ISIRI
14096
1st. Edition

جمهوری اسلامی ایران
Islamic Republic of Iran
مؤسسه استاندارد وتحقیقات صنعتی ایران
Institute of Standards and Industrial Research of Iran

استاندارد ملی ایران
۱۴۰۹۶
چاپ اول

فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات- سنجش

Information technology - Security techniques - Information Security Management-Measurement

ICS:35.040

به نام خدا

آشنایی با مؤسسهٔ استاندارد و تحقیقات صنعتی ایران

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

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

پیش نویس استانداردهایی که مؤسسات و سازمان‌های علاقه مند و ذیصلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که مؤسسه استاندارد تشکیل می‌دهد به تصویب رسیده باشد.

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران از اعضای اصلی سازمان ملی استاندارد (ISO)[1] کمیسیون ملی الکتروتکنیک (IEC)[2] و سازمان ملی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین بهبودهای علمی، فنی و صنعتی جهان و استانداردهای ملی بهره‌گیری می‌شود.

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران می‌تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشو ر و / یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. مؤسسه می‌تواند به منظور حفظ بازارهای ملی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سامانه‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش ، مؤسسهٔ استاندارد این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آنها اعطا و بر عملکرد آنها نظارت می‌کند. ترویج دستگاه ملی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این مؤسسه است.

---

* موسسهٔ استاندارد و تحقیقات صنعتی ایران

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

کمیسیون فنی تدوین استاندارد

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

رئیس:	**سمت و/ یا نمایندگی**
سپیده صفایی (کارشناس کامپیوتر)	کارشناس نرم‌افزار مرکز تحقیقات صنایع انفورماتیک
دبیر:	**سمت و/ یا نمایندگی**
منافی ، علیرضا (کارشناس ارشد کامپیوتر)	معاون سیستم‌های فناوری اطلاعات مرکز تحقیقات صنایع انفورماتیک
اعضاء: (اسامی به ترتیب حروف الفبا)	
اخوان، سید انوشیروان (کارشناس ارشد مدیریت IT)	معاون طرح و برنامه شرکت ایزایران
مروجی، سجاد (کارشناس ارشد کامپیوتر)	مدیر توسعه فناوری‌های نوین وزارت بهداشت
سید علیرضا مهدوی (کارشناس ارشد مدیریت IT)	مشاور شرکت داده‌پردازان آبشار
عصمت علی محمد ملایری (کارشناس ارشد نرم‌افزار)	مدرس دانشگاه آزاد ملایر

فهرست مندرجات

ادامه فهرست مندرجات

عنوان **صفحه**

ادامه فهرست مندرجات

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.)

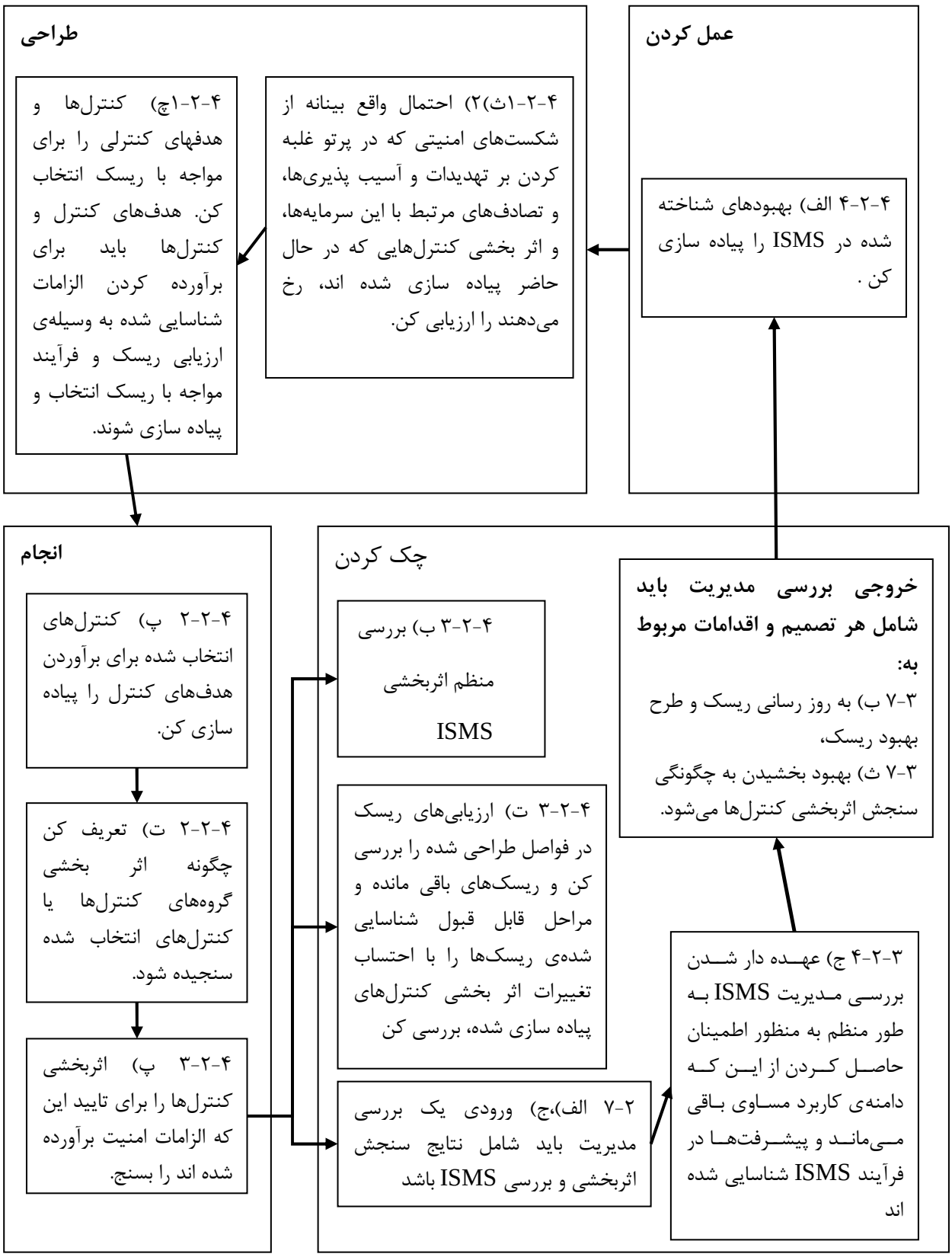
پ) تایید اندازه‌ی برآورده شدن الزامات امنیتی شناخته شده(به ۴-۲-۳ پ در شکل ۱ مراجعه شود.)

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 .
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.
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
خروجی بررسی مدیریت باید شامل هر تصمیم و اقدامات مربوط به:
۷-۳ ب) به روز رسانی ریسک و طرح بهبود ریسک،
۷-۳ ث) بهبود بخشیدن به چگونگی سنجش اثربخشی کنترل‌ها می‌شود.
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

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

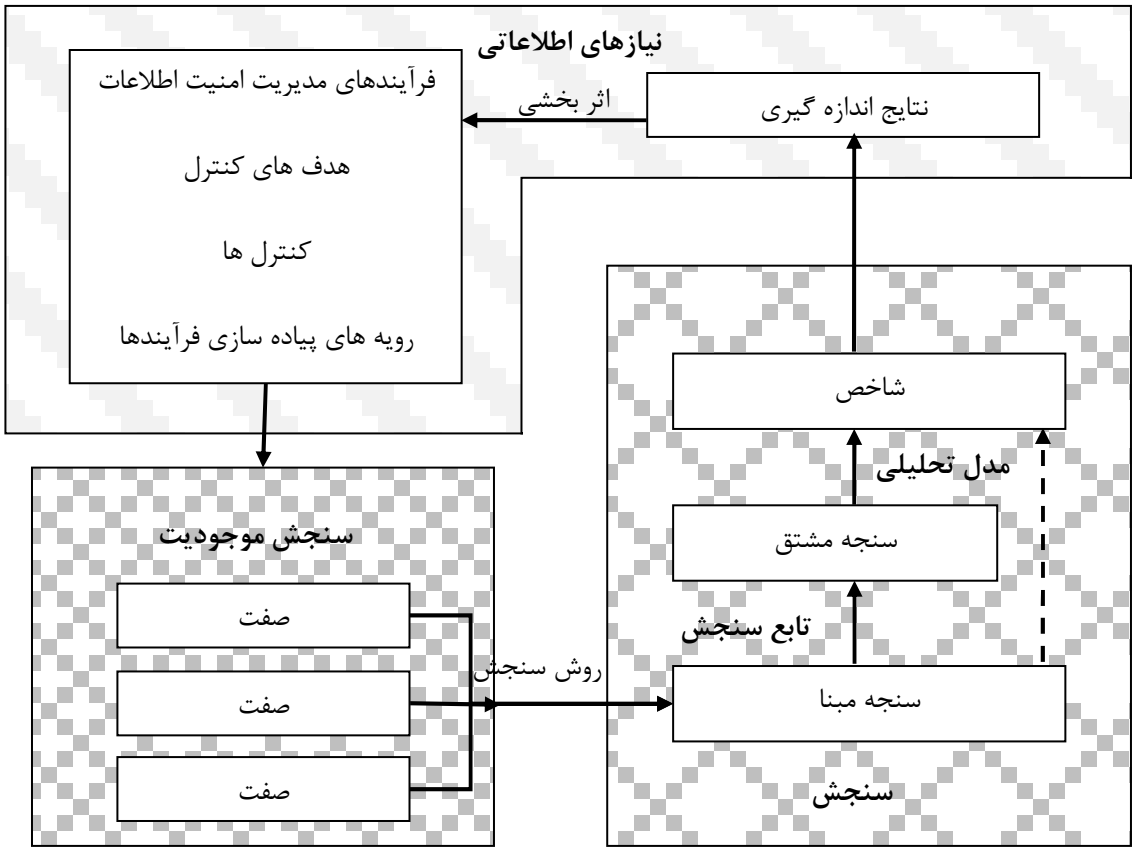
3- Measurment process

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

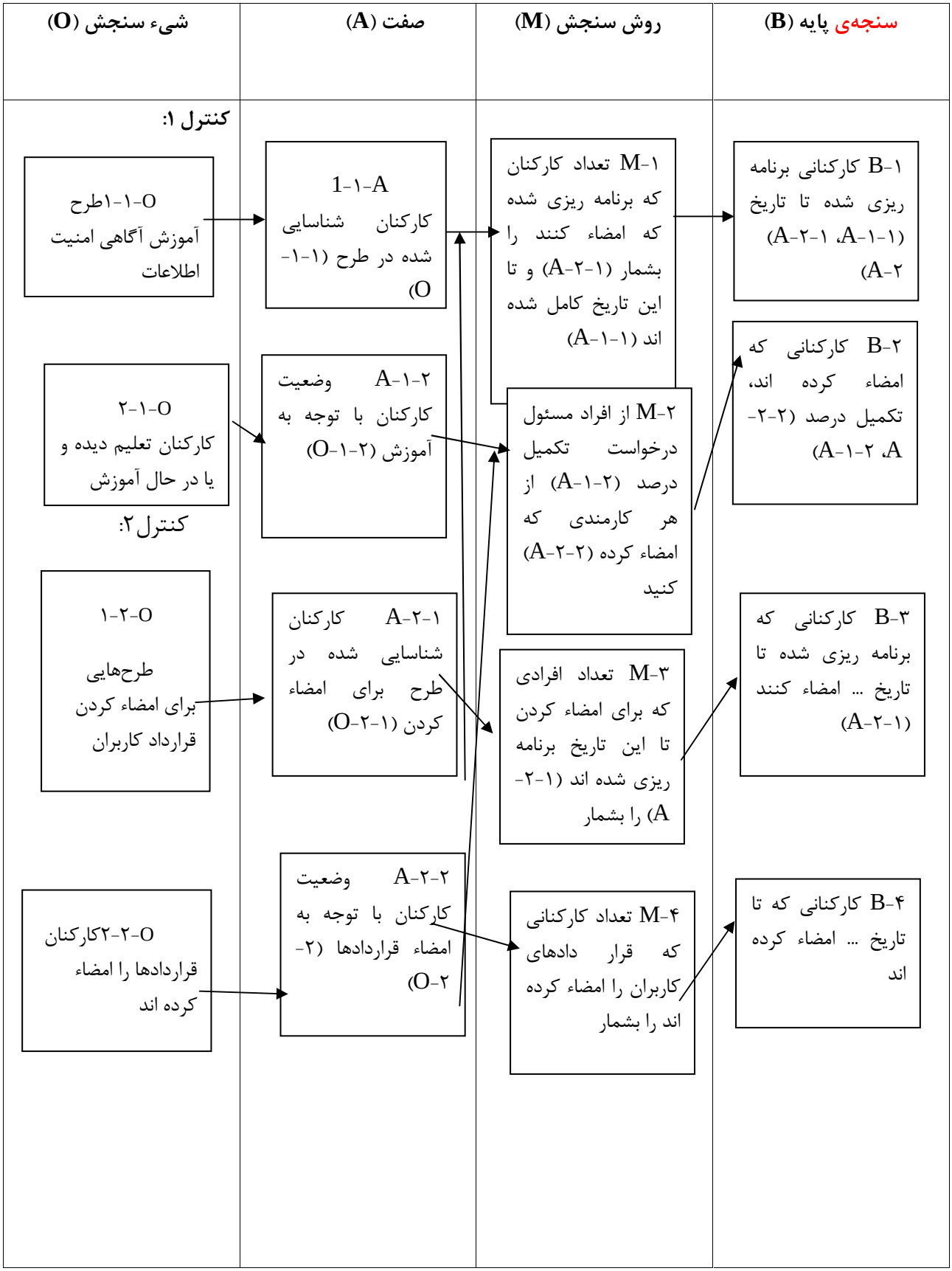
- «کنترل ۲» به مدیریت مسئولیت کنترل ۱-۲-۸-الف در استاندارد ملی ایران - ایزو - آی ای سی ۲۷۰۰۱ - سال ۸۷ اشاره می‌کند («مدیریت باید مستخدمین، پیمان کاران و کاربران شخص ثالث را مستلزم به کار بردن امنیت مطابق با سیاست‌های اتخاذ شده و رویه‌های سازمان کند»)، که به صورت زیر پیاده سازی شده: «تمام کارمندان مربوط 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

۳-۴-۵ سنجه مشتق و تابع سنجش

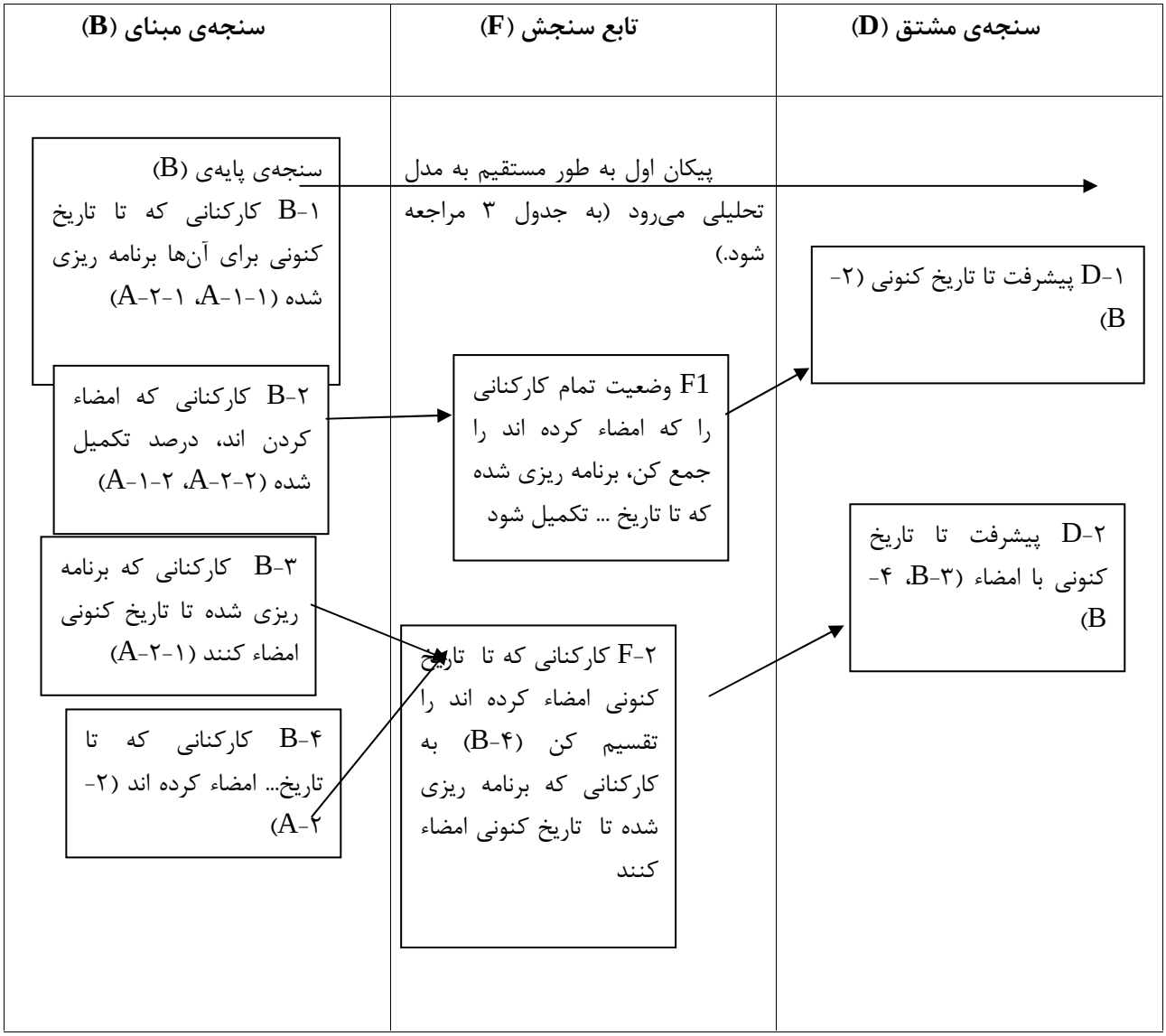
سنجه‌ی مشتق مجموع دو یا بیشتر از سنجه‌های مبنا است. یک سنجه‌ی مبنای داده شده مجاز است که به عنوان ورودی برای چندین سنجه‌ی مشتق به کار رود.

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.

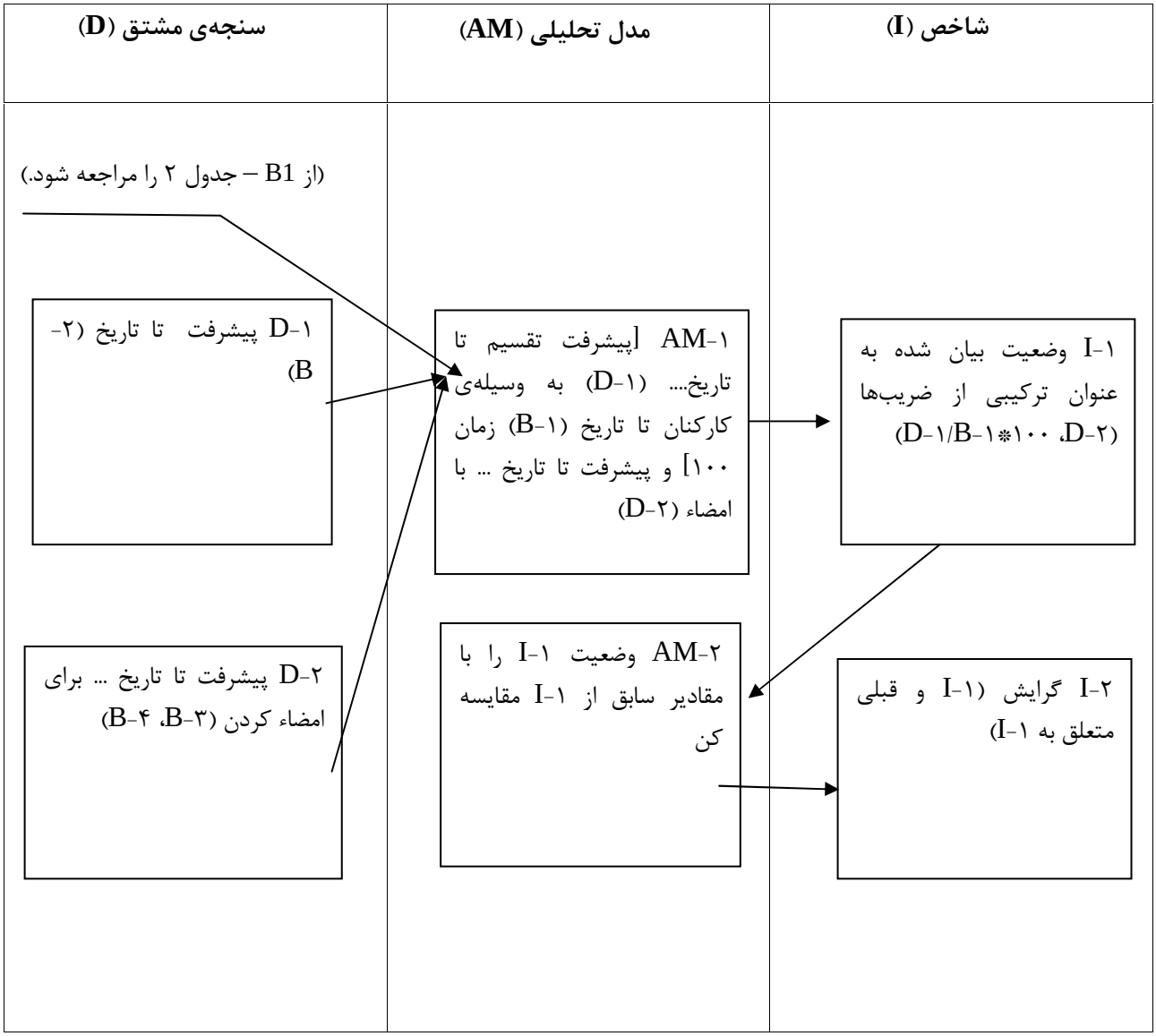


جدول ۲- مثالی از سنجه‌ی مشتق و تابع سنجش

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.

۳-۷ 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.

۸-۷ 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