INSO/ISO
19011
1st.Revision
Identical with
ISO 19011: 2011
(Second edition)
2014

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization

استاندارد ایران- ایزو
۱۹۰۱۱
تجدید نظر اول

۱۳۹۲

رهنمودهایی
برای ممیزی سیستم‌های مدیریت

Guidelines
for auditing management systems

ICS: 03.120.10, 13.020.10

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ ۳ 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.

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

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

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

سازمان ملی استاندارد ایران از اعضای اصلی سازمان 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 می‌کند . در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی ، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می‌تواند 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 کشور و/ یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید.

سازمان می‌تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور ، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید . همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره ، آموزش ، بازرسی ، ممیزی و صدور گواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی ، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش ، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم ، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می‌کند . 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 سازمان است .

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

کمیسیون فنی تدوین استاندارد

"رهنمودهایی برای ممیزی سیستم‌های مدیریت"

(تجدید نظر اول)

رئیس:	**سمت و/ یا نمایندگی**
روزبه، میرمحمد (دکترای مدیریت)	دبیر انجمن علمی کیفیت ایران
دبیر:	
طوماریان، سهیلا (لیسانس مهندسی الکترونیک)	رئیس گروه تایید صلاحیت نهادهای گواهی کننده سیستم‌های مدیریتی مرکز ملی تایید صلاحیت ایران- سازمان ملی استاندارد ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
تجلی، سیامک (کارشناس ارشد مدیریت)	مشاور شرکت مهندسی سامان نیرو پاد
حسینی، شبنم (لیسانس مهندسی صنایع)	شرکت انطباق کیفیت آسیا
رامین، یاسین (کارشناس ارشد مدیریت)	شرکت گواهی کننده سیستم‌های مدیریت CCPL
رسولی، حسنعلی (لیسانس مهندسی مکانیک)	مشاور ارشد شرکت مشاوران فنّاوری اطلاعات آگاهان
زرین چنگ، الهام (لیسانس مهندسی شیمی)	کارشناس تایید صلاحیت نهادهای گواهی کننده سیستم‌های مدیریتی مرکز ملی تایید صلاحیت ایران– سازمان ملی استاندارد ایران

کمیسیون فنی تدوین استاندارد (ادامه)

سید احمدیان، مهستی (لیسانس علوم آزمایشگاهی)	کارشناس ارشد گروه کارشناسان ایران- کیش
شاهوردی، عاطفه (کارشناسی آمار)	کارشناس تایید صلاحیت نهادهای گواهی کننده سیستم‌های مدیریتی مرکز ملی تایید صلاحیت ایران- سازمان ملی استاندارد ایران
فارغ، فریدون (کارشناسی بهداشت حرفه ای)	مدیر عامل شرکت ارزیابان کیفیت خاور میانه
طهماسبی، افشار، منیژه (لیسانس علوم تغذیه)	معاون تایید صلاحیت در امور مشاوران و سیستم‌های مدیریتی مرکز ملی تایید صلاحیت ایران- سازمان ملی استاندارد ایران
منتظری، مریم (کارشناسی ارشد شیمی- معدنی)	کارشناس تایید صلاحیت آزمایشگاه-های آزمون/کالیبراسیون مرکز ملی تایید صلاحیت ایران - سازمان ملی استاندارد ایران
هوسپ سرکسیان، هوسپ (لیسانس مهندسی برق)	کارشناس استاندارد- بازنشسته سازمان ملی استاندارد ایران

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد"رهنمودهایی برای ممیزی سیستم‌های مدیریت "نخستین بار تحت عنوان" رهنمودهایی برای ممیزی سیستم‌های مدیریت کیفیت و/یا زیست محیطی" در سال ۱۳۸۶ تدوین شد. این استاندارد بر اساس پیشنهادهای رسیده و بررسی توسط سازمان ملی استاندارد و تحقیقات صنعتی ایران و تایید کمیسیون‌های مربوط برای اولین بار مورد تجدید نظر قرار گرفت و در یکصد و چهل و ششمین اجلاسیه کمیته ملی مدیریت کیفیت مورخ ۹۲/۱۲/۲۰ تصویب شد.

اینک این استاندارد به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

این استاندارد جایگزین استاندارد ایران – ایزو ۱۹۰۱۱ سال ۱۳۸۶ می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظرخواهد شد و هرپیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظردرکمیسیون فنی مربوط مورد توجه قرارخواهدگرفت. بنابراین، باید همواره ازآخرین تجدید نظراستانداردهای ملی استفاده کرد مگر آن که در استاندارد به صورت دیگری مشخص شده باشد.

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

ISO 19011: 2011 Guidelines for auditing management systems

مقدمه

بعد از انتشار ویرایش اول استاندارد بین المللی ISO 19011 در سال ۲۰۰۲، تعدادی از استانداردهای جدید سیستم مدیریت منتشر شده است. در نتیجه، حالا این نیاز وجود دارد که دامنه شمول وسیع تری از ممیزی سیستم‌های مدیریت و همچنین ارائه راهنمایی‌هایی که عام تر می باشند، در نظر گرفته شود.

در سال ۲۰۰۶، کمیته بین المللی ارزیابی انطباق ISO/CASCO، استاندارد ISO/IEC 17021 را تدوین کرد که الزامات مربوط به گواهی کردن سیستم‌های مدیریت توسط شخص ثالث را بیان می کرد و بر مبنای راهنمایی-های ارائه شده در ویرایش اول استاندارد بین المللی ISO 19011 بود.

ویرایش دوم استاندارد ISO/IEC 17021 که در سال ۲۰۱۱ منتشر گردید برای تبدیل راهنمایی‌های ارائه شده در استاندارد ISO 19011 به الزامات مربوط به ممیزی‌های گواهی کردن سیستم مدیریت، بسط یافته بود. به این مفهوم که ویرایش دوم این استاندارد راهنمایی‌هایی را به تمامی استفاده کنندگان از جمله سازمان‌هایی با اندازه کوچک و متوسط ارائه می‌کند و بر مواردی که معمولا "ممیزی‌های درون سازمانی" (شخص اول) و "ممیزی هایی که توسط مشتریان در مورد تامین کنندگان خود انجام می‌شود" (شخص دوم) نامیده می‌شود، متمرکز است. هرچند آن‌هایی که در ممیزی گواهی کردن سیستم مدیریت دخیل می باشند از الزامات استاندارد ISO/IEC 17021: 2011 پیروی می‌کنند، ممکن است راهنمایی‌های این استاندارد را نیز مفید بیابند.

ارتباط بین استاندارد ISO 19011: 2011 و ISO/IEC 17021: 2011 در جدول ۱ نشان داده شده است.

جدول ۱- دامنه شمول استاندارد ISO 19011: 2011 و ارتباط آن با استاندارد ISO/IEC 17021: 2011

ممیزی درون سازمانی	ممیزی برون سازمانی	
برخی اوقات ممیزی شخص اول نامیده می‌شود	ممیزی تامین کنندگان	ممیزی شخص ثالث
	برخی اوقات ممیزی شخص دوم نامیده می‌شود	برای مقاصد قانونی، مقرراتی و مشابه برای گواهی کردن (همچنین به الزامات استاندارد ISO/IEC 17021: 2011 مراجعه شود)

این استاندارد الزامات را بیان نمی‌کند و لیکن درخصوص مدیریت برنامه ممیزی، درخصوص طرح‌ریزی و انجام ممیزی سیستم مدیریت و نیز در خصوص شایستگی و ارزیابی ممیز و تیم ممیزی راهنمایی‌هایی را ارائه می‌کند.

سازمان‌ها می‌توانند بیش از یک سیستم مدیریت رسمی داشته باشند. به منظور سهولت در قابلیت فهم این استاندارد، اصطلاح "سیستم مدیریت" به صورت مفرد ترجیح داده شده است. با این وجود مخاطب این استاندارد می‌تواند اجرای این راهنمایی‌ها را با موقعیت خاص خود وفق دهد . این موضوع همچنین در خصوص استفاده از "شخص" و "اشخاص"، "ممیز" و "ممیزان" صادق است.

این استاندارد برای به کارگیری در خصوص گستره وسیعی از کاربران بالقوه از جمله ممیزان، سازمان‌هایی که سیستم‌های مدیریت را اجرا می‌کنند و سازمان‌هایی که نیاز به انجام ممیزی‌های سیستم مدیریت به دلایل قراردادی یا مقرراتی دارند، در نظر گرفته شده است. با وجود این کاربران این استاندارد می توانند این راهنمایی را برای ایجاد الزامات خود در ارتباط با ممیزی به کار برند.

راهنمایی‌های ارائه شده دراین استاندارد می‌تواند همچنین به منظور خود اظهاری به کار رود و برای سازمان‌هایی که در آموزش ممیزان یا گواهی کردن کارکنان دخیل هستند، مفید باشد.

راهنمایی‌های ارائه شده در این استاندارد به گونه ای در نظر گرفته شده است که قابل انعطاف باشد. همان گونه که در نقاط مختلف در این متن نشان داده شده است، استفاده از این راهنمایی‌ها بر اساس اندازه و سطح بلوغ سیستم مدیریت سازمان و براساس ماهیت و پیچیدگی سازمان مورد ممیزی و نیز بر اساس اهداف و دامنه شمول ممیزی‌هایی که قرار است انجام شود، می‌تواند متفاوت باشد.

این استاندارد مفهوم ریسک مربوط به ممیزی سیستم‌های مدیریت را معرفی می‌کند. رویکرد پذیرفته شده با هر دو ریسک مربوط به" فرایند ممیزی که اهداف آن تحقق نیافته است" و " ممیزی که امکان بالقوه دارد با اهداف و فعالیت‌های سازمان ممیزی‌شونده تداخل داشته باشد"، مرتبط می‌باشد. این استاندارد راهنمایی‌های مشخصی را در خصوص فرایندهای مدیریت ریسک سازمان ارائه نمی‌کند و لیکن مشخص می‌کند که سازمان‌ها می توانند فعالیت ممیزی را بر روی موضوعات حائز اهمیت برای سیستم مدیریت متمرکز سازند.

این استاندارد رویکردی را که دو یا چند سیستم مدیریت در رشته‌های تخصصی[1] مختلف با یکدیگر ممیزی می-شوند، می پذیرد. این کار اغلب "ممیزی ترکیبی" نامیده می‌شود. هرگاه این سیستم‌ها در یک سیستم مدیریت واحد ادغام شوند، اصول و فرایندهای ممیزی کردن همانند ممیزی ترکیبی می باشند.

در بند ۳، واژه‌ها و اصطلاحات و تعاریف کلیدی به کار رفته در این استاندارد ارائه شده است. تمامی تلاش‌ها به کار گرفته شده است تا اطمینان حاصل شود که این تعاریف با تعاریف به کار رفته در سایر استانداردها در تعارض نباشند.

دربند ۴ اصولی که ممیزی مبتنی بر آن است، تعریف شده است. این اصول به استفاده کننده کمک می‌کند که ماهیت اصلی ممیزی را درک کند و آن‌ها برای درک راهنمایی‌های ارائه شده در بندهای ۵ تا ۷ حایز اهمیت هستند.

در بند ۵ راهنمایی‌هایی در خصوص استقرار و مدیریت برنامه ممیزی، تعیین اهداف برنامه ممیزی و هماهنگی فعالیت‌های ممیزی ارائه شده است.

در بند ۶ راهنمایی‌هایی در خصوص طرح‌ریزی و انجام ممیزی سیستم مدیریت ارائه شده است.

در بند ۷ راهنمایی‌هایی در ارتباط با شایستگی و ارزیابی ممیزان سیستم مدیریت و تیم‌های ممیزی ارائه شده است.

پیوست الف به کارگیری راهنمایی‌های ارائه شده در بند ۷ برای رشته‌های تخصصی مختلف را شرح می دهد.

پیوست ب راهنمایی‌های تکمیلی برای ممیزان در خصوص طرح‌ریزی و انجام ممیزی‌ها را شرح می دهد.

1-Disciplines

رهنمودهایی برای ممیزی سیستم‌های مدیریت

۱ هدف ودامنه کاربرد[1]

این استاندارد راهنمایی‌هایی در مورد ممیزی سیستم‌های مدیریت شامل اصول ممیزی، مدیریت برنامه ممیزی و اجرای ممیزی‌های سیستم مدیریت و نیز راهنمایی‌هایی در مورد ارزیابی شایستگی افراد دخیل در فرایند ممیزی شامل افراد مدیریت کننده برنامه ممیزی، ممیزان و تیم‌های ممیزی ارائه می‌کند.
این استاندارد در خصوص کلیه سازمان‌هایی که نیاز به انجام ممیزی‌های درون سازمانی و برون سازمانی سیستم‌های مدیریت یا مدیریت برنامه ممیزی دارند، قابل استفاده است.
به کارگیری این استاندارد برای سایر انواع ممیزی‌ها، به شرط توجه ویژه به شایستگی خاص مورد نیاز، امکان پذیر است.

۲ مراجع الزامی

این استاندارد فاقد مراجع الزامی است. این بند به منظور حفظ شماره گذاری یکسان با دیگر استانداردهای سیستم مدیریت در نظر گرفته شده است.

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر کاربرد دارد:

۱-۳

ممیزی

فرایندی نظام‌مند، مستقل و مدون به منظور به دست آوردن **شواهد ممیزی** (۳-۳) و ارزیابی آن‌ها به صورت عینی به منظور تعیین میزانی که **معیارهای ممیزی** (۳-۲) برآورده می‌شوند

یادآوری ۱- ممیزی‌های درون سازمانی که گاه "ممیزی شخص اول" نامیده می‌شود توسط خود سازمان یا از جانب آن برای بازنگری مدیریت و سایر مقاصد داخلی انجام می‌گیرد (برای مثال تایید اثر بخشی سیستم مدیریت یا به‌دست آوردن اطلاعات برای بهبود سیستم مدیریت). ممیزی‌های درون سازمانی می‌تواند مبنایی برای خود اظهاری سازمان درباره انطباق باشد. دربسیاری موارد، به ویژه در سازمان‌های کوچک‌تر استقلال را می توان با مبرا بودن از مسئولیت در خصوص فعالیت مورد ممیزی یا مبرا بودن از گرایش و تعارض منافع اثبات نمود.

یادآوری ۲- ممیزی‌های برون سازمانی شامل ممیزی‌های "شخص دوم" و "شخص ثالث" است. ممیزی‌های شخص دوم توسط طرف‌هایی انجام می‌شوند که در سازمان ذی‌نفع می باشند، یا از جانب آن‌ها توسط سایر اشخاص انجام می‌شود. ممیزی-

1-Scope

های شخص ثالث توسط سازمان‌های ممیزی کننده مستقل مانند سازمان‌های تنظیم کننده مقررات [1]یا سازمان هایی که خدمت گواهی کردن را ارائه می‌کنند، انجام می‌شود.

یادآوری ۳- هنگامی که دو یا چند سیستم مدیریت در رشته های تخصصی مختلف (مانند کیفیت، زیست محیطی، ایمنی و سلامت شغلی) با همدیگر مورد ممیزی قرار می گیرند، آن را ممیزی ترکیبی می نامند.

یادآوری ۴- هنگامی که دو یا چند سازمان ممیزی کننده در انجام ممیزی یک سازمان ممیزی‌شونده (۳-۷) همکاری می‌کنند، آن را "ممیزی مشترک"[2] می نامند.

یادآوری ۵- برگرفته از تعریف بند ۳-۹-۱ استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷.

۲-۳

معیارهای ممیزی

مجموعه خط‌مشی ها، روش های اجرایی یا الزامات که به عنوان مبنایی برای مقایسه **شواهد ممیزی** (۳-۳) استفاده می‌شوند

یادآوری۱- برگرفته از تعریف بند ۳-۹-۵ استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷.

یادآوری ۲- اگر معیارهای ممیزی، الزامات قانونی (شامل قوانین و مقررات) باشند، در **یافته های ممیزی** (۳-۴) اغلب از واژه های "پیروی" [3]یا "عدم پیروی" [4]استفاده می‌شود.

۳-۳

شواهد ممیزی

سوابق، بیان واقعیات یا دیگر اطلاعات مربوط به **معیارهای ممیزی** (۳-۲) و قابل تصدیق

یادآوری- شواهد ممیزی می توانند کمی یا کیفی باشند.

[تعریف بند ۳-۹-۴ از استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷]

۴-۳

یافته های ممیزی

نتایج حاصل از ارزیابی **شواهد ممیزی** (۳-۳)گردآوری شده در مقایسه **با معیارهای ممیزی** (۳-۲)

2-Regulators
1-Joint audit
2-Compliant
3-Non-compliant

یادآوری ۱- یافته های ممیزی، انطباق یا عدم انطباق را نشان می دهد.

یادآوری ۲- یافته های ممیزی می‌تواند منجر به شناسایی فرصت های بهبود یا ثبت رویه‌های مطلوب سازمان باشد.

یادآوری ۳- هرگاه معیارهای ممیزی از قوانین یا سایر الزامات انتخاب شوند، یافته ممیزی مطابقت یا عدم مطابقت نامیده می-شود.

یادآوری۴- برگرفته از تعریف بند ۳-۹-۵ استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷.

۳-۵

نتیجه‌گیری ممیزی

ماحصل یک **ممیزی** (۳-۱) بعد از بررسی اهداف ممیزی و کلیه **یافته های ممیزی** (۳-۴)

یادآوری- برگرفته از تعریف بند ۳-۹-۶ استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷.

۳-۶

کارفرمای ممیزی

سازمان یا شخص درخواست کننده **ممیزی (۳-۱)**

یادآوری ۱- در مورد ممیزی درون سازمانی، کارفرمای ممیزی می‌تواند سازمان **ممیزی‌شونده** (۳-۷) یا فرد مدیریت کننده برنامه ممیزی نیز باشد. درخواست های مربوط به ممیزی برون سازمانی می‌تواند از جانب منابعی مانند سازمان های تنظیم کننده مقررات، طرف های قرار داد یا کارفرمایان بالقوه باشد.

یادآوری ۲- برگرفته از تعریف ۳-۹-۷ استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷.

۳-۷

سازمان ممیزی‌شونده

سازمان مورد ممیزی

[تعریف بند ۳-۹- ۸ از استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷]

۳-۸

ممیز

شخصی که یک **ممیزی** (۳-۱) را انجام می‌دهد

۳-۹

تیم ممیزی

یک یا چند **ممیز** (۳-۸) که یک **ممیزی** (۳-۱) را انجام می‌دهند، و در صورت لزوم توسط **کارشناسان فنی** پشتیبانی می‌شوند (۳-۱۰)

یادآوری ۱- یکی از ممیزان تیم ممیزی به عنوان "راهبر تیم ممیزی" تعیین می‌شود.

یادآوری ۲- تیم ممیزی می‌تواند ممیزان در حال آموزش را نیز دربرگیرد.

[تعریف بند ۳-۹- ۱۰ از استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷]

۳-۱۰

کارشناس فنی

شخصی که دانش یا تخصص کارشناسی معینی را برای **تیم ممیزی** (۳-۹) ارائه می‌کند

یادآوری ۱- دانش یا تخصص کارشناسی معین عبارت است از دانش یا تخصصی که به سازمان، فرایند یا فعالیت مورد ممیزی، یا زبان یا فرهنگ مربوط می‌شود.

یادآوری ۲- کارشناس فنی در تیم ممیزی به عنوان ممیز (۳-۸) عمل نمی‌کند.

[تعریف بند ۳-۹- ۱۱ از استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷]

۳-۱۱

ناظر

شخصی که **تیم ممیزی** (۳-۹) را همراهی می‌کند و لیکن ممیزی نمی‌کند

یادآوری ۱- ناظر بخشی از تیم **ممیزی** (۳-۹) نیست و بر انجام **ممیزی** (۳-۱) تاثیر ندارد یا در آن دخالت نمی‌کند.

یادآوری۲- ناظر می‌تواند از طرف سازمان **ممیزی‌شونده** (۳-۷)، از طرف سازمان های تنظیم کننده مقررات قانونی یا طرف ذی‌نفع دیگری باشد که بر **ممیزی** (۳-۱) نظارت می‌کند.

۳-۱۲

راهنما

شخصی که از طرف سازمان **ممیزی‌شونده** (۳-۷) برای کمک به **تیم ممیزی** (۳-۹) تعیین می‌شود

۳-۱۳

برنامه ممیزی

ترتیباتی برای مجموعه ای از یک یا چند **ممیزی** (۳-۱) که برای چارچوب زمانی مشخصی طرح‌ریزی شده است و جهت گیری آن برای نیل به مقاصد خاصی می‌باشد

یادآوری- برگرفته از تعریف بند ۳-۹-۲ استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷.

۳-۱۴

دامنه شمول ممیزی

گستره و حدود یک **ممیزی** (۳-۱)

یادآوری- دامنه شمول ممیزی عموما شامل شرحی از مکان‌های فیزیکی، واحدهای سازمانی، فعالیت‌ها و فرایندها و همچنین مدت زمان دربرگرفته شده می‌باشد.

[تعریف بند ۳-۹- ۱۳ از استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷]

۳-۱۵

طرح ممیزی

شرحی از فعالیت‌ها و ترتیبات برای یک **ممیزی** (۳-۱)

[تعریف بند ۳-۹- ۱۲ از استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷]

۳-۱۶

ریسک

تاثیر عدم قطعیت بر روی اهداف

یادآوری- برگرفته از تعریف ۱-۱ استاندارد ملی ایران شماره ۱۳۲۴۶ سال ۱۳۸۹.

۳-۱۷

شایستگی

توانایی به کارگیری دانش و مهارت ها برای دستیابی به نتایج مورد انتظار

یادآوری- توانایی بیانگر به کارگیری مناسب رفتار شخصی در حین فرایند ممیزی است.

۳-۱۸

انطباق

برآورده شدن یک الزام

[تعریف بند ۳-۶- ۱ از استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷]

۳-۱۹

عدم انطباق

برآورده نشدن یک الزام

[تعریف بند ۳-۶- ۲ از استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷]

۳-۲۰

سیستم مدیریت

سیستمی برای تعیین خطمشی و اهداف و دستیابی به آن اهداف

یادآوری- سیستم مدیریت یک سازمان می‌تواند شامل سیستم های مدیریت مختلف مانند سیستم مدیریت کیفیت، سیستم مدیریت مالی یا سیستم مدیریت زیست محیطی باشد.

[تعریف بند ۳-۲- ۲ از استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷]

۴ اصول ممیزی

ممیزی با اتکا به تعدادی اصول مشخص توصیف می‌شود. این اصول بایستی کمک کند تا ممیزی به ابزاری اثربخش و قابل اطمینان برای پشتیبانی از خطمشی‌ها و کنترل‌های مدیریت از طریق فراهم کردن اطلاعاتی که بر مبنای آن یک سازمان بتواند برای بهبود عملکرد خود اقدام کند، مبدل شود. پیروی از این اصول پیش نیاز ضروری برای ارائه نتیجه‌گیری کافی و مرتبط از ممیزی، و فراهم آوردن این امکان است که ممیزانی که مستقل از یکدیگر کار می‌کنند در شرایط مشابه به نتایج مشابه برسند.

راهنمایی‌های ارائه شده در بندهای ۵ تا ۷ بر مبنای شش اصل ذکرشده به شرح زیر است:

الف- **درستکاری**: مبنای حرفه ای بودن

ممیزان و افراد مدیریت کننده برنامه ممیزی بایستی:

- کار خود را با درستی و دقت و مسئولیت انجام دهند
- تمام الزامات قانونی قابل کاربرد را رعایت و با آن مطابقت کنند
- شایستگی خود را هنگام انجام کار اثبات کنند
- کار خود را به صورت بی‌طرف انجام دهند یعنی در تمام رفتارهای خود منصف و بدون گرایش باشند
- در مورد تاثیراتی که ممکن است بر داوری آن‌ها در حین انجام یک ممیزی اعمال شود، حساس باشند.

ب- **ارائه منصفانه**: التزام به گزارش‌دهی صادقانه و صحیح

یافته های ممیزی، نتیجه‌گیری ممیزی و گزارش های ممیزی بایستی بازتاب صادقانه و صحیح فعالیت‌های ممیزی باشند. موانع مهمی که در طول ممیزی پیش می‌آید و اختلاف نظرات میان تیم ممیزی و سازمان ممیزی‌شونده که حل و فصل نشده‌اند، بایستی گزارش شوند. تبادل اطلاعات بایستی درست، دقیق، هدفمند، به موقع، شفاف و کامل باشد.

ج- **دقت حرفه‌ای مقتضی**: به کارگیری پشتکار و داوری در ممیزی

ممیزان بایستی بنا بر اهمیت وظیفه‌ای که انجام می‌دهند و به خاطر این که طرف اعتماد کارفرماهای ممیزی و سایر طرف‌های ذی‌نفع قرار می‌گیرند در کار خود دقت به خرج دهند. توانایی داوری مستدل در کلیه موقعیت‌های ممیزی عامل مهمی در انجام کار آن‌ها با دقت حرفه‌ای مقتضی است.

د- **محرمانگی**: امنیت اطلاعات

ممیزان بایستی در استفاده و حفاظت اطلاعات به دست آمده در حین انجام وظایف خود احتیاط کنند. اطلاعات ممیزی نبایستی توسط ممیزان یا کارفرمای ممیزی به نحو نامناسبی برای بهره شخصی یا به روشی که برای منافع مشروع سازمان ممیزی‌شونده زیان آور باشد، استفاده شود. این مفهوم برخورد مناسب با اطلاعات حساس یا محرمانه را دربر می‌گیرد.

ه- **استقلال**: مبنای بی طرفی ممیزی و واقع‌گرایی[1] نتیجه‌گیری‌های ممیزی

ممیزان بایستی حتی الامکان از فعالیت مورد ممیزی مستقل بوده و در تمامی موارد به روشی که فارغ از گرایش و تعارض منافع است، عمل کنند. در ممیزی های درون سازمانی ممیزان بایستی مستقل از مدیران اجرایی حوزه‌های کاری مورد ممیزی باشند. ممیزان بایستی در سرتاسر فرایند ممیزی برای

1-Objectivity

حصول اطمینان از این که یافته‌ها و نتیجه‌گیری‌های ممیزی مبتنی بر شواهد ممیزی است، واقع‌گرایی را حفظ نمایند.

در سازمان‌های کوچک، ممکن است ممیزان درون سازمانی کاملا مستقل از فعالیت مورد ممیزی نباشند ولی هرگونه اهتمامی بایستی در جهت برطرف کردن گرایش و ترغیب بر واقع‌گرایی به عمل آید.

و- **رویکرد مبتنی بر شواهد**: روش منطقی برای دستیابی به نتیجه‌گیری‌های قابل اطمینان و تجدید پذیر ممیزی در طی فرایند نظامند ممیزی

شواهد ممیزی بایستی قابل تصدیق و بطور کلی مبتنی بر نمونه‌هایی از اطلاعات موجود باشد، زیرا ممیزی در طول یک دوره زمانی محدود و با منابع محدود انجام می‌شود. از نمونه‌گیری بایستی بهره گیری مناسب شود زیرا با میزان اطمینانی که می توان به نتیجه‌گیری‌های ممیزی داشت ارتباط نزدیک دارد.

۵ مدیریت کردن برنامه ممیزی

۵-۱ کلیات

سازمانی که لازم است ممیزی‌ها را انجام دهد بایستی یک برنامه ممیزی تهیه کند که در تعیین اثر بخشی سیستم‌های مدیریت سازمان ممیزی‌شونده سهیم باشد. برنامه ممیزی می‌تواند شامل ممیزی‌هایی باشد که یک یا چند استاندارد سیستم مدیریت را در نظر می‌گیرد که می‌توانند به صورت جداگانه یا ترکیبی انجام شوند.

مدیریت رده بالا بایستی اطمینان حاصل کند که اهداف برنامه ممیزی تعیین شده‌اند و یک یاچند شخص شایسته را برای مدیریت کردن برنامه ممیزی منصوب کند. گستره برنامه ممیزی بایستی مبتنی بر اندازه و ماهیت سازمان مورد ممیزی و نیز ماهیت، چگونگی کارکرد، پیچیدگی، و سطح بلوغ سیستم مدیریت مورد ممیزی باشد. اولویت بایستی به تخصیص منابع برنامه ممیزی برای ممیزی کردن موضوعات با اهمیت در سیستم مدیریت باشد. این موارد ممکن است ویژگی‌های کلیدی کیفیت محصول یا خطرات مرتبط با سلامت و ایمنی یا جنبه‌های با اهمیت زیست محیطی و کنترل آن‌ها را دربرگیرد.

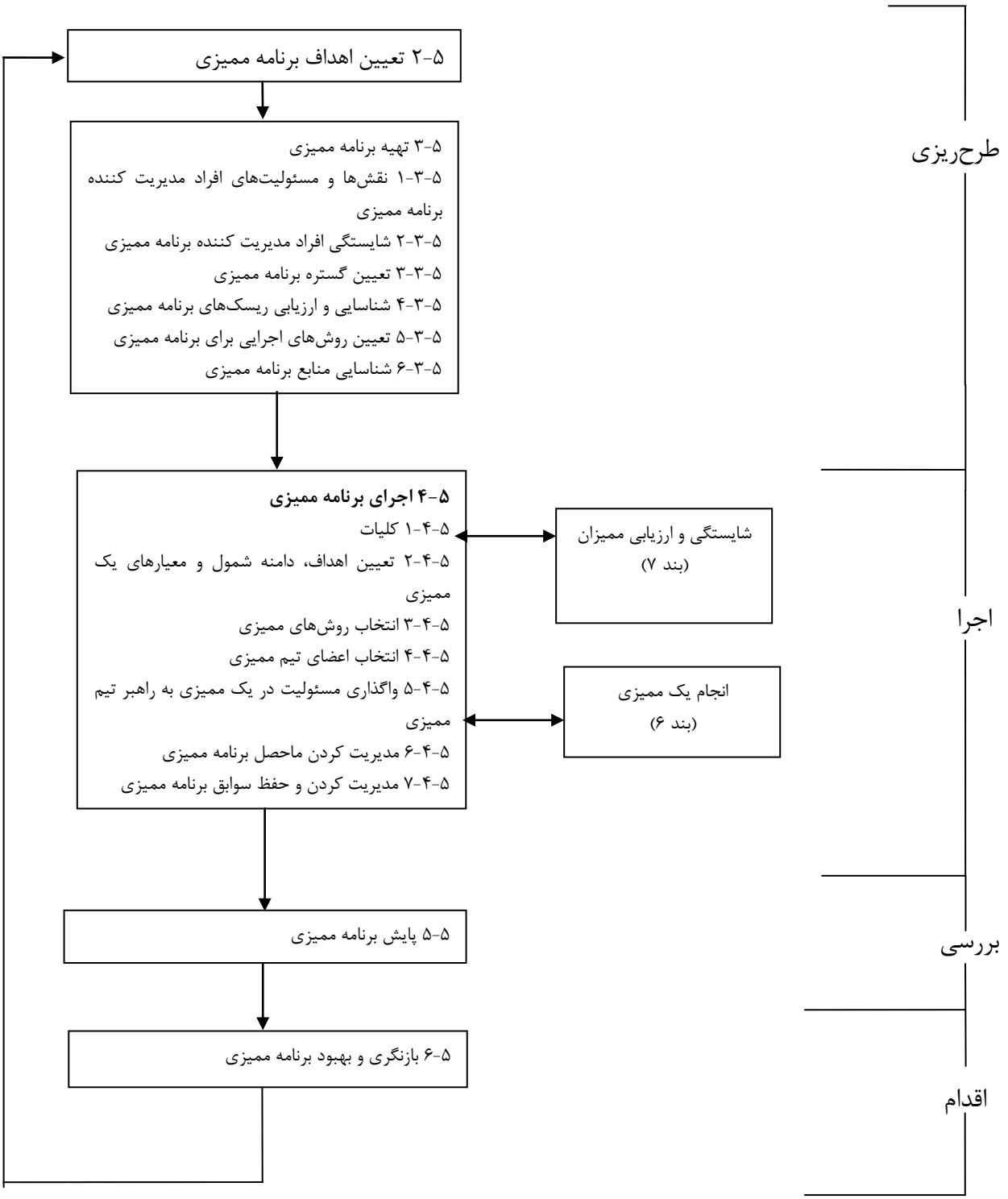
یادآوری- این مفهوم معمولا به عنوان ممیزی کردن مبتنی بر ریسک شناخته شده است. در این استاندارد راهنمایی بیشتر در خصوص ممیزی کردن مبتنی بر ریسک ارائه نشده است.

برنامه ممیزی بایستی اطلاعات و منابع لازم را برای سازماندهی و انجام ممیزی ها به صورت اثربخش و کارا در چارچوب‌های زمانی تعیین شده دربرگیرد و نیز می‌تواند شامل موارد زیر باشد:

- اهداف مربوط به برنامه ممیزی و هر یک از ممیزی‌های
- گستره/تعداد/انواع/مدت زمان/مکان‌ها/جدول زمانی ممیزی‌ها
- روش‌های اجرایی برنامه ممیزی
- معیارهای ممیزی
- روش‌های ممیزی
- انتخاب اعضای تیم ممیزی
- منابع لازم شامل نحوه سفر و محل اقامت
- فرایندهایی برای رعایت محرمانگی، امنیت اطلاعات، سلامت و ایمنی و سایر موضوعات مشابه.

اجرای برنامه ممیزی بایستی برای حصول اطمینان از این که اهداف ممیزی برآورده شده اند، بایستی پایش و اندازه گیری شود. برنامه ممیزی بایستی به منظور شناسایی بهبودهای احتمالی بازنگری شود.

شکل ۱ نمودار جریان فرایند مدیریت برنامه ممیزی را شرح می دهد.



یادآوری ۱- این شکل به کارگیری چرخه طرح‌ریزی- اجرا- بررسی- اقدام را در این استاندارد شرح می دهد.

یادآوری ۲- شماره گذاری بند/بند فرعی به بند/بند فرعی مرتبط در این استاندارد اشاره دارد.

شکل ۱- نمودار جریان فرایند مدیریت برنامه ممیزی

۵-۲ تعیین اهداف برنامه ممیزی

مدیریت رده بالا بایستی اطمینان حاصل کند که اهداف برنامه ممیزی برای هدایت طرح‌ریزی و انجام ممیزی تعیین شده‌اند و نیز بایستی اطمینان حاصل کند که برنامه ممیزی به صورت اثربخش اجرا می‌شود. اهداف برنامه ممیزی بایستی با خط‌مشی و اهداف سیستم مدیریت همخوان باشد و آن را پشتیبانی کند.

این اهداف می توانند مبتنی بر ملاحظات به شرح زیر باشند :

الف- اولویت‌های مدیریت

ب- مقاصد تجاری و سایر مقاصد کسب‌وکار

ج- ویژگی‌های فرایند ها، محصولات و پروژه‌ها و هرگونه تغییر آن‌ها

د- الزامات سیستم مدیریت

ه- الزامات مربوط به قوانین و قراردادها و سایر الزامات که سازمان نسبت به آن‌ها تعهد دارد

و- نیاز به ارزیابی تامین کننده

ز- نیازها و انتظارات طرف‌های ذی‌نفع از جمله مشتریان

ح- سطح عملکرد سازمان ممیزی‌شونده به صورتی که در وقوع عدم موفقیت‌ها یا رویدادها یا شکایات مشتری منعکس می‌شود.

ط- ریسک های مربوط به سازمان ممیزی‌شونده

ی- نتایج ممیزی های پیشین

س- سطح بلوغ سیستم مدیریت مورد ممیزی.

مثال‌هایی از اهداف برنامه ممیزی موارد زیر را شامل می‌شود:

- کمک به بهبود سیستم مدیریت و عملکرد آن
- برآورده کردن الزامات برون سازمانی، برای مثال گواهی کردن بر طبق استاندارد سیستم مدیریت
- تصدیق انطباق با الزامات قراردادی
- دستیابی و حفظ اطمینان به توانمندی یک تامین کننده
- تعیین اثر بخشی سیستم مدیریت
- ارزیابی سازگاری و همسویی اهداف سیستم مدیریت با خط‌مشی سیستم مدیریت و اهداف کلی سازمان.

۵-۳ تهیه برنامه ممیزی

۵-۳-۱ نقش‌ها و مسئولیت‌های مربوط به شخص مدیریت کننده برنامه ممیزی

شخص مدیریت کننده برنامه ممیزی بایستی در موارد زیر اقدام کند:

- تعیین گستره برنامه ممیزی
- شناسایی و ارزیابی ریسک‌های مربوط به برنامه ممیزی
- تعیین مسئولیت‌های تیم ممیزی
- تعیین روش‌های اجرایی برای برنامه‌های ممیزی
- تعیین منابع لازم

- حصول اطمینان از اجرای برنامه ممیزی شامل تعیین اهداف، دامنه شمول و معیارهای هر ممیزی، تعیین روش های ممیزی و انتخاب تیم ممیزی و ارزیابی ممیزان
- حصول اطمینان از مدیریت و نگهداری سوابق مناسب برنامه ممیزی
- پایش، بازنگری و بهبود برنامه ممیزی.

شخص مدیریت کننده برنامه ممیزی بایستی محتوای برنامه ممیزی را به اطلاع مدیریت رده بالا برساند و در موارد لازم تصویب آن‌ها را از وی درخواست نماید.

۵-۳-۲ شایستگی شخص مدیریت کننده برنامه ممیزی

شخص مدیریت کننده برنامه ممیزی بایستی شایستگی لازم برای مدیریت برنامه ممیزی و ریسک‌های مرتبط با آن را به نحو اثر بخش و کارا داشته باشد و نیز در زمینه‌های زیر دانش و مهارت داشته باشد:

- اصول، روش‌های اجرایی و روش‌های ممیزی
- استانداردها و مدارک مرجع سیستم مدیریت
- فعالیت‌ها، محصولات و فرایندهای سازمان ممیزی‌شونده
- الزامات قانونی و سایر الزامات قابل کاربرد مرتبط با فعالیت‌ها و محصولات سازمان ممیزی‌شونده
- در خصوص مشتریان، تامین کنندگان و دیگر طرف‌های ذی‌نفع سازمان ممیزی‌شونده در صورت موضوعیت داشتن.

شخص مدیریت کننده برنامه ممیزی بایستی در فعالیت‌های مناسب برای پیشرفت حرفه ای مداوم به منظور حفظ دانش و مهارت‌های لازم در خصوص مدیریت برنامه ممیزی مشارکت کند .

۵-۳-۳ تعیین گستره برنامه ممیزی

شخص مدیریت کننده برنامه ممیزی بایستی گستره برنامه ممیزی را تعیین کند که می‌تواند مبتنی بر اندازه و ماهیت سازمان ممیزی‌شونده و نیز ماهیت، چگونگی کارکرد، پیچیدگی و سطح بلوغ سیستم مدیریت مورد ممیزی و موضوعات دارای اهمیت برای آن، تغییر کند .

یادآوری- در برخی از موارد، براساس ساختار سازمان ممیزی‌شونده یا فعالیت‌های آن، برنامه ممیزی ممکن است فقط از یک ممیزی تکی تشکیل شود (برای مثال فعالیت مربوط به پروژه کوچک).

سایر عواملی که ممکن است بر گستره برنامه ممیزی تاثیر گذارند شامل موارد زیر است:

- اهداف، دامنه شمول و مدت زمان هر ممیزی و تعداد ممیزی‌هایی که قرار است انجام شود شامل اقدامات پیگیری بعد از ممیزی، در صورت موضوعیت داشتن
- تعداد، اهمیت، پیچیدگی، مشابهت و مکان‌های فعالیت‌هایی که قرار است ممیزی شوند
- آن عواملی که بر اثر بخشی سیستم مدیریت تاثیر می گذارند

- معیارهای ممیزی قابل کاربرد مانند ترتیبات طرح‌ریزی شده برای استانداردهای مدیریت مرتبط، الزامات قانونی و قراردادی و سایر الزاماتی که سازمان به آن متعهد است
- نتیجه‌گیری‌های ممیزی‌های درون سازمانی یا برون سازمانی پیشین
- نتایج بازنگری برنامه ممیزی پیشین
- هرگونه موضوعات مربوط به زبان، فرهنگ و جامعه
- دغدغه‌های طرف‌های ذی‌نفع مانند شکایات مشتری یا عدم مطابقت با الزامات قانونی
- تغییرات مهم در مورد سازمان ممیزی‌شونده یا یا عملیات آن
- دسترسی به فنّاوری‌های اطلاعات و ارتباطات برای پشتیبانی از فعالیت‌های ممیزی به ویژه به کارگیری روش‌های ممیزی از راه دور (به بند ب-۱ مراجعه شود)
- وقوع[1] رخدادهای[2] درون سازمانی و برون سازمانی، مانند خرابی‌های محصول، نشت امنیتی اطلاعات[3]، پیشامدهای[4] ایمنی و سلامت، اقدامات مجرمانه یا پیشامدهای محیطی.

۵-۳-۴ شناسایی و ارزیابی ریسک‌های برنامه ممیزی

ریسک‌های مختلف زیادی در ارتباط با تهیه، اجرا، پایش، بازنگری و بهبود یک برنامه ممیزی وجود دارد که ممکن است در دستیابی به اهداف آن تاثیر گذارد. شخص مدیریت کننده برنامه بایستی این ریسک‌ها را هنگام تدوین برنامه خود در نظر گیرد. این ریسک‌ها ممکن است مرتبط با موارد به شرح زیر باشند:

- طرح‌ریزی، برای مثال عدم موفقیت در تعیین اهداف ممیزی مرتبط و تعیین گستره برنامه ممیزی
- منابع، برای مثال عدم تخصیص زمان کافی برای تدوین برنامه ممیزی یا انجام یک ممیزی
- انتخاب اعضای تیم ممیزی، برای مثال تیم شایستگی جمعی برای انجام ممیزی به نحو اثربخش را ندارد
- اجرا، برای مثال تبادل غیر اثربخش اطلاعات در خصوص برنامه ممیزی
- سوابق و کنترل‌های آن‌ها، برای مثال عدم موفقیت در حفظ سوابق ممیزی به نحو مناسب به منظور اثبات اثربخشی برنامه ممیزی
- پایش، بازنگری و بهبود برنامه ممیزی برای مثال پایش غیر اثربخش ماحصل برنامه ممیزی.

۵-۳-۵ تعیین روش‌های اجرایی برای برنامه ممیزی

شخص مدیریت کننده برنامه ممیزی بایستی یک یا چند روش اجرایی که بر حسب موضوعیت به موارد به شرح زیر می‌پردازد، تعیین کند:

- طرح‌ریزی و زمان‌بندی ممیزی‌ها با در نظر گرفتن ریسک‌های برنامه ممیزی
- حصول اطمینان از امنیت اطلاعات و محرمانگی
- تضمین شایستگی ممیزان و راهبران تیم ممیزی

1-Occurrence
2-Event
3-Information security leaks
4- Incidents

- انتخاب تیم‌های ممیزی مناسب و تعیین نقش‌ها و مسئولیت‌های آن‌ها
- انجام ممیزی‌ها شامل استفاده از روش‌های نمونه‌گیری مناسب
- انجام اقدامات پیگیری بعد از ممیزی ، در صورت موضوعیت داشتن
- گزارش‌دهی به مدیریت رده بالا در خصوص دستاوردهای کلی برنامه ممیزی
- حفظ سوابق برنامه ممیزی
- پایش و بازنگری عملکرد و ریسک‌ها، و بهبود اثربخشی برنامه ممیزی.

۵-۳-۶ شناسایی منابع مربوط به برنامه ممیزی

در شناسایی منابع برای برنامه ممیزی، شخص مدیریت کننده برنامه ممیزی بایستی به موارد زیر توجه کند:

- منابع مالی لازم برای ایجاد، اجرا، مدیریت و بهبود فعالیت‌های ممیزی
- روش‌های ممیزی
- در اختیار داشتن ممیزان و کارشناسان فنی که از شایستگی مناسب برای اهداف خاص برنامه ممیزی برخوردار باشند
- گستره برنامه ممیزی و ریسک‌های برنامه ممیزی
- زمان و هزینه سفر، محل اقامت و سایر نیازهای ممیزی
- در دسترس بودن فنّاوری‌های اطلاعات و ارتباطات.

۵-۴ اجرای برنامه ممیزی

۵-۴-۱ کلیات

شخص مدیریت کننده برنامه ممیزی بایستی برنامه ممیزی را با استفاده از موارد زیر اجرا کند:

- تبادل اطلاعات با طرف‌های ذی‌ربط در مورد قسمت‌های مربوط برنامه ممیزی و مطلع ساختن آن‌ها به صورت دوره‌ای از پیشرفت برنامه ممیزی
- تعیین اهداف، دامنه شمول و معیارهای مربوط به هر یک از ممیزی‌ها
- هماهنگ کردن و زمان‌بندی ممیزی‌ها و سایر فعالیت‌های مرتبط با برنامه ممیزی
- حصول اطمینان از انتخاب تیم‌های ممیزی با شایستگی لازم
- تامین منابع لازم برای تیم‌های ممیزی
- حصول اطمینان از انجام ممیزی‌ها مطابق با برنامه ممیزی و در چارچوب زمانی توافق شده
- حصول اطمینان از این که فعالیت‌های ممیزی ثبت می‌شوند و سوابق به نحو مناسبی مدیریت و حفظ می‌شوند.

۵-۴-۲ تعیین اهداف، دامنه شمول و معیارهای یک ممیزی

هر یک از ممیزی‌ها بایستی مبتنی بر اهداف، دامنه شمول و معیارهای مدون ممیزی باشد. این موارد بایستی توسط شخص مدیریت کننده برنامه ممیزی تعیین شوند و با اهداف کلی برنامه ممیزی همخوان باشند.

اهداف ممیزی مواردی را تعیین می‌کند که باید در هر ممیزی به انجام برسد و ممکن است شامل موارد زیر باشد:

- تعیین حد انطباق سیستم مدیریت مورد ممیزی یا بخش‌هایی از آن با معیارهای ممیزی
- تعیین حد انطباق فعالیت‌ها، فرایندها و محصولات با الزامات و روش‌های اجرایی سیستم مدیریت
- ارزیابی توانمندی سیستم مدیریت برای حصول اطمینان از مطابقت با الزامات مربوط به قوانین و قراردادها و سایر الزامات که سازمان نسبت به آن‌ها تعهد دارد
- ارزیابی اثر بخشی سیستم مدیریت در برآورده کردن اهداف مشخص شده خود
- شناسایی زمینه‌های مربوط به بهبود بالقوه سیستم مدیریت.

دامنه شمول ممیزی بایستی با برنامه ممیزی و اهداف ممیزی همخوان باشد و عواملی مانند مکان‌های فیزیکی، واحدهای سازمانی ، فعالیت‌ها و فرایندهایی که قرار است ممیزی شوند و نیز دوره زمانی ممیزی را دربرگیرد.

معیارهای ممیزی به عنوان مبنایی استفاده می‌شوند که بر اساس آن انطباق تعیین می‌شود و ممکن است خط‌مشی‌ها، روش‌های اجرایی، استانداردها، الزامات قانونی، الزامات سیستم مدیریت، الزامات مربوط به قرارداد، "آیین‌های رفتاری بخش‌های اقتصادی"[1] یا سایر ترتیبات طرح‌ریزی شده قابل کاربرد را شامل شود.

در صورت رخداد هر تغییری در اهداف، دامنه شمول یا معیارهای ممیزی، در صورت لزوم برنامه ممیزی بایستی تغییر داده شود.

هنگامی که دو یا چند سیستم مدیریت در رشته‌های تخصصی مختلف با هم ممیزی می‌شوند (ممیزی ترکیبی)، مهم است که اهداف، دامنه شمول و معیارهای ممیزی با اهداف برنامه‌های ممیزی مربوط همخوان باشند.

۵-۴-۳ انتخاب روش‌های ممیزی

شخص مدیریت کننده برنامه ممیزی بایستی روش‌های مربوط به انجام اثر بخش ممیزی را مبتنی بر اهداف، دامنه شمول و معیارهای مشخص شده ممیزی، انتخاب و تعیین نماید.

یادآوری- در پیوست ب در خصوص چگونگی تعیین روش‌های ممیزی راهنمایی ارائه شده است.

هنگامی که دو یا چند سازمان ممیزی کننده ممیزی مشترک یک ممیزی‌شونده را انجام می دهند، اشخاص مدیریت کننده برنامه‌های مختلف ممیزی بایستی با روش ممیزی موافقت کنند و تبعات مربوط به تامین مجدد منابع و طرح‌ریزی ممیزی را در نظر بگیرند. اگر یک سازمان ممیزی‌شونده یک یا چند سیستم مدیریت در رشته‌های تخصصی مختلف را به کار گیرد، ممیزی‌های ترکیبی ممکن است در برنامه ممیزی گنجانده شود.

1-Sector codes of conduct

۵-۴-۴ انتخاب اعضای تیم ممیزی

شخص مدیریت کننده برنامه ممیزی بایستی اعضای تیم ممیزی شامل راهبر تیم وکارشناسان فنی مورد نیاز برای ممیزی خاص را تعیین کند.

تیم ممیزی بایستی با در نظر گرفتن شایستگی مورد نیاز برای دستیابی به اهداف هر ممیزی در دامنه شمول تعیین شده انتخاب شود. اگرتنها یک ممیز موجود باشد، ممیز بایستی تمام وظایف قابل اجرای مربوط به راهبر تیم ممیزی را انجام دهد.

یادآوری- بند ۷ شامل راهنمایی‌های مربوط به تعیین شایستگی مورد نیاز اعضای تیم ممیزی می‌باشد و فرایندهای مربوط به ارزیابی ممیزان را شرح می‌دهد.

در تصمیم‌گیری درباره اندازه و ترکیب تیم ممیزی برای ممیزی خاص، بایستی به موارد زیر توجه شود:

الف- شایستگی کلی تیم ممیزی که برای دستیابی به اهداف ممیزی با درنظر گرفتن دامنه شمول و معیارها لازم است

ب- پیچیدگی ممیزی و این که ممیزی "ممیزی ترکیبی" یا "ممیزی مشترک" است

ج- روش‌های ممیزی که انتخاب شده‌اند

د- الزامات قانونی و قراردادی و سایر الزامات که سازمان نسبت به آن‌ها تعهد دارد

ه- ضرورت حصول اطمینان از استقلال اعضای تیم ممیزی از فعالیت‌هایی که قرار است ممیزی شوند و اجتناب از تعارض منافع (به اصل ه در بند ۴ مراجعه کنید)

و– توانایی اعضای تیم ممیزی برای تعامل اثربخش با نمایندگان سازمان ممیزی‌شونده و کارکردن با یکدیگر

ز- زبان ممیزی، و ویژگی‌های اجتماعی و فرهنگی سازمان ممیزی‌شونده. این موضوعات ممکن است با اتکا به مهارت‌های شخصی خود ممیزان یا با کمک یک کارشناس فنی در نظر گرفته شوند.

برای تضمین شایستگی کلی تیم ممیزی مراحل به شرح زیر بایستی اجرا شوند:

- شناسایی دانش و مهارت‌های لازم برای دستیابی به اهداف ممیزی
- انتخاب اعضای تیم ممیزی به نحوی که تمامی دانش و مهارت‌های لازم در تیم ممیزی وجود داشته باشد.

اگر تیم ممیزی تمام شایستگی‌های لازم توسط ممیزان را دربر نگیرد، کارشناسان فنی با شایستگی بیشتر بایستی در تیم ممیزی در نظر گرفته شوند. کارشناسان فنی بایستی تحت نظارت یک ممیز فعالیت کنند اما نبایستی به عنوان ممیز عمل کنند.

ممیزان در حال آموزش ممکن است در تیم ممیزی در نظر گرفته شوند اما بایستی تحت نظارت و راهنمایی یک ممیز مشارکت کنند.

تصحیحاتی در خصوص اندازه و ترکیب تیم ممیزی ممکن است در حین ممیزی ضروری باشد یعنی اگر موضوعی در ارتباط با تعارض منافع و شایستگی بروز کند. در صورتی که چنین وضعیتی ایجاد شود قبل از انجام هر گونه اصلاحی در خصوص این مورد باید با طرف‌های مربوط (برای مثال راهبر تیم ، شخص مدیریت کننده برنامه ممیزی، کارفرمای ممیزی یا سازمان ممیزی‌شونده) تبادل نظر شود.

۵-۴-۵ واگذاری مسئولیت در یک ممیزی به راهبر تیم ممیزی

شخص مدیریت کننده برنامه ممیزی بایستی مسئولیت انجام هر ممیزی را به راهبر تیم ممیزی واگذار کند.

این واگذاری بایستی به منظور حصول اطمینان از اثر بخشی طرح‌ریزی ممیزی در فاصله زمانی کافی قبل از تاریخ زمان‌بندی شده ممیزی انجام شود.

به منظور حصول اطمینان از انجام اثر بخش هر یک از ممیزی‌ها، اطلاعات به شرح زیر بایستی به راهبر تیم ارائه شود:

الف- اهداف ممیزی

ب- معیارهای ممیزی و هرگونه مدارک مرجع

ج- دامنه شمول ممیزی، از جمله شناسایی واحدهای سازمانی و کاری و فرایندهایی که قرار است ممیزی شوند

د- روش‌های ممیزی و روش‌های اجرایی

ه- ترکیب اعضای تیم

و- اطلاعات مربوط به تماس با سازمان ممیزی‌شونده، مکان‌ها، تاریخ‌ها و مدت زمان فعالیت‌های ممیزی که قرار است، انجام شود

ز- تخصیص منابع لازم برای انجام ممیزی

ح- اطلاعات مورد نیاز برای ارزیابی و در نظر گرفتن ریسک‌های شناسایی شده برای دستیابی به اهداف ممیزی.

اطلاعات واگذاری بایستی همچنین در صورت مناسبت، موارد به شرح زیر را پوشش دهد:

- زبانی که در انجام ممیزی و گزارش‌دهی آن به کار می رود، هرگاه با زبان ممیز و/یا سازمان ممیزی-شونده متفاوت باشد
- محتوای گزارش ممیزی و توزیع آن که در برنامه ممیزی الزام شده است

- موضوعات مرتبط با محرمانگی و امنیت اطلاعات اگر در برنامه ممیزی الزام شده باشد
- هرگونه الزامات مربوط به سلامت و ایمنی برای ممیزان
- هرگونه الزامات مربوط به امنیت و صدور مجوز
- هرگونه اقدامات پیگیرانه، برای مثال از ممیزی پیشین، در صورت موضوعیت داشتن
- در صورت ممیزی مشترک، هماهنگی با سایر فعالیت‌ها.

هنگامی که یک ممیزی مشترک انجام می‌شود، حائز اهمیت است که سازمان‌های ممیزی کننده پیش از شروع ممیزی درخصوص مسئولیت‌های خاص هر طرف، به ویژه با توجه به اختیارات راهبر تیم تعیین شده برای ممیزی به توافق برسند.

۵-۴-۶ مدیریت کردن ماحصل برنامه ممیزی

شخصی که برنامه ممیزی را مدیریت می‌کند بایستی اطمینان حاصل کند که فعالیت‌ها به شرح زیر اجرا می-شوند:

- بازنگری و تصویب گزارش‌های ممیزی، از جمله ارزیابی و مناسب بودن و کفایت یافته‌های ممیزی
- بازنگری تحلیل علت ریشه‌ای و اثربخشی اقدامات اصلاحی و اقدامات پیشگیرانه
- توزیع گزارش‌های ممیزی به مدیریت رده بالا و سایر طرف‌های مرتبط
- تعیین ضرورت هرگونه ممیزی پیگیرانه.

۵-۴-۷ مدیریت و حفظ سوابق برنامه ممیزی

شخص مدیریت کننده برنامه ممیزی بایستی اطمینان حاصل کند که سوابق ممیزی به منظور اثبات اجرای برنامه ممیزی ایجاد، مدیریت و حفظ می‌شوند. برای حصول اطمینان از این که هرگونه نیازهای محرمانگی مرتبط با سوابق ممیزی در نظر گرفته شده‌اند، فرایندهایی باید ایجاد شود.

سوابق بایستی موارد به شرح زیر را دربرگیرد:

الف- سوابق مرتبط با برنامه ممیزی مانند:

- اهداف و گستره برنامه ممیزی مدون شده
- سوابقی که به ریسک‌های مرتبط با برنامه ممیزی می‌پردازد
- بازنگری‌های مربوط به اثربخشی برنامه ممیزی

ب- سوابق مرتبط با هر یک از ممیزی‌ها ، مانند:

- طرح‌های ممیزی و گزارش‌های ممیزی
- گزارش‌های عدم انطباق

- گزارش‌های اقدام اصلاحی و پیشگیرانه
- گزارش‌های اقدامات پیگیری بعد از ممیزی، در صورت موضوعیت داشتن

ج- سوابق مرتبط با کارکنان ممیزی که مباحث زیر را دربرمی‌گیرد:
- ارزیابی شایستگی و عملکرد اعضای تیم ممیزی
- انتخاب تیم‌های ممیزی و اعضای تیم
- حفظ و بهبود شایستگی.

شکل و سطح جزئیات سوابق بایستی دستیابی به اهداف برنامه ممیزی را اثبات کند.

۵-۵ پایش برنامه ممیزی

شخص مدیریت کننده برنامه ممیزی بایستی اجرای آن را با در نظر گرفتن نیاز به موارد زیر پایش کند:

الف- ارزیابی انطباق با برنامه‌های ممیزی، زمان‌بندی‌ها و اهداف ممیزی

ب- ارزیابی عملکرد اعضای تیم ممیزی

ج- ارزیابی توانایی تیم‌های ممیزی برای اجرای طرح ممیزی

د- ارزیابی بازخور از مدیریت رده بالا، سازمان‌های ممیزی شونده، ممیزان و دیگر طرف‌های ذینفع.

برخی عوامل مانند عوامل زیر، ممکن است نیاز به اصلاح برنامه ممیزی را تعیین کند:

- یافته‌های ممیزی
- سطح اثبات شده اثر بخشی سیستم مدیریت
- تغییرات مربوط به سیستم مدیریت کارفرما یا سازمان ممیزی‌شونده
- تغییرات در استانداردها، الزامات قانونی و قراردادی و سایر الزاماتی که سازمان نسبت به آن‌ها تعهد دارد
- تغییر یافتن تامین کنندگان.

۵-۶ بازنگری و بهبود برنامه ممیزی

شخص مدیریت کننده برنامه ممیزی بایستی برنامه ممیزی را برای ارزیابی این که آیا اهداف برنامه برآورده شده است، بازنگری کند. درس‌های آموخته شده از بازنگری برنامه ممیزی بایستی به عنوان دروندادهای فرایند بهبود مداوم در خصوص برنامه به کار رود.

در بازنگری برنامه ممیزی موارد زیر بایستی در نظر گرفته شود:

الف- نتایج و روندهای حاصل از پایش برنامه ممیزی

ب- انطباق با روش‌های اجرایی برنامه ممیزی

ج- خواسته‌ها و انتظارات رو به افزایش طرف‌های ذی‌نفع

د- سوابق برنامه ممیزی

ه- روش‌های جدید یا جایگزین ممیزی

و- اثربخشی اقداماتی که به ریسک‌های مرتبط با برنامه ممیزی می پردازد

ز- موضوعات مربوط به محرمانگی و امنیت اطلاعات مرتبط با برنامه ممیزی.

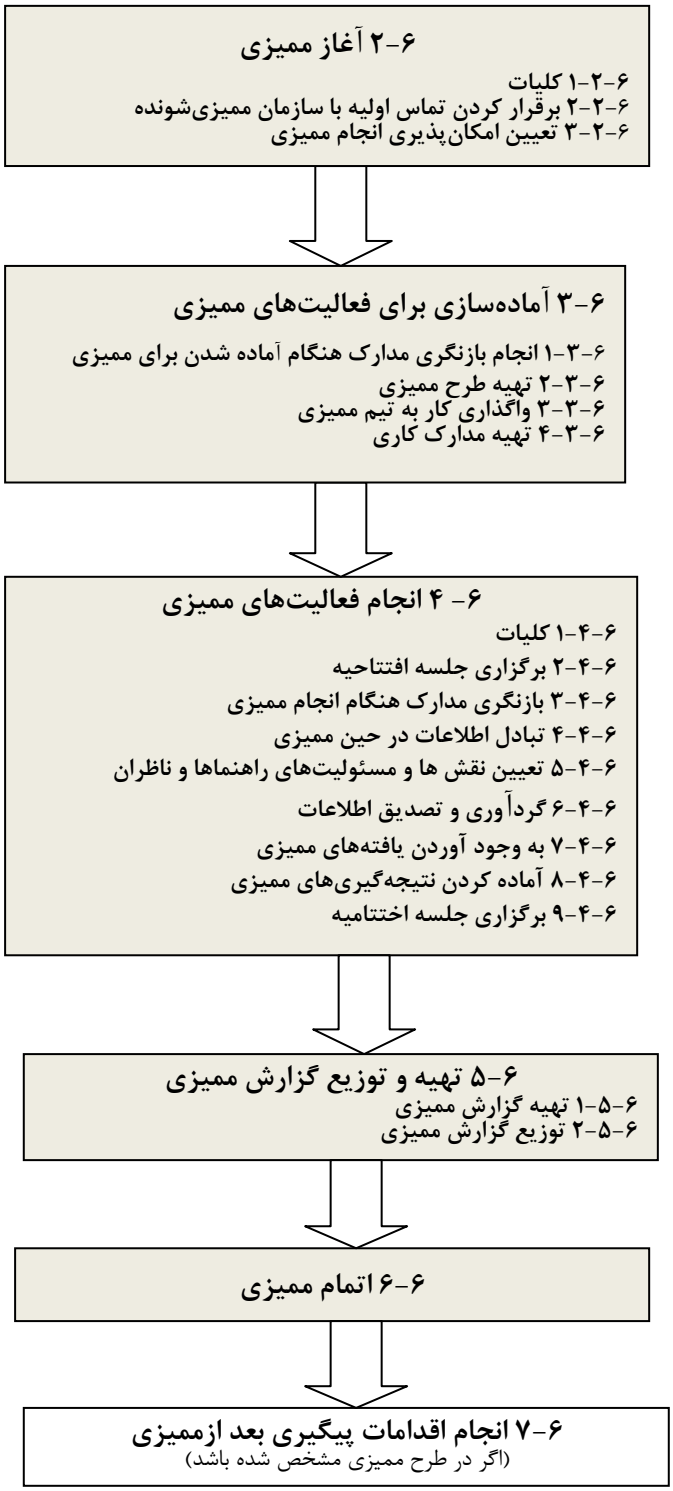
شخص مدیریت کننده برنامه ممیزی بایستی اجرای کلی برنامه ممیزی را بازنگری کند و زمینه‌های بهبود را شناسایی کند، در صورت لزوم برنامه را اصلاح کند و نیز بایستی:

- پیشرفت مداوم حرفه ای ممیزان مطابق با بندهای ۷-۴، ۷-۵ و ۷-۶ را بازنگری کند
- نتایج بازنگری برنامه ممیزی را به مدیریت رده بالا گزارش‌دهی کند.

۶ انجام ممیزی

۶-۱ کلیات

این بند شامل راهنمایی در خصوص آماده شدن و انجام دادن فعالیت‌های ممیزی به عنوان بخشی از برنامه ممیزی می‌باشد. در شکل ۲ دید کلی از فعالیت‌های نوعی ممیزی ارائه شده است. حد کاربرد ضوابط این بند به اهداف و دامنه شمول ممیزی خاص بستگی دارد.



یادآوری– شماره گذاری زیربندها، به زیر بندهای مربوط در این استاندارد اشاره دارد.

شکل ۲- فعالیت‌های نوعی ممیزی

۶-۲ آغاز ممیزی

۶-۲-۱ کلیات

هنگامی که ممیزی آغاز می‌شود، مسئولیت انجام ممیزی تا زمان اتمام ممیزی بر عهده راهبر (به بند ۵-۴-۵ مراجعه شود) تعیین شده می‌باشد (به بند ۶-۶ مراجعه شود).

برای آغاز کردن ممیزی، مراحل شکل ۲ بایستی در نظر گرفته شوند، با این وجود با توجه به سازمان ممیزی-شونده، فرایندها و شرایط مشخص ممیزی، ترتیب آن می‌تواند تغییر کند.

۶-۲-۲ برقرار کردن تماس اولیه با سازمان ممیزی‌شونده

تماس اولیه با سازمان ممیزی‌شونده برای انجام ممیزی می‌تواند به صورت رسمی یا غیررسمی باشد و بایستی توسط راهبر تیم ممیزی انجام شود. قصد از تماس اولیه موارد به شرح زیر است:

- برقراری ارتباطات با نمایندگان "سازمان ممیزی‌شونده"
- تایید اختیار انجام ممیزی
- فراهم کردن اطلاعات در مورد اهداف ممیزی، دامنه شمول، روش‌ها و ترکیب تیم ممیزی از جمله کارشناسان فنی
- درخواست دسترسی به مدارک و سوابق مرتبط برای مقاصد طرح‌ریزی
- تعیین الزامات قانونی و قراردادی قابل کاربرد و سایر الزامات مرتبط با فعالیت‌ها و محصولات سازمان ممیزی‌شونده
- تایید توافق با سازمان ممیزی‌شونده درخصوص میزان افشا و تلقی اطلاعات محرمانه
- ایجاد ترتیباتی برای ممیزی از جمله زمان‌بندی تاریخ‌ها
- تعیین هرگونه الزامات خاص مربوط به مکان به منظور دسترسی، امنیت، تندرستی و ایمنی یا سایر موارد
- توافق در خصوص حضور ناظران و نیاز به راهنماها در تیم ممیزی
- تعیین تمامی زمینه‌های مورد توجه یا با اهمیت برای سازمان ممیزی‌شونده در ارتباط با ممیزی خاص.

۶-۲-۳ تعیین امکان‌پذیری ممیزی

امکان‌پذیری ممیزی بایستی به منظور ایجاد اطمینان معقولانه در خصوص این که می‌توان به اهداف ممیزی دست یافت، تعیین شود.

در تعیین امکان‌پذیری بایستی عواملی نظیر در دسترس بودن موارد زیر در نظر گرفته شود:

- اطلاعات کافی و مناسب برای طرح‌ریزی و انجام ممیزی
- همکاری مناسب از جانب سازمان ممیزی‌شونده
- زمان و منابع در حد کافی برای انجام ممیزی.

هنگامی که ممیزی امکان‌پذیر نباشد، بایستی با توافق سازمان ممیزی‌شونده، جایگزینی به کارفرمای ممیزی ارائه شود.

۶-۳ آماده‌سازی برای فعالیت‌های ممیزی

۶-۳-۱ انجام بازنگری مدارک هنگام آماده شدن برای ممیزی

مستندات مرتبط سیستم مدیریت سازمان ممیزی‌شونده بایستی به منظور موارد زیر بازنگری شود:

- جمع آوری اطلاعات کافی به منظور فعالیت‌های آماده‌سازی ممیزی و تهیه مدارک کاری قابل کاربرد (به بند ۶-۳-۴ مراجعه شود) در خصوص فرایندها وحوزه‌های کاری
- تعیین دید کلی از گستردگی مستندات سیستم برای آشکار شدن کمبودهای[1] احتمالی.

یادآوری- راهنمایی در خصوص چگونگی انجام بازنگری مدارک در پیوست ب-۲ ارائه شده است.

مستندات، بر حسب موضوعیت، بایستی شامل مدارک و سوابق سیستم مدیریت و نیز گزارش‌های پیشین ممیزی باشد. بازنگری مدارک بایستی اندازه، ماهیت و پیچیدگی سیستم مدیریت و سازمان ممیزی‌شونده و اهداف و دامنه شمول ممیزی را در نظر بگیرد.

۶-۳-۲ تهیه طرح ممیزی

۶-۳-۲-۱ راهبر تیم ممیزی بایستی بر اساس اطلاعات موجود در برنامه ممیزی و مستندات ارائه شده توسط سازمان ممیزی‌شونده، طرح ممیزی را تهیه کند. در این طرح بایستی تاثیر فعالیت‌های ممیزی بر روی فرایندهای سازمان ممیزی‌شونده در نظر گرفته شود و مبنایی برای توافق میان کارفرمای ممیزی، تیم ممیزی و سازمان ممیزی‌شونده در خصوص انجام ممیزی باشد. این طرح بایستی زمان‌بندی و هماهنگی کارای فعالیت‌های ممیزی را به منظور دستیابی به اهداف ممیزی به نحو اثر بخش تسهیل کند.

میزان جزئیات ارائه شده در طرح ممیزی بایستی دامنه شمول و پیچیدگی ممیزی و نیز تاثیر عدم قطعیت بر دستیابی به اهداف ممیزی را منعکس کند. هنگام تهیه طرح ممیزی، راهبر تیم ممیزی بایستی از موارد زیر آگاه باشد:

- فنون نمونه‌گیری مناسب (به پیوست ب-۳ مراجعه شود)
- ترکیب تیم ممیزی و شایستگی جمعی آن
- ریسک‌های مربوط به سازمان که توسط ممیزی ایجاد می‌شود.

برای مثال ریسک‌های مربوط به سازمان ممکن است از حضور اعضای تیم ممیزی که بر ایمنی و سلامت، محیط زیست و کیفیت تاثیر می گذارند، ناشی شده باشد و وجود این ریسک‌ها تهدیدی برای محصولات، خدمات، کارکنان یا زیر ساخت (برای مثال: آلودگی در تسهیلات[2] اتاق تمیز) سازمان ممیزی‌شونده می‌باشد.

در خصوص ممیزی‌های ترکیبی، بایستی به تعاملات میان فرایندهای عملیاتی و اهداف رقابتی و اولویت‌های سیستم های مدیریت مختلف توجه ویژه داشت.

1-Gaps
2-Facilities

۶-۳-۲-۲ مقیاس و محتوای طرح ممیزی برای مثال ممکن است بین ممیزی اولیه و ممیزی‌های بعدی و نیز بین ممیزی‌های درون سازمانی و برون سازمانی متفاوت باشد. طرح ممیزی بایستی در حد کافی انعطاف داشته باشد تا تغییراتی را که ممکن است هنگام انجام فعالیت‌های ممیزی ضرورت یابد، امکان‌پذیر سازد.

طرح ممیزی بایستی دربرگیرنده موارد زیر باشد یا به آن‌ها ارجاع دهد:

الف- اهداف ممیزی

ب- دامنه شمول ممیزی، از جمله مشخص کردن واحدهای سازمانی و کاری و نیز فرایندهایی که قرار است ممیزی شوند

ج- معیارهای ممیزی و هرگونه مدارک مرجع

د- مکان‌ها، تاریخ‌ها، زمان مورد انتظار و مدت زمان فعالیت‌های ممیزی که قرار است انجام شوند از جمله جلسات با مدیریت سازمان ممیزی‌شونده

ه- شیوه‌های ممیزی مورد استفاده، شامل میزانی که روش‌های نمونه‌گیری ممیزی جهت کسب شواهد ممیزی مناسب و در صورت موضوعیت داشتن، طراحی طرح نمونه‌گیری مورد نیاز است

و- نقش‌ها و مسئولیت‌های اعضای تیم ممیزی و نیز راهنماها و ناظران

ز- اختصاص منابع مناسب برای زمینه‌های بسیار مهم ممیزی.

طرح ممیزی ممکن است همچنین بر حسب اقتضا شامل موارد زیر باشد:

- شناسایی نماینده سازمان ممیزی‌شونده برای ممیزی
- زبانی که در انجام ممیزی و گزارش‌دهی آن به کار می رود هرگاه با زبان ممیز و/یا سازمان ممیزی‌شونده متفاوت باشد
- سر فصل‌های گزارش ممیزی
- ترتیبات مربوط به پشتیبانی و ارتباطات، از جمله ترتیبات خاص مربوط به مکان‌هایی که قرار است ممیزی شوند
- هر گونه اقدامات خاصی که به منظور درنظر گرفتن تاثیر عدم قطعیت بر دستیابی به اهداف ممیزی بایستی اتخاذ شوند
- موضوعات مرتبط با محرمانگی و امنیت اطلاعات
- هرگونه اقدامات پیگیرانه در خصوص ممیزی‌های پیشین
- هرگونه فعالیت‌های پیگیرانه در خصوص ممیزی طرح‌ریزی شده
- در مورد ممیزی مشترک، هماهنگی با سایر فعالیت‌های ممیزی.

طرح ممیزی ممکن است توسط کارفرمای ممیزی مورد بازنگری و پذیرش قرار گیرد و پس از پذیرش بایستی به سازمان ممیزی شونده ارائه شود. هرگونه مخالفت ممیزی شونده با طرح ممیزی بایستی بین راهبر تیم، سازمان ممیزی شونده و کارفرمای ممیزی حل و فصل شود.

۶-۳-۳ واگذاری کار به تیم ممیزی

راهبر تیم ممیزی، با مشورت تیم ممیزی، بایستی به هر یک از اعضای تیم مسئولیت ممیزیِ فرآیندها، فعالیت‌ها، حوزه‌های کاری یا مکان‌های خاص را واگذار نماید. در این واگذاری‌ها بایستی استقلال و شایستگی ممیزان و استفادهٔ اثربخش از منابع، و همچنین نقش‌ها و مسئولیت‌های متفاوت ممیزان، ممیزانِ در حین آموزش و کارشناسان فنی مورد توجه قرار گیرد.

برای حصول اطمینان از دستیابی به اهداف ممیزی می‌توان در جریان انجام ممیزی تغییراتی در کارهای واگذارشده ایجاد کرد.

در موارد مقتضی، جلسات توجیهی بایستی توسط راهبر تیم ممیزی برای واگذاری کار و تصمیم گیری درمورد تغییرات احتمالی برگزار شود. تغییرات مربوط به واگذاری‌ها می‌تواند برای حصول اطمینان از دستیابی به اهداف ممیزی در جریان انجام امور ممیزی صورت پذیرد.

۶-۳-۴ تهیه مدارک کاری

اعضای تیم ممیزی بایستی اطلاعات مرتبط با وظایف محوله خود در ممیزی را بررسی نموده و مدارکی را که برای ارجاع دادن و برای ثبت شواهد ممیزی لازم است، تهیه کنند. این مدارک کاری ممکن است شامل موارد زیر باشد:

- چک‌لیست‌ها
- طرح‌های نمونه‌برداری ممیزی
- فرم ثبت اطلاعات از قبیل شواهد پشتیبان، یافته‌های ممیزی و صورتجلسات.

استفاده از چک‌لیست‌ها و فرم‌ها نبایستی در گسترهٔ فعالیت‌های ممیزی، که می‌توانند در نتیجهٔ اطلاعات گردآوری‌شده در حین ممیزی تغییر کنند، محدودیتی ایجاد کند.

یادآوری- راهنمایی در خصوص تهیه مدارک کاری در بند ب-۴ ارائه شده است.

مدارک کاری، از جمله سوابق حاصل از به‌کارگیری آن‌ها، بایستی حداقل تا اتمام ممیزی یا همانگونه که در طرح ممیزی تعیین شده است، نگهداری شوند. نحوهٔ نگهداری مدارک پس از اتمام ممیزی در بند ۶-۶ شرح داده شده است. مدارکی که حاوی اطلاعات محرمانه یا دارای مالکیت اختصاصی[1] باشند، بایستی همواره توسط اعضای تیم ممیزی به نحو مناسب حفاظت شوند.

۶-۴ انجام فعالیت‌های ممیزی

۶-۴-۱ کلیات

1-Proprietary

فعالیت‌های ممیزی به طور معمول با ترتیب معین و همانگونه که در شکل ۲ نشان داده شده است، انجام می-گیرد. این ترتیب ممکن است برای مناسب کردن شرایط ممیزی‌های خاص تغییر کند.

۶-۴-۲ برگزاری جلسه افتتاحیه

منظور از تشکیل جلسهٔ افتتاحیه عبارت است از:

الف- تایید موافقتنامه از سوی تمام طرف‌ها (برای مثال سازمان ممیزی‌شونده، تیم ممیزی) در خصوص طرح ممیزی

ب- معرفی تیم ممیزی

ج- حصول اطمینان از این که تمام فعالیت‌های طرح‌ریزی شده ممیزی را می توان انجام داد.

جلسهٔ افتتاحیه بایستی با حضور مدیریت "سازمان ممیزی‌شونده" و در موارد مقتضی، افرادی که مسئولیت حوزه‌های کاری یا فرآیندهای مورد ممیزی را بر عهده دارند برگزار شود و در حین جلسه، فرصتی برای طرح سوالات بایستی فراهم شود.

میزان جزئیات بایستی با مقدار آشنایی سازمان ممیزی‌شونده با فرایند ممیزی همخوان باشد. در بسیاری از موارد برای مثال ممیزی‌های درون سازمانی در سازمانی کوچک، جلسه افتتاحیه ممکن است به سادگی از تبادل اطلاعات در خصوص این که قرار است ممیزی انجام شود و شرحی از ماهیت ممیزی تشکیل شده باشد.

در سایر موقعیت‌های ممیزی، جلسه ممکن است رسمی باشد و سوابق حضور بایستی حفظ شود. ریاست جلسه بایستی بر عهده راهبر تیم ممیزی باشد و در صورت اقتضا موارد زیر بایستی در نظر گرفته شوند:

- معرفی شرکت کنندگان شامل ناظران و راهنماها و خلاصه نقش آن ها
- تایید اهداف، دامنه شمول و معیارهای ممیزی
- تایید طرح ممیزی و سایر ترتیبات مرتبط با سازمان ممیزی‌شونده، نظیر تاریخ و زمان جلسه اختتامیه، هرگونه جلسات میانی مابین تیم ممیزی و مدیریت "سازمان ممیزی‌شونده"و تغییرات بعدی
- ارائه شیوه‌ها و روش‌های اجرایی مورد استفاده برای انجام ممیزی، از جمله یادآوری این نکته به سازمان ممیزی‌شونده که شواهد ممیزی فقط بر اساس نمونه‌ای از اطلاعات موجود خواهد بود
- معرفی شیوه‌هایی برای مدیریت کردن ریسک‌های مرتبط با سازمان که ممکن است از حضور اعضای تیم ممیزی حاصل شود
- تأیید مجاری ارتباط رسمی میان تیم ممیزی و سازمان ممیزی‌شونده
- تأیید زبان مورد استفاده در حین ممیزی
- تأیید این که در حین ممیزی، سازمان ممیزی‌شونده در جریان پیشرفت کار ممیزی قرار خواهد گرفت
- تأیید این که منابع و امکانات مورد نیاز تیم ممیزی فراهم شده است
- تأیید موضوعات مرتبط با محرمانگی و امنیت اطلاعات
- تأیید روش‌های اجرایی مرتبط با موارد سلامتی و ایمنی، اضطرار و امنیت برای تیم ممیزی

- اطلاعات در خصوص روش گزارش‌دهی یافته‌های ممیزی از جمله درجه بندی عدم انطباق‌ها در صورت وجود
- اطلاعات دربارهٔ شرایطی که ممکن است به خاتمه ممیزی بیانجامد
- اطلاعات درباره جلسه اختتامیه
- اطلاعات درخصوص چگونگی برخورد با یافته‌های احتمالی در حین ممیزی
- اطلاعات در خصوص سیستم‌ها برای بازخور از سازمان ممیزی‌شونده در مورد یافته‌های ممیزی از جمله شکایات یا درخواست رسیدگی مجدد.

۶-۴-۳ بازنگری مدارک هنگام انجام ممیزی

مستندات سازمان ممیزی‌شونده در موارد زیر بایستی بازنگری شود:

- تعیین انطباق سیستم با معیارهای ممیزی تا حدی که مدون شده است
- جمع آوری اطلاعات برای پشتیبانی از فعالیت‌های ممیزی.

یادآوری- راهنمایی در خصوص چگونگی انجام بازنگری مدارک در پیوست ب-۲ ارائه شده است.

بازنگری ممکن است با سایر فعالیت‌های ممیزی تلفیق شود و ممکن است در سرتاسر ممیزی ادامه داشته باشد مشروط بر آن که این موضوع در خصوص اثربخشی انجام ممیزی تعیین کننده نباشد.

اگر مستندات کافی را نتوان در چارچوب زمانی ارائه شده در طرح ممیزی فراهم کرد، راهبر تیم ممیزی بایستی شخص مدیریت کننده برنامه ممیزی و سازمان ممیزی‌شونده را مطلع سازد. بر اساس اهداف و دامنه شمول ممیزی در این گونه موارد بایستی نسبت به ادامه ممیزی یا تعویق آن تا زمان حل مسایل مربوط به مستندات، تصمیم‌گیری شود.

۶-۴-۴ تبادل اطلاعات در حین ممیزی

در جریان ممیزی ممکن است ضروری باشد که به منظور تبادل اطلاعات میان اعضای تیم ممیزی و نیز با سازمان ممیزی‌شونده، کارفرمای ممیزی و به ویژه با نهادهای برون سازمانی (برای مثال سازمان‌های تنظیم کننده مقررات) و به خصوص هنگامی که مقررات قانونی گزارش‌دهی اجباری عدم انطباق‌ها را الزام می‌کند، ترتیبات رسمی در نظر گرفته شود.

تیم ممیزی بایستی به تناوب مذاکراتی داشته باشد تا به تبادل اطلاعات، ارزیابی پیشرفت ممیزی و در صورت لزوم واگذاری مجدد کار میان اعضای تیم ممیزی بپردازد.

در حین ممیزی، راهبر تیم ممیزی در صورت اقتضا بایستی پیشرفت کار ممیزی و مسایل را به تناوب با ممیزی‌شونده و کارفرمای ممیزی در میان بگذارد. شواهد گردآوری‌شده در حین ممیزی که بیانگر ریسک فوری و قابل توجهی در خصوص ممیزی‌شونده باشد بایستی فوراً به سازمان ممیزی‌شونده و در صورت اقتضا به کارفرمای ممیزی نیز گزارش شود. هر گونه نکات مورد توجه دربارهٔ موضوعی خارج از دامنه شمول ممیزی

بایستی یادداشت شده و به راهبر تیم ممیزی برای اطلاع دادن به کارفرمای ممیزی و سازمان ممیزی‌شونده گزارش شود.

هرگاه شواهد موجود ممیزی نشان دهد که دستیابی به اهداف ممیزی امکان‌پذیر نیست، راهبر تیم ممیزی بایستی دلایل آن را به منظور تعیین اقدام مناسب به کارفرمای ممیزی و سازمان ممیزی‌شونده گزارش نماید.

این اقدام ممکن است تأیید مجدد طرح ممیزی یا اصلاح آن، تغییر در اهداف یا دامنه شمول ممیزی، یا خاتمه ممیزی باشد.

هر گونه نیاز به تغییرات در طرح ممیزی که ممکن است در جریان انجام فعالیت‌های ممیزی در محل ظاهر شود بایستی توسط کارفرمای ممیزی و درصورت اقتضا توسط شخص مدیریت کننده برنامه ممیزی و سازمان ممیزی‌شونده بررسی و تصویب شود.

۶-۴-۵ تعیین نقش‌ها و مسئولیت‌های راهنماها و ناظران

راهنماها و ناظران (برای مثال سازمان‌های تنظیم کننده مقررات یا سایر طرف‌های ذی‌نفع) ممکن است تیم ممیزی را همراهی کنند. این افراد نبایستی بر انجام ممیزی تاثیر بگذارند یا در آن دخالت نمایند. در صورتی که در این خصوص نتوان اطمینان حاصل کرد، راهبر تیم ممیزی بایستی حق داشته باشد از شرکت دادن ناظران در برخی از فعالیت‌های ممیزی امتناع کند.

در مورد ناظران، هر گونه تعهداتی در ارتباط با سلامت و ایمنی، امنیت و محرمانگی بایستی مابین کارفرمای ممیزی و سازمان ممیزی‌شونده مدیریت شود.

راهنماهای تعیین شده توسط سازمان ممیزی‌شونده، بایستی به تیم ممیزی کمک کنند و بر اساس درخواست راهبر تیم ممیزی عمل نمایند. مسئولیت‌های آنان بایستی موارد زیر را دربرگیرد:

الف- کمک کردن به ممیزان در شناسایی افراد برای مشارکت در مصاحبه‌ها و تایید زمان‌بندی

ب- ترتیب دادن دسترسی به مکان‌های مشخص در سازمان ممیزی‌شونده

ج- حصول اطمینان از این که اعضای تیم ممیزی و ناظران از مقررات مربوط به روش‌های اجرایی ایمنی و امنیتیِ محل آگاهی دارند و آن‌ها را رعایت می‌کنند.

نقش راهنما ممکن است موارد زیر را نیز دربرگیرد:

- شاهد بودن بر انجام ممیزی به نیابت از طرف سازمان ممیزی‌شونده
- ابهام زدایی یا کمک در جمع آوری اطلاعات.

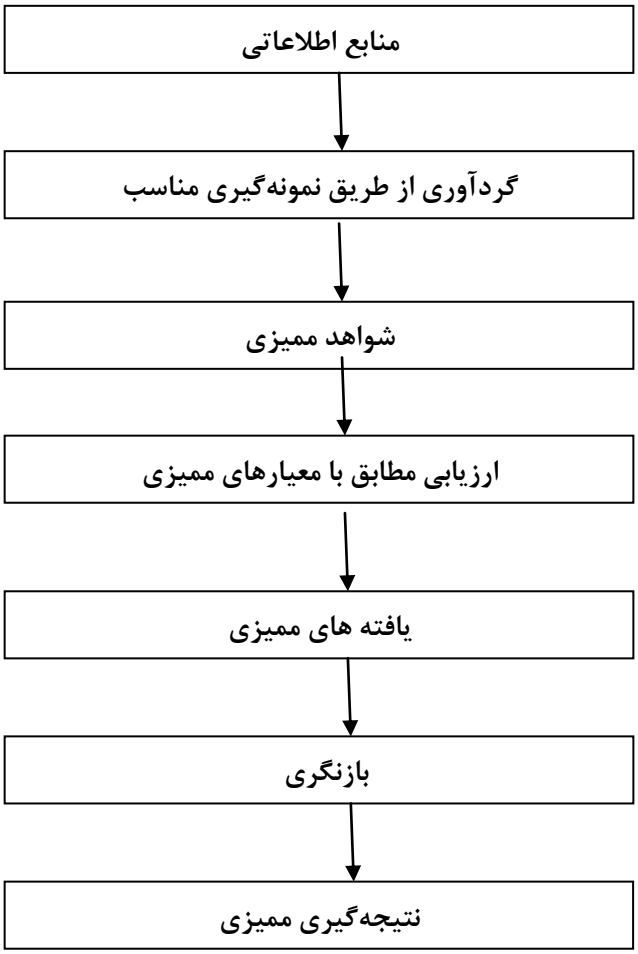
۶-۴-۶ گردآوری و تصدیق اطلاعات

در حین ممیزی، اطلاعات مرتبط با اهداف و دامنه شمول و معیارهای ممیزی، از جمله اطلاعات مربوط به حوزه فعالیت مشترک میان حوزه‌های کاری و فعالیت‌ها و فرآیندها، بایستی از طریق نمونه‌گیری مناسب گردآوری شده و تصدیق شود. فقط اطلاعات قابل تصدیق بایستی به عنوان شواهد ممیزی پذیرفته شوند. شواهد ممیزی که به یافته‌های ممیزی منجر می‌شوند بایستی ثبت شوند. اگر در حین گردآوری شواهد، تیم

ممیزی از هرگونه شرایط جدید یا تغییر یافته یا ریسک‌ها آگاه شود، تیم ممیزی بایستی بر حسب مورد آن‌ها را در نظر گیرد.

یادآوری ۱- راهنمایی در خصوص نمونه‌گیری در پیوست ب-۳ ارائه شده است.

شکل ۳ دید کلی فرآیند ممیزی را از گردآوری اطلاعات تا دستیابی به نتیجه‌گیری‌های ممیزی ارائه می نماید.



شکل ۳- دید کلی از فرایند گردآوری و تصدیق اطلاعات

شیوه های گردآوری اطلاعات موارد زیر را شامل می‌شود:

- مصاحبه‌ها
- ناظر بودن (بر فعالیت‌ها)
- بررسی مدارک از جمله سوابق.

یادآوری۲- راهنمایی در خصوص منابع اطلاعاتی در بند ب-۵ ارائه شده است.
یادآوری۳- راهنمایی درخصوص بازدید از محل سازمان ممیزی‌شونده در بند ب-۶ ارائه شده است.
یادآوری۴- راهنمایی در خصوص چگونگی انجام مصاحبه‌ها در بند ب-۷ ارائه شده است.

۶-۴-۷ به وجود آوردن یافته‌های ممیزی

شواهد ممیزی بایستی برای تعیین یافته‌های ممیزی مطابق با معیارهای ممیزی مورد ارزیابی قرار گیرد. یافته‌های ممیزی می‌تواند بر انطباق یا عدم‌انطباق با معیارهای ممیزی دلالت کند. هرگاه درطرح ممیزی مشخص شده باشد، یافته‌های هر ممیزی بایستی شامل "انطباق" و "رویه‌های خوب" همراه با شواهد پشتیبان آن‌ها، فرصت‌های بهبود و هر گونه توصیه به سازمان ممیزی‌شونده باشد.
عدم انطباق‌ها و شواهد ممیزی پشتیبان آن‌ها بایستی ثبت شوند. عدم انطباق‌ها ممکن است درجه‌بندی شود. این عدم انطباق‌ها بایستی به منظور تصدیق این که شواهد ممیزی درست است و عدم انطباق‌ها درک شده-اند، به همراه سازمان ممیزی‌شونده مورد بررسی قرار گیرند. نهایت تلاش برای رفع هر گونه اختلاف‌نظر دربارهٔ شواهد یا یافته‌های ممیزی بایستی به کار گرفته شود و موارد حل نشده بایستی ثبت شوند.
تیم ممیزی بایستی بر حسب نیاز در مراحل مناسبی در حین ممیزی نشست‌هایی برای بررسی یافته‌های ممیزی داشته باشد.

یادآوری- راهنمایی بیشتر درخصوص شناسایی و ارزیابی یافته‌های ممیزی در بند ب-۸ ارائه شده است.

۶-۴-۸ آماده کردن نتیجه‌گیری‌های ممیزی

اعضای تیم ممیزی بایستی پیش از جلسه اختتامیه برای منظورهای زیر جلسه مشورتی داشته باشند:
الف- بازنگری یافته‌های ممیزی و دیگر اطلاعات مناسب گردآوری‌شده در جریان ممیزی مطابق با اهداف ممیزی
ب- توافق در مورد نتیجه‌گیری‌های ممیزی ضمن در نظر گرفتن عدم قطعیت ذاتی در فرایند ممیزی
ج- آماده کردن توصیه‌ها، در صورتی که در طرح ممیزی تعیین شده باشد
د- تبادل نظر دربارهٔ اقدامات پیگیری بعد از ممیزی، در صورت موضوعیت داشتن.
در نتیجه‌گیری‌های ممیزی می توان مسایلی نظیر موارد زیر را مد نظر قرار داد:

- حد انطباق با معیارهای ممیزی و توانمندی سیستم مدیریت، از جمله اثر بخشی سیستم مدیریت در برآورده کردن اهداف بیان شده
- اجرای اثربخش، نگهداری و بهبود سیستم مدیریت
- توانمندی فرایند بازنگری مدیریت برای حصول اطمینان از تداوم مناسب بودن، کفایت، اثر بخشی و بهبود سیستم مدیریت
- دستیابی به اهداف ممیزی، پوشش داده شدن دامنه شمول ممیزی، و برآورده شدن معیارهای ممیزی
- علل ریشه‌ای یافته‌ها، اگر در طرح ممیزی در نظر گرفته شده باشد

- یافته‌های مشابه به دست آمده در زمینه‌های مختلفی که به منظور شناسایی روندها ممیزی شده‌اند.

چنانچه در طرح ممیزی مشخص شده باشد، نتیجه‌گیری‌های ممیزی می‌تواند به توصیه‌هایی برای بهبود یا فعالیت‌های آتی ممیزی منجر شود.

۶-۴-۹ برگزاری جلسه اختتامیه

جلسه اختتامیه‌ای توسط راهبر تیم ممیزی بایستی برگزار شود تا یافته‌ها و نتیجه‌گیری‌های ممیزی در آن ارائه شوند. مدیریت سازمان ممیزی‌شونده و در موارد مقتضی، افراد مسئول حوزه‌های کاری یا فرایندهایی که ممیزی شده‌اند بایستی از شرکت‌کنندگان در جلسهٔ اختتامیه باشند و کارفرمای ممیزی و سایر طرف‌ها نیز می‌توانند حضور داشته باشند. در صورت موضوعیت داشتن، راهبر تیم ممیزی بایستی سازمان ممیزی‌شونده را از وضعیت‌هایی که در حین ممیزی پیش آمده و ممکن است اطمینانی را که می‌توان به نتیجه‌گیری‌های ممیزی داشت کاهش دهد، مطلع سازد. اگر در سیستم مدیریت یا در موافقتنامه با کارفرمای ممیزی مشخص شده باشد، شرکت کنندگان بایستی در خصوص چارچوب زمانی مربوط به طرح اقدام برای رسیدگی به یافته-های ممیزی توافق کنند.

میزان جزئیات بایستی با سطح آشنا بودن سازمان ممیزی‌شونده با فرایند ممیزی همخوان باشد. در برخی از موقعیت‌های ممیزی، ممکن است جلسه رسمی باشد و صورتجلسه‌ای شامل فهرست سوابق حضور بایستی نگهداری شود. در سایر موارد، از جمله ممیزی‌های داخلی، جلسهٔ اختتامیه کمتر رسمی است و ممکن است صرفاً تبادل اطلاعات در مورد یافته‌ها و نتیجه‌گیری‌های ممیزی باشد.

در صورت موضوعیت داشتن، موارد به شرح زیر بایستی در جلسه اختتامیه به سازمان ممیزی‌شونده توضیح داده شود:

- راهنمایی دادن در خصوص این که شواهد ممیزی گردآوری شده بر مبنای نمونه‌ای از اطلاعات موجود است
- روش گزارش‌دهی
- فرایند رسیدگی به یافته‌های ممیزی وعواقب احتمالی
- ارائه یافته‌ها و نتیجه‌گیری‌های ممیزی به روشی که آن‌ها درک شوند و مدیریت سازمان ممیزی‌شونده اعلام نماید که از آن‌ها مطلع شده است
- هر گونه فعالیت‌های مرتبط بعد از ممیزی (برای مثال اجرای اقدامات اصلاحی، رسیدگی به شکایت ممیزی، فرایند درخواست رسیدگی مجدد).

هر گونه اختلاف‌نظری دربارهٔ یافته‌ها و/یا نتیجه‌گیری‌های ممیزی میان تیم ممیزی و سازمان ممیزی‌شونده بایستی مورد مذاکره قرار گیرد و در صورت امکان حل و فصل شود. در صورت حل و فصل نشدن، این امر بایستی ثبت شود.

چنانچه در اهداف ممیزی مشخص شده باشد، ممکن است توصیه‌هایی برای بهبود ارائه گردد. این نکته بایستی تأکید شود که توصیه‌ها الزام‌آور نیستند.

۶-۵ تهیه و توزیع گزارش ممیزی

۶-۵-۱ تهیه گزارش ممیزی

راهبر تیم ممیزی بایستی نتایج ممیزی را مطابق با روش‌های اجرایی برنامه ممیزی،گزارش کند.

گزارش ممیزی بایستی سابقه‌ای کامل، صحیح، موجز و روشن از ممیزی را فراهم کند و بایستی موارد زیر را دربرداشته یا به آن‌ها ارجاع نماید:

الف - اهداف ممیزی

ب دامنه شمول ممیزی، به‌ویژه مشخص کردن واحدهای سازمانی و حوزه‌های کاری یا فرآیندهایی که مورد ممیزی قرار گرفته‌اند

ج - مشخص کردن کارفرمای ممیزی

د - مشخص کردن اعضای تیم ممیزی و شرکت کنندگان در ممیزی

ه - تاریخ‌ها و مکان‌هایی که فعالیت‌های ممیزی انجام شده است

و - معیارهای ممیزی

ز - یافته‌های ممیزی و شواهد مرتبط

ح - نتیجه‌گیری‌های ممیزی

ط - اظهارکردن در مورد میزانی که معیارهای ممیزی برآورده شده اند.

گزارش ممیزی می‌تواند برحسب اقتضا موارد زیر را نیز دربرداشته یا به آن‌ها ارجاع نماید:

- طرح ممیزی شامل جدول زمان‌بندی
- خلاصه‌ای از فرآیند ممیزی، شامل موانع مواجهه شده که می‌تواند قابلیت اطمینان نتیجه‌گیری‌های ممیزی را کاهش دهد
- تأیید این که به اهداف ممیزی در دامنهٔ شمول آن مطابق با طرح ممیزی دست یافته شده است
- هر زمینه‌ای که در دامنه شمول ممیزی است و ممیزی نشده است
- خلاصه‌ای شامل نتیجه‌گیری‌های ممیزی و یافته‌های اصلی ممیزی پشتیبان آن‌ها
- هر گونه اختلاف‌نظری میان تیم ممیزی و سازمان ممیزی‌شونده که حل و فصل نشده است
- فرصت‌هایی برای بهبود، چنانچه درطرح ممیزی مشخص شده باشد
- "رویه‌های خوب" مشخص شده
- طرح‌های اقدام مورد توافق برای اقدامات پیگیری بعد از ممیزی، در صورت وجود
- اظهار در مورد ماهیت محرمانه محتویات
- هر گونه تبعاتی در خصوص برنامه ممیزی یا ممیزی‌های بعدی
- فهرست گیرندگان گزارش ممیزی.

یادآوری- گزارش ممیزی را می توان پیش از جلسه اختتامیه تهیه کرد.

۶-۵-۲ توزیع گزارش ممیزی

گزارش ممیزی بایستی ظرف مدت‌زمان توافق شده صادر شود. در صورتی که این کار ممکن نباشد، دلایل تأخیر بایستی به اطلاع سازمان ممیزی شونده و شخص مدیریت کننده برنامه ممیزی برسد.

گزارش ممیزی بایستی دارای تاریخ بوده و مطابق با روش‌های اجرایی برنامه ممیزی، بازنگری و تصویب شود.

گزارش ممیزی سپس بایستی برای گیرندگانی که در روش‌های اجرایی یا طرح ممیزی تعیین شده است، ارسال شود.

۶-۶- اتمام ممیزی

ممیزی هنگامی که تمامی فعالیت‌های طرح‌ریزی شده ممیزی به انجام رسیده باشد یا به نحو دیگری که با کارفرمای ممیزی توافق شده است (برای مثال وضعیت غیر منتظره‌ای ممکن است مانع از خاتمه ممیزی مطابق طرح شود)، به اتمام می رسد.

مدارک مرتبط با ممیزی بایستی بر اساس توافق میان طرف‌های شرکت‌کننده و مطابق با روش‌های اجرایی برنامه ممیزی و الزامات قابل کاربرد، حفظ یا امحا شوند.

تیم ممیزی و افراد مدیریت کننده برنامهٔ ممیزی ، نبایستی محتویات مدارک و دیگر اطلاعات به دست‌آمده در حین ممیزی یا گزارش ممیزی را بدون تصویب صریح کارفرمای ممیزی و درصورت اقتضا تصویب سازمان ممیزی‌شونده، برای طرف‌های دیگر فاش نمایند، مگر آن که مطابق قانون الزامی باشد. چنانچه فاش کردن محتوای مدرکی ممیزی الزامی باشد بایستی کارفرمای ممیزی و سازمان ممیزی‌شونده هرچه سریعتر مطلع شوند.

درس‌های آموخته شده از ممیزی بایستی در فرایند بهبود مداوم سیستم مدیریت سازمان‌های ممیزی‌شونده در نظر گرفته شود.

۶-۷ انجام اقدامات پیگیری بعد از ممیزی

نتیجه‌گیری‌های ممیزی می‌تواند براساس اهداف ممیزی، نیاز به اقدامات اصلاحی یا پیشگیرانه یا بهبود بخشی را مشخص نماید. چنین اقداماتی معمولاً توسط سازمان ممیزی‌شونده تصمیم‌گیری و در چارچوب زمانی توافق‌شده انجام می‌شود. درموارد مقتضی، سازمان ممیزی‌شونده بایستی شخص مدیریت کننده برنامه ممیزی و تیم ممیزی را از وضعیت این اقدامات آگاه سازد.

انجام و اثربخشی اقدامات اصلاحی بایستی تصدیق شود. این تصدیق می‌تواند بخشی از ممیزی بعدی باشد.

۷ شایستگی و ارزیابی ممیزان

۷-۱ کلیات

اطمینان به فرایند ممیزی و توانایی دستیابی به اهداف آن، وابسته به شایستگی افرادی است که در طرح‌ریزی و انجام ممیزی‌ها دخیل می باشند ازجمله ممیزان و راهبران تیم ممیزی. شایستگی بایستی از طریق فرایندی

که رفتار شخصی و توانایی به کارگیری دانش و مهارت‌های به دست آمده از طریق تحصیلات، تجربه کاری، آموزش ممیز و تجربه ممیزی را در نظر می‌گیرد، ارزیابی شود. این فرایند بایستی نیازهای برنامه ممیزی و اهداف آن را در نظر گیرد. برخی از دانش و مهارت‌های شرح داده شده دربند ۷-۲-۳ برای ممیزان سیستم مدیریت در هر رشته تخصصی[1] مشترک است، سایر موارد مختص به رشته‌های تخصصی مربوط به هر سیستم مدیریت می باشند. لازم نیست که شایستگی هر ممیز در تیم ممیزی یکسان باشد ولی نیاز است که شایستگی کلی تیم ممیزی برای دستیابی به اهداف ممیزی کافی باشد.

ارزیابی شایستگی ممیز بایستی مطابق با برنامه ممیزی شامل روش‌های اجرایی آن طرح‌ریزی، اجرا و مدون شود تا ماحصلی که واقع گرا، همخوان، منصفانه و قابل اطمینان است، حاصل شود. فرایند ارزیابی بایستی چهار مرحله اصلی به شرح زیر را دربرگیرد:

الف- تعیین شایستگی کارکنان ممیزی به منظور برآورده کردن نیازهای برنامه ممیزی

ب- تعیین معیارهای ارزیابی

ج- انتخاب روش ارزیابی مناسب

د- انجام ارزیابی.

خروجی فرایند ارزیابی بایستی مبنایی برای موارد زیر فراهم آورد:

- انتخاب اعضای تیم ممیزی مطابق با بند ۵-۴-۴
- تعیین نیاز برای بهبود شایستگی (برای مثال آموزش‌های تکمیلی)
- ارزیابی مداوم عملکرد ممیزان.

ممیزان بایستی شایستگی خود را از طریق پیشرفت مداوم حرفه‌ای و شرکت منظم در ممیزی‌ها ایجاد، حفظ و بهبود بخشند (به بند ۷-۶ مراجعه شود).

فرآیندی برای ارزیابی ممیزان و راهبران تیم ممیزی در بندهای ۷-۴ و ۷-۵ شرح داده شده است.

ممیزان و راهبران تیم ممیزی بایستی مطابق با معیارهای ذکر شده در بندهای ۷-۲-۲ و ۷-۲-۳ ارزیابی شوند.

شایستگی مورد نیاز افراد مدیریت کننده برنامه ممیزی در بند ۵-۳-۲ شرح داده شده است.

۷-۲ تعیین شایستگی ممیز به منظور برآورده کردن نیازهای برنامه ممیزی

۷-۲-۱ کلیات

در تصمیم گیری در خصوص دانش و مهارت‌های مورد نیاز ممیز، موارد به شرح زیر بایستی در نظر گرفته شود:

- اندازه، ماهیت و پیچیدگی سازمان مورد ممیزی
- رشته‌های تخصصی سیستم مدیریت مورد ممیزی
- اهداف و گستره برنامه ممیزی

1-Discipline

- سایر الزامات نظیر آن‌هایی که از طریق نهادهای برون سازمانی تحمیل می‌شود، برحسب اقتضا
- نقش فرایند ممیزی در سیستم مدیریت سازمان ممیزی‌شونده
- پیچیدگی سیستم مدیریت مورد ممیزی
- عدم قطعیت در دستیابی به اهداف.

این اطلاعات بایستی با موارد فهرست شده در بندهای ۷-۲-۳-۲، ۷-۲-۳-۳ و ۷-۲-۳-۴ مطابقت داشته باشد.

۷-۲-۲ رفتار شخصی

ممیزان بایستی از ویژگی‌های کیفی لازم برخوردار باشند که بتوانند مطابق اصول ممیزی مشروح در بند ۴ عمل کنند. ممیزان بایستی در حین عملکرد فعالیت‌های ممیزی رفتار حرفه‌ای شامل موارد به شرح زیر از خود نشان دهند:

- پایبندی به اصول اخلاقی[۱]؛ یعنی منصف، صادق، مخلص، درستکار و بصیر
- فکر باز[۲]؛ یعنی آماده برای توجه به نظرات یا سایر دیدگاه‌ها
- تدبیر[۳]؛ یعنی سنجیده عمل کردن در معاشرت با مردم
- تیزبینی[۴]؛ یعنی مشاهده فعالانه محیط فیزیکی پیرامون و فعالیت‌ها
- تیزفهمی[۵]؛ یعنی برخورداری از آگاهی و توانایی غریزی برای درک موقعیت‌ها
- تطبیق‌پذیری[۶]؛ یعنی توانایی تطبیق آسان با شرایط مختلف
- پشتکار[۷]؛ یعنی مصر بودن و تمرکز بر دستیابی به اهداف
- قاطعیت در تصمیم‌گیری[۸]؛ یعنی توانایی دستیابی به نتیجه‌گیری‌های به هنگام بر پایهٔ استدلال و تحلیل منطقی
- اعتماد به نفس[۹]؛ یعنی توانایی انجام وظیفه به صورت مستقل ضمن تعامل اثربخش با دیگران
- شهامت در عمل[۱۰]، یعنی قادر به عمل کردن به صورت مسئولانه و اخلاقی، هرچند که این اقدامات ممکن است همیشه مورد پسند نباشد و در برخی مواقع ممکن است منجر به عدم توافق یا تقابل شود
- استقبال از بهبود[۱۱]، یعنی تمایل به یادگیری از موقعیت‌ها و تلاش برای نتایج ممیزی بهتر
- حساسیت فرهنگی[۱۲]، یعنی تیزبینی و احترام به فرهنگ سازمان ممیزی‌شونده

1-Ethical
2-Open-minded
3-Diplomatic
4-Observant
5-Perceptive
6-Versatile
7- Tenacious
8-Decisive
9-Self-reliant
10-Fortitude
11-Open to improvement
12 -Culturally sensitive

- تشریک مساعی[1]، یعنی تعامل اثر بخش با دیگران، شامل اعضای تیم ممیزی و کارکنان سازمان ممیزی-شونده.

۷-۲-۳ دانش و مهارت‌ها

۷-۲-۳-۱ کلیات

ممیزان بایستی دانش و مهارت‌های لازم را برای دستیابی به نتایج مورد نظر از ممیزی‌هایی که انتظار می رود انجام دهند، دارا باشند. تمام ممیزان بایستی دانش و مهارت‌های عام را داشته باشند و نیز انتظار می رود که برخی از دانش و مهارت‌های مختص به رشته تخصصی و مختص به بخش اقتصادی مورد نظر را داشته باشند. راهبران تیم ممیزی بایستی دانش و مهارت‌های لازم برای راهبری تیم ممیزی را داشته باشند.

۷-۲-۳-۲ دانش و مهارت‌های عام ممیزان سیستم مدیریت

ممیزان بایستی دانش و مهارت‌های لازم را در زمینه‌های ذکر شده به شرح زیر داشته باشند:

الف - اصول، روش‌های اجرایی و فنون ممیزی: دانش و مهارت‌ها در این زمینه ممیز را توانمند می‌سازد تا بتواند اصول، روش‌های اجرایی و شیوه های مناسب را در مورد ممیزی‌های مختلف به کار برد و اطمینان یابد که ممیزی‌ها به نحوی منسجم و نظام‌مند انجام می‌شوند. ممیز بایستی از توانایی‌های انجام موارد زیر برخوردار باشد:

- کاربرد اصول، روش‌های اجرایی و شیوه‌های ممیزی
- طرح‌ریزی و سازمان‌دهی کار به نحو اثربخش
- انجام ممیزی در چارچوب زمان‌بندی مورد توافق
- اولویت‌بندی و تمرکز بر روی موضوعات مهم
- گردآوری اطلاعات از طریق مصاحبه، گوش‌دادن، مشاهده و بررسی مدارک و سوابق و داده‌ها
- درک و درنظرگرفتن نظرات کارشناسان
- درک مناسب بودن و پیامدهای بهره‌گیری از فنون نمونه‌گیری برای ممیزی
- تصدیق مرتبط بودن و درستی اطلاعات گردآوری شده
- تأیید کفایت و مناسب بودن شواهد ممیزی در پشتیبانی از یافته‌ها و نتیجه‌گیری‌های ممیزی
- ارزیابی عواملی که می‌تواند بر قابلیت اطمینانِ یافته‌ها و نتیجه‌گیری‌های ممیزی تأثیر بگذارد
- به کار گیری مدارک کاری برای ثبت فعالیت‌های ممیزی

1-Collaborative

- مدون کردن یافته‌های ممیزی و تهیه گزارش‌های مناسب ممیزی
- حفظ محرمانگی و امنیت اطلاعات، داده‌ها، مدارک و سوابق
- برقراری ارتباط اثربخش به صورت شفاهی و کتبی (توسط شخص یا از طریق استفاده ازمترجمان شفاهی و مترجمان)
- درک انواع ریسک‌های مرتبط با ممیزی.

ب - **سیستم مدیریت و مدارک مرجع**: دانش و مهارت‌ها در این زمینه ممیز را قادر می سازد تا بتواند دامنه شمول ممیزی را درک کند و معیارهای ممیزی را به‌کار ببرد و بایستی موارد زیر را دربرگیرد:

- استانداردهای سیستم مدیریت یا سایر مدارک مورد استفاده به عنوان معیارهای ممیزی
- کاربرد استانداردهای سیستم مدیریت توسط سازمان ممیزی‌شونده و سایر سازمان‌ها، در موارد مقتضی
- تعامل میان اجزای سیستم مدیریت
- تشخیص سلسله مراتب مدارک مرجع
- کاربرد مدارک مرجع برای موقعیت‌های مختلف ممیزی.

ج - **بافت سازمانی**[1] : دانش و مهارت‌ها در این زمینه ممیز را توانمند می سازد تا ساختار، رویه‌های کسب-وکار و مدیریت سازمان ممیزی‌شونده را درک کند و بایستی موارد زیر را دربرگیرد:

- انواع، اداره امور، اندازه، ساختار، حوزه‌های کاری و روابط
- مفاهیم عمومی کسب‌وکار و مدیریت، فرآیندها و اصطلاحات مرتبط با آن از جمله طرح‌ریزی، تنظیم بودجه و مدیریت کارکنان
- آداب و رسوم اجتماعی و فرهنگی سازمان ممیزی‌شونده.

د - **الزامات قانونی و قراردادی قابل کاربرد و سایر الزامات قابل کاربرد در مورد سازمان ممیزی‌شونده**: دانش و مهارت در این زمینه ممیز را توانمند می سازد تا از الزامات قانونی و قراردادی سازمان آگاه باشد و بتواند در چارچوب آن‌ها کار کند. دانش و مهارت‌های خاص برای نظام حقوقی[2] یا برای فعالیت‌ها و محصولات مربوط به سازمان ممیزی‌شونده بایستی موارد زیر را دربرگیرد:

- قوانین و مقررات و سازمان‌های کنترل کننده آن‌ها
- اصطلاحات حقوقی پایه
- عقد قرارداد و مسئولیت مدنی .

1-Organizational context
2-Jurisdiction

۷-۲-۳-۳ دانش و مهارت‌های ممیزان سیستم مدیریت مختص به رشته تخصصی و بخش اقتصادی

ممیزان بایستی دانش و مهارت‌های مختص به رشته تخصصی و بخش اقتصادی که برای ممیزی کردن نوع خاصی از سیستم مدیریت و بخش اقتصادی مناسب است را داشته باشند.

نیازی نیست که شایستگی ممیزان در تیم ممیزی یکسان باشد ولیکن شایستگی جمعی تیم ممیزی برای رسیدن به اهداف ممیزی لازم است کافی باشد.

دانش و مهارت ممیزان مختص به رشته تخصصی و بخش اقتصادی موارد زیر را شامل می‌شود:

- الزامات و اصول سیستم مدیریت مختص به رشته تخصصی و کاربرد آن‌ها
- الزامات قانونی مربوط به بخش اقتصادی و رشته تخصصی به نحوی که ممیز از الزامات خاص مربوط به نظام حقوقی و تکالیف، فعالیت‌ها و محصولات سازمان ممیزی‌شونده آگاه باشد
- الزامات طرف‌های ذی‌نفع مرتبط با رشته تخصصی خاص
- مبانی مربوط به رشته تخصصی و به کارگیری روش‌ها، فنون، فرایندها، و رویه‌های فنی و کسب‌وکار مختص رشته تخصصی که برای توانمند ساختن ممیز به منظور بررسی سیستم مدیریت و ایجاد یافته‌ها و نتیجه‌گیری‌های مناسب ممیزی کفایت کند
- دانش مختص به رشته تخصصی مرتبط با بخش اقتصادی، ماهیت فعالیت‌ها یا محل کار درحال ممیزی، که به منظور ارزیابی فعالیت‌ها، فرایندها و محصولات (کالاها و خدمات) سازمان ممیزی‌شونده برای ممیز کفایت کند
- اصول مدیریت ریسک، روش‌ها و فنون مرتبط با رشته تخصصی و بخش اقتصادی، به طوری که ممیز بتواند ریسک‌های مرتبط با برنامه ممیزی را ارزیابی و کنترل کند.

یادآوری- راهنمایی و مثال‌های تشریحی از دانش و مهارت‌های ممیزان مختص به رشته تخصصی در پیوست الف ارائه شده است.

۷-۲-۳-۴ دانش و مهارت‌های عام راهبر تیم ممیزی

راهبران تیم ممیزی بایستی از دانش و مهارت‌های بیشتر برای مدیریت و راهبری ممیزی برخوردار باشند تا اجرای کارا و اثربخش ممیزی را تسهیل نمایند. راهبر تیم ممیزی بایستی در موارد زیر دانش و مهارت‌های لازم را داشته باشد:

الف- متوازن کردن نقاط ضعف و قوت هر یک از اعضای تیم ممیزی

ب- ایجاد ارتباط کاری هماهنگ میان اعضای تیم ممیزی

ج- مدیریت کردن فرایند ممیزی، از جمله:

- طرح‌ریزی ممیزی و به‌کارگیری اثربخش منابع در حین ممیزی
- مدیریت کردن عدم قطعیت در دستیابی به اهداف ممیزی
- حفاظت کردن از سلامت و ایمنی اعضای تیم ممیزی در حین ممیزی، از جمله حصول اطمینان از مطابقت ممیزان با الزامات مرتبط با سلامت، ایمنی و امنیت

- سازمان‌دهی و هدایت اعضای تیم ممیزی
- هدایت و راهنمایی ممیزان در حین آموزش
- پیشگیری و حل و فصل تعارضات منافع، در صورت لزوم

د نمایندگی تیم ممیزی در ارتباطات با شخص مدیریت کننده برنامه ممیزی، کارفرمای ممیزی و سازمان ممیزی‌شونده

ه- راهبری تیم ممیزی برای رسیدن به نتیجه‌گیری‌های ممیزی

و- تهیه و تکمیل گزارش ممیزی.

۷-۲-۳-۵ دانش و مهارت‌های ممیزی کردن سیستم‌های مدیریت مربوط به چند رشته تخصصی

ممیزانی که قصد دارند به عنوان عضو تیم ممیزی در ممیزی کردن سیستم‌های مدیریت مربوط به چند رشته تخصصی شرکت کنند بایستی شایستگی لازم را حداقل برای ممیزی در یکی از رشته‌های تخصصی سیستم مدیریت داشته باشند و تعامل و هم‌افزایی میان سیستم‌های مدیریت مختلف را درک کنند.

راهبران تیم ممیزی که ممیزی سیستم‌های مدیریت مربوط به چند رشته تخصصی را انجام می دهند بایستی الزامات هر یک از استانداردهای سیستم مدیریت را درک کنند و محدوده دانش و مهارت خود در هریک از رشته‌های تخصصی را تشخیص دهند.

۷-۲-۴ دستیابی به شایستگی ممیز

دانش و مهارت‌های ممیز می‌تواند با استفاده از موارد به شرح زیر کسب شود:

- تحصیلات/ آموزش رسمی و تجربه می‌تواند در بهبود دانش و مهارت‌ها در رشته تخصصی و بخش اقتصادی سیستم مدیریت که ممیز قصد ممیزی آن را دارد، سهیم باشد
- برنامه‌های آموزشی که دانش و مهارت‌های عام ممیزان را دربرمی‌گیرد
- تجربه در سمت فنی، مدیریتی یا حرفه ای مرتبط که مستلزم داوری، تصمیم‌گیری، حل مشکلات و تبادل اطلاعات با مدیران، متخصصان حرفه ای، همترازان، مشتریان و سایر طرف‌های ذی‌نفع می‌باشد
- تجربه ممیزی کسب شده تحت نظارت ممیز در همان رشته تخصصی.

۷-۲-۵ راهبران تیم ممیزی

راهبر تیم ممیزی بایستی برای بهبود دانش و مهارت‌های مشروح در بند ۷-۳-۲ تجربهٔ بیشتری از ممیزی را کسب کرده باشد. این تجربهٔ بیشتر بایستی با انجام وظیفه تحت هدایت و راهنمایی یک راهبر تیم ممیزی دیگر کسب شده باشد.

۷-۳ تعیین معیارهای ارزیابی ممیز

معیارها بایستی کیفی باشند (از قبیل صفات شخصی، میزان دانش یا اجرای مهارت‌ها که حین آموزش یا در محل کار اثبات شده است) و یا کمی باشند (از قبیل تعداد سال‌های تجربه کاری و تحصیلات، تعداد ممیزی‌های انجام شده، ساعات آموزش ممیزی).

۷-۴ انتخاب روش مناسب ارزیابی ممیز

ارزیابی بایستی توسط شخص یا هیئتی با استفاده از یک یا چند روش انتخاب شده از میان روش‌های جدول شماره ۲ صورت پذیرد. هنگام استفاده از جدول شماره ۲ بایستی به موارد زیر توجه شود:

- روش‌های تشریح شده، گستره‌ای از گزینه‌ها را ارائه می‌کنند و ممکن است در تمامی موقعیت‌ها کاربرد نداشته باشند
- روش‌های مختلف تشریح شده ممکن است از نظر قابلیت اطمینان با هم تفاوت داشته باشند
- معمولاً برای حصول اطمینان از رسیدن به نتیجه‌ای که واقع گرا و منسجم و منصفانه و قابل‌اطمینان باشد بایستی ترکیبی از روش‌ها را مورد استفاده قرار داد.

جدول ۲- روش‌های ممکن ارزیابی

روش ارزیابی	اهداف	مثال‌ها
بررسی سوابق	تصدیق سوابق ممیز	تحلیل سوابق مربوط به تحصیلات، آموزش، اشتغال، اعتبار نامه‌های حرفه ای و تجربهٔ ممیزی
بازخور	فراهم کردن اطلاعات درباره چگونگی تلقی از عملکرد ممیز	نظرخواهی‌ها، پرسشنامه‌ها، اشخاص معرف، گواهی‌های شفاهی، شکایات، ارزیابی عملکرد، بررسی توسط همترازان
مصاحبه	ارزیابی صفات شخصی و مهارت‌های ارتباطی، تصدیق اطلاعات، و سنجش دانش و کسب اطلاعات بیشتر	مصاحبه‌ها با اشخاص
ناظر بودن (بر فعالیت‌ها)	ارزیابی صفات شخصی و توانایی به کارگیری دانش و مهارت‌ها	ایفای نقش ممیز، شاهد بودن بر ممیزی‌ها، عملکرد در حین کار
آزمون	ارزیابی صفات شخصی و دانش و مهارت‌ها و کاربرد آن‌ها	آزمون‌های شفاهی و کتبی، آزمون روان‌سنجی
بررسی پس از ممیزی	فراهم کردن اطلاعات در مورد عملکرد ممیز حین فعالیت‌های ممیزی، شناسایی نقاط قوت و نقاط ضعف	بررسی گزارش ممیزی، مصاحبه با راهبر تیم ممیزی، تیم ممیزی و در صورت اقتضا، بازخور از سازمان ممیزی‌شونده

۷-۵ انجام ارزیابی ممیز

اطلاعات گردآوری شده در خصوص شخص بایستی با معیارهای ذکرشده در بند ۷-۲-۳ مقایسه شود. هرگاه شخصی که انتظار می رود در برنامه ممیزی شرکت کند معیارها را برآورده نسازد، در این صورت آموزش، کار یا تجربه ممیزی افزونتری بایستی در نظر گرفته شود و متعاقب آن بایستی ارزیابی مجدد انجام شود.

۷-۶ حفظ و بهبود شایستگی ممیز

ممیزان و راهبران تیم ممیزی بایستی بطور مداوم شایستگی خود را بهبود ببخشند. ممیزان بایستی شایستگی خود را برای ممیزی کردن از طریق مشارکت منظم در ممیزی‌های سیستم مدیریت و پیشرفت مداوم حفظ کنند. پیشرفت حرفه‌ای مداوم مستلزم حفظ و بهبود شایستگی می‌باشد. به این پیشرفت می‌توان از طریق ابزارهایی مانند تجربهٔ کاری بیشتر، آموزش، مطالعه شخصی، مربی‌گری، حضور در جلسات و سمینارها و کنفرانس‌ها یا سایر فعالیت‌های ذیربط دست یافت.

شخص مدیریت کننده برنامه ممیزی بایستی سازوکارهای مناسبی برای ارزیابی مداوم عملکرد ممیزان و راهبران تیم ممیزی ایجاد کند.

در فعالیت‌های مربوط به پیشرفت حرفه‌ای مداوم بایستی موارد زیر در نظر گرفته شود:

- تغییرات در نیازهای فرد و سازمان مسئول برای انجام ممیزی
- رویه ممیزی کردن
- استانداردهای مرتبط و دیگر الزامات.

پیوست الف
(جهت آگاهی)

راهنمایی ها و مثال‌های تشریحی در خصوص دانش و مهارت‌های ممیزان مختص به رشته تخصصی

الف-۱ کلیات

در این پیوست مثال‌های عام در خصوص دانش و مهارت‌های ممیزان سیستم‌های مدیریت مختص به رشته تخصصی ارائه شده است که به عنوان راهنمایی برای کمک به شخص مدیریت کننده برنامه ممیزی برای انتخاب یا ارزیابی ممیزان می‌باشد.

سایر مثال‌های مربوط به دانش و مهارت‌های ممیزان مختص به رشته تخصصی ممکن است برای سیستم‌های مدیریت نیز تعیین شود. توصیه می‌شود هرگاه امکان‌پذیر باشد، این مثال‌ها برای حصول اطمینان از مقایسه-پذیری از ساختار کلی یکسان پیروی کنند.

الف-۲ مثال تشریحی از دانش و مهارت‌های ممیزان در مدیریت ایمنی حمل و نقل

دانش و مهارت‌های مرتبط با مدیریت ایمنی حمل و نقل و به کارگیری روش‌ها، فنون، فرایندها و رویه‌ها بایستی کافی باشد تا ممیز بتواند سیستم مدیریت را بررسی کند و یافته‌ها و نتیجه‌گیری‌های ممیزی را به وجود آورد.

مثال‌ها به شرح زیر می باشند:

- اصطلاحات مدیریت ایمنی
- درکی از رویکرد سیستم ایمنی
- تحلیل عوامل انسانی مرتبط با مدیریت ایمنی حمل و نقل
- ارزیابی و کاهش ریسک
- رفتار و تعامل انسانی
- تعامل مابین انسان‌ها، ماشین‌ها، فرایندها و محیط کار
- خطرات بالقوه و سایر عوامل تاثیرگذار بر ایمنی
- روش‌ها و رویه‌های مربوط به بررسی پیشامدها و پایش عملکرد ایمن
- ارزیابی پیشامدها و حوادث عملکردی
- تعیین اقدامات و سنجه‌های مربوط به عملکرد کنش‌گرایانه و واکنشی[1].

یادآوری- برای اطلاعات بیشتر به استاندارد بین المللی ISO 39001 که توسط ISO/PC 241 در خصوص سیستم‌های مدیریت ایمنی ترافیک جاده ای تدوین شده است، مراجعه شود.

1-Proactive and reactive

الف-۳ مثال‌های تشریحی در خصوص دانش و مهارت‌های ممیزان مختص به رشته تخصصی مدیریت زیست محیطی

دانش و مهارت‌های مرتبط با رشته تخصصی و به کارگیری روش‌ها، فنون، فرایندها و رویه‌های مختص به رشته تخصصی بایستی کافی باشد تا ممیز بتواند سیستم مدیریت را بررسی کند و یافته‌ها و نتیجه‌گیری‌های ممیزی را به وجود آورد.

مثال‌ها به شرح زیر می‌باشد:

- اصطلاحات زیست محیطی
- سنجه‌ها و آمارهای زیست محیطی
- علوم اندازه‌گیری و فنون پایش
- تعامل اکو سیستم‌ها و تنوع زیستی
- واسطه‌های زیست محیطی (مانند، هوا، آب، زمین، گیاهان، جانوران)
- فنون مربوط به تعیین ریسک (برای مثال جنبه‌ها/پیامدهای زیست محیطی، ازجمله روش‌های مربوط به ارزیابی اهمیت آن‌ها)
- ارزیابی چرخه حیات
- ارزیابی عملکرد زیست محیطی
- پیشگیری از آلودگی و کنترل آن (برای مثال بهترین فنون موجود برای کنترل آلودگی یا بازدهی انرژی)
- رویه‌ها و فرایندهای مربوط به کاهش منابع، به حداقل رسانیدن تلفات، استفاده مجدد، بازیافت کردن و عمل‌آوری
- استفاده از مواد خطرناک
- محاسبه و مدیریت گازهای گلخانه‌ای
- مدیریت منابع طبیعی (سوخت‌های فسیلی، آب، گیاهان و جانوران، زمین)
- طراحی با توجه به ملاحظات زیست محیطی
- گزارش‌دهی و افشای زیست محیطی
- خدمت رسانی مرتبط با محصول[1]
- فنّاوری‌های تجدیدپذیر و با کربن پایین.

یادآوری- در خصوص اطلاعات تکمیلی به استانداردهای تدوین شده توسط ISO/TC 207 در مورد مدیریت زیست محیطی مراجعه شود.

1- Stewardship

الف-۴ مثال تشریحی از دانش و مهارت‌های ممیزان مختص به رشته تخصصی مدیریت کیفیت

دانش و مهارت‌های مرتبط با رشته تخصصی و به کارگیری روش‌ها، فنون، فرایندها و رویه‌های مختص به رشته تخصصی بایستی کافی باشد تا ممیز بتواند سیستم مدیریت را بررسی کند و یافته‌ها و نتیجه‌گیری-های ممیزی را به وجود آورد.

مثال‌ها به شرح زیر می‌باشد:

- اصطلاحات مرتبط با کیفیت، مدیریت، سازمان، فرایند و محصول، ویژگی‌ها، انطباق، مستندات، فرایندهای ممیزی و اندازه‌گیری
- مشتری محوری، فرایندهای مرتبط با مشتری، پایش و اندازه‌گیری رضایت مشتریان، رسیدگی به شکایات، آیین رفتار[1]، حل و فصل اختلافات
- نقش راهبری مدیریت رده بالا، مدیریت کردن موفقیت پایدار سازمان، رویکرد مدیریت کیفیت، تحقق منافع مالی و اقتصادی از طریق مدیریت کیفیت، سیستم‌های مدیریت کیفیت و مدل‌های تعالی
- مشارکت دادن افراد، عوامل انسانی، شایستگی، آموزش و آگاهی
- رویکرد فرایندی، تحلیل فرایندی، فنون توانمندی و کنترل، روش‌های بهبود بخشی ریسک‌ها
- رویکرد سیستمی به مدیریت (منطق وجودی سیستم‌های مدیریت کیفیت، تمرکز سیستم‌های مدیریت کیفیت و دیگر سیستم‌های مدیریت، مستندات سیستم مدیریت کیفیت)، انواع و ارزش آن، پروژه‌ها، طرح-های کیفیت، مدیریت پیکره‌بندی
- بهبود مداوم، نوآوری و آموزش
- رویکرد واقع بینانه درتصمیم‌گیری، فنون ارزیابی ریسک (شناسایی، تحلیل و ارزیابی ریسک)، ارزیابی مدیریت کیفیت، (ممیزی، بازنگری و خود ارزیابی)، فنون اندازه‌گیری و پایش، الزامات فرایندهای اندازه-گیری و تجهیزات اندازه‌گیری، تحلیل علت ریشه‌ای، فنون آماری
- ویژگی‌های فرایندها و محصولات شامل خدمات
- روابط سودبخش متقابل با تامین‌کنندگان، الزامات سیستم مدیریت کیفیت و الزامات مربوط به محصولات، الزامات خاص مربوط به مدیریت کیفیت در بخش‌های اقتصادی مختلف.

یادآوری- در خصوص اطلاعات تکمیلی به استانداردهای تدوین شده توسط ISO/TC176 در مورد مدیریت کیفیت مراجعه شود.

الف-۵ مثال تشریحی در مورد دانش و مهارت‌های ممیزان مختص به رشته تخصصی مدیریت سوابق

دانش و مهارت‌های مرتبط با رشته تخصصی و به کارگیری روش‌ها، فنون، فرایندها و رویه‌های مختص به رشته تخصصی بایستی کافی باشد تا ممیز بتواند سیستم مدیریت را بررسی کند و یافته‌ها و نتیجه‌گیری‌های ممیزی را به وجود آورد.

1-Code of conduct

مثال‌ها به شرح زیر می‌باشد:

- سوابق، فرایندهای مدیریت سوابق و سیستم‌های مدیریت مربوط به اصطلاحات سوابق
- بهبود اقدامات و سنجه‌های عملکردی
- تحقیق و بررسی شیوه‌های ثبت سوابق از طریق مصاحبه، ناظر بودن (بر فعالیت‌ها) و صحه گذاری
- تحلیل نمونه از سوابق ایجاد شده در فرایندهای کسب‌وکار. ویژگی‌های کلیدی سوابق، سیستم‌های سوابق، فرایندها و کنترل‌های سوابق
- ارزیابی ریسک (برای مثال ارزیابی ریسک‌ها از طریق عدم موفقیت در ایجاد، حفظ و کنترل کردن سوابق کافی از فرایندهای کسب‌وکار سازمان)
- عملکرد و کفایت فرایندهای مربوط به سوابق در ایجاد، ضبط و کنترل سوابق
- ارزیابی کفایت و عملکرد سیستم‌های مربوط به سوابق (از جمله سیستم‌های کسب‌وکار برای ایجاد و کنترل سوابق)، مناسب بودن ابزارهای فنّاورانه استفاده شده، و امکانات و تجهیزات مستقر شده
- ارزیابی سطوح مختلف شایستگی در مدیریت سوابق مورد نیاز در یک سازمان و ارزیابی آن شایستگی
- اهمیت محتوا، بافت، ساختار، نمایش و کنترل اطلاعات (فرا داده) مورد نیاز برای تعیین و مدیریت کردن سوابق و سیستم‌های سوابق
- روش‌هایی برای ایجاد ابزارهای مختص به سوابق
- فنّاوری‌های مورد استفاده برای ایجاد، ضبط، تبدیل و ارسال، و حفاظت از سوابق الکترونیکی/دیجیتالی در بلند مدت
- شناسایی و اهمیت مستندات مربوط به صدور مجوزها برای فرایندهای مربوط به سوابق.

یادآوری- در مورد اطلاعات تکمیلی به استانداردهای تدوین شده توسط ISO/TC 46/SC 11 در مورد مدیریت سوابق مراجعه شود.

الف-۶ مثال تشریحی در مورد دانش و مهارت‌های ممیزان مختص به رشته تخصصی مدیریت ترمیم‌پذیری، امنیت، آمادگی و مداومت

دانش و مهارت‌های مرتبط با رشته تخصصی و به کارگیری روش‌ها، فنون، فرایندها و رویه‌های مختص به رشته تخصصی بایستی کافی باشد تا ممیز بتواند سیتم مدیریت را بررسی کند و یافته‌ها و نتیجه‌گیری‌های ممیزی را به وجود آورد.

مثال‌ها به شرح زیر می‌باشد:

- فرایندها، علوم و فنّاوری‌ای که مبنای[1] مدیریت ترمیم‌پذیری، امنیت، آمادگی، پاسخگویی، مداومت و بازیابی را تشکیل می‌دهند
- روش‌هایی برای جمع‌آوری اطلاعات و پایش

1-Underlying

- مدیریت کردن ریسک‌های رخدادهای مخرب (پیش‌بینی، اجتناب، پیشگیری، محافظت، کاهش[1]، پاسخگویی به رخداد مخرب و بازیابی آن)
- ارزیابی ریسک (شناسایی و ارزش‌گذاری دارایی و شناسایی، تحلیل، ارزیابی ریسک) و تحلیل پیامد (مرتبط با دارایی‌های منابع انسانی، فیزیکی و ناملموس و نیز زیست محیطی)
- بهبود ریسک (سازگاری، اقدامات کنش‌گرایانه و واکنشی)[2]
- روش‌ها و رویه‌های مربوط به درستی و حساسیت
- روش‌های مربوط به امنیت کارکنان و حفاظت اشخاص
- روش‌ها و رویه‌های مربوط به حفاظت دارایی و امنیت فیزیکی
- روش‌ها و رویه‌های مربوط به مدیریت پیشگیری، بازدارندگی[3] و امنیت
- روش‌ها و رویه‌های مربوط به مدیریت کاهش پیشامدها، پاسخگویی، و مدیریت بحران
- روش‌ها و رویه‌های مربوط به مدیریت مداومت، اضطرار و بازیابی
- روش‌ها و رویه‌های مربوط به پایش، اندازه‌گیری و گزارش‌دهی عملکرد (شامل روش‌های تمرین و آزمون).

یادآوری- در مورد اطلاعات تکمیلی به استانداردهای مرتبط تدوین شده توسط کمیته‌های فنی ISO/TC 8، ISO/TC 223 و ISO/TC 247 در خصوص مدیریت ترمیم‌پذیری، امنیت، آمادگی و مداومت مراجعه شود.

الف-۷ مثال تشریحی از دانش و مهارت‌های ممیزان مختص به رشته تخصصی مدیریت امنیت اطلاعات

دانش و مهارت‌های مرتبط با رشته تخصصی و به کارگیری روش‌ها، فنون، فرایندها و رویه‌های مختص به رشته تخصصی بایستی کافی باشد تا ممیز بتواند سیستم مدیریت را بررسی کند و یافته‌ها و نتیجه‌گیری‌های ممیزی را به وجود آورد.

مثال‌ها به شرح زیر می‌باشد:

- راهنمایی‌هایی برگرفته از استانداردها مانند استانداردهای ISO/IEC 27000، ایران- ایزو- آی ای سی ۲۷۰۰۱، ایران- ایزو- آی ای سی ۲۷۰۰۲، ایران- ایزو- آی ای سی ۲۷۰۰۳، ISO/IEC 27004 و ایران- ایزو- آی ای سی ۲۷۰۰۵[4]
- شناسایی و ارزیابی الزامات مربوط به مشتریان وطرف‌های ذی‌نفع
- قوانین و مقررات مرتبط با امنیت اطلاعات (برای مثال حقوق مالکیت معنوی، محتوا، حفاظت و نگهداری سوابق سازمانی، حفاظت و محرمانه بودن داده‌ها، مقررات مربوط به کنترل‌های رمزنویسی[5]، ضد تروریسم، تجارت الکترونیک، امضای دیجیتالی و الکترونیکی، تحت نظر داشتن محل کار، ارگونومی محل کار،

1-Mitigate
2-Proactive and reactive
3-Deterrence

۴-در مورد استانداردهای ذکر شده به کتاب‌نامه مراجعه شود.

5-Cryptography

رهگیری و پایش داده‌های مخابراتی راه دور (برای مثال: رایانامه[1]) سوء استفاده کامپیوتری، جمع آوری الکترونیکی شواهد، آزمون میزان نفوذ و غیره

- فرایندها، علوم و فنّاوری که مبنای مدیریت اطلاعات را تشکیل می دهد
- ارزیابی ریسک (شناسایی، تحلیل و ارزیابی) و روندهای مربوط به فنّاوری، تهدیدها و آسیب پذیری‌ها
- مدیریت ریسک امنیت اطلاعات
- روش‌ها و رویه‌های مربوط به کنترل‌های امنیت اطلاعات (الکترونیکی و فیزیکی)
- روش‌ها و رویه‌های مربوط به درستی و حساسیت
- روش‌ها و رویه‌های مربوط به اندازه‌گیری و ارزیابی اثربخشی سیستم مدیریت امنیت و کنترل‌های مرتبط
- روش‌ها و رویه‌های مخصوص اندازه‌گیری، پایش و ضبط عملکرد (شامل آزمون، ممیزی‌ها و بازنگری‌ها).

یادآوری- در مورد اطلاعات تکمیلی به استانداردهای مرتبط تدوین شده توسط ISO/IEC JTC 1/SC 27 در خصوص مدیریت امنیت اطلاعات مراجعه شود.

الف- ۸ مثال تشریحی از دانش و مهارت‌های ممیزان مختص به رشته تخصصی مدیریت سلامت و ایمنی شغلی

الف- ۸- ۱ دانش عمومی و مهارت‌ها

دانش و مهارت‌های مرتبط با رشته تخصصی و به کارگیری روش‌ها، فنون، فرایندها و رویه‌های مختص به رشته تخصصی بایستی کافی باشد تا ممیز بتواند سیستم مدیریت را بررسی کند و یافته‌ها و نتیجه‌گیری‌های ممیزی را به وجود آورد.

مثال‌ها به شرح زیر می‌باشد:

- شناسایی خطرات، از جمله عوامل تاثیر گذار بر عملکرد انسان در محل کار و دیگر عوامل (مانند عوامل فیزیکی، شیمیایی و زیست شناسی و نیز جنسیت، سن، معلولیت یا سایر عوامل فیزیولوژی، روانشناختی یا سلامتی)
- ارزیابی ریسک، تعیین کردن کنترل‌ها، و تبادل اطلاعات درخصوص ریسک [تعیین کنترل‌ها بایستی بر مبنای "سلسله مراتب کنترل‌ها" باشد (به بند ۴-۳-۱ از استاندارد ملی ایران شماره ۱۸۰۰۱ سال ۱۳۸۷، سیستم‌های مدیریت ایمنی و بهداشت حرفه ای- الزامات، مراجعه شود)]
- ارزیابی عوامل انسانی و مرتبط با سلامت (شامل عوامل روانشناختی و فیزیولوژی) و اصول مربوط به ارزیابی آن‌ها
- روش‌های مربوط به پایش در معرض آسیب بودن و ارزیابی ریسک‌های مرتبط با سلامت و ایمنی شغلی (شامل آن‌هایی که ناشی از عوامل انسانی ذکر شده در فوق یا مرتبط با سلامت و ایمنی شغلی می‌باشند) و راهبردهای مرتبط برای حذف یا به حداقل رساندن چنین در معرض آسیب بودن‌هایی

1-E-mail

- رفتار فردی، تعاملات فرد با فرد و تعاملات میان افراد با ماشین‌ها، فرایندها و محیط کاری (شامل محل کار، اصول مربوط به ارگونومی و طراحی ایمن، فنّاوری‌های اطلاعات و ارتباطات)
- ارزیابی انواع و سطوح مختلف شایستگی مربوط به سلامت و ایمنی شغلی مورد نیاز در سرتاسر سازمان و ارزیابی آن شایستگی‌ها
- شیوه هایی جهت ترغیب کارکنان برای مشارکت و دخیل بودن
- شیوه‌هایی برای ترغیب "تندرستی یا شادابی"[1] کارکنان و خود مسئولیت‌پذیری (در ارتباط با استعمال دخانیات یا مواد مخدر، موضوعات مرتبط با وزن، ورزش، تنش، رفتار تهاجمی و غیره) در ساعات کاری و در زندگی خصوصی کارکنان
- بهبود، استفاده و ارزیابی اقدامات و سنجه‌های عملکردی کنش‌گرایانه و واکنشی
- اصول و رویه‌های مربوط به شناسایی وضعیت‌های اضطراری بالقوه و مربوط به طرح‌ریزی اضطراری، پیشگیری، پاسخگویی و بازیابی
- روش‌های مربوط به بررسی و ارزیابی پیشامد (شامل حوادث و بیماری‌های مرتبط با کار)
- تعیین و استفاده از اطلاعات مرتبط با سلامتی (شامل داده‌های در معرض آسیب بودن، بیماری ناشی از محل کار و پایش آن) و مبذول کردن توجه ویژه در خصوص رعایت محرمانگی جنبه‌های خاصی از این اطلاعات
- درک اطلاعات پزشکی (شامل اصطلاحات پزشکی که برای درک داده‌های مرتبط با پیشگیری از جراحات و بیماری‌ها کافی باشد)
- سیستم‌های مربوط به مقادیر "حد در معرض آسیب بودن شغلی"
- روش‌های مربوط به پایش و گزارش‌دهی در مورد عملکرد سلامت و ایمنی شغلی
- درک کافی از الزامات قانونی و سایر الزامات مرتبط با سلامت و ایمنی شغلی برای این که ممیز بتواند سیستم‌های مدیریت سلامت و ایمنی شغلی را ارزیابی کند.

الف- ۸- ۲ دانش و مهارت‌های مرتبط با بخش اقتصادی در حال ممیزی

دانش و مهارت‌های مرتبط با بخش اقتصادی در حال ممیزی بایستی در حد کافی باشد تا ممیز بتواند سیستم مدیریت در مفهوم بخش اقتصادی را بررسی و یافته‌ها و نتیجه‌گیری‌های مناسب ممیزی را ایجاد کند.

مثال‌ها به شرح زیر می‌باشد:

- فرایندها، تجهیزات، مواد خام، مواد خطرناک، چرخه‌های فرایندی، نگهداری، پشتیبانی، گردش کار سازمانی، رویه‌های کاری، زمان‌بندی شیفت، فرهنگ سازمانی، راهبری، رفتار و سایر موضوعات مختص به فعالیت یا بخش اقتصادی

1-Wellness or well-being

- خطرات و ریسک‌های نوعی برای بخش اقتصادی، شامل عوامل انسانی و مرتبط با سلامت.

یادآوری- در مورد اطلاعات تکمیلی به استانداردهای تدوین شده ذی‌ربط توسط سازمان بین‌المللی ایزو و گروه پروژه ای OHSAS در خصوص مدیریت سلامت و ایمنی شغلی رجوع کنید.

پیوست ب
(جهت آگاهی)
راهنمایی‌های تکمیلی برای ممیزان در مورد طرح‌ریزی و انجام ممیزی‌ها

ب-۱ به کارگیری روش‌های ممیزی

ممیزی را می توان با استفاده از گستره‌ای از روش‌های ممیزی انجام داد. شرحی از روش‌های معمول مورد استفاده را می‌توان در این پیوست یافت. روش‌های ممیزی انتخاب شده برای ممیزی به اهداف تعیین شده، دامنه شمول و معیارها و نیز مدت زمان و مکان ممیزی بستگی دارد. شایستگی موجود ممیز و هر گونه عدم قطعیت ناشی از به کارگیری روش‌های ممیزی نیز بایستی در نظر گرفته شود. به کارگیری ترکیبی از روش-های ممیزی مختلف و گوناگون می‌تواند کارآیی و اثربخشی فرایند ممیزی و نتایج آن را بهینه سازد.

اجرای یک ممیزی، تعامل میان افراد با سیستم مدیریت مورد ممیزی و فنّاوری مورد استفاده برای انجام ممیزی را شامل می‌شود. در جدول ب-۱ مثال‌هایی از روش‌های ممیزی که می‌تواند به تنهایی یا به صورت ترکیبی برای دستیابی به اهداف ممیزی استفاده شود، ارائه شده است. در صورتی که ممیزی شامل استفاده از تیم ممیزی با چندین عضو باشد، هر دو روش ممیزی در محل و از راه دور می‌تواند به کار رود.

یادآوری- اطلاعات تکمیلی در خصوص بازدیدهایی از محل در پیوست ب-۶ ارائه شده است.

جدول ب-۱- روش‌های قابل کاربرد ممیزی

میزان مشارکت بین ممیز و سازمان ممیزی‌شونده	محل ممیز	
	در محل	از راه دور
تعامل فردی	انجام مصاحبه‌ها تکمیل چک‌لیست‌ها و پرسشنامه‌ها با مشارکت سازمان ممیزی‌شونده انجام بازنگری مدارک با مشارکت سازمان ممیزی‌شونده نمونه‌گیری	از طریق روش‌های تبادل اطلاعات تعاملی: - انجام مصاحبه‌ها - تکمیل چک‌لیست‌ها و پرسشنامه‌ها - انجام بازنگری مدارک با مشارکت سازمان ممیزی‌شونده
بدون تعامل فردی	انجام بازنگری مدارک (برای مثال تحلیل سوابق، داده‌ها) ناظر بودن بر کار در حال انجام انجام بازدید از محل (تکمیل چک‌لیست‌ها) نمونه‌گیری (برای مثال محصولات)	انجام بازنگری مدارک (برای مثال تحلیل سوابق، داده‌ها) ناظر بودن بر کار در حال انجام از طریق بازبینی، ضمن در نظر گرفتن الزامات اجتماعی و قانونی تحلیل داده‌ها
فعالیت‌های ممیزی در محل، در مکان سازمان ممیزی‌شونده انجام می‌شود. فعالیت‌های از راه دور ، صرف‌نظر از قاصله در هر محلی غیر از محل سازمان ممیزی‌شونده انجام می‌شوند. فعالیت‌های تعاملی ممیزی، تعامل بین کارکنان سازمان ممیزی‌شونده و تیم ممیزی را دربر می‌گیرد. فعالیت‌های غیرتعاملی ممیزی، هیچگونه تعامل انسانی با افرادی که نماینده سازمان ممیزی‌شونده می باشند را دربر نمی‌گیرد ولی با تجهیزات، امکانات و مستندات در تعامل است.		

مسئولیت به کارگیری اثر بخش روش‌های ممیزی برای هر ممیزی در مرحله طرح‌ریزی بر عهده شخص مدیریت کننده برنامه ممیزی یا راهبر تیم ممیزی می‌باشد. راهبر تیم مسئولیت انجام فعالیت‌های ممیزی را بر عهده دارد.

امکان‌پذیر بودن فعالیت‌های ممیزی از راه دور، مبتنی بر سطح اطمینان بین ممیز و کارکنان سازمان ممیزی-شونده است.

در سطح برنامه ممیزی، بایستی اطمینان حاصل نمود که به کارگیری روش‌های ممیزی از راه دور و در محل به منظور حصول اطمینان از دستیابی به اهداف برنامه ممیزی، مناسب و متوازن شده است.

ب-۲ انجام بازنگری مدارک

ممیزان بایستی بررسی کنند که آیا اطلاعات ارائه شده در مدارک:

- تکمیل است (کل محتوای مورد انتظار در مدرک گنجانده شده است)
- صحیح است (محتوا با منابع قابل اطمینان مانند استانداردها و مقررات مطابقت دارد)
- همخوان است (مدرک و محتوای آن در درون خود و با مدارک وابسته همخوانی داشته باشد)
- جاری است (محتوا روز آمد است)
- مدارک مورد بازنگری دامنه شمول ممیزی را پوشش می دهد و اطلاعات کافی در خصوص پشتیبانی از اهداف ممیزی ارائه شده است
- استفاده از فنّاوری‌های اطلاعات و ارتباطات بر حسب روش‌های ممیزی، انجام اثر بخش ممیزی را ترویج می‌کند: در مورد امنیت اطلاعات به دلیل مقررات قابل کاربرد برای حفاظت داده‌ها دقت ویژه‌ای لازم است (به ویژه در خصوص اطلاعاتی که در خارج از دامنه شمول ممیزی قرار دارد ولیکن در مدرک نیز ذکر شده است).

یادآوری- بازنگری مدارک می‌تواند حاکی از اثربخشی کنترل مدارک در سیستم مدیریت سازمان ممیزی‌شونده باشد.

ب-۳ نمونه‌گیری

ب-۳-۱ کلیات

نمونه‌گیری هنگامی صورت می‌گیرد که بررسی کلیه اطلاعات موجود در حین ممیزی عملی یا مقرون به صرفه نیست، برای مثال تعداد سوابق بیش از حد زیاد هستند یا از نظر جغرافیایی بسیار پراکنده‌اند به نحوی که بررسی تک تک اقلام جامعه توجیه پذیر نیست. نمونه‌گیری برای ممیزی از یک جامعه بزرگ عبارت است از فرایند انتخاب کمتر از ۱۰۰% اقلام درون کل مجموعه داده‌های موجود (جامعه) برای به دست آوردن و ارزیابی شواهدی در خصوص برخی ویژگی‌های آن جامعه برای این که نتیجه‌گیری در خصوص آن جامعه را شکل دهد.

هدف از نمونه‌گیری در ممیزی، فراهم کردن اطلاعات برای ممیز است تا اطمینان حاصل کند که می‌تواند یا خواهد توانست به اهداف ممیزی دست یابد.

ریسک مرتبط با نمونه‌گیری به این معنی است که نمونه‌ها ممکن است معرف جامعه‌ای که از آن انتخاب شده اند، نباشند و بنابراین نتیجه‌گیری ممیز ممکن است تحت تاثیر قرار گیرد و متفاوت از نتیجه‌گیری باشد که در شرایط بررسی کل جامعه می توانست به دست آید. ممکن است ریسک‌های دیگری بسته به تغییرپذیری در درون جامعه مورد نمونه‌گیری و روش انتخاب شده وجود داشته باشد.

نمونه‌گیری ممیزی نوعا مراحل زیر را شامل می‌شود:

- تعیین اهداف طرح نمونه‌گیری
- انتخاب حدود و ترکیب جامعه مورد نمونه‌گیری
- انتخاب روش نمونه‌گیری
- تعیین اندازه نمونه انتخابی
- انجام فعالیت نمونه‌گیری
- گردآوری، ارزیابی، گزارش‌دهی و مستند سازی نتایج.

هنگام نمونه‌گیری، بایستی کیفیت داده‌های موجود را در نظر گرفت زیرا داده‌های ناکافی و نادرست مربوط به نمونه‌گیری نتیجه مفیدی را فراهم نمی‌کند. انتخاب یک نمونه مناسب بایستی هم بر مبنای روش نمونه-گیری و هم نوع داده‌های مورد نیاز باشد، برای مثال به منظور استنتاج کردن الگوی رفتاری ویژه یا استنتاج‌هایی در مورد یک جامعه.

گزارش‌دهی درخصوص نمونه انتخابی ممکن است اندازه نمونه، روش انتخاب، و تخمین‌هایی بر مبنای نمونه و سطح انتخاب را در نظر گیرد.

در ممیزی می توان از نمونه‌گیری بر مبنای داوری (به بند ب-۳-۲ مرجعه شود) یا نمونه‌گیری آماری استفاده کرد (به بند ب-۳-۳ مرجعه شود).

ب-۳-۲ نمونه‌گیری مبتنی برداوری

نمونه‌گیری مبتنی بر داوری به دانش، مهارت و تجربه تیم ممیزی متکی است (به بند ۷ مراجعه شود).

در نمونه‌گیری مبتنی بر داوری موارد زیر را می توان در نظر گرفت:

- تجربه ممیزی پیشین در دامنه شمول ممیزی
- پیچیدگی الزامات (شامل الزامات قانونی) برای دستیابی به اهداف ممیزی
- پیچیدگی و تعامل فرایندهای سازمانی و اجزای سیستم مدیریت
- میزان تغییر در فنّاوری، عامل انسانی یا سیستم مدیریت
- زمینه‌های ریسک کلیدی و زمینه‌های بهبود که قبلا شناسایی شده‌اند
- ماحصل پایش سیستم‌های مدیریت.

اشکال نمونه‌گیری مبتنی بر داوری این است که می‌تواند هیچ گونه تخمین آماری از تاثیر عدم قطعیت بر یافته‌های ممیزی و نتیجه‌گیری‌های حاصل شده وجود نداشته باشد.

ب-۳-۳ نمونه‌گیری آماری

اگر تصمیم گرفته شده باشد که از نمونه‌گیری آماری استفاده شود، طرح نمونه‌گیری بایستی مبتنی بر اهداف ممیزی و اطلاعات در خصوص ویژگی‌های کل جامعه ای باشد که نمونه‌ها از آن گرفته شده‌اند.

- در طراحی نمونه‌گیری آماری از فرایند انتخاب نمونه بر مبنای نظریه احتمالات استفاده می‌شود. از نمونه-گیری مبتنی بر وصفی‌ها هنگامی استفاده می‌شود که تنها دو نتیجه نمونه احتمالی برای هر نمونه وجود دارد (برای مثال صحیح/ناصحیح یا قبول/مردود). از نمونه‌گیری مبتنی بر متغیرها هنگامی استفاده می‌شود که نتایج نمونه در گستره پیوسته‌ای رخ دهد.
- طرح نمونه‌گیری بایستی احتمال این که نتایج مورد بررسی بر مبنای وصفی‌ها یا بر مبنای متغیرها باشند را در نظر گیرد. برای مثال هنگام ارزیابی انطباق فرم‌های تکمیل شده بر طبق الزامات بیان شده در روش اجرایی، رویکرد مبتنی بر وصفی‌ها می‌توانست به کار گرفته شود. هنگام بررسی وقوع پیشامدهای مربوط به ایمنی مواد غذایی یا تعداد موارد نقض امنیتی، احتمالا یک رویکرد مبتنی بر متغیرها بیشتر مناسب خواهد بود.
- اجزای کلیدی که بر طرح نمونه‌گیری تاثیر خواهند داشت عبارتند از:
  - اندازه سازمان
  - تعداد ممیزان شایسته
  - فراوانی ممیزی‌ها در طول یک سال
  - مدت زمان هر ممیزی
  - هر گونه سطح اطمینان الزام شده بیرون از سازمان.
- هنگامی که طرح نمونه‌گیری آماری تدوین می‌شود، سطح ریسک نمونه‌گیری که ممیز تمایل به پذیرش آن را دارد، عامل مهمی است. به این موضوع اغلب به عنوان سطح اطمینان قابل پذیرش اطلاق می‌شود. برای مثال ریسک نمونه‌گیری ۵% متناظر با سطح اطمینان ۹۵% است. ریسک نمونه‌گیری ۵% به این مفهوم است که ممیز تمایل به پذیرش ریسک آن را دارد که ۵ از ۱۰۰ (یا ۱ از ۲۰) از نمونه‌های بررسی شده مقادیر واقعی قابل مشاهده را چنانچه کل جامعه مورد بررسی قرار می گرفت، منعکس نمی‌کند.
- هنگامی که از نمونه‌گیری آماری استفاده شود، ممیزان بایستی به نحو مناسبی کارهای اجرا شده را مدون کنند. این موضوع بایستی شرحی از جامعه ای که در نظر بوده مورد نمونه‌گیری قرار گیرد، معیارهای نمونه‌گیری مورد استفاده برای ارزیابی (برای مثال نمونه مورد قبول کدام است)، پارامترها و روش‌های آماری به کار گرفته شده، تعداد نمونه‌های ارزیابی شده و نتایج حاصل شده را دربرگیرد.

ب-۴ تهیه مدارک کاری

هنگام تهیه مدارک کاری، تیم ممیزی بایستی پرسش‌های زیر را برای هر مدرک در نظر گیرد:

الف- کدام سابقه ممیزی با استفاده از این مدرک کاری ایجاد خواهد شد؟

ب- کدام فعالیت ممیزی با این مدرک کاری خاص مرتبط است؟

ج- چه کسی استفاده کننده از این مدرک خواهد بود؟

د- چه اطلاعاتی برای آماده کردن این مدرک لازم است؟

در ممیزی‌های ترکیبی، مدارک کاری برای اجتناب از تکرار فعالیت‌های ممیزی از طریق موارد زیر بایستی ایجاد شوند:

- خوشه بندی الزامات مشابه از معیارهای مختلف
- هماهنگی محتوای چک‌لیست‌ها و پرسشنامه‌های مرتبط.

مدارک کاری بایستی برای پرداختن به کلیه اجزای سیستم مدیریت در دامنه شمول ممیزی کفایت کنند و می‌تواند در هر نوع رسانه ای ارائه شوند.

ب-۵ انتخاب منابع اطلاعات

منابع اطلاعات انتخاب شده ممکن است بر حسب دامنه شمول و پیچیدگی ممیزی تغییر کند و ممکن است موارد زیر را شامل شود:

- مصاحبه با کارکنان و سایر اشخاص
- ناظر بودن بر فعالیت‌ها و شرایط و محیط کاری پیرامونی
- مدارک، مانند خط‌مشی‌ها، اهداف، طرح‌ها، روش‌های اجرایی، استانداردها، دستورالعمل‌ها، پروانه‌ها، مشخصات، نقشه‌ها، قراردادها و سفارش‌ها
- سوابق، نظیر سوابق بازرسی، صورتجلسات، گزارش‌های ممیزی، سوابق پایش برنامه‌ها و نتایج اندازه گیری-ها
- خلاصه داده‌ها، تحلیل‌ها و شاخص‌های عملکرد
- اطلاعات در خصوص طرح‌های نمونه‌گیری سازمان ممیزی‌شونده و در خصوص روش‌های اجرایی برای کنترل نمونه‌گیری و فرایندهای اندازه گیری
- گزارش از سایر منابع برای مثال بازخور از مشتریان، نظر خواهی‌ها و اندازه گیری‌های برون سازمانی، سایر اطلاعات مرتبط دیگر از طرف‌های برون سازمانی و رتبه بندی تامین کنندگان
- پایگاه داده‌ها و وب گاه‌ها
- شبیه سازی و مدل‌سازی.

ب-۶ راهنمایی در خصوص بازدید از مکان سازمان ممیزی‌شونده

به منظور به حداقل رسانیدن تداخل بین فعالیت‌های ممیزی و فرایندهای کاری سازمان ممیزی‌شونده و حصول اطمینان از سلامت و ایمنی تیم ممیزی در حین بازدید، موارد زیر بایستی در نظر گرفته شود:

الف- طرح‌ریزی بازدید شامل موارد زیر است:

- حصول اطمینان از اجازه و دسترسی به آن قسمت‌هایی از مکان سازمان ممیزی‌شونده که قرار است مطابق دامنه شمول ممیزی مورد بازدید قرار گیرد

- فراهم کردن اطلاعات کافی (برای مثال ارائه شرح کوتاه) برای ممیزان در خصوص امنیت، سلامت (برای مثال قرنطینه)، موضوعات مربوط به سلامت و ایمنی شغلی و ضوابط فرهنگی برای بازدید از جمله واکسیناسیون تقاضا شده و توصیه شده و اخذ اجازه‌های مربوط، در صورت موضوعیت داشت
- تایید همراهی با سازمان ممیزی‌شونده درخصوص این که هر گونه تجهیزات حفاظتی شخصی (PPE)[1] مورد نیاز در اختیار تیم ممیزی خواهد قرار گرفت، اگر موضوعیت داشته باشد
- حصول اطمینان از این که به غیر از ممیزی‌های موردی غیر برنامه ریزی شده، کارکنان مورد بازدید از اهداف و دامنه شمول ممیزی اطلاع خواهند یافت

ب- فعالیت‌های در محل

- از هر گونه مزاحمت‌های غیر ضروری برای فرایندهای عملیاتی اجتناب شود
- حصول اطمینان از این که تیم ممیزی PPE را به نحو مناسبی به کار می‌گیرد
- حصول اطمینان از این که روش‌های اضطراری اطلاع رسانی شده‌اند (برای مثال خروجی‌های اضطراری، نقاط تجمع)
- زمان‌بندی تبادل اطلاعات به منظور به حداقل رسانیدن اختلال
- تطبیق دادن اندازه تیم ممیزی و تعداد راهنماها و ناظران مطابق با دامنه شمول ممیزی به این منظور که تا حد امکان‌پذیر از تداخل با فرایندهای عملیاتی اجتناب شود
- حتی در صورت شایستگی و یا داشتن مجوز هیچ یک از تجهیزات نبایستی لمس یا دستکاری شود، مگر این که به صراحت اجازه داده شده باشد
- چناچه در طول بازدید از محل پیشامدی رخ دهد رهبر تیم ممیزی بایستی در صورت لزوم موقعیت را با سازمان ممیزی‌شونده بررسی کند و در خصوص این که ممیزی بایستی متوقف شود، دوباره انجام شود یا ادامه پیدا کند به توافق برسند
- در صورت عکس گرفتن یا فیلمبرداری، پیشاپیش از مدیریت اجازه گرفته شود و به امور محرمانه و امنیتی توجه گردد و از گرفتن عکس از افراد بدون اجازه آن‌ها اجتناب شود
- در صورت تکثیر از مدارک از هر نوعی، پیشاپیش اجازه گرفته شود و موضوعات محرمانگی و امنیتی در نظر گرفته شود
- در صورت یادداشت برداری، از جمع آوری اطلاعات شخصی اجتناب نمائید مگر آن که برای اهداف ممیزی یا معیارهای ممیزی مورد نیاز باشد.

1-Personal Protective Equipment

ب-۷ انجام مصاحبه‌ها

مصاحبه‌ها یکی از مهم‌ترین روش‌های گردآوری اطلاعات می باشند و بایستی به صورت تطبیق یافته با موقعیت و شخص مصاحبه شونده یا به صورت رو در رو یا از طریق روش‌های ارتباطی، انجام شود. با این وجود ممیز بایستی موارد زیر را در نظر گیرد:

- مصاحبه‌ها بایستی با اشخاص از سطوح و حوزه‌های کاری مناسب که فعالیت‌ها یا کارها را در دامنه شمول ممیزی انجام می‌دهند، صورت پذیرد
- مصاحبه‌ها بایستی به طور معمول در حین ساعات کاری و در مواردی که عملی است در محل کار عادی شخص مورد مصاحبه صورت پذیرد
- تلاش شود که شخص مورد مصاحبه پیش از مصاحبه و در حین آن احساس راحتی نماید
- دلیل مربوط به مصاحبه و یادداشت برداری بایستی توضیح داده شود
- مصاحبه‌ها ممکن است با پرسش از اشخاص برای شرح وظایف کاری آن‌ها آغاز شود
- انتخاب دقیق نوع پرسش مورد استفاده (برای مثال باز، بسته، پرسش‌های هدایت کننده)
- نتایج حاصل از مصاحبه بایستی جمع بندی شده و با شخص مورد مصاحبه بازنگری گردد
- از مشارکت و همکاری اشخاص مصاحبه شونده بایستی تشکر شود.

ب-۸ یافته‌های ممیزی

ب-۸-۱ تعیین یافته‌های ممیزی

هنگام تعیین یافته‌های ممیزی، موارد زیر بایستی در نظر گرفته شوند:

- پیگیری سوابق و نتیجه‌گیری‌های ممیزی پیشین
- الزامات کارفرمای ممیزی
- یافته‌هایی که فراتر از رویه معمول می باشند، یا فرصت‌های بهبود
- اندازه نمونه
- رده‌بندی (در صورت وجود) یافته‌های ممیزی

ب-۸-۲ ثبت انطباق‌ها

برای ثبت انطباق، موارد زیر بایستی در نظر گرفته شود:

- مشخص کردن معیارهای ممیزی که انطباق بر اساس آن اثبات شده است
- شواهد ممیزی برای پشتیبانی انطباق
- اظهار انطباق، در صورت موضوعیت داشتن.

ب-۸-۳ ثبت عدم انطباق‌ها

برای ثبت عدم انطباق‌ها موارد زیر بایستی در نظر گرفته شوند:

- شرحی از معیارهای ممیزی یا ارجاع به آن‌ها

- اظهار عدم انطباق
- شواهد ممیزی
- یافته‌های مرتبط با ممیزی، در صورت موضوعیت داشتن.

ب-۸-۴ اقدام در مورد یافته‌های مرتبط با معیارهای چند گانه

در حین ممیزی، امکان دارد که یافته‌های مرتبط با معیارهای چند گانه شناسایی شوند. هرگاه یکی از ممیزان یافته‌ی مرتبط با یک معیار را در خصوص ممیزی ترکیبی شناسایی کند، ممیز بایستی تاثیر احتمالی بر روی معیارهای متناظر یا مشابه دیگر سیستم‌های مدیریت را در نظر گیرد.

بر حسب ترتیبات با کارفرمای ممیزی، ممیز ممکن است موارد زیر را در نظر گیرد:

- یافته‌های جداگانه برای هر معیار
- یافته‌ی واحدی که ارجاعات به معیارهای چندگانه را ترکیب می‌کند.

بر حسب ترتیبات با کارفرمای ممیزی، ممیز ممکن است سازمان ممیزی‌شونده را در خصوص چگونگی پاسخگویی در مورد یافته‌های ممیزی راهنمایی کند.

کتاب‌نامه

[۱] استاندارد ISO 2859- 4 [۱] روش‌های اجرایی نمونه‌گیری برای بازرسی از طریق وصفی‌ها، بخش چهارم: روش‌های اجرایی برای ارزیابی سطح ریسک اظهار شده

[۲] استاندارد ایران- ایزو ۹۰۰۰ سال ۱۳۸۷ سیستم‌های مدیریت کیفیت – مبانی و واژگان

[۳] استاندارد ISO 9001 [۲] سیستم‌های مدیریت کیفیت – الزامات

[۴] استاندارد ISO 14001 سیستم‌های مدیریت زیست محیطی- الزامات همراه با راهنمایی برای استفاده

[۵] استاندارد ISO 14050 [۳] مدیریت زیست محیطی- واژه نامه

[۶] استاندارد ایران- ایزو- آی ای سی ۱۷۰۲۱ : ۱۳۹۳ ارزیابی انطباق- الزامات نهادهای ارایه کننده خدمات ممیزی و گواهی کردن سیستم‌های مدیریتی

[۷] استاندارد ISO/IEC 20000-1 فنّاوری اطلاعات- مدیریت خدمات- قسمت ۱: الزامات مربوط به سیستم مدیریت خدمات

[۸] استاندارد ISO 22000 [۴] سیستم‌های مدیریت ایمنی مواد غذایی- الزامات هر سازمان در زنجیره مواد غذایی

[۹] استاندارد ISO/IEC 27000 فنّاوری اطلاعات – فنون امنیتی- سیستم‌های مدیریت امنیت اطلاعات- مرور کلی و واژگان

[۱۰] استاندارد ISO/IEC 27001 [۵] فنّاوری اطلاعات – فنون امنیتی- سیستم‌های مدیریت امنیت اطلاعات- الزامات

[۱۱] استاندارد ISO/IEC 27002 [۶] فنّاوری اطلاعات – فنون امنیتی- آیین کار مدیریت امنیت اطلاعات

[۱۲] استاندارد ISO/IEC 27003 [۷] فنّاوری اطلاعات – فنون امنیتی- راهنمای اجرای سیستم مدیریت امنیت اطلاعات

۱- استاندارد ملی ایران شماره ۴- ۶۶۶۵: ۱۳۸۲، روش‌های اجرایی نمونه برداری برای بازرسی از طریق وصفی‌ها بخش چهارم: روش های اجرایی برای ارزیابی سطح کیفیت اظهار شده بر مبنای ISO 2859-4: 2002 موجود است.

۲- استاندارد ایران – ایزو ۹۰۰۱: ۱۳۸۸، سیستم‌های مدیریت کیفیت- الزامات بر مبنای ISO 9001: 2008 موجود است.

۳- استاندارد ایران- ایزو ۱۴۰۵۰: ۱۳۸۵، مدیریت زیست محیطی – واژه نامه بر مبنای ISO 14050: 2002 موجود است.

۴- استاندارد ایران- ایزو ۲۲۰۰۰: ۱۳۸۶، سیستم‌های مدیریت ایمنی مواد غذایی- الزامات هر سازمان در زنجیره مواد غذایی بر مبنای ISO 22000: 2005 و ISO 22000:2005 / Cor 1: 2006 موجود است.

۵- استاندارد ایران – ایزو- آی ای سی ۲۷۰۰۱: ۱۳۸۷، فنّاوری اطلاعات – فنون امنیتی- سیستم‌های مدیریت امنیت اطلاعات- الزامات بر مبنای ISO/IEC 27001: 2005 موجود است.

۶- استاندارد ایران – ایزو- آی ای سی ۲۷۰۰۲: ۱۳۸۷، فنّاوری اطلاعات – فنون امنیتی- آیین کار مدیریت امنیت اطلاعات بر مبنای استاندارد ISO/IEC 27002: 2005 موجود است.

۷- استاندارد ایران – ایزو- آی ای سی ۲۷۰۰۳: ۱۳۸۹، فنّاوری اطلاعات – فنون امنیتی- راهنمای اجرای سامانه سیستم مدیریت بر مبنای استاندارد ISO/IEC 27003: 2010 موجود است.

کتاب‌نامه(ادامه)

[۱۳] استاندارد ISO/IEC 27004 فنّاوری اطلاعات – فنون امنیتی- مدیریت امنیت اطلاعات- الزامات

[۱۴] استاندارد ISO/IEC 27005 [۱] فنّاوری اطلاعات – فنون امنیتی- مدیریت ریسک امنیت اطلاعات

[۱۵] استاندارد ISO 28000 [۲] سیستم‌های مدیریت امنیت زنجیره تامین- مشخصات

[۱۶] استاندارد ISO 30301 [۳] اطلاعات و مستندات- سیستم مدیریت سوابق - الزامات

[۱۷] استاندارد ISO 31000 [۴] مدیریت ریسک- اصول و رهنمودها

[۱۸] استاندارد ISO 39001 سیستم‌های مدیریت ایمنی ترافیک جاده (RTS) - الزامات همراه با راهنمای استفاده

[۱۹] استاندارد ISO 50001 [۵] سیستم‌های مدیریت انرژی- الزامات همراه با راهنمای استفاده

[۲۰] راهنمای ISO GUIDE 73:2009 [۶] مدیریت ریسک- واژگان

[۲۱] استاندارد ملی ایران ۱۸۰۰۱ : ۱۳۸۷ سیستم‌های مدیریت ایمنی و بهداشت حرفه ای- الزامات

[۲۲] مقاله‌های گروه کاری ممیزی ISO 9001 قابل دسترس در وبگاه: www.iso.org/19011auditing

[۲۳] رهنمودهای تکمیلی ISO 19011 [۷] قابل دسترس در وبگاه: www.iso.org/19011auditing

۱- استاندارد ایران – ایزو- آی ای سی ۲۷۰۰۵: ۱۳۸۸، فنّاوری اطلاعات – فنون امنیتی- مدیریت ریسک امنیت اطلاعات بر مبنای ISO /IEC 27005: 2008 موجود است.

۲- استاندارد ملی ایران- ایزو ۲۸۰۰۰: ۱۳۸۷، سیستم‌های مدیریت امنیت زنجیره تامین- مشخصات بر مبنای ISO 28000: 2007 موجود است.

۳- استاندارد ISO 30301: 2011 از طرف سازمان بین المللی ISO منتشر شده است.

۴- استاندارد ملی ایران ۱۳۲۴۵: ۱۳۸۹، مدیریت ریسک – اصول و رهنمودها بر مبنای استاندارد ISO 31000: 2009 موجود است.

۵- استاندارد ملی ایران- ایزو ۵۰۰۰۱: ۱۳۹۰، سیستم‌های مدیریت انرژی- الزامات همراه با راهنمای استفاده بر مبنای ISO 50001: 2011 موجود است.

۶- استاندارد ملی ایران ۱۳۲۴۶: ۱۳۸۹، مدیریت ریسک- واژگان بر مبنای ISO GUIDE 73: 2009 موجود است.

۷- توسط سازمان بین المللی ISO در دست تهیه می‌باشد.

ICS: 03.120.10, 13.020.10