

# **Biztonsági kihívások napjainkban – kontrollok szerepe az információ biztonságban**

Székesfehérvár, 2011. február 15.

Kirner Attila  
ISACA-HU Elnök  
[kirner.attila@gmail.com](mailto:kirner.attila@gmail.com)

# Kiemelt témák

- Információ- és adatvédelem, IT biztonság
- Új technológiák bevezetése, IT irányítás
- IT kockázatok kezelése
- Compliance – jogszabályi megfelelés

# IT biztonsági trendek

Slágertémák (<http://www.virusbuster.hu/ceginfo/...>):

1. Halászat – az adatok tengerén (megnövekedett phishing)
2. Vadászat – a szellemi tulajdonokra és honlapokra (feltört oldalak)
3. Mobil veszedelem (okos telefonok veszélyei)
4. Halőrök, vadőrök – IT biztonságpolitika (compliance)
5. Áradó levélszemét (spam-ek,)
6. Folt hátán folt (patch-elés)
7. Kiemelkedő kártevők (vírusvédelem, nosztalgikus mail vírusok és hálózati férgek)

További témák (<http://www.symantec.com/connect/...>)

1. Számítási felhő („cloud computing”), virtualizáció
2. Web2.0 vállalati környezetben, válságmenedzselés
3. Kritikus infrastruktúrák védelme
4. „Zero-day” sérülékenységek
5. Politikai motivációk, „cyber” bűnözés

# A „cloud computing” veszélyei

Marne E. Gordan, IBM, előadása az „EuroCACS 2010”-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, licenz 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.

# 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.

# Néhány szó az ISACA-ról

- Alapítás 1969-ben (az ISACA-HU 20 éves)
- Tagok kb. 95 ezer (ISACA-HU 411 tag)
- IT irányítási nyílt szabványok és ajánlások az ITGI segítségével (COBIT, ValIT, RiskIT, ITAF, BMIS, stb.)
- Szabványok integrálása (mapping on ITIL, ISO27001, ISO13335, Basel2, COSO, stb.)
- Nemzetközi minősítések (CISA, CISM, CGEIT, CRISC)
- Szakmai cikkek és kapcsolatok ([www.isaca.hu](http://www.isaca.hu))
- Nemzetközi konferenciák és előadások ([www.isaca.org](http://www.isaca.org))

... és van aki így látja



# 2010. évi 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”

# A COBIT felépítése

## 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)

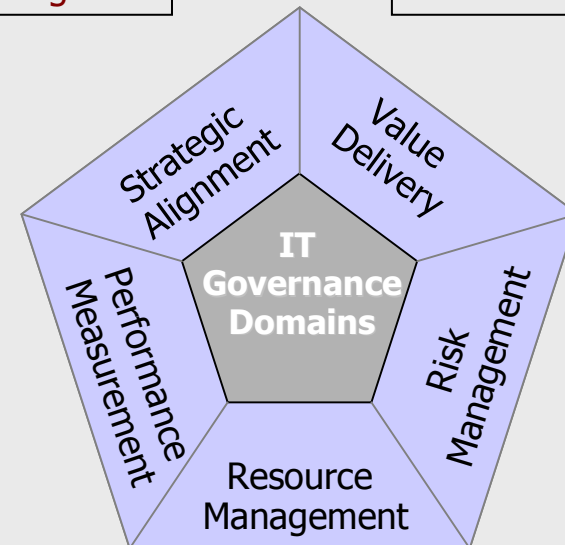
*metrics, IT Scorecards and dashboards*

COBIT® 4.1



Are we doing the right things?

Are we getting the benefits?



2009

Doing something about it

2007

Not doing something about it

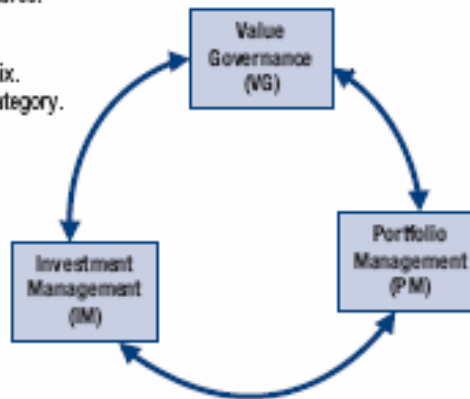
Are we doing them the right way?

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.

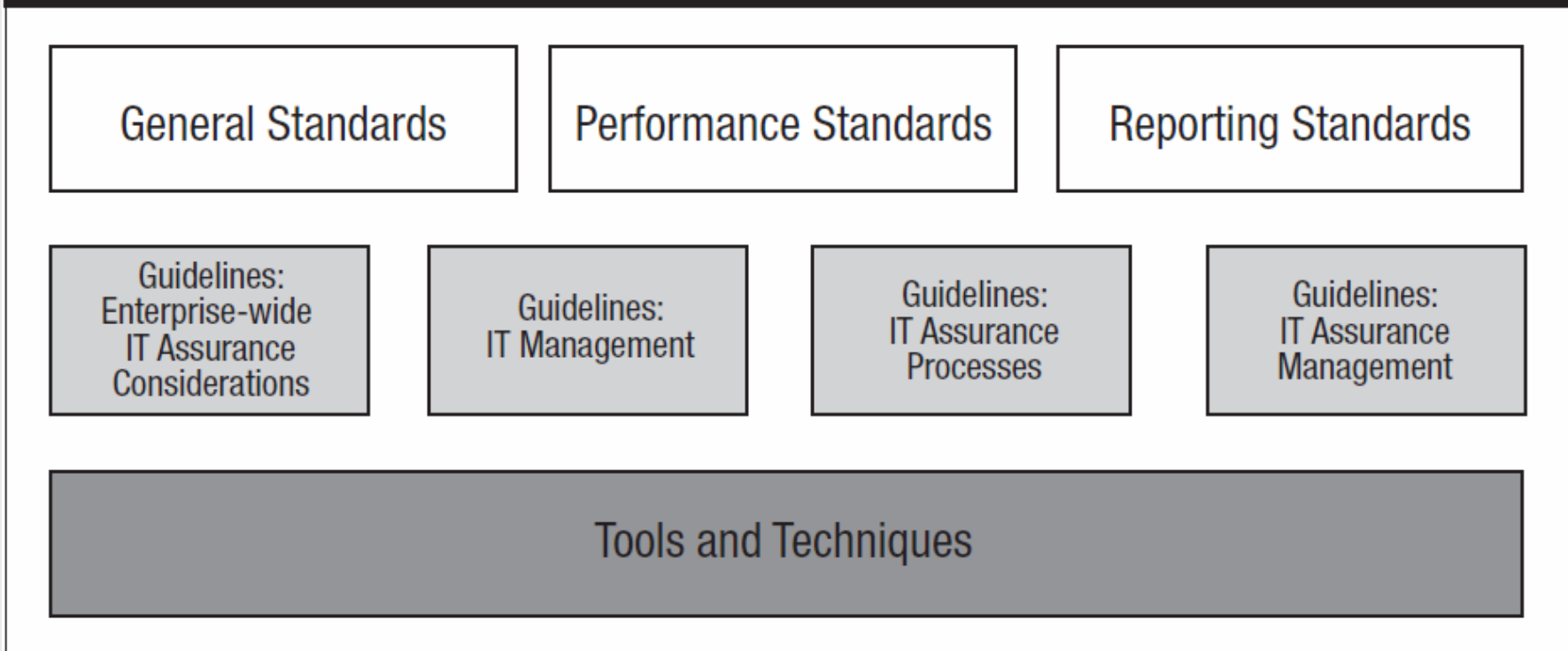


- IM1 Develop a high-level definition of investment opportunity.
- IM2 Develop an initial programme concept business case.
- IM3 Develop a clear understanding of candidate programmes.
- IM4 Perform alternatives analysis.
- IM5 Develop a programme plan.
- IM6 Develop a benefits realisation plan.
- IM7 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.

- 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.

# ITAF – IT Assurance Framework

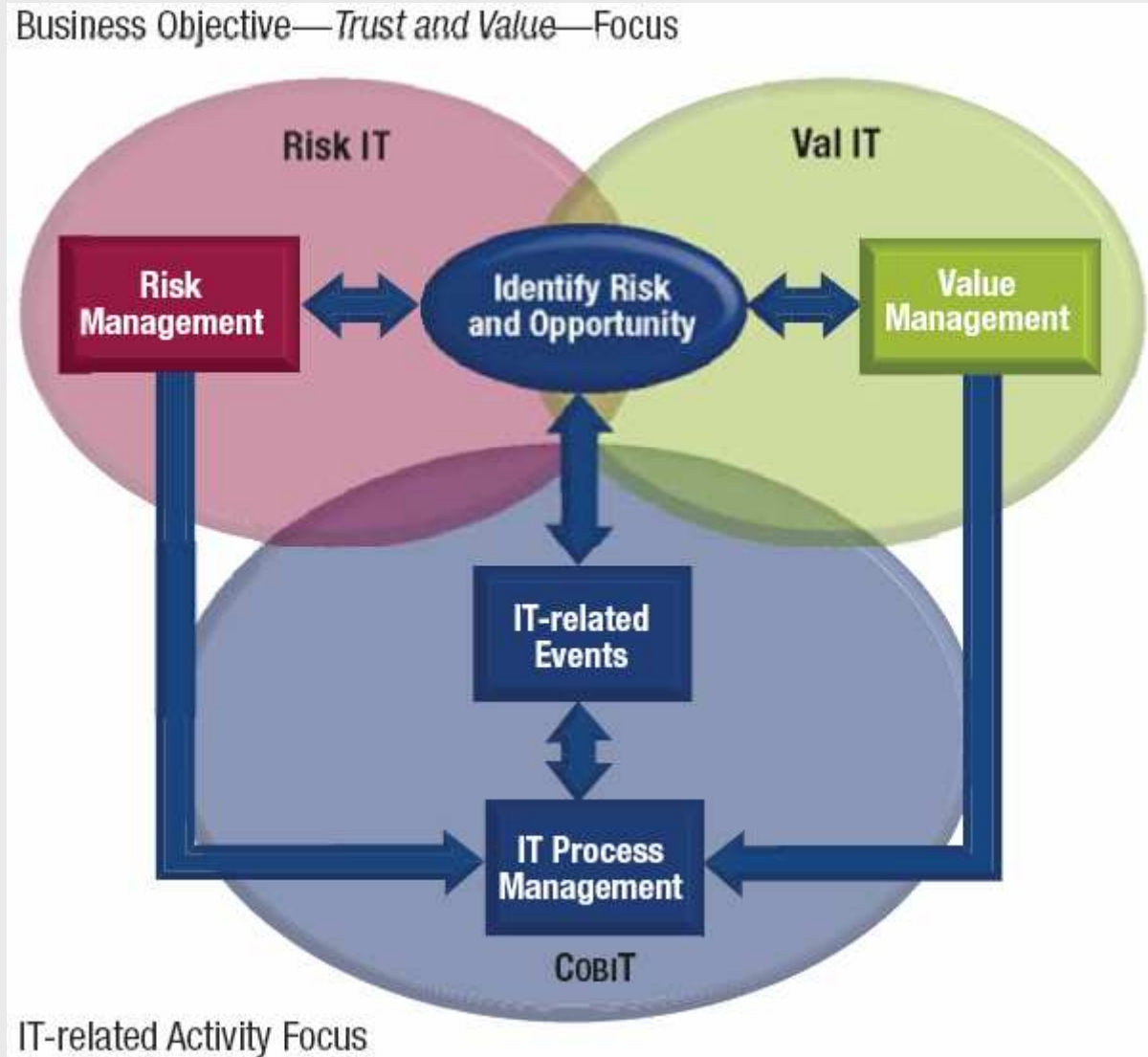
Figure 1—The ITAF Taxonomy: How ITAF is Organised Hierarchically



# Risk IT - kapcsolatok

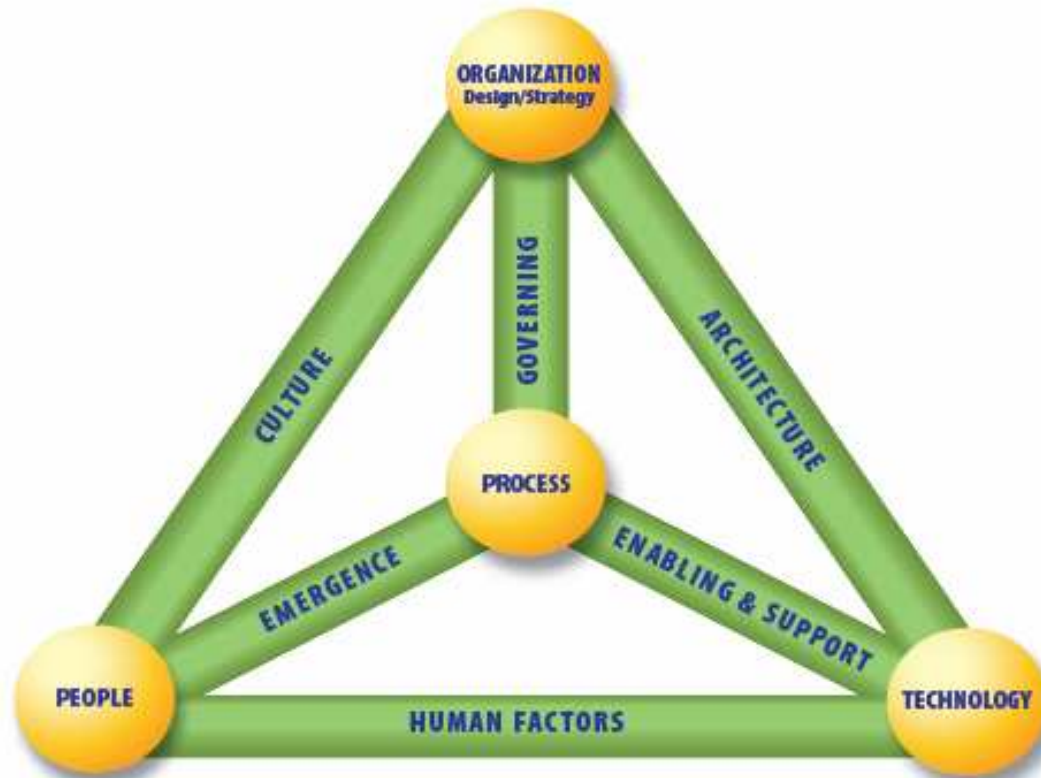
**A Risk IT  
kiegészíti és  
kibővíti a COBIT  
és Val IT  
dokumentumok  
at az IT  
irányítás teljes  
körű elméleti és  
gyakorlati  
megalapozása  
érdekében.**

**„Robert Stroud,  
CGEIT, ISACA  
Board of  
Directors”**



# 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

# 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 prioritási sorrend felállítása
  - Nincs IT biztonsági szakértő általi visszacsatolás
  - Nincs javaslat a kockázatok csökkentésére
  - Nincs vezetői jóváhagyás
  - Nem épül be a vállalati kockázatkezelési rendszerbe
- **COBIT:** „P09 - Kockázatok értékelése”

# Kockázatkezelési kontrollok

Van-e szabályozás a kockázatkezelésre? 83%

Milyen módszertannal? SPARK, CRAMM, OCTAVE, CARISMA, ITBC, CITICUS, ISO27001, COBIT, cégcsoport szintű illetve saját módszertanok

Van-e felelőse a kockázatmenedzselésnek? 77%

A kockázatelemzést elvégezték-e az elmúlt két évben? 82%

A kockázatelemzés eredményként az IT kontrollokat kialakították-e? 83%

A menedzsment felvállalta-e a maradék kockázatokat? 61%

Szerepel-e külsős szolgáltatókból eredő kockázat hatása a kockázatelemzésben? 66%

Lásd **A pénzügyi kiszervezési tevékenység IT biztonsági kérdéseinek elemzése** tanulmányt:

[http://www.pszaf.hu/data/cms2151158/Kiszervezesi\\_palyazat\\_PRAUDIT\\_2010\\_04\\_07\\_v10.pdf](http://www.pszaf.hu/data/cms2151158/Kiszervezesi_palyazat_PRAUDIT_2010_04_07_v10.pdf)

## 2. Jogosultságkezelés

### Hozzáférés- és jogosultságkezelés:

- **Jogszábaály:** 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-es adat!): 2006, 2007, 2008 is!

Központi jogkezelés: 78%-nál

Korszerű szoftveres támogatás: kb. 20%-nál

Lásd **A pénzügyi kiszervezési tevékenység IT biztonsági kérdéseinek elemzése** tanulmányt

# 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): 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,
  - Konceptiótlanság, szabályozatlanság,
  - Felelősök kijelölésének hiánya,
  - Naplófájlok hiánya,
  - Beépített audit lehetőségek hiánya, kihasználatlansága,
  - Automatikus eszközök hiánya,
  - Naplózási feladatok ellenőrizetlensége
- **COBIT:** „A12 – Alkalmazási szoftverek beszerzése és karbantartása”, „A13 – Technológiai infrastruktúra beszerzése és karbantartása”, „A14 – Informatikai eljárások kifejlesztése és karbantartása”, „DS13 – Üzemeltetés irányítása”

# Naplózási kontrollok

Van-e naplózási koncepció: 79%-nál

Van-e naplózási szabályozás: 67%-nál

A külsősök hozzáférését naplózzák-e? 80%

Naplózzák-e a jogosultságok változását? 77%

Naplózzák-e a biztonsági beállítások változását? 69%

A naplóállományokat elemzésre gyűjtik-e? 52%

A naplóállományokat rendszeresen mentik-e? 80%

Naplóelemző szoftvert használnak-e? 33%

A naplóelemzéshez külsős szolgáltatót alkalmaznak-e? 38%

Ez kiszervezés keretében történik-e? 28%

Lásd **A pénzügyi kiszervezési tevékenység IT biztonsági kérdéseinek elemzése** tanulmányt

# 4. Változáskezelés

## Változáskezelés, fejlesztések:

- **Jogszábaály:** 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 jogszábaályban 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:** „A16 – Változások kezelése”, „A15 – Rendszerek üzembe helyezése és jóváhagyása”, PO11 – Minőségirányítás”, „DS1 – Szolgáltatási szintek meghatározása”, „A12 – 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 pénzügyi kiszervezési tevékenység IT biztonsági kérdéseinek elemzése** tanulmányt

# 5. Üzletmenet-folytonosság

Üzletmenet-folytonosság, rendkívüli helyzet kezelés:

- **Jogsabály:** 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) ... 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 megőrizték, **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”

# Üzletmenet-folytonossági kontrollok

- Van-e BCP a kritikus folyamatokra? 83% igen
- Tesztelik-e rendszeresen a BCP-t? 60% igen
- Rendszeresen aktualizálják-e? 77% igen
- A kritikus rendszerekre van-e DRP? 80% igen
- Van-e nyilvántartás az incidensekről? 82% igen
- Az incidens kezelés szabályozott? 74% igen
- Van-e DRP a szállítók megszűnésére? 61% igen
- Van incidens kezelés a szolgáltatókra? 62% igen
- A belső szabályozások érvényesek-e a külsős szolgáltatókra is? 74% igen
- Van-e SLA a külsős szerződésekben? 67% igen

Lásd A pénzügyi kiszervezési tevékenység IT biztonsági kérdéseinek elemzése tanulmányt

# 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 „A11 – Automatizált megoldások meghatározása”

# 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”*

# 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 eszköz **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:** „P04 – Az informatikai részleg szervezeti felépítésének és kapcsolatainak meghatározása”, „P07 – Emberi erőforrások kezelése”

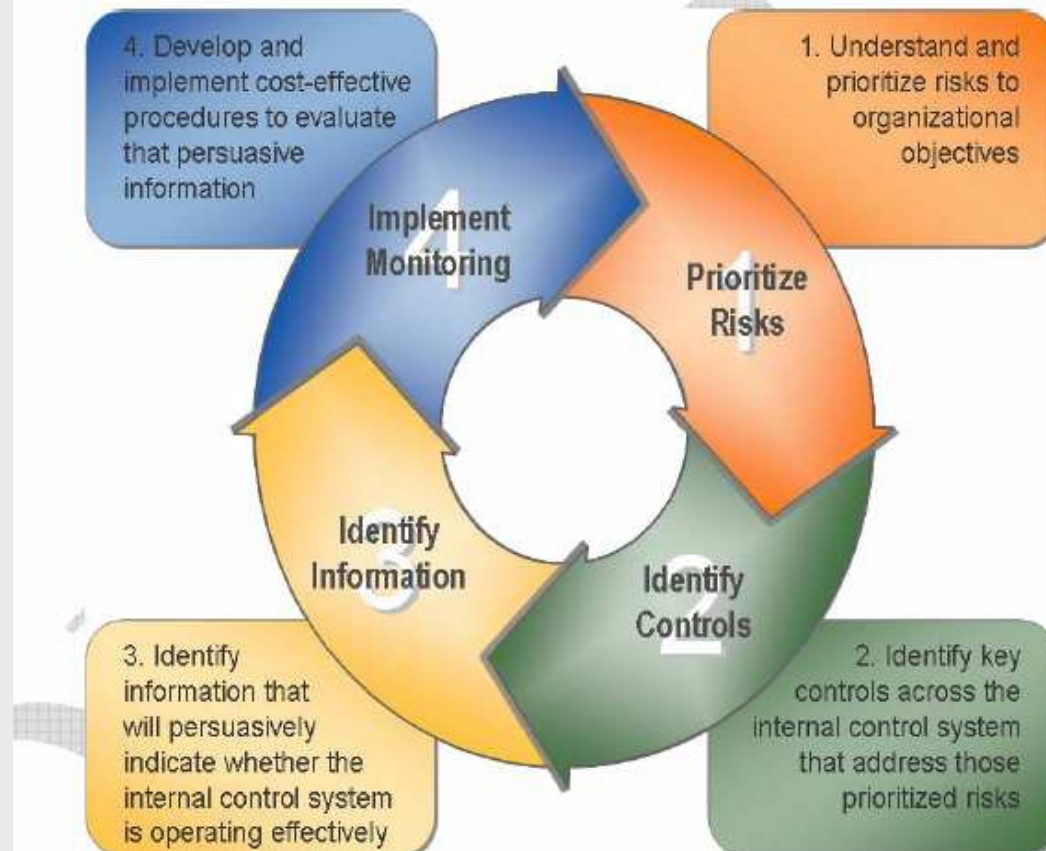
# 10. IT ellenőrzések

## IT irányítás, független ellenőrzés:

- **Jogszábaály: 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



Copyright 2009 by the Committee of the Sponsoring Organizations of the Treadway Commission. All rights reserved. Reprinted with permission.

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

# 11. IT biztonság

## IT biztonság, biztonság tudatosság:

- **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”

# 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”

# Banktitok és adatvédelem

**Jogsabályok:** A Hpt 50-55. §., a Bszt. 117-120. §, az Öpt. 40/A-40/B. §., az Mpt. 78-79. §.-i valamint a Bit. 153-162. §.-i szerint!

**Definíció: Hpt. 50. § (1) Banktitok** minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló **tény, információ**, megoldás vagy **adat**, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik.

**Kivétel: Hpt. 51. § (1)** Banktitok csak akkor adható ki harmadik személynek, ha *a)* a pénzügyi intézmény ügyfele, annak törvényes képviselője a rá vonatkozó kiszolgáltatható banktitokkört pontosan megjelölve közokiratba vagy teljes bizonyító erejű magánokiratba foglaltan kéri, vagy erre **felhatalmazást ad**; ... **Hpt. 54. § (1)** Nem jelenti a banktitok sérelmét *a)* az olyan összesített adatok szolgáltatása, amelyből az egyes ügyfelek személye vagy üzleti adata nem állapítható meg *j)* a hitelintézet által kiszervezett tevékenység végzéséhez szükséges adatátadás **a kiszervezett tevékenységet** végző részére

**Adatvédelem:** az Adatvédelmi törvény (1992. évi LXIII. ) 31/A. § szerint!

# 13. Oktatás

## IT oktatás, IT szakképzettség:

- **Jogszáály: 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: „P07 – Emberi erőforrások kezelése”**

# Összefoglalás, tanulságok

- Alakítsunk ki jól működő IT irányítást, készüljön üzleti és **IT stratégia, kontroll tudatos vezetés (IT GOVERNANCE)**. A legjobb válságmenedzselés a megelőzés (prevenció)! Folyamatos feladat a kontrollok fenntartása, készüljünk fel a problémákra!
- **Kockázatelemzés**, a veszélyforrások felmérése, a működési kockázatok rendszeres kiértékelése és a kontrollok kialakítása (**RISK MANAGMENT**).
- **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**.
- Minden kiszervezhető, de a **felelősség** nem! A kiszervezés **egy lehetőség** a kontrollált külső szolgáltatások alkalmazására!



*Bizalom és értékteremtés az információs rendszerekkel*

**Budapest Chapter**

**Köszönöm a  
figyelmet!**