به نام خدا

راهنمای اعتباربخشی آزمایشگاه

مرکز مدیریت راهبردی افتا

مهر ۹۳

نسخه ۱,۰

پیشگفتار

با توسعه روزافزونی که در محصولات حوزه فتا وجود دارد و با عنایت به این نکته که در تمامی زیرساخت‌های حیاتی، حساس و مهم کشور بصورت کاملاً گسترده از این محصولات استفاده می‌شود، امنیت محصولات مذکور در امنیت سازمان‌ها و به تبع آن کل کشور بسیار حائز اهمیت می‌باشد. لذا وجود تهدیدات در فضای تولید و تبادل اطلاعات، ارزیابی امنیتی محصولات مورد استفاده در این حوزه را امری ضروری و اجتناب‌ناپذیر می‌سازد. بنابراین باید آزمایشگاه‌هایی در حوزه ارزیابی امنیتی محصولات فوق‌الذکر وجود داشته باشند که این مسئولیت را به انجام برسانند. اعتبار بخشی خود این آزمایشگاه‌ها و تأیید صحت عملکرد آن‌ها توسط یک مراجع بالادستی که همان مرکز افتا و سازمان فناوری اطلاعات هستند صورت می‌گیرد. آنچه که در سند «راهنمای اعتبار بخشی آزمایشگاه» مطرح شده روال‌ها و الزاماتی است که برای ارزیابی و اعتباربخشی آزمایشگاه‌ها توسط این مراجع انجام می‌شود.

فهرست

۱ هدف از ارائه سند

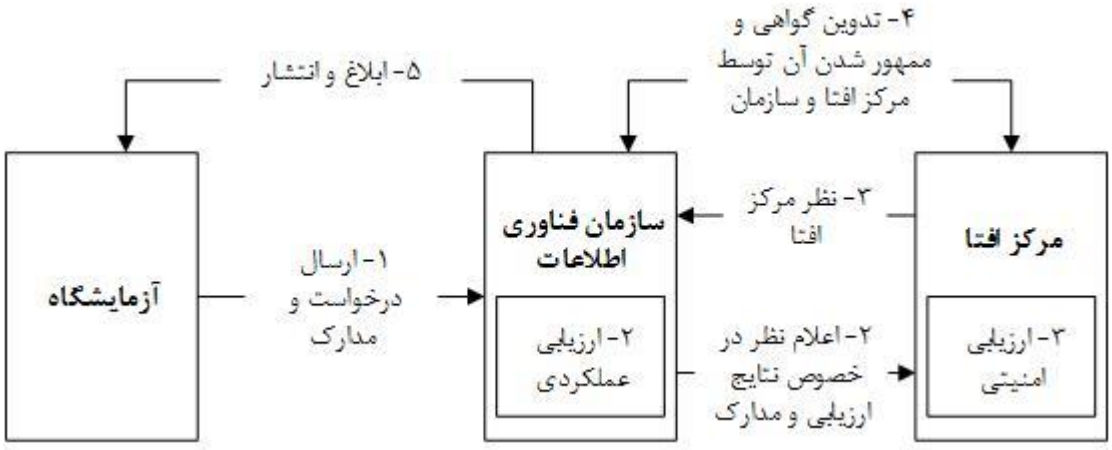
این سند حاوی روال‌ها و الزاماتی برای ارزیابی و اعتباربخشی آزمایشگاه‌ها توسط مرکز افتا و سازمان فناوری اطلاعات می‌باشد.

۱,۱ معرفی اصطلاحات

در این سند از اصطلاحات تعریف شده در سند "طرح ارزیابی امنیتی" استفاده می‌شود.

۲ فرایند اعتباربخشی آزمایشگاه

در این بخش به مسئله اعتباربخشی و ارزیابی آزمایشگاه‌های ارزیابی مبتنی بر معیار مشترک[1] پرداخته می‌شود. شکل شماره (۱) فرایند اعتباربخشی آزمایشگاه را نشان می‌دهد.



شکل ۱: فرایند اعتباربخشی آزمایشگاه

همانگونه که در شکل شماره (۱) نشان داده شده است، فرایند دریافت گواهی آزمایشگاه عبارت است از:

[1] Common Criteria

۱. ارسال درخواست و اسناد و مدارک از سوی آزمایشگاه به سازمان فناوری اطلاعات
۲. بررسی اولیه اسناد آزمایشگاه و ارزیابی عملکردی آزمایشگاه توسط سازمان و اعلام نظر در خصوص نتایج ارزیابی و مدارک و اعلام به مرکز افتا
۳. ارزیابی امنیتی آزمایشگاه توسط مرکز افتا شامل ارزیابی اولیه در محل، آزمون تخصصی، ارزیابی کامل آزمایشگاه و ارزیابی اعتباری کارکنان آزمایشگاه
۴. جمع بندی نتایج ارزیابی‌ها توسط مرکز افتا و اعلام به سازمان
۵. صدور گواهی بر اساس نتایج بند ۴ توسط سازمان و مرکز افتا به صورت مشترک پس از امضاء تعهدنامه محضری در دفتر ثبت اسناد رسمی

تذکر: آزمایشگاه باید تعهد محضری در دفتر ثبت اسناد رسمی دهد که گزارشات و نتایج ارزیابی امنیتی را صرفاً به تولید کننده و مرکز افتا ارائه داده و در حفظ و نگهداری آن نهایت سعی و تلاش خود را انجام می‌دهد.

جزئیات هر مرحله در ادامه شرح داده شده است.

۱,۲ ارسال درخواست و اسناد و مدارک لازم از سوی آزمایشگاه به سازمان فناوری اطلاعات

آزمایشگاه برای دریافت گواهی باید توسط مرکز افتا و سازمان فناوری اطلاعات اعتبار بخشی شود؛ این فرآیند با درخواست آزمایشگاه از سازمان فناوری اطلاعات آغاز می‌شود. آزمایشگاه باید درخواست خود را به همراه مدارک و مستندات زیر برای سازمان ارسال نماید.

۱- درخواست مکتوب که در قالب یک نامه رسمی تنظیم شده است.
۲- مشخصات عمومی از قبیل: نام کامل آزمایشگاه/شرکت، شناسه ملی شرکت، نوع مالکیت (خصوصی، عمومی، ...)، نوع شرکت (سهامی خاص، سهامی عام، تعاونی، مسئولیت محدود)، اسامی هیئت مدیره، مدیرعامل و کارکنان، محل ثبت، تاریخ ثبت، تلفن، دورنگار، پست الکترونیک و نشانی اینترنتی.
۳- تکمیل فرم اعتباری افراد مطابق راهنما. فرم مذکور به همراه راهنمای نحوه تکمیل آن بر روی سایت سازمان قرار گرفته است و آزمایشگاه باید تکمیل شده این فرمها را به صورت مهر و موم شده به سازمان ارسال نماید و سازمان آنها را به همان صورت در اختیار مرکز افتا قرار دهد.

۴- مشخص کردن نوع محصولات امنیتی که آزمایشگاه می‌خواهد مورد ارزیابی قرار دهد. به عنوان مثال آزمایشگاه بیان می‌کند که محصولاتی از قبیل: کارت هوشمند، مسیریاب، فایروال، سوئیچ و ... را می‌خواهد مورد ارزیابی قرار دهد.

۵- تعیین سطح ارزیابی محصولاتی که آزمایشگاه قصد ارزیابی آن‌ها را دارد. آزمایشگاه باید مشخص کند که برای هر یک از محصولات ذکر شده در بند۴ چه سطحی از EAL را پوشش خواهد داد.

۶- تعیین استانداردها و روش‌های آزمون که آزمایشگاه براساس آن‌ها فعالیت می‌کند.

۷- گواهی‌نامه‌های کیفی و مدیریتی (ISO 27001, ISO9001,...) که آزمایشگاه موفق به کسب آن‌ها شده است.

۸- چنانچه آزمایشگاه زیرمجموعه شرکت و نهاد خاصی باشد، ساختار سازمانی آن شرکت که نشان دهنده موقعیت آزمایشگاه در آن ساختار و نحوه تعامل با سایر بخش‌های شرکت می‌باشد اعلام گردد.

۹- کلیه اسناد اثبات کننده برآورده شدن الزامات و نیازها در راستای اعتبار بخشی (شامل: نظامنامه کیفیت و کلیه اسنادی که اثبات کننده الزامات آورده شده در فصول چهارم و پنجم این سند می‌باشد)

۱۰- رزومه کاری مدیرعامل و اعضای هیئت مدیره (شامل: سوابق مدیریتی، گواهی‌های آموزشی مدیریتی و فنی مرتبط با موضوع آیین‌نامه، میزان تحصیلات، مدرک تحصیلی و سوابق شغلی و فردی و سایر موارد مطابق دستورالعمل‌های ابلاغی).

۱۱- رزومه کارکنان آزمایشگاه (شامل: میزان تحصیلات، مدرک تحصیلی، گواهی‌های آموزشی مرتبط با موضوع این آیین‌نامه، سوابق کاری مرتبط و سایر موارد مطابق دستورالعمل‌های ابلاغی) و ماهیت کاری آن‌ها.

۱۲- سوابق کاری آزمایشگاه (شامل: عنوان قرارداد، نام کارفرما، مبلغ قرارداد، تاریخ شروع و اتمام قرارداد، گواهی حسن انجام کار از کارفرما و سایر موارد مطابق دستورالعمل‌های ابلاغی)

۱۳- اساسنامه.

۱۴- اظهارنامه‌های ثبت شده در سازمان امور مالیاتی (شامل: سال مالیاتی، شماره ثبت اظهارنامه، تاریخ ثبت).

۱۵- لیست بیمه کلیه کارکنان آزمایشگاه.

۱۶- آگهی آخرین تغییراتی که در روزنامه رسمی به چاپ رسیده است با قید تاریخ و شماره.

۱۷- سایر اسنادی که بر اساس دستورالعمل‌ها، آیین نامه‌ها و مقرارت ابلاغی توسط مرکز افتا و سازمان فناوری اطلاعات مورد نیاز باشد.

نحوه تکمیل و ارسال این مستندات در سایت سازمان آمده است.

۲,۲ بررسی اولیه اسناد آزمایشگاه

سازمان پس از دریافت اسناد و مدارک، آن‌ها را بررسی کرده و چنانچه در هر قسمت از مدارک ارائه شده نقص یا ابهامی موجود باشد به آزمایشگاه اعلام کرده و آزمایشگاه جهت ادامه فرایند موظف است نواقص و ابهامات را رفع نموده و مدارک تکمیلی را برای سازمان ارسال نماید. سازمان پس از بررسی اولیه و انجام ارزیابی عملکردی (با توجه به اسناد و مدارک)، مدارک و مستندات را به همراه نتیجه ارزیابی عملکردی به مرکز افتا ارسال می‌نماید.

۳,۲ ارزیابی اعتباری کارکنان آزمایشگاه

پس از ارسال اسناد و مدارک و نتایج ارزیابی عملکردی به مرکز افتا، آن مرکز طبق ضوابط اقدام به ارزیابی اعتباری کارکنان آزمایشگاه می‌نماید. در صورت مثبت بودن نتایج، فرایند اعتباربخشی آزمایشگاه ادامه می‌یابد، در غیر اینصورت تا زمان رفع مشکلات مربوطه و مثبت شدن نتایج ارزیابی اعتباری کارکنان آزمایشگاه، فرایند اعتباربخشی آزمایشگاه متوقف خواهد شد.

۴,۲ ارزیابی اولیه در محل

پس از انجام مراحل قبل، ارزیابی اولیه آزمایشگاه در محل توسط مرکز افتا انجام می‌شود. این ارزیابی بدین منظور انجام می‌شود که اطمینان حاصل شود آزمایشگاه دارای کارمندان فنی، ظرفیت‌ها و مولفه‌های سیستم مدیریتی لازم برای تکمیل و انجام موفق آزمون تخصصی بر اساس «استاندارد ارزیابی معیار مشترک و سایر استانداردها، آیین نامه‌ها و دستورالعمل‌های ابلاغی» می‌باشد. در «ارزیابی اولیه در محل» ممکن است تمام الزامات مورد نظر، برآورده نشده و نواقص و عدم تطابق‌هایی در آن مشاهده شود. در این صورت نواقص و عدم تطابق‌های مشاهده شده برای آزمایشگاه ارسال می‌شود. آزمایشگاه باید نواقص را رفع و پاسخی به گزارش عدم تطابق‌های «ارزیابی اولیه در محل» ارائه کند. برخی از عدم تطابق‌های مشخص شده در بازدید اولیه در محل، باید قبل از شروع آزمون تخصصی رفع شوند (نظیر عدم‌تطابق‌های تاثیرگذار بر روی «آزمون تخصصی») و سایر عدم تطابق‌ها نیز باید تا قبل شروع مرحله «ارزیابی کامل در محل»، مرتفع گردند.

۵,۲ آزمون تخصصی

پس از طی موفقیت‌آمیز ارزیابی اولیه در محل و تأیید رفع اشکالات بیان شده در گزارش نمایندگان مرکز افتا و سازمان و جمع بندی نتایج ارزیابی‌ها، مرحله «آزمون تخصصی» توسط مرکز افتا شروع خواهد شد.

به منظور کسب اعتبار، آزمایشگاه باید صلاحیت خود را در انجام ارزیابی بر طبق «استاندارد ارزیابی معیار مشترک و سایر استانداردها، آیین نامه‌ها و دستورالعمل‌های ابلاغی» اثبات کند. در این مرحله از روال اعتباربخشی آزمایشگاه، مرکز افتا محصولی را جهت ارزیابی در اختیار آزمایشگاه قرار می‌دهد تا آزمایشگاه آن را در سطح تضمین مشخصی که آزمایشگاه بر اساس آن اعتبار بخشی می‌شود و در گواهی آزمایشگاه ذکر خواهد شد (مثلاً EAL2) مورد ارزیابی قرار دهد. کیفیت این ارزیابی و تأیید آن توسط مرکز افتا، یکی از موارد تأثیرگذار در اعتباربخشی آزمایشگاه می‌باشد. آزمایشگاه در این ارزیابی هیچ گونه ارتباط مستقیمی با تولید کننده ندارد و کلیه ارتباطات بین تولید کننده و آزمایشگاه باید از طریق مرکز افتا باشد.

آزمایشگاه تنها درصورتی می‌تواند اعتبار لازم را در این مرحله کسب کند که:

- آزمایشگاه فرآیند ارزیابی را بر اساس سند " طرح ارزیابی امنیتی" انجام دهد.
- کارمندان آزمایشگاه درک خود را از «استاندارد ارزیابی معیار مشترک و سایر استانداردها، آیین نامه‌ها و دستورالعمل‌های ابلاغی»و «متدلوژی ارزیابی معیار مشترک» همچنین صلاحیت به کار بردن مناسب آن‌ها نشان دهند.
- در کلیه مراحل ارزیابی کلیه الزامات ابلاغی را رعایت نماید.
- سیستم کیفی را به کار برده و رکوردهای مناسب برای تمامی فعالیت‌های ارزیابی را تولید کرده باشد.

۶,۲ ارزیابی کامل در محل

آزمایشگاه باید قبل از شروع «ارزیابی کامل در محل»، ممیزی داخلی، بازبینی سیستم کیفی، فعالیت‌ها و رکوردهای مرتبط با ارزیابی محصول را انجام دهد. این امر می‌تواند در فواصل زمانی «آزمون تخصصی» یا در پایان ارزیابی محصول انجام شود. مهم این است که این موارد باید قبل از «ارزیابی کامل در محل» خاتمه یافته باشند. پس از اطلاع رسانی آزمایشگاه به مرکز افتا پیرامون طی شدن موفقیت آمیز الزامات فوق، مرکز افتا «ارزیابی کامل در محل» را انجام خواهد داد. آزمایشگاه باید امکانات و تجهیزات با کارکرد مناسب را دارا باشد و و امکانات لازم برای ارزیاب مرکز افتا را از لحاظ زمان و فضای کاری مناسب برای اتمام ارزیابی مستندات حین مدت ارزیابی در محل آزمایشگاه فراهم آورد.

فعالیت‌هایی که در حین «ارزیابی کامل در محل» انجام می‌شود به صورت زیر است:

- جلسه آغازین

نماینده مرکز افتا با مدیر، کارشناسان ارشد و مسئولین آزمایشگاه دیدار کرده و هدف از ارزیابی در محل و همچنین زمانبندی فعالیت‌های ارزیابی را برای آن‌ها بیان می‌کند. در این ملاقات ممکن است اطلاعاتی که در اسناد درخواست آزمایشگاه ذکر شده مورد بحث قرارگیرد.

- مصاحبه با کارکنان آزمایشگاه

نماینده مرکز افتا در صورت نیاز با کارکنان آزمایشگاه مصاحبه خواهد نمود.

- بازرسی رکوردها

نماینده مرکز افتا مستندات مربوط به آزمایشگاه را بررسی می‌کند. این مستندات شامل چشم انداز کیفی، نظامنامه کیفیت، تجهیزات و رکوردهای نگهداری، خط‌مشی‌های حفظ رکوردها، خط‌مشی‌های تست، رکوردها و گزارشات ارزیابی آزمایشگاه، رکوردهای صلاحیت کارکنان (مانند رزومه)، رکوردها و طرح‌های آموزشی کارکنان، خط‌مشی‌های مربوط به بروز رسانی اطلاعات (مانند نسخه‌های «استاندارد ارزیابی معیار مشترک» و «متدلوژی ارزیابی معیار مشترک») و طرح امنیت فناوری اطلاعات و ارتباطات آزمایشگاه جهت حفاظت از محصول و داده‌های حساس مرتبط با آن می‌باشد.

- بازرسی ممیزی و مدیریتی

نماینده مرکز افتا فعالیت‌های مرتبط با ممیزی‌های داخلی و مدیریتی شامل خط‌مشی‌های سیستم کیفی، یافته‌های ممیزی، نتایج وارسی مدیریتی و اقدامات صورت گرفته برای رفع مشکلات مشخص شده را بررسی می‌کند.

- سایر الزامات مدیریتی و فنی ابلاغی

نماینده مرکز افتا سایر الزامات مدیریتی و فنی که در فصول آتی این مستند بیان شده‌اند و یا در قالب آیین نامه‌ها، دستورالعمل‌ها و ضوابط ابلاغ خواهد شد را در آزمایشگاه مورد بازرسی قرار می‌دهد.

- مسائل مربوط به ارزیابی اولیه در محل

نماینده مرکز افتا در مورد «ارزیابی اولیه در محل» با کارکنان صحبت و آن را وارسی می‌کند که شامل تأیید رفع عدم تطابق‌ها، نقطه نظرات و یا مشکلاتی که بعد از آن به وجود آمده بود می‌باشد.

- جلسه پایانی

در پایان «ارزیابی کامل در محل» جلسه‌ای با مدیر آزمایشگاه و دیگر کارکنان برگزار می‌گردد تا در رابطه با یافته‌های نماینده مرکز افتا گفتگو شود. در حین ملاقات، نماینده مسائل مشخص شده را در قالب عدم تطابق‌ها، مشکلات و نقطه نظرات دسته‌بندی می‌کند و راه‌کارهای لازم را بیان می‌دارد.

- گزارش «ارزیابی کامل در محل»

نماینده مرکز افتا «ارزیابی کامل در محل» را با گزارشی از خلاصه یافته‌ها به پایان می‌رساند. این گزارش شامل نتایج ارزیابی و چک لیست‌های مطابق با این سند می‌باشد.

۷,۲ صدور گواهی

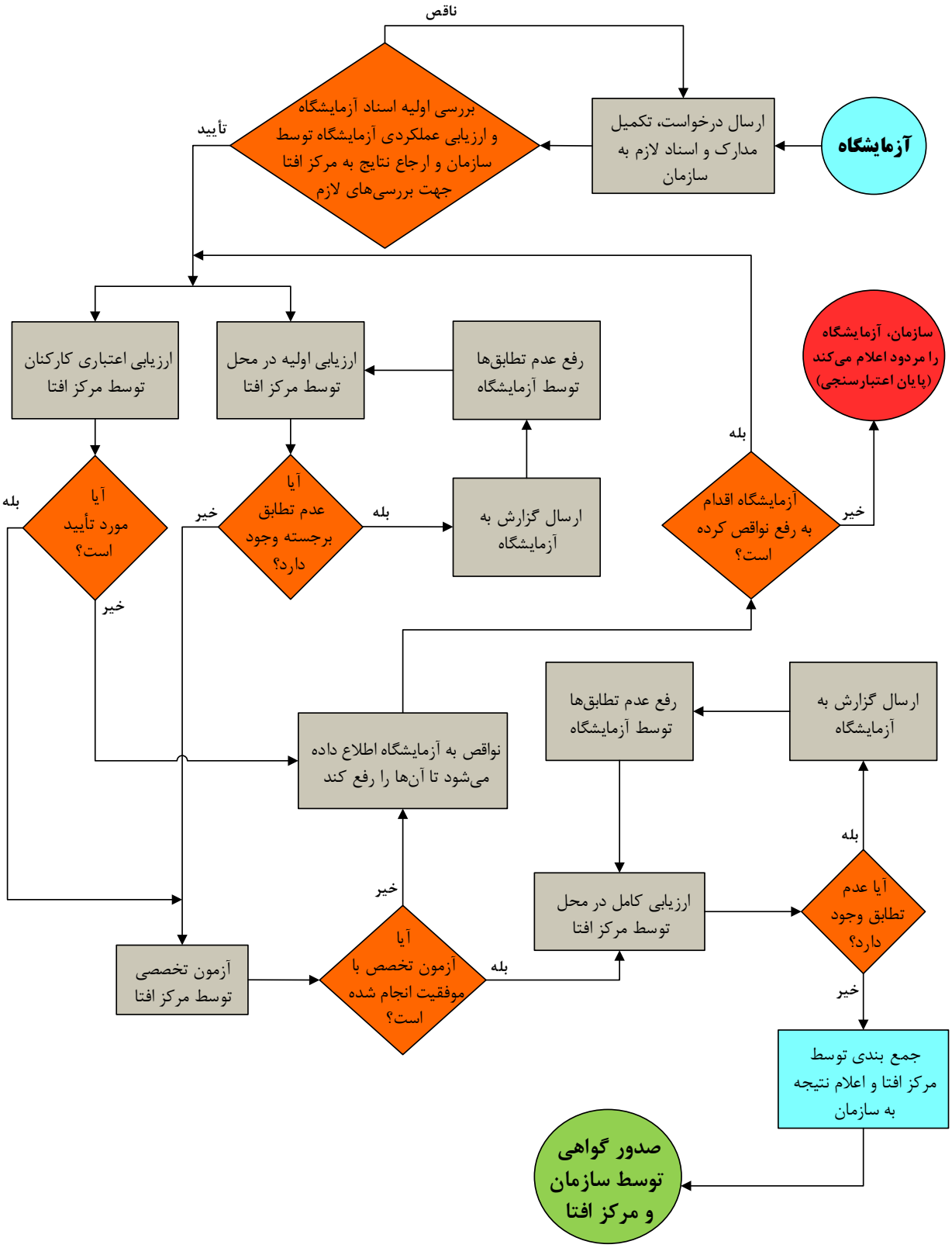
در پایان براساس جمع‌بندی نتایج ارزیابی‌ها مرکز افتا تصمیم نهایی خود را در مورد صدور/ عدم صدور گواهی آزمایشگاه اتخاذ کرده و به سازمان اعلام می‌کند. در صورت مثبت بودن نتایج ارزیابی‌ها، گواهی فعالیت آزمایشگاه به صورت مشترک توسط سازمان و مرکز افتا مهر خواهد شد.

موارد زیر در متن مجوز بیان خواهد شد:

- مدت اعتبار (تاریخ شروع و انقضای اعتبار)
- نوع محصولاتی که آزمایشگاه مجاز به ارزیابی آن‌ها می‌باشد
- سطح تضمین ارزیابی (EAL) محصولات
- تعهد آزمایشگاه به تعهدنامه حفظ کیفیت و محرمانگی

قبل از صدور گواهی، تعهدنامه‌ای محضری تحت عنوان «تعهدنامه حفظ کیفیت و محرمانگی آزمایشگاه ارزیابی امنیتی» که توسط مرکز افتا تهیه و تنظیم شده است باید توسط آزمایشگاه در دفتر اسناد رسمی ثبت، مهر و امضاء شود.

روال کلی اعتباربخشی آزمایشگاه



۸,۲ روال تمدید اعتبار آزمایشگاه

اعتبار آزمایشگاه بصورت سالانه تمدید می‌شود. آزمایشگاه موظف است سه ماه قبل از انقضای مدت اعتبار مجوز خود، بصورت مکتوب تقاضای تمدید اعتبار را به سازمان اعلام نماید. تمدید/ عدم تمدید اعتبار آزمایشگاه بر اساس گزارش نظارت بر فعالیت آزمایشگاه از جهت رعایت الزامات و ضوابط ابلاغی و تعهدنامه و نیز ارزیابی مراقبتی انجام می‌شود.

سازمان پس از دریافت تقاضای مکتوب آزمایشگاه مبنی بر تمدید اعتبار، فرمی را تحت عنوان فرم تمدید به آزمایشگاه متقاضی تمدید، ارسال می‌کند و در آن هزینه، شرایط و اقدامات لازم برای تمدید اعتبار را ذکر می‌نماید.

۹,۲ روال تغییر در حوزه اعتبار

آزمایشگاهی که از سوی سازمان و مرکز افتا اعتبار بخشی شده است، می‌تواند از طریق یک درخواست مکتوب به سازمان تغییر در حوزه اعتبار (تغییر در نوع محصولات مورد ارزیابی و یا سطح EAL تحت پوشش) خود را تقاضا نماید.

اگر آزمایشگاه با درخواست جدید، از سازمان بخواهد حوزه اعتبار خود را ارتقا دهد تا برای سطوح بالاتر (EAL) مورد ارزیابی قرار بگیرد و یا محصولات جدیدی را به حوزه ارزیابی خود اضافه کند باید تمامی الزامات آن ارتقا (حوزه محصولات، سطح ارزیابی و یا استانداردها) را برآورده سازد.

تشخیص نیاز به انجام «ارزیابی در محل» و «آزمون تخصصی مجدد» بر اساس مورد، برعهده مرکز افتا می‌باشد.

چنانچه آزمایشگاه با تغییر حوزه اعتبار خود به هر دلیلی برخی از محصولات را از لیست ارزیابی خارج کند، موظف است قراردادهایی را که در مورد آن محصولات با مشتریان منعقد کرده است دقیقاً مطابق با توافق‌نامه سطح خدمات به پایان برساند و درصورتی‌که آزمایشگاه قادر به انجام این کار نباشد باید هزینه‌های انجام ارزیابی محصول مورد نظر توسط یکی دیگر از آزمایشگاه‌های دارای گواهی و ضرر و زیان وارده شده به تولید کننده را تقبل نماید. چنانچه آزمایشگاه دیگری برای ارزیابی آن محصول موجود نباشد، مرکز افتا حسب مورد تصمیم نهایی را اتخاذ و به آزمایشگاه ابلاغ خواهد کرد.

آزمایشگاه می‌تواند حوزه اعتبار خود را معلق کند که این تعلیق باید حداقل دو ماه قبل به مرکز افتا اعلام شود.

۱۰,۲ روال تعلیق اعتبار

اگر در هر زمان محرز شود که آزمایشگاه هر یک از شرایط لازم برای دریافت اعتبار را از دست داده است، مرکز افتا اعتبار آزمایشگاه را تا زمان برآورده شدن شرایط مورد نظر معلق ساخته و مراتب را جهت انتشار به سازمان فناوری اطلاعات اعلام می‌دارد. همچنین در صورت ورشکستگی آزمایشگاه، اعتبار آن معلق خواهد شد.

عدم اعلام و عدم اخذ موافقت کتبی از مرکز افتا در خصوص هرگونه تغییر در شرایطی که بر اساس آن‌ها آزمایشگاه اعتباربخشی شده است، منجر به تعلیق اعتبار آزمایشگاه تا زمان رفع تخلف خواهد شد.

تعلیق اعتبار همراه با دلیل و اقدامات لازم برای رفع آن توسط مرکز افتا به آزمایشگاه اطلاع داده می‌شود. آزمایشگاه پس از انجام اقدامات لازم آن را به مرکز افتا اطلاع داده و مرکز افتا با هماهنگی سازمان فناوری اطلاعات برای رفع تعلیق آن تصمیم گیری خواهد نمود.

آزمایشگاه در زمان تعلیق اعتبار حق انعقاد هیچ قرارداد جدیدی را نخواهد داشت.

آزمایشگاه موظف است پس از تعلیق اعتبار، بر حسب نظر مرکز افتا، قراردادهای جاری را مطابق با توافق‌نامه سطح خدمات به اتمام برساند و یا هزینه‌های انتقال این قرارداد به آزمایشگاه دارای گواهی و ضرر و زیان وارده به تولید کننده را متقبل شود.

۱۱,۲ روال لغو اعتبار

در صورتی که آزمایشگاه از انجام تعهدات قانونی و نیز مفاد مندرج در «تعهدنامه حفظ کیفیت و محرمانگی آزمایشگاه ارزیابی امنیتی» عدول نماید، مرکز افتا می‌تواند نسبت به لغو اعتبار، در هر مرحله اقدام نماید و آزمایشگاه کلیه حقوق قانونی، قضایی و دعاوی عینی، حقیقی، واقعی، فرضی، تصرفی، صنفی، تصوری و احتمالی را از خود سلب می‌نماید.

در صورت انحلال آزمایشگاه، اعتبار آن لغو خواهد شد. همچنین مرکز افتا می‌تواند در صورت تکرار تخلفی که قبلاً منجر به تعلیق اعتبار آزمایشگاه شده است، اعتبار آن آزمایشگاه را لغو نماید.

آزمایشگاه موظف است پس از لغو اعتبار، هزینه‌های انتقال قراردادهای جاری به یکی دیگر از آزمایشگاه‌های دارای گواهی و ضرر و زیان وارده به تولید کننده را تقبل نماید. چنانچه آزمایشگاه دیگری در آن حوزه وجود

نداشت یا مرکز افتا تشخیص داد که به هر دلیل امکان انتقال قراردادها وجود ندارد، آزمایشگاه موظف است طبق اعلام مرکز افتا عمل نماید.

۳ نظارت بر فعالیت آزمایشگاه

نظارت بر آزمایشگاه توسط مرکز افتا در دو بخش انجام می‌شود:

۱- نظارت بر اعتبار آزمایشگاه
۲- نظارت بر فعالیت آزمایشگاه در فرایند ارزیابی امنیتی محصولات

۱,۳ نظارت بر اعتبار آزمایشگاه

همانگونه که پیشتر شرح داده شد، آزمایشگاه جهت فعالیت در حوزه ارزیابی امنیتی می‌باید دارای شرایطی باشد تا موفق به دریافت گواهی از مرکز افتا و سازمان گردد. پس از دریافت گواهی فعالیت، مرکز افتا استمرار شرایط مذکور را در آزمایشگاه رصد می‌کند و در صورتیکه آزمایشگاه شرایط لازم که براساس آن اعتباربخشی شده است را از دست بدهد، اقدام مقتضی نظیر تذکر جهت رفع، عدم تمدید اعتبار، تعلیق اعتبار، لغو اعتبار و .... به عمل خواهد آورد.

۲,۳ نظارت بر آزمایشگاه در فرایند ارزیابی محصول

این نظارت، نظارت بر آزمایشگاه در فرایند ارزیابی امنیتی محصولات و پایش آن می‌باشد. پس از آنکه فرایند ارزیابی امنیتی محصول آغاز می‌شود، مرکز افتا بر فعالیت آزمایشگاه نظارت می‌کند. هدف از این نظارت آن است که اطمینان حاصل شود آزمایشگاه وظایف خود را به درستی انجام داده و به استانداردها، خط مشی‌ها، آیین نامه‌ها، مقررات، روالها و دستورالعمل‌های ابلاغی پایبند است. این نظارت در کل فرایند ارزیابی انجام می‌شود و ممکن است به صورت مرتب یا موردی باشد.

۴ الزامات مدیریتی برای اعتبار بخشی

ساختار و سازماندهی

آزمایشگاه باید خطمشی‌هایی برای ایفای بیطرفی آزمایشگاه و تمامیت ارزیابی‌های امنیتی محصولات فتا را ایجاد نماید.

تذکر: در ادامه این بخش در ابتدای هر الزام مدیریتی حرف <<م>> قرار گرفته که مخفف کلمه << الزامات مدیریتی>> است.

م۱,۱. آزمایشگاه و یا سازمانی که آزمایشگاه بخشی از آن است، باید یک نهاد حقوقی باشد.

م۱,۲. مسئولیت انجام آزمون، منطبق با الزامات این سند و با توجه به نیازهای مشتری، مقامات، و یا سازمان‌ها، بر عهده آزمایشگاه است.

م۱,۳. مدیریت آزمایشگاه باید امکان اجرای فعالیت‌ها را فراهم آورد.

م۱,۴. اگر آزمایشگاه بخشی از سازمانی باشد که فعالیت‌هایی غیر از آزمون انجام می‌دهد، مسئولیت پرسنل کلیدی سازمان که در انجام فعالیت‌های مربوط به آزمون دخیل هستند یا بر آنها تاثیرگذارند، باید به منظور شناسایی منافع متضاد و بالقوه، تعریف شوند.

نکته ۱: جایی که آزمایشگاه بخشی از یک سازمان بزرگتر است، آرایش سازمانی باید به گونه‌ای باشد که بخش‌های مختلفی که منافع متضاد دارند، مانند تولید، بازاریابی، تجاری یا مالی، تحت تاثیر انطباق آزمایشگاه با الزامات این سند، قرار نگیرند.

م۱,۵. آزمایشگاه باید دارای افراد باتوان مدیریتی و فنی متناسب با مسئولیت خود، باشد که بدون در نظر گرفتن دیگر مسئولیت‌هایشان، از منابع و اختیارات لازم برای انجام وظایف خود از جمله پیاده‌سازی، نگهداری و توسعه‌ی سیستم مدیریتی برخوردار باشند و همچنین امکان شناسایی انحرافات سیستم مدیریت و یا روش‌های اجرای آزمون را داشته و اقدامات اولیه برای جلوگیری و یا به حداقل رساندن انحرافات شناسایی شده را داشته باشند.

م۱,۶. آزمایشگاه باید دارای رویه‌های لازم برای تأمین امنیت اطلاعات و اطمینان یافتن از محافظت اطلاعات محرمانه و حقوق اختصاصی مشتریان خود باشد، همچون روش‌های حفاظت از ذخیره‌سازی الکترونیکی و انتقال نتایج.

م۷٫۱. آزمایشگاه باید دارای رویه‌های لازم برای جلوگیری از شرکت در فعالیت‌هایی که سبب کاهش اعتماد به صلاحیت، قضاوت و بی طرفی و صحت عملیات می‌گردد، باشد.

م۸٫۱. آزمایشگاه باید ساختار مدیریتی و سازمانی، وضعیت در سازمان مادر و ارتباط بین مدیریت کیفی، عملیات فنی و سرویس‌های پشتیبانی را تعریف کند.

م۹٫۱. آزمایشگاه باید اختیارات، مسئولیت‌ها و ارتباطات تمام کارمندانی را مشخص نمایند که «کارهایی انجام می‌دهند، مدیریت می‌کنند یا تائید می‌کنند» که بر روی کیفیت آزمون اثر گذار است.

م۱۰٫۱. آزمایشگاه باید بر کارکنان آزمون نظارت کافی داشته باشد. این نظارت باید توسط افراد متخصص در این امر و بر روی مواردی نظیر آموزش افراد، هدف هر آزمون و با بررسی نتایج آزمون صورت پذیرد.

م۱۱٫۱. آزمایشگاه باید دارای مدیر فنی‌ای باشد که مسئول تمامی فعالیت‌های فنی و همچنین تامین منابع لازم به منظور اطمینان از کیفیت مورد نیاز برای فعالیت‌های آزمایشگاهی است، برخوردار باشد.

م۱۲٫۱. آزمایشگاه باید یکی از کارمندان را به عنوان مدیر کیفی برگزیند که صرف نظر از مسئولیت‌ها و وظایف دیگر او، مسئول تضمین اجرا و پیگیری مداوم سیستم مدیریت کیفیت را داشته باشد. مدیریت کیفیت باید به بالاترین سطح مدیریتی که در آن، در مورد سیاست یا منابع آزمایشگاهی تصمیم‌گیری می‌شود، دسترسی مستقیم داشته باشد.

م۱۳٫۱. آزمایشگاه باید تضمین کند که کارکنان از ارتباط و اهمیت اقدامات خود که آنها را در دستیابی به اهداف سیستم مدیریتی کمک می‌کند، آگاه می‌باشند.

م۱۴٫۱. مدیر ارشد باید از مناسب بودن فرایندهای ارتباطی در داخل آزمایشگاه اطمینان حاصل نماید.

م۱۵٫۱. برای ارزیابی تحت نظر سند "طرح ارزیابی امنیتی" خطمشی‌های آزمایشگاه باید موارد زیر را تضمین کند:

الف: کارمندان آزمایشگاه نمی‌توانند همزمان یک پروفایل حفاظتی، هدف امنیتی و یا محصولی را توسعه و ارزیابی کنند.
ب: کارمندان آزمایشگاه نمی‌توانند همزمان خدمات مشاوره‌ای و ارزیابی در مورد یک پروفایل حفظتی، هدف امنیتی و یا محصولی را انجام دهند.

م۱۶,۱. آزمایشگاه باید کنترل‌های فیزیکی و الکترونیکی را با یک خطمشی صریح و روشن و مجموعه‌ای از رویه-ها افزایش دهد تا هر دو بخش فیزیکی و الکترونیکی بین ارزیاب‌های آزمایشگاه با مشاوران آزمایشگاه، توسعه-دهندگان محصول و بقیه‌ی افرادی که سودی در آن دارند جدا نگه داشته شود.

م۱۷,۱. سیستم مدیریتی باید حاوی خطمشی‌هایی برای تضمین حفاظت از داده‌های حساس باشد. این خطمشی‌ها باید بیان کند که چگونه این داده‌های حساس در مقابل افرادی که خارج آزمایشگاه می‌باشند و همچنین کارمندانی که رابطه‌ای با آن‌ها ندارند، محافظت می‌شود.

۱,۴ سیستم مدیریتی

آزمایشگاه باید سیستم مدیریتی را بکار گیرد که به صورت کامل رویه‌ها و گام‌های لازم برای تضمین کیفیت ارزیابی در آن تدوین شده باشد.

م۱,۲. آزمایشگاه باید سیستم مدیریتی مناسبی با توجه به حوزه فعالیت خود ایجاد، پیاده‌سازی و نگهداری کند.

م۲,۲. آزمایشگاه باید سیاست‌ها، سیستم‌ها، برنامه‌ها، روش‌ها و دستورالعمل‌های لازم را برای تضمین کیفیت نتایج آزمون، مستند نماید، به گونه‌ای که قابل استفاده، قابل فهم و قابل دسترسی باشند.

م۳,۲. خطمشی‌های مربوط به کیفیتِ سیستم مدیریت آزمایشگاه، از جمله «بیانیه خط‌مشی کیفیت»، باید در سند نظامنامه کیفیت تعریف شوند. اهداف کلی آزمایشگاه باید مشخص شوند و در حین بازنگری مدیریتی، بازنگری شوند.

م۴,۲. «بیانیه خط‌مشی کیفیت» باید توسط مدیریت ارشد صادر شود و حداقل شامل موارد زیر باشد:

الف) تعهد مدیریت آزمایشگاه به عملکرد خوب و حرفه‌ای، و با کیفیت بودن آزمون درجهت سرویس‌دهی به مشتریان

ب) بیانیه مدیریت برای استاندارد سرویس‌های آزمایشگاه

ج) هدف از سیستم مدیریت کیفیت

د) تمام پرسنل آزمایشگاه که با فعالیت‌های آزمون مرتبط هستند، باید با مستندات کیفیت و پیاده‌سازی سیاست‌ها و روش‌های کار خود، آشنا باشند.

ه) تعهد مدیریت آزمایشگاه به پیروی از الزامات سند کیفیت و بهبود کارایی سیستم مدیریت، به طور مستمر.

«بیانیه خط‌مشی کیفیت» باید مختصر بوده، وشامل الزاماتی باشد که آزمون‌ها باید همواره مطابق با الزامات مشتری و روش‌های معین انجام شوند. زمانی که آزمون در بخشی از یک سازمان بزرگتر انجام می‌شود، ممکن است برخی از عناصر «بیانیه خطمشی‌کیفیت» در دیگر اسناد سازمان موجود باشد.

م۵,۲. مدیر ارشد باید مدارک تعهد به توسعه و پیاده‌سازی سیستم مدیریت و بهبود کارایی مستمر آن را ارائه دهد.

م۶,۲. مدیر ارشد باید بین سازماندهی اهم الزامات مقتضی مشتری و نیز الزامات نظارتی و قانونی ارتباط برقرار نماید.

م۷,۲. «سند نظامنامه کیفیت» باید شامل پشتیبانی از روال‌ها از جمله روش‌های فنی باشد یا به آنها ارجاع دهد. این سند باید ساختار مستندات مورد استفاده در سیستم مدیریتی را طرح ریزی نماید.

م۸,۲. نقش‌ها و مسئولیت‌های مدیریت فنی و مدیر کیفیت به انضمام مسئولیت‌هایی که در این سند برای آنها مشخص شده است، باید در «سند نظامنامه کیفیت» مشخص شود.

م۹,۲. مدیریت ارشد باید نگهداری از یکپارچگی سیستم را در زمان برنامه‌ریزی و اجرای تغییرات سیستم مدیریتی، تضمین نماید.

م۱۰,۲. الزامات سیستم مدیریتی برای ترویج روش‌های آزمایشگاهی طراحی می‌شوند تا از صحت و یکپارچگی فنی ارزیابی امنیتی و پایبندی به شیوه‌های تضمین کیفیت که برای آزمون‌های امنیت مناسب هستند، اطمینان حاصل نمایند. آزمایشگاه باید برای حصول اطمینان از کیفیت ارزیابی‌های امنیت فناوری اطلاعات، از مستندات سیستم مدیریتی که شامل خطمشی‌ها، اقدامات و مراحل خاصی که از کیفیت ارزیابی امنیت اطمینان حاصل می‌کند، محافظت نماید.

م۱۱,۲. اسناد، استانداردها و نشریات که در بخش مراجع به آنها اشاره شده است، باید برای استفاده کاربران آزمایشگاه که در حال توسعه و نگهداری سیستم مدیریت و انجام ارزیابی هستند، در دسترس باشد، همچنین باید تمام اقدامات سیستم مدیریت ثبت گردد.

م۱۲,۲. هر آزمایشگاه متقاضی و معتبر باید روال‌ها را تدوین و اجرا نماید.

م۱۳,۲. مدیر آزمایشگاه باید نسبت به فراهم آوردن امکانات لازم جهت آموزش و ارتقاء توان فنی تخصصی کارکنان آزمایشگاه متعهد باشد.

۲,۴ کنترل اسناد

۱,۲,۴ کلیات

م۱,۳. آزمایشگاه باید روال‌هایی را برای کنترل تمام اسنادی که بخشی از سیستم مدیریت نظیر مقررات، استانداردها، مدارک و اسناد اصولی دیگر، آزمون و نیز نقشه‌ها، نرم‌افزارها، مشخصات، دستورالعمل‌ها و کتابچه‌های راهنما هستند، تهیه و نگهداری نماید.

نکته ۱: متن "سند" می‌تواند شامل شرحی از سیاست‌ها، روال‌ها، مشخصات، نمودارها، کتاب‌های مرجع، پوستر، اعلامیه‌ها، یادداشت‌ها، نرم‌افزار، نقشه‌ها، طرح‌ها و غیره باشد. این موضوع ممکن است در رسانه‌های مختلف به‌صورت نتیجه‌ی چاپی یا الکترونیکی و یا دیجیتالی، آنالوگ یا به‌صورت عکس نوشته باشد.

۲,۲,۴ تصویب و انتشار سند

م۱,۲,۳. تمام اسنادی که برای کارکنان آزمایشگاه منتشر شده، باید پیش از انتشار جهت استفاده کارکنان، توسط مدیریت، بازنگری و تصویب شوند. در سیستم مدیریت، باید یک لیست اصلی یا یک روال کنترل سند معادل، وضعیت بازبینی نسخه فعلی را مشخص نموده، همچنین اسناد در سیستم مدیریت باید توزیع گردد و آماده دسترسی باشند تا مانع استفاده از اسناد نامعتبر و یا اسناد منسوخ شود.

م۲,۲,۳. روال‌های پذیرفته شده باید تضمین نمایند که:

الف) نسخه‌ی مجاز اسناد مربوطه در کلیه‌ی مکان‌های مورد نیاز آزمایشگاه، در دسترس است.

ب) اسناد به‌صورت دوره‌ای بازنگری می‌شوند و در صورت لزوم برای تضمین تداوم تناسب و انطباق با الزامات قابل اجرا، مورد تجدید نظر قرار می‌گیرند.

ج) اسناد نامعتبر یا منسوخ، فوراً از تمام نقاط صدور یا استفاده حذف می‌شوند و یا درمقابل استفاده‌ی غیرعمدی محفوظ می‌مانند.

د) اسناد غیر متداولی که برای مقاصد قانونی نگهداری می‌شوند به نحو مناسبی مشخص شوند.

م۳,۲,۳. اسناد مدیریتی تولیدشده توسط آزمایشگاه، باید منحصر به فرد بوده و شامل موارد زیر باشند:

الف) تاریخ صدور یا تجدید نظر در شناسایی

ب) شماره صفحه

ج) تعداد کل صفحات یا علامتی برای مشخص کردن پایان سند

د) مقام صادر کننده سند

م۴,۲,۳. آزمایشگاه باید تعهد محضری در دفتر ثبت اسناد رسمی دهد که گزارشات و نتایج ارزیابی امنیتی را صرفاً به تولید کننده و مرکز افتا ارائه داده و در حفظ و نگهداری آن نهایت سعی و تلاش خود را انجام می‌دهد.

۳,۲,۴ تغییرات اسناد

م۱,۳,۳. تغییرات اسناد باید همانند قالبی که براساس آن بازنگری اولیه صورت گرفته است، بازنگری و تصویب گردد مگر آنکه به طور خاص قالب دیگری تعیین شده باشد. افراد تعیین شده بدین منظور باید به اطلاعات زمینه که براساس آن باید بازبینی و تصویب صورت گیرند، دسترسی داشته باشند.

م۲,۳,۳. در مواردی که متنی جدید است یا متنی تغییر می‌یابد، باید در اسناد یا فایل پیوست مربوطه مشخص شود.

م۳,۳,۳. اگر سیستم کنترل اسناد آزمایشگاه تا زمان چاپ مجدد اسناد، اجازه تصحیح اسناد موجود را بدهند، باید روال‌ها و مجوز انجام این اصلاحات، تعریف شود.

م۴،۳،۳. اصلاحات باید به وضوح، مشخص، پاراگراف‌بندی و تاریخ‌گذاری شوند. سند تجدید نظر شده باید به‌طور رسمی و در اسرع وقت چاپ مجدد شود.

م۵،۳،۳. روال‌های توصیف چگونگی اجرا و کنترل تغییرات در اسنادی که در سیستم‌های کامپیوتری نگهداری می‌شوند، باید تهیه شود.

۳،۴ بازنگری درخواست‌ها، مناقصات و قراردادها

م۱،۴. آزمایشگاه‌ها باید رویه‌هایی برای بازنگری درخواست‌ها، پیشنهادها و عقد قراردادها در نظر بگیرد. خطمشی‌ها و رویه‌ها که برای بازنگری‌هایی منجر به عقد قرارداد انجام آزمون اتخاذ می‌شود، باید اطمینان بدهند که:

الف) الزاماتی که روش‌های استفاده شده را در بر می‌گیرند، باید بطور مناسب تعریف و مستندسازی شده همچنین قابل فهم باشند.

ب) آزمایشگاه باید دارای قابلیت‌ها و منابع کافی برای اجرای الزامات باشد.

ج) شیوه‌های مناسب آزمون انتخاب می‌شوند و قادر به برآورده ساختن نیازهای مشتریان هستند.

تذکر: باید توانایی‌های آزمایشگاه مورد بازنگری قرار گیرد تا آزمایشگاه از نظر الزامات فیزیکی، پرسنل و منابع اطلاعاتی واجد شرایط باشد و پرسنل آزمایشگاه دارای مهارت‌ها و تجربه لازم برای آزمون باشند. همچنین بازنگری ممکن است دربرگیرنده «نتایج مشارکت‌های قبلی در مقایسه بین-آزمایشگاهی» یا «مهارت آزمون کردن» و/یا «اجرای برنامه‌های آزمون با استفاده از نمونه‌ها» یا «نمونه‌های مقادیر مشخص به منظور تعریف تردیدهای اندازه‌گیری»، «محدودیت‌های تشخیص»، «محدودیت‌های اطمینان» و غیره باشد.

م۲،۴. نتایج بدست آمده از بازنگری‌ها، به همراه هرگونه تغییر قابل توجه دیگری، باید نگهداری شوند. همچنین رکوردهای مرتبط با مشتری و یا نتایج حاصل از کار در طول زمان اجرای قرارداد باید نگهداری شوند.

نکته: به منظور بررسی مناسب رویه‌های عادی و کارهای ساده دیگر، تاریخ و شناسه شخصی که در آزمایشگاه مسئول انجام امور آن قرارداد است، ثبت می‌شود. در رویه‌های عادی که همواره تکرار می‌شوند، به شرطی که نیازهای مشتری تغییر نکند، تنها در مرحله پرس‌وجوهای اولیه، یا در هنگام تنظیم قرارداد و با یک توافق کلی با مشتری، بازنگری انجام می‌شود. برای کارهای جدید، آزمون پیشرفته یا پیچیده، رکوردهای بیشتری باید نگهداری شوند.

م۳,۴. بازنگری باید زیرقرارداد[۲] را نیز، پوشش دهد.

م۴,۴. مشتری باید از هرگونه انحراف از قرارداد مطلع شود.

م۵,۴. اگر یک قرارداد بعد از انجام کار، احتیاج به اصلاح داشت، باید فرایند مشابهی برای بررسی قرارداد تکرار شود و هرگونه اصلاحات باید به تمام پرسنل مربوطه انتقال یابد.

م۶,۴. رویه‌هایی که به‌منظور تنظیم مجدد قراردادها در نظر گرفته شده باید برای حصول اطمینان از اینکه آزمایشگاه، پرسنل و منابع، با برنامه ارزیابی مطابقت کامل دارد، روش‌هایی داشته باشد.

۴,۴ خرید خدمات و ملزومات

م۱,۵. آزمایشگاه باید خطمشی و رویه(هایی) برای انتخاب و تامین سرویس‌ها و تدارکات داشته باشد، و از آن‌ها در جهت کیفیت بخشیدن به انجام آزمون استفاده کند. به منظور خرید، ثبت و ذخیره تجهیزات و مواد مصرفی آزمایشگاه برای آزمون باید رویه‌هایی وجود داشته باشد.

م۲,۵. آزمایشگاه باید تضمین نماید که تجهیزات خریداری شده و مواد مصرفی آزمایشگاهی که بر کیفیت آزمون تاثیر گذار هستند، تا زمانی که بازرسی نشوند و با مشخصات استاندارد تعریف شده در روش‌های اجرای آزمون

[2] subcontract

مطابقت داده نشده‌اند، استفاده نخواهند شد. سرویس‌ها و تدارکات مورد استفاده باید از الزامات مشخصی پیروی کنند.

م۳,۵. مستندات مربوط به بررسی میزان تطابق، باید نگهداری شوند.

م۴,۵. آزمایشگاه باید تامین‌کنندگان مواد مصرفی حیاتی، لوازم و خدماتی که بر کیفیت آزمون تاثیر می‌گذارند را ارزیابی نماید.

م۵,۵. باید سوابق ارزیابی و لیست کسانی که مورد تایید هستند، نگهداری شود.

۵,۴ ارائه خدمت به مشتری

م۱,۶. آزمایشگاه باید دارای یک خطمشی و رویه‌ی مشخص، برای حل و فصل شکایات رسیده از مشتریان یا دیگر قسمت‌ها باشد.

م۲,۶. رکوردها باید تمام شکایات و تحقیقات و اقدامات اصلاحی انجام گرفته توسط آزمایشگاه را نگهداری نمایند.

۶,۴ کنترل عدم انطباق[۳] آزمون

م۱,۷. آزمایشگاه باید در مواقعی که بخشی از آزمون، یا نتایج کار، با دستورالعمل‌های آزمایشگاه یا الزامات مورد توافق با مشتری، مطابقت نداشته باشد، خطمشی و رویه‌هایی که بدین منظور در نظر گرفته را تحت نظارت مرکز افتا اجرا نماید. این خطمشی و رویه‌ها باید اطمینان بدهند که:

الف) مسئولیت‌ها و اختیارات مدیریت برای موارد بروز عدم انطباق که از سوی مرکز افتا ابلاغ شده است، در نظر گرفته شده و اقداماتی (از جمله متوقف کردن کار و خودداری از گزارش آزمون) برای آن تعریف شده، که در زمان مواجه با این شرایط، اجرا شود.

[3] nonconforming

ب)انجام ارزیابی از عدم انطباق‌ها

نکته: شناسایی عدم انطباق رخ داده یا مشکلات می‌تواند در رابطه با سیستم مدیریت یا با فعالیت‌های آزمـون در مکان‌های مختلفی اتفاق بیافتد. به عنوان نمونه می‌توان به شکایات مشتری، کنترل کیفیت، کالیبراسیون ابزاری، بررسی مواد مصرفی، مشاهدات یا نظارت کارکنان، بررسی گزارش آزمون، بررسی مدیریت و ممیزی‌های داخلی و خارجی اشاره کرد.

۷,۴ بهبود

م۱,۸. آزمایشگاه باید به طور مداوم، کارایی سیستم مدیریت را از طریق استفاده از خط‌مشی کیفیت، اهداف کیفیت، نتایج ممیزی، تجزیه و تحلیل داده‌ها، «اقدامات اصلاحی» و «اقدامات پیشگیرانه» و بررسی مجدد مدیریت بهبود ببخشد.

۸,۴ اقدامات اصلاحی

۱,۸,۴ کلیات

م۱,۹. آزمایشگاه باید زمانیکه در سیستم مدیریت یا عملکرد فنی، کار نامنطبقی صورت می‌گیرد یا از خط‌مشی و رویه‌ها تخطی می‌گردد، خط‌مشی و رویه‌ای را در نظر بگیرد و افراد شایسته‌ای را برای انجام اقدامات اصلاحی برگزینند.

نکته: اگر مشکلی در سیستم مدیریت یا در عملکرد فنی آزمایشگاه وجود داشته باشد، ممکن است با انجام فعالیت‌های مختلفی، مانند کنترل کار نامنطبق، ممیزی‌های داخلی و خارجی، بازنگری مدیریت، بازخورد از مشتریان و از مشاهدات کارکنان، شناسایی شود.

۲,۸,۴ تجزیه و تحلیل علت

م۲,۹. رویه‌ی اقدامِ اصلاحی باید با تحقیق برای مشخص کردن علت(های) اصلی مشکل شروع شود.

نکته: تجزیه و تحلیل علت، گاهی اوقات سخت‌ترین بخش در رویه‌ی اقدام اصلاحی است. اغلب، علت اصلی مشخص نیست، بنابراین یک تجزیه و تحلیل دقیق از تمام علت‌های بالقوه مربوط به مشکل، مورد نیاز است. علت‌های بالقوه می‌توانند شامل الزامات مشتری، مشخصات نمونه‌ها، روش‌ها و رویه‌ها، مهارت‌ها و آموزش کارکنان، مواد مصرفی، و یا تجهیزات و کالیبراسیون آن باشند.

۳,۸,۴ انتخاب و پیاده‌سازی اقدامات اصلاحی

م۳,۹. در مواقع نیاز به اقدامات اصلاحی، آزمایشگاه باید اقدامات اصلاحی بالقوه را شناسایی نماید. همچنین باید اقداماتی که بیشترین احتمال از بین بردن این مشکل را دارند و از تکرار آن جلوگیری می‌کنند، نیز انتخاب و پیاده‌سازی شوند.

م۴,۹. اقدامات اصلاحی باید متناسب با اندازه و خطر ناشی از مشکل به وجود آمده، انجام شوند.

م۵,۹. آزمایشگاه باید هرگونه تغییرات مورد نیاز ناشی از تحقیقات اقدامات اصلاحی را مستند و اجرا کند.

۴,۸,۴ پایش اقدامات اصلاحی

م۶,۹. آزمایشگاه باید نظارتی بر روی نتایج به دست آمده داشته باشد تا از مؤثر بودن اقدامات اصلاحی، اطمینان حاصل کند.

۵,۸,۴ ممیزی‌های اضافی

م۷,۹. در زمان شناسایی عدم‌تطابق‌ها یا انحرافات، در صورتی که در انطباق آزمایشگاه با خطمشی‌ها و رویه‌های خود یا در انطباق با این سند راهنما تردید وجود داشته باشد، آزمایشگاه باید از ممیزی بعضی از فعالیت‌ها، در اسرع وقت اطمینان حاصل نماید.

نکته: ممیزی‌های اضافی اغلب اجرای اقدامات اصلاحی را برای تائید اثر خود دنبال می‌کنند. یک ممیزی اضافی تنها در زمانی ضرورت دارد که یک مسئله یا خطر جدی در کسب و کار، شناسایی شده باشد.

۹,۴ اقدام پیشگیرانه

«اقدامات پیشگیرانه»، فرایندی فعال برای شناسایی فرصت‌های بهبود به‌جای واکنش به شناسایی مشکلات یا شکایات است.

م۱,۱۰. بهبودهای مورد نیاز و منابع بالقوه عدم انطباق‌ها، چه فنی باشد و چه در رابطه با سیستم مدیریت، باید شناسایی شوند.

م۲,۱۰. زمانی‌که فرصت‌های بهبود شناسایی می‌شوند یا اقدامات پیشگیرانه‌ای مورد نیاز است، باید برنامه‌های عملیاتی توسعه، پیاده‌سازی و نظارت گردند تا احتمال وقوع چنین عدم انطباق‌هایی کاهش داده شود و از فرصت‌های بهبود استفاده شود.

م۳,۱۰. خطمشی‌های مربوط به «اقدامات پیشگیرانه» شامل شروع چنین اقداماتی و برنامه های کنترلی می‌باشد تا از موثر بودن آنها اطمینان حاصل گردد.

۱۰,۴ کنترل رکوردها

آزمایشگاه باید سیستم نگهداری رکورد را برای دنبال کردن هر ارزیابی امنیتی فراهم کند. رکوردها باید به آسانی در دسترس باشند و حاوی اطلاعات کافی برای هر ارزیابی باشند. رکوردهای مورد نیاز فعالیت‌های ارزیابی باید مطابق با فعالیت‌های ارزیابی «استاندارد ارزیابی معیار مشترک و سایر استانداردها و دستورالعمل‌های ابلاغی» و «متدلوژی ارزیابی معیار مشترک» باشد رکوردهای مبتنی بر کامپیوتر باید شامل مدخلی باشد که نشان دهنده‌ی تاریخ تولید و مشخصات شخصی که به روی آن عملیاتی انجام داده است باشد. تمام رکوردها باید مطابق خطمشی‌ها و روال‌ها نگهداری شوند به گونه‌ای که صحت رکوردها حفظ گردد. همچنین باید نسخه پشتیبانی از آنها تهیه و آرشیو گردد.

در رکوردها باید به قدر کافی شواهد ارزیابی وجود داشته باشد، به گونه‌ای که ناظر آزمایشگاه (مرکز افتا) بتواند براساس این شواهد، سازگاری کارهایی که برای هر واحد کاری انجام گرفته با حکم صادره را تشخیص دهد. رکوردها شامل یادداشت‌های ارزیاب، رکوردهای مربوط به محصول، رکوردهای واحد کاری و رکوردهای مشتری می‌باشد.

«مرکز افتا» آزمایشگاه‌ها را ملزم به حفظ رکوردها حداقل برای پنج سال می‌نماید. براساس این الزام، رکوردهای آزمایشگاه باید براساس خط مشی آزمایشگاه و توافقی که با مشتری داشته است، نگهداری، منتشر یا منهدم گردد.

۱,۱۰,۴ کلیات

م۱,۱۱. آزمایشگاه باید خطمشی‌هایی برای شناسایی، جمع آوری، دسترسی، نمایه‌سازی، بایگانی، نگهداری، ذخیره و انهدام رکوردهای فنی و کیفی ایجاد و نگهداری نماید. رکوردهای کیفی باید دربرگیرنده‌ی گزارشاتی از ممیزی داخلی و بازنگری مدیریتی و همچنین «اقدامات اصلاحی» و «اقدامات پیشگیرانه» باشد. لازم به ذکر است که رکوردها باید امن و قابل اطمینان باشند.

م۲,۱۱. تمام رکوردها باید خوانا باشند و باید به‌گونه‌ای ذخیره و نگهداری شوند که بازیافت آنها با امکاناتی که یک محیط مناسب برای جلوگیری از آسیب، نابودی و از دست رفتن فراهم می‌کند، به‌راحتی ممکن باشد.

م۳,۱۱. زمان حفظ و نگهداری رکوردها باید مشخص شود.

م۴,۱۱. تمام رکوردها باید به‌صورت امن و مطمئن نگهداری شوند.

م۵,۱۱. آزمایشگاه باید رویه‌هایی را برای حفاظت و پشتیبان‌گیری از رکوردهای ذخیره شده به‌صورت الکترونیکی و نیز جلوگیری از دسترسی غیرمجاز و یا تصحیح این رکوردها، داشته باشد.

م۶,۱۱. آزمایشگاه باید یک سیستم نگهداری از رکوردهای عملکردی را که برای ردیابی هر ارزیابی امنیتی استفاده می‌شود، نگهداری کند. رکوردها باید به راحتی در دسترس افراد مجاز قرار گرفته و شامل اطلاعات کامل برای هر ارزیابی باشند.

م۷,۱۱. رکوردها باید قابلیت ردیابی را برای ارزیاب فراهم نموده و منطبق با «متدولوژی ارزیابی معیار مشترک» باشند.

م۸,۱۱. رکوردهای الکترونیکی، علاوه بر هرگونه اطلاعات مورد نیاز توسط سیستم مدیریت، باید شامل تاریخ ایجاد و افرادی که کار را انجام داده‌اند، باشند.

م۹,۱۱. مطالب موجود در دفترچه‌های آزمایشگاه باید دارای تاریخ و امضا یا پاراف باشند.

م۱۰,۱۱. تمام رکوردها باید با توجه به خطمشی‌ها و رویه‌های آزمایشگاه و به روشی که یکپارچگی رکوردها تضمین شوند، نگهداری شوند.

م۱۱,۱۱. برای رکوردها باید نسخه‌های پشتیبانی تهیه و بایگانی شوند.

۲,۱۰,۴ رکوردهای فنی

م۱۲,۱۱. آزمایشگاه باید برای یک دوره‌ی تعریف شده رکوردهای زیر را نگهداری نماید:

- رکوردهای مربوط به مشاهدات اولیه
- داده‌های حاصل شده و اطلاعات کافی برای ایجاد دنباله‌ی ممیزی
- رکوردهای کارکنان
- یک رونوشت از تمام گزارش‌های آزمون

م۱۳,۱۱. رکوردهای هر آزمون باید دربرگیرنده‌ی اطلاعات کافی باشند تا شناسایی عوامل موثر بر عدم قطعیت و همچنین فعال‌سازی آزمون ی که تا حد امکان تحت شرایطی نزدیک به نسخه‌ی اصلی تکرار شده است، تسهیل گردد.

م۱۴,۱۱. رکوردها باید شامل هویت کارکنانی باشد که مسئول نمونه‌برداری، کارایی هر آزمون و بررسی نتایج می‌باشند. رکوردهای فنی، مجموعه‌ای از داده‌ها و اطلاعات حاصل از انجام آزمون هستند که نشان می‌دهند آیا کیفیت تعیین شده یا پارامترهای فرایند، حاصل شده است. رکوردها ممکن است شامل فرم‌ها، قراردادها،

برگ‌های کاری، سندهای دستور کار، برگ‌های ثبت داده، یادداشت‌های کاری، نمودارهای کنترل، گزارشات آزمون داخلی یا خارجی، یادداشت‌های مشتریان، مقالات و بازخوردها باشند.

م۱۵,۱۱. مشاهدات، داده‌ها و محاسبات باید زمانی که صورت می‌گیرند و ایجاد می‌شوند، ثبت و باید به وظایف خاص قابل شناسایی باشند.

م۱۶,۱۱. زمانیکه خطایی در رکوردها صورت می‌گیرد، خطا نباید پاک، مخدوش و یا حذف شود بلکه باید خط زده شود و مقدار صحیح در کنار آن نوشته شود. تمام این تغییرات در رکوردها باید توسط شخصی که اقدامات اصلاحی را انجام می‌دهد، امضا یا پاراف شوند.

م۱۷,۱۱. در حالتی که رکوردها به‌صورت الکترونیکی ذخیره می‌شوند، باید اقدامات معادل آن برای جلوگیری در برابر از دست دادن داده های اصلی و یا تغییر در آنها، انجام شود.

م۱۸,۱۱. شواهد ارزیابی باید به اندازه کافی در رکوردهای یک گروه مستقل موجود باشند. رکوردها شامل دفترچه‌های ارزیابی، رکوردهای مربوط به محصول، رکوردهای سطح واحد کاری و رکوردهای بخش مشتری می‌باشند.

م۱۹,۱۱. رکوردهای آزمایشگاه باید برای یک دوره حداقل پنج ساله نگهداری شوند. علاوه بر این الزام، رکوردهای آزمایشگاه باید با توجه به خطمشی آزمایشگاه برای اطلاعات اختصاصی و موافقت‌نامه‌های قراردادی با مشتریان، نگهداری و منتشر شوند، یا از بین بروند.

م۲۰,۱۱. رکوردهای زیر باید موجود باشد:

الف) تمام فعالیت‌های سیستم کیفیت

ب) تاریخ آموزش کارکنان و بازبینی صلاحیت

ث) تمام ممیزی‌ها و بازبینی‌های مدیریتی

ت) ایجاد و تغییر رویه‌های ارزیابی و متدولوژی

د) قبول یا رد محصول مورد ارزیابی

ذ) ردیابی کامل نسخه‌های چندگانهٔ شواهد ارزیابی و گزارشات فنی ارزیابی

ر) ردیابی کامل اقدامات ارزیابی در سطح واحد کاری که شامل آنالیز اولیه، مقررات و هرگونه تغییرات بعدی در آن دسته از مقررات، می‌شود

ز) کد اصلی، کد دو دویی قابل اجرا، داده‌ها و اطلاعات پیکربندی کافی برای تولید مجدد هر آزمون انجام شده در طول ارزیابی (این موضوع شامل کد اصلی و کد دو دویی قابل اجرا، هم برای هدف ارزیابی و هم برای ابزار آزمون (در صورت دسترسی)، همراه با داده‌های آزمون و اطلاعات و یا فایل‌های پیکربندی، می‌شود)

س) اطلاعات پیکربندی تمام تجهیزات آزمون استفاده شده در حین ارزیابی به همراه تحلیل تجهیزات برای تائید مناسب بودن تجهیزات آزمون برای انجام آزمونی مطلوب.

۱۱,۴ ممیزی‌های داخلی

م۱,۱۲. آزمایشگاه باید به‌صورت دوره‌ای و مطابق با برنامه‌ی زمانی و رویه‌های از قبل تعیین شده، نسبت به فعالیت‌های خود ممیزی داخلی انجام دهد، تا تداوم عملکرد خود مطابق با الزامات سیستم مدیریتی و این سند راهنما را بررسی نماید. برنامه‌ی ممیزی داخلی باید تمام اجزای سیستم مدیریتی، ازجمله فعالیت‌های آزمون را دربرگیرد. مسئولیت برنامه‌ریزی و سازماندهی ممیزی بر عهده‌ی «مدیر کیفی» است و مسئولیت ممیزی نیز با «مدیر کیفی» است، تا برای نیازمندی‌هایی که توسط مدیریت درخواست شده، برنامه‌ریزی و سازماندهی نماید. چرخه ممیزی داخلی باید به طور معمول در یکسال تکمیل گردد. همچنین رونوشتی از برنامه‌ی زمانی ممیزی داخلی باید برای ارزیاب، پیوست شود.

م۲,۱۲. ممیزی‌ها باید توسط کارکنان آموزش دیده و واجد شرایط انجام شود. چرخه‌ی انجام ممیزی داخلی باید به‌صورت معمول، در طول یک سال کامل شود.

م۳,۱۲. هنگامی که یافته‌های ممیزی در مورد کارایی عملکرد یا صحت یا اعتبار نتایج آزمون آزمایشگاه شبهاتی مطرح می‌نماید، آزمایشگاه باید به‌موقع «اقدامات اصلاحی» را انجام دهد و در صورتی‌که تحقیقات نشان دهد که نتایج آزمایشگاه ممکن است تحت تاثیر قرار گرفته باشد، این مسئله باید به صورت مکتوب به اطلاع مشتریان رسیده شود.

م۴,۱۲. زمینه فعالیت‌های ممیزی، یافته‌های ممیزی و اقدامات اصلاحی که از آنها ناشی می‌شوند، باید ثبت شوند.

م۵,۱۲. فعالیت‌های ممیزی بعدی باید پیاده‌سازی و کارایی اقدامات اصلاحی انجام شده را، بازبینی و ثبت نماید.

م۶,۱۲. ممیزی داخلی باید سیستم مدیریت آزمایشگاه و برنامه سیستم مدیریت را برای تمام اقدامات آزمایشگاه تحت پوشش قرار دهد. ممیزی باید مطابق با الزامات مرکز افتا و الزامات سیستم مدیریت آزمایشگاه پوشش داده شود. ممیزی باید تمام جنبه‌های اقدامات ارزیابی را از جمله کارهایی را که در راستایی ارزیابی صورت گرفته را پوشش دهد.

م۷,۱۲. در مواردیکه تنها یک نفر از کارمندان آزمایشگاه برای انجام بخش خاصی از روش آزمون و انجام ممیزی آن دارای صلاحیت باشد، این مسئله منجر به ممیزی خود فرد از کارش می‌گردد، در این موارد ممیزی ممکن است توسط دیگر افراد آزمایشگاه صورت گیرد. روش آزمون باید براساس «متدلوژی ارزیابی معیار مشترک» مورد ارزیابی قرار گیرد و باید رویه‌ها و دستورالعمل‌های مستند شده را بازبینی و از آنها تبعیت نموده، همچنین گزارشات ممیزی قبلی را نیز بررسی نماید. در این شرایط ممکن است از کارشناسان ماهر خارج از آزمایشگاه پس از تأیید مرکز افتا استفاده گردد.

م۸,۱۲. تازه‌ترین گزارش‌های ممیزی داخلی باید در طول «ارزیابی در محل» آزمایشگاه برای بازبینی در دسترس قرار گیرند.

م۹،۱۲. آزمایشگاه باید پیش از اولین «ارزیابی کامل در محل» حداقل یک ممیزی داخلی را به صورت کامل انجام دهد.

م۱۰،۱۲. باید پیش از «ارزیابی اولیه در محل» مختصر ممیزی داخلی صورت گیرد.

م۱۱،۱۲. رکوردها پیش از یا در طول «بررسی ارزیابی در محل» بازبینی خواهند شد.

م۱۲،۱۲. انجام آزمون و ممیزی آن باید توسط دو گروه متفاوت انجام شود. ممیزی باید بر اساس متدلوژی مشخص و مستند شده باشد. ممیزی داخلی باید قبل از ارزیابی کامل در محل انجام گیرد.

۱۲،۴ بازنگری‌های مدیریت

م۱،۱۳. مدیریت ارشد آزمایشگاه باید به‌صورت دوره‌ای و مطابق با برنامه‌ی زمانی و خطمشی‌های از قبل تعیین شده، بازنگری‌هایی از سیستم مدیریت آزمایشگاه و فعالیت‌های آزمون انجام دهد، تا از کارایی مستمر آن اطمینان حاصل نماید و تغییرات یا اصلاحیه‌های لازم را مطرح نماید.

م۲،۱۳. بازنگری باید مدیریت باید شامل:

۱) مناسب بودن خطمشی‌ها و روال‌ها
۲) گزارشاتی از مدیران و سرپرست‌ها
۳) خروجی تازه‌ترین ممیزی داخلی
۴) «اقدامات اصلاحی» و «اقدامات پیشگیرانه»
۵) ارزیابی توسط نهادهای خارجی
۶) نتایج مقایسه‌ی داخل آزمایشگاه یا «آزمون تخصصی»
۷) تغییر در حجم و نوع کارها
۸) بازخورد مشتری

۹) شکایات

۱۰) پیشنهادات

۱۱) سایر عوامل مربوطه از جمله فعالیت‌های کنترل کیفیت، منابع و آموزش کارکنان

نکته ۱: بازنگری مدیریت معمولا یک بار در سال انجام می‌شود.

نکته ۲: نتایج باید به سیستم برنامه‌ریزی آزمایشگاه بازخورد، داده شود و باید شامل اهداف، برنامه‌های عملیاتی و عینی برای سال آینده باشد.

نکته ۳: بازنگری مدیریت شامل ملاحظاتِ مربوط به موضوعات جلسات منظم مدیریتی است.

م۳،۱۳. یافته‌های مربوط به بازنگری مدیریت و اقدامات ناشی از آنها، باید ثبت شود.

م۴،۱۳. مدیریت باید تضمین نماید که اقدامات در یک مقیاس زمانی مورد توافق و مناسب انجام شده است.

م۵،۱۳. تازه‌ترین گزارش‌های بازنگری مدیریت باید در طول «ارزیابی در محل» آزمایشگاه برای بازبینی در دسترس قرار گیرند.

م۶،۱۳. آزمایشگاه باید پیش از اولین «ارزیابی کامل در محل» حداقل یک بازنگری مدیریت را به صورت کامل انجام دهد.

م۷،۱۳. باید پیش از «ارزیابی اولیه در محل» بازنگری مدیریت صورت گیرد.

م۸،۱۳. رکوردها پیش از یا در طول «بررسی ارزیابی در محل» بازبینی خواهند شد.

۵ الزامات فنی برای اعتباربخشی آزمایشگاه

۱,۵ کلیات

عوامل زیادی در صحت و قابلیت اطمینان عملیات آزمون آزمایشگاه موثر می‌باشد مانند:

۱- عوامل انسانی
۲- شرایط محیطی و مکانی
۳- روش‌های آزمون و اعتبار بخشی روش‌ها
۴- تجهیزات
۵- قابلیت ردیابی اندازه‌گیری
۶- نمونه برداری
۷- کنترل عناصر آزمون
۸- اطمینان از کیفیت نتایج آزمون
۹- گزارش نتایج

میزان عواملی که در عدم قطعیت اندازه‌گیری‌ها سهیم هستند بین انواع آزمون‌ها متفاوت در نظر گرفته شده است. آزمایشگاه باید این عوامل را برای توسعه روش‌های آزمون، روال‌ها، در آموزش و مهارت فنی کارکنان و انتخاب تجهیزات مورد استفاده در نظر بگیرد.

تذکر: در ابتدای هریک از الزامات این بخش حرف <<ف>> که مخفف کلمه <<الزامات فنی>> است، قرار داده شده است.

۲,۵ عوامل انسانی

ف۱,۲. لازم است تا مدیریت آزمایشگاه در تمامی مشاغل و جایگاه‌ها، مخصوصا مشاغل زیر افراد باصلاحیت را به کار بگمارد:

- اداره کنندگان تجهیزات خاص آزمایشگاه
- انجام دهندگان آزمون‌ها
- ارزیابی کنندگان نتایج

- افرادی که گزارشات آزمون را امضاء می‌نمایند.

ف۲,۲. در صورت استفاده از کارکنان تحت آموزش، باید نظارت مناسبی بر روی آن‌ها انجام شود. تخصیص وظایف کارکنان باید بر اساس میزان برخورداری از آموزش، تحصیلات، تجربه یا مهارت آنها باشد.

ف۳,۲. کارکنانی که مسئول برآورد و تفسیر گزارشات آزمون هستند، علاوه بر داشتن مهارت‌های مناسب، آموزش، تجربه و دانش کافی نسبت به آزمون انجام شده، باید:

الف: دارای دانش مرتبط با فناوری مورد استفاده برای ساخت قطعات، مواد، محصولات، آزمون انجام شده، روش مورد استفاده و همچنین نقص‌ها یا انحرافاتی که ممکن است در طول سرویس‌دهی رخ دهد، باشند.

ب: دارای آگاهی از الزامات عمومی بیان شده در قوانین و استانداردها باشند.

ج: دارای درک درست از اختلالات یافت‌شده، با توجه به استفاده‌ی معمولی از قطعات، مواد، محصولات و غیره باشند.

ف۴,۲. مدیریت آزمایشگاه باید با لحاظ نمودن تحصیلات، آموزش و مهارت‌های کارکنان آزمایشگاه، اهداف آموزشی را اولویت‌بندی نماید.

ف۵,۲. آزمایشگاه باید خطمشی و روال‌هایی برای شناسایی آموزش‌های مورد نیاز و همچنین ارائه‌ی آموزش به پرسنل داشته باشد.

ف۶,۲. برنامه‌ی آموزشی باید با وظایف حال حاضر و پیش‌بینی شده‌ی آزمایشگاه منطبق باشد.

ف۷,۲. اثربخشی اقدامات آموزشی انجام شده باید ارزیابی شود.

ف۸,۲ آزمایشگاه باید از کارکنانی که توسط خود آزمایشگاه یا تحت نظر آن استخدام شده‌اند استفاده نماید. در جایی که از کارکنان فنی و پشتیبانی بصورت قراردادی استفاده می‌شود، آزمایشگاه باید دارای روال‌هایی جهت

ارزیابی (فنی و اعتباری)، استخدام و بکارگیری و نظارت بر آنان باشد. همچنن کارکنان مذکور می‌باید تحت سیستم مدیریت آزمایشگاه فعالیت نمایند و تابع ضوابط و مقررات حاکم بر آن باشند.

ف۹,۲. آزمایشگاه باید شرح وظایف شغل کنونی را برای کارکنان مدیریتی، فنی و کارکنان اصلی پشتیبانی که با آزمون‌ها سروکار دارند، مشخص نماید. شرح وظایف شغل می‌تواند به طرق مختلفی انجام شوند. حداقل باید موارد زیر تعریف شوند:

- مسئولیت‌ها با توجه به انجام آزمون‌ها
- مسئولیت‌ها با توجه به برنامه ریزی آزمون‌ها و ارزیابی نتایج
- مسئولیت‌های مرتبط با گزارش نظرات و تفاسیر
- مسئولیت‌ها با توجه به روش اصلاح و توسعه و ارزیابی روش‌های جدید
- تخصص‌ها و تجربه مورد نیاز
- شرایط و برنامه‌های آموزشی
- وظایف مدیریتی

ف۱۰,۲. مدیریت باید به کارکنان معینی، اجازه انجام انواع خاصی از نمونه‌برداری، آزمون، صدور گزارشات آزمون، گرفتن نظرات و تفاسیر و کار با انواع خاصی از تجهیزات را دهد.

ف۱۱,۲. آزمایشگاه باید علاوه بر کارکنان قراردادی، برای کارکنان فنی نیز اطلاعات مرتبط با اختیارات، صلاحیت، مدارک تحصیلی، آموزش، مهارت‌های انجام کار و تجارب آنها را نگهداری نماید. این اطلاعات باید به آسانی قابل دسترسی بوده و همچنین در برگیرنده تاریخ روزی که مجوز و یا صلاحیت تأیید شده است، باشند.

ف۱۲,۲. آزمایشگاه باید دارای متخصص‌ها و مدیرانی با صلاحیت لازم، جهت ارزیابی‌های امنیتی مبتنی بر «استاندارد ارزیابی معیار مشترک و سایر استانداردها و دستورالعمل‌های ابلاغی» باشند.

ف۱۳,۲. آزمایشگاه باید شرح موقعیت شغلی، رکوردهای آموزشی و رزومه‌های پرسنل مسئول، سرپرست و کارکنان آزمایشگاهی را که بر خروجی ارزیابی‌های امنیتی اثرگذار هستند، نگهداری نماید.

ف۱۴,۲. آزمایشگاه باید دربرگیرنده پرسنل زیر برای تکمیل الزامات "طرح ارزیابی امنیتی" باشد:

مدیر آزمایشگاه، نماینده مجاز، امضاءکنندگان مورد تائید، مدیران تیم ارزیابی، ارزیاب‌های ارشد.

ف۱۵,۲. آزمایشگاه باید یکی از کارمندان را به عنوان «مدیر کیفی» معرفی نماید؛ «مدیر کیفی» مسئول سیستم مدیریت، سیستم کیفیت و نگهداری از اسناد سیستم مدیریت است. یک فرد ممکن است در بیش از یک موقعیت کاری به خدمت گرفته شود، اما دو موقعیت کاری «مدیریت آزمایشگاه» و «مدیریت کیفی» لازم است تا مستقل در نظر گرفته شوند.

ف۱۶,۲. کلیه کارکنان آزمایشگاه (رسمی، قراردادی، تمام وقت، پاره وقت و غیره) می‌باید توسط مرکز افتا اعتباربخشی شوند (ارزیابی فنی- امنیتی) و آزمایشگاه باید مرکز افتا را ظرف مدت یک هفته از هرگونه تغییر در پرسنل با خبر سازد. هنگامی که فردی به کارکنان اصلی آزمایشگاه افزوده می‌شود، این تغییرات باید همراه با رزومه کارمند جدید به اطلاع مرکز افتا رسانده شود و قبل از آن اعتباربخشی فردی وی تکمیل شده باشد.

ف۱۷,۲. آزمایشگاه‌ها باید مهارت‌های لازم برای هر موقعیت شغلی را مستند نمایند. اطلاعات شغلی ممکن است در پوشه‌های پرسنلی رسمی یا به صورت جداگانه نگهداری شوند. پوشه‌های رسمی تنها شامل اطلاعاتی است که نماینده مرکز افتا نیاز به بازنگری آنها دارد.

ف۱۸,۲. کارمندان آزمایشگاه که فعالیت‌های ارزیابی امنیتی را انجام می‌دهند، باید حداقل دارای مدرک کارشناس علوم کامپیوتر، مدرک مهندسی کامپیوتر و مدرک مهندسی فناوری اطلاعات، مهندسی برق یا مدرک یکی از رشته‌های فنی یا تجربه‌ای معادل آن را داشته باشند. به طور کلی کارمندان آزمایشگاه باید در زمینه‌های سیستم عامل، ساختمان داده‌ها، طراحی الگوریتم، پایگاه داده‌ها، زبان‌های برنامه نویسی، معماری سیستم‌های

کامپیوتری و شبکه اطلاعات و تجربه‌ای داشته باشند. همچنین کارمندان آزمایشگاه باید در زمینه تکنولوژی‌های خاصی که ارزیابی بر روی آنها انجام می‌شود اطلاعاتی داشته باشند.

ف۱۹,۲. آزمایشگاه باید برای اعضای جدید یا فعلی، جزئیات برنامه آموزشی را مستند نماید. هر کارمند جدید باید برای وظایف که بر عهده‌اش گذاشته می‌شود، آموزش ببیند.

ف۲۰,۲. هنگامیکه «استاندارد ارزیابی معیار مشترک»، «متدلوژی‌های ارزیابی معیار مشترک» و حوزه اعتباربخشی تغییر می‌نماید یا زمانیکه مسئولیت‌های جدیدی به افراد تخصیص داده می‌شود، باید برنامه آموزشی بروزرسانی و کارمندان مجدداً آموزش ببینند. هر کارمندی ممکن است برای مسئولیتی که برای او در نظر گرفته شده به یکی از شیوه‌های زیر آموزش ببیند:

- آموزش حین کار
- حضور در کلاس‌های رسمی
- حضور در کنفرانس‌ها
- دیگر روش‌های مناسب

ف۲۱,۲. کارکنان باید در حوزه‌های زیر آموزش دیده باشند:

- دانش عمومی متدهای آزمون شامل گزارشات ارزیابی
- مفاهیم علوم کامپیوتری
- مفاهیم امنیت کامپیوتر
- دانش کاری استانداردهای امنیتی مورد استفاده
- دانش کاری متدولوژی مرتبط با استانداردهای مورد استفاده

ف۲۲,۲. آزمایشگاه باید سالانه مهارت هر کارمند را در مقام فعلی خود، بازنگری کند

ف۲۳,۲. سرپرست مستقیم کارمندان، یا فرد منصوب شده توسط مدیر آزمایشگاه، باید سالانه، عملکرد هر یک از کارمندان را مشاهده و ارزیابی نماید.

ف۲۴,۲. یک رکورد از بازنگری سالیانه هر فرد باید توسط سرپرست و کارمند، حاوی تاریخ، امضا شود.

ف۲۵,۲. شرح برنامه‌های بازنگری صلاحیت باید در سیستم مدیریت نگهداری شود.

ف۲۶,۲. آزمایشگاه باید اطمینان دهد که تمام افراد شرکت کننده در انجام اقدامات ارزیابی، تمام الزامات سند "طرح ارزیابی امنیتی" را برآورده نموده‌اند.

ف۲۸,۲. برای هر کارمندی که بر خروجی ارزیابی‌ها اثرگذار است باید رکوردهایی نظیر موارد زیر ثبت گردد:

- شرح موقعیت شغلی
- رزومه
- مسئولیتی که بر عهده فرد گذاشته شده است
- بازنگری سالیانه مهارت
- رکوردها و برنامه‌های آموزشی

ف۲۸,۲. توجه به حفظ محرمانگی: آزمایشگاه باید پرسنل مرتبط با ارزیابی را از دیگر پرسنل درون آزمایشگاه یا خارج آن را مجزا کند.

۳,۵ شرایط محیطی و مکانی

ف۱,۳. شرایط محیطی از قبیل گرد خاک، امواج الکترو مغناطیسی، منابع الکتریکی و غیره می‌تواند اثراتی بر روی نتایج آزمون داشته باشد. وظیفه آزمایشگاه در قبال این شرایط، شناسایی و کنترل آن‌ها از طریق خطمشی‌ها و روش‌هایی برای مقابله می‌باشد.

ف۲,۳. امکانات آزمایشگاهی برای آزمون شامل منابع انرژی، روشنایی و شرایط محیطی است اما محدود به آنها نیز نمی‌گردد. این امکانات باید به‌گونه‌ای باشد تا اجرای آزمون را تسهیل نماید.

ف۳,۳. آزمایشگاه باید اطمینان حاصل نماید که شرایط محیطی سبب نامعتبر شدن نتایج نمی‌گردد و بر کیفیت مورد نیاز هرگونه اندازه‌گیری اثر نامطلوب ندارد. هنگامی‌که نمونه‌برداری و آزمون در سایت‌های به جز امکانات دائمی آزمایشگاه انجام می‌شود، مراقبت‌های خاصی باید در نظر گرفته شود.

ف۴,۳. الزامات فنی برای شرایط محیطی و مکانی که می‌تواند بر روی نتایج آزمون تاثیر گذار باشد، باید مستند شوند.

ف۵,۳. آزمایشگاه باید در صورت لزوم توسط معیارها، روش‌ها و روال‌هایی شرایط محیطی را پایش، کنترل و ثبت نماید. باید توجه داشت، مواردی مانند گرد و غبار، اختلالات الکترومغناطیسی، اشعه، رطوبت، منبع برق، درجه حرارت، سطوح صدا و ارتعاش، برای فعالیت‌های فنی مربوطه باید مناسب باشند.

ف۶,۳. آزمون‌ها باید زمانی‌که شرایط محیطی، نتایج آنها را به‌خطر می‌اندازند، متوقف شوند.

ف۷,۳. باید بین مناطق همجواری که فعالیت‌های ناسازگار دارند جداسازی موثری صورت گیرد. اندازه‌گیری[۴] در جهت جلوگیری از آلودگی متقابل[۵] باید انجام شود.

ف۱۱,۳. دسترسی و استفاده از نواحی که بر کیفیت آزمون اثرگذار هستند، باید کنترل شود. آزمایشگاه باید محدوده‌ی کنترل را بر اساس شرایط خاص خود تعیین نماید.

ف۱۲,۳. اقداماتی برای اطمینان از اداره‌ی مناسب کارهای[۶] آزمایشگاه باید انجام شود. در صورت لزوم باید روال‌های خاصی بدین منظور آماده شود.

ف۱۳,۳. آزمایشگاه باید دارای تجهیزات کافی جهت ارزیابی نمودن محصولات فا باشد. این موضوع شامل تجهیزاتی برای ارزیابی امنیتی، آموزش کارکنان، حفظ رکوردها، ذخیره اسناد و ذخیره نرم‌افزارها می‌شود.

[4] Measures

[5] cross-contamination

[۶] همانند نظافت و مرتب نمودن آزمایشگاه

ف۱۴,۳. در محل آزمایشگاه باید سیستم حفاظتی قرار داده شود تا از سخت‌افزار، نرم‌افزار، داده‌های آزمون، رکوردهای الکترونیکی و چاپی و دیگر اطلاعات مشتری، حفاظت کند. این سیستم باید از اطلاعات و تجهیزات اختصاصی در مقابل پرسنل خارج از آزمایشگاه، بازدید کنندگان آزمایشگاه، پرسنل آزمایشگاه غیرمجاز و دیگر اشخاص غیرمجاز محافظت کند.

ف۱۵,۳. آزمایشگاه‌ها باید دارای سیستم‌هایی (مانند سیستم تشخیص نفوذ، دیوار آتش) برای حفاظت از سیستم‌های داخلی در مقابل موجودیت‌های ناامن خارجی، باشد و نتایج رکوردهای آزمایشگاه باید در سیستم‌هایی که از نظر فیزیکی از شبکه اینترنت، مجزا هستند، نگهداری شود.

ف۱۶,۳. اگر اقدامات ارزیابی در بیش از یک محل انجام می‌شوند، در تمام مکان‌ها باید الزامات مرکز افتا رعایت شود و باید سازوکارهایی برای اطمینان از ارتباط امن بین تمام مکان‌ها در محل وجود داشته باشد.

ف۱۷,۳. آزمایشگاه باید بطور منظم حفاظت از تمام سیستم‌ها در برابر ویروس‌ها و دیگر بدافزارها را به‌روزرسانی نماید.

ف۱۸,۳. آزمایشگاه باید دارای سیستم پشتیبانی[۷] موثری باشد؛ تا از بازیابی داده‌ها و رکوردها در صورت از دست رفتن، اطمینان حاصل نماید.

ف۱۹,۳. شبکه‌های آزمایشگاهی که برای ارزیابی برمبنای کلاس‌های تست[۸]و آسیب‌پذیری[۹] بکار می‌روند، باید ایزوله گردند.

ف۲۰,۳. اگر آزمایشگاه به صورت همزمان چندین ارزیابی را انجام می‌دهد، باید محصولات مشتریان مختلف و نتایج ارزیابی‌های آنها را از یکدیگر تفکیک نماید، این موضوع شامل محصول تحت ارزیابی، پلتفرم آزمون، اطلاعات پیرامون، اسناد، رسانه الکترونیکی، راهنماها و رکوردها است.

[7] Backup system
[8] Class ATE: Test
[9] Class AVA:Vulnerability

ف۲۱,۳. در صورت انجام اقدامات ارزیابی خارج از آزمایشگاه، سیستم مدیریتی باید روال‌های مناسبی برای انجام فعالیت‌های ارزیابی امنیتی در سایت مشتری یا سایر مکان‌ها داشته باشد. به‌عنوان مثال، روال‌های سایت مشتری ممکن است چگونگی امن سازی سایت، محل ذخیره سازی رکوردها و مستندات و همچنین چگونگی کنترل دسترسی به تجهیزات آزمون را شرح دهند.

ف۲۲,۳. در صورتی که آزمایشگاه، ارزیابی خود را در سایت مشتری یا دیگر مکان‌های خارج از آزمایشگاه انجام دهد، محیط باید مطابق با الزامات مورد نیاز برای محیط آزمایشگاه باشد.

ف۲۳,۳. اگر یک سیستم مشتری که مورد ارزیابی واقع شده، در طی ارزیابی بطور بالقوه برای دسترسی موجودیت‌های غیرمجاز باز باشد، آزمایشگاه ارزیابی باید محیط ارزیابی را نیز کنترل کند. در این صورت اطمینان حاصل می‌شود که پیش از شروع شدن ارزیابی سیستم‌ها در یک وضعیت تعریف شده و سازگار با الزامات ارزیابی هستند، همچنین اطمینان داده می‌شود که در طول ارزیابی سیستم، موجودیت‌های غیرمجاز به آن دسترسی ندارند.

۴,۵ روش‌های آزمون و اعتبار بخشی روش‌ها

۱,۴,۵ کلیات

ف۱,۴. نسخه «استاندارد ارزیابی معیار مشترک» و «متدلوژی ارزیابی معیار مشترک» که در هر ارزیابی استفاده می‌شوند باید به مرکز افتا اطلاع داده شوند.

ف۲,۴. به منظور حاصل شدن اعتباربخشی محصول توسط استاندارد ارزیابی معیار مشترک، ممکن است آزمایشگاه‌ها ملزم به رعایت تفسیرات بین‌المللی و راهنمایی‌های مرکز افتا گردد. مرکز افتا ممکن است تفاسیر یا

راهنمایی‌هایی جهت تکمیل «استاندارد ارزیابی معیار مشترک» و «متدلوژی ارزیابی معیار مشترک» انتشار دهد. آزمایشگاه باید در بازه زمانی مشخص شده توسط مرکز افتا منطبق بر راهنمایی‌ها و تفسیرها باشد.

ف۳,۴. «استاندارد ارزیابی معیار مشترک»، «متدلوژی ارزیابی معیار مشترک»، تفاسیر و راهنمایی‌های مرکز افتا و روال‌های آزمایشگاه برای انجام ارزیابی‌های امنیتی باید بروز نگهداری شوند و به آسانی در دسترس کارمندان قرار گیرند.

ف۴,۴. آزمایشگاه باید روال‌هایی برای انجام ارزیابی امنیتی با استفاده از «استاندارد ارزیابی معیار مشترک» و «متدلوژی ارزیابی معیار مشترک» و همچنین برای انطباق با راهنمایی‌ها یا تفاسیر مستند نماید و از دنبال شدن آنها اطمینان حاصل نماید.

ف۵,۴. ارزیابی ممکن است با توافق آزمایشگاه، تولید کننده و مرکز افتا در محل مشتری، آزمایشگاه یا دیگر مکان‌ها انجام گیرد. زمانیکه ارزیابی در خارج آزمایشگاه انجام می‌گیرد، آزمایشگاه باید دارای روال‌های بیشتری جهت اطمینان از صحت تمام آزمون‌ها و نتایج ثبت شده باشد.

ف۶,۴. هنگامی که به دلایل فنی، در نظر گرفتن موارد استثنا برای متدولوژی ارزیابی ضروری باشند، آزمایشگاه باید با مرکز افتا برای اطمینان از اینکه متدولوژی جدید همچنان مطابق با تمام الزامات و خطمشی‌ها است رایزنی نماید؛ همچنین مشتری باید مطلع گردد؛ و جزئیات این موارد استثنا باید در گزارش ارزیابی شرح داده شوند.

ف۷,۴. آزمایشگاه باید در حوزه خود از روش‌ها و روال‌های مناسب برای تمام آزمون‌ها استفاده نماید، که شامل نمونه برداری، کنترل، انتقال و آماده سازی و ذخیره‌سازی مواردی که مورد آزمون قرار گرفته‌اند، و در صورت

لزوم برآورد میزان عدم قطعیت اندازه‌گیری و همچنین تکنیک‌های آماری که جهت تحلیل داده‌های آزمون استفاده می‌شوند نیز مشخص گردند.

ف۸,۴. آزمایشگاه باید دستورالعمل‌های مربوط به استفاده و بهره‌برداری از تمام تجهیزات مربوطه و نیز دستورالعمل‌های مربوط به اداره و آماده‌سازی بخش‌های آزمون، یا هر دو را داشته باشد که عدم وجود چنین دستورالعمل‌هایی می‌تواند نتایج آزمون‌ها را به خطر اندازد.

ف۹,۴. تمامی دستورالعمل‌ها، استانداردها، راهنماها و داده‌های مرجع مربوط به کار آزمایشگاه، باید به روز بوده و باید به‌آسانی در دسترس کارکنان قرار گیرند.

ف۱۰,۴. انحراف از روش‌های آزمون باید تنها درصورتی اتفاق بیافتد که انحراف ثبت گردد، از نظر فنی قابل توجیه، مجاز و توسط مشتری پذیرفته شده باشد. استانداردهای بین‌المللی، منطقه‌ای یا ملی و یا سایر مشخصه‌های به رسمیت شناخته شده که حاوی اطلاعات کافی و مختصر درباره چگونگی انجام آزمون‌ها است، اگر به روشی نوشته شده‌اند که می‌توانند توسط کارکنان در یک آزمایشگاه مورد استفاده قرارگیرد، نیازی به تکمیل یا نوشتن مجدد آن‌ها به عنوان روال داخلی نیست.

۲,۴,۵ انتخاب روش‌ها

ف۱۱,۴. آزمایشگاه باید از روش‌های آزمون، شامل روش‌های نمونه‌برداری استفاده نماید که پاسخگوی نیازهای مشتری بوده و برای آزمون که نسبت به آن‌ها متعهد است، مناسب باشد. روش‌های منتشرشده در استانداردهای بین‌المللی، منطقه‌ای یا ملی باید به طور مطلوب مورد استفاده قرار گیرند. آزمایشگاه باید تضمین نماید که از آخرین نسخه‌ی معتبر استاندارد استفاده نموده است مگر اینکه استفاده از آخرین نسخه برای انجام کار مناسب یا امکان‌پذیر نباشد. در صورت لزوم، باید استاندارد استفاده شده برای تضمین سازگاری، با جزییات بیشتری تکمیل شود.

ف۱۲,۴. هنگامی که مشتری روشی را برای استفاده مشخص نکند، آزمایشگاه باید از میان روش‌هایی که در استانداردهای بین‌المللی، منطقه‌ای یا ملی، یا توسط سازمان‌های معتبر فنی، و یا در متون علمی و یا مجلات مرتبط منتشر شده و یا توسط تولیدکننده‌ی تجهیزات تعیین شده، روشی مناسب را انتخاب نماید. روش‌های آزمایشگاهی توسعه‌یافته و یا روش‌هایی که توسط آزمایشگاه پذیرفته شده‌اند، اگر برای کاربرد موردنظر مناسب و معتبر باشند، مورد استفاده قرار می‌گیرند.

ف۱۳,۴. مشتری باید از روش انتخاب‌شده، مطلع شود.

ف۱۴,۴. آزمایشگاه باید تایید کند که می‌تواند بدرستی روش‌های استاندارد را پیش از آزمون به‌کار گیرد. در صورت تغییر یافتن روش استاندارد، آزمایشگاه باید مجدداً بکار بردن این روش‌ها را تائید نماید.

ف۱۵,۴. آزمایشگاه باید مشتری را هنگامی‌که روش پیشنهاد شده توسط او نامناسب و یا از تاریخ گذشته است، مطلع سازد.

۳,۴,۵ روش‌های توسعه‌یافته توسط آزمایشگاه

ف۱۶,۴. معرفی روش‌های آزمون که توسط آزمایشگاه برای استفاده‌های مخصوص خود توسعه می‌یابد باید یک فعالیت برنامه‌ریزی شده باشد و باید به کارکنانی متخصصی که با منابع کافی تجهیز شده‌اند، ارجاع داده شود. برنامه‌ها باید به عنوان نتیجه حاصل از توسعه، به‌روزرسانی شده و روابط موثر درمیان تمام افراد درگیر، تضمین شود.

۴,۴,۵ روش‌های غیر استاندارد

ف۱۷,۴. در مواقعی که نیاز است از روش‌هایی استفاده شود که تحت پوشش روش‌های استاندارد نیست، این موضوع منوط به توافق با مشتری است و باید مبنی بر نیازهای مشتری و هدف از انجام آزمون باشد.

ف۱۸,۴. روش توسعه‌یافته باید پیش از استفاده اعتباربخشی شده باشد.

نکته: برای روش‌های جدید آزمون، خطمشی‌ها باید پیش از انجام آزمون توسعه یابند و باید حداقل شامل اطلاعات زیر باشند:

۱) شناسایی مناسب

۲) حوزه

۳) شرح انواع مواردی که مورد آزمون قرار گرفته‌اند.

۴) پارامترها یا کمیت‌ها و محدوده‌ی تعیین شده

۵) دستگاه‌ها و تجهیزات، شامل الزامات اجرای فنی

۶) استانداردهای مرجع و منابع مرجع مورد نیاز

۷) شرایط محیطی و هر دوره‌ی تثبیت مورد نیاز

۸) شرح روال‌ها شامل:

- الصاق علامت‌های شناسایی، جابجایی، انتقالات، ذخیره‌سازی و آماده‌سازی بخش‌ها
- انجام بررسی پیش از شروع کار
- بررسی عملکرد صحیح تجهیزات و در صورت نیاز، کالیبراسیون و تنظیم تجهیزات پیش از استفاده
- روش ثبت مشاهدات و نتایج
- مشاهده هرگونه اقدامات مربوط به امنیت

۹) ضوابط و یا الزامات برای تایید یا رد شدن برای روش

۱۰) داده‌های ثبت‌شده و روش‌های تجزیه و تحلیل

۱۱) عدم قطعیت یا روال‌های تخمین عدم قطعیت

۵,۴,۵ اعتباربخشی روش‌ها

اعتباربخشی، تایید از طریق بازرسی و امتحان و ارائه‌ی شواهد عینی است که الزامات ویژه‌ای را برای استفاده‌های موردنظر برآورده می‌سازد. آزمایشگاه باید «روش‌های غیر استاندارد»، «روش‌های توسعه یافته توسط آزمایشگاه»، «روش‌های استانداردی که در خارج از محدوده‌ی درنظرگرفته شده برای آنها استفاده می‌شوند» و همچنین «روش‌های استاندارد بسط داده شده و تغییر یافته» را، اعتباربخشی نماید، تا از مناسب بودن آنها برای استفاده‌های مورد نظر اطمینان حاصل نماید.

ف۱۹,۴. آزمایشگاه باید نتایج بدست آمده، روال‌های استفاده شده برای اعتباربخشی و شرحی از مناسب بودن روش برای کاربرد موردنظر را ثبت نماید. اعتباربخشی ممکن است شامل روال‌هایی برای نمونه برداری، اداره نمودن و انتقال باشد. همچنین تکنیک‌های مورد استفاده برای تعیین کارایی یک روش، باید یکی یا ترکیبی از موارد زیر باشد:

- مقایسه‌ی نتایج حاصله با سایر روش‌ها
- مقایسه‌های میان آزمایشگاهی
- ارزیابی سیستماتیک عوامل تأثیرگذار روی نتایج
- ارزیابی از عدم قطعیت نتایج براساس درک علمی اصول تئوری روش‌ها و تجربیات عملی

ف۲۰,۴. در مواقعی‌که تغییراتی در روش‌های غیر استاندارد اعتباربخشی شده ایجاد شوند، تأثیر این تغییرات باید مستند شود و درصورت مناسب بودن، باید اعتباربخشی جدیدی انجام شود.

ف۲۱,۴. دقت مقادیر قابل کسب از روش‌های اعتباربخشی باید متناسب با نیازهای مشتریان باشد. با پیشرفت روند توسعه روش[10]، باید بازنگری منظمی برای تعیین نیازمندی‌های مشتریان که هنوز تکمیل نشده‌اند، انجام

[10] method-development

شود. هر گونه تغییر در الزامات که به تغییراتی روی طرح توسعه نیازمند است، باید تأیید و مجوزدهی شود. اعتباربخشی همیشه در تعادل بین هزینه‌ها، خطرات و امکانات فنی می‌باشد. خیلی موارد وجود دارد که به علت کمبود اطلاعات (مقادیر غیر دقیق) فقط اعتباربخشی مختصری می‌تواند داده شود.

۶,۴,۵ تخمین عدم قطعیت سنجش‌های[۱۱] آزمایشگاه

آزمایشگاه آزمون، باید برای تمام آزمون‌هایی که انجام می‌دهد، روال‌هایی برای تخمین عدم قطعیت سنجش‌های صورت گرفته، داشته باشد.

ف۲۱,۴. آزمایشگاه‌های آزمون باید روال‌هایی برای تخمین عدم قطعیت سنجش‌های صورت گرفته در آزمایشگاه داشته باشند واین روال‌ها را بکار برند. در برخی موارد ماهیت روش آزمون، مانع جدی برای محاسبه عدم قطعیت سنجش‌های صورت گرفته در آزمایشگاه است. در این موارد آزمایشگاه باید حداقل سعی نماید تا تمام بخش‌هایی که سبب عدم قطعیت می‌شوند را شناسایی و یک برآورد معقول نمایند و اطمینان دهند که این شکل از برآورد نمودن، سبب برداشت غلط از عدم قطعیت نمی‌گردد. برآورد معقول باید براساس دانشی که از کارایی روش‌ها وجود دارد و محدوده سنجش‌های صورت گرفته باشد، بطور نمونه باید با استفاده از تجربه های قبلی و داده‌های اعتباربخشی برآوردی از عدم قطعیت صورت گیرد. درجه‌ی دقت مورد نیاز در تخمین عدم قطعیت سنجش‌های صورت گرفته بستگی به عواملی مانند موارد زیر دارد:

- الزامات روش آزمون
- الزامات مشتری
- محدودیت‌هایی که بر روی تصمیم‌گیری برای مطابقت با خصوصیات، وجود دارد.

[۱۱] - برآورد خطای اندازه گیری

ف۲۲,۴. هنگام تخمین عدم قطعیت سنجش‌های صورت گرفته، تمام بخش‌هایی که در عدم قطعیت نقش دارند باید با استفاده از روش‌های تحلیلی مناسب در نظر گرفته شوند. منابعی که در عدم قطعیت نقش دارند اما به آنها محدود نمی‌گردد، عبارتند از:

- استانداردها و منابع مرجع استفاده شده
- روش‌ها و تجهیزات مورد استفاده
- شرایط محیطی
- ویژگی‌ها و شرایط مورد آزمون
- اپراتور

و رفتارهای بلند مدت پیش‌بینی شده‌ی موردی که آزمون شده، به طور معمول در هنگام تخمین عدم قطعیت سنجش صورت گرفته در نظر گرفته نمی‌شوند.

۷,۴,۵ کنترل داده

محاسبات و انتقال داده‌ها، منوط به بررسی مناسب در شیوه‌ای نظام‌مند خواهد بود.

ف۲۳,۴. زمانی که از کامپیوتر یا تجهیزات خودکار برای استفاده، پردازش، ضبط، گزارش، ذخیره‌سازی و بازیابی داده‌های آزمون استفاده می‌شود، آزمایشگاه باید اطمینان حاصل کند که:

الف) نرم‌افزارهای کامپیوتری توسعه یافته توسط کاربر با جزییات کافی مستند شده‌اند و برای استفاده مورد تایید هستند.

ب) روال‌هایی برای حفاظت از داده‌ها، ایجاد و پیاده‌سازی شده‌اند. این روال‌ها شامل مواردی مانند یکپارچگی و محرمانگی داده‌های ورودی و یا جمع‌آوری آن‌ها، ذخیره‌سازی داده‌ها، انتقال داده‌ها و پردازش داده‌ها می‌باشد.

ج) کامپیوترها و تجهیزات خودکار برای اطمینان از عملکرد مناسب نگهداری و با توجه به شرایط محیطی و عملیاتی ارائه می‌شوند، تا صحت و یکپارچگی داده‌های آزمون را حفظ نماید.

نرم‌افزارهای تجاری در دسترس(به عنوان مثال، پردازش کلمه، پایگاه داده و برنامه‌های آماری) ممکن است در محدوده‌ای که برای استفاده آن برنامه طراحی شده به اندازه کافی معتبر باشد. با این حال، باید پیکربندی و یـا تغییرات نرم افزار آزمایشگاه، براساس بند الف الزام بالا تایید شده باشند.

۵,۵ تجهیزات

منظور از تجهیزات آن دسته می‌باشند که با آزمون و یا نتایج آزمون در ارتباط باشند. تجهیزات آزمایشگاه اعم از نرم افزارهای آن‌ها باید دقت و ویژگی‌های لازم برای انجام آزمون را داشته باشند.

ف۱,۵. این تجهیزات قبل از استفاده در آزمون باید الزامات آزمایشگاه و استانداردهای مشخصی را برآورده سازند و برای انجام آزمون کالیبره شوند.

ف۲,۵. تجهیزات باید به طور یکتا مشخص شوند.

ف۳,۵. تجهیزات باید توسط افراد مجاز استفاده شوند.

ف۴,۵. رکوردهای هر یک از تجهیزات باید مشخص شوند.

ف۵,۵. آزمایشگاه باید به تمام اقلام نمونه‌برداری، اندازه‌گیری و تجهیزات آزمون که برای عملکرد صحیح آزمون مورد نیاز است، مجهز شود. (از جمله نمونه‌برداری، آماده‌سازی موارد آزمون، پردازش و تجزیه و تحلیل داده‌های آزمون).

ف۶,۵. در مواردی که آزمایشگاه نیاز به تجهیزاتی دارد که خارج از کنترل دائمی‌اش است، باید از برآورده شدن الزامات این سند اطمینان حاصل نماید.

ف۷,۵. تجهیزات و نرم‌افزار استفاده‌شده برای آزمایش و نمونه برداری باید قادر به دستیابی به دقت و صحت مورد نیاز باشند و باید مطابق با مشخصات مربوط به آزمون‌ها باشند.

ف۸,۵. قبل از آنکه تجهیزات استفاده شوند باید کالیبره شده و یا چک شوند تا تائید گردد که الزامات خصوصیات آزمایشگاه را رعایت نموده ومطابق با مشخصات استاندارد مربوطه می‌باشند.

ف۹,۵. تجهیزات باید توسط پرسنل مجاز اداره شوند. دستورالعمل‌ها برای استفاده و نگهداری از تجهیزات باید به روز شده (از جمله هر نوع راهنمای مرتبط ارائه شده توسط سازنده تجهیزات) و به راحتی در دسترس پرسنل آزمایشگاه قرار داده شوند.

ف۱۰,۵. تجهیزات و نرم افزارهای استفاده شده برای آزمایش، باید بصورت منحصر به فرد مشخص باشند.

ف۱۱,۵. رکوردهای مرتبط با تجهیزات و نرم‌افزارهای استفاده شده در انجام آزمون، باید محافظت شده و حداقل شامل موارد زیر باشد:

الف) شناسه آیتم تجهیزات و نرم افزار آن

ب) نام سازنده، علامت شناسایی و شماره سریال و یا دیگر موارد شناسایی منحصر به فرد

ج)چک کردن مطابقت تجهیزات با خصوصیات

د) موقعیت فعلی

ه) دستورالعمل کارخانه سازنده، در صورت وجود

و) تاریخ‌ها، نتایج و نسخه‌هایی از گزارش‌ها، تنظیمات، معیارهای پذیرش

ز) طرح تعمیر و نگهداری

ح) هر گونه خسارت، نقص، اصلاح یا تعمیر تجهیزات

ف۱۲,۵. آزمایشگاه باید روالی با برنامه برای کنترل امن، حمل و نقل، ذخیره‌سازی، استفاده و نگهداری از تجهیزات اندازه‌گیری داشته باشد، تا از عملکرد مناسب آن و جلوگیری نمودن از آلودگی و یا نابود شدن آنها

اطمینان حاصل نماید. زمانی که تجهیزات اندازه‌گیری در خارج ازمحل دائمی آزمایشگاه برای آزمایش و یا نمونه برداری استفاده می‌شوند، ممکن است نیاز به روال‌های بیشتری باشد.

ف۱۳,۵. تجهیزات زیر باید از سرویس دهی خارج شوند:

- در معرض سربار شدن[۱۲] یا بد بکار برده شدن[۱۳] قرار می‌گیرند،
- نتایج مشکوک می‌دهند،
- معیوب نشان داده می‌شوند
- خارج از محدوده مشخص شده می‌باشند

ف۱۴,۵. این تجهیزات باید تا زمانیکه تعمیر شوند علامت خارج از سرویس بر روی آنها نصب شود.

ف۱۵,۵. همه تجهیزات تحت کنترل آزمایشگاه و همچنین مورد نیاز به کالیبراسیون باید برچسب‌گذاری، کد گذاری شوند، در غیر این صورت دارای شناسه‌ای به منظور نشان دادن وضعیت کالیبراسیون، از جمله تاریخ آخرین کالیبره شدن و تاریخ یا معیار انقضای کالیبراسیون باشد.

ف۱۶,۵. در زمانی که به هر دلیلی، تجهیزات خارج از کنترل مستقیم آزمایشگاه می‌باشند، قبل از آن‌که تجهیزات به سرویس بازگشته شوند، آزمایشگاه باید اطمینان حاصل کند که عملکرد و وضعیت کالیبراسیون تجهیزات بررسی شده و رضایت بخش است.

ف۱۷,۵. آزمون تجهیزات، اعم از سخت‌افزار و نرم‌افزار، باید از تغییراتی که منجر به غیر معتبر شدن آزمون می‌شوند محافظت شوند.

ف۱۸,۵. آزمایشگاه باید سیستم‌های کافی را برای حمایت از ارزیابی‌های امنیت فناوری اطلاعات، مطابق با آزمون‌ها داشته باشد تا منجر به اعتباربخشی گردد.

ف۱۹,۵. آزمایشگاه باید توانایی تولید گزارش الکترونیکی را داشته باشد.

[12] overloading
[13] mishandling

ف۲۰,۵. آزمایشگاه باید رکوردهای تمام تجهیزات آزمون و یا مجموعه‌های آزمونی که در طول آزمون‌های «استاندارد ارزیابی معیار مشترک» استفاده شده‌اند را مستند و نگهداری نماید. آزمایشگاه مسئول پیکربندی و بهره‌برداری از تمام تجهیزات تحت کنترلش می‌باشد.

ف۲۱,۵. سیستم‌های کامپیوتری و دیگر پلتفرم‌های استفاده شده در طی انجام آزمون باید تحت کنترل پیکربندی شوند.

ف۲۲,۵. آزمایشگاه باید دارای روال‌هایی برای حصول اطمینان از اینکه تمام تجهیزات (سخت‌افزاری و نرم‌افزاری) مورد استفاده برای آزمون، قبل از استفاده در یک وضعیت مشخص هستند، باشد.

۶,۵ قابلیت ردیابی اندازه‌گیری

تمامی تجهیزاتی که برای آزمون مورد استفاده قرار می‌گیرد و همچنین تجهیزاتی که برای کنترل شرایط محیطی به کار می‌روند تاثیر مستقیمی به روی آزمون و نتایج آن دارند از این رو آزمایشگاه باید برنامه و خطمشی مدونی برای کالیبره کردن این تجهیزات داشته باشد.

۱,۶,۵ کلیات

ف۱,۶. کلیه تجهیزات مورد استفاده برای آزمون که اثر قابل توجهی در صحت و یا اعتبار نتیجه آزمون و یا نمونه گیری دارند و قبل از اینکه در سرویس قرار گیرند باید کالیبره شده باشند.

ف۲,۶. آزمایشگاه باید برنامه‌ای برای کالیبراسیون تجهیزات خود داشته باشد. چنین برنامه‌ای باید شامل یک سیستم برای انتخاب، استفاده، کالیبره نمودن، بررسی، کنترل و نگهداری استانداردهای اندازه‌گیری و مراجع استفاده شده به عنوان استانداردهای اندازه‌گیری و همچنین اندازه‌گیری و آزمون تجهیزات استفاده شده در انجام آزمون باشد.

۱,۶,۵ الزامات خاص آزمون

ف۳,۶. تجهیزات مورد استفاده برای انجام ارزیابی امنیتی باید مطابق با توصیه‌های سازنده یا مطابق با رویه‌های مستند شده داخلی آزمایشگاه، نگهداری شوند.

ف۴,۶. آزمایشگاه‌ها باید تجهیزات خود را کالیبره کنند. در آزمون‌های ارزیابی امنیت محصولات فناوری اطلاعات، کالیبراسیون به معنای تائید صحت و مناسب بودن است. هرگونه ابزار آزمون مورد استفاده برای انجام ارزیابی امنیتی که بخشی از واحد تحت ارزیابی نیستند باید به تنهایی مورد بررسی قرار گیرند تا اطمینان حاصل شود که بطور درست ارائه شده و همانطور که آنها می‌خواهند ارزیابی می‌شود؛ همچنین باید مورد بررسی قرار گیرند تا از عدم دخالت آنها در انجام آزمون، و عدم تغییر یا تاثیر در یکپارچگی محصول تحت آزمون در هر شرایطی اطمینان حاصل کنند.

ف۵,۶. آزمایشگاه‌ها باید روش‌هایی داشته باشند تا از پیکربندی مناسب تجهیزات آزمون اطمینان حاصل کنند. آزمایشگاه‌ها باید رکوردهای مربوط به پیکربندی تجهیزات آزمون و تمام تجزیه و تحلیل‌ها را برای اطمینان از مناسب بودن تجهیزات آزمون برای اجرای آزمون مورد نظر، نگهداری کنند.

ف۶,۶. برای آزمون ارزیابی امنیت محصولات فناوری اطلاعات، "ردیابی"، به معنی اقدامات ارزیابی امنیتی برای الزامات اساسی استاندارد مورد استفاده و واحدهای کاری متدولوژی ارزیابی که قابل ردیابی هستند، تعبیر می‌شود. این بدان معنی است که ابزار آزمون و متدولوژی‌های ارزیابی نشان می‌دهند که آزمون‌هایی که آنها انجام می‌دهند و اظهارات برآمده از آزمونی که آنها انجام داده‌اند، برای متدولوژی و ضوابط، قابل ردیابی هستند. این مورد برای حصول اطمینان از مدارک قابل اعتماد منصوب به نتایج آزمون ارزیابی امنیت محصولات، ضروری است.

۷,۵ نمونه برداری

آزمایشگاه باید طرح نمونه برداری را مشخص نماید که این طرح باید معقول و بر اساس روشهای آماری باشد.

نمونه برداری به خطمشی گفته می‌شود که طی آن قسمتی از ماده یا محصول برای انجام آزمون انتخاب شده و نماینده کل محصول می‌باشد.

ف۱,۷. آزمایشگاه باید زمانیکه از اشیاء، مواد یا محصولات برای آزمون‌های بعدی نمونه‌برداری انجام می‌دهد، دارای طرح و رویه‌ای برای این نمونه‌برداری‌ها باشد.

ف۲,۷. طرح و رویه نمونه‌برداری باید در محلی که در آن نمونه برداری انجام شده است، در دسترس باشند. همواره طرح‌های نمونه‌برداری باید بر اساس روش‌های آماری مناسب باشند. فرآیند نمونه برداری باید منطبق با عواملی باشد که باعث حصول اطمینان از صحت نتایج آزمون می‌شوند. نمونه‌برداری یک رویه تعریف شده است که بخشی از محصول مورد آزمون را به عنوان نمونه‌ای از کل ارائه می‌دهد. روش نمونه‌برداری به منظور حاصل شدن اطلاعات لازم، باید موارد زیر را در نظر بگیرد:

- نحوه انتخاب نمونه
- طرح نمونه‌برداری
- آماده‌سازی نمونه یا نمونه‌هایی از یک محصول تا اطلاعات لازم حاصل گردد.

ف۳,۷. در جایی که مشتری خواستار آن است که از رویه نمونه‌برداری مستند شده منحرف شود/ یا ازآن مستثنی گردد/ یا به آن ضمیمه نماید؛ این موضوع باید با جزئیات همراه داده‌های نمونه‌برداری ثبت گردد و باید در تمام اسناد حاوی نتایج آزمون در نظر گرفته شود و همچنین به اطلاع پرسنل مربوطه برسد.

ف۴,۷. اطلاعات مربوط به نمونه‌برداری و یا از روش نمونه‌برداری مستند شده را در اختیار نداشته، این موضوع باید با جزئیات و به همراه داده‌های نمونه‌گیری، ثبت شده و در همه اسناد حاوی نتایج آزمون وجود داشته باشد و همچنین به پرسنل مربوطه اطلاع داده شود.

ف۵,۷. آزمایشگاه باید رویه‌ای برای ثبت اطلاعات و اقدامات مربوط به نمونه‌برداری داشته باشد، تا بخشی از آزمون صورت گرفته را به یک شکل و قالب در آورد. این رکوردها باید شامل روش نمونه‌برداری استفاده شده،

مشخصات نمونه‌بردار، شرایط محیطی (در صورت وجود) و نمودار یا معادل‌های آن باشد تا در صورت لزوم موقعیت نمونه‌برداری مشخص شود و به شرط مناسب بودن، آمارگیری‌های رویه نمونه‌برداری بر اساس آن انجام گیرد.

ف۶,۷. آزمایشگاه باید از رویه‌های مستند شده برای نمونه برداری استفاده کند.

ف۷,۷. هرگاه نمونه‌برداری در طول ارزیابی مورد استفاده قرار گیرد، آزمایشگاه باید استراتژی خود را در نمونه‌برداری، فرآیند تصمیم‌گیری و ماهیت نمونه مستند نماید.

ف۸,۷. نمونه‌برداری بخشی از رکورد ارزیابی است.

۸,۵ کنترل نمونه های آزمون

آزمایشگاه باید رویه‌هایی برای انتقال، دریافت و حفاظت از نمونه‌های آزمون برای ئرا داشته باشد.

ف۱,۸.آزمایشگاه باید رویه‌هایی برای انتقال، پذیرش، کنترل، حفاظت، ذخیره‌سازی و نگهداری/ انهدام عناصر آزمون را، علاوه بر تمامی مقررات لازم برای حفاظت از یکپارچگی عناصر آزمون و حفاظت از منافع آزمایشگاه و مشتری داشته باشد.

ف۲,۸. آزمایشگاه باید سیستمی را برای شناسایی نمونه‌های آزمون ارائه کند و تا زمانیکه آن عنصر در آزمایشگاه وجود دارد شناسایی نیز باید باشد. سیستم باید به گونه‌ای طراحی و عملیاتی شود که اطمینان حاصل کند، نمونه های آزمون نمی‌توانند از نظر فیزیکی و یا هنگامی که به رکوردها و یا دیگر اسناد ارجاع داده می‌شوند، اشتباه گرفته شوند.

ف۳,۸. پس از دریافت نمونه آزمون، اختلالات یا خروج از شرایط طبیعی مشخص شده، همانگونه که در روش آزمون شرح داده شده، باید ثبت گردد.

ف۴,۸. هنگامی که نسبت به مناسب بودن یک نمونه برای آزمون شک و تردید وجود دارد، یا وقتی که یک نمونه با توضیحات ارائه شده مطابقت ندارد، و آزمون با جزئیات لازم و کافی مشخص نشده، آزمایشگاه باید قبل از

پردازش چنین نمونه هایی با مشتری برای دستور العمل‌های بیشتر مشورت کند و باید هر آنچه در این مذاکره اتفاق می‌افتد را ثبت کند.

ف۵,۸. آزمایشگاه باید دارای رویه‌ها و امکانات مناسبی برای جلوگیری از آسیب‌رساندن و از دست دادن اطلاعات در طول ذخیره سازی، پردازش و آماده سازی نمونه آزمون باشد.

ف۶,۸. هنگامی که ذخیره سازی نمونه ها مشروط به شرایط محیطی مشخصی باشد، این شرایط باید حفظ، نظارت و ثبت شوند. هنگامیکه نمونه آزمون یا بخشی از یک نمونه به صورت امن نگهداری می‌شوند، آزمایشگاه باید مقرراتی برای ذخیره امن و محافظت از شرایط و صحت و یکپارچگی نمونه هایی که به صورت امن نگهداری می‌شوند داشته باشد. همچنین از جمله دلایل امن نگه داشتن یک نمونه آزمون و می‌تواند به ثبت، ایمنی یا ارزش، یا برای آزمون‌های مکمل که بعدا انجام می‌گیرد، اشاره کرد. همچنین پس از آزمون و در زمانی که نمونه‌های آزمون به محل سرویس‌دهی خود بازگردانده می‌شوند، مراقبت‌های خاصی لازم است تا اطمینان حاصل شود که به آن‌ها خسارت وارد نشده یا آسیبی در طول حمل، آزمون یا فرآیندهای انتظار/ذخیره‌سازی ندیده‌اند. رویه نمونه‌برداری و اطلاعات مربوط به ذخیره و انتقال نمونه‌ها، همانند اطلاعات راجع به عوامل نمونه-برداری که بر روی نتیجه آزمون اثرگذار هستند، باید برای کسانی که مسئول به‌کارگیری و انتقال نمونه‌ها هستند ارائه شود.

ف۷,۸. آزمایشگاه باید محصولات تحت ارزیابی و ابزارهای کالیبره شده را در مقابل استفاده، اصلاح و دسترسی غیرمجاز حفظ کند.

ف۹,۸. آزمایشگاه باید تفاوت‌های بین نمونه‌ها و کنترل بر آنها را در مقابل ارزیابی‌های مختلف که شامل محصول تحت ارزیابی، پلتفرم آن، لوازم جانبی و مستندات می‌شود، حفظ کند.

ف۱۰,۸. هنگامی که محصول تحت ارزیابی شامل اجزای نرم‌افزاری است، آزمایشگاه باید برای جلوگیری از تغییرات ناخواسته در اجزای نرم‌افزار از اینکه مکانیزم‌های مدیریت پیکربندی در طول فرآیند ارزیابی، در مکان خود قرار دارند، اطمینان حاصل کند.

ف۱۱,۸. آزمایشگاه باید رویه‌هایی داشته باشد تا از نگه‌داری، دسترسی یا مراجعت نرم‌افزار و سخت‌افزار بعد از تکمیل ارزیابی اطمینان حاصل کند.

۹,۵ تضمین کیفیت نتایج آزمون

آزمایشگاه باید روش‌های کنترل کیفیت را برای نظارت بر صحت انجام آزمون داشته باشد.

ف۱,۹. داده‌های آزمون باید به گونه‌ای ثبت شوند که قابل تشخیص بوده و در آن باید تکنیک‌های آماری و عملی به منظور بازنگری نتایج به‌کار روند. روش‌های انتخاب شده باید با نوع و حجم کار انجام شده متناسب باشد. این نظارت باید برنامه‌ریزی و بازبینی شده باشد و ممکن است شامل موارد زیر شود که البته محدود به آن‌ها نمی‌باشد:

۱) استفاده منظم از اطلاعات مرجع مجاز و یا کنترل کیفیت داخلی با استفاده از اطلاعات مرجع ثانویه

۲) مشارکت در مقایسه آزمایشگاه‌های داخلی یا برنامه‌های مهارت آزمون

۳) تکرار آزمون با استفاده از روش های یکسان و یا متفاوت

۴) آزمون مجدد نمونه‌های باقی‌مانده

۵) ارتباط نتایج برای ویژگی‌های مختلف یک آزمون

ف۲,۹. داده‌های کنترل کیفیت باید تجزیه و تحلیل شود و در جایی که آنها خارج از معیارهای از پیش تعریف شده هستند، اقدامات برنامه‌ریزی شده‌ای باید انجام شود تا این مشکل اصلاح و از گزارش‌های نادرست جلوگیری گردد.

ف۳,۹. آزمایشگاه باید رویه‌هایی را برای انجام بازنگری نهایی نتایج ارزیابی، گزارش‌های فنی و رکوردهای آزمایشگاه ارزیابی، قبل از انعکاس این نتایج به مشتری و یا مرکز افتا داشته باشد.

۱۰,۵ گزارش نتایج

۱,۱۰,۵ کلیات[14]

نتایج هر آزمون یا مجموعه‌ای از آزمون انجام شده توسط آزمایشگاه باید با دقت، به وضوح، عینی، و مطابق با هر دستورالعمل خاص در روش آزمون گزارش شود.

ف۱,۱۰. نتایج باید به صورت کتبی گزارش شود. معمولا گزارش آزمون، شامل تمام اطلاعات درخواست شده توسط مشتری و اطلاعات لازم برای تفسیر نتایج آزمون و تمام اطلاعات مورد نیاز روش استفاده شده می‌باشد. تا حد ممکن نتایج آزمون انجام شده برای مشتریان داخلی بصورت ساده گزارش شوند. گزارش آزمون گاهی اوقات با نام گواهی آزمون نیز نامیده می‌شود. گزارش آزمون باید به صورت چاپی در سربرگ آزمایشگاه ارائه شود. گزارش آزمون باید در تمام صفحه‌ها دارای شماره صفحه باشد. آزمایشگاه باید دارای روال‌های مشخصی جهت تولید و تکثیر گزارش آزمون باشد تا بر تکثیر و نگهداری گزارشات آزمون در داخل آزمایشگاه و حین انتقال نظارت شود.

[14] General

۲,۱۰,۵ گزارش آزمون

ف۲,۱۰. هر گزارش آزمون باید حداقل اطلاعات زیر را شامل شود، مگر اینکه آزمایشگاه دلایل معتبر برای انجام ندادن آن‌ها داشته باشد.

الف) عنوان (برای مثال، "گزارش آزمون")

ب) نام و آدرس آزمایشگاه، و مکانی که در آن آزمایش انجام می‌شود، اگر متفاوت از آدرس آزمایشگاه باشد.

ج) شناسه منحصر به فرد از گزارش آزمون (از قبیل شماره سریال)، و در هر صفحه یک شناسه به منظور اطمینان از اینکه صفحه به عنوان بخشی از گزارش آزمون است، باشد و شناسه‌ی واضح در پایان گزارش آزمون قرار گیرد.

د) نام و نشانی مشتری

ه) مشخصات روش استفاده شده

و) وضعیت، شرایط، و مشخصات بدون نمونه‌های آزمون

ز) تاریخ دریافت نمونه های آزمون در مواردی که اعتبار و استفاده از نتایج به دست آمده و تاریخ کارایی آزمون، حیاتی و بسیار مهم است.

ح) مراجعه به طرح نمونه‌برداری و رویه‌های استفاده شده توسط آزمایشگاه و یا بخش‌های دیگر در جایی که آن‌ها مربوط به اعتبار و یا استفاده از نتایج به دست آمده می‌باشند.

ط) نتایج آزمون، واحد اندازه گیری

ی) نام‌ها، توابع و امضاها یا شناسه معادل از اشخاص تایید کننده گزارش آزمون

ک) در موارد مورد نیاز، گزارش اثر نتایج مرتبط تنها به نمونه‌های آزمون شده

ف۳,۱۰. آزمایشگاه باید گزارش‌های ارزیابی را با دقت و شفاف، از تجزیه و تحلیل ارزیاب، شرایط آزمون، آزمون و ارزیابی نتایج و تمام اطلاعات مورد نیاز ارائه کند.

ف۴,۱۰. گزارشات ارزیابی باید تمام اطلاعات لازم برای فراهم کردن امکان انجام مجدد آزمون توسط آزمایشگاه دیگر به منظور بدست‌آوردن نتایج قابل مقایسه را فراهم کند.

برای ارزیابی یک محصول دو نوع گزارش ارزیابی ممکن است وجود داشته باشد:

الف) گزارشات ارسالی به مرکز افتا

ب) گزارشاتی که مبتنی بر قرارداد، تولید شده و برای استفاده توسط مشتری در نظر گرفته شده است.

ف۵,۱۰. گزارشات ارزیابی تولید شده برای ارائه به مرکز افتا باید مطابق الزامات مورد تایید آن مرکز باشد.

ف۶,۱۰.گزارش ارزیابی باید شامل اطلاعات کافی برای شرایط دقیق آزمون و نتایج باشد تا در آینده اگر نیاز شد و یا دوباره راجع به آن درخواست شد، مجددا تکرار شود.

ف۷,۱۰. گزارش‌های ارزیابی در آزمایشگاه باید به شکل و روش مشخص شده توسط مرکز افتا، ممیزی و وارسی شوند.

ف۸,۱۰. گزارشاتی که تنها به منظور استفادهٔ مشتری در نظر گرفته شده‌اند، باید با تعهدات ذکر شده در قرارداد آزمایشگاه مطابقت داشته باشد و آن را پوشش دهد.

ف۹,۱۰. گزارشات ارسالی به مرکز افتا باید هم به صورت چاپی (در سربرگ آزمایشگاه و ممهور به مهر و امضا) و هم به صورت الکترونیکی باشند.

ف۱۰,۱۰. گزارش‌های ارزیابی که به فرمت الکترونیکی به مرکز افتا ارائه می‌شوند، باید به طور دیجیتالی امضا شده باشند یا برای حصول اطمینان از درستی گزارش و هویت آزمایشگاهی که گزارش تولید می‌کند، کد چکیده پیام را در آن اِعمال کند.

ف۱۰،۱۱. آزمایشگاه باید ابزار امنی را برای انتقال اطلاعات لازم به مرکز افتا برای تائید امضا یا کد چکیده پیام ارائه کند.

ف۱۰،۱۲. مکانیزم‌های محرمانگی باید برای ایجاد اطمینان از اینکه گزارش ارزیابی صرفاً در اختیار گیرنده‌های مجاز قرار می‌گیرد، استفاده شوند.

ف۱۰،۱۳. آزمایشگاه بایستی دارای آیین نامه‌ها، روال‌ها و خط مشی‌های مشخص و مورد تأیید مرکز افتا جهت حفظ محرمانگی نتایج ارزیابی امنیتی محصولات باشد.

ف۱۰،۱۴. آزمایشگاه می‌باید نتایج ارزیابی امنیتی محصولات را صرفاً به مرکز افتا و تولید کننده محصول ارائه دهد و از افشاء آن نزد هر سازمان، نهاد و شخصیت حقوقی، دستگاه دولتی و خصوصی و غیره اکیداً خودداری نماید.

ف۱۰،۱۵. تغییر در گزارشات ارزیابی تهیه شده برای مرکز افتا باید با توجه به الزاماتی که از سوی آن سازمان ارائه می‌شود، انجام شود.

ف۱۰،۱۶. گزارشات آزمون برای تفسیر نتایج، برای هر آزمون باید در صورت لزوم شامل موارد زیر باشد:

الف) یک شرح از انطباق و یا عدم انطباق با الزامات و یا مشخصات در موارد مرتبط

ب) در موارد قابل اجرا، یک شرح درباره عدم قطعیت تخمین اندازه‌گیری و اطلاعاتی درباره عدم قطعیت که در گزارشات آزمون زمانی‌که وابسته به اعتبار و یا کاربرد نتایج آزمون می‌باشد و زمانی که دستورالعمل مشتری مورد نیاز است و زمانی که عدم قطعیت روی انطباق محدودیت‌های خاص تأثیر می‌گذارد، مورد نیاز است.

ت) در صورت نیاز بیان توضیحات برای رفع ابهامات

ث) اطلاعات اضافی که ممکن است برای روش خاصی، مشتریان و یا گروهی از مشتریان لازم باشد.

ح) علاوه بر الزامات ذکر شده در قبل، گزارشات آزمون که حاوی نتایج حاصل از نمونه‌برداری است باید در جایی که نیاز به تفسیر نتایج آزمون است شامل موارد زیر باشد.

۱. تاریخ نمونه‌گیری
۲. مشخصات دقیق اطلاعات، اجزای تشکیل دهنده یا محصول نمونه (شامل نام کارخانه سازنده، مدل یا نوع طراحی و شماره سریال مناسب)
۳. محل نمونه‌برداری، از جمله هرگونه نمودارها، طرح‌ها یا تصاویر
۴. یک مرجعی برای طرح نمونه‌برداری و روش‌های استفاده
۵. جزئیات شرایط محیطی در حین نمونه‌گیری که می‌تواند بر تفسیر نتایج آزمون تأثیر گذارد.
۶. هر یک از استانداردها یا دیگر مشخصات برای روش یا رویه نمونه‌برداری، و انحراف، اضافه کردن به یا حذف بر اساس مشخصات مورد نظر.

۳,۱۰,۵ نظرات و تفاسیر

ف۱۵,۱۰. زمانی‌که در آزمایشگاه برای موضوعی نیاز به نظرات و تفاسیر وجود دارد، نظرات و تفاسیر باید به صورت واضح در یک گزارش آزمون مشخص شوند.

۴,۱۰,۵ انتقال الکترونیکی نتایج

ف۱۶,۱۰. در مواردی که انتقال نتایج آزمون از طریق تلفن، تلکس، فکس یا سایر ابزارهای الکترونیکی یا الکترومغناطیسی صورت گیرد، الزامات این سند باید رعایت شود.

۵,۱۰,۵ قالب گزارش‌ها

ف۱۷,۱۰. قالبی باید برای هر نوع آزمون انجام شده، طراحی شود تا امکان سوء تفاهم و سوء استفاده به حداقل برسد.

۶,۱۰,۵ اصلاحات گزارش آزمون

ف۱۸,۱۰. اصلاحاتی که در یک گزارش آزمون نیاز است، صرفاً می‌باید با استفاده از یک سند اضافی که شامل عنوان «الحاقیه به گزارش آزمون، شماره سریال... (یا هرچیز مشخص شده دیگر)» است، انجام شود.

- اصلاحات مذکور باید تمام الزامات این سند را در برگیرد.
- در مواردی که اصلاحات در حوزه کل سند اصلی گزارش آزمون است، اصلاحات باید منحصرا قابل شناسایی باشد.

۱۱,۵ تأمین امنیت فناوری اطلاعات و ارتباطات آزمایشگاه

ف. ۱,۱۱. آزمایشگاه باید نسبت به تأمین امنیت فناوری اطلاعات و ارتباطات و حفاظت از اطلاعات مرتبط با ارزیابی امنیتی محصولات تحت نظارت مرکز افتا اقدام نماید.

ف. ۲,۱۱. آزمایشگاه موظف است، طرح‌ها و دستورالعمل‌های امن سازی آزمایشگاه و فرایندها و روال‌های مربوط به آن را به تأیید مرکز افتا رسانده و سپس به اجرایی و عملیاتی کردن آنها بپردازد.

ف. ۳,۱۱. آزمایشگاه موظف به تولید، پردازش، ذخیره سازی و نگهداری نتایج ارزیابی امنیتی محصولات در سیستم‌هایی می‌باشد که از نظر فیزیکی از شبکه اینترنت، مجزا هستند.

ف۴,۱۱. آزمایشگاه باید دارای فرایندها و روال‌های مطابق با الزامات مرکز افتا برای امحاء اطلاعات مربوط به ارزیابی امنیتی محصولات باشد.