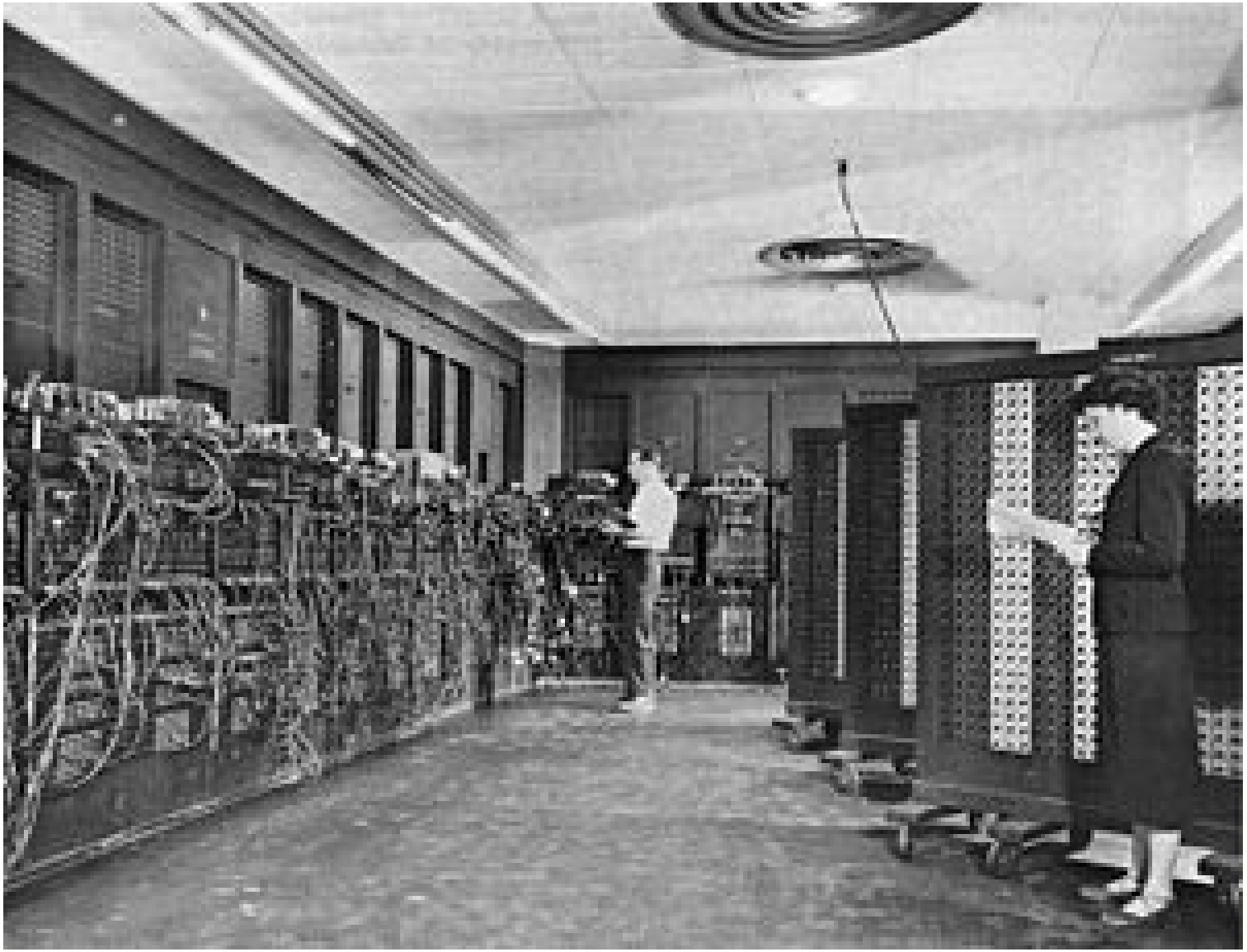
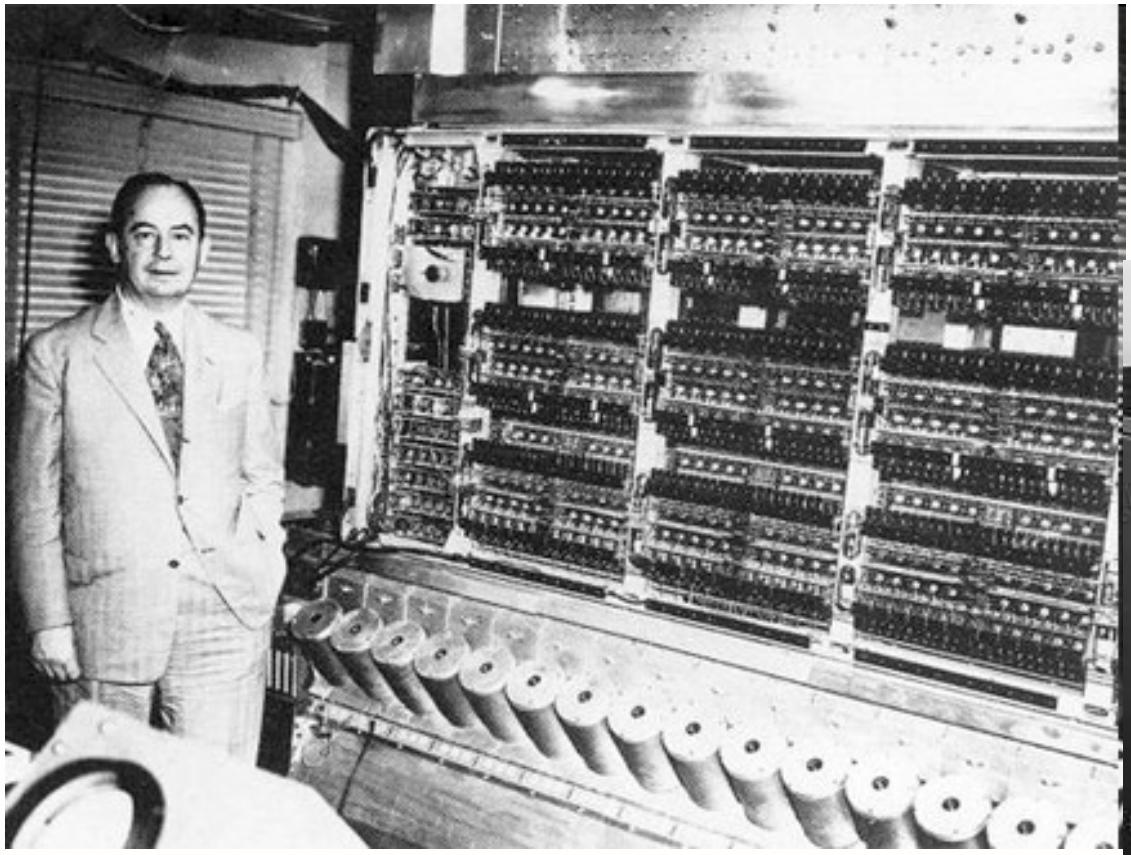
Számítógépes rendszerek minőségbiztosítása

Biró András
Inspektor

Tartalomjegyzék

- Informatikai alapfogalmak
- Szoftver meghatározása
- Számítógépes rendszerek használatának kockázatai (történelmi példák)
- Nemzetközi és helyi szabályozások számítógépes rendszerekre
- Validálások
- Felhőrendszerek
- Mesterséges Intelligencia



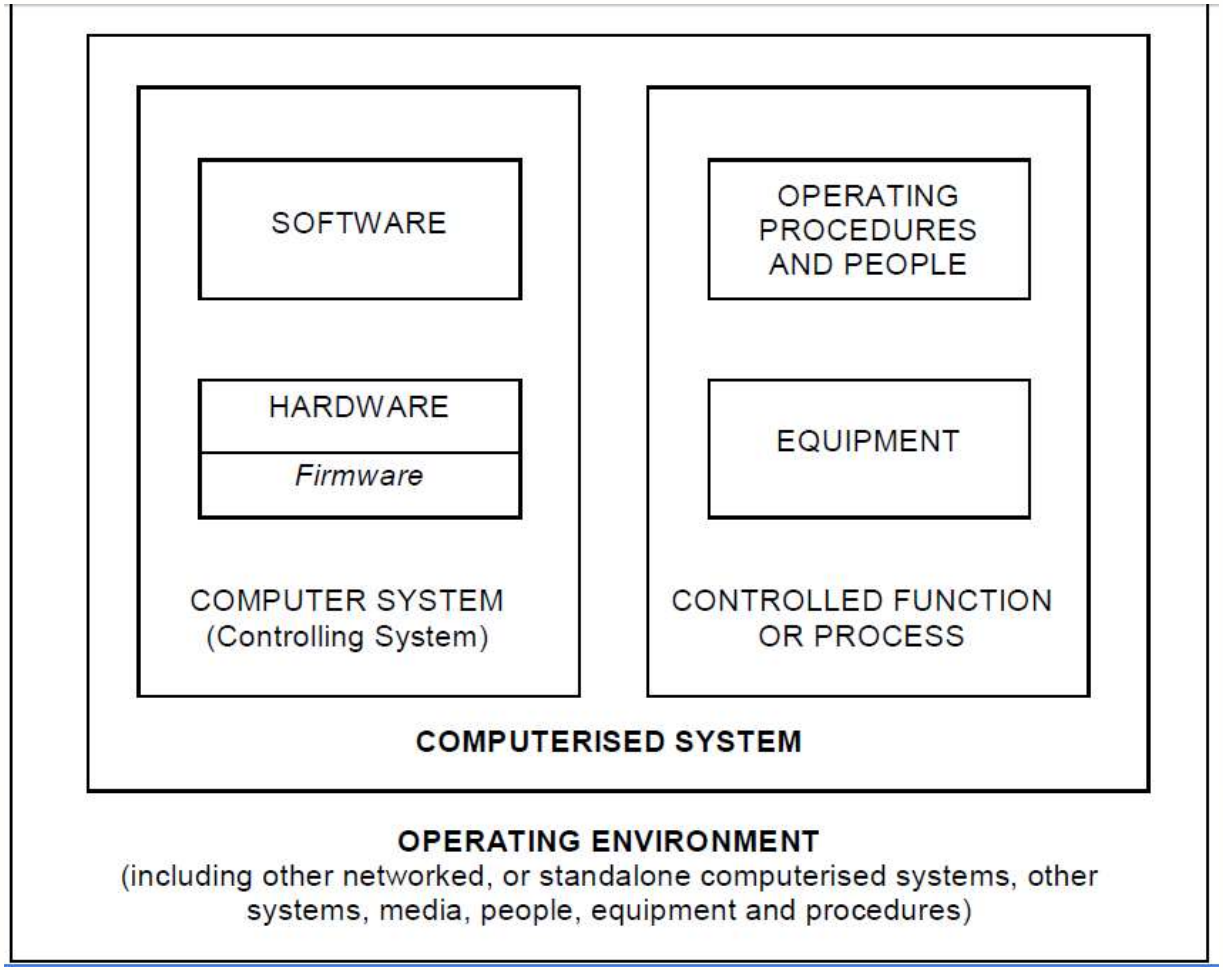



IBM

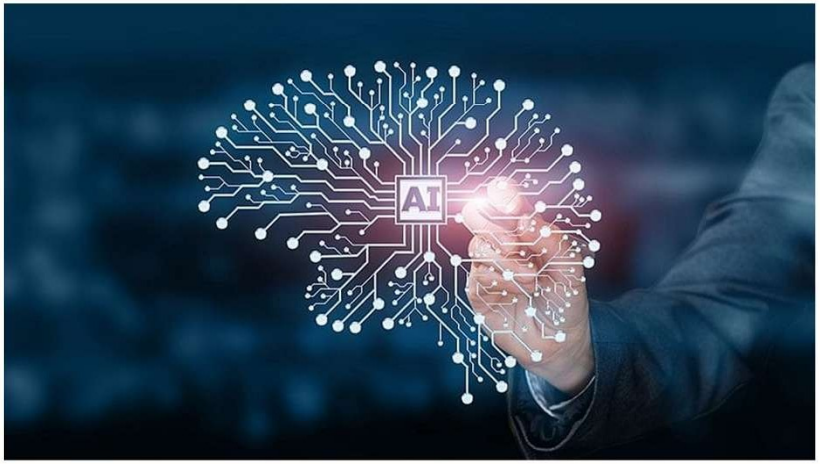
Informatikai alapfogalmak

PICS

A számítógépes rendszer olyan szoftver és hardverkomponensek összessége, amelyek együttesen bizonyos funkciókat látnak el. A szoftvert (vagyis alkalmazást) validálni kell, az infrastruktúrát pedig kvalifikálni.



Informatikai alapfogalmak



- Hardver (angolul: *hardware)* alatt a számítógép fizikailag megfogható részeinek összességét értjük. A számítógép működéséhez alapvetőn hardver és szoftver szükséges, a kettő közötti kapcsolatot a firmware hozza létre, ami a hardverekbe a gyártók által „beépített” szoftvernek tekinthető.
- A firmware (angol: a.m. gyári beépített szoftver) egy olyan szoftverfajta, amely a hardvereszközbe van beépítve, és a hardver működtetéséhez szükséges legalapvetőbb feladatokat látja el (esetleg figyeli az eszköz állapotát, arról információkat nyújt a külvilágnak).

Informatikai alapfogalmak

Szoftver:

Eudralex

A számítógépes rendszer olyan szoftver és hardverkomponensek összessége, amelyek együttesen bizonyos funkciókat látnak el. A szoftvert (vagyis alkalmazást) validálni kell az infrastruktúrát pedig kvalifikálni.

ISO 9001:2008:

Szoftvernek kell tekinteni minden olyan programozható eszközt, amely a minőségirányítás körébe bevont és annak eredményeit biztosító berendezésben, eszközben megtalálható, vagyis amelyet, adatok rögzítésére, tárolására, feldolgozására, fogadására, továbbítására, jelentés készítésére vagy vezérlésre használnak.

FDA

(Code of Federal Regulations, Title 2 1, Parts 800 - 895). A szoftver lehet egy teljesen önálló, vagy egy önmagában több részegységből felépülő, vagy a felhasználás céljából különálló eszköz.

A szoftverek funkciójuk szerint

- Aszerint, hogy egy szoftver specifikusan mennyire inkább a gép puszta működtetését, avagy az ember által igényelt feladatmegoldást segíti elő, a következő *funkcionális* csoportokat különböztetjük meg:
  - indítóprogram vagy alapszoftver – a felhasználó által a legkevésbé manipulálható, a gép üzemszerű működését beállító program(ok), ide tartozik a firmware is
  - rendszerszoftverek – a gép és perifériái kommunikációját lebonyolító programok, beleértve a felhasználó oly mértékű kiszolgálását, amely lehetővé teszi a számára más szoftverek elkészítését és üzembe helyezését is
  - alkalmazói szoftverek vagy alkalmazások – a felhasználót a számítógép használatán túl mutató céljainak elérésében támogató specifikus programok.

Magyar hatósági szabályozások

- 44/2005 (X.19.) EüM. Rendelet „Az emberi alkalmazásra kerülő gyógyszerek gyártásának személyi és tárgyi feltételeiről”
- Eat. - 2001. évi XXXV. törvény az elektronikus aláírásról

Nemzetközi szabályozások

- Számítógépes rendszerek kezelésére, validálására vonatkozóan:
  - FDA 21 CFR part 211.
  - GMP directive 2003/94.
- az elektronikus adatok és aláírások kezelésére:
  - Annex 11 of the GMP
  - a 21 CFR part 11 használatos.
- Az európai és amerikai FDA által elfogadott az ipari területen alkalmazandó útmutatások:
  - GAMP 5
  - és az alkalmazás részletezéséről szóló IEEE és PICS

Nemzetközi szabályozások (Kidolgozás alatti szabályozások)

- Annex 22 (AI rendszerek)
  - AI validálása és emberi felügyelet
  - Kockázat-alapú megközelítés
- Felhőrendszerekre vonatkozó új előírások
  - Adatbiztonság pontosítása
  - Audit trail követelmények erősítése
- Új Annex 11 tervezet
  - PQS kiterjesztése számítógépes rendszerekre
  - Részletes kockázatmenedzsment és validálás
  - Audit trail, identitás- és hozzáférés-kezelés, biztonság
  - Backup és archíválás hangsúlyos előírásai

Inspektori gyakorlat ellenőrzésnél

Amikor egy GxP ellenőrnek egy szabályozott felhasználó telephelyén telepített számítógépes rendszert kell értékelnie, akkor néhány vagy az összes is szempontba vehető:

- Az ellenőr figyelembe veszi az automatizált rendszertől a vizsgálat minőségére vagy az adatintegritásra vonatkozó potenciális kockázatokat, amelyeket a szabályozott felhasználó azonosít és dokumentál a rendszer(ek) alkalmas célra való értékelése érdekében.
- A vállalat kockázatelemző nyilvántartásai is hivatkozási pontot képezhetnek ebben a folyamatban.
- Az ellenőr értékelése magában foglalhatja a rendszer életciklusát, minőségbiztosítási intézkedéseket, validálási és üzemeltetési irányítási bizonyítékokat a vezérlő rendszerre vonatkozóan, valamint validálási és üzemeltetési tapasztalatokat az irányított folyamat terén is.

Adatbiztonság

Elektronikus adat: Elektronikus adatok: Az információk, tények vagy számítógépes programok olyan formában vagy rajtuk, amelyeken létrejönnek, használatosak vagy továbbítódnak számítógépes szoftveren (beleértve a rendszerek és alkalmazások szoftverét is),

ERES

Elektronikus aláírás: Amennyiben vannak elektronikus adatok ezek alá is íhatóak elektronikusan. Az elektronikus aláírásokra az alábbiak elvárhatók **Eudralex Volume 4 Annex 11 14**: Eat. - 2001. évi XXXV. törvény az elektronikus aláírásról - Jogtár

a. Azonos hatással legyenek, mint a kézzel írott aláírások a vállalat belső keretein belül,
b. Tartósan kapcsolódjanak a megfelelő rekordhoz,
c. Tartalmazzák az alkalmazásuk időpontját és dátumát.

Kockázat

Eudralex Volume 4 Annex 11 1 A kockázatkezelést az informatikai rendszer teljes életciklusa során alkalmazni kell, figyelembe véve a páciens biztonságát, az adatintegritást és a termék minőségét. A kockázatkezelési rendszer részeként a validálás és az adatintegritás ellenőrzéseinek mértékéről szóló döntéseket alapos és dokumentált kockázatértékelésen kell alapulniuk az informatikai rendszer esetében.

Adatbiztonság
Elektronikus aláírás az Eat. (2001. évi XXXV. törvény) szerint

Alapfogalmak

•**Elektronikus aláírás**: elektronikus dokumentumhoz azonosítás céljából hozzárendelt és elválaszthatatlanul összekapcsolt elektronikus adat.

•**Fokozott biztonságú elektronikus aláírás**:

- egyedülállóan az aláíróhoz köthető,
- kizárólag az aláíró ellenőrzése alatt áll,
- minden dokumentummódosítás érzékelhető.

Jogi hatás

•Az elektronikus aláírás jogilag az írásbeli aláírással egyenértékű lehet, ha megfelel a törvényben meghatározott feltételeknek.

•Biztosítja:

- az aláíró személyének hiteles azonosítását,
- a dokumentum sértetlenségét.

Adatbiztonság
Elektronikus aláírás az Eat. (2001. évi XXXV. törvény) szerint

A **2001. évi XXXV. törvény az elektronikus aláírásról (Eat.)** kimondja, hogy:

- **Egyszerű elektronikus aláírás**: pl. név + dátum egy dokumentumban, ez **önmagában nem minősül joghatással bíró aláírásnak**, de belső minőségbiztosítási célra elfogadható, ha szabályozott környezetben történik.
- **Fokozott biztonságú elektronikus aláírás**: amely egyedi azonosításhoz kötött, és bizonyított, hogy kizárólag az aláíró rendelkezik felette.
- **Minősített elektronikus aláírás**: csak akkreditált hitelesítésszolgáltató (pl. NISZ, Microsec) által kibocsátott tanúsítvány alapján jön létre, és teljes joghatással **egyenértékű a kézzel írott aláírással**.

Adat integritási alapelvek

Adatintegritás azt jelenti, hogy a digitális információ sérülésmentes és csak azok által érhető el vagy módosítható, akik erre jogosultak. Az adatintegritás azt írja le, hogy az adatok teljes, pontos, következetes és biztonságos módon vannak tárolva az egész életciklusuk során az alábbiak szerint: Teljes.

Adat integritási elemei

Eudralex Volume 4, Annex 11, 5:
Az adat: A számítógépes rendszerek elektronikus úton adatokat cserélnek más rendszerekkel. Az adatok helyes és biztonságos bevitelének, feldolgozásának és továbbításának érdekében megfelelő beépített ellenőrzéseket kell alkalmazni a kockázatok minimalizálása érdekében.

Eudralex Volume 4, Annex 11, 5:
A pontosság ellenőrzése: A kritikus adatok manuális bevitele esetén be kell vezetni egy további ellenőrzést a pontosság tekintetében. Ez az ellenőrzés lehet egy második felhasználó vagy egy validált ellenőrzési megoldás által végzett. A kritikus adatok helytelen vagy hibás bevitele kritikus lehet, és ennek lehetséges következményeit a rendszerre vonatkozó kockázatkezelési intézkedésekben kell figyelembe venni.

Adat integritási elemei

Az adatok tárolása
Eudralex Volume 4, Annex 11, 7:
7.1 Az adatokat fizikai és elektronikus eszközökkel egyaránt védeni kell a sérülés ellen. Tárolt adatokat ellenőrizni kell az elérhetőség, olvashatóság és pontosság szempontjából. Az adatokhoz való hozzáférés biztosítva kell legyen a megőrzési időszak teljes egészében.

Eudralex Volume 4, Annex 11, 7:
7.2 Az összes releváns adat rendszeres biztonsági mentéseket kell végezni. A biztonsági mentés adatok integritása és pontossága, valamint az adatok helyreállításának képessége ellenőrzésre kerül a validálás során, és időszakosan figyelmeztetve kell lenni.

Adat integritási elemei

Nyomtatványok, nyomtatások

Lehetőségnek kell lennie az elektronikusan tárolt adatok nyomtatott másolatainak előállítására.

Adat integritási elemei

Fizikai és/vagy logikai ellenőrzéseket kell alkalmazni a számítógépes rendszerhez való illetéktelen hozzáférés megakadályozása érdekében. Az engedély nélküli belépés megakadályozására alkalmas módszerek közé tartozhatnak a különböző kulcsok, kártyák, személyes kódok és jelszavak, biometrikus azonosítás, korlátozott hozzáférés a számítógépes berendezésekhez és adattárolási területekhez.

A biztonsági ellenőrzések mértéke a számítógépes rendszer kritikusságától függ

Audit trail ellenőrzése minden esetben kihívás. Nem csak a rendszernek kell képesnek lennie minden audit trail rögzítésére törölhetetlen módon, de ebben képesnek kell lennünk keresni, és megfelelő stratégiát felállítani az ellenőrzésére lehetőleg kockázati alapon.

Az audit trailnek tehát:

- Kikapcsolhatatlannak
- Minden adatokat vagy rendszert érintő változást követhetőnek
- Törölhetetlennek
- És kereshetőnek
- Olvashatónak

Kell lennie.

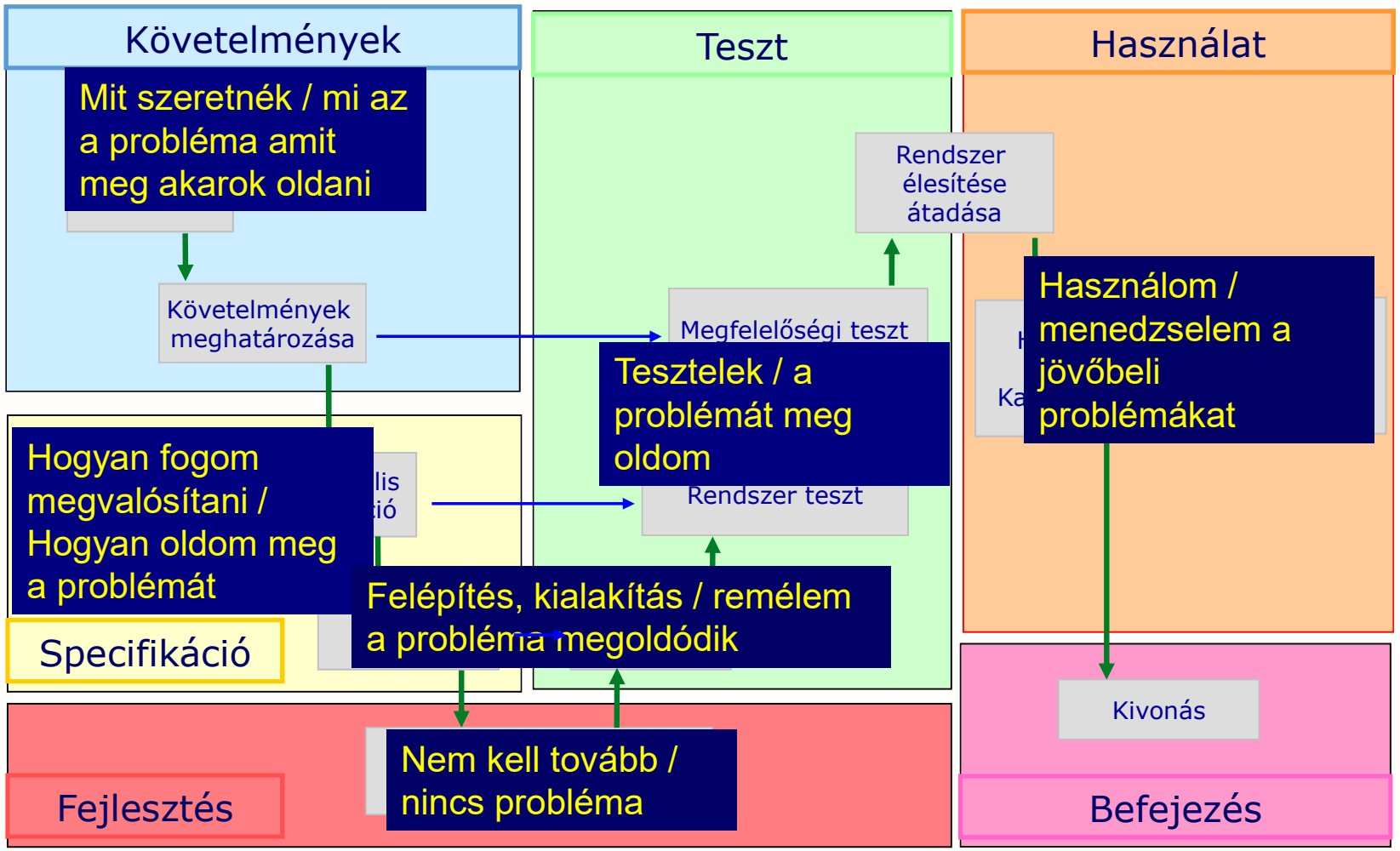
Adat integritási elemei

Biztonság

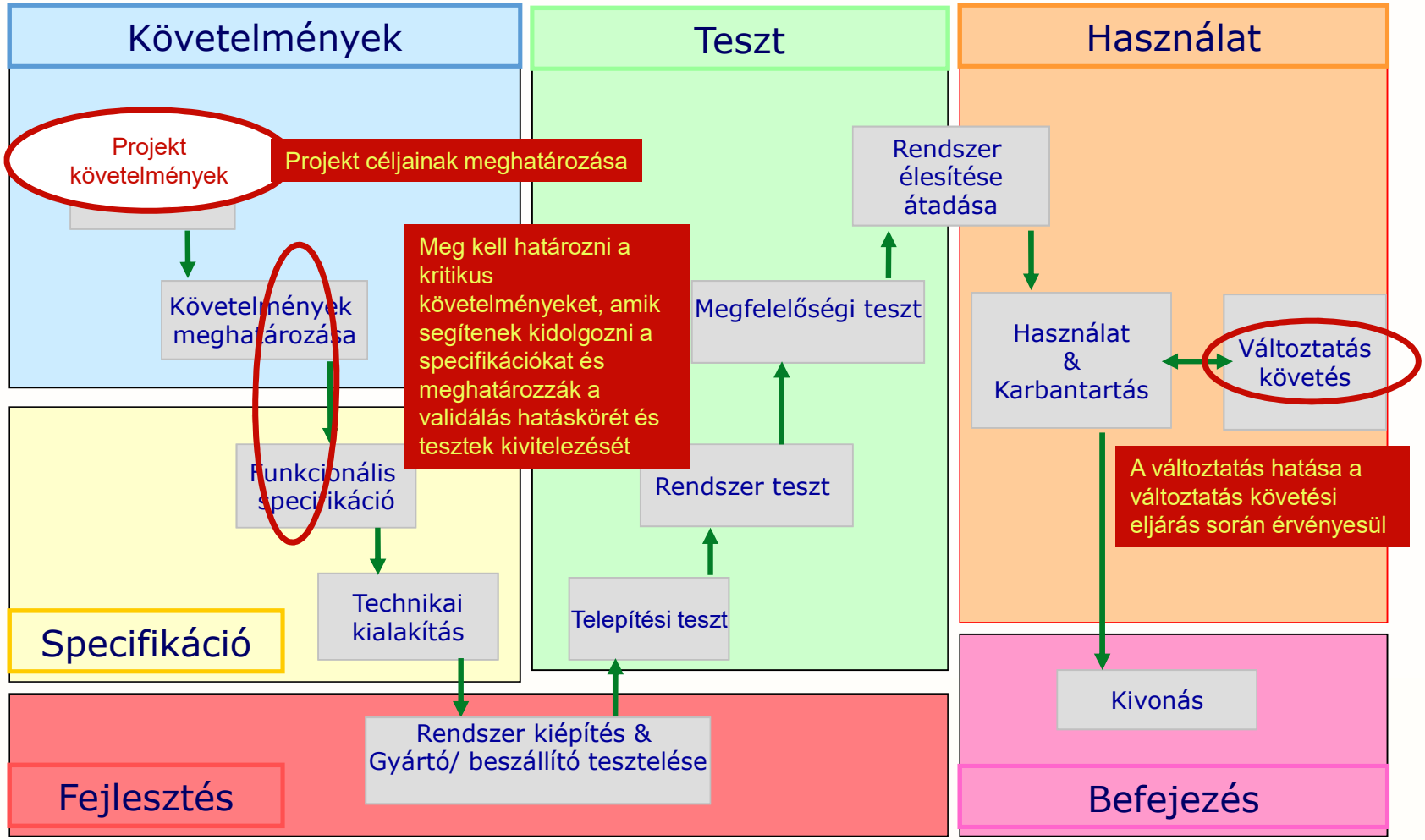
Az engedélyek létrehozásának, módosításának és megszüntetésének ténye rögzítésre kerüljön.

Az adatok és dokumentumok kezelési rendszereinek rögzíteni kell a belépő, módosító, megerősítő vagy törlő felhasználó azonosítását, beleértve a dátumot és az időt.

Tipikus validálási életút (V-model)

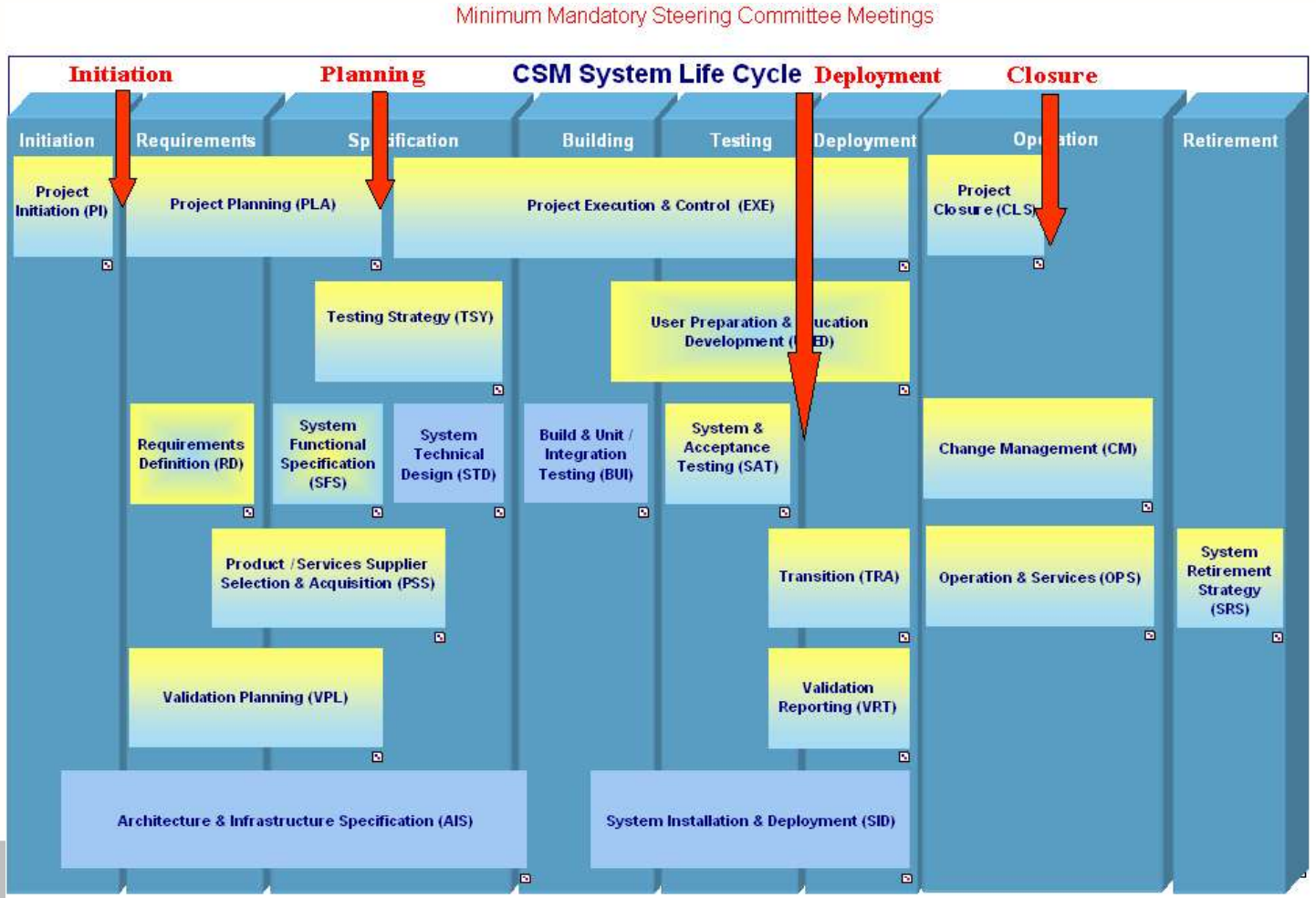


Validálási életút – Kockázat menedzsment



Számítógépesített rendszerek, validálási életútja

Az életciklus: Az összes rendszer életében jelentős fázis, kezdve az első követelményektől egészen a rendszer kivonásáig (megszüntetéséig). Ezen időszak során a rendszer tervezésen, specifikáción, programozáson, tesztelésen, telepítésen, működtetésen és karbantartáson megy keresztül.



Kommunikáció, interface

- A számítógépes rendszerekkel kapcsolatos kommunikáció nagyjából két kategóriába sorolható: számítógépek közötti és számítógépek és perifériális komponensek közötti kommunikáció.
- Minden kommunikációs kapcsolat potenciális hiba lehetőséget rejt magában, ami adatvesztést vagy adathibát eredményezhet. Ezért megfelelő biztonsági és rendszerintegritási ellenőrzéseket kell elvégezni a számítógépes rendszerek fejlesztése, validálása, üzemeltetése és karbantartása során.

Karbantartás

Az összes számítógépes rendszert úgy kell telepíteni és karbantartani, hogy az a pontos működés folytonosságát biztosítsa.

Migrálás

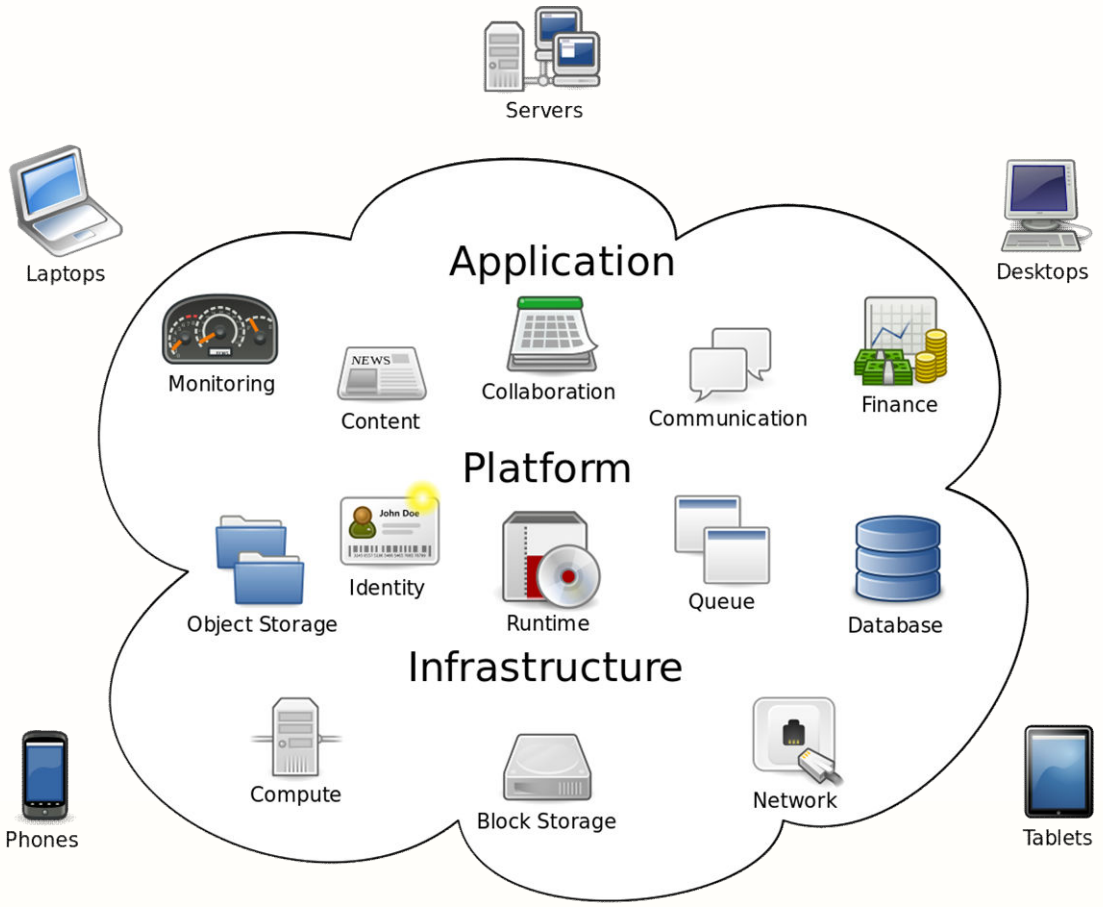
- Ahol a teljes funkcionalitás migrációja technikailag nem lehetséges, ott kockázat elemzést kell végezni és meg kell határozni hogy a migrálás mely részeire és hogyan terjed ki az adatoknak.
- A migrációs fájlformátumot úgy kell kiválasztani, hogy az kiegyensúlyozza a hosszú távú hozzáférés kockázatát, vagyis azt a tényt , hogy az adatok visszaolvashatósága a visszaolvasó technikával változhat.
- Fontos felismernünk, hogy a hozzáférhetőség fenntartásának szükségessége olykor azt eredményezheti, hogy a migráció olyan fájlformátumba történik, amely elveszít néhány attribútumot és/vagy dinamikus adatfunkciót. A TFM (Technikai File Menedzsment) felelőssége annak értékelése, hogy ilyen veszteségek milyen hatással vannak az adatra, minden esetben fenn kell tartani a linket amiben olvasható formátumban szerepel audit trail vagy elektronikus aláírások és az auditált adat illetve a közöttük való kapcsolat.


Apple I
ABC 80
Commodore 64
ZX 81
ZY Spectrum
Enterprise

Kvantum előny

A kvantumszámítógép előnye pár éve még másodpercekben volt mérhető, azóta exponenciálisan nőtt a teljesítmény.

- A Google kvantumszámítógépe, a Sycamore legutóbbi változata olyan műveleteket végez el másodpercek alatt, amivel napjaink leggyorsabb szuperszámítógépe 47 év alatt birkózna csak meg – derül ki egy, a szaksajtóban még nem megjelent beszámolóból.
- A számítógépek bináris rendszerben számolnak, egy bit értéke 1 vagy 0 lehet. A kvantumszámítógépek qubitjei a kvantum világ törvényein alapulnak, így értékük 1-es, 0 vagy mindkettő lehet. Ahogy a hagyományos processzorok teljesítményét nagyban meghatározza, hogy 8, 16, 32 vagy 64 bitesek, a kvantumszámítógépeknél a teljesítményük szempontjából is alapvető kérdés, hogy hány qubitet kezelnek.
- A kvantumszámítógépek potenciálisan sokkal hatékonyabbak komplex számítások elvégzésében, és amióta fejlesztik őket, fontos mérföldkő, hogy mikor képesek legyőzni a hagyományos szuperszámítógépeket. Az 53 qubites Sycamore négy évvel ezelőtt még másodpercekkel győzte le a legerősebb szuperszámítógépet, a Frontiert. A Google kvantumszámítógépe ekkor érte el az úgynevezett kvantumfölényt, megelőzve a hagyományos számítógépet.
- A Sycamore azóta 17 qubittel bővült, amivel számítási kapacitása exponenciálisan nőtt.


Servers
Laptops
Desktops
Application
Monitoring
Content
Collaboration
Communication
Finance
Platform
Identity
Object Storage
Runtime
Queue
Database
Infrastructure
Compute
Block Storage
Network
Phones
Tablets
Cloud computing

Mi a felhő?

- Informatikai szolgáltatások gyűjteménye
  - Kiszolgálók (szerverek)
    - Web, fájlszerver, csoportmunka, stb.
  - Adatbázisok
  - Hálózati szolgáltatások
  - Elemzési és BI lehetőségek
    - Dahsboard, riport szolgáltatás,
- Előnyök
  - Rugalmasan skálázható
    - Igazítani lehet a szükséges erőforrás mennyiséget a kívánalmakhoz
  - Magas szintű adatbiztonság és rendelkezésre állás
  - Költséghatékony
    - Nincs üzemeltetési költség

Hogy is működik?

- A szolgáltató biztosítja a hozzáférést a virtuális környezethez
  - Privát vagy nyilvános a szolgáltatás
  - Az adat- és információbiztonság a szolgáltatás része, mértéke egyéni igényeken is alapul
  - A megrendelő dönt a virtuális környezetben felépített IT eszközökről és szolgáltatásokról
    - Milyen szerver konfigurációt, adatbázist hoz létre
    - Milyen szoftveres támogatást igényel
    - Milyen biztonsági szinteket, biztonsági eljárásokat választ
- A szolgáltató dedikálja az infrastruktúrát, de nincs lehetősége hozzáférni a tartalmakhoz!

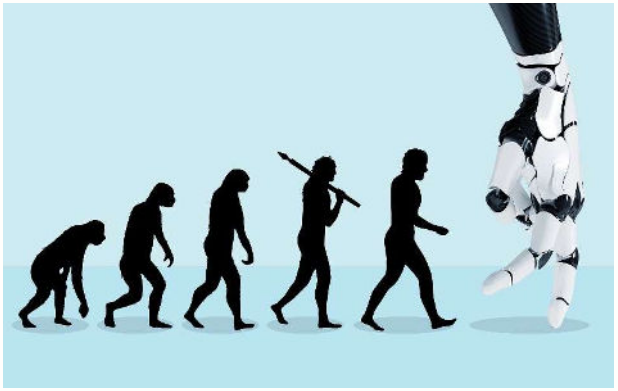
A mesterséges intelligencia fajtái

- **Asszisztens AI (Narrow AI)**
  Meghatározott feladatokra specializált rendszerek.
  Példák: képfelismerés, nyelvi feldolgozás, minőségellenőrzés, prediktív karbantartás.
  → Az Annex 22 főként ezekre vonatkozik, mivel jelenleg ezeket alkalmazzák GxP környezetben.
- **Általános AI (General AI)**
  Olyan intelligencia, amely képes bármilyen probléma megoldására, emberi gondolkodáshoz hasonlóan.
  → Egyelőre elméleti szinten van, de Annex 22 előkészíti a kereteket, ha a jövőben megjelenik.
- **Szuper AI (Super AI)**
  Hipotetikus szint, amely minden területen meghaladja az emberi képességeket.
  → Szabályozói szempontból még távoli, inkább koncepcionális kategória.

Mesterséges intelligencia kihívásai

A mesterséges intelligencia egy eszköz, mely lerövidítheti, illetve helyettesítheti az emberi beavatkozást a vizsgálatokhoz tartozó:

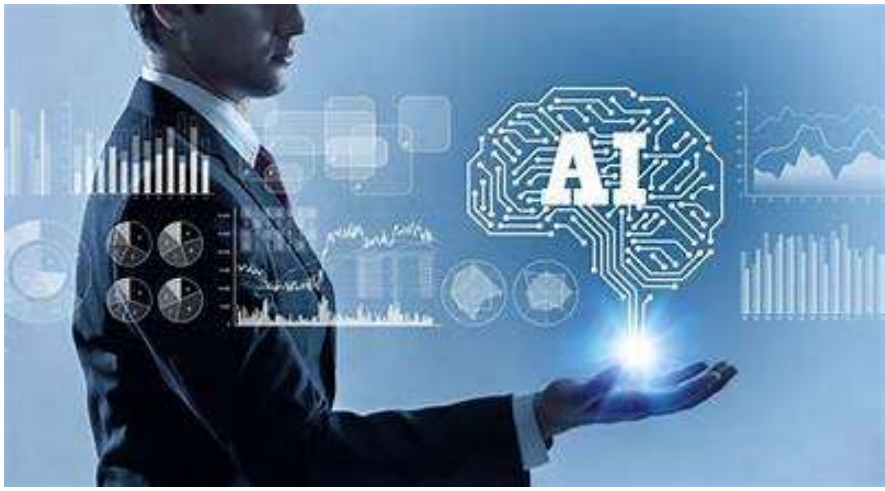
- Adatok bevitelében
- Adatok Kezelésében
- Mérések kivitelezésében
- Eredményeinek feldolgozásában.



Ugyanakkor ezek megbízható működését és működtetését igazolni kell tudni, validálni kell.

Annex 22 – Emberi ellenőrzés

- Emberi felügyelet nélkül nem engedélyezett AI-döntés GxP környezetben
- A végső felelősség mindig a felhasználónál / QP-nél marad
- AI által javasolt eredményeket review / approve folyamatban validálni kell
- Transzparencia és magyarázhatóság (explainability): a felhasználó megértse, mit és hogyan számolt a rendszer
- Követelmény a kockázat-alapú dokumentálás, hogyan biztosítják a felügyeletet



Annex 22 – AI betanítás és validálás

- Adatkészletek minősége és integritása kulcskérdés (adatforrások validálása)
- Bias / torzítás elkerülése: tréningadatok kiegyensúlyozottságának igazolása
- Reproducibilitás: AI betanítási folyamat dokumentáltan ismételhető legyen
- Tesztelés élesítés előtt – validált környezetben, kockázatértékelés alapján
- Folyamatos monitoring és újratanítás kontrollált környezetben, változáskezelés alá vonva


thank you
thank you
thank you
thank you
thank you
thank you
thank you
thank you

!!