IT ellenőrzés feladata válság idején

Budapest, 2010. április 28.

BEMSZ rendezvény, Budapest, V. Szabadság tér 5-6.

Kirner Attila, Főosztályvezető-helyettes
PSZÁF Informatika Felügyeleti Osztály
kirner.attila@pszaf.hu

Gondolatok a válságról

- Definíció: „A válság az egyén, egy csoport vagy a társadalom életében megnyilvánuló súlyos zavar, nehéz helyzet …” (NYÁRÁDY – SZELES, 2005)
- Lényege: A kimenetele jó is, rossz is lehet (minden rosszban van valami jó)! „… a kínai nyelvben a válság szónak kettős jelentése van, veszély és lehetőség, …” (BARLAI – KŐVÁGÓ, 2004)
- Szakaszai: „veszély, kialakulás, emelkedés, tetőpont (krízis), hanyatlás, megoldás” (NYÁRÁDY – SZELES, 2005)
- Természete: globális (világméretű), komplex (pénzügyi, gazdasági, társadalmi, bizalmi), gyors.
- Okai: „ A ’90-es évek válságaiért 75,2%- ban a menedzsment a felelős„ (ICM - Institute for Crisis Management felmérés)
- Megoldása: azonnali erőforrásokkal, folyamatos prevencióval.
- „A válságkommunikáció alapvető feladata, hogy a működési zavar kommunikációs problémáit gyors, precíz és megbízható információáramlással megoldja.” (BARLAI – KŐVÁGÓ, 2004)

Tanulmányok a válságról

Tanulmányok:

Az USA jelzálogválságának elemzése, tapasztalatai, tanulságai és hatása a magyar jelzáloghitel piacra

http://www.pszaf.hu/data/cms1565391/Tanulmny_vs_2_doc0805011.pdf

Lámfalussy Sándor: Pénzügyi válságok a fejlődő országokban

http://*szakolczai-gyorgy.avfweb.hu/?download=t43.pdf*

- És egy link: Institute for Cirsis Management http://www.crisisexperts.com/

A Soc.Gen. probléma tanulságai

A Banque de France javaslatai a Societé General probléma kezelésére (Banque de France: Initial lessons to be drawn from Societe Generale event – 2008.02.15.) :

- A hitelintézetek belső kontrollrendszerének erősítése.
- Áttekinteni és javítani a belső vezetői beszámolási rendszert.
- A belső kontroll rendszer szabályozásának kibővítése a működési kockázatok kontrolljaival.
- A visszaélések elleni kontrollokkal kibővíteni a belső ellenőrzési rendszert.
- Az irányítási rendszer kockázatmenedzselési részének erősítése.
- A Bankfelügyeleti szankciók lehetőségeinek szélesítése.
- Nemzetközi összefogás és konzultációk kezdeményezése a reputációs kockázatok csökkentése és a transzparens működés tárgyában.

PSZÁF feladatok

A PSZÁF feladata, célja (2007. évi CXXXV. törvény):

„A törvény célja, hogy a pénzügyi piacok **zavartalan és eredményes működése**, a piaci viszonyok **átláthatósága**, a **tisztességes piaci verseny** fenntartása, illetve a pénzügyi piacokkal szembeni **bizalom erősítése** érdekében szabályozza a piaci szereplők felügyeletét körébe utal.”

3. § (1) A Felügyelet ellátja mindazon feladatot, amelyet törvény vagy törvény felhatalmazása alapján kiadott jogszabály a hatáskörébe utal.

3. § (2): „A Felügyelet feladatai ellátása során együttműködik a Magyar Nemzeti Bankkal (a továbbiakban: MNB), a Gazdasági Versenyhivatallal és a 4. §-ban meghatározott szervezetek vagy személyek ellenőrzését ellátó más hatóságokkal.”

Felügyeleti prioritások

2009	2010
Likviditás	Likviditás
Stratégia	Felelős hitelezés
Hitelkockázatok kezelése	Tőke és jövedelmezőség
Tisztességes piaci magatartás biztosítása, működési kockázatok	Ügyfelek érdekvédelme, fogyasztóvédelem, működési kockázatok kezelése

EuroCACS gondolatok

ISACA 2010 szlogenje: „Trust in and value from IT systems” – Bizalom és értékteremtés az információs rendszerekkel”

Idézet Paul Williams, ISACA stratégiai elnök előadásából:

„Alacsony színvonalú folyamatok, gyenge minőségű terméket eredményeznek”

„A COBIT és a Val IT szerinti folyamatok bevezetése, menedzselése és monitorozása jobb minőségű végtermékhez vezet”

És egy tanulmány:

A pénzintézeti kiszervezési tevékenység IT biztonsági kérdései
http://www.pszaf.hu/data/cms2151158/Kiszervezesi_palyazat_PRAUDIT_2010_04_07_v10.pdf

1. Kockázatkezelés

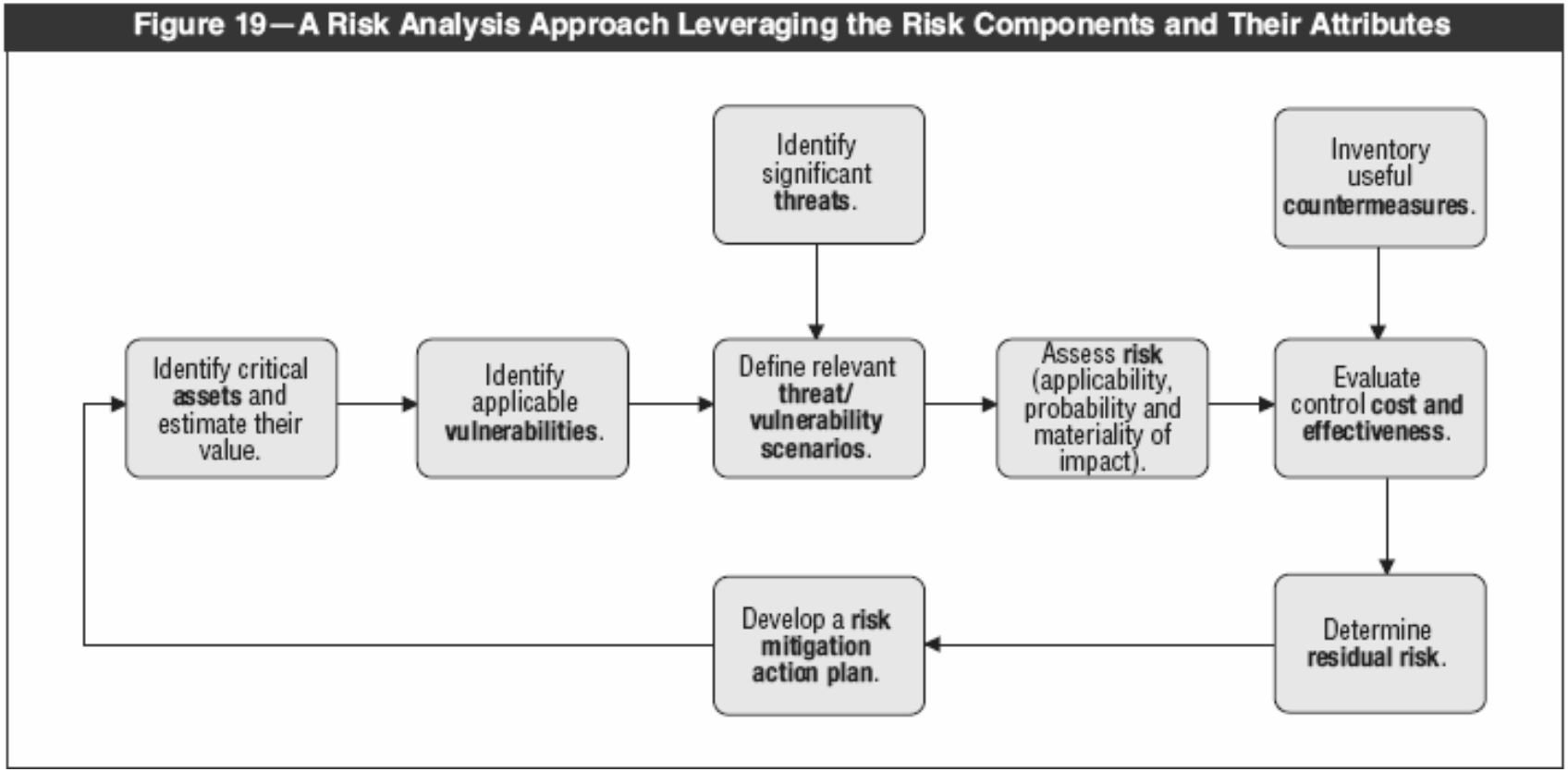
Kockázatkezelés:

- **Jogszabály: Mpt. 77/A. § (2) bekezdés, Öpt. 40/C. § (2) bekezdés, Bszt. 12. § (2) bekezdés, Hpt. 13/C. § (2)**A pénzügyi szervezet köteles az informatikai rendszer **biztonsági kockázatelemzését** szükség szerint, **de legalább kétévente** felülvizsgálni és aktualizálni**.**

- **Jellemző problémák:**
  - Nincs módszertan
  - Nincs szabályozás
  - Nem történik meg az értékelés és a priorítási sorrend felállítása
  - Nincs IT biztonsági szakértő általi visszacsatolás
  - Nincs javaslat a kockázatok csökkentésére
  - Nincs vezetői jóváhagyás
  - Nem épül be a vállalati kockázatkezelési rendszerbe

- **COBIT:** *„PO9 - Kockázatok értékelése”*

ITAF – Kockázat elemzés



Risk IT – 3 fő területe

A Risk IT 3 fő területe:

1) Risk Governance

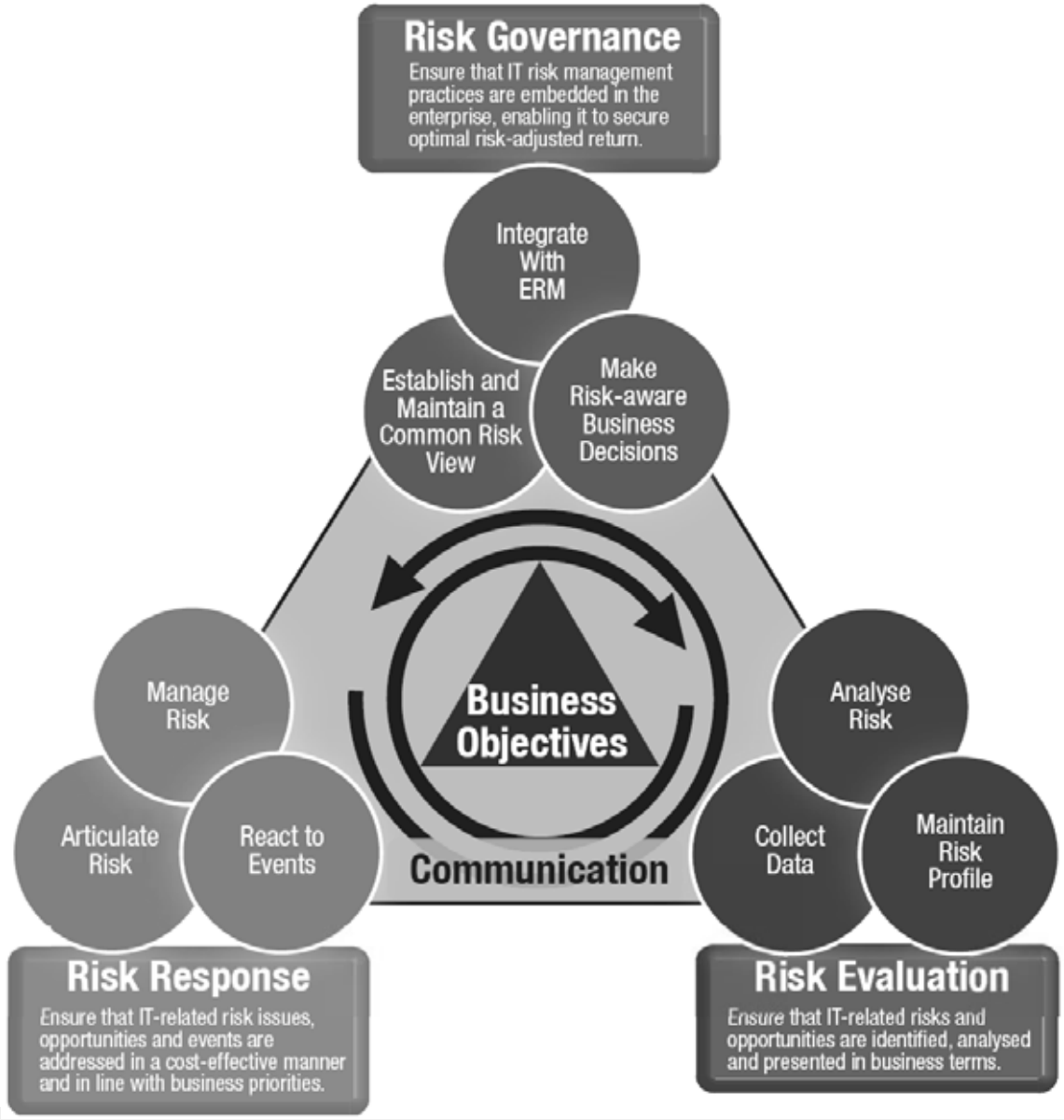
- **Responsibility and accountability for risk**
- **Risk appetite and tolerance**
- **Awareness and communication**
- **Risk culture**

2) Risk Evaluation

Risk scenarios
Business impact descriptions

3) Risk Response

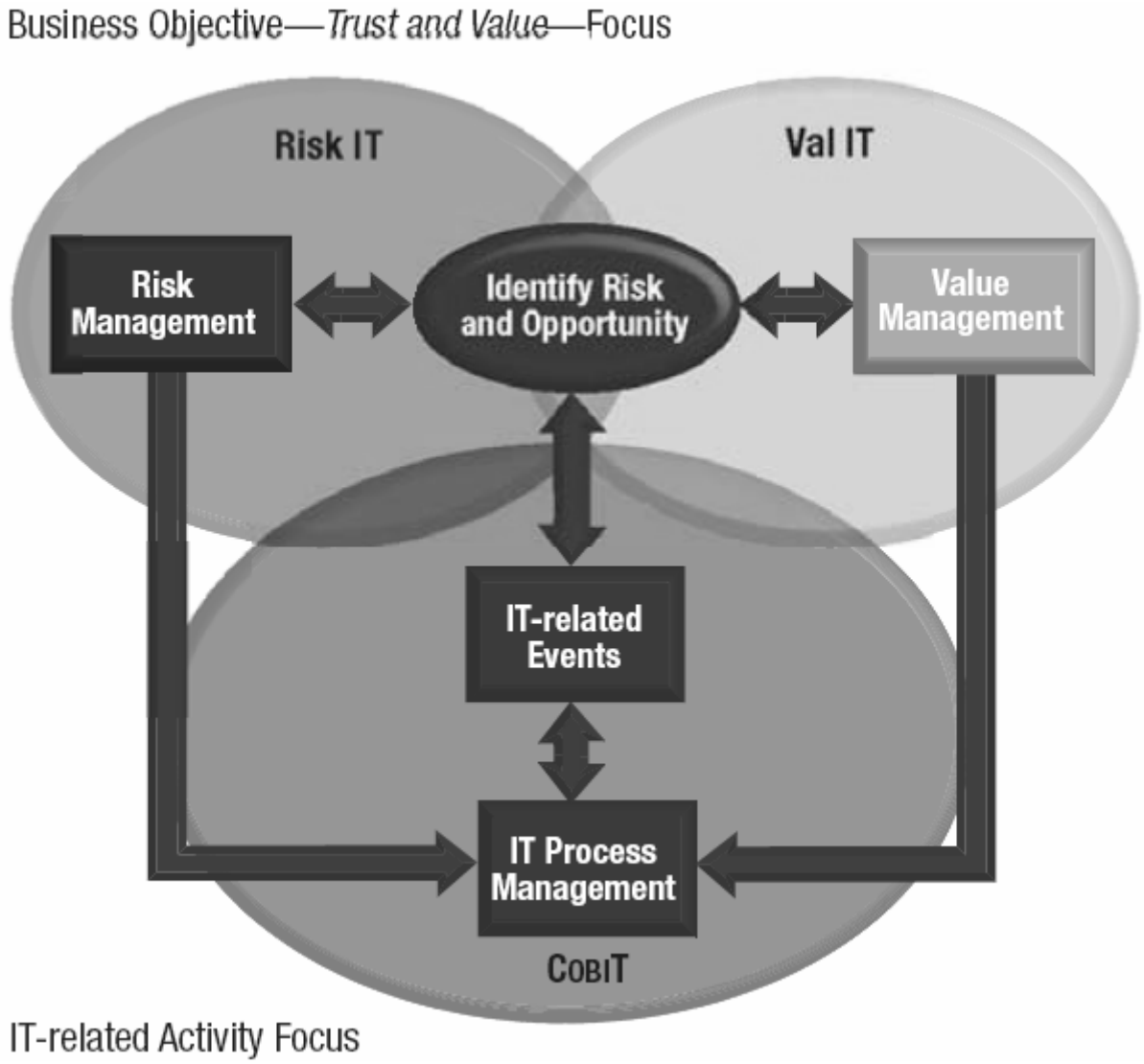
Key risk indicators (KRIs)
Risk response definition and prioritisation



Risk IT - kapcsolatok

A Risk IT kiegészíti és kibővíti a COBIT és Val IT dokumentumok at az IT irányítás teljes körű elméleti és gyakorlati megalapozása érdekében.

„Robert Stroud, CGEIT, ISACA Board of Directors”



Bázel2 - működési kockázatok

- **Működési kockázat** definíció: 76/J. § (1) A hitelintézet a – nem megfelelő belső folyamatok és rendszerek, külső események vagy a személyek nem megfelelő feladatellátása miatt felmerülő illetőleg jogszabály, szerződés vagy belső szabályzatban rögzített eljárás megsértése vagy nem teljesítése miatt keletkező, eredményét és szavatoló tőkéjét érintő – működési kockázat tőkekövetelményét
- A) az alapmutató módszerével (BIA),
- B) a sztenderdizált módszerrel (TSA, ASA),
- C) a fejlett mérési módszerrel (AMA) vagy
- D) az a)-c) pontokban rögzített módszerek kombinálásával számítja ki.
- Részletes szabályozás a 200/2007. Korm. Rendeletben (a működési kockázat kezeléséről és tőkekövetelményéről).

Bázel2 - Veszteség típusok

Bázel II kockázati eseménytípusok a kapcsolódó IT vonatkozással és CobiT folyamattal (lásd 200/2007. Korm.rend. 13§)		
Bázel II eseménytípusok	**IT vonatkozás**	**CobiT folyamatok**
Belső csalás	• Szándékos programmanipulálás • Módosító funkció jogosulatlan használata • Rendszerparancsok szándékos manipulálása • Hardver szándékos manipulálása • Rendszer- és alkalmazási adat szándékos megváltoztatása behatolás révén • Hozzáférési jogosultságok belső megkerülése • Liszensszel nem rendelkező vagy nem jóváhagyott szoftver másolása	• PO6 vezetői célok és irányvonal kommunikálása • DS5 rendszer biztonságának biztosítása • DS9 konfiguráció kezelése
Külső csalás	• Rendszer- és alkalmazási adat szándékos megváltoztatása behatolás révén • Külső fél birtokába kerülnek bizalmas dokumentumok • Hozzáférési jogosultságokat megkerülő külső fél • Kommunikációs vonalakkal kapcsolatos lehallgatás és aktív beavatkozás • Felfedett jelszó • Számítógépes vírusok	• DS5 rendszer biztonságának biztosítása
Munkáltatói gyakorlat és munkabiztonság	• IT eszközök nem rendeltetésszerű használata • A biztonsági tudatosság hiánya	• PO6 vezetői célok és irányvonal kommunikációja
Ügyfél, üzleti gyakorlat, marketing és termékpolitika	• Egy alkalmazott érzékeny információt szivárogtat ki külső fél számára • Külső beszállítók kezelése	• PO6 vezetői célok és irányvonal kommunikációja • DS2 külső szolgáltatások kezelése
Tárgyi eszköz károk	• A fizikai IT infrastruktúra szándékos vagy véletlen rongálása	• DS12 technikai környezet kezelése
Üzletmenet fennakadása és rendszerhiba	• Hardver vagy szoftverhiba, Kommunikációszakadás • Alkalmazott szabotázsa, IT kulcsmunkatárs elvesztése • Program- vagy adatfájlok megsemmisülése • Érzékeny adat vagy szoftver eltulajdonítása • Számítógépes vírusok • Mentés hiánya • (Elosztott) szolgáltatásmegtagadási támadás • Konfiguráció-kontroll hiba	• DS3 teljesítmény és kapacitás kezelése • DS4 folyamatos működés biztosítása • DS5 rendszer biztonságának biztosítása • DS9 konfiguráció kezelése • DS10 problémák kezelése
Végrehajtás, teljesítés és folyamatkezelés	• Elektronikus adathordozó hibás kezelése • Felügyelet nélkül hagyott munkaállomás • Hiba a változáskezelésben • Nem teljes körű tranzakció bevitel, Hibás adatbevitel/kivitel • Programozási/tesztelési hiba • Operátori hiba (pl. hiba a visszaállítási folyamatban)	• AI5 rendszerek kiépítése és jóváhagyása • AI6 változások kezelése • DS5 rendszer biztonságának biztosítása • DS10 problémák kezelése

Bázel2 - COBIT mapping

A CobiT alkalmazása a kockázatkezelésre (ISACA: IT control objectives for Basel2)		
Bázeli alapelv	**Érintett IT terület**	**Kapcsolódó CobiT folyamat**
1. Az Igazgatóságnak tudatában kell lenni, hogy szükség van egy működési kockázatkezelő keretrendszerre.	IT kockázatkezelés	PO9 Kockázatfelmérés és kezelés
2. A belső ellenőrzés hatásos és átfogó vizsgálatnak veti alá a kockázatkezelő keretrendszert.	IT belső ellenőrzés	ME4 IT ellenőrzés biztosítása
3.Dolgozzák ki a működési kockázat kezelésének szabályozását, folyamatait és eljárásait.	IT kockázatkezelés	PO9 Kockázatfelmérés és kezelés
4. A működési kockázat feltérképezése és értékelése.	IT kockázatkezelés	PO9 Kockázatfelmérés és kezelés
5. Rendszeresen figyelni kell a működési kockázati profil változását és a jelentős veszteségi kitettséget.	IT kockázatkezelés	PO9 Kockázatfelmérés és kezelés
6. Rendelkezzenek olyan szabályzatokkal, folyamatokkal és eljárásokkal, amelyek ellenőrzés alatt tartják és/vagy csökkentik a jelentős működési kockázatokat.	IT kockázatkezelés	PO9 Kockázatfelmérés és kezelés
7. Legyen az intézménynek rendkívüli helyzet kezelésére vonatkozó terve és üzletmenet folytonossági terve.	Folyamatos működés biztosítása	DS4 Folyamatos működés biztosítása
8. Legyen olyan működőképes keretrendszere az intézménynek, amely képes beazonosítani, felmérni, monitorozni és ellenőrzés alatt tartani / csökkenteni a jelentős működési kockázatokat.	IT kockázatkezelés	PO9 Kockázatfelmérés és kezelés
9. Végezzenek rendszeres független ellenőrzést az intézmény működési kockázatát érintő szabályzatait, eljárásait és gyakorlatát illetően.	IT belső ellenőrzés	ME2 Belső kontrollkörnyezet monitorozása és értékelése
10. Megfelelő szintű közzététel.	IT incidensek jelentése a vezetésnek	ME2 Belső kontrollkörnyezet monitorozása és értékelése

Bázel2 - Kézikönyvek

Basel II követelmények:

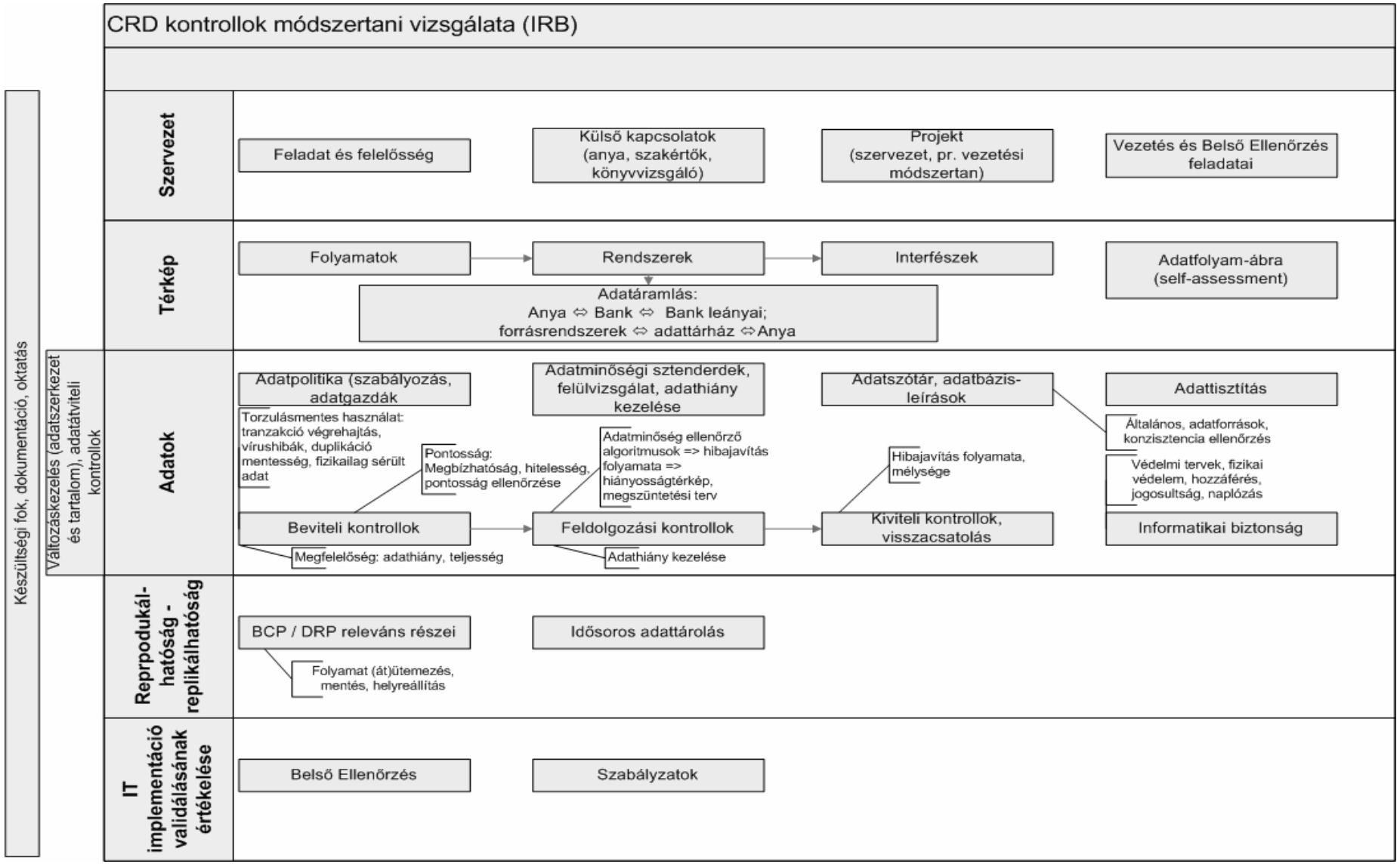
- GL10 point 350: „Egy jól működő **IT infrasturktúra elengedhetetlen** feltétele a megbízható tőkeszámításnak.”
- GL10 point 351: „Az intézményeknek olyan IT rendszerekkel kell rendelkeznie, amely biztosítja 1) a szükséges adatbázisok **folyamatos rendelkezésre állását és karbantartását**, 2) az adatbázisok és a tőkeszámítási eredmények reprodukálhatóságát.
- A 2006/48/EC direktíva (VII. Melléklet, 4. rész): „Egy „minősítési rendszernek” fel kell ölelnie az összes módszert, folyamatot, ellenőrzést, adatgyűjtő és **informatikai rendszert**, amelyek a hitelkockázat minősítését, a kitettségek minősítési kategóriákba vagy poolokba sorolását, valamint az egyes kitettség típusokhoz tartozó nemteljesítési és veszteségi becslések mennyiségi meghatározását támogatják.”
- GL10 point 21: „A kézikönyv **nem tartalmazza az információs technológiára vonatkozó részletes követelményeket** mert ezen feltételek jóval túlmutatnak a tőkeszámítás keretein. Elvárható, hogy ezt a felügyelők a szélesebb értelemben vett, általános kontroll struktúra részének tekintsék.”

Bázel2 - vizsgálati program

Basel2 vizsgálati program:

- Szervezet
  - Feladat és felelősségelhatárolás
  - Külső kapcsolatok
  - Projekt (szervezet, projekt módszertan)
  - A Vezetés és Belső ellenőrzés feladatai
- Térkép
  - Folyamatok
  - Rendszerek (adatáramlás, forrás rendszerek és adattárház kapcsolat, anya-leány kapcsolat)
  - Interfészek
  - Adatfolyam ábra (önértékelés)
- Adatok
  - Adatpolitika (adatgazdák, szabályozás
  - Adatminőség (sztenderdek, felülvizsgálat, adathiány kezelése, algoritmusok)
  - Adatszótár (adatbázis leírások, adatforrások, konzisztencia ellenőrzés)
  - Adattisztítás
  - Változáskezelés
  - Kontrollok (beviteli-, feldolgozási-, kiviteli kontrollok)
  - Informatikai biztonság (védelmi tervek, fizikai védelem, hozzáférésmenedzselés, naplók)
- Reprodukálhatóság (BCP, DRP, Idősoros adattárolás)
- IT validálás (készültségi fok, szabályzatok, dokumentációk, oktatás, belső ellenőrzés)

Bázel2 - vizsgálati területek



2. Jogosultságkezelés

Hozzáférés- és jogosultságkezelés:

- **Jogszabály: Mpt. 77/A. § (5) c), Öpt. 40/C. § (5) c), Bszt. 12. § (5) c), Hpt. 13/C. § (5) c)** A biztonsági kockázatelemzés eredményének értékelése alapján a **biztonsági kockázattal arányos** módon gondoskodni kell **legalább** a rendszer **szabályozott**, **ellenőrizhető** és **rendszeresen ellenőrzött felhasználói adminisztrációjáról** (hozzáférési szintek, egyedi jogosultságok, engedélyezésük, felelősségi körök, hozzáférés naplózás, rendkívüli események)

- **Jellemző problémák:**
  - Nem megfelelő igénylési folyamat,
  - Papír alapú és hiányos igénylések,
  - Nincs nyilvántartás,
  - Nincs szoftveres támogatás,
  - Nem egyező nyilvántartás, nincs rendszeres ellenőrzés.

- **COBIT:** *„DS5 – A rendszer biztonságának biztosítása”, a „DS7 – Felhasználók képzése” és a „DS8 – Informatikai felhasználók segítése”*

Jogosultsági kontrollok

Jogosultságok szabályozása: 91%-nál
Távoli hozzáférések szabályozása: 85%-nál
Külsős szolgáltatókra vonatkozó szabályok: 84%-nál
Adatgazdák dokumentált kinevezése: 73%-nál
Nyilvántartott rendszerek: 87%-nál
Nyilvántartás teljeskörűsége: 75%-nál
Külsősök a nyilvántartásban: 67%-nál
Külsősök távoli hozzáféréssel: 53%-nál
A külsős hozzáférések területe: üzemeltetés, karbantartás, hibaelhárítás, fejlesztés és támogatás.
Utolsó felülvizsgálat 2009-ben: 2006, 2007, 2008 is!
Központi jogkezelés: 78%-nál
Korszerű szoftveres támogatás: kb. 20%-nál

3. Naplózási feladatok

Naplózás, log-ellenőrzés:

- **Jogszabály (Hpt. 13/C. § (5) d), Bszt. 12. § (6) d), Mpt. 77/A. § (5) d), Öpt. 40/C. § (5) d)): . § (5) d)** A **biztonsági kockázatelemzés** eredményének értékelése alapján a biztonsági **kockázattal arányos módon** gondoskodni kell legalább olyan **biztonsági környezetről**, amely az informatikai rendszer működése szempontjából **kritikus folyamatok** eseményeit **naplózza** és alkalmas e naplózás **rendszeres** (esetleg önműködő) és **érdemi értékelésére**, illetve lehetőséget nyújt a nem rendszeres események kezelésére,
- **Jellemző problémák:**
  - IT biztonsági kockázatmenedzselési hiányosságok,
  - Koncepciótlanság, szabályozatlanság,
  - Felelősök kijelölésének hiánya,
  - Naplófájlok hiánya,
  - Beépített audit lehetőségek hiánya, kihasználatlansága,
  - Automatikus eszközök hiánya,
  - Naplózási feladatok ellenőrizetlensége
- **COBIT:** *„AI2 – Alkalmazási szoftverek beszerzése és karbantartása”, „AI3 – Technológiai infrastruktúra beszerzése és karbantartása”, „AI4 – Informatikai eljárások kifejlesztése és karbantartása”„DS13 – Üzemeltetés irányítása”*

Naplózás - 2

Elvárások:

- Koncepció és szabályozás szerint (milyen folyamattal).
- Gondoskodni kell a kritikus rendszerek (mit) eseményeinek gyűjtéséről.
- Események dátuma, ideje, tartalma, rekonstruálhatósági adatok (mit).
- A naplóállományok rendelkezésre állása, törölhetetlensége (hol).
- A gyűjtött állományok rendszeres mentése és ellenőrzése (meddig).
- Naplóállományok hozzáférésének menedzselése (ki).
- Automatikus eszközök az értékeléshez (hogyan).
- Riportok, riasztások (miért).

Típusok:

- Alkalmazási célú (csalások, belső kontroll megszegése, ellenőrizhetőség)
- Üzemeltetési célú (rendelkezésre állás, meghibásodás, performancia, kihasználtság)
- IT biztonsági célú (sikeres/sikertelen ki/bejelentkezés, felhasználók adminisztrálása, biztonsági paraméterek állítása, logolási paraméterek állítása, kritikus fájlok létrehozása/törlése/módosítása, stb.)

Naplózás - 3

Milyen területeken:

- Operációs rendszer szinten: sikeres/sikertelen be/kilépés, kritikus rendszerfájlok létrehozása/módosítása/törlése, jogosultsági rendszer változások, op.rendszer naplózási paraméterek változtatása, konfigurációs fájlok létrehozása/módosítása/törlése, hozzáférést biztosító alkalmazások működése, stb.
- Adatbázis szinten: közvetlen adatbázis hozzáférések, sikeres/sikertelen ki/belépések, adatbázis/adatszerkezet változtatások, program/trigger/tárolt eljárás változtatások, adatbázis jogosultságok változása, adatbázis naplózásának változása,
- Alkalmazás szinten: sikeres/sikertelen be/kilépés, sikeres/sikertelen alkalmazás indítás, jogosultsági rendszer változások, jogcsoportok/felhasználók létrehozása/törlése/módosítása, alkalmazás napló leállítása/indítása, naplózandó üzleti események (tranzakciók bevitele/törlése/módosítása),
- Eszköz szinten (routerek, tűzfalak, IDS, Web szerver, stb.): konfigurációs rendszer sikeres/sikertelen be/kilépés, konfiguráció változások/módosítások, eszköz paraméter változások, stb.)

Feladatok és felelősségek:

- Szabályozás – IT biztonsági menedzser
- Üzemeltetés – rendszergazda
- Napló gyűjtés, tárolás, mentés – rendszergazda
- Napló elemzés értékelés – IT biztonsági menedzser

4. Változáskezelés

Változáskezelés, fejlesztések:

- **Jogszabály: Mpt. 77/A. § (6) d), Öpt. 40/C. § (6) d), Bszt. 12. § (6) d), Hpt. 13/C. § (6) d)** … **meg kell valósítania** … az **alkalmazási környezet biztonságos elkülönítését** a fejlesztési és tesztelési környezettől, valamint a **megfelelő változáskövetés és változáskezelés fenntartását**. **Hpt. 13/C. § (8)** A **szoftvereknek együttesen alkalmasnak** kell lenni legalább: *a)* a működéshez szükséges és jogszabályban előírt adatok **nyilvántartására**, *b)* a tárolt adatok **ellenőrzéséhez való felhasználására**, *c)* a biztonsági kockázattal arányos **logikai védelemre és a sérthetetlenség védelmére**.
- **Jellemző problémák:**
  - Nincs változásmenedzser,
  - A változások kezelése nem dokumentált, nem ellenőrzött és nem ellenőrizhető,

- **COBIT:** *„AI6 – Változások kezelése”, „AI5 – Rendszerek üzembe helyezése és jóváhagyása”, PO11 – Minőségirányítás”, „DS1 – Szolgáltatási szintek meghatározása”, „AI2 – Alkalmazói szoftverek beszerzése és karbantartása”, „DS5 – A rendszer biztonságának megvalósítása”,„DS11 – Adatok kezelése”*

Változáskezelési kontrollok

- Van-e szabályozás? 67%-nál igen
- Van-e változásmenedzser? 54%-nál igen
- Volt-e független ellenőrzés a változáskezelési folyamat működésére az elmúlt két évben? 49%-nál igen
- A változáskezelési folyamat érvényes-e a külsősökre? 59%-nál igen

(lásd „A pénzintézeti kiszervezési tevékenység IT biztonsági kérdései” c. tanulmányt)

5. Üzletmenet-folytonosság

Üzletmenet-folytonosság, rendkívüli helyzet kezelés:

- **Jogszabály: Mpt. 77/A. § (6), Öpt. 40/C. § (6), Bszt. 12. § (6), Hpt. 13/C. § (6)** … **meg kell valósítania** a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket és rendelkeznie kell legalább: ***b)*** **minden olyan dokumentációval**, amely … működését - még a szállító tevékenységének megszűnése után is - biztosítja, ***c)*** … informatikai rendszerrel, … **tartalék berendezésekkel**, … szolgáltatások folytonosságát biztosító - megoldásokkal, ***e)*** … biztonsági **mentésekkel és mentési renddel** … és tűzbiztos módon kell tárolni, valamint gondoskodni kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről, ***f)*** … **alkalmas adattároló rendszerrel**, amely biztosítja, hogy az archivált anyagokat … legalább öt évig megőrizzék, ***g)*** a … **rendkívüli események kezelésére** szolgáló tervvel.
- **Jellemző problémák:**
  - Hiányzó BCP és DRP,
  - A tervek elkészítését az IT-re bízzák illetve azok nem aktualizáltak,
  - A tesztelés nem történik meg illetve nem teljes körű.
- **COBIT:** *„DS2 – Külső szolgáltatások kezelése”, „DS3 – Teljesítmény és kapacitás kezelése”, „PO11 – Minőségirányítás”, „DS1 – Szolgáltatási szintek meghatározása”, „DS4 – Folyamatos működés biztosítása” „DS10 – Rendkívüli események kezelése”*

6. Szabályozási feladatok

Szabályozás:

- **Jogszabály: Mpt. 77/A. § (1) bekezdés, Öpt. 40/C. § (1) bekezdés, Bszt. 12. § (1) bekezdés, Hpt. 13/C. § (1)** A pénzügyi szervezetnek **ki kell alakítania** a tevékenységének ellátásához használt informatikai rendszer biztonságával kapcsolatos **szabályozási rendszerét** és gondoskodnia kell az informatikai rendszer **kockázatokkal arányos védelméről**, amely kiterjed a bűncselekményekkel kapcsolatos kockázatok kezelésére is. A szabályozási rendszerben ki kell térni **az információtechnológiával szemben támasztott követelményekre**, a használatából adódó biztonsági **kockázatok felmérésére és kezelésére** a tervezés, a beszerzés, az üzemeltetés és az ellenőrzés területén.

- **Jellemző problémák:**
  - Szabályzatok hiányoznak
  - A szabályzatok nem aktualizáltak.
  - Nincs szabályozási rend és struktúra (irányelvek – szabályzatok – eljárásrendek).
  - A szabályzatok nem egyeznek a gyakorlattal

- **COBIT:** *„PO6 - Vezetői célok és irányvonal közlése”* , a *„PO8 - Külső követelmények betartása”* és az *„AI1 – Automatizált megoldások meghatározása”*

Jogszabályi változások - 1

- Hpt. módosítások:
  - az európai tőke megfelelési szabályok átültetése
  - a korábbi jogharmonizációs célú módosítások
  - a kockázatok csökkentését célzó, átláthatóbb és kiegyensúlyozottabb szabályozási környezet kialakítása
- „13/D. § **Vállalatirányítási rendszer**” → 13/D. § (1) A hitelintézetnek mérete, az általa végzett tevékenysége jellege, nagyságrendje és összetettsége arányában megbízható vállalatirányítási rendszerrel kell rendelkeznie (szervezet, felelősségelhatárolás, kockázatmenedzselés, szabályozás, stb.)
- Kötelező **írásban rögzített szabályzatok** → 13/D. § (3) e): „a működési kockázatok mérésére, kezelésére valamint vészhelyzeti és üzletmenet-folytonossági tervvel a folyamatos működés fenntartása továbbá a súlyos üzletviteli fennakadásokból következő esetleges veszteségek mérséklése érdekében,”

Jogszabályi változások - 2

- **Hitelezési kockázat** előírása a 76/A. § (1)-ban, amely „a hitelintézetek mindenkori fizetőképességének fenntartása érdekében az általa végzett tevékenység kockázatának fedezetét mindenkor biztosító megfelelő szavatoló tőkével kell rendelkezni, amely …
- Részletes szabályozás a 196/2007. Korm. Rendeletben („a rendelet célja, hogy a hitelintézet számára meghatározza *a)* a hitelezési kockázat tőkekövetelményének **sztenderd (STA) módszerrel (Hpt. 76/A. §),** illetőleg **belső minősítésen alapuló (FIRB, AIRB) módszerrel (Hpt. 76/B-76/D. §)** történő kiszámításának,
- A 76/B. § (1) belső minősítésen alapuló módszer feltételei között:
  - „a kockázatkezelés és **minősítési rendszerei megbízhatóak és átfogóak**”
  - „**független** hitelkockázat-ellenőrzési egységgel rendelkezzen”
  - „**évente legalább egyszer** jóváhagyja és dokumentálja minősítési rendszereit”
  - „bevezetése előtt **legalább három éven át**” megfelelő minősítési rendszert működtet
- A 76/K § (1) a tőkemegfelelési rendszer értékelési folyamat feltételei között:
  - „A hitelintézetnek **megbízható, hatékony és átfogó stratégiával** és eljárással kell rendelkeznie”
  - „**legalább évente** felül kell vizsgálnia stratégiáját”

7. IT stratégia

IT stratégia, fejlesztési tervek:

- **Jogszabály: Mpt. 77/A. § (6) a), Öpt. 40/C. § (6) a), Bszt. 12. § (6) a), Hpt. 13/C. § (6) a)** A pénzügyi szervezet tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez meg kell valósítania a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket és rendelkeznie kell legalább az informatikai rendszerének működtetésére vonatkozó **utasításokkal és előírásokkal**, valamint **a fejlesztésre vonatkozó tervekkel**,
- **Jellemző problémák:**
  - Nincs IT stratégia,
  - Nincs összhangban az üzleti stratégiával.
  - Az IT stratégia nem került aktualizálásra,
- **COBIT:** *COBIT „PO1 – Informatikai stratégiai terv kidolgozása”, a „PO2 – Információ-architektúra meghatározása”, a „PO3 – Technológiai irány meghatározása”, a „PO5 – Informatikai beruházások kezelése”, a „PO10 – Projektek irányítása”, a „DS6 – Költségek megállapítása és felosztása” valamint a „DS13 – Üzemeltetés irányítása”*

A COBIT felépítése - 2

1. Stratégiai tervezés (Strategic Alignment)
aligning with the business and providing collaborative solutions

2. Érték teremtés (Value Delivery)
focus on IT costs and proof of value

3. Erőforrások kezelése (Resource Management)
IT assets, knowledge, infrastructure and partners

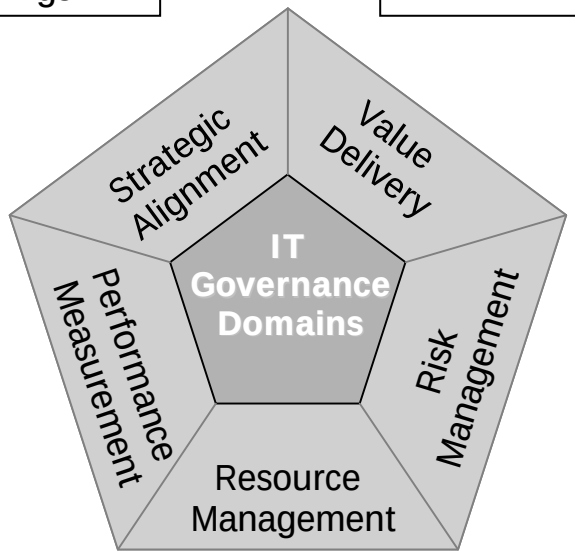
4. Kockázatkezelés (Risk Management)
safeguarding assets, business continuity and compliance

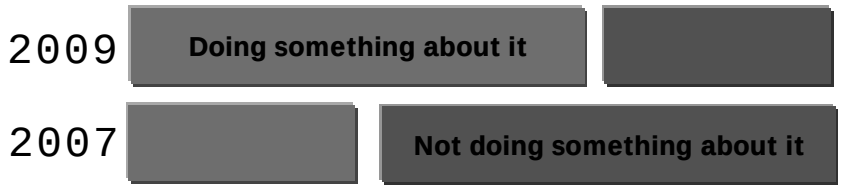
5. Teljesítmény mérés (Performance Measurement)
metrics, IT Scorecards and dashboards

COBIT® 4.1 Val IT

Are we doing the right things?

Are we getting the benefits?





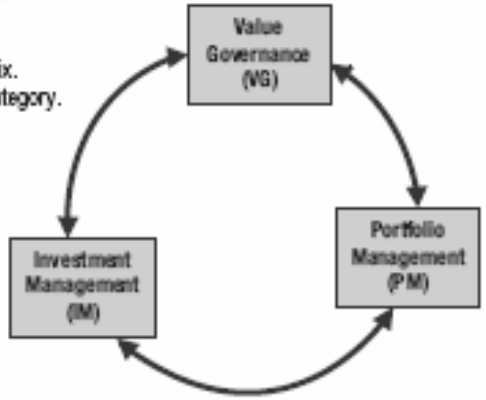
Are we doing them the right way?

Are we getting them done well?

A Val_IT felépítése

Figure 8—Key Management Practices Supporting the Three Val IT Processes

VG1 Ensure informed and committed leadership.
VG2 Define and implement processes.
VG3 Define roles and responsibilities.
VG4 Ensure appropriate and accepted accountability.
VG5 Define information requirements.
VG6 Establish reporting requirements.
VG7 Establish organisational structures.
VG8 Establish strategic direction.
VG9 Define investment categories.
VG10 Determine a target portfolio mix.
VG11 Define evaluation criteria by category.

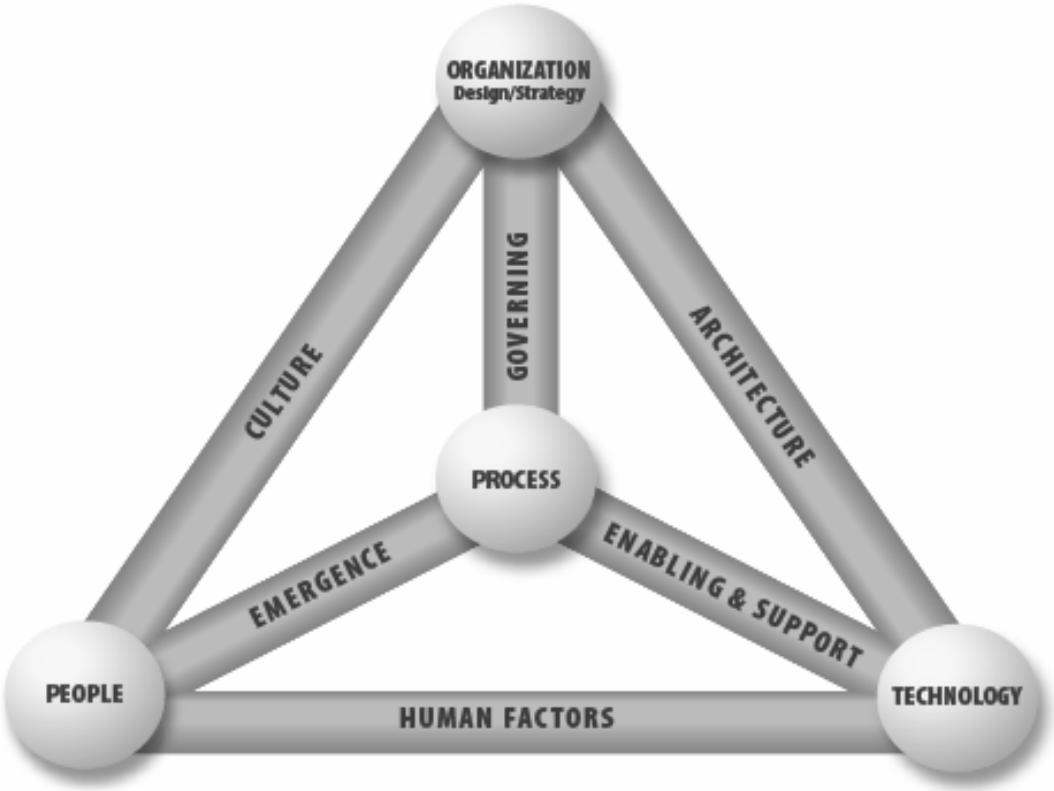


PM1 Maintain a human resource inventory.
PM2 Identify resource requirements.
PM3 Perform a gap analysis.
PM4 Develop a resourcing plan.
PM5 Monitor resource requirements and utilisation.
PM6 Establish an investment threshold.
PM7 Evaluate the initial programme concept business case.
PM8 Evaluate and assign a relative score to the programme business case.
PM9 Create an overall portfolio view.
PM10 Make and communicate the investment decision.
PM11 Stage-gate (and fund) selected programmes.
PM12 Optimise portfolio performance.
PM13 Re-prioritise the portfolio.
PM14 Monitor and report on portfolio performance.

IM1 Develop a high-level definition of investment opportunity.
IM2 Develop an initial programme concept business case.
IM3 Develop a clear understanding of candidate programmes.
IM4 Perform alternatives analysis.
IM5 Develop a programme plan.
IM6 Develop a benefits realisation plan.
IM7 Identify full life cycle costs and benefits.
IM8 Develop a detailed programme business case.
IM9 Assign clear accountability and ownership.
IM10 Initiate, plan and launch the programme.
IM11 Manage the programme.
IM12 Manage/track benefits.
IM13 Update the business case.
IM14 Monitor and report on programme performance.
IM15 Retire the programme.

BMIS – Business Model for IT Security

Figure 1—The Business Model for Information Security



Source: Adapted from the USC Marshall School of Business Institute for Critical Information Infrastructure Protection

8. Nyilvántartások

Nyilvántartások:

- **Jogszabály: Mpt. 77/A. § (5) a), Öpt. 40/C. § (5) a), Bszt. 12. § (5) a), Hpt. 13/C. § (5) a)** A biztonsági kockázattal arányos módon **gondoskodni kell legalább** a rendszer legfontosabb elemeinek (eszközök, folyamatok, személyek) **egyértelmű és visszakereshető azonosításáról**, **(7)** A pü-i szervezetnél **mindenkor rendelkezésre kell állnia**: ***a)*** az általa fejlesztett, megrendelésére készített informatikai rendszer felépítésének és működtetésének az ellenőrzéséhez **szükséges rendszerleírásoknak és modelleknek**, ***b)*** az **adatok szintaktikai szabályainak, az adatok tárolási szerkezetének**, ***c)*** az informatikai rendszer elemeinek **biztonsági osztályokba sorolási rendszerének**, ***d)*** az adatokhoz történő **hozzáférési rend meghatározásának**, *e)* az adatgazda és a **rendszergazda kijelölését** tartalmazó okiratnak, ***f)*** az alkalmazott szoftver eszközök **jogtisztaságát** bizonyító szerződéseknek, ***g)*** az informatikai rendszert alkotó ügyviteli, üzleti **szoftvereszközök teljes körű és naprakész nyilvántartásának**.

- **Jellemző problémák:**
  - Az IT architektúra nem jól dokumentált,
  - Nyilvántartási hiányosságok.

- **COBIT:** *„DS9 – Konfiguráció kezelése”*

9. Feladat- és felelősség elhatárolás

Feladat és felelősség elhatárolás:

- **Jogszabály: Mpt. 77/A. § (3), Öpt. 40/C. § (3), Bszt. 12. § (3), Hpt. 13/C. § (3)** Az informatika alkalmazásából fakadó biztonsági kockázatok figyelembevételével meg kell határozni a **szervezeti és működési rendeket**, a **felelősségi, nyilvántartási és tájékoztatási szabályokat**, a **folyamatba épített ellenőrzési** követelményeket és szabályokat.

- **Jellemző problémák:**
  - Nem megfelelő feladat és felelősség elhatárolás
  - A szükséges feladatoknak nincs felelőse
  - Összeférhetetlen feladatok egy kézben

- **COBIT:** *„PO4 – Az informatikai részleg szervezeti felépítésének és kapcsolatainak meghatározása”, „PO7 – Emberi erőforrások kezelése”*

Összeférhetetlenségi mátrix

Összeférhetetlen feladatok és felelősségek (CobiT szerint)										
	Felhasználó	IT ellenőr	Fejlesztő	Szoftver könyvtáros	Felh. támogató	Rendszer admin.	Hálózati admin	Adatbázis admin.	Operátor	IT biztonsági felelős
Felhasználó			X	X	X		X	X	X	
IT ellenőr			X	X	X	X	X	X	X	
Fejlesztő	X	X		X	X	X	X	X	X	X
Szoftver könyvtáros	X	X	X		X	X	X			X
Felh. támogató	X	X	X	X		X	X	X		X
Rendszer admin.		X	X	X	X			X	X	
Hálózati admin	X	X	X	X	X			X	X	
Adatbázis admin.	X	X	X		X	X	X			
Operátor	X	X	X			X	X	X		X
IT biztonsági felelős			X	X	X				X	

Az **X** jelöli az összeférhetetlen feladatokat és felelősségeket

Zöld szín: összefoglalva üzemeltetés

10. IT ellenőrzések

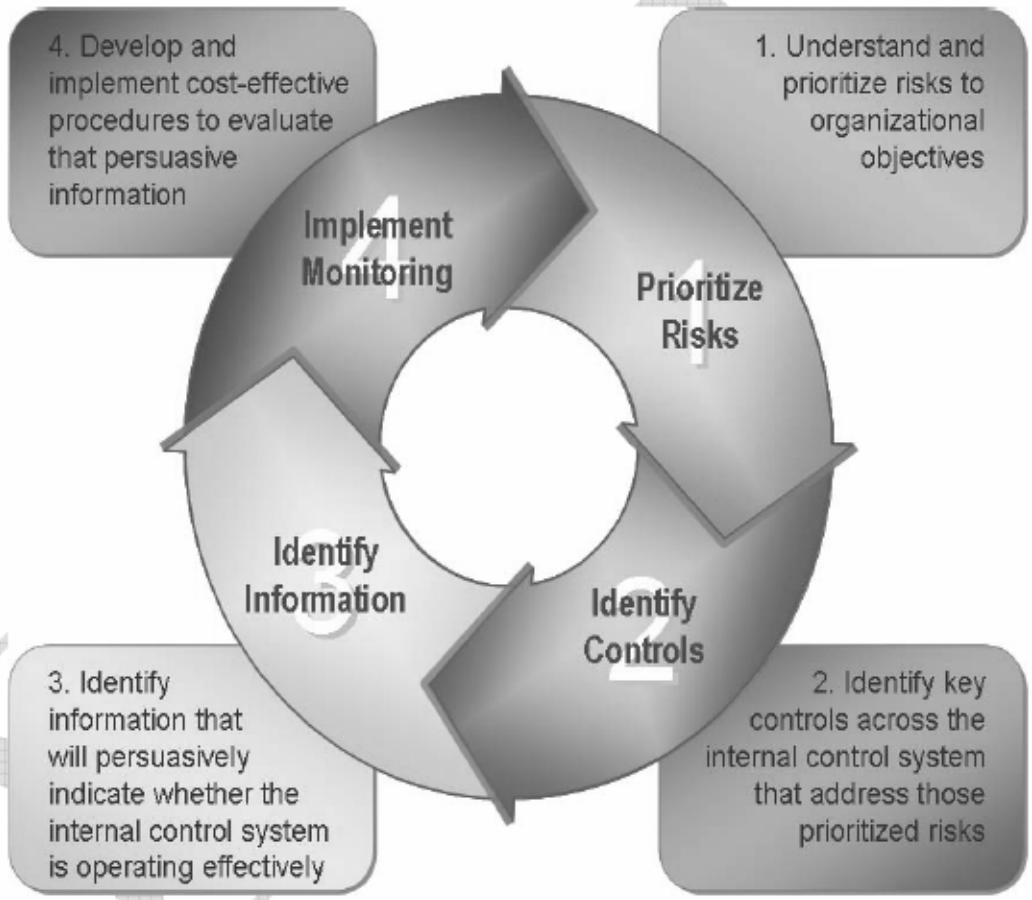
IT irányítás, független ellenőrzés:

- **Jogszabály: Mpt. 77/A. § (4), Öpt. 40/C. § (4), Bszt. 12. § (4), Hpt. 13/C. § (4)** A pénzügyi szervezetnek ki kell dolgoznia az informatikai rendszerének biztonságos működtetését felügyelő **informatikai ellenőrző rendszert és azt folyamatosan működtetnie** kell.

- **Jellemző problémák:**
  - Nem kellő mennyiségű és mélységű IT vizsgálat,
  - Sok kontroll hiányosság,
  - Nem megfelelő kontrollkörnyezet,
  - Nem rendszeres ellenőrzés,
  - Nem a legnagyobb kockázatokra,
  - Nem megfelelő képzettség.
-
- **COBIT:** *„M1 – Eljárások felügyelete”, az „M2 – Belső ellenőrzés megfelelőségének felmérése”, az „M3 – Független értékelés végeztetése” és az „M4 – Független audit elvégeztetése”*

Kontrollok ellenőrzése

Figure 5—Four-step Process to Design an Effective Monitoring Process



Lásd : „Monitoring of internal controls and IT” http://www.isaca.org/itmonitoring

11. IT biztonság

IT biztonság, biztonságtudatosság:

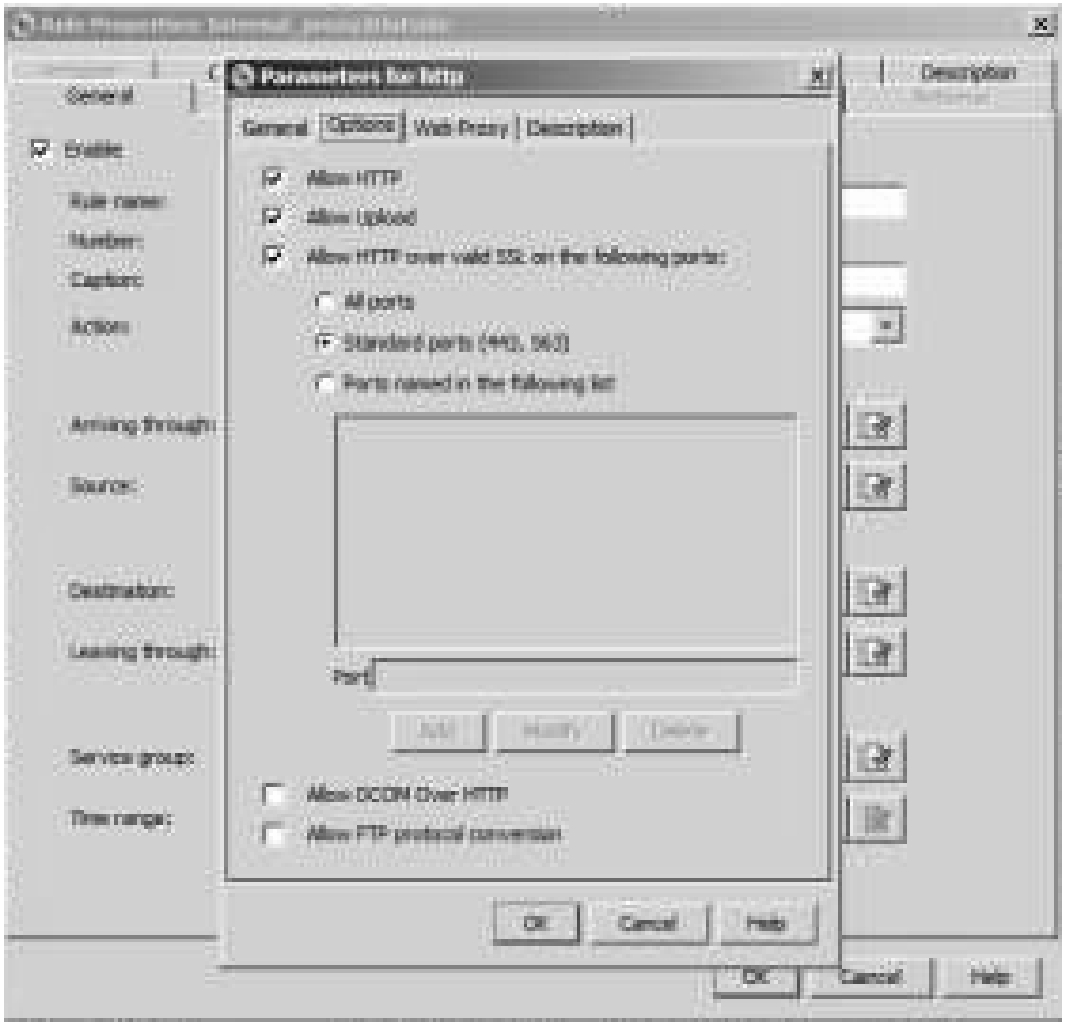
- **Jogszabály: Mpt. 77/A. § (5) b), Öpt. 40/C. § (5) b), Bszt. 12. § (5) b), Hpt. 13/C. § (5) b)** A biztonsági kockázatelemzés eredményének értékelése alapján a **biztonsági kockázattal arányos** módon gondoskodni kell legalább az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljes körűségét biztosító **ellenőrzésekről, eljárásokról**.

- **Jellemző problémák:**
  - A biztonság tudatosság alacsony színvonalú,
  - A beépített IT biztonsági elemek kihasználatlanok,
  - Az IT biztonsági szempontok csak utólag kerülnek beépítésre,
  - Kevés IT biztonsági felülvizsgálat.

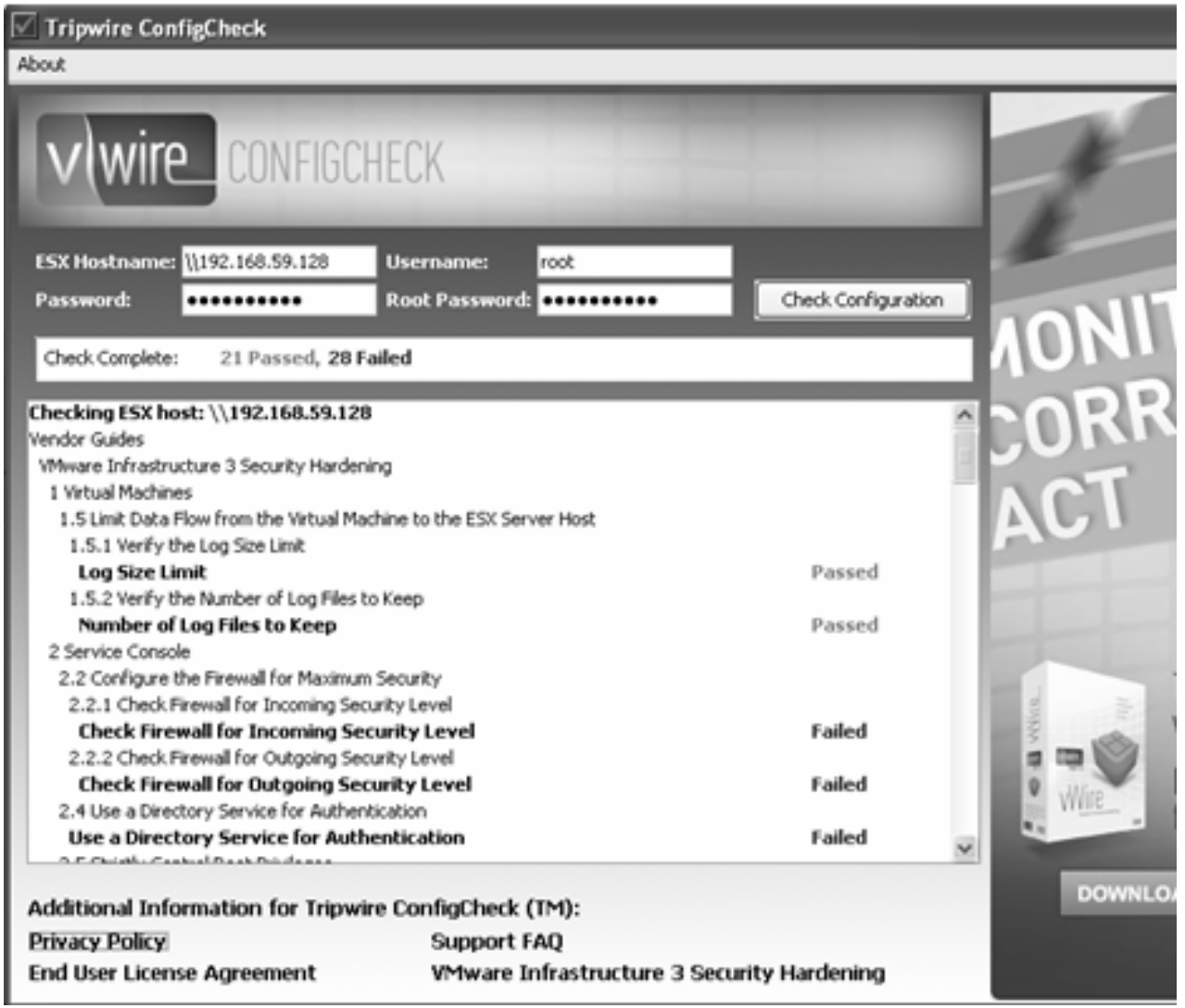
- **COBIT:** *„DS5 – A rendszer biztonságának megvalósítása”, „DS12 – Létesítmények kezelése”*

- 2009. évi tanulmány az internet-bankolásról: http://www.pszaf.hu/data/cms2102150/Puskas_Tivadar_Kozalapitvany_Internet_Biztonsagi_Tanulmany.pdf

SGS tűzfal alap beállítás



VMWare beállítások



A „cloud computing” veszélyei

Marne E. Gordan, IBM, előadása az EuroCACS-en:

1. Adatvédelem (titkosítás, hálózati topológia, stb.)
2. Hozzáférés és jogosultságkezelés (sok felhasználó, nagyobb kitettség)
3. Üzembe helyezés és változtatás (egyszerűbb hibázás, véletlen patch-elés, licensz túllépés egy egér billentyűre)
4. Tesztelés (alaposabban a sebezhetőség miatt)
5. SLA (pontosabb szerződés, 50-50% felelősség, biztonság!)
6. Sérülékenység menedzselés (még fontosabb, tűzfal beállítások, incidens jelentések)
7. BCM (továbbra is fontos, tudni kell, hogy milyen gyorsan lehet átállni, a szolgáltató BCM-je is fontos)
8. Audit és kontrollok (új audit feladatok, kontrollok működtetése)
9. Határon átnyúló szolgáltatás (jogi-, teljesítmény, biztonsági megfontolások)
10. Tulajdonjogi és export megfontolások (helyszín, veszteségek)

Lásd még a http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/?searchterm=cloud%20computing%20benefits linken.

12. Adatvédelem

Adattitkosítás, adatátvitel biztonsága:

- **Probléma:** Külsős hozzáférések problémái, adatbiztonsági hiányosságok, adat- és titokvédelmi szabályzatok, nyilatkozatok hiánya.
- **Jogszabály: Mpt. 77/A. § (5) e), Öpt. 40/C. § (5) e), Bszt. 12. § (5) e), Hpt. 13/C. § (5) e)** A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon **gondoskodni kell legalább** a távadat-átvitel, valamint a kizárólag elektronikus úton megvalósuló pénzügyi tranzakciók **bizalmasságáról, sértetlenségéről és hitelességéről**,
- **COBIT:** *„DS5 – Rendszerek biztonsága" és a „DS11 – Adatok kezelése"*

Adathordozók kezelése:

- **Probléma:** Adathordozók megbízható, naprakész nyilvántartásának hiánya.
- **Jogszabály: Hpt. 13/C. § (5) f)** A biztonsági kockázatelemzés eredménye alapján a biztonsági kockázattal arányos módon **gondoskodni kell legalább** az adathordozók szabályozott és biztonságos kezeléséről,
- **COBIT:** *„DS11 – Adatok kezelése"*

Vírusvédelem:

- **Probléma:** Nem kockázatarányos, nem aktualizált vírusvédelem.
- **Jogszabály: Hpt. 13/C. § (5) g)** A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon **gondoskodni kell legalább** a rendszer biztonsági kockázattal arányos vírusvédelméről.
- **COBIT:** *„DS5 – Rendszerek biztonsága" és a „DS9 – Konfiguráció kezelése"*

13. Oktatás

IT oktatás, IT szakképzettség:

- **Jogszabály: Hpt. 13/C. § (9)** A pénzügyi szervezet belső szabályzatában meg kell határozni az egyes munkakörök betöltéséhez **szükséges informatikai ismeretet.**

- **Jellemző problémák:**
  - Még mindig nagy a szakadék az üzlet és az IT között (specifikációs hibák, kihasználatlan eszközök, nem megfelelő feladat- és felelősség elhatárolás, stb.)
  - Kevés a belső szakértelem, erős kiszolgáltatottság a külső szállítóknak,
  - A biztonság tudatosság alacsony színvonalú,

- **COBIT:** *„PO7 – Emberi erőforrások kezelése”*

Összefoglalás, tanulságok

- A legjobb válságmenedzselés a megelőzés (prevenció)!
- Ne bagatelizáljuk el a problémákat, folyamatos feladat a kontrollok fenntartása, készüljünk fel a válságra!
- **Kockázatelemzés**, a veszélyforrások felmérése, a működési kockázatok rendszeres kiértékelése és a kontrollok kialakítása (Risk management).
- Minden válságot egyedileg kell kezelni!
- Alapelvek: - Csak semmi pánik, - Nyerjünk időt, - Legyen stratégiánk.
- Alakítsunk ki jól működő IT irányítást, készüljön üzleti és **IT stratégia (tudatos vezetés, IT governance)**
- **Feleljünk meg** a hazai és a nemzetközi jogszabályoknak és szabványoknak valamint a gyakorlatot az előírások szerint alakítsuk ki (Compliance)!
- Az IT kontrollok működtetése (IT szabályozási rendszer működtetése, Nyilvántartások vezetése, **Kockázatmenedzselés**, **Jogosultságkezelés**, Fejlesztés- és **változásmenedzselés**, **Üzletment-folytonosság** menedzselése, **Naplózási feladatok**, IT biztonság menedzselése, stb.)
- A **biztonság tudatosság erősítése**, a biztonsági szempontok érvényesítése a fejlesztésekben, rendszeres oktatások és képzések.
- Belső **IT szakértelem** és külsősök feletti kontroll erősítése.
- A független **ellenőrzés** fokozása, hatékony IT auditok.

Köszönöm a figyelmet!