Kiszervezett szolgáltatások ellenőrzési és irányítási eljárásainak javítása

Ivanyos János, Memolux Kft.

Dr. Biró Miklós – Budapesti Corvinus Egyetem

Tartalom

- Kontroll és Érettségi modellek
- Külső követelmények
- Megfelelés (Compliance) és Üzleti érték (Business Value)
- Kockázat alapú elemzések (Control and Risk Self Assessment)
- Kulcs kontroll folyamatok (Key Control Processes)
- Eredményesség mérése (Effectiveness Conclusion)
- Eredmények bemutatása, külső audit támogatása
- ISO 15504 konform COSO alapú folyamat-felmérési modell

Kontroll Modellek

- COSO
- COBIT
- COSO ERM
- Stb. (CoCo, Turnbull, ISO9001, …)

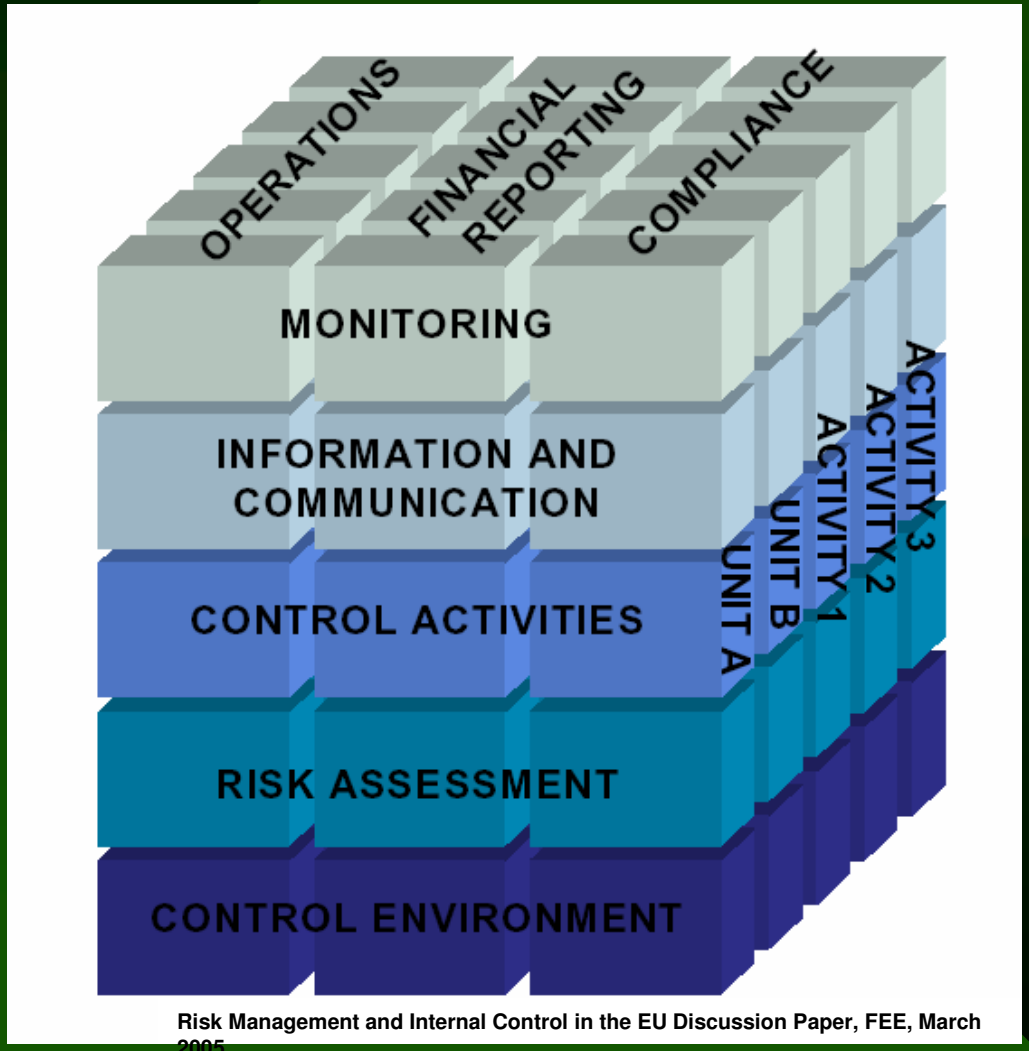
Internal Control - definíció

A ***process*** effected by an entity's Board of Directors, management and other personnel, designed to provide ***reasonable assurance*** regarding the ***achievement of objectives*** in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations
- Safeguarding of assets

COSO Definition

Kontroll modellek:
COSO Keretrendszer

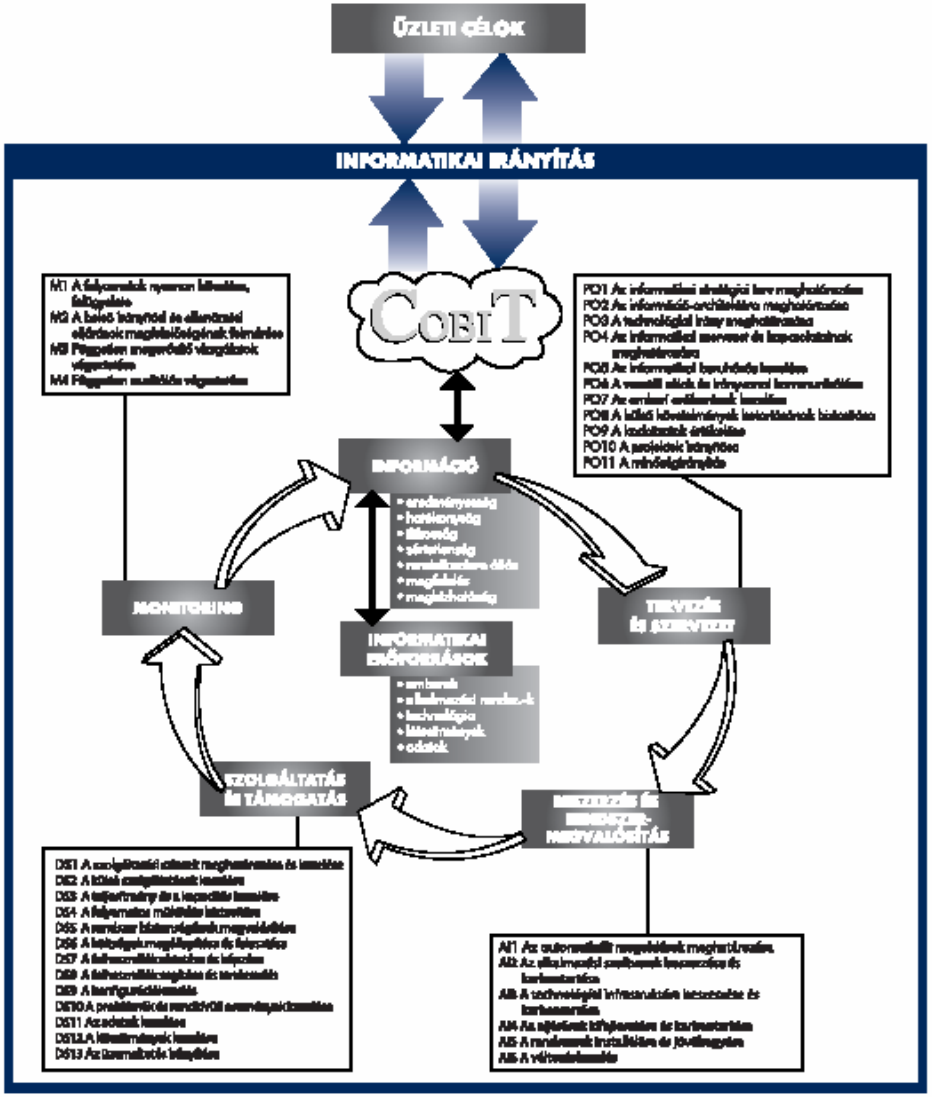


Risk Management and Internal Control in the EU Discussion Paper, FEE, March 2005

- 3 kategória
- 5 komponens

=>tevékenység

Kontroll modellek:
COBIT



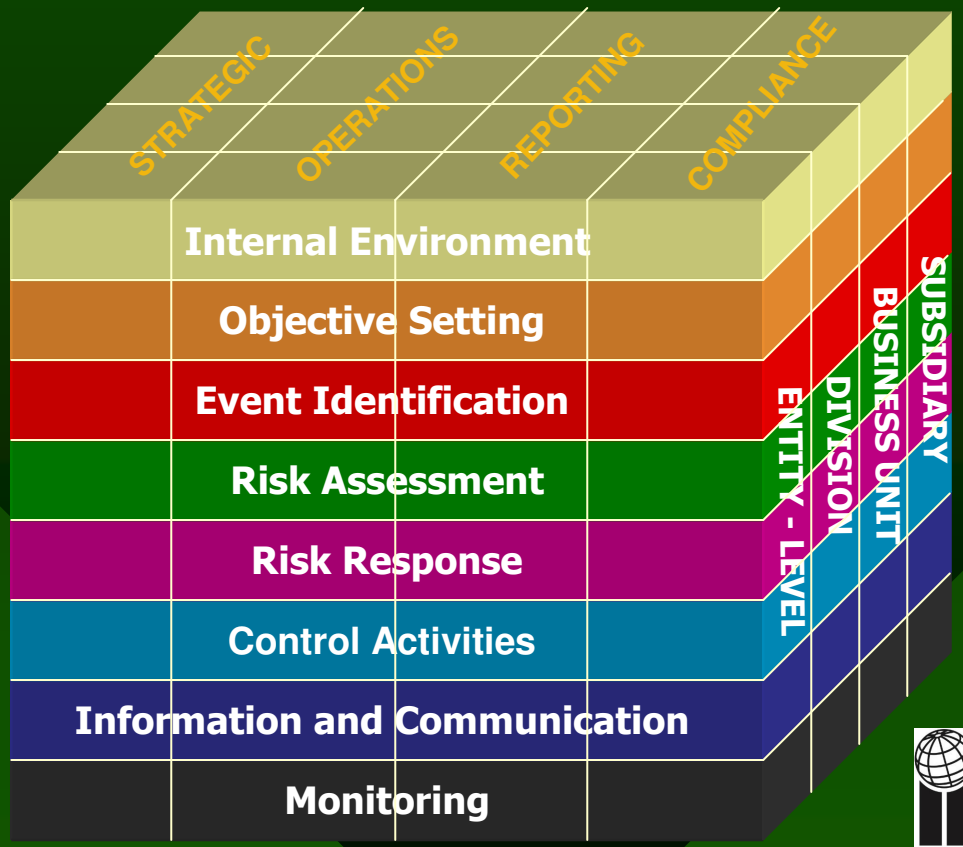
- 4 terület
- 34 kulcs folyamat
- 7 kritérium
- 5 IT erőforrás

300< részletes kontroll célkitűzés

Kontroll modellek:
COSO ERM

- 4 kategória
- 8 komponens

=> Szervezeti egység



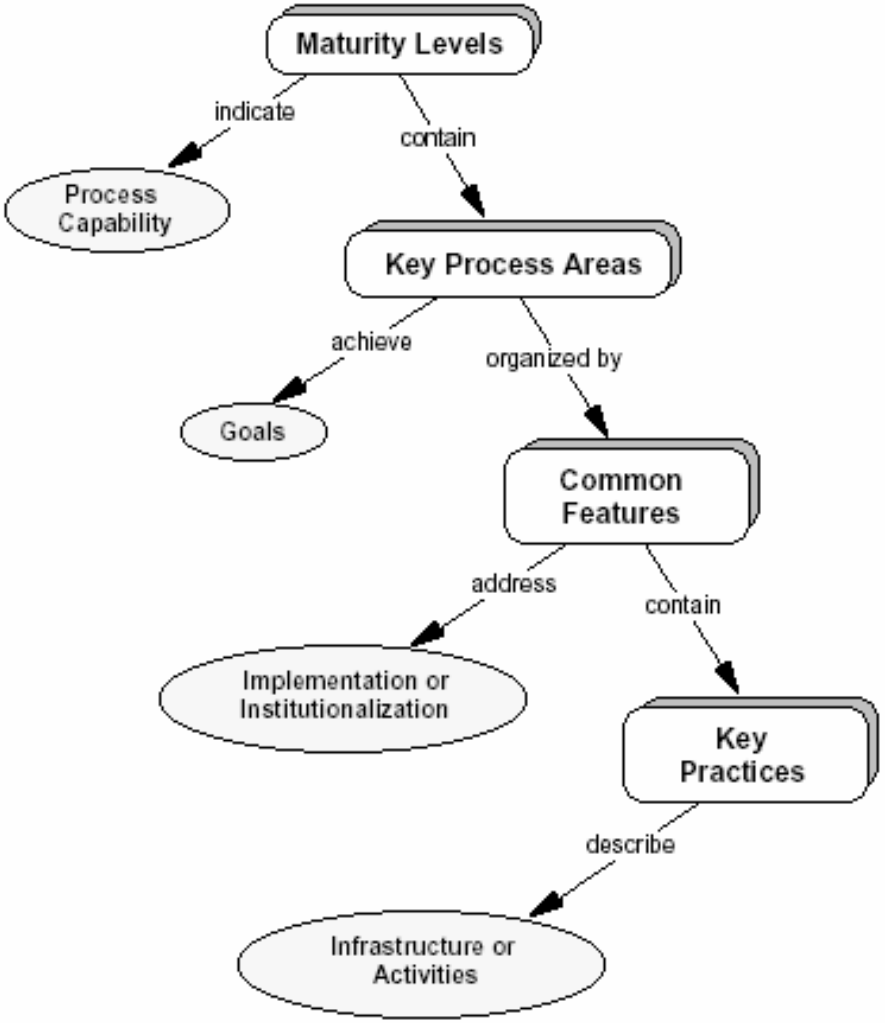
Kontroll modellek:
Implementálási nehézségek

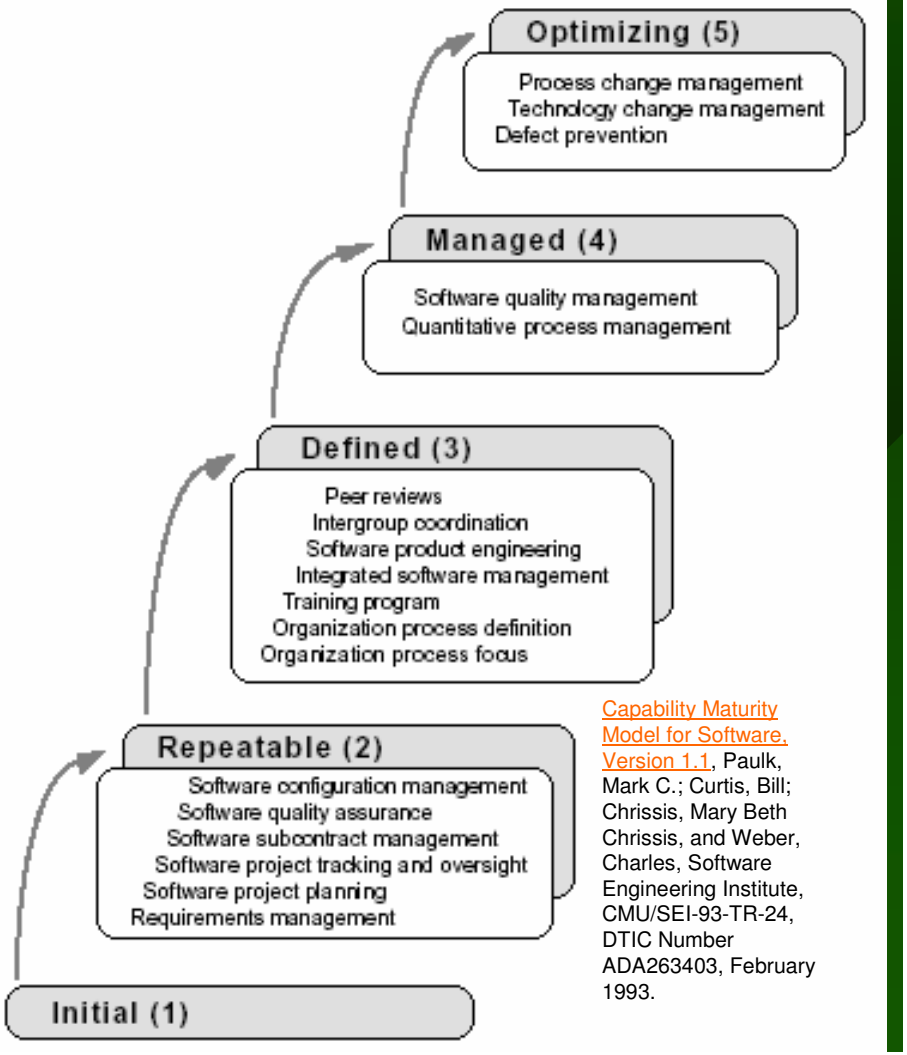
- A modellek túl bonyolultak
- A vezetés tudása és elkötelezettsége „hiányos”
- Nehéz kapcsolatot találni az üzleti eredmény mutatóihoz: „Ha nem megy a bolt, akkor nincs rá anyagi fedezet, ha megy a bolt, akkor minek?”
- A megvalósítás külső támogatást igényel (drága)
- Ki hiszi el nekünk? (auditor, befektető,…)

Érettségi modellek

- CMM(s)
- eSCM(s)
- COBIT(!)
- ISO 15504

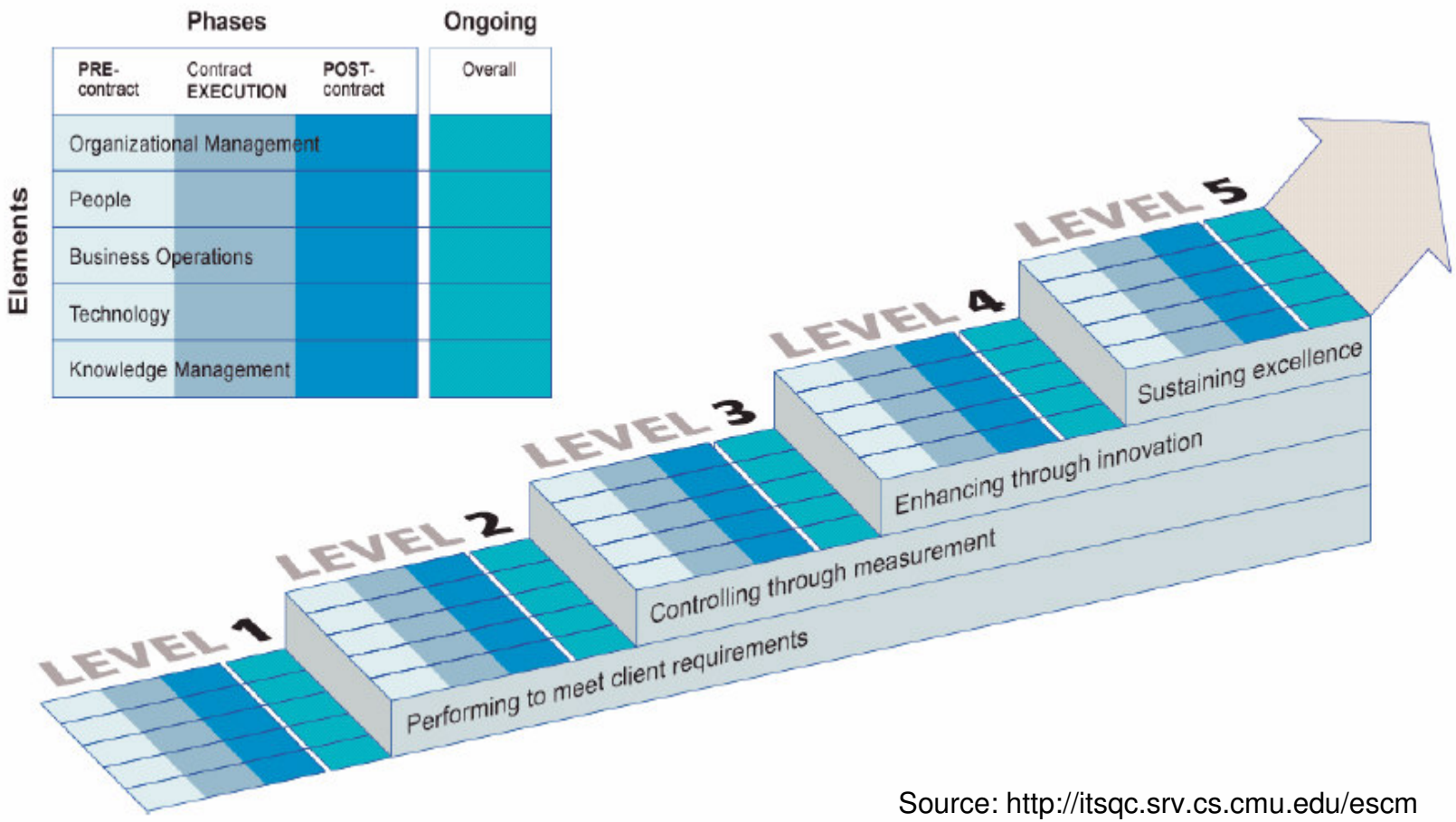
Érettségi modellek:
Capability Maturity Models®





Capability Maturity Model for Software, Version 1.1, Paulk, Mark C.; Curtis, Bill; Chrissis, Mary Beth Chrissis, and Weber, Charles, Software Engineering Institute, CMU/SEI-93-TR-24, DTIC Number ADA263403, February 1993.

Érettségi modellek:
The eSourcing Capability Model



Source: http://itsqc.srv.cs.cmu.edu/escm

Érettségi modellek:
COBIT

Table 1—Maturity Levels

0—Non-existent	Management processes are not applied at all.
1—Initial	Processes are *ad hoc* and disorganized.
2—Repeatable	Processes follow a regular pattern.
3—Defined	Processes are documented and communicated.
4—Managed	Processes are monitored and measured.
5—Optimised	Best practices are followed and automated.

Table 2—Fifteen Most Important Processes of COBIT

PO1	Define a strategic IT plan
PO3	Determine technological direction
PO5	Manage the IT investment
PO9	Assess risks
PO10	Manage projects
AI1	Identify automated solutions
AI2	Acquire and maintain application software
AI5	Install and accredit systems
AI6	Manage changes
DS1	Define and manage service levels
DS4	Ensure continuous service
DS5	Ensure systems security
DS10	Manage problems and incidents
DS11	Manage data
M1	Monitor the process

The left column refers to the domains in which the processes are classified: PO = Planning and Organisation, AI = Acquisition and Implementation, DS = Delivery and Support, M = Monitoring.

Figure 1—Respondents by Location, Size and Sector

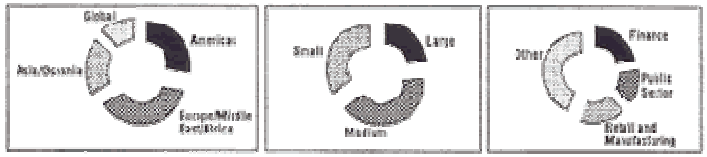
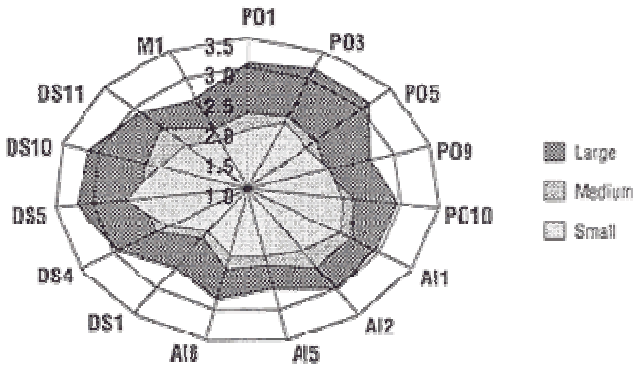


Figure 3—Results by Size

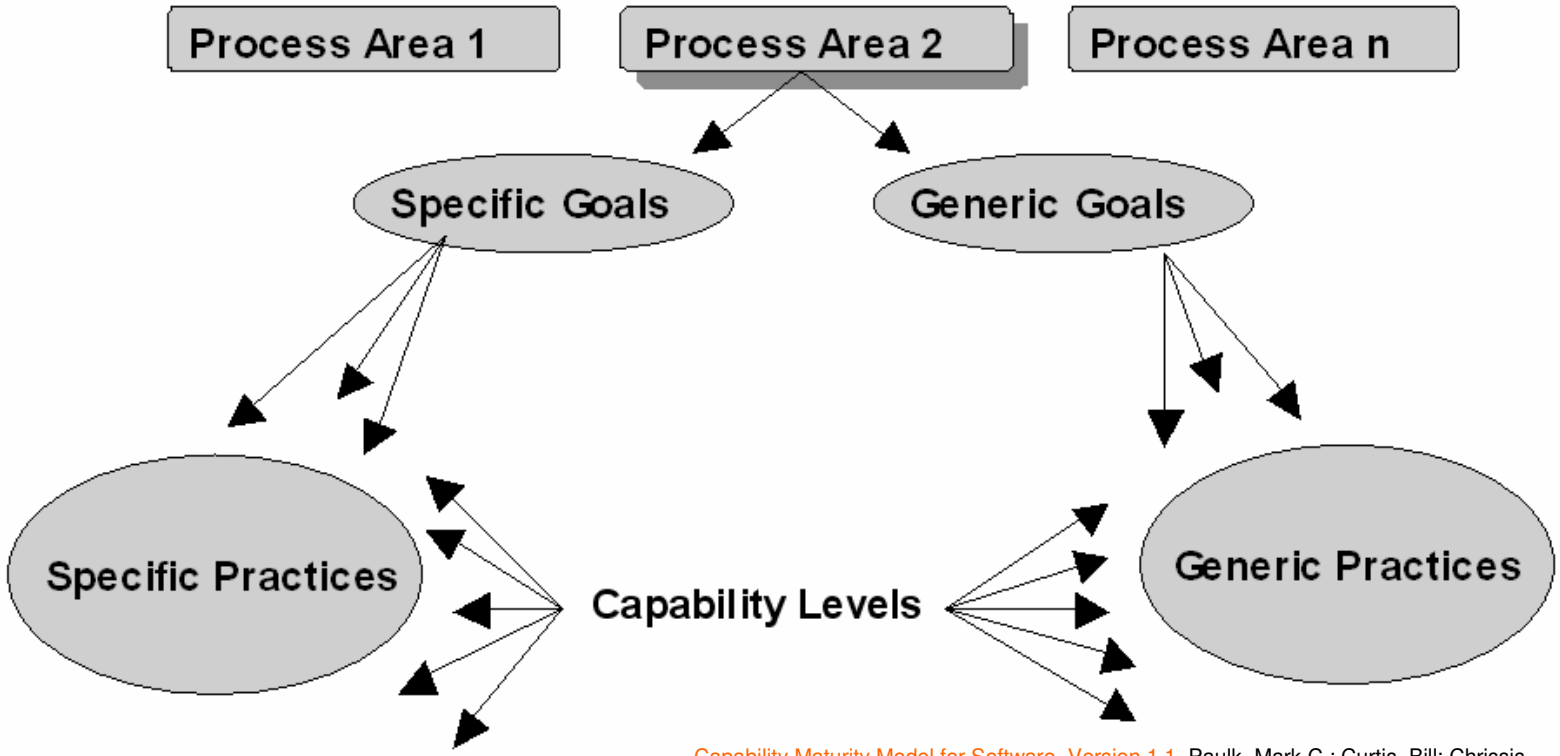


Information Systems Control Journal, Volume 6, 2002

Control and Governance Maturity Survey: Establishing a Reference Benchmark and a Self-assessment Tool

By Erik Guldentops, CISA, Wim Van Grembergen, Ph.D., and Steven De Haes

Érettségi modellek:
A (kontroll) folyamatok jellemzői érettségi szintenként meghatározhatóak (súlyozhatóak)



Capability Maturity Model for Software, Version 1.1, Paulk, Mark C.; Curtis, Bill; Chrissis, Mary Beth Chrissis, and Weber, Charles, Software Engineering Institute, CMU/SEI-93-TR-24, DTIC Number ADA263403, February 1993.

2005. június

MAGYAR SZABVÁNY MSZ ISO/IEC 15504-2

Informatika. Folyamatfelmérés

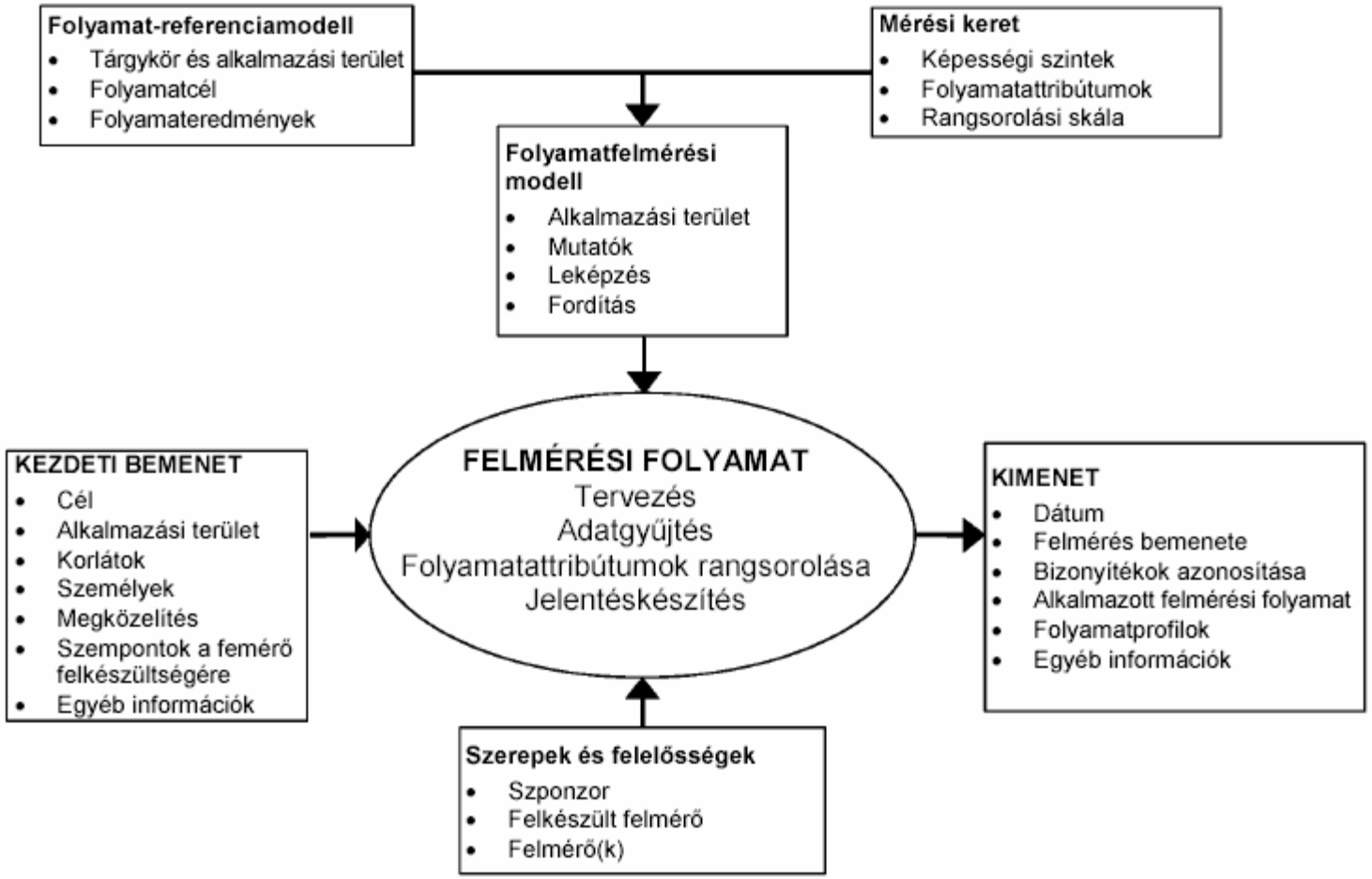
2. rész: A felmérés végrehajtása

Information technology. Process assessment.
Part 2: Performing an assessment

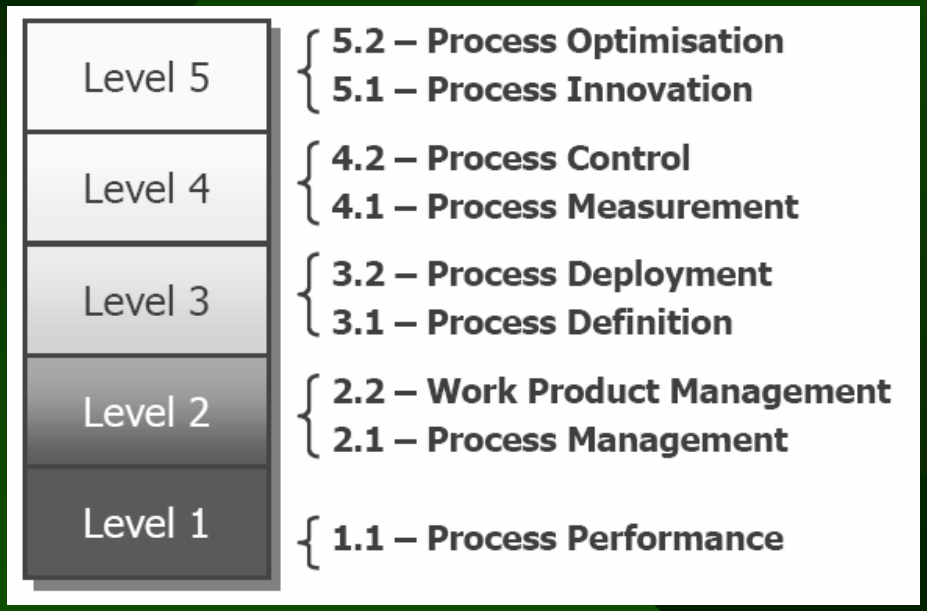
Ez a magyar nemzeti szabvány teljesen megegyezik az ISO/IEC 15504-2:2003 nemzetközi szabvánnyal és tartalmazza annak ISO/IEC 15504-2:2003/Cor.1:2004 műszaki helyesbítését is.

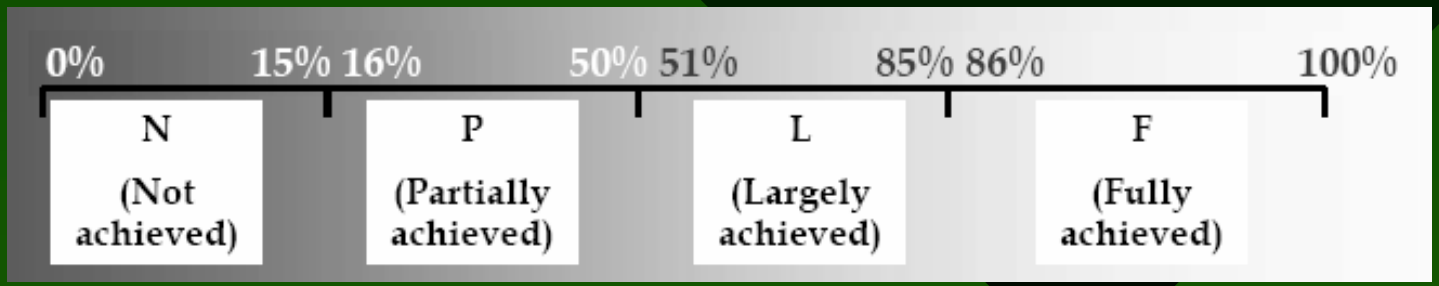
This Hungarian National Standard is identical with the International Standard ISO/IEC 15504-2:2003 and includes its Technical Corrigendum ISO/IEC 15504-2:2003/Cor.1:2004 too.

ISO/IEC 15504 A folyamatfelmérés nemzetközi szabványa



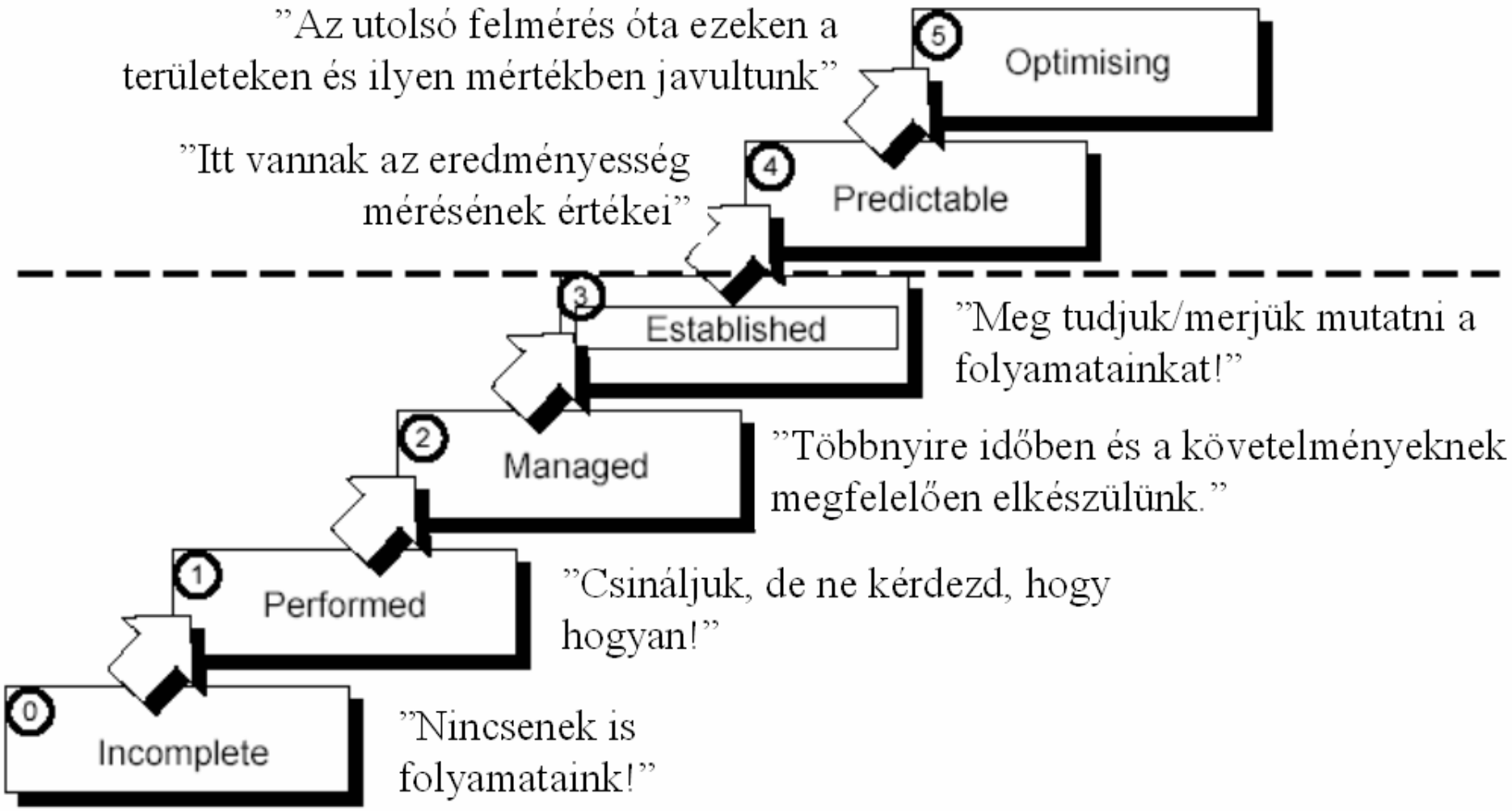
ISO 15504 Mérési keretrendszer





1. táblázat: A képességi szint rangsorolása

Szint	Folyamatattribútumok	Rangsorolás
1. szint	Folyamat-végrehajtás	Nagyjából vagy hiánytalanul
2. szint	Folyamat-végrehajtás	Hiánytalanul
	Végrehajtás-irányítás	Nagyjából vagy hiánytalanul
	Munkatermék-kezelés	Nagyjából vagy hiánytalanul
3. szint	Folyamat-végrehajtás	Hiánytalanul
	Végrehajtás-irányítás	Hiánytalanul
	Munkatermék-kezelés	Hiánytalanul
	Folyamatmeghatározás	Nagyjából vagy hiánytalanul
	Folyamatalkalmazás	Nagyjából vagy hiánytalanul
4. szint	Folyamat-végrehajtás	Hiánytalanul
	Végrehajtás-irányítás	Hiánytalanul
	Munkatermék-kezelés	Hiánytalanul
	Folyamatmeghatározás	Hiánytalanul
	Folyamatalkalmazás	Hiánytalanul
	Folyamatmérés	Nagyjából vagy hiánytalanul
	Folyamatellenőrzés	Nagyjából vagy hiánytalanul
5. szint	Folyamat-végrehajtás	Hiánytalanul
	Végrehajtás-irányítás	Hiánytalanul
	Munkatermék-kezelés	Hiánytalanul
	Folyamatmeghatározás	Hiánytalanul
	Folyamatalkalmazás	Hiánytalanul
	Folyamatmérés	Hiánytalanul
	Folyamatellenőrzés	Hiánytalanul
	Folyamatinnováció	Nagyjából vagy hiánytalanul
	Folyamatoptimalizáció	Nagyjából vagy hiánytalanul


”Az utolsó felmérés óta ezeken a területeken és ilyen mértékben javultunk”
5
Optimising
”Itt vannak az eredményesség mérésének értékei”
4
Predictable
3
Established
”Meg tudjuk/merjük mutatni a folyamatainkat!”
2
Managed
”Többnyire időben és a követelményeknek megfelelően elkészülünk.”
1
Performed
”Csináljuk, de ne kérdezd, hogy hogyan!”
0
Incomplete
”Nincsenek is folyamataink!”

Érettségi modellek előnyei

- Közérthetőek (szöveges leírás)
- Gyenge és erős pontok bemutatása
- Bármikor, önállóan is használhatóak (self-assessment)
- Összehasonlíthatóság (benchmarking)
- Testreszabhatóság (iparág, méret, tulajdonos, stb. szerint)
- A folyamatjavítás következő lépései könnyen meghatározhatók
- Nem (feltétlenül) igényelnek külső szakértőket

Külső követelmények

- SOX
- Tervezett EU Direktívák

  (Corporate Governance kiterjesztése)
- Felelős Vállalatirányítási Ajánlások, Basel II, …
- Nemzeti szabályozások (pl. 193/2003 Korm. rendelet)

Külső követelmények

Példa:Informatikai megfelelőségi követelmények köre folyamatosan bővül

LHS

Compliance Requirement Is Increasingly Severe

- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Computer Misuse act 1990
- E-commerce Regulations 2002
- Human Rights Act 1998
- Copyright. Designs & Patents Act 2002
- Freedom of Information act 2000
- Anti-money laundering (Criminal Justice Act 1998, Drug Trafficking Justice Act 1994, Terrorism Act 2000)
- Financial Services Authority and Markets Act 2000
- International Financial Reporting standards
- Information Commissioner's Code on Employer's Monitoring Practices
- Basel II Accord
- EU Directive on Privacy and Electronic Communications 2003
- EU Insurance Mediation Directive
- EU Directive on Data Protection
- US Sarbanes-Oxley Act

Külső követelmények:
Sarbanes-Oxley

			Types of risk		
			Financial reporting	Compliance	Operational and strategic
Types of activity	Manage risks	Identify and evaluate	✓		
		Respond	✓		
		Conclude on effectiveness	✓		
	Disclose	Overall process			
		Management of specific risks			
		Effectiveness conclusion	✓		

Risk Management and Internal Control in the EU Discussion Paper, FEE, March 2005

Külső követelmények:
EU 8. Direktíva módosítása
(Proposed Directive on Statutory Audit requirements)

			Types of risk		
			Financial reporting	Compliance	Operational and strategic
Types of activity	Manage risks	Identify and evaluate	✓	✓	✓
		Respond	✓	✓	✓
		Conclude on effectiveness	✓	✓	✓
	Disclose	Overall process			
		Management of specific risks			
		Effectiveness conclusion			

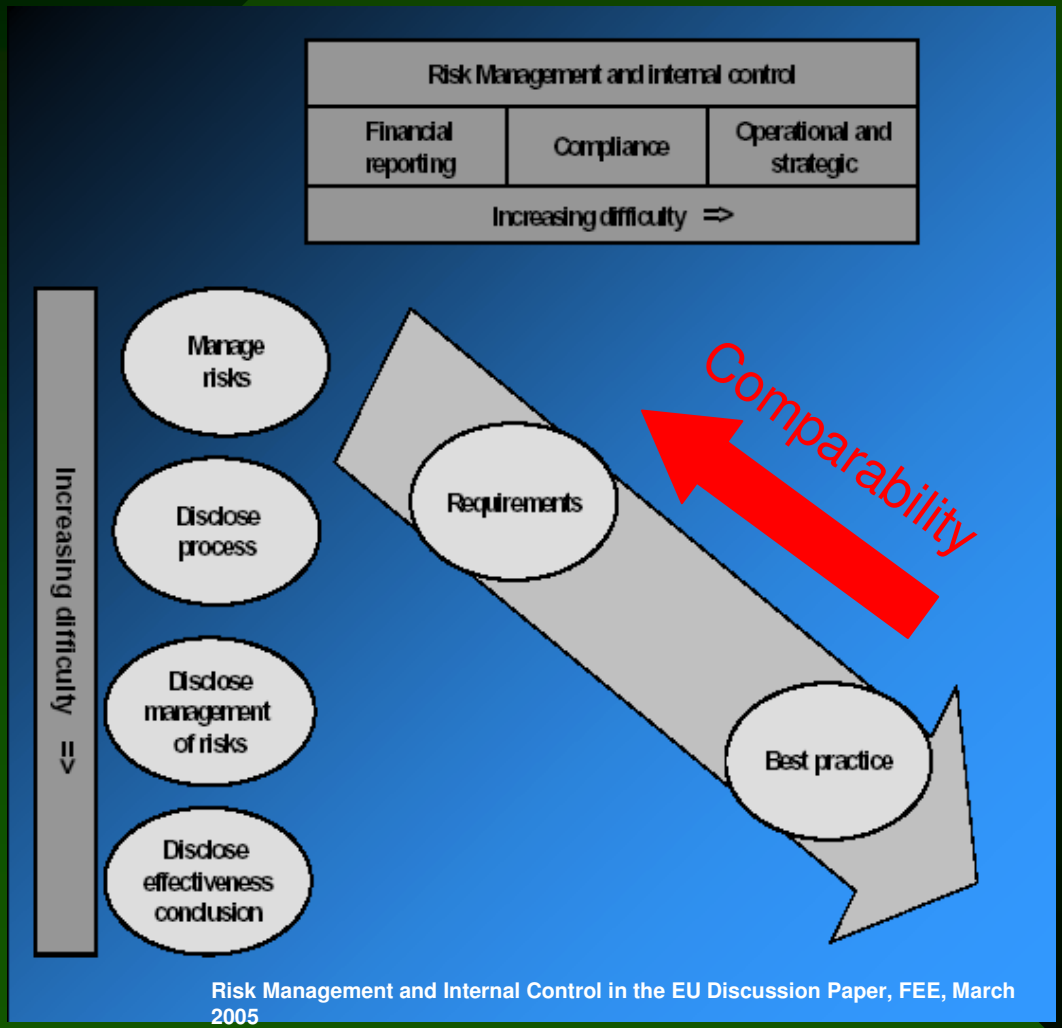
Risk Management and Internal Control in the EU Discussion Paper, FEE, March 2005

Külső követelmények:
Felelős Vállalatirányítás
Proposed Fourth and Seventh Directives requirements (corporate governance statement)

			Types of risk		
			Financial reporting	Compliance	Operational and strategic
Types of activity	Manage risks	Identify and evaluate			
		Respond			
		Conclude on effectiveness			
	Disclose	Overall process	✓		
		Management of specific risks			
		Effectiveness conclusion			

Risk Management and Internal Control in the EU Discussion Paper, FEE, March 2005

Külső követelmények:
Folyamatos (evolúciós) fejlődés



Risk Management and Internal Control in the EU Discussion Paper, FEE, March 2005

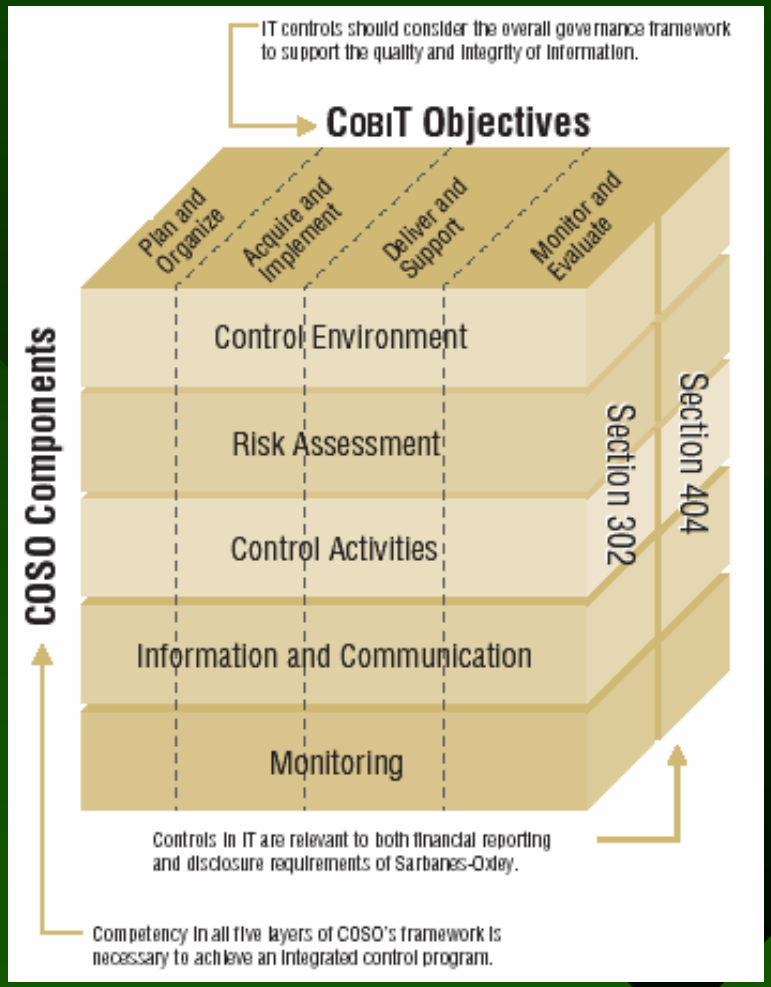
Megfelelés és Üzleti érték

- COSO és IT kontrollok alkalmazása a SOX megfeleléshez
- Kontroll megbízhatóság és Üzleti érték

  (Control reliability and Busines Value)
- Fenntarthatóság és Érettség

  (Sustainability and Maturity)
- Sikertényezők

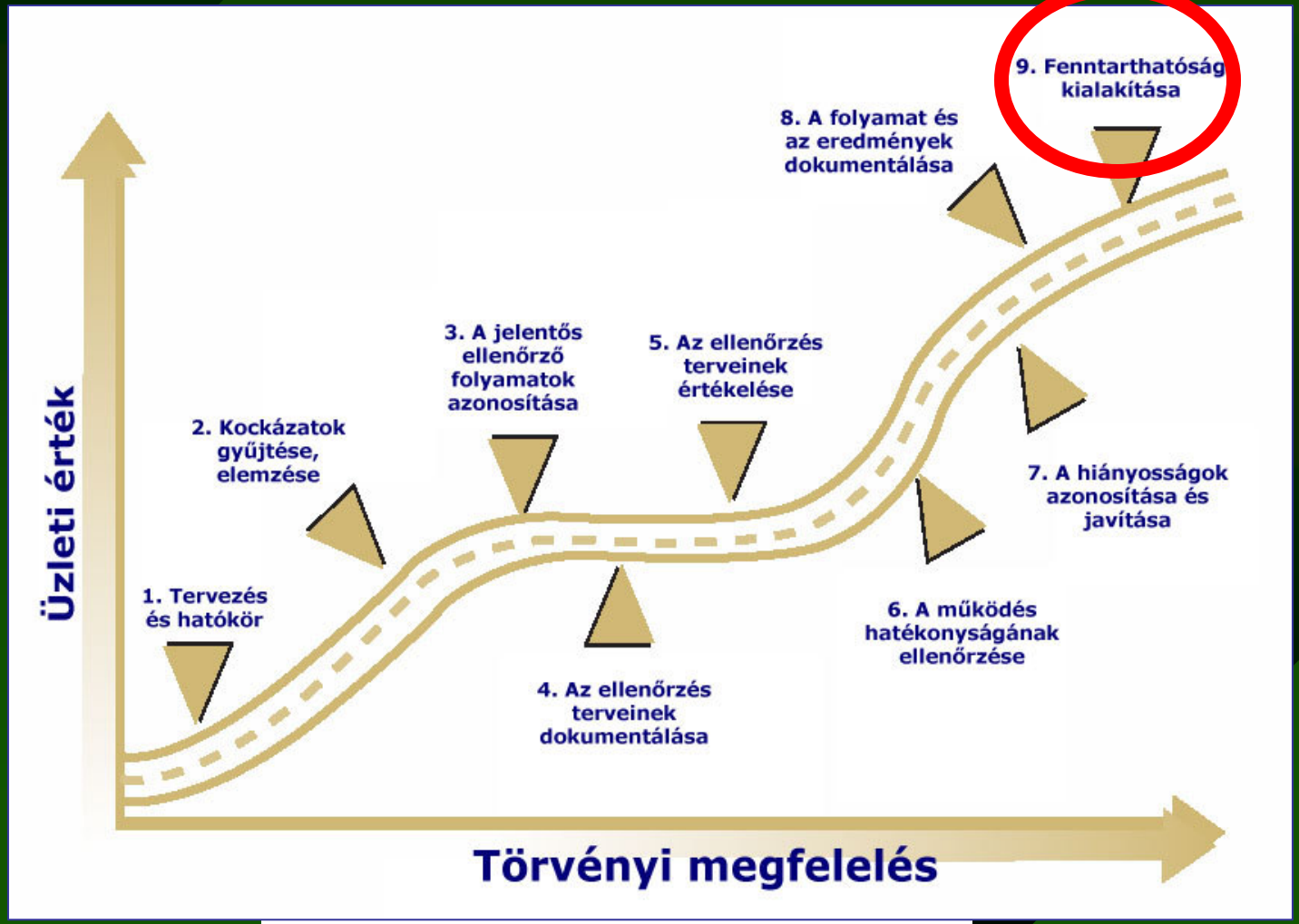
Kontroll modellek alkalmazása:
COSO és IT kontrollok alkalmazása SOX megfeleléshez



IT Control Objectives for Sarbanes-Oxley

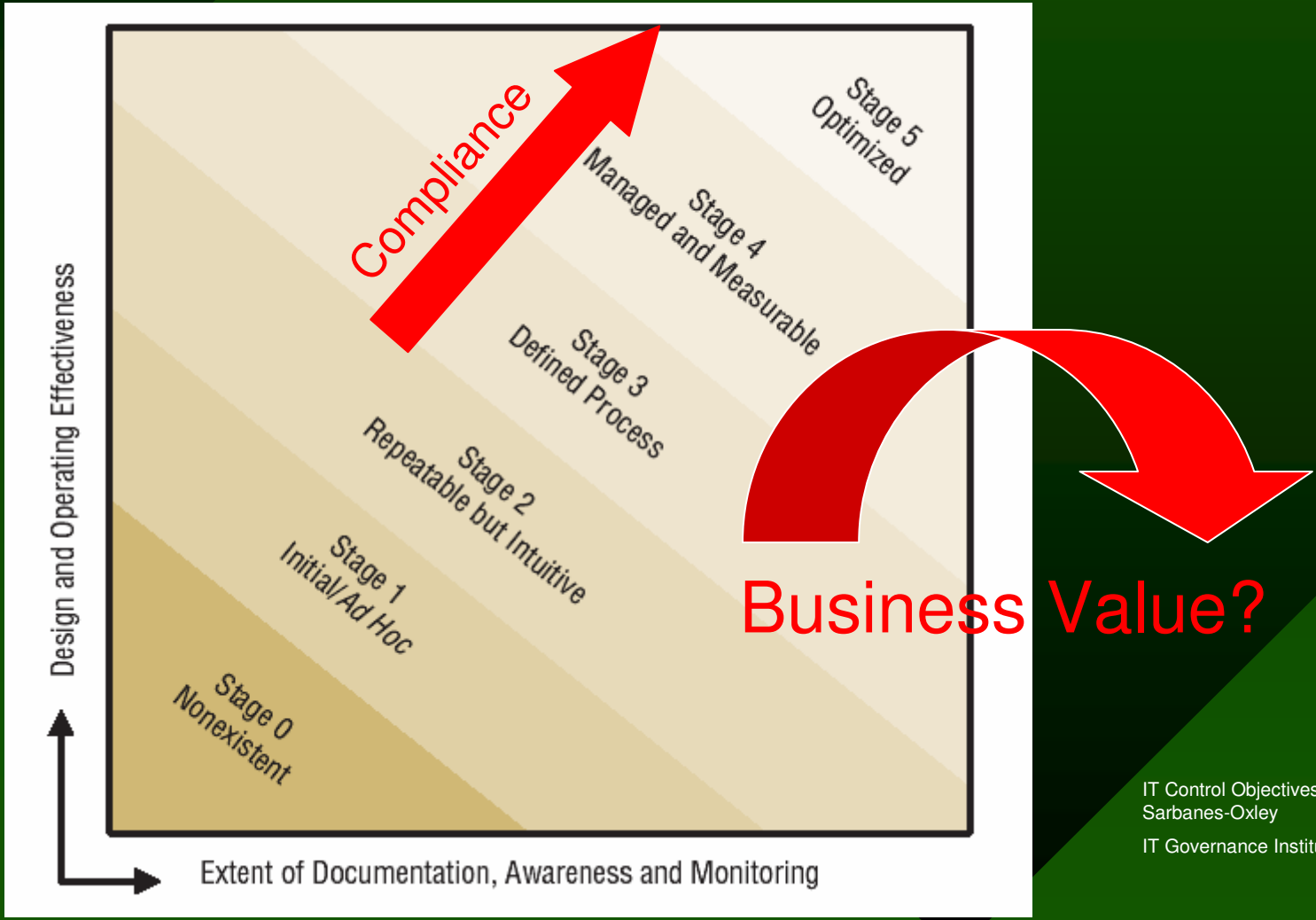
IT Governance Institute, 2004

Kontroll modellek alkalmazása:
Megvalósítási útvonal - elméletben



IT Control Objectives for Sarbanes-Oxley, IT Governance Institute, 2004

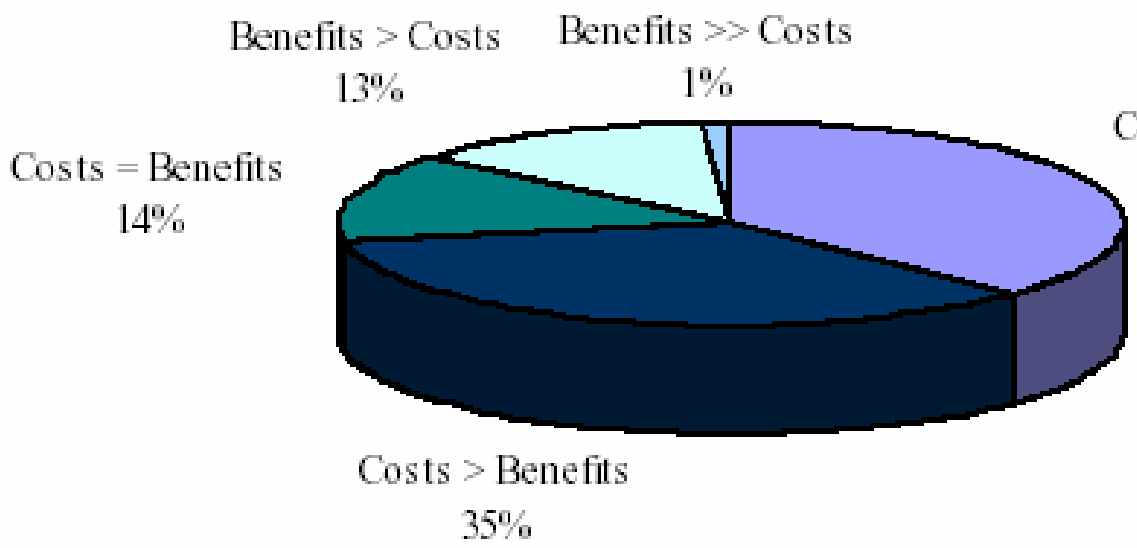
Kontroll modellek alkalmazása:
Kontroll megbízhatóság és Üzleti érték



IT Control Objectives for Sarbanes-Oxley

IT Governance Institute, 2004

Kontroll modellek alkalmazása:
SOX: A felkészülés költségei és a haszon



Sarbanes-Oxley Section 404 Work: Looking at the Benefits

January 2005

The IIA Research Foundation

Kontroll modellek alkalmazása:
SOX: Költség/Haszon várakozások

Relationship of Cost of Readiness Activities and Benefits

	First Year -- Readiness Effort		Looking Forward to Steady State of Control Assessments	
Costs Greatly Exceed Benefits	37%		6%	
Costs Exceed Benefits	35%		30%	
Costs Equal Benefits	14%		25%	
Benefits Exceed Costs	13%	28%	31%	64%
Benefits Greatly Exceed Costs	1%		8%	

Sarbanes-Oxley Section 404 Work: Looking at the Benefits, January 2005

The IIA Research Foundation

Kontroll modellek alkalmazása:
Kontroll megbízhatóság és fenntarthatóság

	0. szint - Kaotikus	1. szint - Kezdetleges	2. szint - Megismételhető	3. szint - Meghatározott	4. szint - Menedzselt	5. szint - Optimalizált
Jellemzők	Nincs felismerhető kontroll folyamat vagy kapcsolódó eljárás. A szervezet még fel sem ismerte ezek hiányát, ezért szóba sem kerül ez a kérdés.	Felismerte a szervezet a kontroll folyamatok és kapcsolódó eljárások jelentőségét, és annak szükségességét, hogy ezzel foglalkozni kell. Azonban nincsenek kontrollok, kapcsolódó szabályok és eljárások. Esemény kezelési és közzétételi folyamat nem létezik. Az alkalmazottak nem ismerték fel a kontroll folyamatokban játszott felelősségüket. A kontroll tevékenységek működési hatékonyságát nem értékelik rendszeresen. A kontroll hiányosságokat nem tárják fel.	Léteznek kontrollok, kapcsolódó szabályok és eljárások, de nem mind dokumentált. Létezik esemény kezelő és közzétételi folyamat, de nem dokumentált. Előfordul, hogy az alkalmazottak nem ismerik fel a kontroll folyamatokban játszott felelősségüket. A kontroll tevékenységek működési hatékonyságának rendszeres értékelése nem megfelelő és a folyamat nem dokumentált. A kontroll hiányosságokat feltárják, de nem orvosolják kellő időben.	Léteznek kontrollok, kapcsolódó szabályok és eljárások, és dokumentáltak. Létezik esemény kezelő és közzétételi folyamat, és dokumentált. Az alkalmazottak felismerik a kontroll folyamatokban játszott felelősségüket. A kontroll tevékenységek működési hatékonyságát rendszeresen értékelik, de a folyamat nem teljesen dokumentált. A kontroll hiányosságokat feltárják, és kellő időben orvosolják.	Léteznek kontrollok, kapcsolódó szabályok és eljárások, és dokumentáltak. Az alkalmazottak felismerik a kontroll folyamatokban játszott felelősségüket. Létezik esemény kezelő és közzétételi folyamat, dokumentált és monitorozott, de nem értékelik újra a változások tükrében. A kontroll tevékenységek működési hatékonyságát rendszeresen értékelik, és a folyamat teljesen dokumentált. A folyamatok, kontroll célok és tevékenységek dokumentálására korlátozottan használják a technológiát.	Olyan "enterprisewide control and risk management" program valósul meg, melyben a kontrollok és folyamatok jól dokumentáltak és folyamatosan felülvizsgálatra kerülnek, reagálva a lényeges folyamatokban bekövetkező, illetve a szervezeti változásokra. Létezik önértékelési folyamat a kontrollok tervezésének és eredményességének kiértékelésére. Információ-technológia lehetőségeit teljesen kiaknázzák a folyamatok, a kontroll célok és tevékenységek dokumentálására, a hiányosságok azonosítására, továbbá a kontrollok eredményességének kiértékelésre.

IT Control Objectives for Sarbanes-Oxley

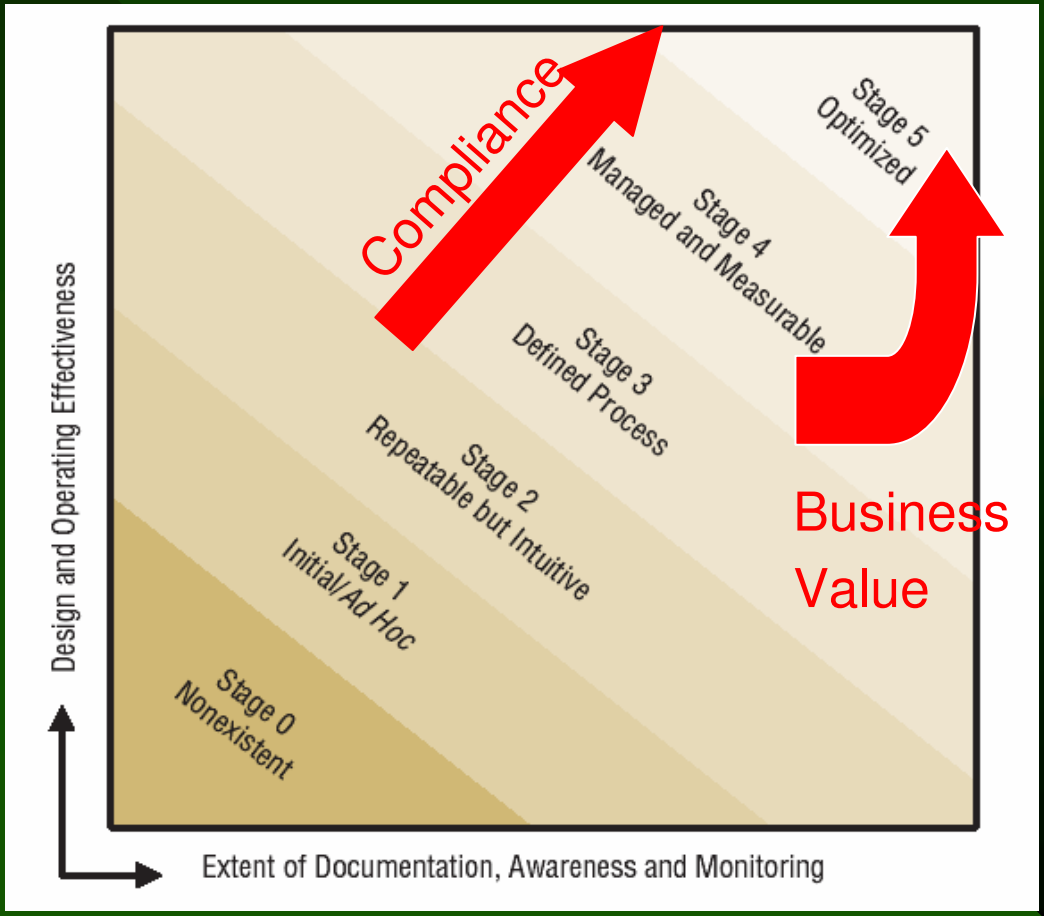
IT Governance Institute, 2004

Kontroll modellek alkalmazása:
Kontroll megbízhatóság és fenntarthatóság

	0. szint - Kaotikus	1. szint - Kezdetleges	2. szint - Megismételhető	3. szint - Meghatározott	4. szint - Menedzselt	5. szint - Optimalizált
Következmények	A szervezet még egy minimális szinten sem képes megfelelni a jogszabályi kötelezettségeknek.	Nem elegendők a létező kontrollok, szabályok, eljárások és dokumentálás ahhoz, hogy képes legyen alátámasztani a vezetőség megállapításait. A dokumentálás, ellenőrzés és helyesbítő kontrollok nagyon magas erőforrás-igényűek.	Habár léteznek kontrollok, kapcsolódó szabályok és eljárások, de nem elégséges a dokumentálás mértéke ahhoz, hogy képes legyen alátámasztani a vezetőség megállapításait. A dokumentálás, ellenőrzés és helyesbítő kontrollok magas erőforrás-igényűek.	Elégséges mértékű dokumentáció támasztja alá a vezetőség megállapításait. A dokumentálás, ellenőrzés és helyesbítő kontrollok erőforrás-igénye jelentős lehet a szervezet körülményeitől függően.	Elégséges mértékű dokumentáció támasztja alá a vezetőség megállapításait. A dokumentálás, ellenőrzés és helyesbítő kontrollok erőforrás-igénye lényegesen kisebb lehet a szervezet körülményeitől függően.	A 4. szintű következmények mellett: A minőségi és gyors információ következtében fejlett döntéshozó rendszer hozható létre. A belső erőforrásokat hatékonyan és eredményesen használja fel. Az információ aktuális és megbízható.

IT Control Objectives for Sarbanes-Oxley, IT Governance Institute, 2004

Kontroll modellek alkalmazása:
Fenntarthatóság sikertényezői:
ERM + CRSA + Technology



IT Control Objectives for Sarbanes-Oxley

IT Governance Institute, 2004

Kockázat alapú elemzések:
Példa: Bérszámfejtés outsourcing – folyamatok

BÉRSZÁMFEJTÉS

- Bér és munkaügyi változások
- Munkaidő adatok kezelése
- TB ügyintézés
- Számfejtés
- Banki és postai utalás
- Kapcsolattartás

HR

- Dolgozói állomány változások
- Jelenlét nyilvántartás kezelése
- Kifizetések kezdeményezése
- Kapcsolattartás

ZÁRÁS

- Éves SZJA ügyintézés
- Adóév zárása
- Új év nyitása
- Kapcsolattartás

IRÁNYÍTÁS

- SLA kezelése
- Éves ütemezés kezelése
- Új igények kezelése
- Problémák kezelése
- Kapcsolattartás

Kockázat alapú elemzések:
Példa: Bérszámfejtés outsourcing – testre szabott kontroll célok

A bérszámfejtési folyamatok értékelése során a COSO ERM-Integrated Framework általános kontroll területeit (Strategic, Operations, Reporting, Compliance) 5 (testre szabott) kontroll cél szempontjából vizsgáljuk:

- **célszerű** (üzleti célokat támogató, hatékony és eredményes működést biztosító)
- **szabályszerű** (jogszabályoknak és más rendelkezéseknek megfelel)
- **hibátlan** (pontos, teljeskörű, helyes besorolású - időszakra és más kategóriákba)
- **megalapozott** (valós adatokon és dokumentumokon alapul, bizonyítottan helyes módszereket alkalmazó)
- **védett** (engedélyezett, felelősségkör szerint megosztott, a vagyontárgyak védettek, a megkívánt logikai és fizikai biztonsági védelem megvalósul)

Kockázat alapú elemzések:
Példa: Bérszámfejtés outsourcing – megállapítások

BÉRSZÁMFEJTÉSI RÉSZFOLYAMATOK	KONTROLL CÉLOK: Célszerű	Szabályszerű	Hibátlan	Megalapozott	Védett
Bér és munkaügyi változások	✓	✓	✗		✓
Munkaidő adatok kezelése	✗		✗	✗	✓
TB ügyintézés	✓		✓		✓
Számfejtés	✗	✗	✓	✓	✓
Banki utalás	✗	✓	✓	✗	✓
Adatszolgáltatás a számfejtett bérről	✗	✓	✓	✗	✓
Adatkapcsolat a könyveléssel	✓	✓	✗	✓	✓
Személyes kapcsolattartás	✓	✗	✗	✗	✓

Jelmagyarázat:

kritikus | jelentős | nem fontos | ✓ megfelelő | ✗ hiányos

Kockázat alapú elemzések:

Példa: Bérszámfejtés outsourcing – részfolyamatok

BÉRSZÁMFEJTÉS

- Bér és munkaügyi változások
- Munkaidő adatok kezelése
- TB ügyintézés
- Számfejtés
- Banki és postai utalás
- Kapcsolattartás

HR

- Dolgozói állomány változások
- Jelenlét nyilvántartás kezelése
- Kifizetések kezdeményezése
- Kapcsolattartás

ZÁRÁS

- Éves SZJA ügyintézés
- Adóév zárása
- Új év nyitása
- Kapcsolattartás

IRÁNYÍTÁS

- SLA kezelése
- Éves ütemezés kezelése
- Új igények kezelése
- Problémák kezelése
- Kapcsolattartás

MUNKAIDŐ ADATOK KEZELÉSE

- Munkaidő adatok megadása
- Munkaidő adatok továbbítása
- Munkaidő adatok módosítása
- Munkaidő adatok jóváhagyása
- Munkaidő adatok feldolgozása
- Hibalisták készítése
- Riportok készítése

Kockázat alapú elemzések:

Példa: Bérszámfejtés outsourcing – felülvizsgálandó kontroll követelmények ↔ szabályszerűség ellenőrzése

Részfolyamat	Tevékenység	Kontroll követelmény
Munkaidő adatok kezelése	***Alapadatok rögzítése***	■ Minden alapadat a keletkezéséhez legközelebbi helyen kerüljön rögzítésre. ■ Az alapadatok bizonylatait őrizzék meg.
	Alapadatok továbbítása	■ Az adat tulajdonosa ellenőrizze, hagyja jóvá és továbbítsa a rögzített adatokat. ■ Az adatok továbbítása az ütemezés szerint történjen. ■ Az adattovábbítás védett csatornán történjen.
	Alapadatok módosítása	■ Az adatmódosítás kérésére jogosultak köre rögzített legyen. ■ A bérszámfejtő csak egyértelmű és hivatalos adatközlés nyomán változtathassa meg a rögzített alapadatokat, erről értesítse az adat tulajdonosát. ■ Minden adat-karbantartási tevékenység nyomon-követhető és visszakereshető legyen.
	Alapadatok feldolgozása	■ Az adatok feldolgozása az ütemezés szerint történjen. ■ Minden feldolgozási tevékenység nyomon-követhető és visszakereshető legyen.
	Eredmény lekérése …	■ Az adat tulajdonosa értesüljön a feldolgozás elvégzéséről. ■ Az adat tulajdonosa hozzáférjen a feldolgozás eredményéhez.

Kulcs kontroll folyamatok

- Kulcs kontrollok (Key Controls)
- Kulcs kontroll folyamat megvalósítása
- Verifikálás

Kulcs kontroll folyamatok:
Kulcs kontrollok

- **Kulcs kontrollok** definíciója (IIA Research Foundation)

  ”A Kulcs kontrollok azok a lényeges kontrollok az üzleti folyamatokban, melyek ha megfelelően működnek, **biztosítják és bizonyosságot adnak** arra, hogy a szervezet eléri a kulcsfontosságú üzleti céljait.”
- A **Kulcs kontrollok** a **Kontroll Tevékenységek közé tartoznak** (a subset of Control Activities)!
- A Pénzügyi Jelentés Készítés ”üzleti” célja: A management igényeknek és a jogszabályi követelményeknek megfelelő **pontos pénzügyi információ** nyújtása **eredményesen, hatékonyan és időben**
- A pénzügyi folyamatok tipikus **Kontroll Célkitűzései**: meghatalmazás, hitelesség, értékelés, teljesség, osztályozás, valódiság, időbeliség, megőrzés, felelősségek elkülönítése
- Megfelelő informatikai rendszer szükséges ahhoz, hogy a **„teljesítmény” információk elérhetőek és nyomon követhetőek** legyenek annak érdekében, hogy a **meghatározott kontroll célkitűzések teljesüljenek**
- A Kulcs kontrollok biztosítják a **folyamatba épített ellenőrzések rendszerét**

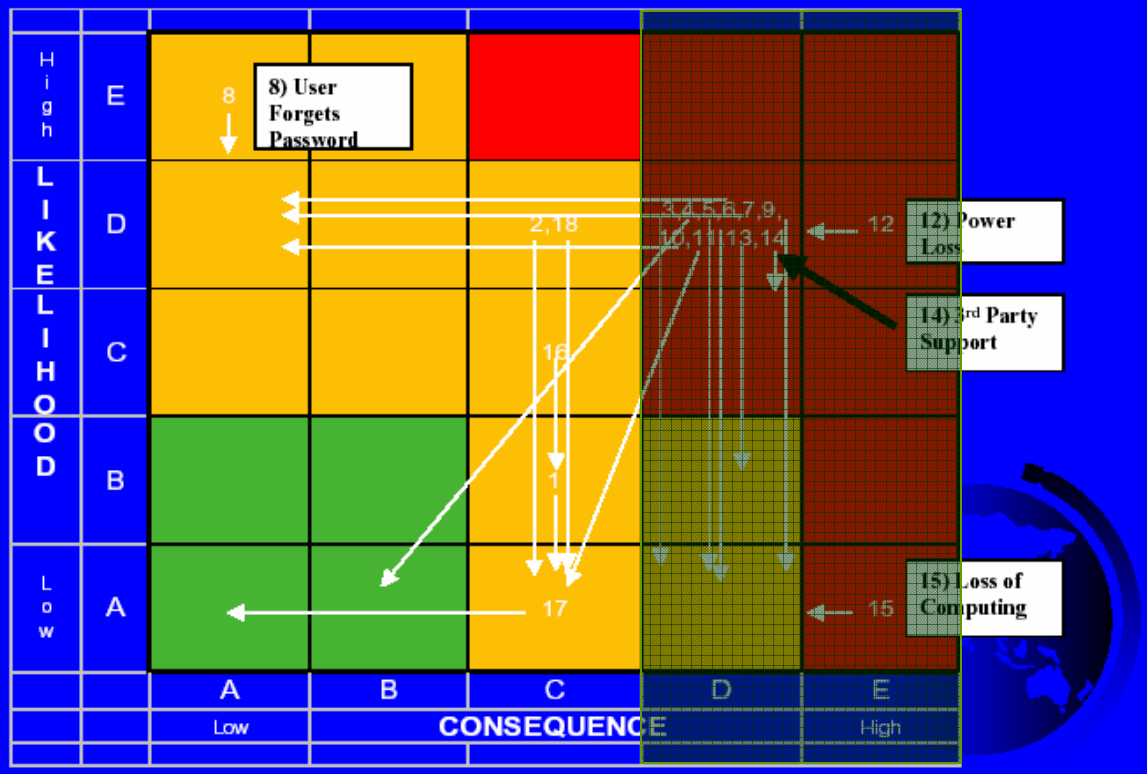
  (+ Minőségbiztosítási és Kockázat értékelési folyamatokat)

Key Controls: The Solution for Sarbanes-Oxley Internal Control Compliance, James Brady Vorhies, 2004

Kulcs kontroll folyamatok:
Kockázatok és Lehetőségek

LHS

Real Value Added



Kulcs kontroll folyamatok:
Kulcs kontroll folyamat megvalósítása

- Az általános (pl. pénzügyi) kontroll célok **testreszabása** a szervezet (egység) típusára, méretére, stb.
- A „teljesítmény” jelentések folyamátának szemlézése és **dokumentálása**
- **Hiányzó kontrollok** feltárása
- Azonosított kontrollok **tesztelése**
- ”**Minimum kontroll szintek**” kifejlesztése
- Kulcs kontrollok és kontroll eltérések **szemlézése**
- **Verifikáció** a Minimum kontroll szint követelmények alapján

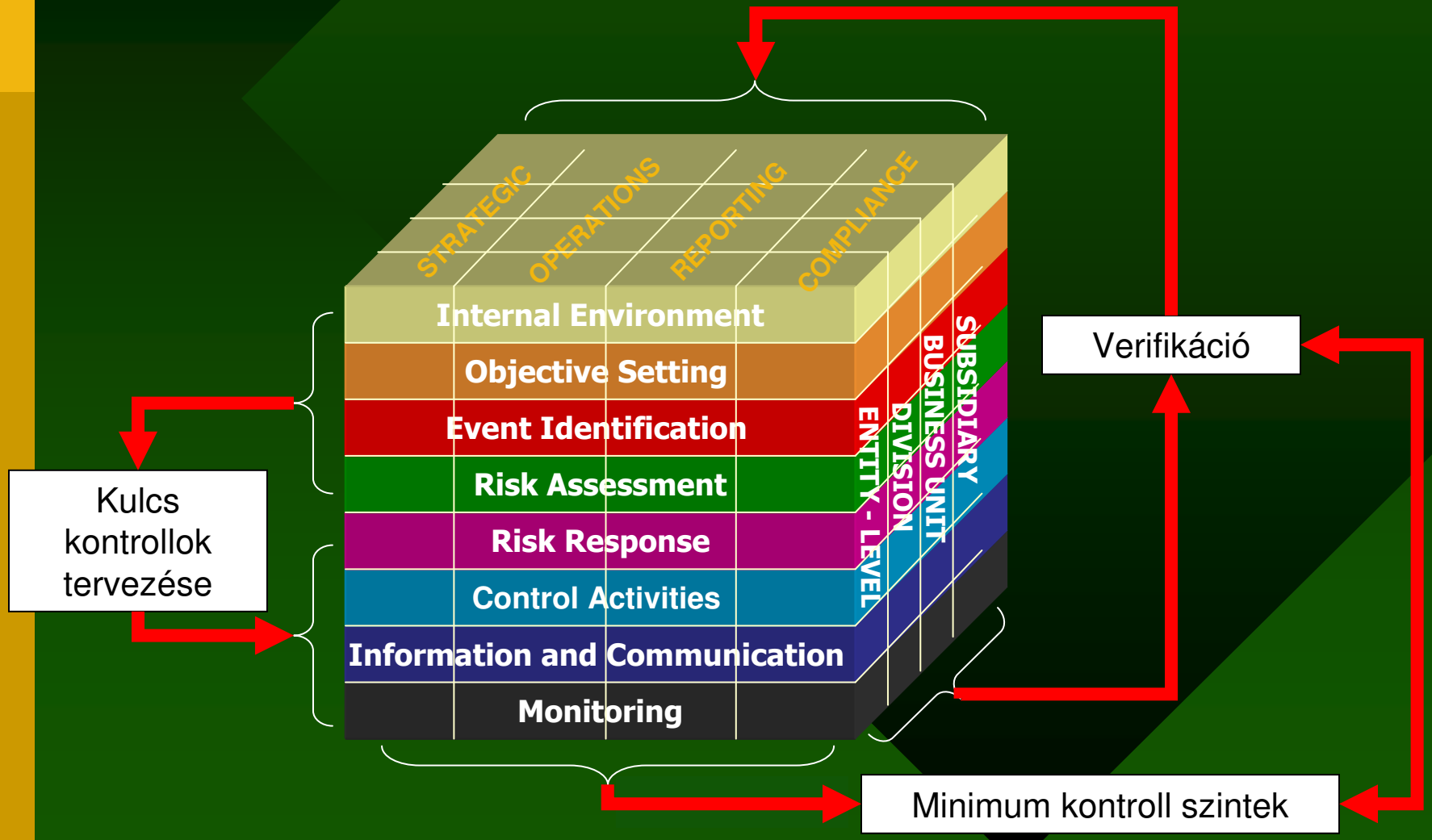
”Minimum kontroll szintek biztosítják, hogy a Kulcs kontrollok végrehajtásával elérjük a kontroll célkitűzéseket figyelembe véve a teljességi, időbeli és pontossági jellemzőket. Emiatt a minimum kontroll szintek a Kulcs kontrollok által elérendő a kontroll célokhoz kapcsolódnak. Ha megfelelően kerülnek kialakításra, akkor a minimum kontroll szintek a kulcs kontrollok által megelőzendő kockázatok kontroll hiányosságaiból vezethetőek le.”

Key Controls: The Solution for Sarbanes-Oxley Internal Control Compliance, James Brady Vorhies, 2004

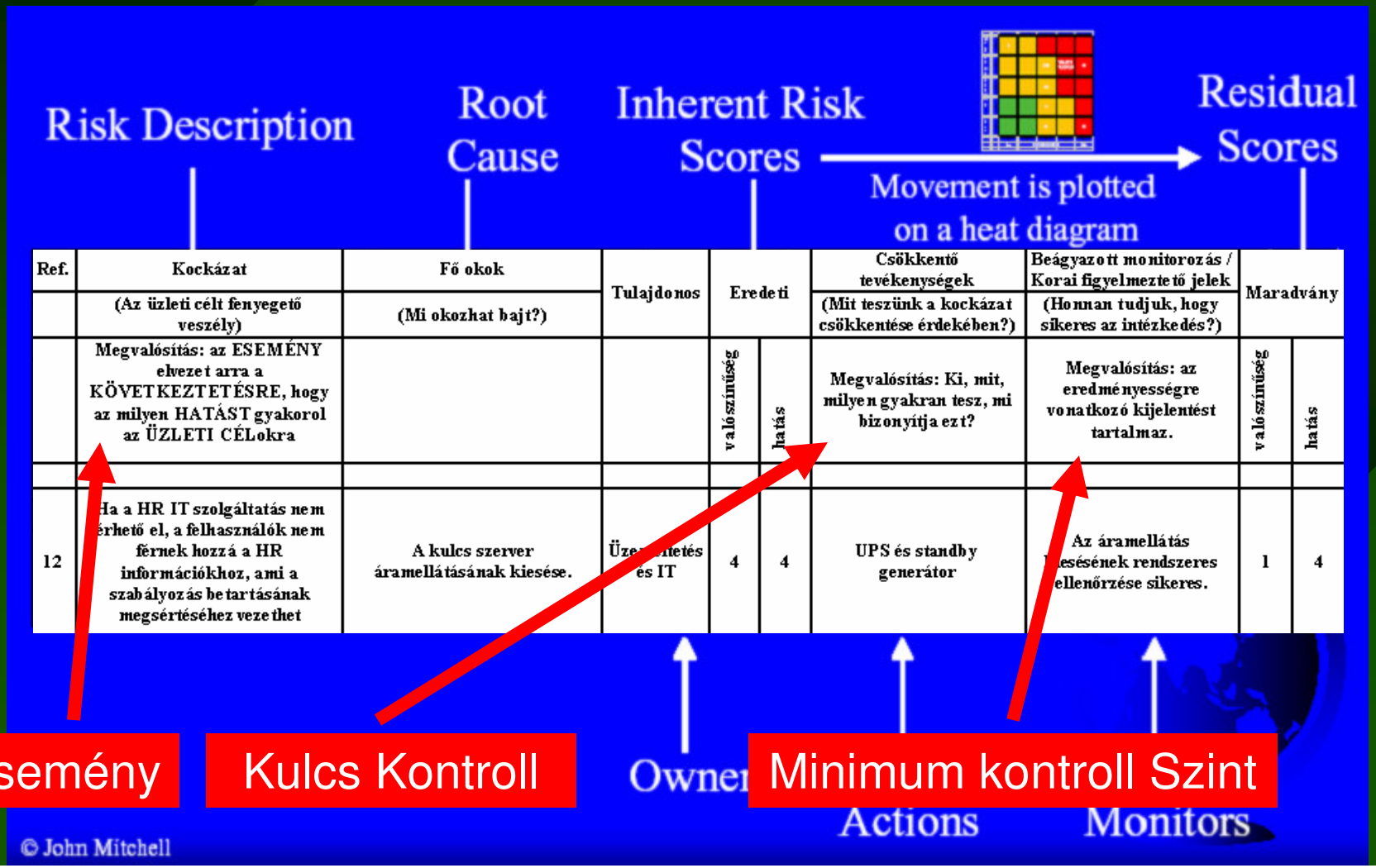
Kulcs kontroll folyamatok:
Verifikáció

- Az üzleti folyamatokra szabott **Kontroll Célok** alapján
- Meghatározott gyakoriséggal
- A ”**minimum kontroll szintek**” használatával meggyőződni arról, hogy a Kulcs kontroll teljesül
- Jelenteni a **kivételeket és kontroll hiányosságokat** a minimum kontroll szintek továbbfejlesztéséhez
- **Egyszerű és elfogadott formátumban** minden szervezeti egység számára

Kulcs kontroll folyamatok:
Kulcs kontrollok és a COSO ERM



Kulcs kontroll folyamatok:
Minimum kontroll szintek az eredményesség méréséhez



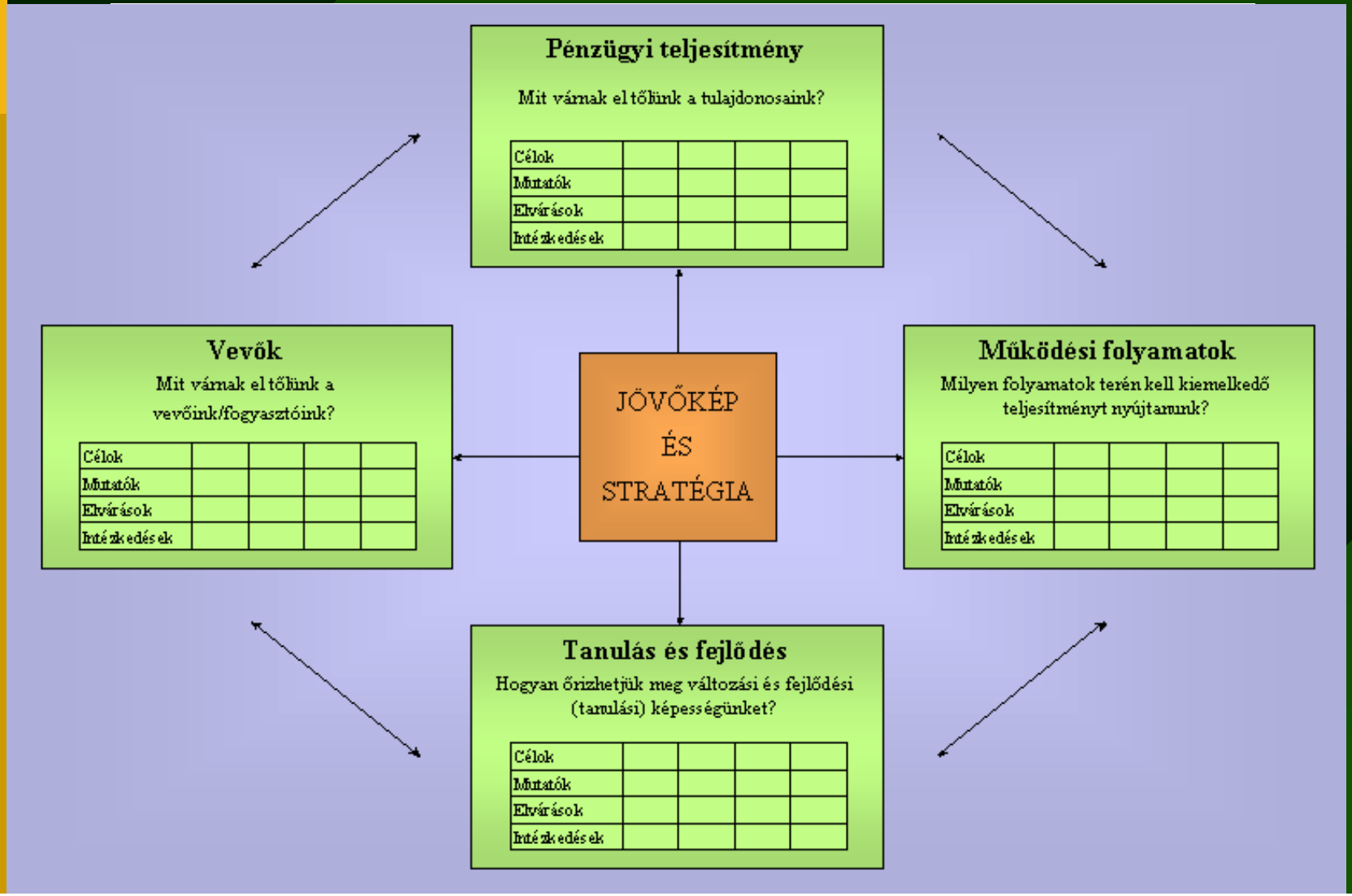
Ref.	Kockázat	Fő okok	Tulajdonos	Eredeti		Csökkentő tevékenységek	Beágyazott monitorozás / Korai figyelmeztető jelek	Maradvány	
	(Az üzleti célt fenyegető veszély)	(Mi okozhat bajt?)				(Mit teszünk a kockázat csökkentése érdekében?)	(Honnan tudjuk, hogy sikeres az intézkedés?)		
	Megvalósítás: az ESEMÉNY elvezet arra a KÖVETKEZTETÉSRE, hogy az milyen HATÁST gyakorol az ÜZLETI CÉLokra			valószínűség	hatás	Megvalósítás: Ki, mit, milyen gyakran tesz, mi bizonyítja ezt?	Megvalósítás: az eredményességre vonatkozó kijelentést tartalmaz.	valószínűség	hatás
12	Ha a HR IT szolgáltatás nem érhető el, a felhasználók nem férnek hozzá a HR információkhoz, ami a szabályozás betartásának megsértéséhez vezethet	A kulcs szerver áramellátásának kiesése.	Üzemeltetés és IT	4	4	UPS és standby generátor	Az áramellátás kiesésének rendszeres ellenőrzése sikeres.	1	4

Eredményesség mérése

- A Balanced Scorecard alapmodellje
- Egymásba épülő mérő és mutatószámok (COBIT)
- Példa: Internal Audit Scorecard
- Kulcs Kontroll Mutatószámok (Key Control Scorecard)
- Kiszervezés hatékonyságának mérése

  Monitoring (evaluating) co-sourcing effectiveness (as contribution to the achievement of business objectives
- Internal Audit kiszervezési példák
- Példa: Service Organisation Audit Scorecard

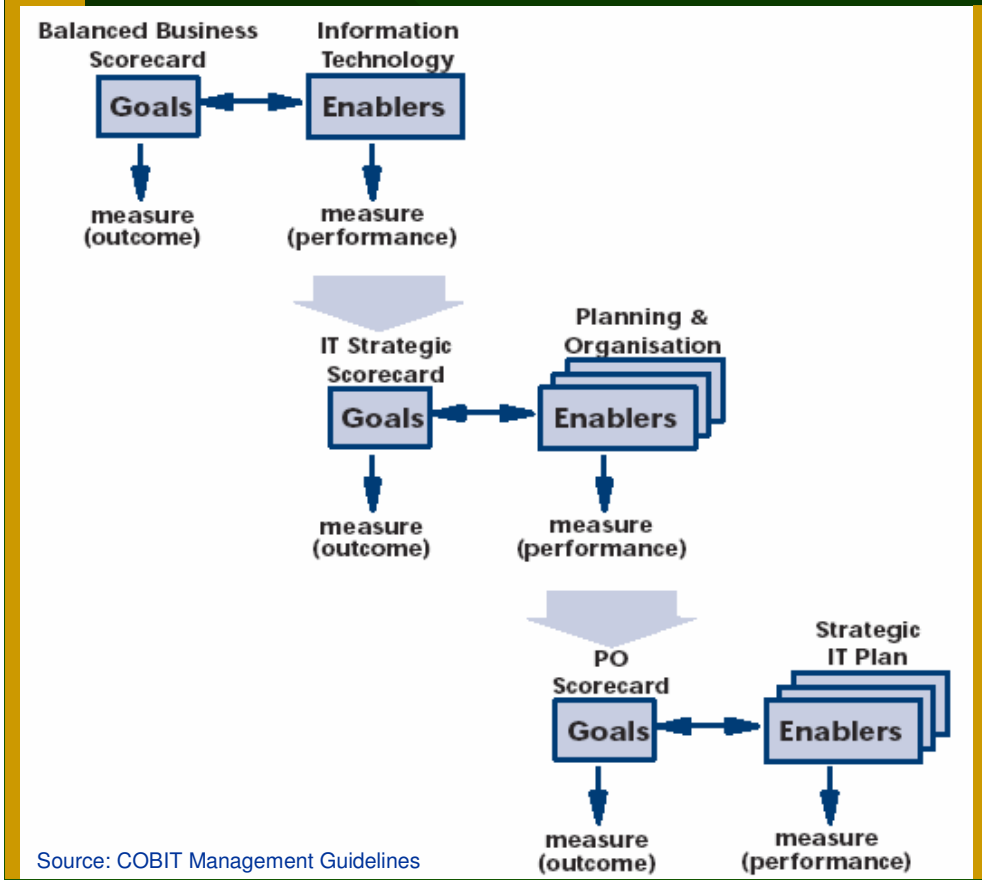
Eredményesség mérése:
A BSC alapmodellje



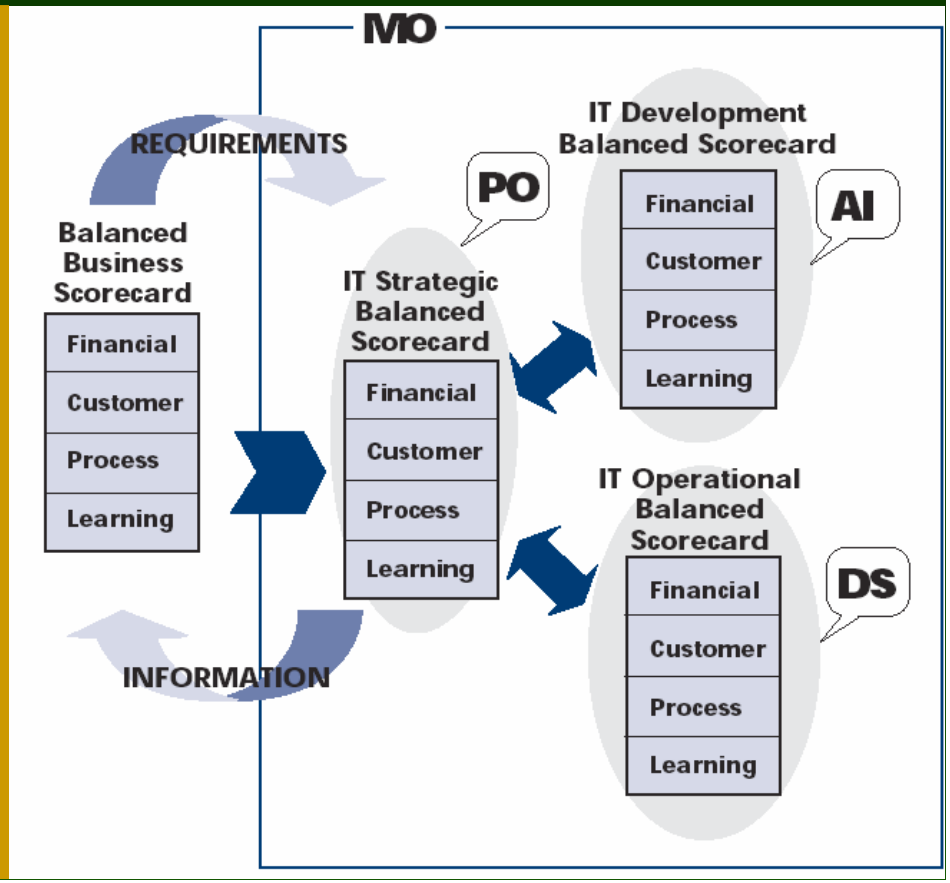
Eredményesség mérése:
BSC példa: szoftvercég

	Stratégiai cél	Mutatószám	Konkrét jellemző
Pénzügyi nézőpont: Milyenek legyünk befektetői szempontból?	Ágazat feletti eszközmegtérülés	A működő tőke megtérülése	24% fölötti eszközmegtérülés
	A piacinál gyorsabb megtérülés	Értékesítés növekedése	13% fölötti növekedési ráta
	Cash-flow növelése	Diszkontált független cash-flow	Évi 15%-os növekedés
Vevői nézőpont: Milyenek legyünk vevői nézőpontból?	Innovátor arculat	Az új termékek és szolgáltatások értékesítésének aránya	A 2 évnél fiatalabb termékek és szolgáltatások aránya 60% fölötti legyen
	Kiváló ár / teljesítmény arány	Vevőértékelés	A vevők legalább 60%-nál legyünk első számú szállítók
	Legyünk „házi" beszállítók	Törzsvevőkön keresztüli értékesítési arány	Az értékesítés 50% fölötti aránya a törzsvevőkön keresztül történjen
Működési folyamatok nézőpontja: Mely folyamatokban kell kiválót nyújtanunk?	Időben történő reagálás a vevői igényekre	A vevőkkel teljesített tanácsadói órák az ajánlati szakasz előtt	Évi 5%-kal való növekedés
	Az „A" regionális piac fejlesztése	Új vevők száma az „A" régióban	Évi 30%-os növekedés
	Gyors hardver installáció	A rendelés feladása és a hardver installáció közötti munkanapok száma	Az esetek 90%-ban tíz munkanapnál kevesebb
	Kiváló projektmenedzselés	Költségtúllépés nélküliprojektek száma	90%
Tanulási és fejlődési nézőpont: Hogyan maradhatunk rugalmasak és képesek a folyamatos javulásra?	Folyamatos javítás	Félidő index értéke	Évente 10% fölötti javulás
	Magas fokú alkalmazotti elégedettség	Alkalmazotti elégedettség indexe	80% fölötti elégedettségi index
		Tökélesítésre irányuló javaslatok száma alkalmazottanként	Alkalmazottanként 20-nál több javaslat

Eredményesség mérése:
Egymásba épülő mérő és mutatószámok
Embedded Balanced Scorecards (COBIT)



Source: COBIT Management Guidelines



Eredményesség mérése:
Példa: Internal Audit Scorecard

Example Internal Audit Balanced Scorecard

25% People
- Quality of professional staff
- Ability to address specialised and technical needs
- Understanding of the business and the global business environment
- Interaction and communication with line management executives
- Development of management talent for the organisation

25% Internal Audit Process Effectiveness
- Rapid and effective start-up
- Effective and timely communications
- Development and delivery of practical recommendations to improve internal controls and corporate governance
- Results of auditee satisfaction questionnaires

Vevő

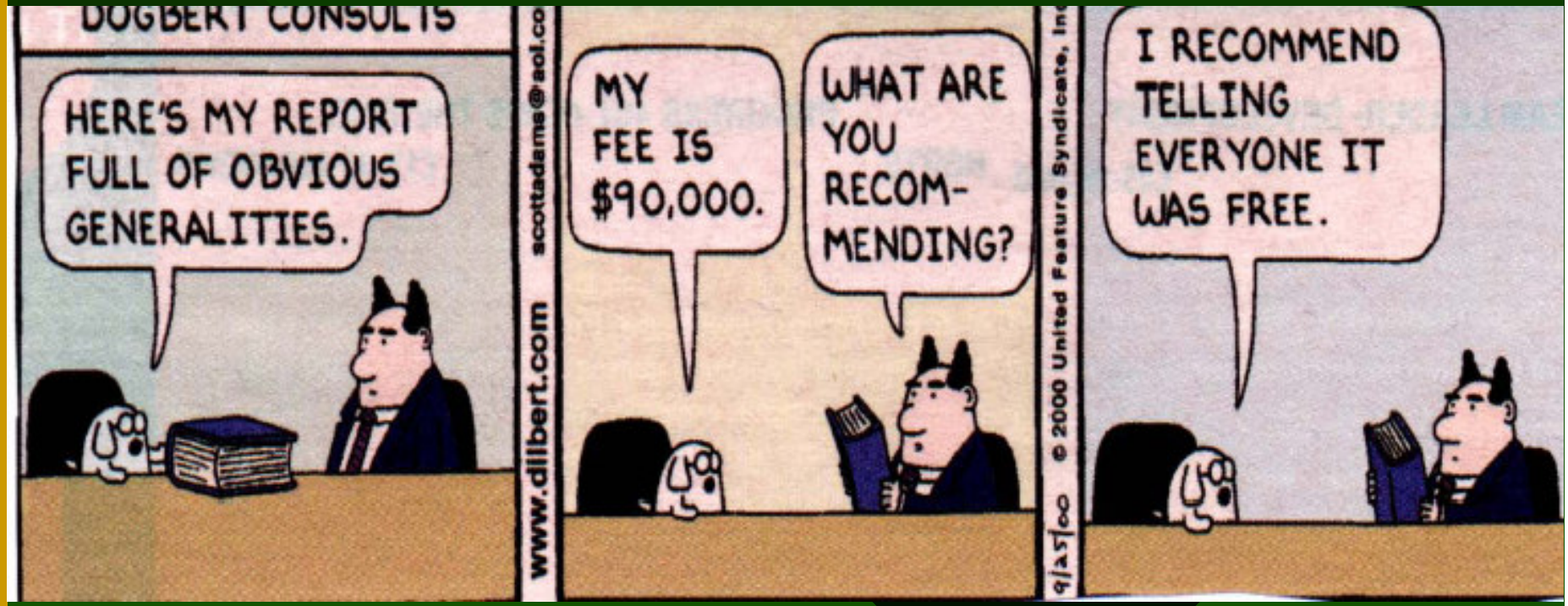
25% Risk Management
- Timely and effective identification of key business risks
- Percentage of audit activities and resources allocated to addressing key business risks
- Adaptability and responsiveness to emerging risks
- Understanding and fulfillment of the needs of:
  - The audit committee
  - Executive management

25% Value Added to the Business
- Protection of shareholder value through an improved control environment
- Enhanced shareholder value through:
  - Cost reductions
  - Reduced revenue leakage
  - Reduced working capital
  - Enhanced cash flow.

Eredményesség mérése:
Kulcs Kontroll Scorecard

Key Control Scorecard	
Vevők Hogy ítélik meg a kulcs kontroll folyamatot a megbízók?	**Pénzügyi teljesítmény** Mit vár el a vezetés a kulcs kontroll folyamattól?
Jövőkép Teljesíteni a törvényi megfeleléssel kapcsolatos elvárásokat és növelni a megbízók elégedettségét. **Célok** • Független Audit teljesítmény • Megbízók elégedettsége **Mutatók** • Az audit eredmények siker rátája • Megbízói elégedettség felmérés eredménye	**Jövőkép** A KC folyamat az elvárható mértékben járuljon hozzá az üzleti eredményességhez. **Célok** • A törvényi megfeleléssel kapcsolatos kiadások kontrollja • Az ületi lehetőségek maximális feltárása **Mutatók** • Aktuális és tervezett kiadások/ erőforrások aránya • Aktuális és tervezett bevétel aránya • Üzleti érték növekménye
Működési folyamatok Milyen eredményes a kulcs kontroll folyamat?	**Tanulás és fejlődés** Képes-e a szervezet megfelelni a kulcs kontroll kihívásoknak?
Jövőkép Biztosítani és biztosítékot nyújtani arra, hogy a szervezet eléri a kulcs üzleti folyamattal kapcsolatos céljait **Célok** • Nagy hatású kockázatok csökkentése • Nagy hatású lehetőségek kihasználása • Minimum standardok alkalmazása és fejlesztése **Mutatók** • Elért kontra szándékolt hatás és valószínűségi érték (eredményesség) • Tényleges kontra tervezett verifikálási gyakoriság • Kontroll hibák/ hiányosságok • Megelőző és helyesbítő tevékenységek	**Jövőkép** A lehetőségek olyan irányú fejlesztése, mely képessé tesz megfelelni a jövő kihívásaira. **Célok** • Képzett és motivált stáb • Alkalmazható innovatív technológiák • Folyamatjavítás **Mutatók** • Képzettség értékelés • A technológiai lehetőségek korai felismerése és elemzése • Érettség alapú értékelés (Képesség felmérés)

Eredményesség mérése:
Kiszervezés eredményességének mérése



Eredményesség mérése:
Internal Audit kiszervezési példák

Hub and Spokes Resource Model

PRICEWATERHOUSECOOPERS

Eredményesség mérése:
Kiszervezés kockázatai

- Nem megfelelőség (SLA szerint)
- Negatív hatás az alapvető üzleti folyamatokra
- Negatív hatás a (Kulcs) kontroll folyamatokra (kontroll eredményesség csökkenése)
- Külső/belső audit költségek növekedése

Eredményesség mérése:
Példa: Service Organisation Audit (SAS70) BSC

SAS-70 BSC	
Vevők Hogy ítélik meg az audit folyamatot a megbízók?	**Pénzügyi teljesítmény** Mit vár el a vezetés az audit folyamattól?
Jövőkép Teljesíteni a megbízók audittal szembeni elvárásait és növelni elégedettségüket. **Célok** ▪ Audit teljesítmény ▪ Megbízók elégedettsége **Mutatók** ▪ SAS-70 audit eredmények elfogadottsági foka ▪ Megbízói elégedettség felmérés eredménye	**Jövőkép** Az audit folyamat az elvárható mértékben járuljon hozzá az üzleti eredményességhez. **Célok** ▪ Az audit kiadások kontrollja ▪ Az ületi lehetőségek maximális feltárása **Mutatók** ▪ Hozzáadott értéket nyújt a megbízók számára ▪ Pozitív hatással van a szolgáltatás-vezetésre ▪ Aktuális és tervezett kiadások aránya
Működési folyamatok Milyen eredményes az audit folyamat?	**Tanulás és fejlődés** Képes-e a szervezet megfelelmi az audit jövőbeni kihívásainak?
Jövőkép Hatékony audit folyamat **Célok** ▪ Az audit folyamat fejlesztése ▪ Eredményes számviteli audit ▪ Eredményes audit beszámolók ▪ Az audit észrevételeinek eredményes kezelése **Mutatók** ▪ Audit érettségi szint ▪ Sikeres számviteli auditok száma ▪ Elfogadott audit riportok aránya ▪ A határidőre nem rendezett nem-megfelelőségek száma	**Jövőkép** A lehetőségek olyan irányú fejlesztése, mely képessé tesz megfelelni a jövő kihívásaira. **Célok** ▪ a szolgáltató munkatársak és a megbízók kapcsolattartóinak SAS 70 audit képzése ▪ Audit követelmény felülvizsgálatainak figyelemmel kísérése ▪ Belső és külső benchmarking kutatások **Mutatók** ▪ Oktatási költségvetés a teljes audit büdzséhez képest ▪ Az oktatásba bevont szolgáltató stáb és megbízó kapcsolattartók aránya a teljes stábhoz képest ▪ Audit követelmény felülvizsgálataira fordított költségvetés aránya ▪ A kutatócsoport által kezdeményezett, sikeres megújító projektek száma

Eredmények bemutatása, külső audit támogatása

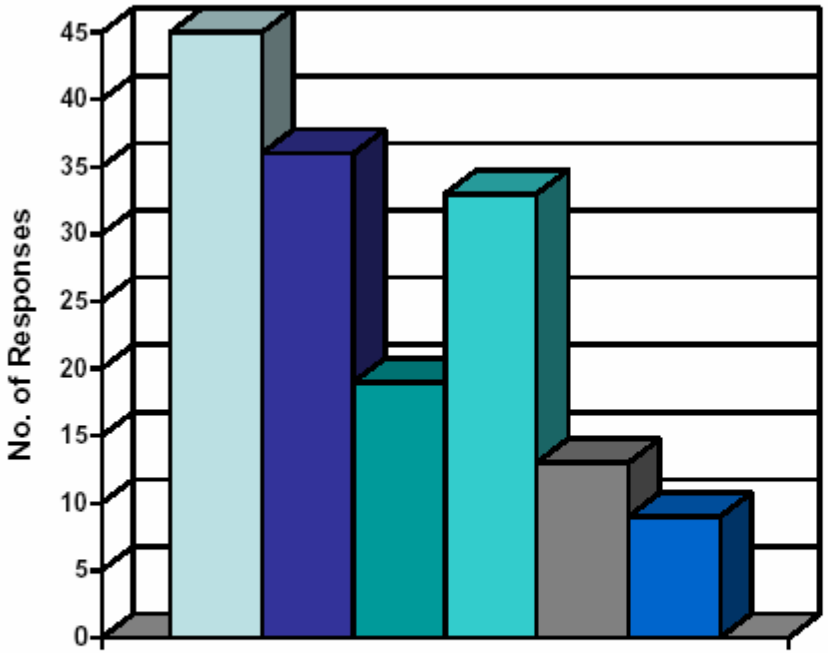
- 5. (Optimalizált) Érettségi szint által meghatározott sikertényezők: ERM + Control and Risk Self Assessment + Technology
- Külső auditot segítő dokumentáció és folyamatkezelés a vezetés munkájának támogatására
- Technológiák

Eredmények bemutatása, külső audit támogatása:
5. (Optimalizált) Érettségi szint sikerténye zői:
ERM + Control and Risk Self Assessment + Technology

- Olyan ”enterprisewide control and risk management” program valósul meg, melyben a kontrollok és folyamatok jól dokumentáltak és folyamatosan felülvizsgálatra kerülnek reagálva a lényeges folyamatokban bekövetkező, illetve a szervezeti változásokra.
- Létezik önértékelési folyamat a kontrollok tervezésének és eredményességének kiértékelésére.
- Információ-technológia maximális kiaknázása a folyamatok, a kontroll célok és tevékenységek dokumentálására, a hiányosságok azonosítására, továbbá a kontrollok eredményességének kiértékelésre.

IT Control Objectives for Sarbanes-Oxley, IT Governance Institute, 2004

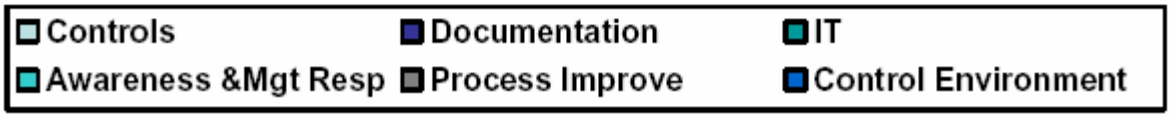
Eredmények bemutatása, külső audit támogatása:
SOX: Legfontosabb kontroll fejlődési területek



Sarbanes-Oxley Section 404 Work: Looking at the Benefits

January 2005

The IIA Research Foundation



Eredmények bemutatása, külső audit támogatása:
SOX: Kiforrott dokumentum-kezelés és kontroll bizonyíték

Dokumentáció-kezelés javulása az alábbi területeken:

- Folyamatok, workflow-k és kontrollok
- Annak dokumentálása, hogy a kontrollok működnek

A vizsgálati eredmények azt mutatták, hogy kevés a bizonyíték (dokumentum) arra, hogy a létező kontrollok valóban működnek!

Sarbanes-Oxley Section 404 Work: Looking at the Benefits, January 2005
The IIA Research Foundation

Eredmények bemutatása, külső audit támogatása:

SOX: Külső auditot segítő dokumentáció és folyamatkezelés a vezetés munkájának támogatására

Annak igazolása, hogy

- a vezetés kockázat elemzése és célkitűzése elégséges,
- a COSO szervezeti (egység) szinten alkalmazott kontrolljai értelmezhetőek és elégségesek,
- az elsődleges üzleti folyamatok és tranzakciók megismerhetőek és független ”bejárással” verifikálhatóak,
- minden lényeges tranzakció típus érintve van,
- minden lényeges pénzügyi jelzés (assertion) kialakításra került a lényeges számlák és közzétételek (disclosure) vonatkozásában,
- a kontrollok eredményességi tesztjei visszaellenőrizhetőek,
- a kiválasztott kulcs kontrollok eredményességének független tesztelése a kiválasztott lényeges helyszineken megtörtént.

Sarbanes-Oxley Section 404 Work: Looking at the Benefits, January 2005

The IIA Research Foundation

Eredmények bemutatása, külső audit támogatása:
Integrált audit megfontolások

- Meg kell érteni azokat az üzleti kockázatokat, melyeket kezelő kontrollok értékelésre és tesztelésre kerülnek (pl. a beazonosított üzleti kockázatokra közös érvényesség és célkitűzések vonatkozzanak).
- Kulcs kontrollok beazonosítása, beleértve mind a ”kézi”, mind az automatizált elemeket.
- ”Csak” *ezeket* a Kulcs kontrollokat kell dokumentálni, értékelni, és tesztelni!

The More Things Change, By Norman Marks, Internal Auditor, August 2004

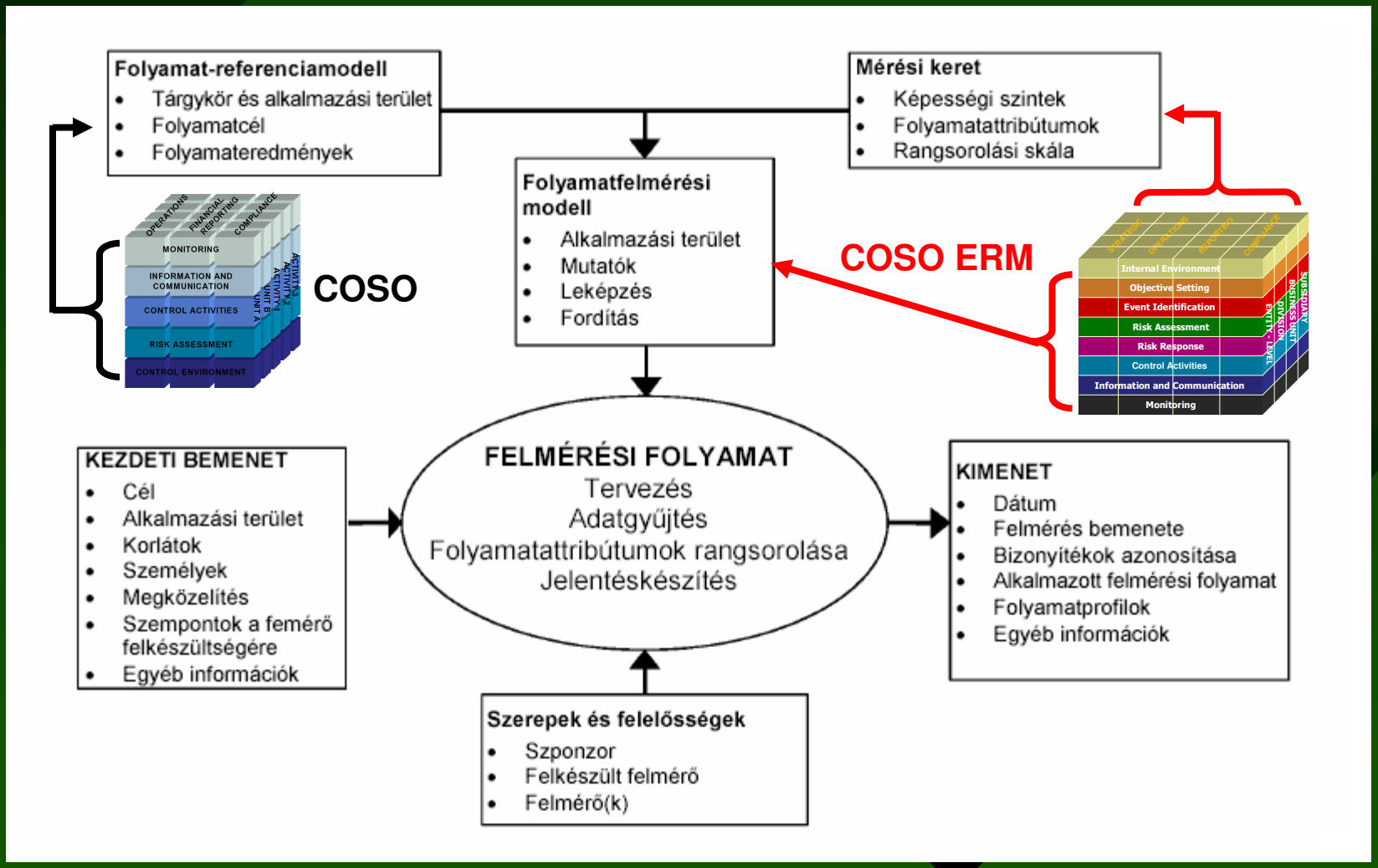
Eredmények bemutatása, külső audit támogatása:

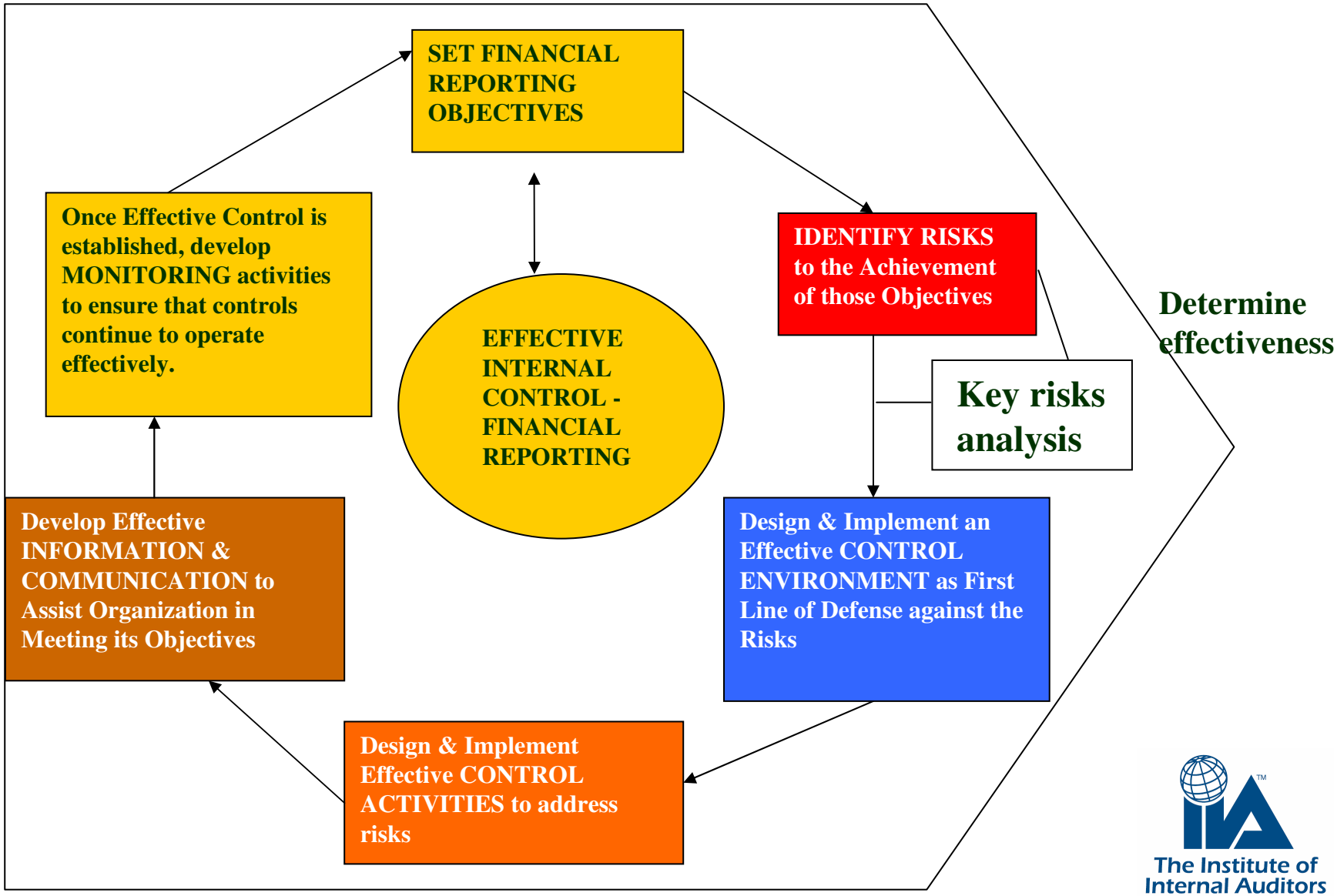
A dokumentáció- és folyamatkezelést támogató technológiák

- ✓ Risk Analysis and Risk Management
- ✓ Inventory of the Audit Universe
- ✓ Internal Control Evaluation
- ✓ Planning and Scheduling
- ✓ Project Management and Audit Tracking
- ✓ Personnel Database and Skills Inventory
- ✓ Audit Reference Library
- ✓ Communications
- ✓ Presentations
- ✓ Tracking of Results and Findings
- ✓ Customer Satisfaction Assessment
- ✓ Training and Education
- ✓ Internet

ISO/IEC 15504

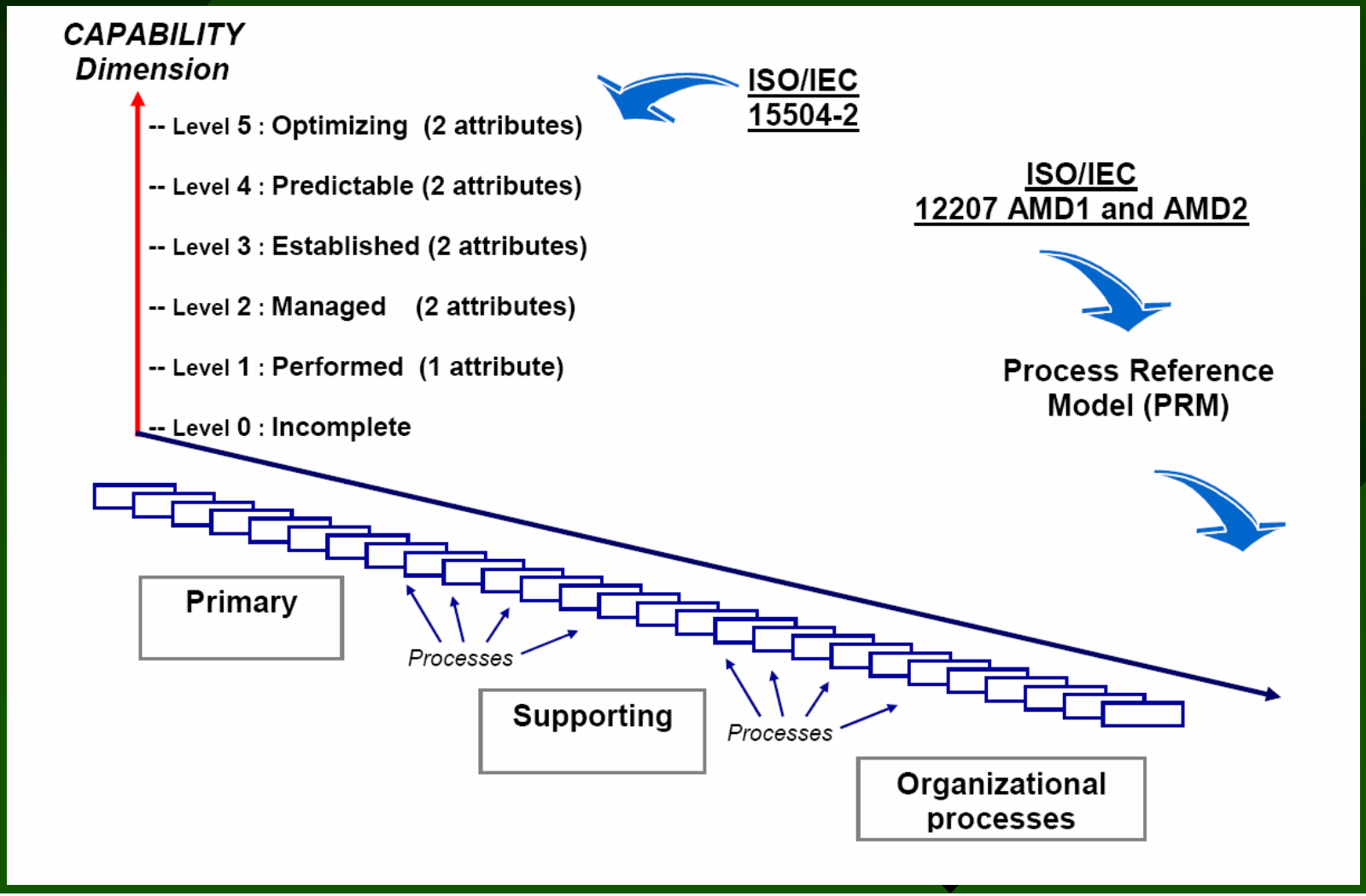
A folyamatfelmérés nemzetközi szabványa és a COSO keretrendszerek





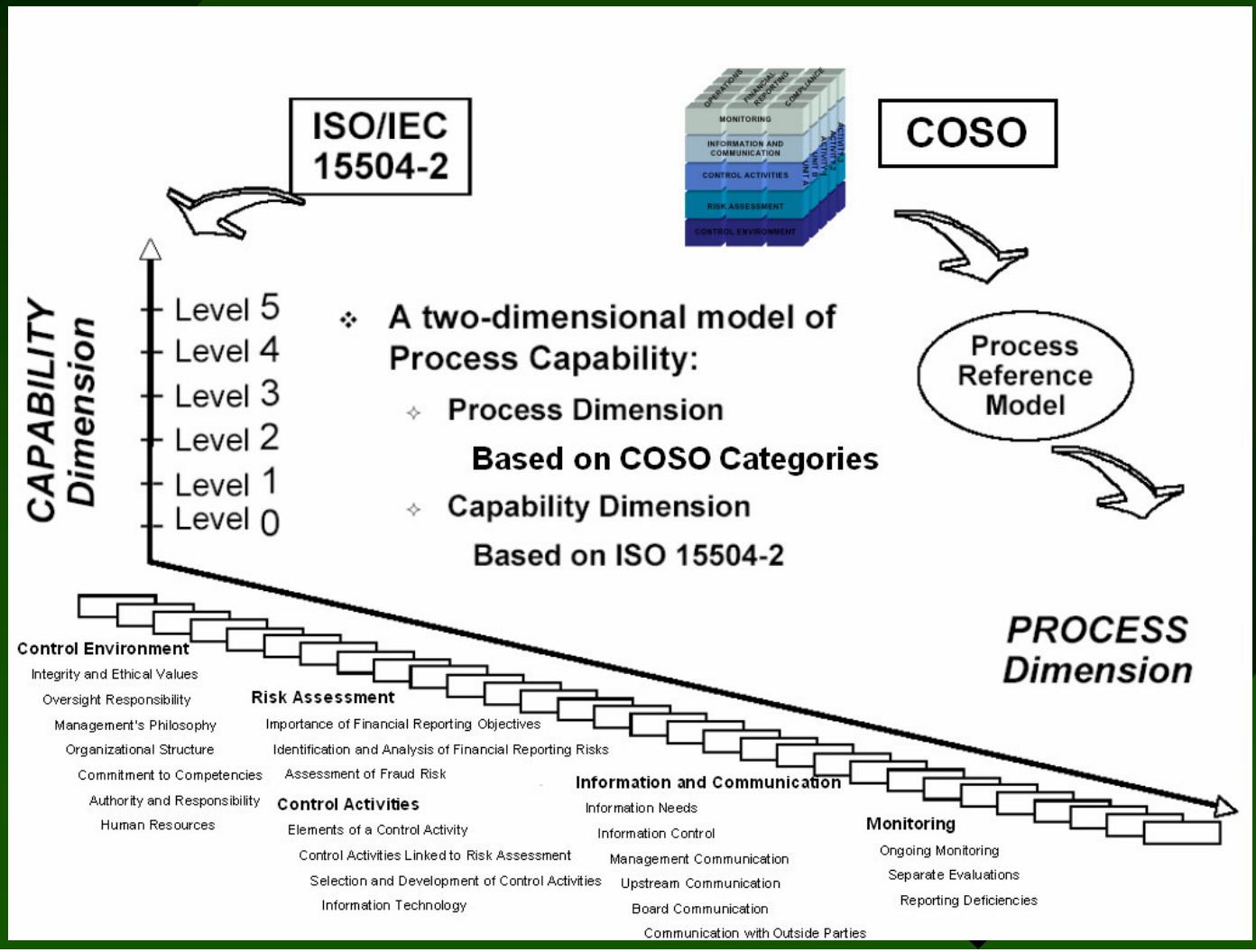
The Institute of Internal Auditors

ISO/IEC 15504-5
A szoftverfejlesztési folyamatok felmérési modelje

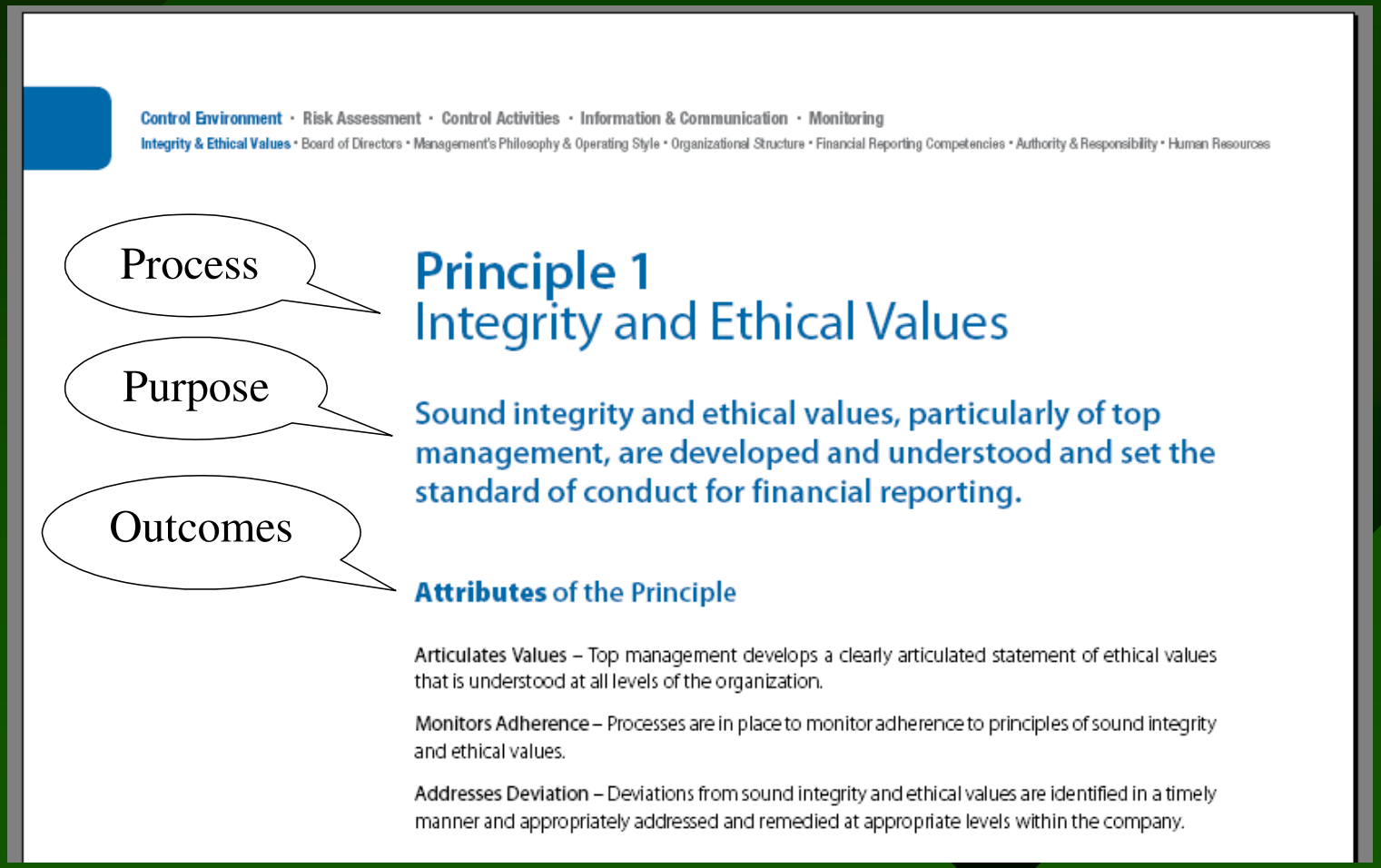


COSO és az ISO 15504

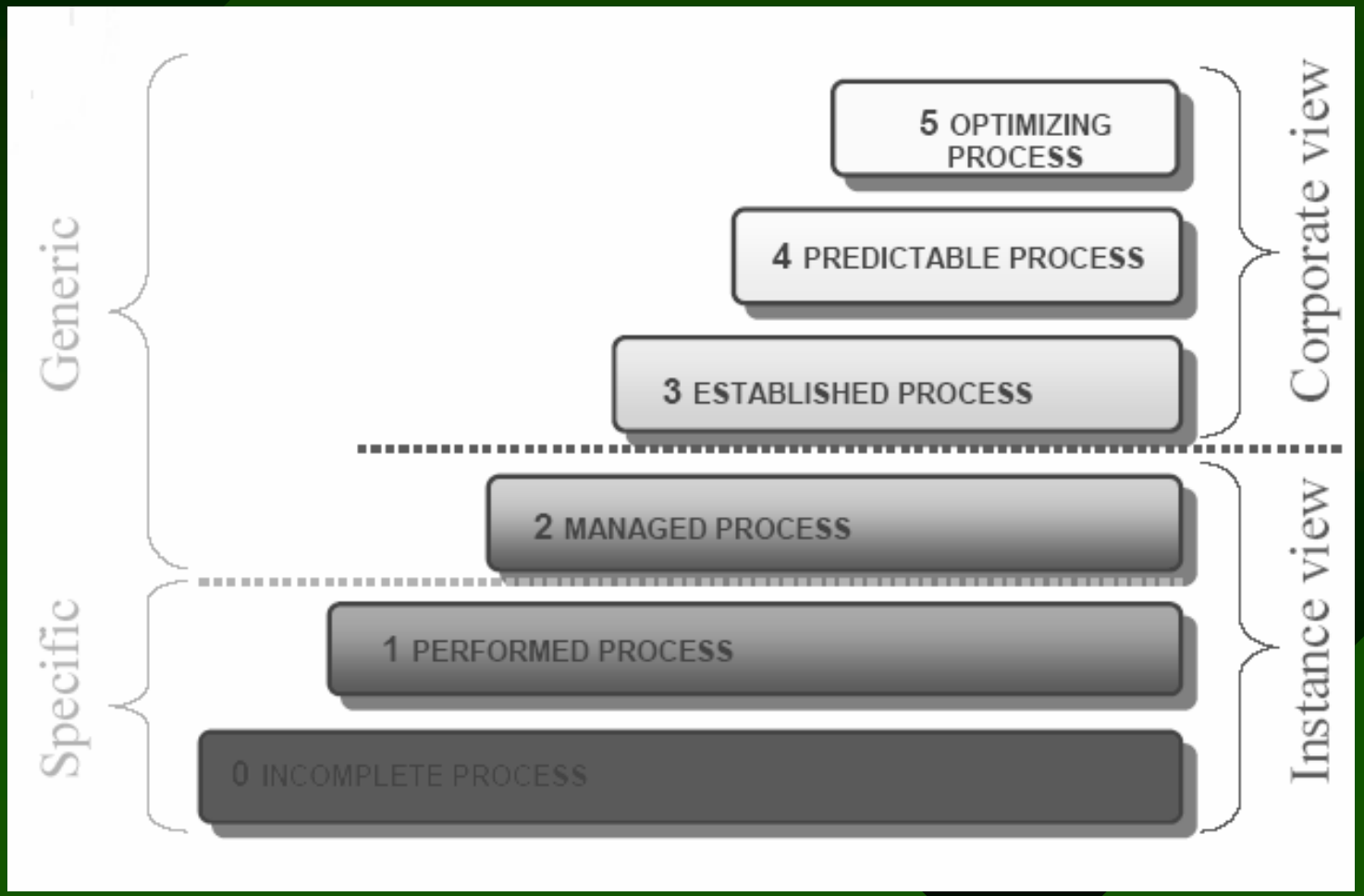
COSO Kategóriák mint Folyamat Dimenzió



COSO SB Guidance – ISO 15504 Folyamat-referencia Modell



Képességi szintek és a szervezeti dimenzió



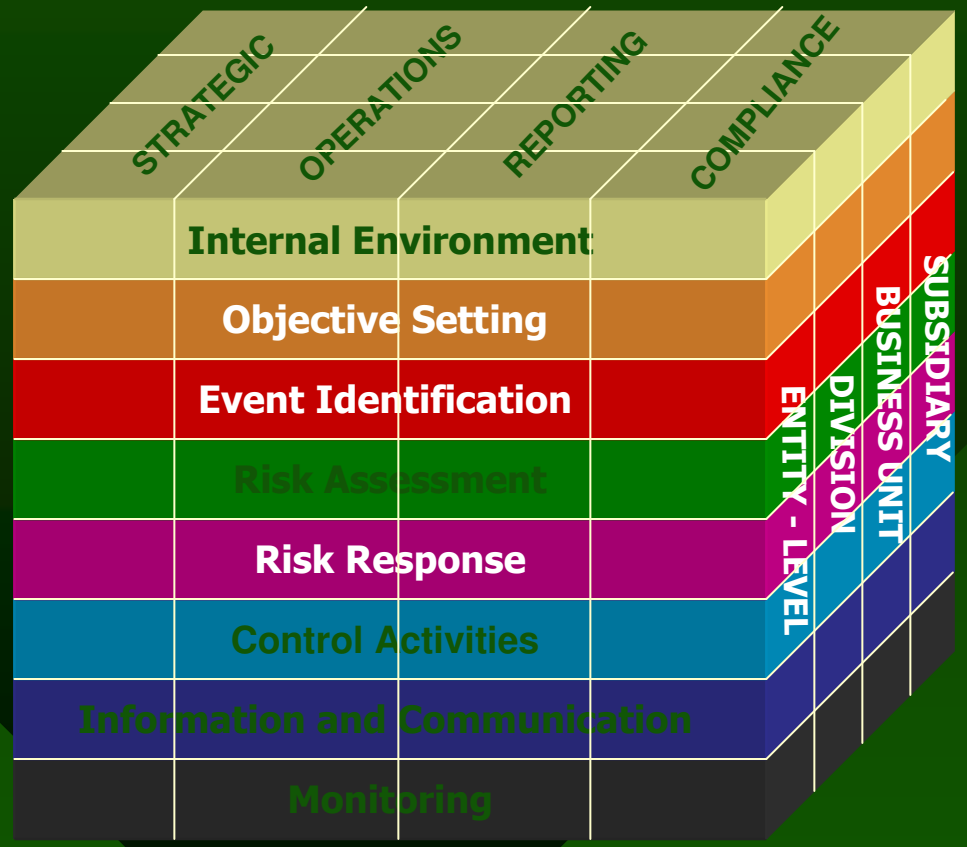
COSO és az ISO 15504

Kockázat alapú döntések (COSO ERM)

Mi a kockázati toleranciánk?

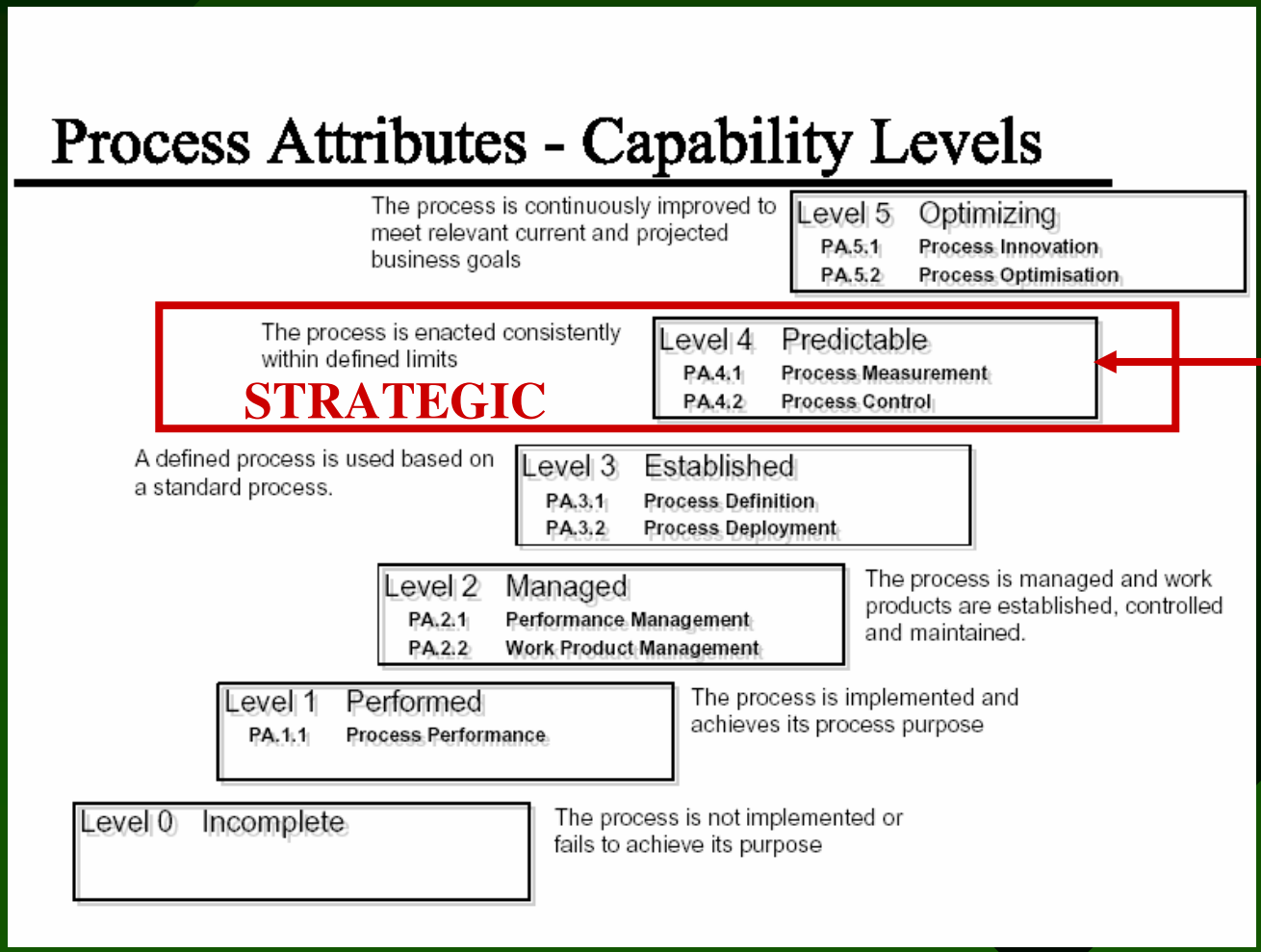
Hogyan es(het)nek meg a „dolgok”?

Hogyan kezeljük az eltérést/hiányosságot?



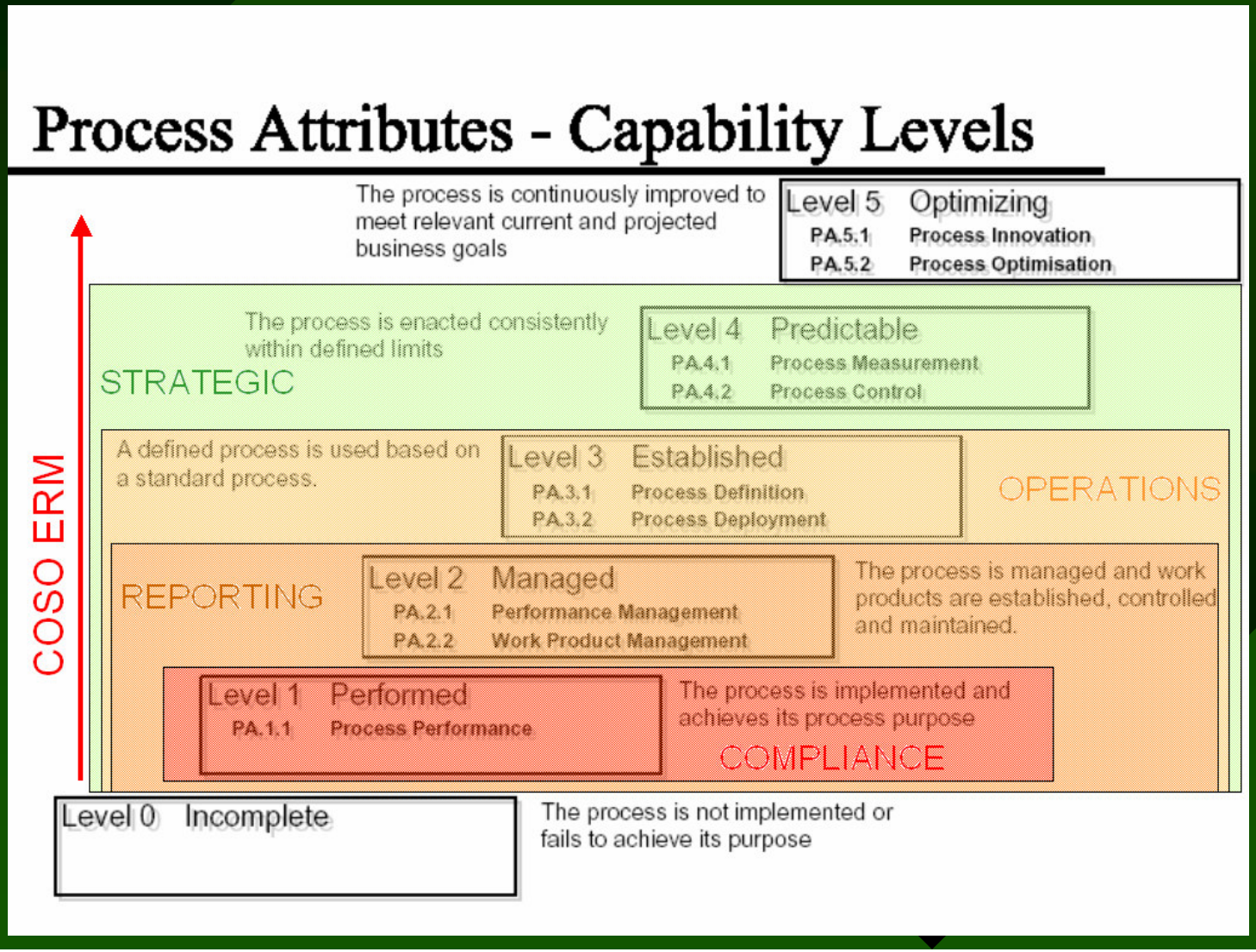
COSO és az ISO 15504

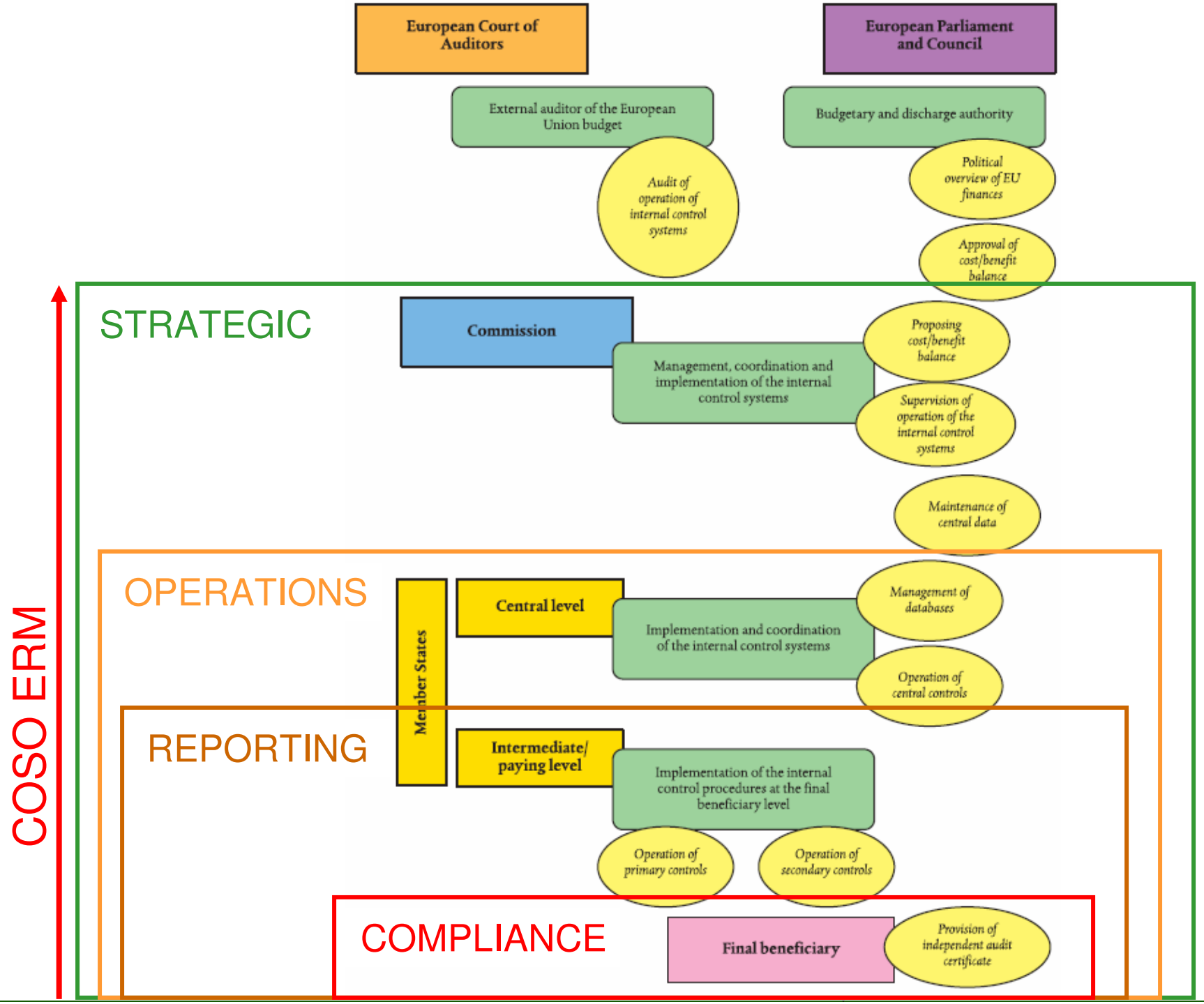
Kockázat alapú döntések és a folyamat attribútumok



COSO és az ISO 15504

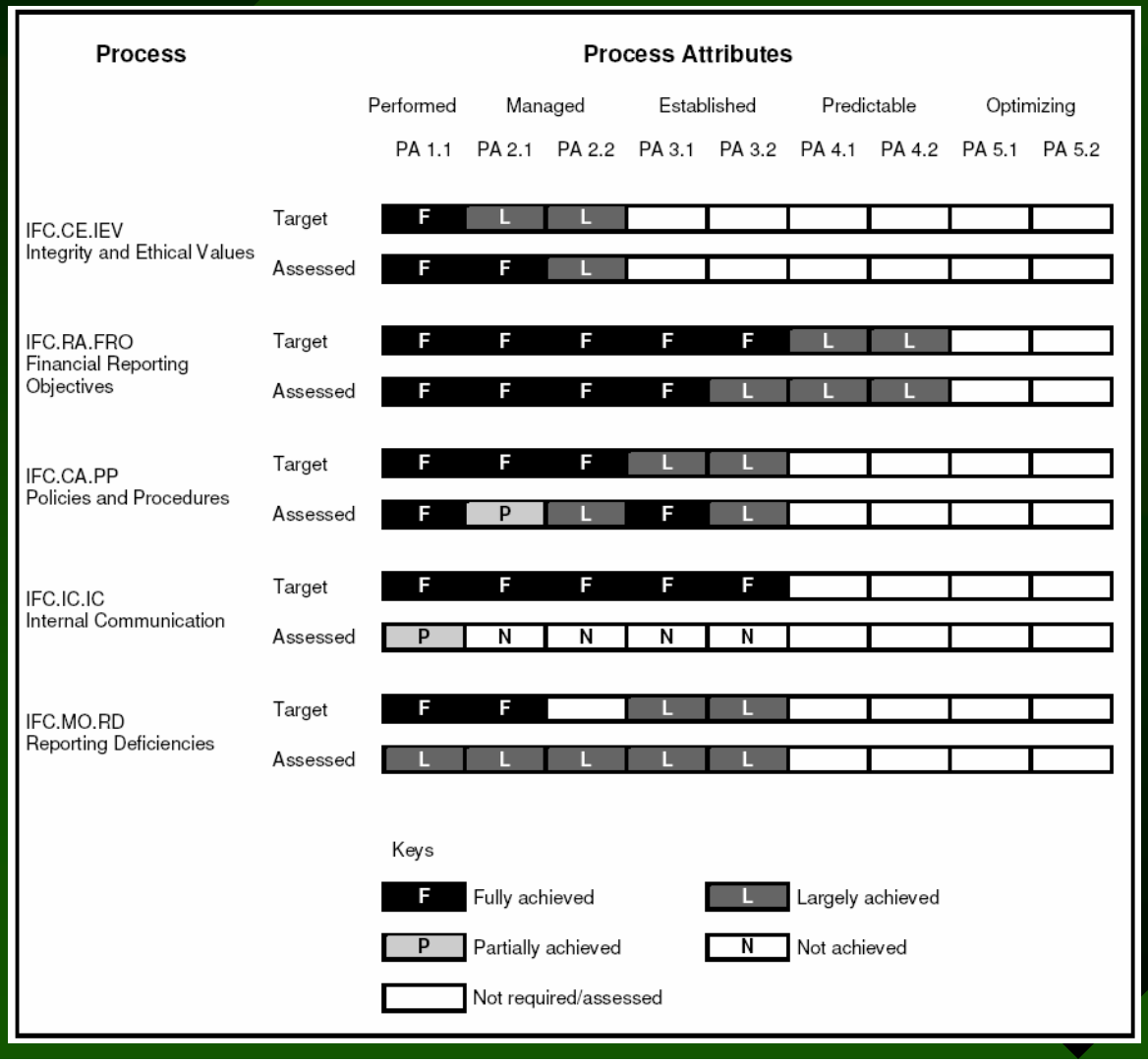
COSO Célok és a Képességi Szintek




European Court of Auditors
European Parliament and Council
External auditor of the European Union budget
Budgetary and discharge authority
Audit of operation of internal control systems
Political overview of EU finances
Approval of cost/benefit balance
COSO ERM
STRATEGIC
Commission
Management, coordination and implementation of the internal control systems
Proposing cost/benefit balance
Supervision of operation of the internal control systems
Maintenance of central data
OPERATIONS
Member States
Central level
Implementation and coordination of the internal control systems
Management of databases
Operation of central controls
REPORTING
Intermediate/ paying level
Implementation of the internal control procedures at the final beneficiary level
Operation of primary controls
Operation of secondary controls
COMPLIANCE
Final beneficiary
Provision of independent audit certificate

Control Risk Assessment

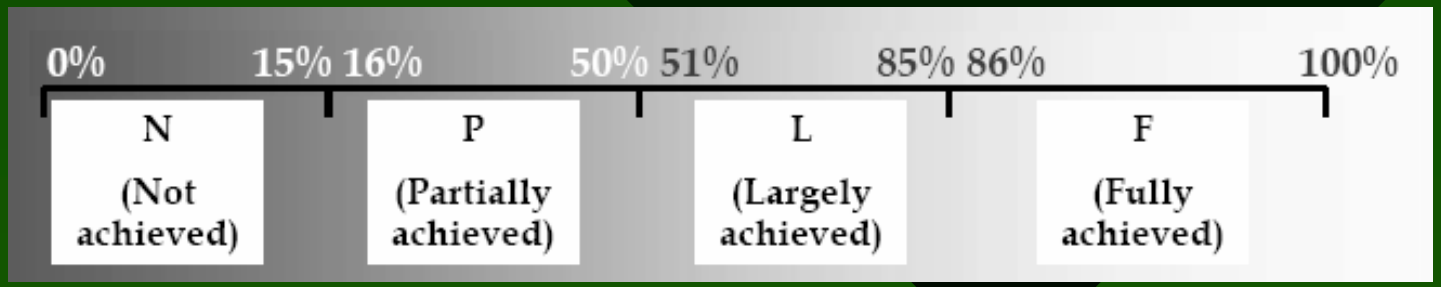
Cél- és felmért attribútumok



Control Risk Assessment

Folyamat attribútum hiányosságok kategorizálása

- „None”
- „Minor” – one-step gap – egy lépés különbség „Fully achieved” cél esetén
- „Major” – több lépés különbség a „Fully achieved”cél esetében, ill. akár egy lépés különbség a „Partially achieved” cél esetében.



Control Risk Assessment
Képességi szint hiányosságok kategorizálása

A kontroll-hiányosságból eredő probléma előfordulási valószínűsége a folyamat attribútum hiányosságból és a vonatkozó képességi szintből származtatható. Az alábbi kategóriákat használjuk:

- None - No major or minor gaps
- Slight - No gap at Level 1, and only minor gaps at higher levels
- Significant - A minor gap at Level 1, or a single major gap above
- Substantial - A major gap at Level 1, or more than one major gap above

Control Risk Assessment
ISO 15504 alapú kockázati térkép

Consequence Indicated by capability level where gap occurs	Probability Indicated by extent of capability level gap Slight	Significant	Substantial
5 – Optimizing	Low Risk	Low Risk	Low Risk
4 - Predictable	Low Risk	Low Risk	Medium Risk
3 - Established	Low Risk	Medium Risk	Medium Risk
2 - Managed	Medium Risk	Medium Risk	High Risk
1 - Performed	Medium Risk	High Risk	High Risk

Control Risk Assessment

ISO 15504 alapú kontroll kockázat értékelés

IFC.RA.FRO - Financial Reporting Objectives

	Level 1	Level 2		Level 3		Level 4	
	PA 1.1	PA.2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2
Target profile	F	F	F	F	F	L	L
Assessed profile	F	F	F	F	L	L	L
Process attribute gap	-	-	-	-	minor	-	-
Capability level gap	-	-		slight		-	
Capability level risk	-	-		low		-	
Process related risk	low						

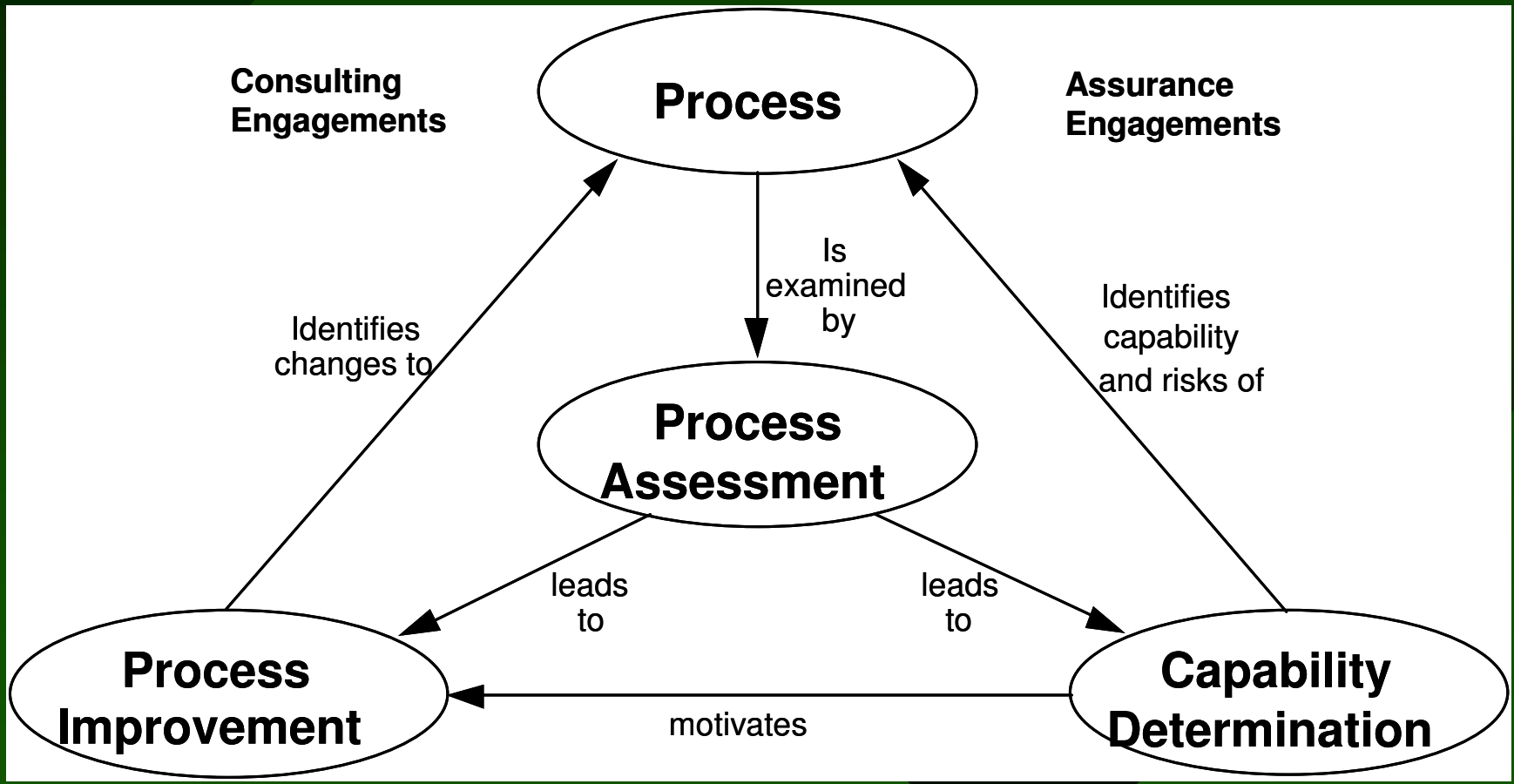
IFC.CA.PP - Policies and Procedures

	Level 1	Level 2		Level 3		Level 4	
	PA 1.1	PA.2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2
Target profile	F	F	F	L	L	-	-
Assessed profile	F	P	L	F	L	-	-
Process attribute gap	-	major	minor	-	-	-	-
Capability level gap	-	significant		-		-	
Capability level risk	-	medium		-		-	
Process related risk	medium						

IFC.IC.IC - Internal Communication

	Level 1	Level 2		Level 3		Level 4	
	PA 1.1	PA.2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2
Target profile	F	F	F	F	F	-	-
Assessed profile	P	N	N	N	N	-	-
Process attribute gap	major	major	major	major	major	-	-
Capability level gap	subst.	substantial		substantial		-	
Capability level risk	high	high		medium		-	
Process related risk	high						

Ellenőrzés (Audit) és ISO 15504 (Assessment)



Kulcsszavak:

- Kontroll és érettségi modellek (COSO ERM, COBIT)
- Megfelelés és Üzleti érték (Compliance and Business Value)
- Control and Risk Self Assessment
- Kulcs kontrollok (Key Controls)
- Eredményesség mérése (Effectiveness Conclusion)
- ISO 15504 és COSO

Köszönöm a figyelmüket!

Ivanyos János

Memolux Kft., IIA Hungary

+36 1 460 7403
+36 1 336 1505
ivanyos@memolux.hu
janos.ivanyos@iia.hu