IT rendszerek minőségbiztosítása

Dr. Szaller Zoltán

IT rendszerek minőségbiztosítása

- Köszönetnyilvánítás

• Köszönet Dr. Ronald Bauernak (AGES, Ausztria) a 13. OECD Training Course-on tartott remek előadásáért és bemutatójáért

• Köszönet Martijn Baetennek (Scientific Institue of Public Health, Belgium) a 13. OECD Training Course-on tartott remek előadásáért és bemutatójáért

Mindkettejük gondolatait felhasználtam ehhez az oktatáshoz

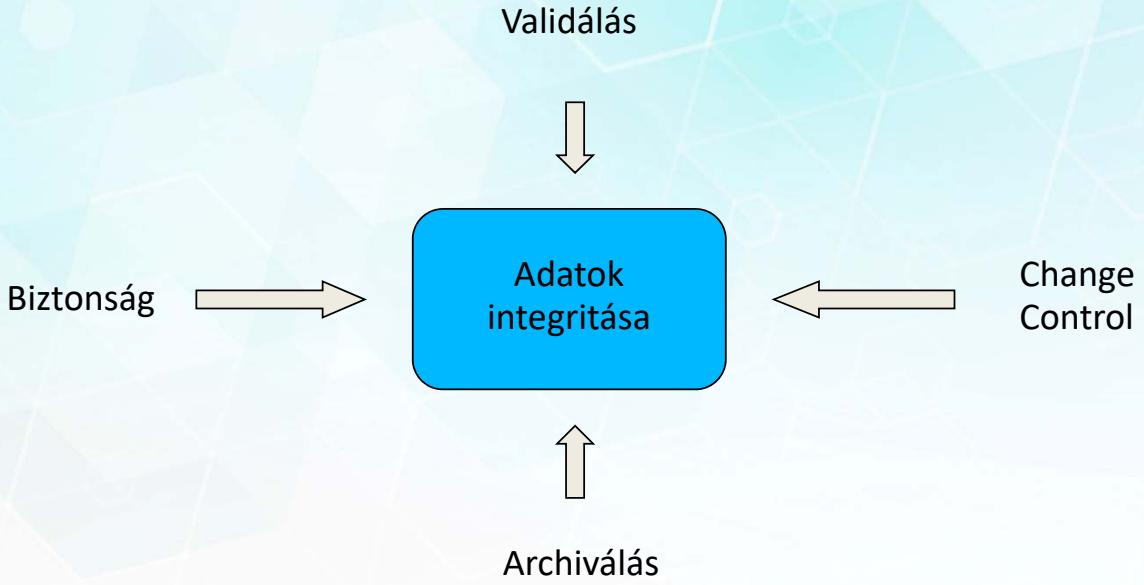
IT rendszerek minőségbiztosítása

- Általános meggondolások:

  - Az inspektált félnek meg kell győznie a hatóságot az adatok minőségéről és megbízhatóságáról

IT rendszerek minőségbiztosítása

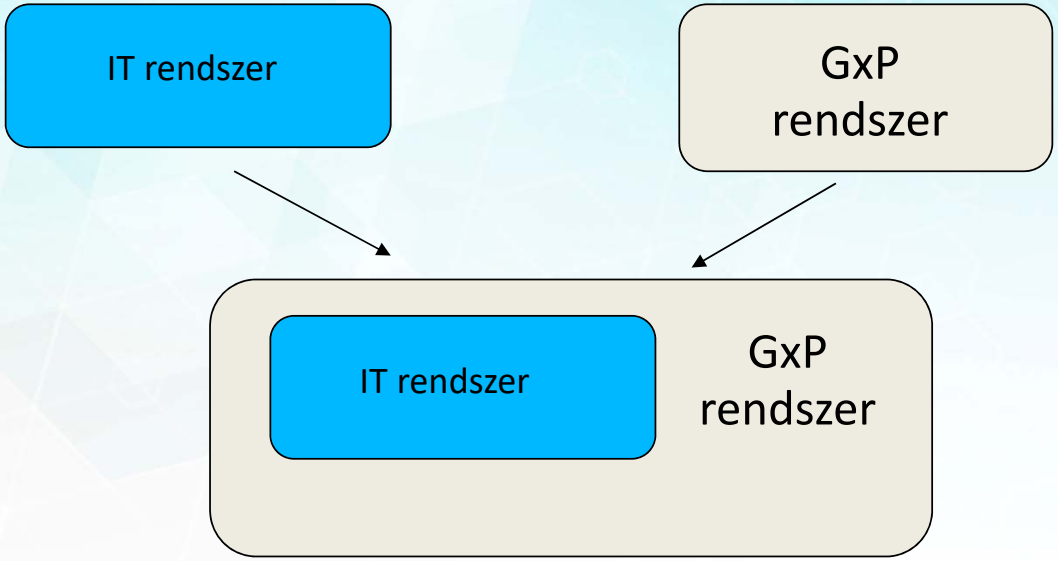
- Általános meggondolások



IT rendszerek minőségbiztosítása

- Általános meggondolások

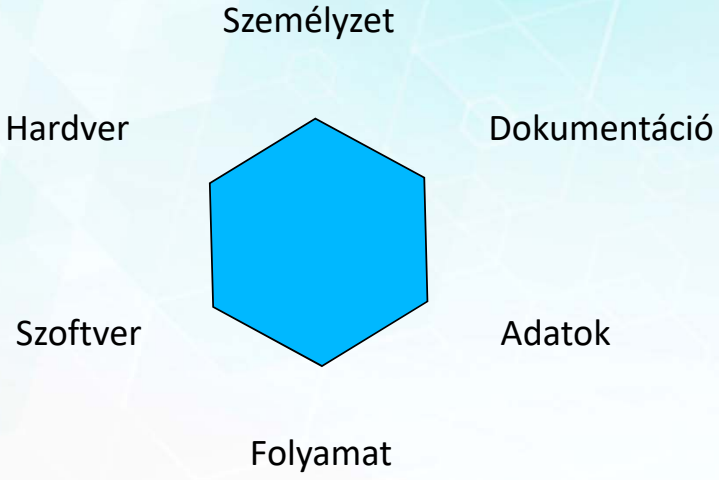
A számítógépes rendszerek legyenek a GxP rendszer részei



IT rendszerek minőségbiztosítása

- Általános meggondolások

A GxP megfelelőség többváltozós egyenlet eredménye:



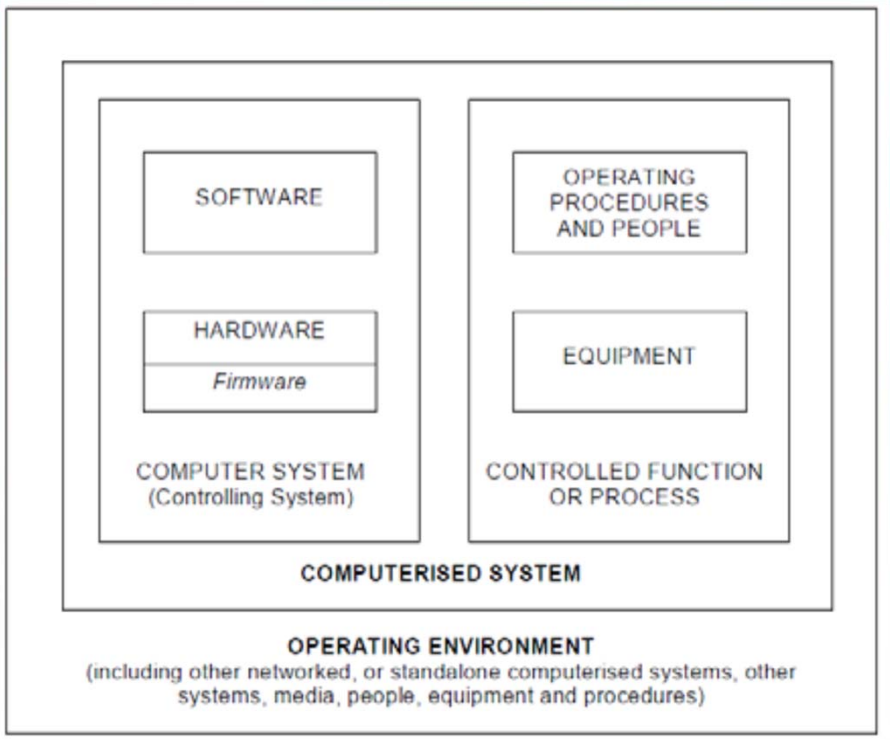
IT rendszerek minőségbiztosítása

- Definíciók

"A computerized system is a function (process or operation) integrated with a computer system and performed by trained personnel. The function is controlled by the computer system. The controlling computer system is comprised of hardware and software. The controlled function is comprised of equipment to be controlled and operating procedures performed by personnel." PIC/S PI 11-3 "Good Practices for ComputerisedSystems in Regulated GxP Environments"

IT rendszerek minőségbiztosítása

- Definíciók



IT rendszerek minőségbiztosítása

- Definíciók

Komplex rendszerek: kromatográfiás menedzsment rendszerek, laboratóriumi információs rendszerek, adatgyűjtő / monitorozó rendszerek, archiváló / dokumentációs rendszerek, vállalati menedzsment rendszerek stb.

IT rendszerek minőségbiztosítása

- Definíciók

Egyszerű rendszerek: automata pipetták, pH-mérők, mérlegek, hűtők stb.

IT rendszerek minőségbiztosítása

- „ An **audit trail** (also called **audit log**) is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event. „ (Wikipedia)
- Az audit trailt generáló folyamatnak tipikusan állandóan privilegizált módban kell futnia azért, hogy hozzáférjen és felügyelni tudja az összes felhasználó minden tevékenységét.

A felhasználóknak nem lehet arra lehetőségük, hogy az audit trailt leállítsák vagy a futási módját megváltoztassák. Az audit trailt tároló táblázatok, adatbázisok a felhasználók számára hozzáférhetetlenek kellenek, hogy legyenek. Egy másik módja ennek a szerepkörökre alapozott biztonsági modell. A szoftver működhet zárt-hurkolt ellenőrzéssel, vagy mint „zárt rendszer”.

Egy informatikai rendszer akkor **zárt**, ha minden lehetséges inputja ismert és kontrollált.

IT rendszerek minőségbiztosítása

- Definíciók

GAMP 5 szoftver kategóriák

Category	What comes under?	Description
Category 1	Infrastructure Software (Standard Software)	Operating Systems,
Category 2	Firmware (Discontinued)	Laboratory equipment
Category 3	Non configured products	Products cannot be configured or sometimes can be configured but only the default configuration can be used
Category 4	Configured products	Configuration can be done to meet the user specific needs.
Category 5	Custom applications	These applications are developed to meet the specific needs of the regulated company.

IT rendszerek minőségbiztosítása

- Validálás

Alapvető fontosságú annak dokumentált bizonyítása, hogy a számítógépes rendszer megfelel a tervezett céljának. Ezt hívjuk a számítógépes rendszer validálásának.

Mit is próbálunk megválaszolni:

- megfelel a rendszer a tervezett célnak?
- megbízhatunk a rendszer által szolgáltatott adatokban?

A validálás önmagában *nem garantálja* feltétlenül az adatok megbízhatóságát (de lehetővé teszi bizonyos inkonzisztenciák feltárását). Fontos, hogy a számítógépesített rendszert ***megfelelően*** használják.

Ugyanakkor a validálás gyengesége jelezheti az adatok gyengeségét.

IT rendszerek minőségbiztosítása

- Validálás

Megfelel a célnak – az mit is jelent?

• Sok (a legtöbb) esetben a rendszereknek vannak olyan funkcióik, amiket sohasem használnak.

• De validálni kell minden olyan funkciót, amit GxP célokra használnak

•Kockázatelemzés➡ URS (User requirement Specification)➡ Functional Design / Specification ➡ Kockázatelemzés➡ Validálási terv ➡ Validálás➡ Validálási jelentés

➢SOP-k

➢Oktatás

IT rendszerek minőségbiztosítása

- Validálás

Validálni kell, ha:

- a rendszer által generált vagy szolgáltatott adatok benyújtásra kerülnek az értékelő hatósághoz
- a rendszer által generált vagy szolgáltatott adatok érdemi GxP döntés alapjául szolgálnak (pl. felszabadítás vagy study értékelése)
- a rendszer által generált vagy szolgáltatott adatok direkt vagy indirekt módon támogatnak más GxP releváns adatokat

A validálásnak prospektívnak kell lennie!

IT rendszerek minőségbiztosítása

- Validálási stratégia

• Értsd meg a számítógépesített folyamatot

•Mérd fel, hogy mely rendszereket és azoknak mely funkcióit fogod használni

•Gondold át magadban az adatáramlás útját (a számítógépesített folyamatot leíró SOP-k, illetve a szoftver(ek) kézikönyve(i) segíthetnek)

•Gondold át az adatok nyerésének / rögzítésének a módját

•Gondold át a számolások módját (SOP-k)

IT rendszerek minőségbiztosítása

- Ne felejtsd el!

• Egy validált számítógépes rendszer is

  •használható nem megfelelő módon

  •használható manipulációra (szándékosan és szándékolatlanul is)

IT rendszerek minőségbiztosítása

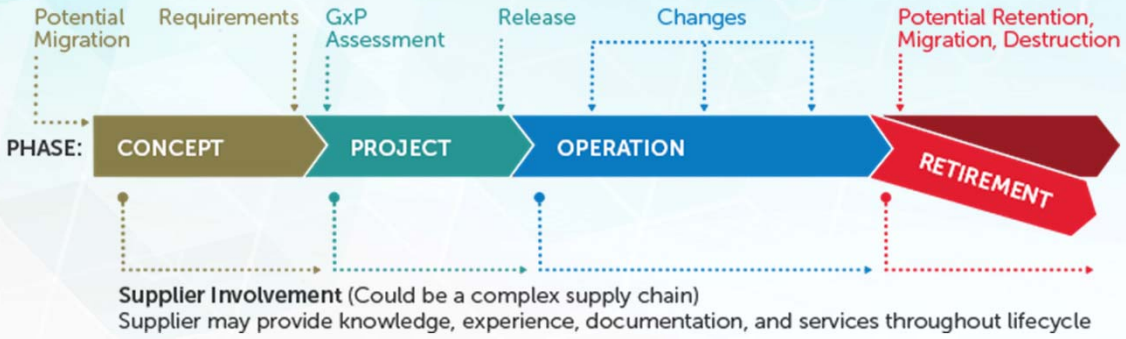
- Változtatások, konfiguráció-kontroll (az életciklus minden fázisára alkalmazandó)

• Szerepek és felelősségek

• Hardver és szoftver

• Folyamatok (áttekintés, jóváhagyások, tesztelések, kockázatelemzés stb.)

• Szoftver kategorizálása a GAMP5 szerint



IT rendszerek minőségbiztosítása

- Személyzet, szerepkörök, felelősségek

A menedzsment:

• viseli a végső felelősséget a rendszerek validált állapotáért

• definiálja a szerepeket és felelősségeket a számítógépes rendszerek fejlesztésével, validálásával, működtetésével és karbantartásával kapcsolatban

• delegálja a felelősségeket részben vagy teljes egészében a megfelelően oktatott személyzetnek

• értékeli a beszállítókat kockázati és komplexitási alapon (bizonyítási kötelezettség!)

• biztosítja, hogy a társaságon belül globálisan működő számítógépes rendszert lokálisan megfelelően üzemeltessék és tartsák karban a vonatkozó GxP rendszer szerint

• Szükség lehet írásba foglalt belső „szerződésekre”

IT rendszerek minőségbiztosítása

- Személyzet, szerepek, felelősségek

A felhasználó (különösen a QP, illetve GLP-ben a Study Director) viseli a felelősséget:

• az elektronikus adatok megbízhatóságáért (ALCOA – Attributable, Legible, Contemporaneous, Original, Accurate) ugyanúgy, mint a papíron rögzített adatoknál

• A rendszer tulajdonosa (system owner) felelős a megfelelő oktatás biztosításáért, hogy a folyamatot jól megértsék és a rendszert helyesen használják

• GLP esetében a Study Director igazolja, hogy a számítógépes rendszer megfelel a vizsgálat céljainak és validált állapotban van a vizsgálat elvégzése során

IT rendszerek minőségbiztosítása

- Személyzet, szerepek, felelősségek

A QA

• tudatában kell legyen a GxP-releváns számítógépes rendszereknek

• igazolja, hogy a számítógépes rendszer validálása, működtetése és fenntartása során betartják a szabványokat és előírásokat, akár saját szakértelme által, akár külső szakértőket bevonva

• igazolja a megfelelő használatot: ehhez olyan oktatás kell, ami biztosítja a számítógépesített folyamat teljes és részletes megértését

• auditálja az adatokat: ehhez olvasási hozzáféréssel kell rendelkeznie a számítógépes rendszerekben tárolt adatokhoz, különösen az *audit trail*-ekhez

IT rendszerek minőségbiztosítása

- Személyzet, szerepek, felelősségek

Felhasználók azonosítása

•Jogilag megkövetelt, hogy minden felhasználót egyedileg kell azonosítani GxP kritikus rendszerekben.

•Történhet egyedi usernév / jelszó párossal, de ez jogilag nem minősül elektronikus aláírásnak – az ilyen rendszer informatikai zártságát igazolni kell!

•Az elektronikus aláírást az Európai Unió területén kötelező elfogadni, a felhasználót egyértelműen és egyedileg azonosítja, valamint biztosítja, hogy az aláírt adatok az alírás után már ne legyenek nyom nélkül megváltoztathatóak

IT rendszerek minőségbiztosítása

- Személyzet, szerepek, felelősségek

Az elektronikus aláírás

•**Az elektronikus aláírás nem a beszkennelt kézzel írott aláírást jelenti, nem is a usernév/jelszó párost, hanem a kódolás egy speciális változatát**. Ha egy dokumentumot elektronikusan írunk alá, akkor olyan módon kódoljuk, hogy a létrejött kódolt dokumentum hitelességét annak szerkezete biztosítja.

•A bekódolás az ún. titkos kulccsal történik – ez csak az aláíró személy birtokában van, ezt ki nem adja (ha jót akar magának). A kulcs használatához a felhasználónak valamilyen módon azonosítania kell magát (intelligens kártya, biometrikus azonosítás stb.).

•A kikódolás az ún. nyilvános kulccsal történik – ez része az aláírt dokumentumnak, megfelelő programok (pl. MS Word, Adobe Reader stb.) eleve képesek felismerni és használni.

•A kódolás egyirányú, a nyilvános kulcsból nem lehet visszakövetkeztetni a titkos kulcsra.

IT rendszerek minőségbiztosítása

- Személyzet, szerepek, felelősségek

Az elektronikus aláírás

•Az aláírás létrehozásához szükség van egy aláírás-létrehozó adatra és egy tanúsítványra. Mindkettő csak hiteles, a kormányzat által akkreditált forrásból szerezhető be, személyes azonosítás után. A kódolást egy erre a célra kifejlesztett szoftver végzi el.

•Az elektronikus aláírásnak két szintje van: minősített és fokozott biztonságú. A minősített a legmagasabb biztonsági szintű. Az Eat. szerint a minősített aláírás olyan fokozott biztonságú elektronikus aláírás, amely minősített tanúsítványra épül, és amelyet biztonságos aláírás-létrehozó eszköz (pl. egy speciális minősítésű intelligens kártya avagy chipkártya) segítségével hoztak létre. A minősített elektronikus aláírás mindenképpen kriptográfiai technológiákra épül a Nemzeti Hírközlési Hatóság által meghatározott kriptográfiai algoritmuskészletek alapján. A fokozott biztonságú elektronikus aláírás a minősítettnél alacsonyabb biztonsági szintet képvisel, sokkal kevesebb szabály vonatkozik rá. A fokozott biztonságú aláírás is kriptográfiai megoldásokra épül, de nem olyan szigorú.

IT rendszerek minőségbiztosítása

- Személyzet, szerepek, felelősségek

Az elektronikus aláírás

•Az elektronikusan aláírt dokumentum tartalmaz egy időtanúsítványt is (ezt megint csak megfelelő szolgáltatótól lehet beszerezni), ezzel válik az aláírás időpontja hitelessé.

•Az elektronikusan aláírt dokumentum **minden elektronikus másolata eredeti**nek számít, mert az elektronikus aláírás minden eleme változatlanul megtalálható bennük.

•Az elektronikusan aláírt dokumentum **kinyomtatva elveszíti a hitelességét**, mert a papíron létező másolat az elektronikus aláírás egyetlen elemét sem tartalmazza teljes egészében, a hitelességet és változatlanságot biztosító és bizonyító kódolást pedig egyáltalán nem tartalmazza.

IT rendszerek minőségbiztosítása

- Létesítmények, elhelyezés

Fizikai elhelyezés: megfelelő környezeti körülmények (hőmérséklet, páratartalom, por), fizikai hozzáférés korlátozhatósága

Legyen mentes zavaró elektromágneses interferenciáktól (mikrohullámú sütő a gipszkarton fal túloldalán)

Elektromos áram ellátás: elegendő kapacitás, megfelelő bekötés (ezeket igazolni kell az IQ során!), szünetmentes tápellátás, hosszabb távú backup (pl. dízelgenerátor)

Megfelelő létesítmény az archivált e-adatok tárolásához: a tároláshoz használt média határozza meg a követelményeket. A hozzáférés korlátozására legyen alkalmas

IT rendszerek minőségbiztosítása

- Dokumentáció

Naprakész lista a GxP rendszerekről és a használt funkcionalitásukról.

Naprakész hálózati térkép a GxP rendszerek hálózaton belüli elhelyezkedéséről, kapcsolatairól, a rendszerek közötti kommunikáció interfészeiről.

Felhasználói policy: felhasználói szerepkörök listája rendszerenként a szerepkörökhöz rendelt jogosultságokkal; felhasználók létrehozásának, jogosultságok módosításának, felhasználók visszavonultatásának az eljárása és dokumentálása

IT rendszerek minőségbiztosítása

- Dokumentáció

Backup policy: mentések gyakorisága, kiterjedése (mit, honnan, hova, milyen gyakran), felelőssége, dokumentálása, ellenőrzése (ki végzi, milyen módszerrel, dokumentálás)

Archiválási policy: mit, mennyi ideig, milyen módon kell megőrizni. Külön figyelmet érdemel az archivált adatok migrálása (egyik adathordozó típusról a másikra, illetve a megszűnő, elavult számítógépes rendszerről a helyébe lépő újra). Az archivált adatoknak is olvashatóaknak kell lenniük a teljes megőrzési idő alatt: emiatt szükség lehet akár a teljes számítógépes rendszer archiválására is

IT rendszerek minőségbiztosítása

- Dokumentáció

Biztonsági policy: jelszavak kezelése (minimális jelszóhossz, korábbi jelszavak használata, jelszócsere gyakorisága, egyedi jelszavak, próbálkozások limitálása stb.). Kritikus rendszerek fizikai vagy logikai leválasztása a hálózat többi részéről (pl. extra tűzfallal, domain kontrollal). Vírusvédelem. Betörések (hacking) elleni védelem (felhasználók oktatása különösen fontos!). Elavult operációs rendszerek használata külön figyelmet és speciális intézkedéseket igényel.

Karbantartási policy: frissítések keresése (firmware, BIOS, operációs rendszer, driverek, szoftverek), telepítésének eljárása (change control releváns lehet!) és dokumentálása, illetve ezek felelőssége. Fizikai karbantartás, tesztelés (pl. memóriatesztek, portalanítás stb.) és ezek dokumentálása.

IT rendszerek minőségbiztosítása

- Dokumentáció

A felhasznált számítógépes rendszer legyen nyomonkövethető a releváns dokumentációkban is (gyártási dokumentáció, study report stb.)

A gyártási / study dokumentációnak legyenek kötelezően részei a számítógépesített rendszerek által nyomtatott protokollok. Vonatkozik a PLC-vel vezérelt rendszerekre is!

IT rendszerek minőségbiztosítása

Kérdés?