INSO-ISO-IEC

27041

1st.Edition

2016

Identical with

ISO/IEC 27041: 2015

جمهوری اسلامی ایران

Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standards Organization

استاندارد ملی ایران –ایزو آی ای سی

۲۷۰۴۱

چاپ اول

۱۳۹۵

# فناوری اطلاعات-

# فنون امنیتی- راهنماهایی برای تضمین مناسب بودن و کفایت روش تحقیقات رخداد

# Information technology — Security techniques — Guidelines on assuring suitability and adequacy of incident investigative method

ICS: 35.040

**سازمان ملی استاندارد ایران**

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.org

**Iranian National Standardization Organization (INSO)**

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri.org

## به نام خدا

## آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد 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 وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و کسب‌وکار است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های 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.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

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

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، پیاده‌سازی بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، پیاده‌سازی استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

---

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

## کمیسیون فنی تدوین استاندارد
## «فناوری اطلاعات- فنون امنیتی- راهنماهایی برای تضمین مناسب بودن و کفایت روش تحقیقات رخداد»

| **رئیس:** | **سمت و/ یا محل اشتغال:** |
|---|---|
| ایزدپناه، سحرالسادات<br>(فوق لیسانس مهندسی فناوری اطلاعات) | رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران |
| **دبیر:** | |
| میر اسکندری، سید محمدرضا<br>(لیسانس مهندسی کامپیوتر نرم‌افزار، فوق لیسانس مدیریت اجرایی) | مدیرکل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات |
| **اعضاء:** (اسامی به ترتیب حروف الفبا) | |
| ناظمی، اسلام<br>(دکترای مهندسی کامپیوتر) | استادیار دانشگاه شهید بهشتی |
| نصیری آسایش، حمید رضا<br>(کارشناسی ارشد فناوری اطلاعات معماری سازمانی) | پژوهش‌گر دانشگاه شهید بهشتی |
| یعقوبی رفیع، کمال الدین<br>(کارشناسی ارشد فناوری اطلاعات معماری سازمانی) | پژوهش‌گر دانشگاه شهید بهشتی |
| دوست‌محمدی، وحید<br>(کارشناسی ارشد مهندسی صنایع گرایش فناوری اطلاعات) | کارشناس مرکز مدیریت راهبردی افتا |
| محمدیان، بهزاد<br>(فوق لیسانس مهندسی برق) | کارشناس مرکز مدیریت راهبردی افتا |
| ابوالقاسمی، پیمان<br>(کارشناسی ارشد مهندسی کامپیوتر) | پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) |
| ارجمند، مهدی<br>(کارشناسی ارشد مهندسی کامپیوتر) | پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) |

| | |
|---|---|
| رادمهر، وحید<br>(کارشناسی مهندسی کامپیوتر) | پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) |
| جوادزاده، غزاله<br>(کارشناسی ارشد مهندسی کامپیوتر) | پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) |
| مغانی، مهدی<br>(فوق لیسانس ریاضی کاربردی) | کارشناس تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران |

**ویراستار:**

| | |
|---|---|
| قسمتی، سیمین<br>(کارشناسی ارشد مهندسی فناوری اطلاعات) | مشاور مرکز آپا دانشگاه تربیت مدرس |

# فهرست مندرجات

**عنوان** **صفحه**

## پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- راهنماهایی برای تضمین مناسب بودن و کفایت روش تحقیقات رخداد» که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است، در چهارصد و سی‌امین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات داده مورخ ۱۳۹۵/۰۲/۲۶ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

منبع و مأخذی که برای تهیه و تدوین این استاندارد مورد استفاده قرار گرفته به توصیف زیر است:

ISO/IEC 27041: 2015, Information technology — Security techniques — Guidelines on assuring suitability and adequacy of incident investigative method

## مقدمه

### درباره این استاندارد ملی

این استاندارد ملی در پی ارائه تضمینی است که فرایند بررسی استفاده شده برای رخدادهای تحت بررسی و نتایج مورد نیاز مناسب باشد. همچنین به طور خلاصه مفهوم فرایندهای شکستن ظاهر پیچیده به مجموعه-ای از بخش‌های تفکیک ناپذیرکوچک‌تر، را که توصیه می‌شود به توسعه روش‌های بررسی ساده و در عین حال قوی کمک کند، تشریح مینماید. توصیه می‌شود این مورد به وسیله هر شخص صاحب اختیار، یا کسی که دستورالعمل می‌دهد، مدیریت می‌کند یا بررسی را هدایت می‌کند در نظر گرفته شود. توصیه می‌شود پیش از هر بررسی در زمینه اصول و فرایندها (تعریف شده در استاندارد ISO/IEC 27043:215) و آماده-سازی و طرح (تعریف شده در استاندارد ISO/IEC 27035-2) برای اطمینان از مناسب بودن روش‌های استفاده شده در فرایندهای بررسی تشریح شده در استانداردهای ISO/IEC 27037:2012 و ISO/IEC 27042:2015 به کار رود.

### رابطه با سایر استانداردها

این استاندارد ملی در نظر دارد سایر استانداردها و اسنادی که راهنمایی در مورد بررسی و آماده‌سازی تحقیقات رخدادهای امنیتی اطلاعات ارائه می‌دهند را تکمیل کند. این یک راهنمایی جامع نیست اما اصول بنیادی معینی را وضع می‌کند که در نظر دارند از ابزار، فنون، و روش‌های انتخاب شده مناسب اطمینان حاصل کند و نشان دهد برای هدف نیاز به وجود آمده مناسب هستند.

همچنین این استاندارد ملی در نظر دارد تصمیم‌گیرندگانی که نیاز به تعیین قابلیت اطمینان شواهد رقمی دارند را آگاه سازد. این استاندارد برای سازمان‌هایی که نیاز به حفاظت، تحلیل و ارائه شواهد رقمی بالقوه دارند کاربردپذیر است. این استاندارد مربوط به نهادهای تعیین‌کننده خط مشی است که روش‌های اجرایی مربوط به شواهد رقمی، اغلب به عنوان بخشی از نهاد بزرگ‌تر شواهد را ایجاد و ارزیابی می‌کنند.

این استاندارد ملی قسمتی از فرایند جامع بررسی را تشریح می‌کند که شامل نواحی موضوعی زیر است اما به این‌ها محدود نمی‌شود:

- مدیریت رخداد شامل آماده‌سازی و طرح برای بررسی
- اداره کردن شواهد رقمی
- استفاده از، موارد ناشی از، ویرایش
- سامانه‌های آشکارسازی و جلوگیری از نفوذ شامل اطلاعاتی که می‌تواند از این سامانه‌ها به دست آید.
- امنیت ذخیره‌سازی شامل پاکسازی ذخیره‌ساز
- اطمینان از مناسب بودن روش‌های بررسی برای هدف
- انجام تحلیل و تفسیر شواهد رقمی
- درک اصول و فرایندهای بررسی شواهد رقمی

- مدیریت رویداد رخداد امنیتی شامل اشتقاق شواهد از سامانه‌های شامل شده در مدیریت رویداد رخداد امنیتی
- رابطه بین اکتشاف الکترونیکی و سایر روش‌های بررسی مانند استفاده از فنون اکتشافات الکترونیکی در سایر بررسی
- حاکمیت بررسی شامل بررسی قانونی[1]

به این نواحی موضوعی در قسمتی از استانداردهای ISO/IEC زیر پرداخته شده است:

- استاندارد ISO/IEC 27037:2012

این استاندارد ملی وسایلی که در مراحل اولیه بررسی شامل پاسخ اولیه، استفاده می‌شوند را تشریح می‌کند و می‌تواند اطمینان یابد که شواهد رقمی بالقوه مناسب گرفته شده‌اند تا به بررسی اجازه دهد به طور مناسب انجام شوند.

- استاندارد ISO/IEC 27038:2014

برخی اسناد می‌توانند حاوی اطلاعاتی باشند که نباید برای برخی نهادها فاش شود. اسناد اصلاح شده می‌توانند بعد از پردازش مناسب سند اصلی به این نهادها داده شوند. فرایند حذف اطلاعاتی که نباید فاش شود «ویرایش» نام دارد.

ویرایش رقمی اسناد منطقه نسبتاً جدیدی از عملیات مدیریت سند است که مخاطره‌های بالقوه و موضوعات منحصر به فردی را بالا می‌برد. در جایی که اسناد رقمی ویرایش شده‌اند، اطلاعات حذف شده نباید قابل بازیابی باشد. بنابراین باید مراقب بود اطلاعات ویرایش شده به طور دائمی از سند رقمی حذف شوند (مثلاً نباید به سادگی در قسمت غیرقابل نمایشی سند پنهان شود).

ISO/IEC 27038:2014 روش‌هایی برای ویرایش رقمی اسناد رقمی مشخص کرده است. همچنین الزاماتی برای نرم‌افزاری که برای ویرایش استفاده می‌شود را مشخص کرده است.

- استاندارد ISO/IEC 27040:2015

این استاندارد ملی جزئیات راهنمایی فنی در مورد اینکه چگونه یک سازمان می‌تواند سطح مناسبی از کاهش مخاطره را به وسیله به کارگیری یک رویکرد اثبات شده و سازگار در طرح، طراحی، سندسازی، و پیاده‌سازی امنیت ذخیره‌سازی داده تعریف کند، را فراهم می‌کند.

امنیت ذخیره‌سازی در حفاظت (امنیت) از اطلاعاتی که ذخیره شده‌اند و در امنیت اطلاعات منتقل شده در بین پیوندهای ارتباطات همبسته با ذخیره‌سازی به کار می‌رود. امنیت ذخیره‌سازی شامل امنیت افزاره‌ها و رسانه، امنیت فعالیت‌های مرتبط با افزاره‌ها و رسانه، امنیت برنامه‌های کاربردی و خدمات، و امنیت مرتبط با کاربران نهایی در طی طول عمر افزاره‌ها و رسانه و بعد از پایان استفاده از آن‌ها می‌باشد.

راه‌کارهای امنیتی مثل رمزنگاری و پاکسازی می‌توانند بر توانایی فرد در بررسی به وسیله‌ی معرفی راه‌کار مبهم و تاریک تأثیر گذارد. آن‌ها باید پیش از انجام بررسی یا در طی آن در نظر گرفته شدند. همچنین آن‌ها

1 - Forensic

می‌توانند در حصول اطمینان از اینکه ذخیره‌سازی مواد مدرکی در طی بررسی و بعد از آن به طور مناسب آماده و امن شده‌اند، اهمیت داشته باشد.

- استاندارد ISO/IEC 27042:2015

این استاندارد ملی چگونگی طراحی و پیاده‌سازی روش‌ها و فرایندهای استفاده شده در طی بررسی به منظور دستیابی به ارزیابی مناسبی از شواهد رقمی بالقوه، تفسیر شواهد رقمی، و گزارش مؤثر یافته‌ها را تشریح می‌کند.

- استاندارد ISO/IEC 27043:2015

این استاندارد ملی اصول و فرایندهای کلیدی رایج و متضمن تحقیقات رخداد را معرفی کرده و الگو چارچوبی برای تمام مراحل بررسی فراهم می‌کند.

همچنین پروژه‌های ISO/IEC زیر نواحی موضوعی شناسایی شده در بالا را نشانی می‌دهند و می‌توانند منجر به انتشار استانداردهای مرتبط بعد از انتشار این استاندارد ملی شوند.

- استاندارد ISO/IEC 27035 (تمام قسمت‌ها)

این استاندارد ۳ قسمت دارد که رویکرد طرح و ساختاربندی شده به منظور مدیریت رخدادهای امنیتی برای سازمان‌ها فراهم می‌کند. این استاندارد از موارد زیر تشکیل شده است:

- استاندارد ISO/IEC 27035-1

این قسمت مفاهیم پایه و مراحل مدیریت رخداد امنیت اطلاعات را ارائه می‌دهد. این قسمت مفاهیم فوق را با اصولی در رویکرد ساختاربندی شده برای کشف، گزارش، ارزیابی، پاسخ و به کارگیری درس‌های آموخته شده ترکیب می‌کند.

- استاندارد ISO/IEC 27035-2

این قسمت مفاهیمی درباره طرح و آماده‌سازی پاسخ به رخداد ارائه می‌کند. مفاهیم شامل طرح و خط مشی مدیریت رخداد، تأسیس گروه پاسخگویی به رخداد، و جلسه آموزش آگاهی هستند و براساس مرحله طرح و آماده‌سازی الگو ارائه شده در استاندارد ISO/IEC 27035-1 می‌باشند. این قسمت مرحله «درس‌های آموخته شده» مدل را هم پوشش می‌دهد.

- استاندارد ISO/IEC 27035-3

این قسمت شامل مسئولیت‌ها و فعالیت‌های پاسخگویی به رخداد عملیاتی کارکنان در بین سازمان است. تمرکز ویژه‌ای به فعالیت‌های گروه پاسخگویی رخداد مثل پایشگری، اکتشاف، تحلیل و فعالیت‌های پاسخ‌گویی برای داده جمع‌آوری شده یا رخدادهای امنیتی اختصاص یافته است.

- استاندارد ISO/IEC 27050 (تمام قسمت‌ها)

این استاندارد به فعالیت‌هایی در اکتشاف الکترونیکی می‌پردازد که شامل شناسایی، حفظ، جمع‌آوری، پردازش، مرور کلی، تحلیل و تولید الکترونیکی اطلاعات ذخیره شده[1] (ESI) می‌باشد اما محدود به آن‌ها

1 - Electronically Stored Information

نیست. به علاوه راهنمایی در اندازه‌گیری به دست آمده از تولید اولیه ESI از طریق وضعیت نهایی آن، که سازمان می‌تواند برای کاهش مخاطره و هزینه متقبل شود را فراهم می‌کند. توصیه می‌شود اکتشاف الکترونیکی به یک موضوع تبدیل گردد. این استاندارد به کارمندان فنی و غیرفنی شامل شده در برخی یا تمام فعالیت‌های اکتشاف الکترونیکی مرتبط است.

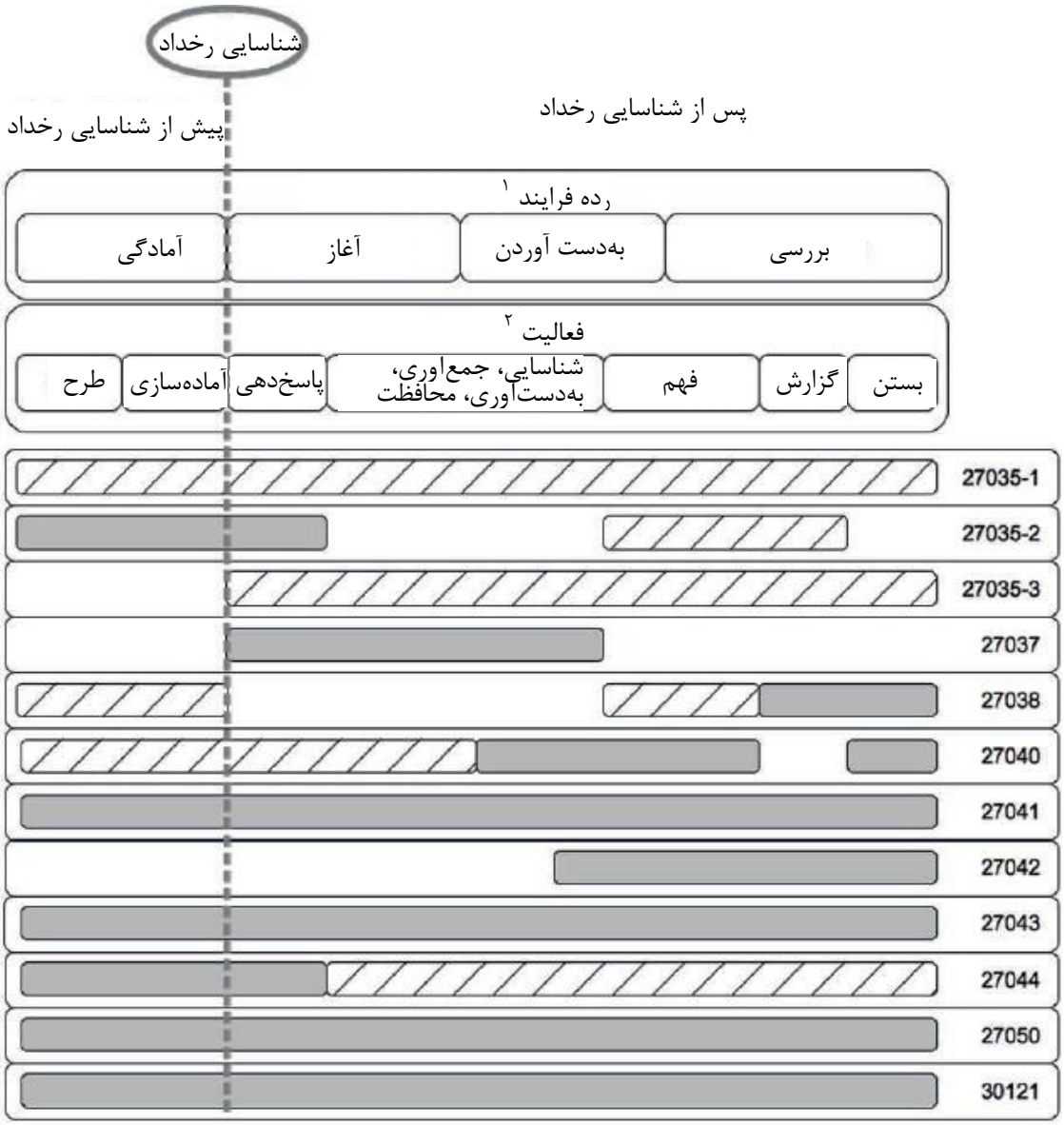
یادآوری این نکته اهمیت دارد که این راهنمایی قصد تناقض یا جایگزینی با قوانین قضایی محلی و آیین نامه‌های تنظیمی را ندارد.

اکتشاف الکترونیکی اغلب به عنوان راه‌انداز بررسی، مانند فعالیت‌های اداره کردن و کسب شواهد خدمت عمل می‌کند، به علاوه گاهی حساس بودن و بحرانی بودن داده حفاظت‌هایی مانند امنیت ذخیره‌سازی در برابر نقض داده‌ها را ضروری می‌کند.

- استاندارد ISO/IEC 30121:2015

این استانداردهای چارچوبی برای نهادهای حاکمیت سازمان‌ها (شامل مالکان، اعضای هیئت مدیره، مدیران، شرکاء، مدیران ارشد یا مشابه) در بهترین حالت برای آماده‌سازی سازمان در بررسی رقمی قبل از رخداد آن فراهم می‌کند. این استاندارد ملی در توسعه فرایندهای (و تصیمات) راهبردی مرتبط با نگهداری، در دسترس بودن، و مقرون به صرفه بودن افشاء شواهد رقمی به کار می‌رود. این استاندارد ملی برای تمام انواع و اندازه-های سازمان کاربردپذیر است. استاندارد ملی درباره آماده‌سازی راهبردی محتاط برای بررسی رقمی یک سازمان است. اعلام آمادگی قانونی اطمینان می‌یابد که یک سازمان آماده‌سازی راهبردی مرتبط و مناسب برای پذیرش رخدادهای بالقوه یک ماهیت مدرکی دارد. ممکن است فعالیت‌ها به عنوان نتیجه نقض امنیت اجتناب ناپذیر، کلاهبرداری و ادعای شهرت رخ دهد. در هر وضعیتی فناوری اطلاعات (IT) باید برای بیشینه کردن تأثیر در دسترس بودن شواهد و مقرون به صرفه بودن به طور راهبردی گسترده شود.

شکل۱ فعالیت‌های نوعی پیرامون یک رخداد و بررسی آن را نشان می‌دهد. اعداد نشان داده شده در این نمودار (مثل ۲۷۰۳۷) استانداردهای فهرست شده در بالا را مشخص می‌کنند و خط تیرها آنچه بیشتر کاربردپذیری مستقیم دارد یا تأثیری روی فرایند بررسی می‌گذارد را نشان می‌دهند (مثل تنظیم خط مشی یا ایجاد محدودیت‌ها). به هر حال توصیه می‌شود تمام آن‌ها پیش از مراحل طرح و آماده‌سازی رایزنی شوند. طبقات فرایند نشان داده شده به طور کامل در این استاندارد ملی تعریف شده‌اند و فعالیت‌های شناسایی شده مطابق با فعالیت‌های مطرح شده با جزئیات در استانداردهای ISO/IEC 27035-2، ISO/IEC 27037:2012 و ISO/IEC 27042:2015 می‌باشند.




راهنما

استاندارد می‌تواند مستقیما در این فعالیت‌ها کاربرد دارد

استاندارد حاوی اطلاعاتی است که ممکن است بر این فعالیت ها تاثیر داشته باشد و/یا به آن‌ها کمک کند.

۱- رده‌های فرایند در استاندارد ISO/IEC 27043 تعریف شده‌اند.

۲- جزییات فعالیت‌ها در استانداردهای ISO/IEC 27035-2، ISO/IEC 27037:2012 و ISO/IEC 27042 آمده است.

**شکل ۱- کاربست‌پذیری استانداردها در رده‌ها و فعالیت‌های فرایند بررسی**

# فناوری اطلاعات- فنون امنیتی- راهنماهایی برای تضمین مناسب بودن و کفایت روش تحقیقات رخداد

## ۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین و ارائه راهنماهایی برای حصول اطمینان از در این مورد که روش‌ها و فرایندهای مورداستفاده در تحقیقات رخدادهای امنیت اطلاعات، «مناسب برای هدف» است. این استاندارد حاوی به‌روش[1] در رابطه با تعریف الزامات، شرح روش‌ها و تهیه شواهد است که به‌موجب آن‌ها می‌توان نشان داد پیاده‌سازی روش‌ها می‌تواند الزامات را برآورده سازد. این استاندارد شامل چگونگی امکان استفاده از آزمون طرف سوم و فروشنده در کمک به این فرایند تضمین است.

اهداف این استاندارد به شرح زیر است:

- ارائه راهنما در زمینه به‌دست آوردن[2] و تحلیل الزامات کارکردی و غیرکارکردی مرتبط با تحقیقات رخداد امنیت اطلاعاتی (IS)[3]
- ارائه راهنما در زمینه استفاده از اعتبارسنجی به‌عنوان ابزاری برای تضمین مناسب بودن فرایندهای درگیر در بررسی،
- ارائه راهنما به منظور ارزیابی سطوح اعتبارسنجی لازم و شواهد مورد نیاز از یک اجرای اعتبارسنجی،
- ارائه راهنماهایی در زمینه چگونگی به‌کارگیری آزمون بیرونی و مستندسازی در فرایند اعتبارسنجی.

## ۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آن‌ها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

**۲-۱** استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۴، فناوری اطلاعات -فنون امنیتی -سامانه‌های (سیستم-های) مدیریت امنیت اطلاعات مرور کلی و واژگان

1 - Best practice
2 - Capture
3 - Information Security

## ۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۴، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود:

**۳-۱**

**تفکیک‌ناپذیر**[1]

انجام تنها یک کارکرد واحد است.

**یادآوری ۱-** *روشی* (۳-۱۱) برای بازیابی تمامی پرونده‌های زنده[2] از یک افزاره[3] می‌تواند تفکیک‌ناپذیر باشد اگر تنها بر روی استفاده از فرا-داده سامانه پرونده‌ها تکیه کند. بعید است که روش بازیابی تمام پرونده‌های حذف شده، تفکیک‌ناپذیر باشد، اگر نیازمند برخی روش‌های جانبی است که ساختارهای پرونده‌ی ویژه را از داده‌های موجود بر روی افزاره‌ی ذخیره‌سازی بر اساس دانش محتوای پرونده (برای مثال jpg.، png.، odt.، XML و غیره) شناسایی و استخراج می‌کنند.

**۳-۲**

**آزمون جعبه سیاه**[4]

آزمودن یک فرایند، از طریق استفادهٔ آن فرایند برای پردازش ورودی‌های شناخته شده و مقایسه نتایج با خروجی‌های پیش‌بینی شده‌ای که الزامات مرتبط با فرایند را منعکس می‌کنند.

**۳-۳**

**کارخواه**[5]

شخص یا سازمانی که به نمایندگی از او، بررسی صورت می‌گیرد.

**۳-۴**

**تایید**[6]

ارزیابی رسمی شواهد عینی موجود که به‌موجب آن‌ها یک فرایند برای یک منظور خاص مناسب است (یا مناسب باقی می‌ماند).

1 - Atomic
2 - Live files
3 - Device
4 - Black box testing
5 - Client
6 - Confirmation

**۵-۳**

**یادداشت‌های هم‌زمان[1]/ سابقه هم‌زمان[2]**

سابقه مکتوب از اقدامات و تصمیمات، که هم‌زمان با اقدامات و تصمیمات، یا تا آن‌جا که ممکن است بلافاصله بعد از آن‌ها صورت می‌گیرد.

**یادآوری ۱–** در بسیاری از حوزه‌های قضایی، لازم است که یادداشت‌های هم‌زمان، در دفاتر یادداشت شواهد و با دست و به‌صورت پاک نشدنی نوشته شوند تا به قابل قبول بودن و رد نشدن یادداشت‌ها کمک شود.

[منبع: بند ۳-۴ استاندارد ISO/IEC 27042:2015]

**۶-۳**

**آزمودن[3]**

مجموعه‌ای از فرایندها، که به‌منظور شناسایی و بازیابی شواهد رقمیِ بالقوه‌ی مرتبط از یک یا چند منبع دیگر، مورد استفاده قرار می‌گیرند.

[منبع: بند ۳-۴ استاندارد ISO/IEC 27042:2015]

**۷-۳**

**بررسی[4]**

به‌کارگیری *آزمودن‌ها* (۳-۶)، تحلیل‌ها، و تفسیرها برای کمک به درک یک رخداد است.

[منبع: ISO/IEC 27042:2015, 3.10]

**۸-۳**

**رهبر بررسی[5]**

فردی که بررسی را در سطحی راهبردی رهبری می‌کند.

[منبع: ISO/IEC 27042:2015, 3.11]

1 - Contemporaneous notes
2 - Contemporaneous record
3 - Examination
4 - Investigation
5 - Investigative lead

**۹-۳**

**گروه بررسی**[1]

تمام افرادی که به‌طور مستقیم در اجرای بررسی دخیل هستند.
[منبع: ISO/IEC 27042:2015, 3.12]

**۱۰-۳**

**بررسی‌کننده**[2]

عضو *گروه بررسی* (۳-۹)، شامل *رهبر بررسی* (۳-۸) است.
[منبع: ISO/IEC 27042:2015, 3.13]

**۱۱-۳**

**روش**

تعریف [عملیات]ی که برای تولید داده‌ها یا به‌دست آوردن اطلاعات به‌عنوان یک خروجی از ورودی‌های خاص می‌توانند استفاده شوند.

**یادآوری ۱–** به‌طور مطلوب، یک *روش* (۳-۱۱) باید *تفکیک‌ناپذیر* (۳-۱) باشد (یعنی، توصیه می‌شود که بیش از یک کارکرد را انجام ندهد) تا بتواند امکان استفاده مجدد از روش‌ها و *فرایندهای* (۳-۱۲) به‌دست‌آمده از آن‌ها را فراهم کند و میزان کار لازم برای اعتبارسنجی فرایندها را کاهش دهد.

**۱۲-۳**

**فرایند**

پیاده‌سازی عملیاتی یک *روش* (۳-۱۱) است.

**۱۳-۳**

**تهیه‌کننده**[3]

خالق یا فراهم‌کننده[4] یک *ابزار* (۳-۱۷)، شامل هر فردی که یک ابزار را اصلاح یا سفارشی می‌کند.

**یادآوری ۱–** شخص(ها) یا سازمان(های) مسئول برای خلق یا نگهداری ابزار یا سفارشی‌سازی یک ابزار، تهیه‌کننده است.

**یادآوری ۲–** تهیه نبشته‌ها[1] برای خودکارسازی کارکردهای رایجی که یک ابزار را اصلاح یا سفارشی می‌کند.

1 - Investigative team
2 - Investigator
3 - Producer
4 - Provider

**۱۴-۳**

**الزامات**

عبارتی که نیاز و محدودیت‌ها و شرایط مربوط به آن را ترجمه کرده یا بیان می‌کند

**یادآوری ۱–** الزامات در لایه‌های مختلف وجود داشته و نیاز را به شکل سطح-بالا شرح می‌دهد (برای مثال، الزام مولفه نرم‌افزاری)

[منبع: بند ۴-۱-۱۷ استاندارد ISO/IEC 29148:2011]

**۱۵-۳**

**تحلیل الزامات**

*فرایندی* (۳-۱۲) که از طریق آن درک و اولویت‌بندی *الزامات* (۳-۱۴) محقق می‌شود

**۱۶-۳**

**درآوردن الزامات**[۲]

*فرایندی* (۳-۱۲) که از طریق آن *الزامات* (۳-۱۴) برای یک فرایند کشف می‌شوند، بازنگری[۳] می‌شوند، با دقت موردبررسی قرار می‌گیرند و مستند می‌شوند

**۱۷-۳**

**ابزار**

نرم‌افزار، سخت‌افزار یا ثابت‌افزار[۴] مورد استفاده در یک *فرایند* (۳-۱۲) است

**۱۸-۳**

**اعتبارسنجی**

تایید (۳-۴)، از طریق فراهم آوردن شواهد عینی، در این مورد که *الزامات* (۳-۱۴) برای یک استفاده یا کاربرد خاص درنظرگرفته شده برآورده شده‌اند.

**یادآوری ۱–** اعتبارسنجی بر روی یک فرایند (۳-۱۲) برای حصول اطمینان از مطابقت با اهداف صورت می‌پذیرد، به‌عنوان مثال تضمین این که فرایند همان‌طور که پیاده‌سازی شده است، نتایج مورد انتظار را به شیوه‌ای سازگار، قابل تکرار و قابل تولید مجدد ایجاد می‌کند.

---

5 - Scripts
1 - Requirements capture
2 - Reviewed
3 - Firmware

[منبع: بند ۳-۱۷ استاندارد ISO/IEC 27004:2009، اصلاح‌شده- یادآوری ۱ اضافه شده است]

**۳-۱۹**

**مجموعه اعتبارسنجی**

مجموعه‌ای از آزمون‌های عینی همراه با اهداف، ورودی‌ها، و خروجی‌های به‌وضوح تعریف شده که مستقیما با *الزامات* توافق شده (۳-۱۴) برای *فرایند* (۳-۱۲) تحت *اعتبارسنجی* (۳-۱۸) مرتبط است

**۳-۲۰**

**درستی‌سنجی**[1]

*تایید* (۳-۴) از طریق فراهم آوردن شواهد عینی در این مورد که الزامات برآورده شده باشند.

**یادآوری ۱–** درستی‌سنجی تنها این تضمین را ایجاد می‌کند که یک محصول با مشخصه‌های خود مطابقت دارد.

[منبع: بند ۳-۱۸ استاندارد ISO/IEC 27004:2009، اصلاح‌شده- یادآوری اصلی حذف شده است، یادآوری ۱ اضافه‌شده است]

**۳-۲۱**

**تابع درستی‌سنجی**[2]

تابعی است که برای بررسی یکسانی دو مجموعه داده استفاده می شود.

[منبع: بند ۳-۲۵ استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳[3]، اصلاح‌شده- یادآوری‌ها حذف شدند]

**۳-۲۲**

**آزمون جعبه سفید**[4]

آزمونی که شامل بازرسی جزئیات پیاده‌سازی است

**۳-۲۳**

**دستورالعمل**[5]

شرح کامل چگونگی انجام و ثبت یک *فرایند* (۳-۱۲) است.

1 - Verification
2 - Verification Function

۳ - بر اساس منبع ISO/IEC 27037: 2012

4 - White box testing
5 - Work Instruction

[منبع: بند ۳-۱ گزارش فنی ISO/TR 10013:2001، اصلاح‌شده- تغییر یافته از حالت جمع به مفرد، *کار* به *فرایند* تغییر یافته است]

## ۴ کوته‌نوشت‌ها

| | | |
|---|---|---|
| ATA | AT Attachment | پیوست AT |
| SATA | Serial ATA | ATA متوالی |
| USB | Universal Serial Bus | همه‌گذر |

## ۵ توسعه و تضمین روش

### ۵-۱ مرورکلی

تضمین مناسب بودن و کفایت روش‌های تحقیقات رخداد به منظور نشان دادنِ شفاف این نکته می‌تواند مورد تقاضا قرار گیرد که کدام‌یک از روش‌های مورد استفادهٔ بررسی‌کننده مناسب برای هدف بررسی بوده است و کدام‌یک از آن‌ها در معرض خطاهای غیرقابل‌قبول یا عدم قطعیت قرار داشتند. شواهد رقمی منتج از کاربرد روش‌های نامطمئن را می‌توان به‌عنوان روش‌های ذاتا عیب دار و چالش‌برانگیز منظور کرد که می‌توانند در راستای اهداف تحقیق بی‌استفاده باشند.

این استاندارد یک مدل تضمین را ارائه می‌دهد. این مدل شامل تمامی مراحل توسعه آن دسته از فعالیت‌ها است که بررسی را از شناسایی اولیه تا استقرار و نگهداشت تشکیل می‌دهند (همان‌طور که در استاندارد ISO/IEC 27042:2015 شرح داده شده است).

### ۵-۲ اصول عمومی[1]

توصیه می‌شود روش‌های تضمین مناسب بودن و کفایت روش‌های تحقیقات رخداد از یک مدل مناسب از قبیل مدل طرح-اجرا-بررسی-اقدام[2] پیروی کنند، که در استاندارد ملی ایران شماره ۹۰۰۱: سال ۱۳۸۸ مورد استفاده قرار گرفت، در راستای تضمین این که تمامی فرایندها، دست کم زمانی که به‌کار گرفته می‌شوند، مورد بازنگری قرار می‌گیرند.

### ۵-۳ مدل عمومی توسعه و استقرار[3]

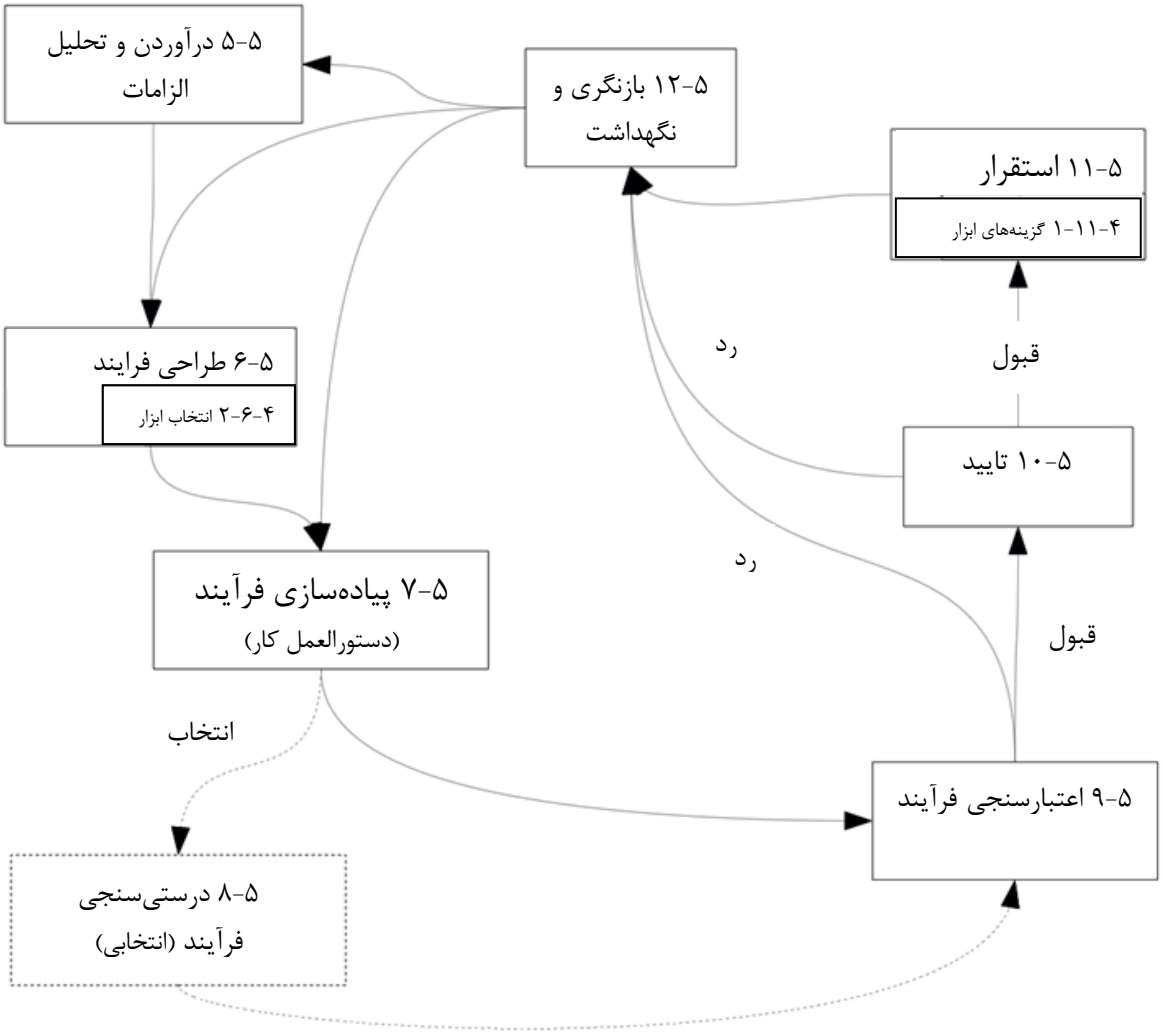
توصیه می‌شود پیش از استقرار فرایند برای استفاده در بررسی، فرایند مناسب توسعه طی شود تا از مناسب

1 - General Principles
2 - Plam-Do-Check-Act
3 - General Development and deployment model

بودن آن برای هدف اطمینان حاصل شود. شکل ۲ مراحل نوعی را در این فرایند نشان می‌دهد که به شرح زیر است:

- درآوردن و تحلیل الزامات
- طراحی فرایند
- پیاده‌سازی فرایند
- درستی‌سنجی فرایند (اختیاری و غیرضروری)
- اعتبارسنجی فرایند
- تایید
- استقرار
- بازنگری و نگهداشت

هرکدام از این مراحل به شرح زیر با جزئیات بیشتر مورد بحث قرار می‌گیرند.




**شکل ۲- فرایند توسعه و استقرار، شامل مراحل تضمین**

### ۵-۴ مراحل تضمین

توصیه می‌شود تضمین در مدل استقرار بالا طی مراحل کلیدی تضمین زیر لحاظ شود:

- درآوردن و تحلیل الزامات
- اعتبارسنجی فرایند
- تایید
- بازنگری و نگهداشت

**یادآوری**- راهنمایی‌های بیشتر در مورد اجرای این مراحل در شرح مدل‌های تضمین در بند ۵ ارائه شده است.

### ۵-۵ درآوردن و تحلیل الزامات

#### ۵-۵-۱ اصول عمومی الزامات

پیش از طراحی یک فرایند به منظور استفاده در آزمودن، توصیه می‌شود مجموعه مناسبی از الزامات تولید شود، از سوی مشتری پذیرفته شود و با توجه به شیوه مطلوب ثبت شود. توصیه می‌شود این مجموعه الزامات از الزامات شناسایی‌شده برای بررسی کامل به دست آید و ممکن است شامل هر دو نوع الزام کارکردی و غیرکارکردی باشد.

هر الزام یک قابلیت، مشخصه یا عامل کیفیت ضروری را تعریف می‌کند. توصیه می‌شود هر یک عبارت الزام دارای این صفات باشد: ضروری[1]، غیر وابسته به پیاده‌سازی[2] (یعنی تنها چیزی که لازم است را بیان کند، نه چگونگی برآوردن الزام)، واضح[3]، کامل، منفرد[4] و سازگار با دیگر الزامات موجود در مجموعه.

الزامات از لحاظ مقصود و نوع خواصی که بازنمایی می‌کنند، متغیر است. آن‌ها را می‌توان در انواع مشابه به‌منظور تحلیل و درستی‌سنجی گروه‌بندی کرد. مثال‌هایی از انواع الزامات شامل موارد زیر می‌شوند:

- **کارکردی**- کارکردها و کار در نظر گرفته شده به منظور انجام را شرح داده و شامل نکاتی چون ورودی‌ها و خروجی‌های پیش‌بینی شده است؛
- **عملکرد**- گستره، چگونگی و شرایط انجام کارکرد یا وظیفه را تعریف می‌کند؛
- **واسط**- چگونگی تعامل راهکار با سامانه‌های بیرونی یا چگونگی تعامل عناصر موجود در راهکار (شامل عناصر انسانی) با همدیگر را تعریف می‌کند.
- **فرایند**- رعایت قوانین محلی و فرایندها یا الزامات اجرایی را شامل می‌شود؛
- **غیرکارکردی**- چگونگی در نظر گرفتن یک راهکار را تعریف می‌کند شامل الزامات کیفی از قبیل قابلیت حمل، اطمینان‌پذیری، قابلیت نگهداشت و امنیت یا الزامات عوامل انسانی از قبیل ایمنی، کارایی یا بهداشت و سلامت.

1 - Necessary
2 - Implementation-free
3 - Unambiguous
4 - Singular

علاوه بر تمامی الزامات ضروری، توصیه می‌شود فهرست‌های تهیه شده از الزامات شامل تعاریف واضحی از کرانه‌های عملیات مرتبط با شواهد رقمی بالقوه پیش‌بینی شده و فرایندهای بررسی مربوطه باشد (برای مثال، اندازه بیشینه پرونده، بیشینه و کمینه تعداد مقادیر ورودی).

ممکن است فهرست جدیدی از الزامات برای تمامی بررسی در حال انجام تنظیم شود تا از تحقق صحیح الزامات این مورد آزمودن اطمینان حاصل شود. استفاده از یک رویکرد یکپارچه برای طراحی مستلزم یک اعتبارسنجی قابل ملاحظه بوده و درنتیجه به کاربر توصیه می‌شود تا جایی که امکان دارد آن دسته از مراحل تفکیک‌ناپذیر از پیش طراحی شده را انتخاب کند که با پارامترهای پویای ورودی قابل تعریف از سوی کاربر مطابق است.

با این روش، تغییرات منحصربه‌فرد الزامات معمولا محدود به پارامترهای ورودی آن مورد، خاص خواهد بود و درنتیجه اعتبارسنجی این مورد خاص قطعا محدود به پارامترهای عرضه شده به مورد تحت بررسی محدود می‌شود و نه به کارکرد یا فرایند اصلی که توصیه می‌شود در گام آماده‌سازی طراحی شده باشد.

**مثال**- درحالی‌که جستجوی کلیدواژگان خاص مستقیما به مورد تحت بررسی وابسته است، فرایند پالایه[1] کلیدواژه توصیه می‌شود، درصورتی‌که به‌طور صحیح طراحی شده باشد، یک فرایند تفکیک‌ناپذیر باشد که مستقل از کلید واژگان مورد استفاده است. محیطی که مستلزم اعتبارسنجی هر مورد خاص منحصربه‌فرد است همان تعریف صحت کلید واژگان اعمال‌شده است (یعنی خطای عدم قطعیت تعریف نشده در طراحی کاربری اصطلاحات جستجوی خاص قرار خواهد گرفت، برای مثال تنها برای جستجوی "Joe Blogs" منابع مرتبط با "Joe Bloggs"، "Mr Blogs"، "J.Blogs"، "Joe"، "Joey" و غیره منظور نمی‌شوند).

توصیه می‌شود رخداد تحت بررسی به‌خوبی شناسایی و تعریف شده و محدودیت‌های مرتبط با دامنه بررسی را نیز لحاظ کند. این توصیه نیز داده می‌شود که منابع شواهد رقمی بالقوه و سوالات مورد نظر به منظور پاسخ شناسایی شوند. منابع مخاطره و اثرات بالقوه آن‌ها بر روی بررسی، کارکنان و سامانه‌ها نیز توصیه می‌شود شناسایی شود.

توصیه می‌شود به محض شناسایی الزامات بررسی، گروه بررسی در گام بعدی الزامات را برای آن دسته از آزمودن‌ها، تحلیل‌ها و فرایندها توسعه دهد که بررسی را تشکیل خواهند داد (به استاندارد ISO/IEC27042:2015 مراجعه شود).

### ۵-۵-۲ الزامات کارکردی

الزامات کارکردی آن دسته از الزامات است که مستقیماً ناشی از نیازهای بررسی بوده و از سوی کاربران فرایند پیش‌بینی می‌شوند. این الزامات چگونگی اجرای فرایند را تعریف نمی‌کنند بلکه شامل نکاتی از جمله ورودی‌ها و خروجی‌های پیش‌بینی شده است. توصیه می‌شود تمامی الزامات کارکردی از سوی بررسی محقق گردند.

**مثال**- نیاز به پردازش یک نوع خاص از سامانه پرونده یک الزام کارکردی است همان‌طور که مستقیماً ناشی از یک منبع

1 - Filter

شواهد رقمی بالقوه می‌شود.

### ۵-۵-۳ درستی‌سنجی الزامات

به‌کارگیری یک شیوه به منظور درستی‌سنجی الزامات این نکته را تضمین خواهد کرد که الزامات تعیین شده به‌خوبی شکل گرفته‌اند و این که نیازهای روش بررسی به شکل صحیحی بیان شده‌اند. در واقع درستی سنجی الزامات با تحلیل الزامات درآورده‌شده به منظور شناسایی مشکلات مرتبط می‌باشد از قبیل الزامات متناقض، از دست رفته، ناقص، مبهم، ناسازگار یا نامتجانس. توصیه می‌شود هر مشکل شناسایی شده قبل از رفتن به مرحله تضمین بعدی، حل شود.

## ۵-۶ طراحی فرایند

### ۵-۶-۱ مرور کلی

توصیه می‌شود طراحی یک فرایند تمامی الزامات شناسایی شده را به‌عنوان نتیجه‌ای از مراحل درآوردن و تحلیل الزام در نظر بگیرد. این طراحی توصیه می‌شود جزئیات چگونگی پیاده‌سازی روش را ارائه دهد، الزامات غیر کارکردی مورد قبول را در نظر بگیرد و در نقطه‌ای قرار گیرد که در آن توصیه می‌شود انتخاب ابزار صورت پذیرد. نیازی نیست که طراحی جزئیات دقیق هر عنصر فرایند را تعیین کند بلکه توصیه می‌شود به‌وضوح جریان فعالیت و مواد مربوط به شواهد را از یک مرحله به مرحله بعدی شناسایی کند.

### ۵-۶-۲ انتخاب ابزار

طی گام طراحی، توصیه می‌شود هر ابزاری که ممکن است در فرایند شرکت داشته باشد شناسایی شده و نقش(های) آن‌ها در فرایند منتج شناسایی شود. درجایی که ابزار متعددی می‌توانند کارکرد یکسانی را در فرایند انجام دهند، شناسایی بخشی یا تمامی از این ابزار ممکن است مفید باشد تا از تغییر در محیط های عملیاتی ممانعت به عمل آید (برای مثال مسدودسازهای[1] نوشتن ممکن است واسط‌های مختلفی را ارائه دهند از قبیل ATA، SATA، USB و غیره). با این حال، دقت کافی باید منظور شود تا این نکته نیز تضمین شود که مجاز شمردن الزامات متغیر با این روش باعث تأثیر معکوس بر روی ماهیت تفکیک‌ناپذیر فرایند نخواهد شد.

توصیه می‌شود با استفاده از فرایند مستندشده، یک گروه ابزار به منظور استفاده تعریف شود، همراه با مخاطره شناسایی شده و در صورت امکان واجد شرایط به منظور توابع تفکیک‌ناپذیر خاص مربوطه به هر کدام از ابزار فهرست شده.

1 - Blocking

### ۵-۶-۳ ارزیابی عدم قطعیت و مخاطره

تمامی ابزار، چه مبتنی بر سخت‌افزار یا مبتنی بر نرم‌افزار، درمعرض سطحی از خطا قرار دارند. این یک واقعیت غیرقابل انکار است که آن‌ها برخی مؤلفه‌های تولیدشده به شکل فیزیکی[۱] است و در یک رواداری از پیش تعریف شده از یک نقطه مطلوب طراحی و پیاده‌سازی شده‌اند که نمی‌توان آن را ٪۱۰۰ کامل تضمین کرد. این خطا ممکن است در محدوده‌ای از نسبتاً بالا تا بسیار کم قرار گیرد، ولی در هر صورت وجود خواهد داشت و نمی‌توان آن را به‌طور کامل حذف کرد، تنها می‌توان آن را کنترل کرده و منظور کرد.

توصیه می‌شود آشنایی بررسی‌کننده[۲] با ابزار پیشنهادی یا فرایند پیشنهاد شده نیز منظور شود، چراکه اگر یک کاربر آشنایی کمتری با ابزار یا فرایند داشته باشد، شانس بیشتری وجود خواهد داشت که خطاهای کنترل نشده دیگری نیز رخ دهند. آموزش مؤثر و آزمون کارایی منظم فنونی است که از لحاظ کمک به کمینه سازی این نوع خاص از خطا مورد قبول عام قرار گرفته اند.

این خطاها در کل به‌عنوان شاخصه‌های عدم قطعیت هر عنصر یا مؤلفه یک فرایند شناخته می‌شوند و به زبان ساده می‌توانند به‌عنوان نقاط قوت یا ضعف فرایند منظور گردند.

شاخصه‌های عدم قطعیت به طور معمول در ماهیت یک سامانه خطی اضافه می‌شوند، از قبیل مدل توصیف‌شده، و درنتیجه به طور معمول همگام و به نسبت تعداد فرایندهای مورد استفاده افزایش خواهند یافت.

در راستای جبران مسئله فوق، توصیه می شود برخی فرایندهای همپوشان قدرتمند و متناسب طراحی شوند تا این نکته نیز تضمین شود که این فرایندها منشأ تمامی شواهد رقمی یافت شده را تقویت خواهند کرد.

پیش از استفاده از یک ابزار یا روش تعیین شده به منظور هدایت بررسی، توصیه می‌شود بررسی‌کنندگان اثرات احتمالی تمامی نقاط ضعف توالی فرایند کامل انتخاب‌شده را در نظر بگیرند. از طریق به‌کارگیری یک فرایند انتخاب صحیح و تحلیل یا ارزیابی‌های قوی مخاطره مستند شده، درک منطقی نقاط ضعف یک فرایند باعث می‌شود که این خطاها به‌طور مؤثر کنترل شوند.

استفاده از عناصر تفکیک‌ناپذیر اعتبارسنجی شده در یک توالی فرایند نیز می‌تواند کمک چشمگیری در تسهیل درک و کنترل این موارد عدم قطعیت باشد و همان دلیل اصلی در نظرگرفتن روش‌های تضمین با جزئیات کامل در این سند است.

در نهایت، این نکته حائز اهمیت است که اگرچه یک فرایند خاص ممکن است یک نقطه ضعف ناشناخته یا شدیدی را نشان دهد، اما ضرورتاً این ضعف را تا حد کفایت از بین نخواهد برد. درواقع در برخی موارد، اگر فرایند تنها به منظور تکمیل یک کار تقاضا شده وجود داشته باشد، احتمالاً این امر بی‌ارزش شناخته شود.

---

۱ - نرم افزار روی رایانه فیزیکی مقیم می شود، بنابراین از هر دو نوع خطای سخت افزاری و نرم افزاری موثر می شود.

3 - Investigator

## ۵-۷ پیاده‌سازی فرایند

### ۵-۷-۱ مرور کلی

پس از تکمیل فرایند، توصیه می‌شود به شکل یک دستورالعمل مستند شده با جزئیات پیاده‌سازی شود که دستورالعمل‌های گام به گامی برای اجرای صحیح هر مرحله از فرایند ارائه می‌دهد. طی این مرحله، تصمیمات نهایی در مورد انتخاب ابزار (برای مثال انتخاب بین رونوشت‌های جایگزین نوع ابزار مشابه) ممکن است در راستای بهبود فرایند درآورده شوند.

### ۵-۷-۲ گزینش ابزار- راهنمایی به منظور استقرار

درجایی که طراحی فرایند شامل فهرستی از ابزاری است که ممکن است به منظور انجام کارکردهای یکسان یا مشابه است، توصیه می‌شود دستورالعمل راهنمایی (به زیربند ۵-۶-۲ مراجعه شود) را در مورد چگونگی گزینش ابزار از سوی بررسی‌کننده برای شرایط مواجه شده طی آزمودن، ارائه دهد. با این حال، توصیه می‌شود دقت کافی به عمل آید که تضمین مجاز شمردن تغییر در این روش باعث تأثیر معکوس بر روی ماهیت تفکیک‌ناپذیر فرایند نمی‌شود.

نگهداشت یک ثبات مخاطره[1] که شامل ارزیابی‌های مخاطره و عدم قطعیت برای ابزار در دسترس است، می‌تواند به گزینش ابزار کمک کند. یک ابزار می‌تواند با یک ورودی تهی در این ثبات شروع به کار کند اما توصیه می‌شود جدید بودن و ارزیابی نشدن ابزار با جزئیات به‌عنوان یک مخاطره در نظر گرفته شود.

ابزاری که در واقع مناسب‌ترین ابزار برای شرایط خاص نباشد ممکن است همچنان برای استفاده تا زمان ارزیابی آن گزینش شود و استفاده از فرایند تعریف شده همراه با مخاطره‌های مرتبط به وضوح تعریف شود.

**یادآوری**- یک ابزار ممکن است به این دلیل گزینش شود که بهترین گزینه در میان مجموعه‌ای از راهکارهای عموماً ضعیف است یا به این دلیل که تنها ابزار در دسترس است که می‌تواند هر شکلی از نتیجه قابل استفاده را تولید کند.

## ۵-۸ درستی‌سنجی فرایند

### ۵-۸-۱ اصول عمومی درستی‌سنجی

درستی‌سنجی، سطحی از تضمین را فراهم می‌کند که یک فرایند یا ابزار با مشخصات خود مطابقت دارد. این امر تضمین نخواهد کرد که کار به شیوه مورد نظر در زمینه یک بررسی یا فرایند کامل انجام می‌شود. شواهد درستی‌سنجی در برابر الزاماتی که شبیه به الزامات کارکرد مورد نظر است توصیه می‌شود به‌عنوان یک شاخص اولیه به کار گرفته شوند که به موجب آن ابزار یا فرایند ممکن است به منظور استقرار در زمینه بررسی مناسب باشند، اما نه یک تضمین کامل که الزامات را به منظور کارکرد مورد نظر محقق خواهد ساخت. توصیه می‌شود درستی‌سنجی به‌عنوان یک بخش اختیاری اما به‌طور بالقوه مفید از تضمین در نظر

1 - Maintenance of a risk register

گرفته شود.

### ۵-۸-۲ درستی‌سنجی فرایندها

پس از توسعه دستورالعمل، توصیه می‌شود دستورالعمل با طراحی و شواهد تهیه‌شده مقایسه شود تا چگونگی مطابقت آن با طراحی به اثبات برسد. طراحی ممکن است به منظور انعکاس تغییرات پیاده‌سازی صورت گرفته طی تولید دستورالعمل اصلاح شود (برای مثال نتیجه‌ای از رفتارهای پیش‌بینی نشده یا ابزار جدید). درستی‌سنجی به طور معمول با استفاده از «آزمون جعبه سفید» صورت می‌پذیرد تا امکان مقایسه با طراحی فراهم شود.

### ۵-۸-۳ درستی‌سنجی ابزارها

ابزارها از سوی کاربر، تهیه‌کننده یا طرف سوم قابل درستی‌سنجی است. در جایی که ابزار از سوی تهیه‌کننده یا طرف سوم درستی‌سنجی می‌شود، درستی‌سنجی به طور معمول مبتنی بر الزامات طراحی برای آن ابزار خواهد بود. یک درستی‌سنجی صورت گرفته از سوی طرف سوم یا تهیه‌کننده تنها به‌عنوان بخشی از اعتبارسنجی مفید است، درصورتی‌که اطلاعات کامل در مورد درستی‌سنجی فراهم شود، شامل الزامات طراحی که بر اساس آن‌ها درستی ابزار سنجیده می‌شود. اگر این الزامات طراحی را بتوان در الزامات مرتبط با به‌کارگیری ابزار در فرایند مورد نظر نگاشت، داده‌های درستی‌سنجی هماهنگ کننده می‌توانند شواهد جزئی را در مورد اعتبارسنجی برای آن دسته از مراحل فرایند فراهم سازند که در آن‌ها ابزار دخیل است. درستی-سنجی به نوبه خود برای تحقق اعتبارسنجی یک فرایند کافی نیست همان‌طور که درستی‌سنجی روشی را در نظر نمی‌گیرد که در آن کاربر ابزار قصد استفاده از ابزار را در فرایند دارد.

## ۵-۹ اعتبارسنجی فرایند

### ۵-۹-۱ اصول عمومی اعتبارسنجی

اعتبارسنجی نشان می‌دهد که فرایند تعریف شده در دستورالعمل الزامات مورد توافق با مشتری را محقق می‌سازد. اعتبارسنجی مستقیماً پیاده‌سازی تعریف شده توسط دستورالعمل را در نظر نمی‌گیرد بلکه شواهدی را فراهم می‌کند که بر اساس آن‌ها فرایند خروجی‌های صحیح را برای مجموعه تعریف شده از ورودی‌ها تولید می‌کند. در صورت امکان، فرایند اعتبارسنجی توصیه می‌شود شرایط مرزی و نرخ‌های خطا را نیز تعیین کند. به طور معمول، فرایند اعتبارسنجی از طریق «آزمون جعبه سیاه» صورت خواهد گرفت تا از این نکته اطمینان حاصل شود که دانش جزئیات پیاده‌سازی بر هدایت آزمون یا تأثیرگذاری بر روی نتایج اثرگذار نیست.

یک برنامه اعتبارسنجی و داده‌های مربوطه توصیه می‌شود به‌طور مستقل از مراحل طراحی و پیاده‌سازی تولید شوند و توصیه می‌شود که صرفاً بر الزامات مورد توافق مبتنی باشند.

**یادآوری**- فرایندهایی که از ابزار یا روش‌های نامعتبر استفاده می‌کند را می‌توان اعتبارسنجی کرد اگر نتایج سازگاری را فراهم کند (برای مثال الزامات مربوط به قابلیت تکرار و قابلیت تکثیر توصیف‌شده در استاندارد ملی ایران شماره ۲۷۰۳۷: سال

.(۱۳۹۳

### ۵-۹-۲ اعتبارسنجی جامع

اعتبارسنجی جامع به شیوه‌ای از اعتبارسنجی اشاره می‌کند که یک فرایند را تحت تمامی شرایط ممکن مورد آزمون قرار می‌دهد (برای مثال بر اساس تمامی پیکربندی سخت‌افزاری ممکن برای تمامی ورودی‌های احتمالی). این نوع اعتبارسنجی به‌عنوان تأیید ضروری منظور نمی‌شود و احتمالاً برحسب زمان و منابع مورد نیاز شیوه‌ای هزینه‌بر باشد. در جایی که یک فرایند یک بخش کلیدی از چندین تحلیل را تشکیل می‌دهد، و احتمال استقرار به‌طور منظم را دارد، تأیید اعتبار جامع می‌تواند ضروری باشد اما ممکن است برای فرایندهایی اعمال نشود که در چندین نوع مختلف از بررسی توسط گروه‌های بررسی مختلف مورد استفاده قرار می‌گیرند.

در شرایطی دیگر (برای مثال، برای یک فرایند «one-off» که به منظور حل یک مسئله فوری و نه محتمل به منظور استفاده مجدد منظور می‌شود)، یک اعتبارسنجی کافی می‌تواند مناسب باشد. توصیه می‌شود اعتبارسنجی پس از استقرار انجام نشود مگر آن که به طور قطعی ضروری باشد. برخی انواع ساده اعتبارسنجی پیش از استقرار را توصیه می‌شود همیشه امتحان کرد (بر اساس مجموعه محدودی از الزامات) اما اعتبارسنجی پس از استقرار کامل‌تر را توصیه می‌شود هرچه سریع‌تر انجام داد، به‌خصوص اگر فرایند به منظور استفاده در آینده در نظر گرفته شده باشد.

**مثال**- فرایند بازیابی داده‌ها از کارت‌های مغناطیسی ممکن است به‌طور جامع اعتبارسنجی شود همان‌طور که قالب‌های نسبتاً کمی برای مرتب‌سازی داده‌ها بر روی چنین کارت‌هایی وجود دارد.

### ۵-۹-۳ اعتبارسنجی کافی[1]

اعتبارسنجی کافی به شیوه‌ای از اعتبارسنجی اشاره دارد که مبتنی بر الزامات کارکردی و غیر کارکردی مورد توافق برای شرایط مربوط به زمان بررسی است. اعتبارسنجی یک شیوه از لحاظ پیکربندی‌های نرم‌افزاری و سخت‌افزاری که به بررسی مرتبط نیستند، ضروری نیست، همچنین در نظر گرفتن اعتبارسنجی برای داده‌هایی که پردازش نخواهند شد نیز ضرورتی ندارد.

اعتبارسنجی کافی شیوه‌ای است که نشان می‌دهد فرایند نتایج صحیح را برای نوع ورودی‌های مواجه شده در بررسی مورد نظر تولید می‌کند، یعنی اعتبارسنجی کافی نشان می‌دهد که یک فرایند برای یک کارکرد ویژه مناسب است همان‌طور که از سوی الزامات شناسایی شده تعریف می‌شود.

### ۵-۹-۴ فرایندهای کاملاً اعتبارسنجی شده

فرایندی که اعتبار آن مورد تأیید قرار گرفته است را ممکن است به‌عنوان فرایند کاملاً اعتبارسنجی شده برای کارکرد تعریف شده در برنامه اعتبارسنجی شرح کرد. توصیه می‌شود که یک فرایند به طور معمول

1 - Sufficient validation

مستقر نشود تا زمانی که به‌طور کامل اعتبار آن مورد تأیید قرار گیرد.

### ۵-۹-۵ عدم تأیید اعتبار

اگر اعتبار فرایندی مورد تأیید قرار نگیرد، توصیه می‌شود الزامات، طراحی و پیاده‌سازی بازنگری شده و به شکل صحیحی اصلاح شوند. به‌محض تکمیل، فرایند توصیه می‌شود مجدداً به منظور اعتبارسنجی مورد آزمون قرار گیرد.

### ۵-۱۰ تأیید

آخرین مرحله قبل از استقرار فرایند همان تأیید است که به‌طور رسمی ارزیابی می‌کند که آیا فرایند الزامات مورد توافق را محقق ساخته و شواهد لازمی را فراهم می‌کند که بر اساس آن‌ها فرایند به منظور استفاده در بررسی مناسب است.

به منظور انجام تأیید، توصیه می‌شود شواهد اعتبارسنجی برای فرایند از لحاظ الزامات مورد توافق برای کارکرد مورد نظر فرایند مورد بررسی قرار گیرند. یک فرایند ممکن است تنها در صورتی تأیید شود که به‌طور کامل اعتبار آن مورد تأیید قرار گرفته است.

فرایندی که اعتبار آن قبلاً مورد تأیید قرار گرفته است را ممکن است بدون اعتبارسنجی بیشتر مورد تأیید قرار داد اگر اعتبار آن به‌طور کامل برای بررسی فعلی مورد تأیید قرار گیرد. این امر شامل فرایندهایی است که در معرض اعتبارسنجی بیرونی قرار گرفته‌اند.

تأیید می‌تواند گام نهایی اعتبارسنجی یا اعتبارسنجی مجدد باشد یا می‌تواند مرحله‌ای را تشکیل دهد که به‌نوبه خود یک ثبت رسمی را تهیه می‌کند که قبلاً شواهد اعتبارسنجی را تهیه کرده و از بررسی قبلی برای بررسی فعلی مناسب است.

### ۵-۱۱ استقرار

وقتی فرایند مورد قبول واقع شد، می‌توان آن را به منظور استفاده در آزمودن‌ها استقرار داد که بررسی را تشکیل می‌دهند. توصیه می‌شود تمامی تخلفات صورت گرفته از نتایج مورد نظر یا رفتارها را درآورده و اقدامات اصلاحی اعمال گردند. جایی که اقدامات اصلاحی با یک تغییر برای فرایند سروکار داشته یا تخلف از رفتار پیش‌بینی شده با نتایج اعتبارسنجی قبلی متناقض است، ممکن است اعتبارسنجی مجدد تقاضا شود.

#### ۵-۱۱-۱ گزینش ابزار

طی استقرار یک فرایند، بررسی‌کننده ممکن است مجبور به گزینش ابزار از میان چندین نوع ابزار باشد که کارکرد یکسان یا مشابهی را فراهم می‌سازد. اگرچه توصیه می‌شود دستورالعمل شامل راهنمایی در مورد چگونگی گزینش ابزار باشد اما توصیه می‌شود بررسی‌کننده نیز گزینش ابزارهای صورت گرفته را به طور کامل درآورد و عواملی را حفظ کند که بر روی گزینه‌ها تأثیر گذاشته‌اند.

### ۵-۱۲ بازنگری و نگهداشت

پیرو استقرار فرایند، توصیه می‌شود عملکرد آن مورد بازنگری قرار گیرد تا هرگونه الزام فراموش شده یا تغییراتی شناسایی شوند که ممکن است به منظور مقابله با تغییرات به منظور ابزار مورد استفاده لازم شوند (برای مثال موارد ارتقا اجباری به دلیل تغییر در بن‌سازه‌ها[1]، شرایط پایان زندگی[2] و غیره). پس از بازنگری، ممکن است درآوردن و تحلیل الزامات، طراحی فرایند یا مراحل پیاده‌سازی فرایند اصلاح شوند تا یک عمل نگهداشت را تولید نمایند. هر مرحله‌ای که مورد استفاده قرار گیرد، خود آن مرحله و مراحل آتی باید کامل شوند تا اطمینان حاصل شود که اعتبارسنجی فرایند اصلاح‌شده را می‌توان تأیید کرد.

## ۶ مدل‌های تضمین

### ۶-۱ مرور کلی

در راستای تامین سطح بیشتری از اطمینان از این که فرایندها به شکل صحیحی برای کاربرد مورد نظر خود مناسب است، در زمینه مراحل تضمین، مراحل تضمین خاص تا جایی که امکان دارد توصیه می‌شود مستقل از توسعه فرایندها صورت پذیرند (یعنی توسط افرادی به غیر از توسعه دهندگان صورت پذیرد). در راستای تحقق این مهم، توصیه می‌شود گام‌های لازم برداشته شود تا اطمینان حاصل شود مراحل تضمین به شیوه‌ای انجام می‌شوند که عدم تاثیرپذیری از نکات طراحی و پیاده‌سازی را تضمین می‌کنند.

این بخش آن دسته از مدل‌های تضمین را مورد بحث قرار می‌دهد که به منظور کمک به حصول اطمینان از معرفی نکردن تاثیرات غیر ضروری، قابل استفاده هستند. در کل، تضمین ممکن است در داخل سازمانی صورت پذیرد که از فرایندها استفاده می‌کنند (به زیربند ۶-۲ مراجعه شود) توسط سازمان دیگر (به زیربند ۶-۳ مراجعه شود) استفاده خواهند کرد یا ترکیبی از دو سازوکار (به زیربند ۶-۴ مراجعه شود) را به کار خواهند گرفت. هر مدلی که مورد استفاده قرار گیرد، توصیه می‌شود شواهد مناسب تضمین (به بند ۷ مراجعه شود) را تولید و حفظ کند.

### ۶-۲ تضمین درون‌سازمانی[3]

تضمین درون‌سازمانی را ممکن است برای هر فرایند بررسی که در داخل سازمان استقرار می‌یابند اعمال کرد. توصیه می‌شود سازمان از یک مجموعه اعتبارسنجی استفاده کند که معرف کاربردهای مورد نظر خودش برای فرایندها است، آزمون‌های مربوطه را انجام دهد و از طریق تأیید رسمی، مناسب بودن فرایندها برای هدف مورد نظر را ثبت کند.

1 - Platforms
2 - End of life conditions
1 - In-house assurance

### ۶-۳ تضمین برون‌سازمانی

در این مدل تضمین، مسئولیت هدایت اعتبارسنجی به نهاد دیگری سپرده می‌شود.
در جایی که نهاد بیرونی تنها در حال هدایت اعتبارسنجی است، توصیه می‌شود سازمان پیاده کننده فرایند و نهاد اعتبارسنج در مورد الزامات و مجموعه اعتبارسنجی قبل از هدایت اعتبارسنجی و بازنگری به‌عنوان بخشی از مرحله تأیید به توافق برسند.
در جایی که نهاد بیرونی فرایندها را تولید کرده است، سازمان پیاده‌سازی کننده فرایند توصیه می‌شود دقت کافی داشته باشد تا اطمینان حاصل شود که یک اعتبارسنجی کافی، بر اساس الزامات تأیید، ایجاد شده است تا معیارهای تأیید برای فرایند ایجاد شود. جزئیات الزامات و مجموعه اعتبارسنجی توصیه می‌شود از نهاد تأیید کننده اعتبار به دست آید.

### ۶-۴ تضمین ترکیبی

در مدل ترکیبی تضمین، ترکیبی از دو مدل تشریح شده در بالا (درون‌سازمانی و برون‌سازمانی) مورد استفاده قرار می‌گیرد. این امر معمولا در شرایطی رخ می‌دهد که یک فرایند تولیدشده به شکل بیرونی قرار است با برخی اصلاحات به منظور الزامات پیاده‌سازی شده و استقرار یابد تا الزامات محلی تحقق یایند. ممکن است نیاز باشد نتایج اعتبارسنجی بیرونی با اعتبارسنجی اضافیِ درون سازمانی تکمیل شود تا شواهدی را فراهم شود که فرایند، الزامات اصلاح‌شده را برآورده سازد.

**مثال**- فرایند اعتبارسنجی‌شدهٔ منتشر شده برای تصویرگیری از لوح‌های مغناطیسی می‌تواند برای تصویرگیری از ذخیره‌سازها با حالت ثابت استفاده شود. اگر هیچ شواهد اعتبارسنجی خارجی معتبری در دسترس نیست، توصیه می‌شود فرایند اصلاح شد، در معرض اعتبارسنجی درون‌سازمانی اضافی قرار گیرد.

## ۷ تولید شواهد به منظور تضمین

### ۷-۱ مرور کلی

درصورتی که شواهد رقمی برای هدف مورد نظر مناسب نباشند؛ می‌توانند چالش‌هایی در زمینه روش‌های مورد استفاده برای تولید داشته باشند. به این دلیل، این نکته حائز اهمیت است که شواهد تناسب برای هدف را بتوان تولید کرد. این امر را می‌توان با اعمال مراحل تضمین (به زیربند ۵ مراجعه شود) و نگهداشت از طریق سوابق فرایند تضمین، برآورده کرد. یک روش برای تولید این شواهد تضمین در زیر شرح داده شده است.

### ۷-۲ آماده‌سازی پیش از اعتبارسنجی[1]

پیش از آن که اعتبارسنجی صورت پذیرد، توصیه می‌شود یک برنامه اعتبارسنجی و نمونه‌های مربوطه (برنامه و

1 - Pre-validation preparation

نمونه‌ها باهم مجموعه اعتبارسنجی را تشکیل می‌دهند) ایجاد شوند. در راستای جلوگیری از تناقض حاصل از دانش پیاده‌سازی و فرضیات صورت گرفته، توصیه می‌شود مجموعه اعتبارسنجی از سوی طرفی تکمیل شود که در طراحی، پیاده‌سازی و درستی‌سنجی فرایند دخالتی ندارد. در غیر این صورت، توصیه می‌شود فرایند مورد استفاده به منظور اعتبارسنجی به‌وضوح و یکنواخت مستند شود به‌طوری‌که ممکن است از سوی یک طرف مستقل به منظور ارزیابی بی‌طرفی مورد بازنگری قرار گیرد.

طرح اعتبارسنجی به طور عادی مجموعه‌ای از آزمون‌های جعبه سیاه را تعریف خواهد کرد که مستقیما به الزامات مورد توافق نگاشته می‌شوند. هر آزمون ورودی‌هایی که باید ارائه شود و خروجی‌های مورد انتظار را بیان می‌کند. توصیه می‌شود آزمون‌ها فعالانه با هدف فرایندهای آزمون-تنش صورت پذیرند، شامل ابزاری که می‌توانند در آن فرایندها حضور یابند، در راستای کسب اطمینان از این مسئله که فرایندها به حد کافی قدرتمند بوده و مناسب برای هدف هستند.

توصیه می‌شود یک بررسی نهایی بر روی مجموعه اعتبارسنجی صورت پذیرد تا اطمینان حاصل شود این مجموعه به منظور برآورده ساختن الزامات عنوان‌شده کافی و مناسب است. در موقعیت‌هایی که مجموعه‌های اعتبارسنجی طرف سوم باید مورد استفاده قرار گیرند، این امر از اهمیتی خاص برخوردار است. وقتی یک عبارت واضح تولید نمی‌شود که بر اساس آن مجموعه اعتبارسنجی مطابق با مورد توافق است، اعتبارسنجی ممکن است به شکل ناقص منظور شود و درنتیجه ممکن است فرایندهای مربوطه به‌عنوان فرایندهای نامعتبر اظهار شوند. توصیه نمی‌شود این بررسی فقط توسط طرف سوم صورت پذیرد بلکه از سوی سازمانی نظارت شود که مسئول اداره کردن نتایج هر بررسی است.

### ۷-۳ تولید شواهد اعتبارسنجی

وقتی مجموعه اعتبارسنجی مورد تایید قرار گرفته است، توصیه می‌شود فرایند، با توجه به دستورالعمل، برای هر آزمون تعریف شده در مجموعه اعتبارسنجی، با استفاده از نمونه‌های اعتبارسنجی متناظر انجام شود. توصیه می‌شود یک ردیف ثبتی شامل خروجی هر آزمون باشد (یعنی قبول یا رد) به همراه جزئیات هر مشکل مواجه شده یا تغییرات لازم به‌عنوان نتیجه‌ای از فرایند اعتبارسنجی. توصیه می‌شود این ردیف ثبتی شامل جزئیات مجموعه اعتبارسنجی مورد استفاده بوده و شواهد اعتبارسنجی را تشکیل دهد.

### ۷-۴ نگهداشت اعتبارسنجی

توصیه می‌شود مجموعه‌های اعتبارسنجی و شواهد اعتبارسنجی به‌طور دوره‌ای مورد بازنگری قرار گیرند تا اطمینان حاصل شود همچنان برای کاربردهای درنظرگرفته شده در فرایندهای مربوطه مناسب هستند. توصیه می‌شود فرایندها مورد بازنگری قرار گیرند تا اطمینان حاصل شود شواهد آن‌ها در زمینه اعتبارسنجی همچنان صحیح است و این که به شکل مناسبی معتبر باقی می‌مانند.

فرایندی که دیگر به شکل مناسبی معتبر نیست یا دیگر دارای شواهد جاری در زمینه اعتبارسنجی نیست (برای مثال به دلیل آن که تاریخ بازنگری قبول شده است یا به دلیل تغییرات در الزامات غیرکارکردی) توصیه می‌شود به‌عنوان فرایند فاقد اعتبار منظور شود تا زمانی که اعتبارسنجی مجددا رخ دهد.

اگر یک مجموعه اعتبارسنجی اصلاح یا به‌روزرسانی شود (برای مثال به دلیل تغییرات در الزامات کارکردی یا غیرکارکردی)، تمامی فرایندهای اعتبارسنجی‌شده با استفاده از این مجموعه توصیه می‌شود بررسی شوند تا تعیین شود آیا مجموعه اعتبارسنجی تجدیدنظر شده اعمال شده است یا خیر. اگر مجموعه اعتبارسنجی تجدیدنظرشده قابل اجرا نباشد، فرایندها از طریق استفاده از مجموعه اعتبارسنجی اصلی معتبر باقی می‌مانند. اگر مجموعه اعتبارسنجی تجدیدنظرشده برای فرایندهای فعلی قابل اجرا باشد، توصیه می‌شود با استفاده از مجموعه اعتبارسنجی تجدیدنظرشده مورد اعتبارسنجی مجدد قرار گیرند.

### ۷-۵ اعتبارسنجی آزمودن‌ها

آزمودن را در صورتی می‌توان معتبر شمرد که اعتبار تمامی فرایندهای تشکیل دهنده آزمودن مورد تایید قرار گیرند. انجام یک اعتبارسنجی مجزا برای آزمودن به منظور افزایش اطمینان مناسب بودن و کفایت ممکن است ضروری باشد، به‌خصوص در شرایطی که فرایندهای مختص آزمودن (برای مثال انجام تغییرات جزئی بر روی خروجی از یک فرایند یا انجام تحلیل به منظور مناسب ساختن آن برای ورودی فرایند دیگر) معرفی شده باشند. توصیه می‌شود دقت کافی صورت پذیرد تا اطمینان حاصل شود اعتبارسنجی آزمودن تا جایی که امکان دارد، کامل است.

آزمون شایستگی (به استاندارد ISO/IEC 17043:2010 مراجعه شود) را ممکن است به منظور تهیه درجه بیشتری از تضمین مناسب بودن و کفایت آزمودن‌ها مورد استفاده قرار داد، البته توصیه می‌شود به‌عنوان جایگزینی برای تضمین مناسب به‌کار گرفته نشود همان‌طور که آزمون شایستگی معمولا به آزمودن کاربرد فرایندها در شرایط آزمون محدود می‌پردازند.

### ۷-۶ اعتبارسنجی بررسی

بررسی که تنها شامل بررسی‌های اعتباریافته است را می‌توان به‌عنوان آزمودن معتبر منظور کرد.

بررسی ممکن است شامل مراحلی باشند که در آن‌ها خروجی‌های فرایندها و آزمودن‌ها مستلزم تفسیر بوده و این امر ممکن است وابسته به صلاحیت بررسی‌کننده باشد. بنابراین، توصیه می‌شود بررسی مطابق با هدف در نظر گرفته شود که در آن آزمودن‌ها و فرایندهای منتج به اطلاعات واقعی به‌طور کامل اعتبارسنجی شده‌اند.

شواهد صلاحیت کارکنان و آزمون شایستگی باعث فراهم ساختن سطح دیگری از تضمین می‌شود که بررسی مطابق با اهداف است.

# پیوست الف

# (آگاهی‌دهنده)

# مثال‌ها

## الف-۱ دستورالعمل

| | |
|---|---|
| فرایند/فعالیت | ۰۰۱: تصویربرداری از لوح سخت رابط فناوری پیشرفته‌ی متوالی[1] (SATA) |
| هدف | تولید رونوشت مدرکی از لوح سخت |
| گزارش به | تحلیل‌گر شواهد رقمی |
| قانون‌گذاری و خط‌مشی‌ها | خط‌مشی اداره کردن شواهد، قانون‌گذاری محلی، استاندارد ملی ایران شماره ۲۷۰۳۵: سال ۱۳۹۲، استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳، استاندارد ISO/IEC 27042، استاندارد ISO/IEC 27041 |
| تجهیزات موردنیاز | وفق دهنده[2] واسط SATA، منبع تغذیه SATA، مسدودکننده نوشتن SATA (سخت‌افزاری یا نرم‌افزاری)، ابزار تصویربرداری (نرم‌افزار+ایستگاه کاری مربوطه یا افزاره تصویربرداری سخت‌افزاری)، افزارهٔ ذخیره‌ساز «بی‌بار» که به حد کافی برای پذیرش تصویر در قالب انتخابی بزرگ است. |
| صلاحیت کارکنان | مطابق با استاندارد UK e-crime NOS CO.3 «درآوردن و حفظ شواهد الکترونیک بالقوه» یا تعریف صلاحیت در استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳ |
| شایستگی | آموزش‌دیده یا باتجربه در زمینه استفاده از تجهیزات منتخب و این فرایند است. |
| فرایند | بررسی مهروموم‌ها و ایجاد استمرار. جداسازی افزاره منبع از بسته‌بندی |
| | ثبت شناسه افزاره و مشخصات آن همان‌طور که بر روی برچسب‌ها بیان شده است |
| | کسب اطمینان از این که مسدودسازی نوشتن فعال است و اتصال افزاره به واسط مناسب. اقدامات ثبت شود. |
| | ثبت شناسه افزاره و مشخصات همان‌طور که توسط ابزار تعیین شده است. |
| | درستی‌سنجی این که رسانه ذخیره‌سازی مقصد دارای ظرفیت کافی است. |
| | از تابع درستی‌سنجی (به استاندارد ملی ایران شماره ۲۷۰۳۷: سال ۱۳۹۳ مراجعه شود) به منظور ایجاد «امضا» برای افزاره استفاده می‌کند. نتایج ثبت شود. |
| | تصویربرداری با استفاده از ابزار مناسب و بررسی خطاها طی فرایند را تکمیل می‌کند. اقدامات و نتایج ثبت شود. |
| | در پایان فرایند، استفاده از تابع درستی‌سنجی به منظور ایجاد «امضا» برای تصویر و کسب اطمینان از این که با افزاره اصلی مطابقت دارد، یا محاسبه اختلافات (برای مثال به دلیل خطاها). اقدامات و نتایج ثبت شود. |
| | در صورت بروز خطاها، تعیین این که آیا خطا در تصویر یا افزاره اصلی قرار دارد یا خیر و پیگیری فرایند برای آن موقعیت انجام شود. |
| | اگر خطایی یافت نشد، قطع ایمن افزاره اصلی و بسته‌بندی مجدد، پیرو روال صحیح استمرار انجام |

1 - Serial Advanced Technology Attachment
2 - Adapter

| | |
|---|---|
| | شود. اقدامات ثبت شود. |
| | اگر خطایی یافت نشد، قطع ایمن افزاره اصلی و بسته‌بندی مناسب به منظور آزمودن آتی انجام شود. اقدامات ثبت شود. |
| | بازگرداندن افزاره مبدا به محل نگهداری شواهد. اقدامات ثبت شود. |
| | تسلیم افزاره اصلی به محل نگهداری شواهد. اقدامات ثبت شود. |

**الف-۲ برنامه اعتبارسنجی**

| | |
|---|---|
| فرایند (دستورالعمل) درنظرگرفته شده به منظور اعتبارسنجی | ۰۰۱: تصویربرداری از لوح سخت[1] SATA |
| روش اعتبارسنجی | ۱- رانه‌های[2] دارای کارکرد کامل<br>الف- نمونه معرف رایج‌ترین انواع رانه‌ها از لحاظ تولیدکننده و ظرفیت از میان جمعی از رانه‌های خوش‌نام انتخاب شود.<br>ب- آماده‌سازی رانه‌ها با نوشتن داده‌های معلوم در هر کدام (برای مثال رشته کامل رانه با استفاده از "dd" برای نوشتن صفرها، سپس بخش‌بندی و نصب سامانه‌عامل).<br>دستورالعمل به منظور تولید یک رونوشت از هر رانه اعمال شود.<br>پ- تابع درستی‌سنجی به منظور آزمودن رانه و رونوشت برای بررسی صحت تصاویر اعمال شود.<br>ت- دستورالعمل پیش‌نمای اعتباریافته برای منبع و رونوشت به منظور بررسی معادل بودن محتویات اعمال شود.<br>۲- رانه‌های آسیب‌دیده<br>الف- نمونه معرف رایج‌ترین انواع رانه‌ها از لحاظ تولیدکننده و ظرفیت از میان جمعی از رانه‌های بدنام انتخاب شود.<br>ب- از دستورالعمل تشخیصی اعتباریافته به منظور استقرار و درآوردن مناطق آسیب بر روی رانه استفاده شود.<br>پ- از دستورالعمل پیش نمای اعتباریافته به منظور درآوردن محتویات هر رانه استفاده شود.<br>ت- دستورالعمل تصویربرداری به منظور تولید یک رونوشت از هر رانه به نوبت اعمال شود.<br>ث- دستورالعمل پیش‌نمای اعتباریافته به منظور به دست آوردن و درآوردن محتویات هر رونوشت اعمال شود.<br>ج- مقایسه محتویات رونوشت با محتویات رانه اصلی، در واقع کسب اطمینان از این که مناطق آسیب‌دیده به شکل مناسبی به‌کاربرده شده‌اند (یعنی توصیه می‌شود هر بلوک خسارت‌دیده بر روی رانه مبدا منجر به یک بلوک تهی در رونوشت شود) |
| معیارهای موفقیت اعتبارسنجی | ۱- برای رانه‌های دارای کارکرد کامل، رونوشت توصیه می‌شود نتیجه یکسانی را از تابع درستی‌سنجی در مقایسه با رانه اصلی تولید کند. محتویات رانه مبدا و رونوشت توصیه |

1 - Hard disk
2 - Drives

| | |
|---|---|
| | می‌شود یکسان باشند وقتی دستورالعمل پیش‌نمای اعمال می‌شود.<br>۲- برای رانه‌های آسیب‌دیده، تمامی داده‌های قابل خواندن بر روی رانه مبدا توصیه می‌شود در محل معادل در رونوشت ظاهر شوند. محتویات رانه مبدا و رونوشت توصیه می‌شود معادل یکدیگر باشند وقتی دستورالعمل پیش‌بین اعمال می‌شود. |
| نسخه: ۰۰۱ | تاریخ تهیه: ۱۲/آوریل/۲۰۱۲ |
| آخرین بررسی: ۱۱/آوریل/۲۰۱۳ | موعد بازنگری: ۱۲/آوریل/۲۰۱۴ |

### الف-۳ شواهد اعتبارسنجی

| شماره مرجع | V001 | تاریخ | ۱۳/آوریل/۲۰۱۳ |
|---|---|---|---|
| دستورالعمل تحت اعتبارسنجی | | ۰۰۱: تصویربرداری از رانه سخت[1] SATA | |
| روش اعتبارسنجی/نسخه | | ۰۰۱: تصویربرداری از رانه سخت SATA / ۰۰۱ | |
| آزمون | شرح آزمون | نتیجه | خروجی |
| ۱ | روش ۱ برای WD5000AJS (Caviar SE) با شماره متوالی WCAPW0863110 اعمال شد. رانه‌ها پاک شد و ویندوز ۷ بر روی یک افراز نصب شد. | Drive MD5: 853f9d81e22a4e-03f92aa61171471516<br><br>Copy MD5: 853f9d81e22a4e-03f92aa61171471516<br><br>پیش نمای‌ها: سلسله مراتب محتویات و پرونده یکسان است، ۱۰۰<br>پرونده‌های نمونه‌برداری شده یکسان است. | قبول |
| . | . | . | . |
| . | . | . | . |
| . | . | . | . |
| ۹۹ | روش ۲ برای WD5000 AJS (Caviar SE) با شماره متوالی WCAPW0862110 اعمال شده. این رانه دارای بد سکتور[2] در بخش‌های ۶۴، ۱۰۳۵، ۹۱۱۹، ۹۱۲۰، ۹۱۲۱، ۹۱۲۲ است | برنامه تشخیصی WD بلوک‌های آسیب دیده را به شرح فهرست تایید کرد.<br>فرایند تصویربرداری بلوک‌های آسیب دیده را به شرح فهرست گزارش کرد.<br>به منظور اطلاع قبلی: سلسله مراتب محتویات و پرونده‌ها یکسان است.۹۹<br>پرونده‌های نمونه‌برداری شده یکسان است.<br>یکی از پرونده‌های نمونه‌برداری شده از سکتور ۹۱۲۰ استفاده کرد و یکسان | قبول |

1 - Hard drive
2 - Bad sector

| | | | |
|---|---|---|---|
| | | نبود.<br>سکتورهای رونوشت که متناظر با سکتورهای آسیب‌دیده است تهی است. | |
| نسخه: ۰۰۱ | | تاریخ تهیه: ۱۲/آوریل/۲۰۱۲ | |
| آخرین بررسی: ۱۱/آوریل/۲۰۱۳ | | موعد بازنگری: ۱۲/آوریل/۲۰۱۴ | |

**الف-۴ بیانیه تایید**

| | |
|---|---|
| مرجع بررسی | INT/001 |
| الزامات | تعیین این که آیا رانه‌های سخت در ایستگاه‌های کاری استاندارد حاوی داده‌های صفحه گسترده است<br>تولید نسخه‌های رونوشت از شواهد و پرونده‌های سامانه همراه با داده‌های صفحه گسترده<br>بازیابی داده‌های صفحه گسترده نسخه‌های رونوشت از شواهد و پرونده‌های سامانه |
| فرایندها/ دستورالعمل‌های موردنظر به منظور استقرار | شواهد اعتبارسنجی و تاریخ |
| ۰۰۱: تصویربرداری از رانه‌های سخت SATA<br>۰۰۲: ارزیابی رانه‌های سخت SATA با پرونده‌های سامانه‌ای NTFS<br>۰۰۳: بازیابی داده‌های صفحه گسترده از پرونده‌های سامانه‌ای NTFS | V001: ۱۳/آوریل/۲۰۱۳<br>V002: ۰۱/دسامبر/۲۰۱۲<br>V006: ۱۲/نوامبر/۲۰۱۲ |
| بیانیه تایید | الزامات فرایندها با الزامات بررسی هم‌خوانی دارند. فرایندها مورد آزمون کافی قرار گرفته‌اند تا شواهد کافی را به منظور اعتبارسنجی فراهم سازند. بنابراین، این‌جانب تایید می‌کنم که فرایندهای توصیف‌شده فوق برای استقرار در این بررسی مناسب است. |
| نام | E.Lestrade |
| امضا | |
| تاریخ | ۱۴/آوریل/۲۰۱۳ |

## کتاب‌نامه

[۱] استاندارد ملی ایران شماره ۱۷۰۲۴: سال ۱۳۸۶، ارزیابی انطباق - الزامات کلی برای موسسه‌های گواهی کننده اشخاص

[۲] استاندارد ملی ایران شماره ۱۷۰۴۳: سال ۱۳۹۳، ارزیابی انطباق-الزامات عمومی آزمون مهارت

**[3]** ISO/IEC/IEEE 29148:2011, Systems and software engineering — Life cycle processes — Requirements engineering

[۴] استاندارد ملی ایران شماره ۱۷۰۲۵: سال ۱۳۸۶، الزامات عمومی برای احراز صلاحیت آزمایشگاه‌های آزمون و کالیبراسیون

**[5]** ISO/IEC 27004:2009, Information technology — Security techniques — Information security management — Measurement