



بسمه تعالی

# آیین‌نامه ساماندهی خدمات افتا

مرکز مدیریت راهبردی افتا

سازمان فناوری اطلاعات

سال ۱۳۹۴

## پیشگفتار

با رشد روز افزون تهدیدات در فضای فناوری اطلاعات، مسئله امنیت جایگاه ویژه‌ای پیدا نموده است. در این راستا تولیدکنندگان محصولات فناوری اطلاعات، در صدد تولید محصولاتی هستند که با تهدیدات موجود مقابله نماید. در نتیجه وجود مرجع تائید کننده جهت حصول اطمینان مشتریان از عملکرد امنیتی محصولات، امری لازم و ضروری می‌باشد.

مرکز افتا و سازمان فناوری اطلاعات به عنوان مرجع تائید کننده براساس روال‌ها و خط‌مشی‌های موجود برای محصولات، گواهی امنیتی صادر می‌نمایند. در سند «تداوم گواهی: راهنمای نگهداری و ارزیابی مجدد» ساختار، فرایندها، روال‌ها، نقشها و تعاملات فی مابین آنها پس از صدور گواهی را شرح می‌دهد.

## فهرست

## مقدمه

در راستای اجرایی سازی بند سوم از راهبرد دوم سند افتا در ارزیابی امنیتی محصولات فتا، «تداوم گواهی: راهنمایی برای نگهداری و ارزیابی مجدد» جهت ساماندهی گواهی صادر شده برای محصولات فتا مبتنی بر استاندارد ارزیابی امنیتی معیار مشترک[1] و سایر استانداردها و دستورالعمل‌های ابلاغی، از سوی مرکز افتا تهیه گردیده است. هدف از «تداوم گواهی: راهنمایی برای نگهداری و ارزیابی مجدد»، ارائه الزامات لازم جهت حفظ گواهی، ارزیابی مجدد و تحلیل آسیب‌پذیری‌های محصول دارای گواهی می‌باشد، تا ارزیابی امنیتی توسط آزمایشگاه‌ها را به حداقل برساند. این سند یکی از مجموعه اسناد تهیه شده توسط مرکز افتا برای شرح چگونگی عملکرد «طرح ارزیابی امنیتی» جهت تداوم گواهی امنیت محصول می‌باشد و شامل پنج فصل اصلی به شرح ذیل می‌باشد:

فصل اول، به معرفی اصطلاحات و تعاریف پرداخته و اهداف «تداوم گواهی: راهنمایی برای نگهداری و ارزیابی مجدد» را شرح می‌دهد.
فصل دوم رویکرد و روال‌های نگهداری، ارزیابی مجدد و تحلیل آسیب‌پذیری محصول تائید شده را شرح می‌دهد.
فصل سوم چگونگی دسته‌بندی تغییرات محصول را شرح می‌دهد.
فصل چهارم چگونگی تحلیل اثر تغییرات را شرح می‌دهد.
فصل پنجم ساختار گزارش تحلیل اثر تغییرات را شرح می‌دهد.

# ۱ کلیات

## ۱,۱ اصطلاحات

مرجع اصطلاحات بکار رفته در این سند، سند «طرح ارزیابی امنیتی» می‌باشد.

[1] ISO 15408 (Common Criteria)

## ۲,۱ اهداف تداوم گواهی

این سند تعریف «طرح ارزیابی امنیتی» مرکز افتا در زمینه‌ی نگهداری و ارزیابی مجدد محصولات می‌باشد که تحت عنوان فرآیند «تداوم گواهی» نامبرده می‌شود و روالهای لازم بعد از دریافت گواهی را شرح می‌دهد.
هدف از فرآیند تداوم گواهی، قادر نمودن تولیدکنندگان در ارائه‌ی به موقع و کارامد محصولات معتبر به جامعه بین المللی (مصرف کنندگان) می‌باشد.
اعطای گواهی استاندارد ارزیابی معیار مشترک بر این موضوع دلالت دارد که تمام کارهای لازم برای ارزیابی صورت گرفته و هدف ارزیابی تمام الزامات تضمین را برآورده نموده است، همچنین مرکز افتا نسبت به برآورده نمودن اهداف امنیتی در نظر گرفته شده برای محصول یا سامانه، توسط آن محصول اطمینان حاصل نموده است.
فرآیند تداوم گواهی رویکردی برای به حداقل رساندن ارزیابی امنیتی توسط آزمایشگاه است، براساس این رویکرد در رابطه با تغییرات صورت گرفته در محصول تائید شده تصمیم‌گیری و نیاز به ارزیابی مجدد محصول بررسی می‌گردد. برای درخواست تداوم گواهی محصول، نباید از مدت زمان تعیین شده در گواهی گذشته باشد و به ازای هر هدف ارزیابی تغییر یافته یکبار باید این فرآیند انجام شود. همچنین تولید کننده موظف است تا هر ساله گزارش تحلیل آسیب پذیری محصول خود را برای سازمان فناوری اطلاعات ارسال نماید.

## ۳,۱ نقش‌ها در فرآیند تداوم گواهی

به منظور برقراری امنیت در محصولات فناوری اطلاعات، مرکز افتا طرحی را تحت عنوان «طرح ارزیابی امنیتی» تدوین نموده که سند «تداوم گواهی» بخشی از روال‌ها و الزامات این طرح را تعریف نموده است. شرکای اصلی «طرح ارزیابی امنیتی» عبارتند از:

- تولید کننده

تولید کننده محصول یا پروفایل حفاظتی، از سازمان فناوری اطلاعات درخواست ارزیابی محصول یا پروفایل حفاظتی می‌نماید. تولید کننده‌ی هدف ارزیابی در فرآیند تداوم گواهی مسئول موارد زیر است:

- تولید هدف ارزیابی بروز شده
- آزمون رگرسیون هدف ارزیابی بروز شده
- بروزرسانی تمام مدارک تحت تاثیر تغییرات هدف ارزیابی تائید شده
- انجام تحلیل اثر تغییرات هدف ارزیابی تائید شده، مستند نمودن نتایج در گزارش تحلیل اثر
- تفویض کامل فرآیند تداوم گواهی به مرکز افتا و سازمان فناوری اطلاعات ایران
- گزارش تحلیل آسیب‌پذیری

- آزمایشگاه

آزمایشگاه براساس سند «اعتباربخشی آزمایشگاه» و توسط مرکز افتا اعتباربخشی و تائید می‌شود تا براساس استاندارد ارزیابی امنیتی معیار مشترک و با استفاده از متدلوژی ارزیابی معیار مشترک، ارزیابی امنیتی انجام دهد.

در فرآیند تداوم گواهی، مرکز افتا مستقیماً در تعامل با تولید کننده است و آزمایشگاه نقش صریحی در این فرآیند ندارد. با این حال تولید کننده ممکن است درخواست خدماتی از آزمایشگاه یا مشاوره برای فرآیند تداوم گواهی داشته باشد.

- مرکز افتا

به عنوان یک نهاد دولتی بالاترین سطح در استاندارد ارزیابی معیار مشترک است که آزمایشگاه‌های ارزیابی را اعتبارسنجی و ارزیابی محصولات را نظارت می‌نماید. برای اطلاع بیشتر از مسئولیت‌های مرکز به سند «طرح ارزیابی امنیتی» مراجعه شود.

مسئولیت‌های مرکز افتا در فرآیند تداوم گواهی عبارتند از:

- اطمینان یافتن از مستند شدن تغییرات هدف ارزیابی در گزارش تحلیل اثر تغییرات، همچنین تحلیل نمودن اثر تغییرات رخ داده
- تائید عمده بودن یا اندک بودن تغییرات
- مستند نمودن هر آنچه که از بررسی و تحلیل فرآیند تداوم گواهی حاصل آمده
- در صورت اندک بودن تغییرات؛ تولید گزارش نگهداری و ضمیمه نگهداری سازگار با نتایج مستند شده در گزارش تحلیل اثر تغییرات
- بررسی گزارش تحلیل آسیب‌پذیری

- سازمان فناوری اطلاعات

به عنوان یک نهاد دولتی همراه با مرکز افتا بالاترین سطح در استاندارد ارزیابی معیار مشترک است که مسئول صدور گواهی برای محصول تائید شده توسط مرکز و منتشر نمودن اسناد عمومی مربوطه در سایت سازمان می‌باشد.

مسئولیت‌های سازمان در فرآیند تداوم گواهی عبارتند از:

- اطلاع‌رسانی روال‌ها و خط‌مشی‌های «طرح ارزیابی امنیتی»
- انتشار گزارشات اعتبارسنجی و صدور گواهی معیار مشترک برای ارزیابی‌های موفقیت آمیز

- انتشار و نگهداری لیست محصولات معتبر، ارائه جزئیات تمام محصولات و پروفایل‌های حفاظتی ارزیابی شده و گواهینامه‌های صادر شده

### ۴,۱ ساختار سند

مجموعه اسنادی که توسط مرکز افتا تدوین شده و این سند تکمیل کننده آنهاست عبارتند از:

سند ۱: طرح ارزیابی امنیتی

سند ۲: سند نظامنامه کیفیت

سند ۳: راهنمای اعتبارسنج

سند ۴: راهنمای آزمایشگاه‌ها

سند ۵: راهنمای تولیدکننده

سند ۷: راهنمای نوشتن پروفایل حفاظتی/سند هدف امنیتی

سند ۸: راهنمای اعتباربخشی آزمایشگاه‌ها

### ۵,۱ مفاهیم

مفاهیم استفاده شده در این رویکرد عبارتند از:

- محصول **تائید شده**، به نسخه‌ای از محصول اشاره دارد که ارزیابی شده و گواهی برای آن صادر شده است.
- محصول **تغییر یافته**، به نسخه‌ای از محصول اشاره دارد که با نسخه تائید شده متفاوت می‌باشد.
- محصول **نگهداری شده**، محصول تغییر یافته که تحت روال نگهداری است و گواهی محصول تائید شده برای آن نیز اعمال می‌گردد.
- **ضمیمه نگهداری**، اشاره به ضمیمه‌ای دارد که به گواهی محصول تائید شده در سایت سازمان اضافه می‌گردد. ضمیمه نگهداری، لیست کننده‌ی نسخه‌هایی از محصول است که در فاز نگهداری قرار گرفته‌اند.
- **گزارش تحلیل اثر تغییرات**، اشاره به گزارشی دارد که نتایج تحلیل اثر تغییرات محصول تائید شده را ثبت می‌نماید. این گزارش توسط تولیدکننده‌ای که درخواست حفظ گواهی نموده، تولید می‌شود. تولید کننده می‌تواند برای تولید این گزارش از مشاورانی از آزمایشگاه یا خارج از آن استفاده نماید.
- **گزارش نگهداری**، به گزارش عمومی اشاره دارد که تمام تغییرات صورت گرفته در محصول که در روال نگهداری پذیرفته شده‌اند را شرح می‌دهد. این گزارش توسط تولید کننده تهیه و سپس توسط مرکز افتا مورد بررسی قرار گرفته و نهایی می‌شود و بر روی سایت سازمان منتشر می‌شود.

- **گزارش تحلیل آسیب پذیری** گزارشی است که هرساله پس از صدور گواهی توسط تولیدکننده برای مرکز افتا تولید می‌شود. در این گزارش برطرف نمودن آسیب‌پذیری‌های کشف شده پس از صدور گواهی تشریح می‌شود.
- **مدارک تولیدکننده،** اشاره به تمام اطلاعات و مستنداتی است که تولیدکننده جهت ارزیابی محصول خود تهیه و ارائه داده است.
- **ارزیابی مجدد،** اشاره به فرآیندی دارد که تشخیص می‌دهد تغییرات صورت گرفته در محصول نیاز به ارزیابی مستقلی دارد. فرآیند ارزیابی مجدد حداکثر استفاده را از نتایج ارزیابی‌های قبلی خواهد داشت.
- **نگهداری،** فرآیندی که تعیین می‌کند تغییرات صورت گرفته در محصول تائید شده اثر منفی بر روی تضمین محصول ندارد و لزومی به ارزیابی مجدد نمی‌باشد.

### ۶,۱ فرضیات

فرضیات این سند عبارتند از:

- از نظر تولیدکننده و ارائه دهنده مدارک ارزیابی، مرکز افتا و سازمان فناوری اطلاعات نهادهای قابل اطمینانی هستند.
- مرکز افتا از این سند به عنوان مبنایی برای اجرایی نمودن فرآیند تداوم گواهی استفاده می‌نماید.
- برای روال نگهداری زیر نظر مرکز افتا، تولیدکننده برای هر هدف ارزیابی تغییر یافته باید گزارش «تحلیل اثر تغییرات» به سازمان فناوری اطلاعات ایران، ارسال نماید.
- برای روال نگهداری زیر نظر مرکز افتا، تولیدکننده برای هر هدف ارزیابی تایید شده باید گزارش «تحلیل آسیب پذیری» را سالیانه به سازمان فناوری اطلاعات ایران، ارسال نماید.
- الگو و راهنمایی برای حصول اطمینان از سازگاری میان آزمایشگاه‌ها در تعیین تغییرات عمده و جزئی وجود دارد.
- تولیدکننده برای محصول بروز شده بر اساس خط‌مشی مرکز در بازه زمانی تعیین شده برای اعتبار گواهی، درخواست فرآیند تداوم گواهی می‌دهد.

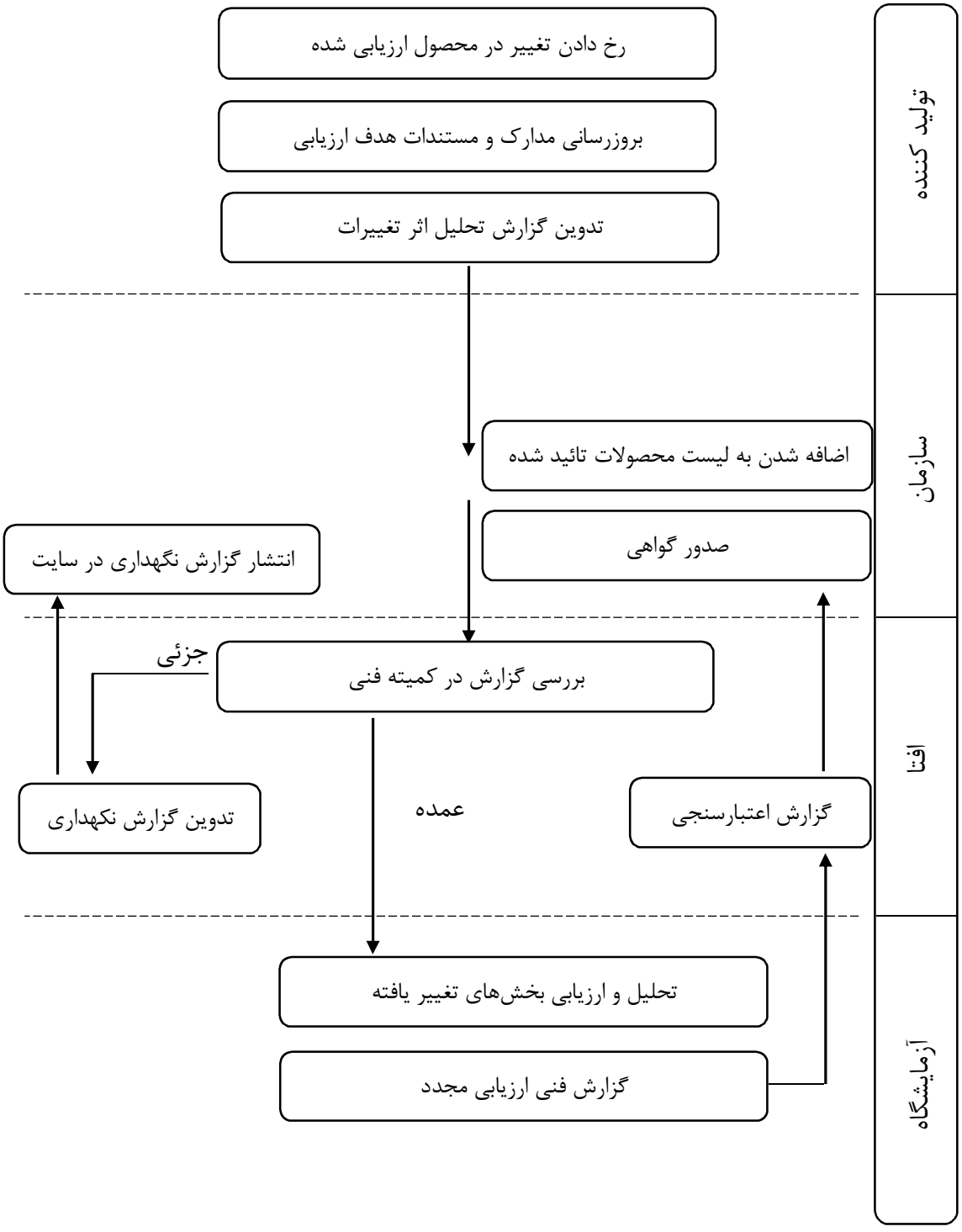
## ۲ رویکرد فرآیند تداوم گواهی

در فرآیند تداوم گواهی حتی در صورت تغییر محصول یا محیط آن، نیازی به تکرار شدن کار ارزیابی قبلی نمی‌باشد. از اینرو رویکرد تداوم گواهی، روال‌هایی را برای «نگهداری»، «ارزیابی مجدد» و «تحلیل آسیب‌پذیری» تعریف نموده که هر سه روال سعی در تکمیل کار ارزیابی قبلی دارند.

در صورتیکه تولیدکننده در محصول تغییراتی را ایجاد نماید که منجر به ارتقاء نسخه گردد، محصول به عنوان «هدف ارزیابی تغییریافته» باید وارد فرآیند نگهداری شود. در این فرآیند اثر تغییرات صورت گرفته بر روی تضمین محصول بررسی می‌گردد. چنانچه تغییرات رخ داده دارای اثر امنیتی نامطلوبی باشند محصول باید مجدد مورد ارزیابی قرار گیرد، در غیر این صورت گواهی محصول حفظ و گزارش نگهداری آن در سایت سازمان ضمیمه می‌گردد.

لازم به ذکر است که فرآیند نگهداری تنها اثر تغییرات رخ داده بر روی تضمین اولیه محصول را در نظر می‌گیرد و نسبت به ایمن بودن محصول به آسیب‌پذیری‌های جدید یا روش‌های حمله‌ای که در ارزیابی و گواهی اولیه در نظر گرفته نشده، اطمینان نمی‌دهد، اما تولید کننده ملزم به برطرف نمودن آنها براساس روال «تحلیل آسیب-پذیری» می‌باشد.

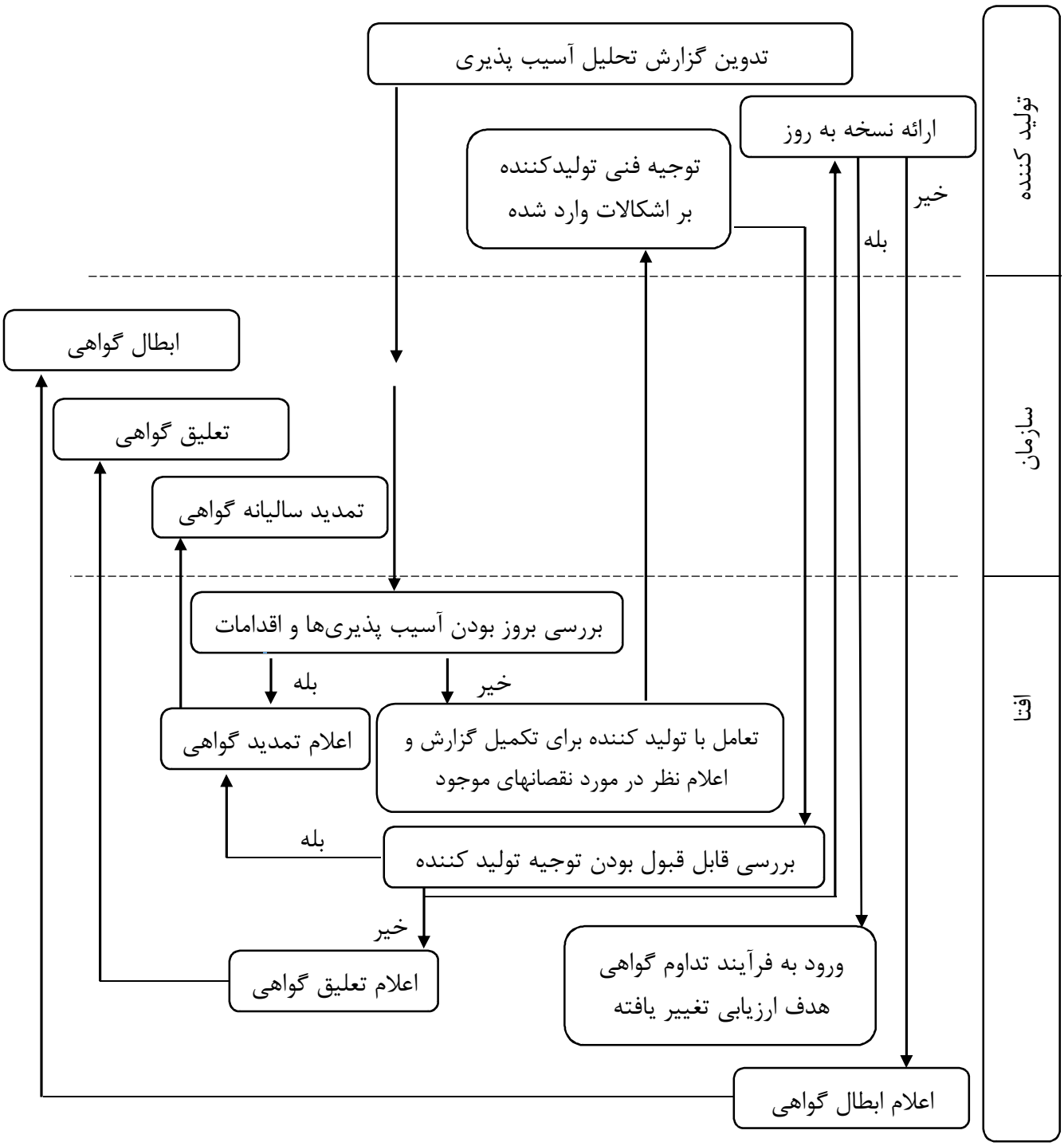
در شکل ۱ فرآیند تداوم گواهی نشان داده شده است، رخ دادن تغییر در محصول دارای گواهی نقطه شروع «روال نگهداری» و «ارزیابی مجدد» می‌باشد.




شکل ۱: فرآیند تداوم گواهی برای هدف ارزیابی تغییر یافته

شکل ۱: فرآیند تداوم گواهی برای هدف ارزیابی تغییر یافته

تولید کننده و آزمایشگاه با توجه به اثر نتایج تغییر بر روی تضمین محصول، اقداماتی انجام می‌دهند (شماره ۲).
تولیدکننده محصول تحلیلی از اثر تغییرات صورت گرفته را در قالب گزارش «تحلیل اثر تغییرات» مستند نموده و در اختیار مرکز قرار می‌دهد. مرکز افتا با بهره گیری از این گزارش و فاکتورهای مشخص، عمده یا جزئی بودن اثر تغییرات را تعیین می‌نماید. در فصل پنجم فاکتورهایی که در تشخیص تغییرات عمده یا جزئی تغییرات به مرکز کمک می‌نمایند شرح داده شده است (شماره ۳).
در صورتیکه مرکز به این نتیجه برسد که تغییرات اثر اندک و جزئی بر روی تضمین محصول دارند، براساس گزارش تحلیل اثر تغییرات برای محصول گزارش نگهداری تدوین نموده و محصول و گزارش نگهداری آن به صورت ضمیمه به لیست محصولات تائید شده در سایت سازمان اضافه می‌گردد (شماره ۴).
در شرایطی‌که مرکز به این نتیجه برسد که تغییرات محصول، عمده بوده؛ محصول باید مجدداً مورد ارزیابی قرار گیرد. در روال ارزیابی مجدد از مدارک تولید شده در ارزیابی قبلی و همچنین گزارش تحلیل اثر تغییرات حداکثر استفاده صورت خواهد گرفت که منجر به محصول تائید شده جدید با گزارش اعتبارسنجی و گواهی جدیدی خواهد شد (شماره ۵ و ۶).
پس از صدور گواهی محصول، ممکن است آسیب‌پذیری‌های جدیدی کشف گردند که توسط محصول پوشش داده نشده باشند. بنابراین تولیدکننده ملزم به برطرف نمودن آسیب‌پذیری‌های کشف شده‌ی جدید و بروزرسانی محصول خود می‌باشد.
بدین منظور لازم است سالانه گزارشی تحت عنوان «تحلیل آسیب‌پذیری» توسط تولیدکننده برای سازمان فناوری اطلاعات ارسال شود، که بیانگر آسیب‌پذیری‌های برطرف شده در محصول می‌باشد. در شکل ۲ فرآیند تحلیل آسیب‌پذیری نشان داده شده است.


تدوین گزارش تحلیل آسیب پذیری
ارائه نسخه به روز
توجیه فنی تولیدکننده
بر اشکالات وارد شده
خیر
بله
ابطال گواهی
تعلیق گواهی
تمدید سالیانه گواهی
بررسی بروز بودن آسیب پذیری‌ها و اقدامات
بله
خیر
اعلام تمدید گواهی
تعامل با تولید کننده برای تکمیل گزارش و
اعلام نظر در مورد نقصانهای موجود
بله
بررسی قابل قبول بودن توجیه تولید کننده
خیر
اعلام تعلیق گواهی
ورود به فرآیند تداوم گواهی
هدف ارزیابی تغییر یافته
اعلام ابطال گواهی
تولید کننده
سازمان
افتا

تولیدکننده‌ی «هدف ارزیابی تائید شده» پس از صدور گواهی هر ساله موظف به تهیه گزارش «تحلیل آسیب-پذیری» می‌باشد. با تهیه این گزارش و ارسال آن برای مرکز فرآیند تحلیل آسیب‌پذیری آغاز می‌گردد. لازم به ذکر است عدم ارسال این گزارش از سوی تولیدکننده برای مرکز تا پیش از تاریخ تمدید گواهی، منجر به ابطال گواهی محصول خواهد شد.

مرکز گزارش ارسالی را بررسی و در صورت لزوم از آزمایشگاهی که محصول سابقاً در آن ارزیابی شده بود، کمک می‌گیرد. در صورت کامل بودن گزارش و برطرف شدن آسیب‌پذیری‌های جدید، گواهی محصول برای یکسال آینده تمدید خواهد شد. در غیر این صورت مرکز با تولیدکننده جهت برطرف نمودن نقصانهای موجود تعامل می‌نماید. چنانچه تولیدکننده مرکز را از نظر فنی نسبت به اشکالات وارده توجیه نماید، گواهی برای یکسال دیگر تمدید خواهد شد. در غیر این صورت گواهی محصول برای یک بازه زمانی مشخص شده توسط مرکز تعلیق می‌گردد، تا به تولید کننده فرصت برطرف نمودن آسیب‌پذیری‌ها داده شود. در صورت ارائه نسخه جدید و برطرف نمودن آسیب‌پذیری‌ها محصول وارد فرآیند تداوم گواهی می‌شود تا اثر تغییرات رخ داده بررسی گردد. اما چنانچه در این بازه نسخه جدیدی از محصول ارائه نشود، گواهی آن ابطال خواهد گردید.

## ۱,۲ روال نگهداری

هدف از روال نگهداری در فرآیند تداوم گواهی، اجازه حفظ گواهی محصولاتی است که در نسخه جدید آن تغییرات اندکی رخ داده باشد. بدین منظور تولیدکننده باید اثر امنیتی تغییرات رخ داده در محصول را نسبت به تضمین اولیه محصول بررسی و نتایج آن را در اختیار مرکز قرار دهد. روال نگهداری در ادامه شرح داده شده است:

### ۱,۱,۲ شرح روال

روال نگهداری به صورت ورودی‌های لازم، اقدامات و خروجی‌هایی تعریف شده که منجر به ضمیمه نگهداری برای گواهی استاندارد معیار مشترک می‌شود.

به منظور شروع فرآیند نگهداری و بررسی گزارش تولیدکننده توسط مرکز افتا، باید موارد زیر توسط تولیدکننده در اختیار مرکز افتا قرار گیرد:

- گواهی محصول تایید شده (شامل ضمیمه نگهداری)
- گزارش اعتبارسنجی محصول تایید شده
- سند هدف امنیتی محصول تائید شده
- سند هدف امنیتی محصول بروز شده (با اعمال تغییرات)
- گزارش تحلیل اثر تغییرات

مرکز افتا با بررسی گزارش تحلیل اثر تغییرات و دیگر مدارک مربوطه و در صورت لزوم با مشورت گرفتن از تولیدکننده و آزمایشگاه، اثر تغییرات بر روی تضمین محصول را تعیین و گزارش تحلیل اثر را تکمیل می‌نماید. نتیجه بررسی یک از دو حالت زیر می‌باشد که به تولیدکننده اطلاع داده می‌شود:

- مرکز افتا تعیین می‌نماید که اثر تغییرات هدف ارزیابی عمده است و ضمیمه نگهداری تولید نمی‌شود و در صورت درخواست تولیدکننده، محصول مجدداً ارزیابی می‌گردد.
- مرکز افتا تعیین می‌نماید که اثر تغییرات هدف ارزیابی اندک است و ضمیمه نگهداری تولید می‌شود تا نشان دهد گواهی محصول تمدید شده است.

در صورت اندک بودن اثر تغییرات گزارش نگهداری و ضمیمه نگهداری به روزی برای آن محصول بر روی سایت سازمان منتشر می‌شود. لازم به ذکر است گزارش تحلیل اثر تغییرات تنها بین تولیدکننده و مرکز به اشتراک گذارده می‌شود.

### ۲،۱،۲ گزارش نگهداری

گزارش نگهداری در برگیرنده جزئیات تمام تغییرات رخ داده در محصول تحت روال نگهداری می‌باشد و به گزارش اعتبارسنجی محصول ضمیمه می‌گردد. برای نگارش این گزارش از بخش‌هایی از گزارش تحلیل اثر تغییرات استفاده می‌گردد، از جمله بخش‌هایی که باید در گزارش نگهداری در نظر گرفته شوند عبارتند از:

- معرفی
- شرح تغییرات
- مدارک موثر تولیدکننده

محتوای هریک از بخش‌های بالا در فصل هفتم با جزئیات شرح داده شده است. با اعمال تغییراتی در بخش‌های مطرح شده از سند تحلیل اثر تغییرات می‌توان از آنها در گزارش نگهداری استفاده نمود.

### ۳،۱،۲ ضمیمه نگهداری

ضمیمه نگهداری به عنوان ضمیمه گواهی برای هدف ارزیابی تائید شده به کار می‌رود، در این ضمیمه هدف‌های ارزیابی نگهداری شده لیست می‌گردند.

## ۲,۲ روال ارزیابی مجدد

هنگامیکه تغییرات رخ داده در هدف ارزیابی تائید شده، دارای تاثیرات عمده‌ای بر روی تضمین محصول باشد، لازم است جهت تضمین محصول تغییر یافته، تحلیل‌های بیشتری توسط ارزیاب انجام گیرد.

ارزیابی مجدد مشابه ارزیابی اولیه بوده و از نتایج ارزیابی اولیه که هنوز قابل اعمال بوده مجدداً استفاده می‌گردد تا از تکرار فعالیت‌های قبلی جلوگیری شود. بدین ترتیب ارزیابی مجدد همانند ارزیابی اولیه باید از روال‌ها و خط‌مشی‌های مرکز پیروی نماید.

در مواقعی که هدف ارزیابی تا حد زیادی دستخوش تغییر گردیده به گونه‌ای که تشابه کمی با هدف ارزیابی اولیه داشته باشد لزومی به تدوین گزارش تحلیل اثر تغییرات توسط تولیدکننده نمی‌باشد و محصول باید مجدداً ارزیابی گردد.

در صورتیکه تولید کننده اثر تغییرات رخ داده در محصول تغییر یافته را نسبت به محصول تائید شده تحلیل نماید و نتایج آن را در قالب گزارش تحلیل اثر تغییرات مستند و به آزمایشگاه ارائه دهد، گزارش تولید شده مبنای شناسایی بخش‌های تغییر یافته نسبت به هدف ارزیابی تائید شده قبلی قرار می‌گیرد.

همان‌طور که قبلاً نیز عنوان شده لزومی به ارزیابی بخش‌های تغییر نیافته‌ی هدف ارزیابی نمی‌باشد و می‌توان از نتایج ارزیابی قبلی برای این بخش‌ها بهره برد. حداقل موارد لازم برای ارزیابی مجدد با توجه به ارزیابی قبلی انجام شده، عبارتند از:

- مستندات پشتیبانی و محصول (ارائه شده از سوی تولیدکننده)
- سند هدف امنیتی جدید (ارائه شده از سوی تولیدکننده)
- سند هدف امنیتی قبلی
- گزارش فنی ارزیابی قبلی
- گزارش اعتبارسنجی/گواهی قبلی
- گواهی ارزیابی امنیتی صادر شده توسط سازمان فناوری اطلاعات
- بسته‌های کاری ارزیابی اصلی (در صورت وجود)

آزمایشگاه برای تعیین اثر تغییرات، لازم است تغییرات بین سندهای هدف امنیتی جدید و قبلی را تحلیل و بررسی نماید و تنها زمانی ارزیابی مجدد انجام دهد که الزامی تغییر یافته یا تحت تاثیر دیگر تغییرات باشد.

در صورت دسترسی ارزیاب به نتایج و بسته‌های کاری ارزیابی قبلی، باید حداکثر استفاده را از آنها نماید. به طورکلی آزمایشگاهی که ارزیابی فعلی را انجام می‌دهد، باید از هرگونه مدرک ارزیابی قبلی که سودمند بوده استفاده نماید تا هزینه ارزیابی را کاهش و نسبت به صحت فنی ارزیابی اطمینان حاصل نماید.

در تکمیل ارزیابی محصول تغییر یافته، سازمان سند هدف امنیتی جدید را همراه با گزارش اعتبارسنجی و گواهی جدید منتشر می‌نماید و این محصول مبنای فعالیت «تداوم گواهی» در آینده خواهد بود.

### ۳,۲ روال تحلیل آسیب پذیری هدف ارزیابی تایید شده

پس از صدور گواهی برای محصول، تولیدکننده موظف به برطرف نمودن آسیب‌پذیری‌های کشف شده جدید می‌باشد. بدین منظور لازم است تولیدکننده هر ساله گزارشی تحت عنوان «تحلیل آسیب پذیری» برای سازمان ارسال نماید تا آسیب پذیری‌های برطرف شده محصول در یک سال گذشته را در آن شرح دهد. سازمان گزارش مذکور را برای بررسی در اختیار مرکز افتا قرار می‌دهد؛ مرکز براساس این گزارش بروز بودن آسیب‌پذیری‌ها و اقدامات انجام شده در قبال آنها را بررسی می‌نماید و در صورت لزوم از آزمایشگاه کمک می‌گیرد، در صورت تائید بروز بودن آسیب‌پذیری‌ها و اقدامات انجام شده، گواهی برای یک سال دیگر توسط مرکز تمدید می‌گردد. به عبارتی اعتبار گواهی صادر شده برای محصول در مدت زمان تعیین شده توسط مرکز منوط به تمدید هر ساله‌ی آن می‌باشد.

در صورتیکه مرکز افتا بروز بودن آسیب‌پذیری‌ها و اقدامات انجام شده در قبال آنها را تائید ننماید، سازمان علت عدم تائید را به صورت مکتوب برای تولیدکننده ارسال می‌نماید. تولیدکننده جهت برطرف نمودن نقصان‌های موجود و تکمیل گزارش «تحلیل آسیب‌پذیری» با مرکز افتا تعامل می‌نماید و در صورت برطرف نمودن آسیب-پذیری‌ها، بنا به صلاحدید مرکز وارد فرآیند تداوم گواهی برای هدف ارزیابی تغییر یافته (بنا بر تغییر رخ داده در محصول: نگهداری یا ارزیابی مجدد) می‌گردد.

در صورتیکه آسیب‌پذیری‌های محصول توسط تولید کننده بر طرف نشود و تولیدکننده مرکز را از نظر فنی توجیه نماید که آسیب‌پذیری امنیت محصول را تحت شعاع قرار نمی‌دهد، گواهی صادر شده برای یک سال آینده تمدید خواهد شد.

اما در شرایطی‌که تولیدکننده نتواند از منظر فنی مرکز افتا را توجیه نماید، گواهی صادره برای مدت زمانی (زمان توسط مرکز مشخص و به تولید کننده اعلام می‌گردد) تعلیق می‌گردد تا تولیدکننده بتواند نواقص موجود را برطرف نماید اگر در این بازه زمانی نواقص برطرف گردد، محصول وارد فرآیند تداوم گواهی برای هدف ارزیابی تغییر یافته (بنا بر تغییر رخ داده در محصول: نگهداری یا ارزیابی مجدد) می‌گردد، در غیر این صورت گواهی صادره باطل خواهد شد.

### ۴,۲ فرآیند بررسی گزارش تحلیل اثر تغییرات

سه مرحله اصلی جهت بررسی گزارش ارسال شده برای تداوم گواهی وجود دارد:

- مرحله بررسی، در این مرحله مرکز افتا کامل بودن موارد ارسال شده توسط تولید کننده برای سازمان را بررسی می‌نماید.
- مرحله تحلیل، در این بخش مرکز افتا ادعای نگهداری تولیدکننده را تحلیل می‌نماید.
- مرحله نتیجه گیری، در طول این مرحله مرکز افتا گزارش نگهداری و ضمیمه نگهداری تولید می‌نماید و به سازمان جهت انتشار بر روی سایت ارسال می‌نماید.

هریک از این سه مرحله با جزئیات بیشتر در ادامه شرح داده شده است:

### ۱,۴,۲ مرحله بررسی گزارش ارسال شده

مرکز افتا کامل بودن موارد ارسالی از سوی تولیدکننده را بررسی می‌نماید، دو نتیجه ممکن بررسی عبارتند از:

- مرکز افتا به تولید کننده اطلاع می‌دهد که بسته ارسالی شامل تمام موارد درخواستی می‌باشد و مرکز افتا وارد مرحله تحلیل موارد ارسالی خواهد شد و یک بازه زمانی تخمینی برای مرحله تحلیل در نظر می‌گیرد.
- مرکز افتا به تولیدکننده اطلاع می‌دهد که موارد ارسالی کامل نبوده و نواقص مستندات را به تولیدکننده اعلام می‌نماید.

### ۲,۴,۲ مرحله‌ی تحلیل گزارش ارسالی

به شرط آنکه تولیدکننده دلایل کافی جهت تاثیر هر تغییر ارائه دهد، مرکز افتا تغییرات اعلام شده در گزارش تحلیل اثر تغییرات را بررسی نموده و اثر آنها را بر روی تضمین هدف ارزیابی تعیین و نتایج تحلیل را به صورت مکتوب برای تولید کننده ارسال می‌نماید. چهار نتیجه احتمالی عبارتند از:

- تمام تغییرات جزئی هستند، تمام مدارک تولیدکننده تحت تاثیر این تغییرات بروز شده و هدف ارزیابی برای تداوم گواهی نگهداری می‌شود. در این مورد، فرآیند وارد مرحله نگهداری می‌شود.
- تمام تغییرات جزئی هستند اما برخی از مدارک تولید کننده که تحت تاثیر تغییر هستند به طور کامل بروزرسانی نشده است. در این مورد، لازم است تولیدکننده مدارک را بروز رسانی نماید. هنگامیکه تمام مدارک تولیدکننده (تحت تاثیر تغییرات) بروزرسانی شد، هدف ارزیابی برای تداوم گواهی نگهداری می‌شود. این فرآیند وارد مرحله نتیجه‌گیری می‌شود.
- جزئیات یک یا بیش از یک بخش از «گزارش تحلیل اثر» ناکافی است. در این موارد، تولید کننده لازم است جزئیات بیشتری ارائه دهد، که ممکن است به فعالیت‌های تحلیل اثر بیشتری از سوی تولیدکننده

نیاز باشد. این امر ممکن است منجر به بازنویسی گزارش تحلیل اثر تغییرات و ارسال مجدد آن برای مرکز افتا گردد. هنگامیکه تمام مدارک تولیدکننده (تحت تاثیر تغییرات رخ داده در محصول) بروزرسانی شد، هدف ارزیابی برای تداوم گواهی نگهداری می‌شود و فرآیند وارد مرحله نتیجه‌گیری می‌گردد.

- تغییرات رخ داده عمده می‌باشد و ارزیابی مجدد نیاز است (حتی در صورت یک تغییر عمده).

### ۳,۴,۲ مرحله نتیجه‌گیری گزارش ارسالی

مرکز افتا از گزارش تحلیل اثر تغییرات به عنوان مبنایی برای تولید گزارش نگهداری و ضمیمه نگهداری استفاده می‌نماید و برای محتوای گزارش نگهداری اختیار تام دارد.

- گزارش نگهداری

گزارش نگهداری هدف ارزیابی تائید شده به گزارش اعتبارسنجی ضمیمه می‌گردد و تغییرات رخ داده در هدف ارزیابی تائید شده که تحت روال نگهداری، پذیرش شده‌اند را معرفی می‌نماید.

گزارش نگهداری شامل اطلاعات زیر است که از گزارش تحلیل اثر تغییرات برگرفته شده است:

- معرفی
- شرح تغییرات
- مدارک تغییر یافته محصول

- ضمیمه نگهداری

ضمیمه نگهداری به عنوان ضمیمه‌ی گواهی هدف ارزیابی تائید شده به کار می‌رود. ضمیمه نگهداری شامل اطلاعات زیر است:

- شناسه منحصر به فرد از نسخه‌ی فعلی هدف ارزیابی نگهداری شده
- تاریخ پایان نگهداری
- شناسه منحصربه فرد از تمام هدف ارزیابی‌های نگهداری شده‌ی قبلی
- ارجاع منحصر به فرد برای هدف ارزیابی تائید شده
- گزارش نگهداری

## ۳ تغییرات

مرکز افتا با بررسی تغییرات شرح داده شده در گزارش تحلیل اثر تغییرات، تاثیر آنها را بر روی تضمین هدف ارزیابی تائید شده مشخص می‌نماید. تغییر اندک و جزئی روی تضمین محصول اثری ندارد و بدین ترتیب نیازی به ارزیابی مستقل توسط ارزیاب نمی‌باشد (هرچند انتظار می‌رود تولیدکننده تغییرات را به عنوان بخشی از آزمون رگرسیون، تست نماید). در مقابل، تغییرات عمده به صورت قابل توجهی تضمین را تحت تاثیر قرار می‌دهند و در نتیجه لازم است فعالیت‌های ارزیابی مجدداً تکرار شود.

نکته مهم تفاوت بین اثر تغییرات بر روی محصول تائید شده و تضمین آن است. ممکن است در محصول تغییرات زیادی صورت گرفته باشد اما این بدان معنا نیست که اثر زیادی بر روی تضمین امنیتی محصول داشته است، بلکه ممکن است اثر آن اندک باشد. همچنین ممکن است در محصول تغییرات اندکی صورت گرفته باشد اما این بدان معنا نیست که اثر اندکی بر روی تضمین امنیتی محصول داشته است، بلکه ممکن است اثر آن گسترده باشد.

در ادامه راهنمای کلی در رابطه با تفاوت بین تغییرات عمده و اندک ارائه شده است.

### ۱,۳ انواع تغییرات جزئی

تغییرات جزئی معمولاً شامل تغییراتی هستند که اثری بر روی ادعاهای هدف ارزیابی ندارند. مثالی از این دسته تغییرات که مناسب است تحت روال نگهداری قرار گیرد، عبارتند از:

- **تغییرات بر روی محیط IT که اثری بر روی هدف ارزیابی تائید شده ندارند.** برای مثال:

رخ دادن تغییر در سخت‌افزارهای زیرین یا بخش‌های نرم‌افزاری محصول که خارج از حوزه‌ی هدف ارزیابی هستند در صورت تغییر نکردن واسط[۲] آنها جزئی در نظر گرفته می‌شود.

استفاده از نسخه‌های بالاتر برای پلتفرم‌های زیرین (ارتقاء نسخه پلتفرم‌های زیرین)، معمولاً در صورت تغییر ننمودن واسط به پلتفرم‌ها جزئی در نظر گرفته می‌شود.

انتقال به یک پلتفرم زیرین متفاوت (به طور مثال، از پلتفرم مبتنی بر ویندوز به سمت پلتفرم مبتنی بر لینوکس) غالباً به علت اثر بالقوه بر روی واسط‌های زیرین، عمده در نظر گرفته می‌شود، در این شرایط باید مجدداً تست‌های لازم انجام گیرد تا نسبت به مطرح نشدن آسیب‌پذیری‌ها در پلتفرم جدید اطمینان حاصل گردد.

- **تغییرات در هدف ارزیابی تائید شده که تاثیری بر روی مدارک تضمینی ندارد.** برای مثال، اگر هدف ارزیابی در سطح EAL1 تائید شده باشد، تغییر روی شماتیک سخت افزاری تاثیری بر روی مستندات

[۲] Interface

تضمین ندارد. با این حال، تولید کننده تغییرات رخ داده را به عنوان بخشی از آزمون رگرسیون استاندارد تست می‌نماید.

- **تغییرات مربوط به حوزه‌های غیر امنیتی کارکرد هدف ارزیابی.** تغییر یا اضافه نمودن کارکرد غیر امنیتی جزئی در نظر گرفته می‌شود. اما تغییرات یا اضافه نمودن کارکردهای امنیتی ممکن است جزئی یا عمده در نظر گرفته شود.

- **تغییرات نگارشی (دستوری، تایپی و قالب بندی)** که در هریک از مدارک تضمین رخ می‌دهد. برای مثال تغییرات نگارشی در شرح کارکرد محصول، جزئی در نظر گرفته می‌شود.

- **تغییرات متن‌های غیر اجرایی در کد اصلی** (مثل توضیحات) این تغییرات معمولاً جزئی در نظر گرفته می‌شود. اما تغییرات در دستورالعمل‌های کامپایلر معمولاً تغییرات عمده‌ای در نظر گرفته می‌شوند.

- **تغییرات در محیط توسعه** که اثر قابل توجهی بر روی تضمین محصول ندارند. برای مثال، بروزرسانی ابزار مدیریت پیکربندی در صورتی به عنوان تغییر جزئی در نظر گرفته می‌شود که بروزرسانی بر روی هدف ارزیابی اثر نگذارد. اگر بروزرسانی ابزار مدیریت پیکربندی نتایج کاملاً جدیدی تولید نماید بنابراین هدف ارزیابی باید مجدداً ارزیابی و تغییرات عمده در نظر گرفته شود.

- **تغییر در پیشگفتار سند هدف امنیتی،** تغییر در معرفی سند هدف امنیتی یا شناسه هدف ارزیابی (همانند تغییر نام محصول) جزئی در نظر گرفته می‌شود. اگر هر یک از بخش‌های تهدیدات، خط‌مشی‌ها، فرضیات یا تغییر اهداف امنیتی بدون آنکه منجر به تغییر الزامات امنیتی گردد، به عنوان تغییر جزئی در نظر گرفته می‌شود. در صورت تغییر نمودن هریک از الزامات، تغییر عمده محسوب می‌گردد.

- **ادعای انطباق به پروفایل حفاظتی جدید،** تغییر در ادعای انطباق به پروفایل حفاظتی غالباً عمده در نظر گرفته می‌شود، اما زمانیکه پروفایل حفاظتی همزمان با سند هدف امنیتی تولید شود و ارزیابی این سند پیش از نهایی شدن پروفایل حفاظتی، تکمیل گردد، ادعای انطباق به این پروفایل حفاظتی به تنهایی تغییر جزئی در نظر گرفته می‌شود.

### ۲,۳ انواع تغییرات عمده

تغییرات عمده معمولاً شامل تغییراتی است که در رابطه با هدف ارزیابی ادعا شده است. مثالی از تغییرات عمده که باید تحت روال ارزیابی مجدد قرار گیرد عبارتند از:

- **تغییرات در الزامات تضمین امنیتی ادعا شده**. تغییر در الزامات به دو صورت اضافه شدن یا حذف آنها می‌باشد؛ اضافه نمودن الزام شامل اضافه شدن خانواده جدید یا عنصر بالاتری در همان خانواده می‌باشد.

- **تغییر در الزامات کارکردی ادعا شده**، سبب تغییر در حوزه هدف ارزیابی می‌گردد و باید صحت و سقم تغییر رخ داده تحت روال ارزیابی مجدد بررسی گردد.

- **استفاده از روال‌هایی بررسی نشده در ارزیابی اولیه**، استفاده نمودن از روال‌هایی که در ارزیابی اولیه استفاده نشده‌اند، همانند استفاده از روال متفاوت تحویل به عنوان تغییر عمده در نظر گرفته می‌شود.

- **تغییر در حوزه هدف ارزیابی**، اضافه و حذف نمودن یک کارکرد یا سازوکار امنیتی که الزام کارکرد امنیتی ادعا شده را تغییر یا سبب اضافه شدن الزام کارکرد امنیتی جدیدی می‌گردد.

- **مجموعه‌ای از تغییرات جزئی که در کنارهم اثر عمده‌ای بر روی امنیت هدف ارزیابی می‌گذارند.** هرچند تغییرات ممکن است به تنهایی اثر جزئی داشته باشند، اما مجموع تغییرات جزئی ممکن است دارای اثر امنیتی عمده‌ای بوده و بنابراین لازم است ارزیابی مجددی صورت گیرد.

- **تکرار چندین بار فرآیند نگهداری در مجموع منجر به تفاوت زیاد هدف ارزیابی با نسخه اولیه آن می‌گردد**، در این شرایط نیاز به ارزیابی مجدد خواهد بود.

- **اضافه نمودن ادعای انطباق پروفایل حفاظتی**، در صورت ادعای انطباق به پروفایل حفاظتی جدید در سند هدف امنیتی، احتمالاً سبب رخ دادن تغییراتی در بخش‌های مختلف این سند بالاخص الزامات آن می‌گردد. در این صورت محصول مجدداً باید ارزیابی گردد.

- **تغییر در هدف ارزیابی پس از مدت زمان سپری شده از زمانی که ارزیابی یا نگهداری شده است.** در صورتیکه تغییری در هدف ارزیابی رخ دهد و بیش از دو سال از زمان ارزیابی یا آخرین اقدامات نگهداری گذشته باشد، نیاز به ارزیابی مجدد محصول خواهد بود.

- **تغییر در نسخه‌ی استاندارد ارزیابی امنیتی معیار مشترک،** بروزرسانی این استاندارد یا به صورت نسخه‌های تجدیدنظر است (تغییر نسخه از ۲,۱ به ۲,۲) که این تغییرات به عنوان تغییر جزئی در نظر گرفته می‌شود یا نسخه جدیدی از استاندارد منتشر می‌شود (تغییر نسخه از ۲ به ۳) که در این صورت محصولی که قبلاً به نسخه ۲ ادعای انطباق داشته و حال بخواهد به نسخه ۳ ادعای انطباق نماید نیاز به ارزیابی مجدد خواهد داشت.

### ۳,۳ معیار بروزرسانی استاندارد

در صورت اتخاذ نسخه جدیدی از استاندارد ارزیابی معیار مشترک، یک جدول زمانی توسط مرکز افتا برای انطباق با نسخه جدید ارائه خواهد شد که ضرب الاجلی برای پایان استفاده از نسخه قبلی استاندارد معیار مشترک را تعیین می‌نماید. این جدول زمانی همچنین پایان زمان استفاده از نسخه‌ی قدیمی برای فعالیت‌های نگهداری را تعیین می‌نماید. لازم است تمام ارزیابی‌های تحت کنترل مرکز افتا از این ضرب‌الاجل پیروی نمایند.

## ۴ تحلیل نمودن اثر تغییرات

### ۱,۴ ورودی

در زیر ورودی‌های اصلی برای فرآیند تحلیل اثر تغییرات آورده شده است:

- مدارک تولید کننده مرتبط با هدف ارزیابی تائید شده
- شرح تغییرات (احتمالاً از فرآیندها و روال‌های کیفی چرخه‌ی حیات تولید می‌شوند)

### ۲,۴ مراحل انجام تحلیل اثر تغییرات

در طول روال نگهداری یکی از مسئولیت‌های تولیدکننده اطمینان دادن نسبت به برآورده شدن محتوای تغییریافته مدارک توسط هدف ارزیابی می‌باشد. همچنین باید پس از شناسایی اثر تغییرات بر روی مدارک، اثر امنیتی این دسته از تغییرات را تخمین بزند.

**مرحله اول – شناسایی هدف ارزیابی تائید شده**

تعیین مدارک تولیدکننده که به عنوان مبنای تضمین هدف ارزیابی تائید شده، ارائه شده‌اند. تمام تغییرات در قبال این مبنا اعمال می‌گردند.

**مرحله دوم – معرفی و شرح تغییرات**

- شرح تغییرات محصول و همچنین معرفی و شرح تغییرات محیط توسعه مربوط به هدف ارزیابی تائید شده
- شرح تغییرات در حدی که بتوان درکی از آنچه که رخ داده به دست آورد، اما لازم به شرح چگونگی انجام تغییرات نمی‌باشد.

**مرحله سوم – تعیین مدارک تولیدکننده**

هدف این مرحله تعیین و در نظر گرفتن هر تغییر مرحله‌ی قبلی، و آن دسته از مدارک تولیدکننده که با توجه به این تغییرات نیاز به بروزرسانی دارند.

این مرحله باید اصولی انجام شود، بنابراین هریک از کامپونت‌های تضمین در بسته‌ی تضمین هدف ارزیابی، اثر تغییر بر روی کامپونت تضمین و همچنین مدارکی که برای آن کامپونت ارائه شده‌اند در نظر گرفته می‌شود.

لیست زیر جهت تسهیل این رویکرد در نظر گرفته شده است. برای هریک از تغییراتی که در محصول رخ داده، موارد زیر باید درنظر گرفته شود:

- آیا تاثیری بر روی سند هدف امنیتی دارد؟
- آیا تمام خط‌مشی‌های قابل اجرای مرکز افتا را برآورده می‌نماید؟
- آیا بر روی لیست موارد پیکربندی هدف ارزیابی اثر گذار است؟
- آیا بر روی هر یک از سطوح انتزاعی توابع امنیتی هدف ارزیابی (همانند مشخصات کارکردی، نمایش پیاده‌سازی و غیره) یا ارتباط بین آنها اثر گذار است؟
- آیا مدل فرآیند نرم‌افزار تیمی[۳] را تحت تاثیر قرار می‌دهد؟
- آیا بر روی مستندات راهنما اثر گذار است؟
- آیا بر روی مستندات تست، چون سند تحلیل تست پوشش، تحلیل عمق تست یا سند تست تاثیر گذار است؟
- آیا بر روی تحلیل کانال پنهانی، تحلیل مستندات راهنما و تحلیل آسیب‌پذیری اثر گذار است؟

[۳] Team Software Process(TSP)

برای هر تغییری که در محیط توسعه رخ می‌دهد، موارد زیر باید در نظر گرفته شود:

- آیا تاثیری بر روی سند هدف امنیتی دارد؟
- آیا تمام خط‌مشی‌های قابل اجرای مرکز افتا را برآورده می‌نماید؟
- آیا بر روی مستندات مدیریت پیکربندی اثر گذار است؟
- آیا بر روی روال‌های تحویل اثر گذار است؟
- آیا بر روی روال‌های ضروری برای نصب امن، تولید و راه‌اندازی هدف ارزیابی اثر گذار است؟
- آیا بر روی روال اصلاح نقص اثر گذار است؟
- آیا بر روی مدل چرخه حیات اثر گذار است؟
- آیا بر روی ابزارهای توسعه اثر گذار است؟

با توجه به شرح تغییرات باید اثر تمام آنها بر روی مدارک تولیدکننده در نظر گرفته شود، تا اثرات بالقوه‌ی آنها بررسی گردد.
با توجه به این موارد سند هدف امنیتی به احتمال زیاد دستخوش تغییر خواهد شد، حتی اگر این تغییرات بسیار کم و به سند اولیه مشابه باشد. در صورت تغییر هدف ارزیابی، سند هدف امنیتی باید بروزرسانی شده تا حداقل شماره نسخه‌ی هدف ارزیابی در آن بروزرسانی گردد.
نسخه‌ی قبلی گزارش تحلیل اثر تغییرات می‌تواند به عنوان ورودی این مرحله مورد استفاده قرار گیرد. برای برخی از اقدامات تولیدکننده تعیین نمودن اثر تغییرات ممکن است ساده باشد (به طور مثال، واسط کاربری گرافیکی جدید برای هدف ارزیابی تغییر یافته، که به همان شیوه‌ی مورد استفاده برای هدف ارزیابی تحویل داده شده، تاثیری بر روی الزامات تحویل ندارد) درحالیکه برای دیگر الزامات ممکن است خیلی سخت باشد (به طور مثال، آیا معرفی GUI جدید، لیست واسط‌های توابع امنیتی هدف ارزیابی را تغییر می‌دهد).
خروجی این مرحله لیست از اقدامات تولیدکننده است که تحت تاثیر تغییرات قرار گرفته است.

### مرحله چهارم –تغییر دادن مدارک تولیدکننده

هدف از این مرحله تغییر دادن محتوای آن دسته از مدارک تولیدکننده می‌باشد که تحت تاثیر تغییرات رخ داده در محصول بوده‌اند (مدارکی که در مرحله‌ی قبل معرفی شده‌اند). ممکن است جهت بروزرسانی مدارک لازم باشد «آزمون رگرسیون» انجام گیرد، تولید کننده ممکن است یک نمونه از تست‌هایی که برای ارزیابی تحویل داده را

تکرار نماید. در صورت نوشته شدن تست جدید برای تغییر، این تست و هدف از آن باید در گزارش تحلیل اثر آورده شود.

در صورت مخفی بودن تغییرات توابع امنیتی هدف ارزیابی در پائین ترین سطح انتزاعی در دسترس توابع امنیتی هدف ارزیابی (به طور مثال، پائین‌ترین سطح از تجزیه توابع امنیتی هدف ارزیابی در مبنای تضمین بالاترین سطح طراحی است همچنین برخی کدهایی که در طول روال نگهداری تغییر داده می‌شوند اما با تغییر آنها نیازی به تغییر بالاترین سطح طراحی نمی‌باشد)، تولیدکننده باید چگونگی تست این دسته از تغییرات را نشان دهد و در گزارش تحلیل اثر تغییرات باید کافی بودن این تست شرح داده شود. در پایان این مرحله لیستی از مدارک بروز شده می‌باشند.

### مرحله پنجم – نتیجه‌گیری

تعیین اثر کلی تغییرات معرفی شده بر روی تضمین هدف ارزیابی تائید شده و نتیجه گیری در مورد جزئی بودن یا عمده بودن این دسته از تغییرات خروجی این مرحله می‌باشد. برای مشخص نمودن جزئی یا عمده بودن تغییرات به فصل ۵ مرتجعه شود.

### مرحله ششم – گزارش

تحلیل انجام شده و یافته‌های تحلیل، در گزارش تحلیل اثر تغییرات آورده شده است (فصل ۷). این گزارش توسط مرکز افتا بررسی می‌گردد.

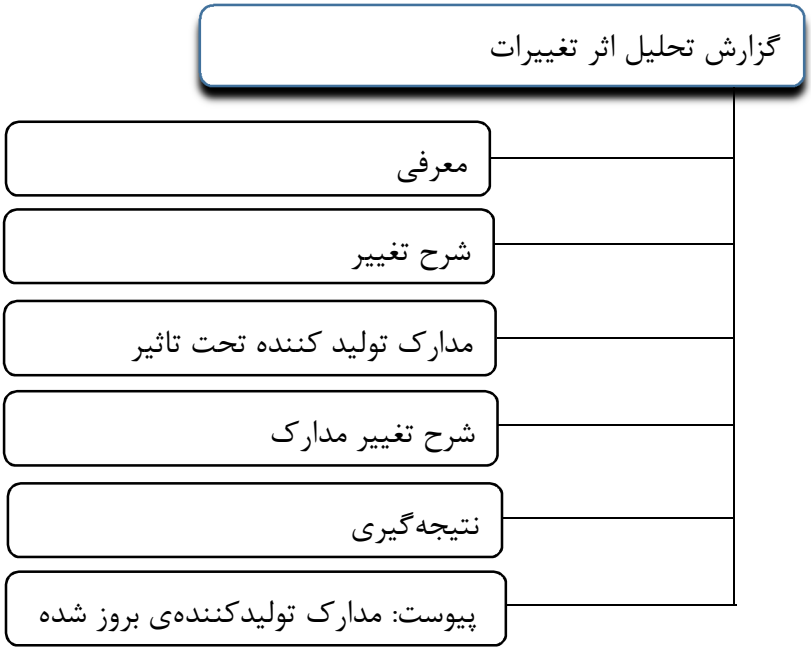
## ۳,۴ خروجی

گزارش تحلیل اثر تغییرات

بروزرسانی مدارک تولید کننده

# ۵ گزارش تحلیل اثر

در این فصل حداقل محتوای گزارش تحلیل اثر تغییرات شرح داده شده است. در شکل ۲ بخش‌های این گزارش نشان داده شده است. از این شکل به عنوان راهنما در زمان فهرست نویسی سند گزارش تحلیل اثر می‌توان استفاده نمود. این گزارش ورودی روال نگهداری می‌باشد.




شکل ۲محتوای گزارش تحلیل اثر

### ۱,۵ معرفی

تولیدکننده باید شناسه‌های کنترل پیکربندی گزارش تحلیل اثر تغییرات را گزارش نماید.

*این شناسه شامل اطلاعات معرفی کننده‌ی گزارش تحلیل اثر تغییرات می‌باشد (به عنوان مثال نام، تاریخ و شماره نسخه)*

تولیدکننده باید شناسه‌های کنترل پیکربندی هدف ارزیابی فعلی را گزارش نماید.

*این شناسه‌ها معرفی کننده‌ی نسخه‌ی فعلی هدف ارزیابی است که منعکس کننده‌ی تغییرات هدف ارزیابی تائید شده می‌باشد.*

تولیدکننده باید شناسه‌های کنترل پیکربندی گزارش فنی ارزیابی، گزارش اعتبارسنجی و هدف ارزیابی تائید شده را گزارش نماید.

*این شناسه‌ها لازم است مبنای تضمین و مستندات مربوط به آن را معرفی نماید همچنین هر تغییر دیگری که ممکن است در این مبنای تضمین رخ دهد.*

تولیدکننده باید شناسه‌های کنترل پیکربندی برای نسخه سند هدف امنیتی مربوط به هدف ارزیابی تائید شده را گزارش نماید.

تولیدکننده باید هویت تولیدکننده را گزارش نماید.

*هویت تولیدکننده‌ی هدف ارزیابی لازم است تا بخش که مسئول تولید هدف ارزیابی، انجام تحلیل آسیب-پذیری و بروزرسانی مدارک است را مشخص نماید.*

*هویت تولیدکننده ممکن است حاوی اطلاعاتی راجع به جنبه‌های حقوقی و قانونی باشد، برای مثال مربوط به محرمانگی سند.*

### ۲,۵ شرح تغییرات

تولیدکننده باید تغییرات محصول را گزارش دهد.

*تغییرات معرفی شده مربوط به هدف ارزیابی تائید شده می‌باشد.*

تولیدکننده باید تغییرات محیط توسعه را گزارش دهد.

*تغییرات معرفی شده مربوط به محیط توسعه هدف ارزیابی تائید شده می‌باشد.*

### ۳,۵ مدارک تولیدکننده تحت تاثیر

برای هر تغییر تولید کننده باید لیست مدارک تولید کننده که تحت تاثیر این تغییر قرار گرفته‌اند را گزارش نماید.

*برای هر تغییر محصول (هدف ارزیابی تائید شده) یا محیط توسعه آن، هر مورد از مدارک تولید کننده که تحت تاثیر آن بوده و لازم است تغییر یابد، باید در این قسمت معرفی گردد.*

### ۴,۵ شرح تغییرات مدارک تولید کننده

تولیدکننده باید به طور خلاصه تغییرات لازم مدارکی که تحت تاثیر تغییر هستند را شرح دهد.

*برای هر مورد از مدارک تولیدکننده که تحت تاثیر تغییر بوده، تغییرات لازم به محتوای مدارک باید به طور خلاصه شرح داده شود.*

### ۵,۵ نتیجه‌گیری

برای هر تغییر تولید کننده باید گزارش دهد که تاثیر این تغییر بر روی تضمین محصول عمده یا اندک بوده است. (در پیوست الف لیستی ارائه شده که می‌تواند مورد استفاده قرار گیرد تا اطمینان دهد که تمام فضاهایی که ارزیابی شده‌اند در گزارش تحلیل اثر تغییر در نظر گرفته شده است).

*تولید کننده باید برای هر تغییر علت اثری که برای آن گزارش شده را ذکر نماید.*

تولیدکننده باید اثر کلی تغییرات را به صورت عمده یا اندک گزارش نماید.

*تولیدکننده باید علت این تصمیم را ذکر نماید.*

### ۶,۵ پیوست: مدارک تولید کننده بروز شده

تولیدکننده باید برای هر مورد از مدارک بروز شده تولیدکننده اطلاعات زیر را گزارش نماید:

- عنوان
- مرجع منحصر به فرد (به عنوان مثال تاریخ صدور و شماره نسخه)

*تنها مدارکی که تغییرات ویژه‌ای نموده‌اند لازم است لیست شوند.*

**پیوست الف**

| | |
|---|---|
| **واسط‌های توابع امنیتی هدف ارزیابی** | |
| [ ] واسط‌های جدید توابع امنیتی هدف ارزیابی<br>[ ] واسط‌های توابع امنیتی هدف ارزیابی تغییریافته<br>[ ] واسط‌های توابع امنیتی هدف ارزیابی تغییرنیافته | شرح: |
| **پلتفرم توابع امنیتی هدف ارزیابی (سخت‌افزار هدف ارزیابی)** | |
| [ ] سخت‌افزار پایدار<br>[ ] کامپوننت‌های جدید<br>[ ] سیستم‌عامل جدید<br>[ ] هیچ سخت‌افزاری تغییرنیافته | شرح: |
| **الزامات کارکرد امنیتی** | |
| [ ] الزامات کارکرد امنیتی تغییریافته<br>[ ] الزامات کارکرد امنیتی تغییرنیافته | شرح: |
| **کارکرد امنیتی جدید** | |
| [ ] کارکرد امنیتی جدید<br>[ ] بدون کارکرد امنیتی جدید | شرح: |

| | |
|---|---|
| **فرضیات و اهداف** | |
| [ ] تغییر فرضیات و اهداف<br>[ ] تغییر ننمودن فرضیات و اهداف | شرح: |
| **مستندات تضمین** | |
| [ ] تغییرات ACM<br>[ ] تغییرات AGD, ADO<br>[ ] تغییرات ATE<br>[ ] تغییرات AVA<br>[ ] تغییرات ALC<br>[ ] بدون هیچ مدرک تضمین جدید | شرح: |
| **ویژگی جدید** | |
| [ ] ویژگی غیرامنیتی جدید<br>[ ] بدون ویژگی غیرامنیتی جدید | شرح: |
| **رفع اشکال** | |
| [ ] رفع اشکال‌های امنیتی<br>[ ] رفع اشکال‌های غیرامنیتی<br>[ ] بدون اشکال | شرح: |
| **محیط توابع امنیتی هدف ارزیابی** | |

| | |
|---|---|
| **نتیجه گیری:**<br><br>[ ] **اقدام نگهداری واضح**. تنها لازم است سند هدف امنیتی بروز گردد.<br><br>[ ] **اقدام نگهداری جزئی**. تست مجدد لازم است اما نه بیشتر.<br><br>[ ] **ارزیابی مجدد لازم**. استفاده مجدد مدارک امکان پذیر است.<br><br>[ ] **ارزیابی مجدد**. مدارک مجدداً نمی-تواند استفاده گردد. | شرح: |