ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel

Információbiztonsági szabványok

egyetemi jegyzet

Szádeczky Tamás

Nemzeti Közszolgálati Egyetem

Budapest, 2014

Tartalom

Bevezetés

Az előző évszázad közepétől hatalmas fejlődés volt tapasztalható a számítástechnika területén. Az első otthoni Commodore 64-esünk és az elszigetelt BBS-ek[1] használata óta eljutottunk az egész életünket átszövő informatikai eszközök és hálózatok garmadájáig: okostelefon, notebook, Internet, amelyek táptalaján egy egész virtuális világ alakult ki. Ebben a virtuális világban a való világban tapasztalható jelenségekhez többé vagy kevésbé hasonló jelenségek tapasztalhatók. Kriminológusok vitatkozhatnak azon, hogy bizonyos bűncselekmények virtuális világban történő végrehajtása eltér-e a való világban történő elkövetéstől. Ami viszont mindenképpen egyedi: a védelem technikai végrehajtásának módja és lehetőségei. Az informatikai biztonság és védelem magába olvaszt elemeket a hagyományos területekből, mint a katonai védelem vagy a vagyonvédelem, viszont azoktól merőben eltérő tulajdonságai is vannak. Az informatikai biztonság különlegességére és fontosságára való rádöbbenés időszaka hazánkban a kilencvenes évekre tehető. Ekkor még minden biztonságról szóló dokumentumban fogalommagyarázatokat kellett feltüntetni és el kellett magyarázni, hogy ez az egész terület miért fontos. Húsz év alatt a biztonsági szakma kiharcolta létjogosultságát, az informatikai biztonságot alkalmazók, azt megfizetők többé-kevésbé tudják, hogy fontos ez a terület. A kérdés a huszonegyedik század elején nem a *miért*, hanem a *hogyan* és a *mennyire*. Az üzleti szférában – a gazdasági világválság idején különösen – nem létezik elég olcsó, nincs olyan kötelező kiadás, amiből ne akarnának még egy kicsit lefaragni. A cél viszont elérendő: az állampolgárok, a shareholderek,[2] a stakeholderek[3] és az állam célja is, hogy mindenhol – úgy az üzleti, a magánéletben és az állami szférában is – megfelelő informatikai biztonsági szint kerüljön kialakításra és fenntartásra. Nap, mint nap tapasztaljuk, hogy a biztonság oltárán való áldozat értéke a költségvetés csökkenésével négyzetesen arányos mértékben csökken. Amíg egy nagy távközlési cég esetében szinte soha nem lehet komoly hiányosságot találni, addig az otthoni számítógépére a felhasználó gyakran még az ingyenes védelmi eszközöket sem telepíti fel. Nyilván ennek rendkívül sok oka lehet: például a szakmai ismeretek,

[1] Bulletin Board System, 1970-1990 között használatos terminálcsatlakozást lehetővé tévő közösségi számítógépek elsősorban fájlmegosztás céljára.
[2] tulajdonos, részvényes
[3] a szervezet működésében érdekelt illetve érintett felek összessége

tapasztalat, információ, pénz, érdeklődés hiánya, de mindemellett a figyelem felhívása sem történik meg a területre, valamint a későbbi felelősségre vonhatóságra. A felelősségre vonhatóság pedig fontos tényező, hiszen a jogalkotó szempontjából nincs teljes megfelelés, mindenen lehet még javítani, az elérendő cél a tökéletesség.

1. Szabványosítás

A szabványosítás nem más, mint az egységesítésre irányuló törekvés. A szabványosítás történelme – ha nem is a mai formában – a régmúltban, az ösztönös szabványosítással kezdődött, amikor kialakultak a nyelvek és számrendszerek, biztosítva az egységes kommunikációt a csoportokon belül. A mértékegységek rendszerének kialakulása volt a tudatos szabványosítás eszköze, a kereskedelem, az adószedés, fegyvergyártás tette ezt szükségessé. A mértékegységek eleinte emberi testrészek voltak, de mivel ezek egyedi biometrikus jellemzői az embernek, a szabvány etalonja az uralkodó volt, az ő testméretei határozták meg a mértékegység tényleges értékét.[4] Így például a hüvelyk (digitus, Zoll, inch) a hüvelykujj szélessége az első ízületnél (kb. 25 mm), a láb (pes, Fuss, foot) a lábfej hosszúsága a sarokcsonttól a nagylábujj végéig (kb. 0,3 m), a kisarasz a kifeszített hüvelyk- és mutatóujj végei között lévő távolság, nagyarasz a kifeszített hüvelyk- és kisujj végei között lévő távolság, a rőf (Reif) a mellkas közepétől számított kartávolság (kb. 0,78 m), és a yard a király orrhegye és kinyújtott karjának hüvelykujjhegye közötti távolság (kb. 0,91 m). Nyilvánvalóan az uralkodóváltások kisebb metrológiai katasztrófát jelenthettek, ezért felmerült az igény az egységesítésre, de erre csak az 1790-es években került sor, Talleyrand francia püspök javaslatára, a méter és prefixumainak meghatározásával (a Párizson áthaladó délkör negyedének tízmilliomod része, amely mérhető és számítható is volt), törvénybe iktatásával és az ősetalon elkészítésével.

A szervezett szabványosítás a nemzeti szabványügyi szervek megalakításával kezdődött a XX. században, amikor is először 1901-ben Londonban megalakították az Engineering Standards Committee-t. Magyarországon két évtizeddel később, 1921-ben alakították meg az ennek megfelelő Magyar Ipari Szabványügyi Intézetet. A szabványosítás legújabb generációja a nemzetközi szabványosítás, amely csak kis késéssel követte a nemzeti szabványosítás szintjét. 1906-ban alakult a Nemzetközi Elektrotechnikai Bizottság (IEC), majd 1928-ban a Nemzeti Szabványügyi Testületek Nemzetközi Szövetsége (ISA).

---

[4] Pleplár Gábor (2009): Bevezetés a fizikába.
http://aagk.hu/jegyzetek/9_10_alapfogalmak.doc [2014. 03. 08.], p. 1.

A történelmi áttekintés után a modern szabványosítás főbb jellemzőit és kategóriáit érdemes áttekinteni. Először is a szabványosítás fogalma – amelyet természetesen szabvány határoz meg – a következő:

„Szabványosítás: olyan tevékenység, amely általános és ismételten alkalmazható megoldásokat ad fennálló vagy várható problémákra azzal a céllal, hogy a rendező hatás az adott feltételek között a legkedvezőbb legyen."[5]

A szabványosítás feladata a szabványok kidolgozása, kibocsátása, és alkalmazása. A szabványosítás eredménye fokozza a termékek, eljárások, szolgáltatások rendeltetésszerű alkalmasságát, elhárítja a kereskedelem termékekkel, szolgáltatásokkal kapcsolatos technikai akadályait és elősegíti a technológiai együttműködést. Egységesíti például a rajzjeleket, a terminológiát, a vizsgálati módszereket és a betartandó követelményeket.

A szabványosításnak több szintje van, melyek közül a legmagasabb a nemzetközi szabványosítás, ebben bármely ország illetékes szervei részt vehetnek. Nemzetközi szintű szabványügyi szervek a Nemzetközi Szabványügyi Szervezet (International Organization for Standardization, ISO), melynek hazánk 1947 óta tagja, a Nemzetközi Elektrotechnikai Bizottság (International Electrotechnical Commission, IEC) és a Nemzetközi Távközlési Unió (International Telecommunication Union, ITU), amely az ENSZ szakosított szerve.

A regionális szabványosítás olyan szabványosítás, amelyben a világ csak egy meghatározott földrajzi, politikai vagy gazdasági területéhez tartozó országok illetékes testületei vehetnek részt. Regionális szabványügyi szervek például az Európai Szabványügyi Bizottság (Comité Européen de Normalisation, CEN), Európai Elektrotechnikai Szabványügyi Bizottság (Comité Européen de Normalisation Electrotechnique, CENELEC) és az Európai Távközlési Szabványügyi Intézet (European Telecommunications Standards Institute, ETSI).

A nemzeti szabványosítás egy meghatározott ország szintjén folyó szabványosítás. Nemzeti szabványügyi szervek például a Magyar Szabványügyi Testület (MSZT), British Standards Institution (BSI), Deutsches Institut für Normung e.V. (DIN), és az American National Standards Institute (ANSI).

Vállalati szabványosításról beszélhetünk, ha a gazdasági társaság a saját szervezetén belül érvényes, általában kötelező, többnyire termékhez kapcsolódó műszaki előírást

[5] MSZ EN 45020:2007 (ISO/IEC Guide 2:2004)

készít és alkalmaz, biztosítja a nemzeti szabvány vállalati szintű végrehajtását.[6] A vállalati szabványok betartását a beszállítótól is megkövetelhetik.
Látható, hogy a szakmai kompetencia tekintetében a magasabb szinteken egy távközlési, egy elektrotechnikai és egy általános szabványügyi szerv került megalakításra. Az ilyen szervezetekben műszaki bizottságok (Technical Committee, TC) végzik az operatív munkát. Manapság a fent ismertetett hierarchikus rend mellett sok esetben összetettebb a helyzet az informatikai szabványosítás területén és sok olyan szervezet készít de facto szabványokat, amelyek eddig nem végeztek ilyet.[7]
A szabványok jelölésében először a kibocsátói jel(ek)et kell feltüntetni. Ez magyar nemzeti szabvány esetén MSZ, ISO szabvány esetén ISO, brit szabvány esetén BS, német szabvány esetén DIN, és így tovább. A szabvány rendelkezik egy azonosító jelzettel, más néven szabványszámmal, majd egy kettőspont után feltüntetésre kerül a közzététel évszáma. Ilyen módon egységesen és egyértelműen lehet hivatkozni a szabványokra. A közzétételi évszám nélkül hivatkozott szabvány a legújabb kiadást jelenti.

Jelen mű szempontjából nézve a kérdést, a non-ius szabályozási módok közül az egyik legeredményesebb forma a szabványok használata. A szabványosítás definíció szerint olyan tevékenység, amely általános és ismételten alkalmazható megoldásokat ad fennálló vagy várható problémákra azzal a céllal, hogy a rendező hatás az adott feltételek között a legkedvezőbb legyen. Esetünkben az informatikai biztonsági kihívásokra adott válaszok optimalizálása a céljuk. A számítógéprendszerek és hálózatok eredő biztonságát az egyes építőelemek közül a leggyengébbnek a biztonsága határozza meg (leggyengébb láncszem elve). A szabványok alkalmazásának a legnagyobb előnye ezen gyengeségek kiküszöbölése azáltal, hogy minden elemet egyenlő szintre hoz. a szabványok nélküli biztonság-kialakítás lehetséges, de nem megbízható, hiszen nem lehet a szabványosságot, mint formális objektív mércét használni. Az informatikai biztonság megfelelőségének biztosítása más esetekben is szükséges lehet, mint például minőségirányítási rendszer bevezetése, compliance vagy beszállítói audit esetén. Jelen esetben a szabvány fogalmát tágabb értelemben vesszük, a hangsúly a non-ius-on van, nem a szabvány formai

[6] Forgács László (2004): A magyar szabványosítás jogharmonizációja, Bányászati és Kohászati Lapok – Bányászat, 137. évfolyam, 1. sz., p. 30.
[7] Jakobs, K.: ICT Standardisation - Co-ordinating the Diversity, Innovations in NGN - Future Network and Services. An ITU-T Kaleidoscope Event. IEEE Press, 2008., p. 3

követelményein. Formailag ugyanis a de jure szabványokat nemzeti vagy nemzetközi szabványügyi szervezetek fogadták el és tették közzé. Szabványnak tekintjük ezeken felül a de facto szabványokat is, amelyeket általában széles körűen elismert nemzetközi civil szervezetek vagy kormányzati intézmények, szabványosítási céllal, de a szabvány formai követelményeinek teljesítése nélkül alkotnak. Ez utóbbi esetben általában verziószámozást alkalmaznak a változatok megkülönböztetésére, szemben a de jure szabványoknál alkalmazott kihirdetés évével. Szokásos eljárás, hogy a de facto szabvány egy adott változata de jure szabvánnyá válik. Ebben az esetben is szakmailag célszerűbb a de facto szabvány alkalmazása, ugyanis a de jure változatban általában nem jelennek a verziófrissítések, amelyek esetenként elég gyakoriak. Külön nehézséget okozhat az eredeti nemzetközi szabvánnyal egyébként betűre egyező nemzeti szabvány kiadása és annak változáskövetése. Erre a követésre jelent rossz példát a későbbiekben részletesen bemutatásra kerülő Common Criteria for Information Technology Security Evaluation de facto szabvány, amelynek aktuális verziója a 3.1 Revision 3 (2009. júliusi kiadás), a legfrissebb nemzetközi de jure szabvány egyik tagja az ISO/IEC 15408-2:2008, amely a 2.3-a de facto verzióból készült, a legújabb magyar szabvány pedig az MSZ ISO/IEC 15408-2:2003, ami a régen elavult 2.0 változat magyar fordítása.

A szabványok alkalmazása a magyar jog szerint nem kötelező,[8] de nyilvánvalóan érdemes. Az egyenszilárdságú informatikai biztonság kialakításának ez a legcélszerűbb módja, viszont kötelező erő hiányában a megvalósítás nem várható el. A kérdés az, hogy hogyan lehet a szabványok jó technológiai szint-követését és jól definiáltságát a kötelező erővel rendelkező jogi követelményekkel összemérni.

A gyakorlatban az informatikai biztonsági szabványok az informatikai biztonságot szabályozó jogszabályokhoz hasonlóan nem egységesek. Egyrészről azon belül, hogy informatikai biztonsági (vagy azt nagy részben lefedő) szabványok, érdemes kisebb alkalmazási csoportokat alkotnunk, amelyeket olyan módon osztunk fel, hogy

[8] 1995. évi XXVIII. tv. 6. § (1)

elsősorban milyen aspektusra vonatkozik az adott szabvány. Így az alábbi csoportokat tudjuk megalkotni:[9]

- műszaki szabványok és leírások
- termék, rendszer követelményei, azok tesztelése, értékelése és tanúsítása
- ellenintézkedések leírása
- irányítási rendszer, folyamat és tanúsítása

Az ilyen módon, célterület alapján besorolt szabványok nem egy időben jelentek meg, a lista a szabványtípusok tipikus megjelenése szerinti időrendben van. Az időrendiség sem a jelen felsorolás tekintetében, sem általánosságban nem befolyásolja a szabványok alkalmazhatóságát, a jogszabályokkal szemben ugyanis a szabványok bármeddig használhatók, másrészről viszont a visszavont szabványok esetében bizonyos korlátokba lehet ütközni, például, ha tanúsítás a visszavont szabványra már nem adható ki. Sokkal inkább tehát a népszerűség határozza meg, hogy egy szabvány meddig kerül elfogadásra. A lent olvasható történeti áttekintésben említett akár ’80-as évekbeli szabvány is máig használt, de egyes, főképp a műszaki szabványok és leírások kategóriába tartozó szabványok soha nem váltak széleskörűen elfogadottá és még egy tapasztalt szakember sem találkozott minddel.

A számítástechnika őskorában, az 1960-70-es években a korábban említett kötegelt feldolgozású mainframe számítógépek esetében a külön szabványalkotás a jogi szabályozás megalkotásához hasonlóan nem volt szükséges, a hagyományos papíralapú titokvédelmi eljárások megfelelően működtek.[10] A több felhasználós, erőforrásokat megosztó rendszerek támasztottak először új igényeket, amire válaszként 1970-ben szakértői jelentés készült „Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security” címmel.[11] A dokumentum elemezte az új kockázatokat és javaslatot tett a bevezetendő intézkedésekre. 1972-ben jelent meg az egyik első követelményrendszer Computer Security Technology Planning Study, amelyet az Air Force Systems Command

[9] Krauth Péter: Információbiztonsági szabványok fejlődése az elmúlt időszakban, avagy az 17799-es esete a 13335-össel, Magyar Minőség, 2003. XII. évf. 7. sz. pp. 6-8. ISSN 1789-5510, p. 6. alapján, módosítással

[10] Krauth Péter: Az információbiztonság fejlődése a szabványok tükrében. In: Horváth Zsolt (szerk. et al.): Információbiztonsági rendszermenedzser tanfolyami témaváz. EOQ MNB., 2007.

[11] Ware, Willis H. (ed.): Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security. Office of the Secretary of Defense, USA, 1970.

készített.[12] Az informatikai biztonság értékelése egyre inkább előtérbe került, melyre példa az 1979-es Proposed Technical Evaluation Criteria for Trusted Computer Systems.[13]

[12] Anderson, James P. : Computer Security Technology Planning Study Volume I-II, ESD-TR-73-51 Vol. I-II, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA, USA, 1972.
[13] Nibaldi, Grace H.: Proposed Technical Evaluation Criteria for Trusted Computer Systems, M79-225, The MITRE Corporation, Bedford, MA, USA, 1979.

2. TCSEC

Az első valóban széles körben elerjedt és mindmáig szórványosan alkalmazott informatikai biztonsági szabvány a Trusted Computer Systems Evaluation Criteria (TCSEC, Orange Book) volt, amelyet az Amerikai Egyesült Államok Védelmi Minisztériuma készített 1983-ban, majd javításra került 1985-ben.[14] A TCSEC célja a hidegháború alatt az Amerikai Egyesült Államok által beszerzett számítógéprendszerek biztonsági szintjeinek meghatározása[15] és egységesítése volt a minősített adatok védelmében. A de facto szabvány négy fő kategóriát nevesít D-től A-ig, azon belül alkategóriákat. A legmagasabb biztonságot az A1 fölötti kategória jelenti. A meghatározott kategóriák és főbb jellemzőik a következők:

- D - Minimal Protection

Olyan rendszer, amely értékelésre került, de nem felelt meg semmilyen magasabb kategóriának.

- C - Discretionary Protection
  - C1 - Discretionary Security Protection

Megvalósul a felhasználók és adatok szétválasztása és a tetszés szerinti hozzáférés-szabályozás (Discretionary Access Control, DAC), amellyel egyedileg meghatározhatóak a hozzáférési jogosultságok.

  - C2 - Controlled Access Protection

A C1-esnél részletesebb hozzáférés-szabályozás, egyénenkénti elszámoltathatóság a bejelentkeztetés segítségével, audit ösvények (audit trails) és az erőforrások elkülöníthetősége jellemzik.

- B - Mandatory Protection
  - B1 - Labeled Security Protection

Félhivatalos informatikai biztonsági politikát kell létrehozni, az adatokat érzékenységük alapján címkézni kell, ezeket igény szerint exportálni lehessen. Kötelező a hozzáférés-szabályozás (Mandatory Access Control, MAC) meghatározott objektumokon, minden felfedezett biztonsági rést meg kell szüntetni vagy más módon ártalmatlanná kell tenni.

  - B2 - Structured Protection

[14] A szabvány történeti jelentősége miatt került itt feltüntetésre.
[15] F. Ható Katalin: Adatbiztonság, adatvédelem. Számalk, Budapest, 2000.

Formálisan dokumentált, egyértelmű informatikai biztonsági politikát kell létrehozni, a hozzáférést szabályozni kell minden objektumon és védekezni kell az engedély nélküli rejtett tárolók ellen. A rendszerelemeket fel kell osztani védelemkritikus és nem védelemkritikus részekre. Előírás az összetett tervezés és kiépítés, a megerősített azonosítási eljárások, az adminisztrátor és operátor szerepek szétválasztása és szigorú konfiguráció-menedzsment szabályok kialakítása.

- B3 - Security Domains

A biztonsági politika betartatásához nem szükséges kódot a rendszer ne futtasson. A rendszer összetettségét minimalizálni kell, támogatni kell a biztonsági adminisztrátor munkáját és a biztonsági eseményeket auditálni kell. Automatikus behatolás-érzékelést, értesítési és reagálási módszereket és megbízható rendszer-helyreállítási eljárásokat kell kialakítani. A rejtett időzítési csatornák ellen védekezni kell.

- A - Verified Protection
- A1 - Verified Design

Funkcionálisan megegyezik a B3 szinttel. Ezen felül formális tervezési és ellenőrzési technikákat és felsőszintű specifikációt, valamint formális menedzsment és osztályozási eljárásokat kell létrehozni.

- Beyond A1

Az önvédelmi követelmények teljességét demonstráló rendszer-architektúrát jelent. A felső- és alacsony szintű követelményekből automatikusan generált biztonsági tesztelést kell végezni, forráskód szintű ellenőrzést kell végezni lehetőleg formális eljárásokkal, a tervezési környezetnek biztonságosnak, a személyzetnek megbízhatónak kell lennie.

3. ITSEC, CTCPEC, FC

A TCSEC európai megfelelőjeként Nagy-Britannia, Franciaország, Hollandia és Németország 1991-ben megalkotta az Information Technology Security Evaluation Criteria (ITSEC) de facto szabványt, amely hasonlóan szintező jellegű volt E0-tól E6-ig, valamint példákat is adott egyes rendszerek elvárható követelményszintjeire.[16] A következő biztonsági szinteket határozza meg az ITSEC:

- Level E0

Nincs megfelelő garancia.

- Level E1

Biztonsági előirányzat (Security Target), valamint a tanúsítás tárgyának (TOE) informális leírása készül. Funkcionális tesztekkel kerül bizonyításra a biztonsági előirányzatnak való megfelelés.

- Level E2

Az E1 szintnél leírtak mellett a részletes terv leírásával is rendelkezni kell. A funkcionális tesztelés bizonyítékait is értékelni kell, valamint konfiguráció-kontroll- és elfogadott disztribúciós eljárást kell kialakítani.

- Level E3

Az E2 szinten felül forráskód illetve tervrajz biztonsági értékelést kell végezni. Ezen biztonsági mechanizmusok tesztelési bizonyítékait is értékelni kell.

- Level E4

Rendelkezni kell a biztonsági előirányzatot támogató biztonsági politika-modellel, valamint félformális stílusban kell meghatározni a biztonsági funkciókat, a magas szintű és alacsony szintű terveket.

- Level E5

A forráskód illetve tervrajz meg kell, hogy feleljen az alacsony szintű terveknek.

- Level E6

Formális stílusban kell meghatározni a biztonsági funkciókat, a magas szintű és alacsony szintű terveket, amelyek megfelelnek a biztonsági politika-modellnek.

[16] Az ITSEC szabvány, valamint a CTCPEC, FC szabványok is csak történeti jelentőségük miatt kerültek itt feltüntetésre, mai használatuk elhanyagolható mértékű.

Az ITSEC-ben meghatározásra került tíz példa funkcionális osztály, melyek rendszer-specifikus követelményeket határoznak meg. Az F-C1, F-C2, F-B1, F-B2, F-B3 példaosztályok a TCSEC osztályok funkcionális követelményeiből kerültek levezetésre. Az F-IN példa funkcionális osztály a magas adat- és program-integritási igényű értékelési tárgyakra vonatkozik, például adatbázis-kezelő rendszerekre. Az F-AV példa funkcionális osztály a magas rendelkezésre állási igényű értékelési tárgyakra vonatkozik, ipari vezérlőkhöz ajánlott. Az F-DI osztály az adatátvitel során magas adatintegritás igénylő alkalmazásokra használható. Az F-DC osztály a legnagyobb bizalmasságot biztosítja adatátvitel során, így például kriptográfiai rendszereknél alkalmazható. Az F-DX osztály magas bizalmasság és integritás igényű hálózatokra alkalmazható, így például bizalmas információ nem biztonságos hálózaton való átvitelére.[17]

Kanadában a TCSEC és az ITSEC alapján a Communications Security Establishment elkészítette saját biztonságértékelési szabványukat, Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) néven. Az Amerikai Egyesült Államok a TCSEC 9 éves tapasztalatán 1992-ben új szabványt tervezett, a Federal Criteria-t, ami viszont soha nem került véglegesítésre.

[17] Muha Lajos – Bodlaki Ákos: Az informatikai biztonság. PRO-SEC, Budapest, 2001. p. 37.

4. Common Criteria (ISO/IEC 15408)

A fenti korai informatikai biztonsági termékszabványok után az azokat megalkotó szereplők a TCSEC, ITSEC, CTCPEC bázisán 1996-ban elkészítették a Common Criteria for Information Technology Security Evaluation, rövid nevén Common Criteria (CC) de facto szabványt. A CC az az informatikai biztonsági termékszabvány, amely ma az informatikai biztonság területén etalonnak tekinthető, a világon egyre szélesebb körben elfogadott és folyamatos fejlesztés alatt áll. 1.0-ás változatát az Európai Közösség, az Amerikai Egyesült Államok és Kanada együttesen fogadták el, 2.0-ás verziója ISO/IEC 15408 jelzettel de jure nemzetközi szabvánnyá vált. Az aktuális és a megelőző változat szabadon elérhető a http://www.commoncriteriaportal.org/ oldalról. A CC magyar érdekessége, hogy 2.0-ás változatát az Informatikai Tárcaközi Bizottság 16. számú ajánlásaként magyar nyelven közreadta, majd az MSZ ISO/IEC 15408 jelzetű szabvány is lefordításra került. Problémát jelent, hogy a de jure szabványok verziókövetése esetenként igen lassú. A CC jelenlegi verziója a 3.1 Revision 4 (2012. szeptember), az ISO/IEC szabvány kiadási ideje a kötettől függően 2009 vagy 2008, míg a magyar szabványé 2003 illetve 2002.

A szabványban a funkcionális követelmények, bizonyossági követelmények és értékelési bizonyossági szintek (EAL) mátrixaként határozhatóak meg az alkalmazandó biztonsági követelmények. A követelmények konkretizálása céljából az általános, eszköz fajtájára jellemző védelmi profilok (Protection Profile, PP) alapján biztonsági célkitűzést (Security Target, ST) kell készíteni, amely már az eszköztípusra vonatkozó követelményeket tartalmazza, és ez alapján kerül megvalósításra maga a termék, a vizsgálat tárgya (Target of Evaluation, TOE).

A Common Criteria három részből áll:[18]

- Part 1: Introduction and general model (Bevezetés és általános modell[19])
- Part 2: Security functional requirements (A biztonság funkcionális követelményei)

[18] Common Criteria for Information Technology Security Evaluation Part 1, 2006, p. 2.
[19] A magyar nyelvű megnevezések a magyar nyelvű MSZ ISO/IEC 15408 jelzetű szabványból származnak.

- Part 3: Security assurance requirements (A biztonság garanciális követelményei)

A Common Criteria második kötete tizenegy funkcionális osztályt határoz meg, mely osztályokon belül a funkcionális követelmények részletezésre kerültek. Ezek a következők:[20]

- Class FAU: Security audit (Biztonsági átvilágítás)
- Class FCO: Communication (Kommunikáció)
- Class FCS: Cryptographic support (Kriptográfiai támogatás)
- Class FDP: User data protection (Felhasználói adatvédelem)
- Class FIA: Identification and authentication (Azonosítás és hitelesítés)
- Class FMT: Security management (Biztonságirányítás)
- Class FPR: Privacy (Titoktartás)
- Class FPT: Protection of the TSF (A TSF védelme)
- Class FRU: Resource utilisation (Erőforrás-felhasználás)
- Class FTA: TOE access (TOE-hozzáférés)
- Class FTP: Trusted path/channels (Bizalmi útvonal/csatornák)

Minden osztályban több család van, és családonként több komponens, amelyeket a következő módon jelölünk: FAU_ARP.1 Minden komponens egy adott követelményt fejt ki.

„A garancia az alapja annak a bizalomnak, hogy egy IT termék vagy rendszer kielégíti biztonsági céljait. A garancia származtatható az olyan forrásokra hivatkozásból, mint a meg nem erősített állítások, az idevágó korábbi vagy speciális tapasztalatok. Azonban e szabvány az aktív vizsgálatok révén nyújt garanciát. Az aktív vizsgálat az IT termék vagy rendszer olyan értékelését jelenti, amely meghatározza annak biztonsági tulajdonságait.”[21]

A vonatkozó garanciális követelmények a 2.x és a 3.x verziókban jelentős változáson estek át.

A garanciaosztályok a CC 2.1-2.3 változatában a következők:[22]

- Class ACM: Configuration management (A konfigurációmenedzselés)
- Class ADO: Delivery and operation (Kiszállítás és üzemeltetés)

[20] Common Criteria for Information Technology Security Evaluation Part 2, 2009, p. 4.
[21] MSZ ISO/IEC 15408-3:2003 1.2.2.3. p. 12.
[22] Common Criteria for Information Technology Security Evaluation Part 3, 2005, p. 5.

- Class ADV: Development (Fejlesztés)
- Class AGD: Guidance documents (Útmutató dokumentumok)
- Class ALC: Life cycle support (Az életciklus támogatása)
- Class ATE: Tests (Vizsgálatok)
- Class AVA: Vulnerability assessment (A sebezhetőség felmérése)

A garanciaosztályok a CC 3.1 változatában a következők:[23]

- Class APE: Protection Profile evaluation (Védelmi Profil értékelése)
- Class ASE: Security Target evaluation (Biztonsági Előirányzat értékelése)
- Class ADV: Development (Fejlesztés)
- Class AGD: Guidance documents (Útmutató dokumentumok)
- Class ALC: Life cycle support (Az életciklus támogatása)
- Class ATE: Tests (Vizsgálatok)
- Class AVA: Vulnerability assessment (A sebezhetőség felmérése)
- Class ACO: Composition (Összeállítás)

A követelmények teljesülésének bizonyosságát, a garanciaszintet (Evaluation Assurance Level, EAL) az ITSEC E0..E6 szintjeihez hasonlóan a CC is szintezi:[24]

- EAL1 - functionally tested (funkcionálisan vizsgálva)
- EAL2 - structurally tested (strukturálisan vizsgálva)
- EAL3 - methodically tested and checked (módszeresen vizsgálva és ellenőrizve)
- EAL4 - methodically designed, tested, and reviewed (módszeresen tervezve, vizsgálva és átnézve)
- EAL5 - semi formally designed and tested (félformálisan tervezve és vizsgálva)
- EAL6 - semi formally verified design and tested (félformálisan igazolt módon tervezve és vizsgálva)
- EAL7 - formally verified design and tested (formálisan igazolt módon tervezve és vizsgálva)

[23] Common Criteria for Information Technology Security Evaluation Part 3, 2009, p. 5.
[24] Ibid. pp. 5-6.

A Common Criteria szerinti vizsgálatok végrehajtását támogatja a Common Methodology for Information Technology Security Evaluation (CEM), amely részletes módszertani útmutatóként egységes metodológiát határoz meg a vizsgálatokhoz. Ez is megjelent nemzetközi szabványként ISO/IEC 18045:2008 jelzettel.

Jelenleg a terméktanúsítási szabványok közül a Common Criteria a leginkább elterjedt, különösen az európai terméktanúsításban piacvezető Németországban.[25]

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

7. ábra: EAL összegzés[26]

[25] Spindler, Gerald (et. al.): Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären. Studie im Auftrag des BSI durchgeführt von Prof. Dr. Gerald Spindler, Universität Göttingen. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2007, p. 68.

[26] Common Criteria for Information Technology Security Evaluation Part 3, 2009. p. 31. 1. táblázat

5. ITIL és ISO/IEC 20000

Az IT Infrastructure Library (ITIL), bár elsősorban informatikai üzemeltetésére és fejlesztésére szolgáló módszertani gyűjtemény, folyamatszabvány és nem biztonsági szabvány, előírásaiban érinti a biztonsági területet. Nemzetközi legjobb gyakorlatként az IT szolgáltatások területén szolgál követelményhalmazként. A 80-as években alkotta az Egyesült Királysági Central Computing and Telecommunications Agency (CCTA), legutóbbi változata a 2007-es v3. Jelenleg az Office of Government Commerce (OGC) gondozza. Brit nemzeti szabványként BS 15000 jelzettel, majd nemzetközi szabványként ISO/IEC 20000 jelzettel, több kötetben jelent meg, ez azonban nem azonos az ITIL-lel. Amíg az ITIL egy jó gyakorlatokról szóló irányelv (best practice guide), addig az ISO 20000 az ezekből levezetett kötelező minimumkövetelmények, amelyek minimálisan elvárhatóak az IT szolgáltatások biztosítása terén. Céljaik és gyökerük viszont azonos, így azokat célszerű együtt kezelni.

Az ITIL célja a jó minőségű, költséghatékony IT szolgáltatások támogatása, a minőségügyben ismert Plan-Do-Check-Act (PDCA) elv alkalmazásával. A biztonsági követelmények elsősorban IT szolgáltatás-folytonossági követelményként kerültek be a keretrendszerbe. A szűken vett információbiztonsági kontrollok tekintetében egy alfejezetben[27] tartalmaz előírásokat, valamint javasolja az ISO/IEC 17799 (ma már ISO/IEC 27002) alkalmazását.

Az ITIL öt kötetből áll, melyek a következők:[28]

- Szolgáltatás-stratégia (Service Strategy): A bevezetendő informatikai szolgáltatások által kiaknázható piaci lehetőségeket lehet kiválasztani a folyamat keretében. A kiválasztás során stratégiai terv készül, amely bemutatja a tervezés, implementáció, üzemeltetés és a folyamatos fejlesztés lépéseit és ezek összefüggéseit. Az új szolgáltatás értéknövelő szerepű. A könyv legfontosabb részei a Szolgáltatás-portfólió kezelése és Pénzügyi menedzsmentje.
- Szolgáltatás-tervezés (Service Design): Az elkészült stratégiában foglaltak megvalósítására projektterv készül a tervezett szolgáltatás gyakorlati

[27] ISO/IEC 20000-2:2005, 6.6 Information security management
[28] ITIL v3 Service Strategy 1.2.3

megvalósítására. A tervben megtalálható a bevezetés minden lépése, valamint a konkrét bevezetéshez kapcsolódó más átalakítandó folyamatok megnevezése. Legfontosabb fejezetei az Üzemeltetés és üzemvitel biztosítása, Kapacitástervezés valamint az Informatikai- és üzembiztonság. Ezen fejezetek miatt tekintjük a szabványt (részben) informatikai biztonsági jellegűnek.

- Szolgáltatás-létesítés és változtatás (Service Transition): A gyakorlati bevezetés lépéseit tartalmazza, különös tekintettel az előző fejezetben megnevezett módosítandó kapcsolódó és érintett folyamatokra. Lényegi részei a Változás- és verziókezelés, Konfiguráció-menedzsment és Dokumentáció-kezelés.
- Szolgáltatás-üzemeltetés (Service Operation): Az előző kötet alapján létesített rendszer üzemeltetésének folytonosságáról és a hibamentesség biztosításáró szól. Ehhez meghatározott folyamatokat és adminisztratív intézkedéseket kell bevezetni. Az elvárt rendelkezésre állási követelményeket szolgáltatási szint-megállapodás (SLA) rögzíti, amelynek betartatása az elődleges célja a kötetnek. Fő fejezetei a Hiba- és igény- és incidenskezelés.
- Állandó szolgáltatás-fejlesztés (Continual Service Improvement): A folyamatos, PDCA-elvet követő minőségjavításról szóló kötet, legfontosabb részei a Szolgáltatási szint mérése, jelentése és menedzsmentje című fejezetek.

Az ISO/IEC 20000 szabvány kötetei a következők:

- ISO/IEC 20000-1:2011 Service management system requirements
- ISO/IEC 20000-2:2012 Guidance on the application of service management systems
- ISO/IEC 20000-3:2012 Guidance on scope definition and applicability of ISO/IEC 20000-1
- ISO/IEC TR 20000-4:2010 Process reference model
- ISO/IEC TR 20000-5:2010 Exemplar implementation plan for ISO/IEC 20000-1

A fentiek közül magyar szabványként az alábbiak jelentek meg:

- MSZ ISO/IEC 20000-1:2013 Informatika. Szolgáltatásirányítás. 1. rész: A szolgáltatásirányítási rendszer követelményei

- MSZ ISO/IEC 20000-2:2007 Informatika. Szolgáltatásirányítás. 2. rész: Alkalmazási útmutató: Ez még a korábbi, ISO/IEC 20000-2:2005 magyar nyelvű fordítása

6. ISO/IEC 27000 szabványsorozat

Szintén a szigetországból indult egy szabványcsalád, amely mára széles körben ismertté és alkalmazottá vált. 1995-ben a Department of Trade and Industry (DTI) által készített BS 7799 jelzetű szabvány informatikai biztonsági követelményeket foglalt össze, melyek menedzsment szinten alkalmazhatók. Ez nemzetközi szabvánnyá vált ISO/IEC 17799 jelzettel. A BS 7799-2, mint az információbiztonsági irányítási rendszerre vonatkozó szabvány 1999-ben került kifejlesztésre és csatolásra a korábbi BS 7799-hez, amely BS 7799-1-re lett átszámozva, majd ISO/IEC 27001 jelezettel került a nemzetközi porondra, ami után az ISO/IEC 17799-et szintén átszámozták ISO/IEC 27002-re[29] és beindult egy irányítási rendszer szabványcsalád kifejlesztése az ISO 9000-es sorozathoz hasonlóan. A kezdeti szabvány különlegessége volt, hogy fentről-lefelé, az üzleti igényekből határozta meg a biztonsági követelményeket. Az ISO/IEC 27001 abból a célból készült, hogy modellként szolgáljon információbiztonsági irányítási rendszerek (ISMS, IBIR) kialakításához, megvalósításához, működtetéséhez, figyelemmel kíséréséhez, átvizsgálásához, fenntartásához és fejlesztéséhez.[30] A szabvány folyamatközpontú, alkalmazza a Plan-Do-Check-Act (PDCA) modellt és a megvalósított IBIR integrálható a meglévő minőségirányítási (ISO 9001) és a környezetirányítási (ISO 14001) rendszerekkel. A követelmények tekintetében célszerű az ISO/IEC 27002 szabvány alkalmazása.

Az ISO/IEC 27000 szabványsorozat publikált és előkészítés alatt álló tagjai:

- ISO/IEC 27000:2012 Information security management systems – Overview and vocabulary: áttekintés és szótár, ismerteti a szabványsorozat főbb elveit és meghatározza a kulcsfogalmakat
- ISO/IEC 27001:2013 Information security management systems – Requirements: a korábban ismertetettek szerint a menedzsment rendszer követelményeit írja le
- ISO/IEC 27002:2013 Code of practice for information security controls: a korábban ismertetettek szerint a gyakorlat követelményeit írja le

[29] A magyar szabvány ezt az átszámozást nem követte, jelenleg is MSZ ISO/IEC 17799:2006 jelzetű, valamint a 27000-es sorozat többi tagja (az MSZ ISO/IEC 27001-en kívül) sem jelent még meg magyar szabványként.

[30] MSZ ISO/IEC 27001:2006 p. 19.

- ISO/IEC 27003:2010 Information security management system implementation guidance: a bevezetésre vonatkozó iránymutatásokat tartalmazza
- ISO/IEC 27004:2009 Information security management – Measurement: a biztonság szintjének mérésével foglalkozik
- ISO/IEC 27005:2011 Information security risk management: a kockázatmenedzsment egy ajánlott keretrendszerétismerteti, az ISO/IEC 13335-3 és az ISO/IEC 13335-4 szabványokból került kifejlesztésre, kompatibilis az ISO 31000:2009 általános kockázatmenedzsment irányelvvel.
- ISO/IEC 27006:2011 Requirements for bodies providing audit and certification of information security management systems: az ISO/IEC 27001 alapján tanúsítást végző szervezetekre vonatkozó követelményeket határozza meg
- ISO/IEC 27007:2011 Guidelines for information security management systems auditing: az auditálás módszertanára vonatkozó iránymutatást tartalmazza
- ISO/IEC TR 27008:2011 Guidelines for auditors on IS controls: az auditoroknak nyújt iránymutatást a helyes ISO/IEC 27002 szerinti kontrollokról
- ISO/IEC 27010:2012 Information security management for inter-sector and inter-organizational communications: a szervezetek és a különböző szektorok közötti bizalmas információ-megosztásra ad iránymutatást, különös tekintettel a kritikus infrastruktúrák közötti adatkezelésre.
- ISO/IEC 27011:2008 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002: a hírközlési szolgáltatókra vonatkozó különleges követelményeket tartalmazza
- ISO/IEC 27013:2012 Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001: a szabvány iránymutatást nyújt az ISO/IEC 20000-1 (vö. ITIL) és az ISO/IEC 27001 szerinti IBIR integrált bevezetésére
- ISO/IEC 27014:2013 Governance of information security: Az információbiztonság irányítására vonatkozó irányelveket mutatja be (vö. COBIT)

- ISO/IEC 27015:2012 Information security management guidelines for financial services: Az ISO/IEC 27002:2005 kiegészítése képpen iránymutatást ad a pénzügyi szektorban kialakítandó biztonsági kontrollokra
- ISO/IEC TR 27019:2013 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry: Kiterjeszti a 27000-es sorozat hatókörét a folyamatszabályozásra és automatikára, az energiaszolgáltatók (beleértve a villamosenergia-, gáz- és hőszolgáltatást) digitális rendszereinek (a védelmi reléktől a PLC-ken át a vezérlőközpontokig) védelmében.
- ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity: Az informatikai és kommunikációs szolgáltatások üzletmenet-folytonossági felkészítésére mutat be keretrendszert és folyamatokat.
- ISO/IEC 27032:2012 Guidelines for cybersecurity: iránymutatásokat fogalmaz meg a kiberbiztonság növelése érdekében, ami magában foglalja az információ- ,hálózat- és internetbiztonságot, valamint a kritikus információs infrastruktúrák védelmét.
- ISO/IEC 27033-1:2009 Network security: Overview and concepts: A szabvány áttekintést nyújt a hálózati biztonságról, valamint ismerteti a tématerülethez kapcsolódó definíciókat
- ISO/IEC 27033-2:2012 Network security: Guidelines for the design and implementation of network security: Iránymutatást nyújt szervezeteknek a hálózati biztonság tervezésére, kivetelezésére és dokumentációjára
- ISO/IEC 27033-3:2010 Network security: Threats, design techniques and control issues: a szabvány bemutatja a veszélyeket, tervezési technikákat és a kontrollokra vonatkozó kérdéseket különféle példákon keresztül
- ISO/IEC 27033-5:2013 Securing communications across networks using Virtual Private Networks (VPNs): a szabvány a virtuális magánhálózatok (VPN) biztonságossá tételéhez nyújt iránymutatásokat
- ISO/IEC 27034-1:2011 Application security. Overview and concepts: Alkalmazásbiztonsági fogalmak, koncepciók, irányelvek. Egy készülőben lévő hatkötetes sorozat első eleme.

- ISO/IEC 27035:2011 Information security incident management: Irányelv az informatikai biztonsági incidens-menedzsment strukturált és tervezett megvalósítására, elsősorban közepes- és nagyvállalatok számára (ez magyar viszonylatban csak nagyvállalatokra ajánlott).
- ISO/IEC FDIS/DIS/WD 27036-1..4 Information security for supplier relationships: A beszállítói kapcsolatok információbiztonsági kérdéseit tartalmazó, előkészítés alatt álló négykötetes szabvány.
- ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence: az igazságügyi informatika (digital forensics) számára nyújt iránymutatást a digitális nyomok azonosítására, rögzítésére és megőrzésére
- ISO 27799:2008 Health informatics – Information security management in health using ISO/IEC 27002: az egészségügyi szolgáltatókra vonatkozó különleges követelményeket tartalmazza

A fentiek közül magyar szabványként csak az alábbiak jelentek meg:

- MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények (A szabvány nemzetközi 2013-as változatának a magyar fordítása folyamatban van)
- MSZ ISO/IEC 27002:2011 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (A szabvány nemzetközi 2013-as változatának a magyar fordítása folyamatban van)
- MSZ ISO/IEC 27006:2013 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszereinek auditját és tanúsítását végző testületekre vonatkozó követelmények (Angol nyelvű szabvány)

Az MSZ ISO/IEC 27001:2006 szabvány fejezetei a következők:

0. Bevezetés
1. Alkalmazási terület
2. Rendelkező hivatkozások
3. Szakkifejezések és meghatározásuk
4. Az információbiztonság irányítási rendszere
5. A vezetőség felelőssége

6. Belső ISMS-auditok
7. Az ISMS vezetőségi átvizsgálása
8. Az ISMS fejlesztése

A melléklet (előírás): Szabályozási célok és intézkedések

B melléklet (tájékoztatás): Az OECD-irányelvek és e nemzetközi szabvány

C melléklet (tájékoztatás): Kapcsolat az ISO 9001:2000, az ISO 14001:2004 és e nemzetközi szabvány között

Az MSZ ISO/IEC 27002:2011 szabvány fejezetei a következők:

0. Bevezetés
1. Alkalmazási terület
2. Szakkifejezések és meghatározásuk
3. E szabvány felépítése
4. Kockázatfelmérés és kockázatjavítás
5. Biztonságpolitika
6. Az információbiztonság szervezete
7. Vagyontárgyak kezelése
8. Emberi erőforrások biztonsága
9. Fizikai és környezeti biztonság
10. A kommunikáció és az üzemeltetés irányítása
11. Hozzáférés-ellenőrzés
12. Információs rendszerek beszerzése, fejlesztése és karbantartása
13. Az információbiztonsági incidensek kezelése
14. A működés folytonosságának irányítása
15. Megfelelőség

Tekintettel arra, hogy a szabványnak való megfelelőség tanúsítható, az arról szóló tanúsítvány üzleti előnyt jelenthet a cégnek. Mivel a tanúsításokat magáncégek végzik és kötelező regiszter nem létezik, ezért a világszerte vagy akár a Magyarországon tanúsított cégek pontos számának megállapítása szinte lehetetlen. Van azonban egy olyan nemzetközi regiszter, amelybe a legnagyobb tanúsítók (pl. BSI, Bureau Veritas, DNV, KPMG, LRQA, SGS, TÜV) önkéntesen bejelentik a kiadott tanúsítványaikat.

Jelenleg a világon e regiszter szerint 6826 db ISO 27001 kiadott tanúsítvány van. Ezek országonkénti bontásban a következők:[31]

Japan	3632	Philippines	15	Macau	3
India	492	Pakistan	14	Portugal	3
China	483	Vietnam	14	Argentina	2
UK	453	Iceland	13	Belgium	2
Taiwan	371	Saudi Arabia	13	Bosnia Herzegovina	2
Germany	139	Netherlands	12	Cyprus	2
Korea	106	Singapore	12	Isle of Man	2
USA	96	Indonesia	11	Kazakhstan	2
Czech Republic	86	Bulgaria	10	Morocco	2
Hungary	71	Kuwait	10	Ukraine	2
Italy	60	Norway	10	Armenia	1
Poland	56	Russian Federation	10	Bangladesh	1
Spain	54	Sweden	9	Belarus	1
Malaysia	40	Colombia	8	Denmark	1
Ireland	37	Bahrain	7	Dominican Rep.	1
Thailand	36	Iran	7	Jersey	1
Austria	35	Switzerland	7	Kyrgyzstan	1
Hong Kong	32	Canada	6	Lebanon	1
Greece	30	Croatia	6	Luxembourg	1
Romania	30	South Africa	5	Macedonia	1
Australia	29	Sri Lanka	5	Mauritius	1
Mexico	24	Lithuania	4	Moldova	1
Brazil	23	Oman	4	New Zealand	1
Slovakia	21	Peru	4	Sudan	1
Turkey	21	Qatar	4	Uruguay	1
UAE	20	Chile	3	Yemen	1
France	19	Egypt	3		

[31] International Register of ISMS Certificates. http://www.iso27001certificates.com/ [2010. 10. 17.] Version 201 September 2010 – Az oldal sajnos megszűnt, így frissebb eredmények nem hozzáférhetők

Slovenia	17	Gibraltar	3		

Ezek az értékek természetesen a fenti okok miatt nem megbízhatóak, viszont arányaikban helyesnek tekinthetők. Így a listán a világranglistában tízedik helyünk meglepően jó eredmény.
A kiadott tanúsítványok darabszáma nem egyenlő a tanúsított szervezetek számával. Egy szervezet számára ugyanis több külön tanúsítvány kiadható hatóköri, telephelyi vagy időbeli érvényességi okokból. A tanúsított szervezetek listája szintén lekérdezhető a regiszterből. Ez a lista és a kutatás alapján történő bővítése összesen 98 szervezet 103 tanúsítványát tartalmazza, amely így valós értékhez jobban közelít.

A Hétpecsét Információbiztonsági Egyesület[32] évente információt kér a Magyarországon működő tanúsítóktól a sikeresen lezárt auditok darabszámáról a tanúsított szervezet nevének közlése nélkül. Az adatgyűjtés célja az ISO/IEC 27001 szabvány hazai elterjedtségének vizsgálata. A 13 tanúsító cég nyilatkozatai szerint 2010 januárjáig 138 sikeres auditon átesett magyarországi cég van, ami a 2009. januári 131 céghez képest öt százalékos növekedést jelent. A sikeresebb tanúsítók között a piaci részesedés eloszlása: SGS 35%, CERTOP 14%, DNV 12%.[33] Minden bizonnyal ezen felmérés értékei a legpontosabbak, hátránya viszont, hogy a cégnevek nem ismertek. A cégnevek ismerete azért lenne fontos, mert a tanúsítvány fő értéket maga a tanúsító szervezet adja az adott szektorban. Tehát ha az élelmiszeripari cégek túlnyomó részét egy cég tanúsította, akkor az iparágon belül az a tanúsítvány a leginkább elfogadott. Ha egy új belépő másik céggel tanúsíttatja magát, lehet, hogy az iparágon belül (pl. beszállítók, partnerek) nem fogadják el a tanúsítványát.[34]

Az informatikai biztonsági irányítási rendszer kialakításának lépései a szabvány alapján a következők:[35]

- Az IBIR alkalmazási területének és határainak meghatározása.[36]
- Az IBIR szabályzatának megalkotása.[37]

[32] http://hetpecset.hu/ [2010. 05. 10.]
[33] Bitport: Háttérbe szorul a megfelelőség? Bitport, 2010.01.27. http://www.bitport.hu/biztonsag/hatterbe-szorul-a-megfeleloseg. [2014. 03. 10.]
[34] Horváth Zsolt: Miért nem mindegy, hogy kit választok tanúsítónak? Minőségdoktorok.hu., 2008.
[35] MSZ ISO/IEC 27001:2006 4.2.2.
[36] MSZ ISO/IEC 27001:2006 1.2.
[37] MSZ ISO/IEC 27001:2006 4.2.1. c)

- Kockázatfelmérés megközelítési módjának meghatározása, kockázatok azonosítása, kockázatelemzés készítése, lehetséges változatok értékelése, maradványkockázatok elfogadtatása a vezetőséggel.[38] Ez legösszetettebb feladatcsoport, ezért részletesen is kifejtésre kerül.
- Vezetés felhatalmazásának megszerzése az IBIR bevezetésére és működtetésére.
- Alkalmazhatósági nyilatkozat készítése.
- Kockázatjavítási terv kidolgozása, amely meghatározza a megfelelő irányítási beavatkozásokat, a forrásokat, a felelősségi köröket és a fontossági sorrendet az információbiztonsági kockázatok kezelésére.[39]
- Kockázatjavítási terv bevezetése, ami magában foglalja a finanszírozás, valamint a feladat- és felelősségi körök kijelölésének kérdéseit is.
- Kiválasztott intézkedések bevezetése a szabályozási célok teljesítése érdekében.[40]
- Kiválasztott intézkedések, illetve intézkedéscsoportok hatékonyságának mérési módszerének meghatározása.[41]
- Képzési és tudatosítási (awareness) programok bevezetése.[42]
- ISMS működésének irányítása.
- Gazdálkodás az ISMS erőforrásaival.[43]
- Biztonsági események azonnali észlelése és a biztonsági incidensek megválaszolása.[44]

A kockázatelemzés során meg kell határozni, hogy az egyes fenyegetések mely rendszerelemekre hatnak. Az elemzés során szükséges megbecsülni, hogy az egyes fenyegetések várhatóan milyen gyakorisággal, mekkora valószínűséggel fognak bekövetkezni. Másik fontos szempont, hogy a már bekövetkezett esemény károkozásának forintban kifejezett mértéke várhatóan mekkora lesz. E két szempont egymáshoz való viszonya rajzolja ki a kockázati mátrixot. A konkrét fenyegetések a rendszerelemekre hatnak, így a védelmi intézkedésekkel is ezeket kell megcélozni. A

[38] MSZ ISO/IEC 27001:2006 5.1. f), 4.2.1. c)
[39] MSZ ISO/IEC 27001:2006 5.
[40] MSZ ISO/IEC 27001:2006 4.2.1. g)
[41] MSZ ISO/IEC 27001:2006 4.2.3.c)
[42] MSZ ISO/IEC 27001:2006 5.2.2.
[43] MSZ ISO/IEC 27001:2006 5.2.
[44] MSZ ISO/IEC 27001:2006 4.2.3. a)

védelem teljes körűsége érdekében minden lehetséges rendszerelemet figyelembe kell venni és értékelni kell.

A szabvány alkalmazása önmagában nem elégséges egy teljes kockázatelemzés elvégzéséhez, így egy olyan módszertan alkalmazása szükséges, amely kitölti a szabvány által maghatározott kereteket. Ilyen kockázatelemzési módszertan például az ISO/IEC 27005 szabványon alapuló francia MEHARI,[45] amely egységes veszélyforrás-meghatározásokat, tapasztalati alapon előre kalkulált valószínűségeket és számított kárhatásokat tartalmaz, egységessé és kiszámíthatóvá téve a kockázatelemzési eredményeket. A gyakorlati megvalósítás például a MEHARI-Risk szoftverrel[46] történhet, amely egyszerűsíti az adatbevitelt és megkíméli a kockázatelemzést végző személyt a bonyolult számítások elvégzésétől.
A kárérték-besorolási és kárgyakorisági osztályozások a MEHARI-ban az alábbiak:

A MEHARI hatásszintjei (MEHARI Impact levels)

- Nagyon alacsony hatású (very low impact)
- Alacsony hatású (low impact)
- Közepes hatású (medium impact)
- Magas hatású (high impact)

A MEHARI gyakoriság szintjei (Exposure levels MEHARI)

- Nagyon alacsony gyakoriság (very low exposure)
- Alacsony gyakoriság (low exposure)
- Közepes gyakoriság (medium exposure)
- Magas gyakoriság (high exposure)

A MEHARI-nál a következő, a kalkulációhoz felhasznált bemenő adatok és részeredmények vannak:

[45] http://www.clusif.asso.fr/en/production/mehari/ [2014. 02. 22.]
[46] http://www.mehari-risk.com/ [2014. 02. 22.]

Jelleg	MEHARI
Valószínűségi tényezők	STATUS-EXPO Natural exposure (1..4) Az esemény bekövetkezésének valószínűsége védekezés nélkül.
	STATUS-DISS Effectiveness of dissuasive measures (1..4) Az esemény elleni védekezés eltérítési hatékonysága.
	STATUS-PALL Effectiveness of palliative measures (1..4) Az esemény elleni védekezés tompítási hatékonysága.
	STATUS-PREV Effectiveness of preventive measures (1..4) Az esemény elleni védekezés megelőzési hatékonysága.
	STATUS-PROT Effectiveness of protective measures (1..4) Az esemény elleni védekezés kivédési hatékonysága.
	STATUS-RECUP Effectiveness of recuperative measures (1..4) Az esemény elleni védekezés tompítási hatékonysága. Az esemény elleni védekezés helyrehozási hatékonysága.
	STATUS-P Potentiality of event described by risk scenario (1..4) Az esemény bekövetkezésének valószínűségéből és az esemény elleni védekezések hatékonyságából számított bekövetkezési valószínűség.
Kockázati szint tényezők	Availability (1..4) Rendelkezésre állási szinttel szembeni elvárás mértéke.
	Confidentiality (1..4) Bizalmassági szinttel szembeni elvárás mértéke.
	Integrity (1..4) Sértetlenség, integritás szintjével szembeni elvárás mértéke.
	STATUS-RI Impact reduction (1..4) Hatást csökkentő tényezők.

	STATUS-I Impact (1..4) Eredő hatás: az elvárásokból és a hatást csökkentő tényezőkből kerül kiszámításra. Nincs pénzben mért kárérték tényező a MEHARI-ban.
Értékelési eredmény	SERIOUSNESS Risk seriousness for specific scenario (1..4) Az adott esemény súlyossága kockázatok az ellenintézkedésekkel csökkentve, tehát maradványkockázat.

7. COBIT

Az Information Systems Audit and Control Association (ISACA), mint nemzetközi szinten elismert amerikai IT auditor egyesület és az IT Governance Institute (ITGI) együtt 1992-ben kifejlesztették a Control Objectives for Information and Related Technology (COBIT) de facto informatikai biztonsági szabványt, mint az IT vezetés keretrendszerét. Ebben több információs folyamatra írtak elő követelményeket. A COBIT az ITIL-hez hasonlóan egy bevált gyakorlat-gyűjtemény, tulajdonképpen informatikai auditálási, vezetéstámogatási módszertan, ami üzleti követelményeken alapul. Soha nem vált de jure szabvánnyá, valamint nem is lehet az annak való megfelelést tanúsítani. A COBIT 4.1 verziója 34 magas szintű folyamatot, ezen belül 210 kontroll célkitűzést tartalmaz, amelyek négy szakterület köré csoportosulnak:

- Tervezés és szervezés (Planning and Organization)
- Beszerzés és megvalósítás (Acquisition and Implementation)
- Szolgáltatás és támogatás (Delivery and Support)
- Figyelemmel kísérés és értékelés (Monitoring and Evaluation)

A COBIT 4.1 folyamatok a következők:[47]

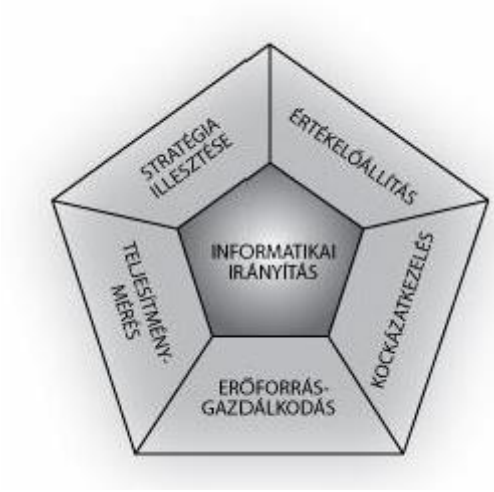
- Tervezés és szervezés (Planning and Organization)
  - PO1 Az informatikai stratégiai terv meghatározása
  - PO2 Az információ-architektúra meghatározása
  - PO3 A technológiai irány kijelölése
  - PO4 Az informatikai folyamatok, szervezet és a kapcsolatok meghatározása
  - PO5 Az informatikai beruházások irányítása
  - PO6 Tájékoztatás a vezetői célokról és irányról
  - PO7 Az informatikai humán erőforrások kezelése
  - PO8 Minőségirányítás
  - PO9 Az informatikai kockázatok felmérése és kezelése
  - PO10 A projektek irányítása
- Beszerzés és megvalósítás (Acquisition and Implementation)
  - AI1 Az automatizált megoldások meghatározása

[47] Source: COBIT 4.1. ©1996-2007 ITGI. All rights reserved. Used by permission.

- AI2 Az alkalmazási szoftverek beszerzése és karbantartása
- AI3 A technológiai infrastruktúra beszerzése és karbantartása
- AI4 Az üzemeltetés és a használat támogatása
- AI5 Az informatikai erőforrások beszerzése
- AI6 A változtatások kezelése
- AI7 A megoldások és változtatások üzembe helyezése és bevizsgálása

- Szolgáltatás és támogatás (Delivery and Support)
  - DS1 A szolgáltatási szintek meghatározása és betartása
  - DS2 Külső szolgáltatások igénybevételének irányítása
  - DS3 Teljesítmény- és kapacitáskezelés
  - DS4 A szolgáltatás folyamatosságának biztosítása
  - DS5 A rendszerek biztonságának megvalósítása
  - DS6 A költségek azonosítása és felosztása
  - DS7 A felhasználók oktatása és képzése
  - DS8 A rendkívüli események kezelése és a felhasználói támogatás működtetése
  - DS9 Konfigurációkezelés
  - DS10 Problémakezelés
  - DS11 Az adatok kezelése
  - DS12 A fizikai környezet biztosítása
  - DS13 Az üzemeltetés irányítása
- Figyelemmel kísérés és értékelés (Monitoring and Evaluation)
  - ME1 Az informatika teljesítményének figyelemmel kísérése és értékelése
  - ME2 A belső irányítási és ellenőrzési rendszer figyelemmel kísérése és értékelése
  - ME3 Külső követelményeknek való megfelelőség biztosítása
  - ME4 Az informatikai irányítás megteremtése

	• A **stratégia illesztése** az üzleti területek, és az informatika terveinek illesztésére; az informatikai érték előállítására vonatkozó ajánlat meghatározására, aktualizálására, és érvényesítésére; valamint az informatikai működés és a vállalati



működés illesztésére összpontosít.[48]

• **Érték-előállítás** (hasznosság, használati érték): a termelési ciklus során a tervezett többletérték létrehozásával foglalkozik, gondoskodva arról, hogy az informatika a stratégiai tervben meghatározott hasznokat megtermelje, koncentrálva a költségek optimalizálására és arra, hogy az informatika a belső értékét bizonyítsa.

• Az **erőforrás-gazdálkodásnak** az a lényege, hogy a létfontosságú informatikai erőforrásokba – alkalmazásokba, információfeldolgozásba, infrastruktúrába és az emberekbe történő befektetés optimális legyen, és azokkal megfelelően gazdálkodjanak. Kulcsfontosságú kérdései a tudás és az infrastruktúra optimalizálásával kapcsolatosak.

• A **kockázatkezelé**shez szükség van arra, hogy a szervezet felső vezetői tisztában legyenek a kockázatokkal, hogy egyértelmű legyen a vállalat kockázatvállalási hajlandósága, hogy tisztában legyenek a megfelelőségi követelményekkel, hogy ismertek legyenek a vállalat jelentős kockázatai, és hogy a kockázatkezelési felelősséget beépítsék a szervezetbe.

• A **teljesítménymérés** nyomon követi és figyelemmel kíséri a stratégia megvalósítását, a projektek befejezését, az erőforrások felhasználást, a folyamatok teljesítményét és a szolgáltatás biztosítását, felhasználva például a kiegyensúlyozott stratégiai mutatószám rendszert, amely lefordítja a stratégiát tevékenységekre a hagyományos számvitel i mutatókkal nem mérhető célok elérése érdekében.

8. ábra:[49] Az informatikai irányítás központi területei

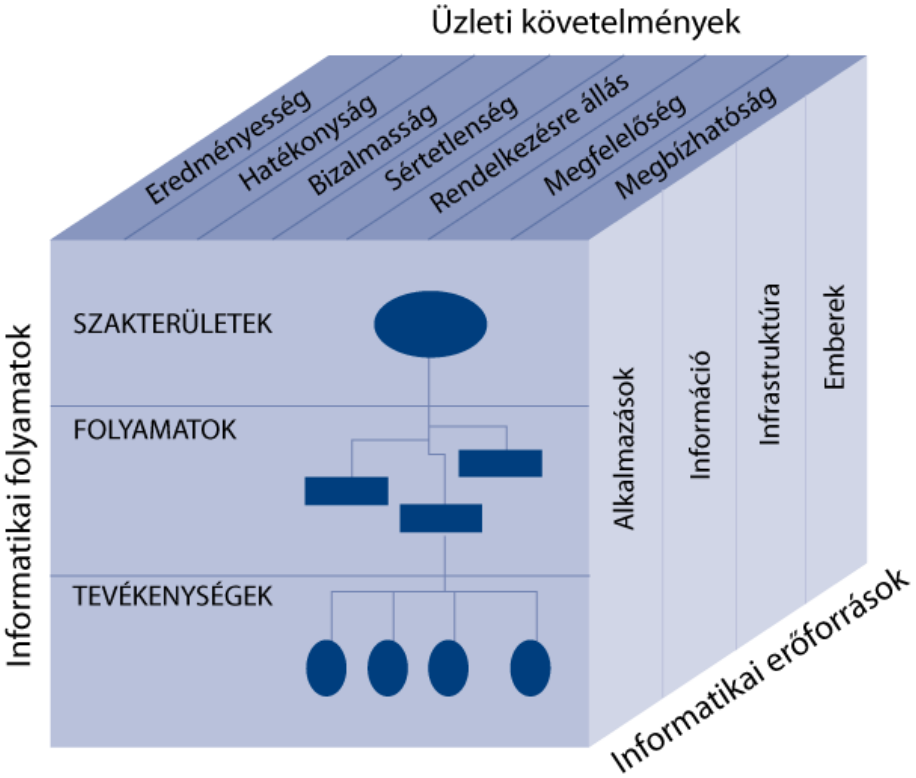
A COBIT nagy figyelmet fordít az informatikai irányítás elméleti hátterére, így több aspektusból elemzi az informatikai irányítás lényegét és területeit, valamint a

[48] Bővebben ld. Muha Lajos: Infokommunikációs biztonsági stratégia, Hadmérnök, 2009, IV. évf. 1. sz. pp. 214-224.

[49] Source: COBIT 4.1. ©1996-2007 ITGI. All rights reserved. Used by permission.

különböző követelmények egymásra hatását és összefüggéseit. Példa ezekre az informatikai irányítás központi területeit bemutató 8. ábra, amelyen minden egyes folyamat ismertetésekor kiemelésre kerülnek az érintett területek, valamint a 9. ábrán bemutatott COBIT kocka, amely a COBIT által lefedett három dimenziót, az üzleti követelmények – informatikai folyamatok – informatikai erőforrások dimenzióit és azok elemeit mutatja be.

Annak ellenére, hogy a COBIT-nek nem deklarált célja más szabványokkal való együttműködés, több megfeleltetés készült az ISACA szervezésében, például az ITIL, ISO/IEC 27002 és PMBOK szabványokkal.



9. ábra:[50] COBIT kocka

Mivel a COBIT szerint nincsen lehetőség tanúsításra, ezért elterjedtségének mértékére nincsen hiteles adat. Tény viszont az, hogy a COBIT-ra épülő Certified Information Systems Auditor (CISA) és Certified Information Security Manager (CISM) szakvizsgák világszerte széles körben, valamint az Amerikai Egyesült Államok

[50] Source: COBIT 4.1. ©1996-2007 ITGI. All rights reserved. Used by permission.

Védelmi Minisztériuma (DoD) által is elismert[51] informatikai biztonsági szakvizsgák. A COBIT Magyarországon a pénzügyi szektorban elsődlegesen követett szabvány.

A COBIT legújabb, ötödik kiadása magába foglalja a COBIT 4.1-et, a Val IT 2.0-t[52] és a Risk IT keretrendszereket, valamint jelentős mértékben hatással van rá a Business Model for Information Security (BMIS)[53] az Information Technology Assurance Framework (ITAF)[54]. A COBIT 5 szemléletében és a hatókörében is bővült a 4.1-hez képest, ugyanis a korábbi informatikai irányítás (IT Governance) hatókörét az érdekelt csoportok (stakeholders) igényeivel bővítve már nagyvállalati informatikai irányításról (Governance of Enterprise IT) beszélhetünk. Többek között a folyamatok és a kontroll célkitűzések is bővültek, módosultak.

A COBIT 5 folyamatai:

- Értékelés, irányítás és figyelemmel kísérés (Evaluate, Direct and Monitor, EDM)
- Összehangolás, tervezés és szervezés (Align, Plan and Organise, APO)
- Építés, beszerzés és megvalósítás (Build, Acquire and Implement, BAI)
- Szállítás, szolgáltatás és támogatás (Deliver, Service and Support, DSS)
- Figyelemmel kísérés, értékelés és felmérés (Monitor, Evaluate and Assess, MEA)

A COBIT 5 magyar nyelvű fordítása jelen könyv írásakor már elkezdődött, de még nem készült el.

[51] Department of Defense Directive 8570
[52] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Val-IT-Framework-2.0.aspx [2014. 03.11.]
[53] http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx [2014. 03.11.]
[54] www.isaca.org/itaf [2014. 03.11.]

8. Tanúsítás, ellenintézkedések, termékszabványok

A tanúsítási tevékenységre több szabvány vonatkozik, ilyenek például:

- MSZ EN ISO/IEC 17021:2011 Megfelelőségértékelés. Irányítási rendszerek auditját és tanúsítását végző testületekre vonatkozó követelmények (ISO/IEC 17021:2011)MSZ EN ISO 19011:2012 Útmutató irányítási rendszerek auditálásához (ISO 19011:2011)MSZ ISO/IEC 27006:2013 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszereinek auditját és tanúsítását végző testületekre vonatkozó követelmények (Angol nyelvű): az ISO/IEC 27001 alapján tanúsítást végző szervezetekre vonatkozó követelményeket határozza meg
- MSZ EN ISO/IEC 17024:2013 Megfelelőségértékelés. Személyek tanúsítását végző testületek általános követelményei (ISO/IEC 17024:2012)
- MSZ EN ISO/IEC 17025:2005 Vizsgáló- és kalibrálólaboratóriumok felkészültségének általános követelményei (ISO/IEC 17025:2005)
- ISO/IEC 17065:2012 Conformity assessment – Requirements for bodies certifying products, processes and services: termék-, folyamat- és szolgáltatástanúsítást végző testületekkel szembeni követelmények, jelenleg még magyar szabványként nem jelent meg, az előző változatot kell használni: MSZ EN 45011:1999 Terméktanúsítási rendszereket működtető szervezetekre vonatkozó általános követelmények (ISO/IEC Guide 65:1996)

A megfelelő szabványok alkalmazása a tanúsító szervek számára kötelező, ezek megfelelő alkalmazását értékeli a nemzeti akkreditáló szerv, Magyarországon a Nemzeti Akkreditáló Testület.

Az informatikai biztonsági ellenintézkedésekre is több szabványt találunk:

- MSZ ISO/IEC TR 15947:2004 Informatika. Biztonságtechnika. Az informatikai behatolás érzékelésének keretszabálya
- MSZ ISO/IEC TR 18044:2006 Informatika. Biztonságtechnika. Az információbiztonsági incidensek kezelése

- Systems Security Engineering Capability Maturity Model (SSE-CMM)[55] de facto szabvány

Amiből viszont olyan sok van, hogy a felsorolásuk is szinte lehetetlen: a műszaki szabványok és leírások. Ezeknek az alkalmazása konkrét technológiai megvalósításkor, elsősorban termékek tervezésekor, gyártásakor szükséges. Természetesen az ezeknek való megfelelés is ellenőrizhető a tanúsítás során. A teljesség igénye nélkül tehát pár példaként szolgáló szabvány:

- MSZ ISO/IEC 18028-3:2009 Informatika. Biztonságtechnika. IT-hálózatbiztonság. 3. rész: Hálózatok közötti biztonságos kommunikáció biztonsági átjárók alkalmazásával
- MSZ ISO/IEC 18028-4:2005 Informatika. Biztonságtechnika. IT-hálózatbiztonság. 4. rész: Biztonságos távoli hozzáférés
- MSZ ISO/IEC 14888-1:2001 Információtechnika. Biztonságtechnika. Digitális aláírások függelékkel. 1. rész: Általános ismertetés
- MSZ ISO/IEC 14888-2:2001 Információtechnika. Biztonságtechnika. Digitális aláírások függelékkel. 2. rész: Azonosítás alapú módszerek
- MSZ ISO/IEC 14888-3:2001 Információtechnika. Biztonságtechnika. Digitális aláírások függelékkel. 3. rész: Tanúsítvány alapú módszerek
- MSZ ISO/IEC 18014-1:2004 Informatika. Biztonságtechnika. Időbélyegzési szolgáltatások. 1. rész: Keretszabály
- MSZ ISO/IEC 18014-2:2004 Informatika. Biztonságtechnika. Időbélyegzési szolgáltatások. 2. rész: Független adattokokat előállító mechanizmusok
- MSZ ISO/IEC 18014-3:2005 Informatika. Biztonságtechnika. Időbélyegzési szolgáltatások. 3. rész: Összerendelt adattokokat előállító mechanizmusok
- MSZ ISO/IEC 15816:2005 Informatika. Biztonságtechnika. A hozzáférés-ellenőrzés biztonsági információobjektumai
- MSZ ISO/IEC 13888-1:2005 Informatika. Biztonságtechnika. Letagadhatatlanság. 1. rész: Általános ismertetés
- MSZ ISO/IEC 13888-2:2001 Információtechnika. Biztonságtechnika. Letagadhatatlanság. 2. rész: Szimmetrikus technikákon alapuló módszerek

[55] http://www.sse-cmm.org/docs/ssecmmv3final.pdf [2014. 03.12.]

- MSZ ISO/IEC 13888-3:2001 Információtechnika. Biztonságtechnika. Letagadhatatlanság. 3. rész: Aszimmetrikus technikákon alapuló módszerek
- MSZ ISO/IEC 15945:2002 Informatika. Biztonságtechnika. Ajánlás/nemzetközi szabvány bizalmi harmadik fél (TTP) digitális aláírások alkalmazását támogató szolgáltatásaira
- MSZ ISO/IEC 11770-1:2005 Informatika. Biztonságtechnika. Kulcsgondozás. 1. rész: Keretrendszer
- MSZ ISO/IEC 11770-2:2005 Informatika. Biztonságtechnika. Kulcsgondozás. 2. rész: Szimmetrikus technikákat alkalmazó mechanizmusok
- MSZ ISO/IEC 11770-3:2005 Informatika. Biztonságtechnika. Kulcsgondozás. 3. rész: Aszimmetrikus technikákat alkalmazó mechanizmusok
- MSZ ISO/IEC 11770-4:2008 Informatika. Biztonságtechnika. Kulcsgondozás. 4. rész: Gyenge titkosságon alapuló mechanizmusok
- CEN CWA 14168:2001 Secure Signature-Creation Devices "EAL 4"
- CEN CWA 14169:2004 Secure Signature-Creation Devices "EAL 4+"
- CEN CWA 14170:2004 Security Requirements for Signature Creation Applications
- CEN CWA 14171:2004 General guidelines for electronic signature verification
- ANSI X9.30-1:1997 Public-Key Cryptography for the Financial Services Industry - Part 1: The Digital Signature Algorithm (DSA), American Bankers Association, 1997.
- ANSI X9.30-2:1997 Public Key Cryptography Using Irreversible Algorithms - Part 2: The Secure Hash Algorithm (SHA-1)
- CEN CWA 13987-1:2003 D/E/F, October 2003 Smart Card Systems: Interoperable Citizen Services: Extended User Related Information - Part 1: Definition of User Related Information and Implementation
- ETSI TS 102 176-1 V2.0.0 (2007-11-19) Electronic Signatures and Infrastructures (ESI);
- Algorithms and Parameters for Secure Electronic Signatures;
- Part 1: Hash functions and asymmetric algorithms
- ETSI TS 101 903 V1.4.1 (2009-06-15) XML Advanced Electronic Signatures (XAdES)

- ISO/IEC 10118-3:2004/Amd 1:2006
- (2006-02-17) Dedicated Hash-Function 8 (SHA-224)
- ISO/IEC 7816-1:1998 Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics
- ITU X.509 ITU-T Recommendation X.509, Information Technology – Open Systems Interconnection – The directory: authentication framework
- IAS ECC TS 1.0.1 European Card for E-Services and National e-Id Applications
- FIPS[56] PUB 197 Advanced Encryption Standard (AES), 2001
- PKCS[57] #1 V2.1: June 14, 2002 RSA Cryptography Standard
- RFC[58] 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC 5758 Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA

Látható, hogy a szabványok témakörei és a kibocsátó szervek köre nagyon széles körű, az alkalmazandó szabványok kiválasztása a tervezés során komoly szabványismeretet igényel.

[56] Federal Information Processing Standards, az Egyesült Államok szövetségi kormányának szabványa, nem katonai célú szabvány
[57] public-key cryptography standards, az RSA, az EMC Corporation biztonsági divíziójának, korábban RSA Data Security Inc.-nek a nyilvános kulcsú titkosításra vonatkozó szabványsorozatának része
[58] Request for Comments, az Internet Engineering Task Force (IETF) által kibocsátott Internetes technológiákkal kapcsolatos feljegyzés, de facto szabványnak tekinthető

9. Szabványosult ajánlások

Végül, de nem utolsó sorban szükséges foglalkoznunk azokkal a magyar ajánlásokkal, amelyek vagy teljes mértékben magyar szakemberek munkája által, vagy a nemzetközi szabványok felhasználásával készültek és Magyarországon tulajdonképpen szabványként használhatók (másrészről tekinthetőek viszont az állami irányítás egyéb jogi eszközeinek is), tehát például tanúsítható az azoknak való megfelelés is.[59] Ami miatt a szabványok között kerülnek ezek felsorolásra, az a felépítésük és jellegük. Ezek kibocsátói egy szervezet és annak jogutódjai: az Informatikai Tárcaközi Bizottság (ITB), a Kormányzati Informatikai Egyeztető Tárcaközi Bizottság (KIETB), és a Közigazgatási Informatikai Bizottság (KIB).

A téma szempontjából legfontosabb ajánlások a következők:

- Informatikai Tárcaközi Bizottság 8. sz. ajánlása, Informatikai biztonsági módszertani kézikönyv[60]
- Informatikai Tárcaközi Bizottság 12. sz. ajánlása, Informatikai rendszerek biztonsági követelményei[61]
- Közigazgatási Informatikai Bizottság 25. számú ajánlása, Magyar Informatikai Biztonsági Ajánlások (v1.0, 2008. június)
    - 25/1 – Magyar Informatikai Biztonság Irányítási Keretrendszer (MIBIK)
        - 25/1-1 – Informatikai Biztonság Irányítási Rendszer (IBIR)
        - 25/1-2 – Informatikai Biztonság Irányítási Követelmények (IBIK)
        - 25/1-3 – Az Informatikai Biztonság Irányításának Vizsgálata (IBIV)
    - 25/2 – Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)
    - 25/3 – Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX)

[59] Az Ibtv. (2013. évi L. tv.) 4.§-ában nevesítés nélkül utal arra, hogy az ilyen bevezetett rendszereket a NEIH az eljárása során figyelembe veszi.
[60] Az ajánlás már érvényét vesztette, viszont történeti jelentősége miatt szükséges megemlíteni.
[61] Az ajánlás már érvényét vesztette, viszont történeti jelentősége miatt szükséges megemlíteni.

- Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár[62]

A Magyar Informatikai Biztonsági Ajánlások (MIBA) nevet viselő Közigazgatási Informatikai Bizottság 25. számú ajánlássorozata az Informatikai Tárcaközi Bizottság korábbi 8, 12 és 16 számú ajánlásait hivatott kiváltani, mintegy modernizálva, bővítve azokat. Az ajánlások kialakításakor követték a 2008-ban hatályos elektronikus közigazgatásra vonatkozó követelményrendszert (amely azóta nagymértékben megváltozott ld. Ekszt.) és a magyar közszféra realitásait. Az ajánlások alapján meghatározhatóak a szabályok, eljárásrendek, előállíthatóak a szükséges dokumentációk és az értékelés- illetve tanúsítás[63] is elvégezhető azok alapján. Az ajánlás nemzetközi szabványokon alapul, azok fordításával és adaptációjával készült. Felhasználja az ISO/IEC 27001, ISO/IEC 27002, Common Criteria fontosabb elemeit, az informatikai biztonságot irányítási rendszernek tekinti, alkalmazza a PDCA elvet. Sajnos gyakorlati alkalmazásának mértéke elmaradt az elvárttól.
A Közigazgatási Informatikai Bizottság az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytárat 28. számú ajánlásaként adta ki, amely az elektronikus közigazgatás fejlesztéséhez szükséges teljes eszköztárat magában foglalja. Az informatikai biztonsági követelményeken túl funkcionális és módszertani követelményeket is egyesít magában.

[62] A követelménytár elérhető a http://kovetelmenytar.complex.hu/ weblapon [2014. 01.08.]
[63] ld. Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)

Szabványjegyzék

De jure szabványok

ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model

ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components

ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components

ISO/IEC 18045:2008 Information technology -- Security techniques -- Methodology for IT security evaluation

ISO/IEC 20000-1:2011 Information technology -- Service management -- Part 1: Service management system requirements

ISO/IEC 20000-2:2005 Information technology -- Service management -- Part 2: Code of practice

ISO/IEC TR 20000-3:2009 Information technology -- Service management -- Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1

ISO/IEC TR 20000-4:2010 Information technology -- Service management -- Part 4: Process reference model

ISO/IEC TR 20000-5:2010 Information technology -- Service management -- Part 5: Exemplar implementation plan for ISO/IEC 20000-1

ISO/IEC 26300:2006 Open Document Format for Office Applications (OpenDocument) v1.0

ISO/IEC 27000:2012 Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27003:2010 Information technology – Security techniques – Information security management system implementation guidance

ISO/IEC 27004:2009 Information technology – Security techniques – Information security management – Measurement

ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management

ISO/IEC 27006:2011 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27007:2011 Information technology – Security techniques – Guidelines for information security management systems auditing

ISO/IEC TR 27008:2011 Information technology – Security techniques – Guidelines for auditors on information security controls

ISO/IEC WD 27009 The Use and Application of ISO/IEC 27001 for Sector/Service-Specific Third-Party Accredited Certifications

ISO/IEC 27010:2012 Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications

ISO/IEC 27011:2008 Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

ISO/IEC 27013:2012 Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001

ISO/IEC 27014:2013 Information technology – Security techniques – Governance of information security

ISO/IEC TR 27015:2012 Information security management guidelines for financial services

ISO/IEC DTR 27016 Information technology – Security techniques – Information security management – Organizational economics

ISO/IEC WD 27017 Information technology – Security techniques – Code of practice for information security controls for cloud computing services based on ISO/IEC 27002

ISO/IEC CD 27018 Code of practice for data protection controls for public cloud computing services

ISO/IEC TR 27019:2013 Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity.

ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity

ISO/IEC 27033-1:2009 Information technology – Security techniques – Network security: Overview and concepts

ISO/IEC 27033-2:2012 Information technology – Security techniques – Network security: Guidelines for the design and implementation of network security

ISO/IEC 27033-3:2010 Information technology – Security techniques – Network security: Threats, design techniques and control issues

ISO/IEC 27033-5:2013 Securing communications across networks using Virtual Private Networks (VPNs)

ISO/IEC 27034-1:2011 Information technology – Security techniques – Application security – Part 1: Overview and concepts

ISO/IEC 27035:2011 Information technology – Security techniques – Information security incident management

ISO/IEC FDIS 27036-1 Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts

ISO/IEC DIS 27036-2 Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements

ISO/IEC FDIS 27036-3 Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security

ISO/IEC WD 27036-4 Information technology – Information security for supplier relationships – Part 4: Guidelines for security of Cloud services

ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence

ISO 27799:2008 Health informatics – Information security management in health using ISO/IEC 27002

ISO/TR 13569:2005 Financial services – Information security guidelines

MSZ EN 45020:2007 A szabványosítás és az azzal kapcsolatos tevékenységek. Általános szakszótár (ISO/IEC Guide 2:2004)

MSZ EN ISO 27799:2009 Egészségügyi informatika. Az információbiztonság irányítása az egészségügyben az ISO/IEC 27002 alkalmazásával (ISO 27799:2008)

MSZ ISO/IEC 13335-1:2005 Informatika. Biztonságtechnika. Az informatikai és távközlési biztonság menedzselése. 1. rész: Az informatikai és távközlési biztonság menedzselésének fogalmai és modelljei

MSZ ISO/IEC TR 13335-3:2004 Informatika. Az informatikai biztonság menedzselésének irányelvei. 3. rész: Az informatikai biztonság menedzselésének technikái

MSZ ISO/IEC TR 13335-4:2004 Informatika. Az informatikai biztonság menedzselésének irányelvei. 4. rész: A biztonsági ellenintézkedések megválasztása

MSZ ISO/IEC TR 13335-5:2004 Informatika. Az informatikai biztonság menedzselésének irányelvei. 5. rész: A hálózatbiztonság menedzselési útmutatója

MSZ ISO/IEC 15408-1:2002 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 1. rész: Bevezetés és általános modell

MSZ ISO/IEC 15408-2:2003 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 2. rész: A biztonság funkcionális követelményei

MSZ ISO/IEC 15408-3:2003 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 3. rész: A biztonság garanciális követelményei

MSZ ISO/IEC 18028-4:2005 Informatika. Biztonságtechnika. IT-hálózatbiztonság. 4. rész: Biztonságos távoli hozzáférés

MSZ ISO/IEC 17799:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve

MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények

De facto szabványok, ajánlások, módszertanok

Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 1, September 2006.

Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1 Revision 3 Final, July 2009.

Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.3, August 2005.

Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1 Revision 3, July 2009.

Control Objectives for Information and related Technology (COBIT) 4.1, ISACA

Information Technology Security Evaluation Criteria (ITSEC)

IT Infrastructure Library (ITIL)

(röv. ITB 8. sz. ajánlás) Informatikai Tárcaközi Bizottság ajánlásai. Informatikai biztonsági módszertani kézikönyv 8. sz. ajánlás. Budapest, 1994.

(röv. ITB 12. sz. ajánlás) Informatikai Tárcaközi Bizottság ajánlásai. Informatikai rendszerek biztonsági követelményei 12. sz. ajánlás. Budapest, 1996.

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/1. kötet: Magyar Informatikai Biztonsági Keretrendszer (MIBIK) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/1-1. kötet: Informatikai Biztonsági Irányítási Rendszer (IBIR) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/1-2. kötet: Informatikai Biztonság Irányítási Követelmények (IBIK) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/1-3. kötet: Az Informatikai Biztonság Irányításának Vizsgálata (IBIV) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2. kötet: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-1. segédlet: MIBÉTS - Modell és Folyamatok 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-2. segédlet: MIBÉTS – Útmutató a Megbízók számára 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-3. segédlet: MIBÉTS – Útmutató a Fejlesztők számára 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-4. segédlet: MIBÉTS – Útmutató Értékelőknek 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-5. segédlet: MIBÉTS – Értékelési módszertan 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/3. kötet: Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX) 1.0 verzió

A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár http://kovetelmenytar.complex.hu/

Trusted Computer Systems Evaluation Criteria (TCSEC)

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.