب و کار سازمان برآورده می‌شود. سنجش موثر اطمینان حاصل می‌کند که کنترل به طور موثر در حال کاهش مخاطرات مربوطه است. در زمان ممیزی عملکرد ISMS، ممیز باید ارزیابی کند که چگونه سازمان از اثربخشی کنترل‌ها اطمینان حاصل می‌کند. برای این منظور ممیز باید گستره و کفایت سنجش ISMS را ارزیابی کند.
الف-۵ پایش و بازنگری ISMS (استاندارد ISO/IEC 27001 بند ۴-۲-۳)	
معیار ممیزی	استاندارد ISO/IEC 27001 بند ۴-۲-۳
استانداردهای مربوط	استاندارد ISO/IEC 27005 بند ۱۲-۱، ۱۲-۲
شواهد ممیزی	شواهد ممیزی عبارتند از: • گزارش‌های رویدادهای امنیتی/گزارش‌های رخدادها؛ • مستنداتی برای بازنگری‌های مدیریت (ورودی‌ها و خروجی‌ها)؛ • تعریف (روش‌های اجرایی) سنجش اثربخشی کنترل‌ها و سوابق مربوط به سنجش و ارزشیابی کنترل‌ها؛ • سوابق مربوط به استفاده از سنجش (شامل سنجش برای تقویت کنترل‌ها، سوابق اقدامات اصلاحی و پیشگیرانه و یک طرح برطرف‌سازی مخاطره)؛ • مستندات شامل اطلاعات در مورد دارایی‌های اطلاعاتی، تحلیل و ارزشیابی مخاطره، طرح برطرف‌سازی مخاطره و بیانیه کاربست پذیری؛ • طرح یک ساله برای امنیت اطلاعات.
راهنمای عملی ممیزی	ممیز باید پایش ISMS را بازنگری کند و فرآیندها را با استفاده از شواهدی نظیر طرح‌ها، صورت جلسات جلسات بازنگری، گزارش‌های مدیریتی بازنگری/ ممیزی داخلی ISMS، گزارش‌های نقض/حادثه و غیره را بازنگری کند. ممیز باید گستره‌ای که پردازش اشتباهات، نقض‌های امنیتی و دیگر رخدادهای شناسایی شده،گزارش شده و نشان داده شده است را ارزشیابی کند. مهم است تعیین شود که چگونه سازمان به طور موثر و فعالانه پیاده‌سازی ISMS را بازنگری می‌کند تا این اطمینان حاصل شود که کنترل‌های امنیتی شناسایی‌شده در طرح برطرف‌سازی مخاطره، خط‌مشی و غیره به درستی پیاده‌سازی شده و در حال بهره‌برداری هستند. ممیز همچنین باید سنجش ISMS و استفاده از آن‌برای راه‌اندازی بهبودهای مستمر ISMS را مورد بازنگری قرار دهد. همچنین باید تایید شود تغییراتی که باید در نظر گرفته شود (بند ۴-۳-۲ ت ۱ تا ۶ در استاندارد ISO/IEC 27001) در فرآیندهای شناسایی، تحلیل، ارزیابی و برطرف‌سازی مخاطرات منعکس شده است. علاوه بر این، باید تایید شود که مستندات و سوابق ISMS مربوط به ارزشیابی مخاطره به روز شده است. ممیز باید مراقبت ویژه‌ای در طول فرایندهای ممیزی پایش و بازنگری ISMS در نظر بگیرد. این‌ها بسته به نوع و اندازه سازمان کاملا متفاوت خواهد بود، اما فعالیت‌هایی که نیاز است توسط سازمان نشان داده شود، به طور واضح در استاندارد ISO/IEC 27001 آورده شده است. از نگرانی‌های خاص ممیزان موضوع تغییر است و این که آیا سازمان تغییرات داخلی و/یا خارجی برای عملیات خود در نظر گرفته است، و این که آیا این تغییرات بر ISMS اثر خواهد داشت.
الف-۶ نگهداری و بهبود ISMS (استاندارد ISO/IEC 27001 بند ۴-۲-۴ و ۸)	

معیار ممیزی	استاندارد ISO/IEC 27001 بند ۴-۱، ۴-۲-۴ و ۸
استانداردهای مربوط	استاندارد ISO/IEC 27001بند ۴-۲-۴ و ۸
شواهد ممیزی	شواهد ممیزی عبارتند از: • گزارش‌های بهبودهای تعیین شده از فعالیت‌های تعریف شده در ۲۷۰۰۱ بند ۴-۲-۳؛ • عدم تطابق گزارش‌ها؛ • گزارش‌های اقدام اصلاحی/پیشگیرانه ؛ • گزارش‌های رویداد امنیت/گزارش‌های رخداد؛ • روش‌های اجرایی مستند و کنترل‌ها در پشتیبانی از ISMS • سوابق عملیات ISMS • گزارش‌های ارزشیابی مخاطره • روش‌های اجرایی برای اقدام اصلاحی و پیشگیرانه • بیانیه کاربست پذیری
راهنمای عملی ممیزی	**نگهداری و بهبود ISMS (۴-۲-۴)**
	بهبودهای تعیین شده در بند ۴-۲-۲ الف از استاندارد ISO/IEC 27001 نشان دهنده بهبودهایی است که از طریق پایش و بازنگری فرآیندها در بند ۴-۲-۳ از استاندارد ISO/IEC 27001 شناسایی شده است. ممیز باید ابزار و سوابقی که برای بهبود های ISMS تعیین شده است و روش چگونگی پیاده‌سازی بهبودها را بازنگری کند. ممیز باید هم چنین به دنبال شواهد در فرم یادداشت‌های مدیریت، صورت جلسات، گزارش‌ها، رایانامه‌ها و غیره، برای مستندسازی نیاز به بهبود، مجوز دهی به آن‌ها و انجام آن‌ها باشد. ممیزان ISMS باید به دنبال شواهد ملموس بهبود در خط‌مشی‌ها، روش‌های اجرایی، روش‌ها و کنترل‌ها، ارزشیابی‌های مخاطرات جدید، بازنگری‌ها و تغییرات خط‌مشی IS، فعالیت‌های جدید کسب و کار شامل طرفین ذینفع جدید[1]، نگهداری (نه تنها در IT بلکه تسهیلات و تخمین طول عمر برای نصب)، ظرفیت و فعالیت‌های مدیریت رخداد، تغییرات اداره اطلاعات و روش‌های اجرایی انتقال همانند تغییرات در قانون، انطباق فنی و امنیتی برای طرفین خارجی، باشند. بنابراین در ممیزی، باید تایید شود که روش‌های اجرایی و فرایندها به منظور پیاده‌سازی بهبود، با الزامات مشخص شده در بند ۴-۲-۴ ب تا ت از استاندارد ISO/IEC 27001 انطباق دارد.
	بهبود ISMS (۸)
	بهبود مداوم (۸-۱)
	ممیز باید تصدیق کند[2] چگونه سازمان تعیین کرده است که آیا ISMS می‌تواند بهبود یابد، چگونه مخاطرات مرتبط را ارزیابی کرده و چگونه به الزامات امنیت شناسایی‌شده و پایش عملکرد ISMS مرتبط است. ممیز باید تصدیق کند که چگونه کل اهداف سازمان از طریق فرآیندهای مناسب به الزامات امنیت اطلاعات داخلی ، ترجمه شده است و چگونه این الزامات ابلاغ و پایش شده است.

1- New interested parties
2- Verify

بنابراین، ممیز باید شواهدی که سازمان در حال تحلیل داده‌های آن‌ها از پایش ISMS است را جستجو کند و سپس در صورت لزوم نتایج را برای ارزیابی اثر بخشی ISMS و بهبود ISMS در نظر گیرد.

ممیز باید تایید کند که اهداف و اولویت های بهبود، با اهداف ISMS سازگار هستند. به هر حال، باید به این نتیجه رسید که سازمانی که خط‌مشی و اهداف مربوط به بهبود مستمر را ندارد، به وضوح مطابق با استاندارد نیست.

اگر مدیریت هدفی (واقعی) برای بهبود تنظیم کرده و شواهدی برای بهبود وجود ندارد، این اطلاعات باید به مدیریت به منظور بازنگری بازخورد داده شود. از این رو مدیریت می‌تواند تصمیم بگیرد که چه نوع اقدامی مناسب است. برای مثال تنظیم مجدد هدف یا فراهم آوری وسایل دیگر به منظور تاثیر بر فرآیندها.

اگر سازمان از آمار عملکرد (به عنوان مثال، کاهش تعداد رخدادهای امنیتی خاص) برای سنجش پیشرفت‌ها استفاده کند ، ممیز باید با دقت ارزیابی کند که آمار به طور واقعی مربوط به مخاطرات شناسایی شده است یا انتخاب بر اساس سادگی محاسبه است.

اقدام اصلاحی (۸-۲)

ممیز باید اطلاعات مربوط به اقدامات اصلاحی ISMS از قبیل گزارش‌ها و برنامه‌های اجرایی[1] را از بازنگری (های) مدیریتی یا ممیزی‌ها (به استاندارد ISO/IEC 27001 بخش ۷-۳ مراجعه شود)، درخواست‌های تغییر ISMS، بودجه ها/طرح سرمایه گذاری و موارد کسب و کار و غیره به دست آورده و بازنگری کند. ممیز باید شواهدی که ISMS به طور عمده بهبود یافته به عنوان یک نتیجه از بازخورد - وارسی مستندسازی مربوط به خاتمه برنامه اجرایی و غیره را برای تایید این که آیا عدم انطباق و علل ریشه‌ای آن‌ها در واقع به طور موثر توسط مدیریت در بازه‌های زمانی معقول حل شده‌اند جستجو کند.

اغلب مواردی وجود دارند که چاره‌هایی[2] برای عدم انطباق در نظر گرفته می‌شوند، اما اقدامات به منظور جلوگیری از وقوع مجدد آن‌ها هنوز به کار گرفته نشده است چرا که تحلیل ریشه علل، شکست خورده است. با گزارش‌های اقدام اصلاحی، ممیز باید سوابق را از اقدامات اصلاحی بازنگری کند و تایید کند که آیا اقدامات ضبط شده از طریق راهبری مشاهدات در پایگاه موثر بوده و کاربردپذیر است.

در رابطه با مدیریت مخاطرات ISMS، تحلیل ریشه علت باید انجام شود تا:

- تعیین این که آیا به دلیل این حقیقت است که مخاطرات شناسایی نشده است؛
- اگر مخاطرات شناسایی شده است، وارسی کنید که آیا کنترل ها (سنجش‌ها) به مخاطرات اعمال شده است؛
- اگر مخاطرات شناسایی شده است و کنترل ها اعمال شده است، وارسی کنید که آیا کنترل های به کار گرفته برای مخاطرات مناسب هستند؛ و
- اگر مخاطرات شناسایی شده است و کنترل ها اعمال شده است، تصدیق شود که آیا کنترل‌ها به طور موثر پیاده‌سازی شده یا همانطور که انتظار می‌رود انجام شده است.

هر یک یا ترکیبی از موارد بالا عامل عدم تطابق خواهد بود. در زمینه مدیریت مخاطرات،

1- Action plans
2 - Remedies

رخداد عدم تطابق می‌تواند به عنوان مخاطرات کنار گذاشته شده در نظر گرفته شود و عدم تطابق‌های بالقوه می‌تواند به عنوان مخاطرات پیش بینی شده در نظر گرفته شود. ممیز باید تصدیق و تایید کند که آیا علت ریشه‌ای عدم انطباق با تحلیل جزیی توصیف شده در بالا شناسایی شده است و اقدامات به کار گرفته شده در صورت امکان برای عدم تطابق با سوابق و حقایق مشاهده شده در پایگاه مناسب است.	
اقدام پیشگیرانه (۸-۳)	
علاوه بر بهبود ISMS ناشی از عدم انطباق واقعی از پیش شناسایی شده، ممیز باید تعیین کند که آیا سازمان مواضع فعالی را برای نشان دادن بهبود بالقوه، الزامات جدید پیش‌بینی‌شده یا جدید و غیره به کار می‌گیرد. ممیز باید به دنبال شواهد تغییرات ISMS (مانند اضافه کردن، تغییر یا از بین بردن کنترل‌های امنیت اطلاعات) در پاسخ به شناسایی مخاطرات تغییر یافته قابل توجه باشد. موارد زیر می‌تواند در زمان اقدامات پیشگیرانه ممیزی در نظر گرفته شود: ۱- چگونه سازمان عدم تطابق بالقوه و علل آن‌ها را تعیین می‌کند. مثال‌های نمونه عبارتند از: • شناسایی مخاطرات تغییر یافته یا جدید از طریق به روز رسانی ارزشیابی مخاطره (استاندارد ISO/IEC 27001 بند ۴-۲-۳ ت و ۸-۳)؛ • تحلیل روند[1] برای مشخصه‌های ISMS. روند بدتر می‌تواند نشان دهد که اگر اقدامی به‌کارگرفته نشود، سبب رخ دادن عدم انطباق می‌شود؛ • هشدارها به منظور اخطار زود هنگام از نزدیک شدن به شرایط عملیاتی «خارج از کنترل»؛ • پایش رخداد و روند تحلیل رخدادها؛ • ارزیابی عدم انطباق‌ها که در شرایط مشابه برای بخش های دیگر ISMS یا بخش های دیگر سازمان یا حتی در سازمان های دیگر رخ داده است؛ • فرآیند طرح‌ریزی برای شرایط قابل پیش بینی (به عنوان مثال به منظور گسترش، نگهداری یا تغییرات کارکنان) و برای موقعیت‌های غیرقابل پیش بینی (به عنوان مثال، تغییرات در قوانین، مشکلات وقایع طبیعی مانند طوفان، زمین لرزه، سیل و غیره) ۲- چگونه سازمان تعیین می‌کند چه اقدامی مورد نیاز است و چگونه پیاده‌سازی شده است. ممیز باید شواهدی را جستجو کند که: • سازمان علل عدم انطباق‌های بالقوه را تحلیل کرده است (استفاده از نمودار علت و معلول و دیگر ابزارهای امنیت اطلاعات ممکن است مناسب باشد.) • اقدامات لازم در تمام قسمت‌های مربوط سازمان به موقع مستقر شده است؛ • تعاریف روشنی از مسئولیت‌ها برای شناسایی، ارزیابی، پیاده‌سازی و بازنگری اقدامات پیشگیرانه وجود دارد؛ و • آموزش کافی برای کنترل‌های جدید یا تغییر یافته، ارائه شده است. ۳- ممیز باید تایید کند که: • سوابق مناسب، نگهداری می شود. • سوابق، انعکاسی درستی از نتایج است.	

1- Trend

	• سوابق، مطابق با استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷: در بند ۴-۳-۳ کنترل شده است. ۴- برای بازنگری اقدامات پیشگیرانه اخذ شده، ممیز باید در نظر بگیرد که آیا: • اقدامات موثر بوده‌اند (به عنوان مثال آیا از وقوع عدم تطابق‌ها جلوگیری شده و منافع اضافی ایجاد گردیده است؟) • نیازی برای ادامه اقدامات پیشگیرانه به همان روشی که هستند وجود دارد. • اقدامات پیشگیرانه باید تغییر کنند، یا لازم است اقدامات جدیدی طرح‌ریزی شود.
الف-۷ مستند سازی ISMS (استاندارد ISO/IEC 27001 بند ۴-۳)	
معیار ممیزی	استاندارد ISO/IEC 27001 بند ۴-۳-۱ تا ۴-۳-۳
استانداردهای مربوط	-
شواهد ممیزی	شواهد ممیزی مورد زیر را شامل می‌شود: مستند ISMS توصیف شده در استاندارد ۲۷۰۰۱ بند ۴-۳-۱ الف تا خ.
راهنمای عملی ممیزی	**الزامات مستندسازی (۴-۳)**
	مستندسازی ISMS (۴-۳-۱)
	شناسایی الزامات مستندسازی مشخص شده در ISMS مهم است . ممیز باید الزامات استاندارد ISO/IEC 27001 بند ۴-۳-۱ و چندین جای نشان داده شده در بندهای ۵ تا ۸، به علاوه کنترل‌های پیوست الف و همچنین الزامات مشخص شده درمستندسازی ISMS توسط سازمان را در نظر بگیرد. ممیز باید اطلاعات فرآیندهای عملیاتی ممیزی شونده‌ها را درخواست کرده و بدست آورد، با کارکنان درتمام سطوح (از جمله کارکنان اداری، کاربران و صاحبان فرآیند) مصاحبه کند و فعالیت‌های و رفتار های آن‌ها و کارایی فرآیند برای این که پیاده‌سازی و عملکرد ISMS در پایگاه مطابق با الزامات مشخص و مستند شده را مشاهده نماید. ضرورت برای هر مستندسازی باید با توجه به نیاز به سازگاری مشاهده شده ، اهمیت اطلاعاتی که در بر دارد و نقشی که هر مستندسازی می‌تواند در اجتناب از هر گونه مخاطرات قابل توجه، شناسایی‌شده بازی کند، ارزیابی شود.
	کنترل مستندسازی ISMS (۴-۳-۲)
	ممیز باید وجود و انطباق با روش اجرایی مستندشده برای کنترل به روز رسانی مستندسازی ISMS، خط‌مشی‌ها، روش‌های اجرایی، سوابق و غیره را وارسی کند. ممیز هم چنین باید تعیین کند که آیا تغییرات مستندسازی ISMS به طور رسمی کنترل شده است، به عنوان مثال تغییرات بازنگری شده و توسط مدیریت پیش تصویب شده و به تمام کاربران مستندسازی ISMS اعلام شده است، به عنوان مثال با به روز رسانی مرجع قطعی مجموعه‌ای از آنچه که در اینترانت شرکت نگهداری می‌شود و/یا اعلام صریح به همه کاربران مرتبط.
	سوابق ISMS (۴-۳-۳)
	ممیز باید محافظت کنترل‌های سوابق مهم ISMS مانند بازنگری‌های مختلف امنیت اطلاعات متنوع و گزارش‌های ممیزی، برنامه اجرایی، مستندات رسمی ISMS (ازجمله تغییرات

	مشابه)، کتاب‌های بازدیدکنندگان، دسترسی به فرم‌های مجوز/تغییر و غیره را ارزیابی کند. لازم است کفایت کنترل‌ها بر شناسایی، ذخیره‌سازی، حفاظت، بازیابی، زمان نگهداری و وضع مستندات به ویژه در شرایطی که الزامات قانونی و قراردادی وجود دارد و سایر الزامات مورد نیاز مربوط به پیاده‌سازی ISMS در انطباق با استاندارد ISO/IEC 27001 (به عنوان مثال حفاظت از اطلاعات شخصی) بازنگری شود.
الف-۸ مسئولیت مدیریت (استاندارد ISO/IEC 27001 بند ۵)	
معیار ممیزی	استاندارد ISO/IEC 27001 بند ۵-۱، ۵-۲-۱ و ۵-۲-۲
استانداردهای مربوط	استاندارد ISO/IEC 27006 ۹-۲-۳-۲-۲ خ استاندارد ISO/IEC 27001 بند ۴-۲-۱ب، ۵، پیوست الف ۵-۱-۱، الف ۶-۱-۱ استاندارد ISO/IEC 17021 بند ۹-۲-۳-۲ ج استاندارد ISO/IEC 27006 بند ۹-۲-۳-۲-۲ ج استاندارد ISO/IEC 27005 بند ۹-۲
شواهد ممیزی	شواهد ممیزی عبارتند از: • خط‌مشی ISMS با تاریخ تصویب، امضا و غیره؛ • سوابق بازنگری خط‌مشی ISMS؛ • طرح‌ها/برنامه‌های زمانبندی امنیتی برای فعالیت های ISMS، به عنوان مثال طرح برطرف‌سازی مخاطره، طرح/ برنامه تعلیم و آموزش، طرح/برنامه ممیزی داخلی و غیره؛ • صورت جلسات بازنگری مدیریت با مستندات ورودی/خروجی، صورت جلسات کمیته امنیت اطلاعات سازمان و غیره؛ • مستندات نقش‌ها و مسئولیت‌ها؛ • گزارش ممیزی‌های داخلی؛ • مصاحبه مدیریت؛ • سوابق تصویب مخاطرات باقی‌مانده، تصویب طرح برطرف‌سازی مخاطره، سوابق بازنگری‌های مدیریتی، تصمیم گیری بودجه برای طرح کسب و کار و نتایج تصویب درخواست‌های تصمیم گیری؛ • سوابق بازنگری‌های کنترل‌ها و فعالیت های PDCA؛ • معیارهای شایستگی؛ • منابع انسانی و سوابق شایستگی؛ • برنامه/طرح های آموزش؛ • گزارش‌های آموزش و سوابق.
راهنمای عملی	**تعهد مدیریت (۵-۱)**

ممیزی	ممیز باید میزان تعهد مدیریت به امنیت اطلاعات را با استفاده از شواهد زیر بازنگری کند: • تصویب مدیریتی رسمی خط‌مشی ISMS؛ • پذیرش مدیریت اهداف و طرح های پیاده‌سازی ISMS، با تخصیص منابع کافی و تعیین اولویت‌های مناسب به فعالیت‌های مربوط (به ۵-۲-۱ مراجعه شود) • نقش‌ها و مسئولیت‌های واضح برای امنیت اطلاعات از جمله فرآیندی برای تخصیص و پذیرش جوابگویی به منظور حفاظت مناسب از دارایی‌های اطلاعات با ارزش؛ • تفاهم‌نامه‌های مدیریت، رایانامه‌ها، صورت جلسات، سخنرانی‌ها، جلسات، کار، تشریح کار و غیره، بیان پشتیبانی و تعهد به ISMS؛ • معیار پذیرش مخاطره و پذیرش رسمی آن‌ها، مخاطره‌پذیری و غیره مربوط به مخاطرات امنیت اطلاعات؛ و • هدف‌گذاری[1]، تخصیص منابع و آماده سازی ممیزی‌های داخلی و بازنگری‌های مدیریت ISMS.
	تخصیص منابع ISMS (۵-۲-۱)
	ممیز باید تصدیق کند که منابع لازم برای پیاده‌سازی، نگهداری و بهبود ISMS به طور مناسب مدیریت می‌شود. بدین معنی که سازمان نیاز به شناسایی، طرح‌ریزی، دسترس‌پذیری، استفاده، پایش و تغییر منابع مناسب مورد نیاز دارد. توصیه می‌شود، مدیریت منابع به صورت مجزا بازنگری نشود. صرف نظر از روشی که سازمان فرآیندهایش را ساختار داده و شناسایی کرده است، ممیزان باید به تصدیق کفایت و موثر بودن مدیریت منابع برای دستیابی به نتایج طرح ریزی شده، قادر باشند. برای ممیزان مهم است که تصدیق کنند که آیا سازمان عملکرد حال و گذشته را (به عنوان مثال تحلیل هزینه-سود ، ارزشیابی مخاطره) در زمان تصمیم‌گیری این که چه منابعی باید تخصیص داده شود، ارزیابی کرده است. مدیریت منابع می‌تواند به وسیله مصاحبه با مدیریت و سایر کارکنان مسئول برای وارسی این که فرایندهای مناسب در جای خود هستند، ارزیابی شود. این امر نیازمند پشتیبانی با شواهد عینی جمع آوری شده در طول ممیزی است. شواهد می تواند در مراحل مختلف ممیزی – ورودی‌های بازنگری، عملکرد فرایند و خروجی‌ها کسب شود. این امر باید در زمان ممیزی همه فرآیندها و سامانه‌های مربوط و مستندسازی فرایند انجام شود، از قبیل: • تعهد مدیریت و مسئولیت ها؛ • فرآیند بازنگری مدیریت؛ • فرآیندهای ISMS از جمله مدیریت مخاطرات، اقدامات پیشگیرانه و اصلاحی و بهبود مستمر؛ • تشریح کار؛ و • بودجه و سوابق زمانی برای فعالیت‌های خاص ISMS. ممیزان باید از قضاوت‌های ذهنی در مورد کفایت منابع تخصیص داده شده به وسیله سازمان اجتناب کنند و باید نقش آن‌ها را برای ارزیابی اثر بخشی فرایندهای مدیریت منابع محدود کنند.
	آگاه‌سازی و آموزش ISMS (۵-۲-۲)

1- Scoping

ممیز باید آموزش کسانی که به طور خاص در عملکرد ISMS درگیر هستند و فعالیت‌های آگاه‌سازی امنیت اطلاعات کلی که همه کارمندان را هدف قرار می‌دهد، بازنگری کنند. باید وارسی شود که صلاحیت‌های لازم و الزامات آموزش/آگاه‌سازی برای متخصصان امنیت اطلاعات و سایر افراد با نقش‌ها و مسئولیت‌های خاص به طور واضح شناسایی شده، و آموزش امنیت اطلاعات و نیازهای آگاه‌سازی با بودجه مناسب پشتیبانی شده است. ممیز باید گزارش ارزیابی آموزش و غیره را بازنگری کند و به دنبال شواهد برای تایید اینکه همه اقدامات بهبود ضروری به درستی به کار گرفته شده‌اند، باشد. لازم است با نمونه برداری وارسی شود که سوابق منابع انسانی کارمندان، آموزش مرتبط با ISMS را ذکر کرده است. ممیز باید ارزشیابی کند که سطح کلی آگاه‌سازی امنیت اطلاعات با پیمایش[1]/ نمونه‌برداری یا بازنگری نتایج پیمایش/ نمونه‌ها به عنوان قسمتی از ISMS راهبری شده است. به منظور برآورده سازی صلاحیت/ اثربخشی الزامات استاندارد ISO/IEC 27001 ، سازمان به طور معمول به انجام چندین مورد نیاز خواهد داشت ازجمله: • شناسایی اینکه چه صلاحیت‌هایی برای کارکنان انجام دهنده کارهایی که امنیت اطلاعات را تحت تاثیر قرار می دهد، مورد نیاز است؛ • شناسایی کارکنان آماده انجام کار دارای شایستگی لازم؛ • تصمیم درباره صلاحیت‌های اضافی مورد نیاز؛ • تصمیم درباره چگونگی دستیابی به این صلاحیت‌های اضافی - آموزش کارکنان (خارجی یا داخلی)،آموزش تئوری یا عملی، استخدام کارکنان شایسته جدید، تخصیص کارکنان توانمند موجود به کارهای مختلف؛ • بازنگری اثر بخشی اقدامات صورت گرفته برای برآورده‌سازی نیازهای صلاحیت؛ و • بازنگری دوره‌ای شایستگی کارکنان. در طی فرایند، سازمان نیاز به نگهداری سوابق مناسب تحصیل، آموزش، مهارت و تجربه دارد. استاندارد ISO/IEC 27001 چگونگی پایه‌گذاری فرآیندی یا ماهیت دقیق نگهداری سوابق نگهداری را مشخص نمی‌کند. ۱- در ممیزی انطباق سازمان با شایستگی و الزامات ارزیابی آموزش، ممیز به طور معمول به دنبال شواهدی که موضوعات زیر در آدرس‌دهی می‌کند، می‌باشد: سازمان نیاز به شناسایی صلاحیت‌هایی مورد نیاز توسط کارکنان انجام دهنده کار که بر امنیت اطلاعات تاثیر گذارند، دارد. اهداف ممیز باید تعیین شود تا مشخص شود، رویکردی نظام‌مند برای شناسایی این صلاحیت‌ها و تصدیق اینکه رویکرد موثر است، وجود دارد. خروجی فرایند ممکن است یک فهرست، ثبت[2]، پایگاه داده، طرح منابع انسانی، طرح توسعه شایستگی ها، قرارداد، طرح محصول یا پروژه و غیره باشد. گفتگوها می‌تواند در ابتدا با مدیریت به منظور اطمینان از اینکه آن‌ها اهمیت شناسایی شایستگی موردنیاز را درک کرده‌اند، برگزار شود. این‌ها می تواند منابع بالقوه اطلاعات راجع به فرآیندها یا فعالیت‌های تغییر داده شده یا جدید، که ممکن است به سمت الزامات مختلف شایستگی در سازمان هدایت شود، باشد. بازنگری صلاحیت‌ها ممکن است زمانی که یک مناقصه یا قرارداد جدید در حال مطرح شدن است، مورد نیاز باشد. شواهد آن ممکن است در	

1- Surveying
2- Register

	سوابق مربوط یافت شود. الزامات شایستگی ممکن است در مستندات قرارداد آنجایی که فعالیت‌های پیمانکاران فرعی تاثیرگذار در فرآیندها و/یا امنیت اطلاعات است، گنجانده شود. ممیزان به تعیین این که سازمان نیازهای جدید یا تغییر داده شده شایستگی را، (به عنوان مثال در طول ممیزی نظارت) شناسایی کرده، نیاز دارند. ۲- ممیز باید بازنگری کند که کارکنان توانمند به کارهایی که به فعالیت‌های لازم برای کنترل امنیت اطلاعات نیاز دارد، تخصیص داده شده‌اند. ممیز باید تصدیق کند که نوعی از فرایند ارزیابی به منظور حصول اطمینان از مناسب بودن شایستگی ها برای فعالیت های سازمان، در محل وجود دارد. و اینکه کارکنان توانمند انتخاب شده در حال اثبات شایستگی مناسب می‌باشند. همچنین، فرایند باید اطمینان حاصل کند که همه کمبودها مورد توجه قرار گرفته و اثربخشی کارکنان درحال سنجش است. لازم است بررسی شود فعالیت‌هایی که امنیت اطلاعات را تحت تاثیر قرار می دهند به وسیله اشخاص صالح انتخاب شده انجام می شوند. شواهد ممکن است در طی ممیزی با تاکید بر فرایندها، فعالیت‌ها، کار و محصولات که دخالت انسانی ممکن است بزرگترین تاثیر را داشته باشد، به دست بیاید. ممیز ممکن است، تشریح کار، فعالیت‌های بازرسی یا آزمایش، فعالیت‌های پایش، سوابق بازنگری مدیریت، تعریف مسئولیت‌ها و مجوزها، سوابق عدم انطباق، گزارش‌های ممیزی، شکایات مشتری، سوابق اعتبارسنجی فرآیندها و غیره را بازنگری کند. ۳- سازمان به ارزیابی اثر بخشی اقدامات صورت گرفته برای برآورده‌سازی نیاز های شایستگی نیاز دارد. سازمان ممکن است از تعدادی از فناوری‌ها شامل نقش– بازی، بازنگری دوگانه، مشاهده، بازنگری آموزش و سوابق شغلی و/یا مصاحبه ها (به استاندارد ISO 19011:2011، جدول ۲، برای نمونه های بیشتر مراجعه شود) استفاده کند.. تناسب یک روش ارزیابی ویژه به عوامل بسیاری بستگی دارد. برای مثال، سوابق آموزش می تواند برای تصدیق اینکه یک دوره آموزشی به طور موفق کامل شده، دیده شود. به هر حال، این روش مشابه برای ارزیابی اینکه آیا ممیز به طور رضایت بخش در طی ممیزی کار کرده است، قابل پذیرش نخواهد بود. در عوض، ممکن است نیاز به مشاهده، بازنگری دوگانه، مصاحبه و غیره داشته باشد. سازمان ممکن است به اثبات حصول شایستگی کارکنان با تلفیقی از تحصیل، آموزش و یا تجربه نیاز داشته باشد. ۴- حفظ صلاحیت ممیز به تصدیق این که نوعی از فرایند پایش موثر به کار گرفته شده و اعمال شده، نیاز دارد. راه های انجام آن شامل فرایند توسعه تخصصی مداوم (مطابق بند ۷-۴ استاندارد ISO 19011)، ارزیابی منظم کارکنان و عملکرد آن‌ها، یا بازرسی منظم، آزمون یا ممیزی محصول یا سامانه برای افراد یا گروه های مسئول، است. تغییرات مداوم در الزامات شایستگی ممکن است نشان دهد که یک سازمان در نگهداری سطوح عملکرد کارکنان فعال است.
الف- ۹ ممیزی داخلی ISMS و بازنگری مدیریت ISMS (استاندارد ISO/IEC 27001 بند ۶ و ۷) این بند راهنمایی به منظور ممیزی خارجی یا خود وارسی یا راهنمایی ارزیابی دوگانه برای ممیزی داخلی فراهم می‌کند.	
معیار ممیزی	استاندارد ISO/IEC 27001بند ۶، ۷
استانداردهای مربوط	استاندارد ISO/IEC 27005 بند ۷-۹ استاندارد ISO/IEC 27006 بند ۹-۱-۲، ۹-۱-۴، ۹-۲-۳-۲

	استاندارد ISO/IEC 17021 بند ۹-۲-۳-۲، ۹-۳-۲-۱
شواهد ممیزی	شواهد ممیزی عبارتند از: • برنامه ممیزی‌های داخلی، طرح ها، گزارش‌های و سوابق؛ • صورت جلسات بازنگری مدیریت با مستندات ورودی و خروجی؛ • گزارش‌های ارزشیابی مخاطره.
راهنمای عملی ممیزی	**ممیزی داخلی ISMS (۶)** ممیز باید، ممیزی‌های داخلی ISMS سازمان را با استفاده از برنامه های ممیزی ISMS، طرح ها، گزارش‌های ممیزی، طرح‌های اقدام و غیره بازنگری کند. باید تصدیق شود که مسئولیت‌ها برای راهبری ممیزان داخلی ISMS به طور رسمی، به ممیزان به قدر کافی آموزش دیده و دارای شایستگی اختصاص داده شده است. ممیزان باید حدی که ممیزی‌های داخلی ISMS تایید می‌کنند که ISMS الزامات تعریف شده در استاندارد ISO/IEC 27001 و الزامات قانونی و قراردادی و دیگر الزامات و الزامات ISMS سازمانی مشخص شده از طریق فرآیند ارزشیابی مخاطره را در نظر بگیرند. استاندارد ISO/IEC 27001 بند۶ الف – ۶ د می‌تواند به چک لیست‌ها برای پشتیبانی ممیز توسعه یابد. ممیز باید هم چنین طرح‌های عملیاتی توافق شده، اقدامات اصلاحی و غیره که در بازه‌های زمانی توافقی تایید و توافق شده‌اند را وارسی کند و توجه ویژه‌ای به هرگونه اقدامات عقب افتاده برای مثال‌های جاری نماید. سازمان باید قادر به بیشینه کردن استفاده از منابع در دسترس در طول راهبری فعالیت‌های ممیز ISMS داخلی باشد. باید شواهدی موجود باشد که سازمان: • الزامات شایستگی برای ممیزان داخلی ISMS خود را شناسایی کرده است؛ • آموزش مناسب را فراهم کرده است؛ • فرآیندی برای پایش عملکرد ممیزان داخلی ISMS و تیم‌های ممیزی وجود دارد؛ و • کارکنان تیم‌های ممیزی که دانش مناسب بخش خاص را دارند، در بر می‌گیرد. (از این رو آن‌ها قادر به شناسایی این که تغییر در فرآیند یا فعالیتی خاص ممکن است منجر به پیامدی قابل توجه برای امنیت اطلاعات شود، هستند.) باید معلوم شود که سازمان برای اطمینان از موثر بودن و کارایی استفاده از منابع، ممیزی‌های داخلیISMS را طرح‌ریزی و روش‌های ممیزی آن را تعریف کرده است. هم چنین این امر باید کمک کند تا اطمینان حاصل شود که مخاطرات ذاتی از شکست ممیزی در فرآیند ممیزی و خروجی ممیزی کمینه شود. سازمان باید فرآیندی برای استفاده از نتایج ممیزی گذشته در طرح‌ریزی ممیزی‌های داخلی ISMS آینده داشته باشد. ممیز باید تصدیق کند که سازمان از چنین اطلاعاتی در زمان پایه‌گذاری ممیزی دوره‌ای[1] چنین فرآیندها و فعالیت‌هایی استفاده می‌کند. با در نظر گرفتن عوامل فوق و با بررسی اینکه آیا فرآیند ممیزی داخلی ISMS منجر به بهبودهای ملموس برای ISMS شده است، ممیزان ISMS باید قادر به قضاوت این که آیا سازمان یک برنامه ممیزی داخلی ISMS موثر را پیاده‌سازی کرده است، باشند. همچنین

1- Audit frequency

ممیزISMS باید قادر به قضاوت این باشند که آیا خروجی ممیزی‌های داخلی ISMS شواهد کافی برای استفاده به عنوان بخشی از فرآیند بهبود ISMS را فراهم می‌کند.

بازنگری مدیریت ISMS (۷)

بازنگری مدیریت ممیزی ISMS (۷-۱)

استاندارد ISO/IEC 27001 به مدیریت بازنگریISMS سازمان در طرح‌ریزی زمانی (حداقل یک بار در سال) برای اطمینان از مناسب بودن تداوم ،کفایت و اثر بخشی آن، نیاز دارد. اینکه چه زمانی مدیریت از پیش ISMS را بازنگری کرده و چه زمانی در طرح بعدی باید بازنگری شود، باید تعیین شود. دوره‌های بازنگری‌ها باید تعریف شود، به عنوان مثال، در خط‌مشی ISMS یا کتاب راهنما خط‌مشی ISMS.

بازنگری می‌تواند در یک جلسه جداگانه انجام شود اما این الزام استاندارد نیست. راه‌های بسیاری که مدیریت می‌تواند ISMS را بازنگری کند، وجود دارد، مانند دریافت و بررسی گزارش‌ها، ارتباطات الکترونیکی یا به عنوان بخشی از جلسات منظم مدیریت که مسائلی از قبیل بودجه و اهداف نیز در آن مطرح می‌شود.

مدیریت فرآیند بازنگری نباید فقط یک بررسی انجام شده برای برآورده کردن الزامات استاندارد و ممیزان باشد. این مدیریت باید بخش کاملی از فرآیند مدیریت کسب و کار سازمان باشد. بازنگری مدیریت کلان، فرآیند پیچیده‌ای است که در سطوح مختلف سازمان انجام می‌شود و باید همیشه یک فرآیند دو طرفه باشد،که توسط مدیریت ارشد با ورودی‌ها از تمام سطوح در سازمان تولید شده باشد. این فعالیت‌ها می‌تواند از جلسات روزانه، هفتگی، ماهانه، واحد سازمانی تا بحث‌های ساده و گزارش‌ها متفاوت باشد.

ممیزان باید شواهدی که ورودی ها و خروجی ها فرآیند بازنگری مدیریت مربوط به اندازه و پیچیدگی سازمان هستند و برای بهبود ISMS استفاده می‌شوند را جستجو کنند. هم چنین باید در نظر بگیرند که چگونه مدیریت سازمان ساختار داده شده و فرآیند بازنگری مدیریت در این ساختار استفاده می‌شود.

سوابق بازنگری مدیریت مورد نیاز است اما قالب آن‌ها مشخص نیست. صورت جلسات معمول‌ترین نوع سوابق هستند، اما سوابق الکترونیکی، نمودارهای آماری، ارائه و غیره می‌تواند از انواع سوابق قابل قبول باشد. مهم است که اطمینان حاصل شود شواهدی برای مد نظر قراردادن تمام مسائل فهرست شده در استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ بند ۷ وجود دارد. حتی جایی که تصمیم گرفته شده، هیچ اقدامی لازم نیست.

فرآیند بازنگری مدیریت ممکن است شامل مولفه‌های طرح‌ریزی ISMS جایی که تغییرات برای فرآیندها و سامانه‌ها در نظر گرفته می‌شود، باشد. در این مورد، ممیزان باید بازنگری کنند که نکات زیر در نظر گرفته شده است یا خیر:

- آیا پیشنهاد تغییرات قبل از پیاده‌سازی ارزیابی می‌شوند؟
- در تهیه طرح‌های راهبردی، مسائل مربوط به ISMS در نظر گرفته می‌شود؟
- آیا کنترل‌های مورد نیاز پیش از شناسایی تغییرات پیاده‌سازی می‌شود؟ به عنوان مثال، در شروع برون سپاری یک فرآیند

ورودی بازنگری مدیریت (۷-۲)

استاندارد ISO/IEC 27001 بند ۷-۲ ورودی ها و عناوینی که باید در بر گرفته شود را

مشخص می‌کند. به هر حال، اینها تنها موضوعاتی که می‌توانند در بازنگری گنجانده شوند، نیستند. ممکن نیست آن‌ها به صورت مجزا یا به طور همزمان به عنوان بخشی از بازنگری کلی کسب و کار مورد خطاب قرارگرفته باشند. ممیزان باید آگاه باشند که ورودی ها می‌توانند در اشکال زیادی مانند گزارش‌ها، نمودار روند و به همین ترتیب باشند.

با بازنگری گزارش‌های مدیریت، صورت جلسات و سوابق دیگر و/یا با مصاحبه با آنهایی که درگیر بودند، باید وارسی شود چه چیزی در بازنگری مدیریت قبلی وجود داشته است. (استاندارد ISO/IEC 27001 ، نه مورد مانند نتایج ممیزان /بازنگری‌های دیگر، بازخوردها و پیشنهادات بهبود، اطلاعات آسیب‌پذیری‌ها و تهدیدات و غیره را مشخص می‌کند. لازم است این که تا چه حد مدیریت نقش یک بخش فعال را بازی کرد و به طور کامل و در بازنگری‌ها درگیر شده، ارزشیابی شود.

خروجی بازنگری مدیریت (۷-۳)

استاندارد ISO/IEC 27001 بند ۷-۳ خروجی ها برای فرآیند بازنگری مدیریت و هرگونه تصمیم گیری‌ها و اقدامات مربوط به این موضوع‌های الف-ث که باید شامل شوند را مشخص می‌کند. ممیز باید خروجی‌های هر گونه بازنگری مدیریت قبلی شامل تصمیمات کلیدی مدیریت، طرح‌های اقدام و سوابق مربوط به تایید این که اقدامات توافقی به موقع انجام شده است را وارسی کند. همانند خروجی فرآیند بازنگری مدیریت، باید شواهدی از تصمیمات راجع به الف – ث موجود باشد. از قبیل:

- تغییر اهداف و خط‌مشی ISMS؛
- طرح‌ها و اقدامات ممکن برای بهبودها؛
- تغییر منابع؛
- طرح‌های تجدیدنظر شده کسب و کار؛
- بودجه‌ها؛
- بیانیه کاربست پذیری تجدیدنظر شده؛ و
- سنجش‌های کنترل تجدیدنظر شده.

خروجی فقط مربوط به بهبود یا تغییرات نیست، بلکه می‌تواند شامل تصمیمات دیگر موضوعات مهم مانند طرح‌های معرفی کننده فناوری‌های جدید، سامانه ها یا محصولات باشد. با توجه ویژه به اقداماتی که به موقع یا به طور صحیح تکمیل نشده است، اگر لازم باشد، تایید کندکه اقدامات خاتمه یافته به درستی تکمیل شده اند.

کتاب‌نامه

[1] ISO/IEC 17021:2011, Conformity assessment — Requirements for bodies providing audit and certification of management systems

[۲] استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سیستمهای مدیریت امنیت اطلاعات – آیین کار مدیریت امنیت اطلاعات

[3] ISO/IEC 27003:2010, Information technology — Security techniques — Information security management system implementation guidance

[۴] استاندارد ملی ایران شماره ۱۴۰۹۶: سال ۱۳۸۹، فناوری اطلاعات – فنون امنیتی –مدیریت امنیت اطلاعات – سنجش

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

[۶] استاندارد ملی ایران شماره ۲۷۰۰۶: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – الزامات نهادهای ممیزی‌کننده و گواهی‌کننده سیستم‌های مدیریت امنیت اطلاعات

[7] IAF MD1:2007, IAF Mandatory Document for the Certification of Multiple Sites Based on Sampling International Accreditation Forum

راهبردها

راهبرد اول:

امن سازی زیرساخت های حیاتی کشور در قبال حملات الکترونیکی

راهبرد دوم:

ایجاد و توسعه نظام های فرابخشی امنیت فضایی تبادل اطلاعات

راهبرد سوم:

تامین سلامت و جلوگیری از مخاطرات ناشی از محتوا در امنیت فضایی تبادل اطلاعات

راهبرد چهارم:

تقویت صنعت و توسعه خدمات و محصولات امنیت فضایی تبادل اطلاعات

راهبرد پنجم:

حمایت از تحقیق، ارتقاء سطح آگاهی، دانش و مهارت های مرتبط با امنیت فضایی تبادل اطلاعات

راهبرد ششم:

ارتقاء سطح همکاری های منطقه ای و بین المللی در زمینه امنیت فضای تبادل اطلاعات

منابع :

- سایت سازمان ملی استاندارد ایران **http://www.isiri.org**
- سایت سازمان فناوری اطلاعات ایران **http://www.itc.ir**
- منابع مورد مطالعه در اینترنت

ISMS

Standards

Information Security Management System

Collection and compilation

Engineer hosein maleki
Expert information technology