ÚMFT infovonal:
06 40 638 638
nfu@nfu.gov.hu • www.nfu.hu

RENDSZEREKRE VONATKOZÓ ÉRTÉKELÉSI MÓDSZERTAN

A dokumentum az Új Magyarország Fejlesztési Terv keretében, az Államreform Operatív Program támogatásával, az „Elektronikus közigazgatási keretrendszer” tárgyú kiemelt projekt megvalósításának részeként készült. A dokumentum elkészítésében részt vett:

Metaadat-táblázat

Megnevezés	Leírás
Cím (dc:Title)	Rendszerekre vonatkozó értékelési módszertan
Kulcsszó (dc:Subject)	IT biztonság; értékelés; módszertan
Leírás (dc:Description)	Az elkészült e-közigazgatási alkalmazásokat, valamint az ezeket biztosító informatikai rendszereket használatbavételük, illetve a Központi Rendszerre történő kapcsolódásuk engedélyezése előtt meg kell vizsgálni, hogy megfelelnek-e a rájuk vonatkozó biztonsági követelményeknek. Ez a dokumentum a működő informatikai rendszerek megfelelőség vizsgálatára alkalmazható biztonság értékelési módszertant tartalmazza. Meghatározza az értékelési bizonyítékok létrehozásához kapcsolódó rendszer tulajdonosi és rendszer integrátori feladatokat, valamint a biztonságot értékelők feladatait.
Típus (dc:Type)	Szöveg, táblázat
Forrás (dc:Source)	
Kapcsolat (dc:Relation)	e-Közigazgatási Keretrendszer egyéb dokumentumai
Terület (dc:Coverage)	KOP-ok során megvalósuló projektek, központi IT fejlesztési projektek
Létrehozó (dc:Creator)	e-Közigazgatási Keretrendszer Kialakítása projekt
Kiadó (dc:Publisher)	Miniszterelnöki Hivatal
Résztvevő (dc:Contributor)	Hunguard Kft.
Jogok (dc:Rights)	e-Közigazgatási Keretrendszer
Dátum (dc:Date)	2008.09.19.
Formátum (dc:Format)	.doc
Azonosító (dc:Identifier)	
Nyelv (dc:Language)	Magyar
Verzió (dc:Version)	V4
Státusz (State)	Végleges
Fájlnév (FileName)	EKK_ekozig_rendszer_ertekelesi_modszertan_080919_V4.doc
Méret (Size)	
Ár (Price)	
Felhasználási jogok (UserRights)	Korlátlan

Verziókövetési táblázat

A dokumentum neve	Rendszerekre vonatkozó értékelési módszertan
A dokumentum készítőjének neve	Hunguard Kft
A dokumentum jóváhagyójának neve	
A dokumentum készítésének dátuma	2008.09.19.
Verziószám	**V4**
Összes oldalszám	219
A projekt azonosítója	E-közigazgatási keretrendszer kialakítása

Változáskezelés

Verzió	Dátum	A változás leírása
V0.1	2008.05.10.	Első tartalomjegyzék
V1	2008.05.29.	Első változat
V2	2008.06.20.	Módosítások
V3	2008.08.01	Átadott
V4	2008.09.19.	Végleges változat

Szövegsablon

Megnevezés	**Leírás**
1. Előszó (Foreword)	1. fejezet
2. Bevezetés (Preamble)	2. fejezet
3. Alkalmazási terület (Scope)	
4. Rendelkező hivatkozások (References)	
5. Fogalom-meghatározások (Definitions)	
6. A szabvány egyedi tartalma (UniqueContent)	
7. Bibliográfia	nincs
8. Rövidítésgyűjtemény	9. fejezet
9. Fogalomtár	
10. Ábrák	szövegben
11. Képek	nincs
12. Fogalmak	5. fejezet
13. Verzió	V4
14. Mellékletek (Appendix)	nincs

Tartalomjegyzék

1. Előszó

Jelen dokumentum az e-Közigazgatási Keretrendszer részét képezi.

Az elkészült e-közigazgatási alkalmazásokat, valamint az ezeket biztosító informatikai rendszereket használatbavétel előtt meg kell vizsgálni, hogy megfelelnek-e a rájuk vonatkozó biztonsági követelményeknek.

A megfelelőség vizsgálatra alkalmazható biztonság értékelési módszertan a követelménytár alábbi dokumentumaiban található:

- Termékekre vonatkozó értékelési módszertan [7],
- Összetett termékekre vonatkozó értékelési módszertan [8],
- Rendszerekre vonatkozó értékelési módszertan (jelen dokumentum).

A jelen dokumentumban kifejtett rendszer szintű értékelési módszertan felhasználja a rendszert alkotó összetevőkre (termékekre, illetve összetett termékekre) korábban elvégzett értékelési és tanúsítási munkák eredményeit.

Ez a rendszer szintű értékelési módszertan meghatározza az értékelési bizonyítékok létrehozásához kapcsolódó rendszer integrátori feladatokat, valamint a biztonságot értékelők feladatait.

Az értékelési módszertan a rendszer életciklusának különböző szakaszaiban alkalmazható:

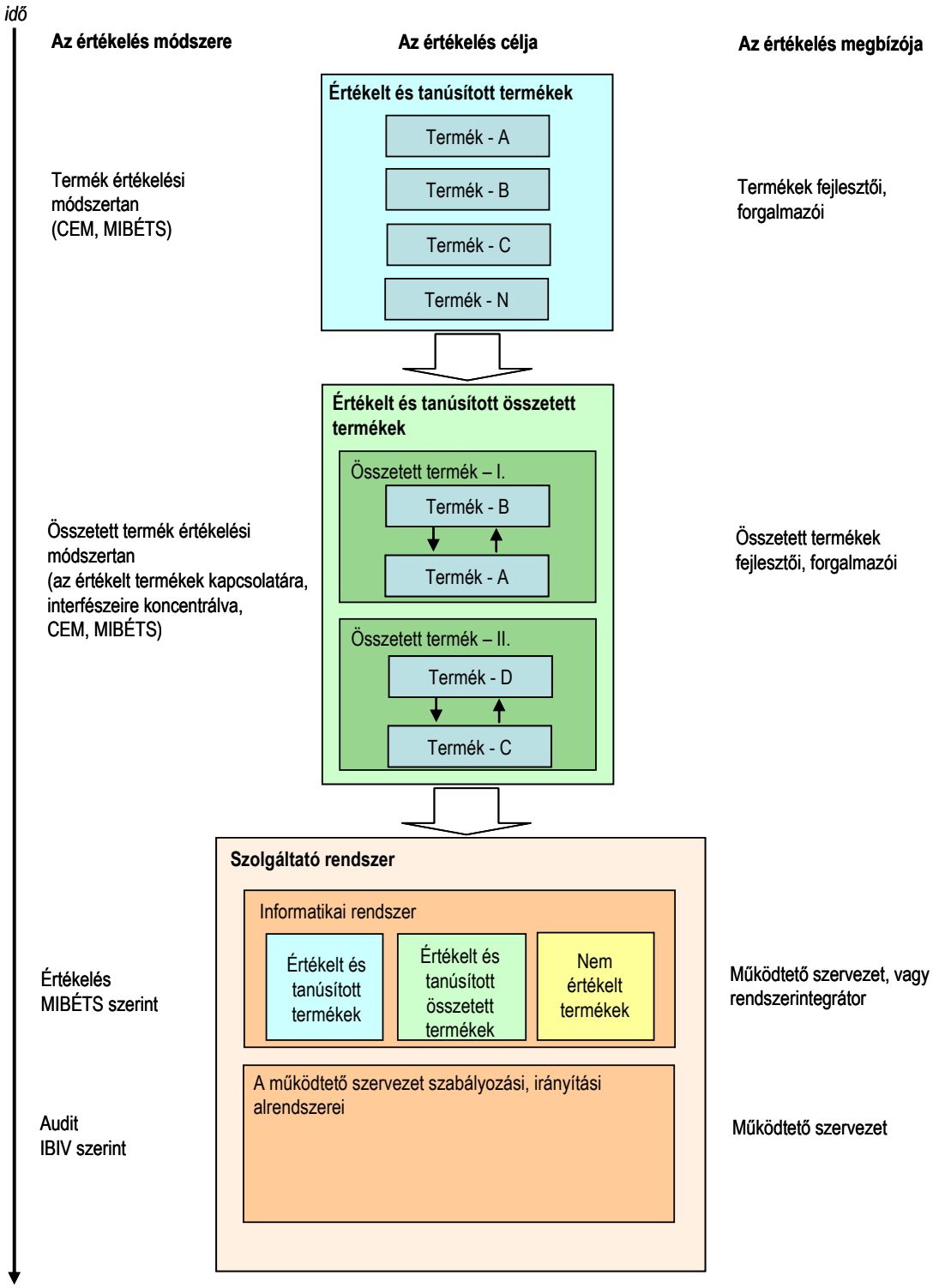
- A fejlesztés/beszerzés, illetve a megvalósítás/integrálás szakaszán belül végrehajtható a rendszer kezdeti értékelése.
- Az üzemeltetés/karbantartás szakaszában pedig a felülvizsgálati rendszer értékelések két típusa hajtható végre: a rendszeresen (tipikusan évente) végrehajtandó tervezett felülvizsgálati értékelés, illetve a jelentősebb módosításokat követő rendkívüli felülvizsgálati értékelés.

A jelen dokumentumban meghatározott értékelési módszertan végrehajtásához kapcsolódó kiegészítéseket, kritikus fontosságú részterületekre vonatkozó gyakorlati útmutatókat tartalmaz a követelménytárban megtalálható alábbi két dokumentum:

- Útmutató rendszer integrátorok számára (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, V1, 2008.08.01) [3],
- Útmutató rendszer értékelők számára (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, V1, 2008.08.01) [4].

Jelen módszertan alapja a Common Criteria [1], de kidolgozása során figyelembe vették annak működő rendszerekre való továbbfejlesztésének egy lehetséges megközelítését [10], valamint a szerzők működő rendszerek biztonsági értékelésére vonatkozó gyakorlati tapasztalatait is.

A három (termék, összetett termék, rendszer) értékelési módszertan kapcsolatát mutatja a következő ábra:



1. ábra – A három értékelési módszertan

2. Bevezetés

2.1. A dokumentum célja

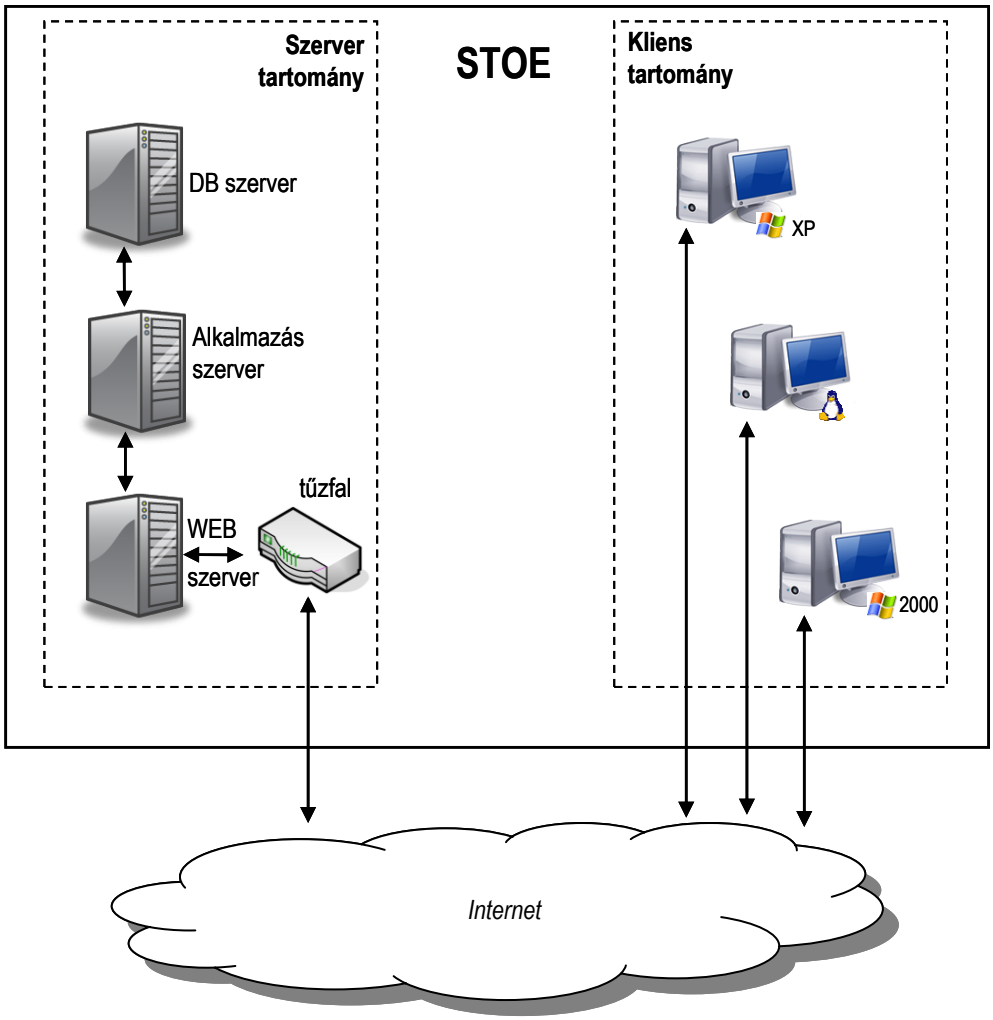
Az elkészült e-közigazgatási alkalmazásokat, valamint az ezeket biztosító informatikai rendszereket használatbavételük, illetve a Központi Rendszerre történő kapcsolódásuk engedélyezése előtt meg kell vizsgálni, hogy megfelelnek-e a rájuk vonatkozó biztonsági követelményeknek.

A jelen dokumentum célja a működő informatikai rendszerek megfelelőség vizsgálatára alkalmazható általános biztonság értékelési módszertan kifejtése. Ez a módszertan meghatározza az értékelési bizonyítékok létrehozásához kapcsolódó rendszer tulajdonosi és rendszer integrátori feladatokat, valamint a biztonságot értékelők feladatait.

A rendszer szintű értékelés jelentős mértékben támaszkodik a rendszer komponenseire (termékekre és összetett termékekre) korábban már elvégzett értékelések eredményeire.

A rendszer értékelés módszertana is több szempontból hasonlít a termékek és összetett termékek biztonsági értékelésére alkalmazható módszertanra. Ugyanakkor jelentős különbségek is vannak, amelyek alapvetően két dologból fakadnak:

- a működő rendszerek sokkal összetettebbek, mint egy-egy termék (a termékekre elvárt értékelési mélység és formalizmus tehát rendszer szinten kivitelezhetetlen),
- A működő rendszernek több olyan különböző részeleme lehet, amelyekkel szembeni biztonsági elvárások (az általuk kezelt adatok, a működtetés környezete, … szempontjából) nem egyformák, nem lehet, vagy nem célszerű azonos szigorúságú követelményeket megfogalmazni, azonos mélységben értékelni. Ezen különböző biztonsági tartományokat mutatja a 2. ábra (az ábrán az egyszerűsítés érdekében – a rendszer értékelés tárgyaként /STOE/ két biztonsági tartományt (azonos biztonsági szabályzat érvényessége alá tartozó területet, eszközöket) jelöltünk, a példában egy szerver- és egy kliens tartományt, melyek technológiai követelményei és értékelési mélysége is különböző,
- egy rendszer konkrét üzemeltetési környezete (benne a konkrét konfigurációk és az alkalmazott üzemeltetési intézkedések) pontosan ismert és vizsgálható (szemben a különböző környezetekben való felhasználásra tervezett termékekkel).



2. ábra – Példa elkülönülő biztonsági tartományokra

A jelen dokumentumban ismertetett rendszer értékelési módszertan összhangban van az [5] által szolgáltató rendszerekre meghatározott életciklus szakaszokkal, valamint a [7] és [8] által leírt értékelési módszertanokkal.

2.2. A dokumentum felépítése

Az 1. fejezet elhelyezi a dokumentumot az e-Közigazgatási Keretrendszeren belül, tájékoztatást adva a célközönségről és a kapcsolódó dokumentumokról.

A 2. fejezet bevezető információkat tartalmaz, megadva a dokumentum célját és felépítését.

A 3. fejezet meghatározza az alkalmazás lehetséges területeit.

A 4. és 5. fejezet a hivatkozásokat, illetve a fogalom-meghatározásokat tartalmazza.

A 6. fejezet tartalmazza a dokumentum lényegi részét, 2 alfejezetben.

A 6.1 alfejezet a biztonsági értékelések előkészítői feladatait határozza meg, elsősorban a rendszer tulajdonosok számára, akik ezeket a feladatokat a gyakorlatban csak a rendszer integrátorok aktív közreműködésével képesek elvégezni.

A 6.1.1 alfejezet általánosan jellemzi a működő (szolgáltató) rendszerek értékelését, megkülönböztetve ezt a termékek értékelésétől.

A 6.1.2 alfejezet ismerteti az értékelési rendszer garanciacsomag fogalmát, majd áttekinti a hierarchikus kapcsolatban álló 3 garanciacsomagot (alap, fokozott és kiemelt).

A 6.1.3 alfejezet „ellenőrző lista”-ként használható módon azokat az előkészítő feladatokat tekinti át (a később részletezettekre való hivatkozással), amelyeket egy rendszer biztonsági értékelés előkészítése érdekében kell elvégezni (a különböző értékelési garanciacsomagok szerint elkülönített csoportosításban).

A 6.1.4 alfejezet meghatározza az egyik fő előkészítő feladatot: a rendszer biztonsági előirányzat elkészítését, mely a három garanciacsomagban jelentősen eltérő feladat (alap szinten lényegesen egyszerűbb, fokozott szinten egyszerűbb, mint a kiemelt szint elvárása, mely utóbbi lényegében a CC [1] biztonsági előirányzatra vonatkozó elvárását általánosítja rendszerekre).

A 6.1.5 – 6.1.9 alfejezetek részletezik a másik fő értékelés előkészítő feladatot: a rendszerekre vonatkozó értékelési bizonyítékok elkészítését. Ehhez az egyes alfejezetek részletesen tárgyalják a rendszer értékelésre vonatkozó 5 garanciaosztályt (Rendszer fejlesztés, Rendszer útmutató dokumentumok, Rendszer konfiguráció kezelés, Rendszer tesztelés, Rendszer sebezhetőség felmérés), az ezekhez tartozó garanciacsaládokat és garancia-összetevőket, meghatározva egyúttal a garancia-összetevők által elvárt tartalmi és formai követelményeket is.

A 6.1.10 alfejezet a rendszer értékelésével megszerzett garancia folyamatosságának fenntartásával foglakozik, kiegészítve a [6] által tárgyalt általános megközelítést

A 6.2 alfejezet a rendszer értékelés feladatait határozza meg.

A rendszer értékelőknek természetesen valamennyi előkészítő feladatot is ismerniük kell. Ez az alfejezet olvasóiról feltételezi a 6.1 alfejezet által meghatározottak ismeretét is.

A 6.2.1 alfejezet a rendszer különböző életciklusában végrehajtott (kezdeti és felülvizsgálati) értékelések feladatait tekinti át.

A 6.2.2 - 6.2.4 alfejezetek a rendszer kezdeti értékelésére választott különböző garanciaszintek (alap, fokozott vagy kiemelt garanciacsomag) mellett megadják az egyre bővülő és szigorodó értékelési követelmények teljesülésére vonatkozó vizsgálatok és elemzések módszertani részleteit.

A 6.2.5 alfejezet a felülvizsgálati értékelés értékelői feladatait, s ezek módszertani részleteit határozza meg.

A 7. fejezet mellékleteket tartalmaz.

A 7.1 melléklet a rendszer értékelési munkaterv, a 7.2 pedig a rendszer értékelési jelentés elvárt felépítését és tartalmát határozza meg.

A 8. - 14. fejezetek kiegészítő információkat tartalmaznak (8. Bibliográfia, 9. Rövidítésgyűjtemény, 10. Fogalomtár, 11. Ábrák, 12. Képek, 13. Táblázatok, 14. Verziószám).

3. Alkalmazási terület

A jelen dokumentumban a rendszerek biztonsági értékelésére meghatározott módszertan elsődlegesen a közigazgatási operatív programok keretében megvalósított szolgáltató rendszerek biztonsági értékelésére vonatkoznak. Ezáltal a közigazgatási fejlesztési operatív programok végrehajtásával elkészülő rendszerekre irányuló megfelelőségi vizsgálatok eljárásrendjének részét képezi.

A rendszerek biztonsági értékelési módszertana az elektronikus közigazgatáson kívül, a közszféra más területein, valamint a magánszférában is alkalmazható, minden olyan esetben, amikor rendszerek megfelelőség vizsgálatára, ezen belül biztonsági értékelésére van szükség.

4. Rendelkező hivatkozások

A jelen dokumentumban megfogalmazott irányelvek és követelmények az alábbi mértékadó dokumentumokon alapulnak:

[1]: Common Criteria for Information Technology Security Evaluation (September 2006 - version 3.1, revision 2) – Part 1: Introduction and general model – Part 2: Security functional components - Part 3: 3: Security assurance components

[2]: IT biztonsági műszaki követelmények a különböző biztonsági szintekre (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, V1, 2008.08.01)

[3]: Útmutató rendszer integrátorok számára (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, V1, 2008.08.01)

[4]: Útmutató rendszer értékelők számára (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, V1, 2008.08.01)

[5]: NIST Special Publication 800-30 – Risk Management Guide for Information Security Systems (July 2002)

[6]: Az értékeléssel megszerzett garancia folyamatosságának biztosítása (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, V2, 2008.06.08)

[7]: Termékekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, V2, 2008.06.08)

[8]: Összetett termékekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, V2, 2008.06.08)

[9]: Szolgáltatások megfelelőség vizsgálatának folyamata és eljárásai (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, V3, 2008.08.01)

[10]: ISO/IEC TR 19791: 2006 Information technology – Security techniques – Security assessment of operational systems

Az 1. táblázat a rendelkező hivatkozások elérhetőségét adja meg.

1. táblázat - A rendelkező hivatkozások elérhetősége

Cím	Külföldi elérhetőség	Magyar elérhetőség
Common Criteria for Information Technology Security Evaluation (September 2006 -version 3.1, revision 2) – Part 1: Introduction and general model – Part 2: Security functional components - Part 3: Security assurance components	CCPart1v3.1R1 CCPart2v3.1R1 CCPart3v3.1R1	
IT biztonsági műszaki követelmények a különböző biztonsági szintekre		e-Közigazgatási Keretrendszer
Útmutató rendszer integrátorok számára		e-Közigazgatási Keretrendszer
Útmutató rendszer értékelők számára		e-Közigazgatási Keretrendszer
NIST Special Publication 800-30 – Risk Management Guide for Information Security Systems (July 2002)	NIST SP 800-30	
Az értékeléssel megszerzett garancia folyamatosságának biztosítása		e-Közigazgatási Keretrendszer
Termékekre vonatkozó értékelési módszertan		e-Közigazgatási Keretrendszer
Összetett termékekre vonatkozó értékelési módszertan		e-Közigazgatási Keretrendszer
Szolgáltatások megfelelőség vizsgálatának folyamata és eljárásai		e-Közigazgatási Keretrendszer
ISO/IEC TR 19791: 2006 Information technology – Security techniques – Security assessment of operational systems	ISO/IEC TR 19791: 2006	

5. Fogalom-meghatározások

Jelen dokumentum az alábbi kiegészítő fogalmakra épül, s ezeket az alábbi értelemben használja:

Alrendszer: Az értékelt rendszer (STOE) tervlebontásának egyik szintje (lásd még komponens és modul). Ez elősegíti annak magas szintű leírását, hogy az STOE egyes nagyobb részei mit és hogyan végeznek. Egy alrendszert tovább lehet bontani komponensekre (termékekre) vagy modulokra.

Általános határozat: „Megfelelt" vagy „nem felelt meg" nyilatkozat, amelyet egy értékelő bocsát ki egy értékelés eredményét illetően.

Biztonsági cél: Szándéknyilatkozat azonosított fenyegetések elleni fellépésről és/vagy meghatározott szervezeti biztonsági szabályzatoknak és feltételezésnek való megfelelésről.

Biztonsági követelmények: Az informatikai biztonsági célok lebontása biztonsági funkcionalitásra (SFR) és garanciára (SAR) vonatkozó szakmai követelmények egy összességére, melyek az értékelt rendszerre és annak üzemeltetési környezetére vonatkoznak.

Biztonsági tartomány: Működő informatikai rendszerek különböző alrendszereinek ugyanazon biztonsági szabályzat alá eső részei.

Biztonsági tulajdonság: Szubjektumokkal, felhasználókkal és/vagy objektumokkal társított olyan információ, amelyet az értékelt rendszerre vonatkozó rendszer biztonsági szabályzat érvényre juttatására használnak.

Család: Összetevők egy olyan csoportja, melyek azonos biztonsági célokkal kapcsolatosak.

Csomag: Összetevők egy közbenső kombinációja. Egy csomag olyan összetartozó követelményeket tartalmaz, amelyek biztonsági célok egy adott részhalmazának felelnek meg.

E-közigazgatási keretrendszer: A Közigazgatási Operatív Programok során alkalmazandó egységes követelményrendszer, amely az egyenszilárdságot és interoperabilitást hivatott biztosítani.

Elem: Oszthatatlan biztonsági követelmény.

Ellenőrizni: (igehasználat követelményen belül): Értékelői határozat előállítása egy egyszerű összehasonlítás segítségével. Értékelői szaktudást nem igényel.

Értékadás: Az egyik megengedett művelet összetevőkön.

Értékelés: Rendszer biztonsági előirányzat, vagy informatikai rendszer felmérése meghatározott szempontok (pl. a CC vagy a MIBÉTS módszertana) alapján.

Értékelési átadandó: Bármely forrás, amelyet az értékelő szervezet kér be a rendszer tulajdonostól vagy a rendszer integrátortól abból a célból, hogy egy vagy több értékelési tevékenységet hajtson végre.

Értékelési bizonyíték: Kézzelfogható értékelési átadandó.

Értékelési garanciaszint: A CC. 3 részének olyan garancia-összetevőiből álló csomag, amelyek egy-egy pontot képviselnek a CC előre meghatározott garanciális skáláján.

Értékelés tárgya: Az az informatikai rendszer, valamint a hozzá kapcsolódó útmutatók, amelyre az értékelés irányul.

Értékelői akció: A CC 3. részben megadott értékelői tevékenység elem. Ezek az akciók vagy közvetlenül értékelői akcióként vannak megadva, vagy pedig közvetett módon, a fejlesztői (rendszer integrátori) akciókból vannak származtatva (származtatott értékelői akciók) a CC 3. rész garancia-összetevőin belül.

Értékelői altevékenység: Az egyik garancia-összetevő alkalmazása. Az értékelési módszertan nem közvetlenül garanciacsaládokra irányul, az értékeléseket egy garanciacsaládból származó valamelyik garancia-összetevőre hajtják végre.

Értékelői tevékenység: Az egyik garanciaosztály (ASST, ASDV, ASGD, ASCM, ASTE, ASVA) alkalmazása.

Észrevételezési jelentés: Jelentés, amelyet az értékelő abból a célból készít, hogy az értékelés során felmerülő kérdések tisztázását kérje, vagy azonosítson egy problémát.

Felhasználó: Az értékelt rendszeren kívüli bármely olyan entitás (humán felhasználó vagy egy külső informatikai entitás), amely kölcsönhatásban áll az értékelt rendszerrel.

Függőség: Két összetevő között függőség lép fel, ha az egyik összetevő önmagában nem elegendő, és egy másik összetevő fennállására támaszkodik.

Garancia: Biztosíték arra nézve, hogy egy egyed megfelel a rá vonatkozó biztonsági céloknak.

Garanciaosztály: Garanciacsaládok egy olyan csoportja, melyek közös feladatokhoz kapcsolódnak. A jelen dokumentumban meghatározott garanciaosztályok az alábbiak: Rendszer biztonsági előirányzat (ASST), Rendszer fejlesztés (ASDV), Rendszer útmutató dokumentumok (ASGD), Rendszer konfiguráció kezelés (ASCM), Rendszer tesztelés (ASTE) és Rendszer sebezhetőség felmérés (ASVA).

Hamisítás: Olyan általános támadási módszer, mely azon alapul, hogy egy támadó megpróbálja a rendszer biztonsági funkcionalitásának (SSF) működését befolyásolni (azaz módosítani vagy hatástalanítani).

Határozat: „Megfelelt” , „nem felelt meg” vagy „nem bizonyított” nyilatkozat, amelyet egy értékelő bocsát ki egy értékelői akcióelemet, garancia-összetevőt vagy garanciaosztályt illetően. (Lásd még általános határozat.)

Informális: Természetes nyelven kifejezett.

Interfész: Különböző informatikai rendszerek közötti, illetve egy informatikai rendszer és felhasználói közötti adatátadást megvalósító rendszerkomponens.

Ismétlés: Az egyik megengedett művelet összetevőkön.

Jelenteni, jelentésbe foglalni (igehasználat követelményen belül): Az értékelési eredmények és az ezeket alátámasztó anyagok belefoglalása egy rendszer értékelési jelentésbe vagy egy észrevételezési jelentésbe.

Kiterjesztés: A biztonsági előirányzat kiegészítése olyan funkcionális biztonsági követelményekkel, amelyek nem szerepelnek a CC 2. részében.

Kiválasztás: Az egyik megengedett művelet összetevőkön.

Komponens: Az értékelt rendszer (STOE) tervlebontásának egyik szintje (lásd még alrendszer és modul). A komponensek a rendszerbe integrált késztermékeket jelentik. A termék szinten értékelt és tanúsított komponensek a rendszer szintű értékelési módszertan alapját, kiinduló pontját biztosítják.

Konfiguráció kezelés (CM) dokumentáció: CM felhasználói dokumentáció és a CM kimenettel együtt.

Konfiguráció kezelés (CM) felhasználói dokumentáció: A CM rendszer részét képező dokumentáció, ami azt írja le, hogy a CM rendszert hogyan határozzák meg és hogyan használják.

Konfiguráció kezelés (CM) kimenet: CM-el kapcsolatos eredmények, melyeket a CM rendszer állít elő vagy juttat érvényre (lehetnek dokumentumok és tevékenységek).

Konfiguráció lista: CM kimeneti dokumentáció, ami felsorolja egy adott rendszer összes konfiguráció elemét, s ezek pontos verzióazonosítóit.

Konfiguráció kezelés (CM) rendszer: Általános kifejezés egy rendszer tulajdonos vagy rendszer integrátor által használt összes eljárásra és eszközre (ideértve a dokumentációkat), amelyek a rendszer konfigurációjának fenntartását szolgálják a rendszer teljes életciklusában.

Konfiguráció kezelés (CM) terv: A CM dokumentáció része, ami azt írja le, hogyan alkalmazzák a CM rendszert egy adott rendszer esetén. (A teljes CM rendszer szempontjából ez egy kimenet dokumentum, amit a CM rendszer alkalmazása során készíthetnek el.)

Közigazgatási informatikai rendszer: A közigazgatási területen alkalmazott, központi szolgáltatásokat megvalósító vagy támogató, illetve ilyen célt szolgáló informatikai rendszer.

Központi Rendszer: A Központi Elektronikus Szolgáltató Rendszer (a továbbiakban: Központi Rendszer) olyan elektronikus rendszer, amely együttesen magában foglalja az elektronikus kormányzati gerinchálózatot, a kormányzati portált, az ügyfélkaput, a kormányzati ügyfél-tájékoztató központot, valamint az ezeken megjelenő, ezeken keresztül elérhető elektronikus szolgáltatásokat. A Központi Rendszer működtetője a Miniszterelnöki Hivatal.

Közvetlen támadás: Olyan általános támadási módszer, mely a permutáción vagy valószínűségen alapuló mechanizmusok feltörésére irányul (pl. az összes lehetséges eset kipróbálásának elvét alkalmazva).

Megkerülés: Olyan általános támadási módszer, mely révén egy támadó megkerülheti a biztonság érvényre juttatását.

Megvizsgálni (igehasználat követelményen belül): Határozat előállítása egy értékelői szaktudást alkalmazó vizsgálat segítségével. Az ezt az igét használó megállapítás meghatározza, hogy mi, és milyen tulajdonságokra vonatkozóan lett vizsgálva.

Modul: Az értékelt rendszer (STOE) tervlebontásának egyik szintje (lásd még alrendszer és komponens). A modul a funkcionalitás legspecifikusabb leírása: ez a megvalósítás leírása. A modul segítségével egy fejlesztő további tervezési döntés nélkül képes az STOE leírt részét megvalósítani.

Módszertan: Elvek, eljárások és folyamatok rendszere, amelyet az informatikai biztonság értékelésére használnak.

Munkaegység: Az értékelői munka legjobban részletezett szintje.

Művelet: Az összetevőket pontosan a biztonsági követelmények katalógusában ([1] és [2]) megadottaknak megfelelően lehet használni, de megengedett műveletek alkalmazásával testre is szabhatóak egy meghatározott biztonsági szabályzat kielégítése, illetve egy meghatározott fenyegetés kivédése érdekében. Minden összetevő meghatározza a megengedett műveleteket, azokat a körülményeket, amelyek mellett ezek alkalmazhatók és az alkalmazás végeredményeit. A megengedett műveletek [1] alkalmazása esetén: ismétlés, értékadás, kiválasztás és pontosítás, míg [2] alkalmazása esetén: értékadás és kiválasztás.

Objektum: Az értékelt rendszer ellenőrzési körén belül található olyan entitás, amely információt tartalmaz vagy fogad, és amelyen szubjektumok műveleteket hajtanak végre.

Összetevő: Valamely csomag vagy rendszer biztonsági előirányzat számára választható elemek legkisebb összessége.

Pontosítás: Az egyik megengedett művelet összetevőkön.

Rendszer: Lásd közigazgatási informatikai rendszer

Rendszer biztonsági előirányzat (SST): Biztonsági követelmények és előírások olyan összessége, amelyet egy értékelt rendszerre, az értékelés alapjaként használnak.

Rendszer biztonsági funkcionalitás (SSF): Az értékelt rendszer mindazon részei, amelyekre a rendszer biztonsági szabályzatának helyes érvényre juttatásához támaszkodni kell, illetve lehet.

Rendszer biztonsági szabályzat: Egy vagy több biztonsági szabály, eljárás, gyakorlat vagy útmutató, amelyet egy informatikai rendszer biztonságos működtetéséhez a rendszer tulajdonosa állít fel.

Rendszer értékelési garanciacsomag (SAP): A jelen dokumentum által meghatározott olyan garancia-összetevőkből álló csomag, amelyek egy-egy pontot képviselnek egy előre meghatározott garanciális skálán. Jelen dokumentum a garanciális skála alábbi három szintjét különbözteti meg: alap (SAP-A), fokozott (SAP-F), kiemelt (SAP-K)

Rendszer értékelési jelentés (SER): Jelentés, amely dokumentálja az általános határozatot és annak indoklását, és amelyet az értékelő állít elő és ad át az értékelés megbízójának és a rendszer akkreditorának.

SAR: Garanciális biztonsági követelmény. (lásd még biztonsági követelmények).

SFR: Funkcionális biztonsági követelmény. (lásd még biztonsági követelmények).

SFR-t érvényre juttató (interfész/alrendszer/modul): Az értékelt rendszer (STOE) olyan részei (interfész/alrendszer/modul), melyek közvetlen szerepet játszanak valamely SFR megvalósításában a TOE-n.

SFR-t támogató (interfész/alrendszer/modul): A TOE olyan részei (interfész/alrendszer/modul), melyek nem juttatják érvényre az SFR-ket, de ebben alátámasztó szerepet játszanak.

SFR-be nem beavatkozó (interfész/alrendszer/modul): A TOE olyan részei (interfész/alrendszer/modul), melyeknek nincs szerepük az SFR-ek megvalósításában, és valószínűleg a környezetük miatt részei a TSF-nek.

Szervezeti biztonsági szabályzat (OSP): Egy vagy több biztonsági szabály, eljárás, gyakorlat vagy útmutató, amelyet egy szervezet saját biztonságos működtetéséhez állít fel.

Szolgáltató (működő, informatikai) rendszer: Egy konkrét informatikai elrendezés meghatározott céllal és üzemeltetési környezettel.

Szubjektum: Az értékelt rendszer ellenőrzési körén belül található olyan entitás, amely a műveletek végzését kiváltja.

Támadó képesség: Támadás esetén annak érzékelt lehetősége, hogy a támadás sikeres lesz, a támadó szaktudásával, erőforrásaival és motivációjával kifejezve (Lehetséges szintjei: alap, megemelt-alap, közepes, magas, A jelen dokumentumban leírt értékelési módszertan lehetséges szintjei: alap, megemelt-alap).

Termék: Informatikai szoftver, förmver és/ vagy hardver által alkotott csomag, amelyek adott használatra vagy különböző szolgáltató rendszerekbe való beépítésre tervezett funkciókészletet biztosítanak.

Visszaélés (helytelen használat): Olyan általános támadási módszer, mely az alábbiakat igyekszik kihasználni a biztonság érvényre juttatásának megakadályozására: hiányos útmutató dokumentáció, ésszerűtlen útmutatók, az STOE véletlenül rossz konfigurálása, az SSF kikényszerített kivételes viselkedése.

6. Rendszerekre vonatkozó informatikai biztonsági értékelési módszertan

6.1. A rendszer integrátorok előkészítő feladatai az informatikai rendszerek biztonsági értékeléséhez

6.1.1. Szolgáltató rendszerek értékelésének jellemzése

6.1.1.1. A szolgáltató rendszerek jellemzése

Egy szolgáltató rendszer kivételes esetben állhat egyetlen termékből, annak egy vagy több funkcióját nyújtva.

Általában azonban egy szolgáltató rendszer több különböző komponensből áll. Egy ilyen rendszer lehet több termékből alkotott egyetlen kliens vagy szerver; több szerver és/vagy kliens és hálózat, heterogén kliensek és szerverek összessége.

Egy szolgáltató rendszerben egyes komponensek lehetnek értékeltek, míg mások nem.

Egy szolgáltató rendszer általában:

a) Több alrendszert és még több komponenst tartalmaz, különböző szintű és típusú garanciával.
b) Meghatározott igények kielégítésére készítették, általában számos funkciót biztosítanak.
c) Az alkotó komponensek sokféle lehetséges konfigurációs beállítási lehetőséget hordoznak magukban, melyek némelyike nincs összhangban a rendszer biztonsági szabályzatával.
d) Jól definiált felügyeleti struktúrával rendelkezik, melyet általában a rendszer tulajdonos biztosít.
e) Lehetővé teszi a rendszer tulajdonos számára, hogy mérlegeljen a műszaki és az üzemeltetési biztonsági intézkedések használata között.
f) Folyamatos változtatási képességet és időszakos alkalmazkodást kíván mind műszakilag, mind az üzemeltetési követelmények tekintetében.

Egy szolgáltató rendszer kialakításakor azonosítani és jellemezni kell a rendszer határait, le kell írni az interfészeket és a rendszer komponensei közötti függéseket, továbbá a komponensek és a környezet közötti interfészeket és függéseket is. A komponensek közötti bizalmi kapcsolatokat is meg kell adni, csakúgy, mint az interfész (kommunikációs) összeköttetésekre vonatkozó biztonsági követelményeket.

A több funkciós rendszerek különböző alrendszereire eltérő biztonsági szabályzatok vonatkozhatnak. Egy ilyen rendszer ugyanazon biztonsági szabályzat alá eső részeit biztonsági tartománynak is nevezik. Minden biztonsági tartományra külön megadhatók a funkcionális és garanciális követelmények, így minden tartomány rendelkezni fog egy saját biztonsági szabályzattal, biztonsági probléma meghatározással, biztonsági célokkal, követelményekkel és specifikációkkal. Minden tartományok egyúttal a nagyobb rendszer általános szabályai, biztonsági problémái, céljai, követelményei és specifikációi körén belül működik. Az egyes tartományoknak lehet saját garanciális követelményrendszere, az adott tartományhoz szükséges bizalom foka és a teljes rendszerhez való hozzájárulása alapján.

A rendszer biztonsági előirányzat adja meg a teljes rendszer biztonsági követelményeit, kitérve a rendszert alkotó biztonsági tartományok speciális elvárásaira is.

6.1.1.2. A rendszer értékelés jellemzői

Egy termék és egy rendszer értékelése közötti fő különbség, hogy egy rendszer értékelése figyelembe veheti az üzemeltetési környezet biztonsági intézkedéseit, míg termék értékeléseknél ez csak feltételezésként szerepelhet.

Egy rendszer általában összetettségében és teljességében is eltér egy terméktől, az alábbi módokon:

a) a rendszert biztonsági tartományokba szervezett több termék alkotja;
b) a rendszer biztonsági tartományokat alkothatja ugyanazon terméktípus több példánya (például: ugyanattól a gyártótól származó operációs rendszerek több példánya), vagy ugyanazon terméktípus több különböző terméke (például: különböző gyártóktól származó több tűzfal);
c) az üzemeltetési környezet biztonsági intézkedései közvetlenül a rendszer részének számítanak. Egy termék esetén feltételezik, hogy ezek az intézkedések léteznek majd a környezet részeként, de nem mérik fel azokat;
d) egy rendszer több olyan szabályzattal is rendelkezhet, amelyek egyes tartományokra vonatkoznak, míg másokra nem.

Egy termék értékelés folyamata feltételez egy általános üzemeltetési környezetet, melyben a terméket el lehet helyezni. A termék értékelés középpontjában a termék által megvalósított, üzemeltetési környezettől független biztonsági tulajdonságok ellenőrzése áll.

Egy termék értékelés elsődleges célja arra vonatkozó garancia megszerzése, hogy a termék biztonsági képességeit megfelelően, helyesen valósították-e meg. A termék értékelés hatóköre a termékre megfogalmazott IT biztonsági követelményekre korlátozódik. Egy termék értékelt konfigurációi nem vesznek figyelembe semmilyen sajátos környezetet, mivel ezek nem ismertek az értékelés idején.

A termék értékelés befejezése után szükség van az értékelt termék más termékekkel való megfelelő összeépítésére, hogy együtt alkossanak egy szolgáltató rendszert, és az így integrált rendszerre ellenőrizni kell, hogy megfelel-e a kívánt biztonsági tulajdonságoknak és viselkedésnek az üzemeltetési környezetben és az üzemeltetési konfigurációban. A termék

értékelés eredményei (értékelési jelentés, tanúsítási jelentés, tanúsítvány) felhasználhatók a termékekből szolgáltató rendszert integráló munka ellenőrzése során.

A rendszer értékelés során azokat a speciális biztonsági intézkedéseket is figyelembe vehetik, amelyeket abban az üzemeltetési környezetben valósítottak meg, amelyben a rendszert használják.

Egy rendszer értékelés elsődleges célja arra vonatkozó garancia megszerzése, hogy a rendszer műszaki és üzemeltetési biztonsági képességeit megfelelően, helyesen és hatékony módon valósították meg. Kiegészítő cél a konfigurált műszaki és üzemeltetési intézkedések kombinálása után maradó kockázat szintjének meghatározása. A maradványkockázat elfogadhatóságára vonatkozó döntés már nem értékelői feladat, ez vezetői felelősség,.

Egy rendszert az ismert üzemeltetési környezet kockázatai alapján biztonsági tartományokra lehet osztani. A környezeti tényezők eltérő veszélyeket jelenthetnek a rendszer komponensei számára. Valószínűleg a rendszer egyes részei nagyobb, míg mások alacsonyabb garanciaszintet igényelnek.

A rendszer értékelés kritikus része azoknak a garanciális intézkedéseknek a meghatározása, amelyeket a rendszer különböző részeire kell alkalmazni. A garanciális intézkedéseket a rendszerre a műszaki és az üzemeltetési intézkedések szerint kell alkalmazni, az alábbiakra összpontosítva:

a) a rendszer informatikai komponensek biztonsági szerkezete és elhelyezése (biztonsági architektúra);
b) a rendszer komponensekre vonatkozó funkcionális biztonsági követelmények;
c) a rendszer komponensek konfigurációja;
d) a rendszer belső működését irányító szabályzatok, szabályok és eljárások;
e) a rendszer környezet biztonsághoz hozzájáruló fizikai és személyzeti tényezők;
f) a külső rendszerekkel való kapcsolódás követelményei és szabályai.

6.1.2. Rendszer garanciacsomagok

Egy rendszer biztonsági értékelését különböző mélységben és szigorúsággal lehet elvégezni, melyet a rendszer garanciacsomagok fejeznek ki.

A jelen dokumentum által meghatározott értékelési módszertan 3 belsőleg konzisztens garanciacsomagot tartalmaz, melyeket az [1] által meghatározott garanciaosztályok összetevőinek felhasználásával alakítottak ki.

A rendszer garanciacsomagok (SAP) egy egyenletesen növekedő skálát alkotnak, melyek arányosak az elérhető garanciával, egyúttal az elért garancia nehézségével és költségével is. A jelen dokumentumban meghatározott értékelési módszertan három hierarchikusan rendezett rendszer garanciacsomagot határoz meg: alap (SAP-A), fokozott (SAP-F) és kiemelt (SAP-K). A garancia növekedését a csomagokban azzal érik el, hogy ugyanazon garanciaosztály hierarchikusan magasabb (szigorúbb) garancia-összetevőit helyettesítik be, illetve más garanciacsaládokból kiegészítő garancia-összetevőket csatolnak.

A rendszer garanciacsomagok illeszkednek a [2] által meghatározott háromszintű besoroláshoz, annak alacsony- fokozott és kiemelt kihatású biztonsági osztályaihoz.

A rendszer garanciacsomagok (SAP) szerkezete hasonló a CC értékelési garanciaszintekéhez (EAL). A két csomag típus közötti fő különbség az, hogy az EAL-ok a termék TOE-kre, míg a SAP-ok az ezekből integrált informatikai rendszerekre (STOE-kre) használhatók.

6.1.2.1. A rendszer garanciacsomagok áttekintése

A SAP-okat olyan STOE-kre lehet alkalmazni, amelyeket különböző (értékelt és nem értékelt) termék komponensekből integráltak össze.

2. táblázat - A rendszer garanciacsomagok összegzése

Garancia-osztály	**Garancia-család**	**Garancia-összetevők az egyes rendszer garanciacsomagokban**			
		Kezdeti értékelés			**Felülvizsgálat**
		SAP-A	**SAP-F**	**SAP-K**	
Rendszer biztonsági előirányzat (ASST)	ASST_INT	1	1	2	
	ASST_CCL	1	2	3	-
	ASST_SPD	-	1	1	-
	ASST_OBJ	1	2	2	-
	ASST_ECD	-	-	1	-
	ASST_REQ	1	2	3	-
	ASST_SSS	1	1	1	-
	ASST_SDI	1	1	1	-
	ASST_SDC	1	2	3	-
	ASST_SDP	-	1	1	-
	ASST_SDO	1	2	2	-
	ASST_SDE	-	-	1	-
	ASST_SDR	1	2	3	-
	ASST_SDS	1	1	1	-
Rendszer fejlesztés (ASDV)	ASDV_ARC	1	1	1	-
	ASDV_SIS	1	1	2	-
	ASDV_SDS	1	1	1	-
	ASDV_OSC	1	1	1	-
	ASDV_MOD	-	-	-	1
Rendszer útmutató dokumentumok (ASGD)	ASGD_PRE	1	2	2	-
	ASGD_OPE	1	2	2	-
	ASGD_CON	1	2	2	-
	ASGD_MOD	-	-	-	1
Rendszer konfiguráció kezelés (ASCM)	ASCM_SBC	1	2	2	2
	ASCM_ECC	1	2	3	a kezdeti értékeléstől függően: 1, 2 vagy 3
Rendszer tesztelés (ASTE)	ASTE_FUN	1	1	1	-
	ASTE_COV	1	1	1	-
	ASTE_DPT	1	2	3	-
	ASTE_IND	1	1	1	1
	ASTE_MOD	-	-	-	1
Rendszer sebezhetőség felmérés (ASVA)	ASVA_VAN	1	2	3	a kezdeti értékeléstől függően: 1, 2 vagy 3

A már értékelt termékekből való integrálás sem ad formális garanciát a termék komponensek közötti kapcsolatokra, illetve az integrálásból eredő esetleges új sebezhetőségekre nézve. A rendszer garanciacsomagok figyelembe veszik ezeket a kapcsolatokat is, és a garancia magasabb szintjein biztosítják, hogy a termék komponensek közötti interfészek is tesztelésre kerülnek. A rendszer szintű sebezhetőség elemzésére is sor kerül a komponensek integrálásából származó esetleges új sebezhetőségek felismerése céljából.

A 2. táblázat a SAP-okat összegzi. Az oszlopok a SAP-ok hierarchikusan rendezett halmazát mutatják, míg a sorok a garanciacsaládokat. A mátrixban látható számok egy adott garancia-összetevőt jelentenek.

A táblázatból látható, hogy mindhárom SAP minden garanciacsaládból legfeljebb egy összetevőt tartalmaz. Az is igaz, hogy mindhárom SAP-ban az összetevők minden garanciafüggése teljesül.

Egy informatikai rendszerre általában egy rendszer garanciacsomagot kell választani.

Kivételes esetben, amennyiben a rendszer olyan biztonsági tartományokra bontható, amelyek biztonsági problémái, céljai vagy követelményei közötti jelentős különbségek ezt indokolják, a biztonsági tartományokra külön lehet választani SAP-ot. Az ilyen választást azonban indokolni kell, az egyes biztonsági tartományra vonatkozó üzemeltetési intézkedéseket és a tartományban integrált termékek értékelésre vonatkozó állapotát is figyelembe véve.

Kivételes esetben az is lehetséges, hogy a SAP-A vagy SAP-B rendszer garanciacsomag kiválasztása mellett bizonyos garancia-összetevőket magasabb garanciacsomagból választanak. Példa erre egy olyan rendszer, melynek egészére elegendő garanciát nyújt a SAP-A, egyetlen kivétellel. A kivételt az okozza, hogy a rendszer osztott rendszer, melynek alrendszerei nyilvános kommunikációs csatornán kapcsolódnak egymáshoz. A nyilvános kommunikációs csatornán megvalósuló adatcserét külön biztonsági mechanizmusok védik, és ezek megfelelő működésének az egész rendszer szempontjából komoly biztonsági jelentősége van. A SAP-A ellenére nem elég tehát a rendszer architektúrájának megfelelő tesztelési mélység (amit a SAP-A ASTE_DPT.1 összetevője biztosít), szükség van az alrendszerek közötti interfészek tesztelésére is (amit csak az ASTE_DPT.2 összetevő biztosít).

A fenti példának megfelelő rendszer garanciacsomagot a következőképpen lehet meghatározni: SAP-A+ (megemelt SAP-A), ahol a megemelés az ASTE_DPT.2 garancia-összetevő hozzáadását jelenti (értelemszerűen ASTE_DPT.1 helyett).

A következő alfejezetek jellemzik az egyes rendszer garanciacsomagokat.

6.1.2.2. Alap rendszer garanciacsomag (SAP-A)

A SAP-A (alap rendszer garanciacsomag) akkor alkalmazható, ha egy rendszert integráltak, s a rendszer integrálás eredményének biztonságos működésére vonatkozóan független bizonyosságot igényelnek.

A SAP-A megköveteli a rendszer integrátor együttműködését a rendszer tervezési és tesztelési eredmények átadására vonatkozóan, de nem igényli a rendszert alkotó termékek fejlesztőinek bevonását.

A SAP-A olyan körülmények között alkalmazható, amikor a rendszer tulajdonosa, akkreditálója és felhasználója független, de alacsony szintű biztonsági garanciát igényel a rendszer biztonságos működésére.

A SAP-A abban az esetben alkalmazható, ha az értékelők tesztelhetik a rendszert alkotó összes termék komponenst, és minden termék komponensre rendelkezésükre állnak az útmutató dokumentumok (előkészítő, konfigurálási és üzemeltetési útmutató) és a rendszer biztonsági tervdokumentációk.

6.1.2.3. Fokozott rendszer garanciacsomag (SAP-F)

A SAP-F (fokozott rendszer garanciacsomag) lehetővé teszi egy rendszer értékelő számára, hogy az STOE-be integrált komponensek közötti kapcsolatok hatásának alrendszer (összetett termék) szintű megértésével garanciát szerezzen a rendszer biztonságos működésére.

A SAP-F megköveteli a rendszer integrátor fokozott együttműködését a rendszer tervezési és tesztelési eredmények átadására vonatkozóan, de nem igényli a rendszert alkotó termékek fejlesztőinek bevonását.

A SAP-F olyan körülmények között alkalmazható, amikor a rendszer tulajdonosa, akkreditálója vagy felhasználója közepes független biztonsági garanciát igényel, de lényeges technológiai visszaállítási munkák nélkül.

A SAP-F abban az esetben alkalmazható, ha a rendszer biztonsági funkcionalitását érvényre juttató termék komponenseket legalább fokozott értékelési garanciaszinten (vagy legalább CC EAL3-n), a rendszer biztonsági funkcionalitását támogató termék komponenseket pedig legalább alap értékelési garanciaszinten (vagy legalább CC EAL2-n) értékelték és tanúsították. Kiegészítő feltétel, hogy az értékelők tesztelhetik a rendszert alkotó összes termék komponenst, és minden termék komponensre rendelkezésükre állnak az útmutató dokumentumok (előkészítő, konfigurálási és üzemeltetési útmutató) és a rendszer biztonsági tervdokumentációk.

6.1.2.4. Kiemelt rendszer garanciacsomag (SAP-K)

A SAP-K (kiemelt rendszer garanciacsomag) lehetővé teszi egy rendszer értékelő számára, hogy az STOE-be integrált komponensek közötti kapcsolatok hatásának modul (termék) szintű megértésével maximális garanciát szerezzen a rendszer biztonságos működésére.

A SAP-K megköveteli a rendszer integrátor fokozott együttműködését a rendszer tervezési és tesztelési eredmények átadására vonatkozóan, egyben minimalizálja az igényt a rendszert alkotó termékek fejlesztőinek bevonására.

A SAP-K olyan körülmények között alkalmazható, amikor a rendszer tulajdonosa, akkreditálója vagy felhasználója közepestől magas szintig terjedő független biztonsági garanciát igényel és kész további biztonság-specifikus technológiai költségeket vállalni.

A SAP-K abban az esetben alkalmazható, ha a rendszer biztonsági funkcionalitását érvényre juttató termék komponenseket legalább kiemelt értékelési garanciaszinten (vagy legalább CC EAL4-n), a rendszer biztonsági funkcionalitását támogató termék komponenseket pedig legalább fokozott értékelési garanciaszinten (vagy legalább CC EAL3-n) értékelték és tanúsították. Kiegészítő feltétel, hogy az értékelők tesztelhetik a rendszert alkotó összes termék komponenst, és minden termék komponensre rendelkezésükre állnak az útmutató dokumentumok (előkészítő, konfigurálási és üzemeltetési útmutató) és a rendszer biztonsági tervdokumentációk.

6.1.3. A rendszer tulajdonos és a rendszer integrátor feladatainak áttekintése

Ez az alfejezet előzetesen összefoglalja azokat a feladatokat, melyet egy rendszer biztonsági értékelés előkészítése érdekében a rendszer tulajdonosának, illetve részben a rendszer integrátornak kell elvégeznie. A feladatok részletezése a későbbi alfejezetekben található.

Egy informatikai rendszer biztonsági értékelése különböző életciklus szakaszokon belül is végrehajtható, ahogyan ezt [9] 6.3.2 alfejezete részletesen kifejti. Ezzel összhangban megkülönböztethető a kezdeti, valamint a (tervezett és rendkívüli) felülvizsgálati rendszer értékelés, melyek előkészítő feladatai jelentősen különböznek.

A kezdeti rendszer értékelés előkészítői feladatait 6.1.3.1, a felülvizsgálati rendszer értékelés előkészítői feladatait pedig 6.1.3.2 tekinti át.

6.1.3.1. A kezdeti rendszer értékelés előkészítői feladatai

Az első feladat a kezdeti rendszer értékelés feltételeinek áttekintésével eldönteni az alábbi kérdéseket:

a) A rendszer értékelés mely garanciacsomagjára (SAP-A, SAP-F, SAP-K) biztosítottak a feltételek?
b) Milyen garanciacsomag (SAP-A, SAP-F, SAP-K) melletti értékelésre van igény?

Ezt a feladatot a 6.1.3.1.1 pont részletezi.

A második feladat a rendszer biztonsági előirányzat elkészítése. A rendszer biztonsági előirányzat a rendszer informatikai biztonsági követelményeit tartalmazza, illetve előírja azokat a funkcionális és garanciális biztonsági intézkedéseket, amelyeket a rendszer (mint a biztonsági értékelés tárgya) ajánl fel a kinyilvánított követelmények kielégítése érdekében. A rendszer biztonsági előirányzat alkotja a megbízó (tipikusan a rendszer tulajdonos) a rendszer integrátor és értékelő között létrejött, az értékelés tárgya biztonsági tulajdonságait és az értékelés hatókörét rögzítő megállapodás alapját.

Ezt a feladatot a 6.1.3.1.2 pont részletezi.

A harmadik feladat a rendszer biztonsági értékeléséhez szükséges értékelői bizonyítékok elkészítése. Az értékelési bizonyítékok (a rendszer biztonsági előirányzaton kívül) az alábbi csoportokra oszthatók:

a) rendszer biztonsági tervdokumentációk,
b) telepítésre, konfigurálásra és üzemeltetésre vonatkozó útmutatók,
c) rendszer konfiguráció kezelésre vonatkozó dokumentációk,
d) biztonsági tesztelésre vonatkozó dokumentációk.

Az értékelői bizonyítékok elkészítésének feladat a választott garanciacsomagtól (SAP-A, SAP-F, SAP-K) függően különböző (egyre bővülő és szigorodó) elvárásoknak való megfelelést igényel.

Ezt a feladatot a 6.1.3.1.3 pont részletezi.

6.1.3.1.1. Garanciacsomag választás (SAP-A / SAP-F / SAP-K)

Az **alap** (SAP-A) garanciacsomag akkor alkalmazható, ha:

a) a függetlenül garantált biztonság alacsonyabb szintjére van csak szükség,
b) az értékelők tesztelhetik a rendszert alkotó összes termék komponenst, és minden termék komponensre rendelkezésükre állnak az útmutató dokumentumok (előkészítő, konfigurálási és üzemeltetési útmutató) és a rendszer biztonsági tervdokumentációk.

A **fokozott** (SAP-F) garanciacsomag akkor alkalmazható, ha:

a) a függetlenül garantált biztonság **fokozott** szintjére van szükség, **lényeges technológiai visszaállítási munkák nélkül**,
b) az értékelők tesztelhetik a rendszert alkotó összes termék komponenst, és minden termék komponensre rendelkezésükre állnak az útmutató dokumentumok (előkészítő, konfigurálási és üzemeltetési útmutató) és a rendszer biztonsági tervdokumentációk,
c) a rendszer biztonsági funkcionalitását érvényre juttató termék komponenseket legalább fokozott értékelési garanciaszinten (vagy legalább CC EAL3-n), a rendszer biztonsági funkcionalitását támogató termék komponenseket pedig legalább alap értékelési garanciaszinten (vagy legalább CC EAL2-n) értékelték és tanúsították.

A **kiemelt** (SAP-K) garanciacsomag akkor alkalmazható, ha:

a) a függetlenül garantált biztonság **magasabb** szintjére van szükség, **s ehhez az értékelés megbízója vállalja a pótlólagos biztonság-technikai munkákat és költségeket,**
b) az értékelők tesztelhetik a rendszert alkotó összes termék komponenst, és minden termék komponensre rendelkezésükre állnak az útmutató dokumentumok (előkészítő, konfigurálási és üzemeltetési útmutató) és a rendszer biztonsági tervdokumentációk,
c) a rendszer biztonsági funkcionalitását érvényre juttató termék komponenseket **kiemelt** értékelési garanciaszinten (vagy legalább CC EAL**4**-n), a rendszer biztonsági funkcionalitását támogató termék komponenseket pedig legalább

fokozott értékelési garanciaszinten (vagy legalább CC EAL**3**-n) értékelték és tanúsították.

A fenti áttekintésben **vastagított betűtípus** jelzi az alacsonyabb szintekhez képesti eltéréseket. Ezt a jelölési technikát az egész 6.1 alfejezet követi, vagyis a hierarchikusan magasabb követelményekben először megjelenő új elvárásokat vagy változásokat mindig vastagított betűtípus emeli ki. (Lásd például 6.1.4.3.1 pontban az ASST_INT.2.10C és ASST_INT.2.11C elemeket.)

6.1.3.1.2. Rendszer biztonsági előirányzat készítése

Az elkészítendő rendszer biztonsági előirányzatra vonatkozó elvárásokat a 6.1.4 alfejezet tekinti át.

6.1.3.1.3. Értékelési bizonyítékok

A kezdeti rendszer értékelések előkészítéséhez szükséges értékelési bizonyítékok elkészítése a rendszer tulajdonos kötelezettsége, ugyanakkor valószínűleg ennek csak a rendszer integrátor szakmai támogatásával képes megfelelni.

Mindhárom garanciacsomag esetén az alábbi értékelési bizonyítékokat kell biztosítani (esetenként az egyes értékelési bizonyítékokra vonatkozó elvárások szigorodnak a magasabb garanciát képviselő csomagokban):

- **a) rendszer biztonsági előirányzat (lásd 6.1.4),**
- **b) rendszer biztonsági tervdokumentációk,**
  - ba) biztonsági architektúra leírás (lásd ASDV_ARC, 6.1.5.2),
  - bb) rendszer interfész specifikációja (lásd ASDV_SIS, 6.1.5.3),
  - bc) rendszer biztonsági terv (lásd ASDV_SDS, 6.1.5.4),
  - bd) rendszer-működési biztonsági koncepció (lásd ASDV_OSC, 6.1.5.5),
- **c) telepítésre, konfigurálásra és üzemeltetésre vonatkozó útmutatók,**
  - ca) előkészítő útmutató (lásd ASGD_PRE, 6.1.6.1),
  - cb) konfigurálási útmutató (lásd ASGD_CON, 6.1.6.2),
  - cc) üzemeltetési útmutató (lásd ASGD_OPE, 6.1.6.3),
- **d) konfiguráció kezeléssel kapcsolatos dokumentáció,**
  - da) CM dokumentáció a rendszer alap konfigurációjához (lásd ASCM_SBC, 6.1.7.1),
  - db) értékelt és tanúsított termék-komponensek listája (lásd ASCM_ECC, 6.1.7.2),
- **e) biztonsági tesztelésre vonatkozó dokumentáció,**
  - ea) tesztdokumentáció (lásd ASTE_FUN, 6.1.8.1),
  - eb) tesztlefedettség bizonyíték/elemzés (lásd ASTE_COV, 6.1.8.2),
  - ec) tesztmélység elemzés (lásd ASTE_DPT, 6.1.8.3),
  - ed) a tesztelésre alkalmas STOE (lásd ASTE_IND, 6.1.8.4),
- **f) rendszer sebezhetőség felmérés,**
  - fa) a tesztelésre alkalmas STOE (lásd ASVA_VAN, 6.1.9.1).

6.1.3.2. A felülvizsgálati rendszer értékelés előkészítői feladatai

Egy felülvizsgálati rendszer értékelés esetén már korábban kiválasztották a szükséges garanciacsomagot, valamint elkészült a rendszer biztonsági előirányzat is. (Amennyiben magasabb szintű garanciacsomag választásra, vagy jelentősen átdolgozott rendszer biztonsági előirányzatra lenne szükség, akkor ezt nem egy felülvizsgálati, hanem egy megismételt kezdeti értékeléssel lehet csak értékelni.)

Egy felülvizsgálati rendszer értékelésre való előkészület így az értékelési bizonyítékok elkészítését jelenti.

A tervezett és rendkívüli felülvizsgálati rendszer értékelésekhez azonos értékelési bizonyítékokra van szükség.

Az értékelési bizonyítékok elkészítése a rendszer tulajdonos kötelezettsége, de ehhez valószínűleg szüksége lesz a rendszer integrátor szakmai támogatására is (feltéve, hogy a két fél között szerződéses kapcsolat van a rendszer támogatására).

Az értékelési bizonyítékok az alábbi csoportokra oszthatók:

a) jelentés a legutolsó (kezdeti vagy felülvizsgálati) rendszer értékelés eredménye alapján készített intézkedési tervben foglalt műszaki és üzemeltetési biztonsági intézkedések megvalósításáról,
b) jelentés a legutolsó (kezdeti vagy felülvizsgálati) rendszer értékelés óta a rendszer összetevőire vonatkozó biztonsági hibakövető eljárások alkalmazásáról, valamint a rendszer szolgáltatására bejelentett és javított biztonsági hibákról,
c) az elvégzett módosítások átvezetésével az értékelési bizonyítékok aktualizálása, ezen belül az alábbiak:
   ca) a biztonsági terv dokumentációk aktualizálása (lásd ASDV_MOD, 6.1.5.6),
   cb) az útmutató dokumentációk aktualizálása (lásd ASGD_MOD, 6.1.6.4),
   cc) a regressziós tesztelés dokumentációja (ASTE_MOD, 6.1.8.5).

A felülvizsgálati rendszer biztonsági értékelést követően a rendszer tulajdonosának valószínűleg ismét szüksége lesz a rendszer integrátor szakmai támogatására, hogy a felülvizsgálati rendszer értékelési jelentésben azonosított esetleges új sebezhetőségek csökkentésére vagy kiküszöbölésére intézkedési tervet készíthessen.

6.1.4. Rendszer biztonsági előirányzat

6.1.4.1. Bevezetés

A szolgáltató rendszer (a továbbiakban STOE) értékeléséhez a rendszer integrátornak rendszer biztonsági előirányzatot (a továbbiakban SST) kell benyújtania, ami azonosítja a rendszerre alkalmazandó garanciacsomagot (SAP-A, SAP-F vagy SAP-K) is.

Az SST legfontosabb célja a szolgáltató rendszer megvalósított biztonsági képességeinek meghatározása. E biztonsági képességeket a rendszer adott üzemeltetési környezetében alkalmazzák a felmért kockázatok kivédésére és a megfogalmazott szervezeti biztonsági

szabályzatok érvényre juttatására, annak érdekében, hogy a maradványkockázat elfogadható szintjét érjék el.

A szolgáltató rendszer műszaki és üzemeltetési biztonsági intézkedések integrált kombinációjából áll.

Az SST leírja a rendszer azon funkcionális viselkedését és követelményeit, melyek megvalósítják a biztonsági célokat, műszaki és üzemeltetési alapú mechanizmusok együttese által. Az SST tárgyalja továbbá azokat az intézkedéseket, amelyek garanciát jelentenek a szolgáltató rendszer azon képességeire nézve, hogy azok teljesítik a funkcionális célokat, mialatt a rendszer a maradványkockázat elfogadható szintjén működik.

Az SST alkalmas kiindulópontot biztosít a szolgáltató rendszerek értékeléséhez. Az SST-nek ezért biztosítania kell a rendszer részletes és magyarázó leírását.

Az SST rendszer leírásának kellően részletesnek kell lennie, kimutatva, hogy a rendszerben minden kockázatot kielégítő módon kivédenek és minden szervezeti biztonsági szabályt megfelelően érvényre juttatnak műszaki és üzemeltetési intézkedések (illetve az ezeket megvalósító mechanizmusok) együttese által.

A rendszer biztonsági előirányzat elvárt felépítése a termék biztonsági előirányzat felépítésének általánosításával született. Az SST-nek az alábbiakat kell tartalmaznia:

a) a teljes STOE-ra alkalmazható közös elemek;
b) tartományra vonatkozó részek, az STOE-ban meghatározott minden biztonsági tartományra az egyes tartományok egyedi szempontjainak leírása.

A közös elemeknek tartalmaznia kell az alábbiakat:

a) SST bevezetés;
b) megfelelőségi nyilatkozatok;
c) biztonsági probléma meghatározás;
d) biztonsági célok;
e) kiterjesztett összetevő meghatározás (csak SAP-K esetén);
f) biztonsági követelmények;
g) STOE összefoglaló előírás.

A tartományra vonatkozó részek keretében a rendszert alkotó minden biztonsági tartományra az alábbiakat kell szerepeltetni:

a) biztonsági tartomány bevezetés;
b) biztonsági tartomány megfelelőségi nyilatkozatok;
c) biztonsági tartomány biztonsági probléma meghatározás;
d) biztonsági tartomány biztonsági célok;
e) biztonsági tartomány kiterjesztett összetevő meghatározás (csak SAP-K esetén);
f) biztonsági tartomány biztonsági követelmények;
g) biztonsági tartomány összefoglaló előírás.

A tartományra vonatkozó rész üres lehet, amennyiben a rendszert nem osztják elkülönülő biztonsági tartományokra.

A tartományra vonatkozó részek egyes szakaszai is opcionálisak. Csak akkor kell őket megadni, ha a biztonsági tartományoknak olyan egyedi megfelelőségi nyilatkozatai, biztonsági problémái, céljai vagy követelményei vannak, amelyek nem vonatkoznak az STOE egészére, vagy azokat tartomány specifikus részletekkel bővítik.

Alap rendszer garanciacsomag (SAP-A) választása esetén az alábbi lényeges egyszerűsítések könnyítik meg az SST elkészítését:

a) A biztonsági követelményeket nem a CC 2. rész követelményeiből, hanem bármilyen mértékadó dokumentumból (szabványból, nyilvános műszaki követelményrendszerből, követelményeket megfogalmazó jogszabályból) lehet kiválasztani.
b) Nem kell megadni a kiterjesztett összetevő meghatározást (amely csak a CC 2. rész követelményeinek formális kiegészítésére szolgálna).
c) A biztonsági követelményeket csak kinyilvánítani kell (hivatkozva a mértékadó dokumentumra), nem pedig származtatni közvetlenül a biztonsági célokból, közvetve a biztonsági problémából.
d) Sem a biztonsági problémát, sem a biztonsági célokat nem kell megfogalmazni.

Fokozott rendszer garanciacsomag (SAP-F) választása esetén az alábbi egyszerűsítések könnyítik meg az SST elkészítését:

a) A biztonsági követelményeket a biztonsági követelményeket nem a CC 2. rész követelményeiből, hanem a kevésbé formális, közérthetőbb [2]–ben meghatározott biztonsági intézkedések katalógusából kell választani.
b) Nem kell megadni a kiterjesztett összetevő meghatározást (amely csak a CC 2. rész követelményeinek formális kiegészítésére szolgálna).
c) Amennyiben az SST a [2]–ben meghatározott fokozott kihatású biztonsági osztály követelményeit módosítás nélkül elfogadja, a biztonsági követelményeket csak kinyilvánítani kell, nem pedig származtatni közvetlenül a biztonsági célokból, közvetve a biztonsági problémából.
d) Amennyiben az SST a [2]–ben meghatározott fokozott kihatású biztonsági osztály követelményeit módosítás nélkül elfogadja, sem a biztonsági problémát, sem a biztonsági célokat nem kell megfogalmazni.

Kiemelt rendszer garanciacsomag (SAP-K) választása esetén a biztonsági követelményeket a [2]–ben meghatározott biztonsági intézkedések, vagy az [1]–ben meghatározott funkcionális biztonsági összetevők katalógusából kell választani. Ez esetben az alábbi egyszerűsítés könnyítheti meg az SST elkészítését:

a) Amennyiben az SST a [2]–ben meghatározott kiemelt kihatású biztonsági osztály követelményeit módosítás nélkül elfogadja, akkor ezeket csak kinyilvánítani kell, nem pedig származtatni közvetlenül a biztonsági célokból, közvetve a biztonsági problémából.
b) Amennyiben az SST a [2]–ben meghatározott kiemelt kihatású biztonsági osztály követelményeit módosítás nélkül elfogadja, sem a biztonsági problémát, sem a biztonsági célokat nem kell megfogalmazni.
c) Amennyiben az SST a [2]–ben meghatározott műszaki biztonsági intézkedések katalógusából választja a biztonsági követelményeket, akkor nem kell megadni a kiterjesztett összetevő meghatározást.

6.1.4.2. Az SST-re vonatkozó elvárások áttekintése

3. táblázat – Az SST-re vonatkozó elvárások

Garanciaosztály	Garanciacsalád	Garancia-összetevők az egyes rendszer garanciacsomagokban		
		SAP-A	SAP-F	SAP-K
Rendszer biztonsági előirányzat (ASST)	ASST_INT	1	1	2
	ASST_CCL	1	2	3
	ASST_SPD	-	1	1
	ASST_OBJ	1	2	2
	ASST_ECD	-	-	1
	ASST_REQ	1	2	3
	ASST_SSS	1	1	1
	ASST_SDI	1	1	1
	ASST_SDC	1	2	3
	ASST_SDP	-	1	1
	ASST_SDO	1	2	2
	ASST_SDE	-	-	1
	ASST_SDR	1	2	3
	ASST_SDS	1	1	1

6.1.4.3. Az SST elvárt szerkezete és tartalma

6.1.4.3.1. SST bevezetés (ASST_INT)

ASST_INT.1 SST bevezetés

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASST_INT.1.1D A rendszer integrátornak biztosítania kell az SST bevezetést.

A bizonyíték elemek tartalma és bemutatása:

ASST_INT.1.1C Az SST bevezetésnek tartalmaznia kell egy SST hivatkozást, STOE hivatkozást, STOE áttekintést, STOE leírást és egy tartomány kialakítás specifikációt.

ASST_INT.1.2C Az SST hivatkozásnak egyedi módon azonosítania kell az SST-t.

ASST_INT.1.3C Az STOE hivatkozásnak azonosítania kell az STOE-t.

ASST_INT.1.4C Az STOE áttekintésnek össze kell foglalnia az STOE használatát és fő biztonsági tulajdonságait.

ASST_INT.1.5C Az STOE áttekintésnek azonosítania kell az STOE típusát.

ASST_INT.1.6C Az STOE leírásnak meg kell adnia az STOE fizikai hatókörét és határait, beleértve a fizikai elemek ábráját.

ASST_INT.1.7C Az STOE leírásnak meg kell adnia az STOE logikai hatókörét és határait, beleértve a logikai elemek ábráját.

ASST_INT.1.8C Az STOE leírásnak azonosítania kell az STOE által igényelt bármilyen külső működő rendszerhez való kapcsolódást és felületet (interfészt).

ASST_INT.1.9C A tartomány kialakítás specifikációnak meg kell határoznia a létrehozott biztonsági tartományok kialakítását, szervezését, az egyes tartományok azonosítási információit.

Értékelői akcióelemek:

ASST_INT.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_INT.1.2E Az értékelőnek meg kell erősítenie, hogy az STOE hivatkozás, STOE áttekintés, STOE leírás és tartomány kialakítás specifikáció összhangban áll egymással.

ASST_INT.2 SST bevezetés biztonsági kapcsolatokkal

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASST_INT.2.1D A rendszer integrátornak biztosítania kell az SST bevezetést.

A bizonyíték elemek tartalma és bemutatása:

ASST_INT.2.1C Az SST bevezetésnek tartalmaznia kell egy SST hivatkozást, STOE hivatkozást, STOE áttekintést, STOE leírást és egy tartomány kialakítás specifikációt.

ASST_INT.2.2C Az SST hivatkozásnak egyedi módon azonosítania kell az SST-t.

ASST_INT.2.3C Az STOE hivatkozásnak azonosítania kell az STOE-t.

ASST_INT.2.4C Az STOE áttekintésnek össze kell foglalnia az STOE használatát és fő biztonsági tulajdonságait.

ASST_INT.2.5C Az STOE áttekintésnek azonosítania kell az STOE típusát.

ASST_INT.2.6C Az STOE leírásnak meg kell adnia az STOE fizikai hatókörét és határait, beleértve a fizikai elemek ábráját.

ASST_INT.2.7C Az STOE leírásnak meg kell adnia az STOE logikai hatókörét és határait, beleértve a logikai elemek ábráját.

ASST_INT.2.8C Az STOE leírásnak azonosítania kell az STOE által igényelt bármilyen külső működő rendszerhez való kapcsolódást és felületet (interfészt).

ASST_INT.2.9C A tartomány kialakítás specifikációnak meg kell határoznia a létrehozott biztonsági tartományok kialakítását, szervezését, az egyes tartományok azonosítási információit.

ASST_INT.2.10C **A tartomány kialakítás specifikációnak azonosítania kell az egyes tartományokra azokat a biztonsági célokat, amelyeket az STOE biztonsági tulajdonságaként más tartományok juttatnak érvényre.**

ASST_INT.2.11C **A tartomány kialakítás specifikációnak azonosítania kell az egyes tartományokra azokat a biztonsági célokat, amelyek az STOE biztonsági szolgáltatásaként más tartományok számára is rendelkezésre állnak.**

Értékelői akcióelemek:

ASST_INT.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_INT.2.2E Az értékelőnek meg kell erősítenie, hogy az STOE hivatkozás, STOE áttekintés, STOE leírás és tartomány kialakítás specifikáció összhangban áll egymással.

6.1.4.3.2. Megfelelőség nyilatkozatok (ASST_CCL)

Ennek a családnak a célja annak meghatározása, hogy a különböző megfelelőségi nyilatkozatok érvényesek-e.

Megfelelőségi nyilatkozatot az alábbiakhoz lehet tenni: mértékadó dokumentum (szabvány, nyilvános műszaki követelményrendszer, követelményeket megfogalmazó jogszabály), [2] (Műszaki biztonsági intézkedések katalógusa), [1] (CC funkcionális biztonsági összetevők katalógusa)

Egy adott biztonsági tartományra vonatkozó megfelelőségi nyilatkozatot a „Biztonsági tartományokra vonatkozó megfelelőségi nyilatkozat” szakasz definiálja.

ASST_CCL.1: Megfelelőség nyilatkozat mértékadó dokumentumhoz

Függések: ASST_INT.1, ASST_REQ.1

Rendszer integrátori akcióelemek:

ASST_CCL.1.1D A rendszer integrátornak biztosítania kell a megfelelőségi nyilatkozatot.

A bizonyíték elemek tartalma és bemutatása:

ASST_CCL.1.1C A megfelelőségi nyilatkozatnak azonosítania kell azt a mértékadó dokumentumot (szabványt, nyilvános műszaki követelményrendszert, követelményeket megfogalmazó jogszabályt), amelyhez az SST és az STOE megfelelőséget állít.

ASST_CCL.1.2C A megfelelőségi nyilatkozatnak azonosítania kell az érintett mértékadó dokumentum azon követelményeit, amelyekhez az SST és az STOE megfelelőséget állít.

Értékelői akcióelemek:

ASST_CCL.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_CCL.2: Megfelelőség nyilatkozat hazai katalógushoz

Függések: ASST_INT.1, ASST_REQ.2

Rendszer integrátori akcióelemek:

ASST_CCL.2.1D A rendszer integrátornak biztosítania kell a megfelelőségi nyilatkozatot.

A bizonyíték elemek tartalma és bemutatása:

ASST_CCL.2.1C A megfelelőségi nyilatkozatnak azonosítania kell azt a mértékadó dokumentumot, amelyhez az SST és az STOE megfelelőséget állít.

ASST_CCL.2.2C A megfelelőségi nyilatkozatnak azonosítania kell a mértékadó dokumentum azon követelményeit, amelyekhez az SST és az STOE megfelelőséget állít.

ASST_CCL.2.3C **A megfelelőségi nyilatkozatban azonosított mértékadó dokumentumnak az alábbinak kell lennie: [2] (A műszaki biztonsági intézkedések katalógusa).**

ASST_CCL.2.4C **A megfelelőségi nyilatkozatnak meg kell határoznia a [2]-ben leírt „fokozott kihatású biztonsági osztály követelményei" biztonsági követelmény csomagra vonatkozó csomag-megfelelőségét: vagy „megfelel a csomagnak" vagy „módosítja a csomagot".**

ASST_CCL.2.5C **Amennyiben a csomag-megfelelőségre vonatkozó nyilatkozat: „módosítja a csomagot", akkor a megfelelőségi nyilatkozat indoklásnak vissza kell vezetnie minden biztonsági követelményt az STOE biztonsági céljaira.**

Értékelői akcióelemek:

ASST_CCL.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_CCL.3: Megfelelőség nyilatkozat hazai vagy CC katalógushoz

Függések: ASST_INT.1, ASST_REQ.2

Rendszer integrátori akcióelemek:

ASST_CCL.3.1D A rendszer integrátornak biztosítania kell a megfelelőségi nyilatkozatot.

A bizonyíték elemek tartalma és bemutatása:

ASST_CCL.3.1C A megfelelőségi nyilatkozatnak azonosítania kell azt a mértékadó dokumentumot, amelyhez az SST és az STOE megfelelőséget állít.

ASST_CCL.3.2C A megfelelőségi nyilatkozatnak azonosítania kell a mértékadó dokumentum azon követelményeit, amelyekhez az SST és az STOE megfelelőséget állít.

ASST_CCL.3.3C A megfelelőségi nyilatkozatban azonosított mértékadó dokumentumnak az alábbiak **egyikének** kell lennie: **[1] (2 rész, funkcionális biztonsági összetevők katalógusa)**, [2] (A műszaki biztonsági intézkedések katalógusa).

ASST_CCL.3.4C **Hazai katalógusnak [2] való megfelelőség vállalása esetén** a megfelelőségi nyilatkozatnak meg kell határoznia a [2]-ben leírt „**kiemelt** kihatású biztonsági osztály követelményei" biztonsági követelmény csomagra vonatkozó csomag-megfelelőségét: vagy „megfelel a csomagnak" vagy „módosítja a csomagot".

ASST_CCL.3.5C **Hazai katalógusnak [2] való megfelelőség vállalása esetén**, amennyiben a csomag-megfelelőségre vonatkozó nyilatkozat: „módosítja a csomagot", akkor a megfelelőségi nyilatkozat indoklásnak vissza kell vezetnie minden biztonsági követelményt az STOE biztonsági céljaira.

ASST_CCL.3.6C **CC [1] megfelelőség vállalása esetén a megfelelőségi nyilatkozatnak le kell írnia az azonosított szabványnak való megfelelőségét: vagy „megfelel a szabványnak" vagy „kiterjeszti a szabványt".**

ASST_CCL.3.7C **CC megfelelőség vállalása esetén a megfelelőségi nyilatkozat nem mondhat ellent a kiterjesztett CC összetevők meghatározásának.**

Értékelői akcióelemek:

ASST_CCL.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.4.3.3. Biztonsági probléma meghatározás (ASST_SPD)

ASST_SPD.1 Biztonsági probléma meghatározás

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASST_SPD.1.1D A rendszer integrátornak biztosítania kell a biztonsági probléma meghatározást.

A bizonyíték elemek tartalma és bemutatása:

ASST_SPD.1.1C A biztonsági probléma meghatározásnak le kell írnia a fenyegetéseket.

ASST_SPD.1.2C Minden fenyegetést le kell írni a támadó, a támadás tárgyát képező vagyon és a támadó tevékenység szerint.

ASST_SPD.1.3C A biztonsági probléma meghatározásnak le kell írnia a szervezeti biztonsági szabályokat.

ASST_SPD.1.4C A biztonsági probléma meghatározásnak le kell írnia az STOE üzemeltetési környezetére vonatkozó feltételezéseket.

Értékelői akcióelemek:

ASST_SPD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.4.3.4. Biztonsági célok (ASST_OBJ)

ASST_OBJ.1: Biztonsági célok az üzemeltetési környezetre

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASST_OBJ.1.1D A rendszer integrátornak biztosítania kell a biztonsági célokról szóló nyilatkozatot.

A bizonyíték elemek tartalma és bemutatása:

ASST_OBJ.1.1C A biztonsági célokról szóló nyilatkozatnak le kell írnia az STOE üzemeltetési környezetre vonatkozó biztonsági célokat.

Értékelői akcióelemek:

ASST_OBJ.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_OBJ.2: Biztonsági célok

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASST_OBJ.2.1D A rendszer integrátornak biztosítania kell a biztonsági célokról szóló nyilatkozatot.

ASST_OBJ.2.2D **A rendszer integrátornak biztosítania kell a biztonsági célok indoklását.**

A bizonyíték elemek tartalma és bemutatása:

ASST_OBJ.2.1C A biztonsági célokról szóló nyilatkozatnak le kell írnia **az STOE-re vonatkozó biztonsági célokat, valamint** az üzemeltetési környezetre vonatkozó biztonsági célokat.

ASST_OBJ.2.2C **A biztonsági célok indoklásának minden STOE-re vonatkozó biztonsági célt vissza kell vezetnie az adott biztonsági cél által kivédett fenyegetésekre, valamint az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra.**

ASST_OBJ.2.3C **A biztonsági célok indoklásának minden üzemeltetési környezetre vonatkozó biztonsági célt vissza kell vezetnie az adott biztonsági cél által kivédett fenyegetésekre, az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra, valamint az adott biztonsági cél által támasztott feltételezésekre.**

ASST_OBJ.2.4C **A biztonsági célok indokolásának szemléltetnie kell, hogy a biztonsági célok lefednek minden fenyegetést.**

ASST_OBJ.2.5C **A biztonsági célok indokolásának szemléltetnie kell, hogy a biztonsági célok érvényre juttatják az összes szervezeti biztonsági szabályzatot.**

ASST_OBJ.2.6C **A biztonsági célok indokolásának szemléltetnie kell, hogy az üzemeltetési környezetre vonatkozó biztonsági célok az összes feltételezést igénylik.**

Értékelői akcióelemek:

ASST_OBJ.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.4.3.5. Kiterjesztett összetevő meghatározás (ASST_ECD)

ASST_ECD.1: Kiterjesztett összetevő meghatározás

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASST_ECD.1.1D A rendszer integrátornak biztosítania kell a biztonsági követelményekre vonatkozó állítást.

ASST_ECD.1.2D A rendszer integrátornak biztosítania kell a kiterjesztett összetevők meghatározását.

A bizonyíték elemek tartalma és bemutatása:

ASST_ECD.1.1C A biztonsági követelményekre vonatkozó állításnak azonosítania kell az összes kiterjesztett biztonsági követelményt.

ASST_ECD.1.2C A kiterjesztett összetevők meghatározásának meg kell adnia minden kiterjesztett követelményre egy kiterjesztett összetevőt.

ASST_ECD.1.3C A kiterjesztett összetevők meghatározásának le kell írnia, hogy az egyes kiterjesztett összetevők hogyan kapcsolódnak a meglévő CC összetevőkhöz, családokhoz és osztályokhoz.

ASST_ECD.1.4C A kiterjesztett összetevők meghatározásának használnia kell a meglévő CC összetevőket, családokat, osztályokat és módszertant a megjelenítés modelljeként.

ASST_ECD.1.5C A kiterjesztett összetevőknek mérhető és objektív elemekből kell állniuk, hogy a megfelelőségük vagy a nem megfelelőségük kimutatható legyen.

Értékelői akcióelemek:

ASST_ECD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_ECD.1.2E Az értékelőnek meg kell erősítenie, hogy nincs olyan kiterjesztett összetevő, ami kifejezhető lenne egyértelműen a meglévő összetevők segítségével.

6.1.4.3.6. Biztonsági követelmények (ASST_REQ)

ASST_REQ.1: Kinyilvánított követelmények

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASST_REQ.1.1D A rendszer integrátornak biztosítania kell a biztonsági követelményekre vonatkozó nyilatkozatot.

A bizonyíték elemek tartalma és bemutatása:

ASST_REQ.1.1C A biztonsági követelményekre vonatkozó állításnak le kell írnia a rendszertől elvárt biztonsági funkcionalitást (SSF) és garanciákat (SAP).

ASST_REQ.1.2C Az elvárt rendszer biztonsági funkcionalitást az alábbi mértékadó dokumentumokból kell választani: hazai vagy nemzetközi szabvány, nyilvános műszaki követelményrendszer, követelményeket megfogalmazó hazai jogszabály.

ASST_REQ.1.3C Az elvárt rendszer garanciacsomagnak az alábbiak egyikének kell lennie: SAP-A vagy megemelt SAP-A.

Értékelői akcióelemek:

ASST_REQ.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_REQ.1.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági követelményekről szóló nyilatkozat belső ellentmondásoktól mentes.

ASST_REQ.2: Hazai katalógusból választott követelmények

Függések: ASST_ECD.1

Rendszer integrátori akcióelemek:

ASST_REQ.2.1D A rendszer integrátornak biztosítania kell a biztonsági követelményekre vonatkozó nyilatkozatot.

ASST_REQ.2.2D **A rendszer integrátornak biztosítania kell a biztonsági követelmények indoklását.**

A bizonyíték elemek tartalma és bemutatása:

ASST_REQ.2.1C A biztonsági követelményekre vonatkozó állításnak le kell írnia a rendszertől elvárt biztonsági funkcionalitást (SSF) és garanciákat (SAP).

ASST_REQ.2.2C Az elvárt rendszer biztonsági funkcionalitást az alábbi mértékadó dokumentumból kell választani: [2] műszaki biztonsági intézkedések katalógusa).

ASST_REQ.2.3C Az elvárt rendszer garanciacsomagnak az alábbiak egyikének kell lennie: SAP-**F** vagy megemelt SAP-**F**.

ASST_REQ.2.4C **A biztonsági követelményekről szóló nyilatkozatnak azonosítania kell a biztonsági követelményekre vonatkozó összes műveletet.**

ASST_REQ.2.5C **Minden értékadási és kiválasztási műveletet be kell fejezni.**

ASST_REQ.2.6C **Minden műveletet jól kell végrehajtani.**

ASST_REQ.2.7C **A biztonsági követelmények indoklásának az SSF-et vissza kell vezetnie az STOE biztonsági céljaira.**

ASST_REQ.2.8C **A biztonsági követelmények indoklásának meg kell mutatnia, hogy az SSF teljesíti az STOE összes biztonsági célját, amelyeket külső rendszerek nem elégítenek ki.**

Értékelői akcióelemek:

ASST_REQ.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_REQ.2.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági követelményekről szóló nyilatkozat belső ellentmondásoktól mentes.

ASST_REQ.2.3E **Az értékelőnek meg kell erősítenie, hogy a biztonsági követelményekről szóló nyilatkozat egy teljes, egymást erősítő követelményrendszert határoz meg.**

ASST_REQ.3: **Hazai vagy nemzetközi katalógusból választott követelmények**

Függések: ASST_OBJ.1, ASST_ECD.1

Rendszer integrátori akcióelemek:

ASST_REQ.3.1D A rendszer integrátornak biztosítania kell a biztonsági követelményekre vonatkozó nyilatkozatot.

ASST_REQ.3.2D A rendszer integrátornak biztosítania kell a biztonsági követelmények indoklását.

A bizonyíték elemek tartalma és bemutatása:

ASST_REQ.3.1C A biztonsági követelményekre vonatkozó állításnak le kell írnia a rendszertől elvárt biztonsági funkcionalitást (SSF) és garanciákat (SAP).

ASST_REQ.3.2C Az elvárt rendszer biztonsági funkcionalitást az alábbi mértékadó dokumentumokból kell választani: [2] műszaki biztonsági intézkedések katalógusa, **[1] CC funkcionális biztonsági összetevők katalógusa.**

ASST_REQ.3.3C Az elvárt rendszer garanciacsomagnak az alábbinak kell lennie: SAP-**K**.

ASST_REQ.3.4C A biztonsági követelményekről szóló nyilatkozatnak azonosítania kell a biztonsági követelményekre vonatkozó összes műveletet.

ASST_REQ.3.5C Minden értékadási és kiválasztási műveletet be kell fejezni.

ASST_REQ.3.6C Minden műveletet jól kell végrehajtani.

ASST_REQ.3.7C **A biztonsági követelmények minden egyes függését vagy teljesíteni kell, vagy a biztonsági követelmények indoklásában igazolni kell a függés ki nem elégítését.**

ASST_REQ.3.8C A biztonsági követelmények indoklásának az SSF-et vissza kell vezetnie az STOE biztonsági céljaira.

ASST_REQ.3.9C A biztonsági követelmények indoklásának meg kell mutatnia, hogy az SSF teljesíti az STOE összes biztonsági célját, amelyeket külső rendszerek nem elégítenek ki.

Értékelői akcióelemek:

ASST_REQ.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_REQ.3.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági követelményekről szóló nyilatkozat belső ellentmondásoktól mentes.

ASST_REQ.3.3E Az értékelőnek meg kell erősítenie, hogy a biztonsági követelményekről szóló nyilatkozat egy teljes, egymást erősítő követelményrendszert határoz meg.

6.1.4.3.7. STOE összefoglaló előírás (ASST_SSS)

ASST_SSS.1: STOE összefoglaló előírás

Függések: ASST_INT.1, ASST_REQ.1

Rendszer integrátori akcióelemek:

ASST_SSS.1.1D A rendszer integrátornak biztosítania kell az STOE összefoglaló előírást.

A bizonyíték elemek tartalma és bemutatása:

ASST_SSS.1.1C Az STOE összefoglaló előírásnak le kell írnia, hogy az STOE hogyan teljesíti az egyes funkcionális biztonsági követelményeket (SFR).

Értékelői akcióelemek:

ASST_SSS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SSS.1.2E Az értékelőnek meg kell erősítenie, hogy az STOE összefoglaló előírás nem mond ellent az STOE áttekintésnek és az STOE leírásnak.

6.1.4.3.8. Biztonsági tartomány bevezetés (ASST_SDI)

ASST_SDI.1: Biztonsági tartomány bevezetés

Függések: ASST_INT.1

Rendszer integrátori akcióelemek:

ASST_SDI.1.1D A rendszer integrátornak biztosítania kell egy biztonsági tartomány bevezetést.

A bizonyíték elemek tartalma és bemutatása:

ASST_SDI.1.1C A biztonsági tartomány bevezetésnek tartalmaznia kell egy biztonsági tartomány hivatkozást, biztonsági tartomány áttekintést és egy biztonsági tartomány leírást.

ASST_SDI.1.2C A biztonsági tartomány hivatkozásnak egyedi módon azonosítania kell a biztonsági tartományt.

ASST_SDI.1.3C A biztonsági tartomány áttekintésnek össze kell foglalnia a biztonsági tartomány használatát és fő biztonsági tulajdonságait.

ASST_SDI.1.4C A biztonsági tartomány leírásnak jellemeznie kell alrendszereit és komponenseit.

ASST_SDI.1.5C A biztonsági tartomány leírásnak le kell írnia a más tartományokkal való kapcsolódásokat és interfészeket.

Értékelői akcióelemek:

ASST_SDI.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDI.1.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági tartomány hivatkozás, a biztonsági tartomány áttekintés és a biztonsági tartomány leírás nem mond ellent egymásnak és az SST bevezetésnek.

6.1.4.3.9. Biztonsági tartomány megfelelőségi nyilatkozatok (ASST_SDC)

ASST_SDC.1: Biztonsági tartomány megfelelőségi nyilatkozat mértékadó dokumentumhoz

Függések: ASST_REQ.1

Rendszer integrátori akcióelemek:

ASST_SDC.1.1D A rendszer integrátornak biztosítania kell egy biztonsági tartomány megfelelőségi nyilatkozatot.

A bizonyíték elemek tartalma és bemutatása:

ASST_SDC.1.1C A biztonsági tartomány megfelelőségi nyilatkozatnak azonosítania kell azt a mértékadó dokumentumot (szabványt, nyilvános műszaki követelményrendszert, követelményeket megfogalmazó jogszabályt), amelyhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.1.2C A biztonsági tartomány megfelelőségi nyilatkozatnak azonosítania kell az érintett mértékadó dokumentum azon követelményeit, amelyekhez a biztonsági tartomány megfelelőséget állít.

Értékelői akcióelemek:

ASST_SDC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDC.2: Biztonsági tartomány megfelelőség nyilatkozat hazai katalógushoz

Függések: ASST_REQ.2

Rendszer integrátori akcióelemek:

ASST_SDC.2.1D A rendszer integrátornak biztosítania kell a biztonsági tartomány megfelelőségi nyilatkozatot.

A bizonyíték elemek tartalma és bemutatása:

ASST_SDC.2.1C A biztonsági tartomány megfelelőségi nyilatkozatnak azonosítania kell azt a mértékadó dokumentumot, amelyhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.2.2C A biztonsági tartomány megfelelőségi nyilatkozatnak azonosítania kell a mértékadó dokumentum azon követelményeit, amelyekhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.2.3C **A biztonsági tartomány megfelelőségi nyilatkozatban azonosított mértékadó dokumentumnak az alábbinak kell lennie: [2] (A műszaki biztonsági intézkedések katalógusa).**

ASST_SDC.2.4C **A biztonsági tartomány megfelelőségi nyilatkozatnak meg kell határoznia a [2]-ben leírt „fokozott kihatású biztonsági osztály követelményei” biztonsági követelmény csomagra vonatkozó csomag-megfelelőségét: vagy „megfelel a csomagnak” vagy „módosítja a csomagot”.**

ASST_SDC.2.5C **Amennyiben a biztonsági tartomány csomag-megfelelőségre vonatkozó nyilatkozat: „módosítja a csomagot", akkor a biztonsági tartomány megfelelőségi nyilatkozat indoklásnak vissza kell vezetnie minden biztonsági követelményt az STOE biztonsági céljaira.**

Értékelői akcióelemek:

ASST_SDC.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDC.3: Biztonsági tartomány megfelelőség nyilatkozat hazai vagy CC katalógushoz

Függések: ASST_REQ.3,

Rendszer integrátori akcióelemek:

ASST_SDC.3.1D A rendszer integrátornak biztosítania kell a biztonsági tartomány megfelelőségi nyilatkozatot.

A bizonyíték elemek tartalma és bemutatása:

ASST_SDC.3.1C A biztonsági tartomány megfelelőségi nyilatkozatnak azonosítania kell azt a mértékadó dokumentumot, amelyhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.3.2C A biztonsági tartomány megfelelőségi nyilatkozatnak azonosítania kell a mértékadó dokumentum azon követelményeit, amelyekhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.3.3C A biztonsági tartomány megfelelőségi nyilatkozatban azonosított mértékadó dokumentumnak az alábbiak **egyikének** kell lennie: [2] (A műszaki biztonsági intézkedések katalógusa), **[1] (2 rész, funkcionális biztonsági összetevők katalógusa)**.

ASST_SDC.3.4C **Hazai katalógusnak [2] való megfelelőség vállalása esetén** a biztonsági tartomány megfelelőségi nyilatkozatnak meg kell határoznia a [2]-ben leírt „**kiemelt** kihatású biztonsági osztály követelményei" biztonsági követelmény csomagra vonatkozó csomag-megfelelőségét: vagy „megfelel a csomagnak" vagy „módosítja a csomagot".

ASST_SDC.3.5C **Hazai katalógusnak [2] való megfelelőség vállalása esetén**, amennyiben a csomag-megfelelőségre vonatkozó nyilatkozat: „módosítja a csomagot", akkor a biztonsági tartomány megfelelőségi nyilatkozat indoklásnak vissza kell vezetnie a biztonsági tartomány minden biztonsági követelményét a biztonsági tartomány biztonsági céljaira.

ASST_SDC.3.6C **CC [1] megfelelőség vállalása esetén a biztonsági tartomány megfelelőségi nyilatkozatnak le kell írnia az azonosított szabványnak való megfelelőségét: vagy „megfelel a szabványnak" vagy „kiterjeszti a szabványt".**

ASST_SDC.3.7C **CC megfelelőség vállalása esetén a biztonsági tartomány megfelelőségi nyilatkozat nem mondhat ellent a kiterjesztett CC összetevők meghatározásának.**

Értékelői akcióelemek:

ASST_SDC.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.4.3.10. Biztonsági tartomány biztonsági probléma meghatározás (ASST_SDP)

ASST_SDP.1 Biztonsági tartomány biztonsági probléma meghatározás

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASST_SDP.1.1D A rendszer integrátornak biztosítania kell egy biztonsági tartomány biztonsági probléma meghatározást.

A bizonyíték elemek tartalma és bemutatása:

ASST_SDP.1.1C A biztonsági tartomány biztonsági probléma meghatározásnak le kell írnia minden olyan egyedi kockázatot, amely a tartományra vonatkozik. Minden kockázatot az elfogadott, elkerülendő, áthárított vagy nem elfogadható kategóriák egyikébe kell sorolni.

ASST_SDP.1.2C Minden kockázatot le kell írni fenyegetések és sebezhetőségek formájában. Minden fenyegetést jellemezni kell a veszély forrása, érték és ellenséges tevékenység tényezőkkel.

ASST_SDP.1.3C A biztonsági tartomány biztonsági probléma meghatározásnak le kell írnia az összes egyedi OSP-t, ami a tartományra vonatkozik.

Értékelői akcióelemek:

ASST_SDP.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDP.1.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági tartomány biztonsági probléma meghatározás belső ellentmondásoktól mentes.

6.1.4.3.11. Biztonsági tartomány biztonsági célok (ASST_SDO)

ASST_SDO.1: Biztonsági tartomány biztonsági célok az üzemeltetési környezetre

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASST_SDO.1.1D A rendszer integrátornak biztosítania kell a biztonsági tartomány biztonsági céljairól szóló nyilatkozatot.

A bizonyíték elemek tartalma és bemutatása:

ASST_SDO.1.1C A biztonsági tartomány biztonsági céljairól szóló nyilatkozatnak le kell írnia a biztonsági tartomány üzemeltetési környezetére vonatkozó biztonsági célokat.

Értékelői akcióelemek:

ASST_SDO.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDO.2: Biztonsági tartomány biztonsági célok

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASST_SDO.2.1D A rendszer integrátornak biztosítania kell a biztonsági tartomány biztonsági célok állítását.

ASST_SDO.2.2D **A rendszer integrátornak biztosítania kell a biztonsági tartomány biztonsági célok indoklását.**

A bizonyíték elemek tartalma és bemutatása:

ASST_SDO.2.1C A biztonsági tartomány biztonsági célok állításának le kell írnia a **biztonsági tartományra vonatkozó biztonsági célokat, valamint** a biztonsági tartomány üzemeltetési környezetére vonatkozó biztonsági célokat.

ASST_SDO.2.2C **A biztonsági tartomány biztonsági célok indoklásának minden biztonsági tartományra vonatkozó biztonsági célt vissza kell vezetnie az adott biztonsági cél által kivédett fenyegetésekre, valamint az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra.**

ASST_SDO.2.3C **A biztonsági célok indoklásának az adott biztonsági tartomány üzemeltetési környezetére vonatkozó minden biztonsági célt vissza kell vezetnie az adott biztonsági cél által kivédett fenyegetésekre, az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra, valamint az adott biztonsági cél által támasztott feltételezésekre.**

ASST_SDO.2.4C **A biztonsági tartomány biztonsági célok indokolásának szemléltetnie kell, hogy a biztonsági célok lefednek minden fenyegetést.**

ASST_SDO.2.5C **A biztonsági tartomány biztonsági célok indokolásának szemléltetnie kell, hogy a biztonsági célok érvényre juttatják az összes szervezeti biztonsági szabályzatot.**

ASST_SDO.2.6C **A biztonsági tartomány biztonsági célok indokolásának szemléltetnie kell, hogy az adott biztonsági tartomány üzemeltetési környezetére vonatkozó biztonsági célok az összes feltételezést igénylik.**

Értékelői akcióelemek:

ASST_SDO.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.4.3.12. Biztonsági tartomány kiterjesztett összetevő meghatározás (ASST_SDE)

ASST_SDE.1: Biztonsági tartomány kiterjesztett összetevő meghatározás

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASST_SDE.1.1D A rendszer integrátornak biztosítania kell a biztonsági tartomány biztonsági követelményekre vonatkozó állítást.

ASST_SDE.1.2D A rendszer integrátornak biztosítania kell a biztonsági tartomány kiterjesztett összetevők meghatározását.

A bizonyíték elemek tartalma és bemutatása:

ASST_SDE.1.1C A biztonsági tartomány biztonsági követelményekre vonatkozó állításnak azonosítania kell az összes kiterjesztett biztonsági követelményt.

ASST_SDE.1.2C A biztonsági tartomány kiterjesztett összetevők meghatározásának meg kell adnia minden kiterjesztett követelményre egy kiterjesztett összetevőt.

ASST_SDE.1.3C A kiterjesztett összetevők meghatározásának le kell írnia, hogy az egyes kiterjesztett összetevők hogyan kapcsolódnak a meglévő CC összetevőkhöz, családokhoz és osztályokhoz.

ASST_SDE.1.4C A kiterjesztett összetevők meghatározásának használnia kell a meglévő CC összetevőket, családokat, osztályokat és módszertant a megjelenítés modelljeként.

ASST_SDE.1.5C A kiterjesztett összetevőknek mérhető és objektív elemekből kell állniuk, hogy a megfelelőségük vagy a nem megfelelőségük kimutatható legyen.

Értékelői akcióelemek:

ASST_SDE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDE.1.2E Az értékelőnek meg kell erősítenie, hogy nincs olyan kiterjesztett összetevő, ami kifejezhető lenne egyértelműen a meglévő összetevők segítségével.

6.1.4.3.13. Biztonsági tartomány biztonsági követelmények (ASST_SDR)

ASST_SDR.1: Biztonsági tartományra kinyilvánított követelmények

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASST_SDR.1.1D A rendszer integrátornak biztosítania kell a biztonsági tartomány biztonsági követelményekre vonatkozó állítást.

A bizonyíték elemek tartalma és bemutatása:

ASST_SDR.1.1C A biztonsági tartomány biztonsági követelményekre vonatkozó állításnak le kell írnia az adott biztonsági tartományra elvárt biztonsági funkcionalitást (SF) és az elvárt rendszer garanciacsomagot (SAP).

ASST_SDR.1.2C Az elvárt biztonsági funkcionalitást az alábbi mértékadó dokumentumokból kell választani: hazai vagy nemzetközi szabvány, nyilvános műszaki követelményrendszer, követelményeket megfogalmazó hazai jogszabály.

ASST_SDR.1.3C Az elvárt rendszer garanciacsomagnak az alábbiak egyikének kell lennie: SAP-A vagy megemelt SAP-A.

Értékelői akcióelemek:

ASST_SDR.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDR.1.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági tartomány biztonsági követelményekről szóló nyilatkozat belső ellentmondásoktól mentes.

ASST_SDR.2: Biztonsági tartományra hazai katalógusból választott követelmények

Függések: ASST_SDO.1

Rendszer integrátori akcióelemek:

ASST_SDR.2.1D A rendszer integrátornak biztosítania kell a biztonsági tartomány biztonsági követelményekre vonatkozó állítást.

ASST_REQ.2.2D **A rendszer integrátornak biztosítania kell a biztonsági tartomány biztonsági követelmények indoklását.**

A bizonyíték elemek tartalma és bemutatása:

ASST_SDR.2.1C A biztonsági tartomány biztonsági követelményekre vonatkozó állításnak le kell írnia az adott biztonsági tartományra elvárt biztonsági funkcionalitást (SF) és az elvárt rendszer garanciacsomagot (SAP).

ASST_SDR.2.2C Az elvárt biztonsági funkcionalitást az alábbi mértékadó dokumentumokból kell választani: [2] műszaki biztonsági intézkedések katalógusa).

ASST_SDR.2.3C Az elvárt rendszer garanciacsomagnak az alábbiak egyikének kell lennie: SAP-**F** vagy megemelt SAP-**F**.

ASST_SDR.2.4C **A biztonsági tartomány biztonsági követelményekről szóló nyilatkozatnak azonosítania kell a biztonsági követelményekre vonatkozó összes műveletet.**

ASST_SDR.2.5C **Minden értékadási és kiválasztási műveletet be kell fejezni.**

ASST_SDR.2.6C **Minden műveletet jól kell végrehajtani.**

ASST_SDR.2.7C **A biztonsági tartomány biztonsági követelmények indoklásának az adott biztonsági tartományra elvárt SF-t vissza kell vezetnie az adott biztonsági tartomány biztonsági céljaira.**

ASST_SDR.2.8C **A biztonsági tartomány biztonsági követelmények indoklásának meg kell mutatnia, hogy az SF teljesíti az adott biztonsági tartomány összes biztonsági célját, amelyeket külső rendszerek nem elégítenek ki.**

Értékelői akcióelemek:

ASST_SDR.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDR.2.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági tartomány biztonsági követelményekről szóló nyilatkozat belső ellentmondásoktól mentes.

ASST_SDR.2.3E **Az értékelőnek meg kell erősítenie, hogy a biztonsági tartomány biztonsági követelményekről szóló nyilatkozat egy teljes, egymást erősítő követelményrendszert határoz meg.**

ASST_SDR.3: Biztonsági tartományra hazai vagy CC katalógusból választott követelmények

Függések: ASST_SDO.1

Rendszer integrátori akcióelemek:

ASST_SDR.3.1D A rendszer integrátornak biztosítania kell a biztonsági tartomány biztonsági követelményekre vonatkozó állítást.

ASST_SDR.3.2D A rendszer integrátornak biztosítania kell a biztonsági tartomány biztonsági követelmények indoklását.

A bizonyíték elemek tartalma és bemutatása:

ASST_SDR.3.1C A biztonsági tartomány biztonsági követelményekre vonatkozó állításnak le kell írnia az adott biztonsági tartományra elvárt biztonsági funkcionalitást (SF) és az elvárt rendszer garanciacsomagot (SAP).

ASST_SDR.3.2C Az elvárt biztonsági funkcionalitást az alábbi mértékadó dokumentumokból kell választani: [2] műszaki biztonsági intézkedések katalógusa), **[1] CC funkcionális biztonsági összetevők katalógusa.**

ASST_SDR.3.3C Az elvárt rendszer garanciacsomagnak az alábbiak egyikének kell lennie: SAP-**K** vagy megemelt SAP-**K.**

ASST_SDR.3.4C A biztonsági tartomány biztonsági követelményekről szóló nyilatkozatnak azonosítania kell a biztonsági követelményekre vonatkozó összes műveletet.

ASST_SDR.3.5C Minden értékadási és kiválasztási műveletet be kell fejezni.

ASST_SDR.3.6C Minden műveletet jól kell végrehajtani.

ASST_SDR.3.7C **A biztonsági követelmények minden egyes függését vagy teljesíteni kell, vagy a biztonsági tartomány biztonsági követelmények indoklásában igazolni kell a függés ki nem elégítését.**

ASST_SDR.3.8C A biztonsági tartomány biztonsági követelmények indoklásának az adott biztonsági tartományra elvárt SF-t vissza kell vezetnie az adott biztonsági tartomány biztonsági céljaira.

ASST_SDR.3.9C A biztonsági tartomány biztonsági követelmények indoklásának meg kell mutatnia, hogy az SF teljesíti az adott biztonsági tartomány összes biztonsági célját, amelyeket külső rendszerek nem elégítenek ki.

Értékelői akcióelemek:

ASST_SDR.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDR.3.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági tartomány biztonsági követelményekről szóló nyilatkozat belső ellentmondásoktól mentes.

ASST_SDR.3.3E Az értékelőnek meg kell erősítenie, hogy a biztonsági tartomány biztonsági követelményekről szóló nyilatkozat egy teljes, egymást erősítő követelményrendszert határoz meg.

6.1.4.3.14. Biztonsági tartomány összefoglaló előírás (ASST_SDS)

ASST_SDS.1: Biztonsági tartomány összefoglaló előírás

Függések: ASST_SDI.1, ASST_SDR.1

Rendszer integrátori akcióelemek:

ASST_SDS.1.1D A rendszer integrátornak biztosítania kell a biztonsági tartományra vonatkozó összefoglaló előírást.

A bizonyíték elemek tartalma és bemutatása:

ASST_SDS.1.1C A biztonsági tartományra vonatkozó összefoglaló előírásnak le kell írnia, hogy a biztonsági tartomány hogyan teljesíti az egyes funkcionális biztonsági követelményeket (SFR).

Értékelői akcióelemek:

ASST_SDS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDS.1.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági tartományra vonatkozó összefoglaló előírás nem mond ellent a biztonsági tartomány áttekintésnek és a biztonsági tartomány leírásnak.

6.1.4.4. Az SST elvárt szerkezete és tartalma SAP-A esetén

4. táblázat – Az SST elvárt szerkezete és tartalma SAP-A esetén

ASST_INT	1 (ASST_INT.1 SST bevezetés)
ASST_CCL	1 (ASST_CCL.1: Megfelelőség nyilatkozat mértékadó dokumentumhoz)
ASST_SPD	-
ASST_OBJ	1 (ASST_OBJ.1: Biztonsági célok az üzemeltetési környezetre)
ASST_ECD	-
ASST_REQ	1 (ASST_REQ.1: Kinyilvánított követelmények)

ASST_SSS	1 (ASST_SSS.1: STOE összefoglaló előírás)
ASST_SDI	1 (ASST_SDI.1: Biztonsági tartomány bevezetés)
ASST_SDC	1 (ASST_SDC.1: Biztonsági tartomány megfelelőségi nyilatkozat mértékadó dokumentumhoz)
ASST_SDP	-
ASST_SDO	1 (ASST_SDO.1: Biztonsági tartomány biztonsági célok az üzemeltetési környezetre)
ASST_SDE	-
ASST_SDR	1 (ASST_SDR.1: Biztonsági tartományra kinyilvánított követelmények)
ASST_SDS	1 (ASST_SDS.1: Biztonsági tartomány összefoglaló előírás)

Az alap rendszer garanciacsomag esetén az alábbi lényeges egyszerűsítések könnyítik (-) meg az SST elkészítését:

a) (-) A biztonsági követelményeket tetszőleges mértékadó követelményből lehet kiválasztani (ASST_CCL: 1, ASST_SDC: 1).
b) (-) A biztonsági követelményeket csak kinyilvánítani kell, nem pedig származtatni közvetlenül a biztonsági célokból, közvetve a biztonsági problémából (ASST_REQ: 1, ASST_SDR: 1).
c) (-) A biztonsági problémát nem kell megfogalmazni (ASST_SPD:-, ASST_SDP:-).
d) (-) Csak az üzemeltetési környezetre vonatkozó biztonsági célokat kell megadni (ASST_OBJ: 1, ASST_SDO: 1).
e) (-) Mivel a biztonsági követelményeket tetszőleges mértékadó követelményből lehet kiválasztani, ezért nem kell megadni a csak CC-re jellemző kiterjesztett összetevő meghatározást (ASST_ECD: -, ASST_SDE: -).

6.1.4.5. Az SST elvárt szerkezete és tartalma SAP-F esetén

5. táblázat - Az SST elvárt szerkezete és tartalma SAP-F esetén

ASST_INT	1 (ASST_INT.1 SST bevezetés)
ASST_CCL	2 (ASST_CCL.2: Megfelelőség nyilatkozat hazai katalógushoz)
ASST_SPD	1 (ASST_SPD.1 Biztonsági probléma meghatározás)
ASST_OBJ	2 (ASST_OBJ.2: Biztonsági célok)
ASST_ECD	-
ASST_REQ	2 (ASST_REQ.2: Hazai katalógusból választott követelmények)
ASST_SSS	1 (ASST_SSS.1: STOE összefoglaló előírás)
ASST_SDI	1 (ASST_SDI.1: Biztonsági tartomány bevezetés)
ASST_SDC	2 (ASST_SDC.2: Biztonsági tartomány megfelelőség nyilatkozat hazai katalógushoz)
ASST_SDP	1 (ASST_SDP.1 Biztonsági tartomány biztonsági probléma meghatározás)
ASST_SDO	2 (ASST_SDO.2: Biztonsági tartomány biztonsági célok)
ASST_SDE	-
ASST_SDR	2 (ASST_SDR.2: Biztonsági tartományra hazai katalógusból választott követelmények)
ASST_SDS	1 (ASST_SDS.1: Biztonsági tartomány összefoglaló előírás)

A fokozott rendszer garanciacsomag esetén az alábbi egyszerűsítések könnyítik (-), illetve az alábbi korlátozások nehezítik (+) az SST elkészítését:

a) (+) A biztonsági követelményeket csak a [2]-ben meghatározott katalógusból lehet kiválasztani (ASST_CCL: 2, ASST_SDC: 2).
b) (-) Amennyiben a [2] katalógusából kiválasztott biztonsági követelmények megegyeznek a fokozott kihatású biztonsági osztály követelményeivel, akkor ezeket a követelményeket csak kinyilvánítani kell, nem pedig származtatni közvetlenül a

biztonsági célokból, közvetve a biztonsági problémából (ASST_REQ: 2, ASST_SDR: 2).

c) (-) Amennyiben a [2] katalógusából kiválasztott biztonsági követelmények megegyeznek a fokozott kihatású biztonsági osztály követelményeivel, akkor a biztonsági problémát és a biztonsági célokat mégsem kell megadni.
d) (-) Mivel a biztonsági követelményeket a [2]-ben meghatározott katalógusból kell kiválasztani, ezért nem kell megadni a csak CC-re jellemző kiterjesztett összetevő meghatározást (ASST_ECD: -, ASST_SDE: -).

6.1.4.6. Az SST elvárt szerkezete és tartalma SAP-K esetén

6. táblázat - Az SST elvárt szerkezete és tartalma SAP-K esetén

ASST_INT	2 (ASST_INT.2 SST bevezetés biztonsági kapcsolatokkal)
ASST_CCL	3 (ASST_CCL.3: Megfelelőség nyilatkozat hazai vagy CC katalógushoz)
ASST_SPD	1 (ASST_SPD.1 Biztonsági probléma meghatározás)
ASST_OBJ	2 (ASST_OBJ.2: Biztonsági célok)
ASST_ECD	1 (ASST_ECD.1: Kiterjesztett összetevő meghatározás)
ASST_REQ	3 (ASST_REQ.3: Hazai vagy nemzetközi katalógusból választott követelmények)
ASST_SSS	1 (ASST_SSS.1: STOE összefoglaló előírás)
ASST_SDI	1 (ASST_SDI.1: Biztonsági tartomány bevezetés)
ASST_SDC	3 (ASST_SDC.3: Biztonsági tartomány megfelelőség nyilatkozat hazai vagy CC katalógushoz)
ASST_SDP	1 (ASST_SDP.1 Biztonsági tartomány biztonsági probléma meghatározás)
ASST_SDO	2 (ASST_SDO.2: Biztonsági tartomány biztonsági célok)
ASST_SDE	1 (ASST_SDE.1: Biztonsági tartomány kiterjesztett összetevő meghatározás)
ASST_SDR	3 (ASST_SDR.3: Biztonsági tartományra hazai vagy CC katalógusból választott követelmények)
ASST_SDS	1 (ASST_SDS.1: Biztonsági tartomány összefoglaló előírás)

A kiemelt rendszer garanciacsomag esetén az alábbi egyszerűsítések könnyíthetik (-), illetve az alábbi korlátozások nehezítik (+) az SST elkészítését:

a) (+) A biztonsági célokat a biztonsági tartományokra is vissza kell vezetni (ASST_INT: 2).
b) (+) A biztonsági követelményeket a [2]-ben és az [1]-ben meghatározott katalógusból lehet kiválasztani (ASST_CCL: 3, ASST_SDC: 3).
c) (+) A biztonsági követelményeket általában nem elég kinyilvánítani, hanem származtatni kell közvetlenül a biztonsági célokból, közvetve a biztonsági problémából (ASST_REQ: 3, ASST_SDR: 3).
d) (-) Amennyiben a biztonsági követelmények megegyeznek a [2] katalógusából összeállított kiemelt kihatású biztonsági osztály követelményeivel, akkor a követelményeket csak kinyilvánítani kell, nem pedig származtatni közvetlenül a biztonsági célokból, közvetve a biztonsági problémából.
e) (-) Amennyiben a [2] katalógusából kiválasztott biztonsági követelmények megegyeznek a kiemelt kihatású biztonsági osztály követelményeivel, akkor a biztonsági problémát és a biztonsági célokat mégsem kell megadni.
f) (+) kiterjesztett CC követelmények beválasztása esetén meg kell adni a kiterjesztett összetevő meghatározást (ASST_ECD: 1, ASST_SDE: 1).

6.1.5. Rendszer fejlesztés garanciaosztály

6.1.5.1. A rendszer fejlesztés garanciaosztály áttekintése

A rendszer fejlesztés garanciaosztály (ASDV) elvárásainak megfelelő értékelési bizonyítékok olyan tervezési információkat nyújtanak az STOE-ról, amelyek alapján az értékelő jobban megismeri az értékelés tárgyát, következésképp hatékonyabban képes végrehajtani a független biztonsági tesztelést és a sebezhetőség vizsgálatát is.

A rendszer fejlesztés garanciaosztály az alábbi 5 garanciacsaládot tartalmazza:

a) **biztonsági architektúra leírás (ASDV_ARC)**, amely a tartomány szétválasztásra, a biztonsági funkcionalitás önvédelmére és nem-megkerülhetőségére vonatkozó tulajdonságok szemléltetését várja el,
b) **rendszer interfész specifikációja (ASDV_SIS),** amely a rendszer külső interfészein keresztül látható biztonsági funkcionalitás meghatározását várja el,
c) **rendszer biztonsági terv (ASDV_SDS)**, amely a biztonsági funkcionalitás belső viselkedésének leírását várja el,
d) **rendszer-működési biztonsági koncepció (ASDV_OSC),** amely a rendszer biztonsági szabályainak, tulajdonságainak és jellegzetességeinek a leírását várja el, különböző részletességgel (alrendszer – komponens – megvalósítási reprezentáció),
e) **a terv dokumentációk aktualizálása (ASDV_MOD)**, amely annak kimutatását várja el, hogy a rendszer biztonságára vonatkozó terv dokumentációkat megfelelően aktualizálták a rendszer komponensek módosítása után.

6.1.5.2. Biztonsági architektúra leírás (ASDV_ARC)

Ennek a garanciacsaládnak az a célja, hogy a rendszer integrátor által a rendszer biztonsági szerkezetéről biztosított magas szintű leírás hozzájáruljon annak vizsgálatához, hogy a rendszer biztonsági funkcionalitása megfelel az elvárásoknak.

A rendszer biztonsági architektúrája a rendszer biztonság alábbi három tulajdonságára koncentrál: tartomány szétválasztás, önvédelem, a megkerülhetetlenség biztosítása.
A rendszer biztonsági architektúrájának ismerete nélkül az értékelőnek a teljes rendszer funkcionalitást vizsgálni kellene.

Ez a család egy garancia-összetevőt tartalmaz, tehát a rendszer biztonsági szerkezetének leírására mindhárom garanciacsomag azonos minőségi követelményeket fogalmaz meg.

6.1.5.2.1. ASDV_ARC.1 Biztonsági szerkezet leírás

Függések: ASDV_SIS.1, ASDV_SDS.1

Rendszer integrátori akcióelemek:

ASDV_ARC.1.1D A rendszer integrátornak úgy kell megterveznie és megvalósítani az STOE-t, hogy a rendszer biztonsági funkcionalitását ne lehessen megkerülni.

ASDV_ARC.1.2D A rendszer integrátornak úgy kell megterveznie és megvalósítania a rendszer biztonsági funkcionalitását, hogy az képes legyen megvédeni magát a nem-megbízható aktív egyedek hamisításaitól.

ASDV_ARC.1.3D A rendszer integrátornak biztosítania kell egy leírást az STOE biztonsági architektúrájáról.

A bizonyíték elemek tartalma és bemutatása:

ASDV_ARC.1.1C A biztonsági architektúra leírásnak ismertetnie kell az STOE-hez kapcsolódó külső informatikai rendszereket, egymáshoz kapcsolódásukat, valamint a köztük folyó információáramlást.

ASDV_ARC.1.2C A biztonsági architektúra leírásnak ismertetnie kell az STOE biztonsági funkcionalitás szerkezetét, olyan részletességgel, amely összemérhető a rendszer interfész specifikáció és az STOE terv részletességével.

ASDV_ARC.1.3C A biztonsági architektúra leírásnak szemléltetnie kell, hogy az STOE meggátolja a funkcionális biztonsági követelményeket érvényre juttató funkcionalitás megkerülését.

ASDV_ARC.1.4C A biztonsági architektúra leírásnak szemléltetnie kell, hogy a rendszer biztonsági funkcionalitás megvédi magát a hamisítással szemben.

Értékelői akcióelemek:

ASDV_ARC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.5.3. Rendszer interfész specifikáció (ASDV_SIS)

Ennek a garanciacsaládnak az a célja, hogy a rendszer integrátor által a rendszer külső interfészéről biztosított leírás hozzájáruljon annak vizsgálatához, hogy a rendszer biztonsági funkcionalitása megfelel az elvárásoknak

A rendszer interfész specifikáció a rendszer kívülről is elérhető szolgáltatásainak biztonsággal kapcsolatos részleteire koncentrál.

A rendszer interfész specifikáció lehetővé teszi a felhasználók számára, hogy kívülről szolgáltatásokat hívjanak meg (a rendszer által feldolgozandó adatok megadásával), s ezekre a szolgáltatás meghívásokra megfelelő válaszokat kapjanak.

A rendszer interfész specifikáció nem írja le azt, hogy a rendszer hogyan dolgozza fel a szolgáltatás meghívásokat, és nem írja le azt a kommunikációt sem, amelynek során a rendszer saját üzemeltetési környezetéből további szolgáltatásokat hív meg; ezeket az információkat az „STOE terv” (ASDV_SDS) család tárgyalja.

A rendszer interfész specifikáció ismerete nélkül az értékelőnek a teljes rendszer interfészt vizsgálni kellene.

Ez a család két garancia-összetevőt tartalmaz, ezek abban különböznek, hogy az interfészek leírására eltérő részletességet kívánnak meg.

Ez a család közvetlen garanciát nyújt, lehetővé téve az értékelő számára annak átlátását, hogy a rendszer biztonsági funkcionalitása megfelel az elvárásoknak

Ez a család közvetetten is nyújt garanciát más garanciacsaládok és garanciaosztályok számára:

a) az ASDV_ARC garanciacsalád számára, ahol a rendszer interfész biztonsággal kapcsolatos részeinek leírása segíti annak jobb megértését, hogy a rendszer biztonsági funkcionalitás hogyan védi magát a hamisítással szemben (vagyis a önvédelem vagy tartomány szétválasztás aláaknázása ellen) és a megkerülés ellen;
b) az ASTE garanciaosztály számra, ahol a rendszer interfész biztonsággal kapcsolatos részeinek leírása fontos bemenet a rendszer integrátori és az értékelői teszteléshez;
c) az ASVA_VAN garanciacsalád számra, ahol a rendszer interfész biztonsággal kapcsolatos részeinek leírása felhasználható a sebezhetőségek keresésénél.

6.1.5.3.1. ASDV_SIS.1: Informális interfész specifikáció

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASDV_SIS.1.1D A rendszer integrátornak biztosítania kell egy rendszer interfész specifikációt.

A bizonyíték elemek tartalma és bemutatása:

ASDV_SIS.1.1C A rendszer interfész specifikációnak informális stílusban le kell írnia az STOE biztonsági funkcionalitását (SSF) és annak külső interfészeit.

ASDV_SIS.1.2C A rendszer interfész specifikációnak belső ellentmondásoktól mentesnek kell lennie.

ASDV_SIS.1.3C A rendszer interfész specifikációnak le kell írnia az SSF minden külső interfészére a használat célját és módját, részletezve a hatásokat, kivételeket és hibaüzeneteket.

ASDV_SIS.1.4C A rendszer interfész specifikációnak teljes mértékben be kell mutatnia az SSF-et.

Értékelői akcióelemek:

ASDV_SIS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_SIS.1.2E Az értékelőnek meg kell állapítania, hogy a rendszer interfész specifikáció az STOE funkcionális biztonsági követelményeinek pontos és teljes megjelenítése.

6.1.5.3.2. ASDV_SIS.2: Teljesen meghatározott külső interfészek

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASDV_SIS.2.1D A rendszer integrátornak biztosítania kell egy rendszer interfész specifikációt.

A bizonyíték elemek tartalma és bemutatása:

ASDV_SIS.2.1C A rendszer interfész specifikációnak informális stílusban le kell írnia az STOE biztonsági funkcionalitását (SSF) és annak külső interfészeit.

ASDV_SIS.2.2C A rendszer interfész specifikációnak belső ellentmondásoktól mentesnek kell lennie.

ASDV_SIS.2.3C A rendszer interfész specifikációnak le kell írnia az SSGF minden külső interfészére a használat célját és módját, **teljesen** részletezve **minden** hatást, kivételt és hibaüzenetet.

ASDV_SIS.2.4C A rendszer interfész specifikációnak teljes mértékben be kell mutatnia az SSF-et.

ASDV_SIS.2.5C A rendszer interfész specifikációnak egy indoklást kell tartalmaznia arról, hogy teljes mértékben bemutatja az SSF-et.

Értékelői akcióelemek:

ASDV_SIS.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_SIS.2.2E Az értékelőnek meg kell állapítania, hogy a rendszer interfész specifikáció az STOE funkcionális biztonsági követelményeinek pontos és teljes megjelenítése.

6.1.5.4. Rendszer biztonsági terv (ASDV_SDS)

A rendszer biztonsági terv (STOE terv) a rendszer biztonsági funkcionalitását (SSF) belülről ismerteti.

A rendszer interfész specifikáció kívülről határozza meg az SSF-t, a kívülről meghívható (biztonsági vonatkozású) szolgáltatások és az erre adott rendszer válaszok leírásával.

A rendszer biztonsági terv azt írja le, hogy a rendszer hogyan dolgozza fel a szolgáltatás meghívásokat, az egyes alrendszerek és komponensek közötti belső egymásra hatások tükrében. A rendszer biztonsági terv azt a kommunikációt is leírja, amelynek során a rendszer saját üzemeltetési környezetéből további szolgáltatásokat hív meg.

Ez a család egy garancia-összetevőt tartalmaz.

6.1.5.4.1. ASDV_SDS.1: Alrendszer és komponens szintű biztonsági terv

Függések: ASDV_SIS.1

Rendszer integrátori akcióelemek:

ASDV_SDS.1.1D A rendszer integrátornak biztosítania kell az STOE rendszer biztonsági tervét (STOE tervét).

ASDV_SDS.1.2D A rendszer integrátornak egy leképezést kell biztosítania a rendszer interfész specifikáció SSFI-je és az STOE terv rendelkezésre álló legalacsonyabb szintű felbontása között.

A bizonyíték elemek tartalma és bemutatása:

ASDV_SDS.1.1C Az STOE tervnek le kell írnia az STOE szerkezetét alrendszerek szerint.

ASDV_SDS.1.2C Az STOE tervnek azonosítania kell az SSF minden alrendszerét.

ASDV_SDS.1.3C Az STOE tervnek leírást kell biztosítania az SSF összes alrendszeréről.

ASDV_SDS.1.4C Az STOE tervnek le kell írnia az SSF összes alrendszere közötti kapcsolatokat.

ASDV_SDS.1.5C Az STOE tervnek le kell írnia az SSF-et komponensek szerint.

ASDV_SDS.1.6C Az STOE tervnek egy leképezést kell biztosítania az SSF alrendszerei és az SSF komponensei között.

ASDV_SDS.1.7C Az STOE tervnek le kell írnia az összes SFR-t érvényre juttató komponenst, megadva céljukat és a többi komponenssel való kapcsolatukat.

ASDV_SDS.1.8C Az STOE tervnek le kell írnia az összes SFR-t érvényre juttató komponenst, megadva SFR vonatkozású interfészeiket, ezen interfészek visszatérési értékeit, valamint a többi komponenssel való kapcsolatukat és meghívott interfészeket.

ASDV_SDS.1.9C Az STOE tervnek le kell írnia az összes SFR-t támogató, illetve az SFR-hez nem kapcsolódó komponenst, megadva céljukat és a többi komponenssel való kapcsolatukat.

ASDV_SDS.1.10C A leképezésnek szemléltetnie kell, hogy az STOE tervben leírt minden működést leképezi az ezeket meghívó SSFI-kre.

Értékelői akcióelemek:

ASDV_SDS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_SDS.1.2E Az értékelőnek meg kell erősítenie, hogy az STOE terv az összes funkcionális biztonsági követelmény pontos és teljes megjelenítése.

6.1.5.5. A rendszer-működés biztonsági koncepciója (ASDV_OSC)

A rendszer-működésre vonatkozó biztonsági koncepció az informatikai rendszer biztonsági szabályait, tulajdonságait és jellegzetességeit határozza meg. E biztonsági koncepció az alábbi szempontokból jellemzi a rendszer működését:

a) a rendszer belső összeköttetésein keresztül megvalósuló információ áramlás ellenőrzés koncepciója,
b) a rendszer külső interfészein keresztül megvalósuló (külső rendszerek felé irányuló) információ áramlás ellenőrzés koncepciója,
c) a rendszerhez való lokális és távoli hozzáférések ellenőrzési koncepciója;
d) a rendszer erőforrásaihoz való hozzáférések ellenőrzési koncepciója;
e) a rendszer működési módjaira, illetve a működési mód specifikus műveletek ellenőrzésére vonatkozó koncepció.

Ez a család egy garancia-összetevőt tartalmaz.

6.1.5.5.1. ASDV_OSC.1: Rendszer-működési biztonsági koncepció

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASDV_OSC.1.1D A rendszer integrátornak biztosítania kell a rendszer-működésre vonatkozó biztonsági koncepció leírását.

A bizonyíték elemek tartalma és bemutatása:

ASDV_OSC.1.1C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer belső (rendszer határain belüli) információ áramlást érvényre juttató képességét.

ASDV_OSC.1.2C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer külső (külső rendszerek felé történő) információ áramlást érvényre juttató képességét.

ASDV_OSC1.3C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer lokális és távoli hozzáféréseket érvényre juttató képességét.

ASDV_OSC.1.4C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer erőforrásokhoz való (hozzáférés közvetítési szabályokon alapuló) hozzáféréseket érvényre juttató képességét.

ASDV_OSC.1.5C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer által nyújtott üzemmódokat, az üzemmódok közötti átmenetek feltételeit, és azokat az érvényesítő mechanizmusokat, amelyek minden azonosított rendszer üzemmódban biztonságos működést biztosítanak.

ASDV_OSC.1.6C A rendszer-működési biztonsági koncepció leírásának belső ellentmondástól mentesnek kell lennie.

Értékelői akcióelemek:

ASDV_OSC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_OSC.1.2E Az értékelőnek meg kell állapítania a rendszer architektúra leírásról és az STOE tervről, hogy azok teljesen megvalósítják a rendszer-működési biztonsági koncepciót.

6.1.5.6. A biztonsági terv dokumentációk aktualizálása (ASDV_MOD)

Ennek a garanciacsaládnak a célja annak kimutatása, hogy a rendszer biztonsági terv dokumentációk helyesek maradnak a rendszer komponensek módosításai után is.

A család egy garancia-összetevőt tartalmaz.

Az ASDV_MOD.1 komponens nem csak a rendszer biztonsági terv dokumentáció módosított részeivel foglalkozik, hanem olyan részekkel is, amelyek esetleg érvényüket veszthették.

6.1.5.6.1. ASDV_MOD.1: A rendszer biztonsági terv dokumentáció ellenőrzése

Függések: ASDV_ARC.1, ASDV_SIS.1, ASDV_SDS.1, ASDV_OSC.1

Rendszer integrátori akcióelemek:

ASDV_MOD.1.1D A rendszer integrátornak a rendszer komponensein történt módosítások után ellenőriznie kell a rendszer biztonsági terv dokumentációkat (biztonsági architektúra

leírás, rendszer interfész specifikáció, STOE terv, rendszer-működési biztonsági koncepció leírás) a helyesség és ellentmondás-mentesség szempontjából.

A bizonyíték elemek tartalma és bemutatása:

ASDV_MOD.1.1C Valamennyi biztonsági terv dokumentáció esetén az ellenőrző vizsgálatnak meg kell mutatnia, hogy a módosítások a tervet nem befolyásolják, vagy a módosításokat figyelembe véve a tervet helyesen aktualizálták.

Értékelői akcióelemek:

ASDV_MOD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.6. Rendszer útmutató dokumentumok garanciaosztály

A rendszer útmutató dokumentumok garanciaosztály (ASGD) elvárásainak megfelelő értékelési bizonyítékok olyan telepítési, konfigurálási és üzemeltetési információkat nyújtanak az STOE-ról, amelyek alapján az értékelő egyrészt jobban megismerheti az értékelés tárgyát, másrészt ellenőrizheti, hogy a rendszer biztonságában különböző felelősségeket betöltő szereplők rendelkeznek-e a szükséges információkkal.

Az ASGD osztály célja a szolgáltató rendszer integrálását és üzemeltetését leíró dokumentáció megfelelőségének megítélése. Egy ilyen dokumentáció magában foglalja mindazon részleteket, amelyek a szolgáltató rendszer integrátorainak, adminisztrátorainak és felhasználóinak szólnak, akiknek nem megfelelő tevékenysége hátrányosan befolyásolhatja a szolgáltató rendszer biztonságos működését és tulajdonságait. A felhasználók nem megfelelő tevékenysége befolyásolhatja a szolgáltató rendszer felhasználói adatok védelmi képességét is.

Az ASGD garanciaosztályban szabályozott tevékenységek szoros kapcsolatban állnak azokkal a folyamatokkal és eljárásokkal, amelyeket az üzemeltetési biztonsági intézkedések határoznak meg. A különböző útmutatók a rendszer műszaki vonatkozásairól és üzemeltetési folyamatairól egyaránt tartalmaznak információkat.

Az útmutatóknak ki kell térniük a rendszer különböző üzemmódjaira is. Ezen belül kötelező megkülönböztetni a karbantartási üzemmódot és egy olyan üzemmódot, amelybe a rendszer egy hibát vagy kivételt követően kerül. Az útmutatóknak a biztonságos üzemelés fenntartása érdekében figyelembe kell venniük e két speciális üzemmód következményeit és velejáróit.

A rendszer fejlesztés garanciaosztály az alábbi 4 garanciacsaládot tartalmazza:

a) **előkészítő útmutató (ASGD_PRE),** amely a rendszer integráció során a rendszert alkotó komponensek átvételével, telepítésével, kezdeti konfigurálásával és aktiválásával kapcsolatos eljárásokra vonatkozó elvárásokat fogalmazza meg,
b) **konfigurálási útmutató (ASGD_CON),** amely azoknak a biztonságot érintő konfigurációs paramétereknek a leírását várja el, amelyek lehetővé teszik, hogy a

rendszer biztonsági funkciói megvalósítsák és érvényre juttassák a rendszer-működési biztonsági koncepciót.

c) **üzemeltetési útmutató (ASGD_OPE),** amely a biztonságosan telepített és konfigurált rendszer biztonságos működtetéséhez szükséges információkat meghatározó útmutatókra vonatkozó követelményeket adja meg,
d) **az útmutató dokumentációk aktualizálása (ASGD_MOD),** amely annak kimutatását várja el, hogy a rendszer biztonságos előkészítésére, konfigurálására és üzemeltetésére vonatkozó útmutatókat megfelelően aktualizálták a rendszer komponensek módosítása után.

6.1.6.1. Előkészítési útmutató (ASGD_PRE)

Ennek a garanciacsaládnak a keretében dokumentálni kell az STOE integrálása során alkalmazott biztonságos előkészületi eljárásokat és lépéseket, amelyeknek biztonságos konfigurációt kell eredményezniük.

Az előkészítés folyamata megköveteli, hogy az STOE-t alkotó komponensek leszállított példányait a rendszer integrátor átvegye, telepítse, konfigurálja és aktiválja annak bizonyítása céljából, hogy a TOE üzemeltetése során aktívak lesznek a szükséges védelmi tulajdonságok.

A család két garancia-összetevőt tartalmaz, amelyek csak abban különböznek, hogy az értékelőtől különböző mélységű ellenőrzési tevékenységet várnak el.

6.1.6.1.1. ASGD_PRE.1: Előkészítő útmutató

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASGD_PRE.1.1D A rendszer integrátornak a működőképes STOE mellé biztosítania kell az előkészítő útmutatót.

A bizonyíték elemek tartalma és bemutatása:

ASGD_PRE.1.1C Az előkészítő útmutatónak le kell írnia az STOE leszállított komponenseinek biztonságos elfogadásához alkalmazott valamennyi lépést, a komponens szállítójának szállítási eljárásaival összhangban.

ASGD_PRE.1.2C Az előkészítő útmutatónak le kell írnia az STOE komponenseinek biztonságos telepítéséhez, az STOE integrálásához és az üzemeltetési környezethez való biztonságos előkészülethez alkalmazott valamennyi lépést, az SST-ben leírt, üzemeltetési környezetre vonatkozó biztonsági célokkal összhangban.

Értékelői akcióelemek:

ASGD_PRE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.6.1.2. ASGD_PRE.2: Az előkészítő útmutató igazolása

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASGD_PRE.2.1D A rendszer integrátornak a működőképes STOE mellé biztosítania kell az előkészítő útmutatót.

A bizonyíték elemek tartalma és bemutatása:

ASGD_PRE.2.1C Az előkészítő útmutatónak le kell írnia az STOE leszállított komponenseinek biztonságos elfogadásához alkalmazott valamennyi lépést, a komponens szállítójának szállítási eljárásaival összhangban.

ASGD_PRE.2.2C Az előkészítő útmutatónak le kell írnia az STOE komponenseinek biztonságos telepítéséhez, az STOE integrálásához és az üzemeltetési környezethez való biztonságos előkészülethez alkalmazott valamennyi lépést, az SST-ben leírt, üzemeltetési környezetre vonatkozó biztonsági célokkal összhangban.

Értékelői akcióelemek:

ASGD_PRE.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_PRE.2.2E **Az értékelőnek független ellenőrzést kell végeznie az előkészítő útmutató tartalmának gyakorlati alkalmazására vonatkozóan az alábbiak útján: [kiválasztás: személyi interjúk, az előkészítő útmutató mintavételezése, az előkészítés eredményének mintavételen alapuló független vizsgálata].**

6.1.6.2. Konfigurálási útmutató (ASGD_CON)

Az ASGD_CON garanciacsalád által elvárt konfigurálási útmutatónak az a célja, hogy megadja azokat a biztonság-vonzatú konfigurációs paramétereket, amelyek támogatják a rendszer komponenseinek az integrálását, és amelyek lehetővé teszik, hogy a rendszer biztonsági funkciói megvalósítsák és érvényre juttassák a rendszer-működési biztonsági koncepciót és az ehhez kapcsolódó szabályzatokat.

A család két garancia-összetevőt tartalmaz, amelyek csak abban különböznek, hogy az értékelőtől különböző mélységű ellenőrzési tevékenységet várnak el.

6.1.6.2.1. ASGD_CON.1: Konfigurálási útmutató

Függések: ASDV_ARC.1, ASDV_OSC.1, ASDV_SSD.1

Rendszer integrátori akcióelemek:

ASGD_CON.1.1D A rendszer integrátornak biztosítania kell egy konfigurálási útmutatót, amely meghatározza azokat a biztonság-vonzatú konfigurációs paramétereket, amelyek támogatják a rendszer komponenseinek az integrálását, és amelyek lehetővé teszik, hogy a szolgáltató rendszer biztonsági funkciói megvalósítsák és érvényre juttassák a szolgáltató rendszer működésre vonatkozó biztonsági koncepcióját és a kapcsolódó szabályzatokat.

A bizonyíték elemek tartalma és bemutatása:

ASGD_CON.1.1C A konfigurálási útmutatónak le kell írnia azokat a biztonsági konfigurációs paramétereket, amelyek a rendszer integrátor vagy az ezzel azonos szerepkörű és felelősségű STOE felhasználók/adminisztrátorok számára elérhetők.

ASGD_CON.1.2C A konfigurálási útmutatónak le kell írnia azoknak a biztonsági paramétereknek a használatát, amelyeket az STOE állíthat be abból a célból, hogy megvalósítsa és érvényre juttassa a rendszer biztonsági szabályzatait.

ASGD_CON.1.3C A konfigurálási útmutatónak figyelmeztetéseket kell tartalmaznia a konfigurálás által hozzáférhető azon funkciókra és privilégiumokra vonatkozóan, amelyeket egy biztonságos feldolgozási környezetben ellenőrizni kell.

ASGD_CON.1.4C A konfigurálási útmutatónak világosan be kell mutatnia az összes konfigurálással kapcsolatos felelősséget, amely az STOE biztonságos működtetéséhez szükséges.

ASGD_CON.1.5C A konfigurálási útmutatónak ellentmondás mentesnek kell lennie az értékeléshez átadott összes többi dokumentumhoz viszonyítva.

ASGD_CON.1.6C A konfigurálási útmutatónak le kell írnia az összes olyan biztonsági követelményt, amely az STOE-ra vonatkozik, beleértve az üzemeltetési környezetet is.

ASGD_CON.1.7C A konfigurálási útmutatónak meg kell mutatnia, hogy az STOE terv megvalósítja az összes olyan komponensre vonatkozó biztonsági paramétert, amelyet a rendszer-működési biztonsági koncepció megkövetel.

Értékelői akcióelemek:

ASGD_CON.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.6.2.2. ASGD_CON.2: A konfigurálási útmutató igazolása

Függések: ASDV_ARC.1, ASDV_OSC.1, ASDV_SSD.1

Rendszer integrátori akcióelemek:

ASGD_CON.2.1D A rendszer integrátornak biztosítania kell egy konfigurálási útmutatót, amely meghatározza azokat a biztonság-vonzatú konfigurációs paramétereket, amelyek támogatják a rendszer komponenseinek az integrálását, és amelyek lehetővé teszik, hogy a szolgáltató rendszer biztonsági funkciói megvalósítsák és érvényre juttassák a szolgáltató rendszer működésre vonatkozó biztonsági koncepcióját és a kapcsolódó szabályzatokat.

A bizonyíték elemek tartalma és bemutatása:

ASGD_CON.2.1C A konfigurálási útmutatónak le kell írnia azokat a biztonsági konfigurációs paramétereket, amelyek a rendszer integrátor vagy az ezzel azonos szerepkörű és felelősségű STOE felhasználók/adminisztrátorok számára elérhetők.

ASGD_CON.2.2C A konfigurálási útmutatónak le kell írnia azoknak a biztonsági paramétereknek a használatát, amelyeket az STOE állíthat be abból a célból, hogy megvalósítsa és érvényre juttassa a rendszer biztonsági szabályzatait.

ASGD_CON.2.3C A konfigurálási útmutatónak figyelmeztetéseket kell tartalmaznia a konfigurálás által hozzáférhető azon funkciókra és privilégiumokra vonatkozóan, amelyeket egy biztonságos feldolgozási környezetben ellenőrizni kell.

ASGD_CON.2.4C A konfigurálási útmutatónak világosan be kell mutatnia az összes konfigurálással kapcsolatos felelősséget, amely az STOE biztonságos működtetéséhez szükséges.

ASGD_CON.2.5C A konfigurálási útmutatónak ellentmondás mentesnek kell lennie az értékeléshez átadott összes többi dokumentumhoz viszonyítva.

ASGD_CON.2.6C A konfigurálási útmutatónak le kell írnia az összes olyan biztonsági követelményt, amely az STOE-ra vonatkozik, beleértve az üzemeltetési környezetet is.

ASGD_CON.2.7C A konfigurálási útmutatónak meg kell mutatnia, hogy az STOE terv megvalósítja az összes olyan komponensre vonatkozó biztonsági paramétert, amelyet a rendszer-működési biztonsági koncepció megkövetel.

Értékelői akcióelemek:

ASGD_CON.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_CON.2.2E **Az értékelőnek mintavételezéssel, függetlenül ellenőriznie kell a konfigurálási útmutatóban meghatározott konfigurációs paraméterek gyakorlati alkalmazását.**

6.1.6.3. Üzemeltetési útmutató (ASGD_OPE)

Az ASGD_OPE garanciacsalád keretében elkészítendő üzemeltetési útmutató minden felhasználói szerepkörre leírja az SSF által nyújtott biztonsági funkcionalitást és interfészeket, tartalmazza a rendszer biztonságos használatához szükséges utasításokat és útmutatást, lefedi az összes üzemmód biztonságos eljárásait, valamint lehetővé teszi az STOE nem biztonságos állapotainak megelőzését és észlelését.

A lehetséges felhasználói szerepkörök az értékelések nagy részénél a „rendszeradminisztrátor”, a „rendszerüzemeltető” és a „végfelhasználó” szerepköröket jelenti, de ezek szükség esetén tovább finomíthatók.

A család két garancia-összetevőt tartalmaz, ezek csak abban különböznek, hogy az értékelőtől különböző mélységű ellenőrzési tevékenységet várnak el.

6.1.6.3.1. ASGD_OPE.1: Üzemeltetési útmutató

Függések: ASDV_SIS.1

Rendszer integrátori akcióelemek:

ASGD_OPE.1.1D A rendszer integrátornak üzemeltetési útmutatót kell biztosítania.

A bizonyíték elemek tartalma és bemutatása:

ASGD_OPE.1.1C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia azokat a felhasználó által elérhető funkciókat és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

ASGD_OPE.1.2C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia, hogy az STOE által biztosított, elérhető interfészeket hogyan kell biztonságos módon használni.

ASGD_OPE.1.3C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági szempontból fontos paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket.

ASGD_OPE.1.4C Az üzemeltetési útmutatónak minden felhasználói szerepkörre világosan be kell mutatnia a felhasználó által elérhető funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból fontos minden esemény típust, beleértve az SSF ellenőrzése alá eső egyedek biztonsági tulajdonságainak megváltoztatását is.

ASGD_OPE.1.5C Az üzemeltetési útmutatónak azonosítani kell az STOE összes lehetséges üzemmódját (beleértve a karbantartási és a meghibásodás vagy üzemeltetési hiba utáni üzemmódokat is), valamint ezek biztonságos üzemeltetésre gyakorolt következményeit és kihatásait.

ASGD_OPE.1.6C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia azokat a betartandó biztonsági intézkedéseket, melyek az SST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

ASGD_OPE.1.7C Az üzemeltetési útmutatónak egyértelműnek és megalapozottnak kell lennie.

Értékelői akcióelemek:

ASGD_OPE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.6.3.2. ASGD_OPE.2: Az üzemeltetési útmutató igazolása

Függések: ASDV_SIS.1

Rendszer integrátori akcióelemek:

ASGD_OPE.2.1D A rendszer integrátornak üzemeltetési útmutatót kell biztosítania.

A bizonyíték elemek tartalma és bemutatása:

ASGD_OPE.2.1C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia azokat a felhasználó által elérhető funkciókat és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

ASGD_OPE.2.2C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia, hogy az STOE által biztosított, elérhető interfészeket hogyan kell biztonságos módon használni.

ASGD_OPE.2.3C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági szempontból fontos paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket.

ASGD_OPE.2.4C Az üzemeltetési útmutatónak minden felhasználói szerepkörre világosan be kell mutatnia a felhasználó által elérhető funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból fontos minden esemény típust, beleértve az SSF ellenőrzése alá eső egyedek biztonsági tulajdonságainak megváltoztatását is.

ASGD_OPE.2.5C Az üzemeltetési útmutatónak azonosítani kell az STOE összes lehetséges üzemmódját (beleértve a meghibásodás vagy üzemeltetési hiba utáni műveleteket is), valamint ezek biztonságos üzemeltetésre gyakorolt következményeit és kihatásait.

ASGD_OPE.2.6C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia azokat a betartandó biztonsági intézkedéseket, melyek az SST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

ASGD_OPE.2.7C Az üzemeltetési útmutatónak egyértelműnek és megalapozottnak kell lennie.

Értékelői akcióelemek:

ASGD_OPE.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_OPE.2.2E **Az értékelőnek független ellenőrzést kell végeznie az üzemeltetési útmutató specifikációinak gyakorlati alkalmazását illetően, az alábbiak útján: [kiválasztás: személyi interjúk, az üzemeltetési útmutató mintavételezése, az üzemeltetés eredményeinek mintavételen alapuló független vizsgálata].**

6.1.6.4. Az útmutató dokumentációk aktualizálása (ASGD_MOD)

Az ASGD_MOD garanciacsalád célja annak kimutatása, hogy a rendszer útmutató dokumentáció helyes marad a rendszer komponensek módosításai után is.

A család egy garancia-összetevőt tartalmaz.

Az ASGD_MOD.1 komponens nem csak a rendszer útmutató dokumentációk módosított részeivel foglalkozik, hanem olyan részekkel is, amelyek esetleg érvényüket veszthették.

6.1.6.4.1. ASGD_MOD.1: Az útmutató dokumentációk aktualizálása

Függések: ASGD_PRE.1, ASGD_CON.1, ASGD_OPE.1

Rendszer integrátori akcióelemek:

ASGD_MOD.1.1D A rendszer integrátornak ellenőriznie kell a rendszer teljes konfigurációját és útmutató dokumentációját abból a szempontból, hogy azok továbbra is helyesek és következetesek-e, a rendszer komponenseinek, konfigurációjának vagy üzemeltetési környezetének módosítása után.

A bizonyíték elemek tartalma és bemutatása:

ASGD_MOD.1.1C Az ellenőrző vizsgálatnak minden útmutatóra meg kell mutatnia, hogy a módosítások a dokumentumot nem érintették, vagy a módosításokat figyelembe véve a dokumentációt helyesen aktualizálták.

Értékelői akcióelemek:

ASGD_MOD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.7. Rendszer konfiguráció kezelés garanciaosztály

A rendszer konfiguráció kezelés garanciaosztály (ASCM) célja, hogy az értékelés során garanciát biztosítson arra, hogy minden rendszer komponens helyes verziója áll az értékelő rendelkezésére. A konfiguráció kezelés a kezdeti értékelés során a fejlesztési/integrálási környezeten belüli intézkedésekre vonatkozik, a felülvizsgálati értékelések során pedig az üzemeltetési/karbantartási környezetre.

A konfiguráció kezelés felügyeli a rendszer értékelt (tanúsított) és nem értékelt (nem tanúsított) termékeit is.

A konfiguráció kezelés meghatározza és leírja a rendszer komponenseit, az integrálás konfigurációját (amely magában foglal minden speciális együttműködési funkcionalitást) és az üzemelési konfigurációt (amely meghatározza a komponensek futásidejű konfigurációjának paraméter beállításait). Változásellenőrzési szabályokról és eljárásokról is gondoskodik a rendszer aktuális változtatásainak ellenőrzésére és nyomon követésére.

A konfiguráció kezelés garanciaosztály az alábbi 2 garanciacsaládot tartalmazza:

a) **rendszer alap konfiguráció (ASCM_SBC),** amely a rendszer értékelt alap konfigurációjának és az ezt alkotó komponensek meghatározását, majd e alap konfiguráción történt változtatások ellenőrzését és nyomon követését várja el.
b) **értékelt és tanúsított komponensek (ASCM_ECC),** amely elvárja, hogy meghatározzák a rendszer értékelt és tanúsított komponenseit, az ezekre tanúsított garancia szintjét, a garancia fenntartásához szükséges üzemeltetési feltételeket, valamint ezek megfelelőségét az elvárt rendszer garanciacsomag szerint.

6.1.7.1. Rendszer alap konfiguráció (ASCM_SBC)

Az ASCM_SBC garanciacsalád célja a rendszer értékelt konfigurációjának és biztonsági komponenseinek a meghatározása, valamint ezen alap konfiguráción történt változtatások ellenőrzése és nyomon követése.

Ez a család mind a műszaki, mind az üzemeltetési intézkedéseket nyomon követi. A rendszer alap konfigurációt minden felülvizsgálati értékelés során aktualizálják, hogy mindig a legfrissebb értékelt alap konfigurációt tükrözze, amely a következő módosítás vagy értékelés vonatkoztatási alapját képezi.

A család két garancia-összetevőt tartalmaz, amelyek csak abban különböznek, hogy az értékelőtől különböző mélységű ellenőrzési tevékenységet várnak el.

6.1.7.1.1. ASCM_SBC.1: Rendszer alap konfiguráció

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASCM_SBC.1.1D A rendszer integrátornak konfiguráció kezelés (CM) rendszert kell használnia a kezdeti/legutolsó értékelt rendszerhez, amelyet „alap konfiguráció”-nak kell nevezni.

ASCM_SBC.1.2D A CM rendszernek nyomon kell követnie és felügyelnie kell minden tervezett és tényleges változtatást a rendszer alap konfigurációján, és ezek értékelési állapotát.

ASCM_SBC.1.3D A rendszer integrátornak vagy rendszer tulajdonosnak CM dokumentációt kell nyújtania a rendszer alap konfigurációjához.

A bizonyíték elemek tartalma és bemutatása:

ASCM_SBC.1.1C A CM rendszernek egyedileg azonosítania kell az STOE alap konfigurációt, az alap konfigurációt alkotó összes rendszer komponenst és ezek értékelési állapotát.

ASCM_SBC.1.2C A CM rendszernek nyomon kell követnie az alap konfigurációhoz, illetve az ezt alkotó rendszer komponensekhez kapcsolódó változtatásokat.

ASCM_SBC.1.3C A CM tervnek le kell írnia, hogy a rendszer alap konfigurációját hogyan kezelik, és hogy az alap konfiguráción történő módosításokat hogyan ellenőrzik és hogyan követik nyomon.

Értékelői akcióelemek:

ASCM_SBC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.7.1.2. ASCM_SBC.2: A rendszer alap konfiguráció igazolása

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASCM_SBC.2.1D A rendszer integrátornak CM rendszert kell használnia a kezdeti/legfrissebb értékelt rendszerhez, amelyet „alap konfiguráció”-nak kell nevezni.

ASCM_SBC.2.2D A CM rendszernek nyomon kell követnie és felügyelnie kell minden tervezett és tényleges változtatást a rendszer alap konfigurációján, és ezek értékelési állapotát.

ASCM_SBC.2.3D A rendszer integrátornak vagy rendszertulajdonosnak CM dokumentációt kell nyújtania a rendszer alap konfigurációjához.

A bizonyíték elemek tartalma és bemutatása:

ASCM_SBC.2.1C A CM rendszernek egyedileg azonosítania kell az STOE alap konfigurációt, az alap konfigurációt alkotó összes rendszer komponenst és ezek értékelési állapotát.

ASCM_SBC.2.2C A CM rendszernek nyomon kell követnie az alap konfigurációhoz, illetve az ezt alkotó rendszer komponensekhez kapcsolódó változtatásokat.

ASCM_SBC.2.3C A CM tervnek le kell írnia, hogy a rendszer alap konfigurációját hogyan kezelik, és hogy az alap konfiguráción történő módosításokat hogyan ellenőrzik és hogyan követik nyomon.

Értékelői akcióelemek:

ASCM_SBC.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASCM_SBC.2.2E **Az értékelőnek független ellenőrzést kell végeznie a CM rendszer alap konfiguráció tartalmára vonatkozóan, személyi interjúk és a módosítások mintavételezése útján.**

6.1.7.2. Értékelt és tanúsított komponensek (ASCM_ECC)

Értékelt komponens-termékek

Az ASCM_ECC garanciacsalád elsődleges célja a rendszert alkotó komponensek közül azok meghatározása, melyeket termékként már függetlenül értékeltek és tanúsítottak. Kiegészítő cél e termékek megszerzett garanciájának megőrzése a rendszer integráció során. Ez a termék tanúsítványokban és tanúsítási jelentésekben megfogalmazott üzemeltetési feltételek vizsgálatával, a rendszer üzemeltetési feltételekkel való egybevetésével, illetve a rendszer üzemeltetési feltételek megfelelő alakításával érhető el. További cél annak ellenőrzése, hogy a rendszerben biztonsági szempontból jelentős szerepet játszó komponensek rendelkeznek-e olyan szintű tanúsítási eredménnyel, melyet az adott garanciacsomag megkövetel.

A család három garancia-összetevőt tartalmaz, annak megfelelően, hogy a különböző garanciacsomagokban a komponensek tanúsítására vonatkozó elvárások eltérőek.

6.1.7.2.1. ASCM_ECC.1: A tanúsított komponensek felmérése

Függések: ASDV_SDS.1, ASCM_SBC.1

Rendszer integrátori akcióelemek:

ASCM_ECC.1.1D A rendszer integrátornak az STOE alap konfigurációját alkotó termék-komponensek közül meg kell határoznia az értékelt és tanúsított termék-komponensek listáját, valamint az ezekre vonatkozó garancia csomagokat.

ASCM_ECC.1.2D A rendszer integrátornak specifikálnia kell minden értékelt és tanúsított rendszer komponensre a termék üzemeltetési feltételeit.

A bizonyíték elemek tartalma és bemutatása:

ASCM_ECC.1.1C Az értékelt és tanúsított termék-komponensek listájában le kell írni az értékelt és tanúsított termékek garancia csomagjait.

ASCM_ECC.1.2C Az értékelt és tanúsított termék-komponensek listájának minden termékre azonosítania kell az értékelési eredményekre vonatkozó tanúsítványt, tanúsítási jelentést és az ezek alapjául szolgáló biztonsági előirányzatot.

ASCM_ECC.1.3C Az értékelt és tanúsított termék-komponensek listájának minden termékre le kell írnia az üzemeltetési feltételeket.

Értékelői akcióelemek:

ASCM_ECC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASCM_ECC.1.2E Az értékelőnek meg kell erősítenie, hogy a rendszer üzemeltetési környezete kielégíti az értékelt és tanúsított termékek tanúsítványaiban és tanúsítási jelentéseiben megfogalmazott üzemeltetési feltételeket.

6.1.7.2.2. ASCM_ECC.2: A tanúsított komponensek ellenőrzése SAP-F elvárásai szerint

Függések: ASDV_SDS.1, ASCM_SBC.2

Rendszer integrátori akcióelemek:

ASCM_ECC.2.1D A rendszer integrátornak az STOE alap konfigurációját alkotó termék-komponensek közül meg kell határoznia az értékelt és tanúsított termék-komponensek listáját, valamint az ezekre vonatkozó garancia csomagokat.

ASCM_ECC.2.2D A rendszer integrátornak specifikálnia kell minden értékelt és tanúsított rendszer komponensre a termék üzemeltetési feltételeit.

A bizonyíték elemek tartalma és bemutatása:

ASCM_ECC.2.1C Az értékelt és tanúsított termék-komponensek listájában le kell írni az értékelt és tanúsított termékek garancia csomagjait.

ASCM_ECC.2.2C Az értékelt és tanúsított termék-komponensek listájának minden termékre azonosítania kell az értékelési eredményekre vonatkozó tanúsítványt, tanúsítási jelentést és az ezek alapjául szolgáló biztonsági előirányzatot.

ASCM_ECC.2.3C Az értékelt és tanúsított termék-komponensek listájának minden termékre le kell írnia az üzemeltetési feltételeket.

Értékelői akcióelemek:

ASCM_ECC.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASCM_ECC.2.2E Az értékelőnek meg kell erősítenie, hogy a rendszer üzemeltetési környezete kielégíti az értékelt és tanúsított termékek tanúsítványaiban és tanúsítási jelentéseiben megfogalmazott üzemeltetési feltételeket.

ASCM_ECC.2.3E **Az értékelőnek meg kell erősítenie, hogy a rendszer biztonsági funkcionalitását érvényre juttató és támogató termék komponensek tanúsítására vonatkozóan teljesülnek a SAP-F garanciacsomag elvárásai.**

6.1.7.2.3. ASCM_ECC.3: A tanúsított komponensek ellenőrzése SAP-K elvárásai szerint

Függések: ASDV_SDS.1, ASCM_SBC.2

Rendszer integrátori akcióelemek:

ASCM_ECC.3.1D A rendszer integrátornak az STOE alap konfigurációját alkotó termék-komponensek közül meg kell határoznia az értékelt és tanúsított termék-komponensek listáját, valamint az ezekre vonatkozó garancia csomagokat.

ASCM_ECC.3.2D A rendszer integrátornak specifikálnia kell minden értékelt és tanúsított rendszer komponensre a termék üzemeltetési feltételeit.

A bizonyíték elemek tartalma és bemutatása:

ASCM_ECC.3.1C Az értékelt és tanúsított termék-komponensek listájában le kell írni az értékelt és tanúsított termékek garancia csomagjait.

ASCM_ECC.3.2C Az értékelt és tanúsított termék-komponensek listájának minden termékre azonosítania kell az értékelési eredményekre vonatkozó tanúsítványt, tanúsítási jelentést és az ezek alapjául szolgáló biztonsági előirányzatot.

ASCM_ECC.3.3C Az értékelt és tanúsított termék-komponensek listájának minden termékre le kell írnia az üzemeltetési feltételeket.

Értékelői akcióelemek:

ASCM_ECC.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASCM_ECC.3.2E Az értékelőnek meg kell erősítenie, hogy a rendszer üzemeltetési környezete kielégíti az értékelt és tanúsított termékek tanúsítványaiban és tanúsítási jelentéseiben megfogalmazott üzemeltetési feltételeket.

ASCM_ECC.3.3E Az értékelőnek meg kell erősítenie, hogy a rendszer biztonsági funkcionalitását érvényre juttató és támogató termék komponensek tanúsítására vonatkozóan teljesülnek a SAP-K garanciacsomag elvárásai.

6.1.8. Rendszer tesztelés garanciaosztály

A rendszer tesztelés garanciaosztály (ASTE) célja annak az ellenőrzése, hogy a működő (szolgáltató) informatikai rendszer komponensei – miután a rendszer architektúrájának és a rendszer konfigurálási útmutatójának megfelelően telepítették, integrálták és konfigurálták - megfelelnek az SST-ben meghatározott funkcionális biztonsági követelményeknek, és hatékonyan érvényre juttatják a rendszer-működtetési biztonsági koncepciót.

A tesztelés megtervezését és végrehajtását segíti a rendszer interfész specifikáció (ASTE_SIS), rendszer biztonsági architektúra leírása (ASTE_ARC), valamint a rendszer biztonsági terve (ASTE_SDS).

A tesztelés értékelése során az értékelő megállapítja, hogy az SSF-t a konfigurálási útmutatóban megadottaknak megfelelően konfigurálták-e, a rendszer biztonsági architektúra leírás és a rendszer biztonsági terv szerint tesztelték-e, valamint megismétli a fejlesztői-integrátori tesztek egy mintáját, és függetlenül teszteli az SSF egy részhalmazát.

A rendszer tesztelés garanciaosztály az alábbi 5 garanciacsaládot tartalmazza:

a) **funkcionális rendszer tesztelés (ASTE_FUN),** mely elvárja, hogy a rendszer integrátor dokumentálja azokat a tesztjeit, melyeket az STOE megfelelő (terv dokumentációkban meghatározott) működésének kimutatására hajtott végre,
b) **a rendszer tesztelés lefedettsége (ASTE_COV),** mely elvárja a rendszer integrátortól annak kimutatását, hogy a biztonsági funkcionalitást letesztelte a rendszer interfész specifikációnak megfelelően,
c) **a rendszer tesztelés mélysége (ASTE_DPT),** melynek különböző összetevői a rendszer integrátortól elvárják annak kimutatását, hogy a biztonsági funkcionalitást letesztelte a rendszer (különböző mélységű) belső működésének megfelelően,

d) **független rendszer tesztelés (ASTE_IND),** mely (az értékelőtől) elvárja, hogy ellenőrizze a rendszer integrátor tesztelését, s ezen felül független biztonsági tesztelést is végezzen.
e) **Regressziós tesztelés (ASTE_MOD),** mely annak kimutatását várja el, hogy a biztonsági funkciók a specifikáltaknak megfelelően működnek a rendszer komponenseken, a rendszer konfiguráción vagy az üzemeltetési környezeten végzett módosítások után is.

6.1.8.1. Funkcionális rendszer tesztelés (ASTE_FUN)

Az ASTE_FUN garanciacsalád célja annak kimutatása, hogy a rendszer minden biztonsági funkciója a specifikáltaknak megfelelően működik. A rendszer integrátornak ehhez teszteléseket kell végeznie és tesztelése eredményeit dokumentálnia kell.

A rendszer integrátor által végrehajtott funkcionális tesztelés megalapozza, hogy az SSF rendelkezik azokkal a tulajdonságokkal, amelyek az SST funkcionális biztonsági követelményeinek a kielégítéséhez szükségesek. Az ilyen funkcionális tesztelés garanciát nyújt arra, hogy az SSF kielégíti legalább a funkcionális biztonsági követelményeket, bár azt nem tudja megállapítani, hogy az SSF nem végez-e a specifikáltaknál többet. A „Funkcionális rendszer tesztelés" garanciacsalád az elvárt dokumentáció és támogató eszközök típusára és mennyiségére koncentrál, valamit arra, hogy mit kell a rendszer integrátori tesztelésnek kimutatnia.

A funkcionális rendszer tesztelés nem korlátozódik annak pozitív megerősítésére, hogy az elvárt funkcionális biztonsági funkciókat biztosították, annak ellenőrzésére vonatkozó negatív tesztelést is tartalmazhat, hogy bizonyos nemkívánatos tulajdonságok valóban nincsenek meg (gyakran a funkcionális követelmények megfordításán alapulva).

A család egy garancia-összetevőt tartalmaz. Ugyanakkor a teszt tervre és az eredmények bemutatására vonatkozóan elvárt információ mennyisége változni fog az ASTE_COV és ASTE_DPT használatával összhangban.

6.1.8.1.1. ASTE_FUN.1: Funkcionális tesztelés

Függések: ASTE_COV.1

Rendszer integrátori akcióelemek:

ASTE_FUN.1.1D A rendszer integrátornak tesztelnie kell a rendszer biztonsági funkcionalitását (SSF-t), és ennek eredményeit dokumentálnia kell.

ASTE_FUN.1.2D A rendszer integrátornak tesztdokumentációt kell biztosítania.

ASTE_FUN.1.3D A rendszer integrátornak biztosítania kell egy vizsgálatot tesztelése teljességéről.

A bizonyíték elemek tartalma és bemutatása:

ASTE_FUN.1.1C A tesztdokumentációnak tartalmaznia kell a teszttterveket, a várt teszteredményeket és a tényleges teszteredményeket.

ASTE_FUN.1.2C A teszttterveknek azonosítaniuk kell a végrehajtandó teszteket, és le kell írniuk minden teszt végrehajtásának forgatókönyvét. Ezen forgatókönyveknek tartalmazniuk kell a más tesztek eredményeitől való minden sorrendbeli függést.

ASTE_FUN.1.3C A várt teszteredményeknek be kell mutatniuk a tesztek sikeres végrehajtásából keletkező várható kimeneteket.

ASTE_FUN.1.4C A tényleges teszteredményeknek összhangban kell állniuk a várt teszteredményekkel.

ASTE_FUN.1.5C A tesztdokumentációnak tartalmaznia kell egy vizsgálatot a teszt eljárás sorrendi függőségeiről.

ASTE_FUN.1.6C A biztonsági intézkedések tesztelésének részletességére vonatkozó vizsgálatának be kell mutatnia, hogy az SST-ben elvárt funkcionális biztonsági követelmények és a tesztdokumentációban megadott tesztek közötti megfeleltetés teljes.

Értékelői akcióelemek:

ASTE_FUN.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.8.2. A rendszer tesztelés lefedettsége (ASTE_COV)

Az ASTE_COV garanciacsalád a teszt lefedettség teljességével foglalkozik, vagyis azt tárgyalja, hogy az SSF milyen mértékben legyen tesztelve a specifikáltaknak megfelelő működés kimutatásához.

A garanciacsalád célja annak megalapozása, hogy az SSF-t a rendszer interfész specifikáció szerint módszeresen letesztelték.

A rendszer integrátornak be kell mutatnia, hogy a megadott tesztek minden biztonsági funkciót tesztelnek, a rendszer interfész specifikációban (ASDV_SIS) leírtaknak megfelelően. A rendszer integrátornak nem csak a tesztek és biztonsági funkciók (biztonsági követelmények) közötti megfeleltetést kell megmutatnia, hanem elegendő információt is kell nyújtania az értékelő számára annak megállapításához, hogy a funkciókat hogyan próbálta ki. Ezeket az információkat az értékelő felhasználhatja kiegészítő független tesztjei tervezésénél.

A család egy garancia-összetevőt tartalmaz.

6.1.8.2.1. ASTE_COV.1: A teszt lefedettség vizsgálata

Függések: ASDV_SIS.1, ASTE_FUN.1

Rendszer integrátori akcióelemek:

ASTE_COV.1.1D A rendszer integrátornak biztosítania kell a teszt lefedettség elemzését.

A bizonyíték elemek tartalma és bemutatása:

ASTE_COV.1.1C A teszt lefedettség elemzésnek be kell mutatnia a tesztdokumentációban azonosított tesztek és a rendszer biztonsági funkcionalitás (ahogyan azt a rendszer interfész specifikáció a külső interfészeken keresztül leírja) közötti megfeleltetést.

Megjegyzés: Bár a rendszer integrátornak be kell mutatnia, hogy a rendszer interfész specifikációban lévő minden funkciót letesztelte, nincs megkövetelve, hogy az egyes funkciókat kimerítően tesztelje.

Értékelői akcióelemek:

ASTE_COV.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.8.3. A rendszer tesztelés mélysége (ASTE_DPT)

Az ASTE_DPT garanciacsalád célja annak a kockázatnak a kivédése, hogy hiba történt az STOE fejlesztésében és integrálásában. E család komponensei (mivel a tesztelés mélysége nagyobb mértékben foglalkozik az SSF belső struktúrájával), nagyobb valószínűséggel feltárhatják a komponensekbe illesztett rosszindulatú kódokat, illetve az integráció során bekerült hibákat.

A speciális belső interfészeket is érintő tesztelés nem csak arra nyújt garanciát, hogy az SSF felmutatja a megkívánt külső biztonsági működést, hanem arra is, hogy ez a működés helyesen működő belső mechanizmusokon alapul.

A rendszer interfész specifikációnak megfelelő teszteléssel az ASTE_COV garanciacsalád foglalkozik.

A család 3 garancia-összetevőt tartalmaz, melyek aszerint különböznek egymástól, hogy az SSF milyen részletességű megjelenítését és tesztelését várják el.

6.1.8.3.1. ASTE_DPT.1: Tesztelés: rendszer architektúra

Ez a garancia-összetevő a rendszer integrátor funkcionális tesztelését a biztonsági architektúra leírással összhangban várja el.

A biztonsági architektúra leírás ismerteti az STOE-hez kapcsolódó külső informatikai rendszereket, egymáshoz kapcsolódásukat, valamint a köztük folyó információáramlást.
Ennek megfelelően a tesztelési bizonyítékoknak meg kell mutatniuk, hogy az STOE és a külső informatikai rendszerek közötti kapcsolódásokat letesztelték.

Függések: ASDV_ARC.1, ASTE_FUN.1

Rendszer integrátori akcióelemek:

ASTE_DPT.1.1D A rendszer integrátornak tesztmélység elemzést kell biztosítania.

A bizonyíték elemek tartalma és bemutatása:

ASTE _DPT.1.1C A tesztmélység elemzésnek be kell mutatnia, hogy a tesztdokumentációban azonosított tesztek elegendőek annak bemutatására, hogy a rendszer biztonsági funkcionalitása a rendszer biztonsági architektúra leírással összhangban működik.

Értékelői akcióelemek:

ASTE_DPT.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.8.3.2. ASTE_DPT.2: Tesztelés: alrendszerek

Ez a garancia-összetevő a rendszer integrátor funkcionális tesztelését az alrendszerek szintjén várja el.

A rendszer biztonsági terv (STOE terv) leírja az STOE szerkezetét alrendszerek szerint, meghatározva az egyes alrendszerek által nyújtott biztonsági funkcionalitást, valamint minden alrendszerhez a csatlakozó interfészeket.

Ennek megfelelően a tesztelési bizonyítékoknak meg kell mutatniuk, hogy az alrendszerek közötti belső interfészeket is letesztelték.

Függések: ASDV_ARC.1, ASDV_SDS.1, ASTE_FUN.1

Rendszer integrátori akcióelemek:

ASTE_DPT.2.1D A rendszer integrátornak tesztmélység elemzést kell biztosítania.

A bizonyíték elemek tartalma és bemutatása:

ASTE _DPT.2.1C A tesztmélység elemzésnek be kell mutatnia, hogy a tesztdokumentációban azonosított tesztek elegendőek annak bemutatására, hogy a rendszer biztonsági funkcionalitása a rendszer biztonsági architektúra leírással, **valamint a rendszer biztonsági terv alrendszerekre vonatkozó leírásával** összhangban működik.

Értékelői akcióelemek:

ASTE_DPT.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.8.3.3. ASTE_DPT.3: Tesztelés: komponensek

Ez a garancia-összetevő a rendszer integrátor funkcionális tesztelését a komponensek szintjén várja el.

A rendszer biztonsági terv (STOE terv) leírja az STOE szerkezetét alrendszerek szerint, meghatározva az egyes alrendszerek által nyújtott biztonsági funkcionalitást, valamint minden alrendszerhez a csatlakozó interfészeket.

A rendszer biztonsági terv azonosítja az alrendszereket alkotó komponenseket is, leírva a komponensek által nyújtott biztonsági funkcionalitást, a komponensek közötti belső összefüggéseket és az egyes komponensek által megvalósított, alrendszerhez csatlakozó interfészeket.

A fentieknek megfelelően a tesztelési bizonyítékoknak meg kell mutatniuk, hogy a komponensek közötti belső interfészeket is letesztelték.

Függések: ASDV_ARC.1, ASDV_SDS.1, ASTE_FUN.1

Rendszer integrátori akcióelemek:

Függések: ASDV_ARC.1, ASDV_SDS.1, ASTE_FUN.1

Rendszer integrátori akcióelemek:

ASTE_DPT.3.1D A rendszer integrátornak tesztmélység elemzést kell biztosítania.

A bizonyíték elemek tartalma és bemutatása:

ASTE _DPT.3.1C A tesztmélység elemzésnek be kell mutatnia, hogy a tesztdokumentációban azonosított tesztek elegendőek annak bemutatására, hogy a rendszer biztonsági funkcionalitása a rendszer biztonsági architektúra leírással, valamint a rendszer biztonsági terv alrendszerekre **és komponensekre** vonatkozó leírásával összhangban működik.

Értékelői akcióelemek:

ASTE_DPT.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.8.4. Független rendszer tesztelés (ASTE_IND)

Az ASTE_IND garanciacsalád célja annak kimutatása, hogy a rendszer biztonsági funkcionalitása a specifikáltaknak megfelelően működik.

További cél annak a kockázatnak a kivédése, hogy a rendszer integrátor pontatlanul értékelte ki saját teszteredményeit.

A független tesztelés az STOE megértését igényli, összhangban az egyéb garancia tevékenységekkel.

A független funkcionális tesztelés eltér a behatolás teszteléstől. Az utóbbi egy tájékozott és módszeres felkutatása a tervben és/vagy megvalósításban lévő sebezhetőségeknek. A behatolás teszteléssel az ASVA_VAN család foglalkozik.

A család egy garancia-összetevőt tartalmaz. Ugyanakkor a független teszteléshez kialakítandó értékelői teszttervnek összhangban kell állnia az egyéb garancia tevékenységek szintjével, így a nagyobb garancia a megismételt tesztek egyre bővebb mintáit és az értékelő egyre több független pozitív és negatív funkcionális tesztjét várja el.

6.1.8.4.1. ASTE_IND.1: Független tesztelés mintán

Függések: ASDV_SIS.1, ASGD_PRE.1, ASGD_OPE.1, ASTE_FUN.1, ASTE_COV.1,

Rendszer integrátori akcióelemek:

ASTE_IND.1.1D A rendszer integrátornak a teszteléshez biztosítania kell az STOE-t vagy az STOE-hez való hozzáférést.

A bizonyíték elemek tartalma és bemutatása:

ASTE_IND.1.1C Az STOE-nek tesztelésre alkalmas állapotban kell lennie.

ASTE_IND.1.2C A rendszer integrátornak biztosítania kell az SSF funkcionális tesztelése során használt erőforrás-készlettel azonos eszközkészletet.

Értékelői akcióelemek:

ASTE_IND.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASTE_IND.1.2E Az értékelőnek végre kell hajtania a tesztdokumentációban szereplő tesztek valamely részhalmazát (mintáját) a rendszer integrátor teszteredményeinek ellenőrzése érdekében.

ASTE_IND.1.3E Az értékelőnek tesztelnie kell az SSF külső és belső interfészeinek egy részét annak megerősítése érdekében, hogy az SSF a specifikáltaknak megfelelően működik.

6.1.8.5. Regressziós tesztelés (ASTE_MOD)

Az ASTE_MOD garanciacsalád célja annak kimutatása, hogy a biztonsági funkciók a specifikáltaknak megfelelően működnek a rendszer komponenseken, a rendszer konfiguráción vagy az üzemeltetési környezeten végzett módosítások után is.

A család egy garancia-összetevőt tartalmaz.

6.1.8.5.1. ASTE_MOD.1: Regressziós tesztelés

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASTE_MOD.1.1D A rendszer integrátornak tesztelnie kell az SSF módosításokkal érintett részeit, és dokumentálnia kell az eredményeket.

ASTE_MOD.1.2D A rendszer integrátornak tesztdokumentációt kell biztosítania.

ASTE_MOD.1.3D A rendszer integrátornak biztosítania kell egy vizsgálatot a regressziós tesztelésről.

A bizonyíték elemek tartalma és bemutatása:

ASTE_MOD.1.1C A tesztdokumentációnak tartalmaznia kell a teszterveket, a teszteljárások leírását, a várt teszteredményeket és a tényleges teszteredményeket.

ASTE_MOD.1.2C A teszterveknek azonosítaniuk kell a módosítások által kiváltott hatásokat és a tesztelendő biztonsági funkciókat, és le kell írniuk a végrehajtandó tesztek célját.

ASTE_MOD.1.3C A teszteljárások leírásának azonosítania kell a módosított részeken végrehajtandó teszteket, és ismertetnie kell minden biztonsági funkcióra a tesztelési forgatókönyveket. A forgatókönyveknek tartalmazniuk kell a sorrendi függőségeket a megváltoztatott részeknek és az egyéb tesztek eredményeinek a vonatkozásában.

ASTE_MOD.1.4C A rendszer integrátor által végrehajtott tesztekből származó eredményeknek meg kell mutatniuk, hogy minden tesztelt biztonsági funkció a specifikáltaknak megfelelően működik, így a módosítások nincsenek kihatással az SSF-re.

ASTE_MOD.1.5C A tesztdokumentációnak tartalmaznia kell egy vizsgálatot a teszt eljárások sorrendi függőségéről.

ASTE_MOD.1.6C A regressziós tesztelésre vonatkozó vizsgálatnak be kell mutatnia, hogy az SST-ben elvárt, módosítások által érintett funkcionális biztonsági követelmények és a tesztdokumentációban megadott tesztek közötti megfeleltetés teljes.

Értékelői akcióelemek:

ASTE_MOD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.9. Rendszer sebezhetőség felmérés garanciaosztály

6.1.9.1. Sebezhetőségi elemzés (ASVA_VAN)

Az ASVA_VAN garanciacsalád célja annak a megállapítása, hogy vannak-e hibák vagy gyengeségek a rendszerben, ahogyan azt konkrét környezetében megvalósították, konfigurálták, illetve hogy ezek kihasználhatók-e. A megállapítás az értékelő által végrehajtott vizsgálatokon alapul.

A sebezhetőségi elemzés az értékelő feladata, ehhez a rendszer integrátornak csak az értékelés tárgyához (STOE) való hozzáférést kell biztosítania.

A sebezhetőségi elemzés természetéből adódóan szorosan kapcsolódik a működő informatikai rendszer biztonsági szabályaihoz és eljárásaihoz, a fizikai biztonsági intézkedésekhez, a személyi biztonsághoz, és a meglévő biztonsági infrastruktúrához, amelynek célja, hogy hatékonyan leküzdjön bármely rendszer sebezhetőséget.

A család három garancia-összetevőt tartalmaz, ezek az értékelő által elvégzendő sebezhetőségi elemzés szigorúságában, illetve a támadókról feltételezett támadó képességi szintben különböznek.

6.1.9.1.1. ASVA_VAN.1: Gyakorlati sebezhetőség vizsgálat

Függések: ASDV_SIS.1, ASGD_PRE.1, ASGD_CON.1, ASGD_OPE.1

Rendszer integrátori akcióelemek:

ASVA_VAN.1.1D A rendszer integrátornak a teszteléshez biztosítania kell az STOE-t vagy az STOE-hez való hozzáférést.

A bizonyíték elemek tartalma és bemutatása:

ASVA_VAN.1.1C Az STOE-nak alkalmasnak kell lennie tesztelésre.

Értékelői akcióelemek:

ASVA_VAN.1.1E: Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASVA_VAN.1.2E: Az értékelőnek egy keresést kell végrehajtania nyilvános forrásokban az STOE lehetséges sebezhetőségeinek azonosítása érdekében.

ASVA_VAN.1.3E: Az értékelőnek az azonosított lehetséges sebezhetőségek alapján automatikus eszközökkel behatolás tesztelést kell végrehajtania, annak megállapítása érdekében, hogy az STOE ellenáll egy alap támadó képességgel rendelkező támadó által végrehajtott támadásnak.

6.1.9.1.2. ASVA_VAN.2: Független sebezhetőség vizsgálat

Függések: ASDV_ARC.1, ASDV_SIS.1, ASDV_SDS.1, ASGD_PRE.1, ASGD_CON.1, ASGD_OPE.1

Rendszer integrátori akcióelemek:

ASVA_VAN.2.1D A rendszer integrátornak a teszteléshez biztosítania kell az STOE-t vagy az STOE-hez való hozzáférést.

A bizonyíték elemek tartalma és bemutatása:

ASVA_VAN.2.1C Az STOE-nak alkalmasnak kell lennie tesztelésre.

Értékelői akcióelemek:

ASVA_VAN.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASVA_VAN.2.2E Az értékelőnek egy keresést kell végrehajtania nyilvános forrásokban az STOE lehetséges sebezhetőségeinek azonosítása érdekében.

ASVA_VAN.2.3E **Az értékelőnek egy független sebezhetőség vizsgálatot kell végrehajtania az STOE-ra, felhasználva az SST, a biztonsági architektúra leírás, a rendszer interfész specifikáció, az STOE terv, a rendszer-működési biztonsági koncepció és az útmutató dokumentációk által biztosított ismereteket, az STOE lehetséges sebezhetőségeinek azonosítása érdekében.**

ASVA_VAN.2.4E Az értékelőnek az azonosított lehetséges sebezhetőségek alapján **automatikus eszközöket is felhasználva**, behatolás tesztelést kell végrehajtania, annak megállapítása érdekében, hogy az STOE ellenáll egy alap támadó képességgel rendelkező támadó által végrehajtott támadásnak.

6.1.9.1.3. ASVA_VAN.3: Ellenállás megemelt-alap támadó képességgel szemben

Függések: ASDV_ARC.1, ASDV_SIS.1, ASDV_SDS.1, ASGD_PRE.1, ASGD_CON.1, ASGD_OPE.1

Rendszer integrátori akcióelemek:

ASVA_VAN.3.1D A rendszer integrátornak a teszteléshez biztosítania kell az STOE-t vagy az STOE-hez való hozzáférést.

A bizonyíték elemek tartalma és bemutatása:

ASVA_VAN.3.1C Az STOE-nak alkalmasnak kell lennie tesztelésre.

Értékelői akcióelemek:

ASVA_VAN.3.1E: Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASVA_VAN.3.2E: Az értékelőnek egy keresést kell végrehajtania nyilvános forrásokban az STOE lehetséges sebezhetőségeinek azonosítása érdekében.

ASVA_VAN.3.3E: Az értékelőnek egy független sebezhetőség vizsgálatot kell végrehajtania az STOE-ra, felhasználva az SST, a biztonsági architektúra leírás, a rendszer interfész specifikáció, az STOE terv, a rendszer-működési biztonsági koncepció és az útmutató dokumentációk által biztosított ismereteket, az STOE lehetséges sebezhetőségeinek azonosítása érdekében.

ASVA_VAN.3.4E: Az értékelőnek az azonosított lehetséges sebezhetőségek alapján automatikus eszközöket is felhasználva, behatolás tesztelést kell végrehajtania, annak megállapítása érdekében, hogy az STOE ellenáll egy **megemelt-alap** támadó képességgel rendelkező támadó által végrehajtott támadásnak.

6.1.10. Rendszer garancia karbantartás

6.1.10.1. Az útmutató dokumentációk aktualizálása: ASDV_MOD.1 értékelése

Függések: ASDV_ARC.1, ASDV_SIS.1, ASDV_SDS.1, ASDV_OSC.1

Rendszer integrátori akcióelemek:

ASDV_MOD.1.1D A rendszer integrátornak a rendszer komponensein történt módosítások után ellenőriznie kell a rendszer biztonsági terv dokumentációkat (biztonsági architektúra leírás, rendszer interfész specifikáció, STOE terv, rendszer-működési biztonsági koncepció leírás) a helyesség és ellentmondás-mentesség szempontjából.

A bizonyíték elemek tartalma és bemutatása:

ASDV_MOD.1.1C Valamennyi biztonsági terv dokumentáció esetén az ellenőrző vizsgálatnak meg kell mutatnia, hogy a módosítások a tervet nem befolyásolják, vagy a módosításokat figyelembe véve a tervet helyesen aktualizálták.

Értékelői akcióelemek:

ASDV_MOD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.10.2. Az útmutató dokumentációk aktualizálása: ASGD_MOD.1 értékelése

Függések: ASGD_PRE.1, ASGD_CON.1, ASGD_OPE.1

Rendszer integrátori akcióelemek:

ASGD_MOD.1.1D A rendszer integrátornak ellenőriznie kell a rendszer teljes konfigurációját és útmutató dokumentációját abból a szempontból, hogy azok továbbra is helyesek és következetesek-e, a rendszer komponenseinek, konfigurációjának vagy üzemeltetési környezetének módosítása után.

A bizonyíték elemek tartalma és bemutatása:

ASGD_MOD.1.1C Az ellenőrző vizsgálatnak minden útmutatóra meg kell mutatnia, hogy a módosítások a dokumentumot nem érintették, vagy a módosításokat figyelembe véve a dokumentációt helyesen frissítették.

Értékelői akcióelemek:

ASGD_MOD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.1.10.3. Regressziós tesztelés: ASTE_MOD.1 értékelése

Függések: Nincsenek függések.

Rendszer integrátori akcióelemek:

ASTE_MOD.1.1D A rendszer integrátornak tesztelnie kell az SSF módosításokkal érintett részeit, és dokumentálnia kell az eredményeket.

A bizonyíték elemek tartalma és bemutatása:

ASTE_MOD.1.1C A tesztdokumentációnak tartalmaznia kell a teszttterveket, a várt teszteredményeket és a tényleges teszteredményeket.

ASTE_MOD.1.2C A teszttterveknek azonosítaniuk kell a módosítások által kiváltott hatásokat és a tesztelendő biztonsági funkciókat, és le kell írniuk a végrehajtandó tesztek célját.

ASTE_MOD.1.3C A teszttervnek azonosítania kell a módosított részeken végrehajtandó teszteket, és ismertetnie kell minden biztonsági funkcióra a tesztelési forgatókönyveket. A

forgatókönyveknek tartalmazniuk kell a sorrendi függőségeket a megváltoztatott részeknek és az egyéb tesztek eredményeinek a vonatkozásában.

ASTE_MOD.1.4C A rendszer integrátor által végrehajtott tesztekből származó eredményeknek meg kell mutatniuk, hogy minden tesztelt biztonsági funkció a specifikáltaknak megfelelően működik, így a módosítások nincsenek kihatással az SSF-re.

ASTE_MOD.1.5C A tesztdokumentációnak tartalmaznia kell egy vizsgálatot a teszt eljárások sorrendi függőségéről.

ASTE_MOD.1.6C A regressziós tesztelésre vonatkozó vizsgálatnak be kell mutatnia, hogy az SST-ben elvárt, módosítások által érintett funkcionális biztonsági követelmények és a tesztdokumentációban megadott tesztek közötti megfeleltetés teljes.

Értékelői akcióelemek:

ASTE_MOD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

6.2. A rendszer értékelők feladatai informatikai rendszerek biztonsági értékelésénél

6.2.1. Értékelési feladatok a rendszer különböző életciklusában

Egy (működő, szolgáltató) informatikai rendszer értékelése különböző életciklus szakaszok keretében is végrehajtható:

a) a fejlesztés/beszerzés, illetve a megvalósítás/integrálás szakaszán belül hajtandó végre a **rendszer kezdeti értékelése,**
b) az üzemeltetés/karbantartás szakaszában hajtandók végre a felülvizsgálati rendszer értékelések. Ennek két típusa van: a rendszeresen (tipikusan évente) végrehajtandó **tervezett felülvizsgálati értékelés**, illetve a jelentősebb módosításokat követő **rendkívüli felülvizsgálati értékelés**.

A kezdeti és a felülvizsgálati értékeléseknek részben eltérők a feladataik, és ebből következően a módszereik is.

6.2.1.1. Kezdeti rendszer értékelés

A kezdeti rendszer értékelés a rendszer megvalósítási/integrálási szakaszára irányul, de egyes elemei már a fejlesztési/beszerzési szakaszban megkezdhetők. Fő feladatai az alábbiak:

a) A részleges rendszer biztonsági előirányzatban megfogalmazott, a rendszer egészére vonatkozó alapvető biztonsági követelmények alapján a maradványkockázatok előzetes felmérése és összesítése. /Az akkreditorral való egyeztetés után döntés a kockázati szint elfogadásáról, vagy kiegészítő követelmények támasztása./

b) A rendszer biztonsági előirányzat előzetes értékelése. /Meggyőződés arról, hogy nincsenek következetlenségek vagy hiányosságok a biztonsági követelmények és a javasolt intézkedések között, illetve a következetlenségekre és hiányosságokra vonatkozó figyelmeztetés./
c) A rendszer architektúra és terv értékelése. /A különböző tervdokumentációk elemzése, valamint az üzemeltetési helytől független biztonsági intézkedések (például hozzáférés ellenőrzés) ellenőrzése, akár még az üzemeltetési helyen történő telepítés előtt./
d) A rendszer telepítési, konfigurálási és üzemeltetési útmutatóinak a vizsgálata. /A rendszer telepítése és konfigurálása után, a tervezett üzemeltetési környezetben, próba üzemeltetés közben az üzemeltetési helytől függő (műszaki és üzemeltetési) biztonsági intézkedések ellenőrzése./
e) A rendszer biztonsági tesztelése.
f) A rendszer sebezhetőség vizsgálata.

A kezdeti rendszer értékelés eredményei a következők:

a) Értékelési jelentés (a kezdeti rendszer értékelésről). /A kezdeti rendszer értékelés eredményeit összefoglaló értékelési jelentés megállapítja, hogy az SST-ben részletezett követelmények teljesülnek-e, a rendszer elfogadható szinten foglalkozik-e minden olyan kockázattal, amelynek kivédésére biztonsági intézkedés szolgál, s mely felsorolja az értékelés során talált összes azonosított sebezhetőséget, és meghatározza a javasolt kiigazító intézkedéseket./
b) Intézkedési terv. /A intézkedési tervet a rendszer tulajdonosa készíti, a rendszer integrátor támogatásával. Az értékelési jelentésben azonosított sebezhetőségek csökkentésére vagy kiküszöbölésére vonatkozó azon intézkedéseket tartalmazza, melyek bevezetését legkésőbb a következő időszakos rendszer értékelésig vállalják./

6.2.1.2. Felülvizsgálati rendszer értékelés

A felülvizsgálati rendszer értékelés a rendszer üzemeltetési/karbantartási szakaszára irányul. Fő feladatai az alábbiak:

a) A legutolsó (kezdeti vagy felülvizsgálati) rendszer értékelés alapján készített intézkedési terv végrehajtásának ellenőrzése és értékelése.
b) A műszaki és üzemeltetési intézkedések hatékony alkalmazásának ellenőrzése,
c) A rendszer különböző elemeit érintő módosítások (javítások és továbbfejlesztések) történetének és ezek következményeinek a felülvizsgálata.
d) A karbantartott értékelői bizonyítékok megfelelőségének mintavételen alapuló vizsgálata.
e) A rendszer biztonsági tesztelése.
f) A rendszer sebezhetőség vizsgálata (a legutolsó rendszer értékelés óta azonosított sebezhetőségek vizsgálatával a maradványkockázatok feltárása és értékelése).

A felülvizsgálati rendszer értékelés eredményei a következők:

a) Értékelési jelentés (a felülvizsgálati rendszer értékelésről).
b) Intézkedési terv.

6.2.2. Kezdeti rendszer értékelés alap garanciacsomag mellett

6.2.2.1. A rendszer biztonsági előirányzat értékelése (ASST)

6.2.2.1.1. Az SST bevezetés (ASST_INT.1) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_INT.1.1E értékelői akció

ASST_INT.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_INT.1.1C Az SST bevezetésnek tartalmaznia kell egy SST hivatkozást, STOE hivatkozást, STOE áttekintést, STOE leírást és egy tartomány kialakítás specifikációt.

ASST_INT.1-1 Az értékelőnek ellenőriznie kell, hogy az SST bevezetés tartalmaz-e SST hivatkozást, STOE hivatkozást, STOE áttekintést, STOE leírást és egy tartomány kialakítás specifikációt.

ASST_INT.1.2C Az SST hivatkozásnak egyedi módon azonosítania kell az SST-t.

ASST_INT.1-2 Az értékelőnek meg kell vizsgálnia az SST hivatkozást annak megállapítása érdekében, hogy az egyértelműen azonosítja-e az SST-t.

Az értékelő állapítsa meg, hogy az SST hivatkozás azonosítja-e az SST-t magát, úgy, hogy az jól megkülönböztethető legyen más SST-ktől, és egyedi módon azonosítja-e az SST minden verzióját, például verziószámmal és/vagy a közzététel dátumával.

Az értékelő ellenőrizheti a hivatkozások egyediségét a konfiguráció lista ellenőrzésével is.

ASST_INT.1.3C Az STOE hivatkozásnak azonosítania kell az STOE-t.

ASST_INT.1-3 Az értékelőnek meg kell vizsgálnia az STOE hivatkozást annak megállapítása érdekében, hogy az egyértelműen azonosítja-e az STOE-t.

Az értékelő állapítsa meg, hogy az STOE hivatkozás oly módon azonosítja az STOE verzióját, például verzió/kibocsátás vagy a kiadás dátuma segítségével.

ASST_INT.1.4C Az STOE áttekintésnek össze kell foglalnia az STOE használatát és fő biztonsági tulajdonságait.

ASST_INT.1-4 Az értékelőnek meg kell vizsgálnia az STOE áttekintést annak megállapítása érdekében, hogy az leírja-e az STOE használatát és fő biztonsági tulajdonságait.

Az STOE áttekintésnek röviden (néhány bekezdésben) le kell írnia az STOE használatát és fő biztonsági tulajdonságait.

Az értékelő állapítsa meg, hogy az áttekintés érthető-e az olvasók számára.

ASST_INT.1.5C Az STOE áttekintésnek azonosítania kell az STOE típusát.

ASST_INT.1-5 Az értékelőnek ellenőriznie kell, hogy az STOE áttekintés azonosítja-e az STOE típusát.

ASST_INT.1.6C Az STOE leírásnak meg kell adnia az STOE fizikai hatókörét és határait, beleértve a fizikai elemek ábráját.

ASST_INT.1-6 Az értékelőnek meg kell vizsgálnia az STOE leírást annak megállapítása érdekében, hogy az leírja-e az STOE fizikai hatókörét és határait.

Az értékelő állapítsa meg, hogy az STOE leírás felsorolja-e az STOE-t alkotó hardvert, szoftvert, förmvert komponenseket és útmutatókat, valamint olyan részletességgel jellemzi-e ezeket, hogy az olvasó általános képet kapjon ezekről.

Az értékelő állapítsa meg azt is, hogy nincs lehetséges félreértés a tekintetben, hogy valamely hardver, szoftver, förmver vagy útmutató elem része-e az STOE-nak vagy sem.

ASST_INT.1-7 Az értékelőnek ellenőriznie kell az STOE leírást annak megállapítása érdekében, hogy az tartalmaz-e egy áttekintő ábrát a fizikai elemekről.

ASST_INT.1.7C Az STOE leírásnak meg kell adnia az STOE logikai hatókörét és határait, beleértve a logikai elemek ábráját.

ASST_INT.1-8 Az értékelőnek meg kell vizsgálnia az STOE leírást annak megállapítása érdekében, hogy az leírja-e az STOE logikai hatókörét és határait.

Az értékelő állapítsa meg, hogy az STOE leírás olyan részletességgel tárgyalja-e az STOE által nyújtott logikai biztonsági szolgáltatásokat, hogy az olvasó általános képet kapjon ezekről.

Az értékelő állapítsa meg azt is, hogy nincs lehetséges félreértés a tekintetben, hogy valamely logikai biztonsági szolgáltatást biztosít-e az STOE vagy sem.

ASST_INT.1-9 Az értékelőnek ellenőriznie kell az STOE leírást annak megállapítása érdekében, hogy az tartalmaz-e egy áttekintő ábrát a logikai elemekről.

ASST_INT.1.8C Az STOE leírásnak azonosítania kell az STOE által igényelt bármilyen külső működő rendszerhez való kapcsolódást és felületet (interfészt).

ASST_INT.1-10 Az értékelőnek meg kell vizsgálnia az STOE leírást annak megállapítása érdekében, hogy az azonosítja-e az STOE által igényelt bármilyen külső működő rendszerhez való kapcsolódást és felületet (interfészt).

ASST_INT.1.9C A tartomány kialakítás specifikációnak meg kell határoznia a létrehozott biztonsági tartományok kialakítását, szervezését, az egyes tartományok azonosítási információit.

ASST_INT.1-11 Az értékelőnek meg kell vizsgálnia a tartomány kialakítás specifikációt annak megállapítása érdekében, hogy az meghatározza-e létrehozott biztonsági tartományok kialakítását, szervezését, az egyes tartományok azonosítási információit.

Az ASST_INT.2.2E értékelői akció

ASST_INT.1.2E Az értékelőnek meg kell erősítenie, hogy az STOE hivatkozás, STOE áttekintés, STOE leírás és tartomány kialakítás specifikáció összhangban áll egymással.

ASST_INT.1-12 Az értékelőnek meg kell vizsgálnia, hogy az STOE hivatkozás, STOE áttekintés, STOE leírás és tartomány kialakítás specifikáció összhangban áll egymással.

6.2.2.1.2. A megfelelőség nyilatkozatok (ASST_CCL.1) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_CCL.1.1E értékelői akció

ASST_CCL.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_CCL.1.1C A megfelelőségi nyilatkozatnak azonosítania kell azt a mértékadó dokumentumot, amelyhez az SST és az STOE megfelelőséget állít.

ASST_CCL.1-1 Az értékelőnek ellenőriznie kell a megfelelőségi nyilatkozatot, hogy az azonosítja-e azt a mértékadó dokumentumot, amelyhez az SST és az STOE megfelelőséget állít.

ASST_CCL.1.2C A megfelelőségi nyilatkozatnak azonosítania kell a mértékadó dokumentum azon követelményeit, amelyekhez az SST és az STOE megfelelőséget állít.

ASST_CCL.1-2 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozatot, hogy az azonosítja-e a mértékadó dokumentum azon követelményeit, amelyekhez az SST és az STOE megfelelőséget állít.

6.2.2.1.3. A biztonsági célok (ASST_OBJ.1) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:
a) SST.

Az ASST_OBJ.1.1E értékelői akció

ASST_OBJ.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_OBJ.1.1C A biztonsági célokról szóló nyilatkozatnak le kell írnia az STOE üzemeltetési környezetre vonatkozó biztonsági célokat.

ASST_OBJ.1-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági célokról szóló nyilatkozat megadja-e az STOE üzemeltetési környezetre vonatkozó biztonsági célokat.

Az értékelő ellenőrizze, hogy az STOE üzemeltetési környezetre vonatkozó biztonsági célokat azonosították-e.

6.2.2.1.4. A biztonsági követelmények (ASST_REQ.1) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:
a) SST.

Az ASST_REQ.1.1E értékelői akció

ASST_REQ.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_REQ.1.1C A biztonsági követelményekre vonatkozó állításnak le kell írnia a rendszertől elvárt biztonsági funkcionalitást (SSF) és garanciákat (SAP).

ASST_REQ.1-1 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot annak megállapítása érdekében, hogy az leírja-e az elvárt rendszer biztonsági funkcionalitást (SSF).

ASST_REQ.1-2 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot annak megállapítása érdekében, hogy az leírja-e az elvárt garanciákat (SAP).

ASST_REQ.1.2C Az elvárt rendszer biztonsági funkcionalitást az alábbi mértékadó dokumentumokból kell választani: hazai vagy nemzetközi szabvány, nyilvános műszaki követelményrendszer, követelményeket megfogalmazó hazai jogszabály.

ASST_REQ.1-3 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot, hogy az abban azonosított mértékadó dokumentum az alábbiak egyike-e: hazai

vagy nemzetközi szabvány, nyilvános műszaki követelményrendszer, követelményeket megfogalmazó hazai jogszabály.

ASST_REQ.1.3C Az elvárt rendszer garanciacsomagnak az alábbiak egyikének kell lennie: SAP-A vagy megemelt SAP-A.

ASST_REQ.1-4 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot, hogy az abban azonosított garanciacsomag az alábbiak egyike-e: SAP-A vagy megemelt SAP-A.

Az ASST_REQ.1.2E értékelői akció

ASST_REQ.1.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági követelményekről szóló nyilatkozat belső ellentmondásoktól mentes.

ASST_REQ.1-5 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy az belső ellentmondásoktól mentes.

Az értékelő állapítsa meg, hogy az SSF és SAP kombinációja belső ellentmondásoktól mentes.

Néhány lehetséges ellentmondás:

SSF egyetlen mértékadó dokumentumokból került kiválasztásra, de a kiválasztott SFR-ek ellentmondanak egymásnak;

SSF több mértékadó dokumentumokból került kiválasztásra és a kiválasztott SFR-ek ellentmondanak egymásnak.

6.2.2.1.5. Az STOE összefoglaló előírás (ASST_SSS.1) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_SSS.1.1E értékelői akció

ASST_SSS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SSS.1.1C Az STOE összefoglaló előírásnak le kell írnia, hogy az STOE hogyan teljesíti az egyes funkcionális biztonsági követelményeket (SFR).

ASST_SSS.1-1 Az értékelőnek meg kell vizsgálnia az STOE összefoglaló előírást annak megállapítása érdekében, hogy az leírja-e, hogy az STOE hogyan teljesíti az egyes SFR-eket.

Az értékelő állapítsa meg, hogy az STOE összefoglaló előírás a biztonsági követelményekről szóló nyilatkozatban szereplő minden SFR-re megadja annak leírását, hogyan teljesül az SFR.

Az értékelő tartsa szem előtt, hogy az egyes leírások célja magas szintű áttekintés nyújtása az olvasók számára arról, hogy a rendszer integrátor hogyan szándékozik kielégíteni az SFR-eket, ezért a leírásnak nem kell túlzottan részletesnek lennie.

Az ASST_SSS.1.2E értékelői akció

ASST_SSS.1.2E Az értékelőnek meg kell erősítenie, hogy az STOE összefoglaló előírás nem mond ellent az STOE áttekintésnek és az STOE leírásnak.

ASST_SSS.1-2 Az értékelőnek meg kell vizsgálnia az STOE összefoglaló előírást annak megállapítása érdekében, hogy az összhangban áll-e az STOE áttekintéssel és az STOE leírással.

Az STOE áttekintés, az STOE leírás és az STOE összefoglaló előírás egyaránt elbeszélő formában leírja az STOE-t, de a részletezettség növekvő szintjén. Ezért ezeknek a leírásoknak összhangban kell lenniük.

6.2.2.1.6. A biztonsági tartomány bevezetés (ASST_SDI.1) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_SDI.1.1E értékelői akció

ASST_SDI.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDI.1.1C A biztonsági tartomány bevezetésnek tartalmaznia kell egy biztonsági tartomány hivatkozást, biztonsági tartomány áttekintést és egy biztonsági tartomány leírást.

ASST_SDI.1-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány bevezetés tartalmaz-e egy biztonsági tartomány hivatkozást, egy biztonsági tartomány áttekintést és egy biztonsági tartomány leírást.

ASST_SDI.1.2C A biztonsági tartomány hivatkozásnak egyedi módon azonosítania kell a biztonsági tartományt.

ASST_SDI.1-2 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány hivatkozás azonosítja-e a biztonsági tartományt.

ASST_SDI.1.3C A biztonsági tartomány áttekintésnek össze kell foglalnia a biztonsági tartomány használatát és fő biztonsági tulajdonságait.

ASST_SDI.1-3 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány áttekintés összefoglalja-e a biztonsági tartomány használatát és fő biztonsági tulajdonságait.

ASST_SDI.1.4C A biztonsági tartomány leírásnak jellemeznie kell alrendszereit és komponenseit.

ASST_SDI.1-4 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány leírás jellemezi-e az adott biztonsági tartomány alrendszereit és komponenseit.

ASST_SDI.1.5C A biztonsági tartomány leírásnak le kell írnia a más tartományokkal való kapcsolódásokat és interfészeket.

ASST_SDI.1-5 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány leírás leírja-e a más tartományokkal való kapcsolódásokat és interfészeket.

Az ASST_SDI.1.2E értékelői akció

ASST_SDI.1.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági tartomány hivatkozás, a biztonsági tartomány áttekintés és a biztonsági tartomány leírás nem mond ellent egymásnak és az SST bevezetésnek.

ASST_SDI.1-6 Az értékelőnek meg kell vizsgálnia, hogy a biztonsági tartomány hivatkozás, a biztonsági tartomány áttekintés és a biztonsági tartomány leírás összhangban áll egymással.

6.2.2.1.7. A biztonsági tartomány megfelelőségi nyilatkozatok (ASST_SDC.1) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_SDC.1.1E értékelői akció

ASST_SDC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDC.1.1C A biztonsági tartomány megfelelőségi nyilatkozatnak azonosítania kell azt a mértékadó dokumentumot, amelyhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.1-1 Az értékelőnek ellenőriznie kell a biztonsági tartomány megfelelőségi nyilatkozatot, hogy az azonosítja-e azt a mértékadó dokumentumot, amelyhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.1.2C A biztonsági tartomány megfelelőségi nyilatkozatnak azonosítania kell a mértékadó dokumentum azon követelményeit, amelyekhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.1-2 Az értékelőnek ellenőriznie kell a biztonsági tartomány megfelelőségi nyilatkozatot, hogy az azonosítja-e a mértékadó dokumentum azon követelményeit, amelyekhez a biztonsági tartomány megfelelőséget állít.

6.2.2.1.8. A biztonsági tartomány biztonsági célok az üzemeltetési környezetre (ASST_SDO.1) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_SDO.1.1E értékelői akció

ASST_SDO.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDO.1.1C A biztonsági tartomány biztonsági céljairól szóló nyilatkozatnak le kell írnia a biztonsági tartomány üzemeltetési környezetére vonatkozó biztonsági célokat.

ASST_SDO.1-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány biztonsági célokról szóló nyilatkozat megadja-e a biztonsági tartomány üzemeltetési környezetre vonatkozó biztonsági célokat.

6.2.2.1.9. Biztonsági tartományra kinyilvánított követelmények (ASST_SDR.1) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_SDR.1.1E értékelői akció

ASST_SDR.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDR.1.1C A biztonsági tartomány biztonsági követelményekre vonatkozó állításnak le kell írnia az adott biztonsági tartományra elvárt biztonsági funkcionalitást (SF) és az elvárt rendszer garanciákat (SAP).

ASST_SDR.1-1 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot annak megállapítása érdekében, hogy az leírja-e az adott biztonsági tartományra elvárt biztonsági funkcionalitást (SF).

ASST_SDR.1-2 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot annak megállapítása érdekében, hogy az leírja-e az elvárt garanciákat (SAP).

ASST_SDR.1.2C Az elvárt biztonsági funkcionalitást az alábbi mértékadó dokumentumból kell választani: hazai vagy nemzetközi szabvány, nyilvános műszaki követelményrendszer, követelményeket megfogalmazó hazai jogszabály.

ASST_SDR.1-3 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, hogy az abban azonosított mértékadó dokumentum az alábbi-e: hazai vagy nemzetközi szabvány, nyilvános műszaki követelményrendszer, követelményeket megfogalmazó hazai jogszabály.

ASST_SDR.1.3C Az elvárt rendszer garanciacsomagnak az alábbiak egyikének kell lennie: SAP-A vagy megemelt SAP-A.

ASST_SDR.1-4 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, hogy az abban azonosított garanciacsomag az alábbiak egyike-e: SAP-A vagy megemelt SAP-A.

Az ASST_SDR.1.2E értékelői akció

ASST_SDR.1.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági tartomány biztonsági követelményekről szóló nyilatkozat belső ellentmondásoktól mentes.

ASST_SDR.1-5 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy az belső ellentmondásoktól mentes.

6.2.2.1.10. A biztonsági tartomány összefoglaló előírás (ASST_SDS.1) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_SDS.1.1E értékelői akció

ASST_SDS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDS.1.1C A biztonsági tartományra vonatkozó összefoglaló előírásnak le kell írnia, hogy a biztonsági tartomány hogyan teljesíti az egyes funkcionális biztonsági követelményeket (SFR).

ASST_SDS.1-1 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány összefoglaló előírást annak megállapítása érdekében, hogy az leírja-e, hogy a biztonsági tartomány hogyan teljesíti az egyes SFR-eket.

Az értékelő állapítsa meg, hogy a biztonsági tartomány összefoglaló előírás a biztonsági követelményekről szóló nyilatkozatban szereplő minden SFR-re megadja annak leírását, hogyan teljesül az SFR.

Az értékelő tartsa szem előtt, hogy az egyes leírások célja magas szintű áttekintés nyújtása az olvasók számára arról, hogy a rendszer integrátor hogyan szándékozik kielégíteni az SFR-eket, ezért a leírásnak nem kell túlzottan részletesnek lennie.

Az ASST_SDS.1.2E értékelői akció

ASST_SDS.1.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági tartományra vonatkozó összefoglaló előírás nem mond ellent a biztonsági tartomány áttekintésnek és a biztonsági tartomány leírásnak.

ASST_SDS.1-2 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány összefoglaló előírást annak megállapítása érdekében, hogy az összhangban áll-e a biztonsági tartomány áttekintéssel és a biztonsági tartomány leírással.

A biztonsági tartomány áttekintés, a biztonsági tartomány leírás és a biztonsági tartomány összefoglaló előírás egyaránt elbeszélő formában leírja a biztonsági tartományt, de a részletezettség növekvő szintjén. Ezért ezeknek a leírásoknak összhangban kell lenniük.

6.2.2.2. A rendszer fejlesztés garanciaosztály (ASDV) értékelése

6.2.2.2.1. Rendszer biztonsági architektúra: ASDV_ARC.1 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) rendszer interfész specifikáció,
c) STOE terv,
d) biztonsági architektúra leírás,
e) üzemeltetési útmutató.

Az ASDV_ARC.1.1E értékelői akció

ASDV_ARC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_ARC.1.1C A biztonsági architektúra leírásnak ismertetnie kell az STOE-hez kapcsolódó külső informatikai rendszereket, egymáshoz kapcsolódásukat, valamint a köztük folyó információáramlást.

ASDV_ARC.1-1 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az ismerteti-e az STOE-hez kapcsolódó külső informatikai rendszereket.

ASDV_ARC.1-2 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az ismerteti-e az STOE és az azonosított külső informatikai rendszerek egymáshoz kapcsolódási módját.

ASDV_ARC.1-3 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az ismerteti-e az STOE és az azonosított külső informatikai rendszerek közötti információáramlást.

ASDV_ARC.1.2C A biztonsági architektúra leírásnak ismertetnie kell az STOE biztonsági funkcionalitás szerkezetét, olyan részletességgel, amely összemérhető a rendszer interfész specifikáció és az STOE terv részletességével.

ASDV_ARC.1-4 Az értékelőnek meg kell vizsgálnia a biztonsági szerkezet leírást annak megállapítása érdekében, hogy az ebben biztosított információk részletessége összemérhető-e a rendszer interfész specifikáció és az STOE terv dokumentáció részletességével.

Az értékelő győződjön meg arról, hogy a rendszer interfész specifikáció ismerteti-e azokat az önvédelmi funkciókat, amelyek nyilvánvalóak az STOE külső interfészén.

Az értékelő győződjön meg arról, hogy az STOE külső interfészén keresztül aktivizálható funkcionalitást leírták.

Az értékelő győződjön meg arról, hogy a biztonsági architektúra leírása tartalmaz-e információt a rendszer biztonsági funkcionalitás (SSF) tartomány elkülönítéséről.

Az ehhez a munkaegységhez kapcsolódó értékelői akció kapjon „nem felelt meg” határozatot, ha a biztonsági architektúra leírás megemlít bármilyen olyan modult, komponenst, alrendszert vagy interfészt, amelyet a rendszer interfész specifikáció vagy az STOE terv dokumentum nem ismertet.

ASDV_ARC.1.3C A biztonsági architektúra leírásnak szemléltetnie kell, hogy az STOE meggátolja a funkcionális biztonsági követelményeket érvényre juttató funkcionalitás megkerülését.

ASDV_ARC.1-5 Az értékelőnek meg kell vizsgálnia a biztonsági architektúra leírást annak megállapítása érdekében, hogy az megfelelő módon ismerteti-e, hogy a funkcionális biztonsági követelményeket érvényre juttató mechanizmusokat milyen mértékben nem lehet megkerülni.

A nem-megkerülhetőség egy olyan tulajdonság, hogy az SSF mindig aktivizálódik. Például, ha a fájlokhoz való hozzáférés az SSF-nek egy funkcionális biztonsági követelményen keresztül specifikált tulajdonsága, akkor nem szabad előfordulnia olyan interfésznek, amin keresztül a fájlokhoz hozzá lehet férni az SSF hozzáférés ellenőrzési mechanizmusa aktivizálása nélkül (vagyis nem szabad előfordulnia például olyan interfésznek, amelyen keresztül közvetlenül hozzá lehet férni egy diszkhez vagy egy adatbázishoz).

Annak leírása, hogy az SSF mechanizmusokat miért nem lehet megkerülni, általában módszeres indoklást igényel. A TSF működésének leírása (amit a rendszer interfész specifikáció és az STOE terv tartalmaz) biztosítja a szükséges hátteret ahhoz, hogy az értékelő megértse, hogy mely erőforrásokat kell védeni, és milyen biztonsági funkciókat kell biztosítani. A rendszer interfész specifikáció adja meg a külső interfészek ismertetését, amelyeken keresztül az erőforrások/funkciók hozzáférhetők.

Az értékelő becsülje fel az átadott leírásokat, és győződjön meg arról, hogy nem áll rendelkezésre az SSF megkerülésére használható interfész.

A megkerülésre egy példa, amikor az SSF által védett adatokhoz egy támadó úgy fér hozzá, hogy kihasználja azokat a (tiltás ellenére létrehozott) közvetlen internetre csatlakozásokat, melyek kikerülik a tűzfal és behatolás észlelő eszközök által ellenőrzött külső interfészeket. Az ilyen esetleges közvetlen internetre csatlakozások feltárása az értékelő gyakorlati sebezhetőség elemzésének és behatolás tesztelésének egyik fontos célja.

A megkerülésre egy másik példa amikor egy felhasználó egy másik felhasználóra vonatkozó információt nyerhet egy válasz vagy egy memória nem törölt részeiből (a maradvány információ védelmének hiányában ekkor a hozzáférés védelem megkerülhető).

Az értékelő győződjön meg arról is, hogy a leírás átfogó, amelyben minden biztonsággal kapcsolatos interfészt megvizsgálnak. Ez megkívánhatja az értékelőtől, hogy egyéb értékelési bizonyítékokat is figyelembe vegyen ehhez.

ASDV_ARC.1.4C A biztonsági architektúra leírásnak szemléltetnie kell, hogy a rendszer biztonsági funkcionalitás megvédi magát a hamisítással szemben.

ASDV_ARC.1-6 Az értékelőnek meg kell vizsgálnia a biztonsági architektúra leírást annak megállapítása érdekében, hogy az kellő információt biztosít annak megállapításához, hogy az SSF képes megvédi magát a nem-megbízható aktív egyedek hamisításával szemben.

Az „önvédelem” az SSF-nek arra a képességére utal, hogy meg tudja védeni saját magát a külső egyedek olyan manipulációival szemben, amelyek az SSF megváltoztatásaihoz vezethetnek. A külső informatikai rendszerektől függő STOE-k esetében gyakran előfordul, hogy az STOE olyan szolgáltatást használ fel funkciói végrehajtásához, amelyeket más informatikai rendszerek szolgáltatnak. Az ilyen esetekben az SSF önmagában nem tudja megvédeni saját magát, mivel más informatikai rendszerektől függ az, hogy valamilyen védelmet tud biztosítani. A biztonsági architektúra leírás szempontjából az önvédelem elve csak azokra a szolgáltatásokra vonatkozik, amelyeket az SSF nyújt a saját külső interfészén keresztül, és nem vonatkozik azokra a szolgáltatásokra, amelyeket az általa használt informatikai rendszerek szolgáltatnak.

Az önvédelem általában számos eszközzel elérhető, az STOE-hoz való hozzáférés fizikai és logikai korlátozásától kezdődően a hardver-alapú (pl. memóriakezelési funkcionalitás) és szoftver-alapú (pl. bemenetek korlát-érték ellenőrzései egy megbízható szerveren) eszközökig. Az értékelő állapítsa meg, hogy minden ilyen mechanizmust ismertettek.

Az értékelő állapítsa meg, hogy a leírás foglakozik-e azzal, hogy az SSF hogyan kezeli a felhasználói bemeneteket abból a szempontból, hogy az ne ronthassa le az SSF-et.

A tartomány elválasztási funkciókhoz hozzájáruló összes mechanizmust le kell írni. Az értékelő a más értékelési bizonyítékokból szerzett ismereteit használja fel annak megállapításához, hogy nincs olyan önvédelemhez hozzájáruló funkcionalitás, melyet a biztonsági architektúra leírás nem ismertet.

Az önvédelmi mechanizmusok leírásának helyessége az a tulajdonság, hogy a leírás hitelt érdemlően ismerteti, hogy mit valósítottak meg. Az értékelő használjon fel egyéb bizonyítékokat annak megállapításához, hogy az önvédelmi mechanizmus leírásai nem

mondanak ellent egymásnak. Ha egy értékelő nem látja át, hogy egy meghatározott önvédelmi mechanizmus hogyan működik a rendszer architektúrában, akkor ez a leírás nem megfelelőségére utalhat.

6.2.2.2.2. A rendszer interfész specifikáció: ASDV_SIS.1 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) rendszer interfész specifikáció,
c) STOE terv.
d) biztonsági architektúra leírás,
e) üzemeltetési útmutató.

Az ASDV_SIS.1.1E értékelői akció

ASDV_SIS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_SIS.1.1C A rendszer interfész specifikációnak informális stílusban le kell írnia az STOE biztonsági funkcionalitását (SSF) és annak külső interfészeit.

ASDV_SIS.1-1 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy az tartalmazza-e az összes szükséges informális magyarázatot. Amennyiben az egész rendszer interfész specifikáció informális, akkor ez a munkaegység nem alkalmazható, következésképp teljesítettnek tekinthető.

A rendszer interfész specifikáció olyan részeihez, melyeket nehéz megérteni csak félformális vagy formális leírásokból, kiegészítésként szükség van magyarázó leírásra is (pl. a formális jelölésrendszer jelentésének megvilágításához).

ASDV_SIS.1.2C A rendszer interfész specifikációnak belső ellentmondásoktól mentesnek kell lennie.

ASDV_SIS.1-2 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy az belső ellentmondásoktól mentes-e.

Az értékelőnek meg kell erősítenie, hogy a rendszer interfész specifikációban az interfészek leírása összhangban áll az SSF funkciók leírásával.

ASDV_SIS.1.3C A rendszer interfész specifikációnak le kell írnia minden külső TSF interfész használatának célját és módját, részletezve a hatásokat, kivételeket és hibaüzeneteket.

ASDV_SIS.1-3 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy az azonosít-e minden külső TSF interfészt.

A "külső" jelző a felhasználó által látottakat jelenti.

ASDV_SIS.1-4 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy leírták-e benne az összes külső TSF interfészt.

ASDV_SIS.1-5 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy az megfelelően és helyesen írja-e le az STOE viselkedését minden külső interfészre a hatások, kivételek és hibaüzenetek tekintetében.

Egy interfész bemutatás megfelelőségének és helyességének vizsgálatát az értékelő a rendszer interfész specifikáció, az SST-ben található STOE összefoglaló előírás, valamint az üzemeltetési útmutató alapján végzi, a következő tényezők értékelése érdekében:

a) Minden biztonsági szempontból fontos bemenő paramétert (vagy az ilyen paraméterek jellemzőit) azonosítani kell.
b) Az útmutatóban leírt biztonsági szempontból fontos teljes működést szerepeltetni kell a rendszer interfész specifikációban. Ennek meg kell határoznia a működést az események és azok hatásának tükrében.
c) Minden interfészt minden lehetséges üzemmódra le kell írni.
d) A biztonsági szempontból fontos paraméterekre és az interfész szintaxis leírására vonatkozó információknak ellentmondás menteseknek kell lenniük a teljes dokumentációban.

A fenti ellenőrzés a rendszer interfész specifikáció és az STOE összefoglaló előírás átvizsgálásával, valamint az üzemeltetési útmutató segítségével történik.

Ez a vizsgálat iteratív is lehet, hiszen az értékelő nem biztos, hogy felfedezi a rendszer interfész specifikáció hiányosságait a tervek vagy egyéb értékelési bizonyítékok vizsgálata nélkül, mely alapján találhat olyan paramétereket vagy hibaüzeneteket, amelyek kimaradtak a rendszer interfész specifikációból.

ASDV_SIS.1.4C A rendszer interfész specifikációnak teljes mértékben be kell mutatnia az SSF-et.

ASDV_SIS.1-6 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt, annak megállapítása érdekében, hogy az SSF-t teljes mértékben bemutatják-e benne.

Az TSF bemutatás teljességét az értékelő az STOE összefoglaló előírás és az üzemeltetési útmutató alapján mérje fel. Ezek egyike sem írhat le olyan biztonsági funkciót, amely hiányzik a rendszer interfész specifikáció TSF bemutatásából.

Az ASDV_SIS.1.2E értékelői akció

ASDV_SIS.1.2E Az értékelőnek meg kell állapítania, hogy a rendszer interfész specifikáció az STOE funkcionális biztonsági követelményeinek pontos és teljes megjelenítése.

ASDV_SIS.1-7 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy az az STOE funkcionális biztonsági követelményeinek teljes megvalósulása-e.

ASDV_SIS.1-8 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy az az STOE funkcionális biztonsági követelményeinek pontos megvalósulása-e.

6.2.2.2.3. Rendszer biztonsági terv: ASDV_SDS.1 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) rendszer interfész specifikáció,
c) biztonsági architektúra leírás,
d) rendszer biztonsági terv (STOE terv).

Az ASDV_SDS.1.1E értékelői akció

ASDV_SDS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_SDS.1.1C Az STOE tervnek le kell írnia az STOE szerkezetét alrendszerek szerint.

ASDV_SDS.1-1 Az értékelőnek meg kell vizsgálnia az STOE tervet annak megállapítása érdekében, hogy az STOE teljes szerkezetét leírták-e alrendszerek szerint.

Az értékelő győződjön meg arról, hogy az STOE minden alrendszerét azonosították. Ez a követelmény a teljes STOE-ra vonatkozik, nem csak az SSF-re.

Az értékelő vizsgáljon meg az STOE-hoz átadott egyéb értékelési bizonyítékot is (pl. SST, üzemeltetési útmutató) annak megállapítása érdekében, hogy az STOE leírása ezekben a bizonyítékokban összhangban áll-e az STOE tervben leírtakkal.

ASDV_SDS.1.2C Az STOE tervnek azonosítania kell az SSF minden alrendszerét.

ASDV_SDS.1-2 Az értékelőnek meg kell vizsgálnia az STOE tervet annak megállapítása érdekében, hogy az az SSF minden alrendszerét azonosítja-e.

ASDV_SDS.1.3C Az STOE tervnek leírást kell biztosítania az SSF összes alrendszeréről.

ASDV_SDS.1-3 Az értékelőnek meg kell vizsgálnia az STOE tervet annak megállapítása érdekében, hogy az SSF minden alrendszerére leírja-e azt a szerepet, amelyet az SST-ben ismertetett SFR-ek érvényre juttatásában tölt be.

Az alrendszer szintű leírásnak az a célja, hogy megadja az értékelő számára követhető, komponens szintű leírásra vonatkozó összefüggéseket. Ezért az értékelő győződjön meg arról, hogy az alrendszer szintű leírás tartalmaz-e ismertetést arról, hogy a funkcionális biztonsági követelmények hogyan valósulnak meg a tervben, de a komponens leírásnál magasabb absztrakciós szinten. Az alrendszerek leírása útmutatást ad az értékelőnek annak megállapításához, hogy mely komponenseket kell alaposabban megvizsgálni.

Az értékelő győződjön meg arról, hogy az SSF minden alrendszerét leírták. Bár a leírásnak arra a szerepre kell koncentrálnia, amelyet az alrendszer az SFR-ek megvalósításának érvényre juttatásában vagy támogatásában tölt be, ahhoz elegendő információt kell bemutatni, hogy az SFR-vonzatú funkcionalitás megértéséhez szükséges összefüggések biztosítva legyenek.

ASDV_SDS.1.4C Az STOE tervnek le kell írnia az SSF összes alrendszere közötti kapcsolatokat.

ASDV_SDS.1-4 Az értékelőnek meg kell vizsgálnia az STOE tervet annak megállapítása érdekében, hogy az SSF alrendszerei közötti kölcsönhatásokat leírja-e.

Az alrendszerek közötti kölcsönhatások leírásának az a célja, hogy segítse az olvasót annak jobb megértésében, hogy az SSF hogyan hajtja végre a funkcióit. Ezeket a kölcsönhatásokat nem szükséges megvalósítási szinten jellemezni (pl. egy alrendszer valamelyik rutinjából paramétereknek az átadása egy másik alrendszerhez tartozó rutin számára; globális változók; hardver jelzések (pl. megszakítások) az egyik hardver alrendszertől egy megszakítás-kezelő alrendszer felé), de fedje le azokat az adatelemeket, amelyeket egy alrendszer egy másik alrendszerben való felhasználásra szánt. Az alrendszerek közötti minden felügyeleti kapcsolatot is ismertetni kell (pl. az egyik alrendszer felelős egy tűzfal rendszer szabályainak konfigurálásáért, a másik alrendszer pedig megvalósítja ezeket a szabályokat).

Meg kell jegyezni, hogy bár a fejlesztőnek jellemeznie kell az alrendszerek közötti összes kölcsönhatást, az értékelőnek magának kell megítélnie a leírás teljességét. Ha egy kölcsönhatás oka nem világos, vagy ha vannak olyan SFR-vonzatú kölcsönhatások (például a komponens szintű dokumentáció vizsgálata közben felfedezve), amelyekről úgy tűnik, hogy nincsenek ismertetve, az értékelő gondoskodjon arról, hogy ezt az információt a rendszer integrátor átadja. Ha azonban az értékelő azt állapítja meg, hogy bizonyos alrendszerek közötti kölcsönhatásokat ugyan nem ismertetett teljes mértékben a rendszer integrátor, de a teljes leírás nem járulna hozzá sem az általános funkcionalitás, sem az SSF által nyújtott biztonsági funkcionalitás megértéséhez, akkor az értékelő dönthet úgy, hogy a leírást elegendőnek tekinti, és nem kívánja meg a teljességet csak önmagáért.

ASDV_SDS.1.5C Az STOE tervnek le kell írnia az SSF-et komponensek szerint.

ASDV_SDS.1-2 Az értékelőnek meg kell vizsgálnia az STOE tervet annak megállapítása érdekében, hogy a teljes SSF-t leírták-e komponensek szerint.

A komponensek a rendszert alkotó termékek.

Az értékelő a komponenseket a speciális tulajdonságok szempontjából más munkaegységekben fogja megvizsgálni; ebben a munkaegységben az értékelő azt állapítsa meg, hogy a komponens szintű leírás lefedi-e a teljes SSF-et, és nem csak az SSF-nek egy részét. Az értékelő ehhez a megállapításhoz használja fel az értékeléshez átadott egyéb bizonyítékokat is (pl. rendszer interfész specifikáció, biztonsági architektúra leírás). Például, ha a rendszer interfész specifikáció tartalmaz a funkcionalitáshoz csatlakozó olyan interfészt, amelyről úgy tűnik, hogy nincsen ismertetve az STOE tervben, akkor lehet, hogy ez egy olyan eset, amikor az SSF egy része nincs megfelelő módon csatolva. Az érintett megállapítás

feltehetően iteratív eljárással hozható meg, amelynek során minél több vizsgálatot végeznek el a többi bizonyítékokon, annál nagyobb bizonyosság szerezhető a dokumentáció teljességét illetően.

ASDV_SDS.1.6C Az STOE tervnek egy leképezést kell biztosítania az SSF alrendszerei és az SSF komponensei között.

ASDV_SDS.1-6 Az értékelőnek meg kell vizsgálnia az STOE tervet annak megállapítása érdekében, hogy az SSF alrendszerei és komponensei közötti megfeleltetés teljes-e.

Az SSF alrendszerei és komponensei közötti megfeleltetés megmutatja, hogy az SSF komponensei hogyan lettek kiosztva az alrendszerek között. Ez útmutatóként fog szolgálni az értékelő számára a komponens szintű kiértékelésnél. A teljesség megállapítása érdekében az értékelő vizsgáljon át minden megfeleltetést, és állapítsa meg, hogy minden alrendszerhez hozzá van-e rendelve legalább egy komponens, és hogy minden komponens pontosan egy alrendszerhez van-e hozzárendelve.

ASDV_SDS.1-7 Az értékelőnek meg kell vizsgálnia az STOE tervet annak megállapítása érdekében, hogy az SSF alrendszerei és komponensei közötti megfeleltetés helyes-e.

Az SSF alrendszerei és komponensei közötti megfeleltetés megmutatja, hogy az SSF komponensei hogyan lettek kiosztva az alrendszerek között. Ez útmutatóként fog szolgálni az értékelő számára a komponens szintű kiértékelésnél. Az értékelő választhatja azt a megoldást is, hogy a megfeleltetés helyességét más munkaegységek végrehajtásával együtt ellenőrzi. „Nem-helyes” egy megfeleltetés, ha a komponens tévesen van hozzárendelve egy alrendszerhez, ahol az alrendszeren belül nem használják a funkcióit. Minthogy a megfeleltetés azt a célt szolgálja, hogy útmutatásként szolgáljon a részletesebb vizsgálatok támogatására, az értékelőnek csak a megfelelő erőfeszítést ajánlott erre a munkaegységre fordítania. A megfeleltetés helyességét ellenőrző széleskörű értékelői erőforrások ráfordítása nem szükséges. Az itt vagy más munkaegységek során feltárt, félreértésre vezető pontatlanságokat kell ehhez a munkaegységhez rendelni és kijavíttatni.

ASDV_SDS.1.7C Az STOE tervnek le kell írnia az összes SFR-t érvényre juttató komponenst, megadva céljukat és a többi komponenssel való kapcsolatukat.

ASDV_SDS.1-8 Az értékelőnek meg kell vizsgálnia az STOE tervet annak megállapítása érdekében, hogy minden SFR-t érvényre juttató komponens céljának a leírása teljes és helyes-e.

Az integrátor megjelölheti a komponenseket SFR-t érvényre juttatóként, SFR-t támogatóként, és SFR-be nem beavatkozóként, bár ezek a „megjelölések” csak annak jelzésére szolgálnak, hogy az integrátor milyen mennyiségű és típusú információt kell szolgáltatnia, és felhasználható azon információ mennyiségének korlátozására, amelyet az integrátornak kell kidolgoznia, ha az előkészítési munkálatok nem állítják elő a megkívánt dokumentációt. Akár kategorizálta a komponenseket az integrátor, akár nem, az értékelő felelőssége annak megállapítása, hogy a komponensek rendelkeznek-e megfelelő információval az STOE-beli szerepüket illetően (SFR-t érvényre juttató, stb.), és a megfelelő információ megszerzése az

integrátortól, ha az elmulasztotta biztosítani a megkívánt információt egy meghatározott komponens esetében.

A komponens célja azt mutatja meg, hogy a komponens melyik funkciót elégíti ki. E munkaegység fő célja, hogy áttekintést nyújtson az értékelőnek a komponens működésmódjáról, annak érdekében, hogy megállapításokat tehessen az SFR-ek megvalósításának megbízhatóságáról. Az ASDV_ARC összetevő kapcsán végrehajtott szerkezeti vizsgálat támogatása is cél. Ha az értékelő teljesen átlátja a komponens működését és annak kapcsolatait az összes többi komponenssel, valamint az STOE-val, mint egésszel, a munkaegység célját teljesítettnek tekintheti, és ne terhelje az integrátort dokumentálási feladatokkal (megkövetelve, például, egy teljes algoritmust egy önmagában is nyilvánvaló megvalósítási reprezentációhoz).

ASDV_SDS.1.8C Az STOE tervnek le kell írnia az összes SFR-t érvényre juttató komponenst, megadva SFR vonatkozású interfészeiket, ezen interfészek visszatérési értékeit, valamint a többi komponenssel való kapcsolatukat és meghívott interfészeket.

ASDV_SDS.1-9 Az értékelőnek meg kell vizsgálnia az STOE tervet annak megállapítása érdekében, hogy hogy minden SFR-t érvényre juttató komponens tartalmaz-e helyes és teljes leírást az SFR-vonzatú paraméterekről és az interfészektől közvetlenül visszatérő értékekről.

Egy komponens SFR-vonzatú interfészei azok az interfészek, amelyeket más komponensek használnak arra, hogy eszközként szolgáljanak a nyújtott SFR-vonzatú műveletek aktivizálásához, illetve arra, hogy bemenetet adjanak át, vagy kimenetet vegyenek át a komponensnek/komponenstől. Az ilyen interfész specifikációk célja a tesztelés lehetővé tétele. A komponensek közötti nem SFR-vonzatú interfészeket nem szükséges specifikálni vagy leírni, minthogy ezek nem kerülnek tesztelésre. Hasonlóan, az egyéb olyan belső interfészeket, amelyek nem kereszteznek SFR-vonzatú végrehajtási útvonalakat (mint amilyenek a rögzített belső útvonalak), nem szükséges specifikálni vagy leírni, minthogy ezek sem kerülnek tesztelésre.

Az SFR-vonzatú interfészek legyenek leírva abból a szempontból, hogy ezek hogyan aktivizálhatóak és hogy milyen értékeket adnak vissza. Ez az értékelés tartalmazzon egy felsorolást az SFR-vonzatú paraméterekről, és egy leírást ezekről.

Az interfész által visszaadott értékek olyan értékek, amelyeket paraméterek vagy üzenetek útján adnak tovább.

ASDV_SDS.1.9C Az STOE tervnek le kell írnia az összes SFR-t támogató, illetve az SFR-hez nem kapcsolódó komponenst, megadva céljukat és a többi komponenssel való kapcsolatukat.

ASDV_SDS.1-10 Az értékelőnek meg kell vizsgálnia az STOE tervet annak megállapítása érdekében, hogy az SFR-t támogató és az SFR-be nem beavatkozó komponensek helyesen lettek-e kategorizálva.

Azokban az esetekben, amikor a fejlesztő eltérő mennyiségű információt nyújt a különböző komponensekről, akkor ezzel egy közvetett kategorizálást végez. Vagyis (például) egy SFR-

vonzatú interfészekkel részletesen bemutatott komponens valószínűleg SFR-t érvényre juttató komponensnek sorolható, bár az értékelő vizsgálatai vezethetnek arra a megállapításra is, hogy ezek egyes részei SFR-t támogatóak vagy SFR-be nem beavatkozók. Azok a komponenseket pedig (például), amelyekre csak a célokat és a többi komponenssel való kölcsönhatásokat írták le, „közvetve” SFR-t támogatóként vagy SFR-be nem beavatkozóként kategorizálták.

ASDV_SDS.1.10C A leképezésnek szemléltetnie kell, hogy az STOE tervben leírt minden működést leképezi az ezeket meghívó SSFI-kre.

ASDV_SDS.1-11 Az értékelőnek meg kell vizsgálnia az STOE tervet annak megállapítása érdekében, hogy az tartalmaz-e teljes és helyes megfeleltetést a rendszer interfész specifikációban leírt SSFI és az STOE tervben leírt SSF komponensek között.

Az STOE tervben leírt komponensek ismertetik az SSF megvalósítását. Az SSFI azt ismerteti hogy a megvalósítás hogyan használható. Az integrátortól származó bizonyíték azonosítja azt a komponenst, amely először aktivizálódik, mikor műveletet kérnek az SSFI-től, valamint azonosítja az aktivizált komponens-láncot, egészen a funkcionalitás megvalósításáért elsődlegesen felelős komponensig. A teljes hívási fa nem szükséges minden egyes SSFI-hez ennél a munkaegységnél.

Az értékelő mérje fel a megfeleltetés teljességét meggyőződve arról, hogy minden SSFI-hez legalább egy komponenst hozzárendeltek.

Az ASDV_SDS.1.2E értékelői akció

ASDV_SDS.1.2E Az értékelőnek meg kell erősítenie, hogy az STOE terv az összes funkcionális biztonsági követelmény pontos és teljes megjelenítése.

ASDV_SDS.1-12 Az értékelőnek meg kell vizsgálnia az STOE funkcionális biztonsági követelményeit és a TOE tervet annak megállapítása érdekében, hogy az STOE terv az SST minden funkcionális biztonsági követelményét (SFR) lefedi-e.

Az értékelő összeállíthat egy megfeleltetést az STOE funkcionális biztonsági követelményei és az STOE terv között. Ez a megfeleltetés feltehetően egy SFR-től az alrendszerek egy halmazáig fog vezetni.

ASDV_SDS.1-13 Az értékelőnek meg kell vizsgálnia az STOE tervet annak megállapítása érdekében, hogy az minden funkcionális biztonsági követelményt helyesen jelenít-e meg.

Az értékelő összeállíthat egy megfeleltetést az STOE funkcionális biztonsági követelményei és az STOE terv között.

6.2.2.2.4. Rendszer-működési biztonsági koncepció: ASDV_OSC.1 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) rendszer interfész specifikáció,

c) biztonsági architektúra leírás,
d) STOE terv.

Az ASDV_OSC.1.1E értékelői akció

ASDV_OSC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_OSC.1.1C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer belső (rendszer határain belüli) információ áramlást érvényre juttató képességét.

ASDV_OSC.1-1 Az értékelőnek meg kell vizsgálnia a rendszer-működési biztonsági koncepció leírását annak megállapítása érdekében, hogy az meghatározza-e a rendszer belső információ áramlást érvényre juttató képességét.

ASDV_OSC.1.2C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer külső (külső rendszerek felé történő) információ áramlást érvényre juttató képességét.

ASDV_OSC.1-2 Az értékelőnek meg kell vizsgálnia a rendszer-működési biztonsági koncepció leírását annak megállapítása érdekében, hogy az meghatározza-e a rendszer külső információ áramlást érvényre juttató képességét.

ASDV_OSC1.3C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer lokális és távoli hozzáféréseket érvényre juttató képességét.

ASDV_OSC.1-3 Az értékelőnek meg kell vizsgálnia a rendszer-működési biztonsági koncepció leírását annak megállapítása érdekében, hogy az meghatározza-e a rendszer lokális hozzáféréseket érvényre juttató képességét.

ASDV_OSC.1-4 Az értékelőnek meg kell vizsgálnia a rendszer-működési biztonsági koncepció leírását annak megállapítása érdekében, hogy az meghatározza-e a rendszer távoli hozzáféréseket érvényre juttató képességét.

ASDV_OSC.1.4C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer erőforrásokhoz való (hozzáférés közvetítési szabályokon alapuló) hozzáféréseket érvényre juttató képességét.

ASDV_OSC.1-5 Az értékelőnek meg kell vizsgálnia a rendszer-működési biztonsági koncepció leírását annak megállapítása érdekében, hogy az meghatározza-e a rendszer erőforrásokhoz való hozzáféréseket érvényre juttató képességét.

ASDV_OSC.1.5C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer által nyújtott üzemmódokat, az üzemmódok közötti átmenetek feltételeit, és azokat az érvényesítő mechanizmusokat, amelyek minden azonosított rendszer üzemmódban biztonságos működést biztosítanak.

ASDV_OSC.1-6 Az értékelőnek meg kell vizsgálnia a rendszer-működési biztonsági koncepció leírását annak megállapítása érdekében, hogy az meghatározza-e a rendszer által nyújtott üzemmódokat.

Legalább az alábbi üzemmódokat biztosítani kell: normál üzemmód, karbantartási üzemmód, egy-felhasználós üzemmód, olyan speciális üzemmód, amelybe a rendszer egy hibát vagy kivételt követően kerül.

ASDV_OSC.1-7 Az értékelőnek meg kell vizsgálnia a rendszer-működési biztonsági koncepció leírását annak megállapítása érdekében, hogy az meghatározza-e a rendszer üzemmódjai közötti átmenetek feltételeit.

ASDV_OSC.1-8 Az értékelőnek meg kell vizsgálnia a rendszer-működési biztonsági koncepció leírását annak megállapítása érdekében, hogy az meghatározza-e a rendszer üzemmódok biztonságos működését biztosító érvényesítő mechanizmusokat.

ASDV_OSC.1.6C A rendszer-működési biztonsági koncepció leírásának belső ellentmondástól mentesnek kell lennie.

ASDV_OSC.1-9 Az értékelőnek meg kell vizsgálnia a rendszer-működési biztonsági koncepció leírását annak megállapítása érdekében, hogy az belső ellentmondástól mentes-e.

Az ASDV_OSC.1.2E értékelői akció

ASDV_OSC.1.2E Az értékelőnek meg kell állapítania a rendszer biztonsági terv dokumentációról (rendszer architektúra leírás, STOE terv), hogy az teljesen megvalósítja a rendszer-működési biztonsági koncepciót.

ASDV_OSC.1-10 Az értékelőnek meg kell vizsgálnia a rendszer architektúra leírást és az STOE tervet annak megállapítása érdekében, hogy azok teljesen megvalósítják-e a rendszer-működési biztonsági koncepciót.

6.2.2.3. A rendszer útmutató dokumentumok garanciaosztály (ASGD) értékelése

6.2.2.3.1. Előkészítési útmutató: ASGD_PRE.1 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) előkészítő útmutató,
c) az STOE komponenseire a szállítók szállítási eljárásainak a leírása.

Az ASGD_PRE.1.1E értékelői akció

ASGD_PRE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_PRE.1.1C Az előkészítő útmutatónak le kell írnia az STOE leszállított komponenseinek biztonságos elfogadásához alkalmazott valamennyi lépést, a komponens szállítójának szállítási eljárásaival összhangban.

ASGD_PRE.1-1 Az értékelőnek ellenőriznie kell, hogy biztosították-e az STOE komponenseire a szállítók szállítási eljárásainak a leírását.

Amennyiben a szállító szállítási eljárásaival kapcsolatban nem várható elfogadási eljárások alkalmazása, akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

ASGD_PRE.1-2 Az értékelőnek meg kell vizsgálnia a biztosított elfogadási eljárásokat annak megállapítása érdekében, hogy azok leírják-e az STOE komponenseinek biztonságos elfogadásához szükséges lépéseket, a szállító szállítási eljárásaival összhangban.

Az elfogadási eljárásoknak legalább a rendszer integrátor arra vonatkozó ellenőrzését tartalmazniuk kell, hogy az STOE valamennyi komponensét az SST-ben jelzett helyes verziókkal szállították-e le.

Az elfogadási eljárásoknak részletes információt kell szolgáltatniuk az alábbiakhoz, amennyiben azok alkalmazhatók:

a) az arról való meggyőződés, hogy a leszállított komponens az SST-ben jelzett helyes verzió
b) a leszállított komponens módosításának vagy hamisításának az észlelése.

ASGD_PRE.1.2C Az előkészítő útmutatónak le kell írnia az STOE komponensek biztonságos telepítéséhez, az STOE integrálásához és az üzemeltetési környezethez való biztonságos előkészülethez alkalmazott valamennyi lépést, az SST-ben leírt, üzemeltetési környezetre vonatkozó biztonsági célokkal összhangban.

ASGD_PRE.1-3 Az értékelőnek ellenőriznie kell, hogy biztosították-e az STOE komponenseinek biztonságos telepítéséhez szükséges eljárásokat.

Amennyiben az STOE-vel és üzemeltetési környezetével kapcsolatban nem várható telepítési eljárások alkalmazása (mert például az STOE-t már működésre alkalmas állapotban szállították le, s nincsenek a környezetére vonatkozó követelmények), akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

ASGD_PRE.1-4 Az értékelőnek meg kell vizsgálnia a biztosított telepítési eljárásokat annak megállapítása érdekében, hogy azok leírják-e az STOE komponensek biztonságos telepítéséhez, valamint az üzemeltetési környezet biztonságos előkészítéséhez szükséges lépéseket, az SST biztonsági céljaival összhangban.

Amennyiben nem várható telepítési eljárások alkalmazása (mert például az STOE-t már működésre alkalmas állapotban szállították le, s nincsenek a környezetére vonatkozó követelmények), akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

A telepítési eljárásoknak részletes információt kell szolgáltatniuk az alábbiakról, amennyiben azok alkalmazhatók:

a) a biztonságos telepítéshez szükséges minimális rendszer követelmények,
b) az üzemeltetési környezetre vonatkozó követelmények, az SST-ben meghatározott biztonsági célokkal összhangban,
c) az SSF ellenőrzése alatt álló egyedek telepítés-specifikus biztonsági tulajdonságainak módosítása,
d) kivételek és problémák kezelése.

6.2.2.3.2. Konfigurálási útmutató: ASGD_CON.1 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:
a) SST,
b) konfigurálási útmutató.

Az ASGD_CON.1.1E értékelői akció

ASGD_CON.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_CON.1.1C A konfigurálási útmutatónak le kell írnia azokat a biztonsági konfigurációs paramétereket, amelyek a rendszer integrátor vagy az ezzel azonos szerepkörű és felelősségű STOE felhasználók/adminisztrátorok számára elérhetők.

ASGD_CON.1-1 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy azok leírják-e a rendszer integrátor vagy az ezzel azonos szerepkörű és felelősségű STOE felhasználók/adminisztrátorok számára elérhető biztonsági konfigurációs paramétereket.

ASGD_CON.1.2C A konfigurálási útmutatónak le kell írnia azoknak a biztonsági paramétereknek a használatát, amelyeket az STOE állíthat be abból a célból, hogy megvalósítsa és érvényre juttassa a rendszer biztonsági szabályzatait.

ASGD_CON.1-2 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy azok leírják-e a biztonsági paramétereknek a használatát.

ASGD_CON.1.3C A konfigurálási útmutatónak figyelmeztetéseket kell tartalmaznia a konfigurálás által hozzáférhető azon funkciókra és privilégiumokra vonatkozóan, amelyeket egy biztonságos feldolgozási környezetben ellenőrizni kell.

ASGD_CON.1-3 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy az tartalmaz-e figyelmeztetéseket a konfigurálás által hozzáférhető azon funkciókra és privilégiumokra vonatkozóan, amelyeket egy biztonságos feldolgozási környezetben ellenőrizni kell.

ASGD_CON.1.4C A konfigurálási útmutatónak világosan be kell mutatnia az összes konfigurálással kapcsolatos felelősséget, amely az STOE biztonságos működtetéséhez szükséges.

ASGD_CON.1-4 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy az bemutatja-e az összes konfigurálással kapcsolatos felelősséget, amely az STOE biztonságos működtetéséhez szükséges.

ASGD_CON.1.5C A konfigurálási útmutatónak ellentmondás mentesnek kell lennie az értékeléshez átadott összes többi dokumentumhoz viszonyítva.

ASGD_CON.1-5 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy az ellentmondás mentes-e az értékeléshez átadott összes többi dokumentummal.

ASGD_CON.1.6C A konfigurálási útmutatónak le kell írnia az összes olyan biztonsági követelményt, amely az STOE-ra vonatkozik, beleértve az üzemeltetési környezetet is.

ASGD_CON.1-6 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy az leírja-e az összes STOE-ra vonatkozó biztonsági követelményt, beleértve az üzemeltetési környezetre vonatkozókat is.

ASGD_CON.1.7C A konfigurálási útmutatónak meg kell mutatnia, hogy az STOE terv megvalósítja az összes olyan komponensre vonatkozó biztonsági paramétert, amelyet a rendszer-működési biztonsági koncepció megkövetel.

ASGD_CON.1-7 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy az STOE terv megvalósítja-e az összes olyan komponensre vonatkozó biztonsági paramétert, amelyet a rendszer-működési biztonsági koncepció megkövetel.

6.2.2.3.3. Üzemeltetési útmutató: ASGD_OPE.1 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) rendszer interfész specifikáció,
c) STOE terv
d) üzemeltetési útmutató.

Az ASGD_OPE.1.1E értékelői akció

ASGD_OPE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_OPE.1.1C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia azokat a felhasználó által elérhető funkciókat és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

AGD_OPE.1-1 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót, annak megállapítása érdekében, hogy az leírja-e azokat a felhasználó által elérhető funkciókat és

jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

Az STOE konfigurálása lehetővé teheti, hogy a különböző felhasználói szerepkörök az STOE különböző funkcióihoz eltérő jogosultságokkal rendelkezzenek. Ezáltal egyes felhasználók számára engedélyezve lesznek olyan funkciók, melyek mások számára nem. Ezeket a funkciókat és jogosultságokat minden felhasználói szerepkörre le kell írni az üzemeltetési útmutatóban.

Az üzemeltetési útmutatónak minden felhasználói szerepkörre azonosítania kell az ellenőrzés alatt tartandó funkciókat és jogosultságokat, az ezek számára szükséges utasítás típusokat, valamint az utasítások okait. Az üzemeltetési útmutatónak figyelmeztetéseket kell tartalmaznia az ellenőrzés alatt tartandó funkciókra és jogosultságokra vonatkozóan. A figyelmeztetéseknek a várt hatásokról, az esetleges mellékhatásokról és a más funkciókkal és jogosultságokkal kapcsolatos lehetséges kapcsolatokról kell szólniuk.

ASGD_OPE.1.2C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia, hogy az STOE által biztosított, elérhető interfészeket hogyan kell biztonságos módon használni.

AGD_OPE.1-2 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e az STOE által biztosított, elérhető interfészek biztonságos használatát.

Az üzemeltetési útmutatónak javaslatokat kell megfogalmaznia az SSF hatékony használatához (például hibajavító csomagok frissítésének javasolt gyakorisága, jelszó kialakítási gyakorlat áttekintése, felhasználói állományok mentésének javasolt gyakorisága, felhasználói hozzáférési jogok megváltoztatása hatásának elemzése).

ASGD_OPE.1.3C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági szempontból fontos paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket.

AGD_OPE.1-3 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket is.

Az üzemeltetési útmutatónak áttekintést kell adnia a felhasználói interfészeken keresztül látható biztonsági funkcionalitásról.

Az üzemeltetési útmutatónak azonosítania kell, és le kell írnia a biztonsági funkciók és interfészek célját, működésüket, illetve egymás között kapcsolataikat.

Minden felhasználó által elérhető interfészre az üzemeltetési útmutatónak:

a) le kell írnia azokat a módszereket, melyekkel az interfész hívható (pl. parancssor, programozási nyelvi rendszerhívások, menükiválasztás, parancsgombok);

b) le kell írnia a felhasználó által állítandó paramétereket, azok célját, érvényes és alapértelmezett értékeiket, a paraméterek biztonságos és nem biztonságos használatát okozó beállításokat, mindezt egyenként vagy paraméter-kombinációkban;
c) le kell írnia a közvetlen TSF válaszokat, üzeneteket vagy visszaadott kódot.

Az értékelőnek elsősorban a rendszer interfész specifikációt és az SST-t kell figyelembe vennie annak megállapítása érdekében, hogy az ezekben leírt TSF összhangban áll-e az üzemeltetési útmutatóval. Az értékelőnek meg kell győződnie az üzemeltetési útmutató teljességéről, vagyis arról, hogy az összes emberi felhasználó számára lehető teszi az elérhető interfészek biztonságos használatát. Az értékelő segítségként elkészítheti az útmutató és ezen dokumentumok közötti informális leképezést. Az ebben fellelhető bármilyen hiányosság az útmutató teljességének csorbulását jelezheti.

ASGD_OPE.1.4C Az üzemeltetési útmutatónak minden felhasználói szerepkörre világosan be kell mutatnia a felhasználó által elérhető funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból fontos minden esemény típust, beleértve az SSF ellenőrzése alá eső egyedek biztonsági tulajdonságainak megváltoztatását is.

AGD_OPE.1-4 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e a felhasználói funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból lényeges minden esemény típust, beleértve az SSF ellenőrzése alá tartozó egyedek biztonsági tulajdonságainak megváltoztatását is.

Minden biztonsági szempontból fontos esemény típust részletezni kell minden felhasználói szerepkörre, hogy minden felhasználó tudja, milyen események fordulhatnak elő, és mit kell tennie (ha szükséges) a biztonság fenntartása érdekében. Az STOE üzemeltetése során előforduló biztonsági szempontból lényeges eseményeket (például naplótár túlcsordulás; rendszerösszeomlás; felhasználói rekordok felülírása, amikor egy felhasználó távozik a szervezettől, és a fiókját eltörlik) kellően meg kell határozni, hogy a felhasználó beavatkozhasson a biztonságos működés fenntartása érdekében.

ASGD_OPE.1.5C Az üzemeltetési útmutatónak azonosítani kell az STOE összes lehetséges üzemmódját (beleértve a karbantartási és a meghibásodás vagy üzemeltetési hiba utáni üzemmódokat is), valamint ezek biztonságos üzemeltetésre gyakorolt következményeit és kihatásait.

AGD_OPE.1-5 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót és az egyéb értékeléshez adott bizonyítékot annak megállapítása érdekében, hogy az útmutató azonosítja-e a TOE összes lehetséges üzemmódját (beleértve a karbantartási és a meghibásodás vagy üzemeltetési hiba utáni üzemmódokat is), valamint ezek következményét és kihatásait a biztonságos üzemelés fenntartására.

Más értékelési bizonyítékot (elsősorban a rendszer interfész specifikációt) az értékelőnek annak megállapításához javasolt használnia, hogy az útmutató megfelelő eligazító leírást tartalmaz-e.

A teszt dokumentációban benyújtott információ is felhasználható annak eldöntésére, hogy az útmutató elegendő útmutató információt tartalmaz-e. A tesztlépéseknél megadott részletek felhasználhatók annak megerősítésére, hogy az üzemeltetési útmutató elégséges az STOE használatához és adminisztrálásához.

Az értékelőnek egy időben egy ember számára látható interfészt ajánlott vizsgálnia, úgy, hogy összehasonlítja az interfészt biztonságos használatáról szóló útmutatást egyéb bizonyítékokkal, annak kiderítése érdekében, hogy az interfésszel kapcsolatos információk valóban jól írják-e le annak biztonságos használatát (azaz megfelelnek-e az SFR-eknek). Az értékelőnek az interfészek közötti kapcsolatokat is át kell néznie, potenciális ellentmondásokat keresve.

ASGD_OPE.1.6C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia azokat a betartandó biztonsági intézkedéseket, melyek az SST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

AGD_OPE.1-6 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e azokat a betartandó biztonsági intézkedéseket, melyek az SST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

Az értékelő elemezze az SST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célokat, majd állapítsa meg, hogy az üzemeltetési útmutató minden felhasználói szerepkörre megfelelően leírja-e a fontos biztonsági intézkedéseket.

Az üzemeltetési útmutatóban leírt biztonsági intézkedéseknek magukban kell foglalniuk az összes fontos külső eljárásrendi, fizikai, személyzeti és kapcsolódásra vonatkozó intézkedést.

ASGD_OPE.1.7C Az üzemeltetési útmutatónak egyértelműnek és megalapozottnak kell lennie.

AGD_OPE.1-7 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót annak megállapítása érdekében, hogy az egyértelmű-e.

Az útmutató akkor nem egyértelmű (félrevezető), ha ez alapján egy felhasználó indokoltan félreértheti teendőit, és az STOE-ra vagy az STOE által nyújtott biztonságra nézve hátrányos módon alkalmazza a leírtakat.

AGD_OPE.1-8 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót annak megállapítása érdekében, hogy az megalapozott-e.

Az útmutató akkor tekinthető megalapozatlannak, ha olyan követelményeket támaszt az STOE használatával vagy üzemeltetési környezetével szemben, melyek nem felelnek meg az SST-nek, vagy indokolatlanul nagy terhet jelentenek a biztonság fenntartásához.

6.2.2.4. A rendszer konfiguráció kezelés garanciaosztály (ASCM) értékelése

6.2.2.4.1. Rendszer alap konfiguráció: ASCM_SBC.1 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) CM dokumentáció a rendszer alap konfigurációjához,
b) STOE terv.

Az ASCM_SBC.1.1E értékelői akció

ASCM_SBC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASCM_SBC.1.1C A CM rendszernek egyedileg azonosítania kell az STOE alap konfigurációt, az alap konfigurációt alkotó összes rendszer komponenst és ezek értékelési állapotát.

ASCM_SBC.1-1 Az értékelőnek ellenőriznie kell, hogy a CM rendszer egyedileg azonosítja-e az STOE alap konfigurációt, az alap konfigurációt alkotó összes rendszer komponenst és ezek értékelési állapotát.

ASCM_SBC.1.2C A CM rendszernek nyomon kell követnie az alap konfigurációhoz, illetve az ezt alkotó rendszer komponensekhez kapcsolódó változtatásokat.

ASCM_SBC.1-2 Az értékelőnek meg kell vizsgálnia a CM rendszert annak megállapítása érdekében, hogy az nyomon követi-e az alap konfigurációhoz, illetve az ezt alkotó rendszer komponensekhez kapcsolódó változtatásokat.

ASCM_SBC.1.3C A CM tervnek le kell írnia, hogy a rendszer alap konfigurációját hogyan kezelik, és hogy az alap konfiguráción történő módosításokat hogyan ellenőrzik és hogyan követik nyomon.

ASCM_SBC.1-3 Az értékelőnek meg kell vizsgálnia a CM tervet annak megállapítása érdekében, hogy az leírja-e, hogy a rendszer alap konfigurációját hogyan kezelik, valamint hogy az alap konfiguráción történő módosításokat hogyan ellenőrzik és hogyan követik nyomon.

6.2.2.4.2. Értékelt és tanúsított komponensek: ASCM_ECC.1 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) CM dokumentáció a rendszer alap konfigurációjához,
b) STOE terv,
c) értékelt és tanúsított termék-komponensek listája.

Az ASCM_ECC.1.1E értékelői akció

ASCM_ECC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASCM_ECC.1.1C Az értékelt és tanúsított termék-komponensek listájában le kell írni az értékelt és tanúsított termékek garanciacsomagjait.

ASCM_ECC.1-1 Az értékelőnek meg kell vizsgálnia, hogy értékelt és tanúsított termék-komponensek listája a rendszer valamennyi STOE tervben azonosított komponensét tartalmazza-e.

ASCM_ECC.1-2 Az értékelőnek ellenőriznie kell, hogy értékelt és tanúsított termék-komponensek listája leírja-e az egyes értékelt és tanúsított termékek garanciacsomagjait.

A leírás az alábbi garanciacsomagokat tartalmazhatja: CC EAL1, CC EAL1+, CC EAL2, CC EAL2+, CC EAL3, CC EAL3+, CC EAL4, CC EAL4 felett, MIBÉTS alap, MIBÉTS fokozott, MIBÉTS kiemelt, nincs tanúsítva.

ASCM_ECC.1.2C Az értékelt és tanúsított termék-komponensek listájának minden termékre azonosítania kell az értékelési eredményekre vonatkozó tanúsítványt, tanúsítási jelentést és az ezek alapjául szolgáló biztonsági előirányzatot.

ASCM_ECC.1-3 Az értékelőnek ellenőriznie kell, hogy értékelt és tanúsított termék-komponensek listája azonosítja-e minden értékelt és tanúsított termék-komponensre az alábbiakat: biztonsági előirányzat, tanúsítási jelentés, tanúsítvány.

ASCM_ECC.1.3C Az értékelt és tanúsított termék-komponensek listájának minden termékre le kell írnia az üzemeltetési feltételeket.

ASCM_ECC.1-4 Az értékelőnek ellenőriznie kell, hogy értékelt és tanúsított termék-komponensek listája leírja-e minden értékelt és tanúsított termék-komponensre annak üzemeltetési feltételeit.

Az ASCM_ECC.1.2E értékelői akció

ASCM_ECC.1.2E Az értékelőnek meg kell erősítenie, hogy a rendszer üzemeltetési környezete kielégíti az értékelt és tanúsított termékek tanúsítványaiban és tanúsítási jelentéseiben megfogalmazott üzemeltetési feltételeket.

ASCM_ECC.1-5 Az értékelőnek meg kell vizsgálnia, hogy értékelt és tanúsított termék-komponensek listájában a termék-komponensekre leírt üzemeltetési feltételek összhangban állnak-e az adott termék tanúsítványában és tanúsítási jelentésében az üzemeltetési feltételekre megfogalmazott korlátozásokkal.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

6.2.2.5. A rendszer tesztelés garanciaosztály (ASTE) értékelése

6.2.2.5.1. Funkcionális rendszer tesztelés: ASTE_FUN.1 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) rendszer interfész specifikáció,
c) tesztdokumentáció.

Az ASTE_FUN.1.1E értékelői akció

ASTE_FUN.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASTE_FUN.1.1C A tesztdokumentációnak tartalmaznia kell a teszttterveket, az elvárt teszteredményeket és a tényleges teszteredményeket.

ASTE_FUN.1-1 Az értékelőnek ellenőriznie kell, hogy a tesztdokumentáció tartalmazza-e a teszttterveket, az elvárt eredményeket és a tényleges teszt eredményeket.

Az értékelő ellenőrizze, hogy a teszttterveket, az elvárt eredményeket és a tényleges teszt eredményeket belefoglalták-e a tesztdokumentációba.

ASTE_FUN.1.2C A teszttterveknek azonosítaniuk kell a végrehajtandó teszteket, és le kell írniuk minden teszt végrehajtásának forgatókönyvét. Ezen forgatókönyveknek tartalmazniuk kell a más tesztek eredményeitől való minden sorrendbeli függést.

ATSE_FUN.1-2 Az értékelőnek ellenőriznie kell, hogy a teszttervek leírják-e minden teszt végrehajtásának forgatókönyvét.

Az értékelőnek meg kell állapítania, hogy a teszttervek nyújtnak-e információkat a használt tesztkonfigurációra vonatkozóan: mind az STOE konfigurációra, mind pedig minden használt tesztberendezésre vonatkozóan. Ennek az információnak a tesztkonfiguráció reprodukálhatóságának biztosításához kellően részletesnek kell lennie.

Az értékelőnek azt is meg kell állapítania, hogy a teszttervek nyújtanak-e információt arról, hogy hogyan kell végrehajtani a tesztet: az összes szükséges automatizált indítási eljárásról (és hogy ezek igényelnek-e futási jogosultságot), az alkalmazandó bemenetekről és ezek alkalmazásáról, hogyan lehet megkapni a kimenetet, valamennyi automatikus törlési eljárásról (és hogy ezek igényelnek-e futási jogosultságot), stb. Ennek az információnak a teszt reprodukálhatóságának biztosításához kellően részletesnek kell lennie.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ASTE_FUN.1-3 Az értékelőnek meg kell vizsgálnia a teszttterveket annak megállapítása érdekében, hogy a TOE teszt konfigurációja megegyezik-e az SST-ben az értékelésre megadott konfigurációval.

Az SST egynél több konfigurációt is meghatározhat az értékeléshez. Az értékelő ellenőrizze, hogy a rendszer integrátor által a tesztdokumentációban azonosított összes teszt konfiguráció megfelel-e az SST-nek.

Az értékelő vegye figyelembe azokat az SST-ben leírt, az STOE üzemeltetési környezetére vonatkozó biztonsági céljait, amelyek a teszt környezetre alkalmazhatók. Lehet hogy néhány cél nem alkalmazható a teszt környezetre. Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ASTE_FUN.1-4 Az értékelőnek meg kell vizsgálnia a teszttervet annak megállapítása érdekében, hogy az elegendő utasítást tartalmaz-e a sorrendi függőségekre.

Bizonyos lépések végrehajtására szükség lehet a kezdeti feltételek kialakítása érdekében. Például a felhasználói fiókokat fel kell venni, mielőtt azokat törölni lehet. Egy példa a sorrendiségi függőségre: először azokat a tevékenységeket kell végrehajtani, melyek naplóbejegyzéseket állítanak elő, s csak ezt követően lehet a naplóbejegyzéseket kereső és rendező tesztekkel foglakozni. Másik példa a sorrendiségi függőségre: egyik teszteset állítja elő azt az adatállományt, amely egy másik teszt eset számára bemenetként szolgál.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ASTE_FUN.1.3C Az elvárt teszteredményeknek be kell mutatniuk a tesztek sikeres végrehajtásából keletkező várható kimeneteket.

ASTE_FUN.1-5 Az értékelőnek meg kell vizsgálnia a tesztdokumentációt annak megállapítása érdekében, hogy az tartalmazza-e az összes várt teszteredményt.

Az elvárt teszteredmények annak megállapításához szükségek, hogy egy tesztet sikeresen végrehajtottak-e vagy sem. Az elvárt teszteredmények akkor tekinthetők kielégítőnek, ha egyértelműek, és megfelelnek az adott tesztelési módszer alapján várt működésnek.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ASTE_FUN.1.4C A tényleges teszteredményeknek összhangban kell állniuk az elvárt teszteredményekkel.

ASTE_FUN.1-6 Az értékelőnek ellenőriznie kell, hogy a tesztdokumentációban szereplő várt teszteredmények összhangban állnak-e a tényleges teszteredményekkel.

A rendszer integrátor által átadott tényleges és várt teszteredmények összehasonlítása felfedi a két eredményhalmaz közötti különbségeket. Lehet, hogy a tényleges teszteredmények közvetlen összehasonlítása nem történhet meg bizonyos adatok egyszerűsítése vagy összevonása előtt. Ilyenkor a rendszer integrátor tesztdokumentációjában ismertetni kell a tényleges adatokat egyszerűsítő vagy összevonó eljárásokat.

Például a rendszer integrátornak tesztelnie kell egy üzenettár tartalmát egy hálózati kapcsolat után, az üzenettár tartalmának megállapítása érdekében. Az üzenettár egy bináris számot

tartalmaz, amelyet valamilyen más adatmegjelenítési formába kell átalakítani az értelmezhetőség érdekében. A rendszer integrátornak tehát le kell írnia az adat magas szintű ábrázolási formába történő átalakításának módját, hogy az értékelő is végre tudja azt hajtani (szinkron vagy aszinkron átvitel, stop bitek száma, paritás, stb.).

Megjegyzendő, hogy a tényleges adatok egyszerűsítő vagy összevonó folyamatának leírását az értékelő nem a szükséges módosítások tényleges elvégzésére használja, hanem a folyamat megfelelőségének értékelésére. A rendszer integrátor feladata az elvárt teszteredmények átalakítása olyan formára, amely könnyen összehasonlítható a tényleges teszteredményekkel. Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ASTE_FUN.1-7 Az értékelőnek jelentést kell készítenie a rendszer integrátor tesztelési munkájáról, áttekintést adva a tesztelési módszerről, konfigurációról, mélységről és eredményekről.

Az értékelési jelentésben rögzített rendszer integrátori tesztelésről szóló információ lehetővé teszi az értékelő számára, hogy bemutassa az általános tesztelési módszert és a rendszer integrátor által az STOE tesztelésébe fektetett munkát. A cél a rendszer integrátor tesztelési munkájának érdemi áttekintése. Nem cél, hogy az értékelési jelentésben a rendszer integrátor tesztelésével kapcsolatos információk a specifikus tesztlépések vagy egyedi tesztek eredményeinek pontos megismétlése legyenek. A cél elegendő részletesség biztosítása más értékelők számára ahhoz, hogy betekintést kapjanak a rendszer integrátor tesztelési módszerébe, a végrehajtott tesztek nagyságrendjébe, az STOE teszt konfigurációjába és a rendszer integrátor tesztelésének általános eredményébe.

Az értékelési jelentés rendszer integrátori tesztekről szóló részében általában az alábbi információk találhatók:

a) STOE teszt konfigurációk. A ténylegesen tesztelt STOE konfigurációk, köztük az, hogy a teszt felállítása vagy a tesztet követő rendteremtés igényelt-e külön jogosultságú kódot.
b) Tesztelési módszer. A rendszer integrátor által alkalmazott tesztelési stratégia áttekintése.
c) Tesztelési eredmények. A rendszer integrátor tesztelési eredményének áttekintő leírása.

ASTE_FUN.1.5C A tesztdokumentációnak tartalmaznia kell egy vizsgálatot a teszt eljárás sorrendi függőségeiről.

ASTE_FUN.1-8 Az értékelőnek ellenőriznie kell, hogy a tesztdokumentáció tartalmaz-e egy vizsgálatot a teszt eljárás sorrendi függőségeiről.

ASTE_FUN.1.6C A biztonsági intézkedések tesztelésének részletességére vonatkozó vizsgálatának be kell mutatnia, hogy az SST-ben elvárt funkcionális biztonsági követelmények és a tesztdokumentációban megadott tesztek közötti megfeleltetés teljes.

ASTE_FUN.1-9 Az értékelőnek ellenőriznie kell, hogy a vizsgálat kimutatja-e az SST-ben elvárt funkcionális biztonsági követelmények és a tesztdokumentációban megadott tesztek közötti megfeleltetés teljességét.

6.2.2.5.2. A rendszer tesztelés lefedettsége: ASTE_COV.1 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) rendszer interfész specifikáció,
c) tesztdokumentáció,
d) tesztlefedettség elemzés.

Az ASTE_COV.1.1E értékelői akció

ASTE_COV.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASTE_COV.1.1C A tesztlefedettség elemzésének be kell mutatnia a tesztdokumentációban azonosított tesztek és a rendszer biztonsági funkcionalitás (ahogyan azt a rendszer interfész specifikáció a külső interfészeken keresztül leírja) közötti megfeleltetést.

ASTE_COV.1-1 Az értékelőnek meg kell vizsgálnia a tesztlefedettség elemzést annak megállapítása érdekében, hogy a tesztdokumentációban azonosított tesztek és a rendszer interfész specifikációban leírt interfészek közötti megfeleltetés pontos-e.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt lefedettség elemzésben szereplő teszteket és interfészeket egyértelműen kell azonosítani.
Emlékeztetjük az értékelőt arra, hogy nem kell a tesztdokumentáció valamennyi tesztjét leképezni a rendszer interfész specifikációban leírt interfészekre.

ASTE_COV.1-2 Az értékelőnek meg kell vizsgálnia a teszttervet annak megállapítása érdekében, hogy a tesztelési módszer minden interfész esetén szemlélteti-e az adott interfész elvárt működését.

Ehhez először is az értékelőnek meg kell értenie a TOE elvárt működését. Ehhez az értékelő választhatja az SSF és a külső interfészek alrendszerekre bontását az SST-ben szereplő SFR-ek (naplózás, hitelesítés, stb.) szerint, majd egyszerre csak egy alrendszerre összpontosíthat. Az értékelő vizsgáljon meg minden SST követelményt, valamint a rendszer interfész specifikáció és az útmutató dokumentáció vonatkozó részeit, hogy megértse azt, milyen működést várnak el az érintett külső interfésztől. Hasonlóan, az értékelő vizsgálja meg az STOE terv és a biztonsági architektúra leírás vonatkozó részeit, hogy megértse azt, milyen működést várnak el az SSF érintett alrendszereitől és komponenseitől.

A tervezett működés megértése után az értékelő vizsgálja meg a teszttervet, hogy áttekintést kapjon a tesztelés módszeréről. A legtöbb esetben a tesztelési módszer egy külső interfész kiváltása, majd a válaszok megfigyelése. A kívülről látható funkcionalitások közvetlenül tesztelhetők, amikor viszont a funkcionalitás az STOE-n kívülről nem látható (például a maradvány információ védelmi funkcionalitás), akkor más eszközöket kell alkalmazni.

Amikor nincs kívülről látható interfész, tipikus megoldás lehet a rendszer integrátor által biztosított belső (integrációs, komponens vagy modul) tesztelés eredményeinek felhasználása.

Ilyen esetekben külön ellenőrizni kell, hogy a belső tesztelési eredmények az STOE aktuális megvalósítását tükrözi-e. Amennyiben a rendszer elemei változtak a tesztelés óta, akkor bizonyítékra van szükség arról, hogy a változtatásokat nyomon követték és elemezték, vagy további tesztekre van szükség.

ASTE_COV.1-3 Az értékelőnek meg kell vizsgálnia a teszt eljárásokat annak megállapítása érdekében, hogy a teszt előfeltételek, a tesztelési lépések és az elvárt eredmény(ek) megfelelően tesztelnek-e minden interfészt.

A tesztelés által megkövetelt kezdeti feltételek kialakításához szükség van a tesztelés előfeltételeire. Ezek kifejezhetők beállítandó paraméterekkel, vagy a tesztelés sorrendjének kialakításával, olyan esetekben, amikor az egyik teszt befejezése teremti meg egy másik teszt szükséges előfeltételeit. Az értékelőnek meg kell állapítania, hogy az előfeltételek teljesek és alkalmasak-e, nehogy a megfigyelt teszteredmények az elvárt eredmény irányába befolyásolják a folyamatot.

A tesztelési lépések és várt eredmények meghatározzák a külső interfészre alkalmazandó feladatokat és paramétereket, valamint, hogy a várt eredményeket milyen módon kell ellenőrizni és mik ezek az eredmények. Az értékelőnek meg kell állapítania, hogy a tesztelési lépések és várt eredmények összhangban vannak-e a rendszer interfész specifikáció interfész leírásával. Ez azt jelenti, hogy az interfész működés rendszer interfész specifikációban közvetlenül leírt minden jellemzőjéhez tartoznia kell tesztnek és várt eredménynek az adott működés ellenőrzése érdekében.

6.2.2.5.3. A rendszer tesztelés mélysége: ASTE_DPT.1 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) rendszer interfész specifikáció,
c) biztonsági architektúra leírás,
d) STOE terv,
e) tesztdokumentáció,
f) tesztmélység elemzés.

Az ASTE_DPT.1.1E értékelői akció

ASTE_DPT.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASTE _DPT.1.1C A tesztmélység elemzésnek be kell mutatnia, hogy a tesztdokumentációban azonosított tesztek elegendőek annak bemutatására, hogy a rendszer biztonsági funkcionalitása a rendszer biztonsági architektúra leírással összhangban működik.

ASTE_DPT.1-1 Az értékelőnek meg kell vizsgálnia a tesztdokumentációt és a tesztmélység elemzést annak megállapítása érdekében, hogy a rendszer biztonsági architektúra leírásban azonosított, az STOE-t külső informatikai rendszerekhez kapcsoló interfészeket tesztelték-e.

Ez a munkaegység ellenőrzi a tesztek és a rendszer biztonsági architektúra leírás megfelelését. Amennyiben az SSF szerkezeti helyességének leírása (az ADV_ARC biztonsági szerkezet leírás keretén belül) speciális mechanizmusokra hivatkozik, ez a munkaegység ellenőrizze a tesztek és az ilyen mechanizmusok üzemeltetési leírása közötti megfelelést is.

ASTE_DPT.1-2 Az értékelőnek meg kell vizsgálnia a tesztdokumentációt és a tesztmélység elemzést annak megállapítása érdekében, hogy azok szemléltetik-e, hogy az STOE és a külső informatikai rendszerek egymásra hatása megfelel a rendszer biztonsági architektúra leírásban foglaltaknak.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt mélység elemzésben szereplő teszteket és a kapcsolódó külső informatikai rendszerek egyértelműen kell azonosítani.

6.2.2.5.4. Független rendszer tesztelés: ASTE_IND.1

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

g) SST,
h) rendszer interfész specifikáció,
i)előkészítő útmutató,
j)konfigurálási útmutató,
k) üzemeltetési útmutató
l)a tesztelésre alkalmas STOE.

Az ASTE_IND.1.1E értékelői akció

ASTE_IND.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASTE_IND.1.1C A STOE-nek tesztelésre alkalmas állapotban kell lennie.

ASTE_IND.1-1 Az értékelőnek meg kell vizsgálnia az STOE-t annak megállapítása érdekében, hogy a teszt konfiguráció megegyezik-e az SST-ben meghatározott, értékelés alatt álló konfigurációval.

Az STOE-t alkotó különálló hardver és szoftver komponenseket az SST-nek megfelelően kell tesztelni. Az értékelő ellenőrizze, hogy valamennyi teszt konfiguráció ellentmondás mentes-e az SST-vel.

Az értékelő vegye figyelembe azokat az SST-ben leírt, az STOE üzemeltetési környezetére vonatkozó biztonsági célokat, amelyek a teszt környezetre alkalmazhatók.

Bármilyen tesztelési erőforrás (mérőműszer, elemző készülék) használatakor az értékelő felelőssége annak biztosítása, hogy ezek az erőforrások megfelelően hitelesítve legyenek.

ASTE_IND.1-2 Az értékelőnek meg kell vizsgálnia az STOE-t annak megállapítása érdekében, hogy annak minden komponensét megfelelően telepítették-e, és ismert állapotban van-e.

ASTE_IND.1.2C A rendszer integrátornak biztosítania kell az SSF funkcionális tesztelése során használt erőforrás-készlettel azonos eszközkészletet.

ASTE_IND.1-3 Az értékelőnek meg kell vizsgálnia a rendszer integrátor által rendelkezésére bocsátott erőforrás-készletet annak megállapítása érdekében, hogy az azonos-e az SSF rendszer integrátor általi funkcionális tesztelése során alkalmazott erőforrásokkal.

A rendszer integrátor által használt erőforrás-készletet a rendszer integrátor teszterv dokumentálja, az ASTE_FUN funkcionális tesztelés családban meghatározott módon. Az erőforrás-készlet többek között felölelhet laboratóriumi hozzáférést és speciális teszt berendezéseket is. Azokat az erőforrásokat, melyek nem egyeznek meg a rendszer integrátor által használtakkal, azonossá kell tenni a teszteredményekre gyakorolt lehetséges hatásuk szerint.

Az ASTE_IND.1.2E értékelői akció

ASTE_IND.1.2E Az értékelőnek végre kell hajtania a tesztdokumentációban szereplő tesztek valamely részhalmazát (mintáját) a rendszer integrátor teszteredményeinek ellenőrzése érdekében.

ASTE_IND.1-4 Az értékelőnek el kell végeznie a tesztelést a rendszer integrátor tesztterében található tesztek egy mintájára.

E munkaegység célja, hogy az értékelő elegendő számú rendszer integrátor teszt végrehajtásával meggyőződjön a rendszer integrátor teszteredményeinek érvényességéről. A minta nagyságáról, és a mintát alkotó tesztekről az értékelő dönt.

A rendszer integrátor összes tesztje visszavezethető speciális interfészekre. Ezért a mintát alkotó tesztek kiválasztásakor figyelembe vett tényezők hasonlóak az ASTE_IND.1-6 munkaegységnél leírtakhoz. Ezen kívül az értékelő alkalmazhat véletlenszerű mintavételezési módszert is a rendszer integrátor tesztjeiből való választáshoz, mintába vételéhez.

ASTE_IND.1-5 Az értékelőnek ellenőriznie kell, hogy a tényleges teszteredmények összhangban állnak-e az elvárt teszteredményekkel.

A tényleges és az elvárt teszteredmények közti különbségek az ellentmondás feloldására késztetik az értékelőt. Az értékelő által feltárt ellentmondást a rendszer integrátor is feloldhatja kielégítő magyarázattal vagy az eltérések feloldásával.

Amennyiben nincs kielégítő magyarázat vagy feloldás, akkor az értékelő kevésbé megbízhatónak ítélheti a rendszer integrátor tesztelését, és növelheti a tesztelési minta nagyságát. Annak megerősítése érdekében, hogy az ASTE_IND.1-4 munkaegységben azonosított mintát megfelelően tesztelték, a rendszer integrátor tesztelésében talált

hiányosságokat meg kell szüntetni, akár a tesztelés kijavításával, akár az értékelő által végzett új tesztekkel.

Az ASTE_IND.1.3E értékelői akció

ASTE_IND.1.3E Az értékelőnek tesztelnie kell az SSF külső és belső interfészeinek egy részét annak megerősítése érdekében, hogy az SSF a specifikáltaknak megfelelően működik.

ASTE_IND.1-6 Az értékelőnek meg kell terveznie egy tesztkészletet.

Az értékelő válassza ki az STOE-nek megfelelő tesztkészletet és tesztelési stratégiát. Egy lehetséges szélsőséges tesztelési stratégia szerint a tesztkészlet annyi interfészt tartalmaz, amennyi csak tesztelhető kevés szigorral. Egy másik lehetséges tesztelési stratégia, hogy a teszt néhány interfészre terjed ki azok fontossága szerint és ezeket igen alapos ellenőrzésnek vetik alá.

Az értékelő által követett tesztelési módszer általában e két szélsőséges eset közé esik. Az értékelőnek ajánlott az interfészek nagy részére legalább egy tesztet végrehajtania, de a tesztelésnek nem kell teljes körű specifikáció-tesztelésnek lennie.

Az értékelőnek a tesztelendő interfész részhalmaz kiválasztásakor az alábbi tényezőket kell figyelembe vennie:

a) A rendszer integrátor tesztelési bizonyítékai, ami a következőkből áll: tesztdokumentáció, teszt lefedettség elemzés, teszt mélység elemzés. Ezek betekintést nyújtanak abba, hogy a rendszer integrátor a tesztelés során hogyan aktivizálta a biztonsági funkciókat. Az értékelő ezt az információt felhasználja az STOE független teszteléséhez szükséges új tesztek tervezésékor. Fokozottan át kell gondolnia a következőket:
   aa) Az interfészekre vonatkozó rendszer integrátori tesztelés bővítése. Az értékelő végrehajthat ugyanolyan típusú teszteket változó paraméterekkel az interfész szigorúbb tesztelése céljából.
   ab) Az interfészekre vonatkozó rendszer integrátori tesztelési stratégia kiegészítése. Az értékelő módosíthatja egy adott interfészeknél alkalmazott tesztelési módszert egy új tesztelési stratégiát alkalmazva.
b) Azon interfészek száma, melyekből a tesztkészlet készül. Amennyiben az STOE csak kis számú, viszonylag egyszerű interfészt tartalmaz, célszerű lehet az összes szigorú tesztelése. Más esetekben ez nem költség-hatékony módszer, ekkor mintavételezésre van szükség.
c) Az értékelési tevékenységek egyensúlyának fenntartása. A tesztelésbe fektetett értékelői munka álljon arányban a többi értékelési feladatba fektetett munkával.

Az értékelő válassza ki az interfészek részhalmazát. Ez a kiválasztás több tényezőtől függ, és e tényezők is hatást gyakorolnak a tesztkészlet méretére:

a) Az interfészek rendszer integrátori tesztelésének szigora. Azokat az interfészeket, melyekre az értékelő további tesztelés szükségességét állapítja meg, ajánlott a tesztkészletbe bevenni.

b) A rendszer integrátori teszteredmények. Amennyiben a rendszer integrátor teszteredmény kétséget támaszt az értékelőben egy interfész megfelelő megvalósításával kapcsolatban, az adott interfészt ajánlott a tesztkészletbe bevenni.
c) Az interfészek fontossága. Azokat az interfészeket, amelyek a többieknél (biztonsági szempontból) fontosabbak, ajánlott a tesztkészletbe bevenni.
d) Az interfészek bonyolultsága. A bonyolult megvalósítást igénylő interfészek erőforrás igényes teszteket követelnek meg a rendszer integrátortól és az értékelőktől. Ugyanakkor a bonyolult interfészeknél nagyobb a hibákra bukkanás valószínűsége. Az értékelőnek e két ellentétes szempontot kell mérlegelnie.
e) Közvetett tesztelés. Egyes interfészek tesztelése gyakran más interfészek közvetett tesztelésével is jár, így ezek tesztkészletbe vétele maximalizálja a tesztelt interfészek számát (még ha csak közvetett módon is). Egyes interfészeket általában széleskörű biztonsági funkcionalitásra használnak, így ezek kiválasztásával hatékonyabb lehet a tesztelés.
f) Az interfészek típusai (pl. programozott, parancs-soros, protokoll). Az értékelőnek az STOE által támogatott minden interfész típusból ajánlott bevennie teszteket.
g) Új vagy szokatlan megoldásokat használó interfészek. Amennyiben az STOE újszerű vagy szokatlan tulajdonságokat tartalmaz, melyek erős üzleti hangsúlyt kaphatnak, az ezeknek megfelelő interfészek is erős jelöltek a tesztelésre.

A fenti útmutató kiemeli a megfelelő tesztkészlet kiválasztási folyamata során figyelembe veendő tényezőket, de nem tekinthető teljesnek.

ASTE_IND.1-7 Az értékelőnek el kell készítenie a tesztkészlethez a tesztdokumentációt, amely kellőképpen részletes a tesztek megismételhetősége érdekében.

Az SSF elvárt működésének az SST-ből, a rendszer interfész specifikációból és az STOE tervből történő megértése után az értékelőnek meg kell határoznia az interfész tesztelésére leginkább alkalmas módot. Az értékelő különösen az alábbiakat vegye figyelembe:

a) a használni kívánt módszer, például egy külső vagy egy belső interfészt tesztelnek, esetleg egy alternatív teszt módszert (különleges esetben például kód vizsgálatot) alkalmaznak,
b) az interfész(ek), melye(ke)t a tesztelésnél és a válaszok megfigyelésénél használnak,
c) a teszteléshez szükséges kezdeti feltételek (például bármely szükséges különleges objektum vagy szubjektum, a szükséges biztonsági tulajdonságokkal),
d) a teszteléshez szükséges speciális berendezések, mely vagy egy interfész aktivizálásához (pl. csomag generátorok), vagy egy interfész megfigyeléséhez (pl. hálózati analizátorok) szükségesek.

Az értékelő tesztelhet úgy is minden interfészt, hogy teszt-esetek sorozatát használja, ahol az egyes teszt-eset az adott interfészt elvárt működésének egy különleges szempontját vizsgálja.

ASTE_IND.1-8 Az értékelőnek végre kell hajtani a tesztelést.

Az értékelő az elkészített tesztdokumentációt alapként használja az STOE tesztelésének végrehajtásához. Bár a végrehajtandó tesztelés alapja a tesztdokumentáció, az értékelő ad hoc is végezhet teszteket. A tesztelés során feltárt STOE viselkedés alapján az értékelő új teszteket is készíthet. Az új teszteket is le kell írni a dokumentációban.

ASTE_IND.1-9 Az értékelőnek jelentésbe kell foglalnia a tesztkészletben szereplő tesztekről az alábbi információkat:

a) a tesztelendő interfész azonosítása;
b) a tesztekhez szükséges berendezések összekapcsolásához és beállításához tartozó utasítások;
c) a teszt előfeltételek kialakítására vonatkozó utasítások;
d) az interfész kiváltására (aktivizálására) vonatkozó utasítások;
e) az interfész működésének megfigyelésére vonatkozó utasítások;
f) az összes elvárt eredmény leírása, valamint a megfigyelt viselkedés és az elvárt eredmények összehasonlításához szükséges elemzések;
g) a tesztek lezárására és az STOE tesztelés utáni állapotának kialakítására vonatkozó utasítások;
h) tényleges teszteredmények.

A leírásnak olyan részletességűnek kell lennie, hogy egy másik értékelő képes legyen megismételni a teszteket és azonos eredményt kapjon. Míg a teszteredmények bizonyos részei eltérhetnek egymástól (pl. naplórekordok dátum és időbejegyzései), az általános eredménynek meg kell egyezni.

Lehetnek olyan esetek, amikor szükségtelen e munkaegységben minden információt megadni (például egy teszt tényleges eredménye nem követeli meg az elemzést, mielőtt az elvárt eredmények összehasonlítása nem történik meg). Ennek eldöntése és a döntés indoklása az értékelő hatásköre.

ASTE_IND.1-10 Az értékelőnek ellenőriznie kell, hogy a tényleges teszteredmények megegyeznek-e az elvárt eredményekkel.

Bármilyen különbözőség az elvárt és tényleges eredmények között az STOE helytelen működését vagy a dokumentáció hibáját jelezheti. A nem várt tényleges eredmény az STOE vagy a tesztdokumentáció javítását, esetleg a tesztek összeállításának módosítását, bizonyos tesztek megismétlését igényelheti. Ennek eldöntése és a döntés indoklása az értékelő hatásköre.

ASTE_IND.1-11 Az értékelőnek az értékelési jelentésben le kell írnia az értékelői tesztelési munkát, áttekintést adva a tesztelési módszerről, konfigurációról, mélységről és eredményekről.

Az értékelési jelentésben rögzített értékelői tesztelésről szóló információ lehetővé teszi az értékelő számára, hogy bemutassa az általános tesztelési módszert és a tesztelésbe fektetett munkát. A cél a tesztelési munka érdemi áttekintése. Nem cél, hogy az értékelési jelentésben a teszteléssel kapcsolatos információk a specifikus tesztlépések vagy egyedi tesztek eredményeinek pontos megismétlése legyenek. A cél elegendő részletesség biztosítása más értékelők számára ahhoz, hogy betekintést kapjanak a választott tesztelési módszerbe, az értékelő által végrehajtott tesztek nagyságrendjébe, a rendszer integrátor által végrehajtott tesztek nagyságrendjébe, az STOE teszt konfigurációjába és a tesztelés általános eredményébe.

Az értékelési jelentés értékelői tesztekről szóló részében általában az alábbi információk találhatók meg:

a) Az STOE teszt konfigurációi. A ténylegesen tesztelt STOE konfigurációk.
b) A megismétlésre kiválasztott tesztelési készlet (minta) nagysága.
c) A mintába kerülő interfészek mennyisége és ennek indoklása, A mintába kerülő interfészek kiválasztásának szempontjai.
d) A függetlenül végrehajtott értékelői tesztek. Ezek mennyisége és a kiválasztásukhoz használt szempontok rövid leírása.
e) A függetlenül tesztelt interfészek.
f) A tevékenység alapján hozott határozat. Az értékelés során végzett tesztelés eredményeinek általános megítélése.

6.2.2.6. A rendszer sebezhetőség felmérés garanciaosztály (ASVA) értékelése

6.2.2.6.1. Sebezhetőség elemzés: ASVA_VAN.1 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) útmutató dokumentációk,
c) a tesztelésre alkalmas STOE,
d) nyilvánosan elérhető információk a lehetséges sebezhetőségek azonosításának támogatására,
e) a lehetséges sebezhetőségekre és támadásokra vonatkozó aktuális, nyilvánosan elérhető információk.

Az ASVA_VAN.1.1E értékelői akció

ASVA_VAN.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASVA_VAN.1.1C Az STOE-nak alkalmasnak kell lennie tesztelésre.

ASVA_VAN.1-1 Az értékelőnek meg kell vizsgálnia az STOE-t annak megállapítása érdekében, hogy az integrált és konfigurált rendszer megfelel-e az SST-ben meghatározott, értékelendő rendszer leírásával (a kiépítés és a konfigurálás szempontjából).

A STOE-t alkotó hardver és szoftver komponensekre az értékelő ellenőrizze, hogy valamennyi komponens konfigurációja ellentmondás mentes-e az SST-vel.

Az értékelő vegye figyelembe azokat az SST-ben leírt, az STOE üzemeltetési környezetére vonatkozó biztonsági célokat, amelyek a rendszer teszt környezetére alkalmazhatók.

Bármilyen tesztelési erőforrás (mérőműszer, elemző készülék) használatakor az értékelő felelőssége annak biztosítása, hogy ezek az erőforrások megfelelően hitelesítve legyenek.

ASVA_VAN.1-2 Az értékelőnek meg kell vizsgálnia az STOE-t annak megállapítása érdekében, hogy a rendszer valamennyi komponensét megfelelően telepítették-e, és ismert állapotban van-e.

Az ASVA_VAN.1.2E értékelői akció

ASVA_VAN.1.2E Az értékelőnek egy keresést kell végrehajtania nyilvános forrásokban az STOE lehetséges sebezhetőségeinek azonosítása érdekében.

ASVA_VAN.1-3 Az értékelőnek tanulmányoznia kell a nyilvánosan rendelkezésre álló információ forrásokat az STOE lehetséges sebezhetőségeinek a meghatározása céljából.

Az értékelő tanulmányozza a nyilvánosan rendelkezésre álló információ forrásokat, amelyek rendelkezésre állnak az STOE lehetséges sebezhetőségei meghatározásainak elősegítéséhez. Sokféle nyilvánosan rendelkezésre álló információ forrás létezik, amelyeket az értékelőnek ajánlatos figyelembe vennie, például a világhálón elérhető, ismert sebezhetőségeket jelentő levelező listákat és biztonsági fórumokat.

Az értékelő ne korlátozza az általa figyelembevett nyilvánosan rendelkezésre álló információkat a fentiekre, hanem vegyen figyelembe bármely egyéb vonatkozó rendelkezésre álló információt.

A nyilvánosan rendelkezésre álló információ keresése célirányosan azokra a forrásokra irányuljon, amelyek az STOE alapját képező komponensekre (termékekre) vonatkoznak.

Az értékelő az átadott bizonyítékok vizsgálata közben használja fel a nyilvános információkat abból a célból, hogy további vizsgálatokat végezzen lehetséges sebezhetőségek felkutatására. Ha az értékelő problémás területeket határozott meg, vegye figyelembe azokat a nyilvánosan rendelkezésre álló információkat, amelyek az adott problémás területre vonatkoznak.

Az olyan információk elérhetősége, amely azonnal rendelkezésre állhat egy támadó számára, s amely elősegíti támadások meghatározását és megkönnyíti a támadások hatékony végrehajtását, jelentősen megnövelheti egy adott támadó támadási lehetőségeit. A sebezhetőségi információk és kifinomult támadó eszközök hozzáférhetősége az Interneten nagyon valószínűvé teszi, hogy ezeket megpróbálják felhasználni az STOE lehetséges sebezhetőségeinek meghatározására és kihasználására. A modern kereső eszközök az ilyen információkat könnyen elérhetővé teszik az értékelő számára, és a publikált lehetséges sebezhetőségekkel, valamint a jól ismert általános támadásokkal szembeni ellenállóképesség költséghatékony módon meghatározható.

A lehetséges sebezhetőségeket tartalmazó nyilvános adatbázisokról lásd [4].

Az értékelőnek jelentést kell készíteni a megvizsgált bizonyítékokról a lehetséges sebezhetőségekre irányuló keresés befejezésekor.

ASVA_VAN.1-4 Az értékelőnek a SER-ben rögzítenie kell a meghatározott lehetséges sebezhetőségeket, amelyek tesztelhetők, és az STOE üzemeltetési környezetében elvileg szóba jöhetnek.

Nem szükséges a lehetséges sebezhetőségek további mérlegelése, ha az értékelő azt állapítja meg, hogy az üzemeltetési környezetben meglévő IT vagy nem-IT intézkedések meggátolják a lehetséges sebezhetőségek kiaknázását az adott üzemeltetési környezetben. Például, ha az STOE-hoz való fizikai hozzáférés kizárólag a jogosult felhasználókra van korlátozva, akkor ez a hamisítás lehetséges sebezhetőségét eredményesen nem kihasználhatóvá teheti.

Az értékelőnek minden okot rögzítenie kell a lehetséges sebezhetőségek további mérlegelésből való kizárására, ha azt állapítja meg, hogy a lehetséges sebezhetőség nem kerülhet szóba az üzemeltetési környezetben. Egyéb esetekben az értékelőnek a lehetséges sebezhetőséget további mérlegelésre rögzítenie kell.

Az értékelőnek a SER-ben meg kell adnia az STOE-val kapcsolatos, annak üzemeltetési környezetében felmerülő lehetséges sebezhetőségek listáját, mely a behatolás tesztelési tevékenység bemeneteként használható.

Az ASVA_VAN.1.3E értékelői akció

ASVA_VAN.1.3E: Az értékelőnek az azonosított lehetséges sebezhetőségek alapján automatikus eszközökkel behatolás tesztelést kell végrehajtania, annak megállapítása érdekében, hogy az STOE ellenáll egy alap támadó képességgel bíró támadó által végrehajtott támadásnak.

ASVA_VAN.1-5 Az értékelőnek ki kell választania behatolás tesztelésre alkalmazandó automatikus eszközt.

Az automatikus eszköz kiválasztásánál az értékelő vegye figyelembe a lehetséges sebezhetőségekre irányuló független keresés eredményeit is.

A behatolás tesztelésre alkalmazható automatikus eszközök áttekintésére lásd [4].

ASVA_VAN.1-6 Az értékelőnek a kiválasztott automatikus eszközzel végre kell hajtania a behatolás tesztelést.

A behatolás tesztelésre alkalmazható automatikus eszközök használatára lásd [4].

ASVA_VAN.1-7 Az értékelőnek rögzítenie kell a behatolás tesztek eredményeit.

Az automatikus eszközök naplóállományokba rögzítik a behatolás tesztek eredményeit.

ASVA_VAN.1-8 Az értékelőnek elemeznie kell az automatikus eszközök által végzett behatolás tesztelés eredményeit.

Az automatikus behatolás tesztelés eredményeiről lásd [4].

ASVA_VAN.1-9 Az értékelőnek az értékelési jelentés keretén belül jelentést kell írnia az értékelői behatolás tesztelésről, leírván a tesztelési módszert, konfigurációt, mélységet és eredményeket.

Az értékelési jelentésben rögzített behatolás tesztelésről szóló információ lehetővé teszi az értékelő számára, hogy bemutassa az általános tesztelési módszert és az ezen tevékenység végrehajtásába fektetett munkát. A cél az értékelő behatolás tesztelési munkájának érdemi áttekintése. Nem cél, hogy az értékelési jelentésben a behatolás teszteléssel kapcsolatos információk a specifikus tesztlépések vagy egyedi behatolás tesztek eredményeinek pontos megismétlése legyenek. A cél elegendő részletesség biztosítása más értékelők számára ahhoz, hogy betekintést kapjanak a választott behatolás tesztelési módszerbe, a végrehajtott behatolás tesztek nagyságrendjébe, az STOE teszt konfigurációjába és a behatolás tesztelési tevékenység általános eredményébe.

Az értékelési jelentés értékelői behatolás tesztelésről szóló része általában az alábbi információkat tartalmazza:

a) STOE tesztkonfigurációk; a behatolás tesztelésnél használt konkrét STOE konfigurációk.
b) A behatolás teszt során tesztelt interfészek. A behatolás tesztelés középpontjában álló interfészek rövid felsorolása.
c) A behatolás tesztelésre felhasznált automatikus eszközök (pontos verziószámmal és beállítási paraméterekkel).
d) Az altevékenység alapján született határozat. A behatolás tesztelés eredményeinek általános megítélése.

ASVA_VAN.1-10 Az értékelőnek meg kell vizsgálnia az összes behatolás teszt eredményét annak megállapítása érdekében, hogy az STOE üzemeltetési környezetében ellenáll-e egy alap támadó képességgel rendelkező támadónak.

Amennyiben az eredmények azt mutatják, hogy az STOE üzemeltetési környezetében kihasználható sebezhetőségeket tartalmaz alap támadó képességgel rendelkező támadók számára, akkor ez az értékelői akció "Nem felelt meg" határozatot eredményez.

[7] 7.3.4 mellékletét kell használni egy adott sebezhetőség kihasználásához szükséges támadó képesség meghatározásához, illetve annak eldöntésére, hogy a sebezhetőség a tervezett üzemeltetési környezetben kihasználható-e. Nem feltétlenül kell minden esetben kiszámolni a támadó képességet, csak ha felmerül annak lehetősége, hogy egy alap támadó képességgel rendelkező támadó kihasználhatja a sebezhetőséget.

ASVA_VAN.1-11 Az értékelőnek az értékelési jelentés keretén belül jelentést kell írnia az összes kihasználható sebezhetőségről és maradvány sebezhetőségről, az alábbi adatokkal:

a) forrás (pl. azon CEM tevékenység, melynek végrehajtása során észlelték, az értékelő ismerte, szakirodalomban olvasott róla);
b) a nem kielégített SFR(-ek);
c) leírás;
d) kihasználható-e vagy sem az üzemeltetési környezetben (vagyis kihasználható vagy maradvány sebezhetőségről van szó);
e) az azonosított sebezhetőség kihasználáshoz szükséges felhasznált idő, szakértelem, TOE ismeret, hozzáférési lehetőség, eszköz, valamint az ezekhez rendelt értékek [7] 7.3.4 mellékletének 7. és 8. táblázata alapján.

6.2.3. Kezdeti rendszer értékelés fokozott garanciacsomag mellett

6.2.3.1. A rendszer biztonsági előirányzat értékelése (ASST)

6.2.3.1.1. Az SST bevezetés (ASST_INT.1) értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.1.1. pont alatt.

6.2.3.1.2. A megfelelőség nyilatkozatok (ASST_CCL.2) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_CCL.2.1E értékelői akció

ASST_CCL.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_CCL.2.1C A megfelelőségi nyilatkozatnak azonosítania kell azt a mértékadó dokumentumot, amelyhez az SST és az STOE megfelelőséget állít.

ASST_CCL.2-1 Az értékelőnek ellenőriznie kell a megfelelőségi nyilatkozatot, hogy az azonosítja-e azt a mértékadó dokumentumot, amelyhez az SST és az STOE megfelelőséget állít.

ASST_CCL.2.2C A megfelelőségi nyilatkozatnak azonosítania kell a mértékadó dokumentum azon követelményeit, amelyekhez az SST és az STOE megfelelőséget állít.

ASST_CCL.2-2 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozatot, hogy az azonosítja-e a mértékadó dokumentum azon követelményeit, amelyekhez az SST és az STOE megfelelőséget állít.

ASST_CCL.2.3C A megfelelőségi nyilatkozatban azonosított mértékadó dokumentumnak az alábbinak kell lennie: [2] (A műszaki biztonsági intézkedések katalógusa).

ASST_CCL.2-3 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozatot, hogy az abban azonosított mértékadó dokumentum az alábbi-e: [2].

ASST_CCL.2.4C A megfelelőségi nyilatkozatnak meg kell határoznia a [2]-ben leírt „fokozott kihatású biztonsági osztály követelményei” biztonsági követelmény csomagra vonatkozó csomag-megfelelőségét: vagy „megfelel a csomagnak” vagy „módosítja a csomagot”.

ASST_CCL.2-4 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozatot, hogy meghatározza-e az alábbiak egyikét: „megfelel a fokozott kihatású biztonsági osztály követelményeinek”, „módosítja a fokozott kihatású biztonsági osztály követelményeit”.

Amennyiben a megfelelőségi nyilatkozat nem határozza meg a ASST_CCL.2-4 alatt említett két lehetőség közül pontosan az egyiket, akkor ez a munkaegység „nem felelt meg” eredményt ad.

ASST_CCL.2.5C Amennyiben a csomag-megfelelőségre vonatkozó nyilatkozat: „módosítja a fokozott kihatású biztonsági osztály követelményeit”, akkor a megfelelőségi nyilatkozat indoklásnak vissza kell vezetnie minden biztonsági követelményt az STOE biztonsági céljaira.

ASST_CCL.2-5 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozatot, hogy amennyiben a meghatározás: „módosítja a fokozott kihatású biztonsági osztály követelményeit”, akkor a megfelelőségi nyilatkozat indoklás visszavezet-e minden biztonsági követelményt az STOE biztonsági céljaira.

Ha a megfelelőségi nyilatkozat „megfelel a fokozott kihatású biztonsági osztály követelményeinek” meghatározás mellett, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

6.2.3.1.3. A biztonsági probléma meghatározás (ASST_SPD.1) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_SPD.1.1E értékelői akció

ASST_SPD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SPD.1.1C A biztonsági probléma meghatározásnak le kell írnia a fenyegetéseket.

ASST_SPD.1-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági probléma meghatározás leírja-e a fenyegetéseket.

Amennyiben minden biztonsági cél csupán a feltételezésekből és a szervezeti biztonsági szabályokból levezethető, akkor a fenyegetésekről szóló nyilatkozatnak nem kell szerepelnie az SST-ben. Ekkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

Az értékelő állapítsa meg, hogy a biztonsági probléma meghatározás leírja-e az STOE és/vagy üzemeltetési környezete által kivédendő fenyegetéseket.

ASST_SPD.1.2C Minden fenyegetést le kell írni a támadó, a támadás tárgyát képező vagyon és a támadó tevékenység szerint.

ASST_SPD.1-2 Az értékelőnek meg kell vizsgálnia a biztonsági probléma meghatározást, hogy az leírja-e a fenyegetéseket a támadó, a támadás tárgyát képező vagyon és a támadó tevékenység szerint.

Amennyiben minden biztonsági cél csupán a feltételezésekből és a szervezeti biztonsági szabályokból levezethető, akkor a fenyegetésekről szóló nyilatkozatnak nem kell szerepelnie az SST-ben. Ekkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

A támadók tovább jellemezhetők a szakértelem, az erőforrás, a lehetőség és a motiváció alapján.

ASST_SPD.1.3C A biztonsági probléma meghatározásnak le kell írnia a szervezeti biztonsági szabályokat.

ASST_SPD.1-3 Az értékelőnek ellenőriznie kell, hogy a biztonsági probléma meghatározás leírja-e a szervezeti biztonsági szabályokat.

Amennyiben minden biztonsági cél csupán a feltételezésekből és a fenyegetésekből levezethető, akkor a szervezeti biztonsági szabályoknak nem kell szerepelnie az SST-ben. Ekkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

Az értékelő állapítsa meg, hogy a szervezeti biztonsági szabályokra vonatkozó nyilatkozatokat az STOE és/vagy annak üzemeltetési környezete által követendő szabályok vagy útmutatók szerint fogalmazták-e meg.

Az értékelő állapítsa meg, hogy minden szervezeti biztonsági szabályt megfelelő részletességgel megmagyaráztak és/vagy értelmeztek ahhoz, hogy érthetőek legyenek. A szabályok világos leírása szükséges ahhoz, hogy a biztonsági célokat vissza lehessen vezetni rájuk.

ASST_SPD.1.4C A biztonsági probléma meghatározásnak le kell írnia az STOE üzemeltetési környezetére vonatkozó feltételezéseket.

ASST_SPD.1-4 Az értékelőnek meg kell vizsgálnia a biztonsági probléma meghatározást annak megállapítása érdekében, hogy az leírja-e az STOE üzemeltetési környezetére vonatkozó feltételezéseket.

Amennyiben nincsenek feltételezések, ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

Az értékelő állapítsa meg, hogy az STOE üzemeltetési környezetére vonatkozó minden feltételezést kellő részletességgel megmagyaráztak ahhoz, hogy a vásárlók ebből meg tudják állapítani, vajon az ő üzemeltetési környezetük megfelel-e a feltételezésnek. Amennyiben a feltételezések nem eléggé világosak, akkor az STOE olyan üzemeltetési környezetben is alkalmazható, amelyben nem biztonságos módon működik.

6.2.3.1.4. A biztonsági célok (ASST_OBJ.2) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_OBJ.2.1E értékelői akció

ASST_OBJ.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_OBJ.2.1C A biztonsági célokról szóló nyilatkozatnak le kell írnia az STOE-re vonatkozó biztonsági célokat, valamint az üzemeltetési környezetre vonatkozó biztonsági célokat.

ASST_OBJ.2-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági célokról szóló nyilatkozat megadja-e az STOE-re, valamint az üzemeltetési környezetre vonatkozó biztonsági célokat.

Az értékelő ellenőrizze, hogy a biztonsági célok mindkét kategóriáját egyértelműen azonosították-e, illetve hogy megkülönböztették-e ezeket egymástól.

ASST_OBJ.2.2C A biztonsági célok indoklásának minden STOE-re vonatkozó biztonsági célt vissza kell vezetnie az adott biztonsági cél által kivédett fenyegetésekre, valamint az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra.

ASST_OBJ.2-2 Az értékelőnek ellenőriznie kell, hogy a biztonsági célok indoklása minden STOE-re vonatkozó biztonsági célt visszavezet-e a biztonsági célok által kivédett fenyegetésekre, valamint a biztonsági célok által érvényre juttatott szervezeti biztonsági szabályzatokra.

Minden STOE-re vonatkozó biztonsági cél visszavezethető a fenyegetésekre, a szervezeti biztonsági szabályokra vagy ezek kombinációjára, de legalább egy fenyegetésre vagy szervezeti biztonsági szabályra való visszavezetés kötelező.

A visszavezethetőség sikertelensége egyaránt jelezheti a biztonsági célok indoklásának hiányosságát, a biztonsági probléma meghatározás hiányosságát, vagy azt, hogy egy STOE-re vonatkozó biztonsági célnak nincs valódi rendeltetése.

ASST_OBJ.2.3C A biztonsági célok indoklásának minden üzemeltetési környezetre vonatkozó biztonsági célt vissza kell vezetnie az adott biztonsági cél által kivédett fenyegetésekre, az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra, valamint az adott biztonsági cél által támasztott feltételezésekre.

ASST_OBJ.2-3 Az értékelőnek ellenőriznie kell, hogy a biztonsági célok indoklása minden üzemeltetési környezetre vonatkozó biztonsági célt visszavezet-e az adott biztonsági cél által kivédett fenyegetésekre, az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra, valamint az adott biztonsági cél által támasztott feltételezésekre.

Minden üzemeltetési környezetre vonatkozó biztonsági cél visszavezethető a fenyegetésekre, a szervezeti biztonsági szabályokra, a feltételezésekre, vagy ezek valamely kombinációjára, de legalább egy fenyegetésre, szervezeti biztonsági szabályra vagy feltételezésre való visszavezetés kötelező.

A visszavezethetőség sikertelensége egyaránt jelezheti a biztonsági célok indoklásának hiányosságát, a biztonsági probléma meghatározás hiányosságát, vagy azt, hogy egy üzemeltetési környezetre vonatkozó biztonsági célnak nincs valódi rendeltetése.

ASST_OBJ.2.4C A biztonsági célok indokolásának szemléltetnie kell, hogy a biztonsági célok lefednek minden fenyegetést.

ASST_OBJ.2-4 Az értékelőnek meg kell vizsgálnia a biztonsági célok indoklását annak megállapítása érdekében, hogy minden egyes fenyegetésre tartalmaz-e megfelelő igazolást arra nézve, hogy a biztonsági célok alkalmasak az adott fenyegetés elhárítására.
Amennyiben nincs fenyegetésre visszavezethető biztonsági cél, e munkaegység „Nem felelt meg” eredményt ad.

Az értékelő állapítsa meg, hogy egy fenyegetésre vonatkozó indoklás megmutatja-e azt, hogy a fenyegetést elhárították, csökkentették, vagy következményeit csillapították.

Az értékelő állapítsa meg, hogy egy fenyegetésre vonatkozó indoklás szemlélteti-e a biztonsági célok elégségességét: ha egy fenyegetésre visszavezetett összes biztonsági cél teljesül, akkor az adott fenyegetést elhárították, elfogadható szintre csökkentették, vagy a fenyegetés következményeit kielégítő módon csillapították.

Megjegyzendő, hogy a biztonsági célok visszavezetése a fenyegetésekre (a biztonsági célok indoklásában) része lehet az igazolásnak, de önmagában nem képez igazolást. Még abban az esetben is szükség van igazolásra, amikor egy biztonsági cél csupán azt mondja ki, hogy egy adott fenyegetés bekövetkezését kívánja megakadályozni, de ekkor az igazolás olyan rövid lehet, mint „az X biztonsági cél közvetlenül kivédi az Y fenyegetést”.

Az értékelő azt is állapítsa meg, hogy egy fenyegetésre visszavezetett összes biztonsági cél szükséges: ha a biztonsági cél teljesül, akkor az ténylegesen hozzájárul az adott fenyegetés elhárításához, csökkentéséhez vagy a következmények csillapításához.

ASST_OBJ.2.5C A biztonsági célok indokolásának szemléltetnie kell, hogy a biztonsági célok érvényre juttatják az összes szervezeti biztonsági szabályzatot.

ASST_OBJ.2-5 Az értékelőnek meg kell vizsgálnia a biztonsági célok indoklását annak megállapítása érdekében, hogy minden szervezeti biztonsági szabályra tartalmaz-e megfelelő igazolást arra, hogy a biztonsági célok alkalmasak az adott szervezeti biztonsági szabály érvényre juttatására.

Amennyiben nincsenek a szervezeti biztonsági szabályokra visszavezethető biztonsági célok, e munkaegység „Nem felelt meg” eredményt ad.

Az értékelő állapítsa meg, hogy egy szervezeti biztonsági szabályra vonatkozó indoklás szemlélteti-e a biztonsági célok elégségességét: ha egy adott szervezeti biztonsági szabályra visszavezetett összes biztonsági cél teljesül, akkor az adott szervezeti biztonsági szabály érvényre jut.

Az értékelő azt is állapítsa meg, hogy egy szervezeti biztonsági szabályra vonatkozó összes biztonsági cél szükséges: ha a biztonsági cél teljesül, akkor az ténylegesen hozzájárul az adott szervezeti biztonsági szabály érvényre juttatásához.

Megjegyzendő, hogy a biztonsági célok visszavezetése a szervezeti biztonsági szabályokra (a biztonsági célok indoklásában) része lehet az igazolásnak, de önmagában nem képez igazolást. Még abban az esetben is szükség van igazolásra, amikor egy biztonsági cél csupán azt mondja ki, hogy egy adott szervezeti biztonsági szabály érvényre jutását kívánja elérni, de ekkor az igazolás olyan rövid lehet, mint „az X biztonsági cél közvetlenül érvényre juttatja az Y szervezeti biztonsági szabályt”.

ASST_OBJ.2.6C A biztonsági célok indokolásának szemléltetnie kell, hogy az üzemeltetési környezetre vonatkozó biztonsági célok az összes feltételezést igénylik.

ASST_OBJ.2-6 Az értékelőnek meg kell vizsgálnia a biztonsági célok indoklását annak megállapítása érdekében, hogy minden üzemeltetési környezetre vonatkozó feltételezésre tartalmaz-e megfelelő igazolást arra, hogy az üzemeltetési környezetre vonatkozó biztonsági célok alkalmasak az adott feltételezés alátámasztására.

Amennyiben nincsenek a feltételezésre visszavezethető, üzemeltetési környezetre vonatkozó biztonsági célok, e munkaegység „nem felelt meg” eredményt ad.

Az értékelő állapítsa meg, hogy egy az STOE üzemeltetési környezetével kapcsolatos feltételezésre vonatkozó indoklás szemlélteti-e a biztonsági célok elégségességét: ha egy adott feltételezésre visszavezetett összes üzemeltetési környezetre vonatkozó biztonsági cél teljesül, akkor az üzemeltetési környezet alátámasztja az adott feltételezést.

Az értékelő azt is állapítsa meg, hogy egy feltételezésre visszavezetett, az STOE üzemeltetési környezetére vonatkozó összes biztonsági cél szükséges: ha a biztonsági cél teljesül, akkor az ténylegesen hozzájárul ahhoz, hogy az üzemeltetési környezet az adott feltételezést alátámassza.

Megjegyzendő, hogy az üzemeltetési környezetre vonatkozó biztonsági célok visszavezetése a feltételezésekre (a biztonsági célok indoklásában) része lehet az igazolásnak, de önmagában nem képez igazolást. Még abban az esetben is szükség van igazolásra, amikor egy üzemeltetési környezetre vonatkozó biztonsági cél csupán megismétlése egy feltételezésnek, de ekkor az igazolás olyan rövid lehet, mint „az X biztonsági cél közvetlenül alátámasztja az Y feltételezést”.

6.2.3.1.5. A biztonsági követelmények (ASST_REQ.2) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_REQ.2.1E értékelői akció

ASST_REQ.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_REQ.2.1C A biztonsági követelményekre vonatkozó állításnak le kell írnia a rendszertől elvárt biztonsági funkcionalitást (SSF) és garanciákat (SAP).

ASST_REQ.2-1 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot annak megállapítása érdekében, hogy az leírja-e az elvárt rendszer biztonsági funkcionalitást (SSF).

ASST_REQ.2-2 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot annak megállapítása érdekében, hogy az leírja-e az elvárt garanciákat (SAP).

ASST_REQ.2.2C Az elvárt rendszer biztonsági funkcionalitást az alábbi mértékadó dokumentumból kell választani: [2] műszaki biztonsági intézkedések katalógusa.

ASST_REQ.2-3 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot, hogy az abban azonosított mértékadó dokumentum az alábbi-e: [2].

ASST_REQ.2.3C Az elvárt rendszer garanciacsomagnak az alábbiak egyikének kell lennie: SAP-F vagy megemelt SAP-F.

ASST_REQ.2-4 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot, hogy az abban azonosított garanciacsomag az alábbiak egyike-e: SAP-F vagy megemelt SAP-F.

ASST_REQ.2.4C A biztonsági követelményekről szóló nyilatkozatnak azonosítania kell a biztonsági követelményekre vonatkozó összes műveletet.

ASST_REQ.2-5 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az azonosítja-e a funkcionális biztonsági követelményekre vonatkozó összes műveletet.

Az értékelő állapítsa meg, hogy minden SFR-ben lévő minden műveletet azonosítottak, ahol használtak ilyet. Az azonosítás elérhető tipográfiai megkülönböztetéssel, vagy explicit azonosítással a környező szöveghez képest, vagy bármilyen más megkülönböztető eszközzel.

ASST_REQ.2.5C Minden értékadási és kiválasztási műveletet be kell fejezni.

ASST_REQ.2-6 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az befejezett-e minden értékadási műveletet.

ASST_REQ.2-7 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az befejezett-e minden kiválasztási műveletet.

ASST_REQ.2.6C Minden műveletet jól kell végrehajtani.

ASST_REQ.2-8 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az minden műveletet helyesen hajt-e végre..

ASST_REQ.2.7C A biztonsági követelmények indoklásának az SSF-et vissza kell vezetnie az STOE biztonsági céljaira.

ASST_REQ.2-9 Az értékelőnek ellenőriznie kell, hogy a biztonság követelmények indoklása visszavezet-e minden SFR-t az STOE biztonsági céljaira.

Az értékelő állapítsa meg, hogy minden egyes SFR visszavezethető legalább egy STOE biztonsági célra.

A visszavezetés sikertelensége vagy azt jelenti, hogy a biztonsági követelmények indoklása nem teljes, az STOE biztonsági céljai nem teljesek, vagy az SFR nem tölt be igazi célt.

ASST_REQ.2.8C A biztonsági követelmények indoklásának meg kell mutatnia, hogy az SSF teljesíti az STOE összes biztonsági célját, amelyeket külső rendszerek nem elégítenek ki.

ASST_REQ.2-10 Az értékelőnek meg kell vizsgálnia a biztonsági követelmények indoklását annak megállapítása érdekében, hogy az STOE összes biztonsági céljára megmutatták, hogy az SFR-k alkalmasak az adott STOE biztonsági cél teljesítésére, vagy az adott biztonsági célt külső rendszerek elégítik ki.

Amennyiben az SFR-ek nem vezethetők vissza az STOE biztonsági céljaira, az e munkaegységhez kapcsolódó értékelői tevékenység során „nem felelt meg” döntés születik.

Az értékelő állapítsa meg, hogy az STOE biztonsági céljainak indoklása megmutatja-e, hogy az SFR-ek kielégítők: azaz, ha a célra visszavezethető minden SFR-t kielégítenek, akkor az STOE biztonsági cél teljesül.

Az értékelő azt is állapítsa meg, hogy egy STOE biztonsági célra visszavezethető összes SFR szükséges: azaz az SFR teljesülése ténylegesen hozzájárul a biztonsági cél eléréséhez.

Az ASST_REQ.2.2E értékelői akció

ASST_REQ.2.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági követelményekről szóló nyilatkozat belső ellentmondásoktól mentes.

ASST_REQ.2-11 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy az belső ellentmondásoktól mentes.

Az értékelő állapítsa meg, hogy az SSF és SAP kombinációja belső ellentmondásoktól mentes.

Néhány lehetséges ellentmondás:

a) SSF egyetlen mértékadó dokumentumokból került kiválasztásra, de a kiválasztott SFR-ek ellentmondanak egymásnak;
b) SSF több mértékadó dokumentumokból került kiválasztásra és a kiválasztott SFR-ek ellentmondanak egymásnak.

Az ASST_REQ.2.3E értékelői akció

ASST_REQ.2.3E Az értékelőnek meg kell erősítenie, hogy a biztonsági követelményekről szóló nyilatkozat egy teljes, egymást erősítő követelményrendszert határoz meg.

ASST_REQ.2-12 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy az egy teljes, egymást erősítő követelményrendszert határoz-e meg.

6.2.3.1.6. Az STOE összefoglaló előírás (ASST_SSS.1) értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.1.6. pont alatt.

6.2.3.1.7. A biztonsági tartomány bevezetés (ASST_SDI.1) értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.1.7 pont alatt.

6.2.3.1.8. A biztonsági tartomány megfelelőségi nyilatkozatok (ASST_SDC.2) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_SDC.2.1E értékelői akció

ASST_SDC.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDC.2.1C A biztonsági tartomány megfelelőségi nyilatkozatnak azonosítania kell azt a mértékadó dokumentumot, amelyhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.2-1 Az értékelőnek ellenőriznie kell a biztonsági tartomány megfelelőségi nyilatkozatot, hogy az azonosítja-e azt a mértékadó dokumentumot, amelyhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.2.2C A biztonsági tartomány megfelelőségi nyilatkozatnak azonosítania kell a mértékadó dokumentum azon követelményeit, amelyekhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.2-2 Az értékelőnek ellenőriznie kell a biztonsági tartomány megfelelőségi nyilatkozatot, hogy az azonosítja-e a mértékadó dokumentum azon követelményeit, amelyekhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.2.3C A biztonsági tartomány megfelelőségi nyilatkozatban azonosított mértékadó dokumentumnak az alábbinak kell lennie: [2] (A műszaki biztonsági intézkedések katalógusa).

ASST_SDC.2-3 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány megfelelőségi nyilatkozatot, hogy az abban azonosított mértékadó dokumentum az alábbi-e: [2].

ASST_SDC.2.4C Hazai katalógusnak [2] való megfelelőség vállalása esetén a biztonsági tartomány megfelelőségi nyilatkozatnak meg kell határoznia a [2]-ben leírt „kiemelt kihatású biztonsági osztály követelményei” biztonsági követelmény csomagra vonatkozó csomag-megfelelőségét: vagy „megfelel a csomagnak” vagy „módosítja a csomagot”.

ASST_SDC.2-4 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány megfelelőségi nyilatkozatot, hogy az [2]-nek való megfelelőség vállalása esetén meghatározza-e az alábbiak egyikét: „megfelel a kiemelt kihatású biztonsági osztály követelményeinek”, „módosítja a kiemelt kihatású biztonsági osztály követelményeit”.

Ha a biztonsági tartomány megfelelőségi nyilatkozat [1]-nek vállal megfelelőséget, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Amennyiben a biztonsági tartomány megfelelőségi nyilatkozat [2]-nek vállal megfelelőséget, de nem határozza meg a ASST_SDC.2-4 alatt említett két lehetőség közül pontosan az egyiket, akkor ez a munkaegység „nem felelt meg” eredményt ad.

ASST_SDC.2.5C Amennyiben a csomag-megfelelőségre vonatkozó nyilatkozat: „módosítja a fokozott kihatású biztonsági osztály követelményeit” akkor a biztonsági tartomány megfelelőségi nyilatkozat indoklásnak vissza kell vezetnie a biztonsági tartomány minden biztonsági követelményét a biztonsági tartomány biztonsági céljaira.

ASST_SDC.2-5 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány megfelelőségi nyilatkozatot, hogy amennyiben az a [2]-nek való megfelelőséget vállalja, „módosítja a fokozott kihatású biztonsági osztály követelményeit” meghatározás mellett, akkor a biztonsági tartomány megfelelőségi nyilatkozat indoklás visszavezet-e minden biztonsági követelményt a biztonsági tartomány biztonsági céljaira.

Ha a biztonsági tartomány megfelelőségi nyilatkozat „megfelel a fokozott kihatású biztonsági osztály követelményeinek” meghatározás mellett, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

6.2.3.1.9. A biztonsági tartomány biztonsági probléma meghatározás (ASST_SDP.1) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_SDP.1.1E értékelői akció

ASST_SDP.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDP.1.1C A biztonsági tartomány biztonsági probléma meghatározásnak le kell írnia az adott biztonsági tartományra irányuló fenyegetéseket.

ASST_SDP.1-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány biztonsági probléma meghatározás leírja-e a az adott biztonsági tartományra irányuló fenyegetéseket.

Amennyiben minden biztonsági cél csupán a feltételezésekből és a szervezeti biztonsági szabályokból levezethető, akkor a fenyegetéseknek nem kell szerepelniük a biztonsági tartomány biztonsági probléma meghatározásban. Ekkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

Az értékelő állapítsa meg, hogy a biztonsági tartomány biztonsági probléma meghatározás leírja-e az STOE és/vagy a biztonsági tartomány üzemeltetési környezete által kivédendő fenyegetéseket.

ASST_SDP.1.2C Minden fenyegetést le kell írni a támadó, a támadás tárgyát képező vagyon és a támadó tevékenység szerint.

ASST_SDP.1-2 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági probléma meghatározást, hogy az leírja-e a fenyegetéseket a támadó, a támadás tárgyát képező vagyon és a támadó tevékenység szerint.

Amennyiben minden biztonsági cél csupán a feltételezésekből és a szervezeti biztonsági szabályokból levezethető, akkor a fenyegetéseknek nem kell szerepelniük a biztonsági tartomány biztonsági probléma meghatározásban. Ekkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

A támadók tovább jellemezhetők a szakértelem, az erőforrás, a lehetőség és a motiváció alapján.

ASST_SDP.1.3C A biztonsági tartomány biztonsági probléma meghatározásnak le kell írnia a szervezeti biztonsági szabályokat.

ASST_SDP.1-3 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány biztonsági probléma meghatározás leírja-e a szervezeti biztonsági szabályokat.

Amennyiben minden biztonsági cél csupán a feltételezésekből és a fenyegetésekből levezethető, akkor a szervezeti biztonsági szabályoknak nem kell szerepelnie a biztonsági tartomány biztonsági probléma meghatározásban. Ekkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

Az értékelő állapítsa meg, hogy a szervezeti biztonsági szabályokra vonatkozó nyilatkozatokat a biztonsági tartomány és/vagy annak üzemeltetési környezete által követendő szabályok vagy útmutatók szerint fogalmazták-e meg.

Az értékelő állapítsa meg, hogy minden szervezeti biztonsági szabályt megfelelő részletességgel megmagyaráztak és/vagy értelmeztek ahhoz, hogy érthetőek legyenek. A szabályok világos leírása szükséges ahhoz, hogy a biztonsági célokat vissza lehessen vezetni rájuk.

ASST_SDP.1.4C A biztonsági tartomány biztonsági probléma meghatározásnak le kell írnia a biztonsági tartomány üzemeltetési környezetére vonatkozó feltételezéseket.

ASST_SDP.1-4 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági probléma meghatározást annak megállapítása érdekében, hogy az leírja-e a biztonsági tartomány üzemeltetési környezetére vonatkozó feltételezéseket.

Amennyiben nincsenek feltételezések, ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekintendő.

Az értékelő állapítsa meg, hogy a biztonsági tartomány üzemeltetési környezetére vonatkozó minden feltételezést kellő részletességgel megmagyaráztak ahhoz, hogy a vásárlók ebből meg tudják állapítani, vajon az ő üzemeltetési környezetük megfelel-e a feltételezésnek. Amennyiben a feltételezések nem eléggé világosak, akkor az STOE olyan üzemeltetési környezetben is alkalmazható, amelyben nem biztonságos módon működik.

6.2.3.1.10. A biztonsági tartomány biztonsági célok (ASST_SDO.2) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_SDO.2.1E értékelői akció

ASST_SDO.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDO.2.1C A biztonsági tartomány biztonsági célokról szóló nyilatkozatnak le kell írnia a biztonsági tartományra vonatkozó biztonsági célokat, valamint a biztonsági tartomány üzemeltetési környezetre vonatkozó biztonsági célokat.

ASST_SDO.2-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány biztonsági célokról szóló nyilatkozat megadja-e a biztonsági tartományra, valamint a biztonsági tartomány üzemeltetési környezetre vonatkozó biztonsági célokat.

Az értékelő ellenőrizze, hogy a biztonsági tartomány biztonsági célok mindkét kategóriáját egyértelműen azonosították-e, illetve hogy megkülönböztették-e ezeket egymástól.

ASST_SDO.2.2C A biztonsági tartomány biztonsági célok indoklásának minden biztonsági tartományra vonatkozó biztonsági célt vissza kell vezetnie az adott biztonsági cél által kivédett fenyegetésekre, valamint az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra.

ASST_SDO.2-2 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány biztonsági célok indoklása minden biztonsági tartományra vonatkozó biztonsági célt visszavezet-e a biztonsági célok által kivédett fenyegetésekre, valamint a biztonsági célok által érvényre juttatott szervezeti biztonsági szabályzatokra.

Minden biztonsági tartományra vonatkozó biztonsági cél visszavezethető a fenyegetésekre, a szervezeti biztonsági szabályokra vagy ezek kombinációjára, de legalább egy fenyegetésre vagy szervezeti biztonsági szabályra való visszavezetés kötelező.

A visszavezethetőség sikertelensége egyaránt jelezheti a biztonsági célok indoklásának hiányosságát, a biztonsági probléma meghatározás hiányosságát, vagy azt, hogy egy biztonsági tartományra vonatkozó biztonsági célnak nincs valódi rendeltetése.

ASST_SDO.2.3C A biztonsági célok indoklásának az adott biztonsági tartomány üzemeltetési környezetére vonatkozó minden biztonsági célt vissza kell vezetnie az adott biztonsági cél által kivédett fenyegetésekre, az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra, valamint az adott biztonsági cél által támasztott feltételezésekre.

ASST_SDO.2-3 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány biztonsági célok indoklása minden az adott biztonsági tartomány üzemeltetési környezetére vonatkozó biztonsági célt visszavezet-e az adott biztonsági cél által kivédett fenyegetésekre, az adott biztonsági cél által érvényre juttatott szervezeti biztonsági szabályzatokra, valamint az adott biztonsági cél által támasztott feltételezésekre.

Az adott biztonsági tartomány minden üzemeltetési környezetére vonatkozó biztonsági cél visszavezethető a fenyegetésekre, a szervezeti biztonsági szabályokra, a feltételezésekre, vagy ezek valamely kombinációjára, de legalább egy fenyegetésre, szervezeti biztonsági szabályra vagy feltételezésre való visszavezetés kötelező.

A visszavezethetőség sikertelensége egyaránt jelezheti a biztonsági tartomány biztonsági célok indoklásának hiányosságát, a biztonsági tartomány biztonsági probléma meghatározás hiányosságát, vagy azt, hogy egy az adott biztonsági tartomány üzemeltetési környezetére vonatkozó biztonsági célnak nincs valódi rendeltetése.

ASST_SDO.2.4C A biztonsági tartomány biztonsági célok indokolásának szemléltetnie kell, hogy a biztonsági célok lefednek minden fenyegetést.

ASST_SDO.2-4 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági célok indoklását annak megállapítása érdekében, hogy minden egyes fenyegetésre tartalmaz-e

megfelelő igazolást arra nézve, hogy a biztonsági célok alkalmasak az adott fenyegetés elhárítására.

Amennyiben nincs fenyegetésre visszavezethető biztonsági cél, e munkaegység „nem felelt meg” eredményt ad.

Az értékelő állapítsa meg, hogy egy fenyegetésre vonatkozó indoklás megmutatja-e azt, hogy a fenyegetést elhárították, csökkentették, vagy következményeit csillapították.

Az értékelő állapítsa meg, hogy egy fenyegetésre vonatkozó indoklás szemlélteti-e a biztonsági célok elégségességét: ha egy fenyegetésre visszavezetett összes biztonsági cél teljesül, akkor az adott fenyegetést elhárították, elfogadható szintre csökkentették, vagy a fenyegetés következményeit kielégítő módon csillapították.

Az értékelő azt is állapítsa meg, hogy egy fenyegetésre visszavezetett összes biztonsági cél szükséges: ha a biztonsági cél teljesül, akkor az ténylegesen hozzájárul az adott fenyegetés elhárításához, csökkentéséhez vagy a következmények csillapításához.

ASST_SDO.2.5C A biztonsági tartomány biztonsági célok indokolásának szemléltetnie kell, hogy a biztonsági célok érvényre juttatják az összes szervezeti biztonsági szabályzatot.

ASST_SDO.2-5 Az értékelőnek meg kell vizsgálnia a biztonsági célok indoklását annak megállapítása érdekében, hogy minden szervezeti biztonsági szabályra tartalmaz-e megfelelő igazolást arra, hogy a biztonsági célok alkalmasak az adott szervezeti biztonsági szabály érvényre juttatására.

Amennyiben nincsenek a szervezeti biztonsági szabályokra visszavezethető biztonsági célok, e munkaegység „Nem felelt meg” eredményt ad.

Az értékelő állapítsa meg, hogy egy szervezeti biztonsági szabályra vonatkozó indoklás szemlélteti-e a biztonsági célok elégségességét: ha egy adott szervezeti biztonsági szabályra visszavezetett összes biztonsági cél teljesül, akkor az adott szervezeti biztonsági szabály érvényre jut.

Az értékelő azt is állapítsa meg, hogy egy szervezeti biztonsági szabályra vonatkozó összes biztonsági cél szükséges: ha a biztonsági cél teljesül, akkor az ténylegesen hozzájárul az adott szervezeti biztonsági szabály érvényre juttatásához.

ASST_SDO.2.6C A biztonsági tartomány biztonsági célok indokolásának szemléltetnie kell, hogy az adott biztonsági tartomány üzemeltetési környezetére vonatkozó biztonsági célok az összes feltételezést igénylik.

ASST_SDO.2-6 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági célok indoklását annak megállapítása érdekében, hogy az adott biztonsági tartomány minden üzemeltetési környezetére vonatkozó feltételezésre tartalmaz-e megfelelő igazolást arra, hogy az üzemeltetési környezetre vonatkozó biztonsági célok alkalmasak az adott feltételezés alátámasztására.

Amennyiben nincsenek a feltételezésre visszavezethető, üzemeltetési környezetre vonatkozó biztonsági célok, e munkaegység „nem felelt meg” eredményt ad.

Az értékelő állapítsa meg, hogy egy az adott biztonsági tartomány üzemeltetési környezetével kapcsolatos feltételezésre vonatkozó indoklás szemlélteti-e a biztonsági célok elégségességét: ha egy adott feltételezésre visszavezetett összes üzemeltetési környezetre vonatkozó biztonsági cél teljesül, akkor az üzemeltetési környezet alátámasztja az adott feltételezést.

Az értékelő azt is állapítsa meg, hogy egy feltételezésre visszavezetett, az adott biztonsági tartomány üzemeltetési környezetére vonatkozó összes biztonsági cél szükséges: ha a biztonsági cél teljesül, akkor az ténylegesen hozzájárul ahhoz, hogy az üzemeltetési környezet az adott feltételezést alátámassza.

6.2.3.1.11. A biztonsági tartomány biztonsági követelmények (ASST_SDR.2) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_SDR.2.1E értékelői akció

ASST_SDR.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDR.2.1C A biztonsági tartomány biztonsági követelményekre vonatkozó állításnak le kell írnia az adott biztonsági tartományra elvárt biztonsági funkcionalitást (SF) és az elvárt rendszer garanciákat (SAP).

ASST_SDR.2-1 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot annak megállapítása érdekében, hogy az leírja-e az adott biztonsági tartományra elvárt biztonsági funkcionalitást (SF).

ASST_SDR.2-2 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot annak megállapítása érdekében, hogy az leírja-e az elvárt garanciákat (SAP).

ASST_SDR.2.2C Az elvárt biztonsági funkcionalitást az alábbi mértékadó dokumentumból kell választani: [2] műszaki biztonsági intézkedések katalógusa).

.

ASST_SDR.2-3 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, hogy az abban azonosított mértékadó dokumentum az alábbi-e: [2].

ASST_SDR.2.3C Az elvárt rendszer garanciacsomagnak az alábbiak egyikének kell lennie: SAP-**F** vagy megemelt SAP-**F**.

ASST_SDR.2-4 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, hogy az abban azonosított garanciacsomag az alábbiak egyike-e: SAP-**F** vagy megemelt SAP-**F.**

ASST_SDR.2.4C A biztonsági tartomány biztonsági követelményekről szóló nyilatkozatnak azonosítania kell a biztonsági követelményekre vonatkozó összes műveletet.

ASST_SDR.2-5 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, hogy az abban azonosított garanciacsomag az alábbiak egyike-e: SAP-F vagy megemelt SAP-F.

ASST_SDR.2.5C A biztonsági tartomány biztonsági követelményekről szóló nyilatkozatnak azonosítania kell a biztonsági követelményekre vonatkozó összes műveletet.

ASST_SDR.2-6 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az azonosítja-e a funkcionális biztonsági követelményekre vonatkozó összes műveletet.

Az értékelő állapítsa meg, hogy minden SFR-ben lévő minden műveletet azonosítottak, ahol használtak ilyet. Az azonosítás elérhető tipográfiai megkülönböztetéssel, vagy explicit azonosítással a környező szöveghez képest, vagy bármilyen más megkülönböztető eszközzel.

ASST_SDR.2.6C Minden értékadási és kiválasztási műveletet be kell fejezni.

ASST_SDR.2-7 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az befejezett-e minden értékadási műveletet.

ASST_SDR.2-8 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az befejezett-e minden kiválasztási műveletet.

ASST_SDR.2.7C Minden műveletet jól kell végrehajtani.

ASST_SDR.2-9 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az minden műveletet helyesen hajt-e végre..

ASST_SDR.2.8C A biztonsági tartomány biztonsági követelmények indoklásának az SF-et vissza kell vezetnie az adott biztonsági tartomány biztonsági céljaira.

ASST_SDR.2-10 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány biztonság követelmények indoklása visszavezet-e minden SFR-t az adott biztonsági tartomány biztonsági céljaira.

Az értékelő állapítsa meg, hogy minden egyes SFR visszavezethető az adott biztonsági tartomány legalább egy biztonsági céljára.

A visszavezetés sikertelensége vagy azt jelenti, hogy a biztonsági tartomány biztonsági követelmények indoklása nem teljes, a biztonsági tartomány biztonsági céljai nem teljesek, vagy az SFR nem tölt be igazi célt.

ASST_SDR.2.9C A biztonsági tartomány biztonsági követelmények indoklásának meg kell mutatnia, hogy az SSF teljesíti az STOE összes biztonsági célját, amelyeket külső rendszerek nem elégítenek ki.

ASST_SDR.2-11 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelmények indoklását annak megállapítása érdekében, hogy az adott biztonsági tartomány összes biztonsági céljára megmutatták, hogy az SFR-k alkalmasak az adott biztonsági tartomány biztonsági céljának a teljesítésére, vagy az adott biztonsági célt külső rendszerek elégítik ki.

Amennyiben az SFR-ek nem vezethetők vissza az adott biztonsági tartomány biztonsági céljaira, az e munkaegységhez kapcsolódó értékelői tevékenység során „nem felelt meg” döntés születik.

Az értékelő állapítsa meg, hogy a biztonsági tartomány biztonsági céljainak indoklása megmutatja-e, hogy az SFR-ek kielégítők: azaz, ha a célra visszavezethető minden SFR-t kielégítenek, akkor a biztonsági tartomány biztonsági célja teljesül.

Az értékelő azt is állapítsa meg, hogy a biztonsági tartomány egy adott biztonsági céljára visszavezethető összes SFR szükséges: azaz az SFR teljesülése ténylegesen hozzájárul a biztonsági cél eléréséhez.

Az ASST_SDR.2.2E értékelői akció

ASST_SDR.2.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági követelményekről szóló nyilatkozat belső ellentmondásoktól mentes.

ASST_SDR.2-12 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy az belső ellentmondásoktól mentes.

Az ASST_SDR.2.3E értékelői akció

ASST_SDR.2.3E Az értékelőnek meg kell erősítenie, hogy a biztonsági tartomány biztonsági követelményekről szóló nyilatkozat egy teljes, egymást erősítő követelményrendszert határoz meg.

ASST_SDR.2-12 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy az egy teljes, egymást erősítő követelményrendszert határoz-e meg.

6.2.3.1.12. A biztonsági tartomány összefoglaló előírás (ASST_SDS.1) értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.1.12 pont alatt.

6.2.3.2. A rendszer fejlesztés garanciaosztály (ASDV) értékelése

A teljes értékelői tevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.2 pont alatt.

6.2.3.3. A rendszer útmutató dokumentumok garanciaosztály (ASGD) értékelése

6.2.3.3.1. Előkészítési útmutató: ASGD_PRE.2 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) előkészítő útmutató,
c) az STOE komponenseire a szállítók szállítási eljárásainak a leírása.

Az ASGD_PRE.2.1E értékelői akció

ASGD_PRE.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_PRE.2.1C Az előkészítő útmutatónak le kell írnia az STOE leszállított komponenseinek biztonságos elfogadásához alkalmazott valamennyi lépést, a komponens szállítójának szállítási eljárásaival összhangban.

ASGD_PRE.2-1 Az értékelőnek ellenőriznie kell, hogy biztosították-e az STOE komponenseire a szállítók szállítási eljárásainak a leírását.

Amennyiben a szállító szállítási eljárásaival kapcsolatban nem várható elfogadási eljárások alkalmazása, akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

ASGD_PRE.2-2 Az értékelőnek meg kell vizsgálnia a biztosított elfogadási eljárásokat annak megállapítása érdekében, hogy azok leírják-e az STOE komponenseinek biztonságos elfogadásához szükséges lépéseket, a szállító szállítási eljárásaival összhangban.

Az elfogadási eljárásoknak legalább a rendszer integrátor arra vonatkozó ellenőrzését tartalmazniuk kell, hogy az STOE valamennyi komponensét az SST-ben jelzett helyes verziókkal szállították-e le.

Az elfogadási eljárásoknak részletes információt kell szolgáltatniuk az alábbiakhoz, amennyiben azok alkalmazhatók:

a) arról való meggyőződés, hogy a leszállított komponens az SST-ben jelzett helyes verzió
b) a leszállított komponens módosításának vagy hamisításának az észlelése.

ASGD_PRE.2.2C Az előkészítő útmutatónak le kell írnia az STOE komponensek biztonságos telepítéséhez, az STOE integrálásához és az üzemeltetési környezethez való biztonságos előkészülethez alkalmazott valamennyi lépést, az SST-ben leírt, üzemeltetési környezetre vonatkozó biztonsági célokkal összhangban.

ASGD_PRE.2-3 Az értékelőnek ellenőriznie kell, hogy biztosították-e az STOE komponenseinek biztonságos telepítéséhez szükséges eljárásokat.

Amennyiben az STOE-vel és üzemeltetési környezetével kapcsolatban nem várható telepítési eljárások alkalmazása (mert például az STOE-t már működésre alkalmas állapotban szállították le, s nincsenek a környezetére vonatkozó követelmények), akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

ASGD_PRE.2-4 Az értékelőnek meg kell vizsgálnia a biztosított telepítési eljárásokat annak megállapítása érdekében, hogy azok leírják-e az STOE komponensek biztonságos telepítéséhez, valamint az üzemeltetési környezet biztonságos előkészítéséhez szükséges lépéseket, az SST biztonsági céljaival összhangban.

Amennyiben nem várható telepítési eljárások alkalmazása (mert például az STOE-t már működésre alkalmas állapotban szállították le, s nincsenek a környezetére vonatkozó követelmények), akkor ez a munkaegység nem alkalmazható, ezért teljesítettnek tekintendő.

A telepítési eljárásoknak részletes információt kell szolgáltatniuk az alábbiakról, amennyiben azok alkalmazhatók:

a) a biztonságos telepítéshez szükséges minimális rendszer követelmények,
b) az üzemeltetési környezetre vonatkozó követelmények, az SST-ben meghatározott biztonsági célokkal összhangban,
c) az SSF ellenőrzése alatt álló egyedek telepítés-specifikus biztonsági tulajdonságainak módosítása,
d) kivételek és problémák kezelése.

Az ASGD_PRE.2.2E értékelői akció

ASGD_PRE.2.2E Az értékelőnek független ellenőrzést kell végeznie az előkészítő útmutató tartalmának gyakorlati alkalmazására vonatkozóan az alábbiak útján: [kiválasztás: személyi interjúk, az előkészítő útmutató mintavételezése, az előkészítés eredményének mintavételen alapuló független vizsgálata].

ASGD_PRE.2-5 Az értékelőnek független ellenőrzést kell végeznie az előkészítő útmutató tartalmának gyakorlati alkalmazására vonatkozóan, a rendszer integrátorral folytatott személyes konzultációk (interjúk) útján, amennyiben a kiválasztás művelete kiválasztotta az alábbi lehetőséget: személyi interjúk.

A személyes konzultációk arra irányuljanak, hogy az előkészítést (tipikusan a telepítést) végző személyek tisztában vannak-e feladatuk fontosságával, illetve rendelkeznek-e biztonságos előkészítés végrehajtásához szükséges ismeretekkel (képzés, oktatás).

ASGD_PRE.2-6 Az értékelőnek független ellenőrzést kell végeznie az előkészítő útmutató tartalmának gyakorlati alkalmazására vonatkozóan, az előkészítő útmutató mintavételezéssel kiválasztott részének vizsgálatával, amennyiben a kiválasztás művelete kiválasztotta az alábbi lehetőséget: útmutató mintavételezése.

A vizsgálat a kiválasztott részek érthetőségére, szakszerűségére és az egyéb értékelési bizonyítékokkal való összhangjára irányuljon.

ASGD_PRE.2-7 Az értékelőnek független ellenőrzést kell végeznie az előkészítő útmutató tartalmának gyakorlati alkalmazására vonatkozóan, az előkészítés eredményének (ami tipikusan a telepített rendszer) mintavételen alapuló független vizsgálatával, amennyiben a kiválasztás művelete kiválasztotta az alábbi lehetőséget: az előkészítés eredményének mintavételen alapuló független vizsgálata.

A vizsgálat a kiválasztott komponensek helyes előkészítésének (telepítésének) gyakorlati ellenőrzésére irányuljon.

6.2.3.3.2. Konfigurálási útmutató: ASGD_CON.2 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) STOE terv,
c) a rendszer-működési biztonsági koncepció
d) konfigurálási útmutató.

Az ASGD_CON.2.1E értékelői akció

ASGD_CON.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_CON.2.1C A konfigurálási útmutatónak le kell írnia azokat a biztonsági konfigurációs paramétereket, amelyek a rendszer integrátor vagy az ezzel azonos szerepkörű és felelősségű STOE felhasználók/adminisztrátorok számára elérhetők.

ASGD_CON.2-1 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy azok leírják-e a rendszer integrátor vagy az ezzel azonos szerepkörű és felelősségű STOE felhasználók/adminisztrátorok számára elérhető biztonsági konfigurációs paramétereket.

ASGD_CON.2.2C A konfigurálási útmutatónak le kell írnia azoknak a biztonsági paramétereknek a használatát, amelyeket az STOE állíthat be abból a célból, hogy megvalósítsa és érvényre juttassa a rendszer biztonsági szabályzatait.

ASGD_CON.2-2 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy azok leírják-e a biztonsági paramétereknek a használatát.

ASGD_CON.2.3C A konfigurálási útmutatónak figyelmeztetéseket kell tartalmaznia a konfigurálás által hozzáférhető azon funkciókra és privilégiumokra vonatkozóan, amelyeket egy biztonságos feldolgozási környezetben ellenőrizni kell.

ASGD_CON.2-3 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy az tartalmaz-e figyelmeztetéseket a konfigurálás által hozzáférhető azon funkciókra és privilégiumokra vonatkozóan, amelyeket egy biztonságos feldolgozási környezetben ellenőrizni kell.

ASGD_CON.2.4C A konfigurálási útmutatónak világosan be kell mutatnia az összes konfigurálással kapcsolatos felelősséget, amely az STOE biztonságos működtetéséhez szükséges.

ASGD_CON.2-4 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy az bemutatja-e az összes konfigurálással kapcsolatos felelősséget, amely az STOE biztonságos működtetéséhez szükséges.

ASGD_CON.2.5C A konfigurálási útmutatónak ellentmondás mentesnek kell lennie az értékeléshez átadott összes többi dokumentumhoz viszonyítva.

ASGD_CON.2-5 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy az ellentmondás mentes-e az értékeléshez átadott összes többi dokumentummal.

ASGD_CON.2.6C A konfigurálási útmutatónak le kell írnia az összes olyan biztonsági követelményt, amely az STOE-ra vonatkozik, beleértve az üzemeltetési környezetet is.

ASGD_CON.2-6 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy az leírja-e az összes STOE-ra vonatkozó biztonsági követelményt, beleértve az üzemeltetési környezetre vonatkozókat is.

ASGD_CON.2.7C A konfigurálási útmutatónak meg kell mutatnia, hogy az STOE terv megvalósítja az összes olyan komponensre vonatkozó biztonsági paramétert, amelyet a rendszer-működési biztonsági koncepció megkövetel.

ASGD_CON.2-7 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy az STOE terv megvalósítja-e az összes olyan komponensre vonatkozó biztonsági paramétert, amelyet a rendszer-működési biztonsági koncepció megkövetel.

Az ASGD_CON.2.2E értékelői akció

ASGD_CON.2.2E Az értékelőnek mintavételezéssel, függetlenül ellenőriznie kell a konfigurálási útmutatóban meghatározott konfigurációs paraméterek gyakorlati alkalmazását.

ASGD_CON.2-8 Az értékelőnek a konfigurálási útmutatóból mintavételezéssel választott részekre függetlenül ellenőriznie kell az ott meghatározott konfigurációs paraméterek gyakorlati alkalmazásának helyességét.

6.2.3.3.3. Üzemeltetési útmutató: ASGD_OPE.2 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) rendszer interfész specifikáció,
c) STOE terv
d) üzemeltetési útmutató.

Az ASGD_OPE.2.1E értékelői akció

ASGD_OPE.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_OPE.2.1C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia azokat a felhasználó által elérhető funkciókat és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

AGD_OPE.2-1 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót, annak megállapítása érdekében, hogy az leírja-e azokat a felhasználó által elérhető funkciókat és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

Az STOE konfigurálása lehetővé teheti, hogy a különböző felhasználói szerepkörök az STOE különböző funkcióihoz eltérő jogosultságokkal rendelkezzenek. Ezáltal egyes felhasználók számára engedélyezve lesznek olyan funkciók, melyek mások számára nem. Ezeket a funkciókat és jogosultságokat minden felhasználói szerepkörre le kell írni az üzemeltetési útmutatóban.

Az üzemeltetési útmutatónak minden felhasználói szerepkörre azonosítania kell az ellenőrzés alatt tartandó funkciókat és jogosultságokat, az ezek számára szükséges utasítás típusokat, valamint az utasítások okait. Az üzemeltetési útmutatónak figyelmeztetéseket kell tartalmaznia az ellenőrzés alatt tartandó funkciókra és jogosultságokra vonatkozóan. A figyelmeztetéseknek a várt hatásokról, az esetleges mellékhatásokról és a más funkciókkal és jogosultságokkal kapcsolatos lehetséges kapcsolatokról kell szólniuk.

ASGD_OPE.2.2C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia, hogy az STOE által biztosított, elérhető interfészeket hogyan kell biztonságos módon használni.

AGD_OPE.2-2 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e az STOE által biztosított, elérhető interfészek biztonságos használatát.

Az üzemeltetési útmutatónak javaslatokat kell megfogalmaznia az SSF hatékony használatához (például hibajavító csomagok frissítésének javasolt gyakorisága, jelszó kialakítási gyakorlat áttekintése, felhasználói állományok mentésének javasolt gyakorisága, felhasználói hozzáférési jogok megváltoztatása hatásának elemzése).

ASGD_OPE.2.3C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági szempontból fontos paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket.

AGD_OPE.2-3 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket is.
Az üzemeltetési útmutatónak áttekintést kell adnia a felhasználói interfészeken keresztül látható biztonsági funkcionalitásról.

Az üzemeltetési útmutatónak azonosítania kell, és le kell írnia a biztonsági funkciók és interfészek célját, működésüket, illetve egymás között kapcsolataikat.

Minden felhasználó által elérhető interfészre az üzemeltetési útmutatónak:

a) le kell írnia azokat a módszereket, melyekkel az interfész hívható (pl. parancssor, programozási nyelvi rendszerhívások, menükiválasztás, parancsgombok);
b) le kell írnia a felhasználó által állítandó paramétereket, azok célját, érvényes és alapértelmezett értékeiket, a paraméterek biztonságos és nem biztonságos használatát okozó beállításokat, mindezt egyenként vagy paraméter-kombinációkban;
c) le kell írnia a közvetlen TSF válaszokat, üzeneteket vagy visszaadott kódot.

Az értékelőnek elsősorban a rendszer interfész specifikációt és az SST-t kell figyelembe vennie annak megállapítása érdekében, hogy az ezekben leírt TSF összhangban áll-e az üzemeltetési útmutatóval. Az értékelőnek meg kell győződnie az üzemeltetési útmutató teljességéről, vagyis arról, hogy az összes emberi felhasználó számára lehető teszi az elérhető interfészek biztonságos használatát. Az értékelő segítségként elkészítheti az útmutató és ezen dokumentumok közötti informális leképezést. Az ebben fellelhető bármilyen hiányosság az útmutató teljességének csorbulását jelezheti.

ASGD_OPE.2.4C Az üzemeltetési útmutatónak minden felhasználói szerepkörre világosan be kell mutatnia a felhasználó által elérhető funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból fontos minden esemény típust, beleértve az SSF ellenőrzése alá eső egyedek biztonsági tulajdonságainak megváltoztatását is.

AGD_OPE.2-4 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e a felhasználói funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból lényeges minden esemény típust, beleértve az SSF ellenőrzése alá tartozó egyedek biztonsági tulajdonságainak megváltoztatását is.

Minden biztonsági szempontból fontos esemény típust részletezni kell minden felhasználói szerepkörre, hogy minden felhasználó tudja, milyen események fordulhatnak elő, és mit kell tennie (ha szükséges) a biztonság fenntartása érdekében. Az STOE üzemeltetése során előforduló biztonsági szempontból lényeges eseményeket (például naplótár túlcsordulás; rendszerösszeomlás; felhasználói rekordok felülírása, amikor egy felhasználó távozik a szervezettől, és a fiókját eltörlik) kellően meg kell határozni, hogy a felhasználó beavatkozhasson a biztonságos működés fenntartása érdekében.

ASGD_OPE.2.5C Az üzemeltetési útmutatónak azonosítani kell az STOE összes lehetséges üzemmódját (beleértve a karbantartási és a meghibásodás vagy üzemeltetési hiba utáni üzemmódokat is), valamint ezek biztonságos üzemeltetésre gyakorolt következményeit és kihatásait.

AGD_OPE.2-5 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót és az egyéb értékeléshez adott bizonyítékot annak megállapítása érdekében, hogy az útmutató azonosítja-e a TOE összes lehetséges üzemmódját (beleértve a karbantartási és a meghibásodás vagy üzemeltetési hiba utáni üzemmódokat is), valamint ezek következményét és kihatásait a biztonságos üzemelés fenntartására.

Más értékelési bizonyítékot (elsősorban a rendszer interfész specifikációt) az értékelőnek annak megállapításához javasolt használnia, hogy az útmutató megfelelő eligazító leírást tartalmaz-e.

A teszt dokumentációban benyújtott információ is felhasználható annak eldöntésére, hogy az útmutató elegendő útmutató információt tartalmaz-e. A tesztlépéseknél megadott részletek felhasználhatók annak megerősítésére, hogy az üzemeltetési útmutató elégséges az STOE használatához és adminisztrálásához.

Az értékelőnek egy időben egy ember számára látható interfészt ajánlott vizsgálnia, úgy, hogy összehasonlítja az interfészt biztonságos használatáról szóló útmutatást egyéb bizonyítékokkal, annak kiderítése érdekében, hogy az interfésszel kapcsolatos információk valóban jól írják-e le annak biztonságos használatát (azaz megfelelnek-e az SFR-eknek). Az értékelőnek az interfészek közötti kapcsolatokat is át kell néznie, potenciális ellentmondásokat keresve.

ASGD_OPE.2.6C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia azokat a betartandó biztonsági intézkedéseket, melyek az SST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

AGD_OPE.2-6 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót annak megállapítása érdekében, hogy az minden felhasználói szerepkörre leírja-e azokat a betartandó biztonsági intézkedéseket, melyek az SST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

Az értékelő elemezze az SST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célokat, majd állapítsa meg, hogy az üzemeltetési útmutató minden felhasználói szerepkörre megfelelően leírja-e a fontos biztonsági intézkedéseket.

Az üzemeltetési útmutatóban leírt biztonsági intézkedéseknek magukban kell foglalniuk az összes fontos külső eljárásrendi, fizikai, személyzeti és kapcsolódásra vonatkozó intézkedést.

ASGD_OPE.2.7C Az üzemeltetési útmutatónak egyértelműnek és megalapozottnak kell lennie.

AGD_OPE.2-7 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót annak megállapítása érdekében, hogy az egyértelmű-e.

Az útmutató akkor nem egyértelmű (félrevezető), ha ez alapján egy felhasználó indokoltan félreértheti teendőit, és az STOE-ra vagy az STOE által nyújtott biztonságra nézve hátrányos módon alkalmazza a leírtakat.

AGD_OPE.2-8 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót annak megállapítása érdekében, hogy az megalapozott-e.

Az útmutató akkor tekinthető megalapozatlannak, ha olyan követelményeket támaszt az STOE használatával vagy üzemeltetési környezetével szemben, melyek nem felelnek meg az SST-nek, vagy indokolatlanul nagy terhet jelentenek a biztonság fenntartásához.

Az ASGD_OPE.2.2E értékelői akció

ASGD_OPE.2.2E Az értékelőnek független ellenőrzést kell végeznie az üzemeltetési útmutató specifikációinak gyakorlati alkalmazását illetően, az alábbiak útján: [kiválasztás: személyi interjúk, az üzemeltetési útmutató mintavételezése, az üzemeltetés eredményeinek mintavételen alapuló független vizsgálata].

AGD_OPE.2-9 Az értékelőnek független ellenőrzést kell végeznie az üzemeltetési útmutató specifikációinak gyakorlati alkalmazására vonatkozóan, az üzemeltetést végzőkkel folytatott személyes konzultációk (interjúk) útján, amennyiben a kiválasztás művelete kiválasztotta az alábbi lehetőséget: személyi interjúk.

A személyes konzultációk arra irányuljanak, hogy az üzemeltetést (beleértve a napi felhasználást és az adminisztrálást is) végző személyek tisztában vannak-e feladatuk fontosságával, illetve rendelkeznek-e biztonságos üzemeltetés végrehajtásához szükséges ismeretekkel (képzés, oktatás).

AGD_OPE.2-10 Az értékelőnek független ellenőrzést kell végeznie az üzemeltetési útmutató specifikációinak gyakorlati alkalmazását illetően, az üzemeltetési útmutatóból mintavételezéssel kiválasztott részek gyakorlati kipróbálása útján, amennyiben a kiválasztás művelete kiválasztotta az alábbi lehetőséget: az üzemeltetési útmutató mintavételezése.

A vizsgálat a kiválasztott részek érthetőségére, szakszerűségére és az egyéb értékelési bizonyítékokkal való összhangjára irányuljon.

ASGD_PRE.2-7 Az értékelőnek független ellenőrzést kell végeznie az üzemeltetési útmutató tartalmának gyakorlati alkalmazására vonatkozóan, az üzemeltetés eredményeinek (ami

tipikusan napló tartalmakat, az üzemeltetés eredményeiről szóló írásos jelentéseket, esetleg az üzemeltetés folyamatosságára és hibamentességére vonatkozó mérőszámokat jelent) mintavételen alapuló független vizsgálatával, amennyiben a kiválasztás művelete kiválasztotta az alábbi lehetőséget: az üzemeltetés eredményeinek mintavételen alapuló független vizsgálata.

A vizsgálat a kiválasztott komponensek helyes üzemeltetésének gyakorlati ellenőrzésére irányuljon, az erre vonatkozó naplóbejegyzések, egyéb írásos jelentések, illetve az üzemeltetés minőségére (pl. folyamatosságára, hibamentességére) vonatkozóan kimutatott mérőszámok tanulmányozásával.

6.2.3.4. A rendszer konfiguráció kezelés garanciaosztály (ASCM) értékelése

6.2.3.4.1. Rendszer alap konfiguráció: ASCM_SBC.2 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) CM dokumentáció a rendszer alap konfigurációjához,
b) STOE terv.

Az ASCM_SBC.2.1E értékelői akció

ASCM_SBC.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASCM_SBC.2.1C A CM rendszernek egyedileg azonosítania kell az STOE alap konfigurációt, az alap konfigurációt alkotó összes rendszer komponenst és ezek értékelési állapotát.

ASCM_SBC.2-1 Az értékelőnek ellenőriznie kell, hogy a CM rendszer egyedileg azonosítja-e az STOE alap konfigurációt, az alap konfigurációt alkotó összes rendszer komponenst és ezek értékelési állapotát.

ASCM_SBC.2.2C A CM rendszernek nyomon kell követnie az alap konfigurációhoz, illetve az ezt alkotó rendszer komponensekhez kapcsolódó változtatásokat.

ASCM_SBC.2-2 Az értékelőnek meg kell vizsgálnia a CM rendszert annak megállapítása érdekében, hogy az nyomon követi-e az alap konfigurációhoz, illetve az ezt alkotó rendszer komponensekhez kapcsolódó változtatásokat.

ASCM_SBC.2.3C A CM tervnek le kell írnia, hogy a rendszer alap konfigurációját hogyan kezelik, és hogy az alap konfiguráción történő módosításokat hogyan ellenőrzik és hogyan követik nyomon.

ASCM_SBC.2-3 Az értékelőnek meg kell vizsgálnia a CM tervet annak megállapítása érdekében, hogy az leírja-e, hogy a rendszer alap konfigurációját hogyan kezelik, valamint

hogy az alap konfiguráción történő módosításokat hogyan ellenőrzik és hogyan követik nyomon.

Az ASCM_SBC.2.2E értékelői akció

ASCM_SBC.2.2E Az értékelőnek független ellenőrzést kell végeznie a CM rendszer alap konfiguráció tartalmára vonatkozóan, személyi interjúk és a módosítások mintavételezése útján.

ASCM_SBC.2-4 Az értékelőnek meg kell vizsgálnia a CM rendszer kimenetét annak megállapítása érdekében, hogy a CM rendszert rendszeresen használják a rendszer aktuális állapotának nyomon követésére.

Az értékelő ezt a vizsgálatot a CM rendszert kezelő személyekkel folytatott interjúkkal is kiegészítheti.

ASCM_SBC.2-5 Az értékelőnek meg kell vizsgálnia a CM rendszert annak megállapítása érdekében, hogy az a rendszer alap konfigurációját helyesen, a rendszer aktuális állapotának megfelelően kezeli.

Az értékelő ezt a vizsgálatot a rendszer néhány kiválasztott komponensére a tényleges állapot és a CM rendszerben aktuális állapotként tárolt virtuális állapot egybevetésével végezze.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

6.2.3.4.2. Értékelt és tanúsított komponensek: ASCM_ECC.2 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) CM dokumentáció a rendszer alap konfigurációjához,
b) STOE terv,
c) értékelt és tanúsított termék-komponensek listája.

Az ASCM_ECC.2.1E értékelői akció

ASCM_ECC.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASCM_ECC.2.1C Az értékelt és tanúsított termék-komponensek listájában le kell írni az értékelt és tanúsított termékek garanciacsomagjait.

ASCM_ECC.2-1 Az értékelőnek meg kell vizsgálnia, hogy értékelt és tanúsított termék-komponensek listája a rendszer valamennyi STOE tervben azonosított komponensét tartalmazza-e.

ASCM_ECC.2-2 Az értékelőnek ellenőriznie kell, hogy értékelt és tanúsított termék-komponensek listája leírja-e az egyes értékelt és tanúsított termékek garanciacsomagjait.

A leírás az alábbi garanciacsomagokat tartalmazhatja: CC EAL1, CC EAL1+, CC EAL2, CC EAL2+, CC EAL3, CC EAL3+, CC EAL4, CC EAL4 felett, MIBÉTS alap, MIBÉTS fokozott, MIBÉTS kiemelt, nincs tanúsítva.

ASCM_ECC.2.2C Az értékelt és tanúsított termék-komponensek listájának minden termékre azonosítania kell az értékelési eredményekre vonatkozó tanúsítványt, tanúsítási jelentést és az ezek alapjául szolgáló biztonsági előirányzatot.

ASCM_ECC.2-3 Az értékelőnek ellenőriznie kell, hogy értékelt és tanúsított termék-komponensek listája azonosítja-e minden értékelt és tanúsított termék-komponensre az alábbiakat: biztonsági előirányzat, tanúsítási jelentés, tanúsítvány.

ASCM_ECC.2.3C Az értékelt és tanúsított termék-komponensek listájának minden termékre le kell írnia az üzemeltetési feltételeket.

ASCM_ECC.2-4 Az értékelőnek ellenőriznie kell, hogy értékelt és tanúsított termék-komponensek listája leírja-e minden értékelt és tanúsított termék-komponensre annak üzemeltetési feltételeit.

Az ASCM_ECC.2.2E értékelői akció

ASCM_ECC.2.2E Az értékelőnek meg kell erősítenie, hogy a rendszer üzemeltetési környezete kielégíti az értékelt és tanúsított termékek tanúsítványaiban és tanúsítási jelentéseiben megfogalmazott üzemeltetési feltételeket.

ASCM_ECC.2-5 Az értékelőnek meg kell vizsgálnia, hogy értékelt és tanúsított termék-komponensek listájában a termék-komponensekre leírt üzemeltetési paraméterek összhangban állnak-e az adott termék tanúsítványában és tanúsítási jelentésében az üzemeltetési feltételekre megfogalmazott korlátozásokkal.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

Az ASCM_ECC.2.3E értékelői akció

ASCM_ECC.2.3E Az értékelőnek meg kell erősítenie, hogy a rendszer biztonsági funkcionalitását érvényre juttató és támogató termék komponensek tanúsítására vonatkozóan teljesülnek a SAP-F garanciacsomag elvárásai.

ASCM_ECC.2-6 Az értékelőnek meg kell vizsgálnia, hogy értékelt és tanúsított termék-komponensek listájában az egyes értékelt és tanúsított termékekre leírt garanciacsomagok összhangban vannak-e a SAP-F garanciacsomag elvárásaival.

Az értékelő a vizsgálat keretében erősítse meg, hogy az STOE tervben meghatározott rendszer biztonsági funkcionalitást támogató komponensek legalább CC EAL2 vagy MIBÉTS alap szintű tanúsítással rendelkeznek.

Az értékelő a vizsgálat keretében erősítse meg, hogy az STOE tervben meghatározott rendszer biztonsági funkcionalitást érvényre juttató komponensek legalább CC EAL3 vagy MIBÉTS fokozott szintű tanúsítással rendelkeznek.

Amennyiben valamely rendszer biztonsági funkcionalitást támogató vagy érvényre juttató komponens nem felel meg az elvárásoknak, akkor ezt a rendszer értékelési jelentésben szerepeltetni kell a maradványkockázatok között.

6.2.3.5. A rendszer tesztelés garanciaosztály (ASTE) értékelése

6.2.3.5.1. Funkcionális rendszer tesztelés: ASTE_FUN.1 értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.5.1 pont alatt.

6.2.3.5.2. A rendszer tesztelés lefedettsége: ASTE_COV.1 értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.5.2 pont alatt.

6.2.3.5.3. A rendszer tesztelés mélysége: ASTE_DPT.2 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) rendszer interfész specifikáció,
c) biztonsági architektúra leírás,
d) STOE terv,
e) tesztdokumentáció,
f) tesztmélység elemzés.

Az ASTE_DPT.2.1E értékelői akció

ASTE_DPT.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASTE _DPT.2.1C A tesztmélység elemzésnek be kell mutatnia, hogy a tesztdokumentációban azonosított tesztek elegendőek annak bemutatására, hogy a rendszer biztonsági funkcionalitása a rendszer biztonsági architektúra leírással, valamint a rendszer biztonsági terv alrendszerekre vonatkozó leírásával összhangban működik.

ASTE_DPT.2-1 Az értékelőnek meg kell vizsgálnia a tesztdokumentációt és a tesztmélység elemzést annak megállapítása érdekében, hogy a rendszer biztonsági architektúra leírásban azonosított, az STOE-t külső informatikai rendszerekhez kapcsoló interfészeket tesztelték-e.

Ez a munkaegység ellenőrzi a tesztek és a rendszer biztonsági architektúra leírás megfelelését. Amennyiben az SSF szerkezeti helyességének leírása (az ADV_ARC biztonsági szerkezet leírás keretén belül) speciális mechanizmusokra hivatkozik, ez a munkaegység ellenőrizze a tesztek és az ilyen mechanizmusok üzemeltetési leírása közötti megfelelést is.

ASTE_DPT.2-2 Az értékelőnek meg kell vizsgálnia a tesztdokumentációt és a tesztmélység elemzést annak megállapítása érdekében, hogy azok szemléltetik-e, hogy az STOE és a külső informatikai rendszerek egymásra hatása megfelel a rendszer biztonsági architektúra leírásban foglaltaknak.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt mélység elemzésben szereplő teszteket és a kapcsolódó külső informatikai rendszerek egyértelműen kell azonosítani.

ASTE_DPT.2-3 Az értékelőnek meg kell vizsgálnia a tesztdokumentációt és a tesztmélység elemzést annak megállapítása érdekében, hogy az STOE tervben azonosított alrendszerek által nyújtott biztonsági funkcionalitást tesztelték-e.

Az STOE tervben szereplő valamennyi alrendszer működését tesztelni kell. Nyilvánvalóan hiányos a tesztelés mélysége, ha az STOE tervben azonosított egyik alrendszer működéséhez nem rendeltek tesztet.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt mélység elemzésben szereplő teszteket és a kapcsolódó alrendszereket egyértelműen kell azonosítani.

ASTE_DPT.2-4 Az értékelőnek meg kell vizsgálnia a tesztdokumentációt és a tesztmélység elemzést annak megállapítása érdekében, hogy az STOE tervben azonosított alrendszerek közötti belső interfészeket tesztelték-e.

Az STOE tervben szereplő alrendszerek összes egymásra hatását tesztelni kell. Nyilvánvalóan hiányos a tesztelés mélysége, ha az STOE tervben azonosított alrendszerek közötti egyik interfészhez nem rendeltek tesztet.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt mélység elemzésben szereplő teszteket és a kapcsolódó alrendszerek közötti interfészeket egyértelműen kell azonosítani.

6.2.3.5.4. Független rendszer tesztelés: ASTE_IND.1 értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.5.4 pont alatt.

6.2.3.6. A rendszer sebezhetőség felmérés garanciaosztály (ASVA) értékelése

6.2.3.6.1. Sebezhetőség elemzés: ASVA_VAN.2 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) rendszer interfész specifikáció,
c) STOE terv,
d) biztonsági architektúra leírása,
e) útmutató dokumentációk,
f) a tesztelésre alkalmas STOE,
g) nyilvánosan elérhető információk a lehetséges sebezhetőségek azonosításának támogatására,
h) a lehetséges sebezhetőségekre és támadásokra vonatkozó aktuális, nyilvánosan elérhető információk.

Az ASVA_VAN.2.1E értékelői akció

ASVA_VAN.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASVA_VAN.2.1C Az STOE-nak alkalmasnak kell lennie tesztelésre.

ASVA_VAN.2-1 Az értékelőnek meg kell vizsgálnia az STOE-t annak megállapítása érdekében, hogy az integrált és konfigurált rendszer megfelel-e az SST-ben meghatározott, értékelendő rendszer leírásával (a kiépítés és a konfigurálás szempontjából).

Az STOE-t alkotó hardver és szoftver komponensekre az értékelő ellenőrizze, hogy valamennyi komponens konfigurációja ellentmondás mentes-e az SST-vel.

Az értékelő vegye figyelembe azokat az SST-ben leírt, az STOE üzemeltetési környezetére vonatkozó biztonsági célokat, amelyek a rendszer teszt környezetére alkalmazhatók.

Bármilyen tesztelési erőforrás (mérőműszer, elemző készülék) használatakor az értékelő felelőssége annak biztosítása, hogy ezek az erőforrások megfelelően hitelesítve legyenek.

ASVA_VAN.2-2 Az értékelőnek meg kell vizsgálnia az STOE-t annak megállapítása érdekében, hogy a rendszer valamennyi komponensét megfelelően telepítették-e, és ismert állapotban van-e.

Az ASVA_VAN.2.2E értékelői akció

ASVA_VAN.2.2E: Az értékelőnek egy keresést kell végrehajtania nyilvános forrásokban az STOE lehetséges sebezhetőségeinek azonosítása érdekében.

ASVA_VAN.2-3 Az értékelőnek tanulmányoznia kell a nyilvánosan rendelkezésre álló információ forrásokat az STOE lehetséges sebezhetőségeinek a meghatározása céljából.

Az értékelő tanulmányozza a nyilvánosan rendelkezésre álló információ forrásokat, amelyek rendelkezésre állnak az STOE lehetséges sebezhetőségei meghatározásainak elősegítéséhez. Sokféle nyilvánosan rendelkezésre álló információ forrás létezik, amelyeket az értékelőnek ajánlatos figyelembe vennie, felhasználva a világhálón elérhető anyagokat, beleértve a következőket:

a) szakértői publikációk (folyóiratok, könyvek);
b) tanulmányok.

Az értékelő ne korlátozza az általa figyelembevett nyilvánosan rendelkezésre álló információkat a fentiekre, hanem vegyen figyelembe bármely egyéb vonatkozó rendelkezésre álló információt.

A nyilvánosan rendelkezésre álló információ keresése célirányosan azokra a forrásokra irányuljon, amelyek az STOE alapját képező komponensekre (termékekre) vonatkoznak.

Az értékelő az átadott bizonyítékok vizsgálata közben használja fel a nyilvános információkat abból a célból, hogy további vizsgálatokat végezzen lehetséges sebezhetőségek felkutatására. Ha az értékelő problémás területeket határozott meg, vegye figyelembe azokat a nyilvánosan rendelkezésre álló információkat, amelyek az adott problémás területre vonatkoznak.

Az olyan információk elérhetősége, amely azonnal rendelkezésre állhat egy támadó számára, s amely elősegíti támadások meghatározását és megkönnyíti a támadások hatékony végrehajtását, jelentősen megnövelheti egy adott támadó támadási lehetőségeit. A sebezhetőségi információk és kifinomult támadó eszközök hozzáférhetősége az Interneten nagyon valószínűvé teszi, hogy ezeket megpróbálják felhasználni az STOE lehetséges sebezhetőségeinek meghatározására és kihasználására. A modern kereső eszközök az ilyen információkat könnyen elérhetővé teszik az értékelő számára, és a publikált lehetséges sebezhetőségekkel, valamint a jól ismert általános támadásokkal szembeni ellenállóképesség költséghatékony módon meghatározható.

A lehetséges sebezhetőségeket tartalmazó nyilvános adatbázisokról lásd [4].

Az értékelőnek jelentést kell készíteni a megvizsgált bizonyítékokról a lehetséges sebezhetőségekre irányuló keresés befejezésekor. A bizonyítékok kiválasztása származhat az értékelő által meghatározott olyan problémás területekből, amely a támadó által is feltehetően elérhető bizonyítékhoz kapcsolódik, vagy megfelelhet az értékelő által adott valamilyen más magyarázatnak.

Az ASVA_VAN.2.3E értékelői akció

ASVA_VAN.2.3E: Az értékelőnek egy független sebezhetőség vizsgálatot kell végrehajtania az STOE-ra, felhasználva az SST, a biztonsági architektúra leírás, a rendszer interfész specifikáció, az STOE terv, a rendszer-működési biztonsági koncepció és az útmutató dokumentációk által biztosított ismereteket, az STOE lehetséges sebezhetőségeinek azonosítása érdekében.

ASVA_VAN.2-4 Az értékelőnek egy célirányos keresést kell folytatnia az SST-re, a biztonsági architektúra leírásra, a rendszer interfész specifikációra, az STOE tervre, a rendszer-működési biztonsági koncepcióra, valamint az útmutató dokumentációkra, abból a célból, hogy meghatározza az STOE-ban esetlegesen előforduló lehetséges sebezhetőségeket.

Hiba hipotézis módszer használata szükséges, amely a specifikációk, a tervezési és útmutató bizonyítékok vizsgálata után az STOE-ban lévő lehetséges sebezhetőségeket feltételezi, illetve ezzel kapcsolatos vizsgálódásokat folytat.

Az értékelő használja fel az STOE-ra szerzett ismereteit, hiba hipotézis módszert alkalmazva, az STOE integrálásában, vagy specifikált üzemmódjában lévő lehetséges hibák azonosítása céljából.

A biztonsági architektúra leírás szolgáltatja a rendszer integrátor sebezhetőség vizsgálatát, minthogy ez dokumentálja, hogy az SSF hogyan védi saját magát a nem-megbízható szubjektumokkal szemben, és hogyan akadályozza meg a biztonságot érvényre juttató funkcionalitás megkerülését. Ennélfogva az értékelő építsen az SSF védelem megértésére, amelyet ezen bizonyíték vizsgálatából nyert, majd hasznosítsa ezt az egyéb fejlesztésre vonatkozó (ASDV) bizonyítékokból nyert ismeretekben.

Az alkalmazott megközelítési módban a problémás területek az irányadók, amelyeket az értékelési tevékenységek során a bizonyítékok vizsgálata közben, illetve az értékelésre átadott tervezési és útmutató bizonyítékok reprezentatív mintájában való keresés közben határoztak meg.

A problémás területek vonatkozhatnak a biztonsági szerkezet leírásban részletezett speciális védelmi tulajdonságok kielégítőségére.

A sebezhetőség vizsgálat során figyelembevett bizonyítékot ahhoz a bizonyítékhoz lehet kapcsolni, amelyhez a támadó feltételezhetően képes hozzájutni.

A nyilvánosan elérhető források esetében ésszerű feltételezni, hogy a támadó is hozzájut e forrásokhoz, és is felhasználja ezeket az STOE elleni támadási kísérleteiben. Ezért az értékelő vegye figyelembe a nyilvánosan elérhető forrásokat a célirányos vizsgálati megközelítési módnál.

A következők példákat mutatnak azokra a feltételezésekre, amelyeket egy hiba hipotézis tehet:

a) hibásan megadott input feltételezése a támadók által elérhető külső interfészeknél;
b) a biztonsági architektúra leírásban említett kulcsfontosságú mechanizmus vizsgálata olyan belső buffer túlcsordulás feltételezése mellett, amely a szétválasztás elromlásához vezethet;
c) kutatás az STOE megvalósítási reprezentációjában létrehozott olyan objektumok meghatározására, amelyeket nem ellenőriz teljes mértékben az SSF, és amelyeket egy támadó felhasználhat az SFR-ek aláaknázására.

Például az értékelő meghatározhatja, hogy az interfészek lehetséges gyenge pontok az STOE-ban, és egy olyan megközelítési módot használhat, hogy „a rendszer interfész specifikációban

és STOE tervben megadott minden interfész specifikáció átvizsgálásra kerül a lehetséges sebezhetőség hipotézisek kialakításához", majd folytathatja azzal, hogy megmagyarázza a hipotézisben használt módszereket.

A meghatározási folyamat iteratív, ahol egy lehetséges sebezhetőség meghatározása egy másik problémás terület meghatározásához vezethet, amely további vizsgálatokat igényel.

Az értékelőnek jelentést kell készíteni arról, hogy mit tett a bizonyítékokban található lehetséges sebezhetőségek meghatározására. Az ilyen típusú keresésre azonban lehet, hogy az értékelő nem tudja a vizsgálat megkezdése előtt leírni a lehetséges sebezhetőségek meghatározására teendő lépéseket, mivel a feldolgozási mód csak a keresés során találtak eredményeként alakul ki. Ilyen esetekben az értékelőnek a vizsgált bizonyítékokról a lehetséges sebezhetőségekre irányuló keresés befejezésekor kell jelentést készíteni. A bizonyítékok kiválasztása származhat az értékelő által meghatározott olyan problémás területekből, amely a támadó által is feltehetően elérhető bizonyítékhoz kapcsolódik, vagy megfelelhet az értékelő által adott valamilyen más magyarázatnak.

Azoktól az SFR-ektől függően, amelyeket az STOE-nak teljesítenie kell az üzemeltetési környezetben, az értékelő független sebezhetőség vizsgálata vegye tekintetbe az összes alábbi általános sebezhetőség típust:

a) az értékelés alatt álló STOE-t alkotó komponensek típusára vonatkozó általános lehetséges sebezhetőségek;
b) megkerülés;
c) hamisítás;
d) közvetlen támadások;
e) megfigyelés;
f) helytelen használat/visszaélés.

A b) - f) tételeket részletesen magyarázza [7] 7.3 melléklete.

A biztonsági architektúra leírást a fenti általános lehetséges sebezhetőségek szem előtt tartása mellett kell mérlegelni. Minden lehetséges sebezhetőséget mérlegelni kell azon lehetséges módok felkutatására, amelyekkel az SSF védelmet hatálytalanítani, az SSF-et aláaknázni lehet.

ASVA_VAN.2-5 Az értékelőnek a SER-ben rögzítenie kell a meghatározott lehetséges sebezhetőségeket, amelyek tesztelhetők, és az STOE üzemeltetési környezetében elvileg szóba jöhetnek.

Nem szükséges a lehetséges sebezhetőségek további mérlegelése, ha az értékelő azt állapítja meg, hogy az üzemeltetési környezetben meglévő IT vagy nem-IT intézkedések meggátolják a lehetséges sebezhetőségek kiaknázását az adott üzemeltetési környezetben. Például, ha az STOE-hoz való fizikai hozzáférés kizárólag a jogosult felhasználókra van korlátozva, akkor ez a hamisítás lehetséges sebezhetőségét eredményesen nem kihasználhatóvá teheti.

Az értékelőnek minden okot rögzítenie kell a lehetséges sebezhetőségek további mérlegelésből való kizárására, ha azt állapítja meg, hogy a lehetséges sebezhetőség nem

kerülhet szóba az üzemeltetési környezetben. Egyéb esetekben az értékelőnek a lehetséges sebezhetőséget további mérlegelésre rögzítenie kell.

Az értékelőnek a SER-ben meg kell adnia az STOE-val kapcsolatos, annak üzemeltetési környezetében felmerülő lehetséges sebezhetőségek listáját, mely a behatolás tesztelési tevékenység bemeneteként használható.

Az ASVA_VAN.2.4E értékelői akció

ASVA_VAN.2.4E: Az értékelőnek az azonosított lehetséges sebezhetőségek alapján automatikus eszközöket is felhasználva behatolás tesztelést kell végrehajtania, annak megállapítása érdekében, hogy az STOE ellenáll egy alap támadó képességgel bíró támadó által végrehajtott támadásnak.

ASVA_VAN.2-6 Az értékelőnek ki kell választania behatolás tesztelésre alkalmazandó automatikus eszközt.

Az automatikus eszköz kiválasztásánál az értékelő vegye figyelembe a lehetséges sebezhetőségekre irányuló független keresés eredményeit is.

A behatolás tesztelésre alkalmazható automatikus eszközök áttekintésére lásd [4].

ASVA_VAN.2-7 Az értékelőnek a kiválasztott automatikus eszközzel végre kell hajtania a behatolás tesztelést.

A behatolás tesztelésre alkalmazható automatikus eszközök használatára lásd [4].

ASVA_VAN.2-8 Az értékelőnek rögzítenie kell a behatolás tesztek eredményeit.

Az automatikus eszközök naplóállományokba rögzítik a behatolás tesztek eredményeit.

ASVA_VAN.2-9 Az értékelőnek elemeznie kell az automatikus eszközök által végzett behatolás tesztelés eredményeit.

Az automatikus behatolás tesztelés eredményeiről lásd [4].

ASVA_VAN.2-10 Az értékelőnek meg kell terveznie a behatolás teszteket a lehetséges sebezhetőségekre irányuló független keresés, valamint az automatikus eszközökkel végzett behatolás tesztelés eredményei alapján.

Az értékelőnek kellően fel kell készülnie a behatolás tesztelésre annak megállapítása érdekében, hogy az STOE üzemeltetési környezetében mennyire érzékeny a nyilvános forrásokban való kereséssel azonosított lehetséges sebezhetőségekre. Az értékelőnek figyelembe kell vennie bármely harmadik féltől kapott, ismert lehetséges sebezhetőségre vonatkozó aktuális információt, valamint a más értékelői tevékenységek eredményeként talált lehetséges sebezhetőségeket is.

Az értékelőnek szem előtt kell tartania, hogy ugyanúgy, mint a biztonsági architektúra leírás mérlegelése esetében, a sebezhetőségek felkutatásánál tesztelést kell végrehajtania a szerkezeti tulajdonságok megerősítésére. A rendszer integrátor tesztelési bizonyítéka olyan tesztelést is tartalmazni fog, amelyet a biztonsági architektúra leírásban részletezett speciális mechanizmusok helyes működésének megerősítése céljából hajtottak végre. A rendszer integrátor tesztelése azonban nem szükségszerűen tartalmaz tesztelést az SSF védelmére szolgáló szerkezeti tulajdonságok minden vonatkozására, minthogy az ilyen tesztelések legtöbbje természetszerűen negatív tesztelés lesz, amely a tulajdonságok megcáfolását kísérli meg. A behatolás tesztelés stratégiájának kialakításakor az értékelőnek garantálnia kell, hogy a biztonsági szerkezet leírás minden vonatkozása tesztelésre kerüljön vagy a funkcionális tesztelésnél, vagy az értékelői behatolás tesztelésnél.

A behatolás tesztelést valószínűleg tesztesetek sorozatával célszerű elvégezni, ahol az egyes tesztesetek egy-egy adott lehetséges sebezhetőséget próbálnak ki.

Az értékelőnek nem kell teszteket végeznie azokon a lehetséges sebezhetőségeken túl (beleértve a nyilvánosan ismerteket is), melyek kihasználásához legfeljebb alap támadó képesség szükséges. Egyes esetekben azonban még a kihasználhatóság meghatározása előtt szükség lehet egy teszt végrehajtására. Amennyiben értékelői tapasztalata segítségével az értékelő egy megemelt-alap, közepes vagy magas támadó képességgel kihasználható sebezhetőséget tár fel, ezt az értékelési jelentésében maradvány sebezhetőségként szerepeltetnie kell.

Egy adott lehetséges sebezhetőség kihasználásához szükséges támadó képesség meghatározásához útmutató található [7] 7.3.4 pontjában.

Az olyan lehetséges sebezhetőségek, melyek feltételezhetően csak megemelt-alap, közepes vagy magas támadó képességgel kihasználhatók, nem eredményeznek „nem felelt meg” eredményt erre az értékelői tevékenységre. Amennyiben vizsgálat támogatja a fenti feltételezést, az érintett lehetséges sebezhetőséget a továbbiakban nem szükséges a behatolás tesztelés bemeneteként kezelni. Ugyanakkor az ilyen sebezhetőséget az értékelési jelentésben maradvány sebezhetőségként szerepeltetni kell.

Az olyan lehetséges sebezhetőségeket, melyek feltételezhetően alap támadó képességgel kihasználhatók, és a biztonsági célok megsértését eredményezik, a legnagyobb elsőbbséggel ajánlott a lehetséges sebezhetőségek azon listájára felvenni, mely alapján az STOE közvetlen behatolás tesztelését végzik.

ASVA_VAN.2-11 Az értékelőnek a lehetséges sebezhetőségek listáján alapulva el kell készítenie a behatolás tesztelési dokumentációt, a tesztek megismételhetőségét lehetővé tévő részletességgel. A tesztelési dokumentációnak tartalmaznia kell az alábbiakat:

a) a lehetséges sebezhetőség azonosítását, melyre az STOE-t tesztelik;
b) a behatolás teszteléshez szükséges minden tesztberendezés csatlakoztatását és beállítását előíró utasítást;
c) a behatolás tesztelés összes kezdeti előfeltételét kialakító utasításokat;
d) az SSF működését kiváltó utasításokat;
e) az SSF viselkedése megfigyeléséhez szükséges utasításokat;

f) minden várható eredmény leírását, valamint a várható eredményekkel való összehasonlításhoz végrehajtandó, megfigyelt működésre vonatkozó elemzéseket;
g) a tesztek befejezéséhez szükséges és az STOE tesztelés utáni állapotát biztosító utasításokat.

Az értékelőnek a lehetséges sebezhetőségek listáján alapulva el kell készítenie a behatolás tesztelési dokumentációt, a tesztek megismételhetőségét lehetővé tévő részletességgel.

Az értékelőre nézve nem elvárás, hogy meghatározza a kihasználhatóságát azon lehetséges sebezhetőségeknek, melyek hatásos támadásához alapnál magasabb támadó képesség szükséges. Ugyanakkor értékelői tapasztalata segítségével az értékelő feltárhat olyan lehetséges sebezhetőséget, melyet csak olyan támadó használhat ki, aki alapnál magasabb támadó képességgel rendelkezik. Az ilyen sebezhetőségeket az értékelési jelentésében maradvány sebezhetőségként szerepeltetni kell.

A lehetséges sebezhetőség ismeretében az értékelő határozza meg a leginkább megfelelő módot az STOE érzékenységének kimutatásához. Az értékelő különösen az alábbiakat vegye tekintetbe:

a) az SSF kiváltására és a válaszok megfigyelésére használt interfészek (SSFI);
b) a tesztekhez szükséges kezdeti feltételek;
c) egy SSFI kiváltásához vagy megfigyeléséhez szükséges speciális tesztberendezések;
d) különösen fontos eset, amikor egy kezdeti teszt eredményeként előre jelezhető, hogy egy támadás adott számú megismétlése valószínűleg sikeres lesz.

Az értékelő a behatolás tesztelést valószínűleg tesztesetek sorozatával találja célszerűnek elvégezni, ahol az egyes tesztesetek egy-egy adott lehetséges sebezhetőséget próbálnak ki.

A tesztelési dokumentáció ilyen szintű részletessége azt hivatott biztosítani, hogy más értékelők is meg tudják ismételni a teszteket, és azonos eredményre juthassanak.

ASVA_VAN.2-12 Az értékelőnek végre kell hajtania a behatolás tesztelést.

Az értékelő az ASVA_VAN.2-10 munkaegység eredményeképpen létrejött behatolás tesztelési dokumentációt az STOE behatolás tesztelésének alapjaként használja, de ez nem zárja ki, hogy más, ad hoc behatolás tesztelést ne végezhessen el. Amennyiben szükséges, az értékelő ad hoc teszteket is elvégezhet a behatolás tesztelés során tapasztaltak következtében, melyeket – ha az értékelő elvégzi azokat - a behatolás tesztelési dokumentációban rögzítenie kell. E tesztekkel szemben követelmény lehet, hogy a nem várt eredményeket vagy megfigyeléseket ellenőrizzék, vagy hogy a tesztelés előkészítési szakaszában az értékelőnek javasolt lehetséges sebezhetőségeket megvizsgálják.

Amennyiben a behatolás tesztelés azt mutatja, hogy egy feltételezett lehetséges sebezhetőség nem létezik, az értékelőnek ajánlott megállapítania, hogy a saját elemzése volt téves, vagy az értékelésre átadandók voltak hibásak, hiányosak.

Az értékelőnek nem kell tesztelést végeznie azokon a lehetséges sebezhetőségeken túl (beleértve a nyilvánosan ismerteket is), melyek kihasználásához legfeljebb alap támadó képesség szükséges. Egyes esetekben azonban még a kihasználhatóság meghatározása előtt

szükség lehet egy teszt végrehajtására. Amennyiben értékelői tapasztalata segítségével az értékelő egy megemelt-alap, közepes vagy magas támadó képességgel kihasználható sebezhetőséget tár fel, ezt az értékelési jelentésében maradvány sebezhetőségként szerepeltetnie kell.

ASVA_VAN.2-13 Az értékelőnek rögzítenie kell a behatolás tesztek tényleges eredményeit.
A tényleges eredmények bizonyos részletei különbözhetnek a várható értékektől (pl. idő és dátummezők a naplóban), de az összeredménynek meg kell egyeznie. Javasolt minden váratlan teszteredményt kivizsgálni, valamint ezek értékelésre gyakorolt hatását kimondani és igazolni.

ASVA_VAN.2-14 Az értékelőnek az értékelési jelentés keretén belül jelentést kell írnia az értékelői behatolás tesztelésről, leírván a tesztelési módszert, konfigurációt, mélységet és eredményeket.

Az értékelési jelentésben rögzített behatolás tesztelésről szóló információ lehetővé teszi az értékelő számára, hogy bemutassa az általános tesztelési módszert és az ezen tevékenység végrehajtásába fektetett munkát. A cél az értékelő behatolás tesztelési munkájának érdemi áttekintése. Nem cél, hogy az értékelési jelentésben a behatolás teszteléssel kapcsolatos információk a specifikus tesztlépések vagy egyedi behatolás tesztek eredményeinek pontos megismétlése legyenek. A cél elegendő részletesség biztosítása más értékelők számára ahhoz, hogy betekintést kapjanak a választott behatolás tesztelési módszerbe, a végrehajtott behatolás tesztek nagyságrendjébe, az STOE teszt konfigurációjába és a behatolás tesztelési tevékenység általános eredményébe.

Az értékelési jelentés értékelői behatolás tesztelésről szóló része általában az alábbi információkat tartalmazza:

a) STOE tesztkonfigurációk; a behatolás tesztelésnél használt konkrét STOE konfigurációk.
b) A behatolás teszt során tesztelt interfészek. A behatolás tesztelés középpontjában álló interfészek rövid felsorolása.
c) Az altevékenység alapján született határozat. A behatolás tesztelés eredményeinek általános megítélése.

ASVA_VAN.2-15 Az értékelőnek meg kell vizsgálnia az összes behatolás teszt eredményét annak megállapítása érdekében, hogy az STOE üzemeltetési környezetében ellenáll-e egy alap támadó képességgel rendelkező támadónak.

Amennyiben az eredmények azt mutatják, hogy az STOE üzemeltetési környezetében kihasználható sebezhetőségeket tartalmaz alap támadó képességgel rendelkező támadók számára, akkor ez az értékelői akció "Nem felelt meg" határozatot eredményez.

[7] 7.3.4 mellékletét kell használni egy adott sebezhetőség kihasználásához szükséges támadó képesség meghatározásához, illetve annak eldöntésére, hogy a sebezhetőség a tervezett üzemeltetési környezetben kihasználható-e. Nem feltétlenül kell minden esetben kiszámolni a támadó képességet, csak ha felmerül annak lehetősége, hogy egy alap támadó képességgel rendelkező támadó kihasználhatja a sebezhetőséget.

ASVA_VAN.2-16 Az értékelőnek az értékelési jelentés keretén belül jelentést kell írnia az összes kihasználható sebezhetőségről és maradvány sebezhetőségről, az alábbi adatokkal:

a) forrás (pl. azon CEM tevékenység, melynek végrehajtása során észlelték, az értékelő ismerte, szakirodalomban olvasott róla);
b) a nem kielégített SFR(-ek);
c) leírás;
d) kihasználható-e vagy sem az üzemeltetési környezetben (vagyis kihasználható vagy maradvány sebezhetőségről van szó);
e) az azonosított sebezhetőség kihasználáshoz szükséges felhasznált idő, szakértelem, TOE ismeret, hozzáférési lehetőség, eszköz, valamint az ezekhez rendelt értékek [7] 7.3.4 mellékletének 7. és 8. táblázata alapján.

6.2.4. Kezdeti rendszer értékelés kiemelt garanciacsomag mellett

6.2.4.1. A rendszer biztonsági előirányzat értékelése (ASST)

6.2.4.1.1. Az SST bevezetés (ASST_INT.2) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_INT.2.1E értékelői akció

ASST_INT.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_INT.2.1C Az SST bevezetésnek tartalmaznia kell egy SST hivatkozást, STOE hivatkozást, STOE áttekintést, STOE leírást és egy tartomány kialakítás specifikációt.

ASST_INT.2-1 Az értékelőnek ellenőriznie kell, hogy az SST bevezetés tartalmaz-e SST hivatkozást, STOE hivatkozást, STOE áttekintést, STOE leírást és egy tartomány kialakítás specifikációt.

ASST_INT.2.2C Az SST hivatkozásnak egyedi módon azonosítania kell az SST-t.

ASST_INT.2-2 Az értékelőnek meg kell vizsgálnia az SST hivatkozást annak megállapítása érdekében, hogy az egyértelműen azonosítja-e az SST-t.

Az értékelő állapítsa meg, hogy az SST hivatkozás azonosítja-e az SST-t magát, úgy, hogy az jól megkülönböztethető legyen más SST-ktől, és egyedi módon azonosítja-e az SST minden verzióját, például verziószámmal és/vagy a közzététel dátumával.

Az értékelő ellenőrizheti a hivatkozások egyediségét a konfiguráció lista ellenőrzésével is.

ASST_INT.2.3C Az STOE hivatkozásnak azonosítania kell az STOE-t.

ASST_INT.2-3 Az értékelőnek meg kell vizsgálnia az STOE hivatkozást annak megállapítása érdekében, hogy az egyértelműen azonosítja-e az STOE-t.

Az értékelő állapítsa meg, hogy az STOE hivatkozás oly módon azonosítja az STOE verzióját, például verzió/kibocsátás vagy a kiadás dátuma segítségével.

ASST_INT.2.4C Az STOE áttekintésnek össze kell foglalnia az STOE használatát és fő biztonsági tulajdonságait.

ASST_INT.2-4 Az értékelőnek meg kell vizsgálnia az STOE áttekintést annak megállapítása érdekében, hogy az leírja-e az STOE használatát és fő biztonsági tulajdonságait.

Az STOE áttekintésnek röviden (néhány bekezdésben) le kell írnia az STOE használatát és fő biztonsági tulajdonságait.

Az értékelő állapítsa meg, hogy az áttekintés érthető-e az olvasók számára.

ASST_INT.2.5C Az STOE áttekintésnek azonosítania kell az STOE típusát.

ASST_INT.2-5 Az értékelőnek ellenőriznie kell, hogy az STOE áttekintés azonosítja-e az STOE típusát.

ASST_INT.2.6C Az STOE leírásnak meg kell adnia az STOE fizikai hatókörét és határait, beleértve a fizikai elemek ábráját.

ASST_INT.2-6 Az értékelőnek meg kell vizsgálnia az STOE leírást annak megállapítása érdekében, hogy az leírja-e az STOE fizikai hatókörét és határait.

Az értékelő állapítsa meg, hogy az STOE leírás felsorolja-e az STOE-t alkotó hardvert, szoftvert, förmvert komponenseket és útmutatókat, valamint olyan részletességgel jellemzi-e ezeket, hogy az olvasó általános képet kapjon ezekről.

Az értékelő állapítsa meg azt is, hogy nincs lehetséges félreértés a tekintetben, hogy valamely hardver, szoftver, förmver vagy útmutató elem része-e az STOE-nak vagy sem.

ASST_INT.2-7 Az értékelőnek ellenőriznie kell az STOE leírást annak megállapítása érdekében, hogy az tartalmaz-e egy áttekintő ábrát a fizikai elemekről.

ASST_INT.2.7C Az STOE leírásnak meg kell adnia az STOE logikai hatókörét és határait, beleértve a logikai elemek ábráját.

ASST_INT.2-8 Az értékelőnek meg kell vizsgálnia az STOE leírást annak megállapítása érdekében, hogy az leírja-e az STOE logikai hatókörét és határait.

Az értékelő állapítsa meg, hogy az STOE leírás olyan részletességgel tárgyalja-e az STOE által nyújtott logikai biztonsági szolgáltatásokat, hogy az olvasó általános képet kapjon ezekről.

Az értékelő állapítsa meg azt is, hogy nincs lehetséges félreértés a tekintetben, hogy valamely logikai biztonsági szolgáltatást biztosít-e az STOE vagy sem.

ASST_INT.2-9 Az értékelőnek ellenőriznie kell az STOE leírást annak megállapítása érdekében, hogy az tartalmaz-e egy áttekintő ábrát a logikai elemekről.

ASST_INT.2.8C Az STOE leírásnak azonosítania kell az STOE által igényelt bármilyen külső működő rendszerhez való kapcsolódást és felületet (interfészt).

ASST_INT.2-10 Az értékelőnek meg kell vizsgálnia az STOE leírást annak megállapítása érdekében, hogy az azonosítja-e az STOE által igényelt bármilyen külső működő rendszerhez való kapcsolódást és felületet (interfészt).

ASST_INT.2.9C A tartomány kialakítás specifikációnak meg kell határoznia a létrehozott biztonsági tartományok kialakítását, szervezését, az egyes tartományok azonosítási információit.

ASST_INT.2-11 Az értékelőnek meg kell vizsgálnia a tartomány kialakítás specifikációt annak megállapítása érdekében, hogy az meghatározza-e létrehozott biztonsági tartományok kialakítását, szervezését, az egyes tartományok azonosítási információit.

ASST_INT.2.10C A tartomány kialakítás specifikációnak azonosítania kell az egyes tartományokra azokat a biztonsági célokat, amelyeket az STOE biztonsági tulajdonságaként más tartományok juttatnak érvényre.

ASST_INT.2-12 Az értékelőnek meg kell vizsgálnia a tartomány kialakítás specifikációt annak megállapítása érdekében, hogy az azonosítja-e azokat a biztonsági célokat, amelyeket az STOE biztonsági tulajdonságaként más tartományok juttatnak érvényre.

ASST_INT.2.11C A tartomány kialakítás specifikációnak azonosítania kell az egyes tartományokra azokat a biztonsági célokat, amelyek az STOE biztonsági szolgáltatásaként más tartományok számára is rendelkezésre állnak.

ASST_INT.2-13 Az értékelőnek meg kell vizsgálnia a tartomány kialakítás specifikációt annak megállapítása érdekében, hogy az azonosítja-e azokat a biztonsági célokat, amelyek az STOE biztonsági szolgáltatásaként más tartományok számára is rendelkezésre állnak.

Az ASST_INT.2.2E értékelői akció

ASST_INT.2.2E Az értékelőnek meg kell erősítenie, hogy az STOE hivatkozás, STOE áttekintés, STOE leírás és tartomány kialakítás specifikáció összhangban áll egymással.

ASST_INT.2-14 Az értékelőnek meg kell vizsgálnia, hogy az STOE hivatkozás, STOE áttekintés, STOE leírás és tartomány kialakítás specifikáció összhangban áll egymással.

6.2.4.1.2. A megfelelőség nyilatkozatok (ASST_CCL.3) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_CCL.3.1E értékelői akció

ASST_CCL.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_CCL.3.1C A megfelelőségi nyilatkozatnak azonosítania kell azt a mértékadó dokumentumot, amelyhez az SST és az STOE megfelelőséget állít.

ASST_CCL.3-1 Az értékelőnek ellenőriznie kell a megfelelőségi nyilatkozatot, hogy az azonosítja-e azt a mértékadó dokumentumot, amelyhez az SST és az STOE megfelelőséget állít.

ASST_CCL.3.2C A megfelelőségi nyilatkozatnak azonosítania kell a mértékadó dokumentum azon követelményeit, amelyekhez az SST és az STOE megfelelőséget állít.

ASST_CCL.3-2 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozatot, hogy az azonosítja-e a mértékadó dokumentum azon követelményeit, amelyekhez az SST és az STOE megfelelőséget állít.

ASST_CCL.3.3C A megfelelőségi nyilatkozatban azonosított mértékadó dokumentumnak az alábbiak egyikének kell lennie: [1] (2 rész, funkcionális biztonsági összetevők katalógusa), [2] (A műszaki biztonsági intézkedések katalógusa).

ASST_CCL.3-3 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozatot, hogy az abban azonosított mértékadó dokumentum az alábbiak egyike-e: [1], [2].

ASST_CCL.3.4C Hazai katalógusnak [2] való megfelelőség vállalása esetén a megfelelőségi nyilatkozatnak meg kell határoznia a [2]-ben leírt „kiemelt kihatású biztonsági osztály követelményei” biztonsági követelmény csomagra vonatkozó csomag-megfelelőségét: vagy „megfelel a csomagnak” vagy „módosítja a csomagot”.

ASST_CCL.3-4 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozatot, hogy az [2]-nek való megfelelőség vállalása esetén meghatározza-e az alábbiak egyikét: „megfelel a kiemelt kihatású biztonsági osztály követelményeinek”, „módosítja a kiemelt kihatású biztonsági osztály követelményeit”.

Ha a megfelelőségi nyilatkozat [1]-nek vállal megfelelőséget, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Amennyiben a megfelelőségi nyilatkozat [2]-nek vállal megfelelőséget, de nem határozza meg a ASST_CCL.3-4 alatt említett két lehetőség közül pontosan az egyiket, akkor ez a munkaegység „nem felelt meg” eredményt ad.

ASST_CCL.3.5C Hazai katalógusnak [2] való megfelelőség vállalása esetén, amennyiben a csomag-megfelelőségre vonatkozó nyilatkozat: „módosítja a kiemelt kihatású biztonsági osztály követelményeit”, akkor a megfelelőségi nyilatkozat indoklásnak vissza kell vezetnie minden biztonsági követelményt az STOE biztonsági céljaira.

ASST_CCL.3-5 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozatot, hogy amennyiben az a [2]-nek való megfelelőséget vállalja, „módosítja a kiemelt kihatású biztonsági osztály követelményeit” meghatározás mellett, akkor a megfelelőségi nyilatkozat indoklás visszavezet-e minden biztonsági követelményt az STOE biztonsági céljaira.

Ha a megfelelőségi nyilatkozat [1]-nek vállal megfelelőséget, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.
.
Ha a megfelelőségi nyilatkozat [2]-nek vállal megfelelőséget, „megfelel a kiemelt kihatású biztonsági osztály követelményeinek” meghatározás mellett, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

ASST_CCL.3.6C CC [1] megfelelőség vállalása esetén a megfelelőségi nyilatkozatnak le kell írnia az azonosított szabványnak való megfelelőségét: vagy „megfelel a szabványnak” vagy „kiterjeszti a szabványt”.

ASST_CCL.3-6 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozatot, hogy az [1]-nek való megfelelőséget vállalása esetén meghatározza-e az alábbiak egyikét: „megfelel a szabványnak”, „kiterjeszti a szabványt”.

Ha a megfelelőségi nyilatkozat [2]-nek vállal megfelelőséget, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Amennyiben a megfelelőségi nyilatkozat [1]-nek vállal megfelelőséget, de nem határozza meg a ASST_CCL.3-6 alatt említett két lehetőség közül pontosan az egyiket, akkor ez a munkaegység „nem felelt meg” eredményt ad.

ASST_CCL.3.7C CC [1] megfelelőség vállalása esetén a megfelelőségi nyilatkozat nem mondhat ellent a kiterjesztett CC összetevők meghatározásának.

ASST_CCL.3-7 Az értékelőnek meg kell vizsgálnia a megfelelőségi nyilatkozatot annak megállapítása érdekében, hogy az összhangban áll-e a kiterjesztett összetevők meghatározásával.

Ha a megfelelőségi nyilatkozat [2]-nek vállal megfelelőséget, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Amennyiben a megfelelőségi nyilatkozat [1]-nek vállal megfelelőséget, „megfelel a szabványnak” megállapítás mellett, akkor az értékelő állapítsa meg, hogy a kiterjesztett összetevők meghatározása nem határoz-e meg funkcionális biztonsági összetevőt.

Amennyiben a megfelelőségi nyilatkozat [1]-nek vállal megfelelőséget, „kiterjeszti a szabványt” megállapítás mellett, akkor az értékelő állapítsa meg, hogy a kiterjesztett összetevők meghatározása meghatároz-e legalább egy kiterjesztett funkcionális biztonsági összetevőt.

6.2.4.1.3. A biztonsági probléma meghatározás (ASST_SPD.1) értékelése

Ez az értékelői altevékenység megegyezik a fokozott garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.3.1.3 pont alatt.

6.2.4.1.4. A biztonsági célok (ASST_OBJ.2) értékelése

Ez az értékelői altevékenység megegyezik a fokozott garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.3.1.4 pont alatt.

6.2.4.1.5. A kiterjesztett összetevő meghatározás (ASST_ECD.1) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_ECD.1.1E értékelői akció

ASST_ECD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_ECD.1.1C A biztonsági követelményekről szóló nyilatkozatnak azonosítania kell minden kiterjesztett funkcionális biztonsági követelményt.

ASST_ECD.1-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági követelményekről szóló nyilatkozatában szereplő összes olyan funkcionális biztonsági követelmény, amelyet nem kiterjesztett biztonsági követelményként azonosítottak, szerepel a CC 2. részében.

ASST_ECD.1.2C A kiterjesztett összetevők meghatározásának minden kiterjesztett funkcionális biztonsági követelményre meg kell határoznia egy kiterjesztett összetevőt.

ASST_ECD.1-2 Az értékelőnek ellenőriznie kell, hogy a kiterjesztett összetevők meghatározása minden kiterjesztett funkcionális biztonsági követelményre meghatároz egy kiterjesztett összetevőt.

Amennyiben az SST nem tartalmaz kiterjesztett funkcionális biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Egyetlen kiterjesztett összetevő használható egy kiterjesztett funkcionális biztonsági követelmény több ismétlésének meghatározásához, nem szükséges megismételni ezt a meghatározást minden ismétlésre.

ASST_ECD.1.3C A kiterjesztett összetevők meghatározásának le kell írnia, hogy az egyes kiterjesztett összetevők hogyan kapcsolódnak a meglévő CC összetevőkhöz, családokhoz és osztályokhoz.

ASST_ECD.1-3 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy az leírja, hogy az egyes kiterjesztett összetevők hogyan kapcsolódnak a meglévő CC összetevőkhöz, családokhoz és osztályokhoz.

Amennyiben az SST nem tartalmaz kiterjesztett biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy a kiterjesztett összetevő:
a) a CC 2. rész meglévő családjának tagja, vagy
b) az SST-ben meghatározott új család tagja.

Amennyiben a kiterjesztett összetevő egy CC 2. részbeli meglévő család tagja, akkor az értékelő állapítsa meg, hogy a kiterjesztett összetevő meghatározása megfelelően leírja-e, hogy a kiterjesztett összetevő miért tagja a szóban forgó családnak, és hogyan kapcsolódik a család más összetevőihez.

Ha a kiterjesztett összetevő az SST-ben megadott új család tagja, akkor az értékelő győződjön meg arról, hogy a kiterjesztett összetevő nem illeszkedik egy meglévő családba sem.

Ha az SST új családot határoz meg, az értékelő állapítsa meg, hogy minden új család:
a) a CC 2. részbeli meglévő osztály tagja, vagy
b) az SST-ben meghatározott új osztály tagja.

Amennyiben a család egy CC 2. részbeli meglévő osztály tagja, akkor az értékelő állapítsa meg, hogy a kiterjesztett összetevő meghatározása megfelelően leírja-e, hogy a család miért tagja a szóban forgó osztálynak, és hogyan kapcsolódik az osztály más családjaihoz.

Ha a család az SST-ben megadott új osztály tagja, akkor az értékelő győződjön meg arról, hogy a család nem illeszkedik egy meglévő osztályba sem.

ASST_ECD.1-4 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy az minden kiterjesztett összetevőre azonosítja-e ezen összetevő minden alkalmazandó függését.

Amennyiben az SST nem tartalmaz kiterjesztett funkcionális biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő ellenőrizze, hogy az SST szerzője nem hagyott ki alkalmazandó függést.

ASST_ECD.1.4C A kiterjesztett összetevők meghatározásának a meglévő CC funkcionális összetevőket, családokat, osztályokat és módszertant kell használnia megjelenítési modellként.

ASST_ECD.1-5 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden kiterjesztett funkcionális összetevő a CC 2. rész összetevőit megjelenítési modellként használja.

Ha az SST nem tartalmaz kiterjesztett funkcionális biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy a kiterjesztett funkcionális összetevő összhangban van-e a CC 2. rész 7.2.3 szakasz (Összetevő felépítés) alatt írtakkal.

Amennyiben a kiterjesztett funkcionális összetevőben műveleteket alkalmaztak, az értékelő állapítsa meg, hogy a kiterjesztett funkcionális összetevő összhangban van-e a CC 2. rész 7.1.2 (CC műveletek) pontjával.

Amennyiben a kiterjesztett funkcionális összetevő hierarchia szerint alárendelt egy meglévő funkcionális összetevőnek, akkor az értékelő állapítsa meg, hogy a kiterjesztett funkcionális összetevő összhangban van-e a CC 2. rész 7.3.1 (Összetevő módosítások kiemelése) szakaszban írtakkal.

ASST_ECD.1-6 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden új funkcionális család a CC meglévő családjait megjelenítési modellként használja.

Ha az SST nem határoz meg új funkcionális családot, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy az összes meghatározott új funkcionális család megfelel-e a CC 2. rész 7.2.2 (A családok szerkezete) szakaszban foglaltaknak.

ASST_ECD.1-7 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden új funkcionális osztály a CC meglévő osztályait megjelenítési modellként használja.

Ha az SST nem határoz meg új funkcionális osztályt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy az összes meghatározott új funkcionális osztály megfelel-e a CC 2. rész 7.2.1 (Az osztályok szerkezete) szakaszban foglaltaknak.

ASST_ECD.1.5C A kiterjesztett összetevőknek mérhető és objektív elemekből kell állniuk, hogy megfelelőségük vagy nem megfelelőségük kimutatható legyen.

ASST_ECD.1-8 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden kiterjesztett összetevő minden eleme mérhető és

olyan objektív értékelési követelményeket állít, amelyeknek való megfelelőség vagy nem megfelelőség kimutatható.

Az ASST_ECD.1.2E értékelői akció

ASST_ECD.1.2E Az értékelőnek meg kell erősítenie, hogy nincs olyan kiterjesztett összetevő, ami kifejezhető lenne egyértelműen a meglévő összetevők segítségével.

ASST_ECD.1-9 Az értékelőnek meg kell vizsgálnia a kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy egyetlen kiterjesztett összetevő sem fejezhető ki egyértelműen a meglévő összetevők segítségével.

Amennyiben az SST nem tartalmaz kiterjesztett funkcionális biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelőnek ennek meghatározása során figyelembe kell vennie a CC 2. részében szereplő összetevőket, az SST-ben meghatározott egyéb kiterjesztett összetevőket, ezen összetevők kombinációit és a lehetséges műveleteket.

Az értékelőnek szem előtt kell tartania, hogy e munkaegység szerepe az olyan összetevők szükségtelen duplázásának megakadályozása, amelyek egyértelműen kifejezhetők más összetevők segítségével. Az értékelőnek nem kell végrehajtania az összetevők összes kombinációjának teljes feltárását, ideértve a műveleteket is, hogy mindenféleképpen kifejezze a kiterjesztett összetevőt a meglévőkkel.

6.2.4.1.6. A biztonsági követelmények (ASST_REQ.3) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_REQ.3.1E értékelői akció

ASST_REQ.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_REQ.3.1C A biztonsági követelményekre vonatkozó állításnak le kell írnia a rendszertől elvárt biztonsági funkcionalitást (SSF) és garanciákat (SAP).

ASST_REQ.3-1 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot annak megállapítása érdekében, hogy az leírja-e az elvárt rendszer biztonsági funkcionalitást (SSF).

ASST_REQ.3-2 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot annak megállapítása érdekében, hogy az leírja-e az elvárt garanciákat (SAP).

ASST_REQ.3.2C Az elvárt rendszer biztonsági funkcionalitást az alábbi mértékadó dokumentumokból kell választani: [2] műszaki biztonsági intézkedések katalógusa, [1] CC funkcionális biztonsági összetevők katalógusa.

ASST_REQ.3-3 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot, hogy az abban azonosított mértékadó dokumentum az alábbiak egyike-e: [1], [2].

ASST_REQ.3.3C Az elvárt rendszer garanciacsomagnak az alábbinak kell lennie: SAP-K.

ASST_REQ.3-4 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot, hogy az abban azonosított garanciacsomag az alábbi-e: SAP-K.

ASST_REQ.3.4C A biztonsági követelményekről szóló nyilatkozatnak azonosítania kell a biztonsági követelményekre vonatkozó összes műveletet.

ASST_REQ.3-5 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az azonosítja-e a funkcionális biztonsági követelményekre vonatkozó összes műveletet.

Az értékelő állapítsa meg, hogy minden SFR-ben lévő minden műveletet azonosítottak, ahol használtak ilyet. Az azonosítás elérhető tipográfiai megkülönböztetéssel, vagy explicit azonosítással a környező szöveghez képest, vagy bármilyen más megkülönböztető eszközzel.

ASST_REQ.3.5C Minden értékadási és kiválasztási műveletet be kell fejezni.

ASST_REQ.3-6 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az befejezett-e minden értékadási műveletet.

ASST_REQ.3-7 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az befejezett-e minden kiválasztási műveletet.

ASST_REQ.3.6C Minden műveletet jól kell végrehajtani.

ASST_REQ.3-8 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az minden műveletet helyesen hajt-e végre..

ASST_REQ.3.7C A biztonsági követelmények minden egyes függését vagy teljesíteni kell, vagy a biztonsági követelmények indoklásában igazolni kell a függés ki nem elégítését.

ASST_REQ.3-9 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy a biztonsági követelmények minden függési viszonyát vagy teljesítették, vagy a biztonsági követelmények indoklása igazolja a függés nem teljesítését.

Egy függés kielégíthető a vonatkozó (vagy hierarchikusan hozzá tartozó) összetevő beemelésével a biztonsági követelményekről szóló nyilatkozatba. A függések kielégítéséhez használt összetevőnek szükség esetén műveletekkel módosíthatónak kell lennie a függés tényleges kielégítéséhez.

Egy függés nem teljesülésének indoklása során ki kell mutatni, hogy:

a) a függés teljesülésére miért nincs szükség, vagy miért nem jár haszonnal; ekkor nincs szükség további információra, vagy
b) a függést az STOE üzemeltetési környezete teljesíti; ekkor az igazolásnak le kell írnia, hogy az üzemeltetési környezetre vonatkozó biztonsági célok hogyan elégítik ki ezt a függést.

ASST_REQ.3.8C A biztonsági követelmények indoklásának az SSF-et vissza kell vezetnie az STOE biztonsági céljaira.

ASST_REQ.3-10 Az értékelőnek ellenőriznie kell, hogy a biztonság követelmények indoklása visszavezet-e minden SFR-t az STOE biztonsági céljaira.

Az értékelő állapítsa meg, hogy minden egyes SFR visszavezethető legalább egy STOE biztonsági célra.

A visszavezetés sikertelensége vagy azt jelenti, hogy a biztonsági követelmények indoklása nem teljes, az STOE biztonsági céljai nem teljesek, vagy az SFR nem tölt be igazi célt.

ASST_REQ.3.9C A biztonsági követelmények indoklásának meg kell mutatnia, hogy az SSF teljesíti az STOE összes biztonsági célját, amelyeket külső rendszerek nem elégítenek ki.

ASST_REQ.3-11 Az értékelőnek meg kell vizsgálnia a biztonsági követelmények indoklását annak megállapítása érdekében, hogy az STOE összes biztonsági céljára megmutatták, hogy az SFR-k alkalmasak az adott STOE biztonsági cél teljesítésére, vagy az adott biztonsági célt külső rendszerek elégítik ki.

Amennyiben az SFR-ek nem vezethetők vissza az STOE biztonsági céljaira, az e munkaegységhez kapcsolódó értékelői tevékenység során „nem felelt meg” döntés születik.

Az értékelő állapítsa meg, hogy az STOE biztonsági céljainak indoklása megmutatja-e, hogy az SFR-ek kielégítők: azaz, ha a célra visszavezethető minden SFR-t kielégítenek, akkor az STOE biztonsági cél teljesül.

Az értékelő azt is állapítsa meg, hogy egy STOE biztonsági célra visszavezethető összes SFR szükséges: azaz az SFR teljesülése ténylegesen hozzájárul a biztonsági cél eléréséhez.

Az ASST_REQ.3.2E értékelői akció

ASST_REQ.3.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági követelményekről szóló nyilatkozat belső ellentmondásoktól mentes.

ASST_REQ.3-12 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy az belső ellentmondásoktól mentes.

Az értékelő állapítsa meg, hogy az SSF és SAP kombinációja belső ellentmondásoktól mentes.

Néhány lehetséges ellentmondás:

a) SSF egyetlen mértékadó dokumentumokból került kiválasztásra, de a kiválasztott SFR-ek ellentmondanak egymásnak;
b) SSF több mértékadó dokumentumokból került kiválasztásra és a kiválasztott SFR-ek ellentmondanak egymásnak.

Az ASST_REQ.3.3E értékelői akció

ASST_REQ.3.3E Az értékelőnek meg kell erősítenie, hogy a biztonsági követelményekről szóló nyilatkozat egy teljes, egymást erősítő követelményrendszert határoz meg.

ASST_REQ.3-13 Az értékelőnek meg kell vizsgálnia a biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy az egy teljes, egymást erősítő követelményrendszert határoz-e meg.

6.2.4.1.7. Az STOE összefoglaló előírás (ASST_SSS.1) értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.1.7 pont alatt.

6.2.4.1.8. A biztonsági tartomány bevezetés (ASST_SDI.1) értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.1.8 pont alatt.

6.2.4.1.9. A biztonsági tartomány megfelelőségi nyilatkozatok (ASST_SDC.3) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_SDC.3.1E értékelői akció

ASST_SDC.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDC.3.1C A biztonsági tartomány megfelelőségi nyilatkozatnak azonosítania kell azt a mértékadó dokumentumot, amelyhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.3-1 Az értékelőnek ellenőriznie kell a biztonsági tartomány megfelelőségi nyilatkozatot, hogy az azonosítja-e azt a mértékadó dokumentumot, amelyhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.3.2C A biztonsági tartomány megfelelőségi nyilatkozatnak azonosítania kell a mértékadó dokumentum azon követelményeit, amelyekhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.3-2 Az értékelőnek ellenőriznie kell a biztonsági tartomány megfelelőségi nyilatkozatot, hogy az azonosítja-e a mértékadó dokumentum azon követelményeit, amelyekhez a biztonsági tartomány megfelelőséget állít.

ASST_SDC.3.3C A biztonsági tartomány megfelelőségi nyilatkozatban azonosított mértékadó dokumentumnak az alábbiak egyikének kell lennie: [2] (A műszaki biztonsági intézkedések katalógusa), [1] (2 rész, funkcionális biztonsági összetevők katalógusa).

ASST_SDC.3-3 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány megfelelőségi nyilatkozatot, hogy az abban azonosított mértékadó dokumentum az alábbiak egyike-e: [1], [2].

ASST_SDC.3.4C Hazai katalógusnak [2] való megfelelőség vállalása esetén a biztonsági tartomány megfelelőségi nyilatkozatnak meg kell határoznia a [2]-ben leírt „kiemelt kihatású biztonsági osztály követelményei” biztonsági követelmény csomagra vonatkozó csomag-megfelelőségét: vagy „megfelel a csomagnak” vagy „módosítja a csomagot”.

ASST_SDC.3-4 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány megfelelőségi nyilatkozatot, hogy az [2]-nek való megfelelőség vállalása esetén meghatározza-e az alábbiak egyikét: „megfelel a kiemelt kihatású biztonsági osztály követelményeinek”, „módosítja a kiemelt kihatású biztonsági osztály követelményeit”.

Ha a biztonsági tartomány megfelelőségi nyilatkozat [1]-nek vállal megfelelőséget, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Amennyiben a biztonsági tartomány megfelelőségi nyilatkozat [2]-nek vállal megfelelőséget, de nem határozza meg a ASST_SDC.3-4 alatt említett két lehetőség közül pontosan az egyiket, akkor ez a munkaegység „nem felelt meg” eredményt ad.

ASST_SDC.3.5C Hazai katalógusnak [2] való megfelelőség vállalása esetén, amennyiben a csomag-megfelelőségre vonatkozó nyilatkozat: „módosítja a csomagot”, akkor a biztonsági tartomány megfelelőségi nyilatkozat indoklásnak vissza kell vezetnie a biztonsági tartomány minden biztonsági követelményét a biztonsági tartomány biztonsági céljaira.

ASST_SDC.3-5 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány megfelelőségi nyilatkozatot, hogy amennyiben az a [2]-nek való megfelelőséget vállalja, „módosítja a kiemelt kihatású biztonsági osztály követelményeit” meghatározás mellett, akkor a biztonsági tartomány megfelelőségi nyilatkozat indoklás visszavezet-e minden biztonsági követelményt a biztonsági tartomány biztonsági céljaira.

Ha a biztonsági tartomány megfelelőségi nyilatkozat [1]-nek vállal megfelelőséget, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Ha a biztonsági tartomány megfelelőségi nyilatkozat [2]-nek vállal megfelelőséget, „megfelel a kiemelt kihatású biztonsági osztály követelményeinek” meghatározás mellett, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

ASST_SDC.3.6C CC [1] megfelelőség vállalása esetén a biztonsági tartomány megfelelőségi nyilatkozatnak le kell írnia az azonosított szabványnak való megfelelőségét: vagy „megfelel a szabványnak” vagy „kiterjeszti a szabványt”.

ASST_SDC.3-6 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány megfelelőségi nyilatkozatot, hogy az [1]-nek való megfelelőséget vállalása esetén meghatározza-e az alábbiak egyikét: „megfelel a szabványnak”, „kiterjeszti a szabványt”.

Ha a biztonsági tartomány megfelelőségi nyilatkozat [2]-nek vállal megfelelőséget, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Amennyiben a biztonsági tartomány megfelelőségi nyilatkozat [1]-nek vállal megfelelőséget, de nem határozza meg a ASST_SDC.3-6 alatt említett két lehetőség közül pontosan az egyiket, akkor ez a munkaegység „nem felelt meg” eredményt ad.

ASST_SDC.3.7C CC megfelelőség vállalása esetén a biztonsági tartomány megfelelőségi nyilatkozat nem mondhat ellent a kiterjesztett CC összetevők meghatározásának.

ASST_SDC.3-7 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány megfelelőségi nyilatkozatot annak megállapítása érdekében, hogy az összhangban áll-e a kiterjesztett összetevők meghatározásával.

Ha a biztonsági tartomány megfelelőségi nyilatkozat [2]-nek vállal megfelelőséget, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Amennyiben a biztonsági tartomány megfelelőségi nyilatkozat [1]-nek vállal megfelelőséget, „megfelel a szabványnak” megállapítás mellett, akkor az értékelő állapítsa meg, hogy a kiterjesztett összetevők meghatározása nem határoz-e meg funkcionális biztonsági összetevőt.

Amennyiben a biztonsági tartomány megfelelőségi nyilatkozat [1]-nek vállal megfelelőséget, „kiterjeszti a szabványt” megállapítás mellett, akkor az értékelő állapítsa meg, hogy a kiterjesztett összetevők meghatározása meghatároz-e legalább egy kiterjesztett funkcionális biztonsági összetevőt.

6.2.4.1.10. A biztonsági tartomány biztonsági probléma meghatározás (ASST_SDP.1) értékelése

Ez az értékelői altevékenység megegyezik a fokozott garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.3.1.10 pont alatt.

6.2.4.1.11. A biztonsági tartomány biztonsági célok (ASST_SDO.2) értékelése

Ez az értékelői altevékenység megegyezik a fokozott garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.3.1.11 pont alatt.

6.2.4.1.12. A biztonsági tartomány kiterjesztett összetevő meghatározás (ASST_SDE.1) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_SDE.1.1E értékelői akció

ASST_SDE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDE.1.1C A biztonsági tartomány biztonsági követelményekről szóló nyilatkozatnak azonosítania kell minden kiterjesztett funkcionális biztonsági követelményt.

ASST_SDE.1-1 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány biztonsági követelményekről szóló nyilatkozatában szereplő összes olyan funkcionális biztonsági követelmény, amelyet nem kiterjesztett biztonsági követelményként azonosítottak, szerepel a CC 2. részében.

ASST_SDE.1.2C A biztonsági tartomány kiterjesztett összetevők meghatározásának minden kiterjesztett funkcionális biztonsági követelményre meg kell határoznia egy kiterjesztett összetevőt.

ASST_SDE.1-2 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány kiterjesztett összetevők meghatározása minden kiterjesztett funkcionális biztonsági követelményre meghatároz egy kiterjesztett összetevőt.

Amennyiben a biztonsági tartomány nem tartalmaz kiterjesztett funkcionális biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Egyetlen kiterjesztett összetevő használható egy kiterjesztett funkcionális biztonsági követelmény több ismétlésének meghatározásához, nem szükséges megismételni ezt a meghatározást minden ismétlésre.

ASST_SDE.1.3C A biztonsági tartomány kiterjesztett összetevők meghatározásának le kell írnia, hogy az egyes kiterjesztett összetevők hogyan kapcsolódnak a meglévő CC összetevőkhöz, családokhoz és osztályokhoz.

ASST_SDE.1-3 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy az leírja, hogy az egyes kiterjesztett összetevők hogyan kapcsolódnak a meglévő CC összetevőkhöz, családokhoz és osztályokhoz.

Amennyiben a biztonsági tartomány nem tartalmaz kiterjesztett biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy a kiterjesztett összetevő:
a) a CC 2. rész meglévő családjának tagja, vagy
b) az SST-ben meghatározott új család tagja.

Amennyiben a kiterjesztett összetevő egy CC 2. részbeli meglévő család tagja, akkor az értékelő állapítsa meg, hogy a kiterjesztett összetevő meghatározása megfelelően leírja-e, hogy a kiterjesztett összetevő miért tagja a szóban forgó családnak, és hogyan kapcsolódik a család más összetevőihez.

Ha a kiterjesztett összetevő az SST-ben megadott új család tagja, akkor az értékelő győződjön meg arról, hogy a kiterjesztett összetevő nem illeszkedik egy meglévő családba sem.

Ha az SST új családot határoz meg, az értékelő állapítsa meg, hogy minden új család:
a) a CC 2. részbeli meglévő osztály tagja, vagy
b) az SST-ben meghatározott új osztály tagja.

Amennyiben a család egy CC 2. részbeli meglévő osztály tagja, akkor az értékelő állapítsa meg, hogy a kiterjesztett összetevő meghatározása megfelelően leírja-e, hogy a család miért tagja a szóban forgó osztálynak, és hogyan kapcsolódik az osztály más családjaihoz.

Ha a család az SST-ben megadott új osztály tagja, akkor az értékelő győződjön meg arról, hogy a család nem illeszkedik egy meglévő osztályba sem.

ASST_SDE.1-4 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy az minden kiterjesztett összetevőre azonosítja-e ezen összetevő minden alkalmazandó függését.

Amennyiben a biztonsági tartomány nem tartalmaz kiterjesztett funkcionális biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő ellenőrizze, hogy az SST szerzője nem hagyott ki alkalmazandó függést.

ASST_SDE.1.4C A biztonsági tartomány kiterjesztett összetevők meghatározásának a meglévő CC funkcionális összetevőket, családokat, osztályokat és módszertant kell használnia megjelenítési modellként.

ASST_SDE.1-5 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden kiterjesztett funkcionális összetevő a CC 2. rész összetevőit megjelenítési modellként használja.

Ha a biztonsági tartomány nem tartalmaz kiterjesztett funkcionális biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy a kiterjesztett funkcionális összetevő összhangban van-e a CC 2. rész 7.2.3 szakasz (Összetevő felépítés) alatt írtakkal.

Amennyiben a biztonsági tartomány kiterjesztett funkcionális összetevőben műveleteket alkalmaztak, az értékelő állapítsa meg, hogy a kiterjesztett funkcionális összetevő összhangban van-e a CC 2. rész 7.1.2 (CC műveletek) pontjával.

Amennyiben a biztonsági tartomány kiterjesztett funkcionális összetevő hierarchia szerint alárendelt egy meglévő funkcionális összetevőnek, akkor az értékelő állapítsa meg, hogy a kiterjesztett funkcionális összetevő összhangban van-e a CC 2. rész 7.3.1 (Összetevő módosítások kiemelése) szakaszban írtakkal.

ASST_SDE.1-6 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden új funkcionális család a CC meglévő családjait megjelenítési modellként használja.

Ha az SST nem határoz meg új funkcionális családot, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy az összes meghatározott új funkcionális család megfelel-e a CC 2. rész 7.2.2 (A családok szerkezete) szakaszban foglaltaknak.

ASST_SDE.1-7 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden új funkcionális osztály a CC meglévő osztályait megjelenítési modellként használja.

Ha az SST nem határoz meg új funkcionális osztályt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelő állapítsa meg, hogy az összes meghatározott új funkcionális osztály megfelel-e a CC 2. rész 7.2.1 (Az osztályok szerkezete) szakaszban foglaltaknak.

ASST_SDE.1.5C A kiterjesztett összetevőknek mérhető és objektív elemekből kell állniuk, hogy megfelelőségük vagy nem megfelelőségük kimutatható legyen.

ASST_SDE.1-8 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy minden kiterjesztett összetevő minden eleme mérhető és olyan objektív értékelési követelményeket állít, amelyeknek való megfelelőség vagy nem megfelelőség kimutatható.

Az ASST_SDE.1.2E értékelői akció

ASST_SDE.1.2E Az értékelőnek meg kell erősítenie, hogy nincs olyan kiterjesztett összetevő, ami kifejezhető lenne egyértelműen a meglévő összetevők segítségével.

ASST_SDE.1-9 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány kiterjesztett összetevők meghatározását annak megállapítása érdekében, hogy egyetlen kiterjesztett összetevő sem fejezhető ki egyértelműen a meglévő összetevők segítségével.

Amennyiben a biztonsági tartomány nem tartalmaz kiterjesztett funkcionális biztonsági követelményt, akkor ez a munkaegység nem alkalmazható, ezáltal teljesítettnek tekinthető.

Az értékelőnek ennek meghatározása során figyelembe kell vennie a CC 2. részében szereplő összetevőket, az SST-ben meghatározott egyéb kiterjesztett összetevőket, ezen összetevők kombinációit és a lehetséges műveleteket.

Az értékelőnek szem előtt kell tartania, hogy e munkaegység szerepe az olyan összetevők szükségtelen duplázásának megakadályozása, amelyek egyértelműen kifejezhetők más összetevők segítségével. Az értékelőnek nem kell végrehajtania az összetevők összes kombinációjának teljes feltárását, ideértve a műveleteket is, hogy mindenféleképpen kifejezze a kiterjesztett összetevőt a meglévőkkel.

6.2.4.1.13. A biztonsági tartomány biztonsági követelmények (ASST_SDR.3) értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST.

Az ASST_SDR.3.1E értékelői akció

ASST_SDR.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASST_SDR.3.1C A biztonsági tartomány biztonsági követelményekre vonatkozó állításnak le kell írnia az adott biztonsági tartományra elvárt biztonsági funkcionalitást (SF) és az elvárt rendszer garanciákat (SAP).

ASST_SDR.3-1 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot annak megállapítása érdekében, hogy az leírja-e az adott biztonsági tartományra elvárt biztonsági funkcionalitást (SF).

ASST_SDR.3-2 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot annak megállapítása érdekében, hogy az leírja-e az elvárt garanciákat (SAP).

ASST_SDR.3.2C Az elvárt biztonsági funkcionalitást az alábbi mértékadó dokumentumokból kell választani: [2] műszaki biztonsági intézkedések katalógusa), [1] CC funkcionális biztonsági összetevők katalógusa.

.

ASST_SDR.3-3 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, hogy az abban azonosított mértékadó dokumentum az alábbiak egyike-e: [1], [2].

ASST_SDR.3.3C Az elvárt rendszer garanciacsomagnak az alábbiak egyikének kell lennie: SAP-**K** vagy megemelt SAP-**K.**

ASST_SDR.3-4 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, hogy az abban azonosított garanciacsomag az alábbiak egyike-e: SAP-**K** vagy megemelt SAP-**K**.

ASST_SDR.3.4C A biztonsági tartomány biztonsági követelményekről szóló nyilatkozatnak azonosítania kell a biztonsági követelményekre vonatkozó összes műveletet.

ASST_SDR.3-5 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az azonosítja-e a funkcionális biztonsági követelményekre vonatkozó összes műveletet.

Az értékelő állapítsa meg, hogy minden SFR-ben lévő minden műveletet azonosítottak, ahol használtak ilyet. Az azonosítás elérhető tipográfiai megkülönböztetéssel, vagy explicit azonosítással a környező szöveghez képest, vagy bármilyen más megkülönböztető eszközzel.

ASST_SDR.3.5C Minden értékadási és kiválasztási műveletet be kell fejezni.

ASST_SDR.3-6 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az befejezett-e minden értékadási műveletet.

ASST_SDR.3-7 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az befejezett-e minden kiválasztási műveletet.

ASST_SDR.3.6C Minden műveletet jól kell végrehajtani.

ASST_SDR.3-8 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekre vonatkozó nyilatkozatot, annak megállapítása érdekében, hogy az minden műveletet helyesen hajt-e végre..

ASST_SDR.3.7C A biztonsági tartomány biztonsági követelmények minden egyes függését vagy teljesíteni kell, vagy a biztonsági követelmények indoklásában igazolni kell a függés ki nem elégítését.

ASST_SDR.3-9 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy a biztonsági követelmények minden függési viszonyát vagy teljesítették, vagy a biztonsági követelmények indoklása igazolja a függés nem teljesítését.

Egy függés kielégíthető a vonatkozó (vagy hierarchikusan hozzá tartozó) összetevő beemelésével a biztonsági követelményekről szóló nyilatkozatba. A függések kielégítéséhez használt összetevőnek szükség esetén műveletekkel módosíthatónak kell lennie a függés tényleges kielégítéséhez.

Egy függés nem teljesülésének indoklása során ki kell mutatni, hogy:

a) a függés teljesülésére miért nincs szükség, vagy miért nem jár haszonnal; ekkor nincs szükség további információra, vagy
b) a függést az STOE üzemeltetési környezete teljesíti; ekkor az igazolásnak le kell írnia, hogy az üzemeltetési környezetre vonatkozó biztonsági célok hogyan elégítik ki ezt a függést.

ASST_SDR.3.8C A biztonsági tartomány biztonsági követelmények indoklásának az SF-et vissza kell vezetnie az adott biztonsági tartomány biztonsági céljaira.

ASST_SDR.3-10 Az értékelőnek ellenőriznie kell, hogy a biztonsági tartomány biztonság követelmények indoklása visszavezet-e minden SFR-t az adott biztonsági tartomány biztonsági céljaira.

Az értékelő állapítsa meg, hogy minden egyes SFR visszavezethető az adott biztonsági tartomány legalább egy biztonsági céljára.

A visszavezetés sikertelensége vagy azt jelenti, hogy a biztonsági tartomány biztonsági követelmények indoklása nem teljes, a biztonsági tartomány biztonsági céljai nem teljesek, vagy az SFR nem tölt be igazi célt.

ASST_SDR.3.9C A biztonsági tartomány biztonsági követelmények indoklásának meg kell mutatnia, hogy az SSF teljesíti az STOE összes biztonsági célját, amelyeket külső rendszerek nem elégítenek ki.

ASST_SDR.3-11 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelmények indoklását annak megállapítása érdekében, hogy az adott biztonsági tartomány összes biztonsági céljára megmutatták, hogy az SFR-k alkalmasak az adott biztonsági tartomány biztonsági céljának a teljesítésére, vagy az adott biztonsági célt külső rendszerek elégítik ki.

Amennyiben az SFR-ek nem vezethetők vissza az adott biztonsági tartomány biztonsági céljaira, az e munkaegységhez kapcsolódó értékelői tevékenység során „nem felelt meg” döntés születik.

Az értékelő állapítsa meg, hogy a biztonsági tartomány biztonsági céljainak indoklása megmutatja-e, hogy az SFR-ek kielégítők: azaz, ha a célra visszavezethető minden SFR-t kielégítenek, akkor a biztonsági tartomány biztonsági célja teljesül.

Az értékelő azt is állapítsa meg, hogy a biztonsági tartomány egy adott biztonsági céljára visszavezethető összes SFR szükséges: azaz az SFR teljesülése ténylegesen hozzájárul a biztonsági cél eléréséhez.

Az ASST_SDR.3.2E értékelői akció

ASST_SDR.3.2E Az értékelőnek meg kell erősítenie, hogy a biztonsági követelményekről szóló nyilatkozat belső ellentmondásoktól mentes.

ASST_SDR.3-12 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy az belső ellentmondásoktól mentes.

Az ASST_SDR.3.3E értékelői akció

ASST_SDR.3.3E Az értékelőnek meg kell erősítenie, hogy a biztonsági tartomány biztonsági követelményekről szóló nyilatkozat egy teljes, egymást erősítő követelményrendszert határoz meg.

ASST_SDR.3-13 Az értékelőnek meg kell vizsgálnia a biztonsági tartomány biztonsági követelményekről szóló nyilatkozatot annak megállapítása érdekében, hogy az egy teljes, egymást erősítő követelményrendszert határoz-e meg.

6.2.4.1.14. A biztonsági tartomány összefoglaló előírás (ASST_SDS.1) értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.1.14 pont alatt.

6.2.4.2. A rendszer fejlesztés garanciaosztály (ASDV) értékelése

6.2.4.2.1. Rendszer architektúra leírás: ASDV_ARC.1 értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.2.1 pont alatt.

6.2.4.2.2. Interfész rendszer interfész specifikáció: ASDV_SIS.2 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
c) rendszer interfész specifikáció,
d) STOE terv.
e) biztonsági architektúra leírás,
f) üzemeltetési útmutató.

Az ASDV_SIS.2.1E értékelői akció

ASDV_SIS.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_SIS.2.1C A rendszer interfész specifikációnak informális stílusban le kell írnia az STOE biztonsági funkcionalitását (SSF) és annak külső interfészeit.

ASDV_SIS.2-1 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy az tartalmazza-e az összes szükséges informális magyarázatot.

Amennyiben az egész rendszer interfész specifikáció informális, akkor ez a munkaegység nem alkalmazható, következésképp teljesítettnek tekinthető.

A rendszer interfész specifikáció olyan részeihez, melyeket nehéz megérteni csak félformális vagy formális leírásokból, kiegészítésként szükség van magyarázó leírásra is (pl. a formális jelölésrendszer jelentésének megvilágításához).

ASDV_SIS.2.2C A rendszer interfész specifikációnak belső ellentmondásoktól mentesnek kell lennie.

ASDV_SIS.2-2 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy az belső ellentmondásoktól mentes-e.

Az értékelőnek meg kell erősítenie, hogy a rendszer interfész specifikációban az interfészek leírása összhangban áll az SSF funkciók leírásával.

ASDV_SIS.2.3C A rendszer interfész specifikációnak le kell írnia minden külső TSF interfész használatának célját és módját, **teljesen** részletezve **minden** hatást, kivételt és hibaüzenet.

ASDV_SIS.2-3 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy az azonosít-e minden külső TSF interfészt.
A "külső" jelző a felhasználó által látottakat jelenti.

ASDV_SIS.2-4 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy leírták-e benne az összes külső TSF interfészt.

ASDV_SIS.2-5 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy az megfelelően és helyesen írja-e le az STOE viselkedését minden külső interfészre a hatások, kivételek és hibaüzenetek tekintetében.

Egy interfész bemutatás megfelelőségének és helyességének vizsgálatát az értékelő a rendszer interfész specifikáció, az SST-ben található STOE összefoglaló előírás, valamint az üzemeltetési útmutató alapján végzi, a következő tényezők értékelése érdekében:

a) Minden biztonsági szempontból fontos bemenő paramétert (vagy az ilyen paraméterek jellemzőit) azonosítani kell.
b) Az útmutatóban leírt biztonsági szempontból fontos teljes működést szerepeltetni kell a rendszer interfész specifikációban. Ennek meg kell határoznia a működést az események és azok hatásának tükrében.
c) Minden interfészt minden lehetséges üzemmódra le kell írni.
d) A biztonsági szempontból fontos paraméterekre és az interfész szintaxis leírására vonatkozó információknak ellentmondás menteseknek kell lenniük a teljes dokumentációban.

A fenti ellenőrzés a rendszer interfész specifikáció és az STOE összefoglaló előírás átvizsgálásával, valamint az üzemeltetési útmutató segítségével történik.

Ez a vizsgálat iteratív is lehet, hiszen az értékelő nem biztos, hogy felfedezi a rendszer interfész specifikáció hiányosságait a tervek vagy egyéb értékelési bizonyítékok vizsgálata nélkül, mely alapján találhat olyan paramétereket vagy hibaüzeneteket, amelyek kimaradtak a rendszer interfész specifikációból.

ASDV_SIS.2.4C A rendszer interfész specifikációnak teljes mértékben be kell mutatnia az SSF-et.

ASDV_SIS.2-6 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt, annak megállapítása érdekében, hogy az SSF-t teljes mértékben bemutatják-e benne.

Az TSF bemutatás teljességét az értékelő az STOE összefoglaló előírás és az üzemeltetési útmutató alapján mérje fel. Ezek egyike sem írhat le olyan biztonsági funkciót, amely hiányzik a rendszer interfész specifikáció TSF bemutatásából.

ASDV_SIS.2.5C **A rendszer interfész specifikációnak egy indoklást kell tartalmaznia arról, hogy teljes mértékben bemutatja az SSF-et.**

ASDV_SIS.2-7 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy az meggyőző indoklást tartalmaz-e arról, hogy az SSF-t teljes mértékben bemutatták benne.

Az értékelő állapítsa meg, hogy meggyőző-e annak indoklása, hogy egyetlen TSF interfész sem maradt ki a rendszer interfész specifikációból. Az indoklás tartalmazhatja annak az eljárásnak vagy módszertannak a leírását, melyet a rendszer integrátor használt annak biztosítására, hogy valamennyi külső interfészt lefedjen. Az indoklás elégtelen, ha az értékelő egy másik értékelői bizonyítékban talál bármilyen olyan parancsot, paramétert, hibaüzenetet vagy egyéb interfészt, mely hiányzik a rendszer interfész specifikációból.

Az ASDV_SIS.2.2E értékelői akció

ASDV_SIS.2.2E Az értékelőnek meg kell állapítania, hogy a rendszer interfész specifikáció az STOE funkcionális biztonsági követelményeinek pontos és teljes megjelenítése.

ASDV_SIS.2-8 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy az az STOE funkcionális biztonsági követelményeinek teljes megvalósulása-e.

ASDV_SIS.2-9 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy az az STOE funkcionális biztonsági követelményeinek pontos megvalósulása-e.

6.2.4.2.3. Rendszer biztonsági terv: ASDV_SDS.1 értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.2.3 pont alatt.

6.2.4.2.4. Rendszer-működési biztonsági koncepció: ASDV_OSC.1 értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.2.4 pont alatt.

6.2.4.3. A rendszer útmutató dokumentumok garanciaosztály (ASGD) értékelése

Ez a teljes értékelői tevékenység megegyezik a fokozott garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.3.3 pont alatt.

6.2.4.4. A rendszer konfiguráció kezelés garanciaosztály (ASCM) értékelése

6.2.4.4.1. Rendszer alap konfiguráció: ASCM_SBC.2 értékelése

Ez az értékelői altevékenység megegyezik a fokozott garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.3.4.1 pont alatt.

6.2.4.4.2. Értékelt és tanúsított komponensek: ASCM_ECC.3 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) CM dokumentáció a rendszer alap konfigurációjához,
b) STOE terv,
c) értékelt és tanúsított termék-komponensek listája.

Az ASCM_ECC.3.1E értékelői akció

ASCM_ECC.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASCM_ECC.3.1C Az értékelt és tanúsított termék-komponensek listájában le kell írni az értékelt és tanúsított termékek garanciacsomagjait.

ASCM_ECC.3-1 Az értékelőnek meg kell vizsgálnia, hogy értékelt és tanúsított termék-komponensek listája a rendszer valamennyi STOE tervben azonosított komponensét tartalmazza-e.

ASCM_ECC.3-2 Az értékelőnek ellenőriznie kell, hogy értékelt és tanúsított termék-komponensek listája leírja-e az egyes értékelt és tanúsított termékek garanciacsomagjait.

A leírás az alábbi garanciacsomagokat tartalmazhatja: CC EAL1, CC EAL1+, CC EAL2, CC EAL2+, CC EAL3, CC EAL3+, CC EAL4, CC EAL4 felett, MIBÉTS alap, MIBÉTS fokozott, MIBÉTS kiemelt, nincs tanúsítva.

ASCM_ECC.3.2C Az értékelt és tanúsított termék-komponensek listájának minden termékre azonosítania kell az értékelési eredményekre vonatkozó tanúsítványt, tanúsítási jelentést és az ezek alapjául szolgáló biztonsági előirányzatot.

ASCM_ECC.3-3 Az értékelőnek ellenőriznie kell, hogy értékelt és tanúsított termék-komponensek listája azonosítja-e minden értékelt és tanúsított termék-komponensre az alábbiakat: biztonsági előirányzat, tanúsítási jelentés, tanúsítvány.

ASCM_ECC.3.3C Az értékelt és tanúsított termék-komponensek listájának minden termékre le kell írnia az üzemeltetési feltételeket.

ASCM_ECC.3-4 Az értékelőnek ellenőriznie kell, hogy értékelt és tanúsított termék-komponensek listája leírja-e minden értékelt és tanúsított termék-komponensre annak üzemeltetési feltételeit.

Az ASCM_ECC.3.2E értékelői akció

ASCM_ECC.3.2E Az értékelőnek meg kell erősítenie, hogy a rendszer üzemeltetési környezete kielégíti az értékelt és tanúsított termékek tanúsítványaiban és tanúsítási jelentéseiben megfogalmazott üzemeltetési feltételeket.

ASCM_ECC.3-5 Az értékelőnek meg kell vizsgálnia, hogy értékelt és tanúsított termék-komponensek listájában a termék-komponensekre leírt üzemeltetési paraméterek összhangban állnak-e az adott termék tanúsítványában és tanúsítási jelentésében az üzemeltetési feltételekre megfogalmazott korlátozásokkal.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

Az ASCM_ECC.3.3E értékelői akció

ASCM_ECC.3.3E Az értékelőnek meg kell erősítenie, hogy a rendszer biztonsági funkcionalitását érvényre juttató és támogató termék komponensek tanúsítására vonatkozóan teljesülnek a SAP-K garanciacsomag elvárásai.

ASCM_ECC.3-6 Az értékelőnek meg kell vizsgálnia, hogy értékelt és tanúsított termék-komponensek listájában az egyes értékelt és tanúsított termékekre leírt garanciacsomagok összhangban vannak-e a SAP-K garanciacsomag elvárásaival.

Az értékelő a vizsgálat keretében erősítse meg, hogy az STOE tervben meghatározott rendszer biztonsági funkcionalitást támogató komponensek legalább CC EAL3 vagy MIBÉTS fokozott szintű tanúsítással rendelkeznek.

Az értékelő a vizsgálat keretében erősítse meg, hogy az STOE tervben meghatározott rendszer biztonsági funkcionalitást érvényre juttató komponensek legalább CC EAL4 vagy MIBÉTS kiemelt szintű tanúsítással rendelkeznek.

Amennyiben valamely rendszer biztonsági funkcionalitást támogató vagy érvényre juttató komponens nem felel meg az elvárásoknak, akkor ezt a rendszer értékelési jelentésben szerepeltetni kell a maradványkockázatok között.

6.2.4.5. A rendszer tesztelés garanciaosztály (ASTE) értékelése

6.2.4.5.1. Funkcionális rendszer tesztelés: ASTE_FUN.1 értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.5.1 pont alatt.

6.2.4.5.2. A rendszer tesztelés lefedettsége: ASTE_COV.1 értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.5.2 pont alatt.

6.2.4.5.3. A rendszer tesztelés mélysége: ASTE_DPT.3 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) rendszer interfész specifikáció,
c) biztonsági architektúra leírás,
d) STOE terv,
e) tesztdokumentáció,
f) tesztmélység elemzés.

Az ASTE_DPT.3.1E értékelői akció

ASTE_DPT.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASTE _DPT.3.1C A tesztmélység elemzésnek be kell mutatnia, hogy a tesztdokumentációban azonosított tesztek elegendőek annak bemutatására, hogy a rendszer biztonsági funkcionalitása a rendszer biztonsági architektúra leírással, valamint a rendszer biztonsági terv alrendszerekre és komponensekre vonatkozó leírásával összhangban működik.

ASTE_DPT.3-1 Az értékelőnek meg kell vizsgálnia a tesztdokumentációt és a tesztmélység elemzést annak megállapítása érdekében, hogy a rendszer biztonsági architektúra leírásban azonosított, az STOE-t külső informatikai rendszerekhez kapcsoló interfészeket tesztelték-e.

Ez a munkaegység ellenőrzi a tesztek és a rendszer biztonsági architektúra leírás megfelelését. Amennyiben az SSF szerkezeti helyességének leírása (az ADV_ARC biztonsági szerkezet leírás keretén belül) speciális mechanizmusokra hivatkozik, ez a munkaegység ellenőrizze a tesztek és az ilyen mechanizmusok üzemeltetési leírása közötti megfelelést is.

ASTE_DPT.3-2 Az értékelőnek meg kell vizsgálnia a tesztdokumentációt és a tesztmélység elemzést annak megállapítása érdekében, hogy azok szemléltetik-e, hogy az STOE és a külső informatikai rendszerek egymásra hatása megfelel a rendszer biztonsági architektúra leírásban foglaltaknak.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt mélység elemzésben szereplő teszteket és a kapcsolódó külső informatikai rendszerek egyértelműen kell azonosítani.

ASTE_DPT.3-3 Az értékelőnek meg kell vizsgálnia a tesztdokumentációt és a tesztmélység elemzést annak megállapítása érdekében, hogy az STOE tervben azonosított alrendszerek által nyújtott biztonsági funkcionalitást tesztelték-e.

Az STOE tervben szereplő valamennyi alrendszer működését tesztelni kell. Nyilvánvalóan hiányos a tesztelés mélysége, ha az STOE tervben azonosított egyik alrendszer működéséhez nem rendeltek tesztet.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt mélység elemzésben szereplő teszteket és a kapcsolódó alrendszereket egyértelműen kell azonosítani.
ASTE_DPT.3-4 Az értékelőnek meg kell vizsgálnia a tesztdokumentációt és a tesztmélység elemzést annak megállapítása érdekében, hogy az STOE tervben azonosított alrendszerek közötti belső interfészeket tesztelték-e.

Az STOE tervben szereplő alrendszerek összes egymásra hatását tesztelni kell. Nyilvánvalóan hiányos a tesztelés mélysége, ha az STOE tervben azonosított alrendszerek közötti egyik interfészhez nem rendeltek tesztet.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt mélység elemzésben szereplő teszteket és a kapcsolódó alrendszerek közötti interfészeket egyértelműen kell azonosítani.

ASTE_DPT.3-5 Az értékelőnek meg kell vizsgálnia a tesztdokumentációt és a tesztmélység elemzést annak megállapítása érdekében, hogy az STOE tervben azonosított komponensek által nyújtott biztonsági funkcionalitást tesztelték-e.

Az STOE tervben szereplő valamennyi komponens működését tesztelni kell. Nyilvánvalóan hiányos a tesztelés mélysége, ha az STOE tervben azonosított egyik komponens működéséhez nem rendeltek tesztet.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt mélység elemzésben szereplő teszteket és a kapcsolódó komponenseket egyértelműen kell azonosítani.

ASTE_DPT.3-6 Az értékelőnek meg kell vizsgálnia a tesztdokumentációt és a tesztmélység elemzést annak megállapítása érdekében, hogy az STOE tervben azonosított komponensek közötti belső interfészeket tesztelték-e.

Az STOE tervben szereplő komponensek összes egymásra hatását tesztelni kell. Nyilvánvalóan hiányos a tesztelés mélysége, ha az STOE tervben azonosított komponensek közötti egyik interfészhez nem rendeltek tesztet.

A megfeleltetés bemutatására egy egyszerű kereszt-táblázat is elegendő lehet. A teszt mélység elemzésben szereplő teszteket és a kapcsolódó komponensek közötti interfészeket egyértelműen kell azonosítani.

6.2.4.5.4. Független rendszer tesztelés: ASTE_IND.1 értékelése

Ez az értékelői altevékenység megegyezik az alap garanciacsomagnál tárgyalt esettel, melyet lásd 6.2.2.5.4 pont alatt.

6.2.4.6. A rendszer sebezhetőség felmérés garanciaosztály (ASVA) értékelése

6.2.4.6.1. Sebezhetőség elemzés: ASVA_VAN.3 értékelése

Az ehhez az értékelői altevékenységhez megkövetelt értékelési bizonyítékok az alábbiak:

a) SST,
b) rendszer interfész specifikáció,
c) STOE terv,
d) biztonsági architektúra leírása,
e) útmutató dokumentációk,
f) a tesztelésre alkalmas STOE,
g) nyilvánosan elérhető információk a lehetséges sebezhetőségek azonosításának támogatására,
h) a lehetséges sebezhetőségekre és támadásokra vonatkozó aktuális, nyilvánosan elérhető információk.

Az ASVA_VAN.3.1E értékelői akció

ASVA_VAN.3.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASVA_VAN.3.1C Az STOE-nak alkalmasnak kell lennie tesztelésre.

ASVA_VAN.3-1 Az értékelőnek meg kell vizsgálnia az STOE-t annak megállapítása érdekében, hogy az integrált és konfigurált rendszer megfelel-e az SST-ben meghatározott, értékelendő rendszer leírásával (a kiépítés és a konfigurálás szempontjából).

Az STOE-t alkotó hardver és szoftver komponensekre az értékelő ellenőrizze, hogy valamennyi komponens konfigurációja ellentmondás mentes-e az SST-vel.

Az értékelő vegye figyelembe azokat az SST-ben leírt, az STOE üzemeltetési környezetére vonatkozó biztonsági célokat, amelyek a rendszer teszt környezetére alkalmazhatók.

Bármilyen tesztelési erőforrás (mérőműszer, elemző készülék) használatakor az értékelő felelőssége annak biztosítása, hogy ezek az erőforrások megfelelően hitelesítve legyenek.

ASVA_VAN.3-2 Az értékelőnek meg kell vizsgálnia az STOE-t annak megállapítása érdekében, hogy a rendszer valamennyi komponensét megfelelően telepítették-e, és ismert állapotban van-e.

Az ASVA_VAN.3.2E értékelői akció

ASVA_VAN.3.2E Az értékelőnek egy keresést kell végrehajtania nyilvános forrásokban az STOE lehetséges sebezhetőségeinek azonosítása érdekében.

ASVA_VAN.3-3 Az értékelőnek tanulmányoznia kell a nyilvánosan rendelkezésre álló információ forrásokat az STOE lehetséges sebezhetőségeinek a meghatározása céljából.

Az értékelő tanulmányozza a nyilvánosan rendelkezésre álló információ forrásokat, amelyek rendelkezésre állnak az STOE lehetséges sebezhetőségei meghatározásainak elősegítéséhez. Sokféle nyilvánosan rendelkezésre álló információ forrás létezik, amelyeket az értékelőnek ajánlatos figyelembe vennie, felhasználva a világhálón elérhető anyagokat, beleértve a következőket:

a) szakértői publikációk (folyóiratok, könyvek);
b) tanulmányok;
c) konferencia kiadványok.

Az értékelő ne korlátozza az általa figyelembevett nyilvánosan rendelkezésre álló információkat a fentiekre, hanem vegyen figyelembe bármely egyéb vonatkozó rendelkezésre álló információt.

A nyilvánosan rendelkezésre álló információ keresése célirányosan azokra a forrásokra irányuljon, amelyek az STOE alapját képező komponensekre (termékekre) vonatkoznak.

Az értékelő az átadott bizonyítékok vizsgálata közben használja fel a nyilvános információkat abból a célból, hogy további vizsgálatokat végezzen lehetséges sebezhetőségek felkutatására. Ha az értékelő problémás területeket határozott meg, vegye figyelembe azokat a nyilvánosan rendelkezésre álló információkat, amelyek az adott problémás területre vonatkoznak.

Az olyan információk elérhetősége, amely azonnal rendelkezésre állhat egy támadó számára, s amely elősegíti támadások meghatározását és megkönnyíti a támadások hatékony végrehajtását, jelentősen megnövelheti egy adott támadó támadási lehetőségeit. A sebezhetőségi információk és kifinomult támadó eszközök hozzáférhetősége az Interneten nagyon valószínűvé teszi, hogy ezeket megpróbálják felhasználni az STOE lehetséges sebezhetőségeinek meghatározására és kihasználására. A modern kereső eszközök az ilyen információkat könnyen elérhetővé teszik az értékelő számára, és a publikált lehetséges sebezhetőségekkel, valamint a jól ismert általános támadásokkal szembeni ellenállóképesség költséghatékony módon meghatározható.

A lehetséges sebezhetőségeket tartalmazó nyilvános adatbázisokról lásd [4].

Az értékelőnek jelentést kell készíteni a megvizsgált bizonyítékokról a lehetséges sebezhetőségekre irányuló keresés befejezésekor. A bizonyítékok kiválasztása származhat az értékelő által meghatározott olyan problémás területekből, amely a támadó által is feltehetően elérhető bizonyítékhoz kapcsolódik, vagy megfelelhet az értékelő által adott valamilyen más magyarázatnak.

Az ASVA_VAN.3.3E értékelői akció

ASVA_VAN.3.3E: Az értékelőnek egy független sebezhetőség vizsgálatot kell végrehajtania az STOE-ra, felhasználva az útmutató dokumentációk, a biztonsági architektúra leírás, a rendszer interfész specifikáció, az STOE terv és a rendszer-működési biztonsági koncepció által biztosított ismereteket, az STOE lehetséges sebezhetőségeinek azonosítása érdekében.

ASVA_VAN.3-4 Az értékelőnek egy célirányos keresést kell folytatnia az SST-re, a biztonsági architektúra leírásra, a rendszer interfész specifikációra, az STOE tervre, a rendszer-működési biztonsági koncepcióra, valamint az útmutató dokumentációkra, abból a célból, hogy meghatározza az STOE-ban esetlegesen előforduló lehetséges sebezhetőségeket.

Hiba hipotézis módszer használata szükséges, amely a specifikációk, a tervezési és útmutató bizonyítékok vizsgálata után az STOE-ban lévő lehetséges sebezhetőségeket feltételezi, illetve ezzel kapcsolatos vizsgálódásokat folytat.

Az értékelő használja fel az STOE-ra szerzett ismereteit, hiba hipotézis módszert alkalmazva, az STOE integrálásában, vagy specifikált üzemmódjában lévő lehetséges hibák azonosítása céljából.

A biztonsági architektúra leírás szolgáltatja a rendszer integrátor sebezhetőség vizsgálatát, minthogy ez dokumentálja, hogy az SSF hogyan védi saját magát a nem-megbízható szubjektumokkal szemben, és hogyan akadályozza meg a biztonságot érvényre juttató funkcionalitás megkerülését. Ennélfogva az értékelő építsen az SSF védelem megértésére, amelyet ezen bizonyíték vizsgálatából nyert, majd hasznosítsa ezt az egyéb fejlesztésre vonatkozó (ASDV) bizonyítékokból nyert ismeretekben.

Az alkalmazott megközelítési módban a problémás területek az irányadók, amelyeket az értékelési tevékenységek során a bizonyítékok vizsgálata közben, illetve az értékelésre átadott tervezési és útmutató bizonyítékok reprezentatív mintájában való keresés közben határoztak meg.

A problémás területek vonatkozhatnak a biztonsági szerkezet leírásban részletezett speciális védelmi tulajdonságok kielégítőségére.

A sebezhetőség vizsgálat során figyelembevett bizonyítékot ahhoz a bizonyítékhoz lehet kapcsolni, amelyhez a támadó feltételezhetően képes hozzájutni.

A nyilvánosan elérhető források esetében ésszerű feltételezni, hogy a támadó is hozzájut e forrásokhoz, és is felhasználja ezeket az STOE elleni támadási kísérleteiben. Ezért az értékelő

vegye figyelembe a nyilvánosan elérhető forrásokat a célirányos vizsgálati megközelítési módnál.

A következők példákat mutatnak azokra a feltételezésekre, amelyeket egy hiba hipotézis tehet:

a) hibásan megadott input feltételezése a támadók által elérhető külső interfészeknél;
b) a biztonsági architektúra leírásban említett kulcsfontosságú mechanizmus vizsgálata olyan belső buffer túlcsordulás feltételezése mellett, amely a szétválasztás elromlásához vezethet;
c) kutatás az STOE megvalósítási reprezentációjában létrehozott olyan objektumok meghatározására, amelyeket nem ellenőriz teljes mértékben az SSF, és amelyeket egy támadó felhasználhat az SFR-ek aláaknázására.

Például az értékelő meghatározhatja, hogy az interfészek lehetséges gyenge pontok az STOE-ban, és egy olyan megközelítési módot használhat, hogy „a rendszer interfész specifikációban és STOE tervben megadott minden interfész specifikáció átvizsgálásra kerül a lehetséges sebezhetőség hipotézisek kialakításához”, majd folytathatja azzal, hogy megmagyarázza a hipotézisben használt módszereket.

A meghatározási folyamat iteratív, ahol egy lehetséges sebezhetőség meghatározása egy másik problémás terület meghatározásához vezethet, amely további vizsgálatokat igényel.

Az értékelőnek jelentést kell készíteni arról, hogy mit tett a bizonyítékokban található lehetséges sebezhetőségek meghatározására. Az ilyen típusú keresésre azonban lehet, hogy az értékelő nem tudja a vizsgálat megkezdése előtt leírni a lehetséges sebezhetőségek meghatározására teendő lépéseket, mivel a feldolgozási mód csak a keresés során találtak eredményeként alakul ki. Ilyen esetekben az értékelőnek a vizsgált bizonyítékokról a lehetséges sebezhetőségekre irányuló keresés befejezésekor kell jelentést készíteni. A bizonyítékok kiválasztása származhat az értékelő által meghatározott olyan problémás területekből, amely a támadó által is feltehetően elérhető bizonyítékhoz kapcsolódik, vagy megfelelhet az értékelő által adott valamilyen más magyarázatnak.

Azoktól az SFR-ektől függően, amelyeket az STOE-nak teljesítenie kell az üzemeltetési környezetben, az értékelő független sebezhetőség vizsgálata vegye tekintetbe az összes alábbi általános sebezhetőség típust:

a) az értékelés alatt álló STOE-t alkotó komponensek típusára vonatkozó általános lehetséges sebezhetőségek;
b) megkerülés;
c) hamisítás;
d) közvetlen támadások;
e) megfigyelés;
f) helytelen használat/visszaélés.

A b) - f) tételeket részletesen magyarázza [7] 7.3 melléklete.

A biztonsági architektúra leírást a fenti általános lehetséges sebezhetőségek szem előtt tartása mellett kell mérlegelni. Minden lehetséges sebezhetőséget mérlegelni kell azon lehetséges

módok felkutatására, amelyekkel az SSF védelmet hatálytalanítani, az SSF-et aláaknázni lehet.

ASVA_VAN.3-5 Az értékelőnek a SER-ben rögzítenie kell a meghatározott lehetséges sebezhetőségeket, amelyek tesztelhetők, és az STOE üzemeltetési környezetében elvileg szóba jöhetnek.

Nem szükséges a lehetséges sebezhetőségek további mérlegelése, ha az értékelő azt állapítja meg, hogy az üzemeltetési környezetben meglévő IT vagy nem-IT intézkedések meggátolják a lehetséges sebezhetőségek kiaknázását az adott üzemeltetési környezetben. Például, ha az STOE-hoz való fizikai hozzáférés kizárólag a jogosult felhasználókra van korlátozva, akkor ez a hamisítás lehetséges sebezhetőségét eredményesen nem kihasználhatóvá teheti.

Az értékelőnek minden okot rögzítenie kell a lehetséges sebezhetőségek további mérlegelésből való kizárására, ha azt állapítja meg, hogy a lehetséges sebezhetőség nem kerülhet szóba az üzemeltetési környezetben. Egyéb esetekben az értékelőnek a lehetséges sebezhetőséget további mérlegelésre rögzítenie kell.

Az értékelőnek a SER-ben meg kell adnia az STOE-val kapcsolatos, annak üzemeltetési környezetében felmerülő lehetséges sebezhetőségek listáját, mely a behatolás tesztelési tevékenység bemeneteként használható.

Az ASVA_VAN.3.4E értékelői akció

ASVA_VAN.3.4E Az értékelőnek az azonosított lehetséges sebezhetőségek alapján automatikus eszközöket is felhasználva, behatolás tesztelést kell végrehajtania, annak megállapítása érdekében, hogy az STOE ellenáll egy megemelt-alap támadó képességgel bíró támadó által végrehajtott támadásnak.

ASVA_VAN.3-6 Az értékelőnek ki kell választania behatolás tesztelésre alkalmazandó automatikus eszközt.

Az automatikus eszköz kiválasztásánál az értékelő vegye figyelembe a lehetséges sebezhetőségekre irányuló független keresés eredményeit is.

A behatolás tesztelésre alkalmazható automatikus eszközök áttekintésére lásd [4].

ASVA_VAN.3-7 Az értékelőnek a kiválasztott automatikus eszközzel végre kell hajtania a behatolás tesztelést.

A behatolás tesztelésre alkalmazható automatikus eszközök használatára lásd [4].

ASVA_VAN.3-8 Az értékelőnek rögzítenie kell a behatolás tesztek eredményeit.

Az automatikus eszközök naplóállományokba rögzítik a behatolás tesztek eredményeit.

ASVA_VAN.3-9 Az értékelőnek elemeznie kell az automatikus eszközök által végzett behatolás tesztelés eredményeit.

Az automatikus behatolás tesztelés eredményeiről lásd [4].

ASVA_VAN.3-10 Az értékelőnek meg kell terveznie a behatolás teszteket a lehetséges sebezhetőségekre irányuló független keresés, valamint az automatikus eszközökkel végzett behatolás tesztelés eredményei alapján.

Az értékelőnek kellően fel kell készülnie a behatolás tesztelésre annak megállapítása érdekében, hogy az STOE üzemeltetési környezetében mennyire érzékeny a nyilvános forrásokban való kereséssel azonosított lehetséges sebezhetőségekre. Az értékelőnek figyelembe kell vennie bármely harmadik féltől kapott, ismert lehetséges sebezhetőségre vonatkozó aktuális információt, valamint a más értékelői tevékenységek eredményeként talált lehetséges sebezhetőségeket is.

Az értékelőnek szem előtt kell tartania, hogy ugyanúgy, mint a biztonsági architektúra leírás mérlegelése esetében a sebezhetőségek felkutatásánál (ahogyan az ASVA_VAN.3-3-ben részletezve van), tesztelést kell végrehajtania a szerkezeti tulajdonságok megerősítésére. A rendszer integrátor tesztelési bizonyítéka olyan tesztelést is tartalmazni fog, amelyet a biztonsági architektúra leírásban részletezett speciális mechanizmusok helyes működésének megerősítése céljából hajtottak végre. A rendszer integrátor tesztelése azonban nem szükségszerűen tartalmaz tesztelést az SSF védelmére szolgáló szerkezeti tulajdonságok minden vonatkozására, minthogy az ilyen tesztelések legtöbbje természetszerűen negatív tesztelés lesz, amely a tulajdonságok megcáfolását kísérli meg. A behatolás tesztelés stratégiájának kialakításakor az értékelőnek garantálnia kell, hogy a biztonsági szerkezet leírás minden vonatkozása tesztelésre kerüljön vagy a funkcionális tesztelésnél, vagy az értékelői behatolás tesztelésnél.

A behatolás tesztelést valószínűleg tesztesetek sorozatával célszerű elvégezni, ahol az egyes tesztesetek egy-egy adott lehetséges sebezhetőséget próbálnak ki.

Az értékelőnek nem kell teszteket végeznie azokon a lehetséges sebezhetőségeken túl (beleértve a nyilvánosan ismerteket is), melyek kihasználásához legfeljebb megemelt-alap támadó képesség szükséges. Egyes esetekben azonban még a kihasználhatóság meghatározása előtt szükség lehet egy teszt végrehajtására. Amennyiben értékelői tapasztalata segítségével az értékelő egy közepes vagy magas támadó képességgel kihasználható sebezhetőséget tár fel, ezt az értékelési jelentésében maradvány sebezhetőségként szerepeltetnie kell.

Egy adott lehetséges sebezhetőség kihasználásához szükséges támadó képesség meghatározásához útmutató található [7] 7.3.4 pontjában.

Az olyan lehetséges sebezhetőségek, melyek feltételezhetően csak közepes vagy magas támadó képességgel kihasználhatók, nem eredményeznek „nem felelt meg” eredményt erre az értékelői tevékenységre. Amennyiben vizsgálat támogatja a fenti feltételezést, az érintett lehetséges sebezhetőséget a továbbiakban nem szükséges a behatolás tesztelés bemeneteként kezelni. Ugyanakkor az ilyen sebezhetőséget az értékelési jelentésben maradvány sebezhetőségként szerepeltetni kell.

Az olyan lehetséges sebezhetőségeket, melyek feltételezhetően alap vagy megemelt-alap támadó képességgel kihasználhatók, és a biztonsági célok megsértését eredményezik, a legnagyobb elsőbbséggel ajánlott a lehetséges sebezhetőségek azon listájára felvenni, mely alapján az STOE közvetlen behatolás tesztelését végzik.

ASVA_VAN.3-11 Az értékelőnek a lehetséges sebezhetőségek listáján alapulva el kell készítenie a behatolás tesztelési dokumentációt, a tesztek megismételhetőségét lehetővé tévő részletességgel. A tesztelési dokumentációnak tartalmaznia kell az alábbiakat:

a) a lehetséges sebezhetőség azonosítását, melyre az STOE-t tesztelik;
b) a behatolás teszteléshez szükséges minden tesztberendezés csatlakoztatását és beállítását előíró utasítást;
c) a behatolás tesztelés összes kezdeti előfeltételét kialakító utasításokat;
d) az SSF működését kiváltó utasításokat;
e) az SSF viselkedése megfigyeléséhez szükséges utasításokat;
f) minden várható eredmény leírását, valamint a várható eredményekkel való összehasonlításhoz végrehajtandó, megfigyelt működésre vonatkozó elemzéseket;
g) a tesztek befejezéséhez szükséges és az STOE tesztelés utáni állapotát biztosító utasításokat.

Az értékelőnek a lehetséges sebezhetőségek listáján alapulva el kell készítenie a behatolás tesztelési dokumentációt, a tesztek megismételhetőségét lehetővé tévő részletességgel.

Az értékelőre nézve nem elvárás, hogy meghatározza a kihasználhatóságát azon lehetséges sebezhetőségeknek, melyek hatásos támadásához közepes vagy magas támadó képesség szükséges. Ugyanakkor értékelői tapasztalata segítségével az értékelő feltárhat olyan lehetséges sebezhetőséget, melyet csak olyan támadó használhat ki, aki közepes vagy magas támadó képességgel rendelkezik. Az ilyen sebezhetőségeket az értékelési jelentésében maradvány sebezhetőségként szerepeltetni kell.

A lehetséges sebezhetőség ismeretében az értékelő határozza meg a leginkább megfelelő módot az STOE érzékenységének kimutatásához. Az értékelő különösen az alábbiakat vegye tekintetbe:

a) az SSF kiváltására és a válaszok megfigyelésére használt interfészek (SSFI);
b) a tesztekhez szükséges kezdeti feltételek;
c) egy SSFI kiváltásához vagy megfigyeléséhez szükséges speciális tesztberendezések;
d) különösen fontos eset, amikor egy kezdeti teszt eredményeként előre jelezhető, hogy egy támadás adott számú megismétlése valószínűleg sikeres lesz.

Az értékelő a behatolás tesztelést valószínűleg tesztesetek sorozatával találja célszerűnek elvégezni, ahol az egyes tesztesetek egy-egy adott lehetséges sebezhetőséget próbálnak ki.
A tesztelési dokumentáció ilyen szintű részletessége azt hivatott biztosítani, hogy más értékelők is meg tudják ismételni a teszteket, és azonos eredményre juthassanak.

ASVA_VAN.3-12 Az értékelőnek végre kell hajtania a behatolás tesztelést.

Az értékelő az ASVA_VAN.3-10 munkaegység eredményeképpen létrejött behatolás tesztelési dokumentációt az STOE behatolás tesztelésének alapjaként használja, de ez nem zárja ki, hogy más, ad hoc behatolás tesztelést ne végezhessen el. Amennyiben szükséges, az

értékelő ad hoc teszteket is elvégezhet a behatolás tesztelés során tapasztaltak következtében, melyeket – ha az értékelő elvégzi azokat - a behatolás tesztelési dokumentációban rögzítenie kell. E tesztekkel szemben követelmény lehet, hogy a nem várt eredményeket vagy megfigyeléseket ellenőrizzék, vagy hogy a tesztelés előkészítési szakaszában az értékelőnek javasolt lehetséges sebezhetőségeket megvizsgálják.

Amennyiben a behatolás tesztelés azt mutatja, hogy egy feltételezett lehetséges sebezhetőség nem létezik, az értékelőnek ajánlott megállapítania, hogy a saját elemzése volt téves, vagy az értékelésre átadandók voltak hibásak, hiányosak.

Az értékelőnek nem kell tesztelést végeznie azokon a lehetséges sebezhetőségeken túl (beleértve a nyilvánosan ismerteket is), melyek kihasználásához legfeljebb megemelt-alap támadó képesség szükséges. Egyes esetekben azonban még a kihasználhatóság meghatározása előtt szükség lehet egy teszt végrehajtására. Amennyiben értékelői tapasztalata segítségével az értékelő egy közepes vagy magas támadó képességgel kihasználható sebezhetőséget tár fel, ezt az értékelési jelentésében maradvány sebezhetőségként szerepeltetnie kell.

ASVA_VAN.3-13 Az értékelőnek rögzítenie kell a behatolás tesztek tényleges eredményeit.

A tényleges eredmények bizonyos részletei különbözhetnek a várható értékektől (pl. idő és dátummezők a naplóban), de az összeredménynek meg kell egyeznie. Javasolt minden váratlan teszteredményt kivizsgálni, valamint ezek értékelésre gyakorolt hatását kimondani és igazolni.

ASVA_VAN.3-14 Az értékelőnek az értékelési jelentés keretén belül jelentést kell írnia az értékelői behatolás tesztelésről, leírván a tesztelési módszert, konfigurációt, mélységet és eredményeket.

Az értékelési jelentésben rögzített behatolás tesztelésről szóló információ lehetővé teszi az értékelő számára, hogy bemutassa az általános tesztelési módszert és az ezen tevékenység végrehajtásába fektetett munkát. A cél az értékelő behatolás tesztelési munkájának érdemi áttekintése. Nem cél, hogy az értékelési jelentésben a behatolás teszteléssel kapcsolatos információk a specifikus tesztlépések vagy egyedi behatolás tesztek eredményeinek pontos megismétlése legyenek. A cél elegendő részletesség biztosítása más értékelők számára ahhoz, hogy betekintést kapjanak a választott behatolás tesztelési módszerbe, a végrehajtott behatolás tesztek nagyságrendjébe, az STOE teszt konfigurációjába és a behatolás tesztelési tevékenység általános eredményébe.

Az értékelési jelentés értékelői behatolás tesztelésről szóló része általában az alábbi információkat tartalmazza:

a) STOE tesztkonfigurációk; a behatolás tesztelésnél használt konkrét STOE konfigurációk.
b) A behatolás teszt során tesztelt interfészek. A behatolás tesztelés középpontjában álló interfészek rövid felsorolása.
c) Az altevékenység alapján született határozat. A behatolás tesztelés eredményeinek általános megítélése.

ASVA_VAN.3-15 Az értékelőnek meg kell vizsgálnia az összes behatolás teszt eredményét annak megállapítása érdekében, hogy az STOE üzemeltetési környezetében ellenáll-e egy megemelt-alap támadó képességgel rendelkező támadónak.

Amennyiben az eredmények azt mutatják, hogy az STOE üzemeltetési környezetében kihasználható sebezhetőségeket tartalmaz alap vagy megemelt-alap támadó képességgel rendelkező támadók számára, akkor ez az értékelői akció "Nem felelt meg" határozatot eredményez.

[7] 7.3.4 mellékletét kell használni egy adott sebezhetőség kihasználásához szükséges támadó képesség meghatározásához, illetve annak eldöntésére, hogy a sebezhetőség a tervezett üzemeltetési környezetben kihasználható-e. Nem feltétlenül kell minden esetben kiszámolni a támadó képességet, csak ha felmerül annak lehetősége, hogy egy alap vagy megemelt-alap támadó képességgel rendelkező támadó kihasználhatja a sebezhetőséget.

ASVA_VAN.3-16 Az értékelőnek az értékelési jelentés keretén belül jelentést kell írnia az összes kihasználható sebezhetőségről és maradvány sebezhetőségről, az alábbi adatokkal:

a) forrás (pl. azon CEM tevékenység, melynek végrehajtása során észlelték, az értékelő ismerte, szakirodalomban olvasott róla);
b) a nem kielégített SFR(-ek);
c) leírás;
d) kihasználható-e vagy sem az üzemeltetési környezetben (vagyis kihasználható vagy maradvány sebezhetőségről van szó);
e) az azonosított sebezhetőség kihasználáshoz szükséges felhasznált idő, szakértelem, TOE ismeret, hozzáférési lehetőség, eszköz, valamint az ezekhez rendelt értékek [7] 7.3.4 mellékletének 7. és 8. táblázata alapján.

6.2.5. Felülvizsgálati rendszer értékelés

A felülvizsgálati rendszer értékelés a következő értékelési tevékenységekből áll:

a) a rendszer fejlesztés aktualizálásának értékelése,
b) a rendszer útmutató dokumentációk aktualizálásának értékelése,
c) a regressziós tesztelés értékelése,
d) független tesztelés,
e) a rendszer alap konfiguráció igazolása,
f) a tanúsított komponensek felmérése vagy ellenőrzése (a kezdeti értékelés szintjétől függően),
g) a kezdeti értékelés szintjének megfelelő sebezhetőség vizsgálat.

6.2.5.1. A rendszer fejlesztés aktualizálásának (ASDV_MOD.1) értékelése

Az ASDV_MOD.1.1E értékelői akció

ASDV_MOD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_MOD.1.1C Valamennyi biztonsági terv dokumentáció esetén az ellenőrző vizsgálatnak meg kell mutatnia, hogy a módosítások a tervet nem befolyásolják, vagy a módosításokat figyelembe véve a tervet helyesen aktualizálták.

ASDV_MOD.1-1 Az értékelőnek meg kell vizsgálnia a biztonsági architektúra leírást annak megállapítása érdekében, hogy a módosítások a biztonsági architektúra leírást nem érintették, vagy a módosításokat figyelembe véve a leírást helyesen frissítették.

ASDV_MOD.1-2 Az értékelőnek meg kell vizsgálnia a rendszer interfész specifikációt annak megállapítása érdekében, hogy a módosítások a rendszer interfész specifikációt nem érintették, vagy a módosításokat figyelembe véve a specifikációt helyesen frissítették.

ASDV_MOD.1-3 Az értékelőnek meg kell vizsgálnia az STOE tervet annak megállapítása érdekében, hogy a módosítások az STOE tervet nem érintették, vagy a módosításokat figyelembe véve az tervet helyesen frissítették.

ASDV_MOD.1-4 Az értékelőnek meg kell vizsgálnia a rendszer-működési biztonsági koncepció leírást annak megállapítása érdekében, hogy a módosítások a rendszer-működési biztonsági koncepció leírást nem érintették, vagy a módosításokat figyelembe véve a leírást helyesen frissítették.

ASDV_MOD.1-5 Az értékelőnek meg kell vizsgálnia valamennyi biztonsági terv dokumentációt annak megállapítása érdekében, hogy a módosítások után sem mondanak egymásnak ellent a különböző terv dokumentációk.

6.2.5.2. A rendszerútmutató dokumentációk aktualizálásának (ASGD_MOD.1) értékelése

Az ASGD_MOD.1.1E értékelői akció

ASGD_MOD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_MOD.1.1C Az ellenőrző vizsgálatnak minden útmutatóra meg kell mutatnia, hogy a módosítások a dokumentumot nem érintették, vagy a módosításokat figyelembe véve a dokumentációt helyesen frissítették.

ASGD_MOD.1-1 Az értékelőnek meg kell vizsgálnia az előkészítő útmutatót annak megállapítása érdekében, hogy a módosítások az előkészítő útmutatót nem érintették, vagy a módosításokat figyelembe véve az előkészítő útmutatót helyesen frissítették.

ASGD_MOD.1-2 Az értékelőnek meg kell vizsgálnia a konfigurálási útmutatót annak megállapítása érdekében, hogy a módosítások a konfigurálási útmutatót nem érintették, vagy a módosításokat figyelembe véve a konfigurálási útmutatót helyesen frissítették.

ASGD_MOD.1-3 Az értékelőnek meg kell vizsgálnia az üzemeltetési útmutatót annak megállapítása érdekében, hogy a módosítások az üzemeltetési útmutatót nem érintették, vagy a módosításokat figyelembe véve az üzemeltetési útmutatót helyesen frissítették.

6.2.5.3. A regressziós tesztelés (ASTE_MOD.1) értékelése

Az ASTE_MOD.1.1E értékelői akció

ASTE_MOD.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASTE_MOD.1.1C A tesztdokumentációnak tartalmaznia kell a teszttterveket, a várt teszteredményeket és a tényleges teszteredményeket.

ASTE_MOD.1-1 Az értékelőnek ellenőriznie kell, hogy a tesztdokumentáció tartalmazza-e a teszttterveket, az elvárt eredményeket és a tényleges teszt eredményeket.

Az értékelő ellenőrizze, hogy a teszttterveket, az elvárt eredményeket és a tényleges teszt eredményeket belefoglalták-e a tesztdokumentációba.

ASTE_MOD.1.2C A teszttterveknek azonosítaniuk kell a módosítások által kiváltott hatásokat és a tesztelendő biztonsági funkciókat, és le kell írniuk a végrehajtandó tesztek célját.

ATSE_MOD.1-2 Az értékelőnek meg kell vizsgálnia, hogy a teszttervek elemzik-e a módosítások által kiváltott hatásokat és azonosítják-e a tesztelendő biztonsági funkciókat.

Az értékelőnek meg kell állapítania, hogy a módosítások hatásvizsgálata kellően megalapozza-e, hogy a biztonsági funkcióknak csak egy részhalmazát kell tesztelni.

ATSE_MOD.1-3 Az értékelőnek ellenőriznie kell, hogy a teszttervek leírják-e a végrehajtandó tesztek célját.

ASTE_MOD.1.3C A teszttervnek azonosítania kell a módosított részeken végrehajtandó teszteket, és ismertetnie kell minden biztonsági funkcióra a tesztelési forgatókönyveket. A forgatókönyveknek tartalmazniuk kell a sorrendi függőségeket a megváltoztatott részeknek és az egyéb tesztek eredményeinek a vonatkozásában.

ATSE_MOD.1-4 Az értékelőnek ellenőriznie kell, hogy a teszttervek leírják-e minden teszt végrehajtásának forgatókönyvét.

Az értékelőnek meg kell állapítania, hogy a teszttervek nyújtnak-e információkat a használt tesztkonfigurációra vonatkozóan: mind az STOE konfigurációra, mind pedig minden használt tesztberendezésre vonatkozóan. Ennek az információnak a tesztkonfiguráció reprodukálhatóságának biztosításához kellően részletesnek kell lennie.

Az értékelőnek azt is meg kell állapítania, hogy a teszttervek nyújtanak-e információt arról, hogy hogyan kell végrehajtani a tesztet: az összes szükséges automatizált indítási eljárásról

(és hogy ezek igényelnek-e futási jogosultságot), az alkalmazandó bemenetekről és ezek alkalmazásáról, hogyan lehet megkapni a kimenetet, valamennyi automatikus törlési eljárásról (és hogy ezek igényelnek-e futási jogosultságot), stb. Ennek az információnak a teszt reprodukálhatóságának biztosításához kellően részletesnek kell lennie.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ASTE_MOD.1.4C A rendszer integrátor által végrehajtott tesztekből származó eredményeknek meg kell mutatniuk, hogy minden tesztelt biztonsági funkció a specifikáltaknak megfelelően működik, így a módosítások nincsenek kihatással az SSF-re.

ASTE_MOD.1-5 Az értékelőnek ellenőriznie kell a tesztdokumentációt annak megállapítása érdekében, hogy az tartalmazza-e az összes várt teszteredményt.

Az értékelő e munkaegység végrehajtása során alkalmazhat mintavételezési módszert.

ASTE_MOD.1-6 Az értékelőnek meg kell vizsgálnia, hogy a tesztdokumentációban szereplő várt teszteredmények összhangban állnak-e a tényleges teszteredményekkel.

ASTE_MOD.1.5C A tesztdokumentációnak tartalmaznia kell egy vizsgálatot a teszt eljárások sorrendi függőségéről.

ASTE_MOD.1-7 Az értékelőnek ellenőriznie kell, hogy a tesztdokumentáció tartalmaz-e egy vizsgálatot a teszt eljárás sorrendi függőségeiről.

ASTE_MOD.1-8 Az értékelőnek meg kell vizsgálnia, hogy a teszt eljárás sorrendi függőségeire vonatkozó vizsgálat helyesen határozza-e meg az egyes tesztek közötti esetleges kötött sorrendet.

ASTE_MOD.1.6C A regressziós tesztelésre vonatkozó vizsgálatnak be kell mutatnia, hogy az SST-ben elvárt, módosítások által érintett funkcionális biztonsági követelmények és a tesztdokumentációban megadott tesztek közötti megfeleltetés teljes.

ASTE_MOD.1-9 Az értékelőnek meg kell vizsgálnia, hogy a vizsgálat kimutatja-e az SST-ben elvárt funkcionális biztonsági követelmények és a tesztdokumentációban megadott tesztek közötti megfeleltetés teljességét.

6.2.5.4. Független tesztelés

A felülvizsgálati rendszer értékelés keretén belül a kezdeti értékelés során végrehajtott független tesztelés megismétlésére van szükség, értelemszerűen az azóta bekövetkező változásokat és a regressziós tesztelés eredményeit is figyelembe véve.

A független tesztelés végrehajtására lásd a 6.2.2.5.4 pontot.

6.2.5.5. A rendszer alap konfiguráció igazolása

A felülvizsgálati rendszer értékelés keretén belül az értékelőnek át kell tekintenie a rendszer értékelt alap konfigurációjában bekövetkezett változtatásokat, illetve ennek nyomon követési módját.

Az értékelőnek független ellenőrzést kell végeznie a CM rendszer alap konfiguráció tartalmára vonatkozóan, személyi interjúk és a módosítások mintavételezése útján.

A fenti feladat végrehajtására lásd a 6.2.3.4.1 pontot.

6.2.5.6. A tanúsított komponensek felmérése vagy ellenőrzése

A felülvizsgálati rendszer értékelés keretén belül az értékelőnek fel kell mérnie vagy ellenőriznie kell a rendszer értékelt és tanúsított komponenseit, attól függően, hogy a kezdeti értékelés garanciacsomagja melyik feladatot várta el.

SAP-A az értékelt és tanúsított komponensek felmérését várja csak el. Ennek végrehajtására lásd a 6.2.2.4.2 pontot.

SAP-F az értékelt és tanúsított komponensek ellenőrzését várja el. Ennek keretében az értékelőnek meg kell erősítenie, hogy a rendszer biztonsági funkcionalitását érvényre juttató és támogató termék komponensek tanúsítására vonatkozóan teljesülnek a SAP-F garanciacsomag elvárásai.. A feladat végrehajtására lásd a 6.2.3.4.2 pontot.

SAP-K az értékelt és tanúsított komponensek ellenőrzését várja el. Ennek keretében az értékelőnek meg kell erősítenie, hogy a rendszer biztonsági funkcionalitását érvényre juttató és támogató termék komponensek tanúsítására vonatkozóan teljesülnek a SAP-K garanciacsomag elvárásai. A feladat végrehajtására lásd a 6.2.4.4.2 pontot.

6.2.5.7. A kezdeti értékelés szintjének megfelelő sebezhetőség vizsgálat

A felülvizsgálati rendszer értékelés keretén belül a kezdeti értékelés során végrehajtott sebezhetőség vizsgálat megismétlésére van szükség, értelemszerűen a rendszerben azóta bekövetkező változásokat, valamint a legutolsó értékelés óta megismert új sebezhetőségeket is figyelembe véve.

A sebezhetőség vizsgálat szigorúsága a kezdeti értékelés garanciacsomagjától függ.

SAP-A az értékelőtől elvárja, hogy keresést hajtson végre nyilvános forrásokban a rendszer lehetséges sebezhetőségeinek azonosítása érdekében. Azt is elvárja, hogy az azonosított lehetséges sebezhetőségek alapján automatikus eszközökkel behatolás tesztelést hajtson végre, annak megállapítása érdekében, hogy a rendszer ellenáll egy alap támadó képességgel bíró támadó által végrehajtott támadásnak. Ezeknek a feladatoknak a végrehajtására lásd a 6.2.2.6.1 pontot.

SAP-F az értékelőtől a SAP-A-ban meghatározottakon túl elvárja, hogy egy független sebezhetőség vizsgálatot hajtson végre a rendszer útmutató dokumentációkat, a rendszer interfész specifikációt, az STOE tervet és a biztonsági architektúra leírást használva, az STOE lehetséges sebezhetőségeinek azonosítása érdekében. Azt is elvárja, hogy ne csak automatikus eszközökkel végezzen behatolás tesztelést, hanem a lehetséges sebezhetőségekre irányuló független keresésén alapulva megtervezett saját tesztesetekkel is. Ezeknek a feladatoknak a végrehajtására lásd a 6.2.3.6.1 pontot.

SAP-K az értékelőtől a SAP-F-ben meghatározottakon túl elvárja, hogy a behatolás tesztelés kimutassa, hogy a rendszer ellenáll egy megemelt-alap támadó képességgel rendelkező támadó által végrehajtott támadásnak is. Ezeknek a feladatoknak a végrehajtására lásd a 6.2.4.6.1 pontot.

7. Mellékletek

7.1. A rendszer értékelési munkaterv felépítése és tartalma

A rendszer értékelési munkaterv az alábbi felépítést kövesse, a példaként megadott tartalmi elemek kifejtésével:

7.1.1. Bevezetés

7.1.1.1. Azonosító adatok

A rendszer neve és verziója:
Az értékelő szervezet adatai:
Az értékelés megbízójának adatai:
A rendszer integrátor adatai:

7.1.1.2. Háttér

Ez a dokumentum az alábbi rendszerre vonatkozó értékelési munkatervet határozza meg: [rendszer név és verzió].

Az értékelési munkaterv az alábbi rendszer biztonsági előirányzatban meghatározott követelmények ellenőrzésére vonatkozik: [SST cím és verzió].

A jelen értékelési munkaterv olvasóira fel van tételezve, hogy ismerik az SST tartalmát.

7.1.1.3. Célok

A jelen értékelési munkaterv legfőbb célja, hogy meghatározza azokat az értékelői tevékenységeket, amelyek annak megalapozásához szükségesek, hogy a [rendszer név és verzió] kielégíti-e az [SST cím és verzió]-ben meghatározott követelményeket.

7.1.1.4. Értékelési mérföldkövek

Az előkészítési szakasz kezdési dátuma:
Az előkészítési szakasz befejezési dátuma:
Az értékelés lebonyolítási szakaszának kezdés dátuma:
Az értékelés lebonyolítási szakaszának befejezési dátuma:
A fejlesztés/integrálás helyszíni látogatásának dátuma(i):
Az üzemeltetési helyszíni látogatásának dátuma(i):
A rendszer biztonsági tesztelésének dátuma(i):
A behatolás tesztelés dátuma(i):
Rendszer értékelési jelentés tervezet elkészítésének dátuma:
Rendszer értékelési jelentés (végleges) elkészítésének dátuma:

7.1.1.5. Az értékelő adatai

Az értékelő munkacsoport vezetője:
Az értékelő munkacsoport tagjai:

7.1.2. Az értékelés megvalósítási módja

7.1.2.1. Alkalmazott módszertan

Az értékelő az alábbi módszertant fogja követni:

a) az e-Közigazgatási Keretrendszer részét képező rendszerekre vonatkozó értékelési módszertan (vagy az alkalmazott egyéb módszertan) azonosítása,
b) az alkalmazott feladat-specifikus útmutatók azonosítása.

7.1.2.2. A rendszer értékelés típusa

A rendszer értékelés típusa: kezdeti / tervezett felülvizsgálati / rendkívüli felülvizsgálati / megismételt kezdeti

Amennyiben az értékelés felülvizsgálati, azonosítani kell a kezdeti értékelés és a legutolsó felülvizsgálati értékelés jellemzőit (értékelt rendszer neve és verziója, az értékelési jelentés címe és dátuma).

7.1.2.3. A rendszer értékelés feladatainak áttekintése

Ez az alfejezet sorolja fel az értékelés során végrehajtandó értékelői tevékenységeket, egyúttal hivatkozzon az SST-ben megadott STOE összefoglaló előírásra az értékelés adott rendszerhez való igazításánál.

Amennyiben alvállalkozókat kell alkalmazni valamely értékelői tevékenységhez, akkor ez az alfejezet világosan jelölje meg, hogy mely tevékenységeket hajtanak végre alvállalkozók.

Ez a fejezet összegezze annak a megoldási módját, hogy a tevékenységek hogyan vannak összhangba hozva az egyéb szervezetek vagy alvállalkozók által végrehajtandó bármely egyéb garancia tevékenységgel, megmutatva azt is, hogy az utóbbi tevékenységek során végzett munka nem lesz feleslegesen megismételve.

7.1.2.4. Lehetséges sebezhetőségek

Ez az alfejezet összegezze az értékelő kezdeti elképzeléseit a rendszer lehetséges sebezhetőségeiről, a már rendelkezésére álló információkon alapulva, és ismertesse ezek kihatásait az értékelői tevékenységekre (elsősorban a sebezhetőség vizsgálatra, ezen belül a behatolás tesztelésre).

Ez az alfejezet összegezze azokat lehetséges sebezhetőségre vonatkozó ötleteket is, amelyek az akkreditorral folytatott megbeszélés során merültek fel.

7.1.2.5. Tesztelési stratégia

Ez az alfejezet összegezze a teszt stratégiára és teszt konfigurációkra vonatkozó kezdeti elképzeléseket. Foglalja magába a tervezett teszt helyszíneket és teszt környezeteket.

A tervezett teszt konfigurációk foglalják magukba a valószerű teszt forgatókönyveket biztosító IT környezetet.

A teszt stratégia indokolja a teszt konfigurációk kielégítő voltát.

A független tesztek biztosítsák, hogy minden rendszer biztonsági funkció a választott rendszer garanciacsomagnak megfelelő mélységben le lesz tesztelve a fejlesztői, rendszer integrátori és értékelői munkák együttesével. Az értékelői (független) tesztelésnek pótolniuk kell a fejlesztői és rendszer integrátori tesztekben lévő hiányosságokat.

Ez az alfejezet összegezze azokat a tesztelési ötleteket is, amelyek az akkreditorral folytatott megbeszélés során merültek fel.

7.1.2.6. Mintavételezési stratégia

Ez az alfejezet részletezze a mintavételezési stratégiát a rendszer integrátorok által végrehajtott biztonsági funkció tesztek megismétléséhez vagy igazolásához. Ez általában ne

haladja meg a rendszer integrátorok által végrehajtott biztonsági funkció tesztek 5-10%-át, kivéve, ha problémákat találnak a rendszer integrátor által benyújtott tesztelési dokumentációban. A mintavételezési stratégia törekedjen arra, hogy a kiválasztott tesztek az értékelt konfigurációban lévő biztonsági funkciók, interfészek és komponensek széles skáláját fedjék le.

7.1.2.7. Teszt eszközök

Ez az alfejezet tekintse át a független és a behatolás teszteléshez tervezett feladat-specifikus eszközöket, beleértve ezek célját. Az áttekintés történhet táblázatba foglalva is.

7.1.2.8. Kriptográfiai értékelés

Ez az alfejezet összegezze a kriptográfiai értékelésért való felelősségeket és a kriptográfiai értékelés módszerét (pl. FIPS 140 szerint értékelt és tanúsított kriptográfiai céltermékek használata).

7.1.2.9. Garancia függőségek

Ez az alfejezet tekintse át a rendszerbe épített tanúsított termékek által biztosított kiegészítő garanciákat, illetve összegezze ezek érvényre juttatási módját (pl. a tanúsítási jelentésekben megfogalmazott függőségek és feltételek ellenőrzésével és biztosításával).

7.1.3. Mellékletek

7.1.3.1. Fogalomtár

Ez a melléklet sorolja fel az értékelési munkatervben használt összes kulcs-fogalmat és határozza meg ezek jelentését.

7.1.3.2. Rövidítésgyűjtemény

Ez a melléklet sorolja fel az értékelési munkatervben használt összes rövidítést és adja meg ezek jelentését.

7.2. A rendszer értékelési jelentés felépítése és tartalma

A rendszer értékelési jelentés (SER) felépítése alapvetően megegyezik a termék értékelési jelentés (ETR) felépítésével (jelentősebb különbségek csak a tartalmi elvárásokban lesznek):

a) Bevezetés
b) A rendszer szerkezeti leírása
c) Az értékelés jellemzése
d) Az értékelés eredményei
e) Következtetések és javaslatok

f) Az értékelési bizonyítékok listája
g) Rövidítések és szakkifejezések
h) Észrevételezési jelentések

A fenti struktúra nem kötelező érvényű, az értékelő hozzáigazíthatja a jelentését az értékelés és az STOE típusához.

7.2.1. Bevezetés

A bevezetés célja az értékelés és a benne érintett szereplők fontosabb adatainak rögzítése.

7.2.1.1. Azonosító adatok

A rendszer neve és verziója:
Az értékelő szervezet adatai:
A megbízó adatai:
A rendszer integrátor adatai:

7.2.1.2. Az értékelés mérföldkövei

Az előkészítési szakasz kezdési dátuma:
Az előkészítési szakasz befejezési dátuma:
Az értékelési szakasz kezdés dátuma:
Az értékelési szakasz befejezési dátuma:
A fejlesztés/integrálás helyszíni látogatásának dátuma:
Az üzemeltetési helyszíni látogatásának dátuma:
A rendszer biztonsági tesztelésének dátuma:
A behatolás tesztelés dátuma:
Rendszer értékelési jelentés tervezet elkészítésének dátuma:
Rendszer értékelési jelentés (végleges) elkészítésének dátuma:

7.2.1.3. Az értékelő adatai

Az értékelő munkacsoport vezetője:
Az értékelő munkacsoport tagjai:

7.2.2. Az STOE szerkezeti leírása

Az értékelőnek jelentésbe kell foglalnia az STOE és fő elemei (biztonsági tartományok és alrendszerek) magas szintű leírását, az SST összegző leírás és az STOE terv értékelési bizonyítékai alapján.

Ennek a fejezetnek a célja a rendszer fő elemei szerkezeti elkülönülésének a jellemzése.

Az STOE architektúrájának a megismerése hozzájárul az értékelés következtetéseinek megértéséhez. A biztonsági architektúrára vonatkozó további megjegyzések is helyet kaphatnak itt, ha azok hasznosak a 4. fejezetben található részletes eredmények hivatkozási alapjaként.

7.2.3. Az értékelés jellemzése

Ebben a fejezetben rövid áttekintést kell adni az alkalmazott értékelési módszerekről, technikákról, eszközökről és szabványokról.

Az értékelőnek itt kell meghatároznia az értékelésre, illetve az értékelési eredmények terjesztésére vonatkozó korlátozásait, valamint az értékelés során tett mindazon feltételezést, mely az eredményekre hatással van.

Az értékelő ebben a részben elhelyezhet jogi kötöttségekre, szervezetre vagy bizalmasságra vonatkozó információkat is.

Ez a fejezet leírhatja az értékelés megközelítését is, azonosítva többek között az alábbiakat:

a) milyen helyszíni szemlék voltak,
b) mikor, hol és hogyan lett az STOE integrálva és tesztelve (és hogy hány különböző tesztelési fázis valósult meg),
c) bármilyen speciális megközelítés, amely a jelentkező akadályok leküzdését szolgálta, mint például, hogy a végleges értékelési bizonyítékok (vagy az STOE végleges verziója) nem álltak rendelkezésre a tesztelés bizonyos fázisaiban,
d) lineáris vagy sebezhetőség vizsgálatra koncentráló megközelítést alkalmazott-e az értékelő munkacsoport (lásd [4] 6.3 alfejezete).

7.2.4. Az értékelés eredményei

Minden értékelési tevékenységére jelentésbe kell foglalni az alábbiakat:

— az érintett tevékenység elnevezését;
— egy határozatot és az ezt alátámasztó indoklást, az adott tevékenységet alkotó valamennyi garancia-összetevőre vonatkozóan.

Az indoklás igazolja a határozatot a vizsgált értékelési bizonyíték felhasználásával, valamint bemutatja, hogy az értékelési bizonyíték hogyan teljesíti vagy nem teljesíti a szempontok valamennyi aspektusát. Leírja a végrehajtott munkát, a felhasznált módszert és az eredmények levezetését.

Az értékelőnek ebbe a fejezetbe kell belefoglalnia minden olyan információt, amit a (jelen dokumentumban meghatározott) rendszer értékelési módszertan egy munkaegysége kimondottan megkövetel.

Az alábbiak részletezik az ASTE (rendszer tesztelés) és ASVA (rendszer sebezhetőség felmérés) garanciaosztály által meghatározott, SER-ben megadandó információkat.

7.2.4.1. Rendszer tesztelés

Az értékelőnek be kell mutatnia a rendszer integrátor tesztelésének általános módszerét és a tesztelésbe fektetett munkát. A cél a rendszer integrátor tesztelési munkájának érdemi áttekintése. (Nem cél a specifikus tesztlépések vagy egyedi tesztek eredményeinek pontos megismétlése.) Az alábbi információkat célszerű megadni:

- A STOE teszt konfigurációk (a ténylegesen tesztelt STOE konfigurációk, köztük az, hogy a teszt felállítása vagy a tesztet követő rendteremtés igényelt-e külön jogosultságú kódot).
- Tesztelési módszer (a rendszer integrátor által alkalmazott tesztelési stratégia áttekintése).
- Tesztelési eredmények (a rendszer integrátor tesztelési eredményének áttekintő leírása).

Az értékelőnek be kell mutatnia a saját tesztelésének általános módszerét és a tesztelésbe fektetett munkát. A cél áttekintést adni a tesztelés módszeréről, konfigurációjáról, mélységéről és eredményeiről. (Nem cél a specifikus tesztlépések vagy egyedi tesztek eredményeinek pontos megismétlése.) Az alábbi információkat célszerű megadni:

- STOE teszt konfigurációk (a ténylegesen tesztelt STOE konfigurációk).
- A kiválasztott tesztkészlet nagysága (az értékelés során tesztelt interfészek mennyisége és ennek rövid indoklása).
- A megismételt rendszer integrátori tesztek kiválasztásának szempontjai (rövid állításokban megfogalmazva).
- A végrehajtott független tesztek (ezek mennyisége és a kiválasztásukhoz használt szempontok rövid leírása).
- A tesztelt interfészek (áttekintő felsorolás).
- A tevékenység alapján hozott határozat (az értékelés során végzett tesztelés eredményének általános megítélése).

7.2.4.2. Rendszer sebezhetőség felmérés

7.2.4.2.1. Alap garanciacsomag esetén

Az értékelőnek be kell mutatnia az (automatikus eszközökkel) végzett behatolás tesztelésének módszerét, konfigurációját, mélységét és eredményeit. A cél az értékelő behatolás tesztelési munkájának érdemi áttekintése. (Nem cél, hogy a behatolás teszteléssel kapcsolatos specifikus tesztlépések vagy egyedi behatolás tesztek eredményeinek pontos megismétlése.) Az alábbi információkat célszerű megadni:

- STOE tesztkonfigurációk (a behatolás tesztelésnél használt konkrét STOE konfigurációk).
- A behatolás teszt során tesztelt interfészek (rövid felsorolás).
- A behatolás tesztelésre felhasznált automatikus eszközök (pontos verziószámmal és beállítási paraméterekkel).
- Az altevékenység alapján született határozat (a behatolás tesztelés eredményeinek általános megítélése).

Az értékelőnek a lehetséges sebezhetőségekre irányuló keresés területéről be kell mutatnia az alábbiakat:

— A meghatározott lehetséges sebezhetőségek (amelyek tesztelhetők és az STOE üzemeltetési környezetében elvileg szóba jöhetnek).

Az értékelőnek meg kell adnia az összes feltárt kihasználható sebezhetőséget és maradvány sebezhetőséget, az alábbi adatokkal:

— Forrás (pl. azon értékelői tevékenység, melynek végrehajtása során észlelték, az értékelő ismerte, pl. szakirodalomban olvasott róla).
— A nem kielégített funkcionális biztonsági követelmények (SFR).
— Leírás (rövid áttekintés a sebezhetőségről).
— Kihasználható-e vagy sem az üzemeltetési környezetben (vagyis kihasználható vagy maradvány sebezhetőségről van szó).
— Az azonosított sebezhetőség kihasználáshoz szükséges felhasznált idő, szakértelem, rendszer ismeret, hozzáférési lehetőség és eszköz megbecslése.

7.2.4.2.2. Fokozott garanciacsomag esetén

Az alap garanciacsomag elvárásain túl még az alábbiakat kell teljesíteni:

Az értékelőnek be kell mutatnia azokról a megvizsgált bizonyítékokról, melyet felhasznált a lehetséges sebezhetőségekre irányuló keresésére. A bizonyítékok kiválasztása származhat az értékelő által meghatározott olyan problémás területekből, amely a támadó által is feltehetően elérhető bizonyítékhoz kapcsolódik, vagy megfelelhet az értékelő által adott valamilyen más magyarázatnak.

Az értékelőnek a lehetséges sebezhetőségekre irányuló keresés területéről be kell mutatnia az alábbiakat is:

— A keresés során megvizsgált bizonyítékok (rövid felsorolás).

Az értékelő a lehetséges sebezhetőségek meghatározásához tanulmányozza a nyilvánosan rendelkezésre álló információ forrásokat, beleértve a következőket:

— szakértői publikációk (folyóiratok, könyvek);
— tanulmányok.

Az értékelőnek áttekintést kell adnia független sebezhetőség vizsgálatáról, mely a rendszer által kielégítendő SFR-ekre nézve vegye tekintetbe az összes alábbi általános sebezhetőség típust:

— az értékelés alatt álló STOE-t alkotó komponensek típusára vonatkozó általános lehetséges sebezhetőségek;
— megkerülés;
— hamisítás;
— közvetlen támadások;
— megfigyelés;
— helytelen használat/visszaélés.

Az értékelőnek szerepeltetnie kell a maradvány kockázatok között az alábbiakat:

— azok a rendszer biztonsági funkcionalitást érvényre juttató komponensek, melyekre nincs CC EAL3 (vagy MIBÉTS fokozott) tanúsítási eredmény,
— azok a rendszer biztonsági funkcionalitást támogató komponensek, melyekre nincs CC EAL2 (vagy MIBÉTS alap) tanúsítási eredmény.

7.2.4.2.3. Kiemelt garanciacsomag esetén

A fokozott garanciacsomag elvárásait az alábbi kiegészítésekkel és módosításokkal kell teljesíteni:

Az értékelő a lehetséges sebezhetőségek meghatározásához tanulmányozza az alábbiakat is:
— konferencia kiadványok.

A kihasználható sebezhetőségek meghatározásánál a támadókról megemelt-alap támadási képességet kell feltételezni (a másik két vizsgálat „alap” támadási képességével szemben).

Az értékelőnek szerepeltetnie kell a maradvány kockázatok között az alábbiakat:
— azok a rendszer biztonsági funkcionalitást érvényre juttató komponensek, melyekre nincs CC EAL4 (vagy MIBÉTS kiemelt) tanúsítási eredmény,
— azok a rendszer biztonsági funkcionalitást támogató komponensek, melyekre nincs CC EAL3 (vagy MIBÉTS fokozott) tanúsítási eredmény.

7.2.5. Következtetések és javaslatok

Az értékelőnek jelentésbe kell foglalnia az értékelés következtetéseit, amelyek alapvetően arra vonatkoznak, hogy az értékelt rendszer megfelel-e rendszer biztonsági előirányzatának.

Az értékelő javaslatokat fogalmazhat meg a rendszer tulajdonos és a rendszer integrátor felé, mely hasznos lehet az akkreditor számára is.

A javaslatok a rendszer értékelése során feltárt hiányosságokra, gyengeségekre, vagy ellenkezőleg, a különösen előnyös tulajdonságokra vonatkozhatnak.

7.2.6. Az értékelési bizonyítékok listája

Ebben a fejezetben az értékelőnek valamennyi értékelési bizonyítékra meg kell adnia az alábbi információkat:
— a kibocsátó szervezet (pl. rendszer tulajdonos, rendszer integrátor),
— cím,
— egyedi azonosító (pl. kibocsátási dátum és verziószám).

7.2.7. Hivatkozások, rövidítések és szakkifejezések

Ebben a fejezetben az értékelőnek meg kell határoznia a SER-ben használt valamennyi hivatkozást, valamint a rövidítések és szakkifejezések jelentését.

7.2.8. Észrevételezési jelentések

Ebben a fejezetben az értékelőnek jelentésbe kell foglalnia az értékelés során keletkezett észrevételezési jelentéseket egyedileg azonosító teljes listát, az egyes OR-ek állapotát is feltüntetve.

A listának minden észrevételezési jelentésre tartalmaznia kell az OR azonosítóját, illetve a címét vagy rövid tartalmi összefoglalását.

8. Bibliográfia

9. Rövidítésgyűjtemény

Jelen dokumentum a 7. táblázatban bemutatott rövidítéseket használja.

7. táblázat – A dokumentumban használt rövidítések

Rövidítés	Angol	Magyar
ASCM	Assurance: System Configuration Management	"Rendszer konfiguráció kezelés" garanciaosztály
ASCM_SBC	ASCM: System Base-Configuration	Rendszer alap konfiguráció garanciacsalád
ASCM_ECC	ASCM: Evaluated and Certified Components	Értékelt és tanúsított komponensek garanciacsalád
ASDV	Assurance: System Development	"Rendszer fejlesztés" garanciaosztály
ASDV_ARC	ASDV: Security Architecture	Biztonsági architektúra garanciacsalád
ASDV_MOD	ASDV: Modification	A terv dokumentációk aktualizálása garanciacsalád
ASDV_OSC	ASDV: Operational Security Concepts	Rendszer-működési biztonsági koncepció garanciacsalád
ASDV_SDS	ASDV: STOE Design	STOE terv garanciacsalád
ASDV_SIS	ASDV: System Interface specification	Rendszer interfész specifikáció garanciacsalád
ASGD	Assurance: System Guidance documents	"Rendszer útmutató dokumentumok" garanciaosztály
ASGD_CON	ASGD: Configuration guidance	Konfigurálási útmutató garanciacsalád
ASGD_MOD	ASGD: Modification	Az útmutató dokumentációk aktualizálása garanciacsalád
ASGD_OPE	ASGD: Operational user guidance	Üzemeltetési útmutató garanciacsalád
ASGD_PRE	ASGD: Preparative guidance	Előkészítő útmutató garanciacsalád
ASST	Assurance: System Security Target	"Rendszer biztonsági előirányzat" garanciaosztály
ASST_CCL	ASST: Conformance Claims	Megfelelőségi nyilatkozatok garanciacsalád
ASST_ECD	ASST: Extended Components Definition	Kiterjesztett összetevő meghatározás garanciacsalád
ASST_INT	ASST: Introduction	ST bevezetés garanciacsalád
ASST_OBJ	ASST: Security Objectives	Biztonsági célok garanciacsalád
ASST_REQ	ASST: IT Security Requirements	IT biztonsági követelmények garanciacsalád
ASST_SPD	ASST: Security Problem Definition	Biztonsági probléma meghatározás garanciacsalád
ASST_SDC	ASST: Security Domain Conformance Claims	Biztonsági tartomány megfelelőségi nyilatkozatok garanciacsalád
ASST_SDI	ASST: Introduction	Bevezetés garanciacsalád
ASST_SDE	ASST: Security Domain Extended Components Definition	Biztonsági tartomány kiterjesztett összetevő meghatározás garanciacsalád
ASST_SDO	ASST: Security Domain Security Objectives	Biztonsági tartomány biztonsági célok garanciacsalád

Rövidítés	Angol	Magyar
ASST_SDP	ASST: Security Domain Security Problem Definition	Biztonsági tartomány biztonsági probléma meghatározás garanciacsalád
ASST_SDR	ASST: Security Domain IT Security Requirements	Biztonsági tartomány IT biztonsági követelmények garanciacsalád
ASST_SDS	ASST: Security Domain Summary Specification	Biztonsági tartomány összefoglaló előírás garanciacsalád
ASST_SSS	ASST: STOE Summary Specification	STOE összefoglaló előírás garanciacsalád
ASTE	Assurance: Security Tests	"Rendszer tesztelés" garanciaosztály
ASTE_COV	ASTE: Coverage	Lefedettség garanciacsalád
ASTE_DPT	ASTE: Depth	Mélység garanciacsalád
ASTE_FUN	ASTE: Functional tests	Funkcionális tesztek garanciacsalád
ASTE_IND	ASTE: Independent testing	Független tesztelés garanciacsalád
ASTE_MOD	ASTE: Modification	Regressziós tesztelés garanciacsalád
ASVA	Assurance: System Vulnerability Assessment	"Rendszer sebezhetőség felmérés" garanciaosztály
ASVA_VAN	ASTE: Vulnerability Analysis	Sebezhetőségi elemzés garanciacsalád
CC	Common Criteria	Közös szempontok
CEM	Common Evaluation Methodology	Közös értékelési módszertan
CM	Configuration Management	Konfiguráció kezelés
EAL	Evaluation Assurance Level	Értékelési garanciaszint
IT	Information Technology	Információs technológia, informatika
KOP	---	Közigazgatási Operatív Programok
MIBÉTS	---	Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma
MEH	---	Miniszterelnöki Hivatal
OSP	Organisational Security Policy	Szervezeti biztonsági szabályzat
OR	Observation Report	Észrevételezési jelentés
SAP	Security Assurance Package	Rendszer garanciacsomag
SAR	Security Assurance Requirement	Garanciális biztonsági követelmény
SER	System Evaluation Report	Rendszer értékelési jelentés
SFR	Security Functional Requirement	Funkcionális biztonsági követelmény
SSF	STOE Security Functionality	Rendszer biztonsági funkcionalitás
SSFI	STOE Security Functions Interface	Rendszer biztonsági funkcionalitás interfésze
SST	System Security Target	Rendszer biztonsági előirányzat
STOE	System Target of Evaluation	Rendszer értékelés tárgya

10. Fogalomtár

-

11. Ábrák

12. Képek

-

13. Táblázatok

14. Verziószám

V4