ISIRI-ISO/IEC
27001
1st. edition

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

استاندارد ایران-ایزو- آی ای سی
۲۷۰۰۱
چاپ اول

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

Information technology - Security techniques - Information security management systems – Requirements

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران
تهران - خیابان ولیعصر، ضلع جنوبی میدان ونک، پلاک ۱۲۹۴، صندوق پستی: ۶۱۳۹-۱۴۱۵۵
تلفن: ۵-۸۸۸۷۹۴۶۱
دورنگار: ۸۸۸۸۷۰۸۰ و۸۸۸۸۷۱۰۳
کرج - شهر صنعتی، صندوق پستی ۱۶۳-۳۱۵۸۵
تلفن: ۸- ۲۸۰۶۰۳۱(۰۲۶۱)
دورنگار: ۲۸۰۸۱۱۴ (۰۲۶۱)
پیام نگار: standard@isiri.org.ir
وب‌گاه: www.isiri.org
بخش فروش، تلفن: ۲۸۱۸۹۸۹ (۰۲۶۱)، دورنگار: ۲۸۱۸۷۸۷ (۰۲۶۱)
بها: ۴۶۲۵ ریال

Institute of Standards and Industrial Research of IRAN
Central Office: No.1294 Valiaser Ave. Vanak corner, Tehran, Iran
P. O. Box: 14155-6139, Tehran, Iran
Tel: +98 (21) 88879461-5
Fax: +98 (21) 88887080, 88887103
Headquarters: Standard Square, Karaj, Iran
P.O. Box: 31585-163
Tel: +98 (261) 2806031-8
Fax: +98 (261) 2808114
Email: standard @ isiri.org.ir
Website: www.isiri.org
Sales Dep.: Tel: +98(261) 2818989, Fax.: +98(261) 2818787
Rls. 4625 Price:

به‌نام 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 رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون های 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، فن‌آوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می‌شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذیصلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر 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 بین المللی استاندارد (ISO)[1] کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC) [5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور، از آخرین پیشرفتهای علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران می‌تواند با رعایت موازین پیش‌بینی 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 بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سا زمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، مؤسسهٔ استاندارد این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آنها نظارت می کند .ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این مؤسسه است.

---

* موسسهٔ استاندارد و تحقیقات صنعتی ایران

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

کمیسیون فنی تدوین استاندارد

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

رئیس:	**سمت و/ یا نمایندگی**
حسینی خیاط، سعید (دکترای مهندسی برق)	عضو هیات علمی دانشکده مهندسی دانشگاه فردوسی مشهد
دبیر:	
خانیکی، رضا (لیسانس مهندسی برق - مخابرات)	اداره کل استاندارد و تحقیقات صنعتی خراسان رضوی
سهی زاده ابیانه ، محمد رضا (فوق لیسانس مهندسی مخابرات- رمز)	شرکت صنایع الکترونیک زعیم (سهامی خاص)
اعضاء: (اسامی به ترتیب حروف الفبا)	
اثنی عشری، امیر مهدی (لیسانس مهندسی برق - کنترل)	موسسه تحقیقات و فن‌آوری پارس
خانیکی ، مریم (فوق لیسانس مدیریت)	شرکت نفت ایران (سهامی عام)
رضایی، امید (فوق لیسانس مهندسی مخابرات- رمز)	شرکت مهندسی ایمن رایانه شرق (سهامی خاص)
روشن روان، راما (لیسانس مهندسی کامپیوتر – نرم‌افزار)	بانک رفاه
صمدی ، فرشید (لیسانس مهندسی صنایع)	موسسه تحقیقات و فن‌آوری پارس
ضیاء علی نسب‌پور، مسعود (فوق لیسانس مهندسی پزشکی)	شرکت صنایع الکترونیک زعیم (سهامی خاص)
مهدوی اردستانی ، سید علیرضا	کارشناس آزاد

فهرست مندرجات

ادامه فهرست مندرجات

عنوان صفحه

پیش گفتار

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

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

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

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

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

۰ مقدمه

۰-۱ کلیات

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

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

۰-۲ دیدگاه فرآیند گرا[2]

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

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

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

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

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

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

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

د) بهبود مستمر برپایه اندازه‌گیری اهداف.

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

1- Interested parties
2- Process approach

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

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

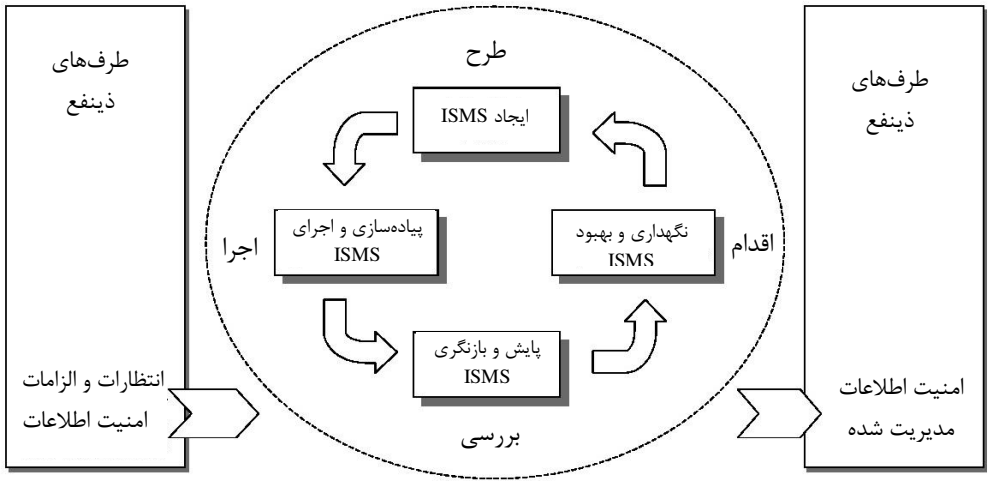
مثال ۱:

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

مثال ۲:

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

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



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

2- Breaches of Information Security

3- Embarrassment

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

۰-۳ سازگاری با سایر سیستم‌های مدیریتی

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

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

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

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

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

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

۱ هدف و دامنه کاربرد

۱-۱ کلیات

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

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

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

۱-۲ کاربرد

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

1- Enterprises
2- Non-profit organizations

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

۲ مراجع الزامی

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

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

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

۳ اصطلاحات و تعاریف

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

۳-۱

دارایی[2]

هر چیزی که برای سازمان دارای ارزش است .

[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

۳-۲

دسترس پذیری[3]

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

[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

۳-۳

محرمانگی[5]

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

[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

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

۴-۳

امنیت اطلاعات[1]

حفظ محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات. همچنین، ویژگی‌هایی از قبیل سندیت[2]، پاسخگویی[3]، انکارناپذیری[4] و قابلیت اطمینان[5]، می‌تواند لحاظ شوند.

[ISO/IEC 17799-1:2005]

۵-۳

رویداد امنیت اطلاعات[6]

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

[ISO/IEC TR 18044:2004]

۶-۳

حادثه امنیت اطلاعات[8]

یک یا مجموعه‌ای از رویدادهای امنیت اطلاعات ناخواسته یا پیش‌بینی نشده که به احتمال زیاد، عملیات کسب وکار را به خطر انداخته و امنیت اطلاعات را تهدید کنند.

[ISO/IEC TR 18044:2004]

۷-۳

سیستم مدیریت امنیت اطلاعات[9] (ISMS)

قسمتی از سیستم مدیریت کلان، بنا شده بر دیدگاه ریسک‌های کسب‌وکار، به منظور ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری و بهبود امنیت اطلاعات.

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

۸-۳

یکپارچگی[10]

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

[استاندارد ملی ایران به شماره ۱-۹۹۷۰]

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

۹-۳

ریسک باقیمانده[1]

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

۱۰-۳

پذیرش ریسک[2]

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

۱۱-۳

تحلیل ریسک[3]

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

۱۲-۳

برآورد ریسک[6]

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

۱۳-۳

ارزیابی ریسک[7]

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

۱۴-۳

مدیریت ریسک[8]

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

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

۳-۱۵

برطرف‌سازی ریسک[1]

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

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

۳-۱۶

بیانیه کاربست‌پذیری[3]

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

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

۴ سیستم مدیریت امنیت اطلاعات

۴-۱- الزامات عمومی

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

۴-۲ ایجاد و مدیریت سیستم امنیت اطلاعات

۴-۲-۱ ایجاد سیستم مدیریت امنیت اطلاعات

سازمان باید موارد ذیل را انجام دهد:

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

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

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

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

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

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

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

۵- توسط مدیریت تصویب شود.

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

پ- تعریف رویکرد برآورد ریسک سازمان.

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

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

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

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

ت- شناسایی ریسک.

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

۲- شناسایی تهدیدهای متوجه آن دارایی‌ها.

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

ث- تحلیل و ارزیابی ریسک .

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

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

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

۳- تخمین سطوح ریسک .

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

ج- شناسایی و ارزیابی گزینه‌هایی برای برطرف‌سازی ریسک .

اقدامات ممکن شامل:

۱- به کار گرفتن کنترل‌های مناسب.

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

۳- اجتناب از ریسک[1] ، و

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

چ- گزینش اهداف کنترلی و کنترل‌ها برای برطرف‌سازی ریسک .

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

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

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

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

ح- دریافت مصوبه مدیریت برای ریسک‌های باقیمانده پیشنهاد شده.

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

د- تهیه بیانیه کاربست‌پذیری.

باید یک بیانیه کاربست‌پذیری، شامل موارد ذیل تهیه شود:

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

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

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

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

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

سازمان باید موارد ذیل را انجام دهد:

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

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

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

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

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

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

ج- مدیریت عملیات سیستم مدیریت امنیت اطلاعات.

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

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

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

سازمان باید موارد ذیل را انجام دهد:

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

1- Formulate

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

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

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

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

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

۱- سازمان.

۲- فن‌آوری.

۳- اهداف و فرآیند های کسب وکار.

۴- تهدیدهای شناسایی شده.

۵- اثربخشی کنترل‌های پیاده‌سازی شده، و

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

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

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

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

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

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

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

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

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

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

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

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

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

۴-۳ الزامات مستندسازی

۴-۳-۱ کلیات

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

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

مستندسازی سیستم مدیریت امنیت اطلاعات باید شامل موارد ذیل باشد:

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

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

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

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

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

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

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

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

خ- بیانیه کاربست‌پذیری.

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

1- Documented

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

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

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

۴-۳-۲ کنترل مدارک

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

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

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

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

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

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

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

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

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

ط- پیشگیری از استفاده ناخواسته از مدارک منسوخ، و

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

۴-۳-۳ کنترل سوابق

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

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

مثال :

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

1- Dispose

۵ مسوولیت مدیریت

۵-۱ تعهد مدیریت

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

الف- ایجاد یک خط‌مشی سیستم مدیریت امنیت اطلاعات.

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

پ- ایجاد نقش‌ها و مسوولیت‌ها برای امنیت اطلاعات.

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

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

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

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

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

۵-۲ مدیریت منابع

۵-۲-۱ فراهم‌آوری منابع

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

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

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

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

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

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

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

۵-۲-۲ آموزش، آگاه‌سازی و صلاحیت

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

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

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

پ- ارزیابی اثربخشی اقدامات انجام شده، و

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

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

۶ ممیزی داخلی سیستم مدیریت امنیت اطلاعات

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

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

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

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

ت- آن‌گونه که انتظار می‌رود، اجرا می‌شوند.

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

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

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

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

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

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

6- Guidelines

۷ بازنگری مدیریت سیستم مدیریت امنیت اطلاعات

۷-۱ کلیات

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

۷-۲ ورودی‌های بازنگری

ورودی‌های بازنگری مدیریت، باید شامل موارد ذیل باشند:

الف- نتایج ممیزی‌ها و بازنگری‌های سیستم مدیریت امنیت اطلاعات.

ب- بازخورهای طرف‌های ذینفع.

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

ت- وضعیت اقدامات اصلاحی و پیشگیرانه.

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

ج- نتایج حاصل از اندازه‌گیری‌های اثربخشی.

چ- اقدامات پیگیرانه از بازنگری‌های قبلی مدیریت.

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

خ- توصیه‌هایی برای بهبود.

۷-۳ خروجی‌های بازنگری

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

الف- بهبود اثربخشی سیستم مدیریت اطلاعات.

ب- به روزآوری برآورد ریسک و طرح‌های برطرف‌سازی ریسک.

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

۱- الزامات کسب وکار.

۲- الزامات امنیتی.

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

۴- الزامات آیین‌نامه‌ای یا قانونی.

۵- تعهدات قراردادی، و

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

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

۸ بهبود سیستم مدیریت امنیت اطلاعات

۸-۱ بهبود مستمر

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

۸-۲ اقدام اصلاحی

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

۸-۳ اقدام پیشگیرانه

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

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

پیوست الف

(الزامی)

اهداف کنترلی و کنترل‌ها

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

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

جدول الف-۱- اهداف کنترلی

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

جدول الف-۱-ادامه

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

جدول الف-۱-ادامه

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

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

جدول الف-۱-ادامه

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

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

جدول الف-۱-ادامه

الف-۹ امنیت فیزیکی و محیطی

1- Orderly manner

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

جدول الف-۱-ادامه

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

1- Premises
2- Supporting utilities

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

جدول الف-۱-ادامه

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

1- Overwritten
2- Modification

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

جدول الف-۱-ادامه

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

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

جدول الف-۱-ادامه

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

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

جدول الف-۱-ادامه

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

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

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

جدول الف-۱-ادامه

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

4- Privilege management

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

جدول الف-۱-ادامه

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

1- Remote diagnostic
2- Remote configuration

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

جدول الف-۱-ادامه

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

1- Session Time-out

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

جدول الف-۱-ادامه

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

1- Validation

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

جدول الف-۱-ادامه

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

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

جدول الف-۱-ادامه

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

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

جدول الف-۱-ادامه

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

1- Loss
2- Destruction
3- Falsification

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

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

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

جدول ب-۱- اصول OECD و مدل PDCA

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

جدول ب-۱-ادامه

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

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

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

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

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

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

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

جدول پ-۱-ادامه

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

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

کتابنامه

انتشارات استانداردها

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

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

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

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

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

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

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

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

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

سایر انتشارات

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

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

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

ICS: 35.040

صفحه : ۳۷