INFORMATIKAI PROJEKTELLENŐR

DR. BEINSCHRÓTH JÓZSEF

IT RELEVÁNS MÓDSZERTANOK, SZABVÁNYOK, JOGSZABÁLYOK

Bevezetés: Iránymutatások szükségessége

- **Iránymutatások**
  - Törvény, szabvány - kötelező
  - Ajánlások, módszertanok – követendők a saját jól felfogott érdek szerint
- **Szabvány típusok**
  - „De facto”: konkrét megoldások, amelyeket igen elterjedten használnak. Alkalmazásuk nem kötelező, de célszerű
  - „De jure”: Szabványosítási szervezetek által kiadott, dokumentált szabvány

Tartalom

- **ITIL**
  - Best practice
  - Komponensek
  - Modellek
  - Szolgáltatás biztosítás/támogatás
  - Érettségi modell
- **COBIT**
- **ISO27000 szabványcsalád**
- **2013. évi L. törvény**
- **2011. évi CXII. törvény**

Activity

ITIL: Az IT üzemeltetés bevált gyakorlata – „best practice”

Library: dokumentációsorozat (IT Infrastructure Library)

Egységes szerkezetben dokumentálja az informatikai üzemeltetés bevált gyakorlatát

Nyilvános, gyártófüggetlen keretrendszer

Az informatikai szolgáltatás-irányításra vonatkozik.

A szervezet üzleti tevékenységének eredményes működését teszik lehetővé.

Konzisztens, integrált megközelítést és terminológiát vezet be, amelyek értékes hozzájárulások a szolgáltatás-irányítás területén.

Szempontrendszert: gondoltunk-e mindenre?

Rendező elv: folyamatok (nem rendszerek)

Milyen komponensekre terjed ki az ITIL?

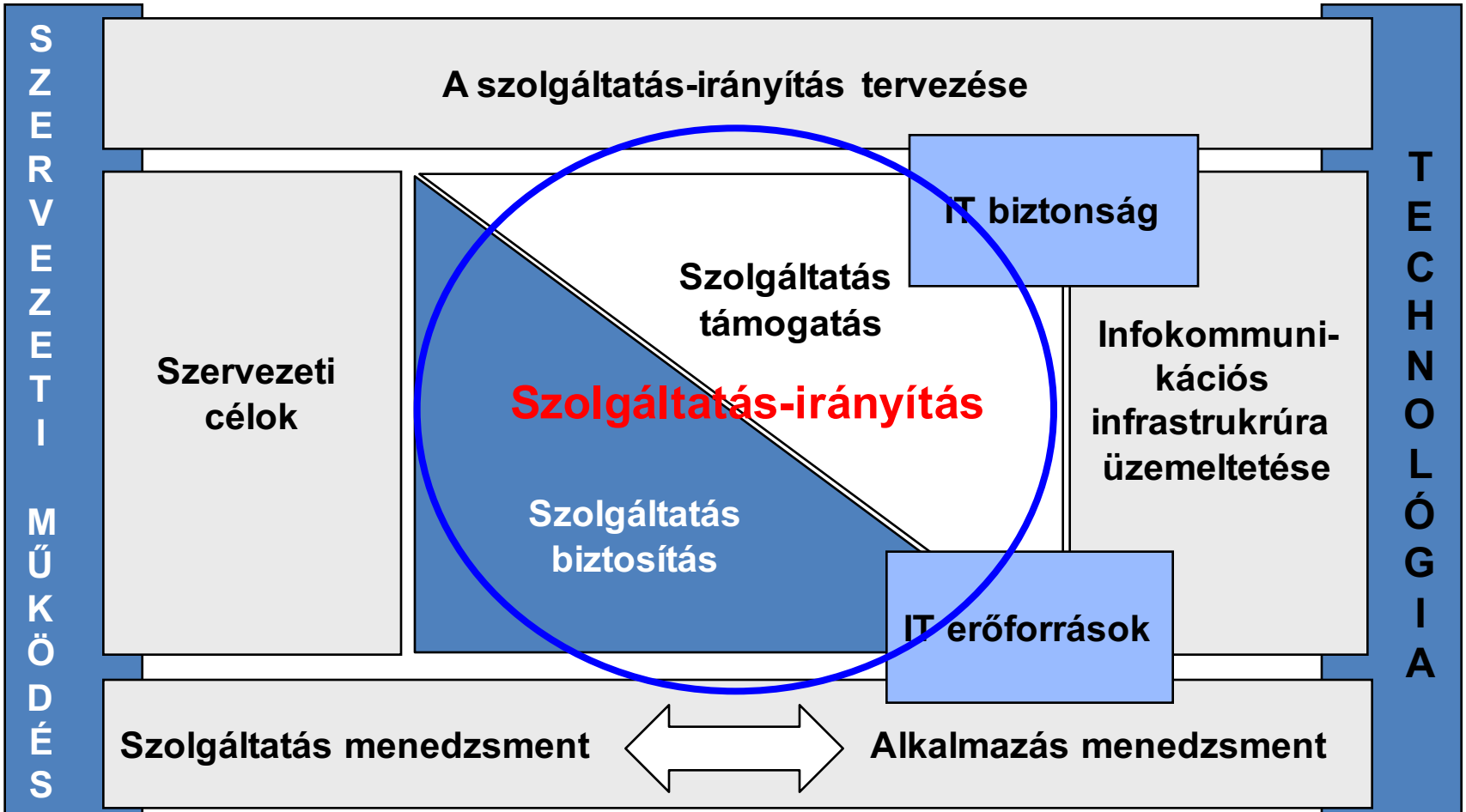
Technológia (Nem kizárólag technológiai, kérdés!)

Eszközök (Eseménykezelő rendszerek, üzleti folyamatok határértékei. Probléma és változáskezelő rendszerek …)

Szervezet (Eszkalációs utak, értesítési mechanizmusok, egyeztetési fórumok, tulajdonos (szolgáltatási tulajdonos, üzleti tulajdonos))

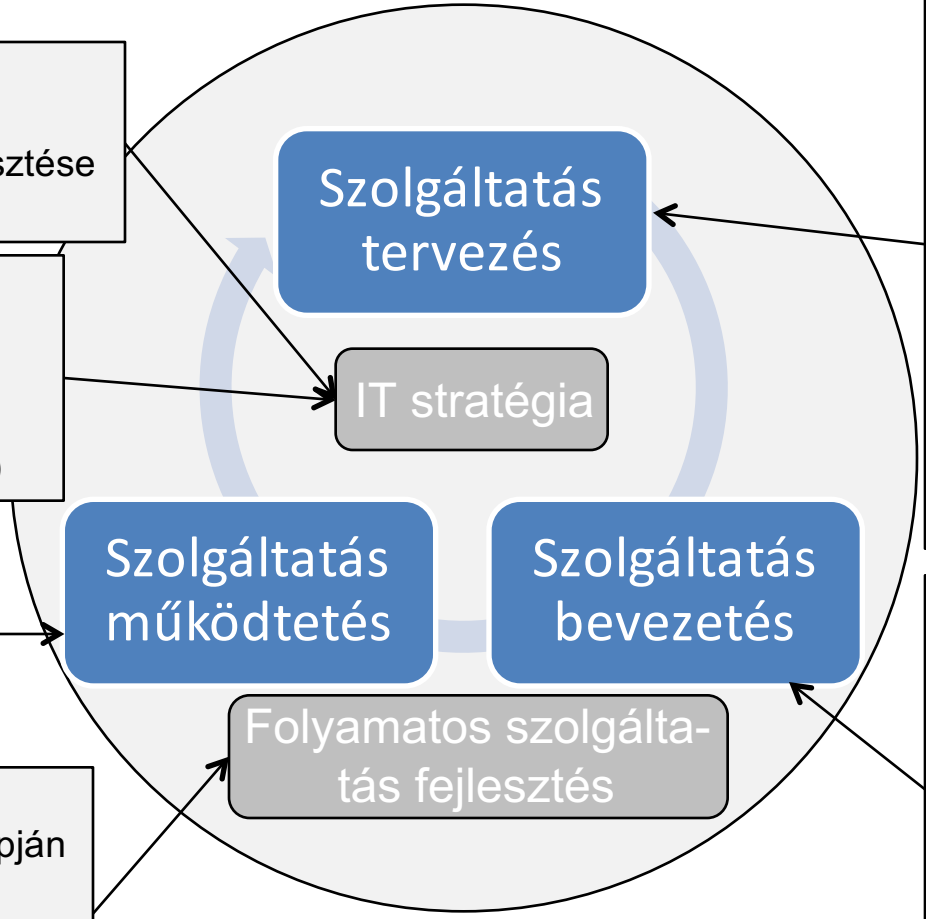
Emberek (Milyen tudás, mennyi ember, szakember szükséges a megbízható üzemeltetéshez?)

ITILv2 modell



Kapcsolat a szervezeti működés és a technológia között

ITILv3 modell



- Piac figyelés
- Kínálat fejlesztés
- A stratégiai erőforrások fejlesztése
- Felkészülés a végrehajtásra

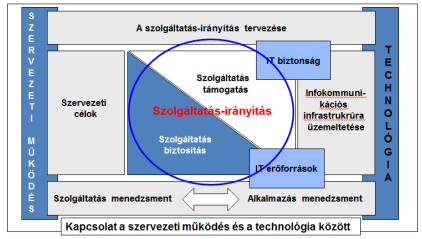
- Pénzügyi irányítás
- Megtérülés (ROI - Return of Investment) stratégiai szint
- Szolgáltatás potfolió mgmt
- Követelés mgmt (beszállítók)

- Eseménykezelés
- Incidenskezelés
- Problémakezelés
- Igények kezelése
- Hozzáférés mgmt

- Üzleti igények
- Fejlesztés a PDCA ciklus alapján
- Riportálás
- Mérés
- Megtérülés (ROI – Return of Investment) szolg. fejl . szint

- Szolgáltatás katalógus mgmt
- Kapacitáskezelés
- Rendelkezésre állás biztosítás
- Informatika-szolgáltatás folytonosság-biztosítás
- IT biztonság mgmt
- Beszállító menedzsment
- Szolgáltatásszint biztosítás

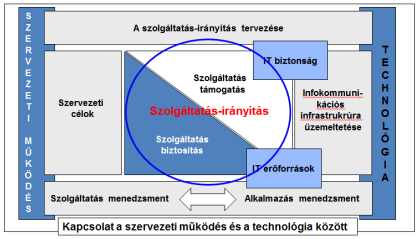
- Bevezetés tervezés és támogatás
- Változáskezelés
- Erőforrás és konfiguráció kezelés
- Kiadáskezelés
- Tesztelés
- Kiértékelés
- Tudásmenedzsment



ITIL - Szolgáltatás támogatás

Ügyfélszolgálat (Szervezeti egység: Service Desk)	• A felhasználók számára szükség esetén **azonnali segítséget** nyújtó szervezete és elérhetőségét lehetővé tevő kommunikációs csatorna
Incidenskezelés (Incident Management)	• A működési zavarok, hibák **lehető legrövidebb időn belül** történő elhárítása előre definiált sémák alapján.
Problémakezelés (Problem Management)	• A működési zavarok, hibák **okainak felderítése** és elhárításukhoz sémák kialakítása, a működési zavarok ismételt előfordulásának megakadályozása
Változáskezelés (Change Management)	• A változások **befogadása** anélkül, hogy az negatív hatással lenne a működésre.
Konfigurációkezelés (Configuration Management)	• Az összes informatikai (üzemeltetési) komponens **rögzítése és felügyelete**
Kiadáskezelés (Release Management)	• Döntés egy-egy új kiadási egység használatba vételéről, a használatba vétel kezdeményezéséről, indokoltságáról. • A használatba vételt megelőző tesztelés és a használatba vétel konkrét **lépéseinek és ütemezésének** meghatározása

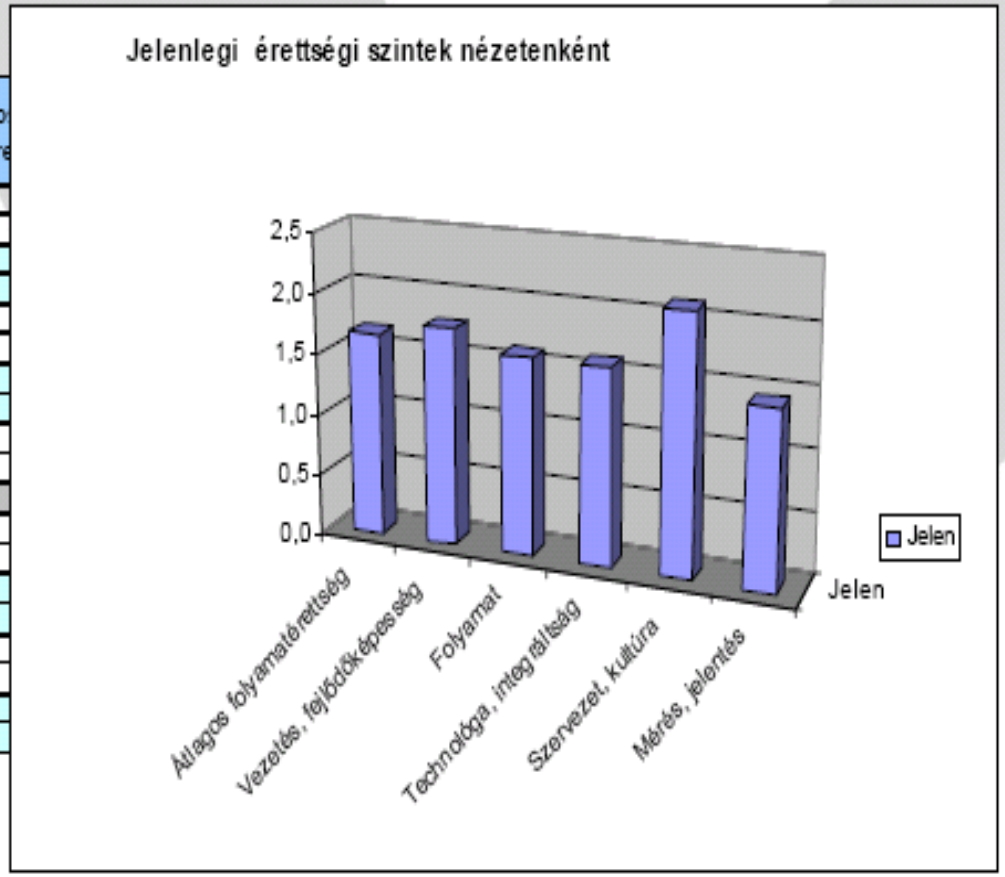
ITIL - Szolgáltatás biztosítás



Szolgáltatásszint biztosítás (Service Level Management - SLM)	• Az informatikai rendszer üzemeltetésének **minőségét** meghatározó megállapodás
Rendelkezésre állás biztosítás (Availability Management - AM)	• Az elvárt rendelkezésre állás eléréséhez szükséges **preventív intézkedések** a technológia, a szervezet és az irányítás területén.
Informatika-szolgáltatás folytonosság-biztosítás (IT Service Continuity Management - ITSCM)	• Az esetleges katasztrófák következtében bekövetkező **kiesések utáni visszaállás** a normál szolgáltatásra reaktív intézkedések alkalmazásával
Kapacitásbiztosítás (Capacity Management– CM)	• A várható kapacitás igények, terhelések felmérése, ezek összevetése a jelenlegi kapacitásokkal, hosszú távon elegendő **informatikai kapacitások biztosítása**
Informatikaszolgáltatás pénzügyi irányítása (Financial Management FM)	• Az igényeknek megfelelő technikai színvonal és szolgáltatási minőség **elfogadható szintű költségek mellett**. • Számviteli rend, ami hitelesen tükrözi a szervezet számára az informatikára fordított költségeket, azok megoszlásá

Az ITIL v3-ban az érettségi modellnek nagy jelentősége van! (Mérés)

Folyamat neve	Rövid név	Állapot	Átlago folyamatére
IT ügyfélszolgálat és Incidenskezelés	SD/IM	Jelen	2,0
Problémakezelés	PM	Jelen	1,5
Konfigurációkezelés	CFG	Jelen	1,5
		Cél	2,0
Változáskezelés	CHG	Jelen	3,0
Kiadáskezelés	REL	Jelen	1,5
Szolgáltatási szintek biztosítása	SLM	Jelen	1,0
		Cél	2,0
Kapacitásbiztosítás	CAP	Jelen	1,0
Rendelkezésreállás biztosítása	AMG	Jelen	1,5
IT szolgáltatásfolytonosság (BCP/DRP)	ITSCM	Jelen	2,0



Az ITIL v3-ban az érettségi modellnek nagy jelentősége van!

Érettségi modell: A fejlettségre vonatkozó mérőszámok előállítására használható.

Hol tartunk?	Hová kívánunk eljutni?	Milyen módon érhetjük el a célt?
Milyen a pozíciónk a versenytársaink-hoz képest?	Hol állunk ezekhez a bevált gyakorlatokhoz képest?	Hogyan érhetjük el a megfelelő irányítást és kontrollt?

Általános érettségi modell

- **0 - Nem létező:** Egyáltalán semmilyen felismerhető folyamat sincsen. A vállalkozás még fel sem ismerte azt, hogy létezik egy olyan terület, amellyel foglalkoznia kell.
- **1 - Kezdeti/Ad Hoc jellegű**: Vannak jelek arra vonatkozóan, hogy a vállalkozás felismerte, hogy létezik egy olyan terület, amellyel foglakoznia kell. Azonban nincsenek szabványosított folyamatok, helyettük ad hoc jellegű megoldásokat alkalmaznak, egyedileg, illetve eseti alapon. Az általános vezetési módszer rendszertelen.
- **2 - Ismétlődő, de ösztönös**: A folyamatok eljutottak arra a szintre, amikor hasonló eljárásokat követnek a különböző, azonos feladatokat végző emberek. A szabványos eljárásoknak nincsen formális oktatása, nincs rendszeres ismertetés és tájékoztatás róluk, és betartásuk az egyének felelőssége. Nagy mértékben hagyatkoznak az egyének tudására, és ezért hibák valószínűek .
- **3 - Szabályozott folyamat**: Az eljárások szabványosítottak és dokumentáltak, a megismertetésük képzésen keresztül történik. Előírták, hogy a ezeket a folyamatokat követni kell, azonban nem valószínű, hogy az eltéréseket felismerik. Az eljárások maguk nem kifinomultak, hanem a létező gyakorlat formalizált változatai.
- **4 - Irányított és mérhető:** A vezetés figyelemmel kíséri, és méri az eljárásoknak történő megfelelőséget, és intézkedik, amennyiben úgy tűnik, hogy a folyamatok nem működnek eredményesen. A folyamatokat állandóan javítják, és azok bevált gyakorlatot testesítenek meg. Az automatizálás, és az eszközök használata korlátozott, vagy a folyamat egyes elemeire terjed csak ki.
- **5 - Optimalizált:** A folyamatokat tökéletesítették a bevált gyakorlat szintjéig, a folyamatos javítás és a többi vállalathoz viszonyított érettségi modellezés eredményei alapján. Az informatikát integrált módon alkalmazzák a munkafolyamat automatizálására, és eszközöket adnak a minőség, és az eredményesség javításához, mellyel a vállalkozást képessé teszik arra, hogy gyorsan alkalmazkodjék.

Példa: Az informatikai stratégiai tervezés érettségi modellje

- **0 - Nem létező:** Az informatikai stratégiai tervezést nem végeznek. A vezetés nincs tudatában annak, hogy szükség van informatikai stratégiai tervezésre az üzleti célok támogatásához.
- **1 - Kezdeti/Ad Hoc jellegű:** Az informatikai vezetés tudja, hogy szükség van informatikai stratégiai tervezésre. Az informatikai tervezést szükség esetén végzik el, válaszul egy-egy konkrét üzleti követelményre. Az informatikai stratégiai tervezést esetenként megvitatják az informatikai vezetői értekezleteken. Az üzleti követelmények, alkalmazások és a technológia összehangolása inkább utólagosan történik és nem egy szervezetet lefedő stratégia részeként. A stratégiai kockázatosságát informálisan állapítják meg projektenként külön.
- **2 Ismételhető, de ösztönös:** Az informatikai stratégiai tervezést közösen végzik az üzleti területek vezetésével akkor, amikor arra szükség van. Az informatikai tervek aktualizálása a vezetés kérésére történik. A stratégiai döntéseket a projektek külön-külön vezérlik anélkül, hogy azok követ-kezetesen követnének egy általános szervezeti stratégiát. A jelentős stratégiai döntések kockázatait és felhasználói előnyeit ösztönösen ismerik fel.
- **3 Szabályozott folyamat:** Irányelv határozza meg, hogy mikor és hogyan kell informatikai stratégiai tervezést végezni. Az informatikai stratégiai tervezés egy strukturált módszert követ, amely dokumentálva van, és amelyet minden munkatárs ismer. Az informatikai tervezési folyama t ésszerűen megalapozott és a helyzetnek megfelelő tervezés végrehajtását valószínűsíti. Azonban az egyes vezetők saját belátásuk szerint járhatnak el a folyamat kivitelezését illetően, és a folyamat vizsgálatára nem léteznek eljárások. Az átfogó informatikai stratégia tartalmazza a kockázat vállalási hajlandóság következetes meghatározását abban a tekintetben, hogy vajon a technológiai élenjáró, vagy a követő stratégiát választották . Az informatika pénzügyi, műszaki és humán erőforrás stratégiája egyre inkább befolyásolja az új termékek és technológiák beszerzését. A vállalati vezetői értekezleteken napirenden van az informatikai stratégiai tervezés.
- **4 Irányított és mérhető:** Az informatikai stratégiai tervezés szabványos gyakorlat és a z anomáliákra a vezetés felfigyelne. Az informatikai stratégiai tervezés egy meghatározott vezetési funkció, amely egy felső vezetőhöz van rendelve. A vezetés figyelemmel tudja kísérni az informatikai stratégiai tervezés folyamatát, kellő információk birtokában döntések et tud hozni annak alapján, és mérni tudja eredményességét. Mind rövid távú, mind hosszú távú informatikai tervezés folyik, és az lefele végig fut a szervezeten, a aktualizálások pedig szükség szerint történnek. Az informatikai stratégia és a szervezet i stratégia egyre jobban illeszkedik annak köszönhetően, hogy foglalkozik az üzleti folyamatokkal és az érték-növelő képességekkel, valamint az alkalmazások, és technológiák használatának üzleti folyamatok átszervezésével történő kiaknázásával. A rendszerfejlesztéshez és az üzemeltetéshez szükséges belső és külső erőforrások felhasználásának meghatározását egy jól szabályozott folyamat szolgálja.
- **5 Optimalizált**: Az informatikai stratégiai tervezés egy dokumentált élő folyamat, és az üzleti célok kitűzésekor folyamatosan figyelem be veszik azt, és olyan észlelhető üzleti értéket eredményez , amely az informatikába történő befektetésen keresztül valósul meg. A kockázati és érték-növelési szempontokat folyamatosan naprakészen tartják az informatikai stratégiai tervezési folyamat keretében. Reális, hosszú távú informatikai terveket dolgoznak ki, és azokat folyamatosan aktualizálják, hogy azok tükrözzék a változó technológiát, és az üzleti tevékenységgel kapcsolatos fejleményeket. Jól ismert és megbízható iparági no rmák alapján összehasonlító értékelést végeznek, és azt integrálják a stratégia kialakításának folyamatába. A stratégiai terv kitér arra, hogy az új technológiai fejlemények hogyan idézhetik elő új üzleti képességek kialakítását, és hogyan javíthatják a szervezet versenyelőnyét.

ACTIVITY – Készítsünk érettségi modellt (tetszőleges) IT folyamathoz

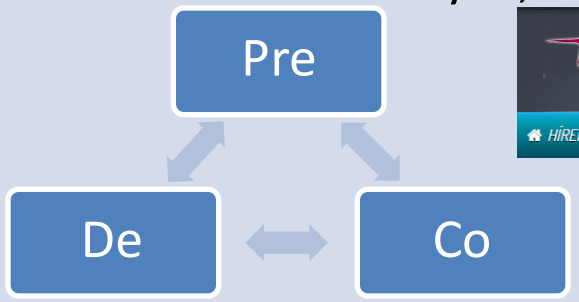
- **0 - Nem létező:**
- **1 - Kezdeti/Ad Hoc jellegű:**
- **2 - Ismétlődő, de ösztönös:**
- **3 - Szabályozott folyamat:**
- **4 - Irányított és mérhető:**
- **5 - Optimalizált:**

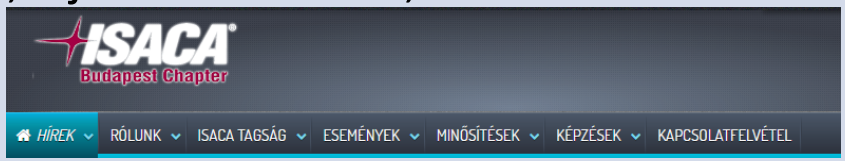
1. **Az informatikai beruházások irányításának érettségi modellje**
2. **Az informatikai humán erőforrások kezelésének érettségi modellje**
3. **Az informatikai kockázatok felmérésének és kezelésének érettségi modellje**
4. **Az informatikai projektek irányításának érettségi modellje**
5. **Az alkalmazási szoftverek beszerzésének és karbantartása érettségi modellje**
6. **A technológiai infrastruktúra beszerzésének és karbantartásának érettségi modellje**
7. **A megoldások és változtatások üzembe helyezése és bevizsgálásának érettségi modellje**
8. **Külső szolgáltatások igénybevételének irányításának érettségi modellje**
9. **A működés folyamatosságának biztosításának érettségi modellje**
10. **A bizalmasság biztosításának érettségi modellje**
11. **A felhasználók oktatásának és képzésének érettségi modellje**
12. **A rendkívüli események kezelésének érettségi modellje**
13. **A fizikai környezet biztosításának érettségi modellje**
14. **Az informatika teljesítményének figyelemmel kísérésének és értékelésének érettségi modellje.**
15. **Külső követelményeknek való megfelelőség biztosításának érettségi modellje**
16. **…**

A COBIT (Control Objectives for IT and Releated Technology) kialakulása, szemlélete

ISACA (Information Systems Audit and Control Association) – konferenciák, oktatás, CISA, CISM…

- Információ rendszerek átvilágítási/auditálási szempontjai
- A COBIT az IT szabványok, módszerek, élenjáró gyakorlatok egységes rendszerbe foglalt módszertani eszköze
- Kontroll kialakítási irányelveket dolgoztak ki. (Kontroll: „Az üzleti célkitűzések megvalósítása és a nemkívánatos események megelőzése, felderítése és korrigálása céljából kialakított szabályok, eljárások normák, és szervezeti struktúrák.”)
  - Preventív
  - Detektív
  - Korrektív





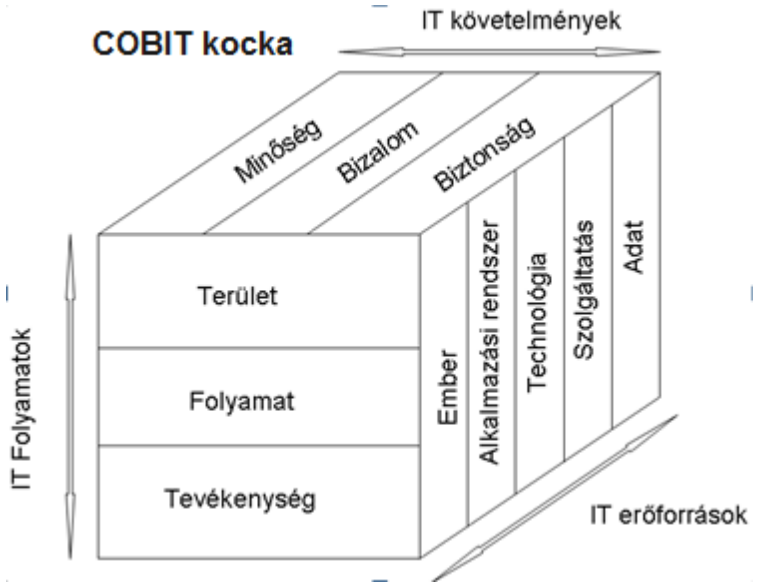
www.isaca.hu
www.isaca.org

A COBIT alapelvei

Az információtechnológiát az **üzleti célok** elérése érdekében alkalmazzuk, ennek során az **IT erőforrások IT folyamatokat** hajtanak végre, ezek eredményei hozzájárulnak az üzleti célok eléréséhez. Közben **veszélyforrások** keletkeznek, ezek különböző **kockázatokat** jelentenek.

Kontrollok alkalmazásával ezek elfogadható szintre csökkenthetők.

Egy-egy szervezet különböző beosztású menedzserei más-más szempontok alapján értékelik az alkalmazott információtechnológiát. Így a **felsővezetők** az informatikához kapcsolódó üzleti követelményeket, az **informatikai vezetők** az általuk menedzselt IT erőforrásokat, a **felhasználók** pedig az IT folyamatokat helyezik előtérbe.



RACI mátrix

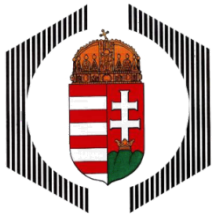
A COBIT szerkezete

Tervezés és szervezés

Beszerzés és megvalósítás

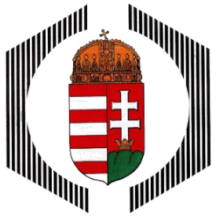
Szolgáltatás és támogatás

Figyelemmel kísérés és értékelés



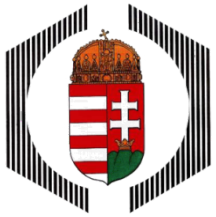
A COBIT szerkezete

PO1 Az informatikai stratégiai terv meghatározása
PO2 Az információ-architektúra meghatározása
PO3 A technológiai irány kijelölése
PO4 Az informatikai folyamatok, szervezet és a kapcsolatok meghatározása
PO5 Az informatikai beruházások irányítása
PO6 Tájékoztatás a vezetői célokról és irányról
PO7 Az informatikai humán erőforrások kezelése
PO8 Minőségirányítás
PO9 Az informatikai kockázatok felmérése és kezelése
PO10 A projektek irányítása



A COBIT szerkezete

AI1 Az automatizált megoldások meghatározása
AI2 Az alkalmazási szoftverek beszerzése és karbantartása
AI3 A technológiai infrastruktúra beszerzése és karbantartása
AI4 Az üzemeltetés és a használat támogatása
AI5 Az informatikai erőforrások beszerzése
AI6 A változtatások kezelése
AI7 A megoldások és változtatások üzembe helyezése és bevizsgálása



A COBIT szerkezete

DS1 A szolgáltatási szintek meghatározása és betartása
DS2 Külső szolgáltatások igénybevételének irányítása
DS3 Teljesítmény- és kapacitáskezelés
DS4 A szolgáltatás folyamatosságának biztosítása
DS5 A rendszerek biztonságának megvalósítása
DS6 A költségek azonosítása és felosztása
DS7 A felhasználók oktatása és képzése
DS8 A rendkívüli események kezelése és a felhasználói támogatás működtetése
DS9 Konfigurációkezelés
DS10 Problémakezelés
DS11 Az adatok kezelése
DS12 A fizikai környezet biztosítása
DS13 Az üzemeltetés irányítása

A COBIT szerkezete

ME1 Az informatika teljesítményének figyelemmel kísérése és értékelése
ME2 A belső irányítási és ellenőrzési rendszer figyelemmel kísérése és értékelése
ME3 Külső követelményeknek való megfelelőség biztosítása
ME4 Az informatikai irányítás megteremtése

ACTIVITY – készítsünk RACI mátrixot (tetszőleges) informatikai folyamathoz

Input	Folyamat lépés	Output	Felelős	Végre-hajtó	Közre-működik	Informá-ciót kap	Megjegy-zés

ACTIVITY – készítsünk RACI mátrixot informatikai folyamathoz - Példa

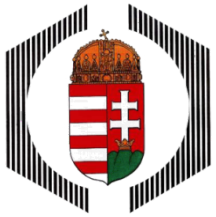
Input	Folyamat lépés	Output	Felelős	Végre-hajtó	Közre-működik	Informá-ciót kap	Megjegy-zés
Éves költségvetési terv és a munkatársak igényei írásban vagy emailben (de nem szóban)	**Beszerzési igények időszakos és eseti gyűjtése**	Összegyűjtött és rögzített igények	Intézeti mérnök			Érintett munkatárs emailben	A félévek elején az igények benyújtásának kezdeményezése Kis értékű fogyóeszközök esetén az Intézeti mérnök további jóváhagyás nélkül beszerzést kezdeményezhet.
Összegyűjtött és rögzített igények	**Az igények aggregálása, konszolidálása**	Aggregált, konszoridált igények	Intézeti mérnök		Érintett munkatársak		Szükség esetén egyeztetések az igénylőkkel. A tervezett beszerzések prioritást élveznek!
Aggregált, konszoridált igények	**Előzetes kalkulációk, árajánlatok bekérése, döntés-előkészítés**	Beszerzési árakat és konkrét eszközöket tartalmazó priorizált lista	Intézeti mérnök		Gazdasági ügyintéző	Intézetigazgató Műszaki, tudományos igazgatóhelyettes	A rendelkezésre álló keretek és címkék (témaszámok)

ISO27000 szabványcsalád

- Az ISO/IEC 27000-es szabványcsalád az **információbiztonsági irányítási rendszerekkel kapcsolatos** szabványokat tartalmazza, melyek egy része előkészítés, illetve korszerűsítés alatt áll, többségük azonban már megjelent és folyamatos korszerűsítés alatt áll.
- Az egyes szabványok többsége magyar szabványként, magyar nyelven nem létezik.
- A szabványcsaládon belül központi helyet foglal el az ISO/IEC 27000 ill. ISO/IEC 27001 szabvány.
  - ISO2700: A szabványcsalád **áttekintését** és a valamennyi szabványra érvényes **fogalomtárat** tartalmazza
  - ISO27001: Általános követelmények
  - A többiek **speciális ágazatok számára** készültek (pl. ISO/IEC 27099 – Health Informatics), speciális biztonsági területekhez tartoznak (pl. ISO/IEC 27031), az auditálást támogatják (pl. ISO/IEC 27006) ill. útmutatóként szolgálnak (pl. ISO/IEC 27003).

Az ISO27001területei

Bevezetés	Alkalmazási terület	Rendelkező hivatkozások	Szakkifejezések és meghatározásuk
A szervezet és környezete	Vezetés	Tervezés	Támogatás
Működés	Teljesítmény értékelés	Fejlesztés	Melléklet: intézkedési célok és intézkedések



Az ISO27001fejezetei

Szervezet és környezete

- A szervezet és környezetésnek megértése
- Az érdekelt felek igényeinek és elvárásainak megértése
- Az alkalmazási terület meghatározása
- Információbiztonság irányítási rendszer

Vezetés

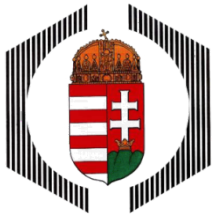
- Vezetői képesség és elkötelezettség
- Politika
- Szervezeti szerepek, felelősségek és hatáskörök

Tervezés

- A kockázatokkal és lehetőségekkel kapcsolatos tevékenységek
- Információbiztonsági célok és elérésük megtervezése

Támogatás

- Erőforrások
- Felkészültség
- Tudatosság
- Kommunikáció
- Dokumentált információ



Az ISO27001fejezetei

Működés

- Működéstervezés és felügyelet
- Az információbiztonsági kockázatok felmérése
- Az információbiztonsági kockázatok kezelése

Teljesítményértékelés

- Megfigyelés, mérés, elemzés és értékelés
- Belső audit
- Vezetőségi átvizsgálás

Fejlesztés

- Nemmegfelelőség és helyesbítő tevékenységek
- Folyamatos fejlesztés

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

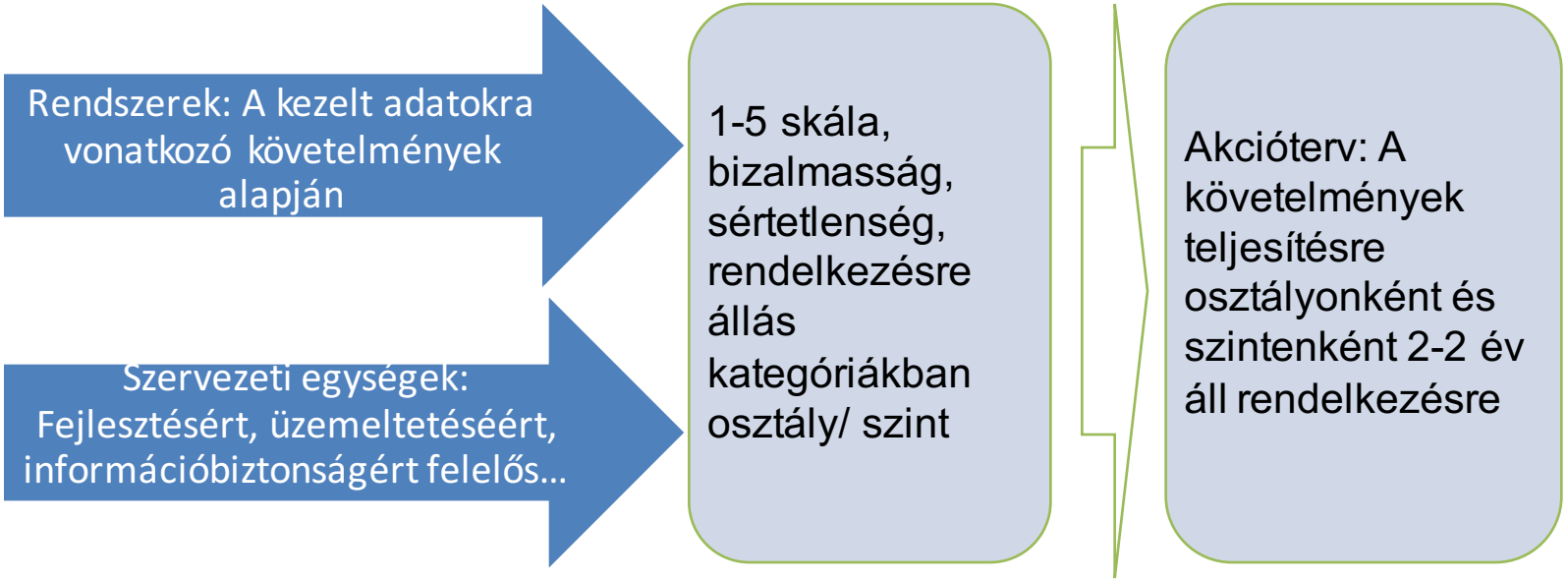
Alapgondolat: A nemzeti vagyon része a nemzeti elektronikus adatvagyon.
Ezt információs rendszereken keresztül kezeljük, így mind a nemzeti elektronikus adatvagyon mind az információs rendszerek biztonsága kiemelkedő fontosságú.

Cél: Az állami és önkormányzati szervek elektronikus információs rendszereiben kezelt adatok és információk

- **bizalmasságának;**
- **sértetlenségének;**
- **és rendelkezésre állásának biztosítása.**

Követelmények

- **zárt;**
- **teljeskörű;**
- **folytonos;**
- **kockázatokkal arányos.**



2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

!

- Magyarország területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira, valamint közérdekű adatra vagy közérdekből nyilvános adatra vonatkozik.

Személyes adat

- Minden, valamely természetes személlyel kapcsolatba hozható információ

Különleges adat

- A faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat

Köszönöm a figyelmet!