IT biztonság

2018/2019 tanév ősz

Szabványok

A valóság

- Ahhoz, hogy teljesítsük a jogszabályi kötelezettségeket, nem kell mást tenni, mint használni az ipari szabványokat
- Néhány ezek közül
  – ISO 27000-es család
  – Common Criteria
  – PCI DSS

Mi az IBIR ?

- Információbiztonsági Irányítási Rendszer
- Az átfogó irányítási rendszernek az a része, amely – egy, a működési kockázatokat figyelembe vevő megközelítésen alapulva – kialakítja, bevezeti, működteti, figyeli, átvizsgálja, fenntartja és fejleszti az információvédelmet.
- Az irányítási rendszer magában foglalja a szervezeti felépítést, a szabályzatot, a tervezési tevékenységeket, a felelősségi köröket, a gyakorlatot, az eljárásokat, a folyamatokat és az erőforrásokat.

IBIR szükségessége

- Az IBIR létrehozásának számos oka lehet:
  - Törvénynek vagy szabályozásnak való megfelelés
  - Az információ értéke olyan nagy, hogy nem lehet védtelenül hagyni
  - Külső nyomás (tulajdonosok, partnerek, vásárlók)
- Ennél kevésbé nyilvánvaló okok is vannak:
  - Az információs rendszerek egyszerűbb kezelése
  - Csökkenő költségek (bár ez elsőre nehezen hihető)

IBIR bevezetése

- IBIR-t bevezetni nem egyszerű, mert
  – viszonylag sok idő kell ahhoz, hogy gördülékenyen működjön (ld. ISO 9000)
  – a bevezetés megakadhat a vállalaton belül
- Szervezeti változások miatt
- A támogatás, az anyagiak vagy az emberek kiesése miatt
- A tapasztalat azt mutatja, hogy a nagyobb szervezeteknél szokott lenni „IBIR-szerű” szabályozás, ami viszont
  – nem alkot összefüggő rendszert,
  – hiányos lehet,
  – nem lehet tanúsítványt szerezni rá, ami bizonyos esetekben fontos lehet

IBIR bevezetése

- Az üzleti (ügymeneti) folyamatok, az informatikai infrastruktúra, valamint ezek védelmi szintjének felmérése
- Kockázatelemzés- és értékelés
- Informatikai Biztonsági Politika elkészítése – főbb IT biztonsági irányvonalak meghatározása
- Informatikai Biztonsági Stratégia
- Informatikai Biztonsági Kézikönyv elkészítése – az információbiztonsági rendszer tartalmának meghatározása
- Az IBIR megvalósítása – szabályzatok, eljárások, egyéb dokumentumok elkészítése, valamint a technikai megoldások kivitelezése
- Oktatás
- Bevezetés
- Előaudit (ISO 27001)

ISO 27001

- Nemzetközileg elfogadott és széles körben elismert biztonsági szabvány
- Definíció szerint „a legszéleskörűbb eljárások, melyek az információs biztonság legjobb gyakorlati megvalósítását szolgálják”.
- Két részre bontható
  - 1. rész : A Code of Practice for Information Security Managementet (magyarul: Az informatikai biztonság menedzsmentjének gyakorlati kódexe)
  - 2. rész: Specification for Information Security Management Systems. (Az informatikai biztonsági menedzsment rendszerének specifikációja)

ISO 27001

- Ahhoz, hogy a fenyegetésekkel szemben hatékonyan lehessen fellépni, nem elegendő kizárólag technikai-szervezési intézkedéseket tenni. Az átfogó védelem alapfeltétele, hogy minden munkatárs minden szinten biztonságtudatos magatartást tanúsítson.
- Az ISO/IEC 27001 szabvány az információ három lényeges jellemzőjére fókuszál: rendelkezésre állás, bizalmas jelleg és sértetlenség.

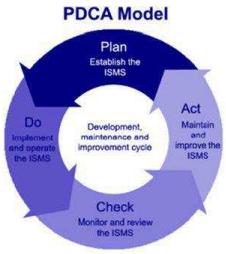
ISO 27001

Alapkoncepció:

- Irányítási rendszer
  - PDCA ciklus
  - Irányítás és felelősség
  - Dokumentálás
  - Oktatás
  - Vezetőségi átvizsgálás
  - Belső auditok
- Értékek meghatározása
- Kockázatmenedzsment
  - Azonosítás
  - Értékelés
  - Védelmi intézkedések gyakorlatba átültetése

ISO 27001

ISO 27001 PDCA Approach



- **Plan:**
  - Study requirements
  - Draft an IS Policy
  - Discuss in IS Forum (committee)
  - Finalize and approve the policy
  - Establish implementation procedure
  - Staff awareness/training
- **Do:**
  - Implement the policy
- **Check:**
  - Monitor, measure, & audit the process
- **Act:**
  - Improve the process

ISO 27001 Sikertényezők

Információvédelmi politika, – célok, intézkedések	üzleti célokra vonatkozzanak
Eljárás és eljárási modell (PDCA keretrendszer)	összehangolása a vállalati kultúrával
A vezetőség támogatása és jóváhagyása	a hierarchia minden szintjén
A kockázatértékelés és -menedzsment helyes megértése	minden érintett oktatása
Információbiztonsági politika ismerete	vezetők, munkatársak és üzleti partnerek képzése
Az információbiztonsági irányítási tevékenységekhez szükséges költségkeret biztosítása	reális költségek betervezése
Ésszerű problématudatosság kialakítása	„nevelés” felvétele az oktatási tervbe
Hatékony folyamat kiépítése információbiztonsági incidensek kezelésére	egyértelmű követelmények meghatározása

ISO 27002

- Jelentős változások történtek a szabvány megközelítésében
- Korábban a CIA követelmények biztosítása volt a fókuszban
- Az új szabvány az üzleti igényeket helyezi előtérbe
  – Az információbiztonság az információ védelme a széleskörű fenyegetésektől, hogy biztosítsák az üzleti folyamatok működésének folytonosságát, a lehető legkisebbre csökkentsék a kockázatot, és legnagyobbra növeljék a befektetési megtérülést és a működési lehetőségeket.

ISO 27002 main chapters

- Information Security Policies
- Organization of Information Security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and environmental security
- Operation Security- procedures and responsibilities, Protection from malware, Backup, Logging and monitoring, Control of operational software, Technical vulnerability management and Information systems audit coordination
- Communication security - Network security management and Information transfer
- System acquisition, development and maintenance - Security requirements of information systems, Security in development and support processes and Test data
- Supplier relationships - Information security in supplier relationships and Supplier service delivery management
- Information security incident management - Management of information security incidents and improvements
- Information security aspects of business continuity management - Information security continuity and Redundancies
- Compliance - Compliance with legal and contractual requirements and Information security reviews

Termékbiztonság

- A vásárlók egyre több, IT biztonsághoz szükséges eszközhöz férnek hozzá, melyek különböző képességekkel rendelkeznek.
- A vásárlóknak dönteniük kell, hogy milyen eszközök alkalmasak informatikai rendszerük kielégítő védelmére.
- Egyre komolyabban veszik az informatikai termékek nemzetbiztonsági vonatkozásait.
- Hatás: a termékek kiválasztása befolyásolja az egész informatikai rendszer biztonságát.

Termékbiztonság

A biztonságos rendszerek építése tehát függ a következőktől:

- Jól meghatározott IT biztonsági követelmények és specifikációk
  – Tulajdonképpen milyen biztonsági funkciókat is akarunk?
- Minőségi biztonsági mérőszámot és megfelelő tesztelést, értékelést, felmérést kell alkalmazni
  – Biztosítékot akarunk arra, hogy amit kapunk, az tényleg az, amit kértünk.

Common Criteria – ISO 15408

- Nemzetközileg elfogadott keretrendszer az IT biztonság területén
  – Közös struktúra és nyelv a termékek/rendszerek IT biztonsági követelményeinek kifejezésére
  – Szabványos IT biztonsági követelmény összetevők és csomagok gyűjteménye a fejlesztési folyamatokra
- Nemzetközileg elfogadott értékelési módszertan, besorolási rendszer
- A szoftverfejlesztés biztonsági szempontjainak elfogadott módszertana (annak minden kritikájával együtt)

CC – amit lefed

- Olyan IT rendszerek és termékek biztonsági tulajdonságainak a specifikációját támogatja, melyek a CIA elvet valósítják meg
- Független értékelések eredményeinek az összehasonlíthatósága
- Hardverben, szoftverben és förmverben implementált védelmi intézkedésekre vonatkoztatható
  - technológia-független
  - a fejlesztő által kívánt kombinációk határozhatók meg
- Értékelés módszertan
  - ezt a Common Evaluation Methodology for Information Technology Security Evaluation (CEM) tartalmazza (ISO/IEC 18045)

CC – és amit nem…

- A személyi és fizikai biztonsági intézkedések implementációjának vizsgálatát
- A CC felhasználását
  - adminisztratív, jogi, eljárásbeli szabályok
  - tanúsítási és akkreditálási eljárások
  - kölcsönös elfogadási megállapodások
- Kriptográfiai algoritmusok leírása

CC – a felhasználók felé

- El tudják dönteni, hogy az adott termék „biztonsági szintje” megfelel-e számukra.
- Össze tudják hasonlítani a különböző termékeket az értékelések alapján.
- Megvalósítástól független struktúra, a Védelmi Profil (PP) alapján láthatják az adott fajta termékkel szemben támasztott általános biztonsági követelményeket.

CC – a fejlesztőknek

- Segítséget nyújt az értékelésre való felkészítéshez.
- Megmutatja a fejlesztőknek, hogy a termék megfelelően biztonságos-e.
- Akár több, különböző követelményeket tartalmazó Védelmi Profilból (PP) egy megvalósítástól függő, az adott termékre vonatkozó Biztonsági Előirányzatot (ST) lehet létrehozni.

CC – az értékelőknek

- Megmondja, hogy milyen vizsgálatokat és melyik biztonsági elemeken kell végrehajtaniuk az értékelőknek.
- Nem mondja meg, hogy ezeket milyen módon kell végrehajtaniuk.

CC – első lépés

- Input:
  - Fizikai környezet
  - Védendő elemek
- Output:
  - Biztonsági célok
    - Fenyegetések elleni fellépés
    - Szervezeti biztonsági szabályoknak való megfelelés

CC – második lépés

- Input:
  - Biztonsági célok
  - Követelménykatalógus
- Output:
  - Funkcionális követelmények
  - Garanciális követelmények
  - Környezeti követelmények

CC – Funkcionális követelmények

- Audit
- Kommunikáció
- Kriptográfiai funkciók
- Adatvédelem
- Azonosítás, hitelesítés
- Biztonsági naplózás
- Biztonságkezelés
- Titoktartás
- Erőforrás használás
- Bizalmi csatornák
- Biztonsági funkciók védelme

COMMON CRITERIA

CC- Garanciális követelmények

A betartandó fejlesztési eljárásrend

- Fejlesztés
- Tesztelés
- Dokumentáció
- Etc.

Garanciaszintek: Az egyre magasabb Értékelési Garanciaszinteken (EAL) egyre több követelmény jelenik meg, illetve a követelményeken belül az összetevők egyre magasabb szintű feltételeket szabnak.

CC - garanciaszintek

EAL1: Functionally Tested. Applies when you require confidence in a product's correct operation, but do not view threats to security as serious. An evaluation at this level should provide evidence that the target of evaluation functions in a manner consistent with its documentation and that it provides useful protection against identified threats.

EAL2: Structurally Tested. Applies when developers or users require low to moderate independently assured security but the complete development record is not readily available. This situation may arise when there is limited developer access or when there is an effort to secure legacy systems.

EAL3: Methodically Tested and Checked. Applies when developers or users require a moderate level of independently assured security and require a thorough investigation of the target of evaluation and its development, without substantial reengineering.

EAL4: Methodically Designed, Tested, and Reviewed.

EAL5: Semi-Formally Designed and Tested.

EAL6: Semi-Formally Verified Design and Tested.

EAL7: Formally Verified Design and Tested.

PCI DSS

- Egy olyan szabvány, ami a bankkártya adatokat feldolgozó cégek
  - biztonsági menedzsmentjével,
  - szabályzati rendszerével,
  - hálózati architektúrájával,
  - szoftvereivel és
  - más védelmi megoldásaival

  kapcsolatos követelményeket támaszt.
- A Payment Card Industry (PCI) Data Security Standard (DSS) szabványt a Visa és a Mastercard alkotta meg. Hozzájuk csatlakozott később az American Express, a Discover Financial Services és a JCB.
- Elsődleges céljuk a bankkártyákkal való nagyarányú visszaélések csökkentése az elektronikus kereskedelemben, a kártyaelfogadóknál és a kereskedőknél.
- Mindenkire vonatkozik, aki bankkártya adatokat tárol, dolgozol fel, vagy továbbít.

PCI DSS tartalma

- Biztonságos hálózat építése és üzemeltetése:
  - 1. követelmény: A kártyabirtokos adatainak védelméért tűzfalat kell telepíteni és üzemeltetni.
  - 2. követelmény: Nem szabad a gyártók által használt alapbeállítású rendszerjelszavakat és biztonsági paramétereket használni.
- A kártyabirtokos adatainak védelme:
  - 3. követelmény: Védeni kell a kártyabirtokosok tárolt adatait.
  - 4. követelmény: A nyílt hálózatokon történő adatátvitel során titkosítani kell a kártyabirtokos adatait.
- Sérülékenység-kezelési program fenntartása:
  - 5. követelmény: Vírusvédelmi megoldásokat kell használni, és rendszeresen frissíteni.
  - 6. követelmény: Biztonságos rendszereket és alkalmazásokat kell fejleszteni és üzemeltetni.

PCI DSS tartalma

- Erős hozzáférés-védelmi megoldások alkalmazása:
  - 7. követelmény: A kártyabirtokos adataihoz csak az férhessen hozzá, akire az tartozik.
  - 8. követelmény: Minden olyan ember, aki hozzáférhet a rendszerhez, rendelkezzen egyedi azonosítóval.
  - 9. követelmény: A kártyabirtokos adataihoz való fizikai hozzáférést meg kell akadályozni.

GDPR NAGYON RÖVIDEN

- A GDPR az EU adatvédelmi rendelete, amely 2018. május 25-től hatályos hazánkban
- A legfonosabbak:
  - Mielőtt bármilyen adatot bekér tőlünk egy szervezet, pontos tájékoztatást kell adnia, hogy mi az adatkezelés célja, hogyan kezeli az adatokat vagy például kik férhetnek hozzá;
  - Egy adatbázisból kérésünk esetén például e-mail-címünk törlésének elmaradása az eddigieknél jobban számonkérhető, szankcionálható lesz
  - Az új jogszabályok magas bírságokkal kényszerítik ki a biztonságos adatkezelést, vagyis azt, hogy személyes adatainkhoz ne férhessenek hozzá illetéktelenek. A bíró gyakorlat még hiányzik, de a bírság akár 20 millió euró vagy az éves árbevétel 4 %- a is lehet…
  - Olyan eseteket is szabályoz és szankcionál a rendelkezés, amikor például egy hackertámadás következtében személyes adataink kikerülnek az adatkezelő rendszeréből, ellopják azokat vagy ha egy rendszerhiba miatt megsemmisülnek.
  - Nagyobb lesz a felelősség az adatkezelőkön;