استاندارد ایران-ایزو- آی ای سی

۲۷۰۰۶

چاپ اول

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

ISIRI-ISO/IEC
27006
1st. edition

فن‌آوری اطلاعات- فنون امنیتی- الزامات نهادهای ممیزی‌کننده و گواهی‌کننده سیستم‌های مدیریت امنیت اطلاعات

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

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران
تهران - خیابان ولیعصر، ضلع جنوبی میدان ونک، پلاک ۱۲۹۴، صندوق پستی: ۶۱۳۹-۱۴۱۵۵
تلفن: ۵-۸۸۸۷۹۴۶۱
دورنگار: ۸۸۸۸۷۰۸۰ و۸۸۸۸۷۱۰۳
کرج - شهر صنعتی، صندوق پستی ۱۶۳-۳۱۵۸۵
تلفن: ۸- ۲۸۰۶۰۳۱(۰۲۶۱)
دورنگار: ۲۸۰۸۱۱۴ (۰۲۶۱)
پیام نگار: standard@isiri.org.ir
وب‌گاه: www.isiri.org
بخش فروش، تلفن: ۲۸۱۸۹۸۹ (۰۲۶۱)، دورنگار: ۲۸۱۸۷۸۷ (۰۲۶۱)
بها: ۶۰۰۰ ریال

Institute of Standards and Industrial Research of IRAN
Central Office: No.1294 Valiaser Ave. Vanak corner, Tehran, Iran
P. O. Box: 14155-6139, Tehran, Iran
Tel: +98 (21) 88879461-5
Fax: +98 (21) 88887080, 88887103
Headquarters: Standard Square, Karaj, Iran
P.O. Box: 31585-163
Tel: +98 (261) 2806031-8
Fax: +98 (261) 2808114
Email: standard @ isiri.org.ir
Website: www.isiri.org
Sales Dep.: Tel: +98(261) 2818989, Fax.: +98(261) 2818787
Price: 6000 Rls.

به‌نام خدا

آشنایی با مؤسسهٔ استاندارد و تحقیقات صنعتی ایران

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

تدوین استاندارد در حوزه‌های مختلف در کمیسیون های فنی مرکب از کارشناسان مؤسسه* صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود 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، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

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

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

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

---

* موسسهٔ استاندارد و تحقیقات صنعتی ایران

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

کمیسیون فنی تدوین استاندارد

« فن‌آوری اطلاعات- فنون امنیتی- الزامات نهادهای ممیزی‌کننده و گواهی‌کننده سیستم‌های مدیریت امنیت اطلاعات »

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

(فوق لیسانس مهندسی پزشکی)	(سهامی خاص)
طوماریان ، سهیلا (لیسانس مهندسی برق - الکترونیک)	موسسه استاندارد و تحقیقات صنعتی ایران
فاطمی نسب، امیر مسعود (فوق‌لیسانس مهندسی سیستم‌های مخابرات دیجیتال)	شرکت سیستم و خدمات اریکسون (سهامی خاص)
مهدوی اردستانی ، سید علیرضا (فوق لیسانس مدیریت فن‌آوری اطلاعات)	کارشناس آزاد
میرمطهری، نوید (فوق لیسانس مهندسی برق- مخابرات)	اداره مخابرات و ارتباطات رادیویی آستان قدس رضوی

فهرست مندرجات

عنوان	صفحه
آشنایی با مؤسسهٔ استاندارد	ج
کمیسیون فنی تدوین استاندارد	د
پیش گفتار	ح
مقدمه	ط
۱ هدف و دامنه کاربرد	۱
۲ مراجع الزامی	۱
۳ اصطلاحات و تعاریف	۲
۴ اصول	۳
۵ الزامات عمومی	۳
۵-۱ موارد قانونی و قراردادی	۳
۵-۲ مدیریت بی‌طرفی	۳
۵-۳ تعهدات مالی و پرداخت ها	۴
۶ الزامات ساختاری	۴
۶-۱ ساختار سازمانی و مدیریت رده بالا	۴
۶-۲ کمیته ای برای رعایت بی‌طرفی	۴
۷ الزامات منابع	۴
۷-۱ شایستگی مدیران و کارکنان	۴
۷-۲ کارکنانی که در فعالیت‌های صدورگواهی دخیل هستند	۶
۷-۳ استفاده از ممیزان بیرونی مستقل و کارشناسان فنی بیرونی	۸
۷-۴ سوابق کارکنان	۹
۷-۵ برون‌سپاری	۹
۸ الزامات اطلاعات	۹
۸-۱ اطلاعات در دسترس عموم	۹
۸-۲ مدارک صدور گواهی	۹
۸-۳ لیست مشتری‌های دارای گواهی	۱۰
۸-۴ ارجاع به گواهی و استفاده از علامت	۱۰
۸-۵ محرمانگی	۱۰
۸-۶ تبادل اطلاعات بین نهاد گواهی‌کننده و مشتریانش	۱۱
۹ الزامات فرآیندی	۱۱

ادامه فهرست مندرجات

عنوان	صفحه
۹-۱ الزامات عمومی	۱۱
۹-۲ ممیزی اولیه و صدورگواهی	۱۶
۹-۳ فعالیت‌های بازبینی	۲۱
۹-۴ صدورگواهی مجدد	۲۳
۹-۵ ممیزی‌های خاص	۲۳
۹-۶ تعلیق، ابطال یا کوچک کردن دامنه شمول گواهی	۲۴
۹-۷ درخواست‌های رسیدگی مجدد	۲۴
۹-۸ شکایات	۲۴
۹-۹ سوابق متقاضیان و مشتریان	۲۴
۱۰ الزامات سیستم مدیریتی برای نهادهای گواهی‌کننده	۲۴
۱۰-۱ گزینه ها	۲۴
۱۰-۲ گزینه ۱- الزامات سیستم مدیریتی مطابق با ISO 9001	۲۵
۱۰-۳ گزینه ۲- الزامات عمومی سیستم مدیریت	۲۵
پیوست الف (اطلاعاتی) تحلیل پیچیدگی سازمان‌های مشتری و موارد مختص بخش	۲۶
پیوست ب (اطلاعاتی) حوزه‌های نمونه از شایستگی ممیز	۳۰
پیوست پ (اطلاعاتی) زمان ممیزی	۳۲
پیوست ت (اطلاعاتی) راهنمایی برای بازنگری کنترل‌های پیاده‌سازی شده از پیوست الف استاندارد ۲۷۰۰۱	۳۹

پیش گفتار

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

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

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

1- ISO/IEC 27006:2007, 1st Ed.: Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

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

مقدمه

استاندارد ISO/IEC 17021 یک استاندارد بین‌المللی است، که معیارهایی را برای نهادهای ممیزی‌کننده[1] و گواهی‌کننده[2] در زمینه سیستم‌های مدیریت سازمان‌ها[3] تعیین می‌کند. برای آنکه چنین نهادهایی جهت ممیزی[4] و ارائه گواهی سیستم‌های مدیریت امنیت اطلاعات بر اساس استاندارد ملی ایران ایزو-آی ای سی به شماره ۲۷۰۰۱ و مطابق با استاندارد ISO/IEC 17021 تایید صلاحیت شوند، الزامات و راهنمایی تکمیلی علاوه‌بر الزامات ISO/IEC 17021 لازم است. این الزامات در این استاندارد ارائه می‌شوند.

این استاندارد معادل استاندارد بین‌المللی ISO/IEC 27006:2007 می‌باشد، و ساختار، بندها، ارجاعات، مفاهیم و شماره این استاندارد ملی هماهنگ با استاندارد بین‌المللی معادل می‌باشد. این استاندارد ملیِ معادل به صورت زیر شناخته می شود:

استاندارد ملی ایران ایزو-آی ای سی به شماره ۲۷۰۰۶: سال ۱۳۸۷.

متن این استاندارد مطابق با ساختار ISO/IEC 17021 بوده و تنها در مواردی که الزامات و راهنمایی تکمیلی مختص ISMS[5] برای بکارگیری ISO/IEC 17021 جهت صدورگواهی ISMS مطرح است، از حروف "IS" استفاده می‌شود.

به منظور روانی و شیوایی متن، سعی شده است در صورت امکان بجای عبارت "استاندارد ملی ایران ایزو-آی ای سی به شماره ۲۷۰۰۱" از عبارت "استاندارد ۲۷۰۰۱" استفاده شود.

اصطلاح «باید» در این استاندارد نشانگر ضوابط[6] اجباری دو استاندارد ISO/IEC 17021 و استاندارد ۲۷۰۰۱ ۲۷۰۰۱ است. اصطلاح «توصیه می‌شود» برای نشان دادن ضوابطی بکاربرده می‌شود که - اگرچه آنها راهنمایی برای کاربرد الزامات تعبیر می‌شوند،- انتظار می‌رود مورد قبول یک نهاد گواهی‌کننده[7] واقع شوند.

یکی از اهداف این استاندارد، قادر ساختن نهادهای تاییدصلاحیت[8] به همسان‌سازی اثربخش‌تر در بکارگیری استانداردهایشان جهت ارزیابی[9] نهادهای گواهی‌کننده است. در این زمینه هرگونه انحراف از راهنمایی[10] از سوی نهاد گواهی‌کننده به عنوان استثناء تلقی می‌شود. چنین انحرافاتی به‌صورت موردی و تنها در صورتی مجاز هستند، که نهاد گواهی‌کننده به نهاد تاییدصلاحیت اثبات کند که این استثناء به‌روشی تقریبا معادل الزامات مربوط به بندی از استاندارد ISO/IEC 17021 و استاندارد ۲۷۰۰۱ و در نتیجه هدف این استاندارد را برآورده می‌سازد.

یادآوری: در سرتاسر این استاندارد، اصطلاح«سیستم مدیریت» و « سیستم» به جای هم استفاده می‌شوند.

1- Body operating audit
2- Body operating certification
3- Organizations
4- Audit
6- Information Security Management Systems
7- Provisions
8- Certification body
9- Accreditation body
10- Assessment
11- Guidance

تعریف اصطلاح « سیستم مدیریت» در استاندارد ISO 9000:2005 موجود است. سیستم مدیریتی که در این استاندارد استفاده می‌شود نباید با انواع دیگر سیستم‌ها از جمله سیستم‌های فن‌آوری اطلاعات اشتباه گرفته شود.

در استانداردهای موضوع "سیستم‌های مدیریت امنیت اطلاعات"، توصیه می شود که در دو مبحث "سیستم مدیریت" و "فن‌آوری اطلاعات"، الزامات و موضوعات مرتبط با هر کدام بـه دقـت مـورد توجـه قـرار گیـرد.

فن‌آوری اطلاعات- فنون امنیتی[1]- الزامات نهادهای ممیزی‌کننده و گواهی‌کننده سیستم‌های مدیریت امنیت اطلاعات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد مشخص کردن الزامات و فراهم آوردن راهنمایی برای نهادهایی است که خدمات ممیزی و یا صدورگواهی سیستم مدیریت امنیت اطلاعات[2] (ISMS) را تامین می‌کنند. این الزامات افزون بر الزاماتی هستند که در استانداردهای ISO/IEC 17021 و استاندارد ۲۷۰۰۱ ارائه می‌شوند. هدف اصلی این استاندارد پشتیبانی از تاییدصلاحیتِ نهادهایِ گواهی‌کننده‌ای است که گواهی ISMS را تامین می‌کنند.

الزاماتی که در این استاندارد وجود دارند، به عنوان شاخصی برای اثبات شایستگی[3] و قابلیت اعتماد[4] هر نهاد نهاد تامین‌کننده گواهیISMS شناخته می‌شوند و راهنمایی که در این استاندارد وجود دارد، تعابیر تکمیلی از این الزامات برای هر نهاد گواهی‌کنندهISMS می‌باشد.

یادآوری: این استاندارد می‌تواند به عنوان مدرک معیار[5] جهت تاییدصلاحیت، ارزیابی همترازی[6] و یا سایر فرآیندهای ممیزی[7] ممیزی[7] مورد استفاده قرار گیرد.

۲ مراجع الزامی

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

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

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران ایزو- آی ای سی به شماره ۲۷۰۰۱ : سال ۱۳۸۷، فن‌آوری اطلاعات- فنون امنیتی- سیستم‌های مدیریت امنیت اطلاعات - الزامات

2-2 ISO/IEC 17021:2006, Conformity assessment - Requirements for bodies providing audit and certification of management systems.

2-3 ISO/IEC 19011, Guidelines for quality and/or environmental management systems auditing.

1- Security techniques
2- Information security management system
3- Competence
4- Reliability
5- Criteria document
6- Peer Assessment (PA)
7- Audit processes

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف ارائه شده در استانداردهای ISO/IEC 17021 و استاندارد ۲۷۰۰۱، اصطلاحات و تعاریف زیر نیز به کار می‌روند.

۳-۱

گواهینامه[1]

گواهینامه بوسیله یک نهاد گواهی‌کننده، مطابق با شرایط تاییدصلاحیت آن نهاد، صادر شده و حاوی یک نماد[2] یا بیانیه[3] تایید صلاحیت از سوی آن نهاد است.

۳-۲

نهاد گواهی‌کننده

شخص‌سومی[4] که ISMS یک سازمان مشتری را، براساس استانداردهای منتشر شده ISMS و سایر مستندات مستندات تکمیلی الزام شده سیستم، ارزیابی و گواهی می‌کند.

۳-۳

مدرک صدور گواهی[5]

مدرکی که نشان می‌دهد ISMS یک سازمان مشتری، با استانداردهای ISMS و مستندات تکمیلی الزام شده در این سیستم مطابقت دارد.

۳-۴

علامت[6]

علامت ثبت شده قانونی و یا هر نماد محافظت‌شده به‌روش‌دیگر که برطبق قوانین نهاد تاییدصلاحیت یا نهاد گواهی‌کننده صادر شده و اثبات‌کننده احراز اطمینان کافی از سیستم‌های اجرا شده توسط یک نهاد بوده و یا اینکه اجزاء[7] و یا محصولات[8] با الزامات یک استاندارد خاص مطابقت دارند.

1- Certificate
2- Symbol
3- Statement
4- Third party
5- Certification document
6- Mark
7- Individuals
8- Products

۵-۳

سازمان

شرکت، شرکت سهامی، دفتر، بنگاه تجاری، موسسه یا مرجع دارای اختیار[1]، یا قسمت یا تلفیقی[2] از قسمتهای متعلق به آن، به صورت ثبت شده و یا ثبت نشده، خصوصی و یا دولتی که دارای ساختار اداری و عملکرد مستقلی بوده و توانایی احراز نهادینه‌سازی امنیت اطلاعات را در سازمان خود دارد.

۴ اصول

اصول بند ۴ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۵ الزامات عمومی

۵-۱ موارد قانونی و قراردادی

الزامات بند ۵-۱ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۵-۲ مدیریت بی‌طرفی

الزامات بند ۵-۲ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۵-۲-۱ موارد تضاد منافع در IS 5.2

نهادهای گواهی‌کننده می‌توانند فعالیت‌های زیر را انجام دهند؛ بدون آنکه به عنوان مشاور شناخته شوند و یا موردی متضاد با منافع داشته باشند.

الف- صدورگواهی، شامل جلسات توجیهی[3]، جلسات طرح‌ریزی[4]، بررسی مدارک[5]، ممیزی(البته نه ممیزی داخلی ISMS یا بازنگری‌های امنیتی داخلی) جهت یافتن و پیگیری عدم‌انطباقات.

ب- برگزاری و شرکت در دوره‌های آموزشی مرتبط با مدیریت امنیت اطلاعات، سیستم‌های مدیریتی و یا ممیزی به عنوان مدرس[6]؛ توصیه می‌شود، نهادهای گواهی‌کننده خود را محدود به تهیه اطلاعات عام و توصیه‌هایی نمایند که آزادانه قابل دسترس عموم هستند. به‌عبارت‌دیگر توصیه نمی‌شود، آنها مختص یک شرکت توصیه‌ای[7] ارائه دهند، که این موضوع تخطی از الزامات بند پ تلقی شود.

پ- در اختیار گذاشتن یا انتشار اطلاعات درخواستی که در برگیرنده تعبیر و تفسیر نهاد گواهی‌کننده از الزامات استانداردهای ممیزی‌صدورگواهی[8] باشد.

1- Authority
2- Combination
3- Information meetings
4- Planning meetings
5- Examination of documents
6- Lecturer
7- Advice
8- Certification audit

ت- فعالیت‌های پیش از ممیزی، تنها با هدف سنجش آمادگی برای ممیزی‌صدورگواهی. با این وجود توصیه می‌شود، چنین فعالیت‌هایی منجر به تهیه پیشنهادات یا توصیه‌هایی نشوند که این بند را نقض می‌کند و توصیه‌می‌شود، نهاد گواهی‌کننده بتواند این مطلب را تایید کند که چنین فعالیت‌هایی نقض این الزامات نبوده و به عنوان توجیهی جهت چشم‌پوشی از رخدادهای حین ممیزی‌صدورگواهی بکار نرفته است.

ث- اجرای ممیزی شخص‌دوم و شخص‌سوم مطابق با استانداردها یا مقررات؛ به‌غیر از آنهایی که قسمتی از دامنه‌شمول تاییدصلاحیت هستند.

ج- ایجاد ارزش افزوده در کار در حین ممیزی‌صدورگواهی و بازدیدهای نظارتی[1]، برای‌مثال با شناسایی فرصت‌های بهبود، در زمانی‌که در حین ممیزی، جزء شواهد ممیزی می‌شوند، بدون پیشنهاد راه‌حل مشخص.

نهاد گواهی‌کننده باید از نهاد یا نهادهایی(شامل افراد نیز می‌شود) که فعالیت ممیزی داخلیِ ISMS سازمان مشتری -که موضوع گواهی است- را بر عهده دارند، مستقل باشد.

۵-۳ تعهدات مالی و پرداختها

الزامات بند ۵-۳ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۶ الزامات ساختاری

۶-۱ ساختار سازمانی و مدیریت رده بالا

الزامات بند ۶-۱ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۶-۲ کمیته ای برای رعایت طرفی

الزامات بند ۶-۲ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۷ الزامات منابع

۷-۱ شایستگی مدیران و کارکنان

الزامات بند ۷-۱ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

1- Surveillance visits

واژه "Surveillance" در معانی بازبینی، نطارتی و مراقبتی مورد استفاده قرار می‌گیرد.

۷-۱-۱ شایستگی مدیریت در IS 7.1

مولفه‌های اصلی شایستگی که برای صدورگواهی ISMS الزامی هستند، عبارتند از: انتخاب، تامین و مدیریت نیروهایی که مهارت‌ها و شایستگی آنها متناسب با فعالیت‌های مورد ممیزی و نیز سایر موارد مرتبط با امنیت اطلاعات می‌باشد.

۷-۱-۱-۱ تحلیل شایستگی و بازنگری قرارداد

نهاد گواهی‌کننده باید اطمینان حاصل‌نماید که دانش بهبود[1] در حوزه فن‌آوری و قانونی مرتبطبه ISMS سازمان‌مشتری، که مورد ارزیابی قرار می‌دهد، را دارا است.

نهاد گواهی‌کننده باید از سیستمی اثربخش[2] جهت تحلیل شایستگی‌هایی که در مدیریت امنیت اطلاعات به آنها نیاز دارد و در تمامی زمینه های فنی که در آنها فعالیت دارد، برخوردار باشد.

به ازای هر مشتری، نهاد گواهی‌کننده باید بتواند اثبات کند که تحلیلی از شایستگی‌ها (ارزیابی[3] مهارت‌ها در پاسخ به نیازهای ارزشیابی شده) در زمینه تمامی الزامات مرتبط با هر بخش، پیش از بازنگری قرارداد را انجام داده‌است. نهاد گواهی‌کننده سپس باید قرارداد را با سازمان مشتری خود، براساس نتایج این تحلیل شایستگی، بازنگری نماید. به‌صورت مشخص، نهاد گواهی‌کننده باید بتواند ثابت نماید، شایستگی انجام فعالیت‌های زیر را دارد:

الف- درک حوزه‌های فعالیت سازمان مشتری و ریسک‌های مرتبط با کسب‌وکار[4] آن.

ب- تعریف شایستگی‌های مورد نیاز در نهاد گواهی‌کننده، برای گواهی‌کردن[5] فعالیت‌های شناسایی‌شده و امنیت اطلاعات مرتبط با تهدیدات دارایی‌ها، آسیب‌پذیری‌ها و پیامدهای آن بر روی سازمان مشتری.

پ- تایید در دسترس بودن شایستگی‌های مورد نیاز.

۷-۱-۱-۲ منابع

مدیریت نهاد گواهی‌کننده باید منابع و فرآیندهای لازم برای تعیین شایسته بودن تک‌تک ممیزان در مورد فعالیت‌هایی که نیازاست در دامنه‌شمول گواهی انجام‌شود را داشته‌باشد. شایستگی ممیزان، ممکن است از طریق سابقه کاری تصدیق‌شده[6] و آموزش خاص یا جلسات توجیهی (به پیوست ب رجوع شود) اثبات شود. نهاد گواهی‌کننده باید بتواند به طور اثربخش با مشتری‌هایی که به آنها خدمت ارائه می‌کند ارتباط برقرار نماید.

1- Development
2- Effective
3- Assessment
4- Business
5- Certify
6- Verified

۷-۲ کارکنانی که در فعالیت‌های صدورگواهی دخیل هستند

الزامات بند ۷-۲ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۷-۲-۱ شایستگی کارکنان نهاد گواهی‌کننده در IS 7.2

نهادهای گواهی‌کننده باید کارکنانی را در اختیار داشته باشند، که شایستگی انجام فعالیت‌های زیر را داشته باشند:

الف- انتخاب و تصدیق[1] شایستگی ممیزان ISMS برای تیم‌های ممیزی و مناسب بودن آنها برای انجام فعالیت ممیزی.

ب- توجیه ممیزان ISMS و تدارک آموزشهای لازم برای آنها.

پ- تصمیم‌گیری در مورد اعطا[2]، حفظ‌ونگهداری[3]، ابطال[4]، تعلیق[5]، افزایش یا کاهش مدت اعتبار گواهی‌ها

ت- تنظیم و اجرای فرآیند درخواست‌های رسیدگی‌مجدد[6] و شکایات.

۷-۲-۱-۱ آموزش تیم‌های ممیزی

نهاد گواهی‌کننده باید معیارهایی را برای آموزش تیم‌های ممیزی داشته باشد، تا به این روش بتواند از موارد زیر اطمینان حاصل نماید:

الف- دانش استاندارد ISMS و سایر مدارک الزامی مرتبط.

ب- درک صحیح از امنیت اطلاعات.

پ- درک صحیح از ارزیابی‌ریسک و مدیریت ریسک از دیدگاه کسب‌وکار.

ت- دانش فنی از فعالیت مورد ممیزی.

ث- دانش کلی از الزاماتِ مقرراتیِ مرتبط با ISMS .

ج- دانش سیستم‌های مدیریتی.

چ- درک صحیح از اصول ممیزی براساس استاندارد ISO 19011 .

ح- دانش بازنگری اثربخشی[7] ISMS و اندازه‌گیری میزان اثربخشی کنترل.

این الزامات آموزشی تمامی اعضای تیم ممیزی را شامل می‌شود، به‌غیر از بند «ت»، که می‌تواند بین اعضای تیم تقسیم شود.

1- Verify
2- Granting
3- Maintaining
4- Withdrawing
5- Suspending
6- Appeals
7- Effectiveness

۷-۲-۱-۱-۱ در زمان انتخاب تیم ممیزی به‌منظور انجام ممیزی‌صدورگواهی خاص، نهاد گواهی‌کننده باید اطمینان حاصل نماید که مهارت‌های لازم برای هر کار به درستی بکار گرفته شده‌اند. تیم باید:

الف- دانش فنی مناسب از فعالیت‌های خاص در دامنه‌شمول ISMSای که صدورگواهی برای آن انجام می‌شود، داشته باشد. این دانش، در موارد مرتبط، روش‌های اجرایی[1] مرتبط و ریسک‌های امنیت اطلاعات بالقوه آنها را شامل می‌شود (کارشناسان فنی[2] که ممیز نیستند، می‌توانند این کار را انجام دهند).

ب- درک مناسبی از سازمان مشتری داشته باشد، تا یک ممیزی قابل اعتماد برای صدورگواهی ISMS در زمینه مدیریت کردن[3] امنیت اطلاعات برای فعالیت‌ها، محصولات و خدمات را انجام دهد.

پ- درک مناسبی از الزامات قانونی که در مورد ISMS سازمان مشتری کاربرد پیدا می‌کند، داشته باشد.

۷-۲-۱-۱-۲ در موارد لازم تیم ممیزی می‌تواند، با استفاده از کارشناسان فنی، که شایستگی آنها در زمینه فن‌آوری مورد ممیزی قابل اثبات است، تکمیل شود. این نکته باید در نظر گرفته شود که نمی‌توان از کارشناسان فنی بجای ممیزان ISMS استفاده کرد. بلکه آنها فقط می‌توانند به ممیزان در زمینه‌های فنی درخصوص سیستم مدیریتِ مورد ممیزی، مشاوره ارائه کنند. نهاد گواهی‌کننده باید روش اجرایی برای موارد زیر داشته باشد:

الف- انتخاب ممیزان و کارشناسان فنی براساس شایستگی، آموزش، اثبات شرایط[4] و تجربه‌شان.

ب- ارزیابی اولیه رفتارِ ممیزان[5] و کارشناسان فنی در یک ممیزی‌صدورگواهی و متعاقب آن پایش عملکرد[6] ممیزان و کارشناسان فنی.

۷-۲-۱-۲ مدیریت فرآیند تصمیم‌گیری

حوزه[7] مدیریت باید از شایستگی و قابلیتهای فنی برای مدیریت فرآیند تصمیم‌گیری، در مورد اعطا، حفظ‌ونگهداری، افزایش مدت اعتبار، کاهش مدت اعتبار، تعلیق و ابطال گواهی ISMS براساس الزامات استاندارد ۲۷۰۰۱، برخوردار باشد.

۷-۲-۱-۳ پیش‌نیازهای تحصیلی، تجربیات کاری، آموزش ممیزی و تجربه ممیزی برای ممیزانی که یک ممیزی ISMS را انجام می‌دهند.

۷-۲-۱-۳-۱معیارهای زیر باید برای هر ممیز تیم ممیزی ISMS لحاظ شود. یک ممیز باید:

الف- تحصیلات دوره متوسطه را گذرانده باشد.

1- Procedures
2- Technical experts
3- Managing
4- Qualification
5- Conduct of auditors
6- Performance
7- Function

ب- دارای حداقل ۴ سال تجربه کاری تمام‌وقت در حوزه فن‌آوری اطلاعات بوده که حداقل دو سال آن مرتبط با امنیت اطلاعات است.

پ- ۵ روز دوره آموزشی را با موفقیت گذرانده باشد که دامنه‌شمول دوره آموزشی باید ممیزی ISMS و مدیریت ممیزی را به‌نحو مناسبی دربرگیرد.

ت- پیش از آنکه مسوولیت‌های ممیزی به وی محول شود، باید در کلیه فرآیندهای ارزیابی امنیت اطلاعات تجربه کسب کرده باشد. توصیه می‌شود این تجربه از طریق شرکت در حداقل چهار ممیزی‌صدورگواهی که دست‌کم ۲۰ روز بوده و شامل بازنگری مدارک، تحلیل ریسک، ارزیابی پیاده‌سازی و گزارش‌دهی ممیزی است، به دست آمده باشد.

ث- تجربیات وی تا حد امکان جدید باشد.

ج- توانایی تصویرسازی کلی از عملیات[1] پیچیده و درک نقش‌ها واحدهای مستقل موجود در سازمان‌های بزرگ‌تر مشتری را داشته باشد.

چ- دانش و توانمندی‌های خود را در زمینه امنیت اطلاعات و ممیزی، از طریق بهبود حرفه‌ای مداوم[2]، روزآمد نماید.

کارشناسان فنی باید مطابق با معیارهای «الف»، «ب»، «ث»، و «ج» انتخاب شوند.

۷-۲-۱-۳-۲ علاوه بر الزامات بند ۷-۲-۱-۳-۱، راهبران تیم‌های ممیزی باید شرایط زیر را برآورده کنند. برآورده شدن این شرایط باید در ممیزی‌ها و مطابق با راهنمایی و تحت نظارت اثبات شود:

الف- دارا بودن دانش و خصوصیات برای مدیریت فرآیند ممیزی‌صدورگواهی.

ب- ممیز بودن در حداقل سه ممیزی کامل ISMS .

پ- اثبات کردن توانمندی[3] برای برقراری ارتباط بصورت اثربخش، به هر دو صورت کتبی و شفاهی.

۷-۳ استفاده از ممیزان بیرونی[4] مستقل و کارشناسان فنی بیرونی

الزامات بند ۷-۳ از استاندارد ۲۷۰۰۱ بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۷-۳-۱ استفاده از ممیزان بیرونی یا کارشناسان فنی بیرونی به‌عنوان قسمتی از تیم ممیزی در IS 7.3

در زمان استفاده از ممیزان بیرونی مستقل یا کارشناسان فنی بیرونی به عنوان قسمتی از تیم ممیزی، نهاد گواهی‌کننده باید اطمینان حاصل نماید که این افراد از شایستگی لازم برخوردار بوده و با ضوابط کاربردی در این استاندارد مطابقت دارند. همچنین به طور مستقیم و یا از طریق کارفرمایشان با طراحی، پیاده‌سازی و یا

1- Operation
2- Continual
3- Capability
4- External

نگهداری از ISMS یا سیستم مدیریت مرتبط با آن به‌گونه‌ای که بی‌طرف بودن ایشان نقض شود، ارتباطی نداشته باشند.

۷-۳-۱-۱ استفاده از کارشناسان فنی

کارشناسان فنی که در زمینه فرآیند و موارد مربوط به امنیت اطلاعات و قوانین تاثیرگذار بر سازمان مشتری از دانشی خاص برخوردارند، ولی همه معیارهای بند ۷-۲ را برآورده نمی‌کنند، می‌توانند قسمتی از تیم ممیزی باشند. کارشناسان فنی باید تحت نظارت یک ممیز فعالیت نمایند.

۷-۴ سوابق[1] کارکنان

الزامات بند ۷-۴ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۷-۵ برون‌سپاری

الزامات بند ۷-۵ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۸ الزامات اطلاعات

۸-۱ اطلاعات در دسترس عموم

الزامات بند ۸-۱ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۸-۱-۱ روش‌های اجرایی برای اعطا، حفظ‌ونگهداری، افزایش مدت اعتبار، کاهش مدت اعتبار، تعلیق و ابطال گواهی ISMS در IS 8.1

نهاد گواهی‌کننده باید سازمان مشتری را ملزم کند تا شواهدی دال بر یک ISMS مستند و پیاده‌سازی‌شده را، مطابق با استاندارد ۲۷۰۰۱ به همراه سایر مدارک لازم برای صدورگواهی، در اختیار وی قرار دهد.
نهاد گواهی‌کننده باید برای موارد زیر روش‌های اجرایی مدونی داشته باشد:
الف- ممیزی‌صدورگواهی اولیه ازISMS سازمان‌مشتری مطابق‌با ضوابط استانداردهای ISO 19011, ISO/IEC 17021 و سایر مدارک مرتبط.
ب- ممیزی‌های بازبینی و ممیزی‌های صدورگواهی‌مجدد ISMS سازمان‌مشتری مطابق با استانداردهای ISO 19011, ISO/IEC 17021 در بازه‌های زمانی مشخص، جهت تداوم انطباق با الزامات مرتبط و همچنین تصدیق و ثبت اینکه سازمان‌مشتری، برمبنای زمان، اقدام‌اصلاحی[2] را درجهت اصلاح تمامی عدم‌انطباق‌هایش انجام می‌دهد.

1- Records
2- Corrective action

۸-۲ مدارک صدور گواهی

الزامات بند ۸-۲ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۸-۲-۱ مدارک صدور گواهی ISMS در IS 8.2

نهاد گواهی‌کننده باید به هر سازمان مشتری خود، که ISMS آن گواهی شده است؛ مدارک صدور گواهی مانند یک نامه و یا یک گواهینامه امضاشده از سوی فردی که چنین مسوولیتی دارد، را ارائه نماید. برای هر سازمان مشتری و هر یک از سیستم‌های اطلاعاتی آن، که بوسیله گواهی پوشش داده می‌شود، این مدارک باید دامنه‌شمول گواهی اعطا شده و استانداردِ "سیستم‌های مدیریت امنیت اطلاعات" -استاندارد ۲۷۰۰۱- که ISMS بر اساس آن گواهی می‌شود را مشخص نماید. به‌علاوه توصیه می‌شود، در گواهینامه به نسخه خاصی از بیانیه کاربردپذیری[1] ارجاع داده شده باشد.

۸-۳ لیست مشتری‌های دارای گواهی

الزامات بند ۸-۳ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۸-۴ ارجاع به گواهی و استفاده از علامت

الزامات بند ۸-۴ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۸-۴-۱ کنترل علامت‌های گواهی در IS 8.4

نهاد گواهی‌کننده باید کنترل‌های مناسبی را بر مالکیت، استفاده و نمایش علامت‌های گواهی ISMS خود اعمال نماید. اگر نهاد گواهی‌کننده مجوز استفاده از علامت را جهت ثبت در گواهی ISMS صادر کرده است؛ توصیه می‌شود، نهاد گواهی‌کننده اطمینان حاصل نماید، سازمان مشتری آن علامت خاص را تنها در مواردی که از سوی نهاد گواهی‌کننده مشخص شده است استفاده کند. نهاد گواهی‌کننده نباید این حق را به سازمان مشتری بدهد که این علامت را روی یک محصول استفاده کند یا به‌گونه‌ای استفاده کند که امکان داشته باشد به‌عنوان دلیل انطباق محصول تفسیر شود.

۸-۵ محرمانگی

الزامات بند ۸-۵ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

1- Statement of applicability

۸-۵-۱ دسترسی به سوابق سازمانی در IS 8.5

پیش از ممیزی‌صدورگواهی، نهاد گواهی‌کننده باید از سازمان مشتری پرسش نماید که آیا سوابقی از ISMS در سازمان وجود دارد، که به‌دلیل حاوی اطلاعات محرمانه یا حساس بودن نمی‌تواند برای بازنگری در اختیار تیم ممیزی قرار گیرد. نهاد گواهی‌کننده باید تعیین نماید، آیا ممیزی ISMS بدون وجود این سوابق، به‌نحومناسب امکان‌پذیر است یا خیر. اگر نهاد گواهی‌کننده به این نتیجه برسد، که امکان ممیزی، به‌نحومناسب، بدون بازنگری سوابق محرمانه یا حساس وجود ندارد، سازمان مشتری باید توجیه شود که ممیزی‌صدورگواهی نمی‌تواند انجام شود؛ تازمانی‌که تمهیدات دسترسی کافی برای نهاد گواهی‌کننده فراهم شود.

۸-۶ تبادل اطلاعات بین نهاد گواهی‌کننده و مشتریانش

الزامات بند ۸-۶ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۹ الزامات فرآیندی

۹-۱ الزامات عمومی

الزامات بند ۹-۱ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۹-۱-۱ الزامات عمومی ممیزی ISMS در IS 9.1

۹-۱-۱-۱ معیارهای ممیزی صدورگواهی

معیارهایی که ISMS یک مشتری بر اساس آن مورد ممیزی قرار می‌گیرد، باید از استاندارد ۲۷۰۰۱ و سایر مدارک مورد نیاز برای صدورگواهی مرتبط با عملکرد آن سازمان، استخراج شده باشد.

اگر نیاز به توضیح درباره کاربرد این مدارک، برای یک برنامه صدورگواهی خاص وجود داشت، چنین توضیحی باید بوسیله افراد یا کمیته‌ای مرتبط و بی‌طرف که از شایستگی فنی لازم برخوردار است، داده شود و از طریق نهاد گواهی‌کننده منتشر شود.

۹-۱-۱-۲ خط‌مشی ها و روش‌های اجرایی

مستندسازی نهاد گواهی‌کننده باید شامل خط‌مشی و روش‌های‌اجرایی برای پیاده‌سازی فرآیند صدورگواهی باشد که شامل بررسی‌های استفاده و کاربرد مدارک بکاررفته در گواهیISMSها و روش‌های اجرایی برای ممیزی و صدورگواهی ISMS در سازمان مشتری می‌شود.

۹-۱-۱-۳ تیم ممیزی

تیم ممیزی باید به طور رسمی منصوب شده و مدارک کاری لازم در اختیار آن قرار گیرد. برنامه و تاریخ ممیزی باید با توافق سازمان مشتری تعیین شود. دستورات ابلاغ شده به تیم ممیزی باید به طور واضح

تعریف و به اطلاع سازمان مشتری برسد. همچنین باید تیم ممیزی ملزم شود ساختار، خط‌مشی‌ها و روش‌های اجرایی سازمان مشتری را بررسی کند و تایید نماید که، این موارد کلیه الزامات مربوط به دامنه‌شمول گواهی را برآورده می‌کنند، و روش‌های اجرایی پیاده‌سازی شده‌اند، و به‌گونه‌ای هستند که بتوان از ISMS سازمان مشتری اطمینان حاصل نمود.

۹-۱- ۲ دامنه‌شمول گواهی در IS 9.1.2

تیم ممیزی باید ISMS سازمان مشتری، مشمول دامنه‌شمول، را از جهت تمامی الزاماتِ قابل اجرا برای صدورگواهی، ممیزی کند. نهاد گواهی‌کننده باید اطمینان حاصل نماید، که دامنه‌شمول و تمامی قیود ISMS سازمان مشتری به طور واضح بر مبنای ویژگیهای[1] کسب‌وکار، سازمان، موقعیت، دارایی‌ها و فن‌آوری آن تعریف شده است. نهاد گواهی‌کننده باید تایید نماید، در دامنه‌شمول ISMS سازمان، الزامات ذکر شده در بند ۱-۲ از استاندارد ۲۷۰۰۱ لحاظ شده‌اند.

نهادهای گواهی‌کننده باید اطمینان یابند، ارزیابی‌ریسک و برطرف‌سازی‌ریسک امنیت‌اطلاعات در سازمان‌مشتری به‌نحومناسبی منعکس‌کننده فعالیت‌های آن سازمان می‌باشد و تا حدود فعالیت‌های آن سازمان وسعت پیدا می‌کند، همانطور که در استاندارد ۲۷۰۰۱ تعریف شده است.

نهادهای گواهی‌کننده باید تایید کنند، این مطلب در دامنه‌شمول ISMS انها و بیانیه کاربردپذیری سازمان مشتری منعکس شده است.

نهادهای گواهی‌کننده باید اطمینان یابند، که فصل‌های مشترک[2] با خدمات یا فعالیت‌ها که به‌طور کامل در دامنه‌شمول ISMS قرارنگرفته‌اند، در داخل ISMSِ موضوعِ‌گواهی قرارگرفته، و در ارزیابی‌ریسک امنیت‌اطلاعات سازمان مشتری قرار داده می‌شوند. مثالی از این حالت، به‌اشتراک‌گذاری تجهیزات (برای‌مثال سیستم‌های IT، سیستم‌های پایگاه داده و ارتباطی) با سازمان‌های دیگر است.

۹-۱- ۳ زمان ممیزی در IS 9.1.3

نهادهای گواهی‌کننده باید زمان کافی را برای انجام تمامی تعهدات ممیزی اولیه، ممیزی بازبینی یا ممیزی صدورگواهی‌مجدد در اختیار ممیزان قرار دهند. توصیه می‌شود، زمان تخصیص داده‌شده براساس فاکتورهای زیر تعیین شود:

الف- ابعاد دامنه‌شمول ISMS (برای‌مثال تعداد سیستم‌های اطلاعاتی استفاده شده و تعداد کارکنان)

ب- پیچیدگی ISMS. (برای‌مثال بحرانی‌بودن سیستم‌های اطلاعاتی و موقعیت ریسک ISMS) همچنین به پیوست الف مراجعه شود.

پ- نوع(انواع) کسب‌وکاری که در دامنه‌شمول ISMS ذکر شده است.

1- Characteristic

2- Interfaces

این واژه به معنی "محیط‌های واسط" نیز بیان می‌شود.

ت- وسعت و گوناگونی فن‌آوری به‌کارگرفته‌شده در پیاده‌سازی اجزای مختلف ISMS (مانند کنترل‌های پیاده‌سازی شده، مستندسازی و/ یا کنترل فرآیند، اقدام اصلاحی/ پیشگیرانه[1] و غیره)

ث- تعداد سایت‌ها.

ج- عملکرد اثبات‌شده قبلی ISMS.

چ- وسعت برون‌سپاری و هماهنگی‌های شخص‌سوم استفاده شده در دامنه‌شمول ISMS.

ح- استانداردها و مقرراتی که جهت صدور گواهی کاربرد دارند.

پیوست پ راهنمایی را برای زمان ممیزی ارائه می‌کند. نهاد گواهی‌کننده باید آماده باشد، تا مدت زمانی که برای هر ممیزی اولیه، ممیزی بازبینی یا ممیزی صدورگواهی‌مجدد استفاده می‌شود را، با دلیل‌ومدرک ثابت کند یا توجیه نماید

۹-۱- ۴ سایت‌های چندگانه در IS 9.1.4

۹-۱-۴-۱

تصمیم‌گیری براساس نمونه‌گیری از چند سایت در حوزه گواهی ISMS پیچیده‌تر از تصمیم‌گیری درباره سیستم‌های مدیریت کیفیت است. جایی‌که سازمان مشتری چندین سایت دارد که معیارهای الف تا پ، که در زیر به آنها اشاره می‌شود، را برآورده می‌کنند، نهادهای گواهی‌کننده مجازند از رویکرد مبتنی بر نمونه‌گیری[2] برای ممیزی‌صدورگواهی چند سایتی استفاده نمایند:

الف- تمامی سایت‌ها تحت یک ISMS، که به طور مرکزی مدیریت و ممیزی شده و تحت بازنگری مدیریتی مرکزی قرار دارند، کار می‌کنند.

ب- تمامی سایت‌ها در برنامه ممیزی داخلی ISMS سازمان مشتری قرار دارند.

پ- تمامی سایت‌ها در برنامه بازنگری مدیریتی ISMS سازمان مشتری قرار دارند.

۹-۱-۴-۲

نهاد گواهی‌کننده، که تصمیم دارد از رویکرد مبتنی بر نمونه‌گیری استفاده نماید، باید روش‌های اجرایی مناسب و به‌جا برای اطمینان از موارد زیر داشته باشد:

الف- بازنگری اولیه قرارداد، تفاوت میان سایت‌ها را تا حد امکان به‌گونه‌ای مشخص‌کرده‌باشد که سطح مناسب نمونه‌گیری را بتوان تعیین نمود.

ب- ازسوی نهادگواهی‌کننده،تعدادی از سایت‌های‌معرف بادرنظرگرفتن مواردزیر به‌عنوان‌نمونه تعیین‌می‌شوند:

۱- نتایج ممیزی داخلی دفتر مرکزی[3] و سایت‌ها.

۲- نتایج بازنگری مدیریتی.

3- Preventive action
1- Sample-based approach
2- Head office

۳- تغییرات در ابعاد سایت‌ها.
۴- تغییرات در اهداف کسب‌وکار سایت‌ها.
۵- پیچیدگی ISMS .
۶- پیچیدگی سیستم‌های اطلاعاتی در سایت‌های مختلف.
۷- تغییرات در رویه‌های کاری.
۸- تغییرات در تعهدات کاری.
۹- تعاملات بالقوه با سیستم‌های اطلاعاتی حیاتی و یا سیستم‌های اطلاعاتی که اطلاعات حساس را پردازش می‌کنند.
۱۰- هر تفاوتی در الزامات قانونی.

پ- سایت نمونه معرف از میان تمامی سایت‌های موجود در دامنه‌شمول ISMS سازمان‌مشتری انتخاب می‌شود. توصیه می‌شود، این انتخاب به‌گونه‌ای حساب شده انجام شود تا در عین دربرداشتن عوامل ذکر شده در ماده ب این بند، مولفه تصادفی بودن را نیز تامین نمایند.

ت- هر سایت که در ISMS قرار دارد و از ریسک‌های مهمی برخوردار است، پیش از صدورگواهی توسط نهاد گواهی‌کننده ممیزی می‌شود.

ث- برنامه بازبینی با توجه به الزامات بالا انجام شده و تمامی سایت‌ها و یا آنهایی‌که در دامنه‌شمول گواهی ISMS سازمان مشتری هستند را در مدت زمان معقولی پوشش دهد.

ج- زمانی‌که عدم‌انطباقی[1] مشاهده شود، چه در دفتر مرکزی و چه در یک سایت دیگر، روش‌اجرایی اقدام اصلاحی به دفتر مرکزی و تمامی سایت‌های تحت پوشش گواهینامه اعمال می‌شود.

ممیزی که در بخش IS 9.1.5 به آن اشاره می‌شود باید فعالیت‌های دفتر مرکزی سازمان مشتری را مدنظر قرار دهد تا اطمینان حاصل‌نماید که یک ISMS منفرد به تمامی سایت‌ها اعمال شده و مدیریت مرکزی تا سطح عملیاتی[2] تسری پیدا می‌کند. ممیزی باید تمام مواردی که در بالا به آنها اشاره شد، را مدنظر قراردهد.

۹-۱- ۵ روش‌شناسی ممیزی در IS 9.1.5

نهاد گواهی‌کننده باید روش‌های اجرایی داشته باشد، که سازمان مشتری را ملزم نماید تا بتواند اثبات کند که ممیزی‌های داخلی ISMS در آن سازمان دارای برنامه زمان‌بندی بوده، و برنامه‌ها و روش‌های اجرایی عملیاتی هستند و این عملیاتی شدن می‌تواند قابل مشاهده باشد.

توصیه نمی‌شود، روش‌های‌اجرایی نهاد گواهی‌کننده شامل پیش‌فرض‌هایی درباره شیوه‌خاصی از پیاده‌سازی ISMS یا شیوه‌خاصی در مستندسازی و حفظ سوابق باشد. روش‌های‌اجرایی صدورگواهی باید تنها متمرکز بر برآورده‌سازی الزامات استاندارد ۲۷۰۰۱ و خط‌مشی‌ها و اهداف سازمان مشتری در ISMS سازمان باشد.

توصیه می‌شود، طرح ممیزی[3]، روش‌های ممیزی شبکه‌ای[1] را که در حین ممیزی در زمان مناسب استفاده خواهند شد، شناسایی نماید.

1- Nonconformity
2- Operational level
3- Audit plan

یادآوری: روش‌های ممیزی شبکه‌ای می‌تواند شامل تله‌کنفرانس، ملاقات از طریق وب، ارتباط تعاملی مبتنی بر وب و دسترسی الکترونیکی از فاصله دور به مستندات ISMS و فرآیندهای آن باشد. توصیه می‌شود، هدف و تمرکز اصلی این شیوه‌ها بالا بردن اثربخشی و کارآیی[۲] ممیزی بوده و درعین حال یکپارچگی فرآیند ممیزی را نیز حمایت نماید.

۹-۱- ۶ گزارش ممیزی‌صدورگواهی در IS 9.1.6

۹-۱-۶-۱ نهاد گواهی‌کننده مجاز است روش‌های اجرایی گزارش‌دهی را با توجه به نیازهای خود اتخاذ کند؛ ولی این روش‌های اجرایی باید دست‌کم بتوانند آن سازمان را از موارد زیر مطمئن کنند:

الف- یک جلسه با حضور تیم ممیزی و مدیریت سازمان مشتری پیش از ترک مکان سازمان مشتری تشکیل شود که در آن تیم ممیزی موارد زیر را ارائه دهد:

۱- یک گزارش شفاهی یا کتبی راجع به انطباق ISMS سازمان مشتری با الزاماتِ خاصِ صدورگواهی.

۲- فرصتی به سازمان مشتری برای پرسیدن سوالاتی درباره یافته‌ها و پایه و اساس آنها.

ب- تیم ممیزی یافته‌هایش راجع به انطباق ISMS سازمان‌مشتری به‌همراه تمامی الزاماتِ صدورگواهی را بصورت یک گزارش‌ممیزی در اختیار نهاد گواهی‌کننده قرار می‌دهد.

۹-۱-۶-۲ توصیه می‌شود، گزارش ممیزی شامل اطلاعات زیر باشد:

الف- گزارشی از ممیزی شامل خلاصه‌ای از بازنگری مدارک.

ب- گزارشی از ممیزی‌صدورگواهی تحلیل ریسک امنیت اطلاعات سازمان مشتری.

پ- کل‌زمان ممیزی صرف‌شده و مشخصات جزئی[۳] زمان گذرانده‌شده برای بازنگری مدارک، ارزیابی تحلیل ریسک، ممیزی در محل و تهیه گزارش ممیزی.

ت- پرسش‌های ممیزی[۴] که پیگیری‌شده‌اند، دلایل انتخاب آنها و روش‌شناسی بکار گرفته شده.

۹-۱-۶-۳ گزارش ممیزی از یافته‌ها، که به نهاد گواهی‌کننده تحویل می‌شود، باید از جزئیات کافی جهت تسهیل و پشتیبانی از تصمیم‌گیری برای صدورگواهی برخوردار بوده و شامل موارد زیر باشد:

الف- موضوعاتی که بوسیله ممیزی پوشش داده شده‌اند. (برای‌مثال الزاماتِ صدورگواهی و محلهایی که ممیزی شده‌اند.) شامل: داده‌های ممیزی مهم[۵] پیگیری‌شده و روش‌شناسی‌های ممیزی استفاده شده (رجوع شود به IS 9.1.5).

ب- مشاهدات انجام گرفته چه مثبت(برای‌مثال نکات برجسته) و چه منفی(برای‌مثال عدم‌انطباقات بالقوه).

4- Network-assisted
5- Efficiency
1- Detailed specification
2- Audit enquiries
3- Significant audit trails

پ- جزئیات هر عدم‌انطباق شناسایی شده، که با استفاده از شواهد عینی[1] و ارجاع این عدم‌انطباقات به الزامات استانداردِ "سیستم‌های مدیریت امنیت اطلاعاتِ" استاندارد ۲۷۰۰۱ یا سایر مدارک لازم برای صدور گواهی پشتیبانی می‌شوند.

ت- اعلام‌نظر درباره انطباق ISMS سازمان مشتری با الزاماتِ صدورگواهی، به همراه بیانیه شفاف درباره عدم‌انطباقات، ارجاع به نسخه بیانیه کاربردپذیری و درجایی‌که امکان‌پذیر است، مقایسه سودمند با نتایج پیشین ممیزی‌های صدورگواهی سازمان مشتری.

پرسشنامه‌های تکمیل شده، چک‌لیست‌ها[2]، مشاهدات، اطلاعات ثبت‌شده وقایع[3]، یا یادداشت‌های ممیز، می‌توانند جزء لاینفک گزارش ممیزی باشند. اگر چنین روش‌هایی بکارگرفته می‌شوند، این مدارک باید به عنوان شواهد پشتیبان در تصمیم‌گیری برای صدورگواهی در اختیار نهاد گواهی‌کننده قرارداده‌شوند. توصیه می‌شود، اطلاعات درباره نمونه‌هایی که در حین ممیزی ارزشیابی شده‌اند نیز در گزارش‌ممیزی یا در دیگر مستندات صدور گواهی، آورده شوند. گزارش باید شایستگی سازمان داخلی و روش‌های اجرایی پذیرفته‌شده بوسیله سازمان مشتری جهت اطمینان از اینکه ISMS ایجاد شده است، را مد نظر قرار دهد.

علاوه بر الزاماتی که در بند ۹-۱-۱۰ از استاندارد ۲۷۰۰۱ برای گزارش‌دهی آورده شده است، توصیه می‌شود، گزارش موارد زیر را نیز پوشش دهد:

- درجه اعتمادی که می‌توان به ممیزی‌های داخلی ISMS و بازنگری‌های مدیریت داشت.
- خلاصه‌ای از مهمترین مشاهدات، چه مثبت و چه منفی، از اثربخشی و پیاده‌سازی ISMS.
- پیشنهاد تیم ممیزی که آیا گواهی برای ISMS سازمان مشتری صادر شود یا خیر و اطلاعاتی که این پیشنهاد را تایید و اثبات نماید.

۹-۲ ممیزی اولیه و صدورگواهی

الزامات بند ۹-۲ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۹-۲-۱ شایستگی تیم ممیزی در IS 9.2.1

علاوه بر الزاماتی که در بند ۷-۲ آورده شده است، الزامات زیر نیز در ارزیابی صدورگواهی لحاظ می‌شوند. در فعالیت‌های بازبینی صرفاً الزاماتی که به برنامه زمان‌بندی آن فعالیت مرتبط هستند کاربرد دارند.

الزامات زیر به کل تیم ممیزی اعمال می‌شود:

الف- در هریک از زمینه های زیر، دست‌کم یکی از اعضای تیم ممیزی باید معیارهای نهاد گواهی‌کننده را، جهت برعهده‌گیری مسوولیت، برآورده نماید:

۱- مدیریت تیم.

۲- سیستم‌های مدیریتی و فرآیند بکار گرفتن آن در مورد ISMS.

4- Objective evidence
1- Checklists
2- Logs

۳- دانش درباره الزامات قانون‌گذاری و مقرارت، بویژه در حوزه امنیت اطلاعات.
۴- شناسایی تهدیدات و روند رخدادهای امنیتی مرتبط با امنیت اطلاعات.
۵- شناسایی آسیب‌پذیری‌های سازمان مشتری و درک احتمال سوء استفاده از آنها، پیامد و چگونگی کاهش[1] و کنترل این پیامدها.
۶- دانش درباره کنترل‌های ISMS و پیاده‌سازی آنها.
۷- دانش درباره بازنگری اثربخشی ISMS و اندازه‌گیری کنترل‌ها.
۸- استانداردهای مرتبط و یا مربوطبه ISMS، بهترین تجربیات عملی، روش‌های اجرایی و خط‌مشی‌های امنیتی.
۹- دانش درباره روش‌های رسیدگی به رخدادهای امنیتی[2] و استمرار[3] کسب‌وکار.
۱۰- دانش درباره دارایی‌های اطلاعاتی ملموس و غیر ملموس و تحلیل پیامدها.
۱۱- دانش درباره فن‌آوری حال حاضر که ممکن است به امنیت مربوط بوده یا موضوع آن باشد.
۱۲- دانش درباره فرآیندها و روش‌های مدیریت ریسک.

ب- تیم ممیزی باید برای دنبال کردن نشانه های یک رخداد امنیتی در ISMS سازمان مشتری را تا رسیدن به مولفه‌های ISMS مربوط به آن، شایسته باشد.

پ- تیم ممیزی باید تجربه کاری و کاربرد عملی مناسبی از موارد فوق داشته باشد (این به‌معنای آن نیست که یک ممیز نیاز دارد گستره وسیعی از تجربیات در همه زمینه‌های امنیت اطلاعات داشته باشد. ولی توصیه می‌شود، تیم ممیزی به‌طور کل، از تجربه کافی برای پوشش دامنه‌شمول ISMS ممیزی شونده برخوردار باشد)

یک تیم ممیزی می‌تواند شامل یک نفر باشد به شرط آنکه وی تمامی معیارهای بخش الف را برآورده سازد.

۹-۲-۱-۱ اثبات شایستگی ممیز در IS 9.2.1.1

ممیزان باید بتوانند دانش و تجربه خود را، همان‌گونه که در بالا اشاره شد، اثبات کنند برای مثال از طریق:

الف- اثبات شرایط به‌رسمیت شناخته‌شده و مختص ISMS.
ب- ثبت نام به عنوان ممیز.
پ- دوره‌های آموزشی تایید شده ISMS .
ت- سوابق روزآمد از بهبود حرفه‌ای مستمر.
ث- تجربیات عملی کسب‌شده از مشاهده کار ممیزان با حضور در فرآیند واقعی ممیزی سیستم‌های مشتری.

1- Mitigation
2- Incident handling
3- Continuity

۹-۲- ۲ تدارکات عمومی برای ممیزی اولیه در IS 9.2.2

نهاد گواهی‌کننده باید از سازمان مشتری بخواهد تا تمامی تدارکات مورد نیاز برای اجرای ممیزی‌صدورگواهی، شامل فراهم کردن شرایط بررسی مستندات و دسترسی به تمامی نواحی، سوابق(شامل گزارشات ممیزی‌های داخلی و گزارشات بازنگری‌های مستقل امنیت اطلاعات) و کارکنان با اهداف ممیزی‌صدورگواهی، ممیزی‌صدورگواهی مجدد و رسیدگی به شکایات را ایجاد کند.

دست‌کم اطلاعات زیر باید پیش از ممیزی‌صدورگواهی درمحل سازمان از سوی مشتری در اختیار مرجع صدورگواهی قرار گیرد:

الف- اطلاعات کلی درباره ISMS و فعالیت‌هایی که پوشش می‌دهد.

ب- یک رونوشت از مستندات مورد نیاز ISMS که در بند ۴-۳-۱ از استاندارد ۲۷۰۰۱ تعیین شده‌اند؛ همچنین مستندات مرتبط در صورت لزوم.

۹-۲- ۳ ممیزی اولیه صدورگواهی در IS 9.2.3

۹-۲-۳-۱ ممیزی مرحله اول[1] در IS 9.2.3.1

در این مرحله از ممیزی، نهاد گواهی‌کننده باید مستندات طراحی ISMS را که پوشش‌دهنده مستندات الزامی در بند ۴-۳-۱ از استاندارد ۲۷۰۰۱ است، دریافت نماید.

هدف از ممیزی مرحله اول، تعیین نقطه تمرکز برای طرح‌ریزی ممیزی مرحله دوم با بدست آوردن درکی از ISMS، در قالب اهداف و خط‌مشیِ ISMS سازمان مشتری و به طور خاص، وضعیت حال حاضر سازمان مشتری و میزان آمادگی آن برای ممیزی است.

ممیزی مرحله اول شامل بازنگری مدارک می‌شود. ولی توصیه می‌شود که محدود به آن نباشد. نهاد گواهی‌کننده باید در این مورد که مدارک کی‌وکجا مورد بازنگری قرار گیرند با سازمان مشتری توافق کند. در هر حال بازنگری مدارک باید پیش از آغاز ممیزی مرحله دوم انجام شود.

نتایج ممیزی مرحله اول باید به صورت مکتوب مدون شوند. نهاد گواهی‌کننده باید پیش از تصمیم بر ادامه کار و رفتن به ممیزی مرحله دوم و همچنین انتخاب تیم ممیزی و تعیین شایستگی آنها، گزارش ممیزی مرحله اول را بازنگری نماید.

نهاد گواهی‌کننده باید سازمان مشتری را از نوع اطلاعات و سوابق بیشتری که ممکن است در ممیزی مرحله دوم برای بررسی‌های دقیق‌تر به آنها نیاز باشد، آگاه کند.

1- Stage 1 audit

منظور از ممیزی مرحله اول، مرحله اول از مراحل انجام ممیزی می باشد.

۹-۲-۳-۲ ممیزی مرحله دوم در IS 9.2.3.2

۹-۲-۳-۲-۱ممیزی مرحله دوم همیشه در محل(های) سازمان مشتری انجام می‌شود. بر اساس یافته‌های موجود در مدارک گزارش ممیزی مرحله اول، نهاد گواهی‌کننده یک طرح ممیزی را برای انجام ممیزی مرحله دوم تهیه می‌نماید. اهداف ممیزی مرحله دوم عبارتند از:

الف- تایید این امر که سازمان مشتری به خط‌مشی ها، اهداف و روش‌های اجرایی‌اش پایبند است.

ب- تایید این امر که ISMS با تمامی الزامات استاندارد الزامی ISMS - استاندارد ۲۷۰۰۱- مطابقت داشته و اهداف خط‌مشی سازمان مشتری را تامین می‌نماید.

۹-۲-۳-۲-۲ جهت دستیابی به این مهم، ممیزی باید تمرکز خود را معطوف موارد زیر از سازمان مشتری نماید:

الف- ارزیابی‌ریسک‌های مرتبط با امنیت اطلاعات و اینکه ارزیابی‌ها نتایج قابل‌قیاس و تجدیدپذیری را بدست دهد.

ب- الزامات مستندسازی ذکر شده در بند ۴-۳-۱ از استاندارد ۲۷۰۰۱.

پ- انتخاب اهداف کنترلی و کنترل‌ها براساس ارزیابی‌ریسک و فرآیندهای برطرف‌سازی ریسک.

ت- بازنگری‌های اثربخشی ISMS و اندازه‌گیری اثربخشی کنترل‌های امنیت اطلاعات، گزارش‌ها و بازنگری‌های اهداف ISMS.

ث- بازنگری‌های مدیریتی و ممیزی‌های داخلی ISMS .

ج- مسوولیت مدیریت در خط‌مشی امنیت اطلاعات.

چ- تطابق بین کنترل‌های انتخابی و کنترل‌های پیاده‌سازی شده، بیانیه کاربردپذیری و نتایج ارزیابی‌ریسک و فرآیند برطرف‌سازی ریسک و خط‌مشی و اهداف ISMS .

ح- پیاده‌سازی کنترل‌ها (به پیوست ت رجوع شود)، با در نظر گرفتن اندازه‌گیری‌های انجام‌شده از سوی سازمان، از میزان اثربخشی کنترل‌ها (بند ت)، جهت تعیین اینکه آیا کنترل‌ها پیاده‌سازی شده و از اثربخشی لازم برای نیل به اهداف بیان‌شده برخوردار هستند یا خیر.

خ- برنامه‌ها، فرآیندها، روش‌های اجرایی، سوابق، ممیزی‌های داخلی، و بازنگری‌های اثربخشی ISMS جهت اطمینان از اینکه این موارد تا تصمیمات مدیریتی، خط‌مشی و اهداف ISMS قابل‌ردیابی[1] هستند.

۹-۲-۳-۳ مولفه‌های مختص ممیزی ISMS در IS 9.2.3.3

نقش نهاد گواهی‌کننده این است که تعیین کند، سازمان‌های مشتری در ایجاد و حفظونگهداری روش‌های اجرایی‌شان برای شناسایی، بررسی و ارزشیابی[2] آسیب‌پذیری‌ها و تهدیداتِ دارایی‌های (تهدیدات مرتبط با امنیت اطلاعات) و پیامدهای آن برای سازمان خود پایبند هستند. نهادهای گواهی‌کننده باید:

1- Traceable
2- Evaluation

الف- سازمان مشتری را ملزم کنند تا اثبات کند که تحلیل امنیتی تهدیدات، کافی و در عین حال مرتبط با عملکرد سازمان مشتری است.

یادآوری- سازمان مشتری مسوول تعریف معیارهایی است، که به کمک آن ریسک‌های مرتبط با امنیت اطلاعات در سازمان مشتری را تحت عنوان «مهم[1]» شناسایی نموده و برای انجام آن روش‌های اجرایی تدوین نماید.

ب- تعیین کند، که آیا روش‌های اجرایی سازمان مشتری برای شناسایی، بررسی و همچنین ارزشیابی تهدیداتِ دارایی‌ها (تهدیدات مرتبط با امنیت اطلاعات)، آسیب‌پذیری‌ها و پیامدها، و نتایج به کار گرفتن آنها در راستای اهداف، خط‌مشی و مقاصد سازمان مشتری قرار دارد یا خیر.

نهاد گواهی‌کننده همچنین باید تعیین کند که آیا روش‌های اجرایی بکارگرفته شده در تحلیل میزان اهمیت[2] بی‌عیب هستند و به‌طور صحیح پیاده‌سازی شده‌اند. اگر یک تهدید دارایی‌ها (تهدید مرتبط با امنیت اطلاعات)، یک آسیب‌پذیری، یا یک پیامد بر سازمان مشتری، مهم تشخیص داده شود، باید در ISMS به آن پرداخته شود.

۹-۲-۳-۳-۱ انطباق با قوانین و مقررات

نگهداری و ارزشیابی تطابق و پیروی از قوانین و مقررات برعهده سازمان مشتری است. نهاد گواهی‌کننده باید خود را تنها به بررسی و نمونه برداری جهت اطمینان از عملکرد سازمان مشتری در این زمینه محدود کند. نهاد گواهی‌کننده باید برخوردار بودن سازمان مشتری را، از یک سیستم مدیریت برای دستیابی به انطباق با قوانین و مقررات قابل‌اجرا درمورد ریسک‌های امنیت اطلاعات و پیامدهای آن، تصدیق کند.

۹-۲-۳-۳-۲ یکپارچه سازی مستندات ISMS با سایر مستندات سیستم‌های مدیریتی

سازمان مشتری می‌تواند مستندات ISMS و سایر سیستم‌های مدیریتی (مانند: کیفیت، بهداشت و ایمنی، و محیط زیست) را با یکدیگر تلفیق کند تا جایی‌که ISMS به وضوح به همراه فصل‌های مشترک مناسب با سایر سیستم‌ها قابل تمیز باشد.

۹-۲-۳-۳-۳ تلفیق ممیزی‌های سیستم مدیریت

یک نهاد گواهی‌کننده مجاز است صدورگواهی سایر سیستم‌های مدیریتی را همراه با صدورگواهی ISMS عرضه کند و یا فقط صدورگواهی ISMS را عرضه کند.

ممیزی ISMS می‌تواند به صورت تلفیقی با ممیزی سایر سیستم‌های مدیریتی انجام شود. این تلفیق به‌شرطی امکان‌پذیر خواهد بود، که بتوان اثبات کرد تمامی الزامات صدورگواهی ISMS برآورده شده‌اند. تمامی مولفه‌های دارای اهمیت برای ISMS باید در گزارشات ممیزی به طور شفاف قابل مشاهده و به سادگی قابل تشخیص باشند. کیفیت ممیزی نباید به هیچ عنوان تحت تاثیر تلفیق ممیزی‌ها قرار گیرد.

3- Significant

1- Analysis of significance

یادآوری- استاندارد ISO19011 راهنمایی جهت انجام ممیزی تلفیقی[1] سیستم مدیریت ارائه می‌کند.

۹-۲- ۴ اطلاعات لازم برای اعطای گواهی اولیه در IS 9.2.4

جهت دستیابی به مبنایی برای، تصمیم‌گیری برای صدورگواهی، نهاد گواهی‌کننده باید گزارشاتی شفاف، که اطلاعات کافی جهت تصمیم‌گیری را در اختیار وی قرار دهد، درخواست نماید.

گزارش‌دهی توسط تیم ممیزی به نهاد گواهی‌کننده در مراحل مختلف فرآیند ممیزی‌صدورگواهی الزامی است.

توصیه می‌شود، علاوه بر اطلاعاتی که در فایل موجود هستند، این گزارشات دست‌کم شامل الزامات ذکر شده در بند IS 9.1.6 باشند.

۹-۲- ۵ تصمیم‌گیری برای صدورگواهی در IS 9.2.5

توصیه می‌شود، موجودیتی[2]- که ممکن است یک فرد باشد- که در نهاد گواهی‌کننده درباره اعطا/ ابطال یک گواهی تصمیم‌گیری می‌کند، شالوده‌ای از دانش‌ها و تجربیات در تمامی زمینه ها باشد، که برای ارزشیابی فرآیندهای ممیزی و همچنین پیشنهادات مرتبط با آن، که توسط تیم ممیزی انجام شده است، مناسب است.

تصمیم صدور یا عدم صدورگواهی برای یک سازمان مشتری باید توسط نهاد گواهی‌کننده و براساس اطلاعات جمع‌آوری شده در فرآیند صدورگواهی و همچنین سایر اطلاعات مرتبط انجام پذیرد.

کسانی که در مورد صدورگواهی، تصمیم‌گیری می‌کنند، نباید در تیم ممیزی حضور داشته باشند. این تصمیم باید براساس یافته‌ها و پیشنهادات تیم ممیزی که در گزارش ممیزی‌صدورگواهی ایشان (رجوع شود به بخش IS 9.1.6) آورده شده است و یا هر اطلاعات مرتبطی که قابل دسترس نهاد گواهی‌کننده است، انجام پذیرد.

معمولاً توصیه نمی‌شود، موجودیتی که درباره اعطای‌گواهی تصمیم‌گیری می‌کند، مخالف نظرات منفی تیم ممیزی تصمیم‌گیری نماید. اگر چنین اتفاقی رخ دهد، نهاد گواهی‌کننده باید دلایل مخالفت با توصیه را مستند و توجیه نماید.

در مورد تصمیم‌گیری درباره صدورگواهی، استاندارد ISO/IEC 17021 هیچ مدت زمان مشخصی را که در آن دست‌کم باید یک ممیزی داخلی کامل ISMS و یک بازنگری مدیریتی در سازمان مشتری انجام شود، مشخص نمی‌کند. نهاد گواهی‌کننده می‌تواند چنین مدت زمانی را تعیین کند. صرف‌نظر از اینکه نهاد گواهی‌کننده جهت انتخاب یک حداقل تناوب[3] تعیین شده است یا نه، اقداماتی از سوی نهاد گواهی‌کننده باید برای اطمینان از اثربخشی فرآیندهای ممیزی داخلی ISMS و بازنگری‌های مدیریتی سازمان مشتری، تعیین شود.

2- Combined audit
1- Entity
2- Minimum Frequency

گواهی نباید به سازمان مشتری اعطا شود، تا زمانی‌که شواهد کافی دال بر این مطلب وجود داشته باشد که: تمهیدات لازم که برای بازنگری‌های مدیریتی و ممیزی‌های داخلی ISMS پیاده‌سازی شده‌اند، اثربخش هستند و به خوبی نگهداری خواهند شد.

۹-۳ فعالیت‌های بازبینی

الزامات بند ۹-۳ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۹-۳-۱ ممیزی‌های بازبینی در IS 9.3

۹-۳-۱-۱ روش‌های اجرایی ممیزی بازبینی باید با روش‌های اجرایی ممیزی‌صدورگواهی ISMS سازمان مشتری، همان‌گونه که در این استاندارد به آنها اشاره شد، هماهنگ باشد.

هدف از بازبینی؛ تصدیق این امر است که ISMSای که قبلاً تاییدشده، همچنان استقرار دارد؛ مدنظر قرار دادن دلایل ضمنی ایجاد تغییرات در سیستم ISMS به‌دلیل تغییراتِ عملکردِ سازمانِ مشتری؛ و تایید تداوم انطباق با الزامات صدور گواهی است. توصیه می‌شود، برنامه‌های بازبینی به‌طورعادی موارد زیر را پوشش دهد:

الف- مولفه‌های نگهداری سیستم شامل: ممیزی‌داخلی ISMS، بازنگری‌مدیریت و اقدام پیشگیرانه و اصلاحی.

ب- ارتباطات اشخاص بیرونی، همان‌گونه که در استاندارد ۲۷۰۰۱ و سایر مدارک لازم برای صدورگواهی الزام شده است.

پ- تغییرات سیستم مستندسازی.

ت- حوزه‌های مورد تغییر قرارگرفته.

ث- مولفه‌های انتخابی از استاندارد ۲۷۰۰۱.

ج- سایر حوزه‌های انتخابی در موارد مقتضی.

۹-۳-۱-۲ بازبینی که از سوی نهاد گواهی‌کننده انجام می‌شود، باید دست‌کم موارد زیر را مورد بازنگری قرار دهد:

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

ب- عملکرد صحیح روش‌های اجرایی در ارزشیابی دوره‌ای و بازنگری مطابقت با قوانین و مقرارت مرتبط با امنیت اطلاعات.

پ- اقدامات انجام شده در راستای از بین بردن عدم‌انطباقات شناسایی شده در آخرین ممیزی.

۹-۳-۱-۳ توصیه می‌شود، بازبینی که از سوی نهاد گواهی‌کننده انجام می‌شود، دست‌کم نکات الزامی ممیزی بازبینی را که در استاندارد ISO/IEC 17021 به آنها اشاره شده است، پوشش دهند. به‌علاوه، توصیه می‌شود، موارد زیر نیز در نظر گرفته شوند:

الف- توصیه می‌شود، نهاد گواهی‌کننده بتواند برنامه بازبینی خود را با موارد امنیت اطلاعات، مرتبط با تهدیداتِ دارایی‌ها، آسیب‌پذیری‌ها و پیامدها، برای سازمان مشتری وفق داده و این برنامه را توجیه کند.

ب- توصیه می‌شود، برنامه بازبینی نهاد گواهی‌کننده، بوسیله نهاد گواهی‌کننده تعیین شود. زمان‌های مشخص بازدید می‌تواند با توافق سازمان مشتری تعیین شود.

پ- ممیزهای بازبینی می‌تواند به صورت تلفیقی با ممیزی‌های سایر سیستم‌های مدیریتی انجام پذیرد. در گزارش باید به طور شفاف موارد مربوط به هر سیستم مدیریتی مشخص باشد.

ت- نظارت نهاد گواهی‌کننده بر نحوه استفاده از گواهینامه الزامی است.

در حین ممیزی‌های بازبینی، نهادهای گواهی‌کننده باید سوابق درخواست‌هایِ رسیدگی‌مجدد و شکایاتِ ازپیش‌ارائه‌شده به نهادگواهی‌دهنده را، در مواردی‌که عدم‌انطباق یا مردودی در الزامات صدور گواهی مشاهده شده است، بررسی نمایند و همچنین تحقیق کنند، آیا ISMS سازمان مشتری روش‌های اجرایی خود را بررسی و اقدام اصلاحی لازم را انجام داده است یا خیر.

یک گزارش بازبینی به طور خاص باید شامل اطلاعاتی مبنی بر برطرف سازی عدم‌انطباقات گزارش شده قبلی باشد. توصیه می‌شود، گزارشاتی که در بازبینی تهیه می‌شوند، دست‌کم تمامی الزامات ذکر شده در بند الف را پوشش دهند.

۹-۴ صدورگواهی مجدد

الزامات بند ۹-۴ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۹-۴-۱ ممیزی صدورگواهی مجدد در IS 9.4

روش‌های اجرایی ممیزی‌صدورگواهی‌مجدد باید با روش‌های اجرایی ممیزی‌صدورگواهی ISMS سازمان مشتری ذکر شده در این استاندارد همخوانی داشته باشد.

نهادهای گواهی‌کننده باید روش‌های اجرایی مشخص و شفاف جهت تبیین شرایط و موقعیت‌هایی که منجر به حفظ گواهی سازمان مشتری می‌شود، داشته باشد. اگر در ممیزی بازبینی یا ممیزی صدورگواهی‌مجدد عدم‌انطباقاتی یافت شود، این عدم‌انطباقات باید به صورت اثربخش و در زمان توافق شده با نهاد گواهی‌کننده اصلاح شوند. اگر این اصلاح در زمان توافق شده انجام نشود، دامنه‌شمول گواهی باید کوچکتر شود یا گواهینامه به حالت تعلیق درآید و یا ابطال شود. توصیه می‌شود، مدت زمانی‌که جهت انجام اقدام‌اصلاحی در اختیار سازمان‌مشتری قرار می‌گیرد با میزان اهمیت عدم‌انطباق و ریسکِ اطمینان ازاین‌که محصولات و خدمات سازمان مشتری الزامات خاصی را رعایت می‌کنند، هم‌خوانی داشته باشد.

۹-۵ ممیزی‌های خاص

الزامات بند ۹-۵ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۹-۵-۱ حالتهای خاص در IS 9.5

فعالیت‌های بازبینی باید تحت ضوابط خاصی قرار گیرند، اگر یک سازمان مشتری که دارای گواهی ISMS است، تغییرات عمده‌ای در سیستم‌اش دهد یا تغییرات دیگری اتفاق بیافتد که بتواند اساس گواهی آن سازمان را تحت تاثیر قرار می‌دهد.

۹-۶ تعلیق، ابطال یا کوچک کردن دامنه‌شمول گواهی

الزامات بند ۹-۶ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۹-۷ درخواست‌های رسیدگی‌مجدد

الزامات بند ۹-۷ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۹-۸ شکایات

الزامات بند ۹-۸ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۹-۸-۱ شکایات در IS 9.8

شکایات بعنوان یک منبع اطلاعات برای نشان دادن عدم‌انطباق احتمالی عمل می‌کنند. توصیه می‌شود، نهاد گواهی‌کننده سازمان مشتری صاحب گواهی را ملزم کند تا در زمان دریافت شکایت، دلیل شکایت را مدون و در زمان مناسب آن را گزارش دهد. این گزارش شامل هر مورد از پیش تعیین شده (یا قبلاً ارائه شده) در ISMS سازمان مشتری است.

توصیه می‌شود، نهاد گواهی‌کننده این‌گونه تعبیر نماید که سازمان مشتری با استفاده از این بررسی‌ها قصد دارد اقدام جبرانی[1]/ اصلاحی را انجام دهد. توصیه می‌شود این امر شامل اقداماتی[2] برای موارد زیر باشد:

الف- مطلع ساختن مراجع دارای اختیار مناسب، درصورتی‌که این‌کار براساس مقررات الزام شده است.

ب- انطباق ترمیمی[3].

پ- اجتناب از وقوع مجدد.

ت- ارزشیابی و کاهش رخدادهای امنیتی مخرب و کاهش پیامدهای آنها.

ث- اطمینان از تعامل رضایت بخش با سایر اجزای ISMS.

ج- ارزیابی اثربخشی اقدامات جبرانی/ اصلاحی اختیار شده.

1- Remedial action
2- Measures
3- Restoring Conformity

نهاد گواهی‌کننده باید هر سازمان مشتری که ISMS آن گواهی شده است، را ملزم کند تا سوابق تمامی شکایات و اقدام اصلاحی انجام پذیرفته در راستای تطابق با الزامات استاندارد ملی ایران ایزو-آی ای سی به شماره ۲۷۰۰۱ را، بنا به درخواست، در اختیار نهاد گواهی‌کننده قرار دهد.

۹-۹ سوابق متقاضیان و مشتریان

الزامات بند ۹-۹ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۱۰ الزامات سیستم مدیریتی برای نهادهای گواهی‌کننده

۱۰-۱ گزینه ها

الزامات بند ۱۰-۱ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۱۰-۲ گزینه ۱- الزامات سیستم مدیریتی مطابق با ISO9001

الزامات بند ۱۰-۲ از استاندارد ISO/IEC 17021 بکارگرفته شود.

۱۰-۳ گزینه ۲- الزامات عمومی سیستم مدیریت

الزامات بند ۱۰-۳ از استاندارد ISO/IEC 17021 بکار گرفته شود. بعلاوه، الزامات و راهنمایی مختص ISMS ذیل نیز بکار گرفته شود:

۱۰-۳-۱ پیاده‌سازی ISMS در IS 10.3

توصیه می‌شود، نهادهای گواهی‌کننده ISMS را مطابق با استاندارد ۲۷۰۰۱ پیاده‌سازی کنند.

پیوست الف

(اطلاعاتی)

تحلیل پیچیدگی سازمان‌های مشتری و موارد مختص بخش

الف- ۱ ریسک بالقوه سازمان

پیچیدگی دامنه‌شمول ISMS باید در زمان تعیین زمان ممیزی یا شایستگی ممیزان در نظر گرفته شود. این پیوست مثالی از تحلیل پیچیدگی یک سازمان مشتری را برای این منظور ارائه می‌کند.

رده‌ی پیچیدگی که به دامنه‌شمول ISMS اختصاص داده می‌شود می‌تواند برای تصمیم‌گیری در موارد زیر استفاده شود:

الف- الزامات شایستگی ممیزان برای ممیزی ISMS (مثالی از آن در پیوست ب شرح داده شده است).

ب- الزامات زمان ممیزی برای ممیزی ISMS (مثالی از آن در پیوست پ شرح داده شده است).

جدول الف-۱ نمایشی کلی از عوامل ممکن که برای تعیین پیچیدگی دامنه‌شمول ISMS درنظر گرفته می‌شوند، را در بردارد. این جدول نیاز دارد برای موقعیت‌های مشخص تطبیق داده شود و یا در موارد مقتضی، فاکتورهای خاص دیگری به آن اضافه شود.

با استفاده از معیار پیچیدگی بطور مجزا (در جدول الف-۱)، جنبه‌های پیچیدگی دامنه‌شمول ISMS می‌تواند به سه رده طبقه‌بندی شود: "بالا"، "متوسط" و "پایین". این سطوح با استفاده از تعدادی عوامل متفاوت بدست می‌آیند. رده اثربخش کلی پیچیدگی می‌تواند با درنظر گرفتن بالاترین رده موجود در بین فاکتورها تعیین شود و ماحصل نیز به صورت رده خواهد بود، به‌عبارت‌دیگر «بالا»،«متوسط» یا «پایین».

جدول الف-۱ – معیارهای پیچیدگی دامنه‌شمول ISMS

عامل پیچیدگی	رده			اهمیت
	بالا	متوسط	پایین	
تعداد کارکنان + کارکنان پیمانکاران	≥۱۰۰۰	≥۲۰۰	<۲۰۰	ابعاد پیاده‌سازی ISMS سیستم مدیریت اطلاعات سیستم‌های تولیدی مرتبط با مدیریت سیستم‌های مرتبط با خدمات عمومی / توزیع / فروش فن‌آوری اطلاعات/ خدمات اطلاعات و سیستم‌های مرتبط ساخت و ساز/ کشتی سازی/ سیستم تاسیسات مرتبط با مهندسی
تعداد کاربران	≥۱میلیون	≥۲۰۰۰۰۰	<۲۰۰۰۰۰	سیستم‌های مالی دولتها، مدارس، سیستم‌های بیمارستانی / پزشکی

جدول الف-۱ – ادامه

عامل پیچیدگی	رده			اهمیت
	بالا	متوسط	پایین	
تعداد سایت‌ها	≥۵	≥۲	۱	مقیاس پیاده‌سازی ISMS امنیت فیزیکی و محیطی (الف-۹ از استاندارد ۲۷۰۰۱)
تعداد سرورها	≥۱۰۰	≥۱۰	<۱۰	مقیاس پیاده‌سازی ISMS امنیت فیزیکی و محیطی (الف-۹ از استاندارد ۲۷۰۰۱) کنترل دسترسی (الف-۱۱ از استاندارد ۲۷۰۰۱) مخابرات و مدیریت عمکرد (الف-۱۰ از استاندارد ۲۷۰۰۱)
تعداد ایستگاههای کاری + رایانه های شخصی + رایانه های قابل حمل	≥۳۰۰	≥۵۰	<۵۰	کنترل دسترسی (الف-۱۱ از استاندارد ۲۷۰۰۱)
تعداد کارکنان بهبود و نگهداری برنامه کاربردی[1]	≥۱۰۰	≥۲۰	<۲۰	اکتساب، بهبود و نگهداری سیستم‌های اطلاعاتی (الف-۱۲ از استاندارد ۲۷۰۰۱)
فن‌آوری رمزنگاری و شبکه	اتصالات بیرونی/ اینترنت با رمزنگاری/ امضای دیجیتال/ الزامات زیرساخت‌کلیدهمگانی (PKI[2])	اتصالات بیرونی/ اینترنت بااستفاده از رمزنگاری موجود در تجهیزات استاندارد و بدون امضای دیجیتال/ الزامات زیرساخت‌کلیدهمگانی (PKI)	اتصالات بیرونی/ اینترنت بدون رمزنگاری/ امضای دیجیتال/ الزامات زیرساخت‌کلیدهمگانی (PKI)	مخابرات و مدیریت عملکرد (الف-۱۰ از استاندارد ۲۷۰۰۱) کنترل دسترسی (الف-۱۱ از استاندارد ۲۷۰۰۱)
اهمیت در انطباق قانونی	عدم برآورده‌سازی پیگرد قانونی دارد.	عدم برآورده‌سازی منجر به پرداخت‌تاوان‌مالی‌مهم یا خدشه‌دارشدن‌اعتبارمهم می‌شود.	عدم برآورده‌سازی منجر به پرداخت‌تاوان‌مالی‌ناچیز یا خدشه‌دارشدن‌اعتبارناچیز می‌شود.	قوانین و راهنمایی‌ها (الف-۱۵ از استاندارد ۲۷۰۰۱)

1- Application
2- Public Key Infrastructure

جدول الف-۱ – ادامه

عامل پیچیدگی	رده			اهمیت
	بالا	متوسط	پایین	
کاربردپذیری ریسک مختص بخش (برای مثال‌هایی از رده‌های‌مختص‌بخش درریسک‌امنیت‌اطلاعات به الف-۲ مراجعه شود)	قانون‌ومقررات مختص‌بخش کاربرد دارد.	قانون‌ومقررات مختص‌بخش، کاربرد ندارد ولی ریسک‌مهم‌مختص‌بخش کاربرد دارد.	قانون‌ومقررات مختص‌بخش، کاربرد ندارد و ریسک‌مختص‌بخش کاربرد ندارد.	مقیاس پیاده‌سازی ISMS قوانین و راهنمایی‌ها (الف-۱۵ از استاندارد ۲۷۰۰۱)

الف-۲ رده‌های مختص بخش در ریسک امنیت اطلاعات

ریسک‌های اطلاعات ممکن است مختص به نوع اطلاعات موردنظر یا بخش فعالیت سازمان، باشد. مثال‌های زیر رده‌های متفاوتی از ریسک را نشان می دهند:

رده‌های خاص کاربردی برای همه سازمان‌ها:

- حقوقها، مستمری‌ها، بهداشت و ایمنی، سوابق سازمانی، اطلاعات درون بخشی یا بین بخشی و غیره؛
- هر اطلاعات قابل تشخیص فردی دیگر؛
- هر اطلاعات تجاری مهم/ حساس دیگر مانند: اطلاعات تحقیق و بهبود، اطلاعات طراحی، اطلاعات مشتریان، نتایج و پیش‌بینی‌های مالی، طرح کسب‌وکار، حقوق مالکیت معنوی، فرآیندهای ساخت، و غیره.

اطلاعات دولتی حساس/ مهم:

- اطلاعات همگانی؛
- برنامه‌های کاربردی دولت الکترونیک[1]؛
- اطلاعات نگهداشته شده درباره شهروندان (برای‌مثال سلامتی، منفعت، مالیات‌ها، سوابق و غیره)؛
- اطلاعاتی که توسط تامین‌کنندگان[2] و سازندگان دولت مورد استفاده قرارمی‌گیرند: مانند طراحی‌های فن‌آوری ارتباطات و اطلاعات[3]، امکانات، محصولات، خدمات و غیره.

رده‌های خاص کاربردی برای کلاس‌های سازمانی:

- اصناف[4]- شرکت‌های لیست شده (احتمالا سایر نهادهای بزرگ).

1- E-government
2- Suppliers
3- Information Communication Technology (ICT)
4- Corporate governance

رده‌های خاص کاربردی برای بخش‌های تجاری:

- بهداشت؛
- تعلیم و تربیت؛
- هوا- فضا؛
- مخابرات؛
- خدمات مالی؛
- سازمان‌های خیریه و غیرانتفاعی.

پیوست ب
(اطلاعاتی)
حوزه‌های نمونه از شایستگی ممیز

ب-۱ ملاحظات کلی شایستگی

شیوه‌های متفاوتی برای اثبات دانش و تجربه یک ممیز وجود دارد. برای مثال دانش و تجربه می‌تواند از طریق اثبات شرایط برسمیت شناخته‌شده نشان‌داده‌شود. ثبت نام ممیز، برای‌مثال در مرکز IRCA[1] یا ثبت‌نام ممیز به هر طریق برسمیت شناخته‌شده دیگر نیز، می‌تواند نشانگر تجربه و دانش لازم برای ممیز باشد. توصیه می‌شود، سطح شایستگی‌های لازم برای تیم ممیزی با درنظر گرفتن حوزه مربوط به فن‌آوری/صنعتی سازمان و عوامل پیچیدگی آن تعیین شود.

ب-۲ ملاحظات مختص شایستگی

ب-۲-۱ آگاهی از کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱

موارد زیر دانش عمومی لازم در ارتباط با ممیزی ISMS را بیان می‌کنند. علاوه بر حوزه‌های کنترلی پیوست الف از استاندارد ۲۷۰۰۱، که در جدول زیر لیست شده‌اند، توصیه می‌شود، ممیزان از مفاد سایر استانداردهای خانواده ۲۷۰۰۰ نیز آگاهی داشته باشند.

دانش و تجربه درباره خط‌مشی‌ها و الزامات کسب‌وکار برای امنیت اطلاعات	خط‌مشی امنیتی
دانش و تجربه عمومی از فرآیندهای کسب‌وکار، اعمال و ساختارهای سازمانی	سازمان امنیت اطلاعات
دانش ارزش‌گذاری دارایی‌ها، سیاهه اموال، طبقه بندی دارایی‌ها و خط‌مشی‌های قابل قبول مورد استفاده در دارایی‌ها	مدیریت دارایی
دانش و تجربه کلی از فرآیندها و روش‌های اجرایی استفاده شده در بخش‌های منابع انسانی	امنیت منابع انسانی
آگاهی از امنیت زیست‌محیطی و فیزیکی	امنیت محیطی و فیزیکی
دانش و تجربه روزآمد از استانداردها، فرآیندها، تکنیک‌ها و روش‌های بکارگرفته شده در امنیت اطلاعات شامل اقدامات مدیریتی و همچنین سطح مناسب تخصص‌های فنی. این مورد همچنین دربرگیرنده آخرین اطلاعات برخی شیوه‌های کسب‌وکار متداول نیز می‌شود.	مدیریت عملکرد و ارتباطات کنترل دسترسی اکتساب، بهبود و نگهداری سیستم‌های اطلاعاتی
دانش و تجربیات روزآمد از فرآیندها و روش‌های اجرایی مدیریت رخدادهای امنیتی	مدیریت رخدادهای امنیت اطلاعات
دانش و تجربیات روزآمد از استانداردها، فرآیندها، برنامه‌ها و روش‌های اجرایی آزمون برای تداوم کسب‌وکار	مدیریت تداوم کسب‌وکار
دانش روزآمد از موارد قراردادی تجاری و قوانین و مقررات متداول و مرتبط	انطباق

1- International Register of Certificated Auditors

با ISMS	

ب-۲-۲ دانش معمول مرتبط با ISMS

توصیه می‌شود، ممیزان درباره موضوعات ممیزی و ISMS ،که در زیر آورده شده‌اند، اطلاع و آگاهی داشته باشند:

- طرح‌ریزی و برنامه‌ریزی ممیزی،
- نوع و روش‌شناسی‌های ممیزی،
- ریسک ممیزی،
- تحلیل فرآیندهای امنیت اطلاعات،
- چرخه دمینگ[1] (PDCA[2]) برای بهبود مداوم،
- ممیزی داخلی برای امنیت اطلاعات.

توصیه می‌شود، ممیزان از الزامات قانونی و مقررات زیر اطلاع و آگاهی داشته باشند:

- مالکیت معنوی،
- محتوی، حفاظت و نگهداری از سوابق سازمانی،
- حفاظت از اطلاعات و حریم شخصی،
- مقررات کنترل‌های رمزنگاری،
- ضد تروریستی،
- تجارت الکترونیکی،
- امضای دیجیتال و الکترونیکی،
- بازبینی‌های محیط کار،
- قطع ارتباط مخابراتی و مشاهده اطلاعات (برای‌مثال پست الکترونیک)،
- سوء استفاده های رایانه‌ای،
- جمع‌آوری شواهد الکترونیکی،
- آزمون نفوذپذیری،
- الزامات ملی و بین‌المللی مختص‌بخش (برای‌مثال بانکداری).

توصیه می‌شود ممیزان از الزامات مدیریتی زیر اطلاع و آگاهی داشته باشند:

- برطرف سازی ریسک‌های امنیت اطلاعات،
- ریسک‌های امنیتی برون سپاری در فن‌آوری ارتباطات و اطلاعات،
- ریسک‌های امنیت اطلاعات در زنجیره تامین.

1- Deming cycle
2- Plan, Do, check, Act

پیوست پ
(اطلاعاتی)
زمان ممیزی

پ-۱ مقدمه

این پیوست حاوی اطلاعات بیشتری درباره بندهای ۹-۱، ۹-۲، ۹-۳ و ۹-۴ از استاندارد ۲۷۰۰۱ است. توصیه می‌شود، این پیوست به همراه بندهای IS 9.1.2، IS 9.1.3، IS 9.1.5، IS 9.1.6، IS 9.2.3.1 ، IS 9.2.3.3 و IS 9.2.3.3 از این استاندارد مطالعه شود. این پیوست راهنمایی برای نهاد گواهی‌کننده در راستای بهبود روش‌های اجرایی آنها در تعیین زمان لازم برای صدورِگواهی، برای دامنه‌شمولِISMS سازمان‌های مشتری، با اندازه و پیچیدگی‌های متفاوت و در طیف وسیعی از فعالیت‌ها، ارائه می‌کند.

نهادهای گواهی‌کننده نیاز دارند مدت زمانی را که برای ممیزی اولیه صدورگواهی، ممیزی بازبینی و ممیزی صدورگواهی مجدد برای هر مشتری و ISMS گواهی شده قبلی صرف می‌شود، تعیین نمایند. استفاده از این پیوست در فاز طرح‌ریزی ممیزی می‌تواند منجر به رویکرد باثباتی برای تعیین زمان مناسب ممیزی شود. در عین حال، راهنمایی که در این پیوست ارائه می‌شود از انعطاف پذیری بر اساس یافته‌های دوره ممیزی، بخصوص در مرحله اول و همچنین پیچیدگی دامنه‌شمول ISMS، برخوردار است.

پ-۲ روش اجرایی تعیین زمان ممیزی

تجربه نشان داده است که دامنه‌شمول ISMS، تعداد کارکنان (همان‌گونه که در جدول پ-۳ نشان داده شده است)، ابعاد، ویژگی‌ها، پیچیدگی‌ها و میزان اهمیت ریسک‌های بالقوه امنیت اطلاعات (همان‌گونه که با جزئیات در زیر تشریح شده‌اند) در میزان زمان ممیزی ISMS تعیین کننده خواهند بود. بند IS 9.1.3 و همچنین بندهای IS 9.2.3.1، IS 9.2.3.2 و IS 9.2.3.3 فهرستی از معیارهایی که توصیه می‌شود در هنگام تعیین زمان مورد نیاز برای ممیزی در نظر گرفته شوند را ارائه می‌کند. این عوامل و عوامل دیگر باید در فرآیند بازنگری قرارداد نهاد گواهی‌کننده مورد بررسی قرار گیرند، زیرا از پیامد بالقوه‌ای بر میزان زمان تخصیص داده شده برای ممیزی، برخوردار هستند.

شایان ذکر است که توصیه شود، تمامی این عوامل برای تعیین زمان ممیزی لحاظ شوند و جدول زمانی ممیز، که در پ -۳ آورده شده است، نمی‌تواند به صورت جداگانه به کار برده شود. مثالهای زیر عواملی را که می‌توانند میزان زمان ممیزی را تحت تاثیر قرار دهند نشان می‌دهد و همچنین عوامل ذکر شده در بند IS9.1.3 را شرح می‌دهند.

- عوامل مرتبط با ابعاد دامنه‌شمول ISMS (برای‌مثال تعداد سیستم‌های اطلاعاتی مورد استفاده، حجم اطلاعات پردازش‌شده، تعداد کاربران، تعداد کاربران با اختیارات ویژه، تعداد بسترهای فن‌آوری اطلاعات، تعداد شبکه‌ها و ابعاد آنها)؛

- عوامل مرتبط با پیچیدگی ISMS (برای‌مثال حیاتی‌بودن سیستم‌های اطلاعاتی، موقعیت ریسک ISMS حجم و نوع اطلاعات حساس و حیاتی که مورد استفاده قرارگرفته و پردازش می‌شوند، تعداد و نوع تراکنش‌های الکترونیکی، تعداد و ابعاد پروژه‌های بهبود، وسعت فعالیت‌های از راه‌دور، وسعت مستندات ISMS)؛
- نوع/ انواع کسب‌وکار انجام پذیرفته در دامنه‌شمول ISMS و الزامات امنیتی، قانونی، مقرراتی، قراردادی و تجاری مرتبط با آن نوع کسب‌وکار؛
- وسعت و گوناگونی فن‌آوری به‌کارگرفته شده در پیاده‌سازی اجزای مختلف ISMS (مانند کنترل‌های پیاده‌سازی شده، مستندسازی و/یا کنترل فرآیند، اقدام اصلاحی/پیشگیرانه، سیستم‌های اطلاعاتی، سیستم‌های فن‌آوری اطلاعات، شبکه‌ها، برای‌مثال آیا ثابت، متحرک، بی‌سیم، بیرونی و یا داخلی هستند.)؛
- تعداد سایت‌های موجود در دامنه‌شمول ISMS؛ تا چه اندازه این سایت‌ها مشابه یا متفاوت هستند، و آیا تمامی این سایت‌ها یا فقط یک نمونه از آنها مورد ممیزی قرار خواهند گرفت؛
- عملکرد اثبات‌شده قبلی ISMS؛
- وسعت برون‌سپاری و توافقات شخص‌سوم استفاده شده در دامنه‌شمول ISMS و همچنین وابستگی به این خدمات؛
- استانداردها، قوانین و مقرراتی که برای صدور گواهی بکار گرفته می‌شوند و هر الزامات مختصِ‌بخش که ممکن است بکار گرفته شود.

صدورگواهی ISMS به طور معمول بیشتر از صدر گواهی سیستم مدیریت کیفیت یا سیستم مدیریت محیط زیست طول می‌کشد و این به علت افزایش الزامات یک سیستم مدیریت امنیت اطلاعات به ازای یک درخواست مشخص برای ISMS است، مانند: خط‌مشی ISMS، مدیریت ریسک و کنترل‌ها و اهداف کنترلی ISMS. نهاد گواهی‌کننده لازم است:

الف- صحت و ثبات شیوه‌ای را که به وسیله آن؛ سازمان مشتری میزان اهمیت ریسک‌های امنیت اطلاعات و پیامدهای آن را تعیین می‌کند، مورد ممیزی قرار دهد؛

ب- تایید کند که سیستم طراحی شده برای دستیابی به انطباق (با همه قوانین و الزامات دیگری که در ISMS بکار گرفته می‌شوند) از قابلیت لازم برخوردار بوده و این سیستم پیاده‌سازی شده و نگهداری می‌شود؛

پ- تایید کند که اهداف کنترلی و کنترل‌ها به درستی انتخاب و پیاده‌سازی شده‌اند و میزان اثربخشی آنها اندازه‌گیری می‌شود و فرآیند دستیابی به «پیشگیری از رخدادهای‌امنیتی و پاسخ مناسب به آنها» درست و مناسب است؛

ت- تایید کند که الزامات مدارک ISMS سازمان مشتری به درستی برآورده شده‌اند؛

ث- به افزایش درخواست‌هایی که از ممیزی مرحله اول ایجاد می‌شوند واکنش نشان دهد.

پ-۳ جدول زمانی ممیز

پ-۳-۱ کلی

جدول زمانی ممیز که در زیر آورده شده است، میانگینی از تعداد روزهای ممیزی اولیه ارائه می‌کند (در اینجا و از این‌به‌بعد، این تعداد شامل روزهای ممیزی مرحله اول و ممیزی مرحله دوم می‌شود)، که تجربه نشان داده است برای دامنه‌شمول ISMS با تعداد کارکنان مشخص مناسب است. تجربه همچنین اثبات کرده است که برای دامنه‌های شمول ISMS با ابعاد مشابه برخی نیاز به زمان کمتر و برخی به زمان بیشتر نیاز دارند.

تغییرات زمانِ صرف‌شده برای صدور هر گواهی، بستگی به تعدادی از عوامل شامل ابعاد، دامنه‌شمول ممیزی، تدارکات، پیچیدگی سازمان و آمادگی آن برای انجام ممیزی دارد (همچنین به پ-۲ رجوع شود). این عوامل و عوامل دیگر لازم است در فرآیند بازنگری قرارداد نهاد گواهی‌کننده مورد بررسی قرار گیرند، زیرا از پیامد بالقوه‌ای بر میزان زمان تخصیص داده شده برای ممیزی برخوردار هستند. بنابراین جدول زمانی ممیز نمی‌تواند جدا از این عوامل مورد استفاده قرار گیرد.

جدول‌زمانی ممیز که در زیر ارائه شده‌است، چارچوبی فراهم می‌آورد، که با استفاده از تعیین یک نقطه آغاز براساس مجموع تعدادکارکنان درتمامی نوبت‌های‌کاری و تنظیم و تغییر آن براساس عوامل‌مهم‌موثر بر دامنه‌شمول ISMS موردممیزی و تخصیص یک‌وزن جمع‌شونده یا کم‌شونده جهت اصلاح عددپایه، می‌تواند در طرح‌ریزی ممیزی مورداستفاده قرارگیرد. اصطلاحات استفاده‌شده در این جدول در پ-۳-۲ ارائه شده‌اند.

جدول زمانی ممیز

تعداد کارکنان	زمان QMS[1] برای ممیزی اولیه (روزهای ممیز)	زمان ممیز EMS[2] برای ممیزی اولیه (روزهای ممیز)	زمان ممیز ISMS برای ممیزی اولیه (روزهای ممیز)	عوامل جمع‌شونده و کم‌شونده	زمان کل ممیزی
۱~۱۰	۲	۳	۵	به پیوست پ-۲ رجوع شود	
۱۱~۲۵	۳		۷	به پیوست پ-۲ رجوع شود	
۲۶~۴۵	۴	۶	۸.۵	به پیوست پ-۲ رجوع شود	
۴۶~۶۵	۵		۱۰	به پیوست پ-۲ رجوع شود	
۶۶~۸۵	۶		۱۱	به پیوست پ-۲ رجوع شود	

1- Quality Management Systems

سیستم‌های مدیریت کیفیت

2- Environmental Management Systems

سیستم‌های مدیریت زیست‌محیطی

۸۶~۱۲۵	۷	۸	۱۲	به پیوست پ-۲ رجوع شود	
۱۲۶~۱۷۵	۸		۱۳	به پیوست پ-۲ رجوع شود	

جدول زمانی ممیز- ادامه

تعداد کارکنان	زمان QMS برای ممیزی اولیه (روزهای ممیز)	زمان ممیز EMS برای ممیزی اولیه (روزهای ممیز)	زمان ممیز ISMS برای ممیزی اولیه (روزهای ممیز)	عوامل جمع‌شونده و کم‌شونده	زمان کل ممیزی
۱۷۶~۲۷۵	۹		۱۴	به پیوست پ-۲ رجوع شود	
۲۷۶~۴۲۵	۱۰		۱۵	به پیوست پ-۲ رجوع شود	
۴۲۶~۶۲۵	۱۱	۱۲	۱۶.۵	به پیوست پ-۲ رجوع شود	
۶۲۶~۸۷۵	۱۲		۱۷.۵	به پیوست پ-۲ رجوع شود	
۸۷۶~۱۱۷۵	۱۳		۱۸.۵	به پیوست پ-۲ رجوع شود	
۱۱۷۶~۱۵۵۰	۱۴		۱۹.۵	به پیوست پ-۲ رجوع شود	
۱۵۵۱~۲۰۲۵	۱۵	۱۸	۲۱	به پیوست پ-۲ رجوع شود	
۲۰۲۶~۲۶۷۵	۱۶		۲۲	به پیوست پ-۲ رجوع شود	
۲۶۷۶~۳۴۵۰	۱۷		۲۳	به پیوست پ-۲ رجوع شود	
۳۴۵۱~۴۳۵۰	۱۸		۲۴	به پیوست پ-۲ رجوع شود	
۴۳۵۱~۵۴۵۰	۱۹		۲۵	به پیوست پ-۲ رجوع شود	
۵۴۵۱~۶۸۰۰	۲۰		۲۶	به پیوست پ-۲ رجوع شود	
۶۸۰۱~۸۵۰۰	۲۱		۲۷	به پیوست پ-۲ رجوع شود	
۸۵۰۱~۱۰۷۰۰	۲۲		۲۸	به پیوست پ-۲ رجوع شود	
>۱۰۷۰۰	روند بالا ادامه یابد		روند بالا ادامه یابد	به پیوست پ-۲ رجوع شود	

پ-۳-۲ توضیح اصطلاحات

«کارکنان» که در جدول زمانی ممیز به آن ارجاع شده است، اشاره به تمامی افرادی دارد که فعالیت‌های کاری‌شان به دامنه‌شمول ISMS مرتبط است. کل تعداد کارکنان در تمامی نوبت‌های کاری نقطه آغازی برای تعیین زمان ممیزی است.

تعداد اثربخش کارکنان شامل: کارکنان غیر رسمی(فصلی، موقت و یا پیمانی) که در زمان ممیزی حضور دارند، می‌شود. توصیه می‌شود، نهاد گواهی‌کننده با سازمان مشتری ممیزی شونده بر سر زمان‌بندی ممیزی، که به بهترین وجه نمایانگر دامنه‌شمول کامل سازمان است، توافق کند. موارد توافق می‌تواند شامل فصل، ماه، روز/تاریخ و نوبت کاری برحسب مورد باشد.

توصیه می‌شود، با کارکنان نیمه وقت نیز مشابه کارکنان تمام وقت رفتار شود. این تصمیم بستگی به تعداد ساعات کاری آنها درمقایسه با کارکنان تمام وقت دارد.

«زمان ممیز» شامل زمانی است که یک ممیز یا تیم ممیزی در، ممیزی مرحله‌اول، ممیزی مرحله‌دوم و مرحله طرح‌ریزی (شامل بازنگری خارج از محل مدارک در صورت نیاز)؛ برقراری ارتباط با سازمان، کارکنان، سوابق، مستندات و فرآیند؛ و نوشتن گزارش، صرف می‌نماید. انتظار می‌رود که «زمان ممیز»، که شامل تلفیقی از زمان برای طرح‌ریزی و نوشتن گزارش است، به طور معمول، مجموع «زمان ممیز» برای حضور در محل را به کمتر از ۷۰٪ زمان نشان داده شده در جدول کاهش ندهد. در جایی که زمان بیشتری برای طرح‌ریزی و/ یا نوشتن گزارش لازم است، انجام این امور توجیه مناسبی برای کاهش میزان زمان ممیز برای حضور در محل نیست. زمان سفر ممیز در محاسبات لحاظ نمی‌شود، و به زمان ممیز که در جدول به آن اشاره شده است اضافه می‌شود.

یادآوری ۱- عدد ۷۰٪ براساس تجربیات ممیزی ISMS بدست آمده است.

اگر از روش‌های ممیزی راه‌دور مانند: همکاری تعاملی از طریق وب، جلسات از طریق وب، تله کنفرانس و/ یا تصدیق الکترونیکی فرآیندهای سازمان برای ارتباط با سازمان استفاده می‌شود؛ توصیه می‌شود، این فعالیت‌ها در طرح ممیزی (به بند IS 9.1.5 رجوع شود) شناسایی شده و می‌تواند به عنوان ملحقات جزئی «زمان ممیز برای حضور در محل» لحاظ شود.

اگر نهاد گواهی‌کننده یک طرح ممیزی را طرح‌ریزی می‌کند که در آن، فعالیت‌های ممیزی راه‌دور بیش از ۳۰٪ زمان برنامه‌ریزی شده برای حضور در محل را تشکیل می‌دهد، توصیه می‌شود نهاد گواهی‌کننده طرح ممیزی را توجیه کرده و مجوزهای خاص را از نهاد تاییدصلاحیت پیش از اجرا اخذ نماید.

یادآوری ۲- منظور از زمان ممیز برای حضور در محل، زمانی است که ممیز برای بازدید از تک‌تک سایت‌ها در محل تخصیص می‌دهد. ممیزی‌های الکترونیکی سایت‌های راه‌دور، ممیزی‌های از راه‌دور لحاظ می‌شوند، حتی اگر ممیزی‌های الکترونیکی از نظر فیزیکی در محل سازمان انجام شود.

«زمان ممیز»، همان‌گونه که در جدول نیز به آن اشاره شده است، برحسب «روزهای ممیز» که در ممیزی صرف می‌شود بیان می‌شود. «روز ممیز» به طور معمول یک روز کاری عادی کامل است.

برای چرخه ممیزی اولیه صدورگواهی، توصیه می‌شود، زمان بازبینی یک سازمان متناسب با زمان صرف شده برای ممیزی اولیه آن به همراه مجموع زمان صرف شده سالیانه برای بازبینی باشد، که در حدود ۱/۳ زمان ممیزی اولیه است. توصیه می‌شود، زمان بازبینی طرح‌ریزی‌شده هر از چندگاهی، با در نظر گرفتن تغییرات سازمان، تکامل سیستم و غیره و دست‌کم در زمان ممیزی‌صدورگواهی‌مجدد، مورد بازنگری قرار گیرد.
کل زمان صرف شده برای اجرای ممیزی‌صدورگواهی‌مجدد به یافته‌های بازنگری، که در بند IS 9.1.6 این استاندارد و بند ۹-۴ از استاندارد ISO/IEC 17021 تعریف شده‌اند، بستگی خواهد داشت. توصیه می‌شود، زمان صرف شده در ممیزی‌صدورگواهی‌مجدد متناسب با زمان ممیزی اولیه صدورگواهی برای آن سازمان بوده و توصیه می‌شود، در حدود ۲/۳ زمانی باشد که برای ممیزی اولیه صدورگواهی همان سازمان مورد نیاز بوده است. زمان ممیزی‌صدورگواهی‌مجدد بیشتر و فراتر از زمان بازبینی معمولی است، ولی زمانی‌که ممیزی‌صدورگواهی‌مجدد انجام می‌شود و همزمان با آن باید برنامه زمان‌بندی بازدید معمول نظارتی انجام گیرد، ممیزی‌صدورگواهی‌مجدد برای پوشش الزامات بازبینی کفایت می‌کند. صرف‌نظر از نتیجه‌نهایی که بدست می آید، راهنمایی موجود در IS 9.1.2 بکار گرفته می‌شود.
زمانی‌که نقطه آغاز جهت تعیین زمان لازم ممیز، برای دامنه‌شمول معمول ISMS، با استفاده از تعداد کارکنان مشخص گردید؛ به‌علت تفاوتهایی که ممکن است زمانِ واقعیِ ممیز را برای اجرای ممیزی اثربخش در یک ISMS خاصِ موردممیزی، تحت تاثیر قرار دهد؛ علاوه بر آنهایی که در پ-۲ بیان شد، برخی اصلاحات دیگر نیز نیاز است تا در این زمان‌بندی لحاظ شوند.

از عوامل نمونه که به زمان ممیز بیشتری نیاز دارند، می‌توان به موارد زیر اشاره کرد:

- تدارکات پیچیده شامل قرارداشتن بیش از یک ساختمان یا مکان در دامنه‌شمول ISMS؛
- کارکنانی که به بیش از یک زبان صحبت می‌کنند (نیاز به مترجم وجود دارد یا مانع از فعالیت مستقل ممیزان می‌شود)؛
- مقررات سطح بالا؛
- ISMS، فرآیندهای بسیار پیچیده یا تعداد زیادی فعالیت‌های نسبتاً منحصر به فرد را در بر می‌گیرد؛
- فرآیندها، شامل تلفیقی از سخت افزار، نرم افزار، فرآیند و خدمت هستند؛
- فعالیت‌هایی که نیازمند بازدید از سایت‌های موقت برای تایید فعالیت‌های سایت‌های دائمی هستند که سیستم مدیریت‌شان موضوع گواهی است (یادآوری ۳ ملاحظه شود).

از عوامل نمونه که اجازه کاهش زمان ممیز را می دهند، می‌توان به موارد زیر اشاره کرد:

- فرآیندها/ محصول با ریسک کم/ بدون ریسک؛
- دانش قبلی از سازمان(برای مثال، در صورتیکه سازمان قبلاً از سوی همین نهاد گواهی‌کننده برای استاندارد دیگری گواهی اخذ کرده باشد)؛

- آمادگی مشتری برای صدور گواهی(برای مثال، قبلاً در برنامه شخص‌سوم دیگری گواهی اخذکرده‌است یا به‌رسمیت شناخته شده است.)؛
- فرآیندها شامل یک فعالیت عمومی واحد باشد.(برای‌مثال صرفاً خدمت)؛
- تکامل سیستم مدیریت در محل؛
- درصد بالایی از کارکنان اعمال ساده و یکسانی را انجام دهند.

یادآوری ۳- در مواقعی‌که مشتری‌گواهی یا سازمان‌دارنده‌گواهی، محصولات یا خدمت خودرا در سایت‌های‌موقت عرضه‌می‌کنند، مساله ارزشیابی چنین سایت‌هایی در برنامه‌های ممیزی‌صدورگواهی یا برنامه‌های بازبینی از اهمیت زیادی برخوردارمی‌شود.

سایت‌های موقت مکان‌هایی هستند به غیر از سایت‌ها یا مکان‌هایی که در مدرک صدورگواهی مشخص شده‌اند که در آنها فعالیت‌هایی، در حوزه دامنه‌شمول گواهی، در مدت زمانی تعیین‌شده انجام می‌پذیرد. گستره این سایت‌ها از سایت‌های مهم مدیریت پروژه گرفته تا سایت‌های کم اهمیت خدمات‌رسانی یا نصب می‌تواند تغییر کند. توصیه می‌شود، نیاز به بازدید این سایت‌ها و همچنین وسعت نمونه‌گیری‌ها، براساس ارزشیابی ریسک‌هایِ‌نقصِ یک محصول یا خدمت در برآورده‌سازی نیازها/ انتظارات به‌دلیل عدم‌انطباق‌سیستم، انجام شود. توصیه می‌شود، نمونه‌های انتخابی از سایت‌ها دربرگیرنده گستره تغییرات خدمات و نیازهای تکاملی سازمان بوده و ابعاد و نوع فعالیت‌ها و همچنین مراحل مختلف پروژه‌های در حال انجام را نیز لحاظ کند.

توصیه می‌شود تمامی مشخصه‌های دامنه‌شمول ISMS، فرآیندها و محصولات/ خدمات، درنظر گرفته شده، و یک تعدیل منصفانه برای آن عوامل اعمال شود، که می‌توانند کم‌وبیش، زمان ممیز برای یک ممیزی اثربخش را توجیه کنند. عوامل جمع‌شونده ممکن است خارج از محل[1] و به همراه عوامل کم‌شونده باشند. در تمامی مواردی که تغییرات در جدول زمان‌بندی ممیز انجام می‌شود، باید شواهد و سوابق کافی که این تغییرات را توجیه می‌کنند، حفظ و نگهداری شوند.

شکل‌زیر تعاملات‌بالقوه عوامل‌جمع‌شونده و کم‌شونده در زمان‌ممیز که درجدول بالا به آنها اشاره‌شد را نشان‌می‌دهد.

\- پیچیدگی سازمان/ سیستم +

بزرگ ساده	**بزرگ پیچیده**
چند سایتی	چند سایتی
تعداد کمی فرآیند(پردازش)	فرآیندهای زیاد
فرآیندهای تکراری	دامنه‌شمول بزرگ
دامنه‌شمول کوچک	فرآیندهای منحصر به فرد
	فرآیندها و محصولات با ریسک بالا

نقطه آغاز از جدول زمان ممیز

1- Off-site

تعداد کمی فرآیند دامنه‌شمول کوچک فرآیندهای تکراری **کوچک ساده**	فرآیندهای زیاد فرآیندها و محصولات با ریسک بالا دامنه‌شمول بزرگ فرآیندهای منحصر به فرد **کوچک پیچیده**

پراکندگی سازمان
- +

پیوست ت
(اطلاعاتی)
راهنمایی برای بازنگری کنترل‌های پیاده‌سازی شده از پیوست الف استاندارد ۲۷۰۰۱

ت-۱ هدف

این پیوست راهنمایی را برای بازنگری پیاده‌سازی کنترل‌های لیست شده در پیوست الف استاندارد ۲۷۰۰۱، و جمع‌آوری شواهد ممیزی[1] از عملکرد آنها در حین ممیزی اولیه و بازدیدهای نظارتی بعدی بدست می‌دهد. لازم است، پیاده‌سازی تمام کنترل‌های انتخابی بوسیله سازمان مشتری برای ISMS (که در بیانیه کاربردپذیری به آنها اشاره شده است) در مرحله دوم ممیزی اولیه و در طول فعالیت‌های بازبینی یا صدور مجدد گواهی مورد بازنگری قرار گیرند.

شواهد ممیزی که نهاد گواهی‌کننده جمع‌آوری می‌کند باید به‌اندازه‌ای باشد که بتوان از آنها نتیجه‌گیری نهایی نمود که آیا کنترل‌های پیاده‌سازی شده اثربخش هستند یا خیر. اینکه از یک کنترل چه عملکردی انتظار می‌رود، در روش‌های اجرایی یا خط‌مشی‌های سازمان مشتری که در بیانیه کاربردپذیری بیان‌شده یا به آنها ارجاع داده شده است مشخص می‌شود. واضح است که آن دسته از کنترل‌هایی که در خارج از دامنه‌شمول ISMS قرار دارند، ممیزی نخواهند شد.

ت-۱-۱ شواهد ممیزی

با کیفیت ترین شواهد ممیزی از طریق مشاهدات ممیز جمع‌آوری می‌شوند. (برای‌مثال، اینکه یک درِ قفل شده، قفل است، افراد توافقهای محرمانگی امضا می‌کنند، ثبت دارایی وجود دارد و شامل اموال رویت شده می‌شود، تنظیمات سیستم‌ها کافی هستند و غیره) . شواهد می‌توانند از طریق مشاهده نتایج اجرایی یک کنترل (برای‌مثال نسخه چاپی حقوق دسترسی داده شده به افراد، که بوسیله مراجع‌دارای‌اختیار امضا شده‌اند، سوابق رسیدگی به رخدادها، فرآیند مجوزدهی‌ها، که بوسیله مراجع‌دارای‌اختیار امضا شده‌اند، صورتجلسات جلسات مدیریتی یا جلسات دیگر)، بدست می آیند. شواهد همچنین می‌توانند نتیجه آزمون مستقیم(یا اجرایِ‌مجدد) کنترل‌ها بوسیله ممیز باشند (برای‌مثال تلاش برای انجام عملی که از نظر کنترل‌ها نباید انجام شود، تعیین اینکه آیا نرم افزاری برای محافظت در برابر کدهای مخرب روی دستگاه نصب شده و به روز است یا خیر، حقوق دسترسی اعطا شده است یا خیر (البته بعد از بررسی مراجع‌دارای‌اختیار) و غیره). شواهد را می‌توان از طریق مصاحبه با کارکنان/پیمانکاران درباره فرآیندها و کنترل‌ها و تعیین صحت و سقم آنها، جمع‌آوری کرد.

1- Audit evidence

ت-۲ چگونگی استفاده از جدول د-۱

ت-۲-۱ ستونهای «کنترل سازمانی» و «کنترل فنی»

علامت «×» در ستون متناظر نشانگر این مطلب است که کنترل مربوطه سازمانی یا فنی است. از آنجایی‌که برخی کنترل‌ها هم سازمانی و هم فنی هستند، این علامت در هردو ستون مربوط به آن کنترل درج شده است.

شواهد اجرایی کنترل‌های سازمانی می‌توانند از طریق بازنگری سوابق اجرایی کنترل‌ها، مصاحبه، مشاهده و بازرسی فیزیکی جمع‌آوری شوند. شواهد اجرایی کنترل‌های فنی می‌توانند از طریق آزمون سیستم (بند بعد ملاحظه شود) یا با استفاده از ابزار تخصصی ممیزی/ گزارش‌دهی جمع‌آوری شوند.

ت-۲-۲ ستون « آزمون سیستم[1]»

«آزمون سیستم» به معنی بازنگری مستقیم سیستم است (برای‌مثال بازنگری تنظیمات سیستم یا پیکربندی). سوالات ممیز ممکن است در پایانه‌نمایش‌سیستم[2] یا از طریق ارزشیابی نتایج بدست آمده از ابزار آزمون پاسخ داده شود. اگر سازمان مشتری از ابزار رایانه‌ای استفاده می‌کند که برای ممیز شناخته شده است، این موضوع می‌تواند پشتیبان ممیزی باشد یا نتایج بدست آمده از ارزشیابی انجام شده بوسیله سازمان مشتری (یا پیمانکاران فرعی آن) می‌تواند بازنگری شود.

دو رده برای بازنگری کنترل‌های فنی وجود دارند:

امکان‌پذیر: آزمون سیستم برای ارزشیابی پیاده‌سازی کنترل امکان‌پذیر است ولی معمولا لازم نیست.

پیشنهادی: آزمون سیستم معمولا لازم است.

ت-۲-۳ ستون «بازرسی چشمی»

«بازرسی چشمی» به این معنی است که این کنترل‌ها معمولا نیازمند بازرسی چشمی در محل برای ارزشیابی اثربخشی‌شان هستند این به‌این‌معنی است که بازنگری مستندات کاغذی مربوطه یا انجام مصاحبه‌ها به تنهایی کفایت نمی‌کند - ممیز نیاز دارد که کنترل را در محلی که پیاده‌سازی می‌شود، تصدیق کند.

ت-۲-۴ ستون «راهنمایی بازنگری ممیزی»

در جایی‌که امکان دارد وجود راهنمایی برای ممیزی یک کنترل مشخص راهگشا باشد، ستون «توضیحات» حوزه تمرکز برای ارزشیابی آن کنترل را به عنوان راهنمایی بیشتر برای ممیز بدست می‌دهد.

1- System testing
2- System console

جدول د-۱- طبقه‌بندی کنترل‌ها

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۵ خط‌مشی امنیتی					
الف-۵-۱ خط‌مشی امنیتی					
الف-۵-۱- ۱ مدرک خط‌مشی امنیت اطلاعات	×				
الف-۵-۱-۲ بازنگری خط‌مشی امنیت اطلاعات	×				صورتجلسه های بازنگری مدیریت.
الف-۶ سازمان امنیت اطلاعات					
الف-۶-۱ سازمان داخلی					
الف-۶-۱-۱ تعهد مدیریت به امنیت اطلاعات	×				صورتجلسه های جلسات مدیریت
الف-۶-۱-۲ هماهنگی امنیت اطلاعات	×				صورتجلسه های جلسات مدیریت.
الف-۶-۱-۳ تخصیص مسوولیتهای امنیت اطلاعات	×				
الف-۶-۱-۴ فرایند مجوزدهی برای امکانات پردازش اطلاعات	×				
الف-۶-۱-۵ توافق‌نامه‌های محرمانگی	×				چند کپی از فایل‌ها به عنوان نمونه برداشته شود.
الف-۶-۱-۶ برقراری ارتباط‌با مراجع‌دارای‌اختیار	×				
الف-۶-۱-۷ برقراری ارتباط با گروههای بامنافع خاص	×				
الف-۶-۱-۸ بازنگری مستقل امنیت اطلاعات	×				گزارشات خوانده شود
الف-۶-۲ اشخاص بیرونی					
الف-۶-۲-۱ شناسایی ریسک‌ها مرتبط با اشخاص بیرونی	×				
الف-۶-۲-۲ نشانی دهی امنیت هنگام سرو کار داشتن با مشتریان	×				
الف-۶-۲-۳ نشانی‌دهی امنیت در توافق‌های شخص‌سوم	×				برخی از شرایط قراردادها آزمون شود.
الف-۷ مدیریت دارایی					
الف-۷-۱ مسوولیت داراییها					
الف-۷-۱-۱ سیاهه اموال	×				دارایی‌ها شناسایی شوند
الف-۷-۱-۲ مالکیت داراییها	×				
الف-۷-۱-۳ استفاده پسندیده از داراییها	×				
الف-۷-۲ طبقه بندی اطلاعات					
الف-۷-۲-۱ راهنمایی‌های طبقه بندی	×				
الف-۷-۲-۲ برچسب‌گذاری و اداره‌کردن‌اطلاعات	×				نام‌گذاری: دایرکتوریها، فایل‌ها، گزارشات چاپ شده، رسانه های ضبط شده(برای‌مثال نوارها، دیسکها و لوحهای فشرده)، پیامهای الکترونیکی و انتقال فایل‌ها.

جدول د-۱- ادامه

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۸ امنیت منابع انسانی					چند فایل منابع انسانی به‌عنوان نمونه برداشته شود.
الف-۸-۱ پیش از اشتغال					
الف-۸-۱-۱ نقش‌ها و مسوولیتها	×				
الف-۸-۱-۲ گزینش	×				
الف-۸-۱-۳ ضوابط و شرایط استخدام	×				
الف-۸-۲ حین خدمت					
الف-۸-۲-۱ مسوولیتهای مدیریت	×				
الف-۸-۲-۲ آگاهی رسانی، تحصیل و آموزش امنیت اطلاعات	×				پرسش ازکارکنان مبنی‌براینکه آیا از مواردی‌مشخصی که توصیه‌می‌شود آگاه‌باشند، مطلع‌هستند یا خیر.
الف-۸-۲-۳ فرآیند انضباطی	×				
الف-۸-۳ خاتمه استخدام یا تغییر در شغل					
الف-۸-۳-۱ مسوولیتهای خاتمه خدمت	×				
الف-۸-۳-۲ عودت دارایی‌ها	×				
الف-۸-۳-۳ حذف حقوق دسترسی	×	×	پیشنهادی		
الف-۹ امنیت فیزیکی و محیطی					
الف-۹-۱ نواحی امن					
الف-۹-۱-۱حصار امنیت فیزیکی	×				
الف-۹-۱-۲ کنترل‌های مداخل فیزیکی	×	×	امکان‌پذیر	×	آرشیو کردن سوابق دسترسی
الف-۹-۱-۳ ایمن سازی دفاتر،اتاقها وامکانات	×			×	
الف-۹-۱-۴ محافظت در برابر تهدید های بیرونی و محیطی	×			×	
الف-۹-۱-۵ کار در نواحی امن	×			×	
الف-۹-۱-۶ دسترسی عمومی، نواحی تحویل و بارگیری	×			×	
الف-۹-۲ امنیت تجهیزات					
الف-۹-۲-۱ استقرار و حفاظت تجهیزات	×	×	امکان‌پذیر	×	
الف-۹-۲-۲ امکانات پشتیبانی	×	×	امکان‌پذیر	×	
الف-۹-۲-۳ امنیت کابل کشی	×			×	
الف-۹-۲-۴ نگهداری تجهیزات	×				
الف-۹-۲-۵ امنیت تجهیزات خارج از ابینه	×	×	امکان‌پذیر		رمزنگاری وسایل قابل حمل
الف-۹-۲-۶ امحاء یا استفاده مجدد از تجهیزات به صورت ایمن	×	×	امکان‌پذیر	×	
الف-۹-۲-۷ از رده خارج‌کردن دارائی	×				
الف-۱۰ مدیریت ارتباطات و عملکرد					
الف-۱۰-۱ روش‌های‌اجرایی‌عملیاتی‌ومسوولیت‌ها					

جدول د-۱- ادامه

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۱۰-۱-۱روش‌های اجرایی عملیاتی مستندشده	×				
الف-۱۰-۱-۲ مدیریت تغییر	×	×	پیشنهادی		
الف-۱۰-۱-۳ تفکیک وظایف	×				
الف-۱۰-۱-۴ جداسازی امکانات بهبود، آزمون و عملیاتی	×	×	امکان‌پذیر		
الف-۱۰-۲ مدیریت تحویل خدمت شخص‌سوم					
الف-۱۰-۲-۱ تحویل خدمت	×				
الف-۱۰-۲-۲ پایش و بازنگری خدمات شخص‌سوم	×	×	امکان‌پذیر		
الف-۱۰-۲-۳ مدیریت تغییرات در خدمات شخص‌سوم	×				
الف-۱۰-۳ طرح‌ریزی و پذیرش سیستم					
الف-۱۰-۳-۱ مدیریت ظرفیت	×	×	امکان‌پذیر		
الف-۱۰-۳-۲ پذیرش سیستم	×				
الف-۱۰-۴ حفاظت در برابر کدهای مخرب‌وسیار					
الف-۱۰-۴-۱ کنترل‌هایی در برابر کدهای‌مخرب	×	×	پیشنهادی		چند نمونه از سرورها، رایانه ها و دروازه های ورود.
الف-۱۰-۴-۲ کنترل‌هایی در برابر کدهای سیار	×	×	امکان‌پذیر		
الف-۱۰-۵ نسخ پشتیبان					
الف-۱۰-۵-۱ ایجاد پشتیبان از اطلاعات	×	×	پیشنهادی		یک بار اطلاعات را بازگردانی کنید.
الف-۱۰-۶ مدیریت امنیت شبکه					
الف-۱۰-۶-۱ کنترل های شبکه	×	×	امکان‌پذیر		
الف-۱۰-۶-۲ امنیت خدمات شبکه	×				خصوصیات امنیتی، SLA ها[1]
الف-۱۰-۷ اداره کرده محیط های ذخیره سازی					
الف-۱۰-۷-۱ مدیریت محیط های ذخیره سازی قابل جابجایی	×	×	امکان‌پذیر		
الف-۱۰-۷-۲ امحای محیط های ذخیره سازی	×				
الف-۱۰-۷-۳ روش‌های‌اجرایی جابجایی‌اطلاعات	×				
الف-۱۰-۷-۴ امنیت مستندات سیستم	×	×	امکان‌پذیر	×	
الف-۱۰-۸ تبادل اطلاعات					
الف-۱۰-۸-۱ خط‌مشی ها و روش‌های اجرایی تبادل اطلاعات	×				
الف-۱۰-۸-۲ توافق‌نامه‌های تبادل	×				

1- Service Level Agreements

جدول د-۱- ادامه

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۱۰-۸-۳ محیط های ذخیره سازی(رسانه) فیزیکی، حین حمل و نقل	×	×	امکان‌پذیر		حفاظتهای فیزیکی یا رمزنگاری
الف-۱۰-۸-۴ پیام رسانی الکترونیکی	×	×	امکان‌پذیر		تطابق پیامهای نمونه با خط‌مشی/ روش‌های اجرایی تایید شود.
الف-۱۰-۸-۵ سیستم‌های اطلاعاتی کسب‌وکار	×				
الف-۱۰-۹ خدمات تجارت الکترونیک					
الف-۱۰-۹-۱ تجارت الکترونیک	×	×	امکان‌پذیر		
الف-۱۰-۹-۲ تراکنش‌های برخط (متصل و مستقیم)	×	×	پیشنهادی		تمامیت و مجوزهای دسترسی بررسی شوند.
الف-۱۰-۹-۳ اطلاعات قابل‌دسترس عموم	×	×	امکان‌پذیر		
الف-۱۰-۱۰ پایش					
الف-۱۰-۱۰-۱ واقعه نگاری ممیزی	×	×	امکان‌پذیر		برخط یا چاپی
الف-۱۰-۱۰-۲ پایش کاربرد سیستم	×	×	امکان‌پذیر		
الف-۱۰-۱۰-۳ حفاظت‌از اطلاعات‌ثبت‌شده‌وقایع	×	×	امکان‌پذیر		
الف-۱۰-۱۰-۴ اطلاعات ثبت‌شده وقایع مربوط‌به متولی سیستم[1] و کاربر	×	×	امکان‌پذیر		
الف-۱۰-۱۰-۵ واقعه نگاری خرابی	×				
الف-۱۰-۱۰-۶ هم زمان سازی ساعتها		×	امکان‌پذیر		
الف-۱۱ کنترل دسترسی					
الف-۱۱-۱ الزامات کسب‌وکار برای کنترل دسترسی					
الف-۱۱-۱-۱ خط‌مشی کنترل دسترسی	×				
الف-۱۱-۲ مدیریت دسترسی کاربر					
الف-۱۱-۲-۱ ثبت کاربر	×				نمونه‌هایی از حقوق دسترسی[2] کارکنان و پیمانکاران به تمامی سیستم‌ها بررسی شود.
الف-۱۱-۲-۲ مدیریت اختیارات ویژه	×	×	امکان‌پذیر		انتقال داخلی کارکنان
الف-۱۱-۲-۳ مدیریت کلمه عبور کاربر	×				
الف-۱۱-۲-۴ بازنگری حقوق دسترسی کاربر	×				
الف-۱۱-۳ مسوولیتهای کاربر					
الف-۱۱-۳-۱ استفاده از کلمه عبور	×				تصدیق خط‌مشی/راهنمایی‌ها در محل کاربران
الف-۱۱-۳-۲ تجهیزات بدون مراقبت کاربر	×				تصدیق خط‌مشی/راهنمایی‌ها در محل کاربران
الف-۱۱-۳-۳ خط‌مشی میز پاک و صفحه پاک	×			×	

1- Administrator
2- Access Rights

جدول د-۱- ادامه

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۱۱-۴ کنترل دسترسی به شبکه					
الف-۱۱-۴-۱ خط‌مشی استفاده از خدمات شبکه	×				
الف-۱۱-۴-۲ احراز اصالت کاربر برای اتصالات بیرونی	×	×	پیشنهادی		
الف-۱۱-۴-۳ شناسایی تجهیزات در شبکه ها	×	×			
الف-۱۱-۴-۴ حفاظت از درگاه عیب یابی و پیکربندی راه‌دور	×	×	پیشنهادی		
الف-۱۱-۴-۵ تفکیک در شبکه ها	×	×	امکان‌پذیر		دیاگرام‌های شبکه: WAN,LAN, VLAN, VPN, بخش‌های شبکه، اشیاء شبکه (برای‌مثال DMZ)
الف-۱۱-۴-۶ کنترل اتصال به شبکه	×	×	پیشنهادی		شبکه‌های مشترک زیاد معمول نیست.
الف-۱۱-۴-۷ کنترل مسیریابی در شبکه	×	×	پیشنهادی		دیوارهای‌آتش،سوییچ‌ها/مسیریاب‌ها: براساس قاعده، لیست کنترل دسترسی، خط‌مشی های کنترل دسترسی
الف-۱۱-۵ کنترل دسترسی به سیستم عامل					
الف-۱۱-۵-۱روش‌های اجرایی ورود امن به سیستم	×	×	پیشنهادی		
الف-۱۱-۵-۲ شناسایی و احراز اصالت کاربر	×	×	پیشنهادی		
الف-۱۱-۵-۳ سیستم مدیریت کلمه عبور	×	×	پیشنهادی		
الف-۱۱-۵-۴ استفاده از برنامه‌های کمکی سیستم	×	×	پیشنهادی		
الف-۱۱-۵-۵ خروج زمانی از لایه ارتباطی	×	×	امکان‌پذیر		
الف-۱۱-۵-۶ محدود سازی زمان اتصال	×	×	امکان‌پذیر		
الف-۱۱-۶ کنترل دسترسی به برنامه‌های کاربردی و اطلاعات					
الف-۱۱-۶-۱ محدودیت دسترسی به اطلاعات	×	×	پیشنهادی		
الف-۱۱-۶-۲ جداسازی سیستم‌های حساس	×	×	امکان‌پذیر		
الف-۱۱-۷ محاسبه سیار و کار از راه‌دور					
الف-۱۱-۷-۱ محاسبه و ارتباطات سیار	×	×	امکان‌پذیر		
الف-۱۱-۷-۲ کار از راه‌دور	×	×	امکان‌پذیر		
الف-۱۲ اکتساب، بهبود و نگهداری سیستم‌های اطلاعاتی					
الف-۱۲-۱ الزامات امنیتی سیستم‌های اطلاعاتی					

جدول د-۱- ادامه

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۱۲-۱-۱ مشخصات و تحلیل الزامات امنیتی	×				
الف-۱۲-۲ پردازش صحیح در برنامه‌های کاربردی					
الف-۱۲-۲-۱ صحه‌گذاری داده[1] ورودی	×	×	پیشنهادی		راهنمایی‌های بهبود نرم افزاری، آزمون نرم افزار؛ در برنامه‌های نمونه کاربردی کسب‌وکار تایید می‌کند که کنترل‌های الزامی کاربران در عمل وجود دارند.
الف-۱۲-۲-۲ کنترل پردازش درونی	×	×	امکان‌پذیر		راهنمایی‌های بهبود نرم افزاری، آزمون نرم افزار؛ در برنامه‌های نمونه کاربردی کسب‌وکار تایید می‌کند که کنترل‌های الزامی کاربران در عمل وجود دارند.
الف-۱۲-۲-۳ تمامیت پیغام		×	امکان‌پذیر		
الف-۱۲-۲-۴ صحه‌گذاری داده خروجی	×	×	امکان‌پذیر		راهنمایی‌های بهبود نرم افزاری، آزمون نرم افزار؛ در برنامه‌های نمونه کاربردی کسب‌وکار تایید می‌کند که کنترل‌های الزامی کاربران در عمل وجود دارند.
الف-۱۲-۳ کنترل‌های رمزنگاری					
الف-۱۲-۳-۱خط‌مشی استفاده از کنترل‌های رمزنگاری	×	×	امکان‌پذیر		همچنین پیاده‌سازی خط‌مشی در موارد مقتضی بررسی شوند.
الف-۱۲-۳-۲ مدیریت کلید	×	×	پیشنهادی		
الف-۱۲-۴ امنیت فایل‌های سیستم					
الف-۱۲-۴-۱ کنترل نرم افزار عملیاتی	×	×	امکان‌پذیر		
الف-۱۲-۴-۲حفاظت از داده‌های آزمون سیستم	×	×	امکان‌پذیر	×	
الف-۱۲-۴-۳ کنترل دسترسی به کدمنبع برنامه	×	×	پیشنهادی		
الف-۱۲-۵ امنیت در فرایندهای بهبود و پشتیبانی					
الف-۱۲-۵-۱ روش‌های اجرایی کنترل تغییر	×				
الف-۱۲-۵-۲ بازنگری فنی نرم افزارهای کاربردی پس از تغییرات سیستم عامل	×				

1- Validation

جدول د-۱- ادامه

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۱۲-۵-۳ محدود سازی در اعمال تغییرات در بسته های نرم افزاری	×				
الف-۱۲-۵-۴ نشت اطلاعات	×	×	امکان‌پذیر		خدمات نا شناخته
الف-۱۲-۵-۵ بهبود نرم افزار برون‌سپاری‌شده	×				
الف-۱۲-۶ مدیریت آسیب پذیری فنی					
الف-۱۲-۶-۱ کنترل آسیب پذیرهای فنی	×	×	پیشنهادی		توزیع وصله های نرم افزاری
الف-۱۳ مدیریت رخدادهای امنیت اطلاعات					
الف-۱۳-۱ گزارش دهی وقایع و ضعفهای امنیت اطلاعات					
الف-۱۳-۱-۱گزارش دهی وقایع امنیت اطلاعات	×				
الف-۱۳-۱-۲ گزارش دهی ضعفهای امنیتی	×				
الف-۱۳-۲ مدیریت رخدادها و بهبودهای امنیت اطلاعات					
الف-۱۳-۲-۱ مسوولیتها و روش‌های اجرایی	×				
الف-۱۳-۲-۲یادگیری‌ازرخدادهای‌امنیت‌اطلاعات	×				
الف-۱۳-۲-۳-گرد آوری شواهد	×				
الف-۱۴ مدیریت استمرار کسب‌وکار					
الف-۱۴-۱ جنبه های امنیت اطلاعات مدیریت استمرار کسب‌وکار					صورتجلسه های بازنگری مدیریت.
الف-۱۴-۱-۱ لحاظ کردن امنیت اطلاعات در فرایند مدیریت استمرار کسب‌وکار	×				
الف-۱۴-۱-۲ استمرار کسب‌وکار و ارزیابی‌ریسک	×				
الف-۱۴-۱-۳ ایجاد و پیاده سازی طرح‌های استمرار در برگیرنده امنیت اطلاعات	×	×	امکان‌پذیر	×	بررسی سایت‌های بازیابی در مواقع بحران، فاصله این سایت‌ها براساس ارزیابی‌ریسک و الزامات قانونی و مقرراتی
الف-۱۴-۱-۴ چارچوب طرح‌ریزی استمرار کسب‌وکار	×				
الف-۱۴-۱-۵ حفظ‌ونگهداری آزمون و ارزیابی مجدد طرح های استمرار کسب‌وکار	×				
الف-۱۵ انطباق					
الف-۱۵-۱ انطباق با الزامات قانونی					
الف-۱۵-۱-۱ شناسایی قوانین قابل اجرا	×				
الف-۱۵-۱-۲ حقوق مالکیت معنوی[1]	×				
الف-۱۵-۱-۳ حفاظت از سوابق سازمانی	×	×	امکان‌پذیر		

1- Intellectual Property Rights (IPR)

جدول د-۱- ادامه

کنترل‌های پیوست الف از استاندارد ۲۷۰۰۱	کنترل سازمانی	کنترل فنی	آزمون سیستم	بازرسی چشمی	راهنمایی بازنگری ممیزی
الف-۱۵-۱-۴ حفاظت داده‌ها و حریم خصوصی اطلاعات شخصی	×	×	امکان‌پذیر		
الف-۱۵-۱-۵ پیشگیری از استفاده نابجا از امکانات پردازش اطلاعات	×				
الف-۱۵-۱-۶ قواعد کنترل‌های رمزنگاری	×				
الف-۱۵-۲ انطباق با خط‌مشی‌ها و استانداردهای امنیتی، و انطباق فنی					
الف-۱۵-۲-۱ انطباق خط‌مشی ها واستانداردهای امنیتی	×				
الف-۱۵-۲-۲ بررسی انطباق فنی	×	×	امکان‌پذیر		فرآیند ارزیابی و پیگیری
الف-۱۵-۳ ملاحظات ممیزی سیستم‌های اطلاعاتی					
الف-۱۵-۳-۱ کنترل‌های ممیزی سیستم‌های اطلاعاتی	×				
الف-۱۵-۳-۲ حفاظت از ابزارهای ممیزی سیستم‌های اطلاعاتی	×	×	امکان‌پذیر		

ICS: 35.040

صفحه : ۴۸