KÖZIGAZGATÁSI INFORMATIKAI BIZOTTSÁG

25. számú Ajánlása

Magyar Informatikai Biztonsági Ajánlások (MIBA)

25/2.
Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)

25/2-4. segédlet
Útmutató Értékelőknek

1.0 verzió

2008. június

Közigazgatási Informatikai Bizottság
25. számú Ajánlása

Készült a
Miniszterelnöki Hivatal megbízásából

Összeállította:
Balázs István

Közreműködött:
Balázs István,
Staub Klára,
Szabó István

Az ajánlás a Közigazgatási Informatikai Bizottság (KIB)
Jogi és Műszaki Szabályozási Albizottsága észrevételei alapján véglegesített tartalommal
a KIB tagjainak 2008. május-júniusi elektronikus távszavazása alapján
került elfogadásra

TARTALOMJEGYZÉK

1. BEVEZETÉS 4
1.1 ELŐZMÉNYEK ÉS ALKALMAZÁSI TERÜLET 4
1.2 JELEN DOKUMENTUM CÉLJA ÉS FELÉPÍTÉSE 5
1.3 KAPCSOLÓDÓ DOKUMENTUMOK 5
1.4. SZAKKIFEJEZÉSEK ÉS MEGHATÁROZÁSOK 6
2. FEJEZET AZ ÉRTÉKELŐ FELADATAI 7
2.1 FELADATOK AZ ÉRTÉKELÉS ELŐKÉSZÜLETI SZAKASZÁBAN 7
2.1.1 A megbízó támogatása az értékelés kereteit meghatározó döntések meghozatalában 7
2.1.2 Felkészülés az értékelésre 10
2.2 FELADATOK AZ ÉRTÉKELÉS LEBONYOLÍTÁSI SZAKASZÁBAN 13
2.2.1 A sebezhetőség felmérés kitüntetett szerepe az értékelési módszertanban 13
2.2.2 Az értékelés során készítendő dokumentumok, értékelői bizonyítékok 13
2.3 FELADATOK AZ ÉRTÉKELÉS KÖVETKEZTETÉSI SZAKASZÁBAN 15
2.4 FELADATOK AZ ÉRTÉKELÉSI ÉS TANÚSÍTÁSI FOLYAMAT LEZÁRÁSÁT KÖVETŐEN 15
2.4.1 A fejlesztői bizonyítékok és a saját bizonyítékok kezelése 15
2.4.2 Garancia karbantartás 15
3. FEJEZET MELLÉKLETEK 16
3.1 AZ MSZ ISO/IEC 9126 SZEMPONTRENDSZERE A SZOFTVERMINŐSÉG ELBÍRÁLÁSÁRA 16
3.2 AZ ISO/IEC 14598 ÉRTÉKELÉSI SZINTJEI ÉS ALAPELVEI SZOFTVERTERMÉKEK ÉRTÉKELÉSÉRE 18
3.3 AZ ÉRTÉKELÉSI MUNKATERV FELÉPÍTÉSE ÉS TARTALMA 19
3.3.1. 1. fejezet: Bevezetés 19
3.3.2 2. fejezet: Az értékelés tárgyának leírása 19
3.3.3 3. fejezet: Értékelői munkacsomagok 20
3.3.4 4. fejezet: A munkaterv indoklása 20
3.3.5 5. fejezet: Korlátozó tényezők 21
3.3.6 1. melléklet: Az értékelői munkacsomagok specifikációja 21
3.3.7 2. melléklet (1. alternatíva): Értékelési ütemterv 22
3.3.8 2. melléklet (2. alternatíva): Az értékelésre átadandó fejlesztői bizonyítékok, és ezek átadásának ütemezése 22
3.4 A CC ÉS A CEM/MIBÉTS STRUKTÚRÁK KÖZÖTTI KAPCSOLAT 23
3.5 ÉRTÉKELŐI HATÁROZATOK 24
3.6 ÁLTALÁNOS ÉRTÉKELŐI FELADATOK 26
3.6.1 Az értékelés bemeneti feladata 27
3.6.2 Az értékelés kimeneti feladata 28
HIVATKOZÁSOK ÉS RÖVIDÍTÉSEK 30
HIVATKOZÁSOK 30
RÖVIDÍTÉSEK JEGYZÉKE 31

1. BEVEZETÉS

1.1 ELŐZMÉNYEK ÉS ALKALMAZÁSI TERÜLET

A Közigazgatási Informatikai Bizottság által kiadott Magyar Informatikai Biztonsági Ajánlások (MIBA) keretében két általános módszertani ajánlás készült, egy szervezeti-irányítási (MIBIK) és egy technológia-biztonsági (MIBÉTS). Mindkettő a biztonságos informatikai rendszerek kialakítását és fenntartását kívánja segíteni:

- a MIBIK (Magyar Informatikai Biztonsági Irányítási Keretrendszer) a szervezeti/irányítási szemléletet és szaktudást igénylő feladatokban,
- a MIBÉTS (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma) pedig a technológiai szemléletet és szaktudást igénylő feladatokban.

A két ajánlás egymást kiegészítve és erősítve támogatást nyújt a rendszerfejlesztési életciklus valamennyi szakaszában a biztonság megtervezéséhez, megvalósításához, értékeléséhez és fenntartásához.

A MIBÉTS célja informatikai termékekre és rendszerekre irányuló, független, nemzetközi módszertanon alapuló értékelési és tanúsítási rendszer kialakítása, mely segíti:

- mind a felhasználókat, beszerzőket a felkínált informatikai termékek és rendszerek biztonsági szintjének megalapozott megítélésében, a rendszerek biztonságos üzemeltetési feltételeinek kialakításában;
- mind a fejlesztőket, gyártókat, forgalmazókat termékeik és rendszereik biztonságára vonatkozó állításaik független igazolásában.

A séma a [3] nemzetközi szabványban meghatározott értékelési módszertan honosítása mellett szervezeti és eljárásbeli keretet ad a Magyarországon belül végrehajtott technológiai értékelések számára, beleértve az értékeléseket végző vizsgálólaboratóriumok (értékelő szervezetek) és tanúsító szervezetek feladatleírását, valamint a javasolt technikák és eljárások meghatározását is.

1.2 JELEN DOKUMENTUM CÉLJA ÉS FELÉPÍTÉSE

Jelen dokumentum a MIBÉTS segédlet sorozatának 4. eleme.

Célja a MIBÉTS keretében végrehajtott technológiai értékelések értékelői számára útmutatás nyújtása az elvégzendő feladatok áttekintésével és magyarázatával. /Az értékelés módszertanát egy külön segédlet - [7] részletezi./

Célközönsége a biztonsági értékelésben érintett értékelő szervezetek és tanúsító szervezet szakértői.

A dokumentum 2. fejezete az értékelők feladatait határozza meg, az értékelés különböző szakaszaiban. Ez a rész a [4] által valamennyi MIBÉTS résztvevő szempontjából áttekintett feladatok részletezését, kibontását jelenti az értékelői feladatok tekintetében.

A 3. fejezet mellékletei az értékeléshez nyújtanak útmutatást:

- a 3.1 alfejezet az MSZ ISO/IEC 9126 szabvány értékelési szempontrendszerét hasonlítja össze a MIBÉTS értékelési szempontrendszerével,
- a 3.2 alfejezet az ISO/IEC 14598 szabvány értékelési szintjeit és alapelveit ismerteti a MIBÉTS hasonló fogalmainak egybevethetőségéhez,
- a 3.3 alfejezet az értékelési munkaterv elvárt felépítését és tartalmát határozza meg,
- a 3.4 alfejezet a CC és a CEM/MIBÉTS struktúrák közötti megfelelést tekinti át,
- a 3.5 alfejezet az értékelői határozatok meghozatalára vonatkozó általános szabályt ismerteti,
- a 3.6 alfejezet pedig az általános értékelői feladatokat írja le.

A segédletet a hivatkozások és a rövidítések jegyzéke zárja.

1.3 KAPCSOLÓDÓ DOKUMENTUMOK

A MIBA jelenlegi verziójához az alábbi segédletek készültek el:

- 1. számú segédlet: **Modell és folyamatok** [4]
- 2. számú segédlet: **Útmutató a megbízók számára** [5]
- 3. számú segédlet: **Útmutató a fejlesztők számára** [6]
- 4. számú segédlet: **Útmutató az értékelők számára** (jelen dokumentum)
- 5. számú segédlet: **Értékelői módszertan** [7]

1.4. SZAKKIFEJEZÉSEK ÉS MEGHATÁROZÁSOK

Jelen dokumentum céljára az alábbi szakkifejezések és meghatározások alkalmazandók.

akció - a CC 3. részben megadott értékelői tevékenység elem. Ezek az akciók vagy expliciten értékelői akcióként vannak megadva, vagy pedig impliciten, a fejlesztői akciókból vannak származtatva (beleértett értékelői akciók) a CC 3. rész garanciösszetevőin belül.

tevékenység – a CC 3. rész egyik garanciaosztályának az alkalmazása.

értékelési átadandó – bármely forrás, amelyet az értékelő vagy átvizsgáló kér be a szponzortól vagy fejlesztőtől abból a célból, hogy egy vagy több értékelési vagy értékelést átvizsgáló tevékenységet hajtson végre.

fejlesztői bizonyíték – kézzelfogható értékelési átadandó.

értékelési jelentés – jelentés, amely dokumentálja az általános határozatot és annak indoklását, és amelyet az értékelő állít elő és ad át egy átvizsgálónak.

módszertan – elveknek, eljárásoknak és folyamatoknak a rendszere, amelyet informatikai biztonságértékelésre használnak.

észrevételezési jelentés – jelentés, amelyet az értékelő készít abból a célból, hogy az értékelés során felmerülő kérdések tisztázását vagy beazonosítását kérje.

általános határozat – megfelelt vagy nem felelt meg nyilatkozat, amelyet egy értékelő bocsát ki egy értékelés eredményét illetően.

jelentés – az értékelési eredményeknek és az alátámasztó anyagnak a belefoglalása egy értékelési jelentésbe vagy egy észrevételezési jelentésbe.

séma – szabályoknak egy összessége, amelyet egy értékelő hatóság vezet be, és amely definiálja az értékelési környezetet, beleértve az informatikai biztonságértékelések végrehajtásához szükséges szempontokat és módszertant.

altevékenység – a CC 3. rész egyik garanciaösszetevőjének az alkalmazása. A garanciacsaládok nincsenek expliciten célbavéve a CEM-ben, mivel az értékelések egy garanciacsaládból származó egyetlen garanciaösszetevőre vonatkozóan vannak végrehajtva.

határozat – megfelelt, nem felelt meg vagy nem bizonyított nyilatkozat, amelyet egy értékelő bocsát ki egy CC értékelési tevékenység elemet, garanciaösszetevőt vagy garanciaosztályt illetően. Lásd még: általános határozat.

munkaegység – az értékelői munka legjobban részletezett szintje. Minden CEM akció egy vagy több munkaegységet foglal magában, amelyek a CEM akción belül csoportosítva vannak a CC tartalom- és bizonyítékbemutatás vagy fejlesztői akcióelem szerint.

2. FEJEZET
AZ ÉRTÉKELŐ FELADATAI

Az értékelő általános felelőssége az alábbiakat foglalja magában:

1. az értékelésre átadandó fejlesztői bizonyítékok átvétele és megfelelő kezelése,
2. az értékelési módszertan által megkövetelt értékelési tevékenységek végrehajtása,
3. a szükséges értékelési támogatás kérése, fogadása (pl. a fejlesztő általi képzés, a tanúsító értelmezései),
4. a tanúsításra átadandók elkészítése,
5. a tanúsító szervezetet az értékelés során képviselő átvizsgáló számára az értékelői általános határozat és minden más közbenső értékelői határozat dokumentálása és indoklása,
6. a MIBÉTS általános elveinek és az értékelésre vonatkozó előírásainak való megfelelés.

Az alábbiak részletesen meghatározzák az értékelő feladatait.

2.1 FELADATOK AZ ÉRTÉKELÉS ELŐKÉSZÜLETI SZAKASZÁBAN

Bár egy értékelés előkészítésénél a megbízónak és a fejlesztőnek van a legtöbb feladata, fontos szerep jut az értékelőnek is. Szakmai támogatást kell nyújtania a megbízó számára, hogy az megalapozottan dönthessen az értékeléssel kapcsolatos alapkérdésekben, illetve reális képet kapjon döntésének következményeiről (a szükséges erőforrásokról és a sikeres értékelés egyéb feltételeiről). Fel kell készülnie az értékelésre, ennek keretén belül szerződést kell kötnie a megbízóval, és értékelési munkatervet (ld. 3.3 alfejezet) kell készítenie.

2.1.1 A MEGBÍZÓ TÁMOGATÁSA AZ ÉRTÉKELÉS KERETEIT MEGHATÁROZÓ DÖNTÉSEK MEGHOZATALÁBAN

Az értékelő jelentős segítséget adhat több olyan alapkérdés eldöntéséhez, melyet a megbízónak az értékelés előtt meg kell hoznia:

- az értékelés tárgya pontos határainak meghatározása,
- a biztonsági előirányzat elkészítése vagy elkészíttetése,
- az értékelési garanciaszint meghatározása,

- választás a fejlesztéssel párhuzamos és a fejlesztést követő értékelés között.

Ezt a segítséget egy opcionális és egy kötelező feladat elvégzésével adja meg.

Megvalósíthatósági tanulmány készítése

Az értékelő egy megvalósíthatósági tanulmányt készíthet, melyben felméri a sikeres értékelés valószínűségét. Ebben a tanulmányban az értékelő olyan változtatásokat tanácsolhat, melyek az értékelés biztosabb megalapozásához szükségesek.

A megvalósíthatósági tanulmány készítésekor (és majd az egész értékelés alatt is) az értékelőnek ajánlott figyelembe vennie a megbízó és a fejlesztő tőle eltérő megközelítési módját és szakmai preferenciáit. A megvalósíthatósági tanulmányban érdemes röviden összefoglalni az esetleges értékelés azon szakmai vonatkozásait, ami jelentősen eltér egy szabványos fejlesztés szempontjaitól, illetve ami nagyon hasonlít ahhoz.

Ehhez az összehasonlításhoz jelen útmutató két figyelemre érdemes szempontot ad.

Az első szempont (a 3.1 alfejezet) egy szoftverminőségre vonatkozó "alapszabvány" szempontrendszerének egybevetése a MIBÉTS elvárásaival.

A mellékletben felsorolt hierarchikus szempontrendszerből jól látható, hogy egy fejlesztőnek (szoftver fejlesztés esetén) a biztonságon kívül nagyon sok más szempontot is figyelembe kell vennie a fejlesztés során.

A MIBÉTS keretén belül az értékelőnek ezt nem szabad figyelmen kívül hagynia. Az ő felelőssége elsődlegesen az informatikai biztonság értékelésére és az ezzel közvetlen kapcsolatban álló területek elemzésére korlátozódik. Amikor egy sokkal általánosabb igényű fejlesztői dokumentációt tanulmányoz (pl. egy felhasználói útmutatót), el kell fogadnia, hogy az adott dokumentáció többről szól, mint amire neki szüksége van. Az értékelő felelőssége ilyenkor a biztonság-kritikus részek megtalálása és annak teljességének, belső és külső ellentmondás mentességének értékelése.

A második szempont (3.2 alfejezet) egy szoftverek kiértékelésére vonatkozó szabvány és a MIBÉTS alapelveinek egybevetése. A mellékletben kiemelt részek világosan mutatják, hogy az ISO/IEC 14598 szabvány alap elvárásai a szoftvertermék kiértékelésére teljes mértékben összhangban vannak a MIBÉTS értékelési módszertanának általános elveivel (az alkalmasság elve, a pártatlanság elve, az objektivitás elve, a megismételhetőség elve, az újraelőállíthatóság elve, az eredmények helyességének elve).

Az értékelőnek érdemes figyelembe vennie ezt a két szempontot (a megbízónak/fejlesztőnek nagyon sok más szempontot is figyelembe kell vennie, mint az

értékelőnek, de az értékeléstől elvárt alapelvek közérthetőek és minden résztvevő számára elfogadhatóak) a megbízóval és a fejlesztővel való együttműködése során.

A biztonsági előirányzat áttekintése, előzetes értékelése

Az előkészületi szakaszban az értékelőnek át kell tekintenie a megbízó által számára biztosított biztonsági előirányzatot annak megállapítása érdekében, hogy az "lényegében teljes". Egy "lényegében teljes" biztonsági előirányzat minden részének valamennyi lényeges információt tartalmaznia kell:

- bevezetés (azonosítás, áttekintés, CC megfelelőségi kijelentés),
- az értékelés tárgya leírása (benne az értékelés tárgya pontos határainak meghatározásával),
- az értékelés tárgya biztonsági környezete (feltételezések, fenyegetések, szervezetbiztonsági szabályzatok),
- biztonsági célok (az értékelés tárgyára vonatkozó és a környezetre vonatkozó célok egyaránt),
- az informatikai biztonság követelményei (funkcionális és garanciális követelmények egyaránt),
- összefoglaló előírás,
- védelmi profil nyilatkozatok (ha van legalább egy kiválasztott védelmi profil),
- indoklások.

Annak tudatában, hogy az egyes részek kiegészítésére vagy módosítására az értékelés tárgyának értékelése során még szükség lehet, az áttekintett biztonsági előirányzatnak elegendő információt kell szolgáltatnia ahhoz, hogy előzetesen eldönthető legyen, vajon jelenlegi formájában alkalmazható-e az értékelés folyamán viszonyítási alapként, követelmény-rendszer meghatározásként.

Pozitív előzetes értékelési eredmény egyben megerősítése annak is, hogy az értékelés tárgya határainak meghatározása pontos, érthető és elfogadható az értékelő számára, egyúttal a megadott értékelési garanciaszintet indokoltnak és elérhetőnek tartja.

A negatív eredmény indoklása pedig közvetlen visszacsatolást biztosít a megbízó számára, mit kell módosítania az értékelés megindíthatósága érdekében.

Az értékelés garanciaszintjének kölcsönös elfogadása jelentősen befolyásolja az értékelésre fordítandó erőforrások nagyságát, egyben az értékeléssel elérhető független garancia mértéket, s ezzel az értékeléstől várt pozitív hatásokat is. A biztonsági előirányzat előzetes

értékelésével az értékelő (anélkül, hogy átvállalná a döntés felelősségét), korábbi tapasztalatai és az értékeléssel kapcsolatos mélyebb szaktudása alapján segíti a megbízót abban, hogy reális határokat és elérhető értékelési garanciaszintet tűzzön ki.

2.1.2 FELKÉSZÜLÉS AZ ÉRTÉKELÉSRE

Szerződéskötés

A szerződéskötésre az [5] segédletben meghatározott szempontok az értékelő számára is irányadók.

Értékelési munkaterv és ütemterv készítése

A megbízó által kiválasztott és megbízott értékelő első feladata a sémába fogadás feltételét is jelentő értékelési munkaterv és (az ennek részét képező, vagy különálló) értékelési ütemterv elkészítése.

A megbízóval és a fejlesztővel folytatott konzultációk eredményét is tartalmazó értékelési munkaterv és értékelési ütemterv az egész értékelési folyamat menetét meghatározó, fontos munkaanyag, melynek (saját munkájának megtervezésén kívül) kettős célja van:

- a megbízó és a fejlesztő tájékoztatása az elvárt fejlesztői támogatás mértékéről és ütemezéséről,
- a tanúsító tevékenységének megalapozása.

Az értékelési munkaterv a tanúsító számára is kritikus jelentőséggel bír, a tanúsítási tevékenységek megtervezése szempontjából. Az értékelési munkaterv tartalmazza az értékelés során végrehajtásra kerülő összes értékelői munkacsomagot, az egyes munkacsomagok várható eredményeit, s ezek dokumentálásának módját.

Az értékelési munkatervet olyan részletességgel kell elkészíteni, amiből kiderül, hogy az értékelő tisztában van feladataival, és képes a séma módszertanának megfelelően végre is hajtani azokat.

A tanúsító az értékelési munkatervet kiindulópontként használja saját tanúsítási terve kidolgozásához. Segítségével pontosabban meg tudja tervezni a tanúsítási tevékenységeket.

A jól megírt és kellően részletes értékelési munkaterv a tanúsító számára betekintést nyújt az értékelő munkacsoport által tervezett folyamatokba és elemzési módszerekbe. Az értékelő így az értékelési munkatervet arra is felhasználhatja, hogy dokumentálja a szükséges értékelési elemzésekre és módszerekre vonatkozó tudását.

A kevés konkrét részletet tartalmazó értékelési munkaterv nem győzi meg a tanúsítót az értékelő kellő felkészültségéről, ezért a tanúsítónak részletesebb ellenőrzésre kell felkészülnie a tanúsítás során.

Az értékelői munkaterv kötelező felépítését és minimálisan elvárt tartalmát a 3.3 melléklet határozza meg.

Az értékelési ütemterv összeállításához az alábbi irányelvek adhatók:

1. **Érdemes elkülönítve tervezni és ütemezni a fejlesztői környezetre vonatkozó általánosabb vizsgálatokat az értékelés tárgyára irányuló konkrétabb értékelői feladatoktól.**

   A fejlesztői környezet jelentősen befolyásolja (elősegítheti vagy megnehezítheti) annak sikerét, hogy a biztonsági előirányzatban meghatározott biztonsági funkciókat a fejlesztés folyamán helyesen valósítják meg.

   A legtöbb fejlesztő előre kidolgozott és elfogadott eljárásokat használ a fejlesztés tárgyának konfiguráció kezelésére, a fejlesztési környezet biztonságának megvédésére, a fejlesztett termék/rendszer életciklusára, ezen belül a felhasználóhoz való szállítására, majd ott a telepítésre és elindításra.

   Sok fejlesztő ezeket a folyamatokat minőségirányítási eljárásai keretében pontosan dokumentálta, s különböző fejlesztéseihez többé-kevésbé egységesen alkalmazza is.

   A MIBÉTS szempontjából legszerencsésebb esetben a fejlesztő még auditáltatta is minőségirányítási rendszerét egy erre szakosodott független szervezettel, mely eredményeket feltétlenül érdemes figyelembe venni a séma informatikai biztonságra koncentráló értékelésénél is.

   Mindhárom fenti eset lehetővé teszi a fejlesztői környezet önálló (az adott értékelés tárgyától részlegesen függetlenített) vizsgálatát. Ez a megközelítés azzal az előnnyel is jár, hogy ugyannak a fejlesztőnek egy másik termékének későbbi értékelésekor az értékelő felhasználhatja a fejlesztői környezetre irányuló értékelési eredményeit.

   Az alábbi értékelői tevékenységek együttes (és az értékelés tárgyától részlegesen elkülönülő) elvégzése javasolható:

   - a konfiguráció kezelés értékelése (mindhárom értékelési garanciaszinten)
   - az életciklus támogatásának értékelése (fokozott és kiemelt garanciaszinten),
   - a szállítás és működtetés értékelése (mindhárom garanciaszinten).

2. Be kell tartani az értékelői tevékenységek közötti sorrendbeli kötöttségeket.

Ezek a kötöttségek az alábbiak:

- a "Tesztelés" garanciaosztály értékelésére alapvetően a "Fejlesztés" garanciaosztály értékelését követően kerüljön sor,
- a "Sebezhetőség felmérése" garanciaosztály értékelésére alapvetően minden más értékelői tevékenységet követően kerüljön sor.

Az "alapvetően" kifejezés azt jelenti, hogy a sorrend elvárás az értékelési tevékenységeken belül végrehajtott értékelői feladatelemek többségére vonatkozik, esetleg egyes összetettebb, összehasonlítást igénylő feladatelem és a határozatok meghozatala kivételével.

3. Érdemes kötött sorrendet tartani egyes értékelői altevékenységek között is.

Az alábbi sorrend betartása erősen javasolt:

- a "Fejlesztés" garanciaosztály értékelésén belül:
  - a funkcionális specifikáció értékelése (ADV_FSP),
  - a magas szintű terv értékelése (ADV_HLD),
  - az alacsony szintű terv (ADV_LLD, csak kiemelt garanciaszinten),
  - a részleges megvalósítás értékelése (ADV_IMP, csak kiemelt garanciaszinten),
  - a reprezentáció megfelelés értékelése (ADV_RCR, mindhárom garanciaszinten),
- az "Útmutató dokumentációk" garanciaosztály értékelésén belül:
  - az adminisztrátori útmutató értékelése (AGD_ADM),
  - a felhasználói útmutató értékelése (AGD_USR),
- a "Tesztelés" garanciaosztály értékelésén belül:
  - a funkcionális tesztelés értékelése (ATE_FUN),
  - a teszt lefedettségének értékelése (ATE_COV),
  - a teszt mélységének értékelése (ATE_DPT, csak fokozott és kiemelt garanciaszinten),
  - a független tesztelés értékelése.

2.2 FELADATOK AZ ÉRTÉKELÉS LEBONYOLÍTÁSI SZAKASZÁBAN

Az értékelő egyik legfontosabb feladata magának az értékelésnek a végrehajtása.

A MIBÉTS keretében alkalmazandó értékelési feladatokat és azok elvégzésének módszertanát [7] határozza meg részletesen.

Jelen útmutató a fenti dokumentumot két új szemponttal egészíti ki, a sebezhetőség felmérés kitüntetett szerepének kihangsúlyozásával (és magyarázatával), valamint a tételesen elkészítendő értékelői anyagok megadásával (és áttekinthető táblázatba foglalásával).

2.2.1 A SEBEZHETŐSÉG FELMÉRÉS KITÜNTETETT SZEREPE AZ ÉRTÉKELÉSI MÓDSZERTANBAN

A sebezhetőség felmérése garanciaosztály az értékelés tárgyában lévő hibák, gyengeségek meglétének és a velük való visszaélések lehetőségének a meghatározására koncentrál. Ez a garanciaosztály már a MIBÉTS módszertan alapját képező Közös szempontokban (CC, [1] ill. [2]) és Közös értékelési módszertanban (CEM, [3]) is fontos szerepet játszik. A MIBÉTS keretében a CC és CEM hazai adaptálásával kidolgozott (egyszerűsített és költség-hatékonyabb) értékelési módszertanban ez a szerep még hangsúlyosabb.

A MIBÉTS módszertanában a legtöbb egyéb értékelői tevékenység a sebezhetőség felmérés valamely elemének (rosszul használhatóság értékelése, biztonsági funkcióerősség értékelés, független sebezhetőség vizsgálat) előkészítését célozza meg. "Nem felelt meg" határozat általában akkor születik, ha a sebezhetőségekkel szembeni ellenállás megkérdőjeleződik.

2.2.2 AZ ÉRTÉKELÉS SORÁN KÉSZÍTENDŐ DOKUMENTUMOK, ÉRTÉKELŐI BIZONYÍTÉKOK

Az értékelés lebonyolítási szakaszában az értékelő szükség esetén bármikor, "észrevételezési jelentés" formájában a megbízóhoz (s ezen keresztül a fejlesztőhöz), illetve a tanúsító szervezethez fordulhat.

A megbízó felé az értékelő észrevételezési jelentésében az értékelés folyamán felvetődő különböző súlyosságú problémákat jelezhet.

A tanúsító számára írt észrevételezési jelentésben az értékelő olyan problémákról írhat az értékelés tárgyával, a sémával, vagy annak módszertanával kapcsolatban, melynek megoldására segítséget, útmutatást vár a tanúsító szervezettől.

Az értékelés során különböző értékelői részjelentéseket (összefoglalókat, jegyzőkönyveket) kell írni, melyek kivonatát az értékelési jelentés eredményei közé (4. fejezet) is be kell venni. Az alábbi táblázat összefoglalja az értékelés során (tehát még az értékelés eredményeit összefoglaló értékelési jelentés megírása előtt) készítendő dokumentumokat, értékelői bizonyítékokat:

észrevételezési jelentés a megbízóhoz (s ezen keresztül a fejlesztőhöz)	opcionális (kijavítandó hiba, hiányosság esetén)
észrevételezési jelentés a tanúsítóhoz	opcionális (általános probléma felvetés, segítség és útmutatás kérése céljából)
az értékelési jelentés 4. fejezetébe kerülő összefoglalókat megalapozó részjelentések	kötelező

2.3 FELADATOK AZ ÉRTÉKELÉS KÖVETKEZTETÉSI SZAKASZÁBAN

Az értékelő másik legfontosabb feladata (az értékelés végrehajtása mellett) az értékelés eredményeinek dokumentálása és indoklása. [4] 7.2 alfejezete tartalmazza az értékelési jelentés szerkezetére és tartalmára vonatkozó séma elvárásokat.

2.4 FELADATOK AZ ÉRTÉKELÉSI ÉS TANÚSÍTÁSI FOLYAMAT LEZÁRÁSÁT KÖVETŐEN

Az értékelőnek az értékelési és tanúsítási folyamat befejezésével sem szűnik meg a felelőssége.

2.4.1 A FEJLESZTŐI BIZONYÍTÉKOK ÉS A SAJÁT BIZONYÍTÉKOK KEZELÉSE

Az értékelési folyamat végén az értékelésre megkapott fejlesztői bizonyítékokkal kapcsolatosan (a megbízóval kötött szerződéses megállapodásnak megfelelően) az értékelőnek az alábbi lehetőségei vannak:

- a bizonyítékokat visszaszolgáltatja a megbízónak, illetve a közvetlenül a fejlesztőktől kapott bizonyítékok esetében a fejlesztőnek,
- archiválja a bizonyítékokat gondoskodva azok bizalmasságának és sértetlenségének megőrzéséről,
- megsemmisíti a bizonyítékokat,
- az értékelési eredményeit megalapozó saját bizonyítékait ugyanakkor mindenképp archiválnia kell.

2.4.2 GARANCIA KARBANTARTÁS

Az értékelést és tanúsítást követően az értékelő folyamatos kötelezettsége lehet az idővel változó értékelés tárgya nyomon követése, s ennek alapján az értékelési eredmények érvényben maradásának vagy elévülésének deklarálása. Ez a tevékenysége ugyanakkor jelenleg a MIBÉTS hatókörén kívül esik (egészen a garancia karbantartására vonatkozó módszerek beépítéséig, mely egy későbbi verzióban várható).

3. FEJEZET
MELLÉKLETEK

3.1 AZ MSZ ISO/IEC 9126 SZEMPONTRENDSZERE A SZOFTVERMINŐSÉG ELBÍRÁLÁSÁRA

Az MSZ ISO/IEC 9126:2000 - "Információtechnika. Szoftvertermékek értékelése. Minőségi jellemzők és használatuk irányelvei" a szoftverminőség elbírálásához az alábbi hierarchikus szempontrendszert határozza meg:

- **funkcionalitás** (Mit kell kielégítenie a szoftvernek?)
- **megbízhatóság** (Milyen korlátokat szabnak a követelmények, a tervezés és a megvalósítás hiányosságai?)
- **használhatóság** (Milyen könnyen érthető meg, tanulható meg, és működtethető?)
- **hatékonyság** (Megfelelőek-e a válasz- és végrehajtási idők, valamint az erőforrás-kihasználás?)
- **karbantarthatóság** (Milyen könnyen módosítható az esetleges hibák kijavítása, továbbfejlesztés, vagy a változó környezethez és követelményekhez történő igazítás érdekében?)
- **hordozhatóság** (A felhasználó képes-e a megszokott módon dolgozni vele megváltozott szervezeti, hardver vagy szoftver környezetben is?)

A szabvány a jellemzők segédjellemzőkre történő alábbi finomítását is javasolja:

Funkcionalitás

- **alkalmasság** (Konkrét feladatokra használható funkciói legyenek.)
- **pontosság** (Helyes eredményt szolgáltasson, illetve az elvárt hatást váltsa ki.)
- **együttműködőképesség** (Legyen képes meghatározott rendszerekkel kölcsönhatásba kerülni.)
- **megfelelés** (Tartsa be a rá vonatkozó szabványokat, szabályokat, törvényi szabályozásokat és egyéb előírásokat.)
- **biztonság** (Akadályozza meg a véletlen vagy szándékos hozzáférési kísérleteket programokhoz és adatokhoz.)

Megbízhatóság

- **Kiforrottság** (Szoftverhiba miatt meghibásodás csak kis valószínűséggel, ritkán következzen be.)
- **Hibatűrés** (A szoftver teljesítményének egy meghatározott szintjét még szoftverhiba bekövetkezésekor és a használatára megadott szabályok megsértése esetén is tartsa fenn.)
- **Helyreállíthatóság** (Meghibásodás után elfogadható idő- és egyéb ráfordítás mellett a szoftver teljesítménye az eredeti szintre visszaállítható legyen, az adatok visszanyerhetők legyenek.)

Használhatóság

- **Érthetőség** (A felhasználó kis ráfordítással felismerhesse a mögöttes elveket és ezek alkalmazhatóságát.)
- **Megtanulhatóság** (A felhasználó kis ráfordítással megtanulhassa alkalmazását (például ellenőrizhesse működését, ismerje a bemeneteket és kimeneteket.))
- **Üzemeltethetőség** (A felhasználó kis ráfordítással ellenőrizhesse működtetését és működését.)

Hatékonyság

- **Időigény** (A válasz- illetve feldolgozási idők kicsik, az egységnyi időre eső teljesítmények nagyok legyenek.)
- **Erőforrásigény** (A felhasznált erőforrások alacsonyak, a felhasználás időtartama rövid legyen.)

Karbantarthatóság

- **Elemezhetőség** (A hibák és meghibásodási okok könnyen feltárhatók, a módosítandó részek egyszerűen azonosíthatók legyenek.)
- **Változtathatóság** (A módosítások, hibaeltávolítások, illetve a változó környezethez igazításhoz alacsony ráfordítás elég legyen.)
- **Stabilitás** (Alacsony legyen a kockázata a módosítások miatt fellépő nem várt következményeknek.)
- **Tesztelhetőség** (A módosított szoftver könnyen tesztelhető legyen.)

Hordozhatóság

- **Adaptálhatóság** (Különböző környezetekhez adaptálni lehessen, kizárólag olyan tevékenységek, illetve eszközök alkalmazásával, amelyekre fel van készítve, illetve el van látva.)
- **Telepíthetőség** (A szoftver egy adott környezetben gyorsan és egyszerűen telepíthető legyen.)
- **Műszaki megfelelőség** (A szoftver tartsa be a hordozhatósággal kapcsolatos szabványokat, illetve szabályokat.)
- **Kiválthatóság** (Egy másik szoftver helyett használni lehessen, annak környezetében, kis ráfordítás igénye mellett.)

3.2 AZ ISO/IEC 14598 ÉRTÉKELÉSI SZINTJEI ÉS ALAPELVEI SZOFTVERTERMÉKEK ÉRTÉKELÉSÉRE

Az ISO/IEC 14598 “Informatika – A szoftvertermék értékelése” című szabvány magának a kiértékelésnek a folyamatát szabályozza. Ennek egyik alapgondolata, hogy a kiválasztott értékelési szint nemcsak magától a terméktől, hanem annak felhasználásától és felhasználási környezetétől is függ, és meghatározza a kiértékelés mélységét vagy alaposságát. Az A, B, C, D szintek fő jellemzőit a következő táblázat foglalja össze.

Értékelési szint	**Kockázat**				**Tipikus alkalmazás**
	Biztonsági	**Gazdasági**	**Védelmi**	**Környezeti**	
D	Jelentéktelen tulajdoni kár, emberekre veszélytelen	Jelentéktelen veszteség	Nincs kockázat	Nincs kockázat	Szórakoztatás, háztartás
C	Tulajdoni kár, emberi sérülésveszély	Jelentős veszteség	Hibakockázat	Helyi szennyezés	Tűzriasztás, folyamat-vezérlés
B	Emberi életveszély	Nagy veszteség	Kritikus adat- és szolgáltatási kockázat	Helyrehozható környezeti szennyezés	Egészségügy, pénzügy
A	Tömeg-katasztrófa	Pénzügyi katasztrófa	Stratégiai adat- és szolgáltatási kockázat	Helyrehozhatatlan környezeti szennyezés	Vasút, atomtechnika

A szabvány 5. része (ISO/IEC 14598-5: Informatika – A szoftvertermék értékelése – 5. rész: Folyamat az értékelők számára) mindazon esetekben alkalmazható (és alkalmazandó is), ha az értékelés eredményének megértése, elfogadása több fél számára is fontos (pl. szállítók, megrendelők, felhasználók, értékelők, tanúsítók). A szabvány megköveteli, hogy az értékelési eljárás a következő tulajdonságokkal rendelkezzen:

- *Megismételhetőség (repeatability)*
  Ugyanazon szoftver vizsgálata ugyanazokra a kiértékelési követelményekre ugyanazon kiértékelő által mindig ugyanarra az eredményre vezessen.
- *Újraelőállíthatóság (reproducibility)*
  Ugyanazon szoftver vizsgálata ugyanazokra a kiértékelési követelményekre különböző kiértékelők által mindig ugyanarra az eredményre vezessen.
- *Objektivitás (objectivity)*
  Az értékelési eredmény legyen tényszerű, ne tartalmazzon egyéni érzéseket vagy véleményt.
- *Pártatlanság (elfogulatlanság, impartiality)*
  Minden részrehajlástól mentes legyen.

3.3 AZ ÉRTÉKELÉSI MUNKATERV FELÉPÍTÉSE ÉS TARTALMA

Az értékelési munkaterv célja az, hogy meghatározza és megindokolja az értékelés célkitűzéseinek kielégítése érdekében végrehajtandó munkacsomagokat.
Kötelező felépítése és minimálisan elvárt tartalma az alábbi:

3.3.1. 1. FEJEZET: BEVEZETÉS

A terv ismertetését tartalmazza, és az alábbi részekből kell állnia:

Azonosítás

Ennek a résznek (legalább) az alábbi információkat kell tartalmaznia:

- az értékelendő termék (rendszer) neve,
- a fejlesztő (fejlesztők) azonosítása,
- a megbízó azonosítása (amennyiben az nem az egyedüli fejlesztő),
- az értékelés tárgya biztonsági előirányzatára történő hivatkozás.

Hatókör

Egy arra vonatkozó nyilatkozat, hogy az adott munkaterv lefedi-e az értékeléssel kapcsolatos összes tervezett tevékenységet (és amennyiben nem fedi le, akkor a terv hogyan lesz aktualizálva), illetve kitér-e olyan előkészítő feladatokra is, melyek a fejlesztői bizonyítékok kiegészítését célozzák meg.

Szerkezet

A munkaterv szerkezetének leírása az olvasó számára.

3.3.2 2. FEJEZET: AZ ÉRTÉKELÉS TÁRGYÁNAK LEÍRÁSA

Ennek a fejezetnek az értékelendő terméket vagy rendszert (azaz az értékelés tárgyát) kellő részletességgel le kell írnia ahhoz, hogy a munkaterv többi része (önmagában, a biztonsági előirányzat áttanulmányozása nélkül is) érthető legyen.

Az értékelés tárgya áttekintése

Az értékelés tárgyának átfogó ismertetése, benne az értékelés tárgya által teljesítendő funkciókkal.

Az értékelés tárgya szerkezeti felépítése

Az értékelés tárgya magas szintű tervének összefoglalása, a tervvel kapcsolatos esetleges korlátozásokkal együtt.

Az értékelés tárgya dokumentáltsága

A megbízó, illetve a fejlesztő által készített főbb dokumentumok leírása, ezek egymáshoz viszonyított kapcsolatával együtt.

3.3.3 3. FEJEZET: ÉRTÉKELŐI MUNKACSOMAGOK

Az értékelés során végrehajtandó munka különböző értékelői munkacsomagokból áll, melyek mindegyike értékelői feladatelemek egy halmaza. Ebben a fejezetben minden munkacsomagra le kell írni legalább az alábbiakat:

- célkitűzés,
- hatókör,
- a munkacsomagban elvégzendő feladatelemek (rövid leírással együtt),
- a munkacsomag tervezett kezdő és záró dátuma,
- a munkacsomaggal kapcsolatos mérföldkövek.

A munkacsomag leírás rövid legyen, mivel az egyes munkacsomagok részletes specifikációját a munkaterv 1. számú mellékletének kell tartalmaznia.

3.3.4 4. FEJEZET: A MUNKATERV INDOKLÁSA

Ennek a fejezetnek a feladata annak bemutatása, hogy a javasolt munka megfelelő, nem túlzottan sok, de nem is kevés értékelői munkát terveznek. Mindez a munkák indoklásával érhető el. Az indoklásnak az alábbiakat kell tartalmaznia:

- arra vonatkozó magyarázat, hogy a munka milyen módon felel meg a sémának,
- annak magyarázata, hogy a munka milyen módon felel meg a séma értékelési módszertanának,
- egy magyarázat arra vonatkozóan, hogy a munka hogyan felel meg a célul kitűzött értékelési garanciaszintnek.

3.3.5 5. FEJEZET: KORLÁTOZÓ TÉNYEZŐK

Ennek a fejezetnek ki kell térnie az esetleges olyan tényezőkre, amelyek az értékelők megítélése szerint korlátozzák az értékelés munkáját, egyúttal ismertetnie kell a korlátozások következményeit az értékelés szempontjából. A korlátozó tényezők értékelésről értékelésre változnak, az alábbi korlátozó tényezők tipikusnak tekinthetők:

- értékelői erőforrások,
- fejlesztési ütemtervek,
- a működtetett értékelés tárgya elérhetőségének korlátozottsága (az időzítés és/vagy az időtartam szempontjából),
- az értékelés (rész)teljesítésének határidői,
- az értékelésben érintett egy vagy több szervezettel történő kapcsolattartás korlátozottsága (esetleges tiltottsága),
- speciális eszközök, illetve módszerek használatának szükségessége.

3.3.6 1. MELLÉKLET: AZ ÉRTÉKELŐI MUNKACSOMAGOK SPECIFIKÁCIÓJA

Ennek a mellékletnek a munkatervben leírt minden egyes munkacsomag részletes specifikációját kell tartalmaznia. A specifikációk célja az, hogy kellő részletességgel meghatározzák a végrehajtandó feladatokat az alábbiak érdekében:

- az értékelésben részt vevők megismerjék az elvárásokat,
- mind a megbízó, mind a tanúsító meggyőződhessen arról, hogy a javasolt munkacsomag szükséges, a többi munkacsomaggal együtt pedig elégséges is az értékelés követelményeinek kielégítéséhez.

Minden munkacsomag specifikációnak tartalmaznia kell legalább az alábbi részeket:

- célkitűzés: amely deklarálja a munkacsomag specifikációban meghatározott munka célkitűzéseit,
- szükséges bemenetek: amely meghatározza azokat az értékelésre átadandó fejlesztői bizonyítékokat, amelyekre szükség lesz a munkacsomag teljesítéséhez,
- módszerek és eszközök: mely deklarálja, hogy a munkacsomagot hogyan kell elvégezni, és azonosítja azokat a konkrét eszközöket és módszereket, amelyeket használni fognak a munkacsomag célkitűzések eléréséhez.

3.3.7 2. MELLÉKLET (1. ALTERNATÍVA): ÉRTÉKELÉSI ÜTEMTERV

Ennek a mellékletnek az egyes munkacsomagok ütemterveire és erőforrásaira vonatkozó részleteket kell tartalmaznia.

Az értékelő ezeket az információkat érzékenynek és magántulajdonúnak tekintheti. Ebben az esetben ezt a részt egy külön dokumentumba (Értékelési ütemterv) foglalhatja, lehetővé téve a két dokumentum elválasztását, és ez utóbbi szűkebb körben történő terjesztését.

Az értékelési ütemtervnek (mindkét változat esetén) az egyes munkacsomagokra vonatkozóan legalább az alábbiakat kell tartalmaznia:

- az adott munkacsomag végrehajtásához szükséges erőfeszítés teljes mennyisége,
- a munkacsomag elvégzéséhez szükséges értékelők száma,
- a tervezett kezdeti és záró dátumok.

Tipikus megvalósítása egy szöveges kiegészítésekkel bővített Gannt diagram lehet.

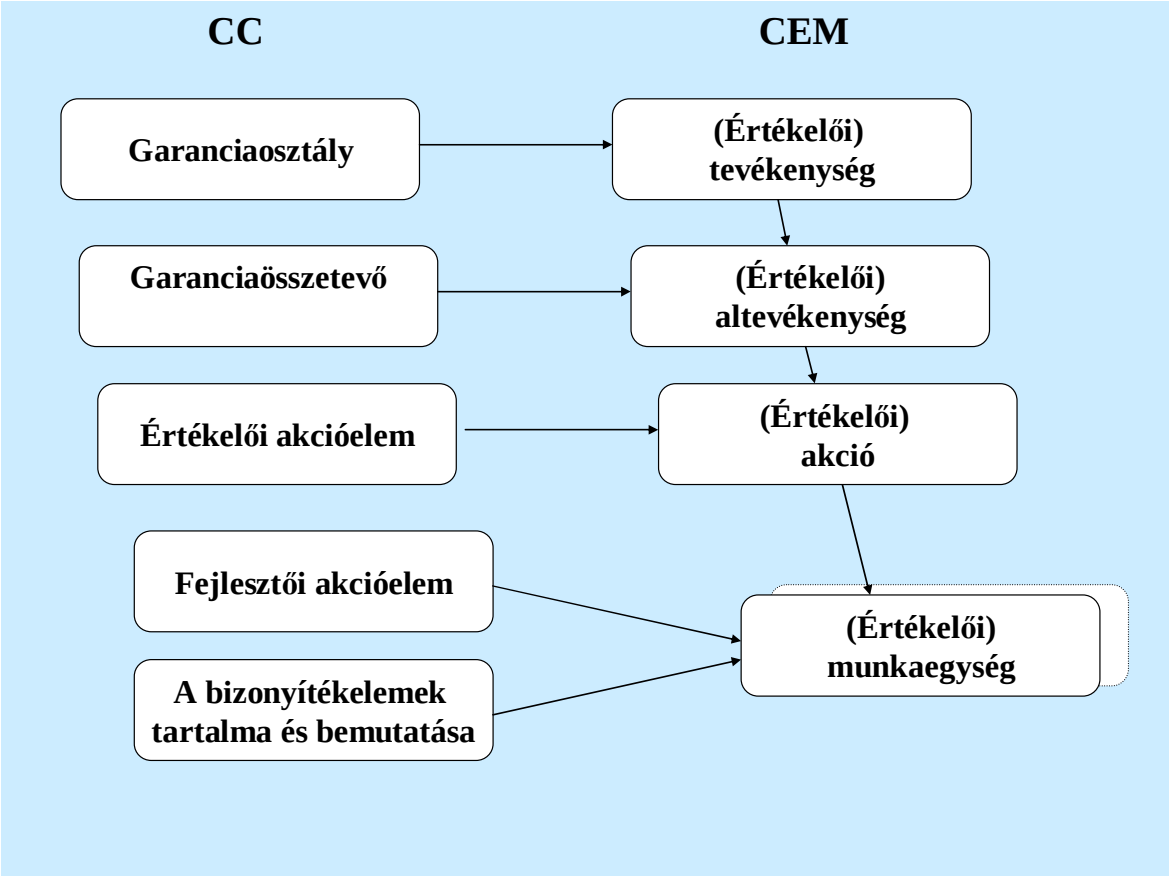
3.3.8 2. MELLÉKLET (2. ALTERNATÍVA): AZ ÉRTÉKELÉSRE ÁTADANDÓ FEJLESZTŐI BIZONYÍTÉKOK, ÉS EZEK ÁTADÁSÁNAK ÜTEMEZÉSE

Amennyiben az értékelő az értékelési ütemtervet egy önálló dokumentumba foglalja, a 2. mellékletben ugyanennek az ütemtervnek egy részleges változatát kell megadni, ami az ütemezéshez a fejlesztői bizonyítékok oldaláról elvárt részeket tartalmazza.

Ennek a mellékletnek tételesen fel kell sorolnia az értékeléshez szükséges valamennyi fejlesztői bizonyítékot, s ezeknek az értékelésre való átadásának határidejét.

3.4 A CC ÉS A CEM/MIBÉTS STRUKTÚRÁK KÖZÖTTI KAPCSOLAT

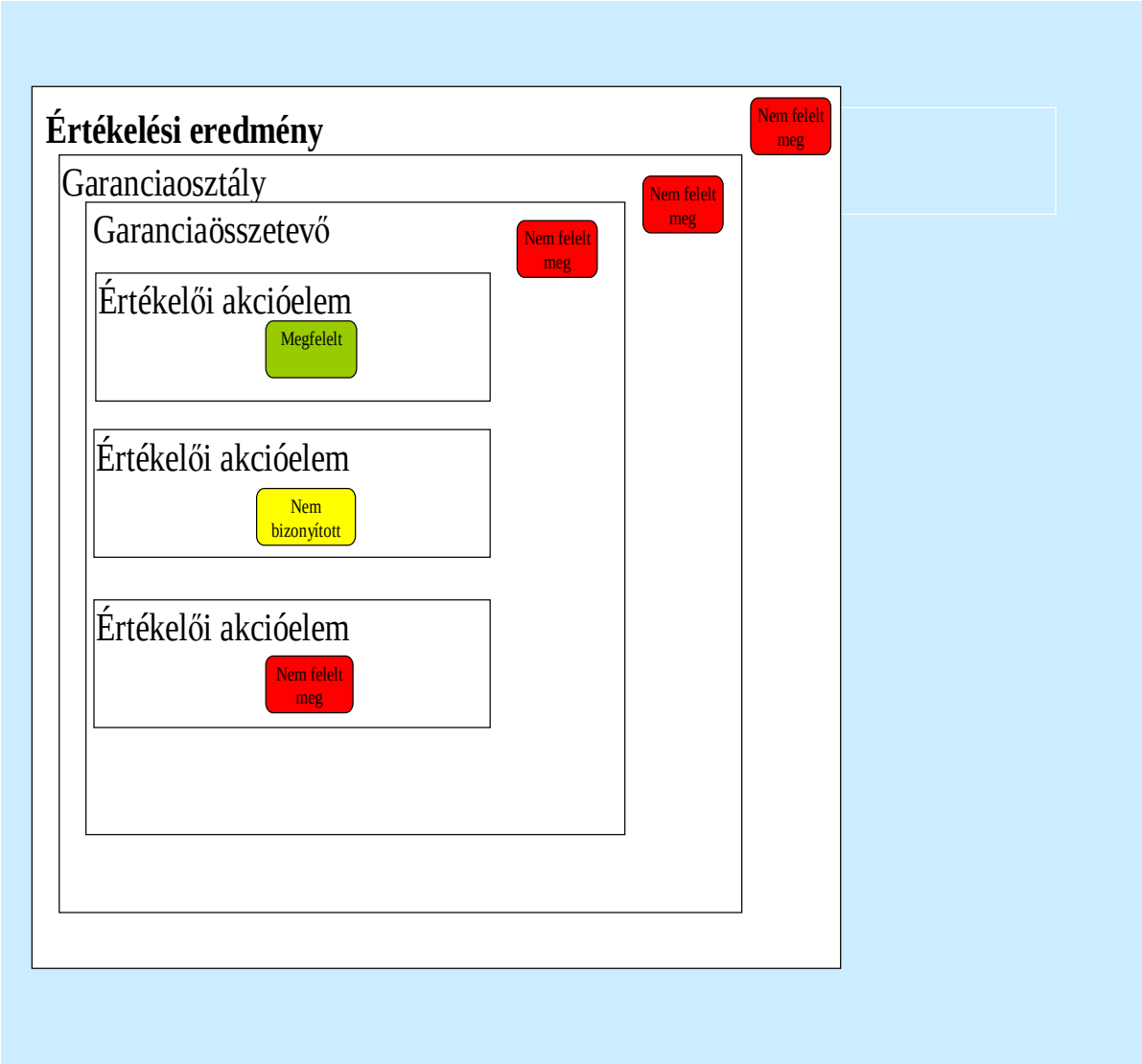
Közvetlen összefüggés áll fenn a CC struktúra (vagyis osztály, család, összetevő és elem) és a CEM (egyben MIBÉTS módszertan) struktúrája között. Az alábbi ábra bemutatja a megfelelést a CC-t alkotó osztály, család és értékelői akcióelemek és a CEM/MIBÉTS tevékenységek, altevékenységek és akciók között.



A CC és a CEM/MIBÉTS struktúráinak megfeleltetése

3.5 ÉRTÉKELŐI HATÁROZATOK

Az értékelő a CC követelményeire hozza meg a határozatokat. A legelemibb CC struktúra, melyhez határozat rendelhető az értékelői akcióelem (közvetlen vagy közvetett). Egy CC értékelői akcióelemhez rendelt határozat a kapcsolódó CEM akció és az azt alkotó munkaegységek végrehajtásának eredményeként születik. Végül előáll egy értékelési eredmény, ahogy ezt az alábbi ábra példája mutatja.



Példa a határozat hozatal szabályára

A MIBÉTS (a CEM alapján) három, egymást kölcsönösen kizáró határozatot ismer el:

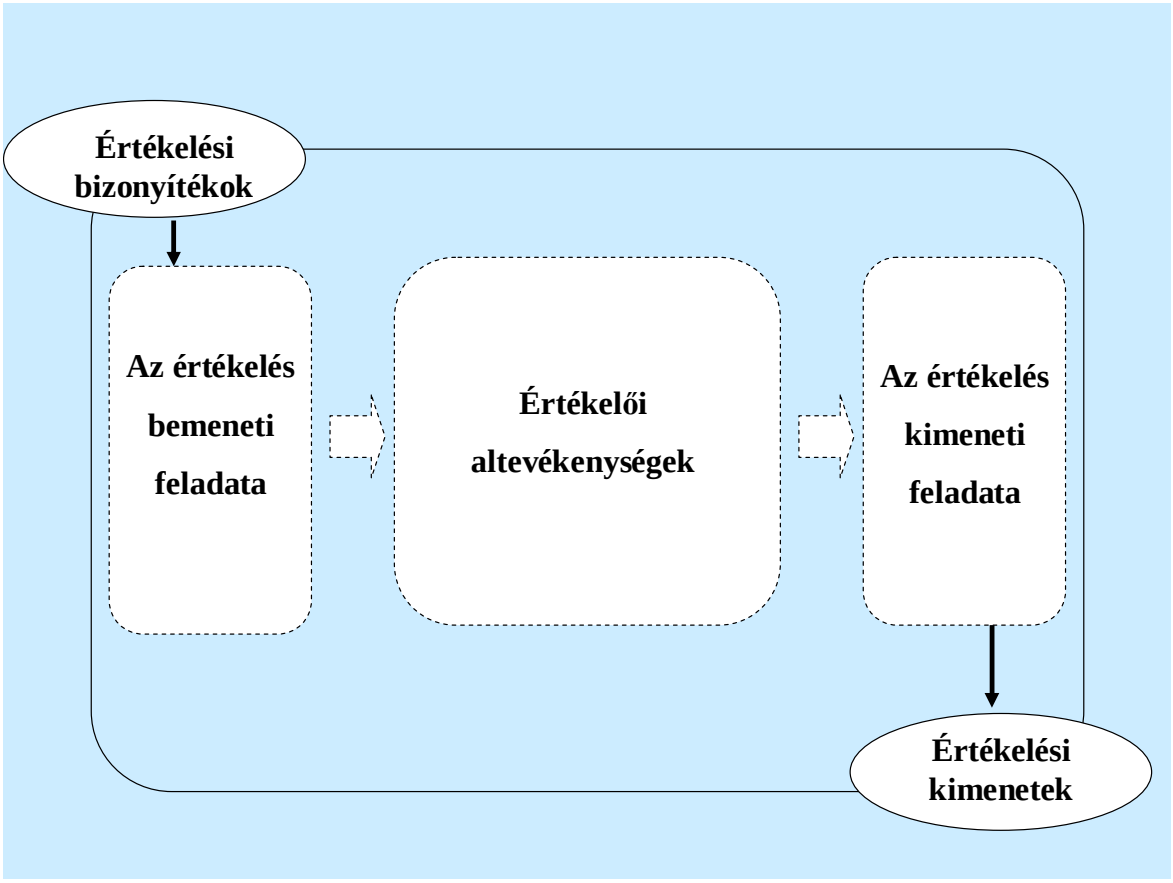
- Egy "Megfelelt" határozat feltétele, hogy az értékelő befejezze a CC értékelői akcióelemet, s megállapítsa, hogy az értékelés alatt álló ST-re vagy TOE-ra vonatkozó követelmények teljesülnek. Az értékelői akcióelem megfelelésének feltételeit az érintett CEM akcióhoz tartozó munkaegységek határozzák meg.
- Egy "Nem bizonyított" határozat feltétele, hogy az értékelő a CC értékelői akcióelemhez tartozó CEM akció egy vagy több munkaegységét ne fejezze be.
- Egy "Nem felelt meg" határozat feltétele, hogy az értékelő befejezze a CC értékelői akcióelemet, s megállapítsa, hogy az értékelés alatt álló ST-re vagy TOE-re vonatkozó követelmények nem teljesülnek.

Minden határozat kezdetben "Nem bizonyított", és az is marad mindaddig, míg nem kap "Megfelelt" vagy "Nem felelt meg" minősítést.

Az általános határozat akkor és csak akkor „Megfelelt”, ha a részét képező valamennyi határozat is „Megfelelt”. Az előző oldal ábráján szemléltetett példában egyetlen értékelői akcióelemre hozott „Nem felelt meg” határozat az érintett garanciaösszetevő és garanciaosztály, valamint az általános határozat „Nem felelt meg” eredményét okozza.

3.6 ÁLTALÁNOS ÉRTÉKELŐI FELADATOK

Minden értékelés a következő részfeladatokból áll: bemeneti feladat, értékelői altevékenységek, kimeneti feladat. Az értékelői altevékenységek részletes meghatározását egy külön MIBÉTS segédlet ([7]) tartalmazza Ez a melléklet a bemeneti és a kimeneti feladatot ismerteti.



Általános értékelési modell

3.6.1 AZ ÉRTÉKELÉS BEMENETI FELADATA

Ennek a feladatnak a célja annak biztosítása, hogy az értékelő számára hozzáférhető legyen az összes szükséges értékelési bizonyíték, egyben azokat megfelelően védjék is meg, hiszen máskülönben nem garantálható sem az értékelés műszaki pontossága, sem az értékelés megismételhetősége és újraelőállíthatósága.

Az értékelőnek (a megbízóval egyeztetve) el kell készítenie az igényelt értékelési bizonyíték (fejlesztői bizonyítékok) listáját. Ez a lista a dokumentációkra való hivatkozásokból állhat. Ez a lista elegendő információt tartalmazzon ahhoz, hogy segítse az értékelőt az elvárt bizonyíték könnyű megtalálásában (pl. minden dokumentum rövid összefoglalásával, vagy legalább a cím tételes megadásával és az érdeklődésre számot tartó részek feltüntetésével).

Az értékelési bizonyítékban foglalt információ a követelmény, nem pedig valamilyen sajátos dokumentum struktúra. Egy altevékenységre vonatkozó értékelési bizonyíték megadható különálló dokumentumok formájában, de egyetlen dokumentum kielégítheti egy altevékenységnek több bemeneti követelményét is.

Az értékelő megbízható és hivatalosan kibocsátott értékelési bizonyítékot igényel. Ugyanakkor egy értékeléshez tervezet is adható, például annak elősegítése érdekében, hogy az értékelő korai, informális megállapításokra juthasson, de ez nem használható a határozathozatal alapjául. Az értékelőt az egyes értékelési bizonyítékok tervezet verziói az alábbi esetekben segíthetik:

- teszt dokumentáció, mely biztosítja, hogy az értékelő a tesztekről és teszt eljárásokról egy előzetes értékelést készítsen,
- a TOE tervezés megértését segítő terv dokumentációk,
- forráskód vagy hardver vázlatok, melyek azt segítik elő, hogy az értékelő felmérje a fejlesztői szabványok alkalmazását.

A bizonyítékok tervezetével általában akkor találkozunk, ha a TOE értékelése a fejlesztéssel párhuzamosan történik. Akkor is találkozhatunk ezzel, mikor egy már kifejlesztett TOE értékelése során a fejlesztő - az értékelő által felvetett probléma megoldására - további módosítást hajt végre (pl. egy tervezési vagy kivitelezési hiba javítására), vagy pedig amikor a biztonságot érintő olyan bizonyítékra van szükség, melyet a dokumentáció nem tartalmaz.

Az értékelési bizonyítékok kezelése

Az értékelőnek képesnek kell lennie az értékelési bizonyítékok kézhez vétele után azok minden tételének az azonosítására és elhelyezésére. Az értékelőnek képesnek kell lennie annak meghatározására is, hogy egy adott dokumentum verzió a birtokában van-e.
Az értékelőnek meg kell védenie az értékelési bizonyítékot a módosítástól vagy elvesztéstől mindazon idő alatt, míg a birtokában van.
Az értékelési folyamat végén az értékelési bizonyítékok eltávolítására az alábbi lehetőségek vannak, melyből egy vagy több is alkalmazható:

- az értékelési bizonyíték visszaszolgáltatása (a megbízónak vagy a fejlesztőnek),
- az értékelési bizonyíték archiválása,
- az értékelési bizonyíték megsemmisítése.

Az értékelőnek munkája során valószínűleg a megbízó és a fejlesztő érzékeny információihoz (pl. TOE tervezési információ, szakértői eszközök) is hozzá kell férniük. Az értékelőnek meg kell védenie az értékelési bizonyíték bizalmasságát.
A bizalmasság követelménye az értékelő munka sok szempontját érinti, beleértve az értékelési bizonyíték kézhez vételét, kezelését, tárolását és eltávolítását is.

3.6.2 AZ ÉRTÉKELÉS KIMENETI FELADATA

Az értékelési eredmények megismételhetősége és újraelőállíthatósága általános elve teljesítése érdekében az értékelési eredményeket konzisztens módon kell rögzíteni. A konzisztencia magában foglalja az észrevételezési jelentésekben és az értékelési jelentésben rögzített információk típusát és mennyiségét is. A különböző értékelések közötti konzisztencia a tanúsító szervezetet képviselő átvizsgáló felelőssége.

Észrevételezési jelentés írás

Az észrevételezési jelentések azt a mechanizmust biztosítják az értékelő számára, amivel egy értékelést érintő problémát tisztázni (pl. egy követelmény alkalmazására vonatkozóan az átvizsgálóval), illetve azonosítani lehet.
Egy "Nem felelt meg" határozat esetén az értékelőnek észrevételezési jelentést kell biztosítania az értékelési eredmény alátámasztására. Ezen kívül az értékelő az észrevételezési jelentést egy probléma tisztázására vonatkozó igény kifejezésére is felhasználhatja.

Az értékelőnek minden észrevételezési jelentésben legalább az alábbiakat rögzítenie kell:

- az értékelt TOE azonosítója,
- az értékelési feladat/részfeladat, mely során az észrevétel felbukkant,
- az észrevétel,
- az észrevétel súlyosságának megbecslése (a MIBÉTS keretében 1., 2., 3. és 4. súlyosságú észrevétel tehető, ahogyan azt [5] 3.3 alfejezete meghatározza),
- a probléma megoldásáért felelős szervezet azonosítása,
- ajánlás a probléma megoldására szolgáló időtartamra,
- az értékelést érintő hatások megbecslése az észrevétel által felvetett probléma megoldásának kudarca esetén.

[5] 3.3 alfejezete példákat mutat be a különböző súlyosságú észrevételezési jelentésekre.

Értékelési jelentés írás

Az értékelőnek értékelési jelentést kell készítenie általános értékelői határozata szakmai indoklásának bemutatására.

Az értékelési jelentés olyan információt is tartalmazhat, mely a fejlesztő, megbízó vagy az értékelő üzleti titkát képezi. Ezért az értékelési jelentés nem nyilvános dokumentum, általában csak a megbízó és a tanúsító számára készül. [4] 7.2 alfejezete meghatározza a felépítésére és tartalmára vonatkozó séma elvárásokat.

HIVATKOZÁSOK ÉS RÖVIDÍTÉSEK

HIVATKOZÁSOK

[1] MSZ ISO/IEC 15408-1:2003 Informatika – Biztonságtechnika – Az informatikai biztonságértékelés közös szempontjai – 1. rész: Bevezetés és általános modell, 2. rész: A biztonság funkcionális követelményei, 3. rész: A biztonság garanciális követelményei

[2] ISO/IEC 15408-1:2005 Information technology - Security techniques — Evaluation criteria for IT security – Part 1: Introduction and general model, Part 2: Security functional requirements, Part 3: Security functional requirements

[3] ISO/IEC 18045:2005 Information technology – Security techniques – Methodology for IT security evaluation

[4] Magyar Informatikai Biztonsági Ajánlás - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma - 1. számú segédlet: Modell és folyamatok

[5] Magyar Informatikai Biztonsági Ajánlás - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma - 2. számú segédlet: Útmutató a megbízók számára

[6] Magyar Informatikai Biztonsági Ajánlás - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma - 3. számú segédlet: Útmutató a fejlesztők számára

[7] Magyar Informatikai Biztonsági Ajánlás - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma - 5. számú segédlet: MIBÉTS értékelési módszertan

RÖVIDÍTÉSEK JEGYZÉKE

CC	Common Criteria (Közös szempontok)
CEM	Common Evaluation Methodology (Közös értékelési módszertan)
MIBÉTS	Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (séma)
PP	Protection Profile (védelmi profil)
SF	Security Function (biztonsági funkció)
ST	Security Target (biztonsági előirányzat)
SOF	Strength of Function (funkcióerősség)
TOE	Target of Evaluation (az értékelés tárgya)
TSF	TOE Security Functions (a TOE biztonsági funkciói)
TSP	TOE Security Policy (a TOE biztonsági szabályzata)