eSec.hu

Hungarian Cyber Security Package

Szabályozások és módszertanok

Compliance megközelítéssel

Tóthmajor Máté, CISSP, CISA
mate.tothmajor@kurt.hu
www.kurt.hu

Agenda

- Szabályozások (inf.sec.)
  - Jogszabályi
  - Iparági
- Módszertanok (inf.sec.)
  - Szabványok és best practise
- Megfelelés – Compliance
- Példák, kézzelfogható esetek, tapasztalatok
- Kérdezzetek bátran on the fly

Miért is szabályozunk?

- Kritikus IT függőség – információs társadalom
  - Társadalmi érdekek, kritikus IT infrastruktúra és szolgáltatások védelme
  - Vállalati saját érdekek, optimális védelmi szint fenntartása

- Mert védelmet ad? Biztonságot?
- Mert viszonyítási pontot ad?
- Mert irányt mutat?
- Mert egyenlő(bb) viszonyokat teremt?
- Mert növeli az átláthatóságot?

Szabályozások ismérvei

- Szabályozunk?
  - Jogszabályi EU, HU, Iparági
  - Törvény, rendelet,
  - Szabványok, ajánlások
  - Anyavállalati, Vállalati
- Szabályozások ismérvei
  - célja
  - tárgya
  - mélysége
  - hatóköre
  - ereje

Információvédelem kérdései

- Szabályozási célok meghatározása:
  - (Mit?)Milyen információt akarunk védeni?
  - (Mitől?) Mitől kell védeni azokat az információkat?
  - (Miért?) Miért fontos mindez nekünk?
  - Milyen egyéb kapcsolódó külső (pl. jogi) előírásnak kell még megfelelni?

- Szabályozás tartalmi elemei:
  - Tiszta **felelősségi körök**, szerepkörök (Ki?)
  - Tiszta **feladat** és **követelmény** leírás (Mit? Hogyan?) - RACI
  - Egyértelmű válasz a **gyakoriság** kérdéseire (Mikor?)

Hazai jogszabályok
(EU direktívák mentén)

- 2011. évi CXII. Törvény az információs önrendelkezési jogról és az információszabadságról
  - Személyes adatok védelme
  - Nemzeti Adatvédelmi és Információszabadság Hatóság
  - http://www.naih.hu/

331/A/2001. számú adatvédelmi biztosi állásfoglalás: a munkáltató csak az érintett hozzájárulásával tekinthet be a munkavállaló munkahelyi e-mail címén történő levelezésébe.

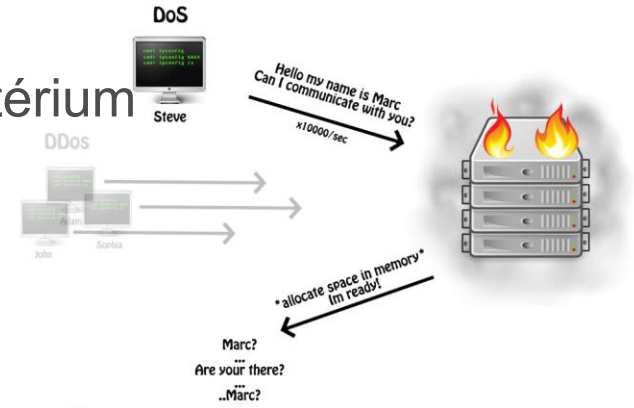
570/A/2001. számú adatvédelmi biztosi állásfoglalás: a munkáltató csak akkor ismerheti meg a munkavállaló Internet-használatával kapcsolatos adatait, ha előzetesen felhívta a figyelmét az ezzel kapcsolatos korlátozásra és az ellenőrzés lehetőségére.

Hazai jogszabályok
(EU direktívák mentén)

- 2001. évi XXXV. tv. Az elektronikus aláírásról
  - E-számla -> ÁFA törvény
- 1996. évi CXII. Törvény a hitelintézetekről és a pénzügyi vállalkozásokról
  - HPT 13/C § Informatikai rendszer védelme
  - PSZAF
  - http://www.pszaf.hu/
  - 4/2012. számú Vezetői körlevél a pénzügyi szervezeteknél a közösségi és publikus **felhőszolgáltatás** Igénybevételéből eredő kockázatokról (SLA)
  - 1/2009 sz. az internet-biztonsági kockázatokról (2 faktor)

Hazai jogszabályok
(EU direktívák mentén)

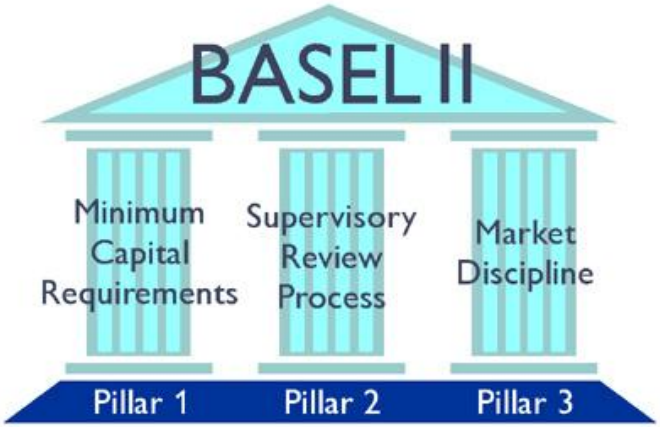
- 85/2012. (IV. 21.) Korm. Rendelet Az elektronikus ügyintézés részletes szabályairól
  - ~~223/2009. (X. 14.) Korm. Rendelet az elektronikus közszolgáltatás biztonságáról~~
- A Kormány 1139/2013. (III. 21.) Korm. Határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
  - CERT HU – Nemzeti Hálózatbiztonsági Központ
  - http://www.cert-hungary.hu/
  - A Közigazgatási és Igazságügyi Minisztérium Nemzeti Biztonsági Felügyelet (NBF)
  - Ddosol a híradó ;)



Nemzetközi szabályozások

- HIPAA / HITECH Act
- PCI DSS v2.0
  - Payment card industry data security standard
- SOX (404)
- Bazel II (and III. in progress)

HIPAA
Health Insurance Portability and Accountability Act



Vállalati szabályozások

- Politika, elvek, célok, hitvallás, nyilatkozat
- Szabályzat
- Eljárások, Utasítások, Tervek
- Flyerek, fényújság, email,
- tudatosítás, képzés

Segítőkezek a rögös úton…

Szabványok, ajánlások

- Szabványok, tanúsítványok
  - ISO27001
  - ISO20000 – alias **ITIL (v3)**
  - COBIT (5.0)
  - ISO15408 (**C**ommon **C**riteria) / MIBÉTS
  - KIB25 , MIBIK - Magyar informatikai biztonsági keretrendszer
  - ISO 22301, ISO 27031 (BCP/DRP)
- Ajánlások
  - Szakmai ajánlások
    - MELASZ - http://melasz.hu/lang-hu/melasz-ready-ajanlas
    - NIST - http://csrc.nist.gov/
    - ISACA – http://www.isaca.org
    - CSA - https://cloudsecurityalliance.org/
    - OWASP - https://www.owasp.org/index.php/Main_Page
      - Web application security
  - EU ajánlások
  - Felügyeleti ajánlások (PSZÁF, ÁSZ, KEHI, NMHH)

ISO27000-es család

- MSZ ISO/IEC 27001:2006 – Magyar szabvány (BS 7799)
- Fontosabb kötetek:
  - ISO 27000 – Szószedet és terminológia
  - **ISO 27001** – Az informatikai biztonság irányítási rendszere
    - ISMS (kialakítás, működtetés, ellenőrzés, fenntartás) + követelmény gyűjtemény – Auditálható!
    - BS 7799-2:2002
  - **ISO 27002** – Gyakorlati útmutató, best practise
    - ISO/IEC 17799:2005
  - ISO 27003 - Kialakítási irányelvek, tanúsítási útmutató
  - ISO 27004 – Eredményesség, inf. biz.t mérése
  - **ISO 27005** - Kockázatmenedzsment
    - BS 7799-3:2005

ISO27000-es család

- További kötetek:
  - ISO 27006 – Tanúsító szervezettel szembeni követelmények
  - ISO 27007 – Útmutató ISMS audithoz
  - **ISO 27031** – DRP szabvány
  - ISO 27032 – cyber-biztonságra vonatkozó irányelvek
  - ISO 27033 – hálózatbiztonságra vonatkozó irányelvek
  - ISO 27034 – alkalmazás biztonságra vonatkozó irányelvek

ISO27001 – 1/2

- Felépítése:
  - 1. Alkalmazási terület
  - 2. Rendelkező hivatkozások
  - 3. Szakkifejezések és meghatározásuk
  - **4. Az információvédelem irányítási rendszere**
  - 5. A vezetőség felelőssége
  - 6. Belső ISMS-auditok
  - 7. Az ISMS vezetőségi átvizsgálása
  - 8. Az ISMS fejlesztése
  - **A melléklet (előírás): Szabályozási célok és intézkedések**
  - B melléklet (tájékoztatás): Az OECD-irányelvek és e nemzetközi szabvány
  - C melléklet (tájékoztatás): Kapcsolat az ISO 9001:2000, az ISO 14001:2004 és e nemzetközi szabvány között

ISO27001 – 2/2 – „A Melléklet”

- A konkrét technikai követelmények, avagy kontrollok:
  - A5. Biztonsági szabályzat
  - A6. Az információ-biztonság szervezete
  - A7. Vagyontárgyak kezelése
  - A8. Az emberi erőforrások biztonsága
  - A9. Fizikai védelem és a környezet védelme
  - A10. A kommunikáció és az üzemeltetés irányítása
    - Üzemeltetés, harmadik felek, rendszertervezés, vírus, mentések, hálózatbiztonság, adathordozók, információcsere, e-commerce, naplózás
  - A11. Hozzáférés-ellenőrzés
    - (OSI – network, OS, App, user)
  - A12. Információs rendszerek beszerzése, fejlesztése és fenntartása
  - A13. Információbiztonsági incidensek kezelése
  - A14. Működés folytonosságának irányítása
  - A15. Követelményeknek való megfelelés

Kontrollok felépítése

MSZ ISO/IEC 27001:2006

A11.3. Felhasználói felelősségek *Cél:* A jogosulatlan felhasználói hozzáférés, valamint az információk és információfeldolgozó eszközök megrongálásának, illetve eltulajdonításának megelőzése.		
A11.3.1.	Jelszóhasználat	*Intézkedés* A felhasználóktól meg kell követelni, hogy a jelszavak kiválasztásában és használatában a jó biztonság gyakorlatot kövessék.
A11.3.2.	Őrizetlenül hagyott felhasználói berendezések	*Intézkedés* A felhasználóknak biztosítaniuk kell az őrizetlenül hagyott berendezések megfelelő védelmét.
A11.3.3.	A „Tiszta asztal, tiszta képernyő” szabályzata	*Intézkedés* Az iratok és eltávolítható adathordozók tekintetében a „tiszta asztal”, míg az információfeldolgozó eszközök tekintetében a „tiszta képernyő” szabályzatát kell alkalmazni.

ISO27002 - Kontrollok útmutatója

11.3.1. Jelszóhasználat

Intézkedés

A használókat kérjék, hogy a jelszavak kiválasztásában és használatában bevált biztonsági gyakorlatot kövessenek.

Bevezetési útmutató

Minden használót arra kell biztatni, hogy

a) tartsa jelszavait bizalmasan;

b) kerülje a jelszavakra vonatkozó feljegyzések megőrzését (pl. papíron, szoftver állományban vagy kézben tartott eszközökön), hacsak nem lehet biztonságosan tárolni és a tárolási módszer nincs jóváhagyva;

c) cserélje jelszavait, amikor bármilyen jele van a lehetséges rendszer- vagy jelszó-veszélyeztetésnek;

d) válasszon olyan minőségi jelszavakat, amelyeknek elegendő a minimális hossza:

1) könnyen megjegyezhető;

2) nem alapul olyan dolgon, amelyet bárki könnyen kitalálhat vagy személyre vonatkozó információból nyerhet;

3) nem sebezhető szótártámadásokkal (azaz nem áll olyan szavakból, amelyek a szótárakban szerepelnek);

4) nem tartalmaz egymás után következő, azonos, csupa számokból vagy csupa abc betűkből álló karaktereket

e) a jelszavakat szabályos időközönként, vagy a hozzáférések számától függően cserélje (előjogokhoz kapcsolódó jelszavakat sokkal gyakrabban kell cserélni, mint a közönséges jelszavakat) és kerülje mind a korábban használt jelszavak ismételt használatát, mind a már használt jelszavak ciklikus átrendezését;

f) cserélje ideiglenes jelszavait az első bejelentkezéskor;

g) ne írja be jelszavait önműködő bejelentkezési folyamatokba, pl. amelyeket makró- vagy funkcionális billentyűk tárolnak;

h) ne osztozzon egyéni használói jelszavakon mással;

i) ne alkalmazzon azonos jelszót kereskedelmi és nem-kereskedelmi célra.

Ha a használóknak igényük van arra, hogy többszörös szolgáltatáshoz, rendszerhez vagy platformhoz is hozzáférjenek és ezért elvárják tőlük, hogy több külön jelszót is tartsanak fenn, akkor figyelmeztessék őket, hogy van lehetőségük valamennyi szolgáltatáshoz egyetlen minőségi jelszó alkalmazására (lásd e szakasz d) pontját), ahol a használót biztosítják, hogy ésszerű védelmi szintet hoztak létre a jelszó tárolásához minden szolgáltatásban, rendszerben vagy platformon.

Kontrollok felépítése

A9.2. Berendezések védelme *Cél:* A vagyontárgyak elvesztésének, károsodásának, eltulajdonításának, illetve megrongálásának, valamint a szervezeti működés fennakadásának megelőzése.		
A9.2.1.	Berendezések elhelyezése és védelme	*Intézkedés* A berendezéseket úgy kell elhelyezni, illetve védeni, hogy csökkenjen a környezeti fenyegetésekből és veszélyekből eredő kockázat, valamint a jogosulatlan hozzáférés lehetősége.
A9.2.2.	Közműszolgáltatások	*Intézkedés* A berendezéseket védeni kell a közüzemi létesítményekben bekövetkező meghibásodások okozta áramkimaradásoktól és más kiesésektől.

Kontrollok felépítése

A8.2 Az alkalmazás időtartama alatt

Cél: Annak biztosítása, hogy valamennyi alkalmazott, szerződő vállalkozó és felhasználó harmadik fél legyen tudatában az információ biztonságát fenyegető veszélyeknek és nyugtalanító tényezőnek, saját felelősségének és kötelezettségeinek, továbbá, hogy legyenek felkészülve mindennapi munkájuk során a szervezet biztonsági politikájának támogatására, s az emberi hibából eredő kockázat csökkentésére.

A8.2.1.	A vállalatvezetés felelőssége	*Intézkedés* A vállalatvezetésnek meg kell követelnie alkalmazottaitól, a szerződőktől és a felhasználó harmadik felektől, hogy a biztonságot a szervezet által meghatározott politikáknak és eljárásoknak megfelelően alkalmazzák.
A8.2.2.	Az információbiztonság tudatosítása, oktatás és képzés	*Intézkedés* A szervezet valamennyi alkalmazottját és, ahol ez jelentőséggel bír, a szerződőket és a felhasználó harmadik feleit megfelelő, tudatosító képzésben kell részesíteni, és a munkaköri feladataiknak megfelelően a szervezeti szabályzatok és eljárások tekintetében rendszeresen friss ismeretanyaggal kell ellátni.
A8.2.3.	Fegyelmi eljárás	*Intézkedés* Hivatalos fegyelmi eljárást kell lefolytatni a biztonsági előírásokat megsértő alkalmazottakkal szemben.

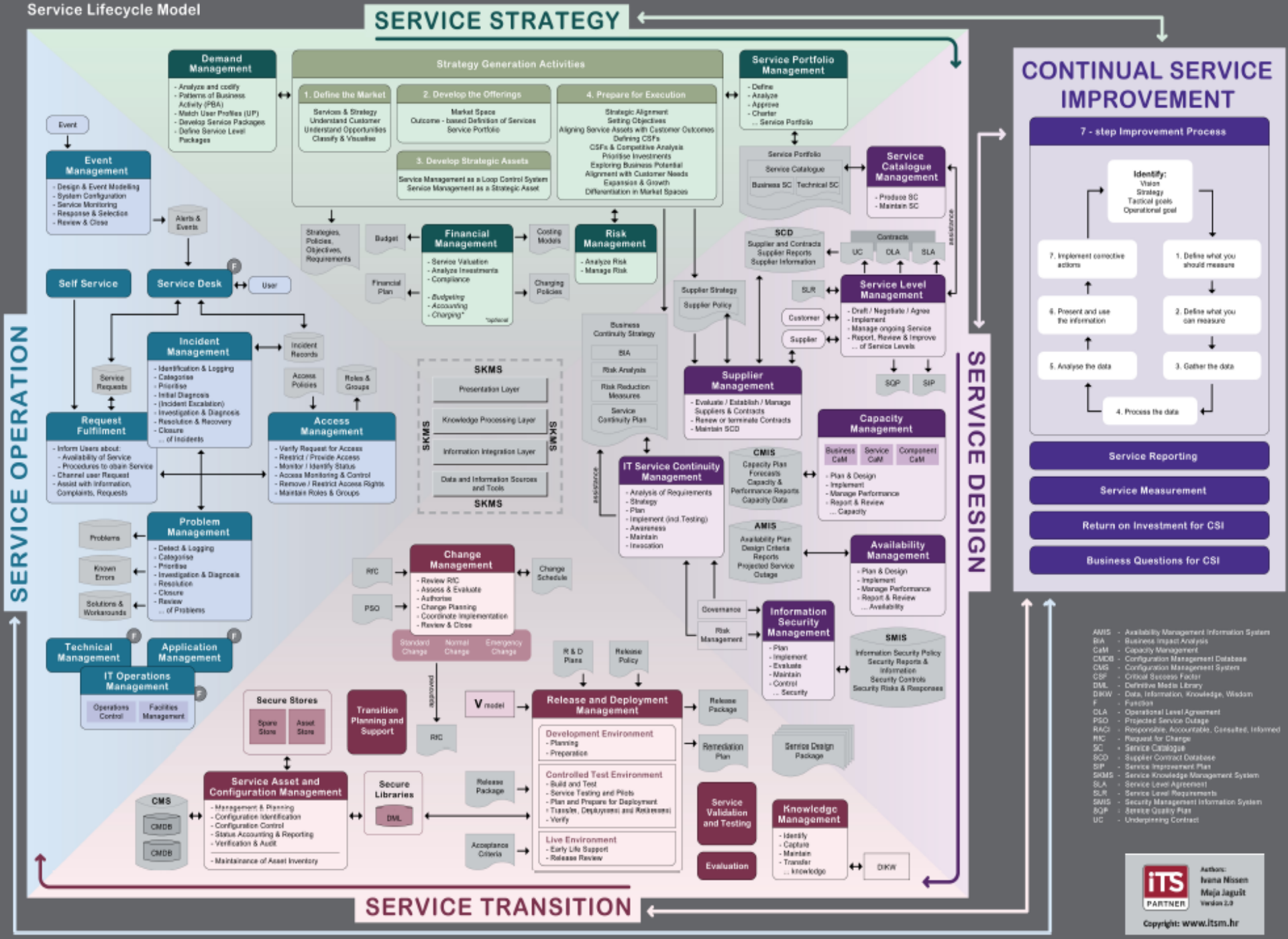
Megszemélyesítés veszélyei

- Ingatlanos honlap:
  - http://www.ingatlanbazar.hu/-><-http://www.ingatlanbazar.com/
- Különbség az ÁSZF-ben rejtezik!
  - Seychelle-szigeteki bejegyzésű… (off-shore)
  - A szolgáltatás ***Free of charge*** (csillagok azonban jelentéssel bírnak)
    - A hirdetés első 30 napja ingyenes csak, de a szerződés minimum 12 hónapra szól…
    - Minden e-mail értesítő ára 500 HUF - :D

ISO20000 – ITIL v3

- ITIL - *Information Technology Infrastructure Library*
  - v1, v2, v3 a jelenlegi
  - IT szolgáltatások kezelésének bevált gyakorlati gyűjteményét tartalmazza
  - *Service, CI, CMDB, SLM, SLA, OLA, KPI, ITSCM….*
  - Hazai szervezete: http://www.itsmf.hu/
  - 5 kötet, 27 folyamat
- Kötetei:
  - Szolgáltatás-stratégia (Service Strategy)
  - Szolgáltatás-tervezés (Service Design)
  - Szolgáltatás-létesítés és -változtatás (Service Transition)
  - Szolgáltatás-üzemeltetés (Service Operation)
  - …e Improvement)

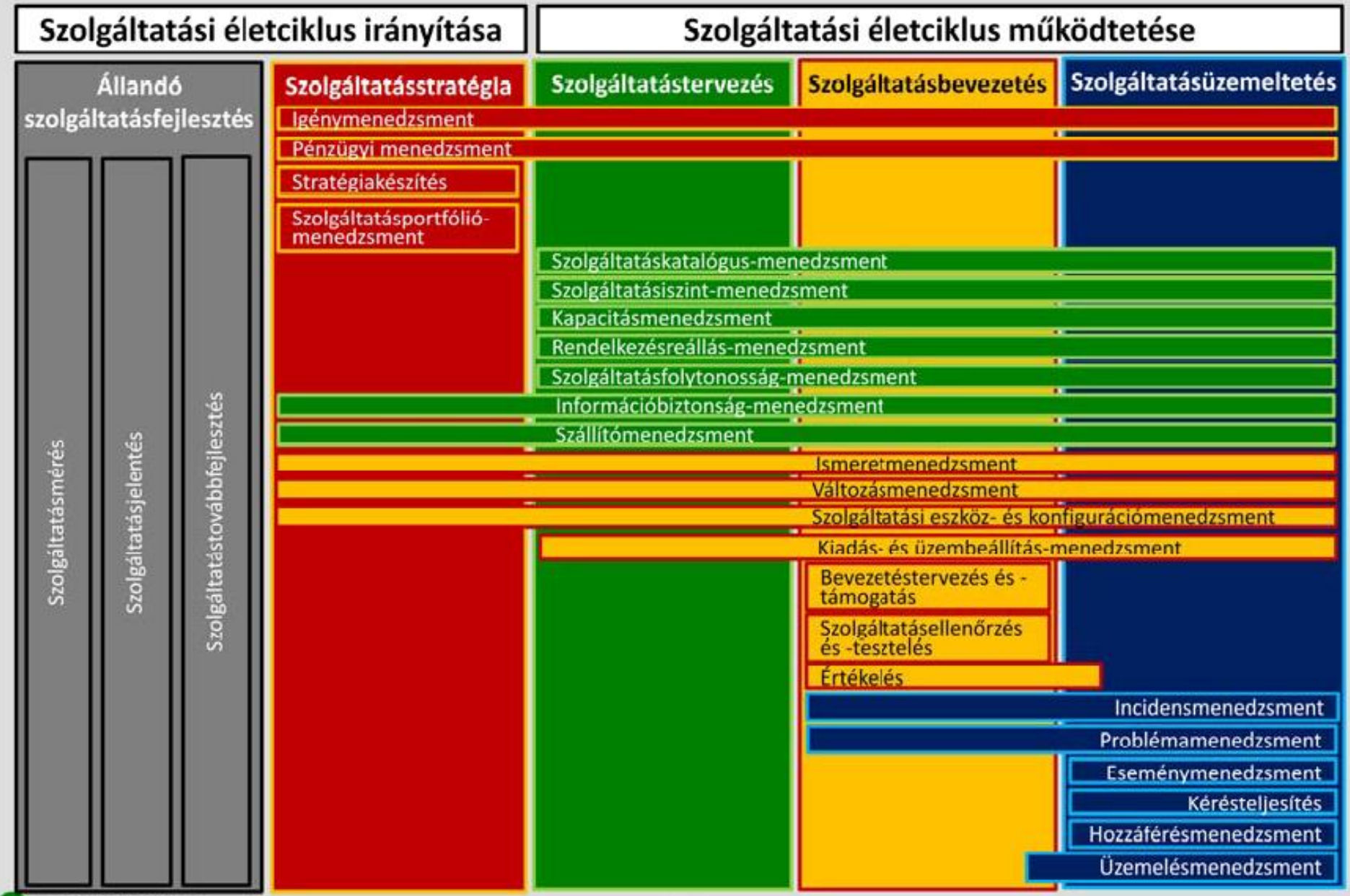
ITIL® V3
Service Lifecycle Model



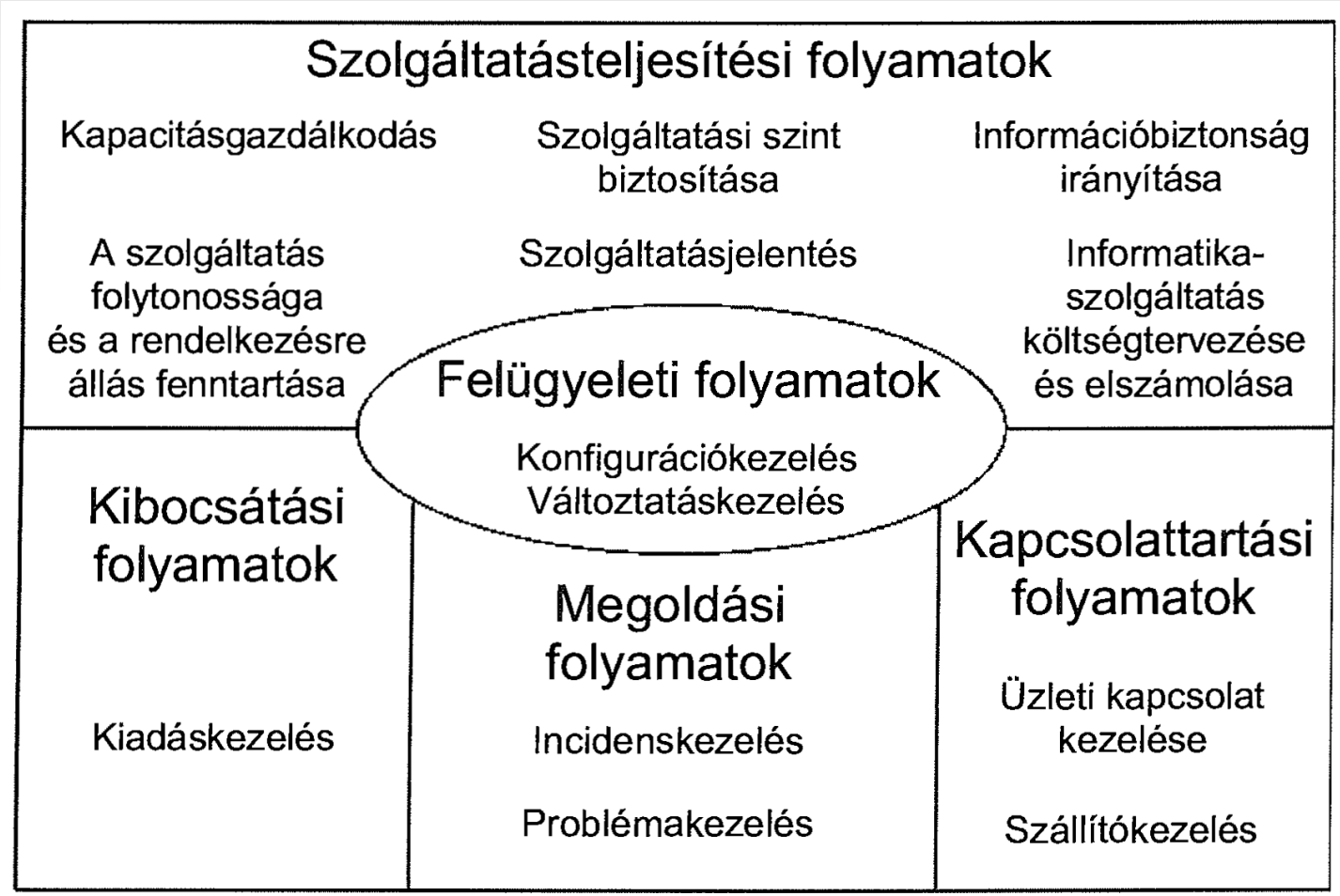
AMIS - Availability Management Information System
BIA - Business Impact Analysis
CaM - Capacity Management
CMDB - Configuration Management Database
CMS - Configuration Management System
CSF - Critical Success Factor
DML - Definitive Media Library
DIKW - Data, Information, Knowledge, Wisdom
F - Function
OLA - Operational Level Agreement
PSO - Projected Service Outage
RACI - Responsible, Accountable, Consulted, Informed
RfC - Request for Change
SC - Service Catalogue
SCD - Supplier Contract Database
SIP - Service Improvement Plan
SKMS - Service Knowledge Management System
SLA - Service Level Agreement
SLR - Service Level Requirements
SMIS - Security Management Information System
SQP - Service Quality Plan
UC - Underpinning Contract

Authors:
Ivana Nissen
Maja Jagušt
Version 2.0

ITIL szolgáltatási életciklus folyamatai



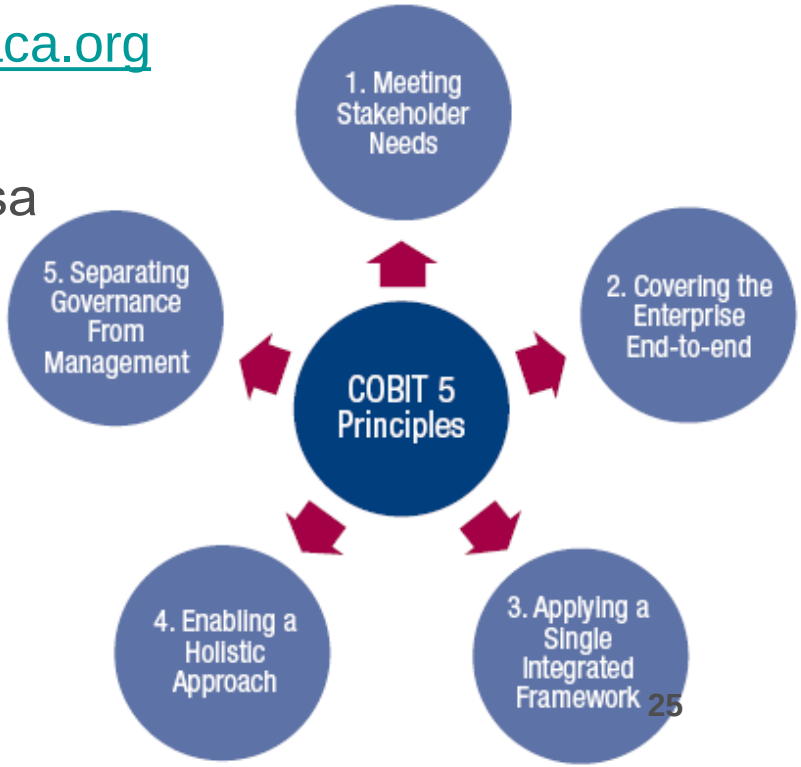
ISO 20000


Szolgáltatásteljesítési folyamatok
Kapacitásgazdálkodás
Szolgáltatási szint biztosítása
Információbiztonság irányítása
A szolgáltatás folytonossága és a rendelkezésre állás fenntartása
Szolgáltatásjelentés
Informatika-szolgáltatás költségtervezése és elszámolása
Felügyeleti folyamatok
Konfigurációkezelés
Változtatáskezelés
Kibocsátási folyamatok
Kiadáskezelés
Megoldási folyamatok
Incidenskezelés
Problémakezelés
Kapcsolattartási folyamatok
Üzleti kapcsolat kezelése
Szállítókezelés

COBIT 5.0

- COBIT – "Információra és a kapcsolatos technológiára vonatkozó kontroll célkitűzések„
  - Informatikai Irányítási és Ellenőrzési Módszertan
  - 2012-ben jelent meg a COBIT 5.0
  - Gondozó szervezete: http://www.isaca.org
  - Az informatikai erőforrások

  az üzleti célok szolgálatába való állítása



COBIT 5.0

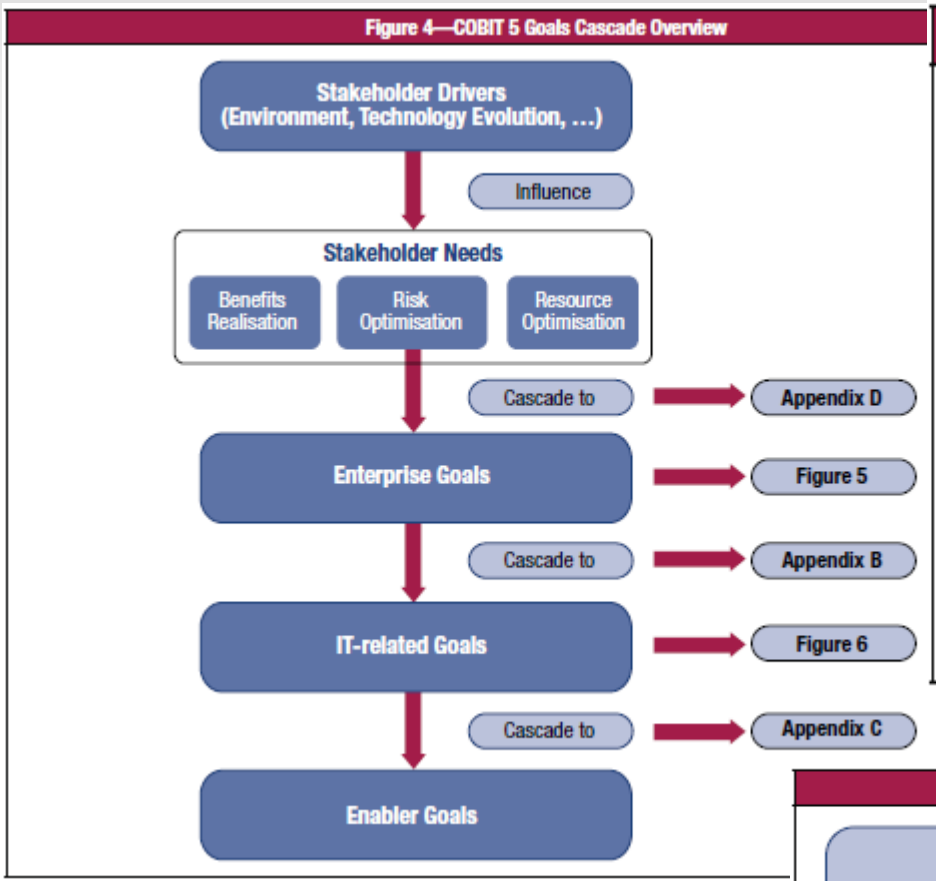


Figure 4—COBIT 5 Goals Cascade Overview
Stakeholder Drivers (Environment, Technology Evolution, ...)
Influence
Stakeholder Needs
Benefits Realisation
Risk Optimisation
Resource Optimisation
Cascade to
Appendix D
Enterprise Goals
Figure 5
Cascade to
Appendix B
IT-related Goals
Figure 6
Cascade to
Appendix C
Enabler Goals

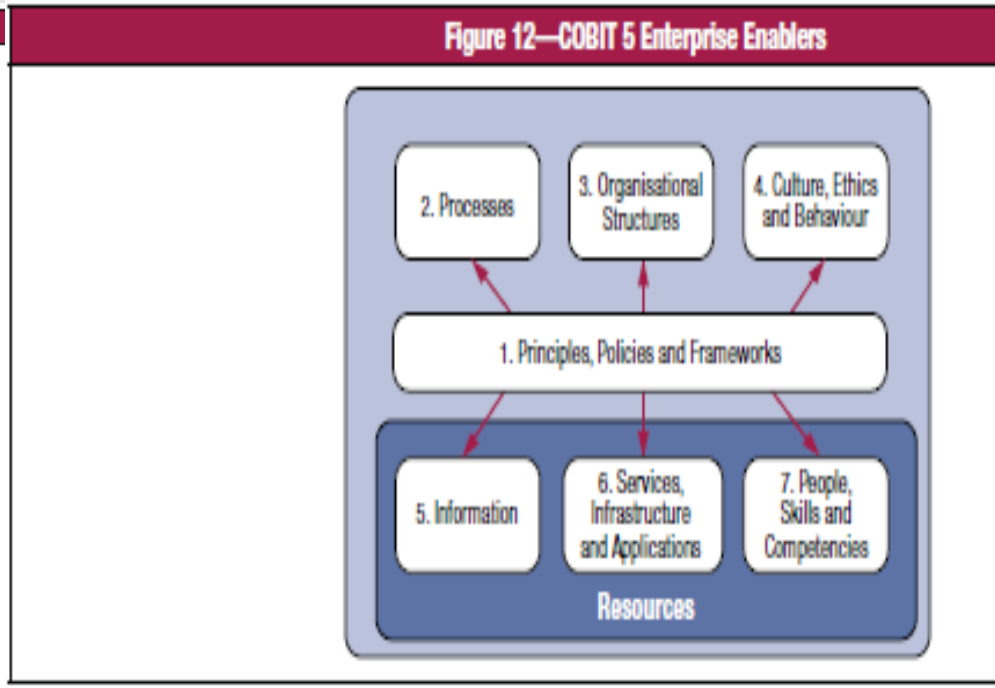


Figure 12—COBIT 5 Enterprise Enablers
2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

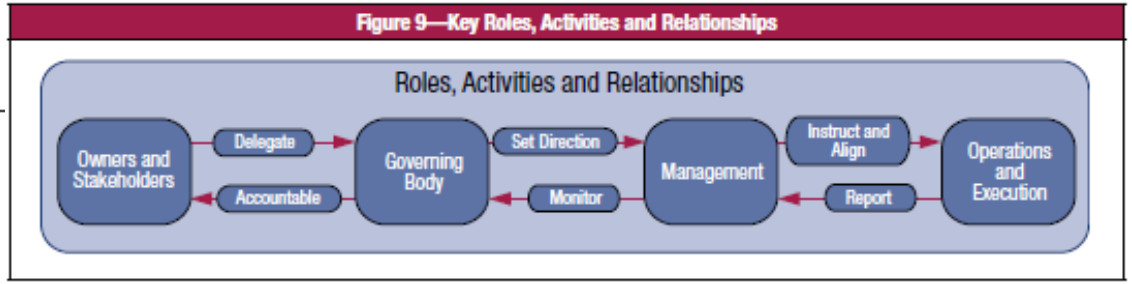


Figure 9—Key Roles, Activities and Relationships
Roles, Activities and Relationships
Owners and Stakeholders
Delegate
Accountable
Governing Body
Set Direction
Monitor
Management
Instruct and Align
Report
Operations and Execution

COBIT 5.0 Process

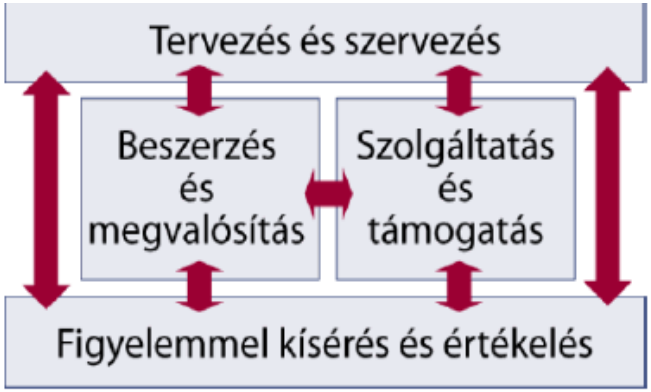
- 37 folyamat:

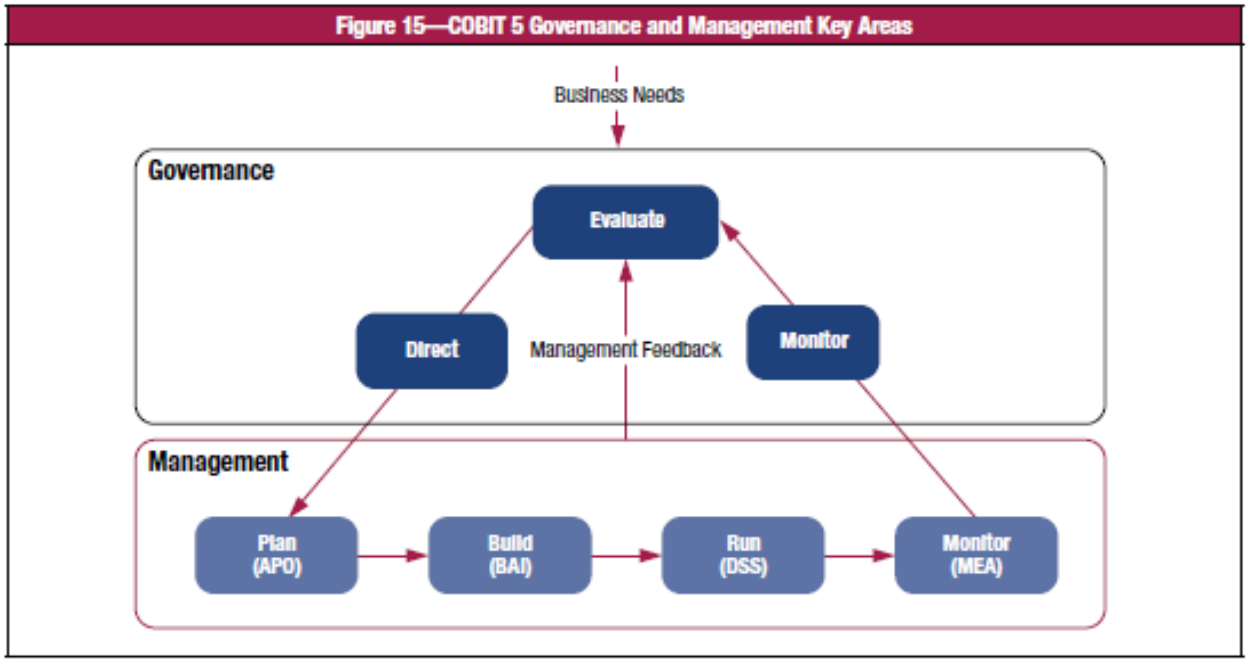
32 Management:

- Align, Plan and Organise (APO)
- Build, Acquire and Implement (BAI)
- Deliver, Service and Support (DSS)
- Monitor, Evaluate and Assess (MEA)

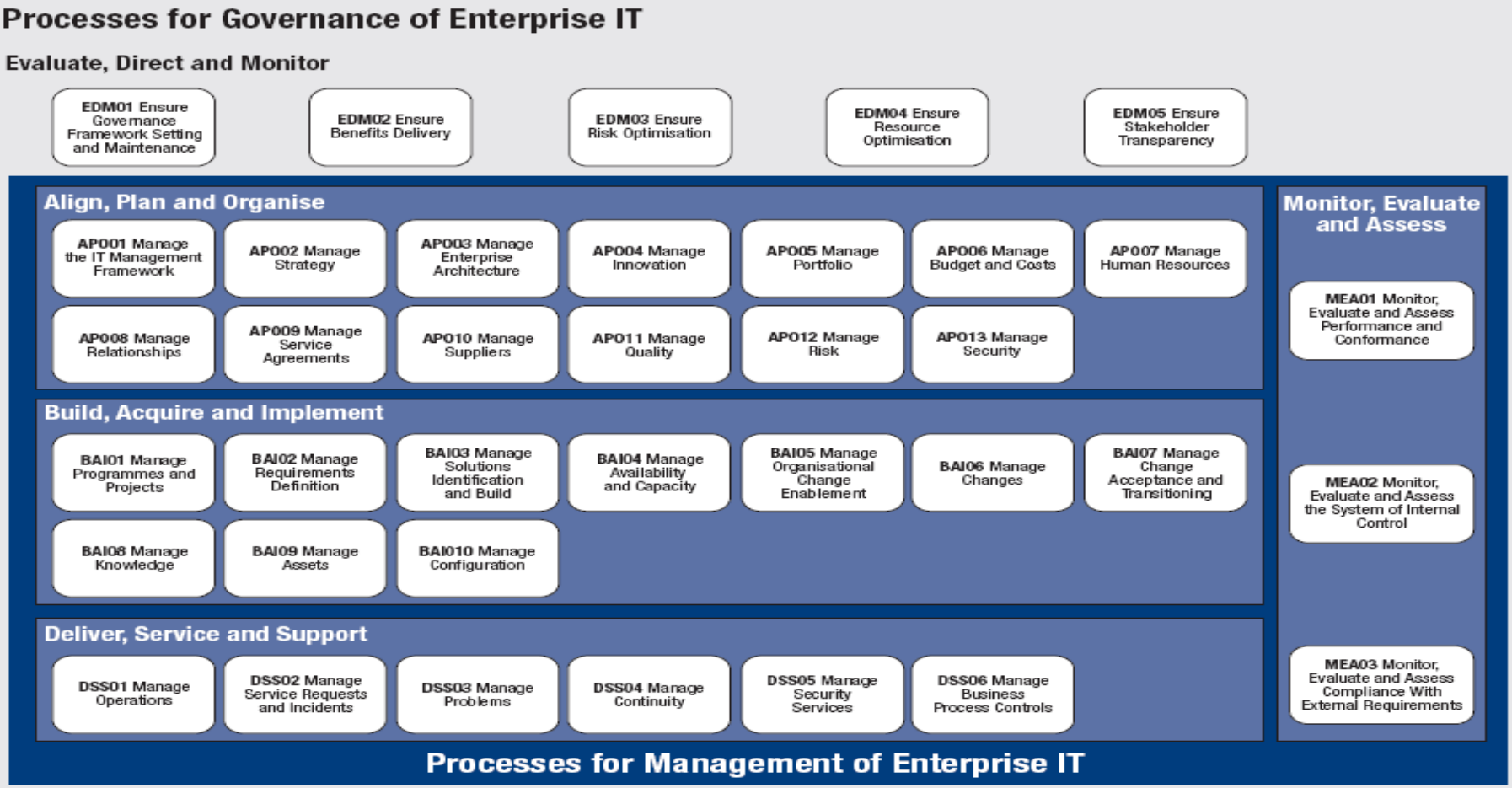
5 Governance:

- Evaluate, Direct and Monitor (EDM)





COBIT 5.0 Process reference modell



ITIL - Cobit Mapping

						Service Support					Service Delivery				
		Business Perspective	Application Mgmt	Infrastructure Mgmt	Security Mgmt	Incident Mgmt	Problem Mgmt	Configuration Mgmt	Change Mgmt	Release Mgmt	Service Level Mgmt	Capacity Mgmt	Availability Mgmt	IT Service Continuity Mgmt	Financial Mgmt for IT Services
PO	***Plan & Organise***														
PO1	Define a Strategic IT Plan	x		x											
PO2	Define the Information Architecture			x											
PO3	Determine Technological Direction			x											
PO4	Define the IT Processes, Organisation and Relationships	x			x	x	x	x	x	x	x	x	x	x	x
PO5	Manage the IT Investment														x
PO6	Communicate Management Aims and Direction	x													
PO7	Manage IT Human Resources	x										x			
PO8	Manage Quality	x	x	x	x	x	x	x	x	x	x	x	x	x	x
PO9	Assess and Manage IT Risks	x			x						x		x	x	
PO10	Manage Projects		x												
AI	***Acquire & Implement***														
AI1	Identify Automated Solutions		x	x											
AI2	Acquire and Maintain Application Software		x							x					
AI3	Acquire and Maintain Technology Infrastructure			x											
AI4	Enable Operation and Use		x												
AI5	Procure IT Resources									x		x			x
AI6	Manage Changes								x						
AI7	Install and Accredit Solutions and Changes									x					
DS	***Deliver & Support***														
DS1	Define and Manage Service Levels										x				
DS2	Manage Third-Party Services										x				
DS3	Manage Performance and Capacity											x			
DS4	Ensure Continuous Service												x	x	
DS5	Ensure Systems Security				x										
DS6	Identify and Allocate Costs														x
DS7	Educate and Train Users	x								x					
DS8	Manage Service Desk and Incidents					x									
DS9	Manage the Configuration							x							
DS10	Manage Problems						x								
DS11	Manage Data			x	x								x	x	
DS12	Manage Physical Environment			x	x			x	x						
DS13	Manage Operations			x	x			x	x						
ME	***Monitor and Evaluate***														
ME1	Monitor and Evaluate IT Performance	x		x	x	x	x	x	x	x	x	x	x	x	x
ME2	Monitor and Evaluate Internal Control				x	x	x	x	x	x	x	x	x	x	x
ME3	Ensure Regulatory Compliance				x			x	x	x				x	
ME4	Provide IT Governance	x			x	x	x	x	x	x	x	x	x	x	x

PCI DSS

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

PCI DSS

- Self Assessment Questionnaires
- Payment Application Data Security Standard (PA-DSS)
- Qualified Security Assessors (QSAs)
- Payment Application Qualified Security Assessors (PA-QSAs)
- Approved Scanning Vendors (ASVs)
- Internal Security Assessor (ISA) (vállalatok belső alkalmazottai)
- https://www.pcisecuritystandards.org

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data [1]	Full Magnetic Stripe Data [2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

SOX az IT-ben

- Sarbane's and Oxley Act USA – 2002 Július 30.
  - Enron, Worldcom - > Protect stakeholders interests
  - „Pénzügyi riportok megbízhatóságának növelése"
  - „Felsővezetői büntetőjogi felelősségvállalás"
  - Sarbanes–Oxley Section 404: Belső ellenőrzési rendszer és a kontrollok értékelése, nyilatkozat tétel.
  - Könyvvizsgáló (big4) értékel
  - IT érintettség elsősorban a 404 kapcsán, IT kontrolok
  - Hatókör: Amerikai tőzsdén (SEC) jegyzett vállalat és leányai!
    - Voda, Flextronics, Tyco…

SOX és SAS70 az IT-ben

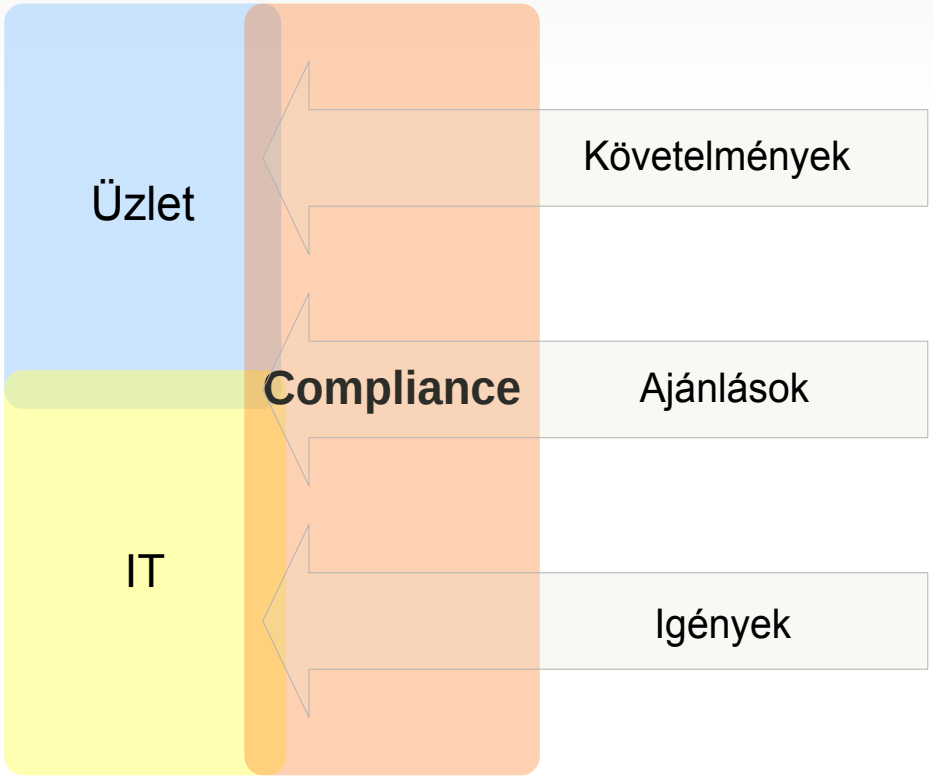
- SOX 404 követelmények
  - Dokumentált folyamatok és kontrolok
  - Megismételhető, dokumentált, bizonyítható tesztek
  - Folyamatos, mintavételezésen alapuló végrehajtás
  - SOD (Segregation of duty)
- SAS 70
  - A SAS 70 hivatalos jelentés valamely szolgáltató szervezet kontroljainak kialakításáról, bevezetéséről és működési hatékonyságáról.
  - Ha a szolgáltatása befolyásolja az ügyfél éves pü beszámolóját

ISO15408 – Common Criteria

- Legfrissebb verzió: CC v3.1. Release 3
- Célja:
  - Egységes értékelési módszertan alapján osztályozni a szoftver/hw **termékeket**, biztonsági minősítés.
- Evaluation Assurance Level (EAL)
  - EAL1 - …. – EAL7 – OS összesen 115 db
    - Microsoft Windows 7, Microsoft Windows Server 2008 R2 - EAL4+
    - Red Hat Enterprise Linux Ver. 5.3 on Dell 11G Family Servers – EAL4+
    - EAL6+ összesen 2 db
- Magyarországon a MIBÉTS (Magyar Informatikai Biztonsági és Tanúsítási Séma)
  - Honosított értékelési módszertan (Logdrill/KÜRT)

Szabályozások és a Compliance

- „Compliance: működési, biztonsági és szabályozási követelményeknek való *megfelelés*.” Üzleti céloknak is!



Megfelelés harmonizálandó területei

Megfelelési vágy

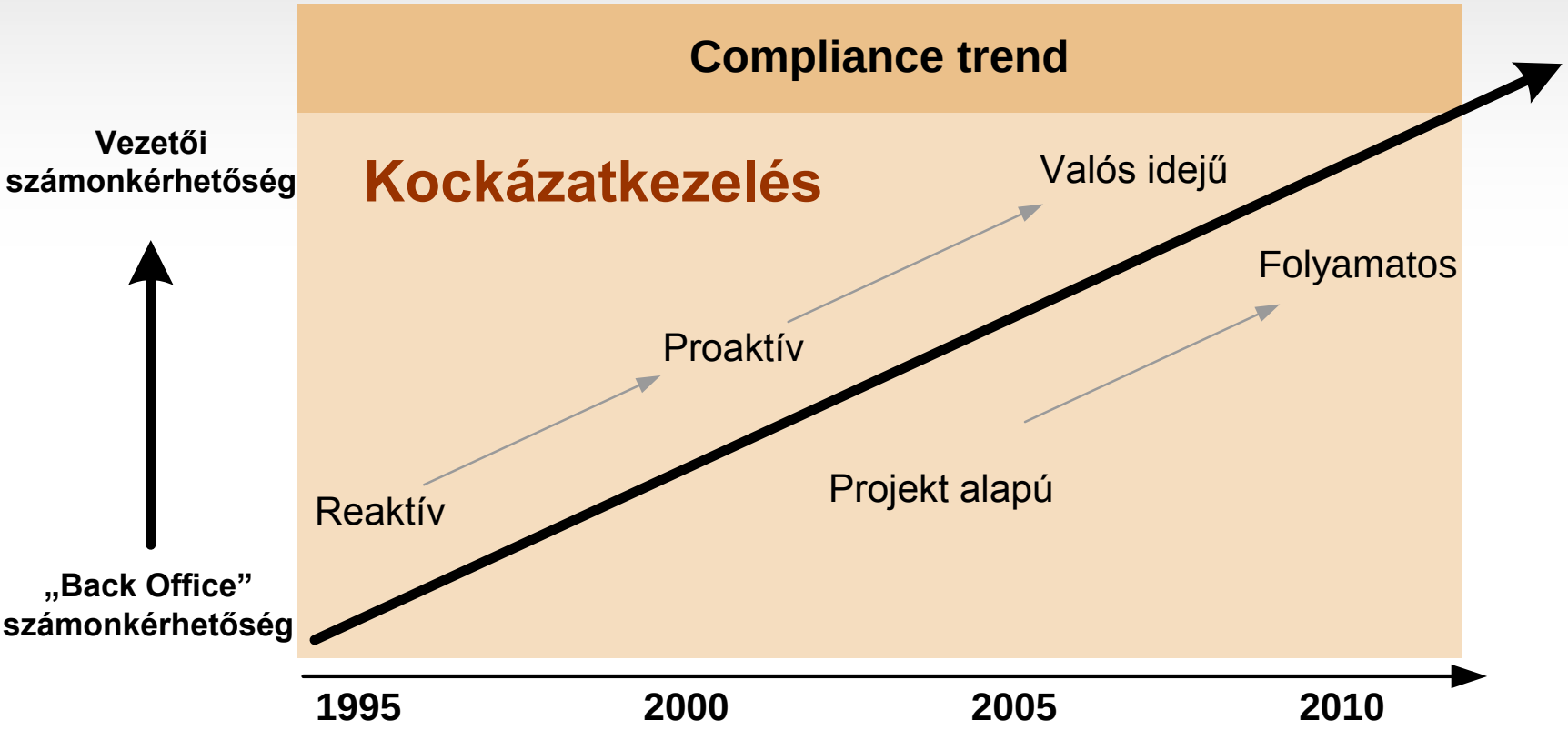
- Törvényi megfelelőség mindenképpen
- Compliance ráfordítások vs Üzleti hatékonyság
- Átláthatóság – Transzparencia, Prudencia
- Hatékonyság növelés, ellenőrzés, elvárások teljesülésének mérhetősége, minőség
  - A Compliance nem határozhatja meg magát a gazdasági tevékenységet, de gondoskodik róla, hogy az akadálytalanul folyhasson, megismételhető, szabály követő gyakorlat alapján
- Tanúsítás

Mérhető a megfelelés?

- Belső Audit
- Független Audit
  - Könyvvizsgálói Audit
  - Minőségügyi Audit
  - IT Audit
- Tanúsítás megszerzése
  - Belső igény és kényszer kell legyen!
  - Már nem előny egy ISO minősítés, hanem követelmény.

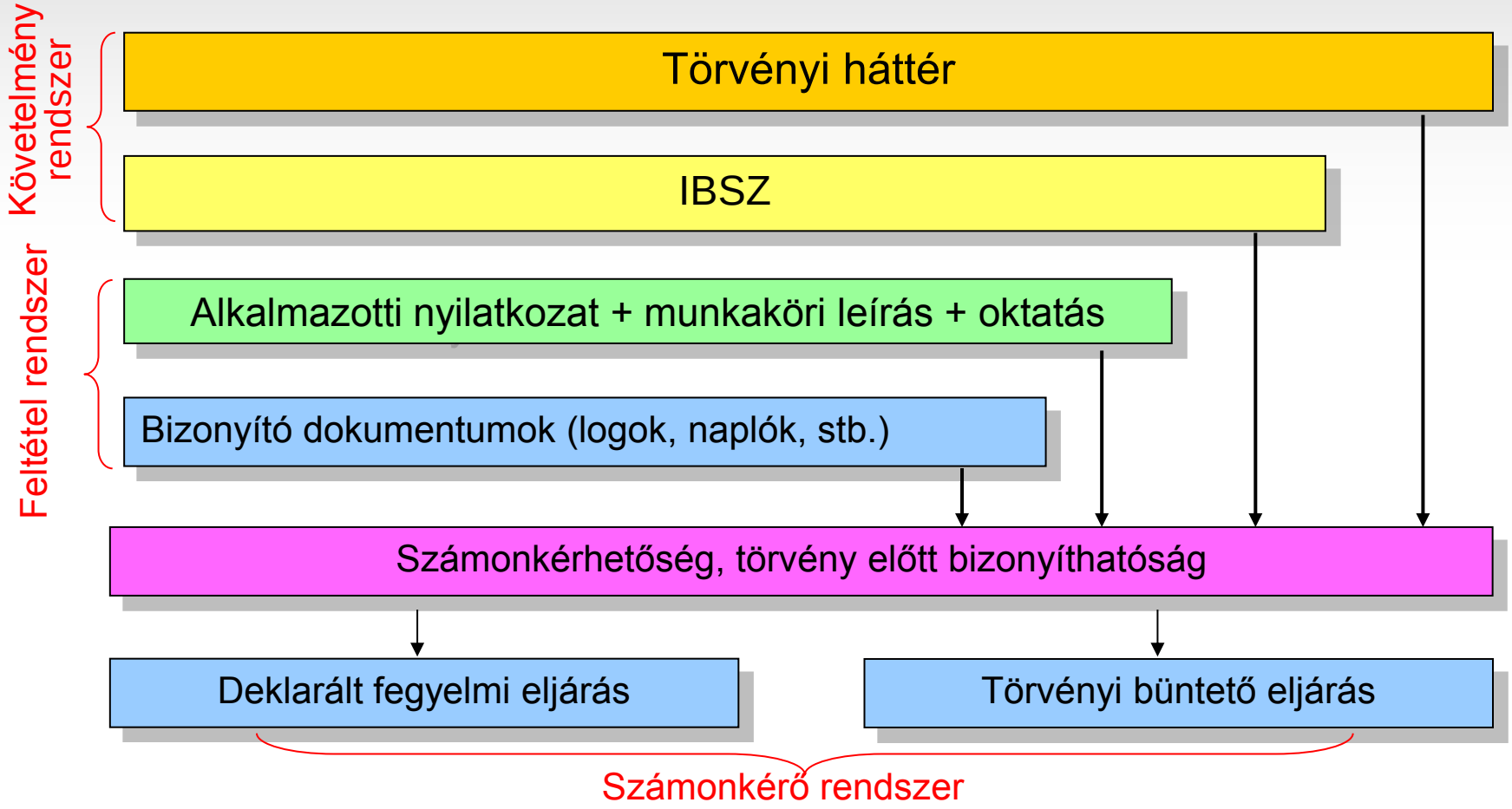
A cél nem a minősítés megszerzése, hanem a MŰKÖDÉSI HATÉKONYSÁG és a VÁLLALT KOCKÁZATOK összhangja.

Megfelelési minták



SW-es támogatás: **SeCube** / KÜRT - http://kurt.hu/termekek/secube/

Számon kérhető szabályzatok



Néhány forrás

- Kevin D. Mitnick: A megtévesztés művészete
- http://www.minosegdoktorok.hu/blog
- http://www.27000.org/
- www.isaca.org
- www.itsmf.hu
- http://www.commoncriteriaportal.org/products/
- http://halozatbiztonsag.hu/documents/MIBETS/Ajanlas_MIBETS.pdf

Utolsó dia

- Kérdések?
- Érdekes volt?
- Ki szeretne dolgozni?

Köszönöm a figyelmet!

Tóthmajor Máté, CISSP, CISA
mate.tothmajor@kurt.hu
www.kurt.hu