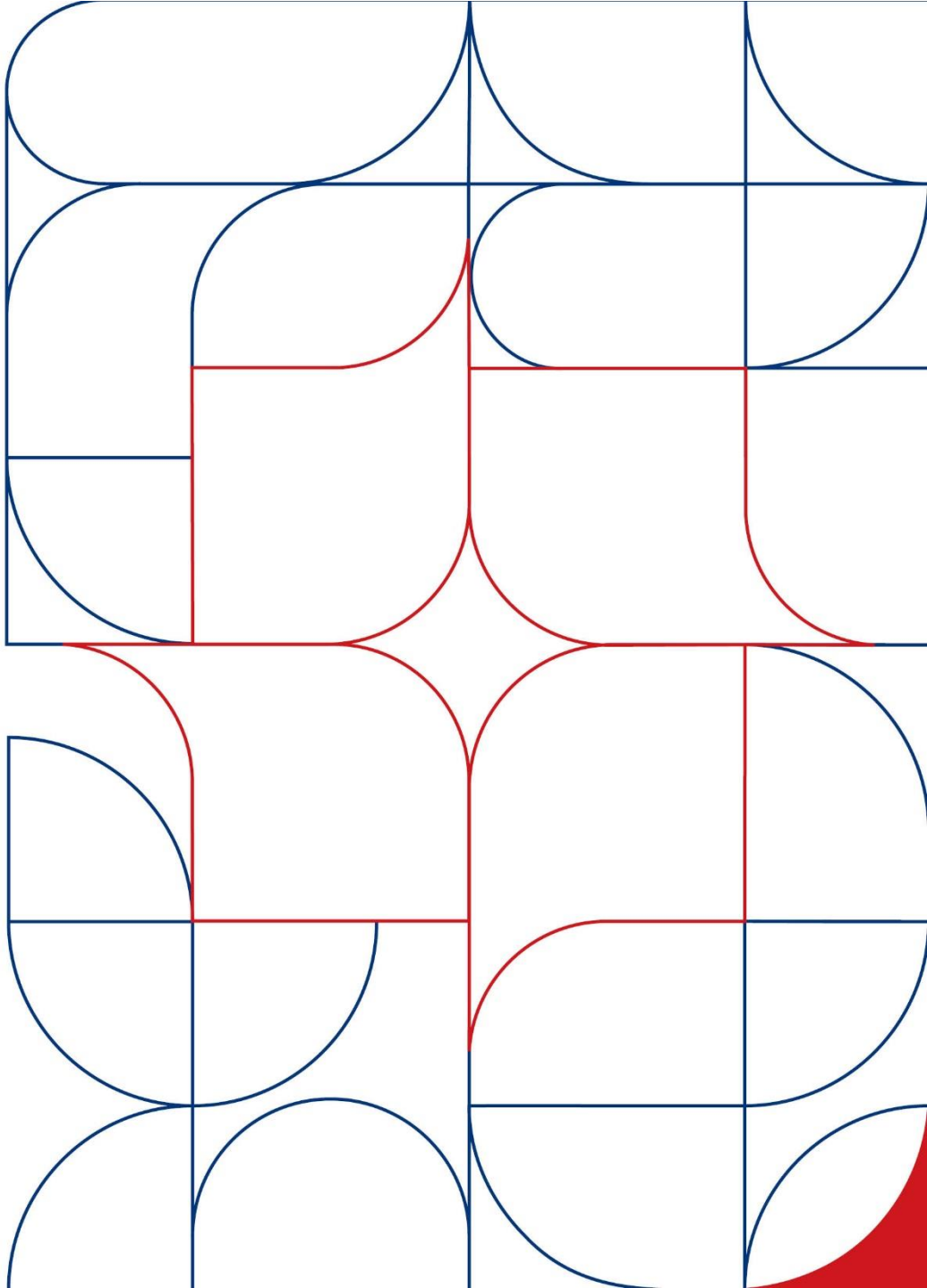
Upravljanje kompjuterizovanim sistemima u proizvodnji i kontroli kvaliteta lekova – primeri iz prakse

30.10.2025.

PRIVREDNA KOMORA SRBIJE
1857

eCommerce ECS Association of Serbia



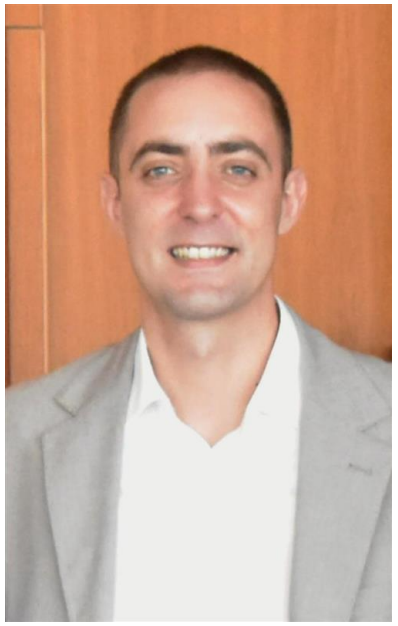
Predavači

Mirjana Ilić Ugljić

Specijalista IT procesa kvaliteta

Nevena Pavlica

Menadžer odeljenja za validaciju kompjuterizovanih sistema



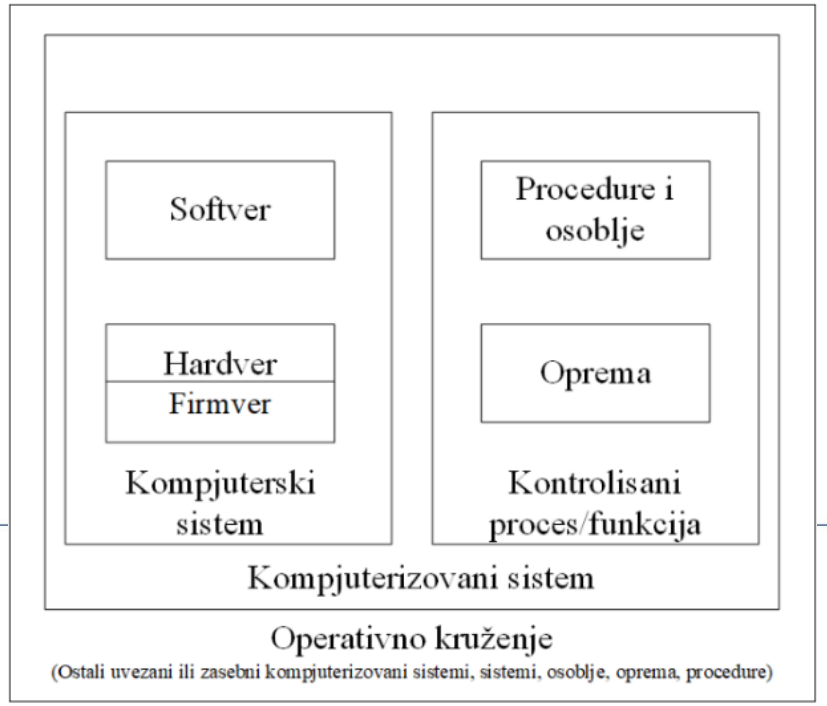
Slobodan Nedeljković

Vođa tima za IT Sistem kvaliteta

Šta su kompjuterizovani sistemi u farmaceutskoj industriji?

- Kompjuterizovani sistemi u farmaceutskoj industriji predstavljaju veliku grupu sistema, uključujući automatizovanu laboratorijsku opremu, laboratorijske informacione sisteme, informacione sisteme za upravljanje dokumentacijom, automatizovane sisteme u proizvodno-tehničkom sektoru itd.

- Kompjuterizovani sistemi(KS) sastoje se od tri međusobno povezane komponente:
  1. Kompjuterskih sistema (hardvera, softvera, mrežnih komponenti)
  2. Procesa kojim sistem upravlja (opreme, procedure, osoblje)
  3. Operativno okruženje (Ostali kompjuterizovani sistemi, osoblje, opreme i procedure)



Regulativa za kompjuterizovane sisteme u farmaceutskoj industriji

➢**GMP Annex 11**

1. Okvir za primenu (Scope)
2. Opšti principi
3. Farmaceutski sistem kvaliteta
4. Upravljanje rizikom
5. Zaposleni i obuka
6. Zahtevi sistema
7. Upravljanje dobavljačima i uslugama
8. Alarmi
9. Kvalifikacija i validacija
10. Upravljanje podacima
11. Upravljanje pristupom
12. Kontrola revizija(Audit trail)
13. Elektronski potpisi
14. Periodična provera
15. Bezbednost
16. Rezervne kopije (Backup)
17. Arhiviranje

➢**FDA 21 CFR Part 11 (SAD)**

A. Opšti zahtevi
B. Elektronski zapisi (Electronic records)
C. Elektronski potpisi

➢**GAMP 5**

Industrijski standard i skup smernica koje pomažu u implementaciji kompjuterizovanih sistema.

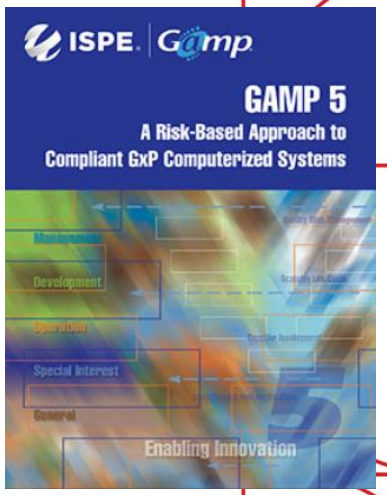
➢**Nacionalni propisi**

Agencija za lekove i medicinska sredstva Srbije (ALIMS) zahteva usklađenost sa **GMP standardima**, uključujući Annex 11.

alims
Agencija za lekove
i medicinska sredstva Srbije

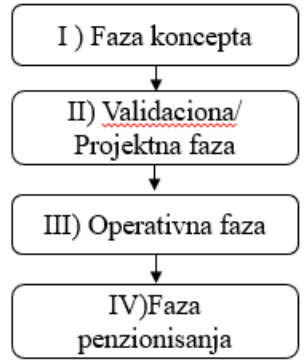
Kategorizacija kompjuterizovanih sistema

Prema ISPE GAMP® 5 (Good Automated Manufacturing Practices) vodiču Međunarodnog udruženja za farmaceutsko inženjerstvo (*International Society for Pharmaceutical Engineering)* postoje sledeće kategorije kompjuterizovanih sistema:



- **GAMP 1 - Infrastrukturni softver** - operativni sistemi, baze podataka, programski jezici, srednji sloj (middleware), statistički paketi, alati za praćenje mreže (infrastrukture) itd.;
- **GAMP 3 - Softver koji se ne može konfigurisati** - sistemi u koje se unose i skladište podaci, ali se oni ne mogu konfigurisati i prilagoditi potrebama biznisa. Primer- aplikacije zasnovane na *firmware-u*, laboratorijski instrumenti;
- **GAMP 4 - Konfigurisani softver** - često veoma složeni softveri, koji se konfigurišu kako bi ispunili specifične zahteve korisnika. Primer- LIMS, ERP (npr. SAP), MRP2, SCADA, CDS, EDMS, eQMS, itd.;
- **GAMP 5** – Custom built, softver specijalno dizajniran i programiran (kodiran) da zadovolji poslovni proces kompanije. Primer- interno i eksterno razvijene IT aplikacije, interno i eksterno razvijene aplikacije za kontrolu procesa itd.

Životni ciklus kompjuterizovanih sistema

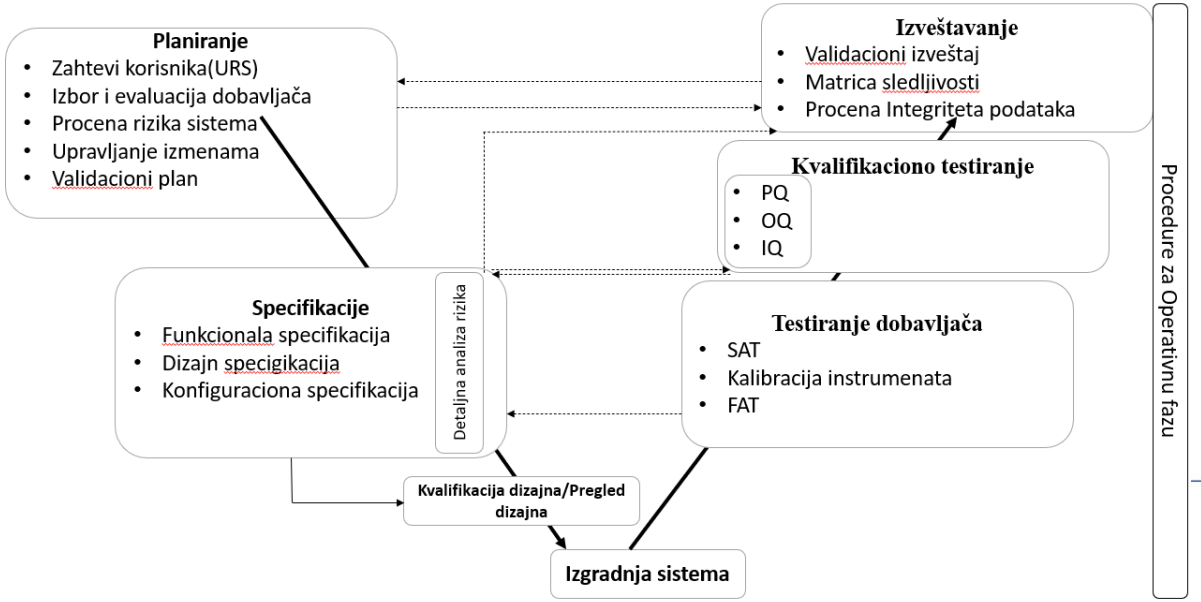


U okviru životnog ciklusa svakog kompjuterizovanog sistema (KS), razlikujemo sledeće faze:

1. **Fazu koncepta**
   - Identifikacija potrebe za uvođenjem novog KS i celina koje će učestvovati u implementaciji.

2. **Validaciona ili Projektna faza**

- Validacija kompjuterizovanih sistema (CSV - Computer system validation) je proces uspostavljanja dokumentovanih dokaza da će kompjuterizovani sistem konstantno raditi u skladu sa unapred određenim specifikacijama i atributima kvaliteta.



Životni ciklus kompjuterizovanih sistema (nastavak)

3. **Operativna faza**

- U okviru operativne faze potrebno je uspostaviti operativno upravljanje i održavanje KS kako bismo obezbedili efikasno održavanje, kontrolisanje i potencijalno unapređivanje sistema u skladu sa regulatornim zahtevima.
- Tokom čitavog životnog ciklusa, KS je neophodno održavati u validiranom stanju.

Procedure za :

- Upravljanje rizikom
- Upravljanje izmenama i konfiguracijom
- Upravljanje dokumentacijom i Obuke
- Upravljanje incidentima i CAPA
- Periodični pregled
- Kontinuitet posla (Business continuity) koji obuhvata procese Izrade I vraćanja rezervne kopije (Bekap i restor), Oporavak posle katastrofe i Rad u vanrednim uslovima
- Bezbednost i administracija sistema
- Upravljanje elektronskim zapisima
- Audit trail
- Kalibracija i održavanje

- Preporuka je da za kompjuterizovane sisteme postoji zasebna inventarska lista koja sadrži sve relevantne podatke koji omogućavaju pregled statusa KS.

4. **Faza penzionisanja**

- Završna faza je povlačenje, odnosno penzionisanje sistema. Uključuje procese kao što su arhiviranje ili migraciju podataka na regulatorno prihvatljiv način.

Opis i podela odgovornosti u životnom ciklusu kompjuterizovanih sistema

Adekvatna podela odgovornosti prilikom implementacije novog (ili održavanju postojećeg) KS je od ključne važnosti za obezbeđivanje kvalitetne i regulatorno prihvatljive implementacije i korišćenja sistema i procesa koji se na njemu sprovode.

- **Vlasnik sistema** (System owner- SO)

Osoba koja je ultimativno odgovorna za dostupnost, podršku i održavanje sistema, kao i za sigurnost podataka koji se nalaze na tom sistemu.

- **Vlasnik poslovnog procesa** (Business process owner- BPO)

Vlasnici procesa kojima sistem upravlja i odgovorni su da sistem bude validiran, efikasan, održavan, da postoje sve neophodne procedure i definisane odgovornosti.

- **Ključni korisnici** (Key User- KU)

Ključni korisnik je zaposleni ili grupa zaposlenih koji koriste sistem i pružaju podršku i obučavaju ostale zaposlene koji su krajnji korisnici sistema (end user). Preporuka je da budu uključeni u dizajn sistema. Takođe mogu učestvovati po potrebi u pisanju test scenarija i izvršavanju validacionih testiranja.

- **Obezbeđenje kvaliteta** (Quality Assurance- QA)

Koordinacija aktivnostima definisanim u kontroli izmena pokrenutoj pri implementaciji KS.
Pregled i odobravanje celokupne dokumentacije koja je propisana procedurama.
Kontrola sprovođenja aktivnosti definisam u procedurama
Vrži periodični pregled KS i izrađuje izveštaj.

- **Administrator sistema**

Odgovoran za kontrolu pristupa (User management) i generalno održavanje sistema. Obezbeđuje tehničke mogućnosti za sprovođenje aktivnosti pregleda audit trail-a, backup & restore, učestvuje u novim implementacijama / unapređenjima sistema.

Elektronski zapisi, elektronski potpis

Elektronski zapis (electronic records- ER)

- Svi zapisi koji se generišu, procesuiraju i čuvaju u elektronskom obliku, a zahtevani su regulativom (npr. GxP, CFR…), smatraju se Regulisanim elektronskim zapisima. **Identifikacija elektronskih zapisa u predmetnom kompjuterizovanom sistemu je od ključne važnosti.**

- Zapisi mogu biti održavani u elektronskoj ili u hibridnoj formi (papirna i elektronska).

Identifikovani elektronski zapisi podležu analizi rizika u kontekstu njihove kritičnosti za kvalitet proizvoda / bezbednost pacijenta na osnovu čega se propisuju zahtevi kao što su:

- Postojanje Audit traila funkcionalnosti KS;
- Postojanje backup&restore mehanizama;
- Mogućnost generisanja istovetnih kopija elektronskih zapisa u papirnoj formi i/ili elektronskoj formi;
- Adekvatna kontrola pristupa, tj mogućnost da pristupe samo autorizovane osobe;
- Arhiviranje podataka.

Elektronski potpis (electronic signature- ES)

- Predstavlja kompilaciju kompjuterskih podataka bilo kog simbola ili serije simbola usvojenih i ovlašćenih od strane pojedinca tako da predstavlja **pravno obavezujući ekvivalent svojeručnom potpisu pojedinca;**

- Svaki elektronski potpis mora biti jedinstven za pojedinca i ne sme biti korišćen od strane drugih zaposlenih što se obezbeđuje jedinstvenim korisničkim nalogom i lozinkom;

- Elektronski potpisani elektronski zapisi moraju da sadrže informacije kao što su: naziv osobe koja je potpisnik, datum i vreme potpisa, razlog potpisa (npr. odobrenje).

Kontrola revizija- Audit trail

- Audit Trail je obezbeđen, kompjuterski generisan, vremenski obeležen log, koji nezavisno beleži vreme i datum pristupanja korisnika i njihovih aktivnosti kreiranja, promene ili brisanja elektronskih zapisa.

- Audit trail mora automatski da beleži kreiranje, izmenu ili brisanje regulisanih elektronskih zapisa pri čemu fokus treba da bude na:

  - ✓ ID (identitet) korisnika;
  - ✓ Stara (ili inicijalna) vrednost;
  - ✓ Nova (ili izmenjena) vrednost;
  - ✓ Datum i vreme izmene;
  - ✓ Razlog za promenu.

- Audit trail funkcionalnost treba da obezbedi komplentnu rekonstrukciju toka događaja na posmatranom elektronskom zapisu;
- Posmatrani KS mora sadržati mehanizam ili funkciju koji onemogućava isključivanje Audit trail-a;
- Svaka izmena, manipulacija ili brisanje sadržaja Audit trail-a mora biti onemogućena.

Razlike između kvalifikacije i validacije:

Kvalifikacija je dokaz da je oprema dobro dizajnirana i instalirana, da ispravno radi i da dovodi do očekivanih rezultata, a sve u skladu sa prethodno definisanim zahtevima u URS-u.

Validacija je proces koji potvrđuje da sistem, proces ili uređaj ispunjava definisane potrebe i očekivanja korisnika u realnim uslovima rada.

Validacija je širi proces koji može uključivati sve aspekte kvaliteta proizvoda i zahteva da se tokom celog životnog ciklusa (od dizajna do penzionisanja) održi usklađenost sa regulatornim smernicama i standardima.

Primer validacije sistema u proizvodnom sektoru – Autoklav

Sistem za sterilizaciju opreme, instrumenata i materijala

Sam proces inicijalne validacije zasniva se na V modelu i ima sledeće osnovne faze:

1. Planiranje
2. Izrada specifikacija
3. Testiranje dobavljača
4. Kvalifikaciono testiranje
5. Izveštavanje
6. Održavanje

V Model

1. Planiranje

Cilj faze Planiranja je da se obezbedi da se aktivnosti validacije izvršavaju na sistematski i kontrolisan način, na osnovu unapred definisane strategije.

U okviru ove faze:

a) Pristupa se dokumentovanju zahteva korisnika (URS):
- Regulatorni zahtevi
- Funkcionalni zahtevi (Upravljanje receptima, alarmima i uređajima)
- Procesni zahtevi (kreiranja različitih ciklusa, generisanje i štampanje izveštaja, sadržaj izveštaja)

b) Vrši se izbor i procena dobavljača
c) Vrši se procena rizika sistema
d) Pravi se plan implementacije (inicira se kontrola izmena)
e) Izrađuje se validacioni plan

V Model

2. Specifikacije

SDS, HDS, FS, CS

Detaljna procena rizika

Procena rizika je fokusirana na proces kojim upravlja sistem i aspekte koji se odnose na bezbednost, integritet i sledljivost podataka.

Detaljnom procenom rizika se do detalja opisuje koji rizici mogu imati uticaj na ispravnost ili pouzdanost sistema na procesnom i funkcionalnom nivou.

V Model

3. Faza Testiranja Dobavljača

Postoje dve glavne vrste testiranja dobavljača:

a) **Prihvatanje kod dobavljača (Factory acceptance test FAT) –** vrši se provera da li su hardver, softver i konfiguracija napravljeni, sastavljeni i programirani u skladu sa onim što je definisano specifikacijama.

a) **Prihvatanje na mestu korišćenja (Site acceptance test SAT/IQ/OQ)** - predstavlja demonstraciju da sistem radi u operativnom okruženju i da nije oštećen. Obično predstavlja ponavljanje prethodno opisanog testiranja (FAT) i pruža potrebne informacije za instalacionu i operacionu kvalifikaciju.

V Model

4. Faza Kvalifikaciono Testiranje

A. **Instalaciona kvalifikacija(IQ)/Konfiguracijsko testiranje**
B. **Operaciona kvalifikacija(OQ)/Funkcionalno testiranje**
C. **Kvalifikacija performansi (PQ)**

A. **Instalaciona kvalifikacija (IQ) -** predstavlja dokumentovanu verifikaciju da je sistem instaliran i konfigurisan u skladu sa napisanom i odobrenom specifikacijom i može da sadrži sledeće provere:

- Pravilnu instalaciju hardvera i softvera
- Postavke konfiguracije (korisnički nalozi i njihove privilegije, password politike, lokacije skladištenja sirovih i bekapovanih podataka)
- Grafički prikazi ekrana

V Model

B. Operaciona kvalifikacija(OQ) - predstavlja dokumentovanu verifikaciju da sistem radi u skladu sa napisanim i odobrenim specifikacijama

Operaciona kvalifikacija (OQ) se fokusira na:
Procenu usaglašenosti u skladu sa zahtevima u okviru 21 CFR deo 11 /
EU GMP Aneks 11, kao i proveru traženih funcionalnosti sistema:

- Elektronksi zapisi/Elektronski potpisi
- Audit Trail
- Integritet podataka
- Kontrola pristupa
- Backup & Restore
- Audit trail
- Upravljanje receptima
- Upravljanje alarmima
- Štampanje izveštaja

V Model

C. **Kvalifikacija performansi (PQ) -** predstavlja završni dokaz da validirani sistem u operativnom okruženje funkcioniše na očekivan način

Kvalifikacija performansi (PQ) se fokusira na:

- Provera SOP-ova
- Test performansi (u realnim uslovima sa realnim materijalima i u skladu sa radnim uputstvom)

V Model

5. Faza Izveštavanja

A. Izveštaji nakon svake pojedinačne faze testiranja
B. Matrica sledljivosti
C. Finalni validacioni izveštaj

A. Izveštaji nakon IQ, OQ i PQ faze:

a) Sumiranje rezultata testiranja
b) Dokumentovanje zaključaka
c) Preporuka za dalju kvalifikaciju ili upotrebu sistema

Naziv testa	Rezultat	Komentar
Test broj #x – Konfiguracija softwera	Prošao	Prilikom testiranja ustanovljeno je da je sistem instaliran u skladu sa specifikacijom i kriterijum prihvatljivosti je ispunjen

V Model

5. Faza Izveštavanja

B. Matrica sledljivosti

URS ID	Naziv zahteva	Oznaka rizika	Specifikacija /Tehnička dokumentacija	Testiranje			Komentar
				IQ	OQ	PQ	
1.	Softwer konfiguracija	XXX	Referenca unutar dokumenta gde je zahtev opisan	Oznaka protokola u kom je zahtev istestiran Test lista br.X	N/A	N/A	N/A
2	Audit trail	XXX	Referenca unutar dokumenta gde je zahtev opisan	N/A	Oznaka protokola u kom je zahtev istestiran Test lista br.X	N/A	N/A
3	Startovanje ciklusa	XXX	Referenca unutar dokumenta gde je zahtev opisan	N/A	N/A	Oznaka protokola u kom je zahtev istestiran Test lista br.X	N/A

V Model

C. Finalni validacioni izveštaj

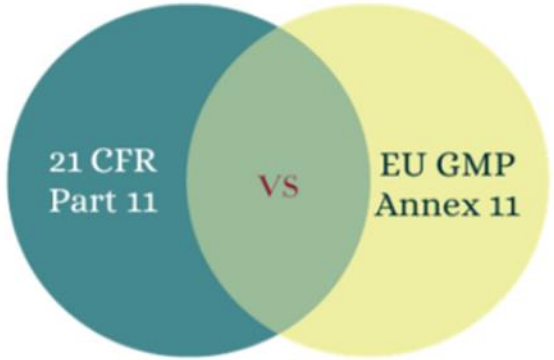
Validaciona faza	Tip dokumenta	Oznaka dokumenta	Datum primene	Datum izvršenja
Planiranje	Validacioni plan	XXXXX	XX.XX.XXXX.	N/A
Procena rizika sistema	Sistemska analiza rizika	XXXXX	XX.XX.XXXX	N/A
	Detaljna analiza rizika	XXXXX	XX.XX.XXXX	N/A
Specifikacije	SDS	XXXXX	XX.XX.XXXX	N/A
	HDS	XXXXX	XX.XX.XXXX	N/A
	CS	XXXXX	XX.XX.XXXX	N/A
Testiranje	FAT	XXXXX	XX.XX.XXXX	XX.XX.XXXX
	SAT	XXXXX	XX.XX.XXXX	XX.XX.XXXX
	IQ protokol	XXXXX	XX.XX.XXXX	XX.XX.XXXX
	OQ protokol	XXXXX	XX.XX.XXXX	XX.XX.XXXX
	PQ protokol	XXXXX	XX.XX.XXXX	XX.XX.XXXX
Izveštavanje	Izveštan nakon IQ	XXXXX	XX.XX.XXXX	N/A
	Izveštaj nakon OQ	XXXXX	XX.XX.XXXX	N/A
	Izveštaj nakon PQ	XXXXX	XX.XX.XXXX	N/A
	Matrica sledljivosti	XXXXX	XX.XX.XXXX	N/A

Značaj kompjuterizovanih sistema

➢**Integritet, Sledljivost, Dostupnost GxP podataka**

➢**Osnovni Zahtevi za GxP Sisteme:**

1. **Validiran:** Dosledno funkcioniše prema specifikacijama
2. **Kontrolisan:** Definisane odgovornosti i pristupi
3. **Praćen i Transparentan:** Audit trail, logovi, e-potpisi, backup
4. **Zaštićen:** Od neovlašćenih izmena i gubitka podataka



➢**Principi Integriteta Podataka (ALCOA+):**

1. **A**ttributable (Ko, gde i kada je odgovoran za podatak)
2. **L**egible (Čitljivo)
3. **C**ontemporaneous (Sve se beleži u realnom vremenu)
4. **O**riginal (Originalno)
5. **A**ccurate (Tačno)
6. + Complete, Consistent, Enduring, Available

➢ Fokus **<u>Inspekcije</u>** uvek na:

✓ Audit Trail

✓ Backup

✓ Restore

Značaj kompjuterizovanih sistema

➢ **Tipična pitanja auditora:**

- Koji su vaši glavni GxP sistemi odnosno spisak komputerizovanih sistema?
- Da li postoji procedura za procenu rizika i validaciju sistema?
- Kako se obezbeđuje integritet podataka u sistemima koji ne koriste papirnu dokumentaciju?

➢ **Kompanije često greše jer:**

- ne razdvajaju IT kontrolu sistema od QA kontrole podataka,
- smatraju da je „backup“ dovoljan dokaz integriteta bez audit traila,
- veruju da obična autentifikacija (korisničko ime/lozinka) ispunjava uslov e-potpisa,
- ne dokumentuju validaciju konfiguracija sistema (promene, verzije).

Propusti u usklađenosti sa regulativom = **Critical/Major** zamerka inspekcije

Audit Trail: Ciljevi i Greške

Svrha da omogući **rekonstrukciju istorije svakog podatka**

Time	Chamber	Chamber number	Idx	User	Messages
6/16/2025 10:15 AM	SDEQ0004	16	0	Ilolic	Confirming message window: WARNING (from: 2025-06-16 10:15:05)
6/16/2025 10:15 AM	SDEQ0004	16	17	Ilolic	+(46)Warn limit temp.
6/16/2025 10:14 AM	SDEQ0004	16	62	Ilolic	+Warn Ranges: Temperature ! 25.00 ! 23.00 >= 25.02 =< 24.00

➢ **Ciljevi pregleda Audit Traila su:**

- Potvrda integriteta podataka
- Identifikacija neautorizovanih aktivnosti
- Provera usklađenosti sa procedurama
- Podrška istragama
- Dokaz za inspekcije

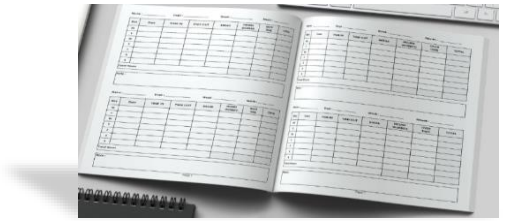
➢ **Najčešće greške u praksi su:**

- Nedostatak razloga za promene
- Audit Trail nije aktivan za sve kritične funkcije
- Neadekvatna frekvencija pregleda
- Nedokumentovani pregledi
- Nedostatak nezavisnosti u pregledu
- Brisanje ili prepisivanje logova
- Audit Trail nije validiran

➢ **Frekvencija pregleda Audit Traila se prilagođava na osnovu**:

- **Kritičnosti podataka:** Visoko kritični podaci, promenljivi od strane operatera, uvek se pregledaju po seriji
- **Korišćenja sistema**: Može se smanjiti ako sistem nije rutinski korišćen (uz procenu rizika i dokumentaciju).
- **Rezultata internih audita/periodičnih pregleda**

Papirni Audit Trail: Neophodan je kao alternativa/dopuna ako elektronski Audit Trail ne postoji ili je nepotpun (npr. ne beleži razlog promene ili staru vrednost)



Audit Trail: PRIMER

➢ **Sistemski Audit Trail:**

- **Frekvenca pregleda:** 2 puta godišnje
- **Pregled aktivnosti korisnika**: kreiranje i brisanje korisnika, upravljanje korisničkim grupama, backup, restore, brisanje projekata i slične sistemske aktivnost
- **Prilikom pregleda se evidentira**:
  - datum pregleda
  - uočena odstupanja
  - ko je izvršio pregled
  - ko je odobrio pregled

👉 *Osoba koja vrši pregled sistemskog Audit Traila treba da bude **nezavisna od procesa** koji se pregleda*

Pregled Audit Trail-a sa ostalom analitičkom dokumentacijom dostavlja se odgovornoj osobi Odeljenja za oslobađanje proizvoda.

➢ **Projektni Audit Trail:**

- **Frekvenca pregleda:** Svakodnevno, za svaku seriju analiza
- **Pregled aktivnosti korisnika:** kreiranje/izmena metoda, akvizicija podataka, obrada i čuvanje rezultata
- **Prilikom pregleda se proverava i evidentira usklađenost sa sledećim kriterijumima**:
  - Instrument metoda u skladu sa analitičkim postupkom
  - Integracioni parametri provereni u skladu sa radnim uputstvom
  - Aktivnosti korisnika u projektnom audit trail-u proverene.
  - Rezultati obrađeni i potpisani

👉 *Osoba koja vrši pregled projektnog Audit Traila je **Supervizor***

Backup GxP Sistema: Ciljevi i Frekvenca

Backup je sigurnosna kopija koja vam omogućava da vratite podatke ili sistem u prethodno, funkcionalno stanje nakon neke „katastrofe“.

➢ **Cilj backup-a da svi elektronski zapisi koji se koriste u okviru GxP aktivnosti budu:**

1. sigurno sačuvani,
2. verodostojno obnovljivi (restorable),
3. dostupni u čitljivom obliku tokom propisanog perioda čuvanja

➢ **Backup mora sadržati**:

- sirove podatke, rezultate i sve povezane metapodatke
- audit trail-ove,
- konfiguraciju sistema

kako bi se omogućila potpuna i tačna rekonstrukcija sistema.

👉 *Neuspeh u adekvatnom backup-u može dovesti do gubitka GxP podataka, što je ozbiljna neusaglašenost jer direktno utiče na sledljivost i integritet proizvodnih i laboratorijskih podataka*

➢ **Frekvenca** izrade rezervne kopije je na dnevnom nivou, svako odstupanje od ove frekvence mora biti dokumentovano procenom rizika koja uzima u obzir kritičnost sistema i podatake koje sistem obrađuje.

Backup GxP Sistema: Greške i Disaster Recovery

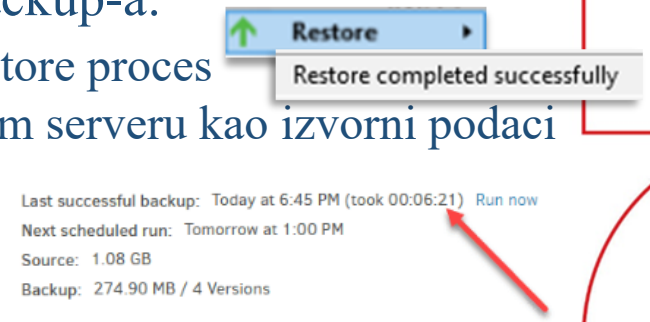
➢ Backup mora biti deo:
- User Requirements Specification (URS)
- Design Specification (DS)
- Operational Qualification (OQ)
- Periodic Review

👉 *Bez ovih dokaza*
sistem se smatra neusaglašenim

➢ Organizacija mora imati **Disaster Recovery Plan** (plan oporavka), koji definiše:
- Potencijalne scenarije (otkaz hardware, otkaz software itd.)
- korake za oporavak sistema,
- prioritete (koji sistemi moraju biti vraćeni prvi)
- odgovorna lica,
- maksimalno prihvatljivo vreme oporavka (RTO – Recovery Time Objective),
- maksimalni gubitak podataka koji je prihvatljiv (RPO – Recovery Point Objective).

👉 *Bez testiranog DR plana, backup nema regulatornu vrednost, jer se ne zna da li je funkcionalan u realnoj situaciji.*

➢ Najčešće **greške** u vezi backup-a:
- Nikada nije testiran restore proces
- Backup se čuva na istom serveru kao izvorni podaci
- Ne postoji procedura
- Nema evidencije
- Backup nije potpun



Hvala na pažnji!

Pitanja?

PRIVREDNA
KOMORA
SRBIJE

1857

www.pks.rs