AZ INFORMATIKAI BIZTONSÁG TANÚSÍTÁSI ÉS MINŐSÍTÉSI ELJÁRÁSRENDJÉNEK TERVE

Készítette:

Bodlaki Ákos,

Muha Lajos.

1996. november

© FIXX Informatikai, Kereskedelmi és Szolgáltató Kft.

TARTALOMJEGYZÉK

ÁBRÁK és TÁBLÁZATOK JEGYZÉKE

1. BEVEZETÉS

A minisztériumok informatikai rendszereinek 1995-ben elvégzett biztonsági vizsgálata az első lépés volt abban a folyamatban, amelynek végső célja az, hogy megteremtődjék a folyamatos összhang a közigazgatási intézményekben az informatikai rendszerek által kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának megőrzése és a funkcionalitásban betöltött szerepük által támasztott követelmények, valamint a megvalósított/megvalósítandó védelmi rendszerek között. E folyamat szükségszerű lépései az informatikai biztonsági követelményrendszer kidolgozása, a reális veszélyek és a biztonság tudatosítása az informatikai rendszereket használók és üzemeltetők körében, a követelmények érvényesítési rendszerének szabályozási, szervezeti és eljárásrendi kialakítása. Csak így lesz biztosítható, hogy a közigazgatási intézményeknél az informatikai biztonság nem esetenként (és eseményenként!) felmerülő kérdés, hanem egy olyan jól szervezett tevékenység lesz, amelyben szabályozási és eljárásrendi garanciák vannak a kezelt adatok érzékenységével, a potenciális fenyegetések által okozott kockázatokkal arányos, zárt és teljes körű védelem *folyamatos* és *minősített* biztosításának.

A közelmúltban jelentős lépések történtek a fent említett folyamatban. A Miniszterelnöki Hivatal Informatikai Koordinációs Irodája (továbbiakban: MeH IKI) kezelésében az Informatikai Tárcaközi Bizottság (továbbiakban: ITB) 12. sz. ajánlásaként rövidesen megjelenik az “Informatikai rendszerek biztonsági követelményei” című dokumentum. További lépésként kormányrendelet tervezet készült el a számítástechnikai és távközlési rendszerek információvédelmi felügyeletének és megfelelősség-vizsgálatának rendjéről, amely jelenleg egyeztetés alatt áll. A tervezet az informatikai biztonsági felügyeletet érintő szervezeti, a minősített adatokat kezelő informatikai rendszerek létesítése, működése és megszüntetése engedélyezésével, valamint a tanúsítók kiválasztásával, a termékek és rendszerek minősítésével kapcsolatos intézkedéseket tartalmaz.

Az informatikai rendszereknek az információvédelmet és a megbízható működést támogató biztonsági rendszerei tervezésében komoly segítséget fog nyújtani az a jelenleg készülő Informatikai Biztonsági Tervezési Kézikönyv, amely minden fenyegetett rendszerelem-csoportra tartalmazza azokat az intézkedéseket, amelyek részletes vizsgálat nélkül is teljes körűen biztosítanak egy minimális védelmet.

Ezek a dokumentumok és rendeletek önmagukban azonban még nem elegendők az informatikai biztonság folyamatos és minősített biztosításához. Az iparilag fejlett országok gyakorlatához hasonlóan a hazai közigazgatás területén is ki kell alakítani az informatikai rendszerek biztonsági szempontból történő rendszeres tanúsításának és minősítésének szervezeti, szabályozási és eljárási rendjét. Ez lehet a biztosítéka annak, hogy az egyszer megvalósított, a kezelt adatok érzékenységével arányos védelmi szint, a jogi és a belső szabályozásnak való megfelelés folyamatosan biztosított legyen. Ez nem valósulhat meg az informatikai rendszerekbe beépülő termékek, komponensek adott követelmények alapján történő biztonsági minősítése nélkül. Tekintve, hogy mind a rendszerek, mind a termékek minősítése magas szakmai kvalifikációt és garantált függetlenséget feltételez, a tanúsító cégek kiválasztási és minősítési szempontrendszere, valamint eljárásrendje kulcskérdés az egész informatikai biztonsági minősítési rendszerben.

Jelen dokumentum egy tervet, javaslatot tartalmaz az informatikai rendszerek, termékek minősítési, valamint a minősítő cégek kiválasztási rendszerére.

1.1. A tanulmány célja, tartalma

Az iparilag fejlett országokban az informatika szerves részét képezi a szervezet működése támogatásának, alapvető szerepet játszik a szervezet hatékony és versenyképes működésében. Ez azonban nem csak az informatikai alkalmazások funkcionalitási szintjétől, hanem az információvédelem és a megbízható működés területén megvalósított tulajdonságoktól is nagymértékben függ. Éles versenyhelyzetben működő cégeknél sok esetben létkérdés a versenyben-maradás, a túlélés szempontjából a szervezet számára érzékeny adatok bizalmasságának, hitelességének, sértetlenségének megőrzése, valamint a szervezet tevékenységéből adódó követelményeknek megfelelő megbízható működés biztosítása.

Az ezekhez kapcsolódó intézkedések, a védelmi rendszerek fejlesztése, megvalósítása és üzemeltetése szempontjából két fontos szempontot *garantáltan érvényesíteni* kell:

- *A védelmi képességeknek már az informatikai rendszer üzemének indításakor meg kell felelni az adott szervezetnél meghatározott információvédelmi (IV) és megbízható működési (MM) osztályoknak megfelelő funkcionális jellegű védelmi köve-*

telményeknek. E követelményeket az ITB 12. sz. ajánlása foglalja össze a fizikai, a logikai és az adminisztratív védelem területén. A követelmények kialakításánál mind a hazai jogszabályok , mind a nemzetközi ajánlások (pl. ITSEC) figyelembe lettek véve.

Ez azt jelenti, hogy :

- A szervezetnél kialakított szervezeti, infrastrukturális és egyéb feltételek között üzemeltetett és működő informatikai rendszer a környezetével együtt megfelel-e a kezelt adatkörök biztonsági osztályai követelményeinek.
- Az informatikai rendszerbe beépítendő termékeket minősíteni kell abból a szempontból, hogy megfelelnek-e a kezelt adatkörök biztonsági osztályai követelményeinek. Adott minősítési osztályú rendszerbe csak azonos osztályú termék kerülhet beépítésre.

♦ Az informatikai rendszer üzemeltetésének indításakor megvalósított védelmi szintet *garantáltan fenn kell tartani a rendszer teljes életciklusa folyamán*.

Ez azt jelenti, hogy:

- Rendszeres biztonsági vizsgálatokkal ellenőrizni kell, hogy az informatikai rendszer legutolsó biztonsági minősítésének megfelelő-e a fizikai, a logikai és az adminisztratív védelem felépítése, üzemeltetése, a biztonsággal kapcsolatos összes tevékenység.
- Ha a legutolsó minősítés óta változás történt a biztonsági követelményekben (pl. az eddiginél magasabb biztonsági osztályba sorolt adatkör kezelését kellett az informatikai rendszerben megoldani), akkor eseti vizsgálattal kell ellenőrizni, hogy megtörténtek-e a szükséges módosítások, kiegészítések a védelmi rendszerben. Ez egyben az alapját képezi annak, a döntésnek, hogy szükséges-e a legutóbbi minősítést módosítani.
- A piacra kerülő informatikai termékeket rendszeresen minősíteni kell informatikai biztonsági szempontból, hogy garantáltan az adott informatikai rendszerre vagy alrendszerre vonatkozó biztonsági követelményeket kielégítő termékek kerüljenek beépítésre. A minősítésekkel követni kell a termékek továbbfejlesztett változatait is. Ez az egyik lényeges garanciája annak, hogy

az informatikai rendszer és környezetének védelmi képességei a teljes életciklus folyamán semmilyen ponton ne csökkenjenek az elviselhető kockázati szint alá.

A minősítési rendszer kialakításának kulcsfontosságú eleme a *tanúsítást végző szervezetek kiválasztási és minősítési követelményrendszere, eljárásrendje*. A rendszerek és termékek minősítésének megbízhatóságát és szakmai tekintélyét, elfogadottságát minden érintett partner által csak az biztosítja, ha olyan szervezetek, cégek kapják csak meg a biztonsági vizsgálatokra feljogosító tanúsítást, amelyek szakmai színvonala és tapasztalata átlag feletti, valamint az informatikai termékeket forgalmazó cégektől és a vizsgált szervezetektől való függetlenségük minden kétséget kizár.

Az informatikai rendszerek és termékek biztonságminősítési rendszerének kialakítási folyamatában a számítástechnikai és távközlési rendszerek információvédelmi felügyeletének és megfelelőség-vizsgálatának rendjéről szóló kormányrendelet tervezet elkészítése volt az első lépés. A jelenleg tárcaközi egyeztetés alatt álló dokumentum javaslatot tesz egy hatósági jogkörrel felruházott szervezet, az Informatikai Biztonsági Főfelügyelet kialakítására, amely meghatározó feladatokat látna el az informatikai rendszerek és termékek biztonsági minősítésében, valamint a független vizsgálatokat végző tanúsító cégek és személyek minősítésében.

A kormányrendelet-tervezet a dokumentum jellegéből adódóan nem foglalkozhat a rendszerek, termékek és cégek minősítési folyamatának és eljárásrendjének olyan részletes leírásával, amely alapján a gyakorlatban a minősítési követelményrendszerek, a minősítés gyakorlati szintű tartalmi és formai lépései, eljárásrendje kialakíthatók lennének.

E dokumentumban megfogalmazott terv célja az, hogy jóváhagyása után alapját képezze:

- a közigazgatás területén működő informatikai rendszerek biztonságminősítési követelményrendszerének, a minősítési folyamat eljárásrendjének és gyakorlati mechanizmusa kialakításának,
- az informatikai termékek biztonságminősítési követelményrendszerének, a minősítési folyamat eljárásrendjének és gyakorlati mechanizmusa kialakításának, beleértve az Európai Közösség által egyszer már megtörtént minősítésekkel és a módosított, továbbfejlesztett termékek újraminősítésével kapcsolatos eljárásokat is,

- a tanúsító szervezetek, cégek kiválasztási követelményrendszerének, a minősítési folyamat eljárásrendjének és gyakorlati mechanizmusa kialakításának.

Jelen dokumentum úgy épül fel, hogy a fentiekben vázolt tartalmi célkitűzések konzekvensen és ellentmondásmentesen kibonthatók legyenek egy általános minősítési rendszer-sémából és alapfogalmi rendszerből kiindulva. A minősítési követelmények, folyamatok és eljárások ismertetése előtt a 3. fejezetben összefoglaljuk azokat a dokumentumokat, amelyek figyelembe vétele alapvetően meghatározta a minősítési követelmények és az eljárások kialakításánál követett szemléletet. A 4. fejezet ismerteti a teljes minősítési rendszer logikai felépítését, tisztázza azokat az alapfogalmakat, amelyek meghatározó jellegűek a teljes minősítési rendszerben. Az 5. fejezet a minősítés tárgyának értékelésére vonatkozó követelményrendszert ismerteti. Az 6. fejezet a piacon beszerezhető informatikai termékek biztonságminősítési folyamatát és eljárásrendjét ismerteti. Külön alfejezetek foglalkoznak a tovább fejlesztett, vagy módosított termékek újraminősítési eljárásával, illetve az EK-ban és más országokban már minősített termékek biztonsági szempontból történő honosítási eljárásával. A 6. fejezet a közigazgatási intézményeknél üzemelő informatikai rendszerekre vonatkozó biztonságminősítési folyamatot és eljárásrendet ismerteti. A 7. fejezet a tanúsítást végző cégek kiválasztási követelményrendszerét és a cégminősítés folyamatát és eljárásrendjét ismerteti.

Jelen dokumentum tervezetként készült a MeH IKI részére azzal a céllal, hogy a szükséges belső egyeztetések után döntéselőkészítő anyagként szolgáljon a minősítési rendszert érintő döntésekben kompetens államigazgatási intézmények részére.

1.2. A figyelembevett ajánlások, jogszabályok

Jelen dokumentum kialakításánál figyelembe veendő ajánlások és jogszabályok kiválasztásánál a következő szempontok domináltak:

- A minősítési rendszerben követett eljárásrendnek illeszkednie kell az ide vonatkozó és hatályos jogszabályokhoz, valamint tervezetekhez.

A figyelembe vett jogszabályok és tervezetek a következők:

- 1995. évi LXV. törvény az államtitokról és szolgálati titokról, a végrehajtására kiadott 79/1995.(VI.30.) Korm. rendelettel együtt,
- 1992. évi LXIII. törvény a személyi adatok védelméről és a közérdekű adatok nyilvánosságáról,
- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról,
- 1995. évi XXIX. törvény a laboratóriumok, a tanúsító és az ellenőrző szervezetek akkreditálásáról, amely hivatkozik az akkreditálási eljárásban alkalmazott MSz EN 45001 - 450013 szabványokra.
- 1995. évi XXVIII. törvény a nemzeti szabványosításról,
- Kormányrendelet-tervezet a számítástechnikai és távközlési rendszerek információvédelmi felügyeletének és megfelelőség-vizsgálatának rendjéről.
- Kormányrendelet-tervezet a minősített adat kezelésének rendjéről szóló 79/1995. (VI.30.) Korm. Rendelet módosításáról.

♦ A közigazgatás területén a MeH IKI által kiadott korábbi, az informatikai biztonságra vonatkozó ajánlásokkal és tervezetekkel jelen dokumentumnak teljesen összhangban kell lennie, a minősítési rendszer kialakításánál az ezekben lefektetett alapelvekre és szempontokra támaszkodtunk.

A MeH IKI többi ajánlása mellett elsősorban a következő ajánlást, illetve tervezetet vettük figyelembe:

- informatikai biztonsági módszertani kézikönyv (8.sz. ajánlás),
- informatikai rendszerek biztonsági követelményei (12. sz. ajánlás tervezet).

♦ Magyarország az EK tagja kíván lenni belátható időn belül. Ha azt kívánjuk, hogy a közigazgatásban felhasznált hazai informatikai termékek minősítése informatikai biztonsági szempontból kompatibilis legyen az EK minősítési követelményeivel, illetve az EK által minősített termékek - a kibocsátott minősítési dokumentumok alapján - már egy egyszerűsített ellenőrző eljárás után is alkalmazhatók legyenek a hazai informatikai rendszerekben, a hazai minősítési rendszernek harmonizálnia kell az EK idevonatkozó ajánlásaival. Az EK ajánlásaival az üzemeltett informatikai rendszerek biztonsági minősítésének is harmonizálnia kell. Ez különösen a hazai és az EK országok intézményei között létrejövő hálózati, illetve

egyéb módon létesülő adatcsere kapcsolatoknak az egyenszilárdságú és azonos követelmények szerint kialakított védelme miatt fontos.

A fenti megfontolások alapján a következő két EK dokumentumot, mint a jelen anyag egészének szemléletét meghatározó forrásokat vettük figyelembe:

- ITSEC[1] : Information Technology Security Evaluation Criteria. Version 1.2.EC DG XIII. 1991. május.
- ITSEM[2]: Information Technology Security Evaluation Manual. Draft V0.2. 1992. április.

A további külföldi dokumentumok közül a következőket vettük figyelembe:

- Trusted Computer System Evaluation Criteria (TCSEC[3]) — Amerikai Egyesült Államok Védelmi Minisztériuma (Orange Book of the Security of Information Systems)
- Trusted Product Evaluations. A Guide for Vendors. National Computer Security Center. USA. NCSC-TG-002. Version-1. 1990. június.
- Trusted Network Interpretation Enviroments Guideline. - National Computer Security Center, USA, 1990 augusztus.
- IT-Grundschutzhandbuch. Schiftenreihe zur IT-Sicherheit. Band 3. - Bundesamt für Sicherheit in der Informationstechnik, 1995.
- UK IT Security Evaluation and Certification Scheme. UK Certified Product List. UKSP 06. 2. kiadás. 1993. április.

---

[1] Information Technology Security Evaluation Criteria (ITSEC) = Információtechnológia Biztonsági Értékelési Kritériumok

[2] Information Technology Security Evaluation Manual (ITSEM) = Információtechnológia Biztonsági Értékelési Kézikönyv

[3] Trusted Computer System Evaluation Criteria (TCSEC) = Biztonságos Számítógépes Rendszerek Értékelési Kritériumai

2. A TANÚSÍTÁSI ÉS MINŐSÍTÉSI FOLYAMAT

A világ iparilag fejlett országaiban az 1980-as évek közepe óta kezdtek intenzíven foglalkozni az informatikai rendszerek és termékek biztonságminősítési rendszerének kialakításával és bevezetésével. A nemzetközi gyakorlatban a minősítés két fő területet fed le. Az üzemelő informatikai rendszerekét, illetve a beépítésre kerülő termékekét.

A rendszerek esetében egy erre felhatalmazott szervezet által elvégzett minősítés hitelesíti annak mértékét, hogy a védelmi rendszer - itt első sorban a logikai védelmi rendszer - tervezése, megvalósítása és üzemeltetése megfelel-e a rendszer által kezelt adatokra vonatkozó - jogszabályokban, szabványokban és ajánlásokban rögzített - biztonsági követelményeknek.

Az informatikai termékek minősítése pedig azért szükséges, hogy egy adott védelmi szintet biztosító informatikai rendszer fejlesztésekor és megvalósításakor kiválaszthatók legyenek azok a termékek, amelyek védelmi képességei kielégítik a rendszerre nézve megszabott biztonsági követelményeket.

Magyarországon semmilyen területen - így a közigazgatás területén sem - alakult ki az informatikai rendszerek, illetve termékek biztonságminősítési rendszere. Ez alól kivételt képez a rejtjelző eszközöknek az Országos Rejtjelfelügyelet által végzett minősítése. E fejezet azt a sémát tartalmazza, amely globális képet ad a minősítés folyamatáról, az abban résztvevőkről, a folyamathoz igényelt input, illetve a folyamat egyes fázisaiban keletkező output dokumentumokról. Ezen túlmenően értelmezi azokat a fontos alapfogalmakat, amelyek meghatározóak a teljes minősítési folyamatban.

A séma kialakításánál két alapvető szempont játszott szerepet:

- a kialakítandó minősítési követelményrendszer, folyamat és eljárásrend feleljen meg a korábban megfogalmazott minősítési céloknak, azaz alkalmas legyen arra, hogy:

- a beépítésre kerülő termékek és a bevezetés kerülő informatikai rendszerekre meghatározható legyen a biztonsági követelményeknek való megfelelés mértéke,
- az informatikai rendszerek, illetve a termékek teljes életciklusa folyamán folyamatosan követhető legyen a megfelelés mértéke,

♦ a minősítési folyamat és az eljárásrend kompatibilis legyen az EK minősítési rendszerével azért, hogy a külföldön minősített termékek hazai minősítése lényegesen leegyszerűsíthető legyen és fordítva, hogy a Magyarországon fejlesztett és minősített termékek külföldön - elsősorban az EK-ban - minél egyszerűbb eljárással kerülhessenek be az adott ország minősített termék listájába.

A fentiekből következik, hogy a jelen dokumentumban ismertetendő követelményrendszer, minősítési folyamat az EK ITSEC ajánlásában foglaltaknak felel meg. A minősítési folyamatok és az eljárásrend kialakításánál ezen túlmenően figyelembe vettük az USA Nemzeti Számítógépes Biztonsági Központja (NCSC: National Computer Security Center) által készített és kiadott Trusted Product Evaluations (Megbízható termékek értékelése) c. dokumentumot és a német IT Biztonság Szövetségi Hivatala által készített és kiadott IT-Grundschutzhandbuch. Schiftenreihe zur IT-Sicherheit (Kiadványsorozat az IT biztonsághoz. IT Alapvédelmi Kézikönyv.) 3. kötetét.

Az 1. ábra mutatja be a minősítési folyamat legfontosabb fázisait, szereplőit és a legfontosabb részfolyamatokat.

Az ábrán látható minősítési folyamat formailag azonos fázisokból áll és - mint később azt látni fogjuk - az értékelés is azonos minősítési szempontok szerint történik attól függetlenül, hogy vásárolt termékről vagy informatikai rendszerről van-e szó, illetve hogy a minősítési folyamat azok megvalósításával párhuzamosan vagy a megvalósítás befejezése után késztermék, illetve működő rendszer állapotban történik. A továbbiakban a minősítendő informatikai terméket, illetve rendszert egységesen a ***minősítés tárgyának (MT)*** nevezzük. A közös értékelési módszer azért is előnyös, mert egy olyan informatikai rendszert könnyebb értékelni, amely már korábban ugyanezzel a módszerrel értékelt termékeket tartalmaz.

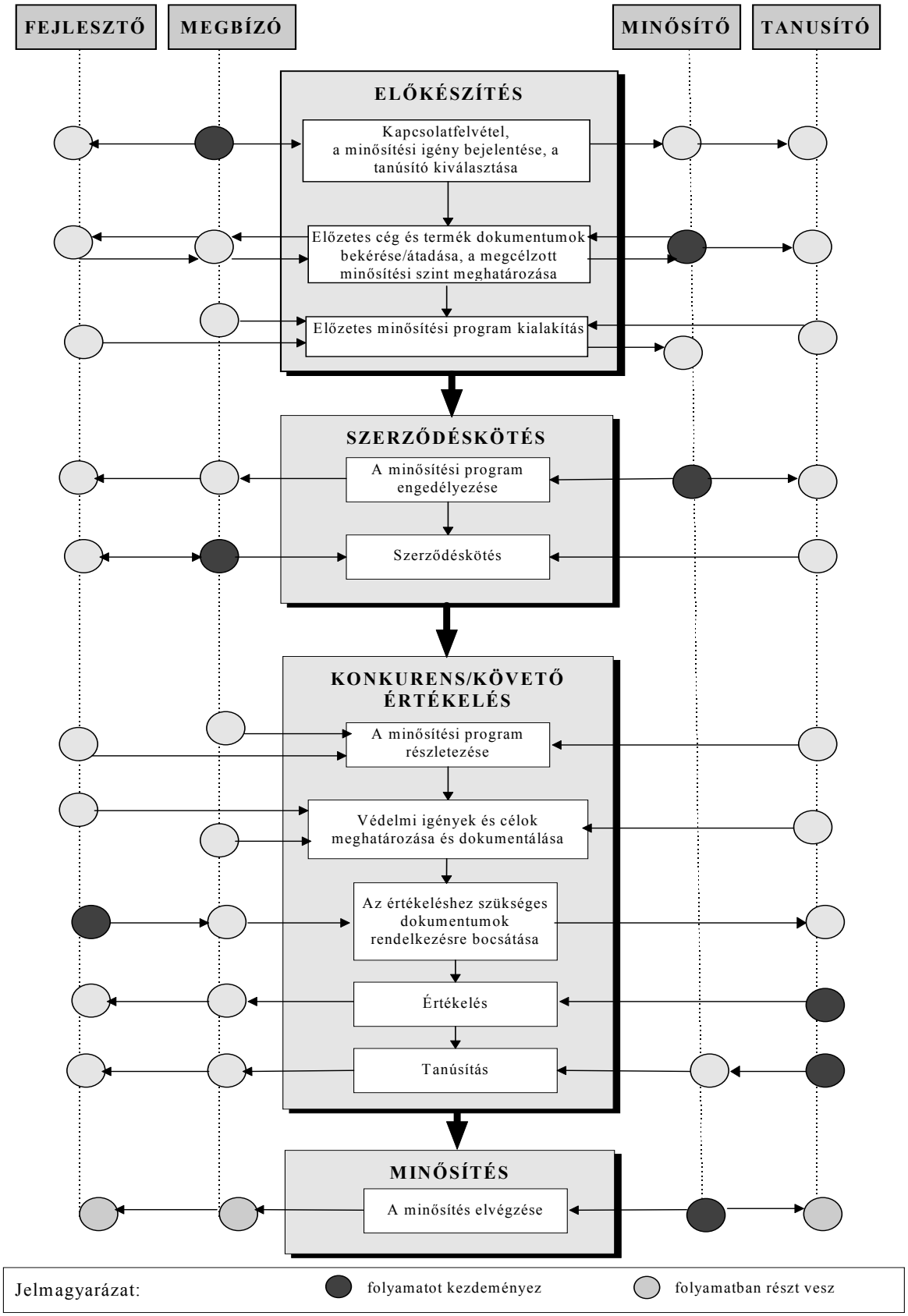
Jelen dokumentumban a minősítési folyamat leírása keretében *informatikai termék*nek nevezünk egy jól meghatározott funkciót vagy funkció-együttest megvalósító informatikai eszközt, amely kereskedelmi forgalomban késztermékként kapható.

Informatikai rendszernek nevezünk az informatikai termékekből álló, jól meghatározott felhasználói követelmények teljesítése érdekében elvégzett integrációs, adaptációs és fejlesztési tevékenységgel létrehozott informatikai eszközök összességét, amely meghatározott, ismert környezetben és feltételek között működik.

A termék és a rendszer közötti éles választóvonal a kereskedelmi és a felhasználói szféra között húzódik meg. Informatikai rendszernek tekintünk egy olyan megvásárolt terméket is, amely funkcionális változtatás nélkül kerül használatba vételre, de a felhasználónál annak igényei, követelményei szerint lesznek a paraméterek beállítva vagy a konfiguráció kialakítva. Jellemző példaként említhetünk egy PC-s konfigurációt, amely a kereskedelemben PC hardver, illetve DOS, Windows és egyéb PC-s szoftver *termékekként* áll rendelkezésre. Informatikai rendszerré válik, amikor a funkcionálisan változatlan termékek egy jól meghatározott konfigurációja installálva, a megfelelő paraméter-beállítással a felhasználóhoz kerül. Általában azonban beszerzés útján a felhasználóhoz került termékek együttese nem elégíti ki azonnal a felhasználói igényeket, azokon még jelentős rendszerintegrációs és adaptációs tevékenység történik, amely által alakul ki az informatikai rendszer.

Az informatikai termék, illetve rendszer fogalmának ez az önkényes értelmezése a minősítési folyamat és a követelményrendszer formailag egységes felépíthetősége miatt szükséges. Az 5. és a 6. fejezetekben láthatók lesznek a formailag azonos minősítési folyamat és követelmények tartalmi és értelmezésbeli különbségei, attól függően, hogy termékről vagy rendszerről van szó.

Természetesen egyébként egy termék is rendszernek tekinthető, amely sok meghatározott funkciójú komponensből áll és együttesen valósítanak meg egy funkciót vagy funkció-együttest, de a tanulmány keretei között ezt nem így értelmezzük.



Az informatikai rendszerek és termékek minősítési folyamatának áttekintő képe
1. ábra

Mind a termékek, mind a rendszerek minősítésre kerülhetnek a megvalósítás folyamatában, de megtörténhet a minősítés késztermék állapotban, pl. amikor egy ország kereskedelmében megjelent, egy másik országban fejlesztett terméket kell minősíteni. Rendszerek esetében történhet a minősítés a megvalósítás befejezése után, a működés időszakában, illetve az újbóli minősítés is ebbe a kategóriába tartozik.

Tehát a minősítés folyamatának fázisai, a minősítési követelmények nemcsak a termék, illetve rendszer esetében azonosak, hanem attól is függetlenek, hogy megvalósítás alatti vagy utáni minősítésről van szó. A megvalósítással párhuzamosan történő minősítést a továbbiakban röviden *egyidejű,* a megvalósítás utánit *követő minősítésnek* nevezzük.

Az 1. sz. ábrán látható minősítési folyamat legfontosabb szereplői:

- A ***minősítő (accreditation body),*** amely szerepkör betöltésére a 3. fejezetben hivatkozott a számítástechnikai és távközlési rendszerek információvédelmi felügyeletének és megfelelőség-vizsgálatának rendjéről szóló kormányrendelet-tervezetben szereplő Informatikai Biztonsági Főfelügyeletet (továbbiakban: Főfelügyelet) létrejöttét tételezzük fel és a továbbiakban a minősítő fogalma alatt a Főfelügyeletet fogjuk érteni.
- A ***tanúsító (certification organization),*** egy, a tanúsítási tevékenységre feljogosított gazdasági társaság lehet. Mindkét esetben a 7. fejezetben ismertetett akkreditálási eljárás után megkapott, a tanúsítási tevékenységre szóló engedéllyel rendelkezik. A továbbiakban a minősítési folyamat leírása azzal a feltételezéssel történik, hogy a tanúsítást gazdasági társaság végzi.
- A ***megbízó (sponsor)*** az a szervezet, intézmény, amely a MT-vel kapcsolatos minősítési igényt a minősítőnél bejelenti és a tanúsítási eljárást a tanúsítónál megrendeli.
- A ***fejlesztő (developer),*** amely az MT fejlesztését végzi vagy végezte.

Vannak esetek, amikor a megbízó és a fejlesztő azonos. A minősítő és a tanúsító szervezetileg mindig külön választott.

A minősítési folyamat a következő fontosabb részfolyamatokból áll:

- *előkészítés,*
- *szerződéskötés,*
- *értékelés és tanúsítás,*
- *minősítés.*

A teljes minősítési folyamatban alapvető feltételezés, hogy tanúsító a megbízóval és az azzal kapcsolatban levő fejlesztővel szoros együttműködésben végzi az egyes fázisokhoz tartozó tevékenységeket. Minden fázisban a későbbi fejezetekben pontosan meghatározott dokumentumokat kell szolgáltatnia teljes felelősséggel a megrendelőnek a fejlesztő támogatása mellett. Minden fázist pontosan definiált output dokumentumok kísérnek.

2.1. Előkészítő fázis

Az előkészítő fázisban először a megbízó felveszi a kapcsolatot a minősítővel és bejelenti a minősítés iránti igényt, amely után a minősítő bekéri az előkészítő dokumentumokat, amelyek a következők:

- termék esetén külföldi társaság általi befolyásra, felügyeletre, tulajdonlásra vonatkozó dokumentumok,
  - az MT fejlesztését végző cég ismertetője,
  - az MT-vel kapcsolatos piaci információk dokumentálása,
- az MT rövid műszaki leírása, különös tekintettel biztonsági funkciókra és a megcélzott minimális mechanizmus erősségi és minősítési szintekre.

A dokumentumok tanulmányozása során a minősítő szóbeli vagy írásbeli kiegészítést kérhet a megbízótól. A minősítő a kapott dokumentumok áttekintése, ellenőrzése és az esetleges kiegészítések bekérése után a megbízóval közösen kiválasztja a tanúsítót. A kiválasztott tanúsító a minősítőtől megkapja a megbízó által szolgáltatott előkészítő dokumentumokat a minősítő esetleges írásbeli megjegyzései kíséretében. Természetesen előfordulhat az is, hogy a minősítő az előkészítő dokumentumok alapján már ebben a szakaszban

megtagadja a minősítés engedélyezését, pl. olyan, a termékkel, a forgalmazóval vagy a fejlesztővel kapcsolatos információkhoz jut, amelyek azt mutatják, hogy a termék minősítésének engedélyezése nem kívánatos vagy más szervezetre (pl. Országos Rejtjelfelügyelet) tartozik.

A következő lépésben vételével a tanúsító, a megbízó - és egyidejű minősítés esetén a fejlesztő - a megcélzott minősítési szint, a minősítési követelményrendszer és az értékelési módszertan figyelembe előzetes jelleggel meghatározzák a tevékenységeket, azok ütemezését és a kísérő dokumentumokat. Ezután a megbízó benyújtja a minősítőhöz az előzetes minősítési programot. Ezzel a szerződéskötés és a minősítési folyamat indításának előkészítése befejeződött.

2.2. Szerződéskötési fázis

A minősítő a megbízó által átadott dokumentumok áttanulmányozása és a szükséges konzultációk, kiegészítések elvégzése után engedélyezi a minősítési programot és az érdemi folyamat megindítását. A minősítő ezt írásban közli a megbízóval és a tanúsítóval.

A minősítő számára ezen a ponton adódik még egy lehetőség, hogy az időközben esetlegesen felmerült újabb információk nyomán a minősítést ne engedélyezze.

Ezt a fázist a tanúsító és a megbízó közötti szerződés megkötése zárja le. A létrejött szerződésben a következőknek kell szerepelniük:

- A tanúsító:
  - kötelezettséget vállal, hogy végig viszi a értékelési folyamatot a tanúsítás befejezéséig, ezt követően javaslatot tesz az MT-nek az értékelés eredményének megfelelő besorolására, elkészíti az értékelési jelentést, a tanúsítási dokumentumot és ezeket továbbítja a minősítőhöz,
  - a megbízó rendelkezésére bocsátja a minősítési folyamat sikeres lebonyolításához szükséges információkat (értékelési módszer, követelményrendszer, stb.),

- megőrzi a megbízóra, a fejlesztőre és az MT-re vonatkozó bizalmas információkat.

♦ A megbízó:

- a tanúsító rendelkezésére bocsátja az általa kért és a minősítési folyamat lebonyolításához szükséges információkat,
- tudomásul veszi az értékelési módszert és követelményeket, azok alkalmazásában együttműködik a tanúsítóval,
- a tanúsítón keresztül a minősítő rendelkezésére bocsát engedélyezés céljából minden olyan, a megbízó, a forgalmazó vagy a fejlesztő által a későbbiekben készített marketing dokumentumot (hirdetés, szórólap, stb.), amelyben hivatkozás történik a minősítőre, a minősítés folyamatára, eljárásaira,
- A megbízó a dokumentumok rendelkezésre bocsátása mellett kötelezettséget vállal a tanúsítónak nyújtandó meghatározott szolgáltatásokra az értékelés alapos elvégzése érdekében. Ezek a következők lehetnek:
  - az MT alapos megismerését szolgáló tréning,
  - konzultációk,
  - hozzáférési lehetőség biztosítása az MT-hez és az ezzel kapcsolatos támogatás biztosítása,

  A fenti szolgáltatások biztosításának módjáról és mértékéről a tanúsító és a megbízó szintén megállapodik egymással.

Javasolható, hogy a megbízó egy másik szerződést is kössön a fejlesztővel, biztosítva annak rendelkezésre állását a teljes minősítési folyamat során.

2.3. Értékelési fázis

Az *értékelési fázis* első lépéseként a tanúsító és a megbízó pontosítják és véglegesítik a minősítési programot, valamint képviselőikből felállítják azt a team-et, amely együttműködik az értékelés során.

Az értékelés módszere alapvetően az informatikai termékek és rendszerek fejlesztésénél szokásos szemléletet tükrözi. A fejlesztéshez hasonlóan az értékelési folyamat is először egy elvontabb ***védelmi igény*** (security object) megfogalmazásából indul ki. Ennek keretében meghatározzák, hogy az MT védelmi rendszerének az általa kezel adatok *bizalmassága, hitelessége, sértetlensége, rendelkezésre állása* elvesztése által okozott alapfenyegetések közül melyek ellen milyen védelmi képességi szinten kell a védelmet realizálnia. Ezt informatikai rendszerek esetében az ***Informatikai Biztonságpolitika,*** termékek esetében a ***Termék Besorolási Ismertető*** tartalmazza.

Minden szervezetnek - így a közigazgatási intézményeknek is - ki kell alakítaniuk az egész szervezet biztonságát elvi szinten szabályozó politikát, az ***Intézményi Biztonságpolitikát,*** amely az érvényes jogszabályok, ajánlások és belső szabályzatok alapján megfogalmazza az alapvető védendő értékek (vagyontárgyak, fizető eszközök, információk, adatok, stb.) védelmének, azok szervezeten belüli és kívüli kezelésének - információ esetében a megosztás - alapszabályait.

Ennek keretében az informatikai rendszerre és környezetére az *Informatikai Biztonságpolitika* fogalmazza meg az érvényes jogszabályok, ajánlások és belső szabályzatok alapján az adatok kezelésének, megosztásának, bizalmasságának, hitelességének, rendelkezésre állásának és funkcionalitásának megőrzésére vonatkozó alapelveket.

Informatikai termékek esetében a *Termék Besorolási Ismertető* a felhasználó - jelen esetben a tanúsító - számára leírja, hogy az adott termék mely alapfenyegetések ellen, milyen környezeti feltételek mellett milyen védelmi képességekkel rendelkezik. Az Informatikai Biztonságpolitikát és a Termék Besorolási Ismertetőt a megbízónak kell a tanúsító rendelkezésére bocsátani.

Az értékelési folyamat következő lépése a ***védelmi cél*** (security target) meghatározása, amely a következő részekből áll:

- az Informatikai Biztonságpolitikában, illetve a Termék Besorolási Ismertetőben megfogalmazott védelmi igények,

- a *védelmet megvalósító funkciók* specifikációja,
- a szükséges *védelmi mechanizmusok* definíciója,
- a *védelmi mechanizmusok erősségének* megfogalmazása,
- a megfogalmazott *megcélzott minimális mechanizmus erősségi és minősítési szint*.

Az MT funkcióit a biztonság szempontjából három kategóriába soroljuk:

- a *védelmet megvalósító funkciók*, amelyek a védelmi képességek közvetlen hordozói és meghatározott védelmi igényt elégítenek ki,
- a *védelmet segítő funkciók*, amelyek nem realizálják közvetlenül a védelmi funkciókat de jelenlétük, működésük feltételt képez azok működéséhez, pl. a biztonsági naplózást megvalósító szoftver modul a védelmet megvalósító funkció része, viszont a naplózást végző nyomtató a védelmet segítő funkció része,
- *egyéb funkciók*, amelyek a védelmi képességek realizálásában nem vesznek részt.

Az MT védelmet megvalósító funkcióinak leírása a védelmi célok megfogalmazásában a legfontosabb részt jelenti. Leírásuk az ITSEC ajánlása szerint következő funkció tagolásban történik:

- azonosítás és hitelesítés (Identification and Authorization),
- hozzáférés szabályozás (Access Control),
- jogosultság ellenőrzés (Accountability),
- auditálhatóság biztosítása (Auditibility),
- erőforrások újrafelhasználhatósága (Object Reuse),
- az adatok konzisztenciájának biztosítása (Accuracy),
- a megbízható szolgáltatások biztosítása (Reliability of Service), amelyen belül a következő részfunkciók vannak:
  - a hibaáthidalás biztosítása (Redundancy),
  - az újraindítás biztosítása (Recovery),

- a funkcionalitás biztosítása (Functionality),

♦ biztonságos adatcsere (Data Exchange), amelyen belül a következő részfunkciók vannak:

- hitelesítés (Authentication),
- hozzáférés szabályozás (Access Control),
- bizalmasság megőrzés (Data Confidentiality),
- az adatok hitelességének és sértetlenségének biztosítása (Data Integrity),
- letagadhatatlanság biztosítása (Non-Repudiation).

A biztonságos adatcsere fenti funkciói között néhány korábbi pontban megadott funkcióval formailag azonos található (pl.: hitelesítés, hozzáférés szabályozás). E funkciók mindegyike a számítógépes hálózatok szintjére vonatkozik.

A tanúsításhoz szükséges MT biztonsági funkció leírásnál a fenti funkció listából az egyes funkciókat az ITSEC biztonsági osztályainak megfelelően kell számításba venni, azaz vannak funkciók, amelyek csak a magasabb biztonsági osztályokban értelmezettek, pl. az F-C1 osztályban csak a hitelesítés és azonosítás, valamint a hozzáférés szabályozás biztonsági funkciók értelmezettek.

Az ITB 12. sz. ajánlásban az információvédelem minimális, illetve a megbízható működés követelményeinek csoportosítása az ITSEC funkció csoportosítást követi. Így a 12. sz. ajánlás funkcionális követelményei és a jelen dokumentum biztonsági funkció értékelési szempontrendszere között biztosított az összhang, azaz, ha egy informatikai rendszer logikai védelmét a 12. sz. ajánlás követelményei alapján építik ki, akkor biztosított, hogy az értékelés is azonos funkcionális szempontok szerint történik, és ha a védelem megvalósítása hatékony, akkor a minősítési besorolás meg fog felelni a védelmi rendszer tervezésekor megcélzott biztonsági osztálynak. Pl. ha egy rendszert az F-C2 szintű biztonsági funkció osztályra terveztek és ez maradéktalanul meg is valósult, valamint megfelelően működtetik is, akkor a minősítési eljárás végén - feltéve, ha a későbbiekben még részletezett egyéb követelmények is teljesülnek - az E2 minősítési szintre lesz besorolva.

Mint azt korábban említettük a TCSEC osztályok, az ITSEC E0-E6 értékelési osztályok és az ITSEC F-C1 - F-B3 funkcionális követelmény osztályok, valamint az ITB 12. sz. ajánlásának osztályozása között egyértelmű a megfeleltetés, amelyet az alábbi táblázat mutat be. Így biztosított az ellentmondásmentes összhang a 12. sz. ajánlás, a jelen dokumentum és az ITSEC között mindegyik relációban.

TCSEC OSZTÁLYOK	ITSEC ÉRTÉKELÉSI OSZTÁLYOK	ITSEC FUNKCIONÁLIS OSZTÁLYOK	12. AJÁNLÁS		
A1	E6	F-B3			
B3	E5	F-B3			
B2	E4	F-B2			
B1	E3	F-B1			
C2	E2	F-C2	**A**	**F**	**K**
C1	E1	F-C1			
D	E0				

A biztonsági követelmények közötti összefüggés

1. táblázat

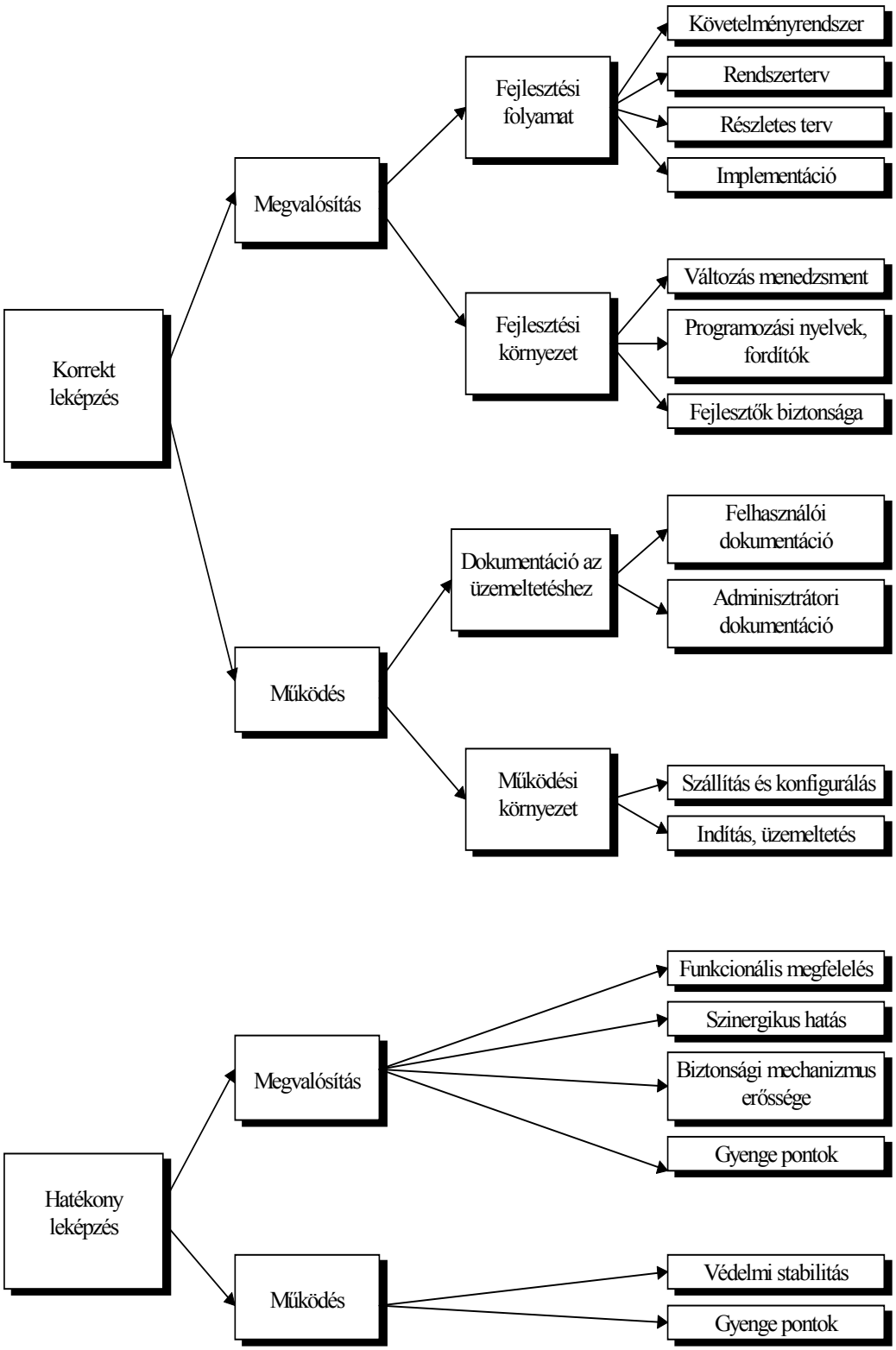
A védelmi célok meghatározásának következő fontos dokumentuma a szükséges *védelmi mechanizmusok* definiálása. Kötelező jelleggel csak az ITSEC F-B2 és F-B3 osztályaira van előírás, hogy a biztonsági funkciók közül a hozzáférés szabályozást milyen mó-

don kell megvalósítani. Az F-B2-nél alacsonyabb osztályokra a védelmi mechanizmusok definiálása nem kötelező. Elképzelhetők azonban olyan speciális védelmi célok, amelyeknél a védelmi mechanizmus megadása szükséges.

A védelmi mechanizmusok erősségének megfogalmazása azt jelenti, hogy a megbízónak a fejlesztővel együtt meg kell ítélnie, hogy az MT-ben realizált védelmet megvalósító funkciók és mechanizmusok mennyire képesek a különböző erősségű támadásoknak ellenállni.

A védelmi célok meghatározásának utolsó dokumentuma a *megcélzott minimális mechanizmus erősségi és minősítési szint* meghatározása, amelyet már a minősítési folyamat előkészítési fázisában előzetes jelleggel meg kellett adnia a megbízónak, hogy a minősítési program tervét ennek figyelembe vételével lehessen összeállítani. A védelmi célok megfogalmazása keretében az előző dokumentumok összeállítása során a megbízó a fejlesztővel együtt ellenőrzi a megcélzott minimális mechanizmus erősségi és minősítési szint realitását és ezek után véglegesíti azt.

Az értékelési fázis következő, lényeges két lépése az értékeléshez szükséges dokumentumok bekérése a megbízótól, valamint magának az értékelésnek az elvégzése a tanúsító által az előre rögzített követelményrendszer szerint. A dokumentumok szerkezetének és tartalmának szigorúan kell követnie az értékelés szempont-rendszerét, amelynek a logikai vázát az 2. sz. ábrán mutatjuk be, majd ezután megadjuk az egyes követelmények fogalmi definícióját.



Az értékelés szempont-rendszere
2. ábra

A tanúsító által bekért dokumentumok előállításának és bekérésének módja különböző attól függően, hogy a megvalósítási folyamattal egyidejűen vagy a megvalósítás befejezése után történik. Az egyidejű *értékelés* esetében a tanúsító, a megbízó és a fejlesztő szoros, operatív kapcsolatban áll egymással, lényegében az MT biztonsági rendszerének fejlesztése a teljes rendszer vagy termék fejlesztés szerves részét képezi. A korrekt leképzés és a hatékony leképzés részletes szempontjai szerint strukturált dokumentumok a fejlesztés előrehaladásának ütemében készülnek el és kerülnek átadásra.

Ha az értékelés követő jellegű, azaz a megvalósítás befejezése után pl. a rendszer működési időszakában vagy a termék kereskedelmi forgalomba történő helyezése után történik, a dokumentumok ugyanúgy a korrekt leképzés és a hatékony leképzés részletes szempontjai szerint kerülnek kialakításra és bekérésre, de utólagosan. Természetesen a tanúsító a követő értékelésnél is igényt tarthat a fent ismertetett egyéb szolgáltatásokra a szerződésben megállapodottak szerint.

Az értékelés szempontrendszere nemcsak az egyidejű, illetve követő értékelés esetében invariáns formailag, hanem attól sem függ, hogy az MT-t informatikai termék vagy működő rendszer testesíti meg. Természetesen a korrekt leképzés és a hatékony leképzés részletes szempontjainak megfelelően összeállított dokumentumok tartalma magán viseli az informatikai termékek, illetve rendszerek sajátosságait, ezekre azonban az 5. és 6. fejezetekben térünk ki részletesebben.

Az MT értékelése a 2. sz. ábrán látható fa struktúrájú szempont-rendszer szerint történik, amelyben a *korrekt leképzés* és a *hatékony leképzés* a két alapszempont. Először a korrekt leképzés szerinti értékelésnek kell megtörténnie, mert az ehhez szolgáltatott dokumentumok szükségesek a hatékony leképzés szerinti értékeléshez is.

Az értékelés folyamat egyes lépései a két alapszempontból induló fa legalsó ágában szereplő részletes szempontok szerint zajlanak le. Minden lépésre egységes követelményrendszer adott a megbízó által szolgáltatott dokumentációra és a tanúsító által megvalósítandó vizsgálati akciókra vonatkozóan:

- a dokumentációra vonatkozó tartalmi és formai követelmények,
- a dokumentáció által szolgáltatott, az MT-re az adott értékelési szempont szerint vonatkozó információk egyértelmű értelmezhetősége,

- a tanúsító értékelési tevékenysége mind a dokumentáció ellenőrzése, mind az MT további ellenőrzése, tesztelése tekintetében.

2.3.1. Korrekt leképzés

A *korrekt leképzés* vizsgálatában az értékelés azt méri, hogy az MT biztonsági funkcióinak és a védelmi mechanizmusainak megvalósítása mennyire korrekt, mennyire fedi a biztonsági funkciók specifikációját.

A korrekt leképzést két alapterületen, a *megvalósítás* és a *működés* területein mérjük.

A megvalósítás területén a fejlesztési folyamat a *követelményrendszer, a rendszerterv, a részletes terv és az implementáció,* a fejlesztési környezet *a változás-menedzsment, a programozási nyelvek, fordítók és a fejlesztők biztonsága* szempontok szerint kerül értékelésre.

A működés területén a korrekt üzemeltetéshez szükséges *felhasználói*, illetve *adminisztrátori dokumentáció* minősége, a működési környezet az MT *szállítása és konfigurálása,* valamint *indítása és üzemeltetése* szempontok szerint kerül értékelésre.

A következőkben *fejlesztési folyamat* értékelésénél szerepet játszó szempontok fogalmi meghatározását adjuk meg.

A *követelményrendszert* az értékelési folyamat 2. lépésében meghatározott *védelmi cél* összeállítás fogalmazza meg, amely tartalmazza az Informatikai Biztonságpolitikában, illetve a Termék Besorolási Ismertetőben meghatározott védelmi igényeket, a védelmet megvalósító funkciók specifikációját, a szükséges védelmi mechanizmusok definícióját (opcionálisan), a megcélzott minimális védelmi mechanizmus erősség és a minősítési szint megfogalmazását. A követelményrendszer a védelmi céloknak a tanúsító számára dokumentált formája, amely a korrekt leképzés szerinti értékelés kiinduló dokumentuma.

A *rendszerterv* az MT leírásának rendszer szintű dokumentációja, amelyből a tanúsító megismeri az MT hardver és/vagy szoftver architektúráját modul szinten. Az értékelés számára dokumentált rendszer terv fontos jellemzője, hogy egyértelműen elkülöníti azokat a modulokat, komponenseket, amelyek a *védelmet megvalósító funkciókat*, a *védelmet segí-*

tő funkciókat, illetve az *egyéb funkciókat* valósítják meg. Ezáltal a tanúsító jó áttekintést kap, hogy az értékelés során mely modulokra kell koncentrálnia.

A *részletes terv* az MT rendszertervének olyan szintű dokumentált lebontása, amely a szoftver esetén programozás, illetve hardver esetén a gyártás alapját képezi. Ez a terv a védelmet megvalósító funkciók, a védelmet segítő funkciók, illetve az egyéb funkciók realizálásában szerepet játszó alap-komponens szintű bontását is tartalmazza. Így a védelmet megvalósító, illetve segítő komponensek hibás működéséből, kieséséből adódó, a védelmi képességekre való hatásokat fel lehessen mérni.

Az *implementáció* a fejlesztési folyamat utolsó fázisát, az MT megvalósítás dokumentált formáját jelenti, amelyben részletesen le van írva az alapkomponensek tesztje az előzőekben rögzített specifikációjukhoz képest. Az informatikai termék vagy a rendszer felépítéstől függően szerepel benne az önálló részfunkciókkal rendelkező alrendszerek tesztje, majd a teljes termék, illetve a rendszer tesztje. A tesztek leírása elsősorban a védelmet megvalósító, illetve segítő funkciókra koncentrál.

A *fejlesztési környezet* értékelésénél szerepet játszó szempontok fogalmi meghatározását a következőkben adjuk meg.

A *változás-menedzsment* a fejlesztés során előállt dokumentum változatok szabályozott módon történő kezelését és követését jelenti. Ezáltal az MT-t és azon belül is a biztonsági funkciókat érintő változtatások, módosítások követhetővé válnak a teljes fejlesztési ciklusra vonatkozóan. A tanúsító számára ez azért fontos, hogy ne történhessen olyan ellenőrizetlen módosítás az MT-n, amely alapvetően megkérdőjelezi a védelmi céloknak való megfelelést.

A *programnyelvek és fordítók* megválasztása csak a szoftverben és firmware-ben implementált alapkomponensek esetében jelentenek szempontot a komponensek biztonsági funkciónak korrekt leképzése szempontjából.

A *fejlesztők biztonsága* azok fizikai és adminisztratív védelmének a fejlesztési környezetben való megvalósítási módjára vonatkozik. Ez a szempont lényeges olyan tekintetben, hogy mennyire áll fenn a közvetlen támadások vagy a fejlesztési információk illetéktelenek tudomására jutásának veszélye.

Az MT *üzemeltetése* területén a korrekt és biztonságos *üzemeltetéshez szükségesek* az *adminisztrátori* és a *felhasználói dokumentációk.* Ezek képviselik azt a médiumot, amelyen keresztül a fejlesztő az adminisztrátorokkal és felhasználókkal kommunikál. Az MT-nek a biztonsági követelményeknek megfelelő használata és üzemeltetése szempontjából fontos, hogy ezek jól áttekinthetőek, jól érthetőek legyenek, az MT-t - ezen belül a biztonsági funkciókat - korrektül képezzék le. A tanúsító ezeket a dokumentációkat ebből a szempontból értékeli.

A *működési környezet* területén az MT *szállítása és konfigurálása,* mint szempont a felhasználóhoz történő biztonságos szállításra, valamint az üzembehelyezés előtti konfigurálásra vonatkozik, olyan szempontból, hogy az MT védelmi képességei ne csökkenhessenek a szállítás, illetve a konfigurálás során bekövetkezett vétlen hiba vagy szándékos visszaélés miatt.

Az *indítás, üzemeltetés* szempontok azokat az eljárásokat érintik, amelyek az MT biztonságos indítására, újra-indítására, leállítására és üzemeltetésére vonatkoznak. A biztonságos üzemeltetés nemcsak a rendszer rendelkezésre állásához kapcsolódik, hanem az MT által kezelt információk védelmére is.

Az MT értékelése korrekt leképzés szempontjából a fenti szempontok alapján történik. *Az értékelés eredményeként az E0-tól E6-ig terjedő osztályok valamelyikébe sorolja be a tanúsító az MT-t.* Az értékelési fázis után következő tanúsítás keretében történik majd meg az MT tanúsítási osztálybasorolása, amely a korrekt leképzés és a hatékony leképzés szerinti értékelések *együttes* figyelembevételével valósul meg. Az egyes szempontokra vonatkozó, a megbízó által teljesítendő követelmények az osztályok növekvő sorrendjének megfelelően szigorodnak. Az ITSEC a szigorodás mértékét azzal is jelzi, hogy a megbízó által szolgáltatott dokumentumok érthetőségére és egyértelműségére vonatkozó egyre szigorodó követelmények érzékeltetésre a következő táblázatban ismertetett kifejezéseket használja.

Osztályok	Követelmény a dokumentumok érthetőségére, egyértelműségére		
E1,E2	Kijelentő jelleg		
E3,E4		Leíró jelleg	
E5,E6			Magyarázó és értékelő jelleg
Követelmény a dokumentumok érthetőségére, egyértelműségére 2. táblázat			

Megállapító jelleg

A dokumentum tényeket állapít meg kijelentő jelleggel, amelyek valódiságáért a megbízó felelősséget vállal.

Leíró jelleg

A dokumentum tényeket állapít meg kijelentő jelleggel*, az ezekkel kapcsolatos fontosabb jellemzőket felsorolja,* A jellemzők valódiságáért a megbízó felelősséget vállal.

Magyarázó és értékelő jelleg

A dokumentum tényeket állapít meg kijelentő jelleggel és az ezekkel kapcsolatos fontosabb jellemzőket felsorolja *és értékeli*. A jellemzők valódiságáért és az értékelésért a megbízó felelősséget vállal.

A következő táblázatok a korábban értelmezett értékelési szempontok szerint kialakított dokumentációkra vonatkozó, az osztályok sorszáma szerint szigorodó követelményeket mutatják be. A táblázatokban az üres mezők azt jelenti, hogy az adott osztályban az előzőekhez képest nincs szigorúbb vagy újabb követelmény.

Korrekt leképzés / Megvalósítás / Fejlesztési folyamat 3. táblázat				
	Követelmények	**Rendszerterv**	**Részletes terv**	**Implementáció**
E1	Védelmi cél dok.	Informális rendszerterv	Nincs követel-mény	Teszt eljárások és eredmények. Nem kötelező
E2			Informális részle-tes terv	Funkcionális teszt eljárások és eredmények
E3				Forráskód, hardver-rajzok, teszt eljárások. Eredmények a mechanizmusokra
E4	Szemiformális funkció spec. és alátámasztó formális biztonság-politikai modell	Szemiformális rendszerterv	Szemiformális részletes terv	
E5				Ua. mint E3 csak alapkompo-nensek szintjére lebontva
E6	Formális funkció speci-fikáció	Formális rend-szerterv		

Fogalom magyarázat:

Informális leírás, specifikáció, terv: természetes nyelven készült leírás, specifikáció, terv.

Szemiformális leírás, specifikáció, terv: szabályelvű természetes nyelven készült leírás, specifikáció, terv pl. strukturált tervezési módszereknél használt adatfolyam, entitás-reláció, állapot-átmenet, stb. diagrammok.

Formális leírás, specifikáció, terv: szintaktikusan és szemantikusan szabályozott specifikációs nyelven készült leírás, specifikáció, terv.

Formális biztonságpolitikai modell: formális nyelven leírt biztonsági politika modell.

Az irodalomban különböző védelmi céloknak megfelelő politikai modellek ismertek, pl. Bell-La Padula modell nemzeti szintre a bizalmasság megőrzésére, Clark és Wilson

modell kereskedelmi tranzakciós rendszerek integritásának biztosítására, Brewer-Nash modell a banki ügyféloldali bizalmasság megőrzésére, Eizenberg modell az időben változó hozzáférési jogok kezelésére, Landwehr modell az üzenet átviteli hálózatok biztonsági követelményeire.

Korrekt leképzés / Megvalósítás / Fejlesztési környezet 4. táblázat			
	Változás-menedzsment	**Programnyelvek, fordítók**	**Fejlesztők biztonsága**
E1	A minősítendő MT egyértelmű azonosítása (változat-szám).		
E2	Változás-menedzsment rendszer a teljes fejlesztési ciklusra		Biztonsági Szabályzat szükséges
E3	Elfogadási eljárás a változás-menedzsmentben	Csak szabványban, ajánlásban szereplő nyelv alkalmazható	
E4	Számítógéppel támogatott változás-menedzsment	A fordítók implementációnál használt jellemzőit dokumentálni kell	
E5	Minden fejlesztési objektumra kiterjedő, a fejlesztőtől független és integrált változás-menedzsment	A forráskódot és a futási idejű könyvtárakat rendelkezésre kell bocsátani.	
E6	A fejlesztés során használt összes eszköz változás-menedzsment alá esik		

Korrekt leképzés / Működés 5. táblázat			
	Üzemeltetéshez szükséges dokumentációk	**Működési környezet**	
		Szállítás és konfigurálás	**Indítás és üzemeltetés**
E1	Felhasználói és adminisztrátori dokumentáció biztosítandó	A szállításnál és a rendszergenerálásnál a biztonsággal kapcsolatos információkat és eljárásokat rögzíteni kell.	Biztonságos indítási és üzemeltetési eljárásokat kell kialakítani
E2		Csak biztonság szempontjából minősített termék építhető be. A rendszergenerálás auditáltan, rekonstruálható módon történhet	Meghatározandók az indításkor, üzemeltetési és karbantartási tevékenység során inaktívvá tehető biztonsági funkciók. Hardver diagnosztika szükséges.
E3			
E4			Biztonságos újra-indítási eljárásokat kell kialakítani.
E5			
E6		A konfiguráció formális definiálása szükséges	

2.3.2. Hatékony leképzés

A hatékony leképzés vizsgálatában az értékelés azt méri, hogy az MT védelmet megvalósító funkciói és a védelmi mechanizmusai milyen mértékben elégítik ki a definiált védelmi célokat. A hatékony leképzést két alapterületen, a *megvalósítás* és a *működés* területein mérjük. A megvalósítás területén *a funkcionális megfelelés, a szinergikus hatás, a biztonsági mechanizmus erőssége és a gyenge pontok,* működés területén *a védelmi stabili-*

tás és a gyenge pontok a részletes szempontok, amelyekkel a védelmi célok és a specifikált biztonsági funkciók hatékony leképzését mérjük.

A következőkben megadjuk a *megvalósításhoz* kapcsolódó értékelési szempontok fogalmi meghatározását.

A *funkcionális megfelelés* értékelése keretében az lesz megvizsgálva, hogy az MT által megvalósított biztonsági funkciók és mechanizmusok nem rendelkeznek-e olyan funkcionális hiányosságokkal, amelyek miatt nem felelnek meg a felállított védelmi igényeknek és bizonyos pontokon nem tudnak ellenállni, informatikai rendszer esetében az Informatikai Biztonságpolitikában, termékek esetében a Termék Besorolási Ismertetőben leírt releváns fenyegetéseknek.

A *szinergikus hatás* értékelése keretében az lesz megvizsgálva, hogy az MT által megvalósított biztonsági funkciók és mechanizmusok milyen módon erősítik vagy gyengítik egymás védelmi képességeit, nem fejtenek-e ki egymásnak ellentmondó hatást, mennyire integráltan valósítják meg a védelmi célokat.

A *biztonsági mechanizmus erőssége* értékelése keretében az lesz megvizsgálva, hogy az MT által megvalósított biztonsági funkciók és mechanizmusok - feltételezve a funkcionális megfelelést - mennyire képesek ellenállni egy képzett támadó direkt támadásának, annak milyen szintű erőforrásokra van szüksége a sikeres támadás megvalósításhoz. Itt a megvalósított biztonsági funkciók robosztusságának mérésről van szó, azaz mennyire képes a mechanizmus a védelem megkerülése, áthidalása, korrupciója mellet a direkt támadásokat is megakadályozni. A korábban ismertettek szerint a biztonsági mechanizmus erősségét *alap, közepes* és *magas* minősítésekkel osztályozzuk.

Alap szintű a védelmi mechanizmus erőssége, ha a védelem ellent tud állni a nem felkészült támadók véletlenszerű támadásának.

Közepes szintű a védelmi mechanizmus erőssége, ha a védelem ellent tud állni a korlátozott erőforrásokkal rendelkező átlagos felkészültségű támadók tudatos támadásának.

Magas szintű a védelmi mechanizmus erőssége, ha a védelem ellent tud állni a szakértői szintű, komoly erőforrásokkal rendelkező támadók tudatos támadásának. Ilyen erősségű védelmi mechanizmus mellett a sikeres támadás valószínűsége rendkívül csekély.

A megvalósítás területén a *gyenge pontok* elemzése keretében azonosítani kell a biztonsági funkciók és mechanizmusok megfelelési, erősségi és szinergikus elemzése során detektált, az MT konstrukciója szintjén jelentkező gyenge pontokat, amelyekről meg kell ítélni egy konkrét vagy feltételezett működési környezetben, hogy - a releváns fenyegetéseket figyelembe véve - potenciális vagy valós sebezhetőséget jelentenek. Az azonosított gyenge pontokra ki kell dolgozni azokat az ellenintézkedéseket az MT konstrukciójára vonatkozóan, amelyekkel a kockázatok elviselhető mértékűre nem csökkenthetők.

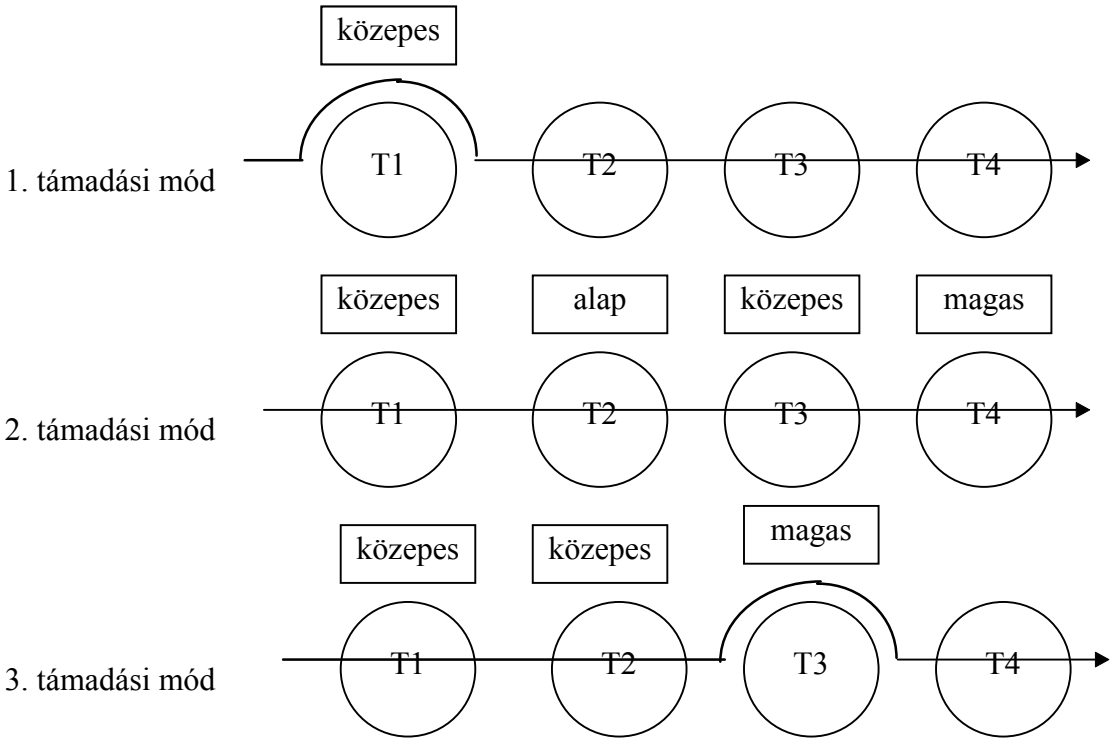
A *működés területén a védelmi stabilitás* értékelése keretében az lesz megvizsgálva, hogy az MT konfigurálása, üzemeltetése során előálló adminisztrátori, kezelői hibák nyomán nem áll-e elő a biztonság szempontjából sebezhető üzemmód, esetleg úgy, hogy az adminisztrátorok, felhasználók számára észrevétlen marad.

A *gyenge pontokat* a megvalósítás területén az MT konstrukciójában található sebezhetőségekként, a működés területén elsősorban az MT üzemeltetési feltételeiben, a környezet szabályozottságában mutatkozó sebezhetőségekként értelmezzük. Ebben az esetben is azonosítani kell a gyenge pontokat és ki kell dolgozni azokat az ellenintézkedéseket az MT környezeti feltételeire és szabályozottságára vonatkozóan, amelyekkel a kockázatok elviselhető mértékűre nem csökkenthetők.

A következő táblázat azt mutatja be, hogy a korrekt leképzés szerint történő értékeléshez bekért és a megcélzott minősítési szint követelményeinek megfelelő dokumentumok közül melyekből gyűjthet ki hasznos információkat a tanúsító az MT gyenge pontjainak megítéléséhez, akár a megvalósítás, akár a működés területén történő értékelésénél. Ez a táblázat egyben demonstrálja a korrekt leképzés és a hatékony leképzés szerinti értékelés közötti kapcsolatokat és összhangot, amely fontos szerepe játszik az értékelési fázis után következő tanúsítás keretében elvégzendő besorolásnál, amelynél a két szempontrendszer szerint elvégzett értékeléseket együtt kell figyelembe venni.

A korrekt leképzéshez szolgáltatott dokumentumok, amelyek a hatékony leképzés értékelésénél is felhasználásra kerülnek 6. táblázat							
		E1	**E2**	**E3**	**E4**	**E5**	**E6**
Védelmi cél dokumentáció		✓	✓	✓	✓	✓	✓
Formális biztonsági politika modell					✓	✓	✓
Biztonsági funkciók specifikációja	**informális** **szemiformális** **formális**	✓	✓	✓	✓ ✓	✓ ✓	✓ ✓
Rendszerterv	**informális** **szemiformális** **formális**	✓	✓	✓	✓	✓	✓
Részletes terv	**informális** **szemiformális**			✓	✓	✓	✓
Implementáció	**hardver-rajz,** **forráskód** **tárgykód**				✓	✓	✓ ✓
Működés (felhasználói/adminisztrátori dok., szállítás és konfigurálás, indítás és üzemeltetés)		✓	✓	✓	✓	✓	✓

A védelmi mechanizmusok erőssége és a gyenge pontok értékelése keretében a követelményrendszer (a 31. sz. táblázatban) *behatolási tesztet* javasol. Egy informatikai termék vagy rendszer védelmének sikeres támadása általában több egymásután bekövetkező támadási lépésből áll, amelynek keretében egy-egy védelmi intézkedés hatástalanítva, megkerülve, stb. lesz. A védelmi intézkedések sorozatát, amely mentén a támadás megvalósul *támadási útvonalnak* nevezzük. Egy adott útvonalon több féle *támadási mód* valósítható meg és az egyes védelmi intézkedések mechanizmusának erőssége különböző szintű lehet a választott támadási móddal szemben. A következő ábrán a támadási útvonalon négy védelmi intézkedést kell legyőzni. Ezt a támadó három fajta támadási móddal kíséreli meg. Egy adott intézkedés, pl. a T3 más és más mechanizmus erősségbeli besorolást kap a támadási módtól függően.



példa a támadási útvonalak, támadási módok és védelmi intézkedések összefüggésére

3. ábra

A védelmi mechanizmusok erőssége és a gyenge pontok értékelése keretében minden lehetséges támadási útvonalra és azon belül minden támadási módra el kell végezni a behatolási elemzést és az intézkedések besorolást védelmi mechanizmus erősség szempontjából. Az értékelés eredménye akkor megfelelő, ha a T védelmi intézkedések mindegyike a

védelmi célok keretében megfogalmazott minimálisan megkövetelt védelmi erősség szintet elérik.

Az értékelési fázis befejező lépései a *besorolás* és a *tanúsítás*. Az MT besorolása az E0-tól E6-ig terjedő besorolási osztályok valamelyikébe történhet. Ha az értékelés azt mutatja, hogy az MT nem sorolható be a védelmi célokban megfogalmazott *megcélzott minősítési szintre,* akkor az MT alacsonyabb szintre sorolható be, amennyiben az értékelés egyértelműen kimutatja az erre a szintre való alkalmasságot. Amennyiben az értékelés során olyan súlyos hiányosságokra derül fény, hogy az MT az E1 szintre sem sorolható be, akkor az E0 szintre kell besorolni vagy vissza kell utasítani a besorolást és ennél fogva a tanúsítást is. Az E0 szintre történő besorolásnál egyetlen védelmi intézkedés mechanizmusának erőssége nem éri el a megcélzott minimális mechanizmus erősségi szintet. Az E0 szintű besorolásnál az MT alkalmazható, illetve üzemeltethető minden, az E1-nél alacsonyabb biztonsági követelményű alkalmazási környezet esetében. Ha a tanúsítás vissza lett utasítva, akkor az MT még az E0 osztály szintjén sem alkalmazható addig, ameddig az MT tökéletesítés után le nem folytatott minősítési folyamat során valamelyik osztályba be nem lett sorolva és a minősítést meg nem kapta.

A 2. sz. ábra alapján elmondható, hogy az ITB 12. sz. ajánlását alapul véve - amely az informatikai rendszerekre vonatkozó biztonság funkcionális követelményeit írja le - a besorolások a közigazgatás területén jelenleg az E0-tól az E4-ig terjedhetnek. Például az E4 besorolás az *információvédelem* területén az informatikai rendszer belső védelmi képességeire - túlnyomórészt a logikai védelemre - vonatkozik és a *kiemelt biztonsági osztály* funkcionális követelményeivel azonos szintnek felel meg. Tekintve, hogy a 12. sz. ajánlás egy folyamat része és a későbbiekben az EK ajánlások szellemében továbbfejlesztett változatai - ezekben a biztonsági osztályok további finomítása is - várhatók. A 12. sz. ajánlás a logikai védelmet megvalósító funkció szempontjából az ITSEC-el konform, de a teljes körűség teljesítése miatt a fizikai és az adminisztratív védelmi területekre vonatkozó követelményeket is tartalmazza.

Az értékelés és a besorolás elvégzése után a tanúsító kiállítja az *értékelési jelentést* és a *tanúsítványt.*

Az értékelési jelentés az MT-nek az összes értékelési szempont szerinti értékelési eredmények rövid összefoglalását tartalmazza.

A tanúsítási dokumentum a következőket tartalmazza:

- a megbízó által megfogalmazott védelmi célok dokumentumára való hivatkozást, amely az értékelés kiindulási alapját képezte,
- az MT-re az értékelés nyomán megítélt E0 - E6 besorolási szintek valamelyikét vagy a tanúsítás sikertelen eredményét,
- az MT védelmi mechanizmusai erősségének minimális szintjét.

Az értékelési jelentés az értékelés lefolyásáról és eredményeiről szóló szakmai természetű tájékoztató dokumentum, amely azonban nem tartalmaz besorolást. A értékelési jelentést a tanúsító megküldi a minősítőnek és a megbízónak. A tanúsítvány - a tanúsító a minősítőtől korábban kapott jogosítványa alapján - hivatalos jelleggel és teljes felelősséggel rögzíti a tanúsítás tényét és végeredményét, amelyet megküld a minősítőnek a minősítés elbírálása támogatása céljából és a megbízónak tájékoztatásul, valamint - az értékelési jelentéssel együtt - a szerződés teljesítési dokumentumaként.

2.4. Minősítési fázis

A minősítő a tanúsító által hozzá eljuttatott értékelési jelentés tanulmányozása után, a tanúsítvány birtokában összegzi a minősítési folyamat előkészítő fázisában a fejlesztőről, a forgalmazóról és az MT-ről kapott piaci és céges információkat és ezek együttes figyelembe vétele után dönt a minősítésről.

A minősítő döntései a következők lehetnek:

1. visszautasíthatja a minősítést úgy, hogy a minősítési eljárás iránt még egyszer már nem lehet folyamodni,
2. visszautasíthatja a minősítést úgy, hogy a minősítési eljárás iránt újból lehet folyamodni,
3. visszautasíthatja a minősítést úgy, hogy a megbízó általi kérelem megújítása nélkül az értékelést és a tanúsítást megismételteti, de másik kiválasztott tanúsítóval,
4. kiadja a minősítést, de nem a megcélzott minősítési szinten,
5. kiadja a minősítést a megcélzott minősítési szinten.

Minden olyan esetben, amikor a minősítés nemleges vagy nem a kitűzött minősítési szintre szól a minősítőnek a megbízó felé e döntését indokolni kell.

A minősítő gondoskodik arról, hogy a minősített termékekről meghatározott információk egy rendszeresen megjelenő kiadványban, a "Biztonsági minősítésű informatikai termékek katalógusá"-ban jelenjenek meg, amelyben minden termékről a következők szerepeljenek:

- a termék típusa, pl. (modem, router, adatbáziskezelő, stb.),
- a termék neve, azonosítója,
- a minősítő által kiadott minősítési szint,
- a termék biztonsági jellemzőinek rövid leírása,
- a termék gyártójának és fejlesztőjének neve és címe,
- a termék forgalmazójának neve és címe,
- a tanúsító cég neve,
- a minősítési dokumentum száma, azonosítója,
- a minősítés kiadásának dátuma.

A katalógusban olyan termékek is szerepeljenek, amelyek minősítési folyamata már túllépett a megbízó és a tanúsító közötti szerződéskötésen.

3. KÖVETELMÉNYRENDSZER

Az MT értékelése az értékelési fázisban a 2. sz. ábrán látható szempontok szerint kialakított követelményrendszer szerint történik, amely az ITSEC-re lett alapozva és annak a szellemét követi abban a tekintetben is, hogy a követelményrendszer egységesen alkalmazandó mind informatikai rendszerre, mind termékre, azaz a Minősítés Tárgyára (MT). A követelményrendszer egységes alkalmazása igaz abból a szempontból is, hogy mind a fejlesztés alatti, mind a fejlesztés utáni időszakra (pl. kereskedelemi forgalomba kerülés, üzembehelyezés után) alkalmazható. Az egyes szempontok szerint megfogalmazott követelményeket értelemszerűen kell alkalmazni attól függően, hogy informatikai termékről vagy rendszerről van szó.

A követelményeket táblázatos formában ismertetjük. A táblázat-rendszer struktúrája a 2. sz. ábráét követi. Minden szempontnál szerepel a megbízó által szolgáltatandó dokumentumra vonatkozó:

- *tartalmi és formai követelmény*,
- a követelmény teljesítésének bemutatását előíró *evidencia követelmény*.

Ezeken túlmenően minden szempontnál szerepel *a tanúsító tennivalói,* amelyeket az adott követelmény MT általi teljesítéséről történő meggyőződés érdekében végre kell hajtania.

3.1. Korrekt leképzés

3.1.1. E1 szint

Rövid jellemzés: ezen a szinten lényeges a védelmi célok megfogalmazása és a rendszerterv informális leírása. Funkcionális tesztnek kell indikálnia az MT megfelelést a védelmi céloknak.

Megvalósítás / Fejlesztési folyamat **7. táblázat**		
A tanúsítónak átadandó		**1. Védelmi célok.** **2. Az MT architektúrájának informális leírása.** **3. Teszt dokumentáció (opcionális).** **4. Az MT teszteléséhez használt tesztprogramok könyvtárai és a teszteszközök (opcionális).**
Követelmény-rendszer	**Tartalmi és formai követelmények**	**A védelmi célok dokumentációjának kijelentő jelleggel tartalmaznia kell:** **1. az MT védelmet megvalósító funkciónak felsorolását,** **2. az Informatikai Biztonságpolitikát (rendszer esetén), a Termék Besorolási Ismertetőt (termék esetén), amelyek azonosítják az MT-vel kapcsolatos védelmi célokat és veszélyeket,** **3. a védelmet megvalósító funkciók informális specifikációját.**
	Evidencia követelmény	**A védelmi célok dokumentációja kijelentő jelleggel tartalmazza, hogy rendszer esetén a valós, termék esetén a feltételezett fenyegetések ellen a védelmi funkciók hogyan fejtenek ki ellenhatást, valamint azt, hogy hogyan felelnek meg a védelmi igényeknek.**
	Tanúsító tennivalója	**Ellenőrizendők a dokumentációk megfelelése tartalmi és formai szempontból, valamint a védelmi cél dokumentáció ellentmondásmentes és teljes körű volta.**
Rendszerterv	**Tartalmi és formai követelmények**	**A rendszerterv kijelentés szinten tartalmazza:** **1. az MT architektúráját rendszer szinten,** **2. a külső interfészeket,** **3. a hardverben és/vagy firmware-ben implementált védelmi funkciók megnevezését.**
	Evidencia követelmény	**Állapítsa meg, hogy a védelmet megvalósító funkciók, hogyan felelnek meg a védelmi céloknak.**
	Tanúsító tennivalója	**Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.**
Részletes terv	**Tartalmi és formai követelmények**	**Nincs követelmény.**
	Evidencia követelmény	**Nincs követelmény.**
	Tanúsító tennivalója	**Nincs tennivaló.**
Implementáció	**Tartalmi és formai követelmények**	**Az opcionális teszt dokumentációnak tartalmaznia kell tesztelési célokat, tervet, eljárásokat és az eredményeket. Opcionálisan átadhatók a teszt program könyvtárak és eszközök a tesztek megismételhetősége céljából.**
	Evidencia követelmény	**Az opcionális tesztdokumentációnak tükröznie kell, a védelmi célokban megfogalmazott védelmet megvalósító funkciók és a tesztek egymás közötti megfelelését.**
	Tanúsító tennivalója	**A védelmet megvalósító funkciók tesztelésével ellenőrizendő, hogy az MT megfelel-e a védelmi céloknak. További tesztek végzendők hibák felderítésére. A megbízó számára elvégzett teszteket nem kell megismételni, de ezen teszteredményeket**

Megvalósítás / Fejlesztési folyamat 7. táblázat		
		ellenőrizni kell.

Megvalósítás / Fejlesztési környezet 8. táblázat		
A tanúsítónak átadandó		**Az értékelésre átadott MT verzióját azonosító konfigurációs lista.**
Változás-menedzsment	**Tartalmi és formai követelmények**	**A konfigurációs listában pontosan meg kell jelölni az MT változat azonosítóját.**
	Evidencia követelmény	**A konfigurációs listában le kell írni az MT azonosítás módját.**
	Tanúsító tennivalója	**Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.**
Programozási nyelvek, fordítók	**Tartalmi és formai követelmények**	**Nincs követelmény.**
	Evidencia követelmény	**Nincs követelmény.**
	Tanúsító tennivalója	**Nincs tennivaló.**
Fejlesztők biztonsága	**Tartalmi és formai követelmények**	**Nincs követelmény.**
	Evidencia követelmény	**Nincs követelmény.**
	Tanúsító tennivalója	**Nincs tennivaló.**

Működés / Üzemeltetéshez szükséges dokumentáció 9. táblázat		
A tanúsítónak átadandó		**1. Felhasználói dokumentáció** **2. Adminisztrátori dokumentáció**
Felhasználói dokumentáció	**Tartalmi és formai követelmények**	**A végfelhasználó számára kijelentő jelleggel tartalmaznia kell a védelmet megvalósító funkcióknak, a biztonsági követelményeknek megfelelő kezelési leírását. Legyen világos felépítésű. Legyen összhangban a többi dokumentációval.**
	Evidencia követelmény	**Kijelentő jelleggel tartalmazza azt, hogy a végfelhasználó hogyan használja az MT a követelményeknek megfelelően.**
	Tanúsító tennivalója	**Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.**
Adminisztrátori dokumentáció	**Tartalmi és formai követelmények**	**Sorolja fel a védelmet megvalósító funkciókat, jelölje meg azokat, amelyeket az adminisztrátor beállíthat és azokat, amelyeket csak lekérdezhet. Sorolja fel az összes az adminisztratív funkciókhoz kapcsolódó és a biztonságot érintő esemény-típust. Írja le adminisztrátori munka biztonságát érint részleteket, hogyan használja hatékonyan és egyenszilárdságúan az adminisztrátor az MT funkcióit és hogyan hatnak azok egymásra. Tartalmazza az MT installálására és konfigurálására vonatkozó utasításokat. Legyen világos felépítésű. Legyen összhangban a többi dokumentációval.**
	Evidencia követelmény	**Kijelentő jelleggel mutassa be, hogy az MT üzemeltetése hogyan valósítható meg biztonságosan.**
	Tanúsító tennivalója	**Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.**

Működés / Működési környezet 10. táblázat		
A tanúsítónak átadandó		**1. Szállítási és konfigurálási dokumentáció** **2. Indítási és üzemeltetési dokumentáció**
Szállítás és konfigurálás	**Tartalmi és formai követelmények**	**Kijelentő jelleggel dokumentálandók a konfigurációs változatok - ha vannak ilyenek - biztonságot érintő hatásait, a szállítással és az installálással/generálással kapcsolatos eljárásokat.**
	Evidencia követelmény	**Kijelentő jelleggel mutassa be, hogy az eljárások hogyan valósíthatók meg biztonságosan.**
	Tanúsító tennivalója	**Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.**
Indítás, üzemeltetés	**Tartalmi és formai követelmények**	**Kijelentő jelleggel mutassa be a biztonságos indítás és üzemeltetés eljárásait.**
	Evidencia követelmény	**Kijelentő jelleggel mutassa be, hogy az eljárások, hogyan szolgálják a biztonságot.**
	Tanúsító tennivalója	**Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.**

3.1.2. E2 szint

Rövid jellemzés: az E1 szinthez további követelményként jelenik meg az MT részletes terveinek informális leírása. A funkcionális teszt egyértelműségét és meggyőző erejét (evidenciáját) értékelni kell. Ezen a szinten már követelmény a változás-menedzsment rendszer és az MT dokumentációinak szabályozott kezelési és hozzáférési rendszere.

Megvalósítás / Fejlesztési folyamat **11. táblázat**		
A tanúsítónak átadandó		1. Védelmi célok. 2. Az MT architektúrájának informális leírása. **1. Az MT részletes terv informális leírása.** **2. Teszt dokumentáció.** **3. Az MT teszteléséhez használt tesztprogramok könyvtárai és a teszteszközök.**
Követelmény-rendszer	**Tartalmi és formai követelmények**	A védelmi célok dokumentációjának kijelentő jelleggel tartalmaznia kell: 1. az MT védelmet megvalósító funkciónak felsorolását, 2. az Informatikai Biztonságpolitikát (rendszer esetén), a Termék Besorolási Ismertetőt (termék esetén), amelyek azonosítják az MT-vel kapcsolatos védelmi célokat és veszélyeket, 3. a védelmet megvalósító funkciók informális specifikációját.
	Evidencia követelmény	A védelmi célok dokumentációja kijelentő jelleggel tartalmazza, hogy rendszer esetén a valós, termék esetén a feltételezett fenyegetések ellen a védelmi funkciók hogyan fejtenek ki ellenhatást, valamint azt, hogy hogyan felelnek meg a védelmi igényeknek.
	Tanúsító tennivalója	Ellenőrizendők a dokumentációk megfelelése tartalmi és formai szempontból, valamint a védelmi cél dokumentáció ellentmondásmentes és teljes körű volta.
Rendszerterv	**Tartalmi és formai követelmények**	A rendszerterv kijelentés szinten tartalmazza: 1. az MT architektúráját rendszer szinten, 2. a külső interfészeket, 3. a hardverben és/vagy firmware-ben implementált védelmi funkciók megnevezését, **4. az MT védelmet megvalósító és egyéb funkciói szétválasztását.**
	Evidencia követelmény	Állapítsa meg, hogy a védelmet megvalósító funkciók, hogyan felelnek meg a védelmi céloknak **és hogyan kerülnek szétválasztásra a védelmet megvalósító és az egyéb funkciók.**
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek-e a tartalmi, formai és evidencia követelményeknek, **valamint, hogy a védelmet megvalósító és az egyéb funkciók szétválasztása mennyire teljesült.**

Megvalósítás / Fejlesztési folyamat 11. táblázat		
Részletes terv	**Tartalmi és formai követelmények**	**Mutassa be kijelentő jelleggel a védelmet megvalósító és a védelmet támogató funkciók kialakítását. Azonosítsa a védelmi mechanizmusokat. A védelmet megvalósító funkciókat le kell képezni a védelmi mechanizmusokra és komponensekre. Dokumentálni kell a védelmet megvalósító és a védelmet támogató komponensek célját és paramétereit, a mechanizmusok definícióit és specifikációját. A specifikációnak alkalmasnak kell lenni a mechanizmusok közötti kölcsönhatások megítélésére. Ahol több szintű a specifikáció, ott a hierarchia szintek közötti kapcsolatokat világosan le kell írni. A nem védelmi célú komponensek specifikációja nem kell.**
	Evidencia követelmény	**Dokumentálni kell kijelentések szintjén, hogy a védelmi mechanizmusok hogyan biztosítják a védelmi célok dokumentációjában specifikált védelmet megvalósító funkciók működését. Kijelentések szintjén legyen megállapítható, hogy azok a komponensek, amelyekre a tervben nincs tervezési információ, nincsenek kapcsolatban sem a védelmet megvalósító, sem a védelmet támogató funkciókkal.**
	Tanúsító tennivalója	**Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.**
Implementáció	**Tartalmi és formai követelmények**	**A kötelező jelleggel átadott** teszt dokumentációnak tartalmaznia kell tesztelési célokat, tervet, eljárásokat és az eredményeket. Az teszt program könyvtárakat és eszközöket **át kell adni** a tesztek megismételhetősége céljából.
	Evidencia követelmény	**A kötelező jelleggel átadott** tesztdokumentációnak tükröznie kell, a védelmi célokban megfogalmazott védelmet megvalósító funkciók és a tesztek egymás közötti megfelelését.
	Tanúsító tennivalója	**Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Az átadott tesztprogramokkal ellenőrizni kell az átadott teszteredményeket.** További tesztek végzendők hibák felderítésére.

Megvalósítás / Fejlesztési környezet **12. táblázat**		
A tanúsítónak átadandó		1. Az értékelésre átadott MT verzióját azonosító konfigurációs lista. **2. A változás-menedzsment rendszerre vonatkozó információk.** **3. A fejlesztési környezet biztonságára vonatkozó információk.**
Változás-menedzsment	**Tartalmi és formai követelmények**	**A fejlesztési folyamatot változás-menedzsment rendszerrel kell támogatni. A konfigurációs listában benne kell lennie az összes olyan komponensek, amelyet az MT-be beépítettek. Az MT-nek, az összes alap-komponensnek és az összes dokumentációnak - beleértve a kézikönyveket is - egyértelmű azonosítóval kell rendelkezniük. Minden dokumentumban csak ezekre lehet hivatkozni. A változás-menedzsment rendszernek biztosítania kell, hogy a minősítésre átadott MT-nek és a dokumentációnak egyértelműen meg kell felelnie egymásnak és abban csak jóváhagyott változtatások történhetnek.**
	Evidencia követelmény	**Az átadott dokumentációnak kijelentő jelleggel ismertetnie kell, hogy hogyan használják a változás-menedzsment rendszert a gyakorlatban és hogyan alkalmazzák a fejlesztésben/gyártásban, összhangban a fejlesztő/gyártó minőségbiztosító követelményrendszerével.**
	Tanúsító tennivalója	Ellenőrizendők **a dokumentált eljárások**, valamint, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.
Programozási nyelvek, fordítók	**Tartalmi és formai követelmények**	Nincs követelmény.
	Evidencia követelmény	Nincs követelmény.
	Tanúsító tennivalója	Nincs tennivaló.
Fejlesztők biztonsága	**Tartalmi és formai követelmények**	**A fejlesztési környezetről szóló dokumentumnak kijelentő jelleggel be kell mutatnia az MT integritása és a kapcsolódó dokumentáció bizalmasságának fizikai, szabályozási, személyes vagy más eszközökkel megvalósított védelmét.**
	Evidencia követelmény	**A fejlesztési környezetről szóló dokumentumnak kijelentő jelleggel be kell mutatnia, hogy az MT integritása és a kapcsolódó dokumentáció bizalmasságának védelme hogyan valósul meg.**
	Tanúsító tennivalója	**Ellenőrizendők a dokumentált eljárások, valamint, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Tesztek végzendők az eljárásokban levő hibák felderítésére.**

Működés / Üzemeltetéshez szükséges dokumentáció **13. táblázat**		
A tanúsítónak átadandó		1. Felhasználói dokumentáció 2. Adminisztrátori dokumentáció
Felhasználói dokumentáció	**Tartalmi és formai követelmények**	A végfelhasználó számára kijelentő jelleggel tartalmaznia kell a védelmet megvalósító funkcióknak a biztonsági követelményeknek megfelelő kezelési leírását. Legyen világos felépítésű. Legyen összhangban a többi dokumentációval.
	Evidencia követelmény	Kijelentő jelleggel tartalmazza azt, hogy a végfelhasználó hogyan használja az MT a követelményeknek megfelelően.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.
Adminisztrátori dokumentáció	**Tartalmi és formai követelmények**	Sorolja fel a védelmet megvalósító funkciókat, jelölje meg azokat, amelyeket az adminisztrátor beállíthat és azokat, amelyeket csak lekérdezhet. Sorolja fel az összes az adminisztratív funkciókhoz kapcsolódó és a biztonságot érintő esemény-típust. Írja le adminisztrátori munka biztonságát érintő részleteket, hogyan használja hatékonyan és egyenszilárdságúan az adminisztrátor az MT funkcióit és hogyan hatnak azok egymásra. Tartalmazza az MT installálására és konfigurálására vonatkozó utasításokat. Legyen világos felépítésű. Legyen összhangban a többi dokumentációval.
	Evidencia követelmény	Kijelentő jelleggel mutassa be, hogy az MT üzemeltetése hogyan valósítható meg biztonságosan.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.

Működés / Működési környezet 14. táblázat		
A tanúsítónak átadandó		1. Szállítási és konfigurálási dokumentáció 2. Indítási és üzemeltetési dokumentáció
Szállítás és konfigurálás	**Tartalmi és formai követelmények**	Kijelentő jelleggel dokumentálandók a konfigurációs változatok - ha vannak ilyenek - biztonságot érintő hatásai, a szállítással és az installálással/generálással kapcsolatos eljárások. **A minősítő által jóváhagyott eljárással ellenőrizni kell, hogy hiteles-e és a megrendelttel azonos-e az MT. Az MT installációja/generálása során a paramétereket, változtatásokat úgy kell naplózni (audit trail), hogy utólagosan is rekonstruálni lehessen mikor és hogyan lett installálva/generálva az MT.**
	Evidencia követelmény	Kijelenő jelleggel mutassa be, hogy az eljárások hogyan valósíthatók meg biztonságosan.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. **Ellenőrizendők a szállítási előírások korrekt betartása. Tesztek végzendők az installációs/generálási eljárásokban levő hibák felderítésére.**
Indítás, üzemeltetés	**Tartalmi és formai követelmények**	Kijelenő jelleggel mutassa be a biztonságos indítás és üzemeltetés eljárásait. **Fel kell tüntetni, ha az indítás, az üzemeltetés vagy a karbantartás alatt a védelmet megvalósító funkció hatástalanítható vagy módosítható. Ha az MT védelmet megvalósító hardver komponenst tartalmaz olyan, az adminisztrátor, a végfelhasználó által vagy automatikusan indítható tesztrendszerrel kell rendelkezni, amellyel az MT tesztje üzemelés közben elvégezhető.**
	Evidencia követelmény	Kijelenő jelleggel mutassa be, hogy az eljárások, hogyan szolgálják a biztonságot. **A megbízónak át kell adnia a védelmet megvalósító hardver komponensekre vonatkozó összes diagnosztikai tesztеredményt, valamint az indítás és az üzemelés során készült biztonsági naplókat.**
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. **Az indítás és az üzemeltetésre vonatkozó naplókat ellenőrizni kell. Tesztek végzendők az eljárásokban levő hibák felderítésére.**

3.1.3. E3 szint

Rövid jellemzés: az E2 szinthez további követelményként jelenik meg, hogy a biztonsági mechanizmusokat tükröző forráskódot és/vagy hardver-rajzokat értékelni kell. A védelmi mechanizmusok tesztelésének evidenciáját értékelni kell.

Megvalósítás / Fejlesztési folyamat **15. táblázat**		
A tanúsítónak átadandó		1. Védelmi célok. 2. Az MT architektúrájának informális leírása. 3. Az MT részletes terv informális leírása. 4. Teszt dokumentáció. 5. Az MT teszteléséhez használt tesztprogramok könyvtárai és a teszteszközök. **1. Az összes védelmet megvalósító és segítő komponens forráskódja és/vagy hardver-rajza.** **2. A forráskód vagy a hardver-rajz valamint a részletes terv közötti összefüggések informális leírása.**
Követelmény-rendszer	**Tartalmi és formai követelmények**	A védelmi célok dokumentációjának **leíró** jelleggel tartalmaznia kell: 1. az MT védelmet megvalósító funkcióit, 2. az Informatikai Biztonságpolitikát (rendszer esetén), a Termék Besorolási Ismertetőt (termék esetén), amelyek azonosítják az MT-vel kapcsolatos védelmi célokat és veszélyeket, 3. a védelmet megvalósító funkciók informális leírását.
	Evidencia követelmény	A védelmi célok dokumentációja **leíró** jelleggel tartalmazza, hogy rendszer esetén a valós, termék esetén a feltételezett fenyegetések ellen a védelmi funkciók hogyan fejtenek ki ellenhatást, valamint azt, hogy hogyan felelnek meg a védelmi igényeknek.
	Tanúsító tennivalója	Ellenőrizendők a dokumentációk megfelelése tartalmi és formai szempontból, valamint a védelmi cél dokumentáció ellentmondásmentes és teljes körű volta.
Rendszerterv	**Tartalmi és formai követelmények**	A rendszerterv **leíró jelleggel** tartalmazza: 1. az MT architektúráját rendszer szinten, 2. a külső interfészeket, 3. a hardverben és/vagy firmware-ben implementált védelmi funkciók megnevezését, 4. az MT védelmet megvalósító és egyéb funkciói szétválasztását.
	Evidencia követelmény	**Leíró jelleggel** mutassa be, hogy a védelmet megvalósító funkciók, hogyan felelnek meg a védelmi céloknak és hogyan kerülnek szétválasztásra a védelmet megvalósító és az egyéb funkciók.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek-e a tartalmi, formai és evidencia követelményeknek, valamint, hogy a védelmet megvalósító és az egyéb funkciók szétválasztása mennyire teljesült.

Megvalósítás / Fejlesztési folyamat 15. táblázat		
Részletes terv	**Tartalmi és formai követelmények**	**Specifikálja az összes alap-komponenst.** Mutassa be **leíró jelleggel** a védelmet megvalósító és a védelmet támogató funkciók kialakítását. Azonosítsa a védelmi mechanizmusokat. A védelmet megvalósító funkciókat le kell képezni a védelmi mechanizmusokra és komponensekre. Dokumentálni kell a védelmet megvalósító és a védelmet támogató komponensek célját és paramétereit, a mechanizmusok definícióit és specifikációját. A specifikációnak alkalmasnak kell lenni a mechanizmusok közötti kölcsönhatások megítélésére. Ahol több szintű a specifikáció, ott a hierarchia szintek közötti kapcsolatokat világosan le kell írni. A nem védelmi célú komponensek specifikációja nem kell.
	Evidencia követelmény	**Leíró jelleggel** dokumentálni kell, hogy a védelmi mechanizmusok hogyan biztosítják a védelmi célok dokumentációjában specifikált védelmet megvalósító funkciók működését. Legyen egyértelműen megállapítható, hogy azok a komponensek, amelyekre a tervben nincs tervezési információ, nincsenek kapcsolatban sem a védelmet megvalósító, sem a védelmet támogató funkciókkal.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.
Implementáció	**Tartalmi és formai követelmények**	**Leíró jelleggel be kell mutatni a forráskód vagy a hardver-rajz valamint az alap-komponensek közötti összefüggéseket.** A kötelező jelleggel átadott teszt dokumentációnak tartalmaznia kell tesztelési célokat, tervet, eljárásokat és az eredményeket. Az teszt program könyvtárakat és eszközöket át kell adni a tesztek megismételhetősége céljából.
	Evidencia követelmény	A kötelező jelleggel átadott tesztdokumentációnak tükröznie kell, a védelmi célokban megfogalmazott védelmet megvalósító funkciók és a tesztek egymás közötti megfelelését. **Leíró jelleggel be kell mutatni a részletes tervben szereplő, védelmet megvalósító és a védelmet támogató funkciók, valamint a tesztek közötti összefüggéseket. Leíró jelleggel be kell mutatni a forráskódban vagy a hardver-rajzokban kialakított védelmi mechanizmusok, valamint a tesztek közötti összefüggéseket. Lényeges a biztonság szempontjából, hogy a hibák felfedése és korrekciója után újbóli tesztekkel kell bizonyítani a hibák kijavítását, illetve, hogy újabb hibák nem lettek bevíve.**
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Az átadott tesztprogramokkal ellenőrizni kell az átadott teszteredményeket. **Ellenőrizendő, hogy a tesztek lefedik-e a részletes tervben szereplő, védelmet megvalósító és a védelmet támogató funkciók, valamint a forráskódban vagy a hardver-rajzokban kialakított védelmi mechanizmusok mindegyikét.** További tesztek végzendők hibák felderítésére.

Megvalósítás / Fejlesztési környezet 16. táblázat		
A tanúsítónak átadandó		1. Az értékelésre átadott MT verzióját azonosító konfigurációs lista. 2. A változás-menedzsment rendszerre vonatkozó információk. **1. Információk az átadás-átvételi eljárásokról.** 2. A fejlesztési környezet biztonságára vonatkozó információk. **3. A fejlesztő nyelvek leírása.**
Változás-menedzsment	**Tartalmi és formai követelmények**	A fejlesztési folyamatot változás-menedzsment rendszerrel **és átadás-átvételi eljárás(ok)kal** kell támogatni. A konfigurációs listában benne kell lennie az összes olyan komponensek, amelyet az MT-be beépítettek. Az MT-nek, az összes alap-komponensnek és az összes dokumentációnak - beleértve a kézikönyveket is -, **a forráskódoknak és/vagy a hardver-rajzoknak** egyértelmű azonosítóval kell rendelkezniük. Minden dokumentumban csak ezekre lehet hivatkozni. A változás-menedzsment rendszernek biztosítania kell, hogy a minősítésre átadott MT-nek és a dokumentációnak egyértelműen meg kell felelnie egymásnak.
	Evidencia követelmény	Az átadott dokumentációnak **leíró jelleggel** ismertetnie kell, hogy hogyan használják a változás-menedzsment rendszert a gyakorlatban és hogyan alkalmazzák a fejlesztésben/gyártásban, összhangban a fejlesztő/gyártó minőségbiztosító követelményrendszerével.
	Tanúsító tennivalója	Ellenőrizendők a dokumentált eljárások, valamint, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.
Programozási nyelvek, fordítók	**Tartalmi és formai követelmények**	**Bármely fejlesztésre használt programnyelvnek jól definiáltnak kell lennie, pl. meg kell felelnie az ISO szabványnak. Bármely, a fejlesztéssel kapcsolatos nyelvi sajátosságot dokumentálni kell.**
	Evidencia követelmény	**A programnyelvnek egyértelműen és ellentmondásmentesen kell definiálni a forráskódban használt összes utasítás tartalmát.**
	Tanúsító tennivalója	**Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.**
Fejlesztők biztonsága	**Tar almi és formai követelmények**	A fejlesztési környezetről szóló dokumentumnak **leíró jelleggel** be kell mutatnia az MT integritása és a kapcsolódó dokumentáció bizalmasságának fizikai, szabályozási, személyes vagy más eszközökkel megvalósított védelmét.
	Evidencia követelmény	A fejlesztési környezetről szóló dokumentumnak **leíró jelleggel** be kell mutatnia, hogy az MT integritása és a kapcsolódó dokumentáció bizalmasságának védelme hogyan valósul meg.
	Tanúsító tennivalója	Ellenőrizendők a dokumentált eljárások, valamint, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Tesztek végzendők az eljárásokban levő hibák felderítésére.

Működés / Üzemeltetéshez szükséges dokumentáció **17. táblázat**		
A tanúsítónak átadandó		1. Felhasználói dokumentáció 2. Adminisztrátori dokumentáció
Felhasználói dokumentáció	**Tartalmi és formai követelmények**	A végfelhasználó számára **leíró jelleggel** tartalmaznia kell a védelmet megvalósító funkcióknak a biztonsági követelményeknek megfelelő kezelési leírását. Legyen világos felépítésű. Legyen összhangban a többi dokumentációval.
	Evidencia követelmény	**Leíró jelleggel** tartalmazza azt, hogy a végfelhasználó hogyan használja az MT a követelményeknek megfelelően.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.
Adminisztrátori dokumentáció	**Tartalmi és formai követelmények**	**Írja le** a védelmet megvalósító funkciókat, jelölje meg azokat, amelyeket az adminisztrátor beállíthat és azokat, amelyeket csak lekérdezhet. **Írja le** az összes az adminisztratív funkciókhoz kapcsolódó és a biztonságot érintő esemény-típust. **Írja le** adminisztrátori munka biztonságát érintő részleteket, hogyan használja hatékonyan és egyenszilárdságúan az adminisztrátor az MT funkcióit és hogyan hatnak azok egymásra. **Írja le** az MT installálására és konfigurálására vonatkozó utasításokat. Legyen világos felépítésű. Legyen összhangban a többi dokumentációval.
	Evidencia követelmény	**Írja le**, hogy az MT üzemeltetése hogyan valósítható meg biztonságosan.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.

Működés / Működési környezet **18. táblázat**		
A tanúsítónak átadandó		1. Szállítási és konfigurálási dokumentáció 2. Indítási és üzemeltetési dokumentáció
Szállítás és konfigurálás	**Tartalmi és formai követelmények**	**Írja le** a konfigurációs változatok - ha vannak ilyenek - biztonságot érintő hatásait, a szállítással és az installálással/generálással kapcsolatos eljárásokat. A minősítő által jóváhagyott eljárással ellenőrizni kell, hogy hiteles és a megrendelttel azonos-e az MT. Az MT installációja/generálása során a paramétereket, változtatásokat úgy kell naplózni (audit trail), hogy utólagosan is rekonstruálni lehessen mikor és hogyan lett installálva/generálva az MT.
	Evidencia követelmény	**Írja le**, hogy az eljárások hogyan valósíthatók meg biztonságosan.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Ellenőrizendők a szállítási előírások korrekt betartása. Tesztek végzendők az installációs/generálási eljárásokban levő hibák felderítésére.
Indítás, üzemeltetés	**Tartalmi és formai követelmények**	**Írja le** a biztonságos indítás és üzemeltetés eljárásait. Fel kell tüntetni, ha az indítás, az üzemeltetés vagy a karbantartás alatt védelmet megvalósító funkció hatástalanítható vagy módosítható. Ha az MT védelmet megvalósító hardver komponenst tartalmaz olyan, az adminisztrátor, a végfelhasználó által vagy automatikusan indítható tesztrendszerrel kell rendelkezni, amellyel az MT tesztje üzemelés közben elvégezhető.
	Evidencia követelmény	**Írja le**, hogy az eljárások, hogyan szolgálják a biztonságot. A megbízónak át kell adnia a védelmet megvalósító hardver komponensekre vonatkozó összes diagnosztikai teszteredményt, valamint az indítás és az üzemelés során készült biztonsági naplókat.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Az indítás és az üzemeltetésre vonatkozó naplókat ellenőrizni kell. Tesztek végzendők az eljárásokban levő hibák felderítésére.

3.1.4. E4 szint

Rövid jellemzés: az E3 szinthez további követelményként jelenik meg, hogy a védelmi célokat alátámasztó biztonsági politika formális leírásának szolgáltatása. A védelmet megvalósító funkciók, a rendszerterv és a részletes tervek szemiformális leírása követelmény.

Megvalósítás / Fejlesztési folyamat **19. táblázat**		
A tanúsítónak átadandó		1. Védelmi célok. **1. Egy alátámasztó, formálisan specifikált biztonsági politika modell definiálűálása vagy hivatkozás.** **2. A modell informális leírása a védelmi cél dokumentumban.** 3. Az MT architektúrájának **szemiformális** leírása. 4. Az MT részletes terv **szemiformális** leírása. 5. Teszt dokumentáció. 6. Az MT teszteléséhez használt tesztprogramok könyvtárai és a teszteszközök. 7. Az összes védelmet megvalósító és segítő komponens forráskódja és/vagy hardver-rajza. 8. A forráskód vagy a hardver-rajz valamint a részletes terv közötti összefüggések informális leírása.
Követelmény-rendszer	**Tartalmi és formai követelmények**	A védelmi célok dokumentációjának leíró jelleggel tartalmaznia kell: 1. az MT védelmet megvalósító funkcióit, 2. az Informatikai Biztonságpolitikát (rendszer esetén), a Termék Besorolási Ismertetőt (termék esetén), amelyek azonosítják az MT-vel kapcsolatos védelmi célokat és veszélyeket,, **3. egy formális biztonsági politika modellt vagy hivatkozni kell rá, amellyel meghatározható az a biztonsági politika amelynek az MT-nek meg kell felelnie,** **4. a modell informális leírását a védelmi célok meghatározása keretében.** 5. a védelmet megvalósító funkciók informális **és szemiformális** leírását a védelmi célok meghatározása keretében.
	Evidencia követelmény	A védelmi célok dokumentációja leíró jelleggel tartalmazza, hogy rendszer esetén a valós, termék esetén a feltételezett fenyegetések ellen a védelmi funkciók hogyan fejtenek ki ellenhatást, valamint azt, hogy hogyan felelnek meg a védelmi igényeknek. **A formális biztonsági politika modell informális leírása be kell, hogy mutassa hogyan felelnek meg a védelmi célok a biztonsági politikának.**
	Tanúsító tennivalója	Ellenőrizendők a dokumentációk megfelelése tartalmi és formai szempontból, valamint a védelmi cél dokumentáció ellentmondásmentes és teljes körű volta. **Ellenőrizendő, hogy a védelmi célok között nincs-e olyan védelmi jellemző, amely ellentmondana a**

Megvalósítás / Fejlesztési folyamat 19. táblázat		
		biztonsági politikának.
Rendszerterv	**Tartalmi és formai követelmények**	**A rendszertervben szemiformális ábrázolásmódot kell alkalmazni, hogy kialakítható legyen a szemiformális leírás.** A rendszerterv leíró jelleggel tartalmazza: 1. az MT architektúráját rendszer szinten, 2. a külső interfészeket, 3. a hardverben és/vagy firmware-ben implementált védelmi funkciók megnevezését, 4. az MT védelmet megvalósító és egyéb funkciói szétválasztását.
	Evidencia követelmény	Leíró jelleggel mutassa be, hogy a védelmet megvalósító funkciók, hogyan felelnek meg a védelmi céloknak és hogyan kerülnek szétválasztásra a védelmet megvalósító és az egyéb funkciók. **Le kell írni, hogy a választott leíró struktúra hogyan fogja össze a független, védelmet megvalósító komponenseket.**
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek-e a tartalmi, formai és evidencia követelményeknek, valamint, hogy a védelmet megvalósító és az egyéb funkciók szétválasztása mennyire teljesült.
Részletes terv	**Tartalmi és formai követelmények**	**A szemiformális részletes terv kialakításához szemiformális ábrázolásmódot kell bevezetni.** Specifikálja az összes alapkomponenst. **A tervezés összes hierarchia szintjén le kell írni, hogy a védelmet megvalósító és a támogató funkciók hogyan valósulnak meg. Leírandó az MT védelmet megvalósító, védelmet támogató és egyéb komponenseinek szétválasztása. Ezeket jól definiált, lehetőleg független alap-komponensek olyan rendszerébe kell struktúrálni, amely tesztelési lehetőségekkel bír, hogy a biztonság potenciális megsértésének lehetősége minimalizálva legyen.** Mutassa be leíró jelleggel a védelmet megvalósító és a védelmet támogató funkciók kialakítását. Azonosítsa a védelmi mechanizmusokat. A védelmet megvalósító funkciókat le kell képezni a védelmi mechanizmusokra és komponensekre. Dokumentálni kell a védelmet megvalósító és a védelmet támogató komponensek célját és paramétereit, a mechanizmusok definícióit és specifikációját. A specifikációnak alkalmasnak kell lenni a mechanizmusok közötti kölcsönhatások megítélésére. Ahol több szintű a specifikáció, ott a hierarchia szintek közötti kapcsolatokat világosan le kell írni. A nem védelmi célú komponensek specifikációja nem kell.
	Evidencia követelmény	Leíró jelleggel dokumentálni kell, hogy a védelmi mechanizmusok hogyan biztosítják a védelmi célok dokumentációjában specifikált védelmet megvalósító funkciók működését. Legyen egyértelműen megállapítható, hogy azok a komponensek, amelyekre a tervben nincs tervezési információ, nincsenek kapcsolatban sem a védelmet megvalósító, sem a védelmet támogató funkciókkal.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.

Megvalósítás / Fejlesztési folyamat 19. táblázat		
Implementáció	**Tartalmi és formai követelmények**	Leíró jelleggel be kell mutatni a forráskód vagy a hardver-rajz valamint az alap-komponensek közötti összefüggéseket. A kötelező jelleggel átadott teszt dokumentációnak tartalmaznia kell tesztelési célokat, tervet, eljárásokat és az eredményeket, **valamint egy értékelést arról, hogy a tesztelés lefedettsége miért megfelelő.** Az teszt program könyvtárakat és eszközöket át kell adni a tesztek megismételhetősége céljából.
	Evidencia követelmény	A kötelező jelleggel átadott tesztdokumentációnak tükröznie kell, a védelmi célokban megfogalmazott védelmet megvalósító funkciók és a tesztek egymás közötti megfelelését. Leíró jelleggel be kell mutatni a részletes tervben szereplő, védelmet megvalósító és a védelmet támogató funkciók, valamint a tesztek közötti összefüggéseket. Leíró jelleggel be kell mutatni a forráskódban vagy a hardver-rajzokban kialakított védelmi mechanizmusok, valamint a tesztek közötti összefüggéseket. Lényeges a biztonság szempontjából, hogy a hibák felfedése és korrekciója után újbóli tesztekkel kell bizonyítani a hibák kijavítását, illetve, hogy újabb hibák nem lettek bevíve.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Az átadott tesztprogramokkal ellenőrizni kell az átadott teszteredményeket. Ellenőrizendő, hogy a tesztek lefedik-e a részletes tervben szereplő, védelmet megvalósító és a védelmet támogató funkciók, valamint a forráskódban vagy a hardver-rajzokban kialakított védelmi mechanizmusok mindegyikét. További tesztek végzendők hibák felderítésére.

Megvalósítás / Fejlesztési környezet 20. táblázat		
A tanúsítónak átadandó		1. Az értékelésre átadott MT verzióját azonosító konfigurációs lista. 2. A változás-menedzsment rendszerre vonatkozó információk. **1. Az MT változás-menedzsment alá eső összes komponensének módosításával kapcsolatos audit dokumentum..** 2. Információk az átadás-átvételi eljárásokról. 3. A fejlesztési környezet biztonságára vonatkozó információk. 4. A fejlesztő nyelvek leírása.
Változás-menedzsment	**Tartalmi és formai követelmények**	A fejlesztési folyamatot változás-menedzsment rendszerrel és átadás-átvételi eljárás(ok)kal kell támogatni. A konfigurációs listában benne kell lennie az összes olyan komponensek, amelyet az MT-be beépítettek. Az MT-nek, az összes alap-komponensnek és az összes dokumentációnak - beleértve a kézikönyveket is -, a forráskódoknak és/vagy a hardver-rajzoknak egyértelmű azonosítóval kell rendelkezniük. Minden dokumentumban csak ezekre lehet hivatkozni. A változás-menedzsment rendszernek biztosítania kell, hogy a minősítésre átadott MT-nek és a dokumentációnak egyértelműen meg kell felelnie egymásnak és abban csak jóváhagyott változtatások történhetnek **feljogosított személy által. A változás-menedzsmentet támogató eszközrendszernek ellenőrizni és rögzítenie kell a változásokat a változás-menedzsment alá eső objektumok különböző verziói között.**
	Evidencia követelmény	Az átadott dokumentációnak leíró jelleggel ismertetnie kell, hogy hogyan használják a változás-menedzsment rendszert a gyakorlatban és hogyan alkalmazzák a fejlesztésben/gyártásban, összhangban a fejlesztő/gyártó minőségbiztosító követelményrendszerével.
	Tanúsító tennivalója	Ellenőrizendők a dokumentált eljárások, valamint, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. **A fejlesztő eszközeit fel kell használni az MT kiválasztott részeinek újraépítésére és össze kell hasonlítani az átadott MT-vel.**
Programozási nyelvek, fordítók	**Tartalmi és formai követelmények**	Bármely fejlesztésre használt programnyelvnek jól definiáltnak kell lennie, pl. meg kell felelnie az ISO szabványnak. Bármely, a fejlesztéssel kapcsolatos nyelvi sajátosságot dokumentálni kell. **A fordítónak a fejlesztéssel kapcsolatos bármely sajátosságát dokumentálni kell.**
	Evidencia követelmény	A programnyelvnek egyértelműen és ellentmondásmentesen kell definiálni a forráskódban használt összes utasítás tartalmát.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.
Fejlesztők biztonsága	**Tartalmi és formai követelmények**	A fejlesztési környezetről szóló dokumentumnak leíró jelleggel be kell mutatnia az MT integritása és a kapcsolódó dokumentáció bizalmasságának fizikai, szabályozási, személyes vagy más eszközökkel megvalósított védelmét.
	Evidencia követelmény	A fejlesztési környezetről szóló dokumentumnak leíró jelleggel be kell mutatnia, hogy az MT integritása és a kapcsolódó dokumentáció bizalmasságának védelme hogyan valósul meg.
	Tanúsító tennivalója	Ellenőrizendők a dokumentált eljárások, valamint, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Tesztek végzendők az eljárásokban levő hibák felderítésére.

Működés / Üzemeltetéshez szükséges dokumentáció **21. táblázat**		
A tanúsítónak átadandó		1. Felhasználói dokumentáció 2. Adminisztrátori dokumentáció
Felhasználói dokumentáció	**Tartalmi és formai követelmények**	A végfelhasználó számára leíró jelleggel tartalmaznia kell a védelmet megvalósító funkcióknak a biztonsági követelményeknek megfelelő kezelési leírását. Legyen világos felépítésű. Legyen összhangban a többi dokumentációval.
	Evidencia követelmény	Leíró jelleggel tartalmazza azt, hogy a végfelhasználó hogyan használja az MT a követelményeknek megfelelően.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.
Adminisztrátori dokumentáció	**Tartalmi és formai követelmények**	Írja le a védelmet megvalósító funkciókat, jelölje meg azokat, amelyeket az adminisztrátor beállíthat és azokat, amelyeket csak lekérdezhet. Írja le az összes az adminisztratív funkciókhoz kapcsolódó és a biztonságot érintő esemény-típust. Írja le adminisztrátori munka biztonságát érintő részleteket, hogyan használja hatékonyan és egyenszilárdságúan az adminisztrátor az MT funkcióit és hogyan hatnak azok egymásra. Írja le az MT installálására és konfigurálására vonatkozó utasításokat. Legyen világos felépítésű. Legyen összhangban a többi dokumentációval.
	Evidencia követelmény	Írja le, hogy az MT üzemeltetése hogyan valósítható meg biztonságosan.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.

Működés / Működési környezet 22. táblázat		
A tanúsítónak átadandó		1. Szállítási és konfigurálási dokumentáció 2. Indítási és üzemeltetési dokumentáció
Szállítás és konfigurálás	**Tartalmi és formai követelmények**	Írja le a konfigurációs változatok - ha vannak ilyenek - biztonságot érintő hatásait, a szállítással és az installálással/generálással kapcsolatos eljárásokat. A minősítő által jóváhagyott eljárással ellenőrizni kell, hogy hiteles és a megrendelttel azonos-e az MT. Az MT installációja/generálása során a paramétereket, változtatásokat úgy kell naplózni (audit trail), hogy utólagosan is rekonstruálni lehessen mikor és hogyan lett installálva/generálva az MT.
	Evidencia követelmény	Írja le, hogy az eljárások hogyan valósíthatók meg biztonságosan.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Ellenőrizendők a szállítási előírások korrekt betartása. Tesztek végzendők az installációs/generálási eljárásokban levő hibák felderítésére.
Indítás, üzemeltetés	**Tartalmi és formai követelmények**	Írja le a biztonságos indítás és üzemeltetés eljárásait. Fel kell tüntetni, ha az indítás, az üzemeltetés vagy a karbantartás alatt a védelmet megvalósító funkció hatástalanítható vagy módosítható. **Olyan eljárásnak kell léteznie, amely biztosítja az MT biztonságos állapotba történő visszaállítását kiesés vagy hardver/szoftver hiba után.** Ha az MT védelmet megvalósító hardver komponenst tartalmaz olyan, az adminisztrátor, a végfelhasználó által vagy automatikusan indítható tesztrendszerrel kell rendelkezni, amellyel az MT tesztje üzemelés közben elvégezhető.
	Evidencia követelmény	Írja le, hogy az eljárások, hogyan szolgálják a biztonságot. A megbízónak át kell adnia a védelmet megvalósító hardver komponensekre vonatkozó összes diagnosztikai teszteredményt, valamint az indítás és az üzemelés során készült biztonsági naplókat.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Az indítás és az üzemeltetésre vonatkozó naplókat ellenőrizni kell. Tesztek végzendők az eljárásokban levő hibák felderítésére.

3.1.5. E5 szint

Rövid jellemzés: az E4 szinthez további követelményként jelenik meg, hogy a részletes terveknek, valamint a forráskódoknak és/vagy a hardver-rajzoknak meg kell felelniük egymásnak.

Megvalósítás / Fejlesztési folyamat **23. táblázat**		
A tanúsítónak átadandó		1. Védelmi célok. 2. Egy alátámasztó, formálisan specifikált biztonsági politika modell definiálása vagy hivatkozás. 3. A modell informális leírása a védelmi cél dokumentumban. 4. Az MT architektúrájának szemiformális leírása. 5. Az MT részletes terv szemiformális leírása. 6. Teszt dokumentáció. 7. Az MT teszteléséhez használt tesztprogramok könyvtárai és a teszteszközök. 8. Az összes védelmet megvalósító és segítő komponens forráskódja és/vagy hardver-rajza. 9. A forráskód vagy a hardver-rajz valamint a részletes terv közötti összefüggések informális leírása.
Követelmény-rendszer	**Tartalmi és formai követelmények**	A védelmi célok dokumentációjának **magyarázó és értékelő** jelleggel tartalmaznia kell: 1. az MT védelmet megvalósító funkcióit, 2. az Informatikai Biztonságpolitikát (rendszer esetén), a Termék Besorolási Ismertetőt (termék esetén), amelyek azonosítják az MT-vel kapcsolatos védelmi célokat és veszélyeket, 3. egy formális biztonsági politika modellt vagy hivatkozni kell rá, amellyel meghatározható az a biztonsági politika amelynek az MT-nek meg kell felelnie, 4. a modell informális leírását a védelmi célok meghatározása keretében. 5. a védelmet megvalósító funkciók informális és szemiformális leírását a védelmi célok meghatározása keretében.
	Evidencia követelmény	A védelmi célok dokumentációja **magyarázó és értékelő** jelleggel tartalmazza, hogy rendszer esetén a valós, termék esetén a feltételezett fenyegetések ellen a védelmi funkciók hogyan fejtenek ki ellenhatást, valamint azt, hogy hogyan felelnek meg a védelmi igényeknek. A formális biztonsági politika modell informális **magyarázata és értékelése** be kell, hogy mutassa hogyan felelnek meg a védelmi célok a biztonsági politikának.
	Tanúsító tennivalója	Ellenőrizendők a dokumentációk megfelelése tartalmi és formai szempontból, valamint a védelmi cél dokumentáció ellentmondásmentes és teljes körű volta. Ellenőrizendő, hogy a védelmi célok között nincs-e olyan védelmi jellemző, amely ellentmondana a biztonsági politikának.

Megvalósítás / Fejlesztési folyamat 23. táblázat		
Rendszerterv	**Tartalmi és formai követelmények**	A rendszertervben szemiformális ábrázolásmódot kell alkalmazni, hogy kialakítható legyen a szemiformális leírás. A rendszerterv **magyarázó és értékelő** tartalmazza: 1. az MT architektúráját rendszer szinten, 2. a külső interfészeket, 3. a hardverben és/vagy firmware-ben implementált védelmi funkciók megnevezését, 4. az MT védelmet megvalósító és egyéb funkciói szétválasztását, **5. a védelmet megvalósító komponensek közötti összefüggéseket.**
	Evidencia követelmény	**Magyarázó és értékelő** jelleggel mutassa be, hogy a védelmet megvalósító funkciók, hogyan felelnek meg a védelmi céloknak és hogyan kerülnek szétválasztásra a védelmet megvalósító és az egyéb funkciók. **Meg kell magyarázni és értékelni kell,** hogy a választott leíró struktúra hogyan biztosítja a függetlenséget a védelmet megvalósító komponensek között. **Megmagyarázandó és értékelendő, hogy miért szükségesek a - létezésük esetén - a védelmet megvalósító komponensek közötti kapcsolatok.**
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek-e a tartalmi, formai és evidencia követelményeknek, valamint, hogy a védelmet megvalósító és az egyéb funkciók szétválasztása mennyire teljesült.

Megvalósítás / Fejlesztési folyamat 23. táblázat		
Részletes terv	**Tartalmi és formai követelmények**	A szemiformális részletes terv kialakításához szemiformális ábrázolásmódot kell bevezetni. Specifikálja az összes alap-komponenst. A tervezés összes hierarchia szintjén **meg kell magyarázni és értékelni kell,** hogy a védelmet megvalósító és a támogató funkciók hogyan valósulnak meg. **Megmagyarázandó és értékelendő** az MT védelmet megvalósító, védelmet támogató és egyéb komponenseinek szétválasztása. Ezeket jól definiált, lehetőleg független alap-komponensek olyan rendszerébe kell strukturálni, amely tesztelési lehetőségekkel bír, hogy a biztonság potenciális megsértésének lehetősége minimalizálva legyen. **Ebben alkalmazni kell szintekre bontást, az absztrakciót, és az adatrejtést.** Mutassa be **magyarázó és értékelő** jelleggel a védelmet megvalósító és a védelmet támogató funkciók kialakítását. Azonosítsa a védelmi mechanizmusokat. A védelmet megvalósító funkciókat le kell képezni a védelmi mechanizmusokra és **funkcionális egységekre**. **A védelmet megvalósító és a védelmet támogató funkciók esetében szükségtelen funkcionalitásokat ki kell zárni.** Dokumentálni kell a védelmet megvalósító, valamint a védelmet támogató komponensek célját és paramétereit, a mechanizmusok definícióit specifikációját és **hatásait**. **Megmagyarázandó az összes olyan változó szerepe, amelyet több funkcionális egység is használ.** A specifikációnak alkalmasnak kell lenni a mechanizmusok közötti kölcsönhatások megítélésére. Ahol több szintű a specifikáció, ott a hierarchia szintek közötti kapcsolatokat világosan le kell írni. A nem védelmi célú komponensek specifikációja nem kell.
	Evidencia követelmény	**Magyarázó és értékelő** jelleggel dokumentálni kell, hogy a védelmi mechanizmusok hogyan biztosítják a védelmi célok dokumentációjában specifikált védelmet megvalósító funkciók működését. **Megmagyarázandó, hogy a fennmaradó funkcionalitások miért nem zárhatók ki a védelmet megvalósító, illetve a védelmet támogató funkciókból.** Legyen egyértelműen megállapítható, hogy azok a komponensek, amelyekre a tervben nincs tervezési információ, nincsenek kapcsolatban sem a védelmet megvalósító, sem a védelmet támogató funkciókkal.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.

Megvalósítás / Fejlesztési folyamat 23. táblázat		
Implementáció	**Tartalmi és formai követelmények**	**A forráskódot és/vagy a hardver-rajzokat teljes mértékben kis, jól körülhatárolt szegmensekre kell bontani. Magyarázó és értékelő** jelleggel be kell mutatni a forráskód vagy a hardver-rajz valamint a **funkcionális egységek** közötti összefüggéseket. A kötelező jelleggel átadott teszt dokumentációnak tartalmaznia kell tesztelési célokat, tervet, eljárásokat és az eredményeket, valamint egy értékelést arról, hogy a tesztelés lefedettsége miért megfelelő**.** Az teszt program könyvtárakat és eszközöket át kell adni a tesztek megismételhetősége céljából.
	Evidencia követelmény	Az átadott tesztdokumentációnak **magyarázó és értékelő** jelleggel tükröznie kell, a védelmi célokban megfogalmazott védelmet megvalósító funkciók és a tesztek egymás közötti megfelelését **Magyarázó és értékelő** jelleggel be kell mutatni a részletes tervben szereplő, védelmet megvalósító és a védelmet támogató funkciók, valamint a tesztek közötti összefüggéseket. **Magyarázó és értékelő** jelleggel be kell mutatni a forráskódban vagy a hardver-rajzokban kialakított védelmi mechanizmusok, valamint a tesztek közötti összefüggéseket. Lényeges a biztonság szempontjából, hogy a hibák felfedése és korrekciója után újbóli tesztekkel kell bizonyítani a hibák kijavítását, illetve, hogy újabb hibák nem lettek bevíve.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Az átadott tesztprogramokkal ellenőrizni kell az átadott teszteredményeket. Ellenőrizendő, hogy a tesztek lefedik-e a részletes tervben szereplő, védelmet megvalósító és a védelmet támogató funkciók, valamint a forráskódban vagy a hardver-rajzokban kialakított védelmi mechanizmusok mindegyikét. További tesztek végzendők hibák felderítésére.

Megvalósítás / Fejlesztési környezet 24. táblázat	
A tanúsítónak átadandó	1. Az értékelésre átadott MT verzióját azonosító konfigurációs lista. 2. A változás-menedzsment rendszerre vonatkozó információk. 1. Az MT változás-menedzsment alá eső összes komponensének módosításával kapcsolatos audit dokumentum. **2. A rendszerintegrálással kapcsolatos információk.** 3. Információk az átadás-átvételi eljárásokról. 4. A fejlesztési környezet biztonságára vonatkozó információk. 5. A fejlesztő nyelvek leírása. **6. A használatba vett összes futási idejű könyvtár forráskódjai.**

Megvalósítás / Fejlesztési környezet 24. táblázat		
Változás-menedzsment	**Tartalmi és formai követelmények**	A fejlesztési folyamatot változás-menedzsment rendszerrel és átadás-átvételi eljárás(ok)kal kell támogatni. **A változás-menedzsmentet kezelő eszközrendszernek ellenőriznie kell, hogy egy fejlesztési objektum átvételéért felelős személy nem azonos-e annak tervezőivel vagy fejlesztőivel.** A konfigurációs listában benne kell lennie az összes olyan komponensek, amelyet az MT-be beépítettek. Az MT-nek, az összes alap-komponensnek és az összes dokumentációnak - beleértve a kézikönyveket is -, a forráskódoknak és/vagy a hardver-rajzoknak egyértelmű azonosítóval kell rendelkezniük. Minden dokumentumban csak ezekre lehet hivatkozni. A változás-menedzsment rendszernek biztosítania kell, hogy a minősítésre átadott MT-nek és a dokumentációnak egyértelműen meg kell felelnie egymásnak és abban csak jóváhagyott változtatások történhetnek feljogosított személy által. **Az átvételi eljáráson átmenő, a fejlesztési ciklus folyamán előállított összes objektumot be kell venni a változás-menedzsmentbe. A változás-menedzsmentbe bevont, védelmet megvalósító, illetve a védelmet támogató funkciókat rájuk jellemző azonosítókkal kell ellátni.** A változás-menedzsmentet támogató eszközrendszernek ellenőrizni és rögzítenie kell a változásokat a változás-menedzsment alá eső objektumok különböző verziói között. **Az ezeken végrehajtott változtatásokat el kell látni a "végrehajtó", "dátum" és "időpont" adatokkal. A változás-menedzsment eszközrendszernek támogatnia kell a menedzsment alá vont objektumok változói közötti kapcsolatok létrehozását és kezelését. Az objektumok bármelyikét érintő változás esetén a menedzsment eszközrendszernek azonosítania kell a menedzsment alá vont és a változás által érintett más objektumokat és ha azok védelmet megvalósító vagy védelmet támogató funkciók, akkor ilyen jelzővel el kell látni azokat.**
	Evidencia követelmény	Az átadott dokumentációnak **magyarázó és értékelő** jelleggel ismertetnie kell, hogy hogyan használják a változás-menedzsment rendszert **és a rendszerintegrációs eljárásokat** a gyakorlatban és hogyan alkalmazzák a fejlesztésben/gyártásban, összhangban a fejlesztő/gyártó minőségbiztosító követelményrendszerével. **Megmagyarázandó és értékelendő, hogy a változás-menedzsment rendszer eszközrendszere hogyan biztosítja annak detekcióját, hogy egy objektum átvételéért felelős személy nem lehet azonos a tervezővel és fejlesztővel. A változás-menedzsment rendszerből mintavételes biztonsági naplózást kell rendelkezésre bocsátani.**
	Tanúsító tennivalója	Ellenőrizendők a dokumentált eljárások, valamint, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. **A mintavételszerű biztonsági naplót ellenőrizni kell.** A fejlesztő eszközeit fel kell használni az MT kiválasztott részeinek újraépítésére és össze kell hasonlítani az átadott MT-vel.

Megvalósítás / Fejlesztési környezet 24. táblázat		
Programozási nyelvek, fordítók	**Tartalmi és formai követelmények**	Bármely fejlesztésre használt programnyelvnek jól definiáltnak kell lennie, pl. meg kell felelnie az ISO szabványnak. Bármely, a fejlesztéssel kapcsolatos nyelvi sajátosságot dokumentálni kell. **A fordítónak a fejlesztéssel kapcsolatos bármely sajátosságát dokumentálni kell. Az összes futási idejű könyvtár forráskódját át kell adni .**
	Evidencia követelmény	A programnyelvnek egyértelműen és ellentmondásmentesen kell definiálni a forráskódban használt összes utasítás tartalmát.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.
Fejlesztők biztonsága	**Tartalmi és formai követelmények**	A fejlesztési környezetről szóló dokumentumnak **magyarázó és értékelő** jelleggel be kell mutatnia az MT integritása és a kapcsolódó dokumentáció bizalmasságának fizikai, szabályozási, személyes vagy más eszközökkel megvalósított védelmét.
	Evidencia követelmény	A fejlesztési környezetről szóló dokumentumnak **magyarázó és értékelő** jelleggel be kell mutatnia, hogy az MT integritása és a kapcsolódó dokumentáció bizalmasságának védelme hogyan valósul meg.
	Tanúsító tennivalója	Ellenőrizendők a dokumentált eljárások, valamint, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Tesztek végzendők az eljárásokban levő hibák felderítésére.

Működés / Üzemeltetéshez szükséges dokumentáció 25. táblázat		
A tanúsítónak átadandó		1. Felhasználói dokumentáció 2. Adminisztrátori dokumentáció
Felhasználói dokumentáció	**Tartalmi és formai követelmények**	A végfelhasználó számára **magyarázó és értékelő** jelleggel tartalmaznia kell a védelmet megvalósító funkcióknak a biztonsági követelményeknek megfelelő kezelési leírását. Legyen világos felépítésű. Legyen összhangban a többi dokumentációval.
	Evidencia követelmény	**Magyarázó és értékelő** módon tartalmazza azt, hogy a végfelhasználó hogyan használja az MT a követelményeknek megfelelően.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.
Adminisztrátori dokumentáció	**Tartalmi és formai követelmények**	**Magyarázza és értékelje** a védelmet megvalósító funkciókat, jelölje meg azokat, amelyeket az adminisztrátor beállíthat és azokat, amelyeket csak lekérdezhet. **Magyarázza és értékelje** az összes az adminisztratív funkciókhoz kapcsolódó és a biztonságot érintő esemény-típust. **Magyarázza és értékelje** adminisztrátori munka biztonságát érintő részleteket, hogyan használja hatékonyan és egyenszilárdságúan az adminisztrátor az MT funkcióit és hogyan hatnak azok egymásra. **Magyarázza és értékelje** az MT installálására és konfigurálására vonatkozó utasításokat. Legyen világos felépítésű. Legyen összhangban a többi dokumentációval.
	Evidencia követelmény	**Magyarázza és értékelje**, hogy az MT üzemeltetése hogyan valósítható meg biztonságosan.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.

Működés / Működési környezet 26. táblázat		
A tanúsítónak átadandó		1. Szállítási és konfigurálási dokumentáció 2. Indítási és üzemeltetési dokumentáció
Szállítás és konfigurálás	**Tartalmi és formai követelmények**	**Magyarázza és értékelje** a konfigurációs változatok - ha vannak ilyenek - biztonságot érintő hatásait, a szállítással és az installálással/generálással kapcsolatos eljárásokat. A minősítő által jóváhagyott eljárással ellenőrizni kell, hogy hiteles-e és a megrendelttel azonos-e az MT. Az MT installációja/generálása során a paramétereket, változtatásokat úgy kell naplózni (audit trail), hogy utólagosan is rekonstruálni lehessen mikor és hogyan lett installálva/generálva az MT.
	Evidencia követelmény	**Magyarázza és értékelje**, hogy az eljárások hogyan valósíthatók meg biztonságosan.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Ellenőrizendők a szállítási előírások korrekt betartása. Tesztek végzendők az installációs/generálási eljárásokban levő hibák felderítésére.
Indítás, üzemeltetés	**Tartalmi és formai követelmények**	Írja le a biztonságos indítás és üzemeltetés eljárásait. Fel kell tüntetni, ha az indítás, az üzemeltetés vagy a karbantartás alatt védelmet megvalósító funkció hatástalanítható vagy módosítható. **Olyan eljárásnak kell léteznie, amely biztosítja az MT biztonságos állapotba történő visszaállítását kiesés vagy hardver/szoftver hiba után.** Ha az MT védelmet megvalósító hardver komponenst tartalmaz olyan, az adminisztrátor, a végfelhasználó által vagy automatikusan indítható tesztrendszerrel kell rendelkezni, amellyel az MT tesztje üzemelés közben elvégezhető.
	Evidencia követelmény	**Magyarázza és értékelje**, hogy az eljárások, hogyan szolgálják a biztonságot. A megbízónak át kell adnia a védelmet megvalósító hardver komponensekre vonatkozó összes diagnosztikai teszteredményt, valamint az indítás és az üzemelés során készült biztonsági naplókat.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Az indítás és az üzemeltetésre vonatkozó naplókat ellenőrizni kell. Tesztek végzendők az eljárásokban levő hibák felderítésére.

3.1.6. E6 szint

Rövid jellemzés: az E5 szinthez további követelményként jelenik meg a védelmet megvalósító funkciók és a rendszerterv formális leírása, amelynek konzisztensnek kell lennie a formálisan specifikált biztonsági politikával.

Megvalósítás / Fejlesztési folyamat **27. táblázat**		
A tanúsítónak átadandó		1. Védelmi célok. 2. Egy alátámasztó, formálisan specifikált biztonsági politika modell definiálása vagy hivatkozás. 3. A modell informális leírása a védelmi cél dokumentumban. 4. Az MT architektúrájának **formális** leírása. 5. Az MT részletes terv szemiformális leírása. 6. Teszt dokumentáció. 7. Az MT teszteléséhez használt tesztprogramok könyvtárai és a teszteszközök, **beleértve olyanokat is, amelyek képesek a védelmet megvalósító, illetve segítő forráskódú komponens forrás- és végrehajtható kódja közötti inkonzisztenciákat detektálni.** 8. Az összes védelmet megvalósító és segítő komponens forráskódja és/vagy hardver-rajza. 9. A forráskód vagy a hardver-rajz valamint a részletes terv közötti összefüggések informális leírása **és a védelmet megvalósító funkciók formális specifikációja.**
Követelmény-rendszer	**Tartalmi és formai követelmények**	A védelmi célok dokumentációjának magyarázó és értékelő jelleggel tartalmaznia kell: 1. az MT védelmet megvalósító funkcióit, 2. az Informatikai Biztonságpolitikát (rendszer esetén), a Termék Besorolási Ismertetőt (termék esetén), 3. a védelmet megvalósító funkciók informális és szemiformális leírását, 4. egy formális biztonsági politika modellt vagy hivatkozni kell rá, amellyel meghatározható az a biztonsági politika amelynek az MT-nek meg kell felelnie, 5. a modell informális **és formális leírását** a védelmi célok meghatározása keretében.
	Evidencia követelmény	A védelmi célok dokumentációja magyarázó és értékelő jelleggel tartalmazza, hogy rendszer esetén a valós, termék esetén a feltételezett fenyegetések ellen a védelmi funkciók hogyan fejtenek ki ellenhatást, valamint azt, hogy hogyan felelnek meg a védelmi igényeknek. A formális biztonsági politika modell informális magyarázata és értékelése be kell, hogy mutassa hogyan felelnek meg a védelmi célok a biztonsági politikának.
	Tanúsító tennivalója	Ellenőrizendők a dokumentációk megfelelése tartalmi és formai szempontból, valamint a védelmi cél dokumentáció ellentmondásmentes és teljes körű volta. Ellenőrizendő, hogy a védelmi célok között nincs-e olyan védelmi jellemző, amely ellentmondana a biztonsági politikának.

Megvalósítás / Fejlesztési folyamat 27. táblázat		
Rendszerterv	**Tartalmi és formai követelmények**	A rendszertervben **formális** ábrázolásmódot kell alkalmazni, hogy kialakítható legyen a **formális** leírás. A rendszerterv magyarázó és értékelő tartalmazza: 1. az MT architektúráját rendszer szinten, 2. a külső interfészeket, 3. a hardverben és/vagy firmware-ben implementált védelmi funkciók megnevezését, 4. szét kell választani az MT védelmet megvalósító és egyéb funkcióit, **5.** a védelmet megvalósító komponensek közötti összefüggéseket.
	Evidencia követelmény	Magyarázó és értékelő jelleggel mutassa be, hogy a védelmet megvalósító funkciók, hogyan felelnek meg a védelmi céloknak és hogyan kerülnek szétválasztásra a védelmet megvalósító és az egyéb funkciók. Meg kell magyarázni és értékelni kell, hogy a választott leíró struktúra hogyan biztosítja a függetlenséget a védelmet megvalósító komponensek között. Megmagyarázandó és értékelendő, hogy miért szükségesek a - létezésük esetén - a védelmet megvalósító komponensek közötti kapcsolatok. **Megmagyarázandó és értékelendő, hogy a formális és az informális leírási technika használatával hogyan biztosítható a formális biztonság politikai modell és a biztonsági politika közötti konzisztencia.**
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek-e a tartalmi, formai és evidencia követelményeknek, valamint, hogy a védelmet megvalósító és az egyéb funkciók szétválasztása mennyire teljesült. **Ellenőrizendők a formális állítások helyessége.**

Megvalósítás / Fejlesztési folyamat 27. táblázat		
Részletes terv	**Tartalmi és formai követelmények**	A szemiformális részletes terv kialakításához szemiformális ábrázolásmódot kell bevezetni. Specifikálja az összes alap-komponenst. A tervezés összes hierarchia szintjén meg kell magyarázni és értékelni kell, hogy a védelmet megvalósító és a támogató funkciók hogyan valósulnak meg. Megmagyarázandó és értékelendő az MT védelmet megvalósító, védelmet támogató és egyéb komponenseinek szétválasztása. Ezeket jól definiált, lehetőleg független alapkomponensek olyan rendszerébe kell strukturálni, amely tesztelési lehetőségekkel bír, hogy a biztonság potenciális megsértésének lehetősége minimalizálva legyen. Ebben alkalmazni kell szintekre bontást, az absztrakciót, és az adatrejtést. Mutassa be magyarázó és értékelő jelleggel a védelmet megvalósító és a védelmet támogató funkciók kialakítását. Azonosítsa a védelmi mechanizmusokat. A védelmet megvalósító funkciókat le kell képezni a védelmi mechanizmusokra és funkcionális egységekre. A védelmet megvalósító és a védelmet támogató funkciók esetében szükségtelen funkcionalitásokat ki kell zárni. Dokumentálni kell a védelmet megvalósító, valamint a védelmet támogató komponensek célját és paramétereit, a mechanizmusok definícióit, specifikációját és hatásait. Megmagyarázandó az összes olyan változó szerepe, amelyet több funkcionális egység is használ. A specifikációnak alkalmasnak kell lenni a mechanizmusok közötti kölcsönhatások megítélésére. Ahol több szintű a specifikáció, ott a hierarchia szintek közötti kapcsolatokat világosan le kell írni. A nem védelmi célú komponensek specifikációja nem kell.
	Evidencia követelmény	Magyarázó és értékelő jelleggel dokumentálni kell, hogy a védelmi mechanizmusok hogyan biztosítják a védelmi célok dokumentációjában specifikált védelmet megvalósító funkciók működését. Megmagyarázandó, hogy a fennmaradó funkcionalitások miért nem zárhatók ki a védelmet megvalósító, illetve a védelmet támogató funkciókból. Legyen egyértelműen megállapítható, hogy azok a komponensek, amelyekre a tervben nincs tervezési információ, nincsenek kapcsolatban sem a védelmet megvalósító, sem a védelmet támogató funkciókkal.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.

Megvalósítás / Fejlesztési folyamat 27. táblázat		
Implementáció	**Tartalmi és formai követelmények**	A forráskódot és/vagy a hardver-rajzokat teljes mértékben kis, jól körülhatárolt szegmensekre kell bontani. Magyarázó és értékelő jelleggel be kell mutatni a forráskód vagy a hardver-rajz valamint a funkcionális egységek közötti összefüggéseket, **valamint forráskódban és /vagy a hardver-rajzokban megjelenő biztonsági mechanizmusok és a védelmi célokban megfogalmazott, a védelmet megvalósító funkciók formális specifikációja közötti megfelelőséget.** A kötelező jelleggel átadott teszt dokumentációnak tartalmaznia kell tesztelési célokat, tervet, eljárásokat és az eredményeket, valamint egy értékelést arról, hogy a tesztelés lefedettsége miért megfelelő. Az teszt program könyvtárakat és eszközöket át kell adni a tesztek megismételhetősége céljából.
	Evidencia követelmény	Az átadott tesztdokumentációnak magyarázó és értékelő jelleggel tükröznie kell, a védelmi célokban megfogalmazott védelmet megvalósító funkciók **formális specifikációja** és a tesztek egymás közötti megfelelését. Magyarázó és értékelő jelleggel be kell mutatni a részletes tervben szereplő, védelmet megvalósító és a védelmet támogató funkciók, valamint a tesztek közötti összefüggéseket. Magyarázó és értékelő jelleggel be kell mutatni a forráskódban vagy a hardver-rajzokban kialakított védelmi mechanizmusok, valamint a tesztek közötti összefüggéseket. Lényeges a biztonság szempontjából, hogy a hibák felfedése és korrekciója után újbóli tesztekkel kell bizonyítani a hibák kijavítását, illetve, hogy újabb hibák nem lettek bevíve.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Az átadott tesztprogramokkal ellenőrizni kell az átadott teszteredményeket. Ellenőrizendő, hogy a tesztek lefedik-e a részletes tervben szereplő, védelmet megvalósító és a védelmet támogató funkciók, valamint a forráskódban vagy a hardver-rajzokban kialakított védelmi mechanizmusok mindegyikét. További tesztek végzendők hibák felderítésére. **Megvizsgálandó bármely, a megbízó által rendelkezésre bocsátott eszközök által végrehajtott teszt közben feltételezett inkonzisztencia a forráskód és a végrehajtható kód között.**

Megvalósítás / Fejlesztési környezet 28. táblázat		
A tanúsítónak átadandó		1. Az értékelésre átadott MT verzióját azonosító konfigurációs lista. 2. A változás-menedzsment rendszerre vonatkozó információk. 3. Az MT változás-menedzsment alá eső összes komponensének módosításával kapcsolatos audit dokumentum. 4. A rendszerintegrálással kapcsolatos információk. 5. Információk az átadás-átvételi eljárásokról. 6. A fejlesztési környezet biztonságára vonatkozó információk. 7. A fejlesztő nyelvek leírása. 8. A használatba vett összes futási idejű könyvtár forráskódjai.
Változás-menedzsment	**Tartalmi és formai követelmények**	A fejlesztési folyamatot változás-menedzsment rendszerrel és átadás-átvételi eljárás(ok)kal kell támogatni. A változás-menedzsmentet kezelő eszközrendszernek ellenőriznie kell, hogy egy fejlesztési objektum átvételéért felelős személy nem azonos-e annak tervezőivel vagy fejlesztőivel. A konfigurációs listában benne kell lennie az összes olyan komponensek, amelyet az MT-be beépítettek. Az MT-nek, az összes alap-komponensnek és az összes dokumentációnak - beleértve a kézikönyveket is -, a forráskódoknak és/vagy a hardver-rajzoknak egyértelmű azonosítóval kell rendelkezniük. Minden dokumentumban csak ezekre lehet hivatkozni. A változás-menedzsment rendszernek biztosítania kell, hogy a minősítésre átadott MT-nek és a dokumentációnak egyértelműen meg kell felelnie egymásnak és abban csak jóváhagyott változtatások történhetnek feljogosított személy által. **A fejlesztés során használt összes eszközt be kell vonni a változás-menedzsmentbe.** Az átvételi eljáráson átmenő, a fejlesztési ciklus folyamán előállított összes objektumot be kell venni a változás-menedzsmentbe. A változás-menedzsmentbe bevont, védelmet megvalósító, illetve a védelmet támogató funkciókat rájuk jellemző azonosítókkal kell ellátni. A változás-menedzsmentet támogató eszközrendszernek ellenőrizni és rögzítenie kell a változásokat a változás-menedzsment alá eső objektumok különböző verziói között. Az ezeken végrehajtott változtatásokat el kell látni a “végrehajtó”, “dátum” és “időpont” adatokkal. A változás-menedzsment eszközrendszernek támogatnia kell a menedzsment alá vont objektumok változói közötti kapcsolatok létrehozását és kezelését. Az objektumok bármelyikét érintő változás esetén a menedzsment eszközrendszernek azonosítania kell a menedzsment alá vont és a változás által érintett más objektumokat és ha azok védelmet megvalósító vagy védelmet támogató funkciók, akkor ilyen jelzővel el kell látni azokat.
	Evidencia követelmény	Az átadott dokumentációnak magyarázó és értékelő jelleggel ismertetnie kell, hogy hogyan használják a változás-menedzsment rendszert és a rendszerintegrációs eljárásokat a gyakorlatban és hogyan alkalmazzák a fejlesztésben/gyártásban, összhangban a fejlesztő/gyártó minőségbiztosító követelményrendszerével. Megmagyarázandó és értékelendő, hogy a változás-menedzsment rendszer eszközrendszere hogyan biztosítja annak detekcióját, hogy egy objektum átvételéért felelős személy nem lehet azonos a tervezővel és fejlesztővel. A változás-menedzsment rendszerből mintavételes biztonsági naplózást kell rendelkezésre bocsátani.
	Tanúsító tennivalója	Ellenőrizendők a dokumentált eljárások, valamint, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. A mintavételszerű biztonsági naplót ellenőrizni kell. A fejlesztő eszközeit fel kell használni az MT kiválasztott

Megvalósítás / Fejlesztési környezet 28. táblázat		
		részeinek újraépítésére és össze kell hasonlítani az átadott MT-vel.
Programozási nyelvek, fordítók	**Tartalmi és formai követelmények**	Bármely fejlesztésre használt programnyelvnek jól definiáltnak kell lennie, pl. meg kell felelnie az ISO szabványnak. Bármely, a fejlesztéssel kapcsolatos nyelvi sajátosságot dokumentálni kell. A fordítónak a fejlesztéssel kapcsolatos bármely sajátosságát dokumentálni kell. Az összes futási idejű könyvtár forráskódját át kell adni.
	Evidencia követelmény	A programnyelvnek egyértelműen és ellentmondásmentesen kell definiálni a forráskódban használt összes utasítás tartalmát.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.
Fejlesztők biztonsága	**Tartalmi és formai követelmények**	A fejlesztési környezetről szóló dokumentumnak magyarázó és értékelő jelleggel be kell mutatnia az MT integritása és a kapcsolódó dokumentáció bizalmasságának fizikai, szabályozási, személyes vagy más eszközökkel megvalósított védelmét.
	Evidencia követelmény	A fejlesztési környezetről szóló dokumentumnak magyarázó és értékelő jelleggel be kell mutatnia, hogy az MT integritása és a kapcsolódó dokumentáció bizalmasságának védelme hogyan valósul meg.
	Tanúsító tennivalója	Ellenőrizendők a dokumentált eljárások, valamint, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Tesztek végzendők az eljárásokban levő hibák felderítésére.

Működés / Üzemeltetéshez szükséges dokumentáció 29. táblázat		
A tanúsítónak átadandó		1. Felhasználói dokumentáció 2. Adminisztrátori dokumentáció
Felhasználói dokumentáció	**Tartalmi és formai követelmények**	A végfelhasználó számára magyarázó és értékelő jelleggel tartalmaznia kell a védelmet megvalósító funkcióknak a biztonsági követelményeknek megfelelő kezelési leírását. Legyen világos felépítésű. Legyen összhangban a többi dokumentációval.
	Evidencia követelmény	Magyarázó és értékelő módon tartalmazza azt, hogy a végfelhasználó hogyan használja az MT a követelményeknek megfelelően.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek.
Adminisztrátori dokumentáció	**Tartalmi és formai követelmények**	Magyarázza és értékelje a védelmet megvalósító funkciókat, jelölje meg azokat, amelyeket az adminisztrátor beállíthat és azokat, amelyeket csak lekérdezhet. Magyarázza és értékelje az összes az adminisztratív funkciókhoz kapcsolódó és a biztonságot érintő esemény-típust. Magyarázza és értékelje adminisztrátori munka biztonságát érintő részleteket, hogyan használja hatékonyan és egyenszilárdságúan az adminisztrátor az MT funkcióit és hogyan hatnak azok egymásra. Magyarázza és értékelje az MT installálására és konfigurálására vonatkozó utasításokat. Legyen világos felépítésű. Legyen összhangban a többi dokumentációval.
	Evidencia követelmény	Magyarázza és értékelje, hogy az MT üzemeltetése hogyan valósítható meg biztonságosan.
	Tanúsító tenniva-	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a

	lója	tartalmi, formai és evidencia követelményeknek.

Működés / Működési környezet **30. táblázat**		
A tanúsítónak átadandó		1. Szállítási és konfigurálási dokumentáció 2. Indítási és üzemeltetési dokumentáció
Szállítás és konfigurálás	**Tartalmi és formai követelmények**	**Magyarázza és értékelje** a konfigurációs változatok - ha vannak ilyenek, **akkor a formális leírású rendszertervben kell azokat definiálni** - biztonságot érintő hatásait, a szállítással és az installálással/generálással kapcsolatos eljárásokat. A minősítő által jóváhagyott eljárással ellenőrizni kell, hogy hiteles-e és a megrendelttel azonos-e az MT. Az MT installációja/generálása során a paramétereket, változtatásokat úgy kell naplózni (audit trail), hogy utólagosan is rekonstruálni lehessen mikor és hogyan lett installálva/generálva az MT.
	Evidencia követelmény	Magyarázza és értékelje, hogy az eljárások hogyan valósíthatók meg biztonságosan.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Ellenőrizendők a szállítási előírások korrekt betartása. Tesztek végzendők az installációs/generálási eljárásokban levő hibák felderítésére.
Indítás, üzemeltetés	**Tartalmi és formai követelmények**	Írja le a biztonságos indítás és üzemeltetés eljárásait. Fel kell tüntetni, ha az indítás, az üzemeltetés vagy a karbantartás alatt a védelmet megvalósító funkció hatástalanítható vagy módosítható. Olyan eljárásnak kell léteznie, amely biztosítja az MT biztonságos állapotba történő visszaállítását kiesés vagy hardver/szoftver hiba után. Ha az MT védelmet megvalósító hardver komponenst tartalmaz olyan, az adminisztrátor, a végfelhasználó által vagy automatikusan indítható tesztrendszerrel kell rendelkezni, amellyel az MT tesztje üzemelés közben elvégezhető.
	Evidencia követelmény	Magyarázza és értékelje, hogy az eljárások, hogyan szolgálják a biztonságot. A megbízónak át kell adnia a védelmet megvalósító hardver komponensekre vonatkozó összes diagnosztikai teszteredményt, valamint az indítás és az üzemelés során készült biztonsági naplókat.
	Tanúsító tennivalója	Ellenőrizendők, hogy a dokumentációk megfelelnek- e a tartalmi, formai és evidencia követelményeknek. Az indítás és az üzemeltetésre vonatkozó naplókat ellenőrizni kell. Tesztek végzendők az eljárásokban levő hibák felderítésére.

3.2. Hatékony leképzés

Hatékony leképzés / Megvalósítás 31. táblázat		
A tanúsítónak átadandó		1. A funkcionális megfelelés analízise 2. Szinergia analízis 3. A biztonsági mechanizmus erősségének analízise 4. Az ismert gyenge pontok listája a megvalósítás területén
Funkcionális megfelelés	**Definíció**	A korrekt megvalósítás értékeléséhez átadott védelmi célok dokumentum ott teljesség és konzisztencia szempontjából kerül ellenőrzésre, a hatékony leképzés esetében az MT védelmi funkcióinak és mechanizmusainak a védelmi célokban azonosított releváns fenyegetésekkel szembeni hatékonysága kerül ellenőrzésre.
	Tartalmi és formai követelmények	A biztonsági funkciókat és a védelmi mechanizmusokat tételesen össze kell rendelni a védelmi célok dokumentumában azonosított fenyegetésekkel, hogy a sebezhető gyenge pontok már a tervezés szintjén kiszűrhetők legyenek
	Evidencia követelmény	Bemutatandó, hogy a biztonsági funkciók és mechanizmusok hogyan képesek a fenyegetéseknek ellenállni. Pontosan kimutatandó, hogy nincs olyan fenyegetés, amely ellen ne lenne specifikálva védelmet megvalósító funkció. A funkcionális megfelelés elemzéséhez a 6. sz. táblázatban megadott, az adott értékelési szintre a megbízó által szolgáltatott dokumentumok információit kell felhasználni.
	Tanúsító tennivalója	A dokumentum ellenőrizendő tartalmi, formai és evidencia követelmények teljesítése szempontjából. Ellenőrizendő, hogy a 6. sz. táblázatban megadott, az adott értékelési szintre vonatkozó dokumentumok információk figyelembe lettek-e véve.
Szinergikus hatás	**Definíció**	A védelmet megvalósító funkciók és a védelmi mechanizmusok egymást erősítő, illetve gyöngítő vagy ellentmondó kölcsönhatásai.
	Tartalmi és formai követelmények	A dokumentumnak tartalmaznia kell a védelmet megvalósító funkciók és mechanizmusok egymás közötti kölcsönhatásai bemutatását.
	Evidencia követelmény	Bemutatandó, hogy a védelmet megvalósító funkciók és mechanizmusok egymás közötti kölcsönhatásai nem kerülhetnek egymással konfliktusba vagy ellentmondásba. A szinergikus hatás elemzéséhez a 6. sz. táblázatban megadott, az adott értékelési szintre a megbízó által szolgáltatott dokumentumok információit kell felhasználni.
	Tanúsító tennivalója	A dokumentum ellenőrizendő tartalmi, formai és evidencia követelmények teljesítése szempontjából. Ellenőrizendő, hogy a 6. sz. táblázatban megadott, az adott értékelési szintre vonatkozó dokumentumok információi figyelembe lettek-e véve.

Hatékony leképzés / Megvalósítás 31. táblázat		
A biztonsági mechanizmus erőssége	**Definíció**	Ha a védelmet megvalósító funkciók nem is kerülhetők meg, nem hidalhatók át, nem korrumpálhatók, előfordulhat sikeres direkt támadás, kihasználva az elvi, algoritmusbeli hiányosságokat. A biztonsági mechanizmus erőssége elsősorban a direkt támadások elleni védelmi képességek erősségét méri 3 szintben. Ez abban is különbözik a többi értékelési szemponttól, hogy itt figyelembe kell venni a a sikeres támadás végrehajtásához szükséges erőforrások szintjét is.
	Tartalmi és formai követelmények	Az MT összes kritikusnak minősített védelmet megvalósító mechanizmusát fel kell sorolni. A dokumentumnak tartalmaznia vagy hivatkoznia kell ezek algoritmusának, elveinek és tulajdonságainak elemzésére.
	Evidencia követelmény	A biztonsági mechanizmus erősségére vonatkozó elemzésnek ki kell mutatnia, hogy az összes kritikusnak minősített mechanizmus kielégíti a védelmi célokban meghatározott minimálisan igényelt védelmi mechanizmus erősségi szintbesorolást. Szintbesorolás definíciója a 2.3.2. pont (hatékony leképzés) szerint. Rejtjelzési mechanizmusok esetében az ezzel kapcsolatos állásfoglalást - minősített adatok kezelése estén - a Magyar Köztársaság Információs Hivatal Országos Rejtjelfelügyeletétől kell megkérni. A többi elemzéshez a 6. sz. táblázatban megadott, az adott értékelési szintre a megbízó által szolgáltatott dokumentumok információit kell felhasználni.
	Tanúsító tennivalója	Ellenőrizendő, hogy: 1. az összes kritikusnak minősített mechanizmus azonosítva lett-e a dokumentumban, 2. a biztonsági mechanizmus erősségére vonatkozó elemzés kielégíti-e a tartalmi, formai és evidencia követelményeket, 3. a 6. sz. táblázatban megadott, az adott értékelési szintre a megbízó által szolgáltatott dokumentumoknak információi figyelembe lettek-e véve, 4. az összes kritikusnak minősített mechanizmus definíciója/specifikációja összhangban van-e a védelmi célokban megcélzott minimális erősségi szintnek. A támadási módoknak megfelelő lehetséges támadási útvonalak figyelembe vételével **behatolási tesztet** kell elvégezni.

Hatékony leképzés / Megvalósítás 31. táblázat		
Gyenge pontok	**Definíció**	Az többi szempontok szerinti értékelés során az MT megvalósításában, konstrukciójában a megbízó és a tanúsító több gyenge pontot (deaktiválhatóság, megkerülhetőség, áthidalhatóság, stb.) detektálhatott. A gyenge pontoknak a hatékony leképzés szerinti elemzése azt vizsgálja, hogy ezek a gyakorlatban kompromitálhatják-e az MT védelmét.
	Tartalmi és formai követelmények	A megbízónak az MT összes, a megvalósítás során előálló konstrukciós gyenge pontokat fel kell sorolnia, amelyek számára ismertek. A sebezhető gyenge pontokat azonosítania, a védelmi képességekre való hatását elemeznie kell és azonosítani kell azokat a javasolt, illetve megvalósított intézkedéseket, amelyek a gyenge pontokat megszüntetik.
	Evidencia követelmény	Az ismert gyenge pontok elemzésének ki kell mutatnia, hogy azok az MT feltételezett vagy valós környezetében nem lesznek még jobban kihasználhatók, támadhatók, azáltal, hogy: 1. a gyenge pontok más, megfelelő funkcionalitású és erősségű, nem kompromitálható, MT-n belüli védelmi mechanizmusokkal ellensúlyozottak, 2. a gyenge pontok irrelevánsak a kitűzött védelmi célok szempontjából, nincs gyakorlati jelentőségük vagy az MT-n kívüli, megfelelően dokumentált technikai, adminisztratív vagy személyi intézkedésekkel ellensúlyozottak. Az elemzéshez a 6. sz. táblázatban megadott, az adott értékelési szintre a megbízó által szolgáltatott dokumentumok információit fel kell használni.
	Tanúsító tennivalója	Ellenőrizendő, hogy: 1. az ismert gyenge pontok listája kielégíti-e a tartalmi, formai és evidencia követelményeket, a 6. sz. táblázatban megadott, az adott értékelési szintre a megbízó által szolgáltatott dokumentumok információi figyelembe lettek-e véve a gyenge pontok hatásainak elemzésénél; egy másik gyenge pont elemzés végzendő, amelynél mind a listában szereplő, mind az értékelés folyamán talált gyenge pontokat figyelembe kell venni, 3. a megismert gyenge pontok összes kombinációinak hatásai, 4. a gyenge pontok hatásainak elemzése nem tartalmaz-e dokumentálatlan vagy alaptalan feltételezéseket a feltételezett/valós működési környezetről, 5. az MT-n kívüli külső biztonsági intézkedésekkel kapcsolatos feltételezések, követelmények megfelelően dokumentáltak-e, A támadási módoknak megfelelő lehetséges támadási útvonalak figyelembe vételével **behatolási tesztet** kell elvégezni az ismert gyenge pontoknak a gyakorlatban történő kihasználhatósága szempontjából.

Hatékony leképzés / Működés 32. táblázat		
A tanúsítónak átadandó		1. Védelmi stabilitás elemzés. 2. A működés közben detektált gyenge pontok listája.
Védelmi stabilitás	**Definíció**	Az MT úgy konfigurálható vagy üzemeltethető, hogy működése alatt a védelmi képességek lecsökkentek, de az adminisztrátorok vagy a végfelhasználók az MT-t biztonságosnak hihetik.
	Tartalmi és formai követelmények	A védelmi stabilitás elemzésének az MT összes működési módját elemeznie kell, beleértve a kiesés vagy kezelési hiba utáni állapotot, valamint azoknak a biztonságos működéssel kapcsolatos vonzatait.
	Evidencia követelmény	A védelmi stabilitás elemzésének ki kell mutatnia, hogy bármely kezelői vagy más hiba, amely kikapcsolja vagy működésképtelenné teszi a védelmet megvalósító funkciókat vagy mechanizmusokat, könnyen detektálható. Kimutatandó, hogy ha az MT-t úgy lehet konfigurálni vagy működtetni, hogy nem lesz biztonságos (azaz a védelmet megvalósító funkciók és mechanizmusok nem felelnek meg a védelmi céloknak) és az adminisztrátorok vagy a végfelhasználók mégis biztosnak hihetik, akkor az a tény detektálható legyen. Az elemzéshez a 6. sz. táblázatban megadott, az adott értékelési szintre a megbízó által szolgáltatott dokumentumok információit fel kell használni.
	Tanúsító tennivalója	Ellenőrizendő, hogy: 1. védelmi stabilitás elemzés kielégíti-e a tartalmi, formai és evidencia követelményeket, 2. a 6. sz. táblázatban megadott, az adott értékelési szintre a megbízó által szolgáltatott dokumentumok információi figyelembe lettek-e véve védelmi stabilitás elemzésnél; 3. az elemzés nem tartalmaz-e dokumentálatlan vagy alaptalan feltételezéseket a feltételezett/valós működési környezetről, 4. az MT-n kívüli külső biztonsági intézkedésekkel (pl. adminisztratív, fizikai vagy emberi) kapcsolatos feltételezések, követelmények megfelelően dokumentáltak-e, Megismétlendők a konfigurálási és installációs. eljárások csupán a felhasználó és az adminisztrátori dokumentációk felhasználásával az MT biztonságos konfigurálásának és működtetésének ellenőrtése céljából. Más tesztek is elvégzendők - ha szükséges -, a védelmi stabilitás ellenőrzése céljából.

Hatékony leképzés / Működés 32. táblázat		
Gyenge pontok	**Definíció**	Az többi szempontok szerinti értékelés során az MT működési módjában a megbízó és a tanúsító több gyenge pontot detektálhatott. A gyenge pontoknak a hatékony leképzés szerinti elemzése azt vizsgálja, hogy ezek a gyakorlatban kompromitálhatják-e az MT védelmét.
	Tartalmi és formai követelmények	A megbízónak az MT összes működési módbeli gyenge pontokat fel kell sorolnia, amelyek számára ismertek. A sebezhető gyenge pontokat azonosítania, a védelmi képességekre való hatását elemeznie kell és azonosítani kell azokat a javasolt, illetve megvalósított intézkedéseket, amelyek a gyenge pontokat megszüntetik.
	Evidencia követelmény	Az ismert gyenge pontok elemzésének ki kell mutatnia, hogy azok az MT feltételezett vagy valós környezetében nem lesznek még jobban kihasználhatók, támadhatók, azáltal, hogy: 1. a gyenge pontok más, megfelelő funkcionalitású és erősségű, nem kompromitálható, MT-n belüli védelmi mechanizmusokkal ellensúlyozottak, 2. a gyenge pontok irrelevánsak a kitűzött védelmi célok szempontjából, nincs gyakorlati jelentőségük vagy az MT-n kívüli, megfelelően dokumentált technikai, adminisztratív vagy személyi intézkedésekkel ellensúlyozottak. Az elemzéshez a 6. sz. táblázatban megadott, az adott értékelési szintre a megbízó által szolgáltatott dokumentumok információit fel kell használni.
	Tanúsító tennivalója	Ellenőrizendő, hogy: 1. az ismert gyenge pontok listája kielégíti-e a tartalmi, formai és evidencia követelményeket, 2. a 6. sz. táblázatban megadott, az adott értékelési szintre a megbízó által szolgáltatott dokumentumok információi figyelembe lettek-e véve a gyenge pontok hatásainak elemzésénél; független gyenge pont elemzés végzendő, amelynél mind a listában szereplő, mind az értékelés folyamán talált gyenge pontokat figyelembe kell venni, 3. a megismert gyenge pontok összes kombinációinak hatásai, 4. a gyenge pontok hatásainak elemzése nem tartalmaz-e dokumentálatlan vagy alaptalan feltételezéseket a feltételezett/valós működési környezetről, 5. az MT-n kívüli külső biztonsági intézkedésekkel kapcsolatos feltételezések, követelmények megfelelően dokumentáltak-e, A támadási módoknak megfelelő lehetséges támadási útvonalak figyelembe vételével behatolási tesztet kell elvégezni az ismert gyenge pontoknak a gyakorlatban történő kihasználhatósága szempontjából.

4. INFORMATIKAI TERMÉKEK TANÚSÍTÁSA ÉS MINŐSÍTÉSE

A 2. és 3. fejezetekben a minősítési folyamat és a értékelés szempontrendszere bemutatásánál a Minősítés Tárgya kifejezést használtuk egységesen attól függetlenül, hogy informatikai termék vagy rendszer kerül minősítésre. A természetesen a folyamat szereplőinek megtestesítői, az egységes követelményrendszer és a követelmény-elemeinek értelmezése árnyaltabb lehet attól függően, hogy termékről vagy rendszerről van szó. A 4. és 5. fejezetekben nem ismételjük meg a minősítési folyamat és a követelményrendszer ismertetését csupán - az eljárásrend áttekintése kíséretében - azokra az értelmezésbeli eltolódásokra térünk ki, amelyek a termékek, illetve a rendszerek esetében fellépnek.

Termék esetében az a jellemző, hogy a *fejlesztő cég* egy olyan profitorientált cég, amely azzal a céllal fejleszti ki az adott terméket, hogy - a termék legyártása után - a saját vagy más cég értékesítési hálózatán keresztül a piacon értékesítse. Ebből következően mind a fejlesztőnek, mind a gyártónak, mind a forgalmazónak fontos érdeke, hogy a termék egyéb minősítések mellett a biztonságminősítést is megkapja, mert bizonyos piaci területeken ez nagymértékben növeli a termék iránt bizalmat és ennél fogva az eladhatóságot. Ezért a *megbízói szerepkört* egyaránt felveheti a fejlesztő, a gyártó és a forgalmazó is amennyiben egyáltalán külön cégként működnek.

Ha *a minősítés egyidejű módon*, tehát a fejlesztési folyamat közben zajlik le, akkor jellemzően az a cég a megbízó, ahol a fejlesztés történik és ő adja le a minősítő felé a termék minősítésére vonatkozó igényt. A megbízó az előkészítő fázisban a minősítő felé szolgáltatja a 2.1 pontban felsorolt dokumentumokat, amelyek a kiválasztásra kerülő tanúsítóval kötendő szerződés előkészítéséhez és engedélyezésének elbírálásához szükségesek. A dokumentumok közül a termékek esetében fontos szerepet játszik az a dokumentum, amely a termék fejlesztését, gyártását végző cég tulajdonosi viszonyait, a többségi tulajdonos felügyeleti, befolyásolási lehetőségeit írja le. A többi dokumentum termékekre egyértelműen értelmezhető. A tanúsító cégnek a minősítővel és a megbízóval történt közös kiválasztása után megtörténik a szerződéskötés a megbízó és a tanúsító között. A minősítés lefolytatását mindig a megbízó finanszírozza.

A szerződéskötés után az értékelési fázis lépései a fejlesztési folyamat egyes lépéseit követik. A tanúsító a védelmi igények, a védelmi célok dokumentumainak szolgáltatása után a fejlesztés előrehaladásának ütemében kapja meg az egyre "mélyebb" dokumentációkat a rendszertervtől a forráskódig és/vagy hardver-rajzokig a minősítési szint követelmények függvényében. A korrekt és a hatékony leképzés szerinti teljes értékelés csak a fejlesztés lezárása után történhet meg, amikor a termékhez tartozó összes dokumentáció (pl. adminisztrátori, felhasználói) elkészült.

Az egyidejű minősítési folyamat rákényszeríti a fejlesztőt, hogy a termék szokásos funkcionális fejlesztési folyamatának szerves részévé tegye a védelmet megvalósító és a védelmet segítő funkciók kifejlesztését, azok specifikációjától az utolsó tesztig bezárólag. Így biztosított lesz - amennyiben a korrekt és a hatékony leképzés követelményei teljesülnek - hogy a termék védelmi funkciói és mechanizmusai a termék integráns részét képezik.

A besorolás, a tanúsítvány kiállítása és a minősítés a 2. fejezetben leírt standard módon történik.

Követő minősítés esetén a megbízó jellemzően a forgalmazó lehet. Ez leginkább olyan esetekben fordulhat elő, amikor a termék a fejlesztő/gyártó cég országán kívül más országban is forgalmazásra kerül. Ilyenkor a forgalmazó cégnek, mint megbízónak a fejlesztőtől utólagosan kell a minősítési folyamathoz szükséges összes dokumentumot bekérni. Ez csak akkor jelenthet komoly problémát ha a termék még a saját országában sem ment keresztül biztonságminősítési folyamaton. A minősítési folyamat és eljárásrend egyébként a standard módon zajlik le.

4.1. Az informatikai termékek ismételt minősítése

Az informatikai termékek - más termékekhez hasonlóan - rendszeres fejlesztés tárgyai. A fejlesztést a piaci versenyképesség növelése, valamint a felhasználási követelmények motiválják. A biztonság esetében motiváló tényező lehet a releváns fenyegetési kép megváltozása is. A releváns fenyegetési kép jelentős megváltozása esetén a minősítő indítványozza a megbízónak az újraminősítést. Amennyiben az indítványra 90 napon belül a

megbízó a minősítési eljárást nem indítja meg, úgy a minősítő a rendszer vagy termék minősítését - a megfelelő indokolással - megszünteti.

Amennyiben egy termék új változata jelentős mértékű változásokat mutat a védelmi funkciók és mechanizmusok tekintetében célszerű egy ismételt minősítési folyamatot elindítani. Ennek kezdeményezésről mindig a megbízónak kell döntenie.

A minősítési folyamat lényegében azonos a 2. fejezetben ismertetettel, azonban az értékelés csak a termék módosítása által érintett részekre terjed ki, a módosítás jellegétől függő mélységben.

Az előkészítő fázisban szokásos dokumentumoknak csak azokat a részeit kell szolgáltatni, amelyekben a legutóbbi minősítést óta változás történt. Ezeken túlmenően dokumentálni kell a minősítő felé:

- az MT előző minősítési szintjét,
- a változás jellegét,
- a változás az MT mely részét érinti funkcionalitás szempontjából.

A változások jellege a következő táblázati konstrukcióban írandó le egy kiragadott példán bemutatva:

példa a változások kezelésére
33. táblázat

Terület	A változtatás oka	A változás típusa	Érintett értékelési szempont
Védelmi célok	A fenyegetések újabb típusa jelent meg. Újabb védelmet megvalósító funkció lesz/lett kifejlesztve.	m m m	Rendszerterv Részletes terv Implementálás
Hatékony leképzés	A gyakorlatban kihasználható gyenge pontot találtak	m m m	Rendszerterv Részletes terv Implementálás
Korrekt leképzés	Problémát találtak a fejlesztési folyamatban	m m m m	Védelmi cél Rendszerterv Részletes terv Implementálás
	Problémát találtak a fejlesztési környezetben	i t i	Változás-menedzsment Programozási nyelvek, fordítók Fejlesztők biztonsága

A változások típusát a következő kategóriákba soroljuk:

- **m**: olyan változtatás, amely lényegesen érinti az MT funkcionalitását,
- **i**: olyan változtatás, amelynek csak indirekt hatása van az MT-re,
- **d**: a dokumentáció olyan változása, amely kihatással van az MT működésére,
- **t**: a fejlesztési eszközökben beállt változás.

Az **m** típusú változásokat a következő négy kategóriába soroljuk:

- **A0**: a változás a védelmi célokat érinti,
- **A1**: a változás a rendszertervet érinti, a védelmi célokat nem,
- **A2**: a részletes tervben elszigetelt változás, amely nem érinti a rendszertervet,
- **A3**: az implementálásban elszigetelt változás, amely nem érinti a részletes tervet.

A változtatásokat az MT funkcionalitása szempontjából a következő kategóriákba soroljuk:

- **T1**: védelmet megvalósító komponensek,
- **T2**: védelmet segítő komponensek,
- **T3**: a védelem szempontjából közömbös komponensek,
- **T4**: a védelmet támogató szoftvereszközök, pl. nyelvek, fordítók.

A megbízónak a változtatások által érintett értékelési szempontokra vonatkozó dokumentumokat az MT előző minősítési szintjének megfelelő mélységben és struktúrában kell szolgáltatnia úgy, hogy megfeleljen az adott minősítési szint *tartalmi, formai és evidencia követelményeinek.*

A változás típus-megjelölése két csoportra osztható az ismételt értékelés eredménye szempontjából:

- **m** típusú változás esetén az ismételt értékelés lefolytatandó a 34. sz. táblázat-rendszer figyelembe vételével és annak eredménye dönti el, hogy marad-e a régi besorolás vagy változik.
- **i, d, t** típusú változások esetén a besorolás és a tanúsítás szintje változatlan marad, de a típustól függően a következő lépéseket kell megtennie a tanúsítónak:
  - **i**: ellenőrizendő, hogy a változás indirekt hatása a védelmet megvalósító funkciókra és mechanizmusokra eléri-e az **m** szintet, ha igen, akkor az előző besorolási szintnek megfelelő értékelést el kell végezni a változások által érintett szempontok szerint.
  - **d**: ellenőrizendő, hogy a dokumentációban történt változások befolyásolják-e a hatékony leképzésen belül a védelmi stabilitást. Ha *nem*, akkor nem szükséges további lépés, a besorolás és a tanúsítás szintje marad. Ha *igen,* akkor a változásokról el kell készítetni a megbízóval az előző besorolási szinten a védelmi stabilitásnál megkövetelt tartalmi, formai és evidencia követelmények szerint a módosított dokumentumot és a változatlan szintű tanúsítványt csak ezután lehet kiadni.
  - **t**: ellenőrizendő, hogy az alkalmazott szoftver fejlesztő eszközökben beállt változások hatása eléri-e a védelmet megvalósító funkciókra és mechanizmusokra az **m** szintet, ha igen, akkor az előző besorolási szintnek megfelelő értékelést el kell végezni a változások által érintett szempontok szerint.

Az **m** változás típus esetén az értékelés egy olyan segéd-táblázat segítségével végzendő el, amelyben minden besorolási szintnek megfelel egy táblázat, amelyet az M változás-típuson belüli **A** altípusok és a változások által érintett **T** komponens csoportok szerint lettek felállítva.

Értékelési segéd-táblázat
34. táblázat

E1	A0	A1	A2	A3
T1	R5	R4	R2	R2
T2	R5	R3	R2	R2
T3	X	R1	R1	R1

E2	A0	A1	A2	A3
T1	R5	R4	R3	R2
T2	R5	R3	R3	R2
T3	X	R1	R1	R1

E3	A0	A1	A2	A3
T1	R5	R4	R4	R3
T2	R5	R4	R3	R3
T3	X	R1	R1	R1

E4	A0	A1	A2	A3
T1	R5	R5	R5	R4
T2	R5	R4	R4	R3
T3	X	R1	R1	R1

E5	A0	A1	A2	A3
T1	R5	R5	R5	R4
T2	R5	R5	R4	R3
T3	X	R1	R1	R1

E6	A0	A1	A2	A3
T1	R5	R5	R5	R5
T2	R5	R5	R5	R4
T3	X	R1	R1	R1

A tanúsítónak az értékelési segéd-táblázatot a következők szerint kell használnia:

1. azonosítsa az MT előző besorolási szintjének (E1 - E6) megfelelő résztáblázatot,
2. azonosítsa a komponens típust (T1 - T3),
3. azonosítsa a változás altípust (A0 - A3).
4. az eredményül kapott mezőben található **R** *intézkedési index* megmutatja a tanúsító további tennivalóit.

Az intézkedési indexek R1-től R5-ig terjednek és jelentésük a következő:

- **R1**: A változás nem befolyásolja a védelmi célokat, funkciókat és mechanizmusokat, azokra irreleváns. Tesztelési dokumentum a megbízótól nem kötelező. Rövid értékelési jelentés készítendő változtatás tényéről és jellegéről (A és T paraméterek). A tanúsítvány - változatlan tartalommal, de az ismételt tanúsítás tényét feltüntetve - kiállítandó. Az értékelési jelentés és az új tanúsítvány a minősítőnek elküldendő.
- **R2**: Az eredeti besorolási szintnek megfelelő, a megbízó által kötelező jelleggel átadott teszt-dokumentumokat ellenőrizni kell. Ha azok evidensen bizonyítják, hogy a védelmi célok, funkciók és mechanizmusok az eredeti besorolási szintnek megfelelőek, akkor az értékelési jelentés és a tanúsítvány - változatlan tartalommal, de az ismételt tanúsítás tényét feltüntetve - kiállítandó. Az értékelési jelentés és az új tanúsítvány a minősítőnek elküldendő. Ha a tanúsító a teszteredmények alapján nem tud megnyugtató döntést hozni, az **R3** szerint jár el.
- **R3**: a megbízó által mindazon dokumentum átadandó az előző besorolási szintek és a változások által érintet értékelési szempontok szerint megfelelően a vonatkozó tartalmi, formai és evidencia követelményeknek megfelelően. A tanúsító mind a korrekt, mind a hatékony leképzés érintett szempontjai szerint elvégzi az ellenőrzést. Ha azok evidensen bizonyítják, hogy a védelmi célok, funkciók és mechanizmusok az eredeti besorolási szintnek megfelelőek, akkor az értékelési jelentés és a tanúsítvány - változatlan tartalommal, de az ismételt tanúsítás tényét feltüntetve - kiállítandó. Az értékelési jelentés és az új tanúsítvány a minősítőnek elküldendő. Ha a tanúsító az ellenőrzések alapján nem tud megnyugtató döntést hozni, az **R4** szerint jár el.
- **R4**: az **R3** szerint kell eljárni, de az MT előző besorolási szintjének és az érintett értékelési szempontoknak megfelelő tanúsítói tennivalókat el kell végezni. Ha ezek után a tanúsító számára egyértelmű, hogy a védelmi célok, funkciók és mechanizmusok az eredeti besorolási szintnek megfelelőek, akkor az értékelési jelentés és a tanúsítvány - változatlan tartalommal, de az ismételt tanúsítás tényét feltüntetve - kiállítandó. Az értékelési jelentés és az új tanúsítvány a minősítőnek elküldendő. Ha a tanúsító az előírt akciók után sem tud megnyugtató döntést hozni, az **R5** szerint jár el.

- **R5**: a tanúsító által összegyűjtött és értékelt információk, valamint az elvégzett ellenőrzési eljárások alapján egy megbeszélést kezdeményez a megbízóval és a minősítővel egy újbóli értékelés terjedelmének és mélységének megállapításáról. A tanúsító a megállapodás szerint az értékelést megismétli a megbízó költségére. A megismételt értékelésről jelentést készt, a tanúsítványt az értékelésnek megfelelő besorolási szint (E0 - E6) feltüntetésével kitölti. Az értékelési jelentés és az új tanúsítvány a minősítőnek elküldendő.

Az **X** intézkedési index azt jelenti, hogy az adott A/T kombinációban semmilyen intézkedés nem értelmezett.

Az R1 - R5 indexek közül az első négyre jellemző az MT előző besorolási szintje változatlan marad alapesetben, illetve a következő intézkedési index szerint kell eljárni, ha a tanúsítónak az ellenőrzés során kifogása támad. Az R5 típusú intézkedésnél kicsi a valószínűsége, hogy az eredeti besorolási szint marad, az új szint az előzőnél lehet magasabb is és alacsonyabb is.

Az ismételt minősítésű terméket a Biztonsági minősítésű informatikai termékek katalógusába be kell vezetni.

4.2. Nemzetközi szervezetek, más országok által minősített informatikai termékek minősítési folyamata és eljárásrendje

A nem hazai fejlesztésű/gyártású informatikai termékeket minden esetben minősíteni kell. Két alapkategória állítható fel:

- EK minősítéssel rendelkező termékek,
- az EK minősítési rendszerétől eltérő minősítésű termékek.

Az EK minősítéssel rendelkező termékek esetében egy egyszerűsített eljárás szerint történik a minősítés, amelynek keretében:

- a megbízó a standard eljárás szerint felveszi a kapcsolatot a minősítővel,

- szolgáltatja az előkészítő fázisra meghatározott dokumentumokat és az EK minősítési dokumentumot és az értékelésre vonatkozó jelentéseket, amelyekből később kideríthető, hogy az értékelés valóban az EK módszerével (jelenleg az ITSEC szerint) történt.
- a minősítő és a megbízó által közösen kiválasztott tanúsító a rendelkezésre bocsátott dokumentumok alapján ellenőrzi, hogy:
  - a megbízó által rendelkezésre bocsátott MT azonos-e azzal, amelyről a minősítés és az értékelési dokumentumok szólnak,
  - az MT értékelése valóban az EK biztonságminősítési módszerével készült.

  Amennyiben az ellenőrzések eredménye pozitív a hazai tanúsítványt ki kell állítani az eredetivel azonos besorolási szinten és a minősítőnek el kell küldeni, amely a tanúsítvány mellett a standard eljárás minősítési fázisában (2.4 fejezet) említett piaci, cég és egyéb információk birtokában dönt a minősítés kiadásáról.

Az EK minősítési rendszerétől eltérő minősítésű termékek esetében a minősítőnek be kell kérnie az előkészítési fázis dokumentációit, amely alapján dönt arról, hogy a tanúsítási folyamat elindítható-e. Pozitív döntés esetén a megbízóval közösen kiválasztott tanúsító az EK tanúsítási és minősítési eljárással kompatibilis módszer szerint bekéri a megbízótól a megcélzott minősítési szintnek megfelelő struktúrájú és mélységű dokumentumokat. Emellett a megbízónak külön dokumentumban kell ismertetnie az eredeti, valamint az EK tanúsítási és minősítési eljárás közötti azonosságok és különbségek leírását. Miután a tanúsító meggyőződik arról, hogy a rendelkezésre bocsátott MT és a dokumentumok egymásnak megfelelnek, megvizsgálja az eredeti és az EK módszer közötti különbségeket (pl. szempontrendszer, követelmény mélység, stb.). Ahol azonosságot talál ott elfogadja az eredeti értékelést ellenőrzés nélkül, azoknál a hazai (és egyben EK) módszer szerinti szempontoknál, amelyekre az eredeti értékelés nem tért ki és csak a most bekért dokumentumok elkészítésekor tett intézkedéseket a fejlesztő és/vagy a gyártó az értékelést a hazai módszernek megfelelően és teljes körűen el kell végezni.

A gyakorlatban az valószínűsíthető, hogy a hazai informatikai piacon túlnyomó részben amerikai és EK-beli termékek jelennek meg. Az EK-beli termékekre a korábban ismertetett egyszerűsített eljárást kell alkalmazni. Az amerikai termékek jelenleg a TCSEC-en

alapuló eljárások szerint kerülnek minősítésre. Az ITSEC kiindulási forrása a TCSEC, ennélfogva sok a hasonlóság, de vannak különbségek is. Így az amerikai termékekre az EK minősítési rendszerétől eltérő esetet kell alkalmazni, de az eljárás éppen a TCSEC és az ITSEC hasonlóságai miatt nem lesz túl bonyolult.

Az egyéb külföldi termékek esetében szintén az EK minősítési rendszerétől eltérő esetet kell alkalmazni, Az eljárás bonyolultsága az eredeti és az EK értékelési eljárás közötti különbségektől függ, azonban ez az eset - legalábbis a jelenlegi trendek alapján - nem várható jellemzőnek.

5. INFORMATIKAI RENDSZEREK TANÚSÍTÁSA ÉS MINŐSÍTÉSE

5.1. A tanúsítás és minősítés folyamata, eljárásrendje

Az informatikai rendszerek esetében az a jellemző, hogy a *megbízó* általában az a szervezet, amely a rendszert használja, működteti. A rendszer által kezelt adatok legtöbbször az ő tulajdonában legtöbbször és így az ő érdekében áll a rendszer minősíttetése. A fejlesztő általában egy vele szerződéses viszonyban álló külső cég, de gyakran előfordul, hogy egyes részeket, pl. bizonyos alkalmazásokat saját fejlesztő gárdával készíttet. Informatikai rendszer esetében - hasonlóan a termékek minősítéséhez - a minősítési folyamat egyidejű vagy követő lehet. Bár ma még nem jellemző, hogy a rendszerek fejlesztésével egy időben foglakozzanak a védelmi rendszerek tervezésével, fejlesztésével és kialakításával, amikor a minősítés már hazánkban gyakorlattá válik, remélhetőleg az egyidejű minősítés is az lesz. Így a rendszerek esetében is garantált lesz, hogy a védelmi rendszer az informatikai rendszer integráns része lesz és ugyanúgy be lesz "illesztve" a technikai, fizikai és humán környezetbe, mint maga az informatikai rendszer.

Ha *a minősítés egyidejű módon* történik, akkor a megbízó a minősítő felé már akkor célszerű, ha leadja a termék minősítésére vonatkozó igényt, amikor a fejlesztési projektre vonatkozó szerződés(ek) megkötésre kerülnek. A szerződő feleknek tudniuk kell, hogy a projekt folyamán a tanúsító és minősítő folyamat is zajlik, mert ez mindegyik szerződő partnerre, akár megbízói, akár beszállítói, akár külső fejlesztői minőségben komoly feladatokat fog számukra jelenteni. A megbízó az előkészítő fázisban a minősítő felé szolgáltatja a 2.1 pontban felsorolt dokumentumokat, amelyek az informatika rendszer esetében könnyen értelmezhetők. Közigazgatási intézmények esetében a tulajdonosi befolyással kapcsolatos dokumentumnak nincs olyan jelentősége, mint termék esetében. A tanúsító cégnek a minősítővel és a megbízóval történt közös kiválasztása után megtörténik a szerződéskötés a megbízó és a tanúsító között. A minősítés lefolytatását rendszer esetében is mindig a megbízó finanszírozza.

A szerződéskötés után az értékelési fázis lépései a fejlesztési folyamat egyes lépéseit követik. A tanúsító a védelmi igények, a védelmi célok dokumentumainak szolgáltatása után a fejlesztés előrehaladásának ütemében kapja meg az egyre "mélyebb" dokumentációkat a rendszertervtől kezdve a rendszer azon elemeinek, alrendszereinek forráskódjáig és a hardver-rajzokig terjedően, amelyek a védelmi funkciók megvalósításában részt vesznek vagy érintettek. Természetesen az egyre mélyülő dokumentációs szintet itt is a megcélzott minősítési szint követelményeinek megfelelően kell szolgáltatni a tanúsító felé. Az informatikai rendszerek esetében a helyzet annyival bonyolultabb a termékhez képest, hogy bizonyos alrendszerekre - a kezelt adatok biztonsági osztályától függően - különbözőek lehetnek a megcélzott besorolási szintek és így a dokumentum szolgáltatás struktúrája és mélysége is ennek megfelelő lesz. A korrekt és a hatékony leképzés szerinti teljes értékelés csak a fejlesztés lezárása után történhet meg, amikor a rendszer összes funkciója a valós működési feltétele között és az összes dokumentáció (pl. adminisztrátori, felhasználói) elkészült.

A besorolás, a tanúsítvány kiállítása és a minősítés a 2. fejezetben leírt standard módon történik.

Követő minősítés rendszerek esetén akkor fordulhat elő, ha a fejlesztési projektet úgy indították, hogy a biztonságminősítés nem volt kötelező, (így a rendszer működtetése nincs minősítéshez kötve), és nem is merült fel szempontként. Utólagosan azért merülhet fel a minősítés igénye, mert például erre előírás született vagy időközben olyan adatok kezelésére kerül sor, amelyek csak az adott szintre minősített rendszerrel dolgozhatók fel. Ilyenkor a működtető intézménynek, mint megbízónak részben a fejlesztőtől utólagosan kell a minősítési folyamathoz szükséges összes dokumentumot bekérni, részben saját magának kell elkészíteni hacsak eleve nem az értékelési követelményeknek megfelelően készül el dokumentáció. A minősítési folyamat és eljárásrend egyébként a standard módon zajlik le.

Az informatikai rendszerek ismételt minősítését bizonyos intervallumokban célszerű megismételni, hogy a védelmi képességi szint folytonossága biztosított legyen. Ettől eltérő esetben akkor kell ismételt minősítést végrehajtani, ha rendszerben olyan mértékű változtatás történt, ami a védelmi funkciókra is jelentős hatással van.

Az ismételt minősítést a terméknél leírt módszer szerint kell elvégezni.

6. A TANÚSÍTÓK MINŐSÍTÉSI RENDSZERE

6.1. Alapfogalmak

Ahhoz, hogy a minősített rendszer vagy termék felhasználói minden körülmények között megbízzanak az általuk használt minősített informatikai rendszer, illetve termék védettségében az ezt leíró minősítésnek egy minden potenciális felhasználó számára elfogadható, el nem kötelezett, független tanúsító értékelés eredményén kell alapulnia. Az értékeléséhez a korábban ismertetett objektív és jól körülhatárolt biztonsági követelményrendszeren túl, egy olyan nemzeti szinten elfogadott, a kiértékelési eredmények hitelességét és egységességét biztosító minősítést kibocsátó testületre, azaz minősítőre van szükség, mely igazolja, hogy a vizsgálatot megfelelő módon hajtották végre. Ennek a nemzeti szervezetnek feladata, hogy:

- meghatározza és karbantartsa az informatikai rendszerek biztonsági követelményeit,
- engedélyezze az állam szempontjából védett informatikai rendszerek létesítését, működtetését és megszüntetését,
- felügyelje és ellenőrizze információvédelmi szempontból az állam szempontjából védett informatikai rendszereket,
- meghatározza és karbantartsa az informatikai rendszerek biztonsági szempontból történő minősítésének követelményeit és eljárását,
- engedélyezze és irányítsa a tanúsítói tevékenységet,
- engedélyezze a rendszerek és termékek minősítésre bocsátását,
- az engedéllyel rendelkező tanúsítók közül (a megbízóval közösen!) kiválassza a tanúsítót,
- engedélyezze a követelményrendszernek megfelelő tanúsítási eljárások lefolytatását,

- a szabályosan lefolytatott kiértékelést követően a biztonsági osztályba sorolására vonatkozó minősítéseket bocsásson ki.

Hasonló szervezet működik a legtöbb fejlett ipari államban, így például:

* az Amerikai Egyesült Államokban a Nemzeti Számítógép Biztonsági Központ[4];
* a Német Szövetségi Köztársaságban a Szövetségi Információtechnológiai Biztonsági Hivatal;
* a Francia Köztársaságban a Központi Informatikai Rendszer Biztonsági Szolgálat.

A fentieket is figyelembe véve készült el a már többször idézett kormányrendelet-tervezet arra, hogy a Kormány e rendeletben határozzon az Informatikai Biztonsági Főfelügyelet (továbbiakban: Főfelügyelet) létrehozásáról, hogy hazánkban is létrejöjjön olyan a Kormány irányítása alatt álló, elsőfokú hatósági jogkörrel rendelkező, önálló, országos hatáskörű szervezet, amely a korábban vázolt feladatokat megfelelő szinten képes ellátni, az ezen a területen várható, az informatika fejlődésével fokozódó biztonsági követelményeket és az azoknak való megfeleltetést kézben tudja tartani.

Az informatikai rendszerek biztonsági értékelése rendkívül szerteágazó feladat, a vizsgálatot végző személyeknek széleskörű szakmai ismeretekkel kell rendelkezni az informatika területén, ugyanakkor felkészültnek kell lenniük egyéb kapcsolódó területek is, mint például a védelemtudományok vagy a minőségügy. E feladat ellátásához a Főfelügyeletnél komoly szakembergárda fenntartása lenne szükséges, amely egyrészt tovább növelné a közigazgatásban foglalkoztatottak számát, másrészt jelentősen megnövelné a Főfelügyelet működtetésének költségeit, ezért az európai gyakorlatot követve a tanúsítást megbízásos alapon független civil szervezetekkel célszerű végeztetni. Informatikai rendszerek biztonsági tanúsítását csak olyan természetes személy, illetve gazdasági társaság végezheti, aki/amely erre jogosító — a Főfelügyelet vezetője által kiadott — engedéllyel rendelkezik. A Főfelügyelet engedélyező, kijelölő és ellenőrző szerepe, az engedélyezett tanúsítókra vonatkozó előírások lehetővé teszi, hogy az állam érdekei kellőképpen érvényesüljenek, ugyanakkor a titokvédelmi előírások se szenvedjenek csorbát.

A biztonságminősítési eljárásban részt vevő tanúsító személyekre és szervezetekre kettős követelmény hárul. Egyrészt megfelelő szintű szakmai kvalifikációt kell bizonyíta-

[4] Az Európai gyakorlattól eltérően az Amerikai Egyesült Államokban a minősítő szervezet, a Nemzeti Számítógép Biztonsági Központ nem csak a minősítést végzi, hanem a tanúsítási eljárást is.

niuk, másrészt megbízhatósági követelményeknek kell eleget tenniük. Ezek a követelmények — ide nem értve a szakmai ismeretek tartalmi részét — leginkább a könyvvizsgálókkal szembeni követelményekkel vethetők össze. Ezért a kormányrendelet-tervezetben alapvetően a könyvvizsgálókra vonatkozó szabályok kerültek figyelembevételre, természetesen bizonyos eltérésekkel. Ilyen, szigorító eltérés, hogy tekintettel az államtitok és szolgálati titok széles körű megismerési lehetőségére csak magyar állampolgárságú személy végezhessen tanúsítói tevékenységet és nemzetbiztonsági ellenőrzésnek is alá kell, hogy vessse magát. Engedmény a könyvvizsgálókhoz képest, hogy tanúsító társaság esetén elegendő, ha annak egy vezető tisztségviselője saját személyében is engedélyezett tanúsító.

A megbízhatósági követelményekhez tartozik, hogy a tanúsító e tevékenysége során legyen független, el nem kötelezett és részrehajlás mentes. Ennek érdekében tanúsító a csak úgy végezheti e tevékenységét, hogy akár személyében, akár a tanúsítást végző társaság vezető tisztségviselője útján hozzátartozói vagy üzleti kapcsolat nem áll fenn az engedélyezett tanúsító és a megbízó (a rendszer vagy termék tervezője, fejlesztője, gyártója, forgalmazója vagy üzemeltetője), illetve annak vezető tisztségviselője között, ezekben az esetekben, továbbá ha az engedélyezett tanúsító bármely egyéb oknál fogva elfogult a tanúsító köteles visszautasítani a vizsgálatra szóló megbízást. A tanúsítót e tevékenysége körében megbízója vagy munkáltatója nem utasíthatja.

6.2. Követelményrendszer

Tanúsítási és más azzal összefüggő informatikai biztonsági vizsgálati tevékenységet csak olyan személy vagy társaság végezhet, aki/amely erre jogosító engedéllyel, “Tanúsítói Igazolvánnyal” rendelkezik és a tanúsítók névjegyzékében szerepel.

Tanúsítói Igazolványtatására az a személy kaphat engedélyt, aki

- büntetlen előéletű magyar állampolgár,
- felsőfokú végzettséggel rendelkezik,
- a minősítő által előírt szakvizsgával rendelkezik,
- legalább hároméves szakmai gyakorlatot igazol és
- a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 68. § (4) e.) pont szerinti biztonsági ellenőrzésnek nyilatkozatával aláveti magát.

A tanúsító engedélyét a minősítő visszavonja, ha

- az engedélyezett tanúsító kéri;
- az engedélyezett tanúsító elhalálozott;
- az engedélyt visszavonták.

Tanúsítási és más azzal összefüggő informatikai biztonsági vizsgálati tevékenység folytatására az a gazdasági társaság kaphat engedélyt:

- amelyik a cégbíróság által bejegyzett gazdasági társaságként működik,
- amelynek tevékenységi körére vonatkozóan a társaság alapító okiratában az informatikai és a biztonsági tevékenységhez kapcsolódó tevékenységet megjelöltek (számítástechnikai és ehhez kapcsolódó tevékenységek, a gazdasági tevékenységet segítő szolgáltatások, nyomozási és biztonsági tevékenység),
- amelynek keretében az engedélyezett tanúsítók névjegyzékébe bejegyzett természetes személyek végzik tagként, alkalmazottként vagy vezető tisztségviselőként a biztonsági vizsgálatot,
- amelynél a szavazati jogok többségével olyan természetes személyek vagy társaságok rendelkeznek akik az engedélyezett tanúsítók névjegyzékébe engedélyezett tanúsítóként bejegyeztek,
- amelynek vezető tisztségviselői között legalább egy olyan természetes személy van aki engedélyezett tanúsító és
- amelynek köztartozása nincs.

A minősítő a tanúsító engedélyét visszavonja és annak tényét azt nyilvánosságra hozza, ha az engedélyezett tanúsító alkalmatlanná vagy méltatlanná vált e tevékenység ellátására, az engedélyét lejártakor nem újítja meg, illetőleg ha olyan körülmény merül fel, amely az engedélyezést kizárná.

A személyi felelősség biztosítása érdekében a tanúsítói engedéllyel rendelkező társaság nevében is csak a társaságnál természetes személyként engedélyezett tanúsítók végezhetik a tanúsítási tevékenységet, az értékelési jelentést és a tanúsítványt egy, a társaságnál bejelentett engedélyezett tanúsító, mint felelős vezető kell, hogy aláírja.

A szükséges ismeretek sokrétűsége miatt az értékelési tevékenységbe Tanúsítói Igazolvánnyal nem rendelkező személyek is bevonásra kerülhetnek, de azok személyét állandó jelleggel vagy egy meghatározott vizsgálathoz a társaság vezetőjének be kell jelentenie.

A tanúsítást végző személyek felkészültségükről a korábban említett szakvizsga keretében kell, hogy számot adjanak. A szakvizsga az alábbi témákra terjed ki:

- **Informatika**
  - *számítástechnikai eszközök*
  - *hálózati rendszerek*
    - a Nyílt Rendszerek Architektúrája (ISO-OSI)
    - helyi és kiterjedt hálózatok (LAN: Local Area Networks, WAN: Wide Area Networks)
    - kommunikációs rendszerek
  - *informatikai rendszerek életciklusa*
  - *projekt menedzsment*
  - *informatikai stratégia*

    informatikai biztonság
    - alapfogalmak (adatvédelem, titokvédelem, információvédelem, információbiztonság, informatikai biztonság, informatikai biztonsági auditálás, informatikai rendszerek és termékek biztonságminősítése)
    - az informatikai biztonság fogalma
    - az informatikai biztonsági koncepció és politika,
    - az informatikai biztonsági stratégia,
    - az adminisztratív, a fizikai és a logikai védelmi rendszerek tervezése;
- **Informatikai rendszerek biztonsági követelményei (MeH ITB 12. sz. ajánlás)**
  - *biztonsági osztályok,*
  - *osztott rendszerek összekapcsolhatósága,*
  - *követelmények az információvédelem (IV) és a megbízható működés (MM) területein;*
- **Informatikai biztonsági vizsgálat**
  - *tanúsítás,*
  - *belső és külső audit;*
- **Auditálási (vizsgálati) módszertan (MeH ITB 8 sz. ajánlás)**
- **Értékelési módszertan (jelen tanulmány)**
- **Jogi és egyéb szabályozások, szabványok, ajánlások**
  - *jogszabályok*

    - a személyes adatok védelme,
    - az államtitok és a szolgálati titok védelme,
    - az üzleti, a bank- és az egyéb szakmai titkok védelme,
    - a közérdekű adatok nyilvánossága,
    - iratok és dokumentumok védelme és kezelése,
    - tűz- és vagyonvédelem,
    - gazdálkodási előírások,
    - államigazgatási alapismeretek;
  - *szervezeti szintű belső szabályozások, amelyek az informatikai biztonságot szabályozzák, illetve érintik*
  - *szabványok, előírások*
  - *ajánlások az informatikai biztonság területén*
- **Általános biztonsági ismeretek.**
  - *az élőerős őrzés,*
  - *a mechanikai védelem informatikai környezetben,*
  - *elektronikai védelem,*
  - *A tűzvédelem eszközei informatikai környezetben.*

6.3. A minősítés folyamata, eljárásrendje

A tanúsító engedélyezése vagy más szóval azok minősítése (akkreditálás) annak hivatalos elismerése, hogy valamely személy vagy szervezet felkészült a tanúsítás meghatározott feltételek szerinti végzésére. A tanúsítási tevékenység folytatására a minősítő ad ki engedélyt.

Az engedélyezési eljárást annak kell kezdeményezni, aki tanúsítói tevékenységet kíván folytatni.

Amennyiben a természetes személy, aki engedélyezett tanúsító szeretne lenni és még nem rendelkezik szakvizsgával, a minősítőnél jelentkezik szóban vagy írásban. A minősítő megadja hogy mikor lesz megtartva a következő szakvizsga, arra milyen témákból kell felkészülni, illetve hol és mikor lehet felkészítő tanfolyamon részt venni. A szakvizsga sikeres abszolválásáról a vizsgázó igazolást kap.

A tanúsítói engedélyért folyamodó a minősítőhöz írásban kell, hogy ilyen irányú kérelmét benyújtsa. A kérelemhez mellékelni kell a szükséges dokumentumok (erkölcsi bizonyítvány, iskolai végzettségről szóló oklevelek, bizonyítvány a szakvizsgáról, illetve társaság esetén a cégbejegyzésről szóló végzés, a társaságnál tevékenykedő tanúsítók igazolványa) hivatalos másolatát, a nyilatkozatokat (gyakorlatról, nemzetbiztonsági ellenőrzésről, illetve társaság esetén a köztartozásokról) és az előírt illetéket.

A minősítő a kérelmeket harminc napon belül elbírálja. Amennyiben a kérelmező az előírásoknak nem felel meg elutasítja a kérelmet. Hiányosan vagy nem egyértelmű adatokkal, dokumentumokkal benyújtott kérelem esetén hiánypótlásra szólítja fel a kérelmezőt, és ha az, az előírt határidőn belül a felhívásnak nem tesz eleget a minősítő a kérelmet elutasítja. A feltételeknek megfelelő kérelem esetén értesíti a kérelmezőt kérelmének pozitív elbírálásáról és arról, hogy mikor kell esküt tennie. Az eskü letétele és írásos megerősítése után a minősítő “Tanúsítói Igazolvány”-t ad ki és felveszi az engedélyezett tanúsítók névjegyzékébe.

7. ÖSSZEFOGLALÁS

Az informatikai terméke és rendszerek biztonságminősítési rendszerének tervét ismerteti a jelen dokumentum, amelynek aktualitását az adja meg, hogy a korábban hivatkozott kormányrendelet-tervezet a számítástechnikai és távközlési rendszerek információvédelmi felügyeletének és megfelelőség-vizsgálatának rendjéről, valamint a kormányrendelet-tervezet a minősített adat kezelésének rendjéről szóló 79/1995. (VI.30.) Korm. Rendelet módosítása jelenleg tárcaközi egyeztetés alatt áll. Az ezekkel kapcsolatos döntések meghozatala után megteremtődik az a szervezeti és szabályozási feltétel rendszer, amely lehetővé teszi egy, az Európai Közösség rendszerével kompatibilis biztonságminősítési rendszer létrehozását. Ezzel lehetővé válik a közigazgatás területén az informatikai rendszerek minősítése. Ennek szabályozott ismétlésével folyamatosan mérhetővé válik a megvalósított biztonság szintje és a követelmények közötti viszony. A termékek vonatkozásában szintén mércét jelent a felhasználók számára az adott biztonsági osztályú rendszerbe történő termék beépítést illetően. Ezen túlmenően megkönnyíti a hazai fejlesztésű informatikai termékek minősítésének elfogadtatását az EK területén és viszont.

A minősítési rendszer kialakításának fontos feltétele a minősítés hatósági jogkörét gyakorló Informatikai Biztonsági Főfelügyelet létrejöttén túlmenően a tanúsítási jogosítvánnyal rendelkező cégek megjelenése, amelyek akkreditálási rendszerének tervét szintén tartalmazza a jelen dokumentum.

Ezzel remélhetőleg a közigazgatás területén működő és működtetendő rendszerek, valamint a felhasználandó informatikai termékek biztonságminősítési rendszerének kialakításához szükséges információt és elgondolást terv szinten tartalmaz a dokumentum, amely egyben kiindulási alapja lehet egy egyeztetési folyamat után a további szükséges részletek kidolgozásához.

8. FOGALOMMAGYARÁZAT

Jelen fejezet tartalmazza az ebben a dokumentumban egyedi értelmezéssel használt műszaki kifejezések definícióit. A dokumentumban használt, de itt nem definiált műszaki kifejezések a dokumentum egészében, annak általánosan elfogadott jelentése szerint értelmezendők.

Akkreditáció: (Accreditiation) a körülményektől függően kétféle jelentése lehet:

a) az adott környezetben való használatra egy IT rendszer elfogadásának folyamata;

b) az a folyamat, melynek során vonatkozó feladatok végrehajtására elismerik egy ellenőrző laboratórium műszaki kompetenciáját, pártatlanságát.

Alany: (Subject) Egy aktív elem, mely általában egy személy, folyamat, vagy berendezés. [TCSEC]

Alap alkotóelem: (Basic Component) az alkotóelem, melyet a részletes tervezés során készülő specifikáció legalacsonyabb hierarchikus szintjén kell azonosítani.

Alkalmazás: (Implementation) a fejlesztési folyamatnak azon szakasza, melyben a kiértékelés tárgyának részletes specifikációja hardware-ben és software-ben valósul meg.

Alkotóelem: (Component) a kiértékelés tárgyának egy beazonosítható része.

Átvételi eljárás: (Acceptance Procedure) az a folyamat, mely a kifejlesztés, előállítás, vagy karbantartás során létrejövő tárgyakat a kiértékelés tárgyához való csatolásra elfogad és melynek pozitív következménye, hogy ezeket a konfiguráció vezérlési rendszer felügyelete alá helyezi.

Behatolási teszt: (Penetration Testing) egy, a kiértékelés tárgyán a kiértékelő által végrehajtott ellenőrzés, melynek során megállapíthatóak, hogy vannak-e a gyakorlatban kiaknázható, ismert gyenge pontok

Besorolás: (Rating) egy, a kiértékelés tárgya által lehetségesen tartalmazott garanciák mérése; amely áll a védelmi célra való hivatkozásból, valamint azon kiértékelési szintből, melyet a valós vagy tervezett működtetési összefüggésben alkalmazásának helyességére, illetve hatékonyságának célkitűzéseire lefolytatott vizsgálat során nyertek, továbbá védelmi mechanizmusai minimális erejének igazolt osztályba sorolása.

Bizalmasság: (Confidentiality) az engedélyezetlen információ kibocsátás elleni védelem.

Biztonságpolitika: (Security Policy) lásd: Intézményi Biztonságpolitika, Informatikai Biztonságpolitika

Biztonságpolitika formális modellje: (Formal Model of Security Policy) a formális módon elkésztett védelmi irányelvek alapmodellje, például a működési környezet által érvényesítendő fontos védelmi célkitűzések elvonatkoztatott, absztrahált meghatározása.

Dokumentáció: (Documentation) a kiértékelés tárgyáról írásos úton késztett (vagy más módon rögzített), a kiértékeléshez szükséges információ. Ezen információt az adott tárgyhoz készített egy, vagy több dokumentum tartalmazhatja.

Eszköz: (Tool) a védelem céljának felépítéséhez és/vagy dokumentálásához használt termék.

Evidencia követelmények: (Requirements for Evidence) az értékelési tevékenységre, vagy az értékelés adott szempontjára vonatkozó elvárások csoportja, melyben azon bizonyítékok vannak meghatározva, amelyből kiderül, hogy a tevékenységre vagy szempontra vonatkozó követelményeknek eleget tett.

Értékelés: (Evaluation) egy IT rendszernek, vagy terméknek kiértékelési kritériumok szerinti vizsgálata.

Értékelő: (Evaluator) a kiértékelést végrehajtó független személy, vagy szervezet.

Értékelői eljárások: (Evaluator Actions) a kiértékelés adott szakaszának, vagy szempontjának megfelelő értékelési fázisa, melyben meghatározásra kerül, hogy a kiértékelés megbízója által rendelkezésre bocsátott információ ellenőrzésére az értékelőnek mit kell tenni, illetve milyen más kiegészítő tevékenységeket kell végrehajtani.

Fejlesztési környezet: (Development Environment) a fejlesztés tárgyának előállítása során érvényesített szervezeti intézkedések, eljárások és szabványok.

Fejlesztési folyamat: (Development Process) a feladatoknak és azok végrehajtási fázisainak azon csoportja, mely révén a kiértékelés tárgya úgy valósul meg, hogy a követelmények a valós hardware-be és software-be beépítésre kerülnek.

Fejlesztő: (Developer) az a személy, vagy szervezet, amely a kiértékelés tárgyát előálltja.

Fejlesztői biztonság: (Developer Security) a fejlesztőnek a fejlesztési környezetére gyakorolt fizikai, eljárási és személyi védelmi szabályozói, biztonsági intézkedései.

Felhasználói dokumentáció: (User Documentation) a fejlesztő által a végfelhasználó részére, a kiértékelés tárgyáról késztett információ.

Folyamatokra és szabványokra vonatkozó követelmények: (Requirements for Procedures and Standards) az értékelési tevékenységre, vagy az értékelés adott szempontjára vonatkozó elvárások csoportja, melyben azonosításra kerül a működési környezet valós működési környezetre való adaptálásakor használatos folyamatok, vagy eljárások természete és/vagy tartalma.

Funkcionális egység: (Functional Unit) egy alap alkotóelem funkcionálisan elkülönülő része.

Funkcionális megfelelés: (Suitability of Functionality) a kiértékelés tárgya hatékonysági vizsgálatának egy tárgya, amely megmutatja, hogy a védelemerősítő funkciói és mechanizmusai alkalmasak-e a kiértékelés tárgyának védelmi céljában meghatározott, a védelmet fenyegető veszélyek valós leküzdésére.

Funkcionalitási osztály: (Functionality Class) a kiegészítő védelemerősítő funkciók előre meghatározott csoportja, melyet a kiértékelés tárgyában alkalmazni lehet.

Funkciók szinergikus kapcsolata: (Binding of Functionality) a kiértékelési tárgy hatékonysági vizsgálatának egyik aspektusa, nevezetesen, hogy a védelemerősítő funkciói és mechanizmusai képesek-e egymást kölcsönösen támogatva, egy integrált egységes egészet képezve, együtt dolgozni.

Garancia: (Assurance) az a bizalmi szint, amelyet a kiértékelés tárgyának biztonsága, védettsége nyújt.

Garancia profil: (Assurance Profile) a működési környezetnek azon, garanciával összefüggő követelménye, hogy a különböző védelemerősítő funkciókban más-más bizalmi szint megvalósulására van szükség.

Gyengepont: (Vulnerability) a kiértékelés tárgya védettségének, biztonságának gyenge eleme (például az analízis, tervezés, alkalmazás, vagy működtetés hibáiból eredően).

Gyengepont vizsgálat: (Vulnerability Assessment) a kiértékelés tárgya hatékonysági vizsgálatának egyik szempontja, nevezetesen, hogy a kiértékelés szempontjának ismert gyenge pontja veszélyeztetheti-e a védelmi célban meghatározott védettséget.

Hatékony leképzés: (Effectiveness) a kiértékelési tárgy egy tulajdonsága, mely rámutat, hogy a valós, vagy tervezett működtetési környezetben mennyire valósul meg a védettség.

Informatikai Biztonságpolitika: (System Security Policy) törvényeknek, szabályoknak és eljárásoknak azon csoportja, mely szabályozza, hogy egy adott rendszeren belül az érzékeny információkat és más eszközöket hogyan kell kezelni, védeni és kibocsátani.

Integritás: (Integrity) az információ engedélyezetlen módosításának megakadályozása.

Intézményi Biztonságpolitika: (Comporate Security Policy) a törvényeknek, szabályoknak és gyakorlati eljárások olyan csoportja, mely meghatározza, hogy a felhasználói szervezetben miként kell kezelni, védeni és kibocsátani eszközöket, ide értve az érzékeny információkat is.

Kezelő: (Administrator) A kiértékelés tárgyával kapcsolatban lévő, üzemeltetésért felelős személy.

Kezelői dokumentáció: (Administration Dokumentation) a fejlesztő által a kezelő részére készített, a kiértékelés tárgyára vonatkozó információ.

Konfigurálás: (Configuration) a kiértékelés tárgyának jellemzői alapján egy lehetséges kombináció-csoport kiválasztása.

Korrekt leképezés: (Correctness) a kiértékelési tárgy olyan tulajdonsága, mely megmutatja, hogy a rendszer, vagy termék pontosan tükrözi a rögzített védelmi célban foglaltakat.

Követelmények: (Requirements) a fejlesztési folyamatnak azon szakasza, melyben a kiértékelés tárgyának védelmi célját határozzák meg.

Kritikus mechanizmus: (Critical Mechanism) egy, a kiértékelés tárgyán belül szereplő mechanizmus, melynek meghibásodása, a védettség, a biztonság gyengülését idézheti elő.

Mechanizmusok ereje: (Strength of Mechanisms) a kiértékelés tárgya hatékonysági vizsgálatának egyik szempontja, nevezetesen azon képesség, hogy a védelmi mechanizmusok képesek-e az azt alátámasztó algoritmusok, irányelvek, vagy tulajdonságok hibás működéséből származó közvetlen támadásnak ellenállni.

Megbízó: (Sponsor) a kiértékelést kérő személy, vagy szervezet.

Megvalósítás: (Construction) a kiértékelés tárgyának felépítési, elkészítési folyamata.

Minősítés Tárgya: (Target of Evaluation) IT rendszer, vagy termék, melynek a védettség kiértékelését el kell végezni

Működés: (Operation) a kiértékelés tárgyának használatát kifejező folyamat.

Működési eljárás, folyamat: (Operating Procedure) a kiértékelés tárgyának helyes használatát definiáló szabályok csoportja.

Működési-üzemeltetési dokumentáció: (Operational Documentation) a fejlesztő által a kiértékelés tárgyáról késztett leírás, melyben meghatározza és bemutatja annak használatát.

Működési környezet: (Operational Environment) a kiértékelés tárgyának működtetése alatt használandó szervezeti intézkedések, eljárások és szabványok.

Programozási nyelvek és fordítók: (Programming Languages and Compilers) a fejlesztési környezetben használt olyan eszköz mely a kiértékelés tárgyának software-ének és/vagy firmware-nek előállítására alkalmas.

Rendszerterv: (Architectural Design) a kifejlesztési folyamatnak az a szakasza, melyben a kiértékelés tárgyának felső szintű definíciója és terve kerül meghatározásra.

Rendelkezésre állás: (Availability) információk, vagy eszközök engedélyezetlen megtagadásának, vagy visszatartásának megelőzése.

Rendszer: (System) egy adott rendeltetéssel és működtetési környezettel bíró, egyedi IT installáció.

Részletes terv: (Detailed Design) a fejlesztési folyamatnak az a szakasza, amelyben a kiértékelés tárgyának felső szintű leírását, tervét finomítják és olyan részletességi szintre bontják, mely már alapja lehet az alkalmazásnak.

Szállítás: (Delivery) az a folyamat, amikor a kiértékelés tárgyának egy másolata, példánya a fejlesztőtől az ügyfélhez kerül.

Tanúsítás: (Certification) egy kiértékelés eredményeit igazoló formális nyilatkozat kibocsátása, melyből kiderül, hogy a kiértékelési követelményrendszert, kritériumokat megfelelően alkalmazták.

Tanúsító szervezet, személy: (Certification Body) egy független, pártatlan, bizonylatolást végző gazdasági társaság vagy személy.

Tartalmi és formai követelmények: (Requirements for Content and Presentation) az értékelési tevékenységre, vagy az értékelés adott szempontjára vonatkozó elvárások csoportja, amely azonosítja, meghatározza, hogy az értékelési szakasz, vagy szempont szerint fontosnak minősülő, a dokumentációban szereplő tételeknek mit kell tartalmazniuk és hogy az ezekre vonatkozó információnak milyen formában kell szerepelni.

Tárgy: (Object) Olyan passzív elem, mely információt tartalmaz, vagy fogad.

Tárolóeszköz: (Storage Object) egy olyan eszköz, mely mind az olvasási, mind az írási hozzáférést lehetővé teszi [TCSEC].

Termelés: (Production) az a folyamat, melynek során a kiértékelés tárgyát vásárlók részére készítik.

Termék: (Product) egy IT software és/vagy hardware csomag, melyet funkcionálisan úgy terveztek meg, hogy alkalmas legyen a használatra, vagy rendszerbe történő beépítésre is.

Termék Besorolási Ismertető: (Product Rationale) egy termék védelmi adottságainak leírása, melyből a jövőbeli vásárló eldöntheti, hogy a termék kielégíti-e , megfelel-e saját biztonságpolitikájának.

Ügyfél: (Customer) az a személy, vagy szervezet, amely a kiértékelés tárgyát megvásárolja.

Változás menedzselés: (Configuration Control) a kiértékelés tárgyának fejlesztési, előállítási és karbantartási folyamatai alatt megvalósuló, változások révén keletkező eszközöket menedzselő rendszer.

Veszély: (Threat) egy olyan művelet, vagy esemény, amely sértheti a védettséget, biztonságot.

Védelem megvalósítás: (Security Enforcing) ami,a kiértékelés tárgya védelmi igényének megfeleléshez közvetlenül hozzájárul.

Védelmet segítő: (Security Relevant) az, ami nem védelemerősítő, de megfelelő működése szükséges ahhoz, hogy a kiértékelés tárgya biztosítani tudja a védettséget.

Védelmi cél: (Security Target) a kiértékelés tárgyától megkövetelt védettség specifikációja, mely alapul szolgál a kiértékeléshez. A védelmi cél fogja meghatározni a kiértékelés tárgyának védelemerősítő funkcióit. Ez fogja továbbá meghatározni a védelmi célkitűzéseket, az ezen célkitűzéseket fenyegető veszélyeket, valamint bármely alkalmazásra kerülő védelmi mechanizmust.

Védelmi igény: (Security Objectives) a védettség azon foka, melyet a kiértékelés tárgya meghatároz.

Védelmi mechanizmus: (Security Mechanism) olyan logikai felépítés, vagy algoritmus, amely hardware-ben, vagy software-ben egy adott védelemerősítő, vagy a védelem szempontjából fontosnak minősülő funkciót alkalmaz.

Védelmi stabilitás: (Ease of Use) a kiértékelési tárgy hatékonysági vizsgálatának egyik aspektusa, melynek során megállapítást nyer, hogy nem használható, vagy konfigurálható a biztonságot, védettséget sértő módon, még ha a kezelő, vagy végfelhasználó joggal hiszi is, hogy az biztonságos, védett.

Védettség, biztonság: (Security) a titkosság, az sérthetetlenség és a rendelkezésre állás kombinációja.

Végfelhasználó: (End-user) azon személy, aki a kiértékelés tárgyának csak a működését veszi igénybe.

9. IRODALOMJEGYZÉK

1. Informatikai biztonsági módszertani kézikönyv. Az Informatikai Tárcaközi Bizottság 8.sz. ajánlása. Budapest, 1994.
2. Informatikai rendszerek biztonsági követelményei Az Informatikai Tárcaközi Bizottság 12.sz. ajánlása (tervezet). Budapest, 1996.
3. Information Technology Security Evaluation Criteria (ITSEC☺. Version 1.2.EC DG XIII. 1991. május.
4. Information Technology Security Evaluation Manual (ITSEM). Draft V0.2. 1992. április.
5. Trusted Computer System Evaluation Criteria (TCSEC) — Amerikai Egyesült Államok Védelmi Minisztériuma (USA DoD). (Orange Book of the Security of Information Systems)
6. Trusted Product Evaluations. A Guide for Vendors. National Computer Security Center. USA. NCSC-TG-002. Version-1. 1990. június.
7. Trusted Network Interpretation Enviroments Guideline. - National Computer Security Center, USA, 1990 augusztus.
8. IT-Grundschutzhandbuch. Schiftenreihe zur IT-Sicherheit. Band 3. - Bundesamt für Sicherheit in der Informationstechnik, 1995.
9. UK IT Security Evaluation and Certification Scheme. UK Certified Product List. UKSP 06. 2. kiadás. 1993. április.

Budapest, 1996. december 05-én