

# Mitől jó egy informatikai rendszer?

*... avagy az informatikai rendszerek fejlesztésének, üzemeltetésének és alkalmazásának minőségbiztosítási garanciái a felhasználók számára*

*... kitekintéssel  
a gyógyszeripar  
számára ...*



© Dr. Horváth Zsolt  
2011.04.01.



# Személyes bemutatkozás



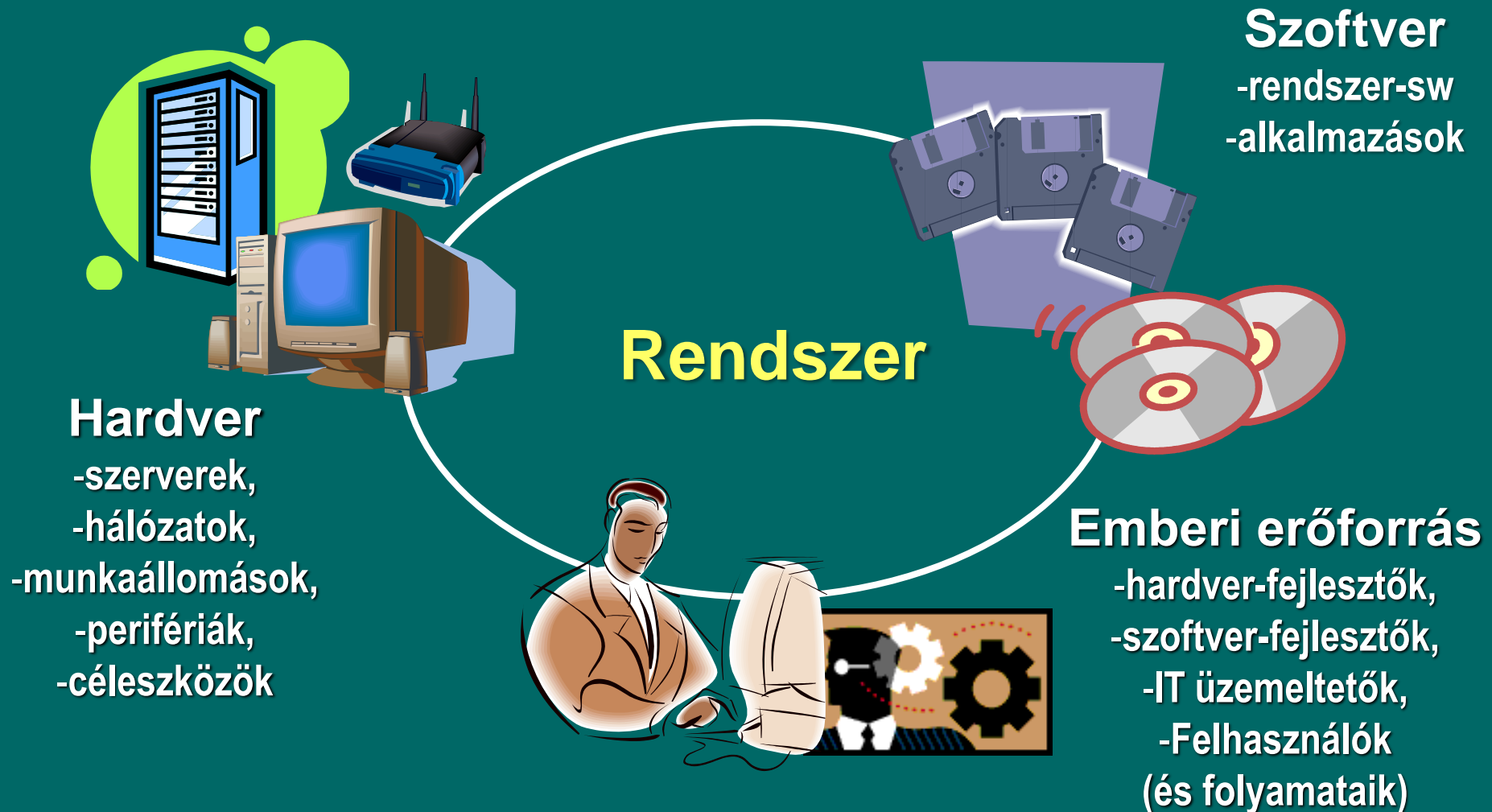
- **Dr. Horváth Zsolt** (51 év), *a műszaki tudomány kandidátusa*
- **Végzettség:**
  - ◆ *okl. szilikátipari mérnök*
  - ◆ *okl. matematikai modellezési szakmérnök*
  - ◆ *EOQ minőségügyi szakértő, menedzser, auditor és vezető tanácsadó*  
*EOQ információbiztonsági menedzser és auditor*
- **Munkahelyek, tevékenységek:**
  - ◆ **Üvegipari Művek Kutató Intézete (7 év)** – *Tud. főmunkatárs (alkalmazott kutatás)*
  - ◆ **MONTAVID Mérnöki RT. (3 év)** – *Tud. tanácsadó (matematikai programozás)*
  - ◆ **HTCC Consulting RT. (3 év)** – *Informatikai menedzser (IT rsz. létrehozása és működtetése)*
  - ◆ **Siemens PSE Kft. (10 év)** – *Minőségirányítási igazgató (szoftver minőségbiztosítás, ISO 9001, ISO 14001 rendszerek, IT biztonság, TQM, EFQM, CMMI, BPR, BSC, ...)*
  - ◆ **TÜV Nord Kft. (9 év)** – *Vezető auditor (ISO 9001, ISO/IEC 27001)*
  - ◆ **MSZT, Eurocert Kft. (10 éve)**– *Vezető auditor (ISO 9001, ISO/IEC 27001)*
  - ◆ **INFOBIZ Informatikai, Információ-biztonsági és Vezetési Tanácsadó Kft. (5 éve)** – *Ügyvezető igazgató (tanácsadás, szakértés, felkészítés és oktatás)*



# Informatika alkalmazása - példák

- Vállalati levelezés, fájlkezelés, irodai munkák
- Elektronikus dokumentációkezelés
- Üzleti folyamatok támogatása, irányítása, workflow-k
- Termelésirányítás, vezérlés
- Anyaggazdálkodás, logisztika
- Ügyfél-adatbázis kezelés,
- Ügyfélszolgálat, elektronikus HelpDesk
- Könyvelés, kontrolling, gazdasági kimutatások
- Vezetői információs rendszerek, döntés-előkészítés
- Stb...

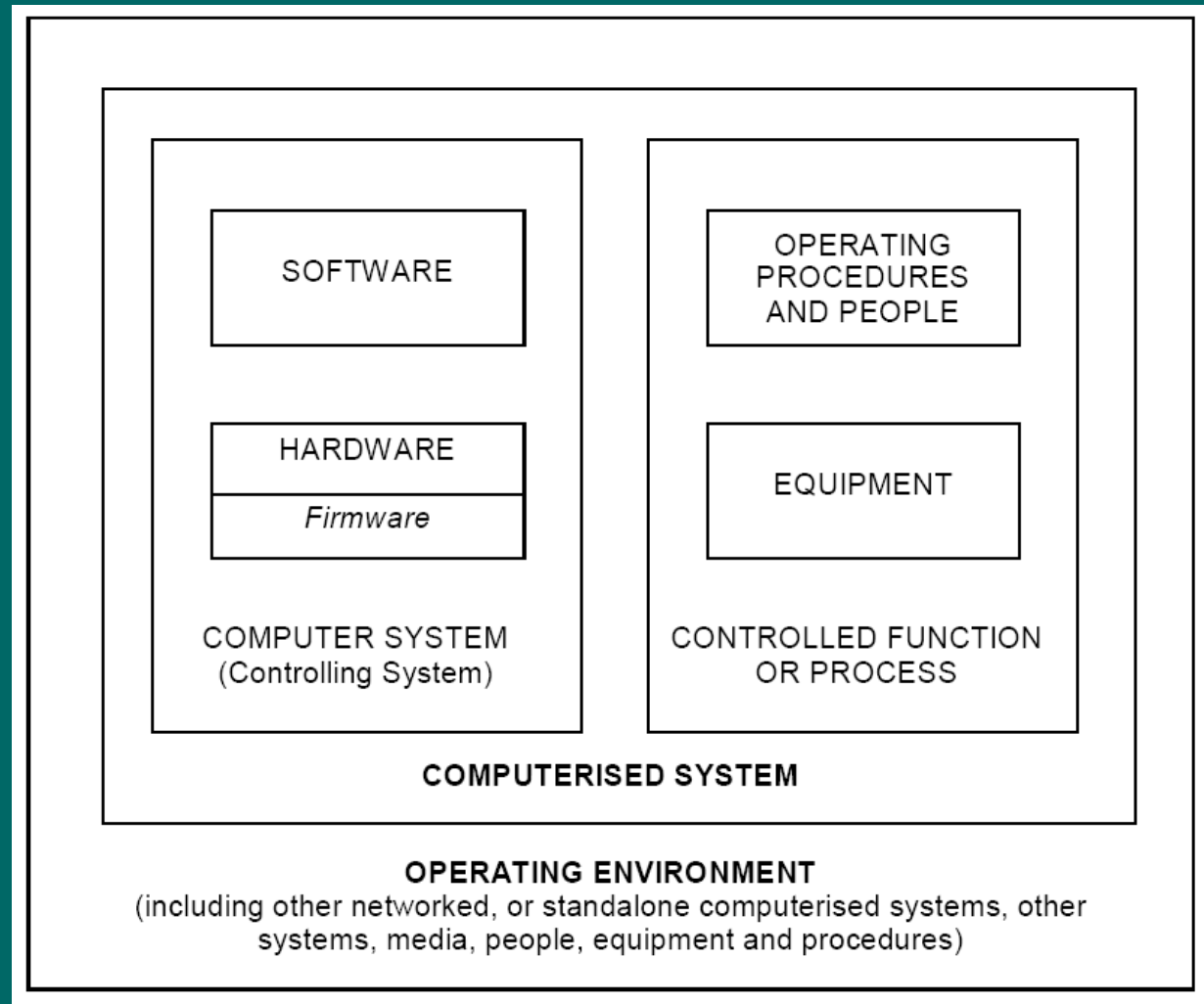
# Informatikai rendszerek felépítése





# Informatikai rendszer sémája a gyógyszeripari követelményekben

Informatikai /  
információs  
rendszer részeinek  
kapcsolatai



# Minek kell jónak lennie?

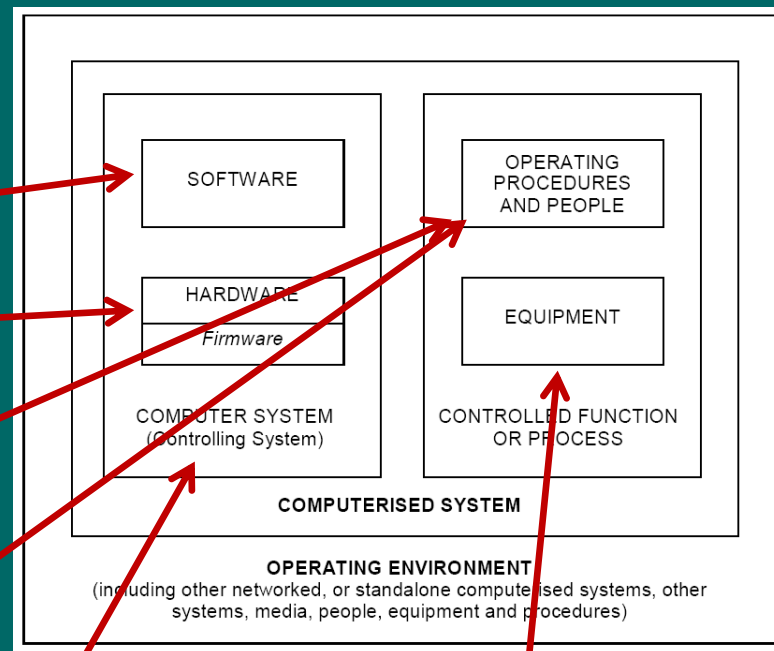
## ■ Az informatikai terméknek

- ◆ Szoftver eszközök
- ◆ Hardver eszközök

## ■ A szereplők tevékenységének, folyamatainak

- ◆ Felhasználók
- ◆ Informatikai üzemeltetők
- ◆ Hardver-fejlesztők, szoftver-fejlesztők, rendszer-fejlesztők

## ■ Az üzemeltetett termelési berendezéseknek





# Alapelvek gyógyszeriparban számítógépes rendszerek validálásához

## MIÉRT VALIDÁLUNK számítógépes rendszereket?

- Ne romoljon a termékek minősége, vagy a minőségbiztosítási rendszer hatékonysága azáltal, hogy a kézi tevékenységet számítógépes rendszer váltja fel.”
- **„A gyártás során alkalmazott kritikus számítógépes rendszereket validálni kell.”**

## MIT VALIDÁLUNK számítógépes rendszereken?

- „A validálást úgy tekintsék, mint a számítógépes rendszer teljes élelciklusának egy részét.”
- „Az élelciklusba beletartoznak a tervezés lépései, a minőségi előírások, a programozás, a vizsgálatok végzése, a kiszállítás, a dokumentálás, a működtetés, az állandó ellenőrzés (monitoring) és a változtatások.”

*Vagyis a teljes rendszer-  
fejlesztési és  
üzemeltetési  
folyamatot!  
De hogyan?*



# Mikor jó a termék?

Beszéljünk itt a **szoftverről** (értelmezés kiterjeszhető teljes rendszerre is!)

- **Ha megfelel a vele szemben támasztott követelményeknek!**



**Követelményeket kell jól meghatározni!**

Követelmények meghatározása nem csak a **funkcionalitásra**,  
hanem egyéb „**nem-funkcionális**” jellemzőkre is!  
(Nemcsak az a fontos, hogy „**MIT**”, hanem az is, hogy „**HOGYAN**”!)



**ELLENŐRZÉS:**

- **Termék ellenőrzése** (termék-verifikálás, termék-validálás)
- **Gyártási folyamat ellenőrzése** (szoftverfejlesztés auditálása)





# Szoftver termék mérése

## Szoftver termék mérésére eljárások:

- Általánosságban tesztelés
- Tesztelés tudatos, módszeres, szabályozott eljárás alapján
- Tesztelés célja, módszere, részletezettsége, eljárása, végrehajtója, értékelése lehet nagyon eltérő, sokféle
- Mi alapján és hogyan mérjük?



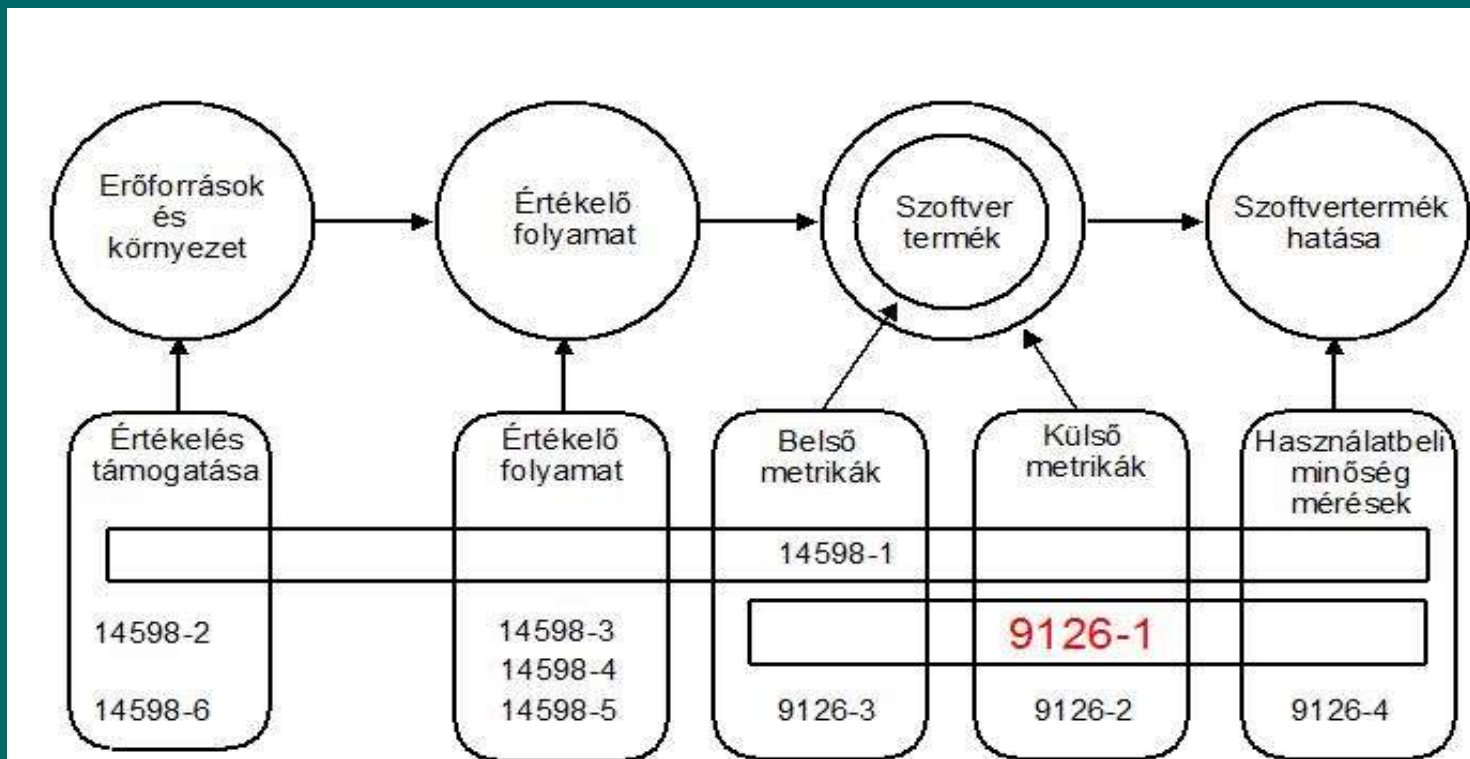
**Szoftver-minőség mérésére VAN szabványos keretrendszer,  
amivel a definiált követelményeknek való megfelelés  
mérhető!**



# Szoftver-minőség értékelésének nemzetközi szabványai

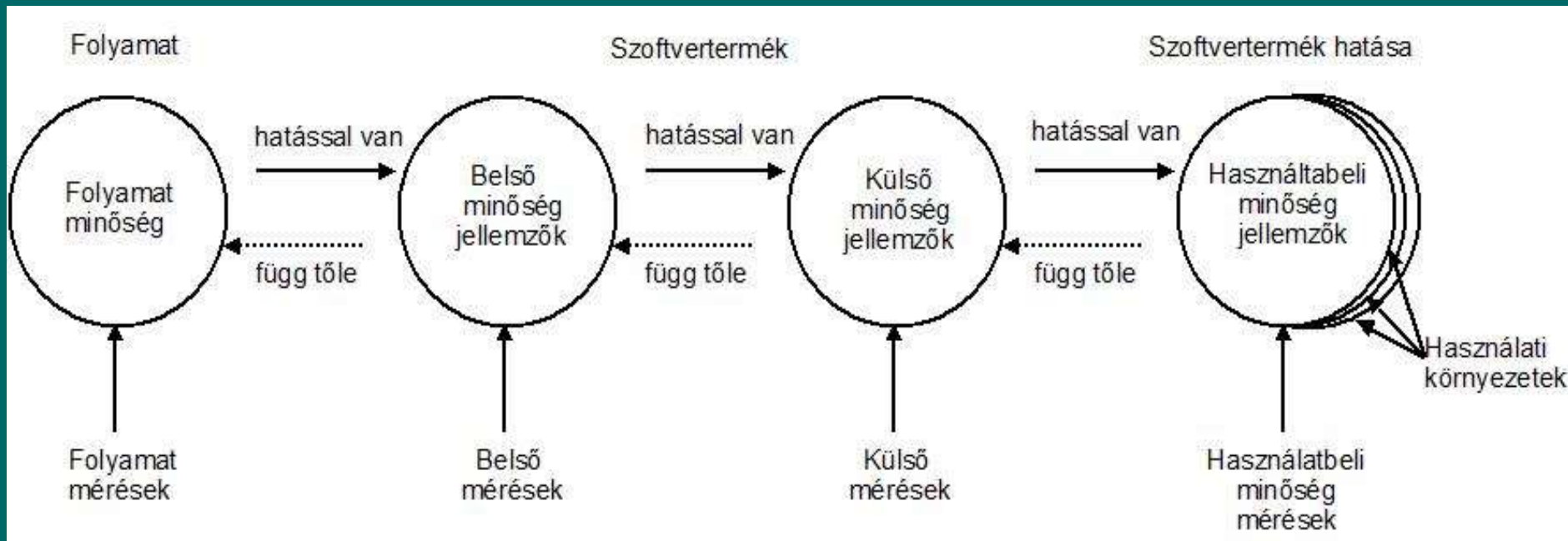
Az ISO/IEC 9126 és ISO/IEC 14598 szabványok közötti összefüggések:

- 9126 szabvány: Szoftver termék minőség (funkcionális és nem funkcionális felhasználói követelmények meghatározásához)
- 14598 szabvány : Szoftver termék értékelés



# Életciklus minőség modell

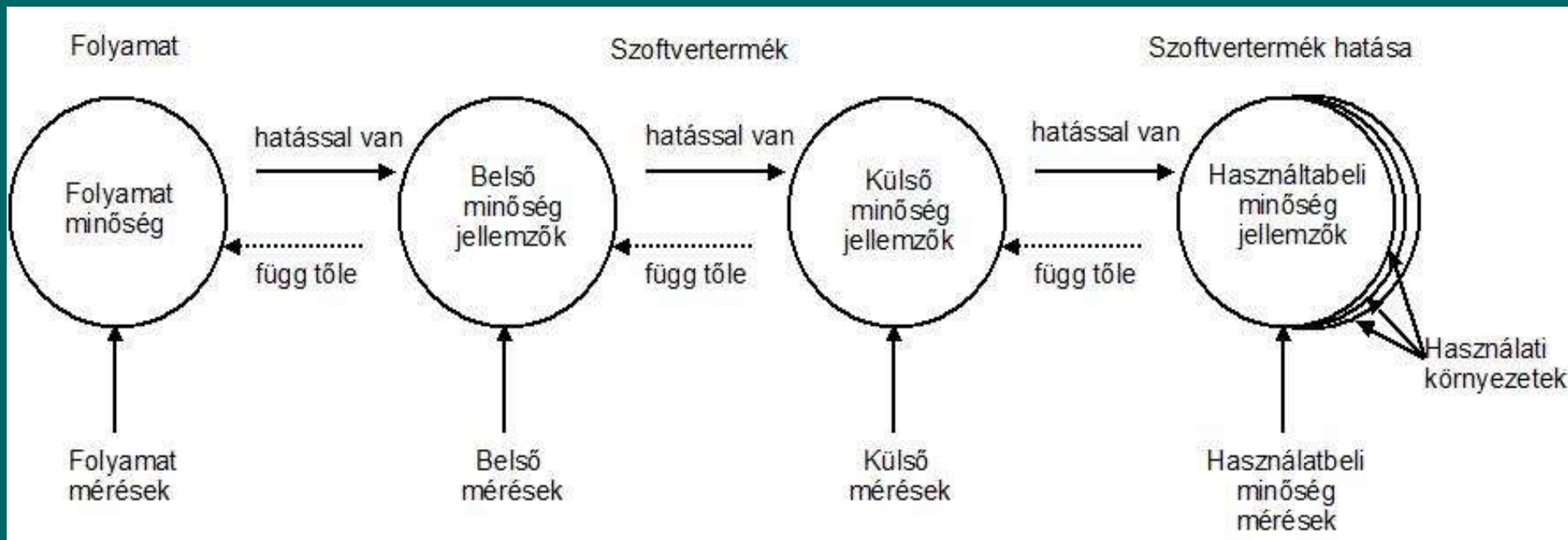
- A folyamat minősége hozzájárul a szoftver termék minőségének javításához, ami elősegíti a használatbeli minőség fejlődését.
- Megfelelő belső szoftver tulajdonságok a szükséges előfeltételei az elvárt külső viselkedés elérésének, és ezen megfelelő külső viselkedés előfeltétele az elvárt használatbeli minőség elérésének.



# Életciklus minőség modell

Ennek megfelelően a szoftver életciklus minőség modell alapján definiálhatók

- Belső minőségjellemzők,
- Külső minőségjellemzők és
- Használati minőségjellemzők.





# Minőség modell – ISO/IEC 9126 szerint



- Ez a modell a külső és belső minőséget definiálja és bontja szét további kategóriákra.
- A kategóriák tulajdonságai (a szabványban definiált) külső és belső metrikákkal mérhetőek.

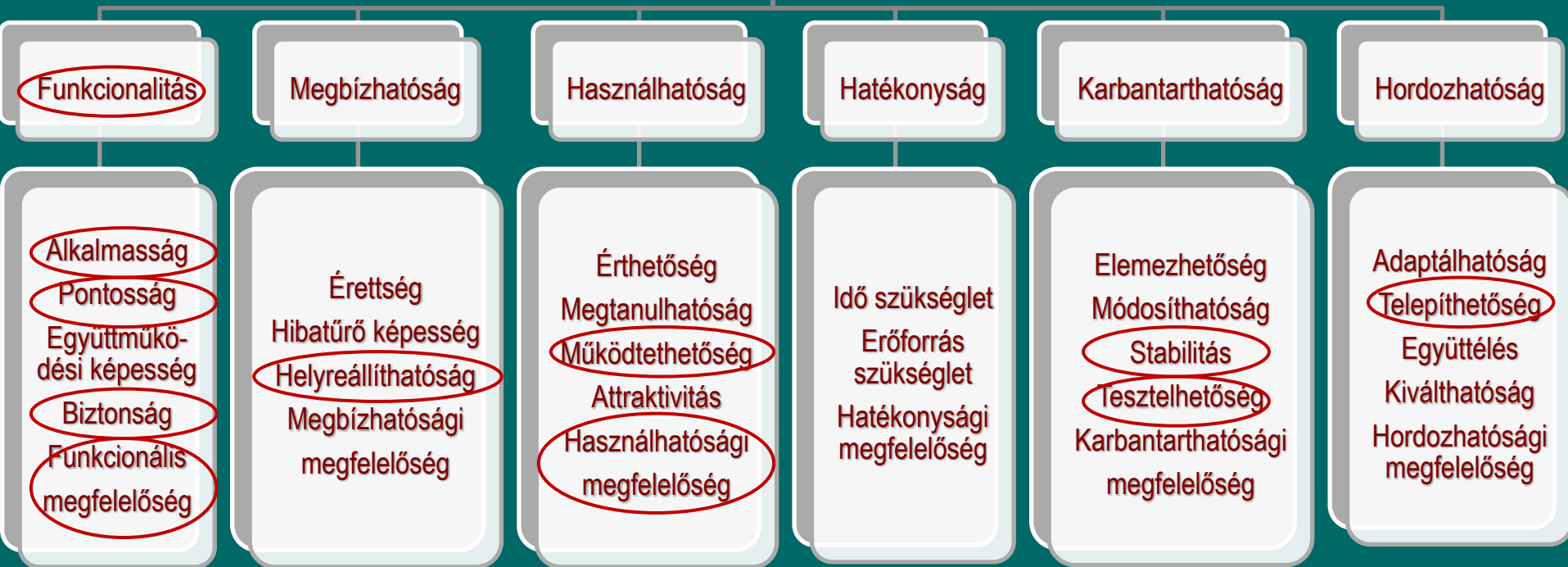


# Minőség modell – kiemelt jellemzői a gyógyszeripari követelményekben

PÉLDÁK

Külső és belső  
minőség

... és mi még?



- A gyógyszeripari GAMP követelmények alapján a következő tulajdonságok a legkritikusabbak, célszerű a mérést azokra összpontosítani.
- (Ezek példák, konkrét alkalmazás értékelésekor egyedileg célszerű megállapítani.)



# A szoftver értékelési folyamat felépítése

## Külső értékelő értékelési folyamata

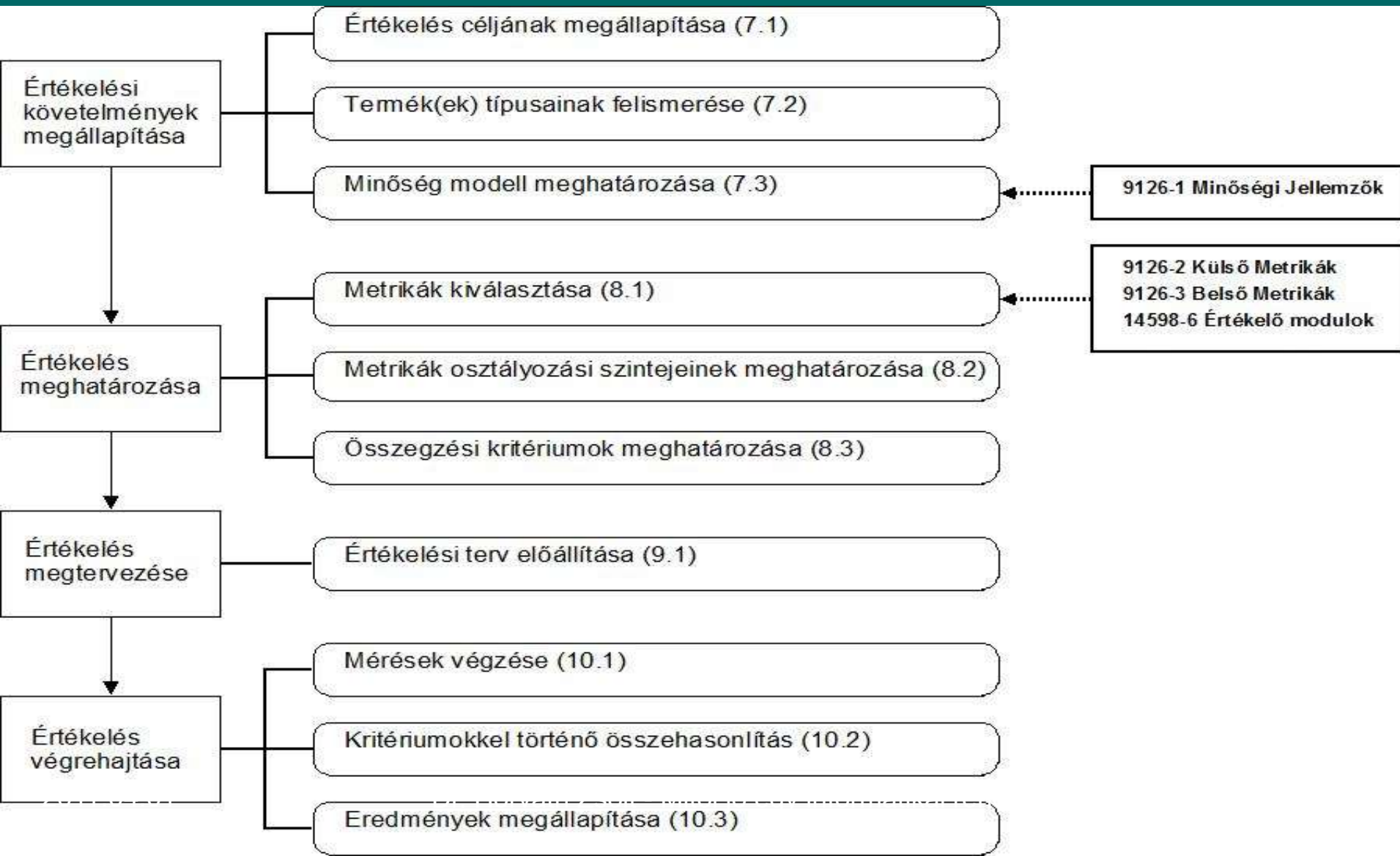
### Kezdeti megállapodás

Az értékelési folyamat 5 tevékenységből áll:

1. **Értékelési követelmények** kidolgozása
2. **Értékelés specifikálása**, az értékelési követelmények szerint.
3. **Értékelés megtervezése**: értékelési terv kialakítása a specifikáció alapján.
4. **Értékelés végrehajtása**: értékelési terv szerinti modellezés, mérés, tesztelés.
5. **Értékelés befejezése**: értékelési jelentés kiadása.



# A szoftver értékelési folyamat felépítése







# Szoftver termék kockázati értékelése (példa)

Szoftver termékek integritási szintjének besorolása a termék kockázati szintje alapján

→ **Meghatározza az értékelés szükséges szigorúságát.**

## Kockázat

## Integritási szint

Magas

A

Közepes

B

Alacsony

C

Jelentéktelen

D

*(Kockázati szint meghatározására példa a következő oldalon.)*



# Szoftver termék kockázati értékelése (példa)

## Kockázati mátrix (példa)

- Minden zöld mezőről meg kell állapodni a tervezők szakértőinek és a sértetlenség biztosítási szakértőknek.
- A kiváltó ok gyakorisága szintén megállapodás és/vagy tapasztalati értékek kombinációja kell legyen és időben változhat.

Előfordulás gyakorisága	A kiváltó okra jellemző gyakoriság (évente)	Következmények súlyossága			
		Katasztrofális	Nagyobb	Súlyos	Kisebb
Gyakori	>1	Magas	Magas	Magas	Közepes
Valószínű	1 - 10 <sup>-1</sup>	Magas	Magas	Közepes	Alacsony
Esetleges	10 <sup>-1</sup> - 10 <sup>-2</sup>	Magas	Magas	Alacsony	Alacsony
Távoli	10 <sup>-2</sup> - 10 <sup>-4</sup>	Magas	Magas	Alacsony	Alacsony
Valószínűtlen	10 <sup>-4</sup> - 10 <sup>-6</sup>	Magas	Közepes	Alacsony	Jelentéktelen
Hihetetlen	< 10 <sup>-6</sup>	Közepes	Közepes	Jelentéktelen	Jelentéktelen



# Mikor jó az „informatikai folyamatok” működése?

... az informatikai termékek megfelelőségén túlmenően, ha teljesülnek a ...

- **rendszer fejlesztőivel** szembeni elvárások
- **rendszer üzemeltetőivel** szembeni elvárások
- **rendszer felhasználóival** szembeni elvárások

**„Mindegyik fontos”**



# Mikor jó a „szereplők” működése?

## ■ Rendszer fejlesztőivel szembeni elvárások

- Fejlesztő szervezet működése, hatékony, gyors, rugalmas
- Rendszer (funkcionális és nem-funkcionális) tulajdonságai megfelelnek az elvárásoknak
- Kevés hiba, azok gyors javítása, megfelelő a tesztelése
- Hibajavításkor, módosításkor nincsenek újabb hibák



**Fejlesztő szervezet működése szabályozott, fejlesztési módszertan szerinti,  
Ellenőrzések végzése szakértői beszállítói audittal**

- Rendszer üzemeltetőivel szembeni elvárások
- Rendszer felhasználóival szembeni elvárások

# Szoftver-fejlesztési módszertanok

- **Szoftverfejlesztési életrajzi modellek** (*vízesés modell, spirálmodell, prototípus modell, evolúciós modell, stb.*)
  - **Szoftverfejlesztési projektmenedzselési módszerek, modellek** (*SSADM, MNS, RUP, Prince, stb.*)
  - **Szoftverfejlesztés szervezeti értékelési modelljei** (*SPICE, V-Modell, CMM, CMMI, ...*)
- Legelterjedtebb és elfogadottabb: **CMMI**
  - INFOBIZ által kifejlesztett értékelési módszertan: **SWPA**  
(*Erre az INFOBIZ elnyerte a „Magyar Minőség Háza 2008” díjat is.*)





# Mi is az a „SWPA”?

## – SoftWare Process Audit –

- **Az INFOBIZ Kft. által kifejlesztett eljárás**
- **Alapjai:**
  - ◆ CMMI V1.2 – DEV modell (DEV = software development)
  - ◆ ISO 9001:2008 és ISO/IEC 90003:2004 szabványok
  - ◆ Szerzők sokéves szoftver-minőségbiztosítói és auditori tapasztalatai
- **Projektműködés orientált**, projektfolyamatokat és szervezeti folyamatokat is vizsgál
- Időbeli lefolytatása **lényegesen rövidebb** az általános CMMI szerinti értékelésnél (assessment-nél) → **Költséghatékony a megrendelő számára**
- **Jól használható** szoftverházak vagy konkrét projektek működésének értékelésére és a fejlesztési lehetőségek feltárására:
  - ◆ belső értékelés vagy
  - ◆ beszállítói audit vonatkozásában is.



# Kétféle követelmény

Minden kulcsfolyamatnak kétféle követelményt kell teljesítenie:

## ■ Speciális, szakmai követelmények

- ◆ Az adott kulcsfolyamat saját szakmai követelményeinek teljesítése
- ◆ Megfelelnek a **CMMI-ben** a speciális célokat (SG) kielégítő speciális tevékenységeknek (gyakorlatoknak) (SP)

## ■ Folyamatmenedzsment követelmények

- ◆ Ezek minden folyamatra közősek, és megmutatják, hogy az adott tevékenységet milyen szervezeten, menedzseltén végzik.
- ◆ Meghatározzák az adott folyamat „kéességi szintjét” (CL)
- ◆ Megfelelnek a **CMMI-ben** az általános célokat (GG) kielégítő általános tevékenységeknek (gyakorlatoknak) (GP)



# SWPA kulcsfolyamatai – kiemelt elemei a gyógyszeripari követelményekben

## 1. Projektmenedzsment:

- 1.1 Szerződéskötés és kapcsolattartás a vevővel
- 1.2 Projekttervezés
- 1.3 Projektkövetés
- 1.4 Kvantitatív projektmenedzsment
- 1.5 Beszállítók és alvállalkozók menedzselése

## 2. Fejlesztés:

- 2.1 Termékstratégia
- 2.2 Követelmények kezelése
- 2.3 Szoftvertervezés
- 2.4 Szoftver kódolás (implementálás) és integráció
- 2.5 Tesztelések
- 2.6 Átadás és karbantartás

## 3. Folyamatmenedzsment:

- 3.1 Folyamatdefiníció és folyamat karbantartás
- 3.2 Szervezeti szintű folyamatelljesítmény (statisztikai folyamat-kontrolling alapján)
- 3.3 Innováció és mérhető, folyamatos fejlesztés

## 4. Szupport:

- 4.1 Szervezeti szintű konfiguráció- és változás-kezelés
- 4.2 Szervezeti képzés
- 4.3 Következetes hibaok-elemzés és hibamegelőzés



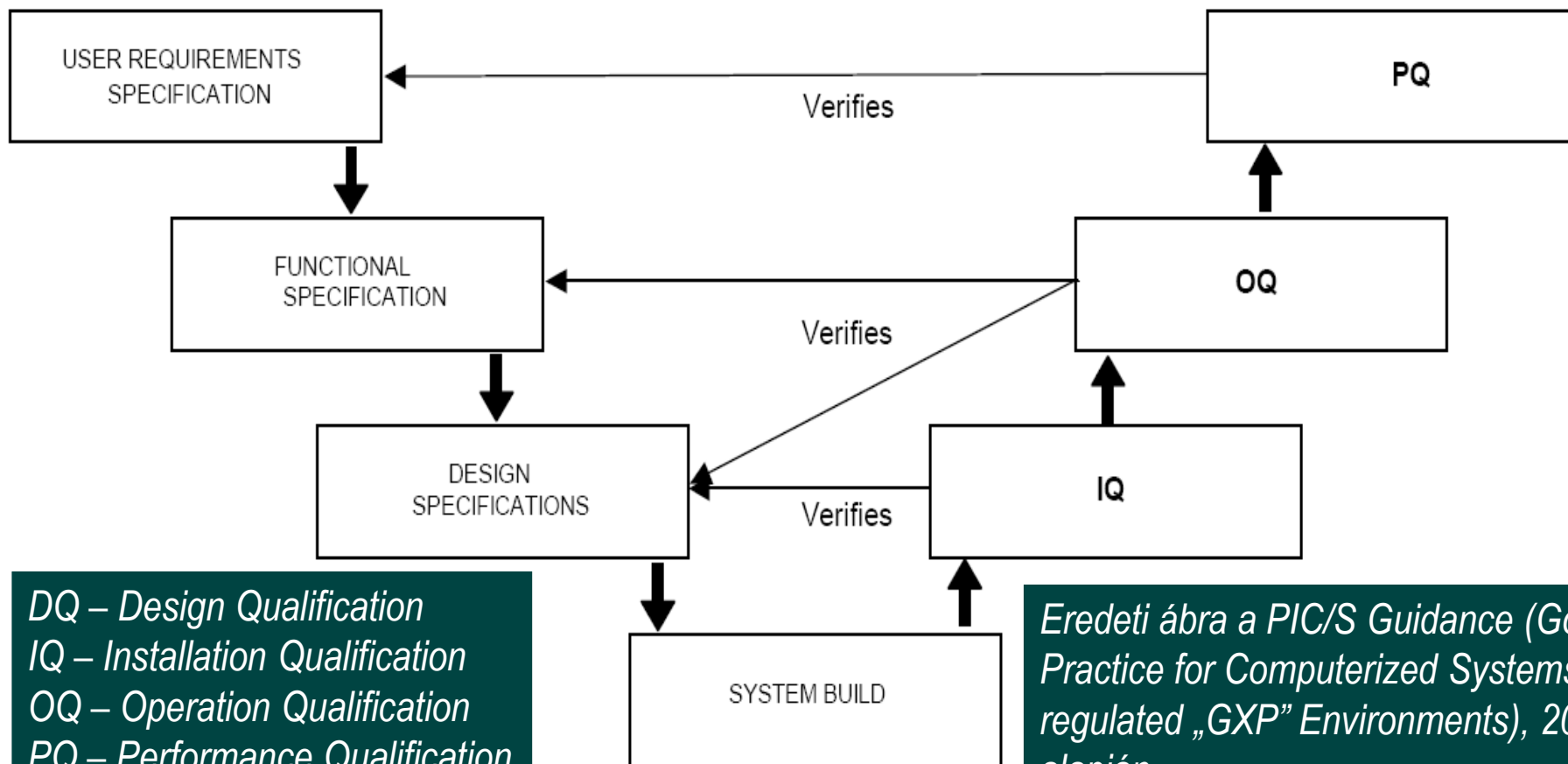


# Folyamatmenedzsment követelmények

## A főbb követelmények, egyszerűen és dióhéjban:

- A szerepek és felelőségek egyértelműen meghatározottak
- A felelősök és végrehajtók rendelkeznek a megfelelő tudással, tapasztalattal, kompetenciával illetve jogosultságokkal
- A szükséges erőforrásokat pontosan felmérték és rendelkezésre állnak
- A tevékenységek tervezése és a végrehajtás kontrollingja
- Szabályozás a vállalati szintű intézményesített folyamat alapján
- Folyamatműködés megfelelése a szabályozott eljárásnak
- A folyamatteljesítmény mérése, és statisztikai szabályozás
- Tanulás és visszacsatolás a tapasztalatokból
- Folyamatfejlesztés

# V-Modell a PIC/S ajánlásaialapján

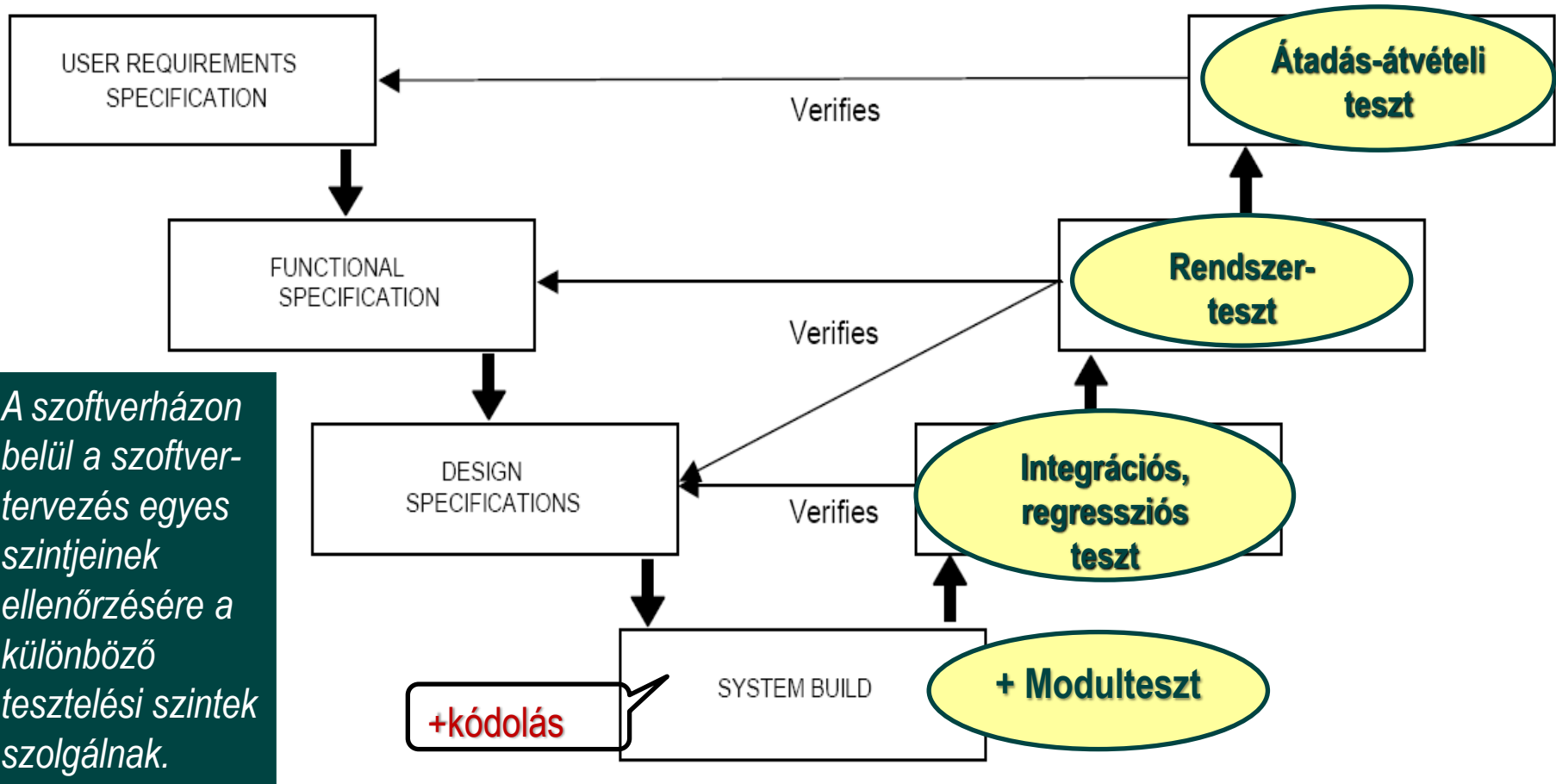


*DQ – Design Qualification*  
*IQ – Installation Qualification*  
*OQ – Operation Qualification*  
*PQ – Performance Qualification*  
*CC – Change Control*

*Eredeti ábra a PIC/S Guidance (Good Practice for Computerized Systems in regulated „GXP” Environments), 2007 alapján*




# V-Modell a szoftver-fejlesztési szakma alapján



Mindegyik szint ellenőrzése a megelőző szintek elfogadott (hibátlanul lezárt) teszt-eredményei után kezdődhet. Az átadás-átvételi teszt hibátlan lezárása után történik a szoftver ügyfélnek való átadása, amit követ a betanítás és üzembe helyezés.



# Mikor jó a „szereplők” működése?

- Rendszer fejlesztőivel szembeni elvárások
  - **Rendszer üzemeltetőivel szembeni elvárások:**
    - Az IT/HW eszközpark (szerver, hálózat, ...) folyamatos és működőképes rendelkezésre állása és működése
    - Hibajavításkor, módosításkor gyorsaság és rugalmasság
    - IT biztonság
- 
- Dokumentált, szabályozott működés, módszertan szerint
  - Elszámolás mérés (SLA) alapon
  - Ellenőrzések végzése szakértői beszállítói audittal
- Rendszer felhasználóival szembeni elvárások



# Az IT szolgáltatásokkal szembeni felhasználói elvárások

A **hasznosság** az, amit az ügyfél kap – **a célra való alkalmasság.**

A **garancia** az, ahogy azt nyújtják – **a használatra való alkalmasság.**

- Funkcionalitás rendben?
- Teljesítmény biztosítva?
- Korlátok megszüntetve?

## HASZNOSSÁG

- Kellő mértékben elérhető?
- Megvan-e a kellő kapacitás?
- Eléggé folyamatos?
- Eléggé biztonságos?

## GARANCIA

Funkcionalitás (funkcionális tulajdonságok)  
Alkalmas-e a célra?

**Előállított érték**

Biztosíték (nem-funkcionális tulajdonságok)  
Alkalmas-e a használatra?



# A minőség = megfelelés az igénynek

**minőség =**

**jelentés**

**SLA**

Az IT szolgáltatások minőségének különböző szintjeit az igények különböző szintjei szerint lehet meghatározni.



# A minőség = megfelelés az igénynek

**minőség =**

**jelentés**

**SLA**

## **SLA (Service Level Agreement) – Szolgáltatási Szint Megállapodás**

minden szolgáltatásra definiált, és

- tartalmazza a szolgáltatás funkcionális és nem-funkcionális mérhető jellemzőinek IT szolgáltató és ügyfél között megállapodott szintjét;
- azok automatikus mérési eredményeinek naplózását, és az azokból generált mérőszámok konkrét értékeit egy rendszeres szolgáltatási jelentésben.



# Az ITIL és az ISO/IEC 20000 kapcsolata

*szabvány*

**ISO/IEC  
20000**

*Az IT-szolgáltatásmenedzsment  
megfelelőségének tanúsítása*

*Jól bevált  
gyakorlat*

**ITIL**

*Útmutatás az IT-  
szolgáltatásmenedzsment  
megvalósításához*

*Munkautasítások és  
intézkedések*

**Belső folyamatok és eljárások**

*Az IT-szolgáltatások nyújtása és  
támogatása*






# Mi az ITIL röviden?

**Az ITIL** (IT Infrastructure Library) az IT szolgáltatás irányítása területén:

- olyan  **folyamatokat és eljárásokat** definiál
- a szolgáltatás  **jó minőségű, költséghatékony** biztosítására és támogatására,
- amelyek a szervezet  **üzleti folyamatainak** eredményes működését teszik lehetővé.
  - *Nyílt, bevált gyakorlat az IT-szolgáltatásmenedzsment területén;*
  - *Egyre inkább „de facto” (és „de jure”) globális szabvány;*
  - *Közös nyelvet biztosít.*



# Mikor jó a „szereplők” működése?

- Rendszer fejlesztőivel szembeni elvárások
  - Rendszer üzemeltetőivel szembeni elvárások
  - **Rendszer felhasználóival szembeni elvárások**
    - Informatikai / információs rendszerek használatának ismerete
    - Rendszerek csak célnak megfelelő használata
    - Biztonsági szabályok és előírások betartása (ISO 27001)
    - Működés során a minőségbiztosítás (ISO 9001) betartása
- 
- **Folyamatok és eljárások használatának ellenőrzése (folyamataudit, folyamat-validálás)**



# Az információbiztonság aktualitása

**Az információbiztonság kérdése** – az informatika rohamos előretörésével – minden vállalatnál **egyre égetőbb kérdéssé válik**. Mindenki tud róla, viszont **senki sem veszi addig komolyan, amíg először „meg nem égette magát” vele**. Elvárások felhasználói oldalról:

- A hatékony munkavégzéshez elvárás, hogy **a szükséges információk a kellő időben és sértetlenül álljanak a rendelkezésre**.
- Minden szervezetnél – akár tudomásul vesszük, akár nem, – **van "információszivárgás"**. Megnyilvánulási formái széles spektrumban jelentkeznek. Az információk jogosulatlan kézbe kerülése jelentős erkölcsi és anyagi károkat okoz(hat) a szervezetnek.

Ott, ahol felismerték a védekezés fontosságát, azzal is szembesülnek, hogy az önállóan (tehát nem rendszerben) alkalmazott védelmi elemek kiépítése, fenntartása rendkívül drága.  
– Ebben a helyzetben segít rendet teremteni az  
információbiztonsági irányítási rendszer!



# Az információ biztonsága

**Információ** = *(számomra értelmes)* **tartalommal bíró adat**

**Információhordozó** – ezen keresztül létezik az információ,  
és ezen keresztül sérülhet a biztonsága is!

**Információ biztonsága =**

- ★ Az információ rendelkezésre állása
- ★ Az információ sértetlensége
- ★ Az információ bizalmassága

# Az információ megjelenési formái





# Az információvédelem értelmezése

Az adatok sérülése, megsemmisülése, jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.

**Két fő területe:**

- ◆ **ADATBIZTONSÁG:** Az információs rendszerek adatvesztés elleni védelmét, az adatok folyamatos rendelkezésre állását biztosító szabályzatok, folyamatok és megoldások.
- ◆ **ADATVÉDELEM:** Az információs rendszerek adataihoz való illetéktelen hozzáférést meggátló szabályozások, folyamatok és megoldások.



# Információbiztonsági irányítási rendszer (ISO/IEC 27001) részei

- Információs vagyon fenyegetettségének átfogó **kockázatelemzése**
- **Védelmi intézkedések**, eljárások megteremtése – különböző területeken a különböző fenyegetettségekre
- **Menedzsment rendszer** – menedzsment elemek kiépítése *(hasonló mint a MIR, KIR, IBIR, ...)*



# Kockázatkezelés – de miért?

- **Biztos, hogy mindenre gondoltam – a kockázatkezelés nélkül is?**
- **Egyenszilárdságú védelem**
  - ◆ *„Minden biztonsági lánc annyira erős, mint a leggyengébb láncszeme!”*
  - ◆ *A veszélyeket, fenyegetettségüket a jelentőségüknek megfelelően kezeli*
  - ◆ *Költséghatékony védekezés, (védelmi beruházások megalapozottak)*
- **Előre felkészülten, tervezetten és tudatosan védekezni a biztonsági incidensek / események ellen**



# A védelem felállításának kérdései



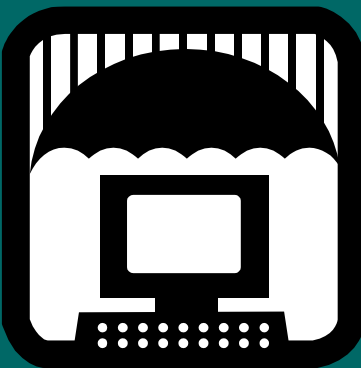
1. **Mit kell védenünk?** – *a védendő értékek feltérképezése*
2. **Mitől?** – *a külső / belső fenyegetettségek, kockázatok azonosítása*
3. **Hogyan?** – *a fizikai / logikai védelem, szabályozók meghatározása*

**„Nincs teljes biztonság, csak optimális, még elfogadható biztonsági szint”**



# Az információvédelmi eljárások szakmai területei

- **objektum, terület védelem,**
- **személy védelem** (rendszerben a személy védelme, vagy a rendszer védelme személyektől),
- **Hagyományos adatok** (pl. papíralapú), **módszerek, eszközök védelme,**
- **informatikai védelem,** (fizikai, logikai és szervezési)
- **elemi károk, természeti csapások elleni védelem** (az információbiztonság szemszögéből üzletmenetfolytonosság és katasztrófaelhárítás).





# Számítógépes rendszerek biztonsági elvárásaira megoldási módszerek

SZEMPONTOK	MÓDSZER (Szabvány)
<b>Adat-biztonság</b> (alapadat-védelem, adathelyesség, stabilitás, audit, hozzáférés-letiltás, eseménynaplózás)	<b>IBIR</b> (ISO 27001), <b>MIR</b> (ISO 9001), <b>IT üzemeltetés</b> (ITIL / ISO 20000)
<b>Rendszer-biztonság</b> (rendelkezésre állás, hozzáférés-kiosztás és letiltás, eseménynaplózás, audit, változások kontrollja)	<b>IBIR</b> (ISO 27001), <b>IT üzemeltetés</b> (ITIL / ISO 20000)
<b>Termék-biztonság</b> (minőség-megfelelőség, minőség-szabályozás, ...)	<b>Szoftver min.értékelés</b> (ISO 9126) <b>Szoftverfejl. MIR /audit</b> (CMMI)
<b>Folyamat-biztonság</b> (workflow-technika, eseménynaplózás, ...)	<b>MIR</b> (ISO 9001) <b>IT üzemeltetés</b> (ITIL / ISO 20000)
<b>Információ-biztonság</b> (személyes adatok és üzleti adatok védelme)	<b>IBIR</b> (ISO 27001)
<b>Kommunikációs biztonság</b> (üzenetek és csoportmunkafolyamatok, internet-intranet)	<b>IBIR</b> (ISO 27001), <b>MIR</b> (ISO 9001), <b>IT üzemeltetés</b> (ITIL / ISO 20000)
<b>Egyéb szempontok</b> (sebesség, technikai nívó, marketing, ...)	Elvárásoktól függ...



# Köszönöm megtisztelő figyelmüket!

**Dr. Horváth Zsolt**  
horvathzs@infobiz.hu  
<http://www.infobiz.hu>