KPMG

cutting through complexity™

Informatikai audit a könyvvizsgálat folyamatában

2011. szeptember 9

Pajdics Veronika

IT Tanácsadás - Információkockázat-kezelés

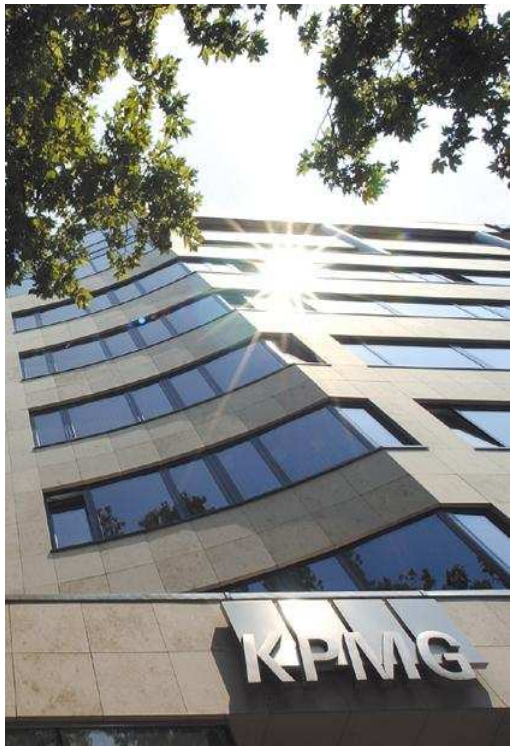
Tartalom

- Bevezető
- Az informatikai audit szerepe a pénzügyi auditban
- Munkamódszer
- Általános IT kontrollok
- Alkalmazási kontrollok
- Tapasztalatok

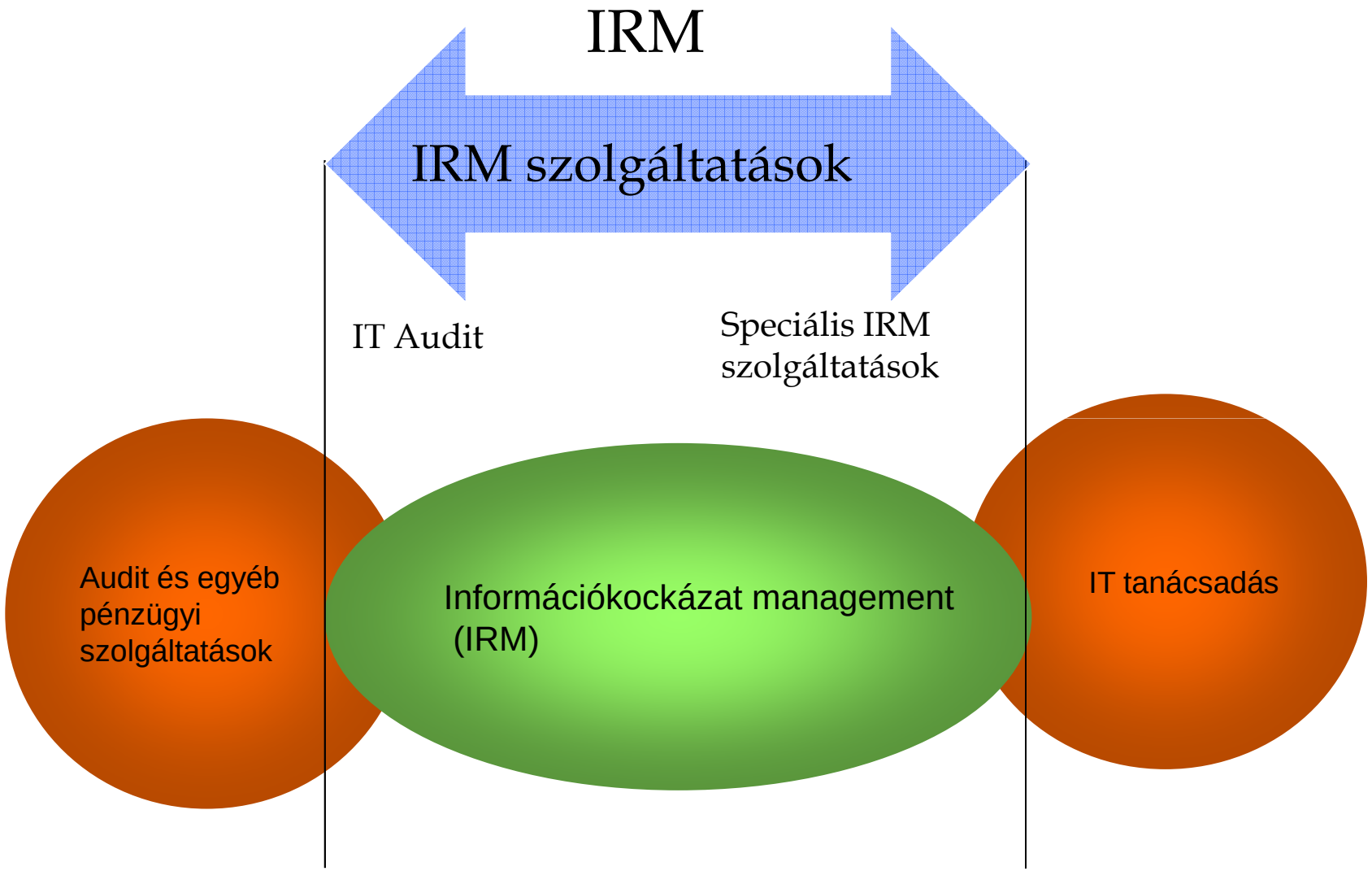
Bevezetés

Információkockázat-kezelés – IRM csoport

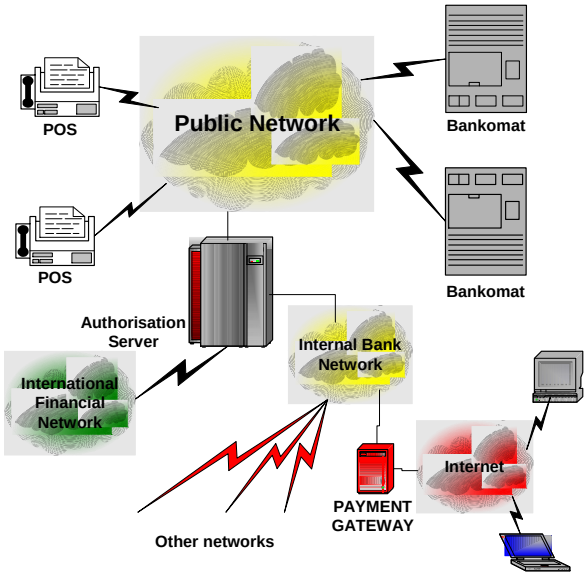
- IRM csoport
  - Audithoz legközelebb álló csoport
  - 32 munkatárs
  - Informatikusok
  - Számviteli ismeretek, könyvvizsgálati ismeretek
  - Audit trainingek
- Szolgáltatások
  - Belső
    - Pénzügyi audit támogatása
  - Külső
    - Kockázatelemzés
    - Informatikai audit, üzletfolytonosság, informatikai belső ellenőrzés
    - Biztonsági vizsgálatok

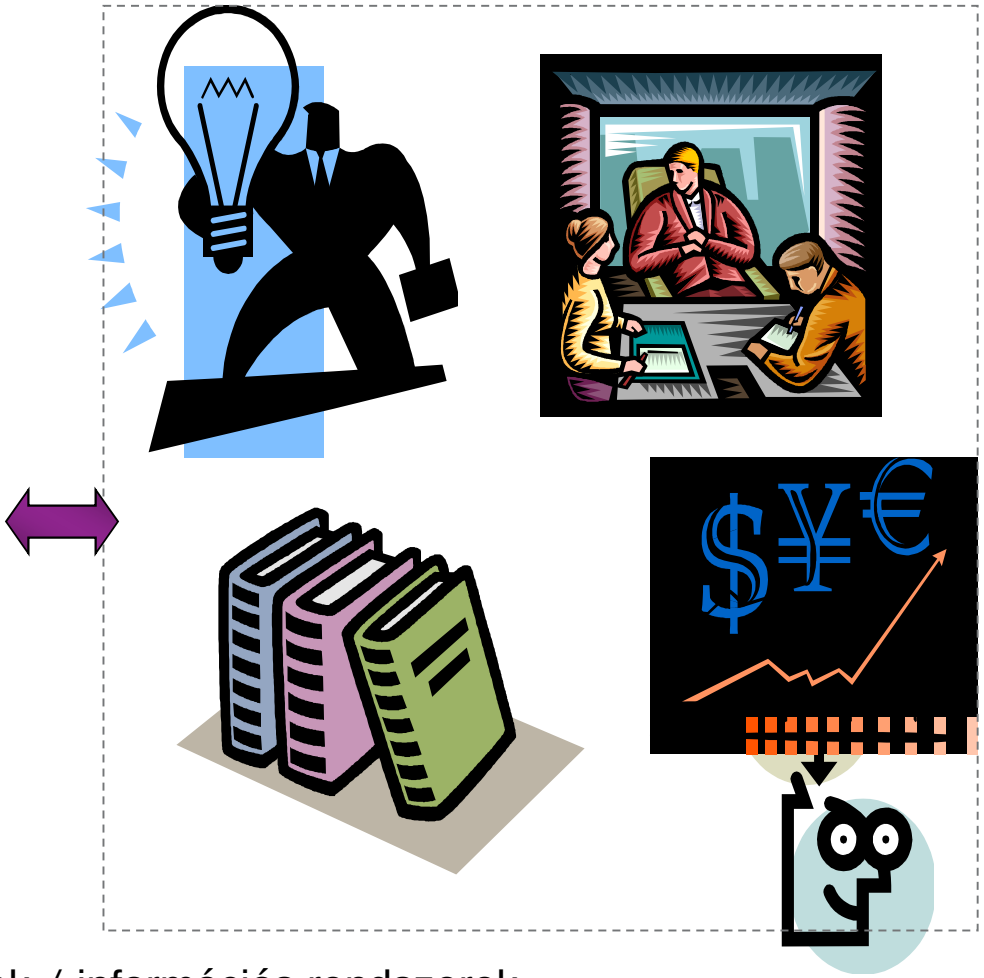


Határterület



IT vagy információs rendszer audit?



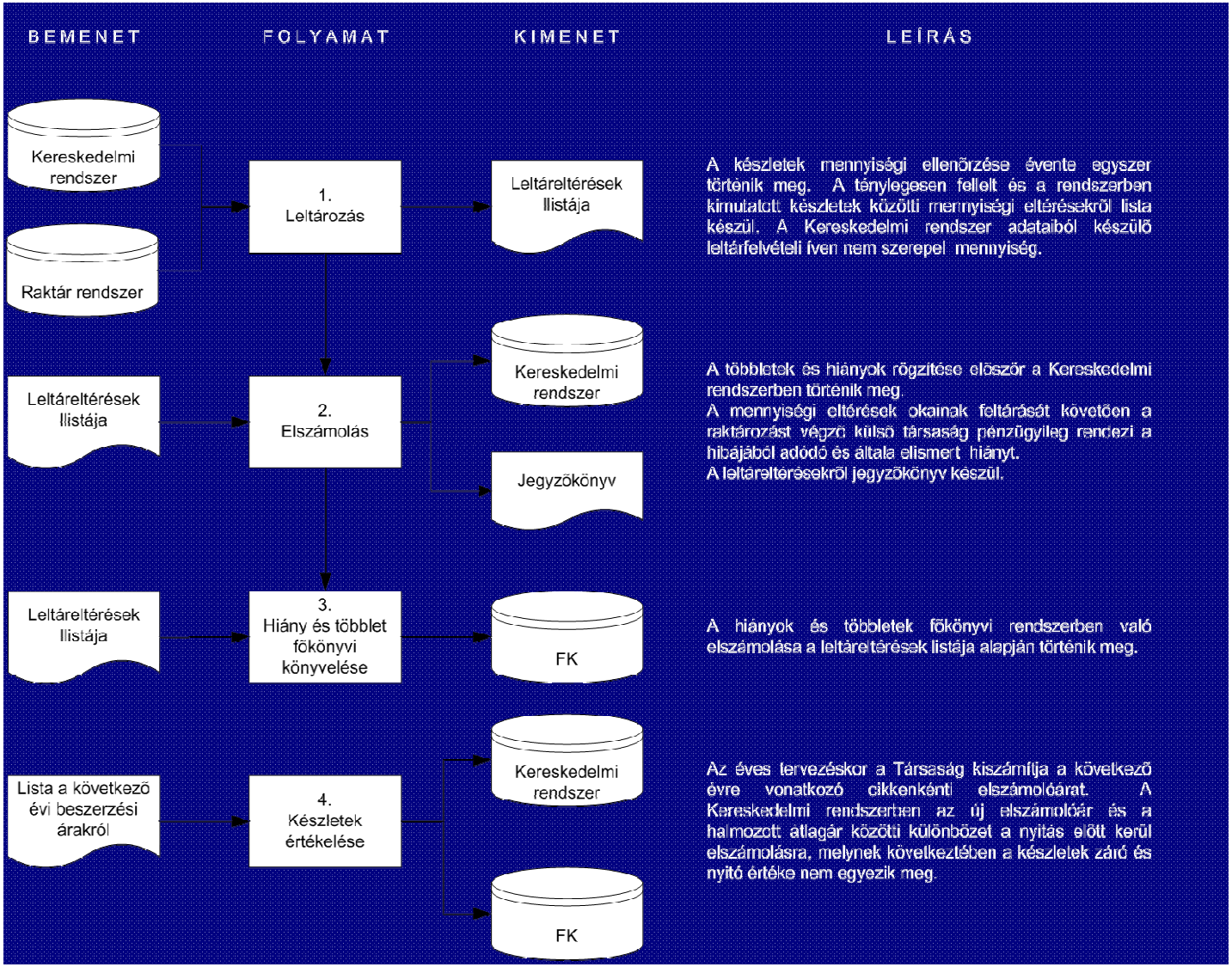


IT rendszerek ≠ információs rendszerek

adat ≠ információ

Az informatikai audit szerepe a pénzügyi auditban

Kapcsolat a folyamatokkal



Miért szükséges az informatikai rendszer vizsgálata?

- A pénzügyi adatokat a vállalatok informatikai rendszerekben tárolják (pl. SAP, Oracle)

  → Honnan tudjuk, hogy megbízhatunk a rendszerekben?

- Az adatokat az informatikai 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
  - IT rendszerek, IT folyamatok felmérése
  - IT kontrollok azonosítása
    - IT kontrollok tesztelése – kialakítás és működési hatékonyság szintjén
  - Szubsztantív tesztek
    - Pl. nagy tömegű / komplex újraszámítások
  - Automatikus kontrollok tesztelése
- 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
- Az IRM által elvégzendő munka mennyisége függ:
  - az audit típusától (KPMG-s kategóriák)
  - ügyfél IT környezetének bonyolultságától
  - audit által végzett kockázatfelméréstől (hol kritikus az IT)

Az IRM szerepe – általános IT kontroll vizsgálat (GITC)

- Leggyakoribb vizsgálat a pénzügyi audit keretében
- Kulcsfontosságú IT alkalmazások meghatározása
  (pénzügyi audit szempontjából fontos alkalmazások és az ebbe közvetlenül vagy közvetve adatot szolgáltató egyéb rendszerek)
- Rendszerek közötti adatkapcsolatok, adatáramlások (interfészek) felmérése, vizsgálata
- Vizsgált időszakban történt nagyobb változások és kezelésük
- Általános IT kontrollok dokumentálása és tesztelése
- Hiányosságok összegyűjtése

Az IRM szerepe – audit munkafázisok támogatása

- Részvétel folyamatfelmérésben, walkthrough-kban
- Rendszer bevezetési 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

IRM által készített dokumentumok

- Munkatípusonként különbözik
- KPMG standard dokumentum: General IT Controls (IRM önállóan tölti ki)
- Audit munkalapok részleteinek a kitöltése pl. vállalati szintű kontrollok
- Management Letter Points (MLP): ügyfélnek kiküldendő dokumentum, amely a főbb hiányosságokat tartalmazza
  észrevétel – kockázat – javaslat tagolásban
- Egyéb munkalapok: pl. tesztek részletes leírása
- Egyéb Memo-k: pl. tervezéssel, munka elvégzésével kapcsolatos információk

Munkamódszer

KPMG Audit Workflow

Activities

1 Risk Assessment

- Perform risk assessment activities, and identify significant accounts/disclosures and relevant assertions
- Identify significant risks
- Determine planned audit approach and understand accounting activities
- Identify relevant controls and evaluate design & implementation
- Undertake a risk assessment and planning discussion

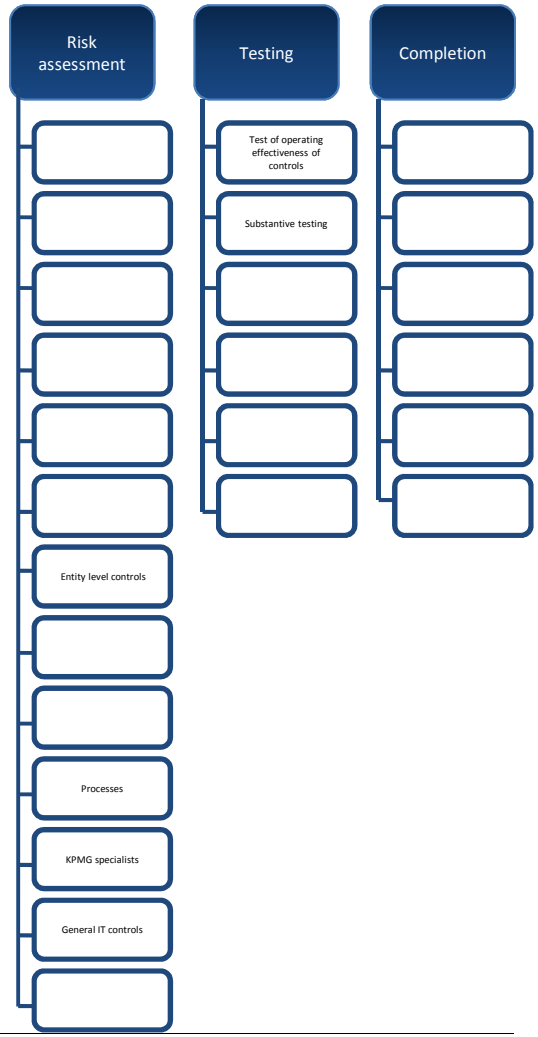
2 Testing

- Test operating effectiveness of selected controls
- Assess control risk and RoMM for each relevant assertion
- Perform substantive testing
- Consider if audit evidence is sufficient and appropriate

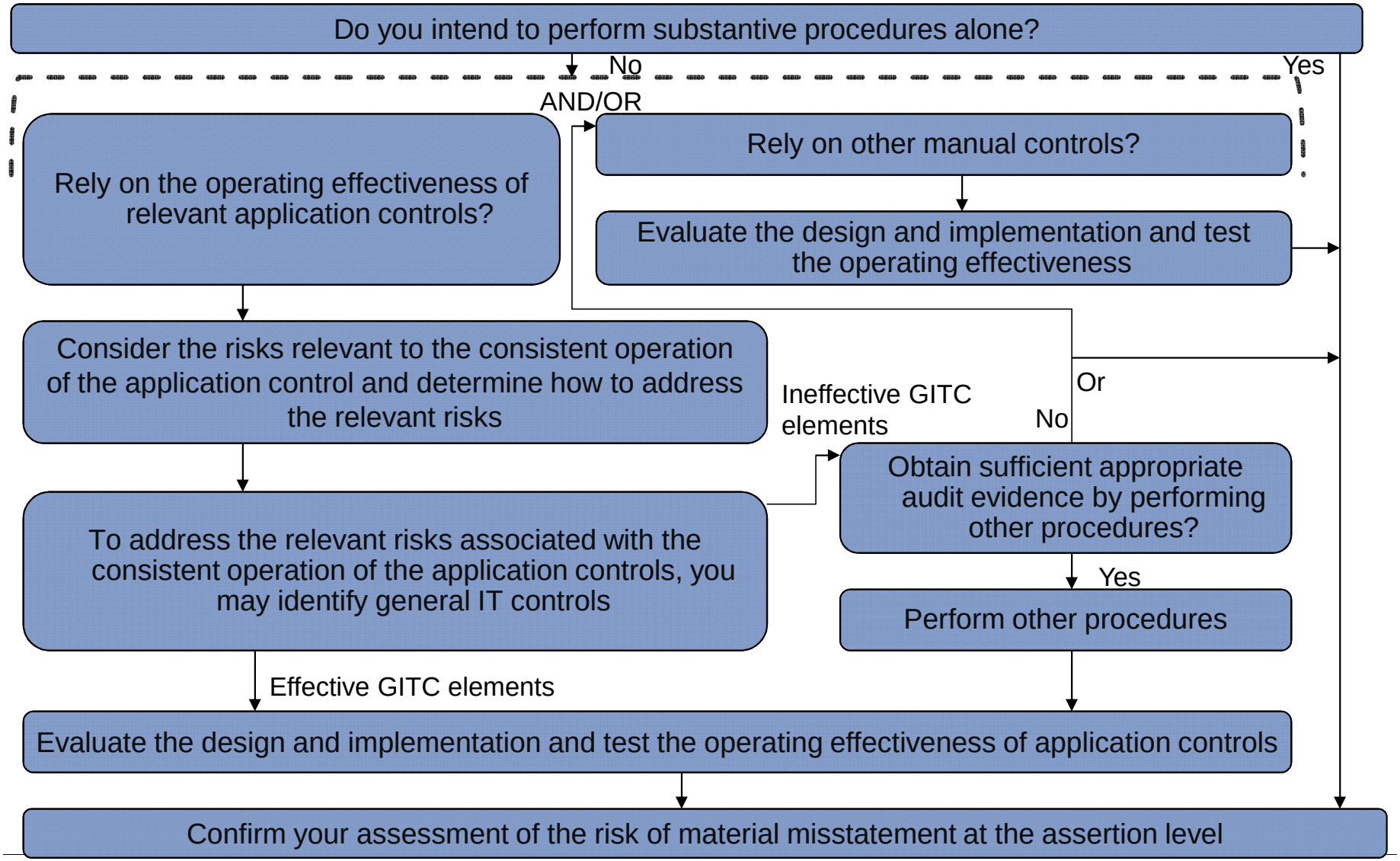
3 Completion

- Perform completion activities
- Perform overall evaluation
- Perform financial reporting activities
- Form the audit opinion

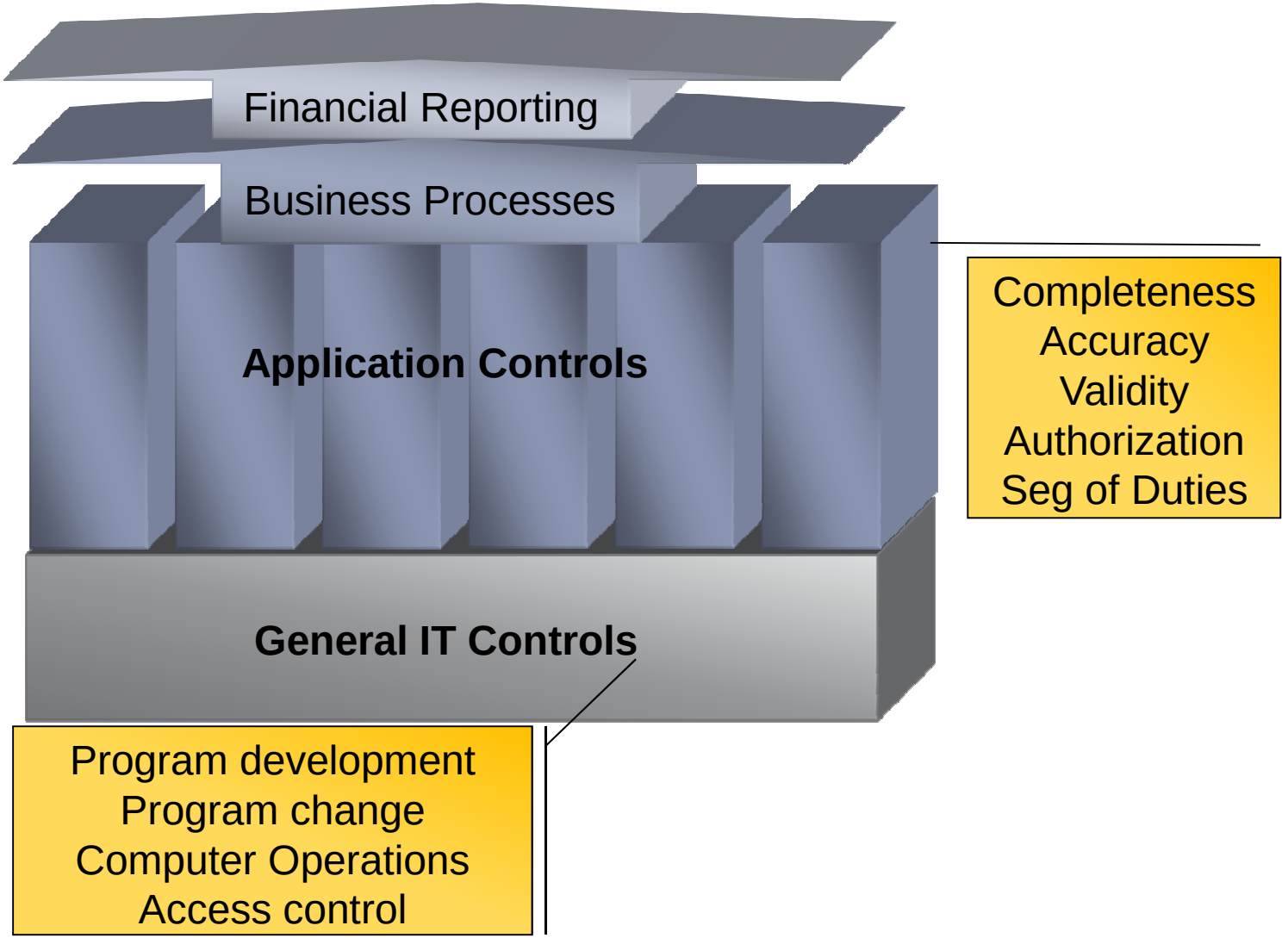
Required Documentation



Audit megközelítés



IT és alkalmazás szintű kontrollok

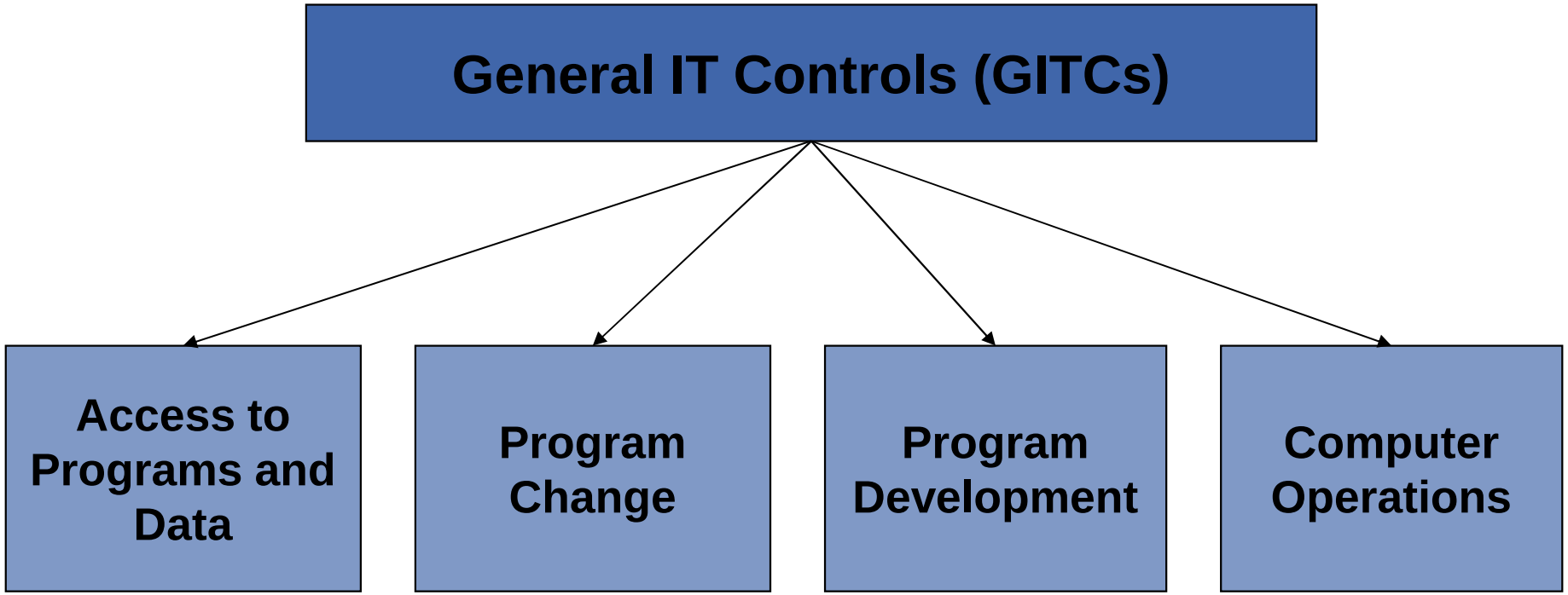


Általános IT kontrollok

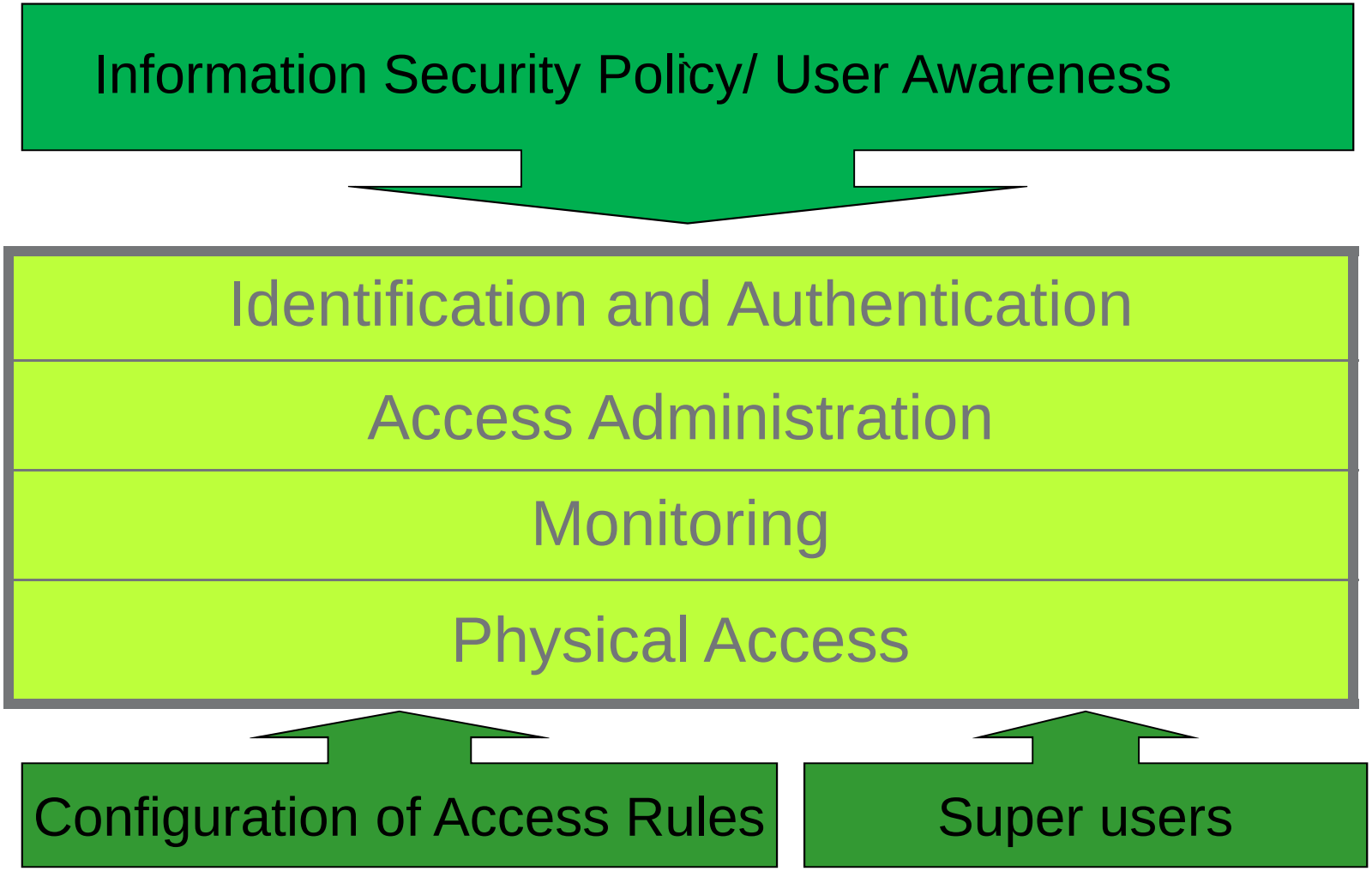
Felhasználói IT - problémák

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

Általános IT kontrollok



Access to Programs and Data



Access to Programs and Data - Kockázatok

- Az IT folyamatok nincsenek szabályozva
- Fizikai biztonság nem megfelelő
- Rendszerekhez való hozzáférés nem szabályozott
  - Hozzáférés engedélyeztetése
  - Kilépett dolgozó, fejlesztő, informatikus hozzáfér a pénzügyi adatokhoz
  - Nem egyedi felhasználói azonosítók használata
  - Adminisztrátori jogosultságok
  - Monitoring

Program Change Management és Program Development

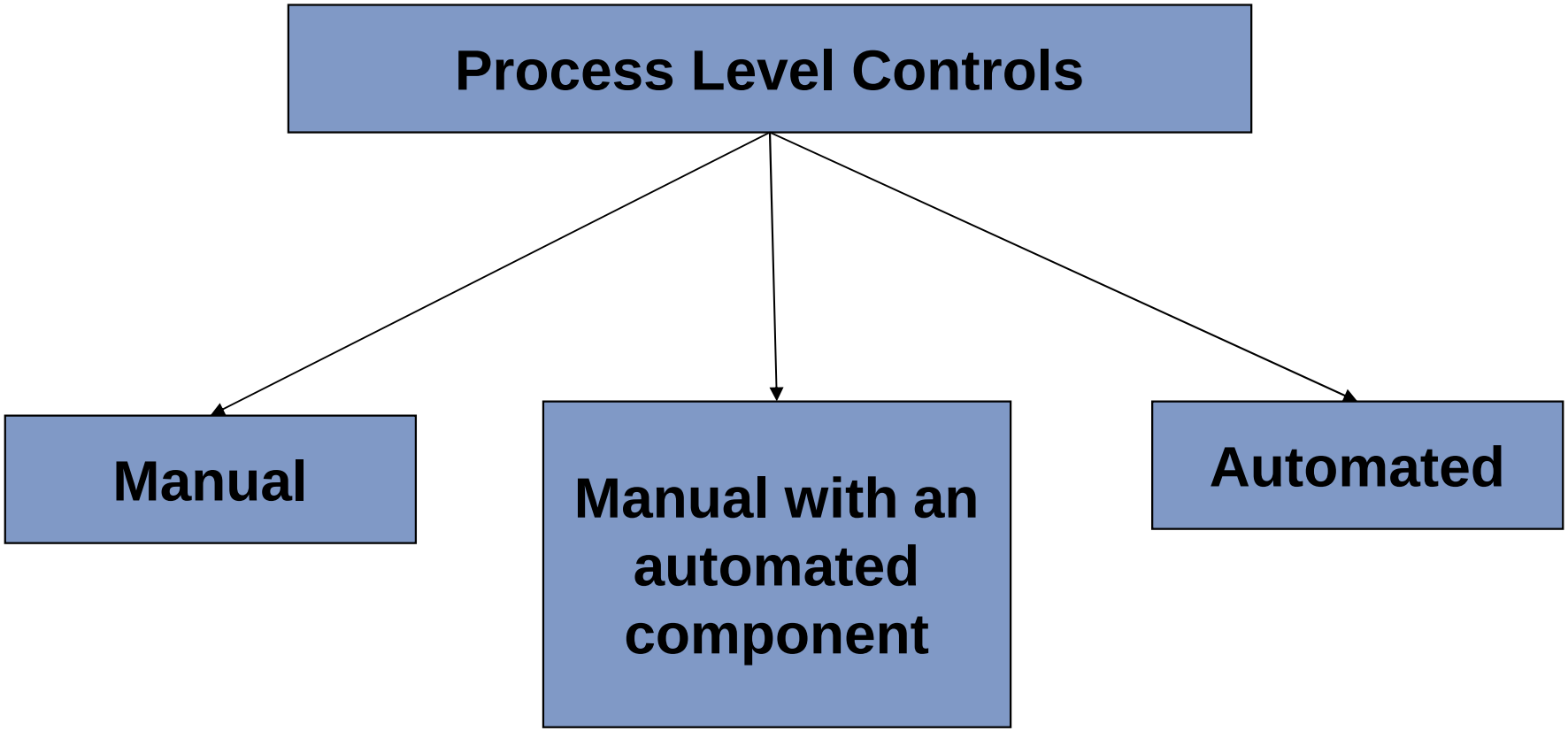
- Programváltoztatás
  - Módosítás folyamata nem dokumentált
    - Engedélyezés
    - Tesztelés
    - Élesbe állítás
- Programfejlesztés
  - Előkészítés
  - Oktatás
  - Migráció
  - Tesztelés

Computer Operation

- Ütemezett feladatok
  - Kontrollok (manuális és automatikus)
- Mentés
  - Adatok és alkalmazások
  - Kontrollok (manuális és automatikus)
- Help-desk

Alkalmazási kontrollok

Alkalmazási Kontrollok



Alkalmazás szintű kontrollok – példák

- Értékesítés, beszerzés, készlet, árfolyamkülönbözet
- Rendszerbeállítások (paraméterek) / számlatükör
  - Validálások, limitek, adatbevitel ellenőrzések
- Riportok
- Limit túllépések, törzsadat módosítások
- Korosítások
- Interfész és konverziós kontrollok
- Logikai hozzáférési kontrollok
  - Jogosultság vizsgálatok
  - 3 way match

CAATs vizsgálatok

- Nagy tömegű adat
- Teljes vizsgálat, nem mintavétel
- Interfész vizsgálat (nagyker cégeknél)
- Migráció vizsgálat
- Főkönyvi feladások újraszámolása
- Készletértékvesztés
- Bonusz kalkuláció
- Szokatlan tranzakciók (főkönyv, készlet)
- Készletmozgások vizsgálata

Tapasztalatok

Tipikus audit támogatási munkák – audit megítélése

- Általános IT kontrollok vizsgálata
  - Egyszerű
  - Kötelező gyakorlat, az audit csapat kis hozzáadott értékűnek tartja
- Folyamatfelmérések, alkalmazásba épített IT jellegű kontrollok tesztelése
  - Viszonylag egyszerű, IT miatt közepesen bonyolult
  - Szakmai tudás szükséges
  - Nagy hozzáadott érték
- Újraszámítások
  - Bonyolult
  - Maximális bizonyosság

Leggyakoribb IT hiányosságok 1

- Információbiztonság – logikai hozzáférés
  - Biztonsági adminisztráció hibái (új dolgozó, kilépő dolgozó, külső hozzáférés)
  - Jelszó hiányosságok
  - Adminisztrátori hozzáférés pénzügyi alkalmazáshoz
  - Nem egyedi azonosítók
- IT management – szabályozás
  - IT stratégia hiánya
  - IT szabályzatok hiánya
  - SLA hiánya
  - Külső szolgáltatótól való függés
  - Törvényi megfelelés biztosításának hiányosságai (13/B)

Leggyakoribb IT hiányosságok 2

- Fizikai biztonság – jogosulatlan hozzáférés
- Programváltoztatás
  - Dokumentáltság hiánya
  - Tesztelés hiánya
- Rendszerfejlesztés
  - Nem megfelelő fejlesztési módszertan
  - Dokumentáltság hiánya
  - Projekt menedzselési hiányosságok
  - Felhasználók nem megfelelő bevonása

Leggyakoribb IT hiányosságok 3

- Üzemeltetés hiányosságai
  - Mentés, visszatöltés
  - SLA szerződés hiánya
- Rendszerfolytonosság – BCP, DPR hiánya
- Belső audit
  - IT audit hiánya
  - Nem megfelelően képzett a belső ellenőr
  - Módszertan hiánya
  - Függetlenség hiánya

Összefoglalás

- Az IT audit egyre fontosabb eleme a pénzügyi auditnak
  - Az ügyfelek egyre inkább kritikus mértékben függnek az információs rendszerektől (különösen bank, biztosító)
  - Audit kockázat csökkentése
- A pénzügyi audit hatékony támogatása megköveteli, hogy annak célját tartsuk szem előtt – ezért a megközelítés eltér a szokványos IT audittól
  - A beszámoló előállításában szerepet játszó rendszerekre fókuszál
  - „IT jellegű” kontrollok
  - Folyamatok – kontroll megközelítés
  - Újraszámítások

Kérdések

Az itt megjelölt információk tájékoztató jellegűek, és nem vonatkoznak valamely meghatározott természetes vagy jogi személy, illetve jogi személyiség nélküli szervezet körülményeire. A Társaság ugyan törekszik pontos és időszerű információkat közölni, ennek ellenére nem vállal felelősséget a közölt információk jelenlegi vagy jövőbeli hatályosságáért. A Társaság nem vállal felelősséget az olyan tevékenységből eredő károkért, amelyek az itt közölt információk felhasználásából erednek, és nélkülözik a Társaságnak az adott esetre vonatkozó teljes körű vizsgálatát és az azon alapuló megfelelő szaktanácsadást.