RISK ADVISORY SERVICES / INFORMATION RISK MANAGEMENT

Informatikai audit a könyvvizsgálat folyamatában

Gaidosch Tamás

Könyvvizsgálói Kamara, 2006.10.12

AUDIT ▪ TAX ▪ ADVISORY

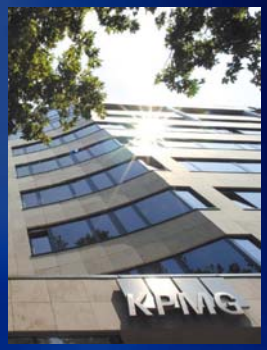
Tartalom

- Bevezető
- Az informatikai audit szerepe a pénzügyi auditban
- Munkamódszer
- Tapasztalatok
- Kérdések

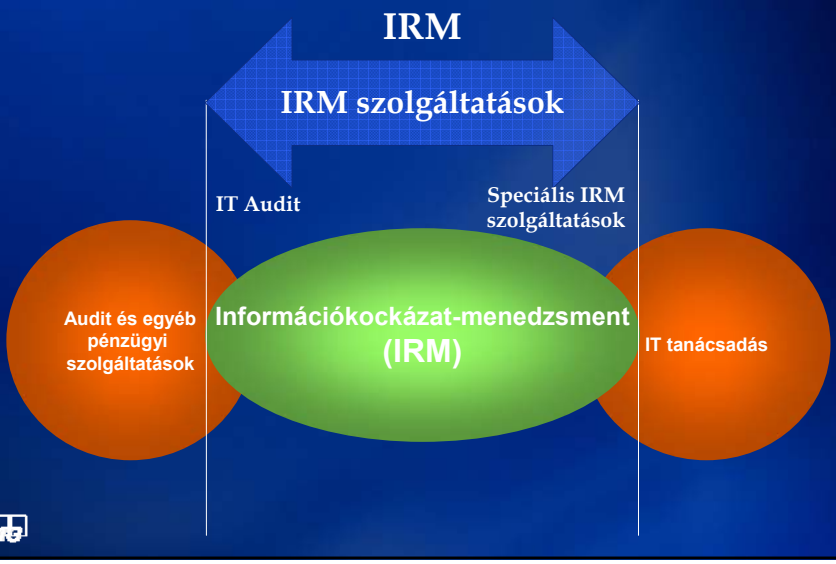
Bevezető

Információkockázat-kezelés (IRM)

- **Audithoz legközelebb álló csoport**
  - 35 munkatárs
  - régiós projektek
- **Szolgáltatások**
  - Külső
    - Projekt kockázatok
    - Információbiztonság, üzletfolytonosság
    - Folyamat-vizsgálatok
  - Belső
    - Pénzügyi audit támogatása
- **Tapasztalat az elmúlt években**
  - Számos audit a pénzintézeti szektorban
  - Speciális biztonsági vizsgálatok

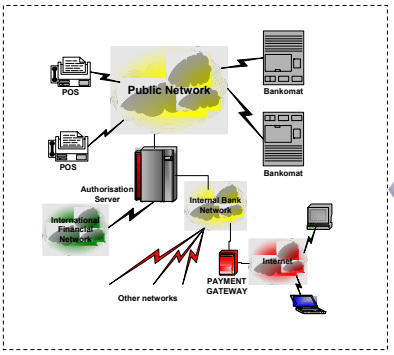


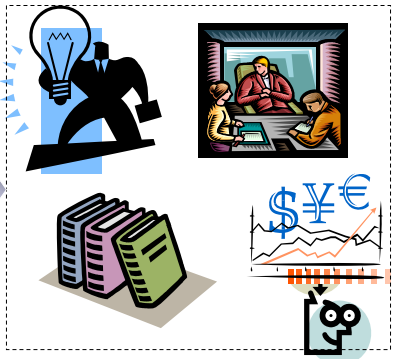
Határterület



5

IT vagy *információs rendszer* audit?



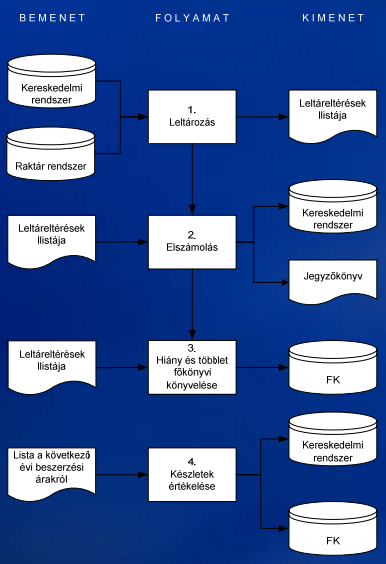


IT rendszerek ≠ információs rendszerek

adat ≠ információ

6

Kapcsolat a folyamatokkal



7

Az informatikai audit (IRM) szerepe a pénzügyi auditban

8

Kérdések

- **A pénzügyi adatokat a vállalatok informatikai rendszerekben tárolják. (pl. SAP, Oracle Financials)**
  → honnan tudjuk, hogy megbízhatunk a rendszerben?
- **Az adatokat a rendszerek feldolgozzák, ellenőrzik, módosítják, átstrukturálják, új adatokat állítanak elő. (pl. előállított adat a pénzügyi beszámoló is)**
  → honnan tudjuk, hogy megbízhatunk az előállított adatokban?
- **A rendszerek manuális folyamatokat váltanak ki, automatizálják a rutin feladatokat, sokszor utólagos emberi ellenőrzés nélkül**
  → honnan tudjuk, hogy megbízhatunk a rendszer által végzett ellenőrzésekben, számításokban?

Az IRM szerepe

- **Az audit kockázat csökkentése**
  - Az általános IT kontrollkörnyezet gyengeségeinek a beszámolóra való hatásának kimutatása
- **Audit munkafázisok támogatása**
  - Folyamatok, rendszerek és kontrollok dokumentálása
  - „IT jellegű” kontrollok értékelése
    - Tervezés (ToD) és működés (ToE) szinten is
  - Szubszantív tesztek
    - Pl. nagy tömegű / komplex újraszámítások
- **Integráns része az audit csapatnak**

Az IRM szerepe

- **Az IRM bevonása a pénzügyi auditba sok esetben kötelező:**
  - tőzsdén jegyzett vállalatoknál
  - pénzügyi intézeteknél
  - 500 munkaórát meghaladó auditoknál
  - ahol az IT kritikus szerepet játszik a vállalat működésében *
    - kérdőívvel mérhető (IT criticality assesment)
- **Az IRM által elvégzendő munka mennyisége függ:**
  - az audit típusától (KPMG-s kategóriák: SOX/FSA/SE/VSE)
  - ügyfél IT környezetének bonyolultságától
  - Audit által végzett kockázatfelméréstől (hol kritikus az IT)

KPMG

11

Az IRM szerepe – általános IT kontroll vizsgálat (ITGC)

- **Legtipikusabb vizsgálat**
- **Kulcsfontosságú IT alkalmazások meghatározása (főkönyvi rendszer és az ebbe közvetlenül vagy közvetve adatot szolgáltató egyéb rendszerek)**
- **Ezek közötti kapcsolatok, adatáramlások (interfészek)**
- **Vizsgált időszakban történt nagyobb változások és kezelésük**
- **Általános IT kontrollok dokumentálása és tesztelése**
- **Hiányosságok összegyűjtése**

KPMG

12

Az IRM szerepe – audit munkafázisok támogatása

- **Részvétel folyamat felmérésben, walkthrough-kban**
- **Rendszerbevezetési kontrollok tesztelése**
  - Pl. migráció ellenőrzése
- **Rendszerbe épített automatikus kontrollok tesztelése**
- **Jogosultság vizsgálat, összeférhetetlenségi vizsgálat**
- **Segítség a tesztelésben:**
  - Audit által végzett manuális tesztek kiváltása
  - IT eszközökkel: Computer Aided Audit Tools (CAATs)
    - ACL, IDEA, Access, Excel
  - Mintavételes teszt helyett teljeskörű teszt
  - Összegző jelentés a talált hiányosságokról

KPMG

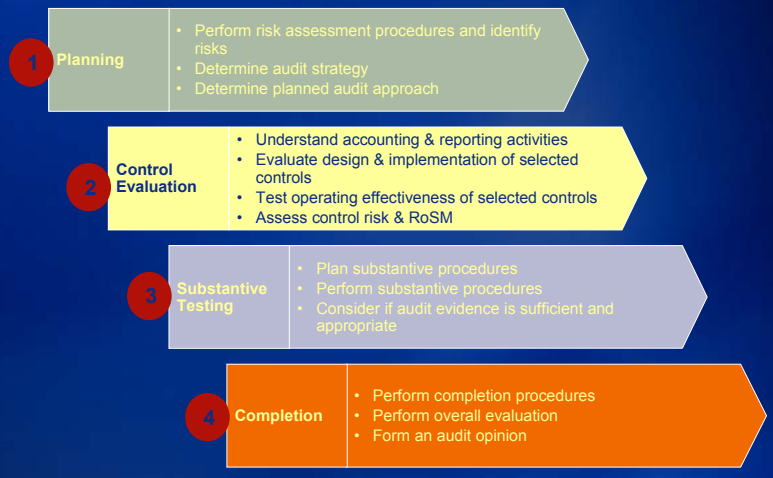
IRM által készített dokumentumok

- **Munkatípusonként különbözik**
- **Alapvető dokumentum amit az IRM önállóan tölt ki: ITGC (IT General Controls Document)**
- **Bedolgozás más munkapapírokba pl. vállalati szintű kontrollok**
- **Management Letter Points (MLP): ügyfélnek kiküldendő dokumentum, amely a főbb hiányosságokat tartalmazza észrevétel – kockázat – javaslat tagolásban**
- **Egyéb munkapapírok: pl. tesztek részletes leírása**
- **Egyéb Memo-k: pl. tervezéssel, munka elvégzésével kapcsolatos információk**

KPMG

Munkamódszer

KPMG audit módszertan



Kockázat és bizonytalanság

A héten tűzvész üthet ki New Yorkban

Az idő holnap talán jobb lesz a megszokottnál

A forint árfolyama zuhanhat

Az olajkészletek elfogyhatnak ötven éven belül

Lavinaveszélyt jeleztek a francia sípályákon

A won árfolyama nagyon ingadozhat a közeljövőben

Nem biztos, hogy lesz ebédszünet

17

Mi tehát a kockázat?

kockázat ≠ bizonytalanság ?

A kockázat olyan bizonytalanság, amely *számít*

hatással van ránk

befolyásolja a céljainkat

18

Ok-okozati összefüggés

Tény

*Bizonytalanság**

Lehetséges következmény

Könnyű összetéveszteni

A projekt vadonatúj technológiát használ

A rendszerhez illetéktelenek férhetnek hozzá

Valószínűleg túllépjük a költségkeretet

Az alkalmazás sérülékeny puffer túlcsordulásra, az adatainkat ellophatják

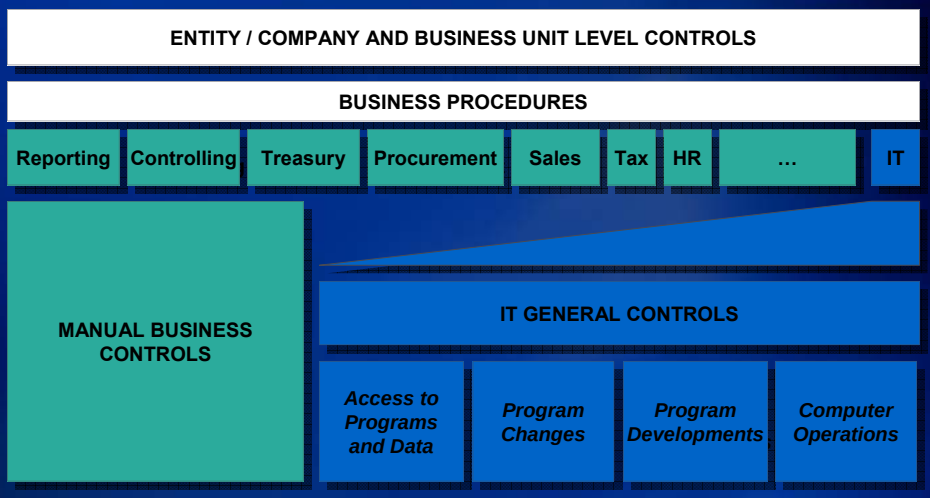
Nincs üzletfolytonossági tervünk

A fejlesztő késhet az alkalmazás átadásával

Az interfész nem fog működni

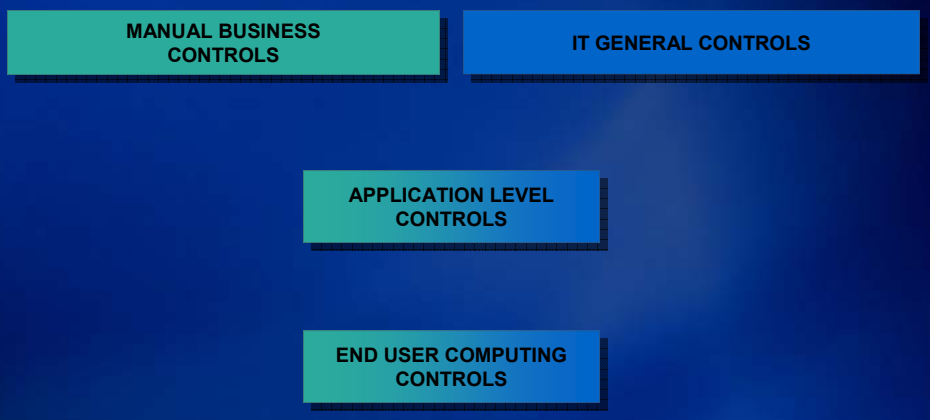
Fennáll a kockázata, hogy a fejlesztő késik az alkalmazás átadásával

Kontroll szemlélet



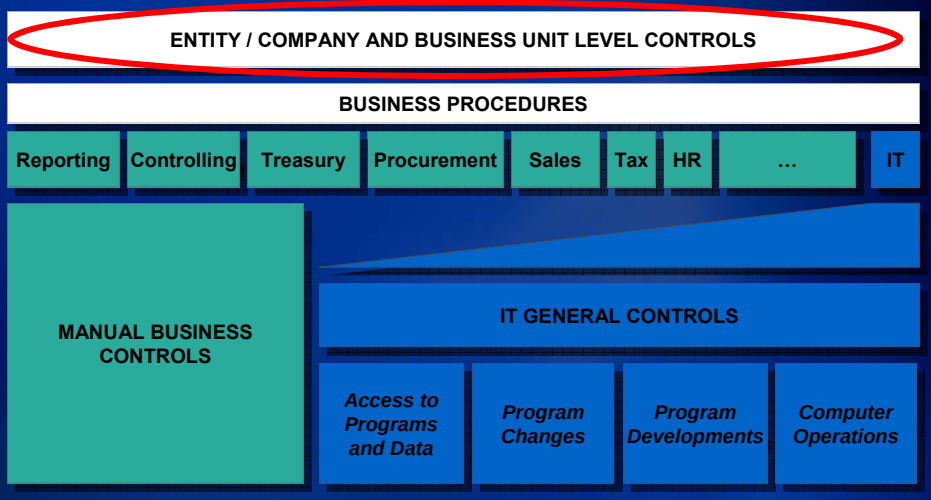
21

„IT jellegű” kontrollok



22

Vállalati szintű kontrollok



KPMG

23

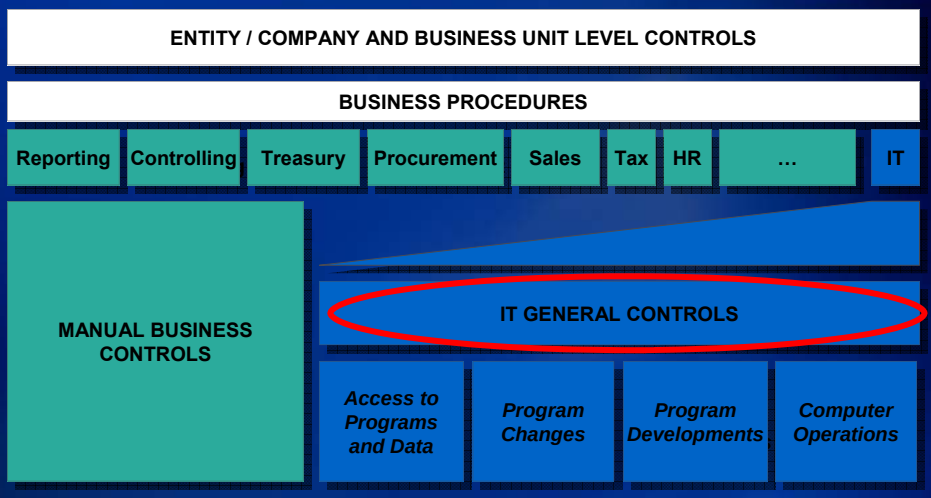
Vállalati szintű kontrollok – példák

- Szervezeti struktúra szabályozottsága: IT vezető feladatköre egyértelműen meghatározott. A felső vezetői üléseken az IT-t az IT vezető képviseli.
- HR kiválasztási folyamat szabályozottsága: IT szakemberek kiválasztását a HR végzi az IT terület által meghatározott szempontok szerint. A kiválasztott jelentkezőkkel az adott IT terület vezetője készít interjút.

KPMG

24

Általános IT kontrollok



25

Általános IT kontrollok – kategorizálás

- Logikai és fizikai hozzáférés
- Változtatás-kezelés
- Fejlesztés
- Üzemeltetés
- Felhasználói IT

26

Általános IT kontrollok – példák

- Egyedi felhasználói azonosítók, jelszavak használata kötelező
- Jogosultságkérés jóváhagyott és dokumentált
- Jogosultsági profilokat használnak az összeférhetetlen szerepkörök szétválasztásának támogatására
- Rendszeres jogosultsági vizsgálatok
- A szoftver változtatásokat formálisan jóváhagyják és tesztelik az éles üzmbe vétel előtt

KPMG

27

„IT jellegű” kontrollok

MANUAL BUSINESS CONTROLS

IT GENERAL CONTROLS

APPLICATION LEVEL CONTROLS

END USER COMPUTING CONTROLS

KPMG

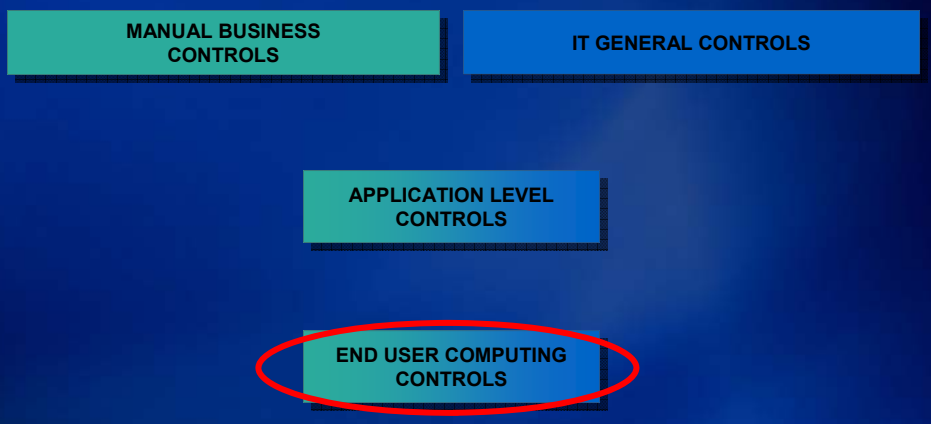
28

Alkalmazás szintű kontrollok – példák

- **Rendszerbeállítások (paraméterek) / számlatükör**
  - Validálások, limitek, adatbevitel ellenőrzések
- **Riportok**
  - Limit túllépések, törzsadat módosítások
  - Korosítások
  - Szokatlan tranzakciók
- **Interfész és konverziós kontrollok**
- **Logikai hozzáférési kontrollok**

29

„IT jellegű” kontrollok



30

Felhasználói IT - példák

- **Excel táblák**
- **Access adatbázisok**
- **Más, felhasználók által fejlesztett programok**

Felhasználói IT - problémák

- **Modell helyesség**
  - ellenőrzés, jóváhagyás elmarad
  - „jól számol, de mit?”
- **Adatintegritás**
  - Forrás adatok konverziója, beolvasása hibás
  - „jól számol, de miből?”
- **Rendelkezésre állás**
  - Biztonsági mentések hiánya
  - „jól számol, de hol van?”

Felhasználói IT – problémák (2)

- **Változtatás-kezelés**
  - Kontrollált folyamat hiánya
  - „jól számolt, de már nem...”
- **Hozzáférés**
  - Gyenge / nem létező jogosultsági rendszer
  - „jól számol, de kinek?”

KPMG

Összegzés: IT kontrollok hatása az auditra

IT control areas	Impact on the Audit	SE Workpapers	FSA Workpapers	SOX Workpapers
Entity Level Controls	• Audit Planning • Audit Strategy	Planning Document	Entity Level Controls Program	Company and Business Unit Level Controls Document
IT General Controls (including End User Computing Controls)	• Reliance on specific automated and/or manual controls • Assessment of risk • Nature, timing, and extent of substantive procedures	IT General Controls Program	IT General Controls Program	IT General Controls Document IT General Controls Summary
Application Level Controls	• Assessment of risk • Nature, timing, and extent of substantive procedures	Audit Program	Audit Program	Audit Program

KPMG

Tapasztalatok

Tipikus banki audit támogatási munkák

- **Általános IT kontrollok vizsgálata**
  - Egyszerű
  - Kötelező gyakorlat, az audit csapat kis hozzáadott értékűnek tartja
- **Folyamatok, IT jellegű kontrollok tesztelése**
  - Viszonylag egyszerű → közepesen bonyolult
  - Nagy hozzáadott érték
- **Újraszámítások**
  - Bonyolult
  - Maximális bizonyosság

Példa

AUDIT PROGRAM
(04/05)
[Insert file section]

110 Kamatráfordítás – betétek

Activities over initiation and authorization
Kamatelhatárolás, kamatjóváírás A termék típus megadásakor automatikusan kerül rögzítésre a kamatláb és a lejárat. Nem standard termékeknél ezt külön kell bevinni. A rendszerbe beállított kamatmértékeket figyelembe véve a kamatok számítása, elhatárolása és jóváírása automatikusan történik. A rendszer alapbeállításként 360 nappal (GBP esetén a nemzetközi standardok miatt 365 nappal) számol. ***Kamattábla frissítése*** A kondíciós listákon szereplő kamatokat a Paramétertáblában tárolják. Ennek változtatását az ALCO Bizottság fogadja el (MNB alapkamat változás vagy akciók esetén jellemző), a rögzítést a Back Office Törzsadat területe végzi.

Significant risk points	Description of control identified	IT component?	To be tested?
Megadhatók nem standard kondíciók (pl. kamat)	Az egyedi kondíciókat összeghatártól függően a megfelelő döntési szinten jóvá kell hagyni.	N	Y
	Authorizálás	Y	Y
	Az ügyfélaktának tartalmaznia kell a felsőbbszintű jóváhagyás dokumentumát. A rögzítő mellett egy másik személy jóváhagyása is szükséges (négy szem elve. **Azonban az is rögzítheti, aki jóváhagyja, így már nem teljesül a négy szem elve.**		

Példa

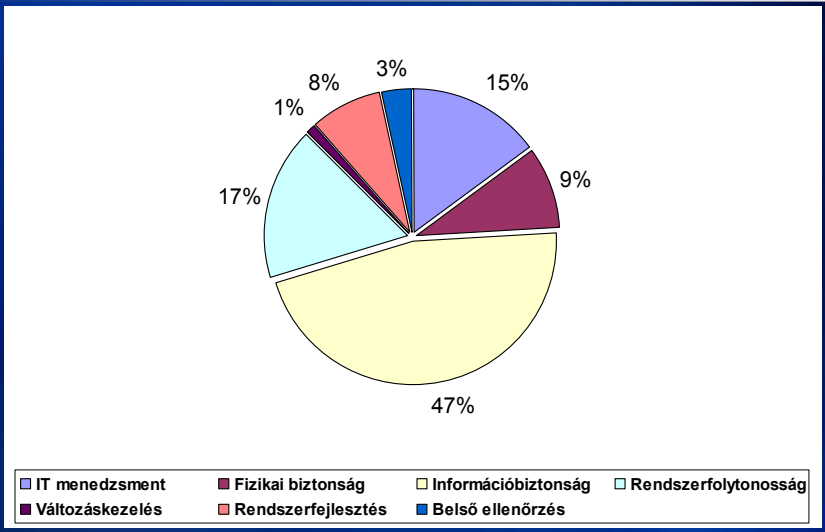
AUDIT PROGRAM
(04/05)
Page 5 of 7
G10AO 122 CEA Elhatárolások (Controls - Acct Bal).doc

A.3 Substantive audit procedures [KAM 5479]

Rationale for RoSM assessment		RoSM
Inherent risk	Low	**Low**
Control risk	Controls are: Effective A jelentős mértékű egyéb költségek elhatárolásának folyamatán nem találtunk megbízható kontrolokat, így az év végi egyenleg megbízhatóságát substantive módszerrel teszteljük.	

Nature and extent of audit procedures [KAM 5116]	Significant account / disclosure	C	E	A	V	O	P	Done by and date	W/P Ref
Substantive analytical procedures [KAM 5300]									
Az év végi állományok alapján az előző évi adatokat és a módosító körülményeket figyelembe véve az elhatárolandó összeg becslése	Aktív időbeli elhatárolások - kamatelhatárolás	**X**	**X**	**X**					
Az év végi állományok alapján az előző évi adatokat és a módosító körülményeket figyelembe véve az elhatárolandó összeg becslése	Passzív időbeli elhatárolások - kamat	X	X	X					
Az év végi állományok alapján az előző évi adatokat és a módosító körülményeket figyelembe véve az elhatárolandó összeg becslése	Kamatbevétel - hitelek	X	X	X					

IT auditok észrevételeinek megoszlása



39

IT menedzsment kontrollok leggyakoribb hiányosságai

- **IT stratégia hiánya**
- **Szervezeti hiányosságok**
- **Külső szolgáltatótól való függés**
- **SLA hiánya**
- **Törvényi megfelelés biztosításának hiányosságai**
  - Hpt 13/A (Kiszervezés) és 13/B (Biztonság)

40

Fizikai biztonsági kontrollok leggyakoribb hiányosságai

- Jogosulatlan hozzáférés (fizikai)
- Környezeti kontrollok hiánya
- Harmadik felek hozzáférései

KPMG

41

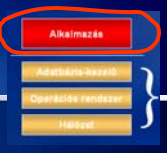
Információbiztonsági kontrollok leggyakoribb hiányosságai

- Jelszó hiányosságok
- Biztonsági adminisztráció hibái
- Szabályok, szabályzatok hiányosságai
- Biztonságilag nem megfelelően konfigurált alkalmazásszerver
- Alkalmazások biztonsági hibái
- Biztonsági frissítések telepítésének elmulasztása
- Nem megfelelő fájlhozzáférések
- Titkosítatlan / törhető protokollok használata

KPMG

42

Alkalmazások biztonsági hibái - példa



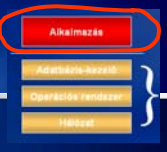

```
load file=/ebank/tmp/cli.upg to=2998 type=FILE
pcfile=UPG.EXE type=HIDDEN
```

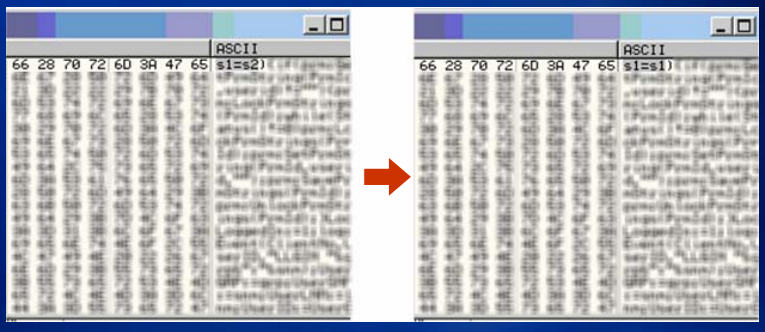
```
load file=/etc/passwd to=2998 type=FILE
pcfile=UPG.exe type=HIDDEN
```

Hiba: A kliens upgrade funkcióban a szerver nem ellenőrzi a kliens upgrade kérését

Eredmény: letölthető a szerver jelszó állománya

Alkalmazások biztonsági hibái - példa

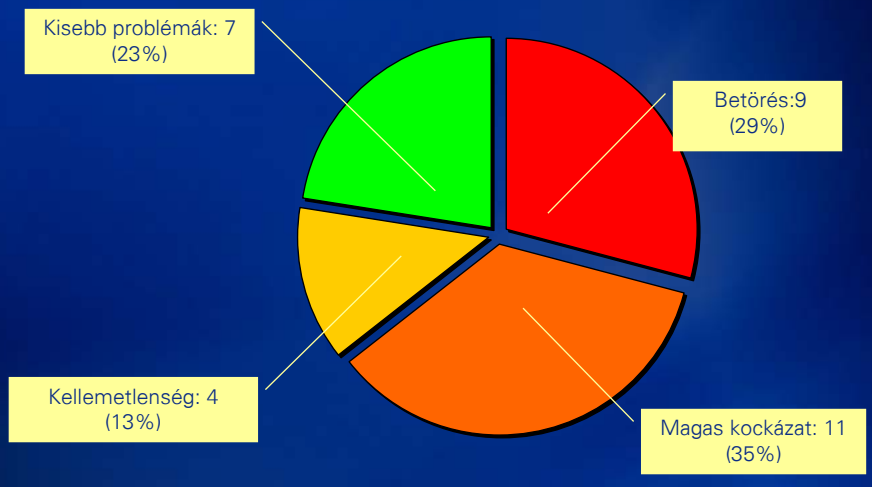




Hiba: Authentikációt eldöntő logikai feltétel kliens oldalon

Eredmény: kis módosítás után bármilyen jelszóval be lehet lépni

Internetes banki rendszerek tesztje: Mennyire rossz a helyzet?



A KPMG Tanácsadó Kft. által az utóbbi négy évben végzett internet banki vizsgálatok alapján

46

Rendszerfolytonossági kontrollok leggyakoribb hiányosságai

- Biztonsági mentések hiányosságai
- BCP, DRP hiánya, hibái
- Konfiguráció-menedzsment hiánya

47

Rendszerfejlesztési kontrollok leggyakoribb hiányosságai

- Nem megfelelő fejlesztési módszertan
- Dokumentáltság hiánya
- Projekt menedzselési hiányosságok
- Felhasználók nem megfelelő bevonása

48

Belső ellenőrzési kontrollok leggyakoribb hiányosságai

- Nincs belső IT audit
- Nem megfelelően képzett a belső ellenőr
- Módszertan hiánya
- Függetlenség hiánya

KPMG

Kérdések

KPMG

Kapcsolatfelvétel:

Gaidosch Tamás

KPMG Tanácsadó Kft.

+36 (1) 887 7139

tamas.gaidosch@kpmg.hu

www.kpmg.hu