INSO-ISO-IEC
27006
Revision.1st
2017

Identical with
ISO/IEC 27006:2015

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران
ایزو- آی ایی سی
۲۷۰۰۶
تجدیدنظر اول
۱۳۹۶

فناوری اطلاعات–
فنون امنیتی – الزامات برای نهادهای ممیزی و صدرو گواهینامه سامانه‌های مدیریت امنیت اطلاعات

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

ICS: 03.100.70 , 35.030

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@isiri.org.ir

وبگاه: http://www.isiri.gov.ir

Iranian National Standardization Organization (INSO)

No.1294 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@isiri.org.ir

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

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

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

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

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

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

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]،کمیسیون بین‌المللی الکتروتکنیک(IEC)[2] و سازمان بین‌المللی اندازه شناسی قانونی(OIML)[3] است و به‌عنوان 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 محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/ یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می‌تواند به‌منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و گواهینامه سامانه‌های مدیریت کیفیت و مدیریت محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تائید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تائید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج افزاره بین‌المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

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

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات – فنون امنیتی – الزامات برای نهادهای ممیزی و گواهینامه سامانه‌های مدیریت امنیت اطلاعات»

«تجدید نظر اول»

رئیس:	**سمت و/ یا مکان اشتغال:**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات- سیستم‌های اطلاعاتی)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
دبیر:	
کیامهر، بیتا (فوق لیسانس مدیریت تکنولوژی)	معاون مدیر کل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
جوادزاده، غزاله (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
رادمهر، وحید (کارشناسی مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
عباسپور، مقصود (دکتری مهندسی کامپیوتر- معماری)	دانشیار– معاون مرکز فناوری دانشگاه شهید بهشتی
طباطبایی ملاذی، هادی (دکتری مهندسی کامپیوتر)	استادیار- دانشگاه شهید بهشتی
طی نیا، رضا (کارشناسی ارشد فناوری اطلاعات)	مدیر عامل– شرکت مهندسی کاربرد سیستم (کاسیس)
مطلق، کامبیز (کارشناسی ارشد فناوری اطلاعات)	معاون فناوری اطلاعات– بانک قوامین
مغانی، مهدی (کارشناسی ارشد ریاضی کاربردی)	کارشناس تدوین استانداردهای حوزه فناوری اطلاعات- سازمان فناوری اطلاعات ایران
ناظمی، اسلام (دکتری مهندسی کامپیوتر)	دانشیار- دانشگاه شهید بهشتی

اعضاء : (اسامی به ترتیب حروف الفبا)

	سمت و/ یا مکان اشتغال:
نصیری آسایش، حمیدرضا (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر- دانشگاه شهید بهشتی
یعقوبی رفیع، کمال الدین (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر- دانشگاه شهید بهشتی

ویراستار:	**سمت و/ یا مکان اشتغال:**
معروف، سینا (لیسانس مهندسی کامپیوتر، سخت‌افزار)	کارشناس تدوین استانداردهای حوزه فناوری اطلاعات- سازمان فناوری اطلاعات ایران

فهرست مندرجات

عنوان **صفحه**

عنوان **صفحه**

صفحه

عنوان

پیش‌گفتار

استاندارد «فناوری اطلاعات– فنون امنیتی– الزامات برای نهادهای ممیزی و صدور گواهینامه سامانه‌های مدیریت امنیت اطلاعات» که نخستین بار در سال ۱۳۸۷ بر مبنای پذیرش استانداردهای بین‌المللی به‌عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی شمارهٔ ۵ تدوین و منتشر شد، بر اساس پیشنهادهای دریافتی و بررسی و تایید کمیسیون‌های مربوط برای اولین بار مورد تجدیدنظر قرار گرفت و در چهارصد و نود و چهارمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۶/۰۱/۳۰ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان 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 زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد جایگزین استاندارد ملی ایران به شماره ایران – ایزو- آی ایی سی ۲۷۰۰۶: سال ۱۳۸۷ است.

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 27006: 2015(E), Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

مقدمه

استاندارد ISO/IEC 17021-1 معیارهایی برای نهادهای مجری ممیزی و صدور گواهینامه سامانه‌های مدیریت تعیین می‌کند. اگر این نهادها[1] مطابق با استاندارد ISO/IEC 17021-1 با هدف ممیزی و گواهینامه سامانه‌های مدیریت امنیت اطلاعات (ISMS) مطابق با استاندارد ISO/IEC 27001:2013 به رسمیت شناخته شوند، الزامات افزون دیگر و راهنمای استاندارد ISO/IEC 17021-1 ضروری است که توسط این استاندارد ارائه شده‌اند.

متن این استاندارد از ساختار استاندارد ISO/IEC 17021-1 پیروی می‌کند و الزامات افزون مختص ISMS و راهنمای کاربردی استاندارد ISO/IEC 17021-1 برای گواهینامه‌ی ISMS با حروف «IS» مشخص شده‌اند.

واژه «باید» در این استاندارد برای نشان دادن شرایطی است که بازتاب دهنده‌ی الزامات استانداردهای ISO/IEC 17021-1 و ISO/IEC 27001 است که اجباری هستند. اصطلاح «توصیه می‌شود» برای نشان دادن توصیه‌ها به‌کار رفته است.

هدف اولیه‌ی این استاندارد توانا کردن نهادهای اعتباربخشی برای هماهنگی موثرتر کاربرد استانداردها در برابر مواردی است که برای ارزیابی نهادهای صدور گواهینامه اجباری تعیین شده‌اند.

در سرتاسر این استاندارد اصطلاحات «سامانهٔ مدیریت» و «سامانه» به جای یکدیگر استفاده شده‌اند. تعریف سامانهٔ مدیریت می‌تواند در استاندارد ISO 9000:2005 وجود دارد. سامانهٔ مدیریت به همان صورت استفاده شده در این استاندارد نباید با انواع دیگر سامانه‌ها مانند سامانه‌های فناوری اطلاعات (IT) اشتباه گرفته شود.

1- Bodies

فناوری اطلاعات – فنون امنیتی – الزامات برای نهادهای ممیزی و صدورگواهینامه سامانه‌های مدیریت امنیت اطلاعات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین الزامات و رهنمودهایی افزون بر الزامات موجود در استاندارد ISO/IEC 17021-1 و استاندارد ISO/IEC 27001 برای نهادهای ممیزی و گواهینامه سامانه مدیریت امنیت اطلاعات است. هدف اولیه آن پشتیبانی از اعتباربخشی به نهادهای صدور گواهینامه ارائه‌دهنده گواهینامه‌ی ISMS است.

نیاز است الزامات موجود در این استاندارد بر حسب صلاحیت و قابلیت اطمینان توسط هر نهاد ارائه‌دهنده گواهینامه‌ی ISMS نشان داده شود و راهنمای موجود در این استاندارد تفسیری افزون بر این الزامات برای هر نهاد ارائه‌دهنده گواهینامه ISMS فراهم می‌کند.

یادآوری – این استاندارد می‌تواند به عنوان سند معیار برای اعتباربخشی، ارزیابی مشترک یا دیگر فرایندهای ممیزی مورد استفاده قرار گیرد.

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 می‌شوند.

درصورتی‌که به مدرکی با ذکر تاریخ انتشار ارجاع داده‌شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن موردنظر این استاندارد ملی ایران نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران شمارهٔ ۲۷۰۰۰: سال ۱۳۹۴، فناوری اطلاعات- فنون امنیتی- سیستم‌های (سامانه-های) مدیریت امنیت اطلاعات- مرور کلی و واژگان

۲-۲ استاندارد ملی ایران شمارهٔ ۲۷۰۰۱: سال ۱۳۹۴، فناوری اطلاعات- فنون امنیتی- سامانه (سیستم) مدیریت امنیت اطلاعات- الزامات

2-3 ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین‌شده در استاندارد ISO/IEC 17021-1 و استاندارد ملی ایران شمارهٔ ۲۷۰۰۰: سال ۱۳۹۴، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود:

۳-۱

اسناد گواهینامه

certification documents

مستنداتی که نشان می‌دهد، ISMS متعلق به مشتری با استانداردهای مشخص شده ISMS و هر مستند تکمیلی مورد نیاز تحت سامانه، انطباق دارد.

۴ اصول[1]

اصول بند ۴ استاندارد ISO/IEC 17021-1 به‌کار می‌روند.

۵ الزامات عمومی

۵-۱ موضوعات قانونی و قراردادی

الزامات بند ۵-۱ استاندارد ISO/IEC 17021-1 به‌کار می‌روند.

۵-۲ مدیریتِ بی‌طرفی[2]

الزامات بند ۵-۲ استاندارد ISO/IEC 17021-1 به‌کار می‌روند. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌رود.

۵-۲-۱ IS 5.2 تضاد منافع[3]

نهادهای صدور گواهینامه ممکن است وظایف زیر را که بدون آن به‌عنوان مشاوره در نظر گرفته می‌شوند یا دارای تضاد بالقوه‌ی منافع خواهند بود، انجام دهند:

الف- تنظیم قرار و شرکت به عنوان مدرس در دوره‌های آموزشی، در جایی که این دوره‌ها مربوط به مدیریت امنیت اطلاعات و به سامانه‌های مدیریت یا ممیزی مرتبط هستند، نهادهای صدور گواهینامه باید خود را به ارائه‌ی اطلاعات عمومی و توصیه که به صورت عمومی در دسترس هستند، محدود کنند، یعنی آن‌ها نباید توصیه‌ای ارائه دهند که تنها مخصوص یک شرکت است و نباید از الزامات مورد ب- تخطی کنند.

1 - Principles
2 - Impartiality
3- Conflict of interest

ب- در دسترس قرار دادن یا انتشار اطلاعات توصیف کننده تفسیر الزامات استانداردهای ممیزی گواهینامه در نهاد صدور گواهینامه بنا به درخواست (به بند ۹-۱-۳-۶ مراجعه شود.)

پ- فعالیت‌های پیش از ممیزی که تنها برای تعیین آمادگی برای ممیزی گواهینامه به‌کار می‌روند؛ هرچند این فعالیت‌ها نباید به ارائه راهنمایی‌هایی منجر شود یا ارائهٔ توصیه‌هایی که از این بند تخطی می‌کنند را به همراه داشته باشد و نهاد صدور گواهینامه باید قادر باشد که عدم تخطی این فعالیت‌ها را از الزامات و عدم استفاده‌ی آن‌ها را برای توجیه کاهش در دوره‌ی آتی ممیزی گواهینامه آتی[1] را تایید کند.

ت- انجام ممیزی‌های طرف دوم و سوم مطابق با استانداردها یا مقررات دیگر به غیر از آن‌هایی که قسمتی از دامنه‌ی کاربرد اعتباربخشی است.

ث- افزودن ارزش در مدت ممیزی‌های گواهینامه و بازدیدهای مراقبتی، به طور مثال، از طریق شناسایی فرصت‌هایی برای بهبود که در مدت ممیزی و بدون توصیه‌ی راه حل‌های خاص، آشکار می‌شوند.

نهاد صدور گواهینامه نباید بازنگری‌های داخلی امنیت اطلاعات ISMS را برای مشتری را برای گواهینامه فراهم کند. علاوه بر این، نهاد صدور گواهینامه باید از نهاد یا نهادهایی (شامل هر شخص حقیقی) که ممیزی داخلی ISMS را ارائه می‌کند، مستقل باشد.

۳-۵ مسئولیت و تامین مالی

الزامات بند ۵-۳ استاندارد ISO/IEC 17021-1 به‌کار می‌روند.

۶ الزامات ساختاری

الزامات بند ۶ استاندارد ISO/IEC 17021-1 به‌کار می‌روند.

۷ الزامات منابع

۱-۷ صلاحیت کارکنان[2]

الزامات بند ۷-۱ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌روند.

۱-۱-۷ IS 7.1.1 ملاحظات عمومی

۱-۱-۱-۷ الزامات عام صلاحیت

نهاد صدور گواهینامه باید اطمینان حاصل کند که دانش کافی در مورد توسعه‌های فناورانه، قانونی و مقررات

1 - Eventual certification
2 - Competence of personnel

تنظیمی مربوط به ISMS مشتریِ مورد ارزیابی، دارد.

نهاد صدور گواهینامه باید به همان صورتی که در جدول الف-۱ در استاندارد ISO/IEC 17021-1 اشاره شده است، الزامات صلاحیت برای هر کارکرد گواهینامه را تعریف کرده باشد. نهاد صدور گواهینامه باید تمامی الزامات مشخص شده در استاندارد ISO/IEC 17021-1 و بندهای ۷-۱-۲ و ۷-۲-۱ این استاندارد را که مربوط به حوزه‌های فنی ISMS معین در نهاد صدور گواهینامه هستند را در نظر بگیرد.

یادآوری- پیوست الف خلاصه‌ای از الزامات مربوط به کارکنانی است که در کارکردهای مشخص گواهینامه همکاری می‌کنند.

۷-۱-۲ IS 7.1.2 تعیین معیار صلاحیت

۷-۱-۲-۱ الزامات صلاحیت برای ممیزی ISMS

۷-۱-۲-۱-۱ الزامات عمومی

نهاد صدور گواهینامه باید دارای معیاری برای درستی‌سنجی تجربه، آموزش خاص یا توجیه اعضای گروه ممیزی داشته باشد تا دست‌کم از موارد زیر اطمینان حاصل کند:

الف- دانش امنیت اطلاعات

ب- دانش فنی از فعالیتی که باید ممیزی شود.

پ- دانش سامانه‌های مدیریت

ت- دانش اصول ممیزی

یادآوری- برای اطلاعات بیشتر در مورد اصول ممیزی، به استاندارد ISO 19011 مراجعه شود.

ث- دانشِ پایشِ، سنجش، تحلیل و ارزیابی ISMS.

موارد الف تا ث به همه‌ی ممیزان که عضو تیم ممیزی هستند اعمال می‌شود؛ بجز مورد ب که می‌تواند بین ممیزین عضو تیم ممیزی به اشتراک گذاشته شود.

گروه ممیزی باید صلاحیت ردیابی شواهد رخدادهای امنیت اطلاعات در ISMS مشتری متناسب با عناصر سیستم مدیریت امنیت اطلاعات را داشته باشند.

گروه ممیزی باید دارای تجربه‌ی کاری مناسب در موارد بالا و کاربردهای عملی این موارد باشد (این امر بدین معنا نیست که ممیز نیازمند بازه‌ای کامل از تجارب تمامی حوزه های امنیت اطلاعات باشد، بلکه به این معناست که گروه ممیزی باید دارای درک و تجربه‌ی کافی برای پوشاندن دامنه‌ی کاربرد ISMS ممیزی شده باشد.)

۷-۱-۲-۱-۲ واژگان[1]، اصول، کار[2]ها و فنون مدیریت امینت اطلاعات

در مجموع، تمامی اعضای گروه ممیزی باید دارای دانش زیر باشند:

الف- ساختار، سلسله مراتب و روابط داخلی مستندات مشخص شده در ISMS

ب- ابزارها، روش‌ها، فنون مربوط به مدیریت امنیت اطلاعات و کاربرد آن‌ها

پ- ارزیابی[3] مخاطره‌ی امنیت اطلاعات و مدیریت مخاطره

ت- فرایندهای کاربردپذیر برای ISMS

ث- فناوری حاضر در هنگامی‌که امنیت اطلاعات ممکن است مربوط به آن باشد.

هر ممیز باید موارد الف، پ و ت را دارا باشد.

۷-۱-۲-۱-۳ استانداردها و مستندات الزامی سامانهٔ مدیریت امنیت اطلاعات

ممیزان ISMS باید اطلاعاتی پیرامون موارد زیر داشته باشند:

الف- تمامی الزامات موجود در استاندارد ISO/IEC 27001 .

در کل، تمامی اعضای گروه ممیزی باید اطلاعاتی از موارد زیر داشته باشند:

ب- تمامی واپایش‌های موجود در استاندارد ISO/IEC 27002 (اگر به صورت الزامی از استانداردهای مشخص بخش تعیین شده باشد) و پیاده‌سازی آن‌ها به صورت زیر طبقه بندی می‌شوند:

۱- خط‌مشی‌های امنیت اطلاعات

۲- سازمان امنیت اطلاعات

۳- امنیت منابع انسانی

۴- مدیریت دارایی

۵- واپایش دسترسی شامل اصالت‌سنجی

۶- رمزنگاری[4]

۷- امنیت فیزیکی و محیطی

۸- امنیت عملیات شامل خدمات IT

۹- امنیت ارتباطات شامل مدیریت امنیت شبکه و انتقال اطلاعات

1 - Terminology
2 - Practice
3 - Assessment
4 - Cryptography

۱۰- اکتساب، توسعه و نگهداشت سامانه

۱۱- روابط تامین‌کنندگان شامل خدمات برون‌سپاری

۱۲- مدیریت رخداد امنیت اطلاعات

۱۳- مفاهیم امنیت اطلاعات مدیریت تداوم کسب‌وکار شامل افزونگی[1]

۱۴- انطباق، شامل بازنگری‌های امنیت اطلاعات

۷-۱-۲-۱-۴ کارهای مدیریت کسب‌وکار

ممیزانی که به ممیزی ISMS مشغول‌اند باید دانش کافی از موارد زیر داشته باشند :

الف- کارهای خوب صنعت امنیت اطلاعات و رویه‌های امنیت اطلاعات

ب- خط‌مشی‌ها و الزامات کسب‌وکار برای امنیت اطلاعات

پ- مفاهیم کلی و کارهای مدیریت کسب‌وکار و روابط داخلی بین خط‌مشی، هدف‌ها و نتایج

ت- فرایندهای مدیریتی و مجموعه واژگان مرتبط

یادآوری- این فرایندها همچنین شامل مدیریت منابع انسانی، ارتباطات درونی و بیرونی و دیگر فرایندهای پشتیبان مربوط می‌شود.

۷-۱-۲-۱-۵ بخش کسب‌وکار مشتری

ممیزانی که به ممیزی ISMS مشغول‌اند باید دانش کافی از موارد زیر داشته باشند:

الف- الزامات قانونی در حوزه‌ی مخصوص امنیت اطلاعات، جغرافیا و اختیارات قانونی

یادآوری- دانش الزامات و مقررات قانونی دلالت بر پیش‌زمینه‌ی عمیق قانونی ندارد.

ب- مخاطره‌های امنیت اطلاعات مربوط به بخش کسب‌وکار

پ- واژگان، فرایندها و فناوری‌های عام مربوط به بخش کسب‌وکار مشتری

ت- رویه‌های مرتبط با بخش کسب‌وکار

معیار مورد الف ممکن است در میان گروه ممیزی مشترک باشد و لازم نباشد که همه دارای دانش مورد الف باشند.

۷-۱-۲-۱-۶ محصولات، فرایندها و سازمان مشتری

در کل، ممیزانی که به ممیزی ISMS مشغول‌اند، باید در موارد زیر دارای دانش کافی باشند:

1 -Redundancies

الف- تاثیر نوع، اندازه، حاکمیت، ساختار، کارکردهای سازمان و روابط در توسعه و پیاده‌سازی ISMS و فعالیت‌های گواهینامه از جمله برون‌سپاری

ب- عملیات پیچیده در چشم انداز گسترده

پ- الزامات قانونی کاربردپذیر برای خدمات یا محصولات

۷-۱-۲-۲ الزامات صلاحیت برای رهبریِ گروه ممیزی ISMS

علاوه بر الزامات ۷-۱-۲-۱، رهبران گروه ممیزی باید الزامات زیر را دارا باشند؛ این الزامات باید در ممیزی‌ها تحت هدایت و نظارت مشهود باشد:

الف- دانش و مهارت برای مدیریت کردن فرایند ممیزی گواهینامه و گروه ممیزی

ب- نمایش توانایی برای ارتباطات موثر، از نظر هم گفتاری و هم نوشتاری

۷-۱-۲-۳ الزامات صلاحیت برای اجرای بازنگری فرم درخواست

۷-۱-۲-۳-۱ استانداردهای سامانهٔ مدیریت امنیت اطلاعات و مستندات الزامی

کارکنان هدایت بازنگری فرم درخواست، برای تعیین الزامات صلاحیتِ گروه ممیزی که نیاز به انتخاب اعضای گروه ممیزی و تعیین زمان ممیزی دارند، باید دارای دانش مربوط به موارد زیر باشند:

الف- استانداردهای مربوط به ISMS و دیگر مستندات الزامی مورد استفاده در فرایند گواهینامه

۷-۱-۲-۳-۲ بخش کسب‌وکار مشتری

کارکنان هدایت بازنگری فرم درخواست، برای تعیین الزامات صلاحیتِ گروه ممیزی که نیاز به انتخاب اعضای گروه ممیزی و تعیین زمان ممیزی دارند، باید دارای دانش مربوط به موارد زیر باشند:

الف- واژگان، فرایندها، فناوری‌ها و مخاطره‌های عام مربوط به بخش کسب‌وکار مشتری

۷-۱-۲-۳-۳ محصولات، فرایندها و سازمان مشتری

کارکنان انجام بازنگری کاربردی برای تعیین کردن صلاحیت الزامی گروه ممیزی، انتخاب کردن اعضای گروه ممیزی و تعیین کردن زمان ممیزی باید دارای دانش مربوط به موارد زیر باشند:

الف- نوع محصولات، فرایندها و سازمان مشتری، اندازه، نظارت، ساختار، کارکردها و روابط در توسعه و پیاده-سازی ISMS و فعالیت‌های گواهینامه، شامل کارکردهای برون‌سپاری

۷-۱-۲-۴ الزامات صلاحیت برای بازنگری گزارش‌های ممیزی و تصمیم گیری در مورد صدور گواهی

۷-۱-۲-۴-۱ کلیات

کارکنانی که گزارش‌های ممیزی را بازنگری و در مورد گواهینامه تصمیم گیری می‌کنند باید دارای دانشی باشند که آن‌ها را قادر به تصدیق تناسب دامنه‌ی کاربرد و تغییرات آن و تاثیر آن‌ها بر اثربخشی ممیزی، به ویژه صحت پیوستگی شناسایی واسطه‌ها و وابستگی‌ها و مخاطرات متناظر کند.

علاوه بر این، کارکنانی که گزارش‌های ممیزی را بازنگری و در مورد گواهینامه تصمیم گیری می‌کنند باید در موارد زیر دارای دانش کافی باشند:

الف- سامانه‌های مدیریت در کل

ب- فرایندها و رویه‌ها

پ- اصول، رویه‌ها و فنون ممیزی

۷-۱-۲-۴-۲ واژگان، اصول و فنون مدیریت امنیت اطلاعات

کارکنانی که گزارش‌های ممیزی را بازنگری و در مورد گواهینامه تصمیم گیری می‌کنند باید در موارد زیر دارای دانش کافی باشند:

الف- موارد فهرست شده در بند ۷-۱-۲-۱-۲- موارد الف و پ و ت

ب- الزامات قانونی مربوط به امنیت اطلاعات

۷-۱-۲-۴-۳ استانداردهای سامانهٔ مدیریت امنیت اطلاعات و مستندات الزامی

کارکنانی که گزارش‌های ممیزی را بازنگری و در مورد گواهینامه تصمیم گیری می‌کنند باید در موارد زیر دارای دانش کافی باشند:

الف- استانداردهای مربوط به ISMS و دیگر مستندات الزامی در فرایندهای گواهینامه

۷-۱-۲-۴-۴ بخش کسب‌وکار مشتری

کارکنانی که گزارش‌های ممیزی را بازنگری و در مورد گواهینامه تصمیم گیری می‌کنند باید در مورد زیر دارای دانش کافی باشند:

الف- واژگان و مخاطره‌های عام مربوط به کارهای بخش کسب‌وکار

۷-۱-۲-۴-۵ محصولات، فرایندها و سازمان مشتری

کارکنانی که گزارش‌های ممیزی را بازنگری و در مورد گواهینامه تصمیم گیری می‌کنند باید در مورد زیر دارای دانش کافی باشند:

الف- محصولات، فرایندها و نوع سازمان، اندازه، حاکمیت، ساختار، کارکردها[1] و روابط مشتری

۷-۲ کارکنانِ دخیل در فعالیت‌های صدور گواهی

الزامات استاندارد ISO/IEC 17021-1 قسمت ۷-۲ اعمال می‌شود. علاوه بر این، الزامات و راهنمای زیر اعمال می‌شود.

۷-۲-۱ IS 7.2 نشان دادن دانش و تجربه‌ی ممیز

نهاد صدور گواهینامه باید نشان دهد که ممیزان دارای دانش و تجربه‌ی کافی دارند، از طریق موارد زیر:

الف- صلاحیت‌های مرتبط به ISMS

ب- هر جه که لازم است باید به عنوان ممیز ثبت نام شده باشد.

پ- شرکت در دوره‌های آموزشی ISMS و کسب اعتبار مربوط کارکنان

ت- سوابق به‌روز رسانی‌شدهٔ ترقی حرفه‌ای

ث- حضور به عنوان ناظر در دیگر ممیزی‌های رسمی ISMS

۷-۲-۱-۱ انتخاب ممیزان

علاوه بر ۷-۱-۲-۱، انتخاب ممیزان باید به گونه‌ای باشد که از موارد زیر اطمینان حاصل شود:

الف- ممیز دارای تحصیلات تخصصی یا آموزش تا سطحی برابر با تحصیلات دانشگاهی است.

ب- ممیز دارای دست‌کم چهار سال سابقه‌ی کاری تمام وقت در فناوری اطلاعات است که دست‌کم دو سال آن در نقش یا کارکرد مربوط به امنیت اطلاعات است.

پ- ممیز، آموزش با زمان دست‌کم ۵ روز در هفته را با موفقیت کامل کرده است، که دامنهٔ این آموزش ممیزی‌های و مدیریت ممیزی ISMS را پوشش می‌دهد.

ت- ممیز باید دارای تجربه کافی در فرایندهای کلی ارزیابی امنیت اطلاعات پیش از کسب مسئولیت ممیزی باشد توصیه می‌شود این تجربه از طریق مشارکت در کمینه چهار موردِ ممیزی گواهینامه ISMS، شامل تمدید گواهینامه و ممیزی مراقبتی، کسب شده باشد. دست‌کم ۲۰ روز که به عنوان کمینه در نظر گرفته می‌شود، دست‌بالا ۵ روز مربوط به ممیزی مراقبتی باشد. مشارکت باید در بردارنده ی بازنگری مستندات و ارزیابی مخاطره، ارزیابی پیاده‌سازی و گزارش ممیزی باشد.

ث- ممیز دارای تجربه مربوط و جاری باشد.

ج- ممیز اطلاعات موجود و مهارت‌های مربوط به امنیت اطلاعات را حفظ کند و در ترقی حرفه‌ای پیوسته به روز باشد.

1 - Functions

کارشناسان فنی باید با معیارهای الف-، ب- و ث- منطبق باشند.

۷-۲-۱-۲ انتخاب ممیزان برای هدایت گروه

علاوه بر ۷-۱-۲-۲ و ۷-۲-۱-۱ معیار برای انتخاب کردن ممیز برای هدایت گروه باید این اطمینان را حاصل کند که این ممیز:

الف- به صورت فعال در تمامی مراحل دست‌کم سه ممیزی ISMS مشارکت دارد. مشارکت باید شامل دامنه‌ی کاربرد آغازی و طرح‌ریزی، بازنگری مستند و ارزیابی مخاطره، ارزیابی پیاده‌سازی و گزارش رسمی ممیزی باشد.

۷-۳ استفاده از ممیزان بیرونی و کارشناسان فنی بیرونی

الزامات بند ۷-۳ استاندارد ISO/IEC 17021-1 به‌کار می‌روند. علاوه بر این، الزامات و راهنمای زیر اعمال می‌شود.

۷-۳-۱ IS 7.3 استفاده از ممیزان بیرونی یا کارشناسان فنی بیرونی به عنوان بخشی از گروه ممیزی

کارشناسان فنی باید تحت نظارت یک ممیز کار کنند. کمینه الزامات برای کارشناسان فنی در ۷-۲-۱-۱ فهرست شده است.

۷-۴ سوابق کارکنان

الزامات بند ۷-۴ استاندارد ISO/IEC 17021-1 به‌کار می‌رود.

۷-۵ برون‌سپاری

الزامات بند ۷-۵ استاندارد ISO/IEC 17021-1 به‌کار می‌رود.

۸ الزامات اطلاعاتی

۸-۱ اطلاعات عمومی

الزامات بند ۸-۱ استاندارد ISO/IEC 17021-1 به‌کار می‌رود.

۸-۲ مستندات گواهینامه

الزامات بند ۸-۲ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به کار می‌رود.

۸-۲-۱ IS 8.2 مستندات گواهینامه ISMS

مستندات گواهینامه باید توسط کسی امضا شود که برای این مسئولیت به‌کار گرفته شده است. نسخه‌ی بیانیه کاربردپذیری باید در مستندات گواهینامه در نظر گرفته شده باشد.

یادآوری- تغییر در بیانیه کاربست پذیری که همگرایی واپایش‌ها را در دامنه‌ی کاربرد تغییر نمی‌دهد نیازمند به روز رسانی مستندات گواهینامه نیست.

شناسایی استانداردهای مشخص استفاده شده ممکن است در مستندات گواهینامه شامل شده باشد.

۸-۳ ارجاع به گواهینامه و استفاده از علامت‌ها

الزامات بند ۸-۳ استاندارد ISO/IEC 17021-1 به‌کار می‌رود.

۸-۴ محرمانگی[1]

الزامات بند ۸-۴ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌رود.

۸-۴-۱ IS 8.4 دسترسی به سوابق سازمانی

اگر هر گونه اطلاعات مرتبط با ISMS (از قبیل سوابق ISMS یا اطلاعات در مورد طراحی و اثربخشی واپایش‌ها) به دلیل این که حاوی اطلاعات محرمانه و حساس است، نمی‌تواند برای بازنگری توسط گروه ممیزی در دسترس باشد، پیش از ممیزی گواهینامه نهاد صدور گواهینامه باید از مشتری درخواست کند که آن‌ها را گزارش دهد. نهاد صدور گواهینامه، باید تعیین کند که آیا ISMS می‌تواند به اندازه‌ی کافی در غیاب این اطلاعات ممیزی را انجام دهد. اگر نهاد صدور گواهینامه نتیجه گیری کند که ممیزی کافی ISMS بدون بازنگری اطلاعاتی محرمانه‌ی شناسایی شده‌یا حساس ممکن نیست، باید به مشتری توصیه کرد که ممیزی گواهینامه صورت نمی‌گیرد مگر اجازه‌ی دسترسی مقتضی داده شود.

۸-۵ مبادله اطلاعات بین نهاد صدور گواهینامه و مشتری‌های آن

الزامات بند ۸-۵ استاندارد ISO/IEC 17021-1 به‌کار می‌رود.

۹ الزامات فرایند

۹-۱ فعالیت‌های پیش از صدور گواهی

۹-۱-۱ درخواست

الزامات بند ۹-۱-۱ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر اعمال

1 - Confidentiality

می‌شود.

۹-۱-۱-۱ آمادگی درخواست

نهاد صدور گواهینامه باید مشتری را ملزم کند که دارای ISMS ای مستند و پیاده‌سازی‌شده باشد که با استاندارد ISO/IEC 27001 و دیگر مستندات مورد نیاز برای گواهینامه مطابقت کند.

۹-۱-۲ بازنگری درخواست

الزامات بند ۹-۱-۲ استاندارد ISO/IEC 17021-1 به‌کار می‌رود.

۹-۱-۳ برنامه‌ی ممیزی

الزامات بند ۹-۱-۳ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر اعمال می‌شود.

۹-۱-۳-۱ IS 9.1.3 کلیات

برنامه‌ی ممیزی برای ممیزی‌های ISMS باید واپایش‌های معین امنیت اطلاعات را در نظر بگیرد.

۹-۱-۳-۲ IS 9.1.3 روشگان[1] ممیزی

رویه نهاد صدور گواهینامه نباید به عنوان روشی ویژه از پیاده‌سازی ISMS یا قالب ویژه برای مستندات و ثبت‌ها در نظر گرفته شود. روش‌های صدور گواهینامه باید بر این اصل باشد که ISMS مشتری الزامات مشخص در استاندارد ISO/IEC 27001 و خط‌مشی‌ها و اهداف مشتری را دارا است.

یادآوری- راهنمای بیشتر در مورد اصالت‌سنجی در استاندارد ISO/IEC 27007 ارائه شده است.

۹-۱-۳-۳ IS 9.1.3 آمادگی‌های کلی برای ممیزی اولیه

نهاد صدور گواهینامه باید الزام کند که مشتری تمامی ترتیبات لازم برای ارزیابی گزارش‌های داخلی ممیزی و گزارش‌های بازنگری‌های مستقل امنیت اطلاعات را ایجاد کند.

در مرحله‌ی ۱ ممیزی گواهینامه، دست‌کم اطلاعات زیر باید توسط مشتری ارائه شود :

الف- اطلاعات کلی مربوط به ISMS و فعالیت‌هایی که آن پوشش می‌دهد.

ب- رونوشتی از مستندات مورد نیاز ISMS در استاندارد ISO/IEC 27001 و در جای مورد نیاز مستندات متناظر.

1 - Methodology

۹-۱-۳-۴ IS 9.1.3 دوره‌های بازنگری

نهاد صدور گواهینامه نباید ISMS را تصدیق کند مگر آنکه دست‌کم در یک بازنگری مدیریتی و ممیزی داخلی ISMS، دامنه‌ی کاربرد گواهینامه را پوشش دهد.

۹-۱-۳-۵ IS 9.1.3 دامنه‌ی کاربرد گواهینامه

گروه ممیزی باید ISMS مشتری را توسط دامنه‌ی کاربرد تعریف شده با تمامی الزامات کاربردپذیر گواهینامه، ممیزی نماید. مشتری نهاد صدور گواهینامه در دامنه‌ی کاربرد ISMS باید تصدیق نماید که مشتری به الزامات بیان شده در بند ۴-۳ در استاندارد ISO/IEC 27001 می‌پردازد.

نهادهای صدور گواهینامه باید اطمینان حاصل کند که ارزیابی مخاطره و رسیدگی به مخاطره‌ی امنیت اطلاعات مشتری به صورت مناسب بازتابی از فعالیت‌های آن‌ها است و تا مرزهای فعالیت‌های تعریف شده در دامنه‌ی کاربرد گواهینامه گسترش یافته است. نهادهای صدور گواهینامه باید تصدیق نمایند که این موضوع در دامنه کاربرد ISMS و بیانیه‌ی دامنه‌ی کاربرد آن‌ها بازتاب داده شده است. نهاد صدور گواهینامه باید تصدیق نماید که دست‌کم یک بیانیه کاربردپذیر در هر دامنه‌ی کاربرد گواهینامه وجود دارد.

نهادهای صدور گواهینامه باید اطمینان یابند که واسط‌ها به همراه خدمات یا اقداماتی که به صورت کامل درون دامنه‌ی کاربرد ISMS نیستند، درون ISMS موضوع گواهینامه پرداخته می‌شود و در ارزیابی مخاطره‌ی امنیت اطلاعات مشتری وجود دارند. مثالی از این موقعیت به اشتراک گذاری تسهیلات (به طور مثال سامانه‌های IT، سامانه‌های پایگاه داده و ارتباطات یا برون‌سپاری کارکرد کسب‌وکار) با سازمان‌های دیگر است.

۹-۱-۳-۶ IS 9.1.3 معیار گواهینامه ممیزی

استاندارد ISO/IEC 27001، باید معیاری باشد که ISMS مشتری با آن معیار ممیزی می‌شود. ممکن است مستندات دیگری مرتبط با کارکردهای اجراشده برای گواهینامه مورد نیاز باشند.

۹-۱-۴ تعیین زمان ممیزی

الزامات بند ۹-۱-۴ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌روند.

۹-۱-۴-۱ IS 9.1.4 زمان ممیزی

نهادهای صدور گواهینامه باید به ممیزان، زمان کافی برای عهده‌دار شدن تمامی فعالیت‌های مرتبط با ممیزی اولیه، ممیزی مراقبتی و ممیزی صدور تمدید گواهینامه بدهند. محاسبه‌ی زمان ممیزی کل باید شامل زمان کافی برای گزارش دادن ممیزی باشد.

نهاد صدور گواهینامه باید از پیوست ب برای تعیین زمان ممیزی استفاده کند.

یادآوری- راهنمای و مثال‌های بیشتر در محاسبه‌ی زمان ممیزی در پیوست پ ارائه شده است.

۹-۱-۵ نمونه برداری چند-مکانی[1]

الزامات بند ۹-۱-۵ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این الزامات و راهنمای زیر به‌کار می‌روند.

۹-۱-۵-۱ IS 9.1.5 مکان‌های متعدد

۹-۱-۵-۱-۱ هنگامی‌که مشتری دارای مکان‌هایی است که معیارهای مورد الف تا پ را رعایت می‌کنند، نهادهای صدور گواهینامه ممکن است استفاده از رویکرد مبتنی بر نمونه برداری را برای ممیزی گواهینامه مکان‌های متعدد در نظر بگیرند:

الف- تمامی مکان‌ها تحت ISMS یکسان در حال انجام عملیات هستند، این ISMS دارای مدیریت و ممیزی مرکزی و تحت نظر بازنگری مدیریت مرکزی است.

ب- تمامی مکان‌ها درون برنامه‌ی ممیزی داخلی ISMS مشتری قرار دارند.

پ- تمامی مکان‌ها درون برنامه‌ی بازنگری مدیریت ISMS مشتری قرار دارند.

۹-۱-۵-۱-۲ نهاد صدور گواهینامه تمایل به استفاده از رویکرد مبتنی بر نمونه باید دارای رویه‌های جاری باشد تا از عوامل زیر اطمینان یابد:

الف- بازنگری اولیه قرارداد، تا بیشترین حدِ ممکن، تفاوت بین مکان‌ها را شناسایی می‌کند به طوری که سطح کافیِ نمونه برداری تعیین شده است.

ب- تعدادی از مکان‌ها به نمایندگی، توسط نهاد صدور گواهینامه نمونه برداری شده‌اند، با در نظر گرفتن عوامل زیر:

۱- نتایج ممیزی داخلی دفتر مرکزی و مکان‌ها

۲- نتایج بازنگری مدیریت

۳- تغییرات در اندازه‌ی مکان‌ها

۴- تغییرات در هدف کسب‌وکار مکان‌ها

۵- پیچیدگی سامانه‌های اطلاعاتی در مکان‌های مختلف

۶- تغییرات در روش‌های کاری

۷- تغییرات در فعالیت‌های متقبل شده

1 - Multi-site sampling

۸- تغییرات در طراحی و عملیات واپایش‌ها

۹- تعامل بالقوه با سامانه‌های حیاتی اطلاعات یا سامانه‌های پردازنده‌ی اطلاعات حساس

۱۰- الزامات قانونی مختلف

۱۱- جنبه‌های جغرافیایی و فرهنگی

۱۲- موقعیت مخاطره‌ی مکان

۱۳- رخدادهای امنیت اطلاعات در مکان‌های ویژه

پ- نمونه‌ی نماینده از تمامی مکان‌های درون دامنه‌ی کاربرد ISMS مشتری انتخاب شده است، این انتخاب باید بر مبنای انتخاب قضاوت برای بازتاب دادن عوامل نشان داده در مورد ب و عناصر تصادفی باشد.

ت- هر مکان موجود در ISMS که در معرض مخاطره‌های مهم است توسط نهاد صدور گواهینامه پیش از گواهینامه ممیزی می‌شود.

ث- برنامه‌ی گواهینامه در سایه‌ی الزامات بالا طراحی شده است و نمونه‌های نماینده‌ی دامنه‌ی کاربرد گواهینامه ISMS را درون دوره‌ی سه ساله پوشش می‌دهند.

ج- در موردی که عدم انطباق در دفتر مرکزی یا یک مکان مشاهده شده است، رویه اصلاح عملیات برای دفتر مرکزی و تمامی مکان‌های پوشش داده شده توسط گواهینامه اعمال می‌شود.

ممیزی باید به فعالیت‌های دفتر مرکزی مشتری را بپردازد تا اطمینان کسب نماید که ISMS به تمامی مکان‌ها اعمال می‌شود و در سطح عملیاتی، مدیریت مرکزی را تحویل می‌دهد. ممیزی باید به تمامی مسائل ذکر شده در بالا بپردازد.

۹-۱-۶ سامانه‌های چندگانه‌ی مدیریت

الزامات بند ۹-۱-۶ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌روند.

۹-۱-۶-۱ IS 9.1.6 یکپارچگی مستندات ISMS با دیگر سامانه‌های مدیریت

تا زمانی که ISMS می‌تواند به صورت روشن همراه با واسطهای مناسب سامانه‌های دیگر شناسایی شود، نهاد صدور گواهینامه ممکن است مستنداتی را بپذیرد که ترکیب شده‌اند (به طور مثال، برای امنیت اطلاعات، کیفیت، سلامت و امنیت و محیط)

۹-۱-۶-۲ IS 9.1.6 ترکیب ممیزی‌های سامانهٔ مدیریت

ممیز ISMS ممکن است با ممیزان دیگر سامانه‌های مدیریت ترکیب شده باشد و نشان داده شده که ممیزی

می‌تواند تمامی الزامات گواهینامه ISMS را برآورده کند. تمامی عناصر مهم ISMS باید آشکار باشند و در گزارش‌های ممیزی به آسانی قابل شناسایی باشد. کیفیت ممیزی نباید توسط ترکیب ممیزی‌ها تحت تاثیر منفی قرار گیرد.

۹-۲ طرح‌ریزی ممیزی‌ها

۹-۲-۱ تعیین اهداف، دامنه‌ی کاربرد و معیار ممیزی

الزامات بند ۹-۲-۱ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌روند.

۹-۲-۱-۱ IS 9.2.1 اهداف ممیزی

اهداف ممیزی باید در بردارنده ی تعیین اثربخشی سامانهٔ مدیریت برای کسب اطمینان از انجام واپایش‌های کاربردپذیر و اکتساب اهداف امنیت اطلاعات توسط مشتری بر مبنای ارزیابی مخاطره باشد.

۹-۲-۲ انتخاب و تخصیص گروه ممیزی

الزامات بند ۹-۲-۲ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌روند.

۹-۲-۲-۱ گروه ممیزی IS 9.2.2

گروه ممیزی باید به صورت رسمی منصوب شود و مستندات کاری مناسب برای آن‌ها تهیه شود. بیانیه ارائه شده به گروه ممیزی باید به صورت واضح تعریف شود و برای مشتری معلوم باشد.

گروه ممیزی ممکن است شامل فردی باشد که تمامی معیارهای بخش ۷-۱-۲-۱ را دارد.

۹-۲-۲-۲ IS 9.2.2 صلاحیت گروه ممیزی

الزامات فهرست شده در ۷-۱-۲ به‌کار می‌رود. برای فعالیت‌های مراقبتی و ممیزی مشخص، تنها الزاماتی اعمال می‌شوند که مربوط به فعالیت مراقبتی برنامه‌ریزی شده و فعالیت ممیزی مشخص هستند.

هنگام انتخاب و مدیریت گروه ممیزی برای ممیزی مشخص گواهینامه، نهاد صدور گواهینامه باید اطمینان یابد که صلاحیت هر تخصیص مناسب است. این گروه باید:

الف- دارای دانش فنی مناسب فعالیت‌های مشخص درون دامنه‌ی کاربرد ISMS برای گواهینامه و هنگامی که مرتبط با رویه متناظر و مخاطره‌های امنیت اطلاعات (کارشناسان فنی ممکن است این کارکرد را تکمیل کنند) باشد.

ب- دارای درک کافی از مشتری برای انجام ممیزی قابل اطمینان گواهینامه ISMS ارائه شده در دامنه‌ی کاربرد و مفاهیم ISMS درون سازمان مدیریتی جنبه‌های امنیت اطلاعات فعالیت‌ها، محصولات و خدماتش

باشد.

پ- دارای درکی مناسب از الزامات قانونی کاربردپذیر برای ISMS مشتری باشد.

یادآوری- منظور از درک مناسب، پیش‌زمینه‌ی قانونی عمیق نیست.

۹-۲-۳ طرح ممیزی

الزامات بند ۹-۲-۳ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌روند.

۹-۲-۳-۱ کلیات IS 9.2.3

طرح ممیزی برای ممیزان باید واپایشهای امنیتی اطلاعات تعیین شده را در نظر بگیرد.

۹-۲-۳-۲ IS 9.2.3 فنون ممیزی مربوط به شبکه

طرح ممیزی باید فنون شناسایی ممیزی مربوط به شبکه را که در مدت ممیزی به میزان مناسب استفاده خواهند شد شناسایی کند.

فنون ممیزی مربوط به شبکه ممکن است به طور مثال شامل عواملی مانند دورسخنی[1]، جلسه‌ی وب، تعامل ارتباطات بر مبنای وب و دسترسی الکترونیکی از دور برای مستندات ISMS یا فرایند ISMS باشد. توصیه می‌شود تمرکز این فنون بر افزایش اثربخشی و کارایی ممیزی باشد و یکپارچگی فرایند ممیزی را پشتیبانی کند.

۹-۲-۳-۳ IS 9.2.3 برنامه‌ریزی زمانی ممیزی

توصیه می‌شود نهاد صدور گواهینامه در مورد برنامه‌ریزی زمانی ممیزی با سازمان مورد نظر برای انجام ممیزی به توافق برسد به گونه‌ای که تمام دامنه‌ی کاربرد سازمان به بهترین شیوه نمایش داده شود. ملاحظات می‌توانند شامل فصل، ماه، روز/تاریخ و نوبت کاری در صورت نیاز باشند.

۹-۳ گواهینامه اولیه

الزامات بند ۹-۳ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌روند.

۹-۳-۱ IS 9.3.1 ممیزی گواهینامه اولیه

۹-۳-۱-۱ IS 9.3.1.1 مرحله ۱

در این مرحله از ممیزی، نهاد صدور گواهینامه باید مستنداتی از طراحی ISMS پوشاننده‌ی مستندات مورد

1 - Teleconference

نیاز در استاندارد ISO/IEC 27001 را به دست آورد.

نهاد صدور گواهینامه باید درکی کافی از طراحی ISMS در محتوای سازمان مشتری، ارزیابی مخاطره و کاهش آن (از جمله واپایش‌های معین)، خط‌مشی امنیت اطلاعات و به صورت ویژه اهداف آمادگی مشتری برای ممیزی به دست آورد. این امر امکان طرح‌ریزی برای مرحله ۲ را می‌دهد.

نتایج مرحله ۱ باید در گزارشی مستند شود. نهاد صدور گواهینامه باید مرحله‌ی ۱ گزارش ممیزی را پیش از تصمیم گیری برای انجام مرحله‌ی ۲ و برای انتخاب اعضای گروه ممیزی مرحله‌ی ۲ یا صلاحیت مناسب بازنگری نماید.

نهاد صدور گواهینامه باید مشتری را از انواع اطلاعات و سوابقی که ممکن است برای تعیین تفصیلی در مرحله ۲ مورد نیاز باشد، آگاه نماید.

۹-۳-۱-۲ IS 9.3.1.2 مرحله ۲

۹-۳-۱-۲-۱ نهاد صدور گواهینامه بر مبنای یافته‌های مستند شده در مرحله‌ی ۱ گزارش ممیزی، طرح ممیزی را برای انجام مرحله‌ی ۲ تدوین می‌کند. علاوه بر این، برای ارزشیابیِ پیاده‌سازی مناسب ISMS، اهداف مرحله ۲ عبارت‌اند از:

الف- تصدیق پایبندی[1] مشتری به خط‌مشی‌ها، اهداف و رویه‌های خود.

۹-۳-۱-۲-۲ برای انجام این مرحله، مشتری باید متمرکز بر عوامل زیر باشد:

الف- رهبریِ مدیریت عالی و الزام وی به خط‌مشی امنیت اطلاعات و اهداف امنیت اطلاعات

ب- الزامات مستند فهرست شده در استاندارد ISO/IEC 27001

پ- ارزیابی امنیت اطلاعات مرتبط با مخاطرات و کسب اطمینان از اینکه اگر ارزیابی تکرار شود دارای نتایجی سازگار، مجاز و قابل مقایسه می‌شود.

ت- تعیین اهداف واپایشی و واپایش‌های بر مبنای ارزیابی امنیت اطلاعات و فرایندهای کاهش مخاطره

ث- عملکرد امنیت اطلاعات و اثربخشی ISMS، ارزیابی کردن اهداف امنیت اطلاعات

ج- مطابقت بین واپایش‌های معین، بیانیه‌ی کاربست پذیری و نتایج ارزیابی مخاطره‌ی امنیت اطلاعات و فرایند کاهش مخاطره و خط‌مشی و اهداف امنیت اطلاعات.

چ- پیاده‌سازی واپایش‌های (پیوست ت)، در نظر گرفتن محتوای درونی و بیرونی و مخاطرات مرتبط، پایش سازمان، سنجش و تحلیل فرایندهای امنیت اطلاعات، تعیین کردن اینکه آیا واپایش‌ها اعمال شده‌اند و اثر و مشاهده‌ی اهداف امنیت اطلاعات بیان شده‌ی آن‌ها

1 - Adhere

ح- برنامه‌ها، فرایندها، رویه‌های، رکوردها، ممیزی‌های داخلی و بازنگری‌های اثربخشی برای کسب اطمینان از اینکه آن‌ها قابل ردیابی برای تصمیم گیری مدیریت عالی و خط‌مشی‌ها و اهداف امنیت اطلاعات هستند.

۹-۴ انجام ممیزی‌ها

الزامات بند ۹-۴ استاندارد ISO/IEC 17021-1 به کار می‌روند. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌روند.

۹-۴-۱ IS 9.4 کلیات

نهاد صدور گواهینامه باید رویه‌های مستند برای موارد زیر داشته باشد:

الف- ممیزی اولیه گواهینامه برای ISMS مشتری، مطابق با ضابطه‌ی استاندارد ISO/IEC 17021-1

ب- ممیزی‌های مراقبتی و تمدید گواهینامه ISMS مشتری مطابق با استاندارد ISO/IEC 17021-1 به صورت دوره‌ای[1] برای انطباقِ پیوسته با الزامات مرتبط و برای درستی‌سنجی و ثبت کردن اینکه مشتری فعالیتی صحیح بر مبنای زمان برای اصلاح تمام عدم مطابقت‌ها انجام می‌دهد.

۹-۴-۲ IS 9.4 عناصر ویژه ممیزی ISMS

نهاد صدور گواهینامه، با نمایندگی گروه ممیزی، باید:

الف- مشتری را ملزم کند تا نشان دهد که ارزیابی مخاطرات مرتبط با امنیت اطلاعات، برای عملیات ISMS در دامنه‌ی کاربرد ISMS، مرتبط و کافی است.

ب- تعیین کند که آیا رویه‌های مشتری برای شناسایی، تعیین و ارزیابی مخاطرات مرتبط با امنیت اطلاعات و نتایج پیاده‌سازی آن‌ها مطابق با خط‌مشی، اهداف و مقاصد مشتری است.

همچنین، نهاد صدور گواهینامه باید تعیین کند که آیا رویه‌های به‌کار گرفته شده در ارزیابی مخاطرات دقیق هستند و به‌درستی پیاده‌سازی می‌شوند.

۹-۴-۳ IS 9.4 گزارش ممیزی

۹-۴-۳-۱ علاوه بر الزامات گزارش دهی در استاندارد ISO/IEC 17021-1 بند ۹-۴-۸ ، گزارش ممیزی باید اطلاعات زیر را فراهم نماید یا اشاره‌ای به آن‌ها داشته باشد:

الف- بیان علت ممیزی شامل خلاصه‌ای از بازنگری سند

ب- بیان علت ممیزی گواهینامه تحلیل مخاطره‌ی امنیت اطلاعات مشتری

1 - Periodic

پ- انحراف از طرحِ ممیزی[1] (به طور مثال صرف نمودن زمان بیشتر یا کمتر به فعالیت‌های برنامه‌ریزی شده)

ت) دامنه‌ی کاربرد ISMS

۹-۴-۳-۲ گزارش ممیزی باید دارای جزئیات کافی برای آسان نمودن و پشتیبانی از تصمیمات گواهینامه باشد. گزارش ممیزی شامل عوامل زیر است:

الف- رَدهای ممیزی[2] مهم دنبال شوند و روشگان ممیزی استفاده شود (بند ۹-۱-۳-۱ مشاهده شود).

ب- مشاهدات انجام شوند، هم مشاهدات مثبت (به طور مثال خصوصیات ارزشمند) و منفی (به صورت مثال عدم انطباق‌های بالقوه)

پ- نظرات در مورد انطباق ISMS مشتری با الزامات گواهینامه با بیانیه‌ی روشن از عدم انطباق‌ها، مرجعی برای نسخه‌ی بیانیه‌ی کاربردپذیری و در جای کاربردپذیر هر مقایسه‌ی مفید با نتایج ممیزی‌های گواهینامه پیشین مشتری.

پرسشنامه‌های تکمیل‌شده، بازبینه‌ها[3]، مشاهدات، گزارش روزانه‌ی عملیات یا یادداشت‌های ممیزی ممکن است قسمتی از گزارش ممیزی را شکل دهند. اگر این روش‌ها استفاده شده باشند، این مستندات باید به نهاد صدور گواهینامه به صورت شواهدی برای پشتیبانی از تصمیم گیری صدور گیری تقدیم شوند. اطلاعات پیرامون نمونه‌های ارزیابی شده در مدت ممیزی باید شامل گزارش ممیزی، یا دیگر مستندات گواهینامه باشند.

این گزارش باید کفایت سازمان داخلی و رویه پذیرفته شده توسط مشتری را در نظر بگیرد تا اعتماد در ISMS را نشان دهد.

علاوه بر الزامات برای گزارش استاندارد ISO/IEC 17021-1، بند ۹-۴-۸، گزارش باید عوامل زیر را پوشش دهد:

- خلاصه‌ای از مشاهدات مهم مثبت و منفی، با توجه به پیاده‌سازی و اثربخشی الزامات ISMS و واپایش‌های ISMS.
- پیشنهادهای گروه ممیزی مانند اینکه آیا توصیه می‌شود ISMS مشتری دارای گواهی شود یا نه، همراه اطلاعات مربوط به اثبات کردن این پیشنهاد.

۹-۵ تصمیم‌گیری برای صدور گواهی

الزامات بند ۹-۵ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌روند.

1 - Audit plan
2 - Audit trails
3 - Checklists

۹-۵-۱ IS 9.5 تصمیم برای صدور گواهی

تصمیم‌گیری برای گواهینامه، علاوه بر الزامات استاندارد ISO/IEC 17021-1، باید بر مبنای توصیه‌های گواهینامه از سوی گروه ممیزی باشد که در گزارش ممیزی گواهینامه آن‌ها ارائه شده است. (بند ۹-۴-۳ را مشاهده نمایید).

توصیه نمی‌شود اشخاص یا کارگروه‌هایی که در مورد گواهینامه تصمیم گیری می‌نمایند به صورت عادی توصیه منفی از گروه ممیزی را نادیده بگیرند. اگر این موقعیت به وجود آمد، نهاد صدور گواهینامه باید اساس تصمیم گیری را در موردِ به کار نبستنِ توصیه‌ها، مستند و توجیه کند.

تا زمانی که شواهد کافی برای نمایش دادن اینکه برنامه‌ریزی موجود برای بازنگری مدیریت و ممیزی‌های داخلی ISMS پیاده‌سازی شده موثر اند و نگه داشته خواهند شد، گواهینامه نباید به مشتری واگذار شود.

۹-۶ نگهداشت گواهی[1]

۹-۶-۱ کلیات

الزامات بند ۹-۶-۱ استاندارد ISO/IEC 17021-1 به‌کار می‌رود.

۹-۶-۲ فعالیت‌های مراقبتی

الزامات بند ۹-۶-۲ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌روند.

۹-۶-۲-۱ IS 9.6.2 فعالیت‌های مراقبتی

۹-۶-۲-۱-۱ رویه‌های ممیزی مراقبتی باید مطابق با ممیزی‌های گواهینامه ISMS مشتری و به صورت توصیف شده در این استاندارد باشد.

هدف مراقبت، تصدیق نمودن این است که ISMS مصوب برای در نظر گرفتن پیاده‌سازی تغییرات که سامانه به صورت نتیجه‌ی تغییرات در عملیات مشتری و تایید کردن صلاحیت پیوسته با الزامات گواهینامه استفاده می‌شود. عواملی که دست‌کم برنامه‌های ممیزی مراقبتی باید پوشش دهد به شرح زیر است:

الف- عناصر نگهداشت سامانه مانند ارزیابی مخاطره‌ی امنیت اطلاعات و نگهداشت واپایش‌ها، ممیزی داخلی ISMS، بازنگری مدیریت و اقدامات اصلاحی.

ب- ارتباطات از طرف‌های بیرونی به صورت مورد نیاز توسط استاندارد ISMS ISO/IEC 27001 و مستندات مورد نیاز دیگر برای صدور گواهی.

پ- تغییرات سامانه‌های مستند شده

1 - Maintaining certification

ت- نواحی در معرض تغییرات

ث- الزامات منتخب از استاندارد ISO/IEC 27001

ج- نواحی منتخب دیگر به صورت مناسب

۹-۶-۲-۱-۲ کمینه، هر مراقبت از طریق نهاد صدور گواهینامه باید موارد زیر را بازنگری کند:

الف- اثربخشی ISMS با توجه به دستیابی به اهداف خط‌مشی امنیت اطلاعات مشتری.

ب- کارکرد رویه‌ها برای ارزشیابی و بازنگری متناوب سازگاری داشتن با قوانین و مقررات مرتبط امنیت اطلاعات

پ- تغییرات برای واپایش‌های تعیین شده و تغییرات حاصل برای بیانیه کاربردپذیری (SoA)[1]

ت- پیاده‌سازی و اثربخشی واپایش مطابق با برنامه‌ی ممیزی

۹-۶-۲-۱-۳ نهاد صدور گواهینامه باید قادر به سازگار نمودن برنامه‌ی نظارتی خود با مسائل امنیت اطلاعات مرتبط با مخاطرات و اثرات بر مشتری و توجیه این برنامه باشد.

ممیزی‌های نظارتی ممکن است با ممیزی‌های دیگر سامانه‌های مدیریت ترکیب شده باشند. گزارش باید به صورت روشن جنبه‌های مرتبط به هر سامانهٔ مدیریت را نشان دهد.

در مدت ممیزی‌های نظارتی، نهادهای صدور گواهینامه باید به سوابق مشهود و شکایت‌ها و عواملی که مشتری ISMS خود و رویه را بررسی کرده رسیدگی کند؛ پیش از نهاد صدورگواهی باید هر عدم مطابقت یا عدم رعایت الزامات گواهینامه آشکار شود .

گزارش نظارتی به صورت ویژه باید شامل اطلاعات عدم انطباق‌های آشکار شده از قبل و نسخه‌ی SoA و تغییرات مهم ممیزی پیشین باشد. گزارش ایجاد شده از نظارت باید برای پوشش دادن الزامات کلی ۹-۶-۲-۱-۱ و ۹-۶-۲-۱-۲ در بالا باشد.

۹-۶-۳ تمدید گواهینامه

الزامات بند ۹-۶-۳ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌روند.

۹-۶-۳-۱ IS 9.6.3 ممیزی‌های تمدید گواهینامه

رویه ممیزی تمدید گواهینامه باید با ممیزی‌های گواهینامه اولیه‌ی ISMS مشتری به صورت توصیف شده در این استاندارد مطابقت داشته باشد.

زمان مجاز برای پیاده‌سازی عملیات اصلاحی باید مطابق با شدت عدم انطباق و متناظر با مخاطره‌ی امنیت

1 - Statement of Applicability

اطلاعات باشد.

۹-۶-۴ ممیزی‌های ویژه[1]

الزامات بند ۹-۶-۴ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌روند.

۹-۶-۴-۱ IS 9.6.4 موردهای ویژه

اقدامات ضروری برای اجرای ممیزی‌های ویژه باید در شرایط ویژه باشد اگر مشتری با ISMS دارای گواهی بیشترین اصلاحات را برای سامانه‌اش ایجاد می‌کند یا اگر تغییرات دیگری رخ می‌دهد که می‌تواند بر گواهینامه آن تاثیر گذارد.

۹-۶-۵ تعلیق، ابطال[2] یا کاهش حوزه‌ی گواهی

الزامات بند ۹-۶-۵ استاندارد ISO/IEC 17021-1 به‌کار می‌رود.

۹-۷ اعتراض[3]

الزامات بند ۹-۷ استاندارد ISO/IEC 17021-1 به‌کار می‌رود.

۹-۸ شکایات[4]

الزامات بند ۹-۸ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به‌کار می‌روند.

۹-۸-۱ IS 9.8 شکایات

شکایات، نمایانگر رخداد بالقوه و نشانگر عدم انطباقِ محتمل است.

۹-۹ سوابق مشتری

الزامات بند ۹-۹ استاندارد ISO/IEC 17021-1 به‌کار می‌رود.

۱۰ الزامات سامانهٔ مدیریت برای نهادهای صدور گواهی

۱۰-۱ گزینه‌ها

الزامات بند ۱۰-۱ استاندارد ISO/IEC 17021-1 به‌کار می‌رود. علاوه بر این، الزامات و راهنمای زیر به‌کار

1 - Special audits
2 - Withdrawing
3 - Appeals
4 - Complaints

می‌روند.

۱۰-۱-۱ IS 10.1 پیاده‌سازی ISMS

پیشنهاد شده است که نهادهای صدور گواهینامه ISMS را مطابق با استاندارد ISO/IEC 27001 پیاده‌سازی نمایند.

۱۰-۲ گزینه‌ی الف: الزامات کلی مدیریت سامانه

الزامات بند ۱۰-۲ استاندارد ISO/IEC 17021-1 به‌کار می‌رود.

۱۰-۳ گزینه‌ی ب: الزامات مدیریت سامانه مطابق با استاندارد ISO 9001

الزامات بند ۱۰-۳ استاندارد ISO/IEC 17021-1 به‌کار می‌رود.

پیوست الف

(آگاهی‌دهنده)

دانش و مهارت‌ها برای ممیزی و صدور گواهینامه ISMS

الف-۱ مرور کلی

جدول الف-۱ خلاصه‌ای از دانش و مهارت‌های مورد نیاز برای ممیزی ISMS و گواهینامه فراهم می‌کند اما آگاهی‌دهنده است زیرا تنها حوزه‌هایی از دانش و مهارت را برای کارکردهای گواهینامه مشخص شناسایی می‌کند.

الزامات صلاحیت برای هر کارکرد در متن اصلی این استاندارد بیان شده و این جدول مرجعی برای الزامات مشخص است.

جدول الف-۱- دانش برای ممیزی و صدور گواهینامه ISMS

	کارکردهای گواهینامه		
	انجام بازنگری کاربرد (انجام بازنگری کاربرد برای تعیین کردن صلاحیت مورد نیاز گروه ممیزی، به منظور انتخاب اعضای گروه ممیزی و تعیین زمان ممیزی)	بازنگری گزارش‌های ممیزی و تصمیم‌گیری‌ها در مورد گواهینامه	ممیزی و هدایت گروه ممیزی
دانش			
واژگان، اصول، کارها و فنون مدیریت امنیت اطلاعات		۷-۱-۲-۴-۲	۷-۱-۲-۱-۲
استانداردها و مستندات الزامی سامانهٔ مدیریت امنیت اطلاعات	۷-۱-۲-۳-۱	۷-۱-۲-۴-۳	۷-۱-۲-۱-۳
کارهای مدیریت کسب‌وکار			۷-۱-۲-۱-۴
بخش کسب‌وکار مشتری	۷-۱-۲-۳-۲	۷-۱-۲-۴-۴	۷-۱-۲-۱-۵
محصولات، فرایندها و سازمان مشتری	۷-۱-۲-۳-۳	۷-۱-۲-۴-۵	۷-۱-۲-۱-۶

الف-۲ ملاحظات کلی در مورد صلاحیت

چندین روش وجود دارد که توسط آن‌ها ممیزان می‌توانند دانش و تجربه‌ی خود را اثبات نمایند. دانش و تجربه می‌توانند ارزیابی شود، به طور مثال با استفاده از مهارت‌های فنی شناسایی شده. رکوردهای ثبت‌نام تحت طرح‌واره‌ی گواهینامه‌ی کارکنان، می‌تواند برای ارزیابی دانش و تجربه‌ی مورد نیاز، استفاده شود. توصیه می‌شود سطح صلاحیت الزامی برای گروه ممیزی متناظر با حوزه‌ی صنعتی/فنی سازمان و پیچیدگی ISMS پایه گذاری شود.

الف-۳ ملاحظات مشخص دانش و تجربه

الف-۳-۱ دانش عمومی مرتبط به ISMS

علاوه بر الزامات ۷-۱-۲، توصیه می‌شود عوامل زیر در نظر گرفته شود. توصیه می‌شود ممیزان دارای دانش و درک از ممیزی زیر و ISMS مورد نظر باشند:

- برنامه نویسی و طرح‌ریزی ممیزی؛
- نوع و روشگان ممیزی؛
- مخاطره‌ی ممیزی؛
- تحلیل فرایندهای امنیت اطلاعات؛
- بهبود پیوسته؛
- ممیزی داخلی امنیت اطلاعات؛

توصیه می‌شود ممیزان دارای دانش و درک از الزامات مقرراتی[1] زیر باشند:

- مالکیت معنوی؛
- محتوا، محافظت و نگهداری از سوابق سازمانی؛
- محافظت و حریم داده؛
- مقرراتِ واپایش‌های رمزنگاری؛
- تجارت الکترونیکی؛
- امضاهای الکترونیکی و رقمی(دیجیتال)؛
- مراقبت فضای کاری؛
- تفسیر ارتباط از دور و پایش داده (به طور مثال رایانامه)؛

1 - Regulatory requirements

- سوء استفاده[1] از رایانه؛
- جمع آوری الکترونیکیِ شواهد؛
- آزمون نفوذ[2]؛
- الزامات بخش-خاص[3] بین‌المللی و ملی (مانند، بانکداری).

1 - Abuse
2 - Penetration testing
3 - Sector-specific

پیوست ب

(الزامی)

زمان ممیزی

ب-۱ مقدمه

این پیوست شامل الزامات بیشتر مرتبط با بند ۹-۱ استاندارد ISO/IEC 17021-1 است. این پیوست کمینه الزامات و راهنما برای نهاد صدور گواهینامه در توسعه‌ی رویه خود به منظور تعیین مقدار زمان مورد نیاز برای گواهینامه دامنه‌های کاربرد ISMS اندازه‌های متفاوت و پیچیدگی در طیف گسترده‌ی فعالیت‌ها فراهم می‌کند.

نهادهای صدور گواهینامه باید مقدار زمان ممیزی را برای هر مشتری و ISMS گواهینامه برای گواهینامه اولیه، نظارت و تمدید گواهینامه شناسایی نمایند. استفاده از این پیوست در مرحله‌ی طرح‌ریزی ممیزی منجر به رویکرد سازگار برای تعیین زمان ممیزی مناسب می‌شود. علاوه بر این، زمان ممیزی ممکن است بر مبنای چیزهای یافت‌شده در حین دوره‌ی ممیزی، تنظیم شود، مخصوصا در حین مرحله‌ی ۱ (به طور مثال، ارزیابی‌های متفاوت پیچیدگی دامنه‌ی کاربرد ISMS یا مکان‌های متفاوت این دامنه‌ی کاربرد).

این پیوست موارد زیر را بیان می‌کند:

- جنبه‌هایی که برای محاسبه‌ی زمان ممیزی مفید هستند (ب-۲)؛
- الزامات برای رویه‌های برای تعیین زمان ممیزی برای مراحل متفاوت ممیزی (ب-۳ تا ب-۶)؛
- الزامات مرتبط به ممیزی‌های چند مکان (ب-۶).

مثال‌هایی برای محاسبه‌ی زمان ممیزی جهت نمایش دادن کاربرد پیوست ب را می‌توان در پیوست پ یافت.

فرض پایه‌ی این رویکرد این است که توصیه می‌شود محاسبه‌ی برنامه‌ی زمانی برای تعیین زمان ممیزی :

الف- تنها ویژگی‌هایی را در نظر بگیرد که می‌توانند تعیین شود؛

ب- به اندازه‌ی کافی آسان باشد تا توسط نهادهای صدور گواهینامه به صورت کارا به کار رود؛

پ- به اندازه‌ی کافی پیچیده باشد تا دارای تمایز کافی باشد.

تعیین زمان ممیزی برمبنای اعداد فراهم شده در جدول ب-۱ («نمودار زمان ممیزی») است و باید عوامل هم بخشی را برای اصلاح در نظر بگیرد.

ب-۲ مفاهیم

ب-۲-۱ تعداد افرادی که تحت واپایش سازمان کار می‌کنند

تعداد کل افرادی که تحت واپایش سازمان کار می‌کنند برای تمامی نوبت‌ها نقطه‌ی آغازگر تعیین زمان ممیزی است.

یادآوری- اصطلاح « افرادی که تحت واپایش سازمان کار می‌کنند» در استاندارد ISO/IEC 17021-1 به کارکنان اطلاق می‌شود.

کارکنان نیمه‌وقت تحت واپایش سازمان در مقایسه با فرد تمام وقت تحت واپایش سازمان با تعداد افرادی که تحت واپایش سازمان متناسب با ساعات کاری کار می‌کنند، همکاری می‌نمایند. این تعیین باید وابسته به تعداد ساعات کاری در مقایسه با کارکنان تمام وقت باشد.

ب-۲-۲ روز ممیز

زمان ممیزی به همان صورت ارجاع داده شده در نمودار برحسب «روزهای ممیزی» سپری شده در مدت ممیزی است. اساس محاسبات پیوست ب، ۸ ساعت کاری در یک روز است.

ب-۲-۳ مکان موقت

مکان موقت موقعیتی به جز مکان‌های شناسایی شده در مستندات گواهینامه است که در آن فعالیت‌های درون دامنه‌ی کاربرد گواهینامه برای دوره‌ی زمانی تعریف شده پیاده‌سازی شده‌اند. این مکان‌ها می‌توانند در گستره مکان‌های عمده مدیریت پروژه تا مکان‌های کمینه خدمات / نصب باشند. توصیه می‌شود نیاز به بازدید این مکان‌ها و گسترش نمونه برداری بر مبنای ارزیابی مخاطرات شکست برای مشاهده‌ی اهداف IS به دلیل عدم انطباق آغاز شده در مکان موقت باشد. توصیه می‌شود نمونه‌ی این مکان‌های منتخب بازه‌ی نیازهای سازگاری سازمان و تغییرات خدمات ملاحظات را برای اندازه‌ها و انواع مختلف مرحله‌های پروژه در حال فرایند نمایش دهد. برای نمونه برداری کلی ۹-۱-۵-۱ مشاهده شود.

ب-۳ رویه برای تعیین زمان ممیزی برای ممیزی اولیه

ب-۳-۱ کلیات

محاسبه‌ی زمان ممیزی باید از رویه مستند پیروی کند.

ب-۳-۲ ممیزی از دور

اگر فنون ممیزی از دور مانند همکاریِ مبتنی بر وب[1]، جلسه‌ی وب، دورسخنی و / یا ممیزی الکترونیکی فرایندهای سازمان برای واسط یا سازمان به‌کار گرفته شود، توصیه می‌شود این فعالیت‌ها در طرح ممیزی شناسایی شوند (۹-۲-۳) و ممکن است به صورت همکاری ویژه به کل «زمان ممیزی در-مکان» در نظر گرفته شوند.

اگر نهاد صدور گواهینامه، طرح ممیزی را برای فعالیت‌های ممیزی از دور بیش از ۳۰٪ زمان ممیزی

1 - Web-based collaboration

طرح‌ریزی شده در-مکان نشان دهد، نهاد صدور گواهینامه باید طرح ممیزی را توجیه کند و شکل قابل قبول از نهاد اعتباربخشی را پیش از پیاده‌سازی به دست آورد.

یادآوری- زمان ممیزی در-مکان به زمان اختصاص داده شده برای ممیزی در مکان برای هر مکان ارجاع داده می‌شود. ممیزی‌های الکترونیکی از دور، ممیزی‌های از دور در نظر گرفته می‌شوند؛ حتی اگر ممیزی‌های الکترونیکی به صورت فیزیکی در فرضیات سازمان در نظر گرفته می‌شوند.

ب-۳-۳ محاسبه‌ی زمان ممیزی

نمودار زمان ممیزی مجموعه‌ای از نقاط آغازی برای تعداد متوسطی از روزهای ممیزی ارائه می‌دهد (این نمودار در اینجا و در ادامه، تعداد روزها برای ممیزی اولیه را تعیین می‌کند (مرحله ۱و۲)) که تجربه نشان می‌دهد برای دامنه‌ی کاربرد ISMS با تعداد معینی کارمند که تحت واپایش سازمان کار می‌کنند، مناسب است. تجربه نشان داده است که برای دامنه‌ی کاربرد ISMS با اندازه‌ی مشابه، ممکن است به زمانی بیشتر یا کمتری نیاز باشد.

نمودار زمان ممیزی زیر، چارچوبی را فراهم آورده است که باید برای طرح‌ریزی ممیزی توسط شناسایی نقطه‌ی آغازی بر مبنای تعداد کل افراد کارمند تحت واپایش سازمان برای تمامی نوبت‌ها و تنظیم کردن این بر مبنای عوامل مهم اعمال شده به دامنه‌ی کاربرد ISMS ممیزی شود و توزیع هر عامل وزن افزایشی یا کاهشی و قیود انحراف بیشینه استفاده شود (ب-۳-۴ و ب-۳-۵ مشاهده شود). واژگان استفاده شده در این نمودار که در ب-۲ بالا و پیوست پ توضیح داده شده‌اند مثال‌هایی از چگونگی انجام آن را ارائه می‌دهند.

جدول ب-۱- نمودار زمان ممیزی

تعداد افرادی که در سازمان کار می‌کنند	زمان ممیزی QMS برای ممیزی اولیه (روزهای ممیزی)	زمان ممیزی EMS برای ممیزی اولیه (روزهای ممیزی)	زمان ممیزی ISMS برای ممیزی اولیه (روزهای ممیزی)	عوامل افزایشی و کاهشی	مجموع زمان ممیزی
۱~۱۰	۲-۱/۵	۳-۲/۵	۵	به بند ب-۳-۴ مراجعه شود	
۱۱~۱۵	۲/۵	۳/۵	۶	به بند ب-۳-۴ مراجعه شود	
۱۶~۲۵	۳	۴/۵	۷	به بند ب-۳-۴ مراجعه شود	
۲۶~۴۵	۴	۵/۵	۸/۵	به بند ب-۳-۴ مراجعه شود	
۴۶~۶۵	۵	۶	۱۰	به بند ب-۳-۴ مراجعه شود	
۶۶~۸۵	۶	۷	۱۱	به بند ب-۳-۴ مراجعه شود	
۸۶~۱۲۵	۷	۸	۱۲	به بند ب-۳-۴ مراجعه شود	
۱۲۶~۱۷۵	۸	۹	۱۳	به بند ب-۳-۴ مراجعه شود	
۱۷۶~۲۷۵	۹	۱۰	۱۴	به بند ب-۳-۴ مراجعه شود	
۲۷۶~۴۲۵	۱۰	۱۱	۱۵	به بند ب-۳-۴ مراجعه شود	
۴۲۶~۶۲۵	۱۱	۱۲	۱۶/۵	به بند ب-۳-۴ مراجعه شود	
۶۲۶~۸۷۵	۱۲	۱۳	۱۷/۵	به بند ب-۳-۴ مراجعه شود	
۸۷۶~۱۱۷۵	۱۳	۱۵	۱۸/۵	به بند ب-۳-۴ مراجعه شود	
۱۱۷۶~۱۵۵۰	۱۴	۱۶	۱۹/۵	به بند ب-۳-۴ مراجعه شود	
۱۵۵۱~۲۰۲۵	۱۵	۱۷	۲۱	به بند ب-۳-۴ مراجعه شود	
۲۰۲۶~۲۶۷۵	۱۶	۱۸	۲۲	به بند ب-۳-۴ مراجعه شود	
۲۶۷۶~۳۴۵۰	۱۷	۱۹	۲۳	به بند ب-۳-۴ مراجعه شود	
۳۴۵۱~۴۳۵۰	۱۸	۲۰	۲۴	به بند ب-۳-۴ مراجعه شود	
۴۳۵۱~۵۴۵۰	۱۹	۲۱	۲۵	به بند ب-۳-۴ مراجعه شود	
۵۴۵۱~۶۸۰۰	۲۰	۲۳	۲۶	به بند ب-۳-۴ مراجعه شود	
۶۸۰۱~۸۵۰۰	۲۱	۲۵	۲۷	به بند ب-۳-۴ مراجعه شود	
۵۸۰۱~۱۰۷۰۰	۲۲	۲۷	۲۸	به بند ب-۳-۴ مراجعه شود	
>۱۰۷۰۰	از توالی فوق پیروی می‌کند	از توالی فوق پیروی می‌کند	از توالی فوق پیروی می‌کند	به بند ب-۳-۴ مراجعه شود	

ب-۳-۴ عوامل برای تنظیم زمان ممیزی

نمودار زمان ممیزی نباید در مجزا استفاده شود. زمان تخصیص داده شده باید عوامل زیر را نیز در نظر بگیرد که متناسب با پیچیدگی ISMS و ارجاع داده شده به تلاش مورد نیاز برای ممیزی ISMS است:

الف- پیچیدگی ISMS (به طور مثال، حساسیت اطلاعات، موقعیت مخاطره ISMS و ....)

ب- نوع(های) کسب‌وکار انجام شده درون دامنه‌ی کاربرد ISMS

پ- عملکرد نشان داده شده‌ی پیشین از ISMS

ت- میزان و گوناگونی فناوری استفاده شده در پیاده‌سازی مولفه های مختلف ISMS (به طور مثال، تعداد بن‌سازه‌های متفاوت IT، تعداد شبکه‌های مجزا)

ث- گسترش برون‌سپاری و آرایش‌های طرف سوم استفاده شده در دامنه‌ی کاربرد ISMS

ج- گسترش توسعه‌ی سامانهٔ اطلاعات

چ- تعداد مکان‌ها و تعداد مکان‌های جایگزین هنگام فاجعه[1] (DR)

ح- برای نظارت یا ممیزی تمدید گواهینامه : میزان و گسترش تغییرات مرتبط با ISMS مطابق با استاندارد ISO/IEC 17021-1,8-5-3

پیوست پ مثال‌هایی در مورد چگونگی در نظر گرفتن این عوامل در زمان محاسبه‌ی زمان حسابرسی ارائه می‌دهد.

نمونه عوامل افزون که نیازمند زمان ممیزی افزون هستند، عبارت‌اند از:

- جابجایی‌های پیچیده‌ای که شامل بیش از یک ساختمان یا موقعیت در دامنه‌ی کاربرد ISMS هستند؛
- کارکنانی که بیش از یک زبان صحبت می‌کنند (نیازمند مفسر یا منع مفسران از کار مستقل است) یا مستندات فراهم شده در بیش از یک زبان؛
- فعالیت‌هایی که نیازمند ملاقات مکان‌های موقت برای تصدیق فعالیت‌های مکان‌های دائم هستند. سامانهٔ مدیریت آن در معرض گواهینامه است (پاراگراف زیر فهرست بعدی مشاهده شود)
- تعداد بالای استانداردها و مقرراتی که برای ISMS به کار می‌روند.

عوامل نمونه‌ای که نیازمند زمان ممیزی کمتری هستند، عبارت‌اند از:

- ایجاد/فرایند کم مخاطره
- فرایندهای درگیر فعالیت عمومی (به طور مثال تنها خدمات)
- درصد بالایی از افرادی که تحت واپایش سازمان کار می‌کنند مسئولیتی مشابه را انجام می‌دهند.
- دانش قبلی از سازمان (به طور مثال اگر سازمان توسط همان نهاد صدور گواهینامه دارای استاندارد دیگری است).
- آمادگی بالای مشتری برای گواهینامه (به طور مثال، دارای گواهینامه یا شناخته شده توسط طرح

1 -Disaster Recovery

طرف سوم)

- بلوغ بالای سامانهٔ مدیریت جاری

در موقعیتی که مشتری گواهینامه یا سازمان دارای گواهی، محصولات یا خدمات خود را در مکان‌های موقت ارائه می‌دهند مهم است که ارزیابی این مکان‌ها در ممیزی گواهینامه و برنامه‌ی نظارتی ثبت شده باشد.

عوامل بالا باید درنظر گرفته شوند و برای آن عواملی که زمان ممیزی بیشتر یا کمتری را برای ممیزی موثر توجیه می‌کنند؛ تنظیماتی ایجاد شود. عوامل دیگر ممکن توسط عوامل کاهشی حذف شده باشند. در تمامی عوامل که تنظیمات برای زمان ارائه شده ایجاد شده‌اند، جدول تنظیم زمان ممیزی و رکوردها باید برای توجیه کردن تغییرات نگهداری شود.

ب-۳-۵ محدودیت انحراف از زمان ممیزی

به منظور اینکه ممیزی موثری انجام شود و حصول اطمینان از اینکه نتایج قابل اطمینان و قابل مقایسه هستند، زمان ممیزی ارائه شده در نمودار زمان ممیزی نباید بیش از ٪۳۰ کاهش یابد.

دلایل مناسبی برای انحراف باید ایجاد و مستند شود.

ب-۳-۶ زمان ممیزی در-مکان

انتظار می‌رود که زمان محاسبه شده برای طرح‌ریزی و نگارش گزارش، زمان ممیزی کل در-مکان را به کمتر از ٪۷۰ زمان نشان داده شده در نمودار ممیزی کاهش ندهد. که زمان افزون برای طرح‌ریزی و / یا گزارش نویسی لازم است، این امر نباید توجیهی برای کاهش زمان ممیزی در-مکان باشد. زمان سفر ممیز در این محاسبه درنظر گرفته نمی‌شود و به زمان ممیزی ارجاع داده شده در نمودار اضافه می‌شود.

یادآوری- ٪۷۰، عاملی بر مبنای تجربه‌ی ممیزان ISMS است.

ب-۴ زمان ممیزی برای ممیزی مراقبتی

برای چرخه‌ی اولیه‌ی گواهینامه، توصیه می‌شود زمان نظارت برای سازمان متناسب با زمان سپری شده در ممیزی اولیه به همراه مقدار کلی زمان سپری شده به صورت سالیانه در نظارت حدود یک سوم زمان سپری شده در ممیزی اولیه باشد. توصیه می‌شود زمان طرح‌ریزی شده برای نظارت زمان به زمان باشد تا تغییراتی که بر زمان ممیزی موثر است، در نظر گرفته شود. زمان سپری شده برای نظارت ممیزی باید افزایش داده شود تا امکان ممیزی تغییرات را در ISMS بدهد (مانند ممیزی واپایش‌های جدید یا تغییر یافته).

ب-۵ زمان ممیزی برای تمدید گواهینامه

مقدار کلی زمان سپری شده‌ی انجام ممیزی تمدید گواهینامه باید وابسته به نتایج هر ممیزی پیشین به صورت تعریف شده در ۹-۴-۳ و استاندارد ISO/IEC 17021-9.6.3 باشد. توصیه می‌شود مقدار زمان سپری شده ممیزی برای تمدید گواهینامه متناسب با زمانی باشد که در ممیزی اولیه‌ی گواهینامه همان سازمان

است و توصیه می‌شود دست‌کم دو سوم (۲/۳) زمانی باشد که برای ممیزی گواهینامه اولیه همان سازمان در زمانی مورد نیاز است که برای تمدید گواهینامه ممیزی شده است.

ب-۶ زمان ممیزی مکان‌های متعدد

تعداد روزهای ممیزی در هر مکان شامل دفتر مرکزی، باید برای هر مکان محاسبه شده باشد.

برای در نظر گرفتن قسمت‌هایی از ممیزی که متناسب با دفتر مرکزی یا مکان‌های مکانی نیستند، تخفیف-هایی باید اعمال شود. دلایل توجیه این تخفیف‌ها باید توسط نهاد صدور گواهینامه ثبت شود.

پیوست پ

(آگاهی‌دهنده)

روش‌های محاسبه‌ی زمان ممیزی

پ-۱ کلیات

این پیوست راهنماهای بیشتری از استنتاج فرمول برای محاسبه‌ی زمان ممیزی ارائه می‌دهد . پ-۲ مثالی از طبقه بندی عواملی است که می‌تواند به صورت مبنایی برای محاسبه‌ی زمانی ممیزی به‌کار رود و پ-۳ مثالی برای محاسبه‌ی زمان ممیزی است.

پ-۲ طبقه‌بندی عوامل محاسبه‌ی زمان ممیزی

جدول پ-۱ مثالی برای طبقه بندی عوامل اصلی برای محاسبه‌ی زمان ممیزی است، همان‌طور که در ب-۳-۴ قسمت الف- تا ح- فهرست شده است. این طبقه بندی می‌تواند توسط نهادهای صدور گواهینامه برای استنتاج کردن برنامه‌ی محاسبه زمان ممیزی هم‌راستا با ۹-۱-۴-۱ به‌کار رود:

جدول پ-۱- طبقه‌بندی عوامل بر محاسبه‌ی زمان ممیزی

	تاثیر بر تلاش		
	تلاش کاهش یافته	**تلاش عادی**	**تلاش افزایش یافته**
عوامل (به بند ب-۳-۴ مراجعه شود)			
الف- پیچیدگی ISMS - الزامات امنیت اطلاعات [محرمانگی، یکپارچگی و دسترس پذیری (CIA)] - تعداد دارایی‌های حیاتی - تعداد فرایندها و خدمات	-تنها اطلاعات با حساسیت یا محرمانگیِ کم، الزامات کمِ دسترس پذیری -تعدادی از دارایی‌هایی حیاتی (به صورت CIA) -تنها یک فرایند کلیدی کسب‌وکار با واسطهای کم و واحدهای کسب‌وکار درگیر	-الزامات بیشتر دسترس پذیری یا بعضی از اطلاعات حساس/محرمانه -بعضی از دارایی‌های حیاتی -۳-۲ فرایند کسب‌وکار ساده با واسطهای کم یا واحدهای کم درگیر کسب‌وکار	-میزان بیشتر اطلاعات حساس یا محرمانه (به طورمثال، سلامت، اطلاعات قابل شناسایی شخصی، بیمه، بانکداری) یا الزامات دسترس پذیری زیاد. -دارایی‌های حیاتی بسیار -بیش از ۲ فرایند پیچیده با واسطهای بسیار و واحدهای کسب‌وکار درگیر

	تاثیر بر تلاش		
	تلاش کاهش یافته	تلاش عادی	تلاش افزایش یافته
عوامل (به بند ب-۳-۴ مراجعه شود)			
ب- نوع کسب‌وکار انجام شده درون دامنه‌ی کاربرد ISMS	-کسب‌وکار کم مخاطره بدون الزامات نظم دهنده	-الزامات بسیار نظم دهنده	-کسب‌وکار پرمخاطره (تنها) با الزامات نظم دهنده‌ی محدود
پ- عملکرد ISMS که اخیرا نمایش داده شده است.	-اخیرا گواهینامه صادر شده -گواهینامه ندارد اما ISMS به صورت کامل در ممیزی‌های مختلف و چرخه های بهبود شامل ممیزی‌های مستند سازی شده‌ی داخلی، بازنگری مدیریتی و سامانه‌های پیشرفت موثر پیوسته پیاده‌سازی شده است.	-ممیزی اخیر نظارتی -دارای گواهینامه نیست اما اندکی ISMS را پیاده‌سازی کرده است: بعضی از ابزارهای سامانهٔ مدیریت، در دسترس هستند و پیاده‌سازی شده‌اند. بعضی از فرایندهای پیشرفت پیوسته جاری هستند اما تا اندکی مستند شده‌اند.	-اخیرا گواهینامه صادر نشده و ممیزی انجام نشده. -ISMS جدید است و به صورت کامل ایجاد نشده است (به طور مثال، نبود سامانهٔ مدیریت مشخص واپایش سازوکارها و فرایندهای بهبود پیوسته‌ی نابهنگام و اجرای فرایند تک کاره
ت- گسترش و گوناگونی فناوری استفاده شده در پیاده‌سازی مولفه های متنوع ISMS (به طور مثال تعداد بن‌سازه‌های مختلف IT، تعداد شبکه‌های مجزا)	-محیط بسیار استاندارد شده با تنوع کم (تعداد کمی از بن‌سازه‌های IT، کارسازها یا سامانه‌های عامل، پایگاه‌های داده و شبکه‌ها)	-استاندارد شده اما دارای بن-سازه‌های IT، کارسازها، سامانه‌های عامل و پایگاه داده‌ها و شبکه‌های متنوع است.	-دارای تنوع یا پیچیدگی بالای IT است (به طور مثال بسیاری از قسمت‌های متفاوت شبکه، انواع کارسازها یا پایگاه داده، تعداد برنامه‌های کاربردی کلیدی)
ث- گسترش برون‌سپاری و آرایش‌های طرف سوم استفاده شده در دامنه‌ی کاربرد ISMS	-فاقد برون‌سپاری و وابستگی کم در فروشندگان -مدیریت‌های برون‌سپاری به خوبی تعریف شده، مدیریت یا پایش شده -برون‌سپاری دارای ISMS دارای گواهینامه است.	-آرایش‌های برون‌سپاری مختلف که تا حدی مدیریت شده	-وابستگی زیاد به برون‌سپاری یا فروشندگان با تاثیر بالا بر فعالیت‌های کسب‌وکاری مهم -مقدار مجهول یا گسترش برون‌سپاری یا -آرایش‌های مختلف برون‌سپاری مدیریت نشده

	تاثیر بر تلاش		
	تلاش کاهش یافته	تلاش عادی	تلاش افزایش یافته
عوامل (به بند ب-۳-۴ مراجعه شود)			
ج- میزان توسعه‌ی سامانه‌های اطلاعاتی	-فاقد توسعه‌ی سامانهٔ خانگی -استفاده از بن‌سازه‌های نرم‌افزاری استاندارد	-استفاده از بن‌سازه‌های نرم‌افزاری استاندارد یا پیکربندی / پارامتر سازی پیچیده -نرم‌افزار سفارشی شده -بعضی فعالیت‌های توسعه‌ای (خانگی یا برون‌سپاری)	-فعالیت‌های توسعه‌ای گسترش داخلی نرم‌افزار یا پروژه‌های در دست اقدام برای اهداف کسب‌وکاری مهم
چ- تعداد مکان‌ها و تعداد مکان‌های بازیابی فاجعه (DR)	-الزامات کم دسترس پذیری و یک یا هیچ مکان جایگزین DR	-الزامات متوسط تا زیاد دسترس پذیری و یک یا هیچ مکان جایگزین DR	-الزامات دسترس پذیری زیاد (به طور مثال خدمات 24/7) -چندین مکان جایگزین DR -چندین مراکز داده
ح- برای نظارت یا ممیزی تمدید گواهینامه: تعداد و محتوای تغییرات مرتبط با ISMS مطابق با استاندارد ISO/IEC 17021-1,8-5-3	-بدون تغییر تا آخرین ممیزی صدور گواهی	-تغییرات جزئی در دامنه‌ی کاربرد SoA متعلق به ISMS، به طور مثال، بعضی خط‌مشی‌ها، مستندات و... -تغییرات جزئی در عوامل بالا	-تغییرات عمده در دامنه‌ی کاربرد یا SoA متعلق به ISMS، به طور مثال فرایند جدید، واحدهای کسب‌وکار جدید، حوزه‌ها، ارزیابی مخاطره، روشگان مدیریت، خط‌مشی‌ها، مستندات، کاهش مخاطره -تغییرات عمده در عوامل بالا

پ-۳ مثالی برای محاسبه‌ی زمان ممیزی

مثال زیر چگونگی استفاده از عوامل ارائه شده در ب-۳ را برای محاسبه‌ی زمان ممیزی توسط نهاد صدور گواهینامه نشان می‌دهد. محاسبه‌ی زمان ممیزی در مثال زیر به صورت زیر است:

مرحله ۱: تعیین عوامل مرتبط با کسب‌وکار و سازمان (به غیر از IT): شناسایی رتبه‌ی مناسب برای هر دسته‌ی داده شده در جدول پ-۲ و جمع کردن نتایج.

مرحله ۲: تعیین عواملی مرتبط با محیط IT : شناسایی کردن رتبه‌های مناسب برای هر دسته‌ی داده شده در جدول پ-۳ و جمع نتایج.

مرحله ۳: برمبنای نتایج مرحله ۱ و۲، شناسایی تاثیر عوامل بر زمان ممیزی توسط انتخاب کردن ورودی مناسب در جدول پ-۴.

مرحله ۴: محاسبه‌ی نهایی: تعداد روزهای تعیین شده توسط به کار بردن نمودار زمان ممیزی (جدول ب-۱) در عامل حاصل از مرحله سه ضرب می‌شود. هنگامی‌که نمونه برداری چند مکان به‌کار رفته است، روزهای ممیزی محاسبه شده بر مبنای تلاش‌های مورد نیاز برای انجام طرح نمونه برداری چند مکان افزایش می‌یابند.

جواب حاصل، تعداد نهایی روزهای ممیزی است.

جدول پ-۲- عوامل مرتبط با کسب‌وکار و سازمان (به غیر از IT)

طبقه	رتبه
انواع کسب‌وکار و الزامات نظم دهنده	۱. سازمان در بخش‌های حیاتی کسب‌وکار و بخش‌های تعدیل نشده کار می‌کند.[a] ۲. سازمان دارای مشتری در بخش‌های حیاتی کسب‌وکار است.[a] ۳. سازمان در بخش‌های حیاتی کسب‌وکار، کار می‌کند.[a]
فرایند و وظایف	۱. فرایندهای استاندارد با وظایف استاندارد و تکراری، بسیاری از افرادی که تحت واپایش سازمان کار می‌کنند مسئولیتی یکسان را انجام می‌دهند، تعداد محصولات و خدمات کم است. ۲. فرایندهای استاندارد اما غیرتکراری با تعداد زیادی محصول یا خدمات ۳. فرایندهای پیچیده؛ تعداد زیاد محصولات و خدمات، بسیاری از واحدهای کسب‌وکار در دامنه‌ی کاربرد گواهینامه جای می‌گیرند(ISMS فرایندهای بسیار پیچیده یا تعداد نسبتا زیادی از فعالیت‌های یا فعالیت‌های منحصربه‌فرد را پوشش می‌دهد)
سطح انتشار MS	۱. ISMS تقریبا به خوبی منتشر شده و / یا دیگر سامانه‌های مدیریت جاری هستند. ۲. بعضی از عناصر دیگر سامانهٔ مدیریت پیاده‌سازی شده و بعضی پیاده-سازی نشده‌اند. ۳. هیچ سامانهٔ مدیریت دیگر پیاده‌سازی نشده است، ISMS جدید است و پایه گذاری نشده است.
[a] قسمت‌های حیاتی کسب‌وکار قسمت‌هایی هستند که ممکن است بر خدمات حیاتی کسب‌وکار را تاثیر بگذارند که این امر منجر به مخاطره‌ی زیاد برای سلامت، امنیت، اقتصاد، توانایی تصویر کردن و دولت می‌شود که ممکن است دارای تاثیر بسیار منفی بر کشور شود.	

جدول پ-۳- عوامل مرتبط با محیط IT

طبقه	رتبه
پیچیدگی زیرساخت IT	۱- بن‌سازه‌های IT، کارسازها، سامانه‌های عامل، پایگاه داده یا شبکه‌های کم یا بسیار استاندارد شده. ۲- بن‌سازه‌های IT، کارسازها، سامانه‌های عامل، پایگاه داده، شبکه‌های مختلف ۳- بن‌سازه‌های IT، کارسازها، سامانه‌های عامل، پایگاه داده‌ها و شبکه‌های بسیار مختلف
وابستگی برون‌سپاری و فروشندگان شامل خدمات ابر	۱- وابستگی کم یا فاقد وابستگی در برون‌سپاری یا فروشندگان ۲- وابستگی در برون‌سپاری یا فروشندگان مرتبط با بعضی از فعالیت‌های کسب‌وکار مهم ۳- وابستگی بالا در برون‌سپاری یا فروشندگان، تاثیر بالا بر فعالیت‌های کسب‌وکاری مهم
توسعه‌ی سامانهٔ اطلاعات	۱- نبود سامانه یا سامانهٔ خیلی محدود خانگی/ توسعه‌ی برنامه‌ی کاربردی ۲- سامانه یا برون‌سپاری خانگی/ توسعه‌ی برنامه‌ی کاربردی برای اهداف کسب‌وکاری مهم ۳- سامانه‌های یا برون‌سپاری خانگی/ توسعه‌ی برنامه‌ی کاربردی برای اهداف کسب‌وکاری مهم

جدول پ-۴- تاثیر عوامل بر زمان ممیزی

		پیچیدگی IT		
		کم (از ۳ تا۴)	متوسط (از ۵ تا۶)	زیاد (از ۷ تا۹)
پیچیدگی کسب‌وکار	زیاد (از ۷ تا۹)	٪ ۵+ تا ٪ ۲۰+	٪ ۱۰+ تا ٪ ۵۰+	٪ ۲۰+ تا ٪ ۱۰۰+
	متوسط (از ۵ تا۶)	٪ ۵- تا ٪ ۱۰-	٪ ۰	٪ ۱۰+ تا ٪ ۵۰+
	کم (از ۳ تا۴)	٪ ۱۰- تا ٪ ۳۰-	٪ ۵- تا ٪ ۱۰-	٪ ۵+ تا ٪ ۲۰+

مثال ۱: سازمانی که باید ممیزی شود دارای ۷۰۰ کارمند است، بدین گونه مطابق با جدول ب-۱ برای ممیزی اولیه نیاز به ۱۷/۵روز است. سازمان در بخش حیاتی کسب‌وکار نیست و دارای وظایف با استاندارد بالا و وظایف تکراری است و تازه ISMS را پایه گذاری کرده است. مطابق با جدول پ-۲ این امر منجر به عامل مرتبط با کسب‌وکار و سازمان ۵ = ۳+۱+۱ می‌شود . این سازمان دارای بن‌سازه‌های IT و پایگاه داده‌های خیلی کم است و از برون‌سپاری گسترده استفاده می‌کند. هیچ توسعه‌ای درون سازمان یا برون‌سپاری وجود ندارد. مطابق با جدول پ-۳ این امر منجر به عامل مرتبط با محیط IT ۵=۳+۱+۱ می‌شود. با استفاده از جدول پ-۴ این امر منجر به هیچ تنظیمی برای زمان ممیزی نمی‌شود.

مثال ۲: همان سازمان مثال قبل را در نظر بگیرید، تنها سامانه‌های مدیریت متعددی جاری وجود دارند و در حال حاضر ISMS به خوبی پایه گذاری شده است. این امر محاسبات را مطابق با جدول پ-۲ به ۳=۱+۱+۱ تغییر می‌دهد. مطابق با جدول پ-۴ این امر منجر به کاهش ٪۵ تا ٪۱۰ زمان ممیزی می‌شود، یعنی زمان ممیزی از ۱ تا ۱/۵ روز کاهش می‌یابد و منجر به زمان کل ۱۶ الی ۱۶/۵ روز می‌شود.

پیوست ت

(آگاهی‌دهنده)

راهنمای بازنگری پیاده‌سازی واپایش‌های پیوست الف از استاندارد ISO/IEC 27001

ت-۱ هدف

پیاده‌سازی واپایش‌هایی که به صورت ضروری توسط مشتری برای ISMS تعیین شده بودند باید در مدت مرحله‌ی ۲ ممیزی اولیه و در مدت فعالیت‌های مراقبتی و تمدید گواهینامه بازنگری شود (۹-۳-۱-۲-۲ چ مشاهده شود).

درک ممیزی که نهاد صدور گواهینامه جمع آوری کرده است باید برای ترسیم نمودن نتیجه گیری برای بررسی موثر بودن واپایش‌ها کافی باشد. به طور مثال اینکه انتظار می‌رود واپایش‌ها چگونه انجام شوند در رویه یا خط‌مشی‌های مشتری مشخص می‌شود.

ت-۱-۱ شواهد ممیزی

بهترین کیفیت شواهد ممیزی از مشاهدات ممیز جمع آوری شده است (به طور مثال اینکه در قفل شده قفل است، افراد موافقت‌نامه‌های محرمانگی را امضا می‌کنند، ثبت دارایی موجود است و شامل دارایی مشاهده شده است، تنظیمات سامانه کافی است و...). شواهد می‌تواند از بررسی نتایج عملکرد واپایشی جمع آوری شده باشد (به طور مثال، چاپ کردن حقوق دسترسی داده شده به مردم که توسط دفتر اصالت‌سنجی امضا شده، سوابقِ حل‌وفصلِ رخداد، فرایند اصالت‌سنجی که توسط دفاتر صحیح اصالت‌سنجی امضا شده‌اند، دقایق ملاقات مدیریت). شواهد می‌تواند نتیجه‌ی آزمون مستقیم (عملکرد مجدد) واپایش ممیزان باشد، به طور مثال تلاش برای انجام وظایفی که باید توسط واپایش‌ها تحریم شود، تعیین اینکه چه نرم‌افزاری باید برای حفاظت در برابر کدهای مخرب نصب و به روز شود، حقوق دسترسی واگذار شده (بعد از بررسی کردن اصالت‌سنجی‌ها) و ... . شواهد می‌تواند توسط مصاحبه با افرادی جمع آوری شود که تحت واپایش سازمان و پیمانکارهای پردازنده و واپایش و تعیین صحت عمل کار می‌کنند.

ت-۲ چگونگی استفاده از جدول ت-۱

ت-۲-۱ کلیات

جدول ت-۱ راهنمایی برای بازنگری کردن پیاده‌سازی واپایش‌های فهرست شده در پیوست الف استاندارد ISO/IEC 27001:2013 و جمع آوری شواهد ممیزی به صورتی که عملکرد آن‌ها در مدت ممیزی اولیه و ممیزی‌های بعد فهرست شده است، ارائه می‌کند. در این جدول مقصود ارائه دادن راهنما برای بازنگری واپایش‌هایی به غیر از پیوست الف در استاندارد ISO/IEC 27001:2013 نیست.

ت-۲-۲ ستون‌های «واپایش سازمانی» و «واپایش فنی»

علامت «X» در ستون نشان دهنده‌ی این است که آیا واپایش سازمانی است یا فنی. از آنجا که بعضی از واپایش‌های هم به صورت سازمانی و هم به صورت فنی هستند، این علامت می‌تواند در هر دو ستون واپایش-ها باشد.

شواهد برای پیاده‌سازی واپایش‌های سازمان می‌تواند از بازنگری کردن ثبت‌های عملکرد واپایش‌ها، مصاحبه[1]ها، مشاهدات و نظارت فیزیکی جمع آوری شده باشد. شواهد اجرا واپایش‌های فنی می‌تواند اغلب از سامانهٔ آزمون و در طول استفاده از ممیزی مشخص/ ابزار گزارش جمع آوری شده باشد.

ت-۲-۳ ستون «آزمون سامانه»

آزمون سامانه به معنای بازنگری مستقیم سامانهٔ اطلاعاتی _ به طور مثال، بازنگری تنظیمات یا پیکربندی سامانه – است. سوال‌های ممیزی می‌توانند در میز فرمان سامانه و توسط ارزیابی کردن نتایج ابزارهای آزمون پاسخ داده شوند. اگر مشتری دارای ابزار رایانه‌ای باشد و این ابزار برای ممیز قابل قبول باشند، این ابزار می‌توانند برای پشتیبانی از ممیزی استفاده شوند یا نتایج ارزیابی انجام شده توسط مشتری (یا دیگر پیمانکاران جزء) بازنگری شود.

این جدول شامل دو طبقه برای بازنگری کردن واپایش‌های فنی است :

«ممکن»: آزمون سامانه برای ارزیابی کردن پیاده‌سازی واپایش اما ممکن است در ممیزی ISMS ضروری نباشد.

«توصیه شده»: آزمون سامانه معمولا در ممیزی ISMS ضروری است.

یادآوری- درون این پیوست «سامانه» به «سامانهٔ اطلاعاتی» اطلاق می‌شود مگر غیر آن ذکر شده باشد.

ت-۲-۴ ستون «بازرسی چشمی[2]»

بازرسی چشمی به این معنا است که این واپایش‌ها معمولا نیازمند بازنگری چشمی در موقعیت ارزیابی اثربخشی‌شان هستند. به این معنا که بازنگری کردن مستندات نمایشگر در کاغذ یا در مصاحبه کافی نیست. توصیه می‌شود ممیز واپایش را در موقعیتی که پیاده‌سازی شده است، بررسی نماید.

ت-۲-۵ ستون «راهنمای بازنگری ممیزی»

ستون راهنمای بازنگری ممیزی، حوزه‌های تمرکز ممکن را برای ارزیابی کردن واپایش‌ها و همچنین راهنمای بیشتری برای ممیزی فراهم می‌کند.

1 - Interview
2 - Visual inspection

جدول ت-۱- طبقه بندی واپایش‌ها

واپایش‌ها در پیوست الف از استاندارد ملی ایران به شماره ایزو-آی ای سی ۲۷۰۰۱: سال ۱۳۹۴	واپایش سازمان	واپایش فنی	آزمون سامانه	بازرسی چشمی	راهنمای بازنگری ممیزی
الف-۵- خط‌مشی‌های امنیت اطلاعات					
الف-۵-۱- جهت گیری مدیریت برای امنیت اطلاعات					
الف-۵-۱-۱- خط‌مشی‌های امنیت اطلاعات	X				
الف-۵-۱-۲- بازنگری خط-مشی‌های امنیت اطلاعات	X				
الف-۶- سازمان امنیت اطلاعات					
الف-۶-۱- سازمان داخلی					
الف-۶-۱-۱- نقش‌ها و مسئولیت‌های امنیت اطلاعات	X				
الف-۶-۱-۲- تفکیک وظایف	X				
الف-۶-۱-۳- برقراری ارتباط با مراجع دارای اختیار	X				
الف-۶-۱-۴- برقراری ارتباط با گروه‌های دارای علاقه‌مندی‌های خاص	X				
الف-۶-۱-۵ امنیت اطلاعات در مدیریت پروژه	X				
الف-۶-۲-افزاره‌های سیار و دورکاری					
الف-۶-۲ -۱ خط‌مشی افزاره سیار	X	X	ممکن		پیاده‌سازی خط‌مشی را در جای مناسب بررسی کنید.
الف-۶-۲-۲- دورکاری	X	X	ممکن		پیاده‌سازی خط‌مشی را در جای مناسب بازبینی کنید.
الف-۷-امنیت منابع انسانی					
الف-۷-۱- پیش از اشتغال					
الف-۷-۱-۱- گزینش	X				

واپایش‌ها در پیوست الف از استاندارد ملی ایران به شماره ایزو-آی ای سی ۲۷۰۰۱: سال ۱۳۹۴	واپایش سازمان	واپایش فنی	آزمون سامانه	بازرسی چشمی	راهنمای بازنگری ممیزی
الف-۷-۱-۲- ضوابط و شرایط اشتغال	X				
الف-۷-۲-در حین خدمت					
الف-۷-۲-۱- مسئولیت‌های مدیریت	X				
الف-۷-۲-۲- آگاه‌سازی، تحصیل و آموزش امنیت اطلاعات	X				از آن‌ها در مورد مسائلی که باید از آن آگاه باشند، سوال شود.
الف-۷-۲-۳- فرایند انضباطی	X				
الف-۷-۳- خاتمه و تغییر اشتغال					
الف-۷-۳-۱- مسئولیت‌های خاتمه یا تغییر اشتغال	X				
الف-۸- مدیریت دارایی					
الف-۸-۱- مسئولیت دارایی‌ها	X				شناسایی دارایی
الف-۸-۱-۲- مالکیت دارایی‌ها	X				شناسایی دارایی‌ها
الف-۸-۱-۳- استفاده‌ی قابل قبول از دارایی‌ها	X				
الف-۸-۱-۴- بازگرداندن دارایی‌ها	X				
الف-۸-۲- طبقه بندی اطلاعات					
الف-۸-۲-۱- طبقه‌بندی اطلاعات	X				همچنین پیاده‌سازی خطمشی را در جای مناسب بازبینی کنید.
الف-۸-۲-۲-علامت‌گذاری اطلاعات	X				نام‌گذاری: دایرکتوری‌ها، پرونده‌ها، گزارش‌های چاپ شده، رسانه‌های ضبط شده
الف-۸-۲-۳- اداره‌کردن دارایی‌ها	X				
الف-۸-۳- اداره‌کردن رسانه‌های ذخیره‌سازی					
الف-۸-۳-۱- مدیریت رسانه‌های	X	X	ممکن		

واپایش‌ها در پیوست الف از استاندارد ملی ایران به شماره ایزو-آی ای سی ۲۷۰۰۱: سال ۱۳۹۴	واپایش سازمان	واپایش فنی	آزمون سامانه	بازرسی چشمی	راهنمای بازنگری ممیزی
ذخیره‌سازی قابل جابه‌جایی					
الف-۸-۳-۲- امحای رسانه‌های ذخیره‌سازی	X			X	فرایند برای مصرف کردن
الف-۸-۳-۳- انتقال رسانه‌های ذخیره‌سازی فیزیکی	X				محافظت فیزیکی
الف-۹- واپایش دسترسی					
الف-۹-۱- الزامات کسب‌وکار واپایش دسترسی					
الف-۹-۱-۱- خط‌مشی واپایش دسترسی	X				همچنین پیاده‌سازی خط‌مشی را در جای مناسب بازبینی کنید.
الف-۹-۱-۲- دسترسی به شبکه و خدمات شبکه	X				همچنین پیاده‌سازی خط‌مشی را در جای مناسب بازبینی کنید.
الف-۹-۲- مدیریت دسترسی کاربر					
الف-۹-۲-۱- ثبت و حذف کاربر	X				
الف-۹-۲-۲- تامین دسترسی کاربر	X	X	ممکن		افراد نمونه که تحت واپایش سازمان یا پیمانکاری اصالت‌سنجی سازمان برای تمام حقوق دسترسی سامانه‌ها کار می‌کنند.
الف-۹-۲-۳- مدیریت حقوق ویژه دسترسی	X	X	ممکن		انتقال داخلی کارکنان
الف-۹-۲-۴- مدیریت اطلاعات محرمانه اصالت‌سنجی کاربران	X				
الف-۹-۲-۵- بازنگری حقوق دسترسی کاربر	X				
الف-۹-۲-۶- حذف یا تنظیم حقوق دسترسی	X				

واپایش‌ها در پیوست الف از استاندارد ملی ایران به شماره ایزو-آی ای سی ۲۷۰۰۱: سال ۱۳۹۴	واپایش سازمان	واپایش فنی	آزمون سامانه	بازرسی چشمی	راهنمای بازنگری ممیزی
الف-۹-۳- مسئولیت‌های کاربر					
الف-۹-۳-۱- استفاده از اطلاعات اصالت‌سنجی	X				شناسایی راهنمایی‌ها/ خط‌مشی‌های جاری برای کاربر
الف-۹-۴- واپایش دسترسی به برنامه‌ی کاربردی و سامانه‌ها					
الف-۹-۴-۱- محدودسازی دسترسی به اطلاعات	X	X	توصیه شده		
الف-۹-۴-۲- رویه‌های ورود امن	X	X	توصیه شده		
الف-۹-۴-۳- سامانهٔ مدیریت کلمه‌ی عبور	X	X	توصیه شده		
الف-۹-۴-۴- استفاده از برنامه‌های کمکی ویژه	X	X	توصیه شده		
الف-۹-۴-۵- واپایش دسترسی به کد منبع برنامه	X	X	توصیه شده		
الف-۱۰-رمزنگاری					
الف-۱۰-۱-واپایش‌های رمزنگاری					
الف-۱۰-۱-۱- خط‌مشی استفاده از واپایش‌های رمزنگاری	X				همچنین پیاده‌سازی خط‌مشی را در جای مناسب بازبینی کنید.
الف-۱۰-۱-۲-مدیریت کلید	X	X	توصیه شده		همچنین پیاده‌سازی خط‌مشی را در جای مناسب بازبینی کنید.
الف-۱۱- امنیت فیزیکی و محیطی					
الف-۱۱-۱- نواحی امن					
الف-۱۱-۱-۱- حصار امنیت فیزیکی	X				
الف-۱۱-۱-۲-واپایش‌های ورودی فیزیکی	X	X	ممکن	X	کسب سوابق دسترسی
الف-۱۱-۱-۳- امن‌سازی دفاتر، اتاق‌ها و امکانات	X		X		

واپایش‌ها در پیوست الف از استاندارد ملی ایران به شماره ایزو-آی ای سی ۲۷۰۰۱: سال ۱۳۹۴	واپایش سازمان	واپایش فنی	آزمون سامانه	بازرسی چشمی	راهنمای بازنگری ممیزی
الف-۱۱-۱-۴-محافظت در برابر تهدیدهای بیرونی و محیطی	X			X	
الف-۱۱-۱-۵- کار در ناحیه‌ی امن	X			X	
الف-۱۱-۱-۶-نواحی تحویل و بارگیری	X			X	
الف-۱۱-۲-تجهیزات					
الف-۱۱-۲-۱- استقرار و محافظت تجهیزات	X			X	
الف-۱۱-۲-۲- امکانات پشتیبانی	X	X	ممکن	X	
الف-۱۱-۲-۳- امنیت کابل‌کشی	X			X	
الف-۱۱-۲-۴- نگهداری تجهیزات	X				
الف-۱۱-۲-۵- خروج دارایی	X				ثبت دارایی‌های از مکان
الف-۱۱-۲-۶- امنیت تجهیزات و خارج از ابنیه	X	X	ممکن		رمزنگاری قابل انتقال افزاره
الف-۱۱-۲-۷- امحاء یا استفاده‌ی مجدد از تجهیزات به صورت امن	X	X	ممکن	X	از بین بردن لوح، رمزنگاری لوح
الف-۱۱-۲-۸- تجهیزات بدون مراقبت	X				تصدیق راهنما/ خط‌مشی جاری برای کاربران
الف-۱۱-۲-۹- خط‌مشی میز پاک و صفحه پاک	X			X	همچنین پیاده‌سازی خط‌مشی را در جای مناسب بازبینی می‌کند.
الف-۱۲- امنیت عملیات					
الف-۱۲-۱- مسئولیت‌ها و رویه-های عملیاتی					
الف-۱۲-۱-۱- رویه‌های عملیاتی مستند	X				
الف-۱۲-۱-۲- مدیریت تغییر	X	X	توصیه شده		
الف-۱۲-۱-۳- مدیریت ظرفیت	X	X	ممکن		

واپایش‌ها در پیوست الف از استاندارد ملی ایران به شماره ایزو-آی ای سی ۲۷۰۰۱: سال ۱۳۹۴	واپایش سازمان	واپایش فنی	آزمون سامانه	بازرسی چشمی	راهنمای بازنگری ممیزی
الف-۱۲-۱-۴- جداسازی محیط توسعه، آزمون و عملیاتی	X	X	ممکن		
الف-۱۲-۲-محافظت در برابر بدافزار					
الف-۱۲-۲-۱- واپایش‌هایی در برابر بدافزار	X	X	توصیه شده		پیکربندی و تمامیت همگرایی نرم‌افزار واپایش بدافزار
الف-۱۲-۳- نسخه‌های پشتیبان					
الف-۱۲-۳-۱- ایجاد پشتیبان از اطلاعات	X	X	توصیه شده		بازنگری خط‌مشی، آزمون‌های بازیابی
الف-۱۲-۴- واقعه‌نگاری و پایش					
الف-۱۲-۴-۱- واقعه‌نگاری رویداد ثبت ورود	X	X	ممکن		
الف-۱۲-۴-۲- محافظت از اطلاعات ثبت‌شده وقایع	X	X	ممکن		
الف-۱۲-۴-۳- ثبت وقایع سرپرست و بهره‌بردار سیستم	X	X	ممکن		
الف-۱۲-۴-۴- هم‌زمان‌سازی ساعت‌ها		X	ممکن		
الف-۱۲-۵ واپایش نرم‌افزار عملیاتی					
الف-۱۲-۵-۱- نصب نرم‌افزار بر سامانه‌های عملیاتی	X	X	ممکن		
الف-۱۲-۶- مدیریت آسیب پذیری فنی					
الف-۱۲-۶-۱- مدیریت آسیب پذیری‌های فنی	X	X	توصیه شده		مدیریت به هم پیوستگی بر مبنای مخاطره و سخت شدگی سامانه‌های عملیاتی، پایگاه داده و برنامه‌ی کاربردی
الف-۱۲-۶-۲- محدودسازی در نصب نرم‌افزار	X	X	ممکن		

واپایش‌ها در پیوست الف از استاندارد ملی ایران به شماره ایزو-آی ای سی ۲۷۰۰۱: سال ۱۳۹۴	واپایش سازمان	واپایش فنی	آزمون سامانه	بازرسی چشمی	راهنمای بازنگری ممیزی
الف-۱۲-۷- ملاحظات ممیزی سامانهٔ مدیریت					
الف-۱۲-۷-۱- واپایش‌های ممیزی سامانهٔ اطلاعاتی	X				
الف-۱۳- امنیت ارتباطات					
الف-۱۳-۱- مدیریت امنیت شبکه					
الف-۱۳-۱-۱- واپایش شبکه‌ها	X	X	ممکن		مدیریت شبکه
الف-۱۳-۱-۲- امنیت خدمات شبکه	X	X	توصیه شده		SLA ها، ضابطه‌ی امنیت اطلاعات خدمات شبکه (به طور مثال VPN، مسیریابی شیکه و واپایش‌های اتصال، پیکربندی افزاره‌های شبکه)
الف-۱۳-۱-۳- تفکیک در شبکه‌ها	X	X	ممکن		نمودارهای شبکه، تقسیم (به طور مثال DMZ) و تفکیک شبکه (به طور مثال VLالفN).
الف-۱۳-۲- انتقال اطلاعات					
الف-۱۳-۲-۱- خط‌مشی‌ها و رویه‌های انتقال اطلاعات	X				همچنین پیاده‌سازی خط‌مشی را در جای مناسب بازبینی کنید.
الف-۱۳-۲-۲- توافق‌نامه‌های انتقال اطلاعات	X				
الف-۱۳-۲-۳- پیام الکترونیکی	X	X	ممکن		تصدیق پیام‌های نمونه مطابق با خط‌مشی/رویه
الف-۱۳-۲-۴- توافقنامه‌های محرمانگی یا عدم افشا	X				
الف-۱۴- اکتساب، توسعه و نگهداری سامانه					
الف-۱۴-۱-الزامات امنیتی					

واپایش‌ها در پیوست الف از استاندارد ملی ایران به شماره ایزو-آی ای سی ۲۷۰۰۱: سال ۱۳۹۴	واپایش سازمان	واپایش فنی	آزمون سامانه	بازرسی چشمی	راهنمای بازنگری ممیزی
سامانه‌های اطلاعاتی					
الف-۱۴-۱-۱- تحلیل و تعیین الزامات امنیت اطلاعات	X				
الف-۱۴-۱-۲- امن‌سازی خدمات کاربردی در شبکه‌های همگانی	X	X	توصیه شده		مخاطره براساس طراحی خدمات برنامه کاربردی
الف-۱۴-۱-۳- محافظت از تراکنش‌های خدمات کاربردی	X	X	توصیه شده		محرمانگی، یکپارچگی، عدم انکار[1]
الف-۱۴-۲- امنیت در فرایندهای توسعه و پشتیبانی					
الف-۱۴-۲-۱- خط‌مشی توسعه‌ی امن	X				همچنین پیاده‌سازی خط‌مشی را به صورت مناسب بررسی می‌کند.
الف-۱۴-۲-۲- رویه‌های واپایش تغییر سامانه	X	X	توصیه شده		
الف-۱۴-۲-۳- بازنگری فنی نرم‌افزارهای کاربردی پس از تغییرات بسترهای نرم‌افزاری	X				
الف-۱۴-۲-۴- محدودسازی در اعمال تغییرات در بسته‌های نرم‌افزاری	X				
الف-۱۴-۲-۵- اصول مهندسی نرم‌افزار امن	X				
الف-۱۴-۲-۶- محیط توسعه امن	X	X	ممکن		
الف-۱۴-۲-۷- توسعه‌ی برون‌سپاری شده	X				
الف-۱۴-۲-۸- آزمون امنیت سامانه	X				
الف-۱۴-۲-۹- آزمون پذیرش سامانه	X	X	ممکن		
الف-۱۴-۳- داده آزمون					

1 - Non-repudiation

واپایش‌ها در پیوست الف از استاندارد ملی ایران به شماره ایزو-آی ای سی ۲۷۰۰۱: سال ۱۳۹۴	واپایش سازمان	واپایش فنی	آزمون سامانه	بازرسی چشمی	راهنمای بازنگری ممیزی
الف-۱۴-۳-۱- محافظت از داده‌های آزمایشی	X	X	ممکن	X	
الف-۱۵- روابط تامین‌کنندگان					
الف-۱۵-۱- امنیت اطلاعات در روابط تامین‌کنندگان					
الف-۱۵-۱-۱- خط‌مشی امنیت اطلاعات برای روابط تامین-کنندگان	X				همچنین پیاده‌سازی خط‌مشی را در جای مناسب بازبینی کنید.
الف-۱۵-۱-۲- پرداختن به امنیت درون توافق‌نامه‌ی تامین-کننده	X				آزمودن بعضی از شرایط قرارداد
الف-۱۵-۱-۳- زنجیره تامین فناوری اطلاعات و ارتباطات	X				آزمودن بعضی شرایط قرارداد
الف-۱۵-۲- مدیریت تحویل خدمات تامین‌کننده					
الف-۱۵-۲- ۱- پایش و بازنگری خدمات تامین‌کننده	X				
الف-۱۵-۲-۲- مدیریت تغییرات در خدمات تامین‌کننده	X				
الف-۱۶-مدیریت رخداد امنیت اطلاعات					
الف-۱۶-۱- مدیریت رخدادهای امنیت اطلاعات و بهبودها					
الف-۱۶-۱-۱- مسئولیت‌ها و رویه‌های	X				
الف-۱۶-۱-۲- گزارش‌دهی رویدادهای امنیت اطلاعات	X				
الف-۱۶-۱-۳- گزارش‌دهی ضعف‌های امنیتی	X				
الف-۱۶-۱-۴- ارزیابی و تصمیم برای رویدادهای امنیت اطلاعات	X				
الف-۱۶-۱-۵- پاسخ به رخدادهای امنیت اطلاعات	X				

واپایش‌ها در پیوست الف از استاندارد ملی ایران به شماره ایزو-آی ای سی ۲۷۰۰۱: سال ۱۳۹۴	واپایش سازمان	واپایش فنی	آزمون سامانه	بازرسی چشمی	راهنمای بازنگری ممیزی
الف-۱۶-۱-۶-یادگیری از رخدادهای امنیت اطلاعات	X				
الف-۱۶-۱-۷- گردآوری شواهد	X				
الف-۱۷- جنبه‌های امنیت اطلاعات مدیریت تداوم کسب‌وکار					
الف-۱۷-۱- تداوم امنیت اطلاعات					یادآوری وقایع بازنگری مدیریت
الف-۱۷-۱-۱- طرح‌ریزی تداوم امنیت اطلاعات	X				
الف-۱۷-۱-۲- پیاده‌سازی تداوم امنیت اطلاعات	X				
الف-۱۷-۱-۳- بررسی، بازنگری و ارزشیابی تداوم امنیت اطلاعات	X				
الف-۱۷-۲- اافزونگی‌ها					
الف-۱۷-۲-۱- دسترس‌پذیری امکانات پردازش اطلاعات	X	X	ممکن		
الف-۱۸- انطباق					
الف-۱۸-۱- انطباق با الزامات قانونی و قراردادی					
الف-۱۸-۱-۱- شناسایی الزامات قانونی و قراردادی قابل‌اجرا	X		توصیه شده		
الف-۱۸-۱-۲-حقوق دارایی فکری	X				
الف-۱۸-۱-۳- محافظت سوابق	X	X	توصیه‌شده		
الف-۱۸-۱-۴- حریم خصوصی و محافظت از اطلاعات قابل-شناسایی شخصی	X				همچنین پیاده‌سازی خطمشی را در جای مناسب بازبینی کنید.
الف-۱۸-۱-۵- قواعد واپایش-های رمزنگاری	X				
الف-۱۸-۲- بازنگری‌های امنیت اطلاعات					

واپایش‌ها در پیوست الف از استاندارد ملی ایران به شماره ایزو-آی ای سی ۲۷۰۰۱: سال ۱۳۹۴	واپایش سازمان	واپایش فنی	آزمون سامانه	بازرسی چشمی	راهنمای بازنگری ممیزی
الف-۱۸-۲-۱- بازنگری مستقل امنیت اطلاعات	X				خواندن و گزارش
الف-۱۸-۲-۲-انطباق با خط‌مشی‌ها و استانداردهای امنیتی	X				
الف-۱۸-۲-۳- بررسی انطباق فنی	X	X			

کتاب‌نامه

[۱] استاندارد ملی ایران شمارهٔ ۱۹۰۱۱: سال ۱۳۹۲، رهنمودهایی برای ممیزی سیستم های مدیریت

[۲] استاندارد ملی ایران شمارهٔ ۲۷۰۰۷: سال ۱۳۹۱، فناوری اطلاعات -فنون امنیتی -راهنماهایی برای ممیزی سامانه های مدیریت امنیت اطلاعات

[۳] استاندارد ملی ایران شمارهٔ ۹۰۰۱: سال ۱۳۸۸، سیستم های مدیریت کیفیت –الزامات