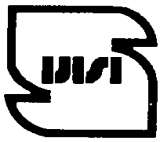
INSO-ISO-IEC
27007
1st. Edition

May.2013

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization



استاندارد ایران-ایزو-آی‌ای‌سی

۲۷۰۰۷
چاپ اول
اردیبهشت ۱۳۹۲

فناوری اطلاعات – فنون امنیتی – راهنماهایی برای ممیزی سامانه‌های مدیریت امنیت اطلاعات

Information technology – Security techniques – Guidelines for information security management systems auditing

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

موسسه استاندارد و تحقیقات صنعتی ایران به موجب بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد 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 حوزه های مختلف در کمیسیون فنی مرکب از کارشناسان سازمان، صاحب نظران مراکز و موسسات علمی، پژوهشی تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانه صاحبان حق و نفع، شامل تولید کنندگان، مصرف کنندگان، صادر کنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان-های دولتی و غیردولتی حاصل می‌شود. پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون‌های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیته ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که موسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیر با رعایت ضوابط تعیین شده تهیه می‌کنند در کمیته ملی طرح و بررسی و در صورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شماره ۵ تدوین و در کمیته ملی استاندارد مربوط که موسسه استاندارد تشکیل می‌دهد به تصویب رسیده باشد.

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

موسسه استاندارد و تحقیقات صنعتی ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و / یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. موسسه می‌تواند به منظور 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 موسسات فعال در زمینه مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم‌های مدیریت کیفیت و مدیریت زیست محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، موسسه استاندارد این گونه سازمان‌ها و موسسات را بر اساس ضوابط نظام تایید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامه تایید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه 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 for Legal Metrology (Organization International de Metrologie Legal)
4- Contact Point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات- فنون امنیتی – راهنماهایی برای ممیزی سامانه‌های مدیریت امنیت اطلاعات »

رئیس:	**سمت و/یا نمایندگی**
قسمتی، سیمین (فوق لیسانس، فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
دبیر:	
میراسکندری، محمدرضا (لیسانس، مهندسی کامپیوتر نرم‌افزار)	مدیر کل اداره خدمات ارزش افزوده سازمان فناوری اطلاعات ایران
اعضا: (اسامی به ترتیب حروف الفبا)	
بختیاری، شیرین (لیسانس، مهندسی برق کنترل)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
رستمی، حبیب (فوق لیسانس، ریاضی کاربردی)	مدیر گروه پژوهشی فناوری اطلاعات، جهاد دانشگاه صنعتی شریف
سعیدی، عذرا (فوق لیسانس، مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
فرهاد شیخ احمد، لیلا (فوق لیسانس، مهندسی کامپیوتر نرم‌افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
فولادیان، مجید (فوق لیسانس، مهندسی مخابرات)	مشاور سازمان فناوری اطلاعات ایران
فیاضی، مهدی (لیسانس، مهندسی برق الکترونیک)	کارشناس مسئول تدوین استاندارد و امنیت شبکه سازمان فناوری اطلاعات ایران
میرزایی رضایی، طیبه (فوق لیسانس، فیزیک)	رییس اداره تدوین استاندارد سازمان فناوری اطلاعات ایران
وکیلی، اسد (فوق لیسانس، مهندسی برق)	هیات علمی موسسه تحقیقات ارتباطات و فناوری اطلاعات
یزدیان، علی (دکترا، مهندسی برق)	هیات علمی دانشگاه تربیت مدرس
یوسف زاده، بهاره (لیسانس مهندسی کامپیوتر)	کارشناس سازمان ملی استاندارد ایران

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- راهنماهایی برای ممیزی سامانه‌های مدیریت امنیت اطلاعات» که پیش نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده و در یکصد و نود وششمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده مورخ ۹۱/۶/۲۰ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

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

منبع و ماخذی که برای تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 27007: 2011, Information technology — Security techniques — Guidelines for information security management systems auditing

- **مقدمه**

این استاندارد ملی راهنمایی بر مدیریت برنامه ممیزی سامانه مدیریت امنیت اطلاعات (ISMS)[1] و راهبری ممیزی‌های داخلی یا خارجی مطابق با استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ ارائه می‌دهد، همچنین راهنمایی درمورد شایستگی و ارزیابی ممیزان ISMS که باید به همراه راهنمایی موجود در استاندارد ISO 19011 استفاده شود را فراهم می‌کند. این استاندارد به بیان الزامات نمی‌پردازد.

این راهنما برای تمام کاربران اعم از سازمان‌هایی با اندازه کوچک و متوسط در نظر گرفته شده است.

استاندارد ISO 19011 (راهنماهایی برای ممیزی سامانه‌های مدیریت)، راهنمایی بر مدیریت برنامه‌های ممیزی، راهبری ممیزی‌های خارجی یا داخلی سامانه‌های مدیریت، همچنین شایستگی و ارزیابی ممیزان سامانه مدیریت را فراهم می‌کند.

متن این استاندارد ملی، از ساختار استاندارد ISO 19011 پیروی می‌کند و راهنمایی اضافی خاص ISMS در کاربرد استاندارد ISO 19011 برای ممیزی ISMS با حروف IS نشان داده می‌شود.

1- Information Security Management System

فناوری اطلاعات – فنون امنیتی – راهنماهایی برای ممیزی سامانه‌های مدیریت امنیت اطلاعات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ارائه راهنمایی‌هایی در مورد راهبری برنامه ممیزی سامانه مدیریت امنیت اطلاعات (ISMS)، هدایت ممیزی‌ها و شایستگی ممیزان ISMS است که علاوه بر راهنماهای موجود در استاندارد ISO 19011 است.

این استاندارد ملی برای آن‌هایی که به درک یا راهبری ممیزی‌های داخلی یا خارجی ISMS یا مدیریت برنامه ممیزی ISMS نیاز دارند، کاربردپذیر است.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود.

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

استفاده از مراجع زیر برای این استاندارد الزامی‌است:

2-1 ISO 19011:2011, Guidelines for auditing management systems

۲-۲ استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سیستم‌های مدیریت امنیت اطلاعات -- الزامات

۲-۳ استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۱، فناوری اطلاعات – فنون امنیتی – سامانه‌های مدیریت امنیت اطلاعات – مرورکلی و واژگان

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف ارائه شده در استاندارد ISO 19011 و استاندارد ISO/IEC 27000 به کار می‌رود.

۴ اصول ممیزی

اصول ممیزی از استاندارد ISO 19011:2011، بند ۴، به کار گرفته می‌شود.

۵ مدیریت کردن برنامه ممیزی

۵-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۵-۱ اعمال می‌شود. علاوه بر آن راهنمای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۵-۱-۱ IS[1] ۵-۱ کلیات

برنامه ممیزی[2] ISMS باید بر اساس وضعیت مخاطره امنیت اطلاعات ممیزی‌شونده توسعه داده شود.

۵-۲ پایه‌گذاری[3] اهداف برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۲ اعمال می‌شود. علاوه بر آن راهنمای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۵-۲-۱ IS ۵-۲ پایه‌گذاری اهداف برنامه ممیزی

اهداف برنامه (های) ممیزی باید به منظور هدایت طرح‌ریزی و راهبری ممیزی و اطمینان از اینکه برنامه ممیزی به طور موثر اجرا می‌شود، پایه‌گذاری شود. این اهداف می‌تواند به موارد زیر وابسته باشد.

الف- الزامات امنیت اطلاعات شناسایی شده؛

ب- الزامات استاندارد ISO/IEC 27001؛

پ- سطح عملکرد ممیزی‌شونده همان طور که در وقوع نقائص امنیت اطلاعات، رخدادها و سنجش‌های اثربخشی‌منعکس شده است؛ و

ت- مخاطرات امنیت اطلاعات برای سازمان در حال ممیزی.

نمونه‌هایی از اهداف برنامه ممیزی ممکن است شامل موارد زیر باشد:

۱- درستی‌سنجی تطابق با الزامات قراردادی و قانونی و سایر الزامات و مفهوم[4] امنیت آن‌ها.

۲- دستیابی و حفظ اعتماد در رابطه با توانایی مدیریت مخاطرات ممیزی‌شونده.

۵-۳ پایه‌گذاری برنامه ممیزی

۵-۳-۱ نقش و مسئولیت‌های مدیر برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۳-۱ به کار گرفته می‌شود.

۵-۳-۲ شایستگی مدیر برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۳-۲ به کار گرفته می‌شود.

1- Information security

۲- در این استاندارد، هر زمان که از اصطلاح «ممیزی» استفاده شد، منظور ممیزی ISMS است.

3- Establish

4- Implication

۵-۳-۳ تعیین گستره برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۳-۳ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۵-۳-۳-۱ IS ۵-۳-۳ تعیین گستره برنامه ممیزی

گستره هر برنامه ممیزی می‌تواند متفاوت باشد. عواملی که می‌تواند بر گستره برنامه ممیزی تاثیر بگذارد، عبارتند از:

الف- اندازه ISMS ، شامل:

۱- تعداد کل کارکنان مشغول به کار در هر مکان و روابط با پیمانکاران طرف سوم که به طور منظم در محلی که باید ممیزی شود کار می‌کنند؛

۲- تعداد سامانه‌های اطلاعاتی؛

۳- تعداد پایگاه‌های[1] پوشش داده شده با ISMS.

ب- پیچیدگی ISMS (شامل تعداد و حساسیت فرآیندها و فعالیت‌ها)

پ- اهمیت مخاطرات امنیت اطلاعات شناسایی شده برای ISMS؛

ت- اهمیت اطلاعات و دارایی‌های وابسته در محدوده ISMS؛

ث- پیچیدگی سامانه‌های اطلاعاتی موجود که باید مورد ممیزی قرار گیرند، شامل پیچیدگی فناوری اطلاعات پیاده‌سازی شده؛

ج- وجود پایگاه‌های مشابه متعدد؛ و

چ- تفاوت در پیچیدگیISMS در گستره پایگاه‌های محدوده ممیزی.

ملاحظات باید در برنامه ممیزی به منظور تنظیم اولویت ها بر اساس مخاطرات امنیت اطلاعات والزامات کسب وکار در رابطه با حوزه‌های ISMS که تضمین کننده بررسی جزیی‌تر است، رعایت گردد.

اطلاعات بیشتر در مورد روش نمونه‌برداری چند پایگاهی می‌تواند در استاندارد ملی ایران شماره ۲۷۰۰۶: سال ۱۳۸۷ و IAF MD 1:2007 یافت شود (به کتابنامه مراجعه شود)، که اطلاعات این اسناد فقط مربوط به گواهی ممیزی‌ها است.

۵-۳-۴ شناسایی و ارزیابی مخاطرات برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۳-۴ به کار گرفته می‌شود.

۵-۳-۵ پایه‌گذاری روش‌های اجرایی برای برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۳-۵ به کار گرفته می‌شود.

۵-۳-۶ شناسایی منابع برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۳-۶ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

1- sites

۵-۳-۶-۱ IS ۵-۳-۶ شناسایی منابع برنامه ممیزی

به طور خاص، برای همه مخاطرات امکان پذیر برای ممیزی شونده ، باید به ممیزان برای تحقیق اثربخشی اقدام کاهش مخاطره مربوطه، زمان کافی تخصیص داده شود.

۵-۴ پیاده‌سازی برنامه ممیزی

۵-۴-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۵-۴-۱ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۵-۴-۱-۱ IS ۵-۴-۱ کلیات

هر جا که کاربردپذیر است، الزامات محرمانگی ممیزی‌شونده‌ها و سایر طرف‌های مربوطه، ازجمله الزامات قراردادی و قانونی ممکن باید در پیاده‌سازی برنامه ممیزی مشخص شوند.

۵-۴-۲ تعریف اهداف، محدوده و معیارهای یک ممیزی جداگانه

راهنماها از استاندارد ISO 19011:2011، بند ۵-۴-۲ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۵-۴-۲-۱ IS ۵-۴-۲ تعریف اهداف، محدوده و معیار برای ممیزی جداگانه

محدوده ممیزی باید مخاطرات امنیت اطلاعات ممیزی شونده، الزامات کسب وکار مربوطه و مخاطرات کسب وکار را منعکس کند.

به علاوه اهداف ممیزی ممکن است موارد زیر را دربرگیرد:

الف- ارزیابی این که آیا ISMS ، به طور مناسب الزامات امنیت اطلاعات را شناسایی و مشخص می‌کند؛

ب- ارزیابی مناسب بودن مداوم اهداف ISMS، تعریف شده توسط مدیریت؛ و

پ- ارزیابی فرآیندها برای نگهداری و بهبود موثر ISMS.

کمک‌های کاربردی- مثال‌هایی از معیارهای ممیزی

موضوعات زیر عناوینی هستند که به عنوان معیار ممیزی در نظر گرفته می‌شوند:

۱- روش ارزشیابی مخاطره امنیت اطلاعات ممیزی‌شونده و ارزشیابی مخاطره و نتایج برطرف‌سازی که این‌ها همه‌ی الزامات مرتبط را نشان می‌دهد؛

۲- نسخه‌ای از بیانیه کاربست پذیری و رابطه آن با نتایج حاصل از ارزشیابی مخاطره؛

۳- پیاده‌سازی موثر کنترل‌ها به منظور کاهش مخاطرات؛

۴- سنجش اثربخشی کنترل‌های پیاده‌سازی شده که این سنجش‌ها، مطابق تعریف اندازه‌گیری اثر بخشی کنترل‌ها به کار گرفته می شوند. (به ISO/IEC 27004[1] مراجعه کنید)؛

۵- فعالیت‌هایی برای پایش و بازنگری کنترل‌ها و فرایندهای ISMS؛

۶- ممیزی‌های داخلیISMS و بازنگری‌های مدیریت و اقدامات اصلاحی سازمان؛

۱- معادل استاندارد ISO/IEC 27004، استاندارد ملی ایران شماره ۱۴۰۹۶: سال ۱۳۸۹ موجود است.

۷- اطلاعاتی در مورد کفایت و تطابق با اهداف، خط‌مشی‌ها و روش‌های اجرایی اتخاذ شده به وسیله ممیزی شونده؛ و
۸- انطباق با الزامات قراردادی و قانونی خاص و سایر الزامات مربوط به ممیزی‌شونده و مفهوم امنیت اطلاعات آن‌ها.
تیم ممیزی باید از تعریف شفاف محدوده و قلمروهای ISMS ممیزی شونده بر مبنای ویژگی‌های کسب و کار، سازمان، مکان، دارایی‌ها و فناوری آن از جمله جزئیات و توجیه برای کنارگزاری هر چیزی از محدوده، اطمینان حاصل کند. تیم ممیزی باید تایید کند که ممیزی شونده، به الزامات بیان شده در بند ۱-۲ استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ در محدوده ISMS، توجه داشته است.
بنابراین ممیزان باید مطمئن شوند که فعالیت‌های ارزشیابی مخاطره امنیت اطلاعات و برطرف‌سازی مخاطرات ممیزی شونده به درستی منعکس شده‌اند و قلمروهای محدوده را پوشش می‌دهد. ممیزان باید تایید کنند که این موضوع در بیانیه کاربست پذیری منعکس شده است.
بنابراین ممیزان باید مطمئن شوند که واسط‌های مربوط به خدمات یا فعالیت‌هایی که به طور کامل در محدوده ISMS نیستند، در ISMS توجه شده است و در ارزیابی مخاطره امنیت اطلاعات ممیزی شونده وارد شده است. مثالی از چنین وضعیتی، به اشتراک‌گذاری تسهیلات (به عنوان مثال سامانه های فناوری اطلاعات، پایگاه‌های داده و سامانه‌های مخابراتی) با دیگر سازمان‌ها است.

۵-۴-۳ انتخاب روش‌های ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۴-۳ اعمال می‌شود. علاوه بر آن راهنمای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۵-۴-۳-۱ IS ۵-۴-۳ انتخاب روش‌های ممیزی

اگر ممیزی مشترک انجام شود، باید در خصوص عدم افشای اطلاعات در طول ممیزی توجه ویژه‌ای شود. قبل از آغاز ممیزی باید همه طرف‌های ذینفع بر سر این موضوع به توافق رسیده باشند.

۵-۴-۴ انتخاب اعضای تیم ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۴-۴ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۵-۴-۴-۱ IS ۵-۴-۴ انتخاب اعضای تیم ممیزی

شایستگی تیم ممیزی روی هم رفته باید موارد زیر را شامل شود:
الف- دانش و درک کافی از مدیریت مخاطرات امنیت اطلاعات که برای ارزیابی روش‌های استفاده شده توسط ممیزی شونده کفایت نماید؛ و
ب- دانش و درک کافی از امنیت اطلاعات و مدیریت امنیت اطلاعات که برای ارزیابی انتخاب کنترل و طرح‌ریزی، پیاده‌سازی، نگهداری واثر بخشی ISMS کفایت نماید.
در جایی که لازم است، باید دقت شود که ممیزان مجوز لازم برای دسترسی به شواهد ممیزی را بدست آورده‌اند.

۵-۴-۵ اختصاص مسئولیت برای ممیزی جداگانه به رهبر تیم ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۴-۵ به کار گرفته می‌شود.

۵-۴-۶ مدیریت دستاورد برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۴-۶ به کار گرفته می‌شود.

۵-۴-۷ مدیریت و نگهداری سوابق برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۴-۷ به کار گرفته می‌شود.

۵-۵ پایش برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۵ به کار گرفته می‌شود.

۵-۶ بازنگری و بهبود برنامه ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۵-۶ به کار گرفته می‌شود.

۶ اجرای ممیزی

۶-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۶-۱ به کار گرفته می‌شود.

۶-۲ راه‌اندازی ممیزی

۶-۲-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۶-۲-۱ به کار گرفته می‌شود.

۶-۲-۲ برقرارکردن تماس اولیه با ممیزی‌شونده

راهنماها از استاندارد ISO 19011:2011، بند ۶-۲-۲ به کار گرفته می‌شود.

۶-۲-۳ تعیین امکان‌سنجی[1] ممیزی

راهنماها از استاندارد ISO 19011:2011، بند۶-۲-۳ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۶-۲-۳-۱ IS ۶-۲-۳ تعیین امکان‌سنجی ممیزی

قبل از شروع ممیزی، باید از ممیزی شونده پرسیده شود، که آیا سوابق ISMS برای بازنگری توسط تیم ممیزی در دسترس نیست، به عنوان مثال به دلیل اینکه آن‌ها شامل اطلاعات حساس و محرمانه است. شخص مسئول مدیریت برنامه ممیزی، باید تعیین کند که آیا ISMS می‌تواند در صورت نبود این سوابق به طور مناسب بررسی شود. اگر نتیجه این است که ممکن نیست که ، ISMS بدون بازنگری سوابق مشخص شده، به طور مناسب ممیزی شود، شخص باید ممیزی‌شونده را آگاه کند که امکان ممیزی تا

1- Feasibility

تضمین شدن مقدمات دسترسی مناسب وجود ندارد و راه‌کار جایگزین می‌تواند به/توسط ممیزی‌شونده پیشنهاد شود.

۶-۳ آماده‌سازی فعالیت‌های ممیزی

۶-۳-۱ اجرای سند خوانی[1] به منظور آماده‌سازی برای ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۳-۱ به کار گرفته می‌شود.

۶-۳-۲ آماده سازی طرح ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۳-۲ به کار گرفته می‌شود.

۶-۳-۳ اختصاص کار به تیم ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۳-۳ به کار گرفته می‌شود.

۶-۳-۴ آماده سازی اسناد کاری

راهنماها از استاندارد ISO 19011:2011، بند ۶-۳-۴ به کار گرفته می‌شود.

۶-۴ هدایت فعالیت‌های ممیزی

۶-۴-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۱ به کار گرفته می‌شود.

۶-۴-۲ برگزاری جلسه افتتاحیه[2]

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۲ به کار گرفته می‌شود.

۶-۴-۳ انجام سند خوانی در هنگام هدایت ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۳ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۶-۴-۳-۱ IS ۶-۴-۳ انجام سند خوانی در هنگام ممیزی

ممیزان باید وارسی کنند که اسناد مورد نیاز استاندارد ISO/IEC 27001 وجود دارد و مطابق با الزامات آن است.

ممیزان باید تایید کنند که کنترل‌های انتخاب شده مربوط به نتایج ارزشیابی مخاطره و فرایند برطرف‌سازی مخاطره است و در نتیجه قابل ردیابی در خط‌مشی و اهداف ISMS است.

یادآوری- پیوست الف این استاندارد راهنمایی در مورد چگونگی ممیزی فرایندها و مستندات ISMS ارائه می‌کند.

۶-۴-۴ تبادل اطلاعات[3] در حین ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۴ به کار گرفته می‌شود.

1- Document review
2- Opening meeting
3- Communicating

۶-۴-۵ اختصاص نقش‌ها و مسئولیت‌های راهنماها و ناظران[1]

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۵ به کار گرفته می‌شود.

۶-۴-۶ جمع آوری و درستی‌سنجی[2] **اطلاعات**

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۶ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۶-۴-۶-۱ IS ۶-۴-۶ گرد آوری و درستی‌سنجی اطلاعات

گردآوری اطلاعات و شواهد که نشان‌دهنده‌ی آن است که فرایندها و کنترل های ISMS پیاده‌سازی شده و قابل اجرا است، بخش مهمی از ممیزی ISMS است. روش‌های ممکن برای جمع آوری اطلاعات مربوطه در طول ممیزی عبارتند از:

الف) بازنگری دارایی‌های اطلاعاتی و فرایندهای ISMS و کنترل‌های پیاده‌سازی شده برای آن‌ها؛ و

ب) استفاده از ابزارهای خودکار ممیزی.

یادآوری– پیوست الف این استاندارد راهنمایی در مورد چگونگی ممیزی فرایندهای ISMS ارائه می‌کند.

ممیزان ISMS باید از اداره[3] مناسب همه‌ی اطلاعات دریافت شده از ممیزی‌شوندگان بر طبق توافق بین ممیزی‌شونده و تیم ممیزی اطمینان حاصل کنند.

۶-۴-۷ ایجاد یافته‌های ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۷ به کار گرفته می‌شود.

۶-۴-۸ آماده‌کردن نتایج ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۸ به کار گرفته می‌شود.

۶-۴-۹ برگزاری جلسه اختتامیه

راهنماها از استاندارد ISO 19011:2011، بند ۶-۴-۹ به کار گرفته می‌شود.

۶-۵ آماده سازی و توزیع گزارش ممیزی

۶-۵-۱ آماده سازی گزارش ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۵-۱ به کار گرفته می‌شود.

۶-۵-۲ توزیع گزارش ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۵-۲ به کار گرفته می‌شود.

۶-۶ اتمام ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۶ به کار گرفته می‌شود.

1- Observer
2- Verify
3- Handling

۷-۶ انجام اقدامات پیگیری بعد از ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۶-۷ به کار گرفته می‌شود.

۷ شایستگی و ارزیابی ممیزان

۷-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۷-۱ به کار گرفته می‌شود.

۷-۲ تعیین شایستگی ممیز به منظور رفع نیازهای برنامه ممیزی

۷-۲-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۱ اعمال می‌شود. علاوه بر آن راهنماهای خاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۷-۲-۱-۱ IS ۷-۲-۱ کلیات

در گزینش دانش و شایستگی‌های مناسب، موارد زیر باید در نظر گرفته شود:

الف- پیچیدگی ISMS (به عنوان مثال، حیاتی‌بودن[1] سامانه‌های اطلاعاتی، وضعیت مخاطره ISMS)

ب- ماهیت(های) کسب و کاری که در محدوده ISMS انجام شده است.

پ- وسعت و تنوع[2] فناوری مورد استفاده در پیاده‌سازی مولفه‌های مختلف ISMS (مانند کنترل‌های پیاده‌سازی شده، مستندات و/یا کنترل فرایند، اقدامات اصلاحی/پیشگیرانه و غیره)؛

ت- تعداد پایگاه‌ها؛

ث- کارایی نشان داده شده[3] قبلی ISMS؛

ج- وسعت برون سپاری و هماهنگی‌های استفاده شده با طرف سوم در محدوده ISMS؛

چ- استانداردها، الزامات قانونی و سایر الزامات مربوط به برنامه ممیزی.

۷-۲-۲ ویژگی‌های شخصی

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۲ به کار گرفته می‌شود.

۷-۲-۳ دانش و مهارت‌ها

۷-۲-۳-۱ کلیات

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۳-۱ به کار گرفته می‌شود.

۷-۲-۳-۲ دانش و مهارت‌های عمومی ممیزان سامانه مدیریت

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۳-۲ به کار گرفته می‌شود.

1- Criticality
2- Diversity
3- Demonstrated

۷-۲-۳-۳ دانش خاص حوزه[1] و بخش و مهارت‌های ممیزان سامانه مدیریت

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۳-۳ اعمال می‌شود. علاوه بـر آن راهنماهـای خـاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۷-۲-۳-۳-۱ IS ۷-۲-۳-۳ دانش خاص حوزه و بخش ومهارت‌های خاص ممی‌زان سامانه مدی‌ری‌ت

ممیزان ISMS باید دانش و مهارت‌هایی در زمینه‌های زیر داشته باشند:

الف- روش‌های مدیریت امنیت اطلاعا:، به منظور قادر ساختن ممیز برای بررسی ISMS و تولید یافته‌های ممیزی و توصیه‌های مناسب. دانش و مهارت در این زمینه باید شامل موارد زیر باشد.

۱- اصطلاحات[2] امنیت اطلاعات؛

۲- اصول مدیریت امنیت اطلاعات و کاربرد آن‌ها؛ و

۳- روش‌های مدیریت مخاطرات امنیت اطلاعات و کاربرد آن‌ها.

ب- دانش عمومی در فناوری اطلاعات و فنون امنیت اطلاعات، به صورت مقتضی (به عنوان مثال، روش‌های کنترل دسترسی فیزیکی و منطقی، حفاظت در برابر نرم افزار مخرب، روش‌های مدیریت آسیب‌پذیری) یا دسترسی به آن.

پ- تهدیدات امنیت اطلاعات موجود، آسیب‌پذیری و کنترل‌ها، به علاوه زمینه وسیع‌تر سازمانی، چارچوب قراردادی و قانونی برای ISMS (به عنوان مثال، روابط و فرایندهای در حال تغییر کسب و کار، فناوری یا قوانین)

اگر دانش خاص یا مهارت‌های اضافه‌تری مورد نیاز باشد، باید از متخصصین امنیت اطلاعـات (بـه عنـوان مثال با شایستگی بخش خاص، شایستگی در امنیت IT، یا مدیریت تداوم کسب و کار) استفاده شـود. در صورت استفاده از متخصصین، شایستگی آن‌ها باید به دقت ارزیابی شده باشد.

۷-۲-۳-۴ دانش و مهارت‌های کلی رهبر تیم ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۳-۴ به کار گرفته می‌شود.

۷-۲-۳-۵ دانش و مهارت‌ها برای ممیزی سامانه‌های مدیریت چند وجهی[3]

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۳-۵ به کار گرفته می‌شود.

۷-۲-۴ کسب شایستگی ممیز

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۴ اعمال مـی‌شـود. عـلاوه بـر آن راهنماهـای خـاص ISMS که در ادامه می‌آید، به کار گرفته می‌شود.

۷-۲-۴-۱ IS ۷-۲-۴ کسب شایستگی ممیز

ممیزان ISMS باید دانش و مهارت‌هایی در زمینه فناوری اطلاعات و امنیت اطلاعات، برای مثال با ارائه‌ی گواهینامه‌های مربوطه داشته باشند و همچنین باید قادر به درک نیازهـای کسـب وکـار مربوطـه باشـند.

1- Discipline
2- Terminology
3- Multiple discipline

همچنین تجربه کاری ممیزان ISMS باید به پیشرفت دانـش و شایسـتگی‌هـای آن‌هـا در رشـته ISMS کمک کند.

۷-۲-۵ رهبر تیم ممیزی

راهنماها از استاندارد ISO 19011:2011، بند ۷-۲-۵ به کار گرفته می‌شود.

۷-۳ تعیین معیارهای ارزیابی ممیز

راهنماها از استاندارد ISO 19011:2011، بند ۷-۳ به کار گرفته می‌شود.

۷-۴ انتخاب روش ارزیابی ممیزِ مناسب

راهنماها از استاندارد ISO 19011:2011، بند ۷-۴ به کار گرفته می‌شود.

۷-۵ هدایت ارزیابی ممیز

راهنماها از استاندارد ISO 19011:2011، بند ۷-۵ به کار گرفته می‌شود.

۷-۶ نگهداری و بهبود شایستگی ممیز

راهنماها از استاندارد ISO 19011:2011، بند ۷-۶ به کار گرفته می‌شود.

پیوست الف

(اطلاعاتی)

راهنمای عملی برای ممیزی ISMS

متن زیر راهنمایی کلی در مورد چگونگی ممیزی فرایندهای ISMS را طبق الزامات استاندارد ISO/IEC 27001 بدون توجه به الزامات مشخص ISMS که ممکن است یک سازمان مجزا داشته باشد (برای مثال، الزامات قانونی و قراردادی و دیگر الزامات مربوط به پیاده‌سازی کنترل‌های امنیت اطلاعات ویژه) ارائه می‌دهد.

این راهنما در درجه اول به منظور رجوع و استفاده به وسیله ممیزانی (داخلی یا خارجی) که ممیزی ISMS را انجام خواهند داد، می‌باشد.

استانداردهای اضافی اختیاری می‌توانند به منظور راهنمایی ممیزی شونده یا ممیز استفاده شوند. این‌ها به عنوان «استانداردهای مربوط» در جداول زیر فهرست شده‌اند. به ممیزان یادآوری می‌شود که تنها عدم انطباق‌ها، بر معیارهای ممیزی و الزامات استاندارد ISO/IEC 27001 را مبنا قرار دهند.

جدول الف-۱: راهنمای عملی ممیزی ISMS

الف-۱ محدوده ISMS، خط‌مشی و رویکرد ارزشیابی مخاطره (استاندارد ISO/IEC 27001 بند ۴-۱ و ۴-۲-۱ الف تا پ	
معیارهای ممیزی	استاندارد ISO/IEC 27001[1] بند ۴-۱، ۴-۲-۱ الف، ب و پ
استانداردهای مربوط	استاندارد ISO/IEC 17021 بند ۹-۲-۱ الف تا ت استاندارد ISO/IEC 27005 بند ۳-۱ تا ۳-۹ (استاندارد ISO/IEC Guide73) استاندارد ISO/IEC 27005 بند ۷-۱، ۷-۲، ۷-۳ و ۷-۴ استاندارد ISO/IEC 27006 بند ۳-۱، ۳-۵، ۹-۱-۲ و ۹-۱-۴-۲ ب تا ت
شواهد ممیزی	شواهد ممیزی عبارتند از: • محدوده ISMS (۴-۳-۱ ب)؛ • نمودار سازمانی؛ • راهبرد سازمان؛ • بیانیه خط‌مشی کسب و کار، فعالیت‌ها و فرایندهای کسب و کار؛ • مستندات نقش‌ها و مسئولیت‌ها؛ • پیکربندی شبکه؛ • اطلاعات پایگاه‌ها، شامل فهرستی از شعب، کسب و کار، دفاتر و تسهیلات، و نقشه طبقات آن‌ها؛ • واسطها و وابستگی‌هایی که فعالیت های انجام شده کسب و کار در محدوده ISMS با افراد بیرون از محدوده دارند؛ • قوانین مربوط، مقررات و قراردادها؛

۱- مراجع بدون تاریخ، به نسخه‌ی استاندارد که در مراجع الزامی یا کتابنامه آمده است، بر می‌گردد.

	• اطلاعات دارایی‌های اولیه؛ • مستند خط‌مشی ISMS.
راهنمای عملی ممیزی	**سامانه مدیریت امنیت اطلاعات (۴)**
	الزامات کلی (۴-۱)
	«۴-۱ الزامات کلی» در استاندارد ISO/IEC 27001 زمینه کلی از ISMS مورد نیاز استاندارد ISO/IEC 27001 را مشخص می‌کند، که همه الزامات مندرج در بندهای بعد از ۴-۱ را پوشش می‌دهد. در راهنمای ممیزی، ISMS باید تحت موارد زیر تایید شود: • سازماندهی شده و انجام شده در زمینه‌ای از فعالیت های کلی کسب و کار سازمان و مخاطراتی که سازمان با آن مواجه است؛ • مستندسازی شده به منظور برآورده‌سازی الزامات (مندرج در۴-۳). به علاوه، باید نشان داده شود که ISMS پایه‌گذاری، پیاده‌سازی، راه‌اندازی، پایش، بازنگری، نگهداری و بهبود داده شده است. به عنوان مثال، سازمان نشان می‌دهدکه قابلیت انجام این فرایندها را دارد.
	پایه‌گذاری و مدیریت ISMS (۴-۲)
	پایه‌گذاری ISMS (۴-۲-۱)
	محدوده ISMS (۴-۲-۱ الف)
	ممیز باید بازنگری و تایید کند که سازمان محدوده و قلمروهای ISMS را مشخص کرده است. محدوده ISMS باید تعیین شود تا از به حساب آمدن همه دارایی‌های مرتبط در ISMS و مدیریت مخاطرات آن اطمینان حاصل شود. به علاوه، قلمروها، واسطها و وابستگی‌ها، برای نشان‌دادن مخاطراتی که ممکن است میان آن‌ها به وجود آید، نیاز است شناسایی شود. باید تایید شود که اطلاعاتی که درباره سازمان برای تعیین زمینه‌ای که سازمان عمل می‌کند و چگونگی ارتباط سازمان به ISMS و فرایندهای مدیریت مخاطرات امنیت اطلاعات آن‌ها، به منظور تعریف محدوده و قلمروها جمع آوری شده است. ممیز باید تایید کند که سازمان، اطلاعات زیر را به منظور تعریف محدوده و قلمروها در نظر گرفته است: • راهبردهای سازمان، اهداف کسب وکار و خط‌مشی‌ها؛ • فرایندهای کسب و کار؛ • ساختار و کارکردهای سازمان؛ • الزامات قراردادی و قانونی و سایر الزامات مربوط به سازمان؛ • دارایی‌های اطلاعاتی اولیه؛ • موقعیت‌های سازمان و مشخصه‌های جغرافیایی آن‌ها؛ • محدودیت‌های تاثیرگذار بر سازمان؛ • انتظار ذینفعان؛ • محیط اجتماعی- فرهنگی؛ و • واسطها (به عنوان مثال، تبادل اطلاعات با محیط)؛ باید بازنگری و تایید شود که سازمان توجیهی برای هر مورد کنارگذاشته شده از محدوده را ارائه می‌کند. باید تایید شود که سازمان، کارکردها و عملیات اجرایی خود را دارد و به اطمینان

	از اینکه ISMS به طور مداوم طبق چرخه حیات (استاندارد ISO/IEC 27001 قسمت ۴-۱ و استاندارد ISO/IEC 27006 قسمت ۳-۵) اجرا شده است، قادر می‌باشد. راهنمایی بیشتر درباره چگونگی ممیزی محدوده ISMS در بخش ۶-۲-۳ آورده شده است.
	خط‌مشی ISMS (۴-۲-۱ ب)
•	• ممیز باید تایید کند که خط‌مشی ISMS سازمان به طور خاص در اصطلاحات مشخصه‌های کسب و کار، سازمان، محل آن، دارایی‌ها و فناوری توصیف شده است. ممیز همچنین باید تایید کند که خط‌مشی ISMS به طور واضح موارد زیر را تعیین می‌کند: • چارچوبی برای تنظیم اهداف ISMS (پیش زمینه و اساس تنظیم اهداف و در صورتی که خط‌مشی ISMS و خط‌مشی‌های امنیت اطلاعات در یک مستند توصیف شده است، اهداف)، همچنین جهت و اصول اقدامات، از نقطه نظر مدیریت؛ • الزامات کسب و کار ضروری، الزامات قراردادی و قانونی و دیگر الزامات مرتبط با ممیزی‌شونده؛ • موقعیت و واسط نحوه تنظیم مدیریت مخاطرات امنیت اطلاعات با مدیریت مخاطرات کلی سازمان شامل CSR، حاکمیت[1] داخلی، کنترل مالی و ایمنی و غیره؛ • اساس مدیریت مخاطرات، مانند اینکه چه دارایی‌هایی اولیه‌ای باید به عنوان دارایی مهم برای حفاظت در نظر گرفته شوند و کدام جنبه‌های امنیت اطلاعات، برای مثال، محرمانگی، یکپارچگی یا دسترس‌پذیری باید به طور جدی هنگام هدایت ارزشیابی مخاطره ISMS ارزیابی شود؛ و • مصوبات و تعهد مدیریت ارشد. ممیزی خط‌مشی ISMS می‌تواند به وسیله موارد زیر انجام شود: • تایید این که خط‌مشی ISMS به عنوان یک سند که شامل امضاها یا مهرهایی که نشان می دهد مدیریت ارشد خط مشی را پایه‌گذاری کرده است، ایجاد شده است؛ • تایید از طریق مستندات مربوط به روش‌های اجرایی پایه‌گذاری خط‌مشی (به عنوان مثال: چگونه خط‌مشی در سازمان مجاز یا بازنگری شده است) و قواعد برای روش‌های اجرایی تعریف شده، نقش‌ها مستند شده و روش‌ها برای کنترل مستندات مشخص شده است؛ • مصاحبه با مدیریت برای درک رویکرد و تعهد آن‌ها به ISMS سازمان؛ • ارزیابی از طریق صورت جلسات و سوابق بازنگری مدیریت، تعهد و درگیری مدیریت در پیاده‌سازی، نگهداری و بهبود خط‌مشی ISMS؛ • ارزشیابی این که آیا مدیریت به طور موثر با خط‌مشی ISMS ارتباط دارد، به عنوان مثال، با تمرکز بر مخاطبان خاص، در تمام سطوح سازمان؛ • انجام مصاحبه با کارکنان در محدوده ISMS، به منظور تایید اینکه آیا آن‌ها از اهمیت اهداف امنیت اطلاعات جلسات، پیروی خط مشی امنیت اطلاعات و وظایف امنیت اطلاعات خود آگاه هستند؛ و • مد نظر قرار دادن خط‌مشی امنیت اطلاعات (اگر در دسترس باشد) و رابطه آن با خط‌مشی ISMS . • ممیزی اهداف ISMS می‌تواند با تایید موارد زیر انجام شود:

1- Governance

	• اهداف ISMS سازمان که تعریف شده، در خط‌مشی ISMS منعکس شده و با اهداف کلان کسب و کار هم تراز[1] شده است. • فرآیندها و کنترل‌های ISMS شناسایی شده و به منظور برآوردسازی اهداف ISMS مستند شده است؛ • اهداف به طور مناسب مستند شده است؛ • اهداف ISMS به طور مناسب با همه سطوح سازمان در ارتباط هستند؛ و • سازمان، کارکنان مسئول را به عنوان منابع مورد نیاز برای دستیابی به اهداف تخصیص داده است. • توصیه می‌شود که ممیز خط‌مشی مستند شده ISMS و اهداف در مرحله ممیزی بازنگری مستند را بررسی کند. • نیاز است اهداف و خط‌مشی ISMS در پاسخ به تغییر زمینه مدیریت مخاطرات بازنگری و به روزرسانی شود. ممیز باید تایید کند که بهبودهای مداوم در زمینه محیط کسب و کار انجام شده است. • ممیز باید به خاطر داشته باشد که انطباق با خط‌مشی ISMS و تحقق اهداف می‌تواند به صورت کمی یا کیفی سنجیده شود.
	رویکرد ارزشیابی مخاطره (۴-۲-۱ پ)
	استاندارد ISO/IEC 27001 ملزم می‌کند که سازمان‌ها یک رویکرد ارزشیابی مخاطره را تعریف کنند و بند ۴-۲-۱ موارد ت تا ج مولفه‌های این رویکرد را مشخص می‌کند. استاندارد ISO/IEC 27001 بیان نکرده است چه رویکرد ارزشیابی مخاطره‌ای باید به کار گرفته شود و هر رویکرد تا زمانی قابل قبول است که مطابق با الزامات استاندارد ISO/IEC 27001 باشد. ممیز باید انطباق رویکرد ارزشیابی مخاطره، با الزامات ارزشیابی مخاطره در استاندارد ISO/IEC 27001 و مناسب بودن آن برای سازمان و مدیریت کلان مخاطرات در محل را تصدیق کند. باید تایید شود که رویکرد ارزشیابی مخاطره به منظور شناسایی مخاطرات فرآیندهای کسب وکار، فعالیت‌ها و اقدامات مناسب در مقابل مخاطرات صورت گرفته، پیاده‌سازی شده است. استاندارد ISO/IEC 27005 راهنمایی را در مورد مدیریت و ارزشیابی مخاطره فراهم می‌کند. ممیز باید آگاه باشد که روش های کیفی و کمی، یا هر ترکیبی از این دو، برای ارزیابی مخاطره وجود دارد و این بستگی به سازمان دارد که تصمیم بگیرد چه روشی را به کار برد. لازم است فرایندها و روش‌های استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ بند ۴-۲-۱-پ تا د به عنوان رویکرد ارزشیابی مخاطره مطابق بیانیه مدیریت که در خط‌مشی ISMS سازمان توصیف شده است (به عنوان مثال ۴-۲-۱ ب، ۴، معیاری که کدام مخاطره ارزیابی خواهد شد) تعریف، پیاده‌سازی و مستند شوند. رویکرد این گونه تعریف می‌شود: در برگرفتن چگونگی انطباق با الزامات قراردادی و قانونی و سایر الزامات مرتبط در ارتباط با مخاطرات و دارایی‌هایی که سازمان باید به صورت راهبردی در زمینه کسب وکار و ارزشیابی مخاطره به‌کار برد. در ممیزی باید تایید شود که رویکرد، همان طور که در استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ بند ۴-۲-۱ ب تا د مورد نیاز است، پیاده‌سازی و انجام شده است.

1- Aligned

	ممیز باید تایید کند که نتایج ارزشیابی مخاطره توسط رویکرد ارزشیابی مخاطره قابل مقایسه و تجدید پذیر هستند. به عبارت دیگر، ممیز باید تایید کند که رویکرد، افراد مختلف عهده دار ارزشیابی مخاطره را قادر می سازد بدون توجه به مکان و زمان راهبری ارزیابی مخاطره، به نتیاج یکسانی دست پیدا کنند، به شرطی که آن‌ها سطح مشخصی از شایستگی در ارزشیابی مخاطره و راهبری ارزشیابی‌ها برای دارایی‌های مشابه مطابق با فرایندها و روش‌های اجرایی تعریف شده در رویکرد دارند و اگر نتیجه مختلفی مطرح شود، آن‌ها را برای شناسایی اینکه کجا و چرا در ارزشیابی مخاطره اختلاف رخ داده قادر می سازد. همچنین برای سازمان ضروری است که دارای رویکردی با توانایی رسیدن به انتخاب یکسان کنترل های برطرف سازی مخاطره در صورت یکسان بودن مخاطرات تخمین زده شده، به عبارت دیگر با سطح مخاطره و مشخصات یکسان (دارایی ها و الزمات امنیتی) باشد. این تاییدیه باید با نمونه برداری سوابق گزارش ارزشیابی مخاطره برای ردیابی رو به جلو و عقب توالی فرایندهای ارزشیابی مخاطره، با ممیزی‌های در پایگاه، بر دارایی‌ها انجام شود. معیارهای پذیرش مخاطرات اغلب تحت تاثیر خط‌مشی‌های مدیریت سازمان، اهداف، فناوری، سرمایه‌ها، قوانین و مقررات وابسته و افراد علاقه مند هستند و آن‌ها در نهایت به وسیله سازمان تعریف می شوند. بنابراین برای ممیزان لازم است با توجه به اثربخشی معیارها بر حسب موجودیت‌های بالا را بازنگری کنند. همچنین باید تایید کنند که آن‌ها تعریف شده و وجود دارند. ممیزان ممکن است برای تفسیرهای دقیق از معیار پذیریش مخاطره به استاندارد ISO/IEC 27005 :2008 بند ۷-۲ مراجعه کنند.
الف-۲ شناسایی مخاطره، تحلیل و ارزیابی و شناسایی و ارزیابی گزینه برطرف‌سازی مخاطره (استاندارد ISO/IEC 27001 بند ۴-۲-۱ت تا ج)	
معیار ممیزی	استاندارد ISO/IEC 27001 بند ۴-۲-۱ ت، ث، ج
استانداردهای مربوط	استاندارد ISO/IEC 27005 بند ۸-۲، ۸-۳، ۹، ۱۰
شواهد ممیزی	شواهد ممیزی شامل می شوند: • فهرستی از دارایی‌ها؛ • مستندات برای روش ارزیابی مخاطره؛ • گزارش‌های ارزیابی مخاطره.
راهنمای عملی ممیزی	**شناسایی مخاطره (بند ۴-۲-۱ ت)**
	ممیز باید فهرست دارایی را برای تایید این که همه دارایی‌های مهم مربوط در محدوده ISMS در فهرست آورده شده و صاحبان پاسخگو برای همه دارایی‌ها شناسایی شده‌اند، بازنگری کند. آن‌ها باید شناسایی تهدیدهای مربوط به دارایی ها، آسیب پذیری بهره‌جویی‌شده با تهدیدات و علت شکست امنیت به وسیله آن‌ها را بازنگری کنند برای مثال سناریوهای رخداد نشان داده شده در استاندارد ISO/IEC 27005.
	تحلیل و ارزیابی مخاطره (بند ۴-۲-۱ث)
	وارسی اینکه ارزشیابی مخاطره تمامی دارایی‌های مهم در محدوده ISMS را نشان می‌دهد و ارزشیابی تهدید/آسیب پذیری در رابطه با دارایی‌ها برای سازمان مناسب است و تنها از فهرست پیشین تهدیدات و آسیب پذیری‌ها استفاده نمی‌شود، مهم است. همچنین به دنبال گشتن مخاطراتی که اساسا اشتباه تعیین شده یا مورد کم توجهی قرار گرفته اند، به عنوان

	مثال آن‌هایی که کنترل های مربوط به آنها هزینه بر بوده یا پیاده سازی آنها سخت است یا جایی که مخاطره اشتباه برداشت شده است، دارا اهمیت می‌باشد. ممیز باید با نمونه‌برداری تایید کند که همه دارایی های مهمی که در فهرست دارایی آمده در ارزشیابی مخاطره در بر گرفته شده و نمونه های سناریوهای ارزیابی مخاطره، رخداد را برای ارزیابی این که آیا آن‌ها نیازها و اثرات کسب و کار را به طور مناسب منعکس می کنند. بازنگری کند. دسترس پذیری کارکنان شایسته برای کارکرد خوب ISMS مهم است. ممیز باید شواهدی را که مخاطره میان مدت و بلند مدت مرتبط با از دست دادن دسترس پذیری کارکنان به طور مناسب توسط سازمان ارزیابی شده و به جدیدترین نسخه بازنگری شده و کنترل‌های امنیت اطلاعات مناسب جهت افزایش انعطاف پذیری سازمان در مقابل این نقصان‌ها پیاده سازی شده، ارزشیابی کند.
	گزینه‌های برطرف‌سازی مخاطره (بند ۴-۲-۱ ج)
	ممیز باید گزینه های برطرف‌سازی مخاطره انتخاب شده سازمان را بازنگری کند. باید بازنگری شود که آیا «برطرف‌سازی» (به عنوان مثال کاهش از طریق استفاده کنترل‌ها مناسب، اجتناب از مخاطره، انتقال مخاطره به طرف‌های سوم و یا پذیرش آگاهانه مخاطرات در صورتی که در مدیریت مخاطره پذیری قرار می‌گیرند.) مناسبی برای تمامی مخاطرات شناسایی شده مشخص شده است. ممیز باید شکاف‌ها و ناهنجاری‌های دیگر را جستجو کند و وارسی کند که آیا تغییرات اخیر (به عنوان مثال سامانه‌های IT جدید یا فرآیند های کسب و کار) به طور مناسب در ارزشیابی مخاطره و تصمیم گیری های برطرف‌سازی مخاطره ثبت شده است.
الف-۳ انتخاب اهداف کنترلی و کنترل ها، مصوبات مخاطرات باقی‌مانده پیشنهاد شده، مجوز مدیریت و بیانیه کاربست پذیری (استاندارد ISO/IEC 27001 بند ۴-۲-۱ چ تا د)	
معیارهای ممیزی	استاندارد ISO/IEC 27001 بند ۴-۲-۱, چ – خ، پیوست الف
استانداردهای مربوط	استاندارد ISO/IEC 27005 بند ۹-۱، ۹-۲، ۱۰ استاندارد ISO/IEC 27006 بند ۹-۱-۲
شواهد ممیزی	شواهد ممیزی شامل موارد زیر است: • مستندات برای روش ارزشیابی مخاطره؛ • گزارش‌های ارزشیابی مخاطره؛ • مستنداتی که میزان کاهش مخاطره توسط کنترل‌های اتخاذ شده (نتایج ارزشیابی مخاطره) را توصیف می کند؛ • سوابق نشان‌دهنده مصوبات مخاطرات باقی‌مانده توسط مدیریت (به ویژه، جایی که مخاطرات باقی‌مانده بالاتر از سطح تعریف شده در معیار پذیرش مخاطرات است، توجیه آن‌ها باید شامل شود)؛ • سوابق نشان‌دهنده مجوز مدیریت در پیاده‌سازی و بهره برداری از ISMS؛ • بیانیه‌ی کاربست پذیری.
راهنمای عملی ممیزی	**انتخاب اهداف کنترلی و کنترل‌ها (بند ۴-۲-۱چ)**

برای الزامات امنیت اطلاعاتی بدست آمده از گزینه‌های ارزشیابی مخاطره و برطرف‌سازی مخاطره انتخاب شده برای الزامات، ممیز باید بازنگری کند که کنترل‌های مناسب انتخاب و اهداف کنترلی به منظور دستیابی با نمونه‌برداری مناسب طراحی می‌شوند. ممیز باید بازنگری کند که کنترل‌ها و اهداف انتخاب شده مطابق با الزامات امنیت اطلاعات در الزامات کنترلی تعریف شده در پیوست الف استاندارد ISO/IEC 27001 می باشند (برای تفسیر الزامات کنترل پیوست الف، نمونه‌های عملی برتر شرح داده شده به عنوان راهنمایی‌های پیاده‌سازی استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷می‌تواند مرجع خوبی باشد). هر اختلاف مهم در الزامات پیوست الف در انتخاب کنترل (به عنوان مثال در صورت وجود اهداف کنترلی پیوست الف و کنترل‌هایی که به وسیله سازمان مورد قبول نیستند یا اهداف اضافی و کنترل های انتخاب شده از خارج پیوست الف) باید از نظر منطقی شناسایی و بازنگری شود. به علاوه، ممیز باید وارسی کند که معمولا بهترین شیوه قابل قبول برای بخش کسب و کار وابسته در فرایند انتخاب کنترل در نظر گرفته شده است. بیان صریح همه الزامات امنیت اطلاعات به وسیله خط‌مشی سازمان، مقررات صنعت، قوانین یا قراردادها و غیره باید وارسی شود که به طور صحیح در اهداف کنترلی مستند و کنترل‌ها، وکاهش مخاطره ها به منظور شفاف سازی معیار پذیرش مخاطره منعکس شده است. باید تایید شود که برطرف‌سازی مخاطرات در صورتی که مخاطرات باقی‌مانده، معیار پذیرش مخاطره را حتی بعد از گزینش کنترل‌ها برآورده نسازند، به طور مکرر اعمال می‌شود.	
تصویب مخاطرات باقی‌مانده پیشنهادی (بند ۴-۲-۱ح) **مجوز مدیریت (بند ۴-۲-۱خ)**	
ممیز باید به طور خلاصه مخاطرات باقی‌مانده امنیت اطلاعات را ارزیابی کند و تایید کند که سازمان مصوبه مدیریت را برای مخاطرات باقی‌مانده که بعد از انتخاب کنترل های برطرف‌سازی مخاطره باقی مانده، به دست آورده است. باید وارسی شود که مدیریت به طور رسمی مخاطرات باقی‌مانده، اینکه مخاطرات در تعریف مخاطره پذیری سازمان هستند، اینکه تصمیمات پذیرش مخاطره به وسیله سطوح مجاز کافی مدیریت و نهادهای تصمیم گیری، گرفته شده اند، و اینکه هر کجا که سطوح مخاطرات باقی‌مانده نمی تواند به زیر معیارهای پذیرش کاهش داده شود، مدیریت تصمیم می گیرد به طور رسمی مخاطرات و دلایلی برای تصمیمی که ثبت شده را بپذیرد، پذیرفته و در نظر گرفته است. علاوه بر این، ممیز باید تایید کند که مدیریت مجاز به پیاده‌سازی و بهره برداری از ISMS است، برای مثال به واسطه یک شراکت نامه رسمی، تصویب پروژه، نامه پشتیبانی از مدیر عامل و غیره. باید وارسی شود که این تشریفات محض نیست و شواهدی که مدیریت واقعا ISMSرا می فهمد و حمایت می‌کند، وجود دارد.	
بیانیه کاربست پذیری[1] (۴-۲-۱ د)	
ممیز باید بیانیه کاربست پذیری سازمان را بازنگری کند که اهداف کنترل و کنترل‌ها را مستند و توجیه می‌کند، ، هم آنهایی که که قابل کاربرد است و هم آنهایی غیر قابل کاربرد است. مهم است که بیانیه کاربست پذیری اتصال بین مخاطرات شناسایی شده و اهداف کنترلی و کنترل‌هایی که برای کاهش آن‌ها انتخاب شده اند، را بیان می‌کند. همچنین مهم است که توجیهات برای کنترل‌های غیر قابل کاربرد ارائه شود. ممیز باید تایید کند که ورودی	

1- Statement of applicability

	های مناسب برای همه اهداف کنترلی و کنترل‌های فهرست‌شده در پیوست الف استاندارد ISO/IEC 27001 وجود دارند. بیانیه کاربست پذیری همچنین به دارا بودن کنترل های موجود، نیاز دارد. ضروری است که بیانیه کاربست پذیری بازنگری شده به وسیله یک سطح مدیریتی مناسب برای بازنگری با سوابق گذشته ایجاد شده، تصویب شده، بازبینی شده و به روز شده و غیره به عنوان شواهدتایید/مجاز شود.
الف-۴ انجام و عملکرد ISMS (۴-۲-۲)	
معیار ممیزی	استاندارد ISO/IEC 27001 بند ۴-۲-۲
استاندارد های مربوط	استاندارد ISO/IEC 27001 پیوست الف استاندارد ISO/IEC 27002 استاندارد ISO/IEC 27005 بند ۸-۲-۱-۴، ۹-۱
شواهد ممیزی	شواهد ممیزی موارد زیر را شامل می شوند: • طرح برطرف‌سازی مخاطره و سوابق پیشرفت پروژه‌های طرح‌ریزی • سوابق و روش‌های اجرایی مستند شده برای سنجش اثربخشی کنترل
راهنمای عملی ممیزی	ممیز باید تایید کند که سازمان طرح برطرف‌سازی مخاطره را با گزینه های برطرف‌سازی مخاطره تعریف شده تنظیم و پیاده‌سازی کرده است. این امر برای تایید موارد زیر مهم است: • طرح برطرف‌سازی مخاطره پیاده‌سازی‌شده، اولویت‌ها و مسئولیت‌ها را به حساب آورده است، طبق تعریف؛ • منابع کافی برای پشتیبانی از بهره برداری ISMS تخصیص داده شده است (به بند پ-۹ مراجعه شود)؛ • اولویت‌ها و زمان بندی برای پیاده‌سازی موثر برطرف‌سازی مخاطره به طور واضح تعریف شده است؛ • بودجه، نقش‌ها و مسئولیت‌ها برای برطرف‌سازی مخاطره به وضوح شناسایی شده است; و • طرح برطرف‌سازی مخاطره به طور فعال به عنوان یک ابزار مدیریت امنیت اطلاعات استفاده و به روز رسانی شده است. ممیز باید به وسیله نمونه‌برداری از پیاده سازی و کارایی کنترل‌ها بازنگری کند که ISMS با الزامات مستند ISMS پیاده سازی و اجرا شده است (بند ۴-۲-۱چ مراجعه شود) و پیوست الف از استاندارد ISO/IEC 27001 . لازم است شواهد مربوط به پشتیبانی یا رد ارتباط بین مخاطرات مستند و برنامه و کنترل های انجام شده جستجو کند. ممیز باید تایید کند که هدف و راه سنجش اثر بخشی کنترل‌های انتخاب شده به طور واضح تعریف شده است. توانایی وارسی این که آیا کنترل‌ها واقعا مخاطرات یا اثرات رخداد را در روش سنجش اثر بخشی کنترل‌ها کاهش می دهند، مهم است. (استاندارد ISO/IEC 27005 بند ۸-۲-۱-۴) در زمان ممیزی سنجش ISMS، توجه کنید که سنجش‌ها می توانند از روش‌های متعددی که برخی از آن‌ها پیچیده‌تر از برخی دیگر هستند، به دست آیند. ممیز باید آگاه شود که اگرچه راهنمایی در مورد سنجش ISMS وجود دارد، اما تا زمانی که معیار برای تولید نتایج قابل مقایسه و تکرارپذیر ارزشیابی اثربخشی کنترل، به وسیله مدیریت، تعریف و پذیرش می‌شود، الزامات استاندارد ISO/IEC 27001 برآورده خواهد شد. همچنین مهم است با در نظر گرفتن نتایج ارزیابی و مخاطره و فرآیندهای بر طرف سازی اطمینان حاصل شود که

	سنجش ISMS، الزامات کسب و کار سازمان برآورده می‌شود. سنجش موثر اطمینان حاصل می‌کند که کنترل به طور موثر در حال کاهش مخاطرات مربوطه است. در زمان ممیزی عملکرد ISMS، ممیز باید ارزیابی کند که چگونه سازمان از اثربخشی کنترل‌ها اطمینان حاصل می‌کند. برای این منظور ممیز باید گستره و کفایت سنجش ISMS را ارزیابی کند.
الف-۵ پایش و بازنگری ISMS (استاندارد ISO/IEC 27001 بند ۴-۲-۳)	
معیار ممیزی	استاندارد ISO/IEC 27001 بند ۴-۲-۳
استانداردهای مربوط	استاندارد ISO/IEC 27005 بند ۱۲-۱، ۱۲-۲
شواهد ممیزی	شواهد ممیزی عبارتند از: • گزارش‌های رویدادهای امنیتی/گزارش‌های رخدادها؛ • مستنداتی برای بازنگری‌های مدیریت (ورودی‌ها و خروجی‌ها)؛ • تعریف (روش‌های اجرایی) سنجش اثربخشی کنترل‌ها و سوابق مربوط به سنجش و ارزشیابی کنترل‌ها؛ • سوابق مربوط به استفاده از سنجش (شامل سنجش برای تقویت کنترل‌ها، سوابق اقدامات اصلاحی و پیشگیرانه و یک طرح برطرف‌سازی مخاطره)؛ • مستندات شامل اطلاعات در مورد دارایی‌های اطلاعاتی، تحلیل و ارزشیابی مخاطره، طرح برطرف‌سازی مخاطره و بیانیه کاربست پذیری؛ • طرح یک ساله برای امنیت اطلاعات.
راهنمای عملی ممیزی	ممیز باید پایش ISMS را بازنگری کند و فرآیندها را با استفاده از شواهدی نظیر طرح‌ها، صورت جلسات جلسات بازنگری، گزارش‌های مدیریتی بازنگری/ ممیزی داخلی ISMS، گزارش‌های نقض/حادثه و غیره را بازنگری کند. ممیز باید گستره‌ای که پردازش اشتباهات، نقض‌های امنیتی و دیگر رخدادهای شناسایی شده،گزارش شده و نشان داده شده است را ارزشیابی کند. مهم است تعیین شود که چگونه سازمان به طور موثر و فعالانه پیاده‌سازی ISMS را بازنگری می‌کند تا این اطمینان حاصل شود که کنترل‌های امنیتی شناسایی‌شده در طرح برطرف‌سازی مخاطره، خط‌مشی و غیره به درستی پیاده‌سازی شده و در حال بهره‌برداری هستند. ممیز همچنین باید سنجش ISMS و استفاده از آن‌برای راه‌اندازی بهبودهای مستمر ISMS را مورد بازنگری قرار دهد. همچنین باید تایید شود تغییراتی که باید در نظر گرفته شود (بند ۴-۳-۲ ت ۱ تا ۶ در استاندارد ISO/IEC 27001) در فرآیندهای شناسایی، تحلیل، ارزیابی و برطرف‌سازی مخاطرات منعکس شده است. علاوه بر این، باید تایید شود که مستندات و سوابق ISMS مربوط به ارزشیابی مخاطره به روز شده است. ممیز باید مراقبت ویژه‌ای در طول فرایندهای ممیزی پایش و بازنگری ISMS در نظر بگیرد. این‌ها بسته به نوع و اندازه سازمان کاملا متفاوت خواهد بود، اما فعالیت‌هایی که نیاز است توسط سازمان نشان داده شود، به طور واضح در استاندارد ISO/IEC 27001 آورده شده است. از نگرانی‌های خاص ممیزان موضوع تغییر است و این که آیا سازمان تغییرات داخلی و/یا خارجی برای عملیات خود در نظر گرفته است، و این که آیا این تغییرات بر ISMS اثر خواهد داشت.
الف-۶ نگهداری و بهبود ISMS (استاندارد ISO/IEC 27001 بند ۴-۲-۴ و ۸)	

معیار ممیزی	استاندارد ISO/IEC 27001 بند ۴-۱، ۴-۲-۴ و ۸
استانداردهای مربوط	استاندارد ISO/IEC 27001بند ۴-۲-۴ و ۸
شواهد ممیزی	شواهد ممیزی عبارتند از: • گزارش‌های بهبودهای تعیین شده از فعالیت‌های تعریف شده در ۲۷۰۰۱ بند ۴-۲-۳؛ • عدم تطابق گزارش‌ها؛ • گزارش‌های اقدام اصلاحی/پیشگیرانه ؛ • گزارش‌های رویداد امنیت/گزارش‌های رخداد؛ • روش‌های اجرایی مستند و کنترل‌ها در پشتیبانی از ISMS • سوابق عملیات ISMS • گزارش‌های ارزشیابی مخاطره • روش‌های اجرایی برای اقدام اصلاحی و پیشگیرانه • بیانیه کاربست پذیری
راهنمای عملی ممیزی	**نگهداری و بهبود ISMS (۴-۲-۴)**
	بهبودهای تعیین شده در بند ۴-۲-۲ الف از استاندارد ISO/IEC 27001 نشان دهنده بهبودهایی است که از طریق پایش و بازنگری فرآیندها در بند ۴-۲-۳ از استاندارد ISO/IEC 27001 شناسایی شده است. ممیز باید ابزار و سوابقی که برای بهبود های ISMS تعیین شده است و روش چگونگی پیاده‌سازی بهبودها را بازنگری کند. ممیز باید هم چنین به دنبال شواهد در فرم یادداشت‌های مدیریت، صورت جلسات، گزارش‌ها، رایانامه‌ها و غیره، برای مستندسازی نیاز به بهبود، مجوز دهی به آن‌ها و انجام آن‌ها باشد. ممیزان ISMS باید به دنبال شواهد ملموس بهبود در خط‌مشی‌ها، روش‌های اجرایی، روش‌ها و کنترل‌ها، ارزشیابی‌های مخاطرات جدید، بازنگری‌ها و تغییرات خط‌مشی IS، فعالیت‌های جدید کسب و کار شامل طرفین ذینفع جدید[1]، نگهداری (نه تنها در IT بلکه تسهیلات و تخمین طول عمر برای نصب)، ظرفیت و فعالیت‌های مدیریت رخداد، تغییرات اداره اطلاعات و روش‌های اجرایی انتقال همانند تغییرات در قانون، انطباق فنی و امنیتی برای طرفین خارجی، باشند. بنابراین در ممیزی، باید تایید شود که روش‌های اجرایی و فرایندها به منظور پیاده‌سازی بهبود، با الزامات مشخص شده در بند ۴-۲-۴ ب تا ت از استاندارد ISO/IEC 27001 انطباق دارد.
	بهبود ISMS (۸)
	بهبود مداوم (۸-۱)
	ممیز باید تصدیق کند[2] چگونه سازمان تعیین کرده است که آیا ISMS می‌تواند بهبود یابد، چگونه مخاطرات مرتبط را ارزیابی کرده و چگونه به الزامات امنیت شناسایی‌شده و پایش عملکرد ISMS مرتبط است. ممیز باید تصدیق کند که چگونه کل اهداف سازمان از طریق فرآیندهای مناسب به الزامات امنیت اطلاعات داخلی ، ترجمه شده است و چگونه این الزامات ابلاغ و پایش شده است.

1- New interested parties
2- Verify

بنابراین، ممیز باید شواهدی که سازمان در حال تحلیل داده‌های آن‌ها از پایش ISMS است را جستجو کند و سپس در صورت لزوم نتایج را برای ارزیابی اثر بخشی ISMS و بهبود ISMS در نظر گیرد. ممیز باید تایید کند که اهداف و اولویت های بهبود، با اهداف ISMS سازگار هستند. به هر حال، باید به این نتیجه رسید که سازمانی که خط‌مشی و اهداف مربوط به بهبود مستمر را ندارد، به وضوح مطابق با استاندارد نیست. اگر مدیریت هدفی (واقعی) برای بهبود تنظیم کرده و شواهدی برای بهبود وجود ندارد، این اطلاعات باید به مدیریت به منظور بازنگری بازخورد داده شود. از این رو مدیریت می‌تواند تصمیم بگیرد که چه نوع اقدامی مناسب است. برای مثال تنظیم مجدد هدف یا فراهم آوری وسایل دیگر به منظور تاثیر بر فرآیندها. اگر سازمان از آمار عملکرد (به عنوان مثال، کاهش تعداد رخدادهای امنیتی خاص) برای سنجش پیشرفت‌ها استفاده کند ، ممیز باید با دقت ارزیابی کند که آمار به طور واقعی مربوط به مخاطرات شناسایی شده است یا انتخاب بر اساس سادگی محاسبه است.	
اقدام اصلاحی (۸-۲)	
ممیز باید اطلاعات مربوط به اقدامات اصلاحی ISMS از قبیل گزارش‌ها و برنامه‌های اجرایی[1] را از بازنگری (های) مدیریتی یا ممیزی‌ها (به استاندارد ISO/IEC 27001 بخش ۷-۳ مراجعه شود)، درخواست‌های تغییر ISMS، بودجه ها/طرح سرمایه گذاری و موارد کسب و کار و غیره به دست آورده و بازنگری کند. ممیز باید شواهدی که ISMS به طور عمده بهبود یافته به عنوان یک نتیجه از بازخورد - وارسی مستندسازی مربوط به خاتمه برنامه اجرایی و غیره را برای تایید این که آیا عدم انطباق و علل ریشه‌ای آن‌ها در واقع به طور موثر توسط مدیریت در بازه‌های زمانی معقول حل شده‌اند جستجو کند. اغلب مواردی وجود دارند که چاره‌هایی[2] برای عدم انطباق در نظر گرفته می‌شوند، اما اقدامات به منظور جلوگیری از وقوع مجدد آن‌ها هنوز به کار گرفته نشده است چرا که تحلیل ریشه علل، شکست خورده است. با گزارش‌های اقدام اصلاحی، ممیز باید سوابق را از اقدامات اصلاحی بازنگری کند و تایید کند که آیا اقدامات ضبط شده از طریق راهبری مشاهدات در پایگاه موثر بوده و کاربردپذیر است. در رابطه با مدیریت مخاطرات ISMS، تحلیل ریشه علت باید انجام شود تا: • تعیین این که آیا به دلیل این حقیقت است که مخاطرات شناسایی نشده است؛ • اگر مخاطرات شناسایی شده است، وارسی کنید که آیا کنترل ها (سنجش‌ها) به مخاطرات اعمال شده است؛ • اگر مخاطرات شناسایی شده است و کنترل ها اعمال شده است، وارسی کنید که آیا کنترل های به کار گرفته برای مخاطرات مناسب هستند؛ و • اگر مخاطرات شناسایی شده است و کنترل ها اعمال شده است، تصدیق شود که آیا کنترل‌ها به طور موثر پیاده‌سازی شده یا همانطور که انتظار می‌رود انجام شده است. هر یک یا ترکیبی از موارد بالا عامل عدم تطابق خواهد بود. در زمینه مدیریت مخاطرات،	

1- Action plans
2 - Remedies

رخداد عدم تطابق می‌تواند به عنوان مخاطرات کنار گذاشته شده در نظر گرفته شود و عدم تطابق‌های بالقوه می‌تواند به عنوان مخاطرات پیش بینی شده در نظر گرفته شود. ممیز باید تصدیق و تایید کند که آیا علت ریشه‌ای عدم انطباق با تحلیل جزیی توصیف شده در بالا شناسایی شده است و اقدامات به کار گرفته شده در صورت امکان برای عدم تطابق با سوابق و حقایق مشاهده شده در پایگاه مناسب است.	
اقدام پیشگیرانه (۸-۳)	
علاوه بر بهبود ISMS ناشی از عدم انطباق واقعی از پیش شناسایی شده، ممیز باید تعیین کند که آیا سازمان مواضع فعالی را برای نشان دادن بهبود بالقوه، الزامات جدید پیش‌بینی‌شده یا جدید و غیره به کار می‌گیرد. ممیز باید به دنبال شواهد تغییرات ISMS (مانند اضافه کردن، تغییر یا از بین بردن کنترل‌های امنیت اطلاعات) در پاسخ به شناسایی مخاطرات تغییر یافته قابل توجه باشد. موارد زیر می‌تواند در زمان اقدامات پیشگیرانه ممیزی در نظر گرفته شود: ۱- چگونه سازمان عدم تطابق بالقوه و علل آن‌ها را تعیین می‌کند. مثال‌های نمونه عبارتند از: • شناسایی مخاطرات تغییر یافته یا جدید از طریق به روز رسانی ارزشیابی مخاطره (استاندارد ISO/IEC 27001 بند ۴-۲-۳ ت و ۸-۳)؛ • تحلیل روند[1] برای مشخصه‌های ISMS. روند بدتر می‌تواند نشان دهد که اگر اقدامی به‌کارگرفته نشود، سبب رخ دادن عدم انطباق می‌شود؛ • هشدارها به منظور اخطار زود هنگام از نزدیک شدن به شرایط عملیاتی «خارج از کنترل»؛ • پایش رخداد و روند تحلیل رخدادها؛ • ارزیابی عدم انطباق‌ها که در شرایط مشابه برای بخش های دیگر ISMS یا بخش های دیگر سازمان یا حتی در سازمان های دیگر رخ داده است؛ • فرآیند طرح‌ریزی برای شرایط قابل پیش بینی (به عنوان مثال به منظور گسترش، نگهداری یا تغییرات کارکنان) و برای موقعیت‌های غیرقابل پیش بینی (به عنوان مثال، تغییرات در قوانین، مشکلات وقایع طبیعی مانند طوفان، زمین لرزه، سیل و غیره) ۲- چگونه سازمان تعیین می‌کند چه اقدامی مورد نیاز است و چگونه پیاده‌سازی شده است. ممیز باید شواهدی را جستجو کند که: • سازمان علل عدم انطباق‌های بالقوه را تحلیل کرده است (استفاده از نمودار علت و معلول و دیگر ابزارهای امنیت اطلاعات ممکن است مناسب باشد.) • اقدامات لازم در تمام قسمت‌های مربوط سازمان به موقع مستقر شده است؛ • تعاریف روشنی از مسئولیت‌ها برای شناسایی، ارزیابی، پیاده‌سازی و بازنگری اقدامات پیشگیرانه وجود دارد؛ و • آموزش کافی برای کنترل‌های جدید یا تغییر یافته، ارائه شده است. ۳- ممیز باید تایید کند که: • سوابق مناسب، نگهداری می شود. • سوابق، انعکاسی درستی از نتایج است.	

1- Trend

	• سوابق، مطابق با استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷: در بند ۴-۳-۳ کنترل شده است. ۴- برای بازنگری اقدامات پیشگیرانه اخذ شده، ممیز باید در نظر بگیرد که آیا: • اقدامات موثر بوده‌اند (به عنوان مثال آیا از وقوع عدم تطابق‌ها جلوگیری شده و منافع اضافی ایجاد گردیده است؟) • نیازی برای ادامه اقدامات پیشگیرانه به همان روشی که هستند وجود دارد. • اقدامات پیشگیرانه باید تغییر کنند، یا لازم است اقدامات جدیدی طرح‌ریزی شود.
الف-۷ مستند سازی ISMS (استاندارد ISO/IEC 27001 بند ۴-۳)	
معیار ممیزی	استاندارد ISO/IEC 27001 بند ۴-۳-۱ تا ۴-۳-۳
استانداردهای مربوط	-
شواهد ممیزی	شواهد ممیزی مورد زیر را شامل می‌شود: مستند ISMS توصیف شده در استاندارد ۲۷۰۰۱ بند ۴-۳-۱ الف تا خ.
راهنمای عملی ممیزی	**الزامات مستندسازی (۴-۳)**
	مستندسازی ISMS (۴-۳-۱)
	شناسایی الزامات مستندسازی مشخص شده در ISMS مهم است . ممیز باید الزامات استاندارد ISO/IEC 27001 بند ۴-۳-۱ و چندین جای نشان داده شده در بندهای ۵ تا ۸، به علاوه کنترل‌های پیوست الف و همچنین الزامات مشخص شده درمستندسازی ISMS توسط سازمان را در نظر بگیرد. ممیز باید اطلاعات فرآیندهای عملیاتی ممیزی شونده‌ها را درخواست کرده و بدست آورد، با کارکنان درتمام سطوح (از جمله کارکنان اداری، کاربران و صاحبان فرآیند) مصاحبه کند و فعالیت‌های و رفتار های آن‌ها و کارایی فرآیند برای این که پیاده‌سازی و عملکرد ISMS در پایگاه مطابق با الزامات مشخص و مستند شده را مشاهده نماید. ضرورت برای هر مستندسازی باید با توجه به نیاز به سازگاری مشاهده شده ، اهمیت اطلاعاتی که در بر دارد و نقشی که هر مستندسازی می‌تواند در اجتناب از هر گونه مخاطرات قابل توجه، شناسایی‌شده بازی کند، ارزیابی شود.
	کنترل مستندسازی ISMS (۴-۳-۲)
	ممیز باید وجود و انطباق با روش اجرایی مستندشده برای کنترل به روز رسانی مستندسازی ISMS، خط‌مشی‌ها، روش‌های اجرایی، سوابق و غیره را وارسی کند. ممیز هم چنین باید تعیین کند که آیا تغییرات مستندسازی ISMS به طور رسمی کنترل شده است، به عنوان مثال تغییرات بازنگری شده و توسط مدیریت پیش تصویب شده و به تمام کاربران مستندسازی ISMS اعلام شده است، به عنوان مثال با به روز رسانی مرجع قطعی مجموعه‌ای از آنچه که در اینترانت شرکت نگهداری می‌شود و/یا اعلام صریح به همه کاربران مرتبط.
	سوابق ISMS (۴-۳-۳)
	ممیز باید محافظت کنترل‌های سوابق مهم ISMS مانند بازنگری‌های مختلف امنیت اطلاعات متنوع و گزارش‌های ممیزی، برنامه اجرایی، مستندات رسمی ISMS (ازجمله تغییرات

	مشابه)، کتاب‌های بازدیدکنندگان، دسترسی به فرم‌های مجوز/تغییر و غیره را ارزیابی کند. لازم است کفایت کنترل‌ها بر شناسایی، ذخیره‌سازی، حفاظت، بازیابی، زمان نگهداری و وضع مستندات به ویژه در شرایطی که الزامات قانونی و قراردادی وجود دارد و سایر الزامات مورد نیاز مربوط به پیاده‌سازی ISMS در انطباق با استاندارد ISO/IEC 27001 (به عنوان مثال حفاظت از اطلاعات شخصی) بازنگری شود.
الف-۸ مسئولیت مدیریت (استاندارد ISO/IEC 27001 بند ۵)	
معیار ممیزی	استاندارد ISO/IEC 27001 بند ۵-۱، ۵-۲-۱ و ۵-۲-۲
استانداردهای مربوط	استاندارد ISO/IEC 27006 ۹-۲-۳-۲-۲ خ استاندارد ISO/IEC 27001 بند ۴-۲-۱ب، ۵، پیوست الف ۵-۱-۱، الف ۶-۱-۱ استاندارد ISO/IEC 17021 بند ۹-۲-۳-۲ ج استاندارد ISO/IEC 27006 بند ۹-۲-۳-۲-۲ ج استاندارد ISO/IEC 27005 بند ۹-۲
شواهد ممیزی	شواهد ممیزی عبارتند از: • خط‌مشی ISMS با تاریخ تصویب، امضا و غیره؛ • سوابق بازنگری خط‌مشی ISMS؛ • طرح‌ها/برنامه‌های زمانبندی امنیتی برای فعالیت های ISMS، به عنوان مثال طرح برطرف‌سازی مخاطره، طرح/ برنامه تعلیم و آموزش، طرح/برنامه ممیزی داخلی و غیره؛ • صورت جلسات بازنگری مدیریت با مستندات ورودی/خروجی، صورت جلسات کمیته امنیت اطلاعات سازمان و غیره؛ • مستندات نقش‌ها و مسئولیت‌ها؛ • گزارش ممیزی‌های داخلی؛ • مصاحبه مدیریت؛ • سوابق تصویب مخاطرات باقی‌مانده، تصویب طرح برطرف‌سازی مخاطره، سوابق بازنگری‌های مدیریتی، تصمیم گیری بودجه برای طرح کسب و کار و نتایج تصویب درخواست‌های تصمیم گیری؛ • سوابق بازنگری‌های کنترل‌ها و فعالیت های PDCA؛ • معیارهای شایستگی؛ • منابع انسانی و سوابق شایستگی؛ • برنامه/طرح های آموزش؛ • گزارش‌های آموزش و سوابق.
راهنمای عملی	**تعهد مدیریت (۵-۱)**

ممیزی	ممیز باید میزان تعهد مدیریت به امنیت اطلاعات را با استفاده از شواهد زیر بازنگری کند: • تصویب مدیریتی رسمی خط‌مشی ISMS؛ • پذیرش مدیریت اهداف و طرح های پیاده‌سازی ISMS، با تخصیص منابع کافی و تعیین اولویت‌های مناسب به فعالیت‌های مربوط (به ۵-۲-۱ مراجعه شود) • نقش‌ها و مسئولیت‌های واضح برای امنیت اطلاعات از جمله فرآیندی برای تخصیص و پذیرش جوابگویی به منظور حفاظت مناسب از دارایی‌های اطلاعات با ارزش؛ • تفاهم‌نامه‌های مدیریت، رایانامه‌ها، صورت جلسات، سخنرانی‌ها، جلسات، کار، تشریح کار و غیره، بیان پشتیبانی و تعهد به ISMS؛ • معیار پذیرش مخاطره و پذیرش رسمی آن‌ها، مخاطره‌پذیری و غیره مربوط به مخاطرات امنیت اطلاعات؛ و • هدف‌گذاری[1]، تخصیص منابع و آماده سازی ممیزی‌های داخلی و بازنگری‌های مدیریت ISMS.
	تخصیص منابع ISMS (۵-۲-۱)
	ممیز باید تصدیق کند که منابع لازم برای پیاده‌سازی، نگهداری و بهبود ISMS به طور مناسب مدیریت می‌شود. بدین معنی که سازمان نیاز به شناسایی، طرح‌ریزی، دسترس‌پذیری، استفاده، پایش و تغییر منابع مناسب مورد نیاز دارد. توصیه می‌شود، مدیریت منابع به صورت مجزا بازنگری نشود. صرف نظر از روشی که سازمان فرآیندهایش را ساختار داده و شناسایی کرده است، ممیزان باید به تصدیق کفایت و موثر بودن مدیریت منابع برای دستیابی به نتایج طرح ریزی شده، قادر باشند. برای ممیزان مهم است که تصدیق کنند که آیا سازمان عملکرد حال و گذشته را (به عنوان مثال تحلیل هزینه-سود ، ارزشیابی مخاطره) در زمان تصمیم‌گیری این که چه منابعی باید تخصیص داده شود، ارزیابی کرده است. مدیریت منابع می‌تواند به وسیله مصاحبه با مدیریت و سایر کارکنان مسئول برای وارسی این که فرایندهای مناسب در جای خود هستند، ارزیابی شود. این امر نیازمند پشتیبانی با شواهد عینی جمع آوری شده در طول ممیزی است. شواهد می تواند در مراحل مختلف ممیزی – ورودی‌های بازنگری، عملکرد فرایند و خروجی‌ها کسب شود. این امر باید در زمان ممیزی همه فرآیندها و سامانه‌های مربوط و مستندسازی فرایند انجام شود، از قبیل: • تعهد مدیریت و مسئولیت ها؛ • فرآیند بازنگری مدیریت؛ • فرآیندهای ISMS از جمله مدیریت مخاطرات، اقدامات پیشگیرانه و اصلاحی و بهبود مستمر؛ • تشریح کار؛ و • بودجه و سوابق زمانی برای فعالیت‌های خاص ISMS. ممیزان باید از قضاوت‌های ذهنی در مورد کفایت منابع تخصیص داده شده به وسیله سازمان اجتناب کنند و باید نقش آن‌ها را برای ارزیابی اثر بخشی فرایندهای مدیریت منابع محدود کنند.
	آگاه‌سازی و آموزش ISMS (۵-۲-۲)

1- Scoping

ممیز باید آموزش کسانی که به طور خاص در عملکرد ISMS درگیر هستند و فعالیت‌های آگاه‌سازی امنیت اطلاعات کلی که همه کارمندان را هدف قرار می‌دهد، بازنگری کنند. باید وارسی شود که صلاحیت‌های لازم و الزامات آموزش/آگاه‌سازی برای متخصصان امنیت اطلاعات و سایر افراد با نقش‌ها و مسئولیت‌های خاص به طور واضح شناسایی شده، و آموزش امنیت اطلاعات و نیازهای آگاه‌سازی با بودجه مناسب پشتیبانی شده است. ممیز باید گزارش ارزیابی آموزش و غیره را بازنگری کند و به دنبال شواهد برای تایید اینکه همه اقدامات بهبود ضروری به درستی به کار گرفته شده‌اند، باشد. لازم است با نمونه برداری وارسی شود که سوابق منابع انسانی کارمندان، آموزش مرتبط با ISMS را ذکر کرده است. ممیز باید ارزشیابی کند که سطح کلی آگاه‌سازی امنیت اطلاعات با پیمایش[1]/ نمونه‌برداری یا بازنگری نتایج پیمایش/ نمونه‌ها به عنوان قسمتی از ISMS راهبری شده است. به منظور برآورده سازی صلاحیت/ اثربخشی الزامات استاندارد ISO/IEC 27001 ، سازمان به طور معمول به انجام چندین مورد نیاز خواهد داشت ازجمله: • شناسایی اینکه چه صلاحیت‌هایی برای کارکنان انجام دهنده کارهایی که امنیت اطلاعات را تحت تاثیر قرار می دهد، مورد نیاز است؛ • شناسایی کارکنان آماده انجام کار دارای شایستگی لازم؛ • تصمیم درباره صلاحیت‌های اضافی مورد نیاز؛ • تصمیم درباره چگونگی دستیابی به این صلاحیت‌های اضافی - آموزش کارکنان (خارجی یا داخلی)،آموزش تئوری یا عملی، استخدام کارکنان شایسته جدید، تخصیص کارکنان توانمند موجود به کارهای مختلف؛ • بازنگری اثر بخشی اقدامات صورت گرفته برای برآورده‌سازی نیازهای صلاحیت؛ و • بازنگری دوره‌ای شایستگی کارکنان. در طی فرایند، سازمان نیاز به نگهداری سوابق مناسب تحصیل، آموزش، مهارت و تجربه دارد. استاندارد ISO/IEC 27001 چگونگی پایه‌گذاری فرآیندی یا ماهیت دقیق نگهداری سوابق نگهداری را مشخص نمی‌کند. ۱- در ممیزی انطباق سازمان با شایستگی و الزامات ارزیابی آموزش، ممیز به طور معمول به دنبال شواهدی که موضوعات زیر در آدرس‌دهی می‌کند، می‌باشد: سازمان نیاز به شناسایی صلاحیت‌هایی مورد نیاز توسط کارکنان انجام دهنده کار که بر امنیت اطلاعات تاثیر گذارند، دارد. اهداف ممیز باید تعیین شود تا مشخص شود، رویکردی نظام‌مند برای شناسایی این صلاحیت‌ها و تصدیق اینکه رویکرد موثر است، وجود دارد. خروجی فرایند ممکن است یک فهرست، ثبت[2]، پایگاه داده، طرح منابع انسانی، طرح توسعه شایستگی ها، قرارداد، طرح محصول یا پروژه و غیره باشد. گفتگوها می‌تواند در ابتدا با مدیریت به منظور اطمینان از اینکه آن‌ها اهمیت شناسایی شایستگی موردنیاز را درک کرده‌اند، برگزار شود. این‌ها می تواند منابع بالقوه اطلاعات راجع به فرآیندها یا فعالیت‌های تغییر داده شده یا جدید، که ممکن است به سمت الزامات مختلف شایستگی در سازمان هدایت شود، باشد. بازنگری صلاحیت‌ها ممکن است زمانی که یک مناقصه یا قرارداد جدید در حال مطرح شدن است، مورد نیاز باشد. شواهد آن ممکن است در	

1- Surveying
2- Register

	سوابق مربوط یافت شود. الزامات شایستگی ممکن است در مستندات قرارداد آنجایی که فعالیت‌های پیمانکاران فرعی تاثیرگذار در فرآیندها و/یا امنیت اطلاعات است، گنجانده شود. ممیزان به تعیین این که سازمان نیازهای جدید یا تغییر داده شده شایستگی را، (به عنوان مثال در طول ممیزی نظارت) شناسایی کرده، نیاز دارند. ۲- ممیز باید بازنگری کند که کارکنان توانمند به کارهایی که به فعالیت‌های لازم برای کنترل امنیت اطلاعات نیاز دارد، تخصیص داده شده‌اند. ممیز باید تصدیق کند که نوعی از فرایند ارزیابی به منظور حصول اطمینان از مناسب بودن شایستگی ها برای فعالیت های سازمان، در محل وجود دارد. و اینکه کارکنان توانمند انتخاب شده در حال اثبات شایستگی مناسب می‌باشند. همچنین، فرایند باید اطمینان حاصل کند که همه کمبودها مورد توجه قرار گرفته و اثربخشی کارکنان درحال سنجش است. لازم است بررسی شود فعالیت‌هایی که امنیت اطلاعات را تحت تاثیر قرار می دهند به وسیله اشخاص صالح انتخاب شده انجام می شوند. شواهد ممکن است در طی ممیزی با تاکید بر فرایندها، فعالیت‌ها، کار و محصولات که دخالت انسانی ممکن است بزرگترین تاثیر را داشته باشد، به دست بیاید. ممیز ممکن است، تشریح کار، فعالیت‌های بازرسی یا آزمایش، فعالیت‌های پایش، سوابق بازنگری مدیریت، تعریف مسئولیت‌ها و مجوزها، سوابق عدم انطباق، گزارش‌های ممیزی، شکایات مشتری، سوابق اعتبارسنجی فرآیندها و غیره را بازنگری کند. ۳- سازمان به ارزیابی اثر بخشی اقدامات صورت گرفته برای برآورده‌سازی نیاز های شایستگی نیاز دارد. سازمان ممکن است از تعدادی از فناوری‌ها شامل نقش– بازی، بازنگری دوگانه، مشاهده، بازنگری آموزش و سوابق شغلی و/یا مصاحبه ها (به استاندارد ISO 19011:2011، جدول ۲، برای نمونه های بیشتر مراجعه شود) استفاده کند.. تناسب یک روش ارزیابی ویژه به عوامل بسیاری بستگی دارد. برای مثال، سوابق آموزش می تواند برای تصدیق اینکه یک دوره آموزشی به طور موفق کامل شده، دیده شود. به هر حال، این روش مشابه برای ارزیابی اینکه آیا ممیز به طور رضایت بخش در طی ممیزی کار کرده است، قابل پذیرش نخواهد بود. در عوض، ممکن است نیاز به مشاهده، بازنگری دوگانه، مصاحبه و غیره داشته باشد. سازمان ممکن است به اثبات حصول شایستگی کارکنان با تلفیقی از تحصیل، آموزش و یا تجربه نیاز داشته باشد. ۴- حفظ صلاحیت ممیز به تصدیق این که نوعی از فرایند پایش موثر به کار گرفته شده و اعمال شده، نیاز دارد. راه های انجام آن شامل فرایند توسعه تخصصی مداوم (مطابق بند ۷-۴ استاندارد ISO 19011)، ارزیابی منظم کارکنان و عملکرد آن‌ها، یا بازرسی منظم، آزمون یا ممیزی محصول یا سامانه برای افراد یا گروه های مسئول، است. تغییرات مداوم در الزامات شایستگی ممکن است نشان دهد که یک سازمان در نگهداری سطوح عملکرد کارکنان فعال است.
الف- ۹ ممیزی داخلی ISMS و بازنگری مدیریت ISMS (استاندارد ISO/IEC 27001 بند ۶ و ۷) این بند راهنمایی به منظور ممیزی خارجی یا خود وارسی یا راهنمایی ارزیابی دوگانه برای ممیزی داخلی فراهم می‌کند.	
معیار ممیزی	استاندارد ISO/IEC 27001بند ۶، ۷
استانداردهای مربوط	استاندارد ISO/IEC 27005 بند ۷-۹ استاندارد ISO/IEC 27006 بند ۹-۱-۲، ۹-۱-۴، ۹-۲-۳-۲

	استاندارد ISO/IEC 17021 بند ۹-۲-۳-۲، ۹-۳-۲-۱
شواهد ممیزی	شواهد ممیزی عبارتند از: • برنامه ممیزی‌های داخلی، طرح ها، گزارش‌های و سوابق؛ • صورت جلسات بازنگری مدیریت با مستندات ورودی و خروجی؛ • گزارش‌های ارزشیابی مخاطره.
راهنمای عملی ممیزی	**ممیزی داخلی ISMS (۶)** ممیز باید، ممیزی‌های داخلی ISMS سازمان را با استفاده از برنامه های ممیزی ISMS، طرح ها، گزارش‌های ممیزی، طرح‌های اقدام و غیره بازنگری کند. باید تصدیق شود که مسئولیت‌ها برای راهبری ممیزان داخلی ISMS به طور رسمی، به ممیزان به قدر کافی آموزش دیده و دارای شایستگی اختصاص داده شده است. ممیزان باید حدی که ممیزی‌های داخلی ISMS تایید می‌کنند که ISMS الزامات تعریف شده در استاندارد ISO/IEC 27001 و الزامات قانونی و قراردادی و دیگر الزامات و الزامات ISMS سازمانی مشخص شده از طریق فرآیند ارزشیابی مخاطره را در نظر بگیرند. استاندارد ISO/IEC 27001 بند۶ الف – ۶ د می‌تواند به چک لیست‌ها برای پشتیبانی ممیز توسعه یابد. ممیز باید هم چنین طرح‌های عملیاتی توافق شده، اقدامات اصلاحی و غیره که در بازه‌های زمانی توافقی تایید و توافق شده‌اند را وارسی کند و توجه ویژه‌ای به هرگونه اقدامات عقب افتاده برای مثال‌های جاری نماید. سازمان باید قادر به بیشینه کردن استفاده از منابع در دسترس در طول راهبری فعالیت‌های ممیز ISMS داخلی باشد. باید شواهدی موجود باشد که سازمان: • الزامات شایستگی برای ممیزان داخلی ISMS خود را شناسایی کرده است؛ • آموزش مناسب را فراهم کرده است؛ • فرآیندی برای پایش عملکرد ممیزان داخلی ISMS و تیم‌های ممیزی وجود دارد؛ و • کارکنان تیم‌های ممیزی که دانش مناسب بخش خاص را دارند، در بر می‌گیرد. (از این رو آن‌ها قادر به شناسایی این که تغییر در فرآیند یا فعالیتی خاص ممکن است منجر به پیامدی قابل توجه برای امنیت اطلاعات شود، هستند.) باید معلوم شود که سازمان برای اطمینان از موثر بودن و کارایی استفاده از منابع، ممیزی‌های داخلیISMS را طرح‌ریزی و روش‌های ممیزی آن را تعریف کرده است. هم چنین این امر باید کمک کند تا اطمینان حاصل شود که مخاطرات ذاتی از شکست ممیزی در فرآیند ممیزی و خروجی ممیزی کمینه شود. سازمان باید فرآیندی برای استفاده از نتایج ممیزی گذشته در طرح‌ریزی ممیزی‌های داخلی ISMS آینده داشته باشد. ممیز باید تصدیق کند که سازمان از چنین اطلاعاتی در زمان پایه‌گذاری ممیزی دوره‌ای[1] چنین فرآیندها و فعالیت‌هایی استفاده می‌کند. با در نظر گرفتن عوامل فوق و با بررسی اینکه آیا فرآیند ممیزی داخلی ISMS منجر به بهبودهای ملموس برای ISMS شده است، ممیزان ISMS باید قادر به قضاوت این که آیا سازمان یک برنامه ممیزی داخلی ISMS موثر را پیاده‌سازی کرده است، باشند. همچنین

1- Audit frequency

	ممیزISMS باید قادر به قضاوت این باشند که آیا خروجی ممیزی‌های داخلی ISMS شواهد کافی برای استفاده به عنوان بخشی از فرآیند بهبود ISMS را فراهم می‌کند.
	بازنگری مدیریت ISMS (۷)
	بازنگری مدیریت ممیزی ISMS (۷-۱)
	استاندارد ISO/IEC 27001 به مدیریت بازنگریISMS سازمان در طرح‌ریزی زمانی (حداقل یک بار در سال) برای اطمینان از مناسب بودن تداوم ،کفایت و اثر بخشی آن، نیاز دارد. اینکه چه زمانی مدیریت از پیش ISMS را بازنگری کرده و چه زمانی در طرح بعدی باید بازنگری شود، باید تعیین شود. دوره‌های بازنگری‌ها باید تعریف شود، به عنوان مثال، در خط‌مشی ISMS یا کتاب راهنما خط‌مشی ISMS. بازنگری می‌تواند در یک جلسه جداگانه انجام شود اما این الزام استاندارد نیست. راه‌های بسیاری که مدیریت می‌تواند ISMS را بازنگری کند، وجود دارد، مانند دریافت و بررسی گزارش‌ها، ارتباطات الکترونیکی یا به عنوان بخشی از جلسات منظم مدیریت که مسائلی از قبیل بودجه و اهداف نیز در آن مطرح می‌شود. مدیریت فرآیند بازنگری نباید فقط یک بررسی انجام شده برای برآورده کردن الزامات استاندارد و ممیزان باشد. این مدیریت باید بخش کاملی از فرآیند مدیریت کسب و کار سازمان باشد. بازنگری مدیریت کلان، فرآیند پیچیده‌ای است که در سطوح مختلف سازمان انجام می‌شود و باید همیشه یک فرآیند دو طرفه باشد،که توسط مدیریت ارشد با ورودی‌ها از تمام سطوح در سازمان تولید شده باشد. این فعالیت‌ها می‌تواند از جلسات روزانه، هفتگی، ماهانه، واحد سازمانی تا بحث‌های ساده و گزارش‌ها متفاوت باشد. ممیزان باید شواهدی که ورودی ها و خروجی ها فرآیند بازنگری مدیریت مربوط به اندازه و پیچیدگی سازمان هستند و برای بهبود ISMS استفاده می‌شوند را جستجو کنند. هم چنین باید در نظر بگیرند که چگونه مدیریت سازمان ساختار داده شده و فرآیند بازنگری مدیریت در این ساختار استفاده می‌شود. سوابق بازنگری مدیریت مورد نیاز است اما قالب آن‌ها مشخص نیست. صورت جلسات معمول‌ترین نوع سوابق هستند، اما سوابق الکترونیکی، نمودارهای آماری، ارائه و غیره می‌تواند از انواع سوابق قابل قبول باشد. مهم است که اطمینان حاصل شود شواهدی برای مد نظر قراردادن تمام مسائل فهرست شده در استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ بند ۷ وجود دارد. حتی جایی که تصمیم گرفته شده، هیچ اقدامی لازم نیست. فرآیند بازنگری مدیریت ممکن است شامل مولفه‌های طرح‌ریزی ISMS جایی که تغییرات برای فرآیندها و سامانه‌ها در نظر گرفته می‌شود، باشد. در این مورد، ممیزان باید بازنگری کنند که نکات زیر در نظر گرفته شده است یا خیر: • آیا پیشنهاد تغییرات قبل از پیاده‌سازی ارزیابی می‌شوند؟ • در تهیه طرح‌های راهبردی، مسائل مربوط به ISMS در نظر گرفته می‌شود؟ • آیا کنترل‌های مورد نیاز پیش از شناسایی تغییرات پیاده‌سازی می‌شود؟ به عنوان مثال، در شروع برون سپاری یک فرآیند
	ورودی بازنگری مدیریت (۷-۲)
	استاندارد ISO/IEC 27001 بند ۷-۲ ورودی ها و عناوینی که باید در بر گرفته شود را

مشخص می‌کند. به هر حال، اینها تنها موضوعاتی که می‌توانند در بازنگری گنجانده شوند، نیستند. ممکن نیست آن‌ها به صورت مجزا یا به طور همزمان به عنوان بخشی از بازنگری کلی کسب و کار مورد خطاب قرارگرفته باشند. ممیزان باید آگاه باشند که ورودی ها می‌توانند در اشکال زیادی مانند گزارش‌ها، نمودار روند و به همین ترتیب باشند.

با بازنگری گزارش‌های مدیریت، صورت جلسات و سوابق دیگر و/یا با مصاحبه با آنهایی که درگیر بودند، باید وارسی شود چه چیزی در بازنگری مدیریت قبلی وجود داشته است. (استاندارد ISO/IEC 27001 ، نه مورد مانند نتایج ممیزان /بازنگری‌های دیگر، بازخوردها و پیشنهادات بهبود، اطلاعات آسیب‌پذیری‌ها و تهدیدات و غیره را مشخص می‌کند. لازم است این که تا چه حد مدیریت نقش یک بخش فعال را بازی کرد و به طور کامل و در بازنگری‌ها درگیر شده، ارزشیابی شود.

خروجی بازنگری مدیریت (۷-۳)

استاندارد ISO/IEC 27001 بند ۷-۳ خروجی ها برای فرآیند بازنگری مدیریت و هرگونه تصمیم گیری‌ها و اقدامات مربوط به این موضوع‌های الف-ث که باید شامل شوند را مشخص می‌کند. ممیز باید خروجی‌های هر گونه بازنگری مدیریت قبلی شامل تصمیمات کلیدی مدیریت، طرح‌های اقدام و سوابق مربوط به تایید این که اقدامات توافقی به موقع انجام شده است را وارسی کند. همانند خروجی فرآیند بازنگری مدیریت، باید شواهدی از تصمیمات راجع به الف – ث موجود باشد. از قبیل:

- تغییر اهداف و خط‌مشی ISMS؛
- طرح‌ها و اقدامات ممکن برای بهبودها؛
- تغییر منابع؛
- طرح‌های تجدیدنظر شده کسب و کار؛
- بودجه‌ها؛
- بیانیه کاربست پذیری تجدیدنظر شده؛ و
- سنجش‌های کنترل تجدیدنظر شده.

خروجی فقط مربوط به بهبود یا تغییرات نیست، بلکه می‌تواند شامل تصمیمات دیگر موضوعات مهم مانند طرح‌های معرفی کننده فناوری‌های جدید، سامانه ها یا محصولات باشد. با توجه ویژه به اقداماتی که به موقع یا به طور صحیح تکمیل نشده است، اگر لازم باشد، تایید کندکه اقدامات خاتمه یافته به درستی تکمیل شده اند.

کتاب‌نامه

[1] ISO/IEC 17021:2011, Conformity assessment — Requirements for bodies providing audit and certification of management systems

[۲] استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سیستمهای مدیریت امنیت اطلاعات – آیین کار مدیریت امنیت اطلاعات

[3] ISO/IEC 27003:2010, Information technology — Security techniques — Information security management system implementation guidance

[۴] استاندارد ملی ایران شماره ۱۴۰۹۶: سال ۱۳۸۹، فناوری اطلاعات – فنون امنیتی –مدیریت امنیت اطلاعات – سنجش

[5] ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk management

[۶] استاندارد ملی ایران شماره ۲۷۰۰۶: سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – الزامات نهادهای ممیزی‌کننده و گواهی‌کننده سیستم‌های مدیریت امنیت اطلاعات

[7] IAF MD1:2007, IAF Mandatory Document for the Certification of Multiple Sites Based on Sampling International Accreditation Forum