INSO-ISO-IEC

27001

2nd Revision

2024

Identical with
ISO/IEC 27001:
2022

جمهوری اسلامی ایران

Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iran National Standards Organization

استاندارد ملی ایران-
ایزو-آی ای سی

۲۷۰۰۱

تجدیدنظر دوم

۱۴۰۲

# امنیت اطلاعات، امنیت سایبری و حفاظت از حریم خصوصی- سامانه مدیریت امنیت اطلاعات- الزامات

# Information security, cybersecurity and privacy protection- Information security management systems- Requirements

ICS: 35.040

**استاندارد ملی ایران-ایزو-آی ای سی شماره۲۷۰۰۱ (تجدیدنظر دوم): سال ۱۴۰۲**

**سازمان ملی استاندارد ایران**

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸-۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@inso.gov.ir

وبگاه: http://www.inso.gov.ir

**Iranian National Standardization Organization (INSO)**

No. ۲۵۹۲ Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@inso.gov.ir

Website: http://www.inso.gov.ir

## به نام خدا

## آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۷ قانون تقویت و توسعه نظام استاندارد ، ابلاغ‌شده در دی ماه ۱۳۹۶، وظیفهٔ تعیین، تدوین، به‌روزرسانی و نشر استانداردهای ملی را بر عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی 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 واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع سودبر و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی 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 پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام واردات، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادرات و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سامانه‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه 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 بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

---

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

## کمیسیون فنی تدوین استاندارد

## «امنیت اطلاعات، امنیت سایبری و حفاظت از حریم خصوصی- سامانه مدیریت امنیت اطلاعات- الزامات»

| **رئیس:** | **سمت و/یا محل اشتغال:** |
|---|---|
| گازرانی فراهانی، حدیث<br>(کارشناسی مهندسی برق الکترونیک) | سازمان فناوری اطلاعات ایران |
| **دبیر:** | |
| گلستانی، امین<br>(دکتری مدیریت استراتژیک) | سازمان فناوری اطلاعات ایران |
| **اعضا:** (اسامی به ترتیب حروف الفبا) | |
| بسطامی، خلیل<br>(دکتری مهندسی کامپیوتر) | عضو کارگروه فاوا - فرهنگستان زبان و ادب فارسی |
| تاج، نسرین<br>(دکتری مدیریت اجرایی) | عضو کارگروه ارزیابی گزارشات رصدی تحلیلی و راهبردی- پژوهشگاه فناوری اطلاعت و ارتباطات |
| علیرضا، حجازی<br>(کارشناس ارشد روابط بین‌الملل) | پژوهشگر- فرهنگستان زبان و ادب فارسی |
| سهرابی صابر، حسن<br>(کارشناسی مهندسی کامپیوتر) | کارشناس اداره زیرساخت و پشتیبانی فناوری اطلاعات - بانک مرکزی |
| طی‌نیا، رضا<br>(کارشناسی ارشد مدیریت فناوری اطلاعات) | مدیرعامل - شرکت مهندسی کاربرد سیستم سدید |
| عروجی، سید مهدی<br>(کارشناسی ارشد فناوری اطلاعات) | رییس گروه تدوین استاندارد - سازمان تنظیم مقررات و ارتباطات رادیویی |
| غریبی سبیل، مینو<br>(کارشناسی ارشد مهندسی فناوری اطلاعات) | مدیر حوزه خدمات افتا - مرکز مدیریت افتا |
| کاظمی، پروانه<br>(کارشناسی ارشد امنیت) | کارشناس ارشد امنیت سامانه‌ها - پلیس فتا |

**اعضا:** (اسامی به ترتیب حروف الفبا)

گرجی، مهدی
(.کارشناسی ارشد فناوری اطلاعات)

نسیمی، زینب
(کارشناسی مهندسی کامپیوتر)

یوسف‌زاده، بهاره
(کارشناس ارشد مدیریت)

**سمت و/یا محل اشتغال:**

رییس فناوری اطلاعات - پژوهشگاه استاندارد سازمان ملی استاندارد ایران

سازمان فناوری اطلاعات ایران

رییس گروه برق الکترونیک - دفتر نظارت بر استاندارد صنایع فلزی سازمان ملی استاندارد ایران

**ویراستار:**

مقبلی کهن‌زاد، فاطمه
(کارشناسی تکنولوژی فناوری اطلاعات- گرایش فناوری اطلاعات)

کارشناس تدوین و ترویج - اداره کل استاندارد استان گیلان

## فهرست مندرجات

**عنوان** **صفحه**

**عنوان** **صفحه**

## پیش‌گفتار

استاندارد «امنیت اطلاعات، امنیت سایبری و حفاظت از حریم خصوصی- سامانه مدیریت امنیت اطلاعات– الزامات» که نخستین‌بار در سال ۱۳۸۷ تدوین و منتشر شد، بر اساس پیشنهادهای دریافتی و بررسی و تأیید کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی به‌عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند۷، استاندارد ملی ایران شماره ۵ برای دومین بار مورد تجدید نظر قرار گرفت و در هفتصد و سی و چهارمین اجلاسیه کمیته ملی فناوری اطلاعات مورخ ۱۴۰۲/۱۱/۱۴ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۷ قانون تقویت و توسعه نظام استاندارد، ابلاغ‌شده در دی ماه ۱۳۹۶، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در بافت صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد جایگزین استاندارد ملی ایران شمارهٔ INSO-ISO-IEC ۲۷۰۰۱ : سال ۱۳۹۴می‌شود.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection Information- security management systems- Requirements

## مقدمه

### ۰-۱ کلیات

هدف از تدوین این استاندارد، تعیین الزامات برای استقرار، پیاده‌سازی، نگه‌داری و بهبود مستمر سامانه مدیریت امنیت اطلاعات است. پذیرش سامانه مدیریت امنیت اطلاعات، تصمیمی راهبردی برای سازمان است. استقرار و پیاده‌سازی سامانه مدیریت امنیت اطلاعات تحت تأثیر نیازها و اهداف و الزامات امنیتی‌سازمان، فرایندهای سازمانی مورداستفاده و اندازه و ساختار سازمان است. انتظار می‌رود به مرورزمان، هرکدام از این عوامل تأثیرگذار، تغییر کند.

سامانه مدیریت امنیت اطلاعات از محرمانگی، یکپارچگی و در دسترس‌بودن اطلاعات با به‌کاربردن فرایند مدیریت مخاطرات محافظت می‌کند و به ذی‌نفعان اطمینان می‌دهد که مخاطرات به حد کافی مدیریت می‌شود.

مهم است که سامانه مدیریت امنیت اطلاعات، جزئی از فرایندهای سازمان و ساختار کلی مدیریتی و به‌صورت یکپارچه با آن باشد و امنیت اطلاعات در طراحی فرایندها، سامانه اطلاعات و کنترل‌ها در نظر گرفته شود. انتظار می‌رود پیاده‌سازی سامانه مدیریت امنیت اطلاعات، متناسب با نیازهای سازمان باشد.

این استاندارد، می‌تواند توسط طرف‌های درونی و بیرونی، برای ارزیابی توانایی سازمان در برآورده‌سازی الزامات امنیت اطلاعات خود سازمان به کار برده شود.

ترتیب ارائهٔ الزامات در این استاندارد، منعکس‌کننده اهمیت یا ترتیب پیاده‌سازی آن‌ها نیست. اقلام فهرست‌شده، فقط برای ارجاع، شماره‌گذاری شده‌اند.

استاندارد ISO/IEC 27000 مرور کلی و واژگان سامانه‌های مدیریت امنیت اطلاعات را توصیف می‌کند که به خانواده استانداردهای سامانه مدیریت امنیت اطلاعات اشاره دارد. (شامل استانداردهای ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005)

### ۰-۲ انطباق با دیگر استانداردهای سامانه مدیریتی

این استاندارد، ساختار سطح بالا، عناوین زیر بند یکسان، متن یکسان، عبارات مشترک، و تعاریف پایه تعریف‌شده در Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement، را به کار می‌برد و بنابراین انطباق با دیگر استانداردهای سامانه مدیریتی که Annex SL را قبول کرده‌اند، را حفظ می‌کند.

این رویکرد مشترک که در Annex SL تعریف شده است، برای آن دسته از سازمان‌هایی که در نظر دارند یک سامانه مدیریت واحد برای برآورده‌سازی الزامات دو یا چند استاندارد سامانه مدیریت، عملیاتی کنند، مفید خواهد بود.

# امنیت اطلاعات، امنیت سایبری و حفاظت از حریم خصوصی- سامانه مدیریت امنیت اطلاعات– الزامات

## ۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین الزاماتی برای استقرار، پیاده‌سازی، نگه‌داری و بهبود مستمر سامانه مدیریت امنیت اطلاعات در بافت[1] سازمان است. این استاندارد همچنین شامل الزامات ارزیابی[2] و برطرف‌سازی[3] مخاطرات امنیت اطلاعات است که متناسب با نیازهای سازمان است. الزامات بیان‌شده در این استاندارد، عمومی بوده و قصد آن است که در کلیه سازمان‌ها، صرف‌نظر از نوع، اندازه و ماهیت، کاربردپذیر باشند. کنارگذاری هر یک از الزامات مشخص‌شده در بندهای ۴ تا ۱۰ هنگامی‌که سازمان ادعای انطباق با این استاندارد را دارد، قابل‌پذیرش نیست.

## ۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آن‌ها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شود. در صورتی که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مرجع زیر برای کاربرد این استاندارد الزامی است:

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

**یادآوری-** استاندارد ملی ایران شماره ۲۷۰۰۰ INSO-ISO-IEC سال ۱۳۹۴، فناوری اطلاعات- فنون امنیتی- سیستم‌های (سامانه‌های) مدیریت امنیت اطلاعات- مرور کلی و واژگان با استفاده از استاندارد ISO/IEC 27000:2014 تدوین شده‌است.

1- Context
2- Assessmen
3- Treatment

## ۳ اصطلاحات، تعاریف و کوته‌نوشت‌ها

در این استاندارد اصطلاحات و تعاریف ارائه‌شده در استاندارد **ISO/IEC 27000** به کار می‌رود.[۱]

## ۴ بافت سازمان

### ۴-۱ درک[۲] سازمان و بافت[۳] آن

سازمان باید عوامل درونی و بیرونی که مرتبط با مقصود[۴] خود است و بر قابلیت آن، برای حصول نتایج تعیین‌شده سامانه مدیریت امنیت اطلاعات تأثیرگذار است را تعیین کند.

**یادآوری-** تعیین این عوامل به بافت بیرونی و درونی سازمان که در زیربند ۵-۴-۱ استاندارد ملی ایران شماره ۱۳۲۴۵ سال: ۱۳۹۸، در نظر گرفته‌شده، اشاره دارد.

### ۴-۲ درک نیازها و انتظارات طرف‌های ذی‌نفع[۵]

سازمان باید موارد زیر را تعیین کند:

الف- ذی‌نفعان مرتبط با سامانه مدیریت امنیت اطلاعات؛ و

ب- الزامات مرتبط با این ذی‌نفعان؛

پ- به کدام یک از این الزامات از طریق سامانه مدیریت امنیت اطلاعات رسیدگی خواهد شد.

**یادآوری-** الزامات ذی‌نفعان ممکن است شامل الزامات قانونی و مقررات تنظیمی و تعهدات قراردادی شود.

### ۴-۳ تعیین محدوده سامانه مدیریت امنیت اطلاعات

سازمان باید مرزها و کاربردپذیری سامانه مدیریت امنیت اطلاعات را به‌منظور استقرار محدوده آن، تعیین کند.

سازمان باید هنگام تعیین این محدوده موارد زیر را در نظر بگیرد:

الف- عوامل بیرونی و درونی اشاره‌شده در زیربند ۴-۱؛

ب- الزامات اشاره‌شده در زیربند ۴-۲؛

---

۱- اصطلاحات و تعاریف به‌کار رفته در استانداردهای ISO و IEC در وبگاه‌های www.iso.org/obp و www.electropedia.org/ قابل دسترس است.

2- Underestanding
3- Context
4- Purpose
5- Interested parties

پ- واسط‌ها[1] و وابستگی‌ها بین فعالیت‌هایی که توسط سازمان انجام می‌شوند و فعالیت‌هایی که توسط سازمان‌های دیگر انجام می‌شوند.

محدوده باید به‌صورت مستند در دسترس باشد.

### ۴-۴ سامانه مدیریت امنیت اطلاعات

سازمان باید سامانه مدیریت امنیت اطلاعات را مطابق با الزامات این استاندارد، شامل فرایندهای موردنیاز و تعاملات آن‌ها، مستقر، پیاده‌سازی و نگه‌داری نماید و به طور مستمر بهبود دهد.

## ۵ رهبری

### ۵-۱ رهبری و تعهد[2]

مدیریت ارشد باید رهبری و تعهد دررابطه با سامانه مدیریت امنیت اطلاعات را توسط موارد زیر نشان دهد[3]:

الف- اطمینان از این‌که خط‌مشی امنیت اطلاعات و اهداف امنیت اطلاعات مستقرشده و سازگار با جهت‌گیری راهبردی[4] سازمان است؛

ب- اطمینان از یکپارچه‌شدن الزامات سامانه مدیریت امنیت اطلاعات در فرایندهای سازمان؛

پ- اطمینان از این‌که منابع موردنیاز سامانه مدیریت امنیت اطلاعات در دسترس است؛

ت- برقراری ارتباط درباره اهمیت مدیریت امنیت اطلاعات اثربخش و اهمیت انطباق با الزامات سامانه مدیریت امنیت اطلاعات؛

ث- اطمینان از این‌که سامانه مدیریت امنیت اطلاعات نتیجه(های) موردنظر خود را به‌دست می‌آورد؛

ج- هدایت و پشتیبانی افراد به‌منظور مشارکت در اثربخشی سامانه مدیریت امنیت اطلاعات؛

چ- بهبود مستمر؛ و

ح- حمایت از سایر نقش‌های مدیریتی مرتبط برای نشان‌دادن رهبری آن‌ها به‌طوری‌که این رهبری در حوزه‌های مسئولیت آن‌ها به کار گرفته شود.

**یادآوری-** عبارت «کسب‌وکار» در این استاندارد را می‌توان به‌طور گسترده به معنای آن دسته از فعالیت‌هایی تفسیر کرد که هسته اصلی اهداف وجودی سازمان هستند.

---

1- Interface
2- Commitment
3- Demonstrate
4- Strategic direction

### ۵-۲ خط مشی

مدیریت ارشد باید یک خط‌مشی امنیت اطلاعات ایجاد کند که؛

الف- متناسب با مقصود سازمان است؛

ب- شامل اهداف امنیت اطلاعات (به زیربند ۶-۲ مراجعه شود) است یا چارچوبی برای تعیین اهداف امنیت اطلاعات فراهم می‌کند؛

پ- شامل تعهد به برآورده‌سازی الزامات کاربردپذیر مرتبط با امنیت اطلاعات باشد؛

ت- شامل تعهد به بهبود مستمر سامانه مدیریت امنیت اطلاعات باشد.

خط‌مشی امنیت اطلاعات باید:

ث- به‌عنوان اطلاعات مستند در دسترس باشد؛

ج- درون سازمان اطلاع‌رسانی شده[1] باشد؛

چ- به طور مناسب، در دسترس ذی‌نفعان باشد.

### ۵-۳ نقش‌ها، مسئولیت‌ها و اختیارات سازمانی

مدیریت ارشد باید اطمینان حاصل کند که مسئولیت‌ها و اختیارات، برای نقش‌های مرتبط با امنیت اطلاعات در سازمان، اختصاص‌یافته و اطلاع‌رسانی شده است.

مدیریت ارشد مسئولیت‌ها و اختیارات را برای موارد زیر اختصاص دهد:

الف- اطمینان از این‌که سامانه مدیریت امنیت اطلاعات با الزامات این استاندارد منطبق است؛

ب- گزارش‌دهی عملکرد سامانه مدیریت امنیت اطلاعات برای مدیریت ارشد.

**یادآوری-** مدیریت ارشد همچنین می‌تواند مسئولیت‌ها و اختیاراتی برای گزارش‌دهی عملکرد سامانه مدیریت امنیت اطلاعات در سازمان اختصاص دهد.

1- Comunicated

# ۶ طرح‌ریزی

## ۶-۱ اقدامات رسیدگی[1] به مخاطرات و فرصت‌ها

### ۶-۱-۱ کلیات

هنگام طرح‌ریزی سامانه مدیریت امنیت اطلاعات، سازمان باید عوامل اشاره‌شده در زیربند ۴-۱ و الزامات اشاره‌شده در زیربند ۴-۲ را در نظر گرفته و مخاطرات و فرصت‌هایی که نیاز است رسیدگی شود را، برای موارد زیر، تعیین کند:

الف- اطمینان از این‌که سامانه مدیریت امنیت اطلاعات می‌تواند به نتایج موردنظر دست یابد؛

ب- اجتناب یا کاهش تأثیرات نامطلوب؛

پ- دستیابی به بهبود مستمر؛

سازمان باید موارد زیر را طرح‌ریزی کند:

ت- اقدامات برای رسیدگی به این مخاطرات و فرصت‌ها؛ و

ث- چگونه:

۱- یکپارچه‌سازی و پیاده‌سازی اقدامات را در فرایندهای سامانه مدیریت امنیت اطلاعات انجام دهد؛ و

۲- اثربخشی این اقدامات را ارزشیابی کند.

### ۶-۱-۲ ارزیابی مخاطرات امنیت اطلاعات

سازمان باید یک فرایند ارزیابی مخاطرات تعریف کرده و به کار گیرد که:

الف- معیارهای مخاطرات امنیت اطلاعات را تعیین و نگه‌داری کند که شامل موارد زیر است:

۱- معیارهای پذیرش مخاطرات؛ و

۲- معیارهایی برای انجام ارزیابی‌های مخاطرات امنیت اطلاعات؛

ب- اطمینان از این‌که تکرار ارزیابی‌های مخاطرات امنیت اطلاعات نتایج سازگار، معتبر و قیاس‌پذیر تولید می‌کند؛

پ- شناسایی مخاطرات امنیت اطلاعات:

1- Address

۱- اعمال فرایند ارزیابی مخاطرات امنیت اطلاعات برای شناسایی مخاطرات مرتبط با ازدست‌دادن محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات در محدوده سامانه مدیریت امنیت اطلاعات؛ و

۲- شناسایی مالکان مخاطرات؛

ت- تحلیل‌های مخاطرات امنیت اطلاعات:

۱- ارزیابی پیامدهای بالقوه که ممکن است در صورت تحقق مخاطرات شناسایی‌شده در زیربند ۶-۱-۲ پ) ۱) رخ دهد؛

۲- ارزیابی واقع‌بینانه احتمال وقوع مخاطرات شناسایی‌شده در زیربند ۶-۱-۲ پ) ۱)؛ و

۳- تعیین سطوح مخاطرات؛

ث- ارزشیابی مخاطرات امنیت اطلاعات:

۱- مقایسه نتایج تحلیل مخاطرات با معیار معین شده مخاطرات در زیربند ۶-۱-۲ الف)؛

۲- اولویت‌بندی مخاطرات تحلیل‌شده برای برطرف‌سازی مخاطرات؛

سازمان باید اطلاعات مستند در مورد فرایند ارزیابی مخاطرات امنیت اطلاعات را نگه‌داری کند.

### ۶-۱-۳ برطرف‌سازی مخاطرات امنیت اطلاعات

سازمان باید فرایند برطرف‌سازی مخاطرات امنیت اطلاعات را تعریف کرده و به‌کار گیرد برای:

الف- انتخاب گزینه‌های مناسب برطرف‌سازی مخاطرات امنیت اطلاعات با درنظرگرفتن نتایج ارزیابی مخاطرات؛

ب- تعیین همه کنترل‌هایی که برای پیاده‌سازی گزینه(های) انتخاب‌شده برای برطرف‌سازی مخاطرات امنیت اطلاعات لازم هستند؛

**یادآوری ۱-** سازمان‌ها می‌توانند کنترل‌های موردنیاز را طراحی نموده یا آن‌ها را از هر منبعی شناسایی کند.

پ- مقایسهٔ کنترل‌های تعیین‌شده در بالا (به زیربند ۶-۱-۳ ب مراجعه شود) با آن‌هایی که در پیوست الف هستند، و تصدیق اینکه هیچ کنترل موردنیازی حذف نشده است؛

**یادآوری ۲-** پیوست الف شامل فهرست کنترل‌های امنیت اطلاعات امکان‌پذیر است. کاربران این استاندارد به استفاده از پیوست الف هدایت می‌شوند تا اطمینان حاصل شود که هیچ کنترل امنیت اطلاعات ضروری نادیده گرفته نشده است.

**یادآوری ۳-** کنترل‌های امنیت اطلاعات فهرست‌شده در پیوست الف فراگیر نیستند و، درصورتِ نیاز، کنترل‌های امنیت اطلاعات دیگری افزوده می‌شوند.

ت- تهیه یک بیانیه کاربردپذیری که شامل:

- کنترل‌های ضروری (به زیربند ۶-۱-۳ ب) و پ) مراجعه شود)؛ و

- توجیه برای انتخاب آن‌ها؛

- فارغ از اینکه کنترل‌های ضروری پیاده‌سازی شده یا نشده باشند؛ و

- توجیه برای کنترل‌های انتخاب نشده از پیوست الف باشد.

ث- تدوین یک طرح برطرف‌سازی مخاطرات امنیت اطلاعات؛ و

ج- دریافت تأیید مالکان مخاطرات برای طرح برطرف‌سازی مخاطرات امنیت اطلاعات و پذیرش مخاطرات امنیت اطلاعات باقیمانده.

سازمان باید اطلاعات مستند در مورد فرایند برطرف‌سازی مخاطرات امنیت اطلاعات را نگه‌داری کند.

**یادآوری ۴**- فرایند ارزیابی و برطرف‌سازی مخاطرات امنیت اطلاعات در این استاندارد، هم‌راستا با اصول و راهنمایی‌های عمومی موجود در استاندارد ملی ایران شماره ۱۳۲۴۵: سال ۱۳۹۸، است.

### ۶-۲ اهداف امنیت اطلاعات و طرح‌ریزی برای دستیابی به آن‌ها

سازمان باید اهداف امنیت اطلاعات را در سطوح و کارکردهای مرتبط ایجاد کند.

اهداف امنیت اطلاعات باید:

الف- سازگار با خط‌مشی امنیت اطلاعات باشد؛

ب- قابل‌سنجش باشد (اگر عملی باشد)؛

پ- الزامات کاربردپذیر امنیت اطلاعات، نتایج ارزیابی مخاطرات و برطرف‌سازی مخاطرات را در نظر بگیرد؛

ت- پایش شود؛

ث- اطلاع‌رسانی شود؛ و

ج- به نحو مناسبی به‌روزرسانی شود؛

چ- به صورت اطلاعات مستند در دسترس باشد؛

سازمان باید اطلاعات مستند از اهداف امنیت اطلاعات را نگه‌داری کند.

زمانی که سازمان برای چگونگی تحقق اهداف امنیت اطلاعات طرح‌ریزی می‌کند، باید موارد زیر را تعیین کند:

ح- چه‌کارهایی انجام خواهند شد؛

خ- چه منابعی موردنیاز خواهد بود؛

د- چه افرادی پاسخگو خواهند بود؛

ذ- چه زمانی تکمیل خواهد شد؛ و

ر- چگونه نتایج ارزشیابی خواهند شد.

### ۶-۳ طرح‌ریزی تغییرات

هنگامی که سازمان نیاز به تغییرات در سامانه مدیریت امنیت اطلاعات را تشخیص دهد، تغییرات باید به‌صورت طرح‌ریزی‌شده انجام شود.

## ۷ پشتیبانی

### ۷-۱ منابع

سازمان باید منابع مورد نیاز برای استقرار، پیاده‌سازی، نگه‌داری و بهبود مستمر سامانه مدیریت امنیت اطلاعات را تعیین و فراهم آورد.

### ۷-۲ شایستگی

سازمان باید:

الف- شایستگی ضروری افرادی که تحت کنترل سازمان کار می‌کنند، و بر روی عملکرد امنیت اطلاعات تأثیرگذار هستند را تعیین کند؛

ب- از این‌که این افراد، بر اساس تحصیلات، آموزش‌ها، یا تجربیات مناسب، شایستگی دارند، اطمینان حاصل کند؛

پ- در صورت کاربردپذیربودن، اقداماتی برای به‌دست‌آوردن شایستگی لازم را انجام داده و اثربخشی اقدامات انجام‌گرفته را ارزشیابی کند؛ و

ت- اطلاعات مستند مناسب به‌عنوان شواهد شایستگی را نگه‌داری کند.

**یادآوری-** اقدامات کاربردپذیر، به‌عنوان نمونه، می‌تواند شامل مواردی مانند: فراهم‌آوری آموزش‌ها، کارورزی، یا جابه‌جایی کارکنان موجود، یا برون‌سپاری یا اشتغال افراد با شایسته باشد.

### ۷-۳ آگاهی

کارکنانی که تحت کنترل سازمان کار می‌کنند باید از موارد زیر آگاه باشند:

الف- خط‌مشی امنیت اطلاعات؛

ب- سهم خود در اثربخشی سامانه مدیریت امنیت اطلاعات، شامل مزایای بهبود عملکرد امنیت اطلاعات؛ و

پ- پیامدهای عدم انطباق با الزامات سامانه مدیریت امنیت اطلاعات.

### ۷-۴ ارتباطات

سازمان باید نیازهای ارتباطات درونی و بیرونی که به سامانه مدیریت امنیت اطلاعات مرتبط است را تعیین کند که شامل موارد زیر است:

الف- در مورد چه موضوعاتی ارتباط برقرار شود؛

ب- چه مواقعی ارتباط برقرار شود؛

پ- با چه افرادی ارتباط برقرار شود؛

ت- چگونه ارتباط برقرار می‌شود.

### ۷-۵ اطلاعات مستند

#### ۷-۵-۱ کلیات

سامانه مدیریت امنیت اطلاعات سازمان باید شامل موارد زیر باشد:

الف- اطلاعات مستند الزام‌شده توسط این استاندارد؛ و

ب- اطلاعات مستندی که توسط سازمان به‌عنوان موارد ضروری برای اثربخشی سامانه مدیریت امنیت اطلاعات تعیین‌شده‌اند.

**یادآوری-** گستره اطلاعات مستند برای سامانه مدیریت امنیت اطلاعات، می‌تواند از یک سازمان به سازمان دیگر بر اساس موارد زیر متفاوت باشد:

۱- اندازه سازمان و نوع فعالیت‌ها، فرایندها، محصولات و خدمات؛

۲- پیچیدگی فرایندها و تعاملات آن‌ها؛ و

۳- شایستگی کارکنان.

#### ۷-۵-۲ ایجاد و به‌روزرسانی

در هنگام ایجاد و به‌روزرسانی اطلاعات مستند، سازمان باید از مناسب‌بودن آن اطمینان حاصل کند:

الف- شناسایی و توصیف (مانند عنوان، تاریخ، نویسنده، یا شماره ارجاع)؛

ب- قالب (مانند زبان، نسخه نرم‌افزار، نگاره[1]) و رسانه (مانند کاغذ، الکترونیکی)؛ و

پ- بازنگری و تأیید مناسب‌بودن و کفایت آن‌ها.

1- Geraphics

### ۷-۵-۳ کنترل اطلاعات مستند

اطلاعات مستند الزام‌شده سامانه مدیریت امنیت اطلاعات و این استاندارد باید کنترل شود تا اطمینان حاصل شود که:

الف- این اطلاعات، در زمان و مکانی که به آن احتیاج است، در دسترس و مناسب برای استفاده است؛ و

ب- به‌اندازه کافی محافظت شده است (در مقابل فقدان محرمانگی، استفاده نادرست، یا از دست‌دادن یکپارچگی).

برای کنترل اطلاعات مستند، سازمان باید به فعالیت‌های زیر، در صورت کاربردپذیربودن بپردازد:

پ- توزیع، دسترسی، بازیابی و استفاده؛

ت- ذخیره‌سازی و محافظت، شامل حفظ خوانایی؛

ث-کنترل تغییرات (مانند کنترل نسخه)؛ و

ج- نگه‌داری و امحا.

اطلاعات مستند با منشأ خارجی که نیاز به آن برای طراحی و عملیاتی‌سازی سامانه مدیریت امنیت اطلاعات توسط سازمان تعیین‌شده است، باید به‌صورت مناسب، شناسایی‌شده و کنترل شود.

**یادآوری-** دسترسی، به‌صورت ضمنی، بیانگر تصمیمی مرتبط با مجوز صرفاً مشاهده اطلاعات، یا مجوز و اختیاردهی برای مشاهده و تغییر اطلاعات مستند و مواردی مانند آن می‌شود.

## ۸ عملیات

### ۸-۱ طرح‌ریزی و کنترل عملیات

سازمان باید فرایندهای موردنیاز برای برآورده‌سازی الزامات و پیاده‌سازی اقدامات تعیین‌شده در بند ۶ را، طرح‌ریزی، پیاده‌سازی و کنترل کند، توسط:

- مقررنمودن معیارهایی برای فرایندها؛

- پیاده‌سازی کنترل فرایندها مطابق با معیارها.

اطلاعات مستند، در حد ضروری برای حصول اطمینان از اینکه فرایندها به همان صورت که طرح‌ریزی‌شده‌اند، انجام می‌شود، در دسترس باشد.

سازمان باید تغییرات طرح‌ریزی‌شده را کنترل کند و تبعات تغییرات ناخواسته را بازنگری کند، و در صورت لزوم، اقدامات مناسبی برای کاهش هرگونه اثرات نامطلوب انجام دهد.

سازمان باید اطمینان یابد که فرایندها، محصولات یا خدمات برون‌سپاری شده مرتبط با سامانه مدیریت امنیت اطلاعات، تحت کنترل هستند.

### ۸-۲ ارزیابی[1] مخاطرات[2] امنیت اطلاعات

سازمان باید در بازه‌های طرح‌ریزی‌شده یا زمان‌هایی که تغییرات عمده‌ای پیشنهاد می‌شود یا اتفاق می‌افتد، ارزیابی مخاطرات امنیت اطلاعات را با درنظرگرفتن معیار تعیین‌شده در زیربند ۶-۱-۲ الف) انجام دهد.

سازمان باید اطلاعات مستند از نتایج ارزیابی مخاطرات امنیت اطلاعات را نگه‌داری کند.

### ۸-۳ برطرف‌سازی مخاطرات امنیت اطلاعات

سازمان باید طرح برطرف‌سازی مخاطرات امنیت اطلاعات را پیاده‌سازی کند.

سازمان باید اطلاعات مستند از نتایج برطرف‌سازی مخاطرات امنیت اطلاعات را نگه‌داری کند.

## ۹ ارزشیابی عملکرد

### ۹-۱ پایش، اندازه‌گیری، تحلیل و ارزشیابی

سازمان باید موارد زیر را تعیین کند:

الف- آنچه نیاز به پایش و اندازه‌گیری دارد، ازجمله فرایندها و کنترل‌های امنیت اطلاعات؛

ب- روش‌های پایش، اندازه‌گیری، تحلیل و ارزشیابی، برای اطمینان از نتایج معتبر، در صورت کاربرد. روش‌های انتخاب‌شده باید نتایج قابل‌مقایسه و تکرارپذیری تولید کنند تا معتبر در نظر گرفته شوند؛

پ- زمان پایش و اندازه‌گیری؛

ت- چه فردی باید پایش و اندازه‌گیری کند؛

ث- چه زمانی نتایج پایش و اندازه‌گیری تحلیل و ارزشیابی شوند؛

ج- چه فردی نتایج را تحلیل و ارزشیابی کند.

باید اطلاعات مستند مناسب، به‌عنوان شواهد نتایج پایش و سنجش، در دسترس باشد.

سازمان باید عملکرد امنیت اطلاعات و اثربخشی سامانه مدیریت امنیت اطلاعات را ارزشیابی کند.

---

1- Assessment

۲- با توجه به‌دست آوردن ارزش مخاطره و نه مقایسه آن از معادل ارزیابی مخاطرات استفاده شده است.

## ۹-۲ ممیزی داخلی

### ۹-۲-۱ کلیات

سازمان باید در بازه‌های زمانی برنامه‌ریزی‌شده ممیزی داخلی انجام دهد تا دربارهٔ وضعیت سامانه مدیریت امنیت اطلاعات در موارد زیر اطلاعات دهد:

الف- مطابقت با

۱- الزامات خود سازمان برای سامانه مدیریت امنیت اطلاعات آن؛

۲- الزامات این استاندارد؛

ب- به طور مؤثر پیاده‌سازی و نگه‌داری می‌شود.

### ۹-۲-۲ برنامه ممیزی داخلی

سازمان باید یک برنامهٔ ممیزی، شامل فراوانی، روش‌ها، مسئولیت‌ها، الزامات طرح‌ریزی و گزارش‌دهی را مستقر، پیاده‌سازی و نگه‌داری کند.

هنگام تهیه برنامه‌های ممیزی داخلی، سازمان باید اهمیت فرایندهای مرتبط و نتایج ممیزی‌های قبلی را در نظر بگیرد.

سازمان باید:

الف- معیار و محدودهٔ ممیزی را برای هر ممیزی تعریف کند؛

ب- ممیزان و ممیزی را به‌گونه‌ای انتخاب کند تا از عینیت و بی‌طرفی فرایند ممیزی اطمینان یابد؛

پ- از گزارش نتایج ممیزی به مدیر مرتبط اطمینان حاصل کند.

اطلاعات مستند به‌عنوان شواهد برنامه‌های ممیزی و نتایج ممیزی باید در دسترس باشد.

## ۹-۳ بازنگری مدیریت

### ۹-۳-۱ کلیات

مدیریت ارشد باید سامانه مدیریت امنیت اطلاعات سازمان را در بازه‌های زمانی برنامه‌ریزی‌شده بازنگری کند تا از تناسب، کفایت و اثربخشی آن اطمینان یابد.

### ۹-۳-۲ ورودی‌های بازنگری مدیریت

بازنگری مدیریت باید شامل ملاحظات زیر باشد:

الف- وضعیت اقدامات بازنگری‌های مدیریت قبلی؛

ب- تغییرات بیرونی و درونی که مرتبط با سامانه مدیریت امنیت اطلاعات هستند؛

پ- تغییرات نیازها و انتظارات ذی‌نفعان که مرتبط با سامانه مدیریت امنیت اطلاعات هستند؛

ت- بازخورد عملکرد امنیت اطلاعات، ازجمله روندهای:

۱- عدم انطباق‌ها و اقدامات اصلاحی؛

۲- نتایج پایش و اندازه‌گیری؛

۳- نتایج ممیزی؛

۴- تحقق اهداف امنیت اطلاعات؛

ث- بازخورد از ذی‌نفعان؛

ج- نتایج ارزیابی مخاطرات و وضعیت طرح مقابله با مخاطره؛

چ- فرصت‌های بهبود مستمر.

### ۹-۳-۳ نتایج بازنگری مدیریت

نتایج بازنگری مدیریت باید شامل تصمیم‌های مرتبط با فرصت‌های بهبود مستمر و هر نیازی برای تغییر در سامانه مدیریت امنیت اطلاعات باشد.

اطلاعات مستند باید به‌عنوان شواهد نتایج بازنگری‌های مدیریت در دسترس باشند.

## ۱۰ بهبود

### ۱۰-۱ بهبود مستمر

سازمان باید به‌صورت مستمر، تناسب، کفایت و اثربخشی سامانه مدیریت امنیت اطلاعات را بهبود دهد.

### ۱۰-۲ عدم انطباق و اقدامات اصلاحی

زمانی که عدم انطباق رخ می‌دهد، سازمان باید:

الف- به عدم انطباق واکنش نشان دهد و در صورت کاربرد:

۱- فعالیتی برای کنترل و اصلاح آن انجام دهد؛

۲- به پیامدها رسیدگی کند؛

ب- به‌منظور جلوگیری از تکرار آن عدم انطباق یا رخ‌دادن در جای دیگری، نیاز به اقدام برای حذف علت‌های عدم انطباق را ارزشیابی کند، با:

۱- بازنگری عدم انطباق؛

۲- تعیین علت‌های عدم انطباق؛ و

۳- تعیین اینکه آیا عدم انطباق‌های مشابه وجود دارد، یا امکان وقوع دارد؛

پ- پیاده‌سازی هر فعالیتی که نیاز است؛

ت- بازنگری اثربخشی هر اقدام اصلاحی انجام‌شده؛ و

ث- ایجاد تغییرات در سامانه مدیریت امنیت اطلاعات، اگر لازم باشد؛

اقدامات اصلاحی باید متناسب با تأثیرات عدم انطباق‌های اتفاق افتاده باشد.

اطلاعات مستند، به‌عنوان شواهد موارد زیر در دسترس باشد:

ج- ماهیت عدم انطباق و هر اقدامی که به‌تبع آن انجام‌شده است؛

چ- نتایج هر اقدام اصلاحی.

# پیوست الف

# (الزامی)

# مرجع کنترل‌های امنیت اطلاعات

کنترل‌های امنیت اطلاعات فهرست‌شده در جدول الف-۱ مستقیماً از بندهای ۵ تا ۸ استاندارد ISO/IEC 27002:2022 اقتباس‌شده و هم‌راستا هستند و باید در محتوای زیربند ۶-۱-۳ استفاده شوند.

**جدول الف-۱ کنترل‌های امنیت اطلاعات**

| | | |
|---|---|---|
| ۵ | **کنترل‌های سازمانی** | |
| ۵-۱ | خط‌مشی‌های امنیت اطلاعات | **کنترل**<br>خط‌مشی امنیت اطلاعات و خط‌مشی‌های موضوعی خاص باید تعریف گردند، توسط مدیریت تأیید شوند، منتشر شده، اطلاع‌رسانی شود و توسط کارکنان و ذی‌نفعان مرتبط تصدیق شوند و در فواصل زمانی برنامه‌ریزی‌شده یا در صورت بروز تغییرات قابل‌توجه، مورد بازنگری قرار گیرند. |
| ۵-۲ | نقش‌ها و مسئولیت‌های امنیت اطلاعات | **کنترل**<br>نقش‌ها و مسئولیت‌های امنیت اطلاعات باید بر اساس نیازهای سازمان، تعریف و تخصیص داده شوند. |
| ۵-۳ | تفکیک وظایف | **کنترل**<br>وظایف کاری و حوزه‌های مسئولیتی متداخل باید از یکدیگر تفکیک شوند. |
| ۵-۴ | مسئولیت‌های مدیریت | **کنترل**<br>مدیریت باید تمام کارکنان را ملزم نماید تا امنیت اطلاعات را، مطابق با خط‌مشی امنیت اطلاعات پیاده‌سازی شده، خط‌مشی‌های موضوعی خاص و روش‌های اجرائی سازمان بکار گیرند. |
| ۵-۵ | برقراری ارتباط با مراجع دارای اختیار | **کنترل**<br>سازمان باید ارتباط مناسبی با مراجع دارای اختیار مرتبط، برقرار و حفظ نماید. |
| ۵-۶ | برقراری ارتباط با گروه‌های با علاقه‌مندی‌های خاص | **کنترل**<br>سازمان باید ارتباطات مناسبی با گروه‌های دارای علاقه‌مندی‌های خاص یا سایر انجمن‌های تخصصی و حرفه‌ای در حوزه امنیت، برقرار و حفظ نماید. |
| ۵-۷ | هوش تهدید | **کنترل**<br>اطلاعات مربوط به تهدیدهای امنیت اطلاعات باید به‌منظور ایجاد هوش تهدید، جمع‌آوری و تحلیل شوند. |

**جدول الف-۱ - ادامه**

| | | |
|---|---|---|
| ۵-۸ | امنیت اطلاعات در مدیریت پروژه | **کنترل**<br>امنیت اطلاعات باید با مدیریت پروژه یکپارچه گردد. |
| ۵-۹ | فهرست اطلاعات و دیگر دارائی‌های مرتبط | **کنترل**<br>فهرست اطلاعات و دیگر دارائی‌های مرتبط که شامل مالکین آن‌ها نیز می‌شود، باید تهیه و نگه‌داری شود. |
| ۵-۱۰ | استفاده قابل‌قبول از اطلاعات و دیگر دارایی‌های مرتبط | **کنترل**<br>باید مقرراتی برای استفاده قابل‌قبول و روش‌های اجرائی برای مدیریت اطلاعات و دیگر دارایی‌های مرتبط، مشخص، مستند و پیاده‌سازی شوند. |
| ۵-۱۱ | بازگرداندن دارایی‌ها | **کنترل**<br>کارکنان و سایر ذی‌نفعان، در صورت لزوم، باید هنگام تغییر در شغل یا خاتمه همکاری، خاتمه قرارداد یا توافقنامه کاری‌شان، دارایی‌های سازمان که در اختیارشان است، را بازگردانند. |
| ۵-۱۲ | طبقه‌بندی اطلاعات | **کنترل**<br>اطلاعات باید مطابق با نیازمندی‌های امنیت اطلاعات سازمان بر اساس محرمانگی، یکپارچگی، در دسترس بودن و الزامات ذی‌نفعان مرتبط طبقه‌بندی گردد. |
| ۵-۱۳ | برچسب‌گذاری اطلاعات | **کنترل**<br>برای برچسب‌گذاری اطلاعات، باید مجموعهٔ مناسبی از روش‌های اجرایی مطابق با طرح طبقه‌بندی اطلاعات مورد پذیرش توسط سازمان، ایجاد و پیاده‌سازی شوند. |
| ۵-۱۴ | انتقال اطلاعات | **کنترل**<br>قواعد، روش‌های اجرائی یا موافقت‌نامه‌های انتقال اطلاعات باید برای همه انواع امکانات انتقال اطلاعات داخل سازمان و همچنین بین سازمان و سایر طرف‌ها وجود داشته باشد. |
| ۵-۱۵ | کنترل دسترسی | **کنترل**<br>قواعد کنترل دسترسی فیزیکی و منطقی به اطلاعات و دیگر دارایی‌های مرتبط باید بر اساس الزامات کسب‌وکار و امنیت اطلاعات، ایجاد و پیاده‌سازی شود. |
| ۵-۱۶ | مدیریت شناسه | **کنترل**<br>چرخه کامل حیات شناسه‌ها باید مدیریت شوند. |
| ۵-۱۷ | اطلاعات احراز اصالت | **کنترل**<br>تخصیص و مدیریت اطلاعات احراز اصالت باید توسط یک فرایند مدیریتی، از جمله راهنمائی پرسنل در مورد مدیریت مناسب اطلاعات احراز اصالت، کنترل شود. |

**جدول الف-۱ – ادامه**

| | | |
|---|---|---|
| ۵-۱۸ | حقوق دسترسی | **کنترل**<br>حقوق دسترسی به اطلاعات و دیگر دارایی‌های مرتبط باید مطابق با خط‌مشی موضوعی خاص سازمان و مطابق با قواعد کنترل دسترسی تأمین، بازنگری، تغییر و حذف شود. |
| ۵-۱۹ | امنیت اطلاعات در ارتباط با تأمین‌کنندگان | **کنترل**<br>فرایندها و روش‌های اجرائی برای مدیریت مخاطرات امنیت اطلاعات، مرتبط با استفاده از محصولات یا خدمات تأمین‌کننده، باید تعریف و پیاده‌سازی شوند. |
| ۵-۲۰ | رسیدگی به امنیت اطلاعات در توافقنامه‌های تأمین‌کننده | **کنترل**<br>الزامات امنیت اطلاعات مرتبط، باید با هر تأمین‌کننده بر اساس نوع رابطه با تأمین‌کننده مقرر و توافق شود. |
| ۵-۲۱ | مدیریت امنیت اطلاعات در زنجیره تأمین فناوری اطلاعات و ارتباطات (ICT). | **کنترل**<br>فرایندها و روش‌های اجرائی باید برای مدیریت مخاطرات امنیت اطلاعات مرتبط با زنجیره تأمین محصولات و خدمات فناوری اطلاعات و ارتباطات، تعریف و پیاده‌سازی شوند. |
| ۵-۲۲ | پایش، بازنگری و مدیریت تغییر خدمات تأمین‌کننده | **کنترل**<br>سازمان باید به طور منظم تغییرات در شیوه‌های جاری‌سازی امنیت اطلاعات و ارائه خدمات تأمین‌کننده را پایش، بازنگری، ارزشیابی و مدیریت کند. |
| ۵-۲۳ | امنیت اطلاعات برای استفاده از خدمات ابری | **کنترل**<br>فرایندهای اکتساب، استفاده، مدیریت و خاتمه استفاده از خدمات ابری باید مطابق با الزامات امنیت اطلاعات سازمان استقرار یابد. |
| ۵-۲۴ | طرح‌ریزی و آماده‌سازی برای مدیریت رخدادهای امنیت اطلاعات | **کنترل**<br>سازمان باید به‌منظور مدیریت رخدادهای امنیت اطلاعات به کمک تعریف، ایجاد و اطلاع‌رسانی فرایندها، نقش‌ها و مسئولیت‌های مربوط به مدیریت رخدادهای امنیت اطلاعات، طرح‌ریزی کرده و آماده شود. |
| ۵-۲۵ | ارزیابی و تصمیم برای رویدادهای امنیت اطلاعات | **کنترل**<br>سازمان باید رویدادهای امنیت اطلاعات را ارزیابی کرده و درباره این‌که آیا می‌توان آن‌ها را به‌عنوان رخدادهای امنیت اطلاعات دسته‌بندی کرد، تصمیم‌گیری نماید. |
| ۵-۲۶ | پاسخگویی به رخدادهای امنیت اطلاعات | **کنترل**<br>باید به رخدادهای امنیت اطلاعات، مطابق با روش‌های اجرائی مستند، پاسخ داده شود. |
| ۵-۲۷ | یادگیری از رخدادهای امنیت اطلاعات | **کنترل**<br>دانش به‌دست‌آمده از رخدادهای امنیت اطلاعات باید برای تقویت و بهبود کنترل‌های امنیت اطلاعات مورداستفاده قرار گیرد. |

**جدول الف-۱ - ادامه**

| | | |
|---|---|---|
| ۵-۲۸ | گردآوری شواهد | **کنترل**<br>سازمان باید روش‌های اجرائی را برای شناسایی، گردآوری، اکتساب و حفظ شواهد مربوط به رویدادهای امنیت اطلاعات، ایجاد و پیاده‌سازی نماید. |
| ۵-۲۹ | امنیت اطلاعات در هنگام اختلال | **کنترل**<br>سازمان باید چگونگی حفظ امنیت اطلاعات را در سطح مناسب، در هنگام وقوع اختلال طرح‌ریزی کند. |
| ۵-۳۰ | آمادگی ICT برای تداوم کسب‌وکار | **کنترل**<br>آمادگی ICT باید بر اساس اهداف تداوم کسب‌وکار و الزامات تداوم ICT طرح‌ریزی، پیاده‌سازی، نگه‌داری و آزمایش شود. |
| ۵-۳۱ | الزامات حقوقی، قانونی، مقرراتی و قراردادی | **کنترل**<br>الزامات حقوقی، قانونی، مقرراتی و قراردادی مربوط به امنیت اطلاعات همچنین رویکرد سازمان برای برآورده‌ساختن این الزامات باید شناسایی، مستند و به‌روز نگاه‌داشته شود. |
| ۵-۳۲ | حقوق مالکیت معنوی | **کنترل**<br>سازمان باید روش‌های اجرائی مناسبی را برای حفاظت از حقوق مالکیت معنوی پیاده‌سازی کند. |
| ۵-۳۳ | حفاظت از سوابق | **کنترل**<br>سوابق باید در برابر گم‌شدن، تخریب، تحریف، دسترسی غیرمجاز و انتشار غیرمجاز محافظت شوند. |
| ۵-۳۴ | حریم خصوصی و حفاظت از اطلاعات هویتی شخصی (PII) | **کنترل**<br>سازمان باید الزامات مربوط به حفظ حریم خصوصی و حفاظت از PII را مطابق با قوانین و مقررات کاربردی همچنین الزامات قراردادی، شناسایی و برآورده کند. |
| ۵-۳۵ | بازنگری مستقل امنیت اطلاعات | **کنترل**<br>رویکرد سازمان نسبت به مدیریت امنیت اطلاعات و پیاده‌سازی آن شامل افراد، فرایندها و فناوری‌ها باید به طور مستقل، در فواصل زمانی برنامه‌ریزی‌شده یا هر زمان که تغییرات قابل‌توجه رخ دهد، بازنگری شود. |
| ۵-۳۶ | انطباق با خط‌مشی‌ها، مقررات و استانداردهای امنیت اطلاعات | **کنترل**<br>انطباق با خط‌مشی امنیت اطلاعات سازمان، خط‌مشی‌های موضوعی خاص، مقررات و استانداردها باید به طور منظم بازنگری گردد. |
| ۵-۳۷ | روش‌های اجرائی عملیاتی مستند | **کنترل**<br>روش‌های اجرائی عملیاتی مرتبط با امکانات پردازش اطلاعات باید مستند شده و در دسترس کارکنانی که به آن‌ها نیاز دارند، قرار گیرد. |

**جدول الف-۱ - ادامه**

| | | |
|---|---|---|
| ۶ | **کنترل‌های انسانی** | |
| ۶-۱ | گزینش [۱] | **کنترل**<br>بررسی صحت‌سنجی سوابق تمام داوطلبان باید قبل از اشتغال و به‌صورت مستمر با در نظر گرفتن قوانین، مقررات و اصول اخلاقی قابل‌اجرا، انجام شود، به‌گونه‌ای که با الزامات کسب‌وکار، طبقه‌بندی اطلاعاتی که باید در دسترس قرار گیرند و مخاطرات قابل‌تصور، متناسب باشد. |
| ۶-۲ | شرایط و ضوابط استخدام | **کنترل**<br>توافق‌نامه‌های قراردادی استخدام باید بیانگر مسئولیت‌های کارکنان و سازمان در قبال امنیت اطلاعات باشد. |
| ۶-۳ | آگاهی‌بخشی، تحصیل و آموزش امنیت اطلاعات | **کنترل**<br>کارکنان سازمان و طرف‌های ذی‌نفع مرتبط، باید در زمینه امنیت اطلاعات، آگاهی، تحصیل و آموزش متناسب را دریافت نمایند و به‌صورت منظم در جریان به‌روزرسانی خط‌مشی امنیت اطلاعات، خط‌مشی‌های موضوعی خاص و روش‌های اجرائی سازمان، مرتبط با وظایف شغلی خود قرار گیرند. |
| ۶-۴ | فرایند انضباطی | **کنترل**<br>یک فرایند انضباطی باید رسماً تدوین و اطلاع‌رسانی شود تا اقدامات لازم در خصوص کارکنان و سایر طرف‌های ذی‌نفعی انجام شود که مرتکب نقض خط‌مشی امنیت اطلاعات می‌شوند. |
| ۶-۵ | مسئولیت‌های پس از خاتمه یا تغییر شغل | **کنترل**<br>مسئولیت‌ها و وظایف امنیت اطلاعات که پس از خاتمه یا تغییر شغل همچنان معتبر باقی می‌مانند باید تعریف و تاکید شود و به کارکنان مرتبط و سایر طرف‌های ذی‌نفع اطلاع‌رسانی شود. |
| ۶-۶ | توافقنامه‌های محرمانگی یا عدم افشا | **کنترل**<br>توافقنامه‌های محرمانگی یا عدم افشا که منعکس‌کننده نیازهای سازمان برای حفاظت از اطلاعات هستند باید شناسایی و مستندشده، به‌صورت مرتب بازنگری شود و توسط کارکنان و سایر طرف‌های ذی‌نفع مرتبط امضا شوند. |
| ۶-۷ | دورکاری | **کنترل**<br>هنگامی که کارکنان از دور، کار می‌کنند باید تمهیدات امنیتی لازم برای حفاظت از اطلاعات قابل‌دسترس، پردازش‌شده یا ذخیره‌شده در خارج از محیط سازمان، پیاده‌سازی شوند. |

**جدول الف-۱ - ادامه**

| | | |
|---|---|---|
| ۸-۶ | گزارش‌دهی رویداد امنیت اطلاعات | **کنترل**<br>سازمان باید سازوکاری برای کارکنان فراهم کند تا رویدادهای امنیت اطلاعات مشاهده شده یا مشکوک را از طریق کانال‌های متناسب، به‌موقع گزارش دهند. |
| ۷ | **کنترل‌های فیزیکی** | |
| ۱-۷ | حصارهای امنیت فیزیکی | **کنترل**<br>حصارهای امنیتی برای محافظت از نواحی که شامل اطلاعات و سایر دارایی‌های مرتبط هستند باید تعریف و استفاده شوند. |
| ۲-۷ | ورودی فیزیکی | **کنترل**<br>نواحی امن باید با کنترل‌های ورودی و نقاط دسترسی متناسب محافظت شوند. |
| ۳-۷ | امن‌سازی دفاتر، اتاق‌ها و امکانات | **کنترل**<br>امنیت فیزیکی برای دفاتر، اتاق‌ها و امکانات باید طراحی و پیاده‌سازی شود. |
| ۴-۷ | پایش امنیت فیزیکی | **کنترل**<br>اماکن باید به‌صورت مستمر برای دسترسی فیزیکی غیرمجاز پایش شوند. |
| ۵-۷ | حفاظت در برابر تهدیدات فیزیکی و محیطی | **کنترل**<br>حفاظت در برابر تهدیدات فیزیکی و محیطی مانند بلایای طبیعی و سایر تهدیدات فیزیکی عمدی یا سهوی برای زیرساخت‌ها، باید طراحی و پیاده‌سازی شود. |
| ۶-۷ | کار در نواحی امن | **کنترل**<br>اقدامات امنیتی برای کار در نواحی امن باید طراحی و پیاده‌سازی شوند. |
| ۷-۷ | میز پاک و صفحه‌نمایش پاک | **کنترل**<br>قواعد میز پاک برای مدارک و رسانه‌های ذخیره‌سازی قابل‌حمل و قواعد صفحه‌نمایش پاک برای امکانات پردازش اطلاعات باید تعریف شده و به نحو مناسب تأکید و اجرا شوند. |
| ۸-۷ | حفاظت و استقرار تجهیزات[۲] | **کنترل**<br>تجهیزات باید به‌صورت امن مستقر و حفاظت شوند. |
| ۹-۷ | امنیت دارایی‌های خارج از اماکن سازمانی | **کنترل**<br>از دارایی‌های خارج از اماکن سازمانی باید محافظت شود. |
| ۱۰-۷ | رسانه ذخیره‌سازی | **کنترل**<br>اکتساب، استفاده، انتقال و امحای رسانه‌های ذخیره‌سازی باید در طول چرخه عمر آن‌ها مطابق با طرح طبقه‌بندی سازمان و الزامات سامان‌دهی، مدیریت شوند. |

**جدول الف-۱- ادامه**

| | | |
|---|---|---|
| ۷-۱۱ | امکانات پشتیبانی | **کنترل**<br>امکانات پردازش اطلاعات باید در برابر مشکلات برقی و سایر اختلالات ناشی از خرابی امکانات پشتیبانی محافظت شوند. |
| ۷-۱۲ | امنیت کابل‌کشی | **کنترل**<br>کابل‌های برق، داده یا خدمات اطلاعات پشتیبان باید در برابر شنود، تداخل یا آسیب حفاظت شوند. |
| ۷-۱۳ | نگه‌داری از تجهیزات | **کنترل**<br>تجهیزات باید به‌درستی نگه‌داری شده تا از در دسترس بودن، یکپارچگی و محرمانگی اطلاعات اطمینان حاصل شود. |
| ۷-۱۴ | امحا یا استفاده مجدد از تجهیزات به‌صورت امن | **کنترل**<br>تجهیزات دارای رسانه ذخیره‌ساز باید قبل از امحا یا استفاده مجدد، به‌صورت کامل بررسی شده تا اطمینان حاصل شود که داده حساس و نرم‌افزار دارای مجوز، حذف یا به روشی امن رونویسی شده‌اند. |
| ۸ | **کنترل‌های فنی** | |
| ۸-۱ | افزاره‌های کاربر نهایی | **کنترل**<br>اطلاعاتی که بر روی افزاره‌های کاربر نهایی ذخیره می‌شود یا بر روی آن‌ها پردازش شده و یا توسط این تجهیزات قابل‌دسترس هستند، باید حفاظت شوند. |
| ۸-۲ | حقوق دسترسی ویژه | **کنترل**<br>تخصیص و استفاده از حقوق دسترسی ویژه باید محدود و مدیریت شود. |
| ۸-۳ | محدودسازی دسترسی به اطلاعات | **کنترل**<br>دسترسی به اطلاعات و دیگر دارایی‌های مرتبط باید مطابق با خط‌مشی موضوعی خاص، در خصوص کنترل دسترسی، محدود شود. |
| ۸-۴ | دسترسی به کد منبع | **کنترل**<br>دسترسی خواندن و نوشتن به کد منبع، ابزارهای توسعه و کتابخانه‌های نرم‌افزاری باید به طور مناسب مدیریت شود. |
| ۸-۵ | احراز هویت امن | **کنترل**<br>فناوری‌ها و روش‌های اجرایی احراز هویت امن باید بر اساس محدودیت‌های دسترسی به اطلاعات و خط‌مشی موضوعی خاص در مورد کنترل دسترسی پیاده‌سازی شوند. |
| ۸-۶ | مدیریت ظرفیت | **کنترل**<br>استفاده از منابع باید مطابق با الزامات ظرفیت فعلی و مورد انتظار، تحت پایش قرار گرفته و تنظیم شود. |

**جدول الف-۱ - ادامه**

| | | |
|---|---|---|
| ۸-۷ | حفاظت در برابر بدافزار | **کنترل**<br>حفاظت در برابر بدافزار باید با آگاهی‌رسانی مناسب کاربر، پیاده‌سازی و پشتیبانی شود. |
| ۸-۸ | مدیریت آسیب‌پذیری‌های فنی | **کنترل**<br>اطلاعات مربوط به آسیب‌پذیری‌های فنی سامانه‌های اطلاعات در حال استفاده باید جمع‌آوری شود، همچنین قرارگرفتن سازمان در معرض این آسیب‌پذیری‌ها باید ارزشیابی شده و اقدامات مناسب اتخاذ شود. |
| ۸-۹ | مدیریت پیکربندی | **کنترل**<br>پیکربندی‌ها شامل پیکربندی‌های امنیتی سخت‌افزارها، نرم‌افزارها، خدمات و شبکه‌ها باید ایجاد، مستند، پیاده‌سازی، پایش و بازنگری شوند. |
| ۸-۱۰ | حذف اطلاعات | **کنترل**<br>اطلاعات ذخیره شده در سامانه‌های اطلاعات، افزاره‌ها یا هر رسانه ذخیره‌ساز دیگر، باید زمانی که دیگر نیازی به آن‌ها نیست، حذف شوند. |
| ۸-۱۱ | داده پوشی[۳] | **کنترل**<br>داده‌پوشی باید مطابق با خط‌مشی‌های موضوعی خاص سازمان مثل کنترل دسترسی و یا سایر خط‌مشی‌های موضوعی مرتبط همچنین الزامات کسب‌وکار و با درنظرگرفتن قوانین قابل‌اجرا، انجام شود. |
| ۸-۱۲ | جلوگیری از نشت داده‌ها | **کنترل**<br>اقدامات جلوگیری از نشت داده‌ها باید برای سامانه‌ها، شبکه‌ها و هر افزاره دیگری اعمال شود که اطلاعات حساس را پردازش، ذخیره یا انتقال می‌دهد. |
| ۸-۱۳ | پشتیبان‌گیری از اطلاعات | **کنترل**<br>نسخه‌های پشتیبان از اطلاعات، نرم‌افزار و سامانه‌ها باید مطابق با خط‌مشی موضوعی خاص توافق‌شده دربارهٔ پشتیبان‌گیری، نگه‌داری و به طور منظم آزموده شوند. |
| ۸-۱۴ | افزونگی امکانات پردازش اطلاعات | **کنترل**<br>امکانات پردازش اطلاعات باید با افزونگی کافی برای برآورده‌ساختن الزامات در دسترس بودن، پیاده سازی شود. |
| ۸-۱۵ | رویدادنگاری[۴] | **کنترل**<br>رویدادنگاری‌هایی که فعالیت‌ها، استثنائات، خطاها و سایر رویدادهای مرتبط را ثبت می‌کنند، باید تولید، ذخیره، حفاظت و تحلیل شوند. |

**جدول الف-۱ - ادامه**

| | | |
|---|---|---|
| ۸-۱۶ | فعالیت‌های پایشی [۵] | **کنترل**<br>شبکه‌ها، سامانه‌ها و برنامه‌های کاربردی باید از نظر رفتار غیرعادی و اقدام‌های متناسب اتخاذ شده به‌منظور ارزشیابی رخدادهای بالقوه امنیت اطلاعات، تحت نظارت قرار گیرند. |
| ۸-۱۷ | هم‌زمان‌سازی ساعت [۶] | **کنترل**<br>ساعت‌های سامانه‌های پردازش اطلاعات مورداستفاده در سازمان باید با منابع زمانی تأیید شده هم‌زمان‌سازی شوند. |
| ۸-۱۸ | استفاده از برنامه‌های کمکی ویژه | **کنترل**<br>استفاده از برنامه‌های کمکی که قابلیت نقض کنترل‌های سامانه و برنامه را دارند، باید محدود شده و به‌شدت کنترل شود. |
| ۸-۱۹ | نصب نرم‌افزار بر روی سامانه‌های عملیاتی | **کنترل**<br>روش‌های اجرائی و اقداماتی باید برای مدیریت ایمن نصب نرم‌افزار بر روی سامانه‌های عملیاتی، پیاده‌سازی شود. |
| ۸-۲۰ | امنیت شبکه | **کنترل**<br>شبکه‌ها و افزاره‌های شبکه باید به‌منظور حفاظت از اطلاعات، سامانه‌ها و برنامه‌های کاربردی، ایمن‌سازی، مدیریت و کنترل شوند. |
| ۸-۲۱ | امنیت خدمات شبکه | **کنترل**<br>سازوکارهای امنیتی، سطوح ارائه خدمت و الزامات خدمات شبکه باید شناسایی، پیاده‌سازی و پایش شوند. |
| ۸-۲۲ | تفکیک شبکه‌ها | **کنترل**<br>گروه‌های خدمات اطلاعات، کاربران و سامانه‌های اطلاعات باید در شبکه‌های سازمان از یکدیگر تفکیک شوند. |
| ۸-۲۳ | پالایش وب | **کنترل**<br>دسترسی به وب‌گاه‌های بیرونی باید به‌منظور کاهش میزان قرارگیری در معرض محتوای مخرب، مدیریت شود. |
| ۸-۲۴ | استفاده از رمزنگاری [۷] | **کنترل**<br>قواعدی برای استفاده اثربخش از رمزنگاری، از جمله مدیریت کلید رمزنگاری باید تعریف و پیاده‌سازی شود. |
| ۸-۲۵ | چرخه عمر توسعه امن | **کنترل**<br>قواعدی باید برای توسعه امن نرم‌افزار و سامانه‌ها ایجاد و اعمال شود. |

**جدول الف-۱ - ادامه**

| | | |
|---|---|---|
| ۸-۲۶ | الزامات امنیتی برنامه‌های کاربردی | **کنترل**<br>الزامات امنیت اطلاعات در هنگام خرید یا توسعه برنامه‌های کاربردی باید شناسایی، مشخص و تأیید شوند. |
| ۸-۲۷ | اصول معماری و مهندسی امن سامانه‌ها | **کنترل**<br>اصول مهندسی امن سامانه‌ها باید ایجاد، مستند و نگه‌داری شده و برای انجام هرگونه فعالیتی در خصوص توسعه سامانه اطلاعات اعمال شوند. |
| ۸-۲۸ | کدنویسی امن | **کنترل**<br>در هنگام توسعه یک نرم‌افزار باید اصول کدنویسی امن در نظر گرفته شود. |
| ۸-۲۹ | آزمون امنیتی در مراحل توسعه و پذیرش | **کنترل**<br>فرایندهای آزمون امنیتی باید در چرخه عمر توسعه، تعریف و پیاده‌سازی شوند. |
| ۸-۳۰ | توسعه برون‌سپاری شده | **کنترل**<br>سازمان باید فعالیت‌های مرتبط با توسعه برون‌سپاری شده سامانه را هدایت، پایش و بازنگری کند. |
| ۸-۳۱ | جداسازی محیط‌های توسعه، آزمون و عملیات | **کنترل**<br>محیط‌های توسعه، آزمون و عملیات باید از یکدیگر تفکیک و ایمن‌سازی شوند. |
| ۸-۳۲ | مدیریت تغییر | **کنترل**<br>هرگونه تغییر در امکانات پردازش اطلاعات و سامانه اطلاعات باید بر اساس روش‌های اجرائی مدیریت تغییر انجام شود. |
| ۸-۳۳ | اطلاعات آزمون | **کنترل**<br>اطلاعات آزمون باید به طور مناسبی انتخاب، حفاظت و مدیریت شوند. |
| ۸-۳۴ | حفاظت از سامانه اطلاعات در حین آزمون‌های ممیزی | **کنترل**<br>آزمون‌های ممیزی و سایر فعالیت‌های صحت‌سنجی که ارزیابی سامانه عملیاتی را در برمی‌گیرند، باید مابین آزمونگر و مدیریت متناسب، برنامه‌ریزی‌شده و مورد توافق قرار گیرند. |

۱- مصوب فرهنگستان، واژه غربالگری است.

2- Equipment
3- Data masking
4- Logging
5- Monitoring
6- Clock synchronization
7- Cryptography

## کتاب‌نامه

[1] ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection- Information security controls

**یادآوری-** استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۹۴، فناوری اطلاعات، فنون امنیتی، آیین کار برای کنترل های امنیت اطلاعات، *با استفاده از استاندارد* ISO/IEC 27002:2013 + Cor1:2014 تدوین شده است.

[2] ISO/IEC 27003, Information technology- Security techniques- Information security management systems- Guidance

**یادآوری-** استاندارد ملی ایران شماره ۲۷۰۰۳: سال ۱۳۸۹، فناوری اطلاعات- فنون امنیتی- راهنمای اجرای سامانه مدیریت امنیت اطلاعات، با استفاده از استاندارد ISO/IEC 27003: 2010 تدوین شده است.

[3] ISO/IEC 27004, Information technology- Security techniques- Information security management- Monitoring, measurement, analysis and evaluation

**یادآوری-** استاندارد ملی ایران شماره ۱۴۰۹۶: سال ۱۳۸۹، فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات - سنجش با استفاده از استاندارد ISO/IEC 27004: 2009 تدوین شده است.

[4] ISO/IEC 27005, Information security, cybersecurity and privacy protection- Guidance on managing information security risks

**یادآوری-** استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۹۲، فناوری اطلاعات- فنون امنیتی- مدیریت مخاطرات امنیت اطلاعات، با استفاده از استاندارد ISO/IEC 27005: 2011 تدوین شده است.

[۵] استاندارد ملی ایران شماره ۱۳۲۴۵: سال ۱۳۹۸، مدیریت ریسک- رهنمودها.