Validace počítačového systému ve farmaceutické společnosti

(příklady z laboratorní praxe)

Vladislav Roháč

TEVA Czech Industries s.r.o.

Obsah

- Validace laboratorního počítačového systému
- Implementace Part 11 a data integrity požadavků
- Řádný provoz počítačového systému
- Kontrola audit trailu
- Periodické hodnocení

Obecně

Předpisy pro řízení počítačových systémů a integritu dat

EU

- EudraLex: Volume 4 Good Manufacturing Practice, Annex 11: Computerized Systems (2011)
- EMA: Questions and Answers: Good Manufacturing Practice – Data Integrity (2016)

FDA

- FDA 21 CFR Part 11: Electronic Records, Electronic Signatures, Final Rule (1997)
- Guidance for Industry: Part 11, Electronic Records; Electronic Signatures — Scope and Application (2003)
- Guidance for Industry: Data Integrity and Compliance with cGMP (2018)

Obecně

Doporučení pro řízení počítačových systémů a integritu dat

Počítačové systémy:

- **GAMP5** - A Risk-Based Approach to Compliant GxP Computerized Systems – Second Edition (2022)
- **GAMP** - Good Practice Guides

Data Integrity:

- **WHO** – Technical Report 996 - Annex 5: Guidance on Good Data and Record Management Practices (2016)
- **ISPE** – Good Practice Guide - Records and Data Integrity (2017)
- **ISPE** – Good Practice Guide – Data Integrity - Key Concepts (2018)
- **ISPE** – Good Practice Guide – Data Integrity – Manufacturing Records (2019)
- **PDA** – Technical Report No. 80 – Data Integrity Management System for Pharmaceutical Laboratories (2018)
- **PDA** – Technical Report No. 84 – Integrating Data Integrity Requirements into Manufacturing&Packaging Operations (2020)
- **PIC/S** - Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments (2021)

TCI lokální předpisová dokumentace

Lokální předpisová dokumentace pro počítačové systémy a integritu dat

- **SOP\QA** Životní cyklus počítačových systémů
- **SOP\QA** Integrita dat

- **SOP\QA** Řízení změn počítačových systémů
- **SOP\QA** Analýza rizik počítačových systémů
- **SOP\QA** Audity dodavatelů počítačových systémů
- **SOP\QA** Periodické hodnocení počítačových systémů
- **SOP\QA** Elektronické záznamy a elektronické podpisy
- **SOP\QA** BCP pro počítačové systémy

Zodpovědnosti

Pro každý systém musí být definovány minimálně tři zodpovědné osoby

Vlastník systému (BO)

- Validační status systému
- Uživatelský manuál a proškolení
- Řízení změn

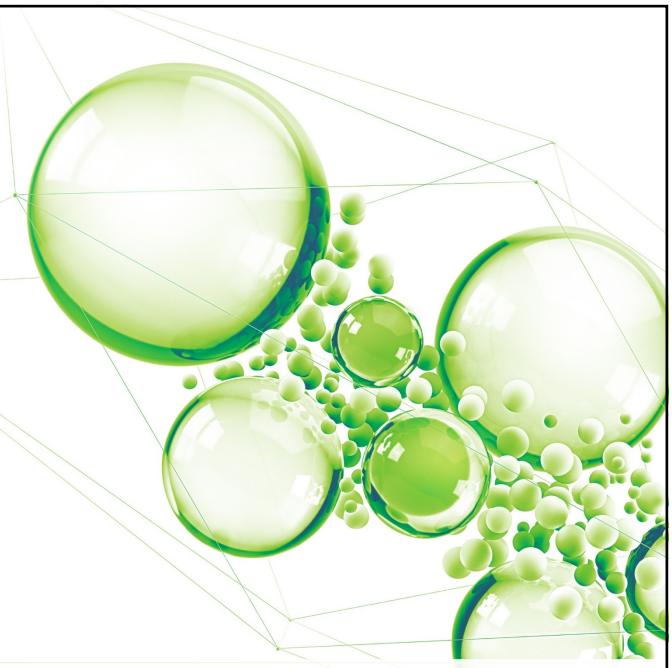
Technický vlastník (TO)

- Provedení validačních a technických aktivit
- Zálohování
- DRP plány
- Nastavení systému a řízení přístupu

QA

- Inventář systémů
- Evidence ve VMP IT
- Schválení a shoda s GMP požadavky

Validace laboratorního počítačového systému (příklad z praxe)



Realizace

- **Modelový příklad** – Výměna analyzátoru TOC v mikrobiologické laboratoři (ZŘ)
- Schválený implementační plán vlastníkem systému, technickým vlastníkem a QA:

Před implementací
1. Vydání URS pro TOC

Po implementaci:
1. Zakoupení zařízení dle požadavků URS
2. Zakoupení počítačové sestavy dle firemních požadavků
3. Instalace a kvalifikace zařízení - dle SOP - Kvalifikace a údržba laboratorních přístrojů a zařízení
4. Instalace a validace SW dle SOP - Životní cyklus počítačových systémů.

Technický správce:
- CDS
- validační plán
- bude požit schválení generický testovací protokol IQ, OQ
(protokol IQ/OQ nebude vydán)
- Provedení IQ, OQ
- Vydata validační souhrnnou zprávu VSR

Vlastník systému:
- LAS-51 - vydání protokolu PQ a provedení PQ

5. Vytvoření návodu na obsluhu pro nový TOC analyzátor
6. Archivace SOP - Přístroj pro měření obsahu TOC - Sievers 900 (bude nahrazen novým NO pro zařízení M9)-
7. Založení karty přístroje v LIMS
8. Aktualizace TWH databáze
9. zrušení úkolu na aktualizaci DS , dokument je pravidelně aktualizován v souladu s SOP

- po zprovoznění nového zařízení:
1. Kvalifikace zařízení TOC_2 před plánovaným vyřazením
2. Vyřazení zařízení TOC_2 z provozu a z LIMS
3. Vyřazení systému DapaPro dle SOP - Životní cyklus počítačových systémů.

Uživatelská specifikace (URS)

Všechny požadavky na počítačový systém musí být popsány v uživatelské specifikaci

- Uživatelské požadavky **by neměly být obecné**, ale „na míru“ daného procesu, případně software
- **Měly by pokrýt očekávaný způsob použití** počítačového systému

Doporučením je dát schválenou uživatelskou specifikaci jako **přílohu obchodní smlouvy**.

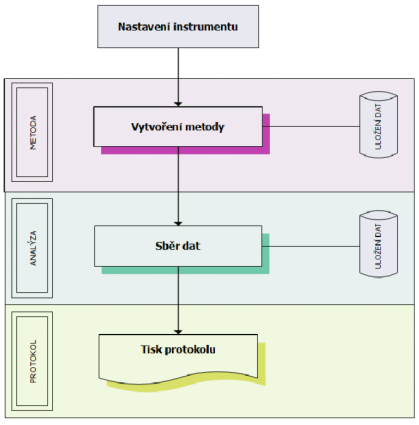
Požadavky na integritu dat se ve velké míře kryjí s požadavky 21 CFR Part 11 – základní požadavek je mít data pod kontrolou po celou dobu životního cyklu dat.

Mělo by být **jasně deklarováno**, jestli systém obsahuje **elektronické záznamy** a **elektronické podpisy** dle 21 CFR Part 11

- **Elektronické záznamy** (podpisy) by měly být v URS **jmenovitě identifikovány**
- Definice: **Elektronický záznam je definován jako regulovaný, pokud** je jeho udržování, nebo předkládání požadováno předpisy SVP, nebo pokud se z něho vychází **při vykonávání činnosti**, kterou předpisy SVP vyžadují.

Uživatelská specifikace (URS)

Popis procesu:



Identifikace elektronických záznamů:

1. Metoda

2. Primární záznamy

3. Výsledky

Příklady URS požadavků

Všeobecné a IT požadavky

Kód požadavku	Popis požadavku	Typ požadavku
URS-ITFR.001	Příručka k systému musí být dostupná správcům v tištěné nebo v elektronické verzi (jazyk musí být angličtina nebo čeština).	Povinný
URS-ITFR.002	Administrátor musí mít přístup k instalačnímu médiu a k licenčním klíčům.	Povinný
URS-ITFR.003	Operační systém na stanici musí být: Windows	Povinný
URS-ITFR.004	Operační systém na stanici musí podporovat jazyk angličtinu nebo češtinu.	Povinný
URS-ITFR.005	Operační systém na serveru musí být:	N/A
URS-ITFR.006	Operační systém na serveru musí podporovat jazyk angličtinu nebo češtinu.	N/A
URS-ITFR.007	Stanice musí být členem domény TEVA.	Povinný
URS-ITFR.008	Systém musí být schopen správně fungovat s nainstalovaným antivirovým programem dle standardu TEVA.	Povinný

Příklady URS požadavků

Procesní požadavky uživatele

Kód požadavku	Popis požadavku	Typ požadavku
URS-PFR.001	Systém umožňuje nastavit připojení instrumentu a monitorování statusu.	Povinný
URS-PFR.006	Systém umožňuje provádět operace v následujícím pořadí (viz URS-ER.07): 1. Volba instrumentové metody a protokolu (šablony pro sekvenci) 2. Analýzy vzorku 3. Tisk reportu	Povinný
URS-PFR.007	Systém umožňuje nastavit parametry instrumentové metody: ▪ Nastavení dávkování Acid ▪ Nastavení dávkování Oxid ▪ Počet opakování měření vzorku ▪ Počet vyloučeným měření Systém neumožní zadat neplatné znaky (viz URS-ER.01)	Povinný
URS-PFR.012	Systém umožňuje identifikovat vzorek a zadat jeho parametry: • ID vzorku • Název vzorku Systém neumožní spustit měření bez identifikace vzorku (viz URS-ER.01)	Povinný

URS požadavky na Part11 a data integrity

Požadavky na elektronické záznamy (ER)

ID	Popis
URS-ER.01	Systém odmítá uložit neplatné položky dat (min. hodnoty znaků v číselných polích a hodnoty mimo rozsah).
URS-ER.02	Systém musí být schopen vytvářet vizuální zobrazení elektronických záznamů a souvisejících metadat.
URS-ER.03	Systém musí být schopen vytvářet elektronické kopie záznamů a souvisejících metadat do souborů.
URS-ER.04	Systém musí být schopen tisknout kopie elektronických záznamů a souvisejících metadat.
URS-ER.05	Kopie elektronických záznamů vytvořené prostřednictvím systému musí obsahovat jednoznačný odkaz na příslušný elektronický záznam.
URS-ER.06	Systém musí získat datum a čas použitý pro časové razítko pouze z autorizovaného zdroje, který uživatel neumí změnit. Systémové datum a čas musí být synchronizovány s časovým serverem.
URS-ER.07	Systém musí podporovat sekvencování operací nebo událostí, aby bylo zajištěno, že kroky jsou prováděny ve správném pořadí.

URS požadavky na Part11 a data integrity

Požadavky na zabezpečení (SE)

ID	Popis
URS-SE.01	Systém musí omezit logický přístup do systému.
URS-SE.02	Systém musí poskytovat více úrovní uživatelských přístupů a přiřazovat uživatelská práva dle přiřazené úrovně.
URS-SE.03	Systém musí vyžadovat, aby dva uživatelé neměli stejný uživatelský přístupový účet.
URS-SE.04	Systém musí skrýt heslo. Systém musí zajistit, aby heslo nebylo nikdy uloženo nebo zobrazeno v lidsky čitelném formátu.
URS-SE.05	Systém musí vynutit změnu hesla po definované době (max. 180 dnů).
URS-SE.06	Systém musí mít schopnost vynutit minimální délku hesla (min. 8 znaků).

FDA 21 CFR Part 11

URS požadavky na Part11 a data integrity

Požadavky na zabezpečení (SE)

ID	Popis
URS-SE.07	Systém musí mít konfigurační funkci, která ukončí relaci po 15 minutách nečinnosti. (např. automatické uzamčení obrazovky nebo automatické odhlášení). Tato funkce nesmí být konfigurovatelná uživatelem.
URS-SE.08	Systém bude vyžadovat, aby uživatel změnil heslo ihned po přihlášení po obnovení hesla správcem systému.
URS-SE.09	Systém musí mít zaznamenávat neautorizované pokusy (např. deaktivace uživatele je součástí audit trail záznamu).
URS-SE.10	Systém musí omezit počet neúspěšných pokusů o přihlášení (max. 5 pokusů)
URS-SE.11	Systém musí mít možnost deaktivovat uživatelské účty.
URS-SE.12	USB porty musí být zabezpečeny proti neoprávněnému použití.

URS požadavky na Part11 a data integrity

Požadavky na audit trail (AT)

ID	Popis
URS-AT.01	Audit trail musí zaznamenávat všechny události, které vytvářejí, upravují nebo odstraňují elektronické záznamy.
URS-AT.02	Systém musí být schopen vytvářet vizuální zobrazení audit trailu elektronických záznamů a spojených metadat. Pokud audit trail dokumentuje změnu dat, pak systém musí zobrazit jasné a přesné změny.
URS-AT.03	Audit trail musí zaznamenávat změny úrovní přístupu uživatele, jejich oprávnění a nastavení zabezpečení (min. délka hesla, exspirace hesla, zablokování a neoprávněné přihlášení uživatele).
URS-AT.04	Všechny záznamy audit trailu musí být generovány automaticky s datem, časem, časovým pásmem (je-li to požadováno) a jménem operátora, který transakci provádí.
URS-AT.05	Systém musí poskytnout možnost zaznamenat "důvod pro změnu" jako součást audit trailu pro změnu kritických dat v systému.

URS požadavky na Part11 a data integrity

Požadavky na audit trail (AT)

ID	Popis
URS-AT.06	Systém musí být schopen vytvářet elektronické kopie audit trailu.
URS-AT.07	Systém musí být schopen vytvářet výtisky audit trailu.
URS-AT.08	Audit trail musí být dostupný pro kontrolu oprávněným uživatelem.
URS-AT.09	Uživatel nesmí být schopen zakázat generování audit trailu.
URS-AT.10	Uživatel nesmí být schopen změnit nebo smazat audit trail.
URS-AT.11	Audit trail musí mít funkce pro vyhledávaní/filtrování/export do CSV formátu.

FDA
21 CFR Part 11

URS požadavky na Part11 a data integrity

Požadavky na integritu dat (DI)

ID	Popis
URS-DI.01	Systém musí automaticky ukládat všechna data do předem definovaného uložiště.
URS-DI.02	Uživatelé nesmí mít možnost měnit umístění vytvořených elektronických záznamů a nesmí mít možnost kopírovat elektronické záznamy do nepovolených umístění. (požadavek platí pro souborový systém).
URS-DI.03	Systém musí zobrazovat datum a čas v jednotném formátu v zobrazení systému a v reportech (výtiscích a elektronickém výstupu).
URS-DI.04	Systém musí chránit data před vymazáním, poškozením a falšováním uživatelem.
URS-DI.05	Použití generického uživatele v aplikaci není povoleno, všechny účty musí být jedinečné a vytvořeny na jméno uživatele.
URS-DI.06	Systém musí zajistit, že pouze role administrátora systému může přidávat, odstraňovat nebo upravovat uživatele a měnit konfiguraci zabezpečení.
URS-DI.07	Systém musí podporovat aktivaci receptury/metody. Receptury/metody nemůže aktivovat stejná osoba, která je vytvořila.

URS požadavky na Part11 a data integrity

Požadavky na zálohování (BU) a archivaci (AR) dat

ID	Popis
URS-AR	**Archivace**
URS-AR.01	Systém musí být schopen archivovat záznamy na alternativní médium pro dlouhodobé uložení (je-li požadováno).
URS-AR.02	Systém musí být schopen načíst archivované záznamy zpět do systému (je-li požadováno).
URS-BU	**Zálohování & Obnova**
URS-BU.01	Systém musí být schopen zálohovat aplikační software a automaticky zálohovat elektronické záznamy a konfiguraci systému na alternativní média.
URS-BU.02	Musí být možné obnovit systém a zálohu dat obnovit zpět do systému.

Součástí URS **nejsou** požadavky na elektronický podpis.

EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

teva

Validační plán (VP) – Dokumentace a definování odpovědností

– Účelem *Validačního plánu* je podrobně definovat rozsah aktivit potřebných pro vykonání validace nové verze počítačového systému pro TOC, který má dle inventáře počítačových systémů kód

Položka	Vyžadováno	Autor	Schvalovatel	Komentář
Počáteční hodnocení systému	☒ Ano ☐ N/A	TO, BO, QA	TO, BO, QA	Součástí tohoto dokumentu
Uživatelská specifikace systému (URS)	☒ Ano ☐ N/A	BO	TO, QA	
Analýza funkčních rizik (FRA)	☒ Ano ☐ N/A	TO, BO, QA	TO, BO, QA	Součástí tohoto dokumentu
Validační plán (VP)	☒ Ano ☐ N/A	TO	BO, QA	Tento dokument
Specifikace konfigurace (CS / CDS)	☒ Ano ☐ N/A	TO	BO, QA	
Instalační kvalifikace (IQ) – Protokol	☒ Ano ☐ N/A	TO	BO, QA	Dle VIP
Instalační kvalifikace (IQ) – Report	☒ Ano ☐ N/A	TO	TO, BO, QA	Dle VIP
Operační kvalifikace (OQ) – Protokol	☒ Ano ☐ N/A	TO	BO, QA	Dle VIP
Operační kvalifikace (OQ) – Report	☒ Ano ☐ N/A	TO	TO, BO, QA	Dle VIP
Procesní kvalifikace (PQ) – Protokol	☒ Ano ☐ N/A	BO (TO)	TO, QA	
Procesní kvalifikace (PQ) – Report	☒ Ano ☐ N/A	BO (TO)	TO, QA	Součástí PQ protokolu
Matice dohledatelnosti (TM)	☒ Ano ☐ N/A	TO	BO, QA	Součástí VSR a VIP
Go-Live „Readiness"	☒ Ano ☐ N/A	TO	BO, QA	Součástí VSR
Souhrnná validační zpráva (VSR)	☒ Ano ☐ N/A	TO	BO, QA	

teva

Počáteční hodnocení počítačového systému

4.1 Hodnocení dopadu systému na GxP

Hodnocení dopadu na GxP	☒ Systém má dopad na GxP ☐ Systém nemá dopad na GxP

4.2 Hodnocení rizika systému

Komplexnost (kategorie) systému	☐ Nízká (C1) - Software infrastruktury ☒ Nízká (C3) - Nekonfigurované softwarové produkty ☐ Střední (C4) - Konfigurované softwarové produkty ☐ Vysoká (C5) - Softwarové aplikace na zakázku
Úroveň rizika	☒ Velká - Systémy s přímým dopadem, které vykonávají nebo řídí procesy, které mají potenciální dopad na produkt (bezpečnost, identitu, sílu, kvalitu nebo čistotu), integritu dat a/nebo na kritické obchodní cíle, pro které jsou funkce systému nutné pro provoz a obchodní proces. Selhání systému může mít za následek produkt mimo specifikaci. Selhání systému nebude detekováno nezávislou verifikační metodou.
Celkový index rizika (RAI)	☐ Velký ☒ Střední ☐ Malý

5.2 Hodnocení elektronických záznamů

Hodnocení elektronických záznamů	ER1: Instrumentové metody ER2: Protokoly (šablony sekvencí) ER3: Výsledky	☒ G1 ☐ G2 ☐ G3 ☒ G1 ☐ G2 ☐ G3 ☐ G1 ☒ G2 ☐ G3

- G1, G2 – je požadována validace podle 21 CFR Part 11

Funkční analýza rizik (FRA)*

Kód požadavku	Popis požadavku	Hrozba	Příčina	Následek	Závažnost	Pravděpodobnost	Detekovatelnost	Priorita rizika	Opatření
URS-PFR.001	Systém umožňuje nastavit připojení instrumentu a monitorování statusu.	Není možné připojit instrument nebo monitorovat jeho status	Špatná konfigurace/ funkčnost systému	Není možno provést požadované analýzy	H	L	M	M	PQ dokumentované testování
URS-PFR.016	Měření musí probíhat na pozadí i po uzamčení stanice.	Při uzamčení dojde k přerušení analýzy	Špatná konfigurace/ funkčnost systému	Analýzy nejsou provedeny	M	M	H	L	PQ testování
URS-PFR.017	Systém umožňuje automatické uložení naměřených dat.	Naměřená data nejsou automaticky uložena.	Špatná konfigurace/ funkčnost systému	Porušení data integrity dat; není pod kontrolou provedené měření	H	M	M	H	PQ dokumentované rozšířené testování

- Metodika FMEA dle GAMP 5.

Specifikace konfigurace (CDS)

- Účelem tohoto dokumentu je poskytnout podrobný popis konfigurace hardware, software, zabezpečení a uživatelských oprávnění systému TOC

- Obsah dokumentu:

PC STANICE	
Název stanice	
Sériové číslo	
Umístění	
CPU	
RAM	
Pevný disk	
Operační systém	
Aplikační software	
Verze software	
Antivirus	
Další software	

NASTAVENÍ PARAMETRŮ	
Vynucení změny hesla	180 dnů
Minimální délka hesla	8 znaků
Max. počet chybných zadání hesla	5
Doba do uzamčení stanice	15 min

PC STANICE – DATA	
Složka na lokálním disku	
Název databáze	

INSTRUMENT	
Název instrumentu	
Kód instrumentu	
Sériové číslo	
Umístění	
Verze firmware	

SERVER – BACKUP	
Název serveru	
Složka na serveru	

Obecný protokol pro ověření ER/ES/DI požadavků

3.1 Přehled plánovaných testů IQ

Přehled testů instalační kvalifikace je uveden v následující tabulce. Testy, které je plánováno provést v rámci kvalifikace, jsou označeny **„Ano"**.

ID testu	Plánované testy instalační kvalifikace	
IQT.01	Ověření předpokladů pro testování	☐ Ano ☐ N/A
IQT.02.01	Ověření HW a SW - Server	☐ Ano ☐ N/A
IQT.02.02	Ověření HW a SW - Stanice/klient	☐ Ano ☐ N/A
IQT.02.03	Ověření HW a SW - PLC	☐ Ano ☐ N/A
IQT.02.04	Ověření HW a SW - HMI	☐ Ano ☐ N/A
IQT.03	Ověření zařízení	☐ Ano ☐ N/A
IQT.04	Ověření konfigurace ukládání dat	☐ Ano ☐ N/A
IQT.05	Ověření konfigurace zálohování / archivace dat	☐ Ano ☐ N/A
IQT.06	Ověření konfigurace zabezpečení systému a Audit Trail	☐ Ano ☐ N/A
IQT.07	Ověření konfigurace uživatelských rolí a oprávnění	☐ Ano ☐ N/A
IQT.08	Ověření dokumentace a příruček	☐ Ano ☐ N/A

Příloha č. 1: Matice dohledatelnosti

ID požadavku	Popis požadavku	ID testu IQ	ID testu OQ
URS-DI.03	Systém musí zobrazovat datum, čas a časovou zónu v jednotném formátu v zobrazení systému, výtiscích a elektronickém výstupu.	-	OQT.02
URS-DI.04	Systém musí chránit data před vymazáním, poškozením a falšováním uživatelem.	IQT.04	OQT.07 OQT.10
URS-DI.05	Použití generického uživatele v aplikaci není povoleno, všechny účty musí být jedinečné a vytvořeny na jméno uživatele.	-	OQT.09
URS-DI.06	Systém musí zajistit, že pouze role administrátora systému může přidávat, odstraňovat nebo upravovat uživatele a měnit konfiguraci zabezpečení.	IQT.07	OQT.08 OQT.09
URS-DI.07	Systém musí podporovat aktivaci metody/receptury. Metoda/receptura nesmí být aktivována stejným uživatelem, který ji vytvořil.	-	OQT.15

3.2 Přehled plánovaných testů OQ

Přehled testů operační kvalifikace je uveden v následující tabulce. Testy, které je plánováno provést v rámci kvalifikace, jsou označeny **„Ano"**.

ID testu	Plánované testy operační kvalifikace	
OQT.01	Ověření předpisové dokumentace	☐ Ano ☐ N/A
OQT.02	Ověření data a času	☐ Ano ☐ N/A
OQT.03	Ověření ukládání dat	☐ Ano ☐ N/A
OQT.04	Ověření neplatných záznamů	☐ Ano ☐ N/A
OQT.05	Ověření posloupnost operací	☐ Ano ☐ N/A
OQT.06	Ověření tisku a elektronické kopie	☐ Ano ☐ N/A
OQT.07	Ověření zabezpečení dat a databáze	☐ Ano ☐ N/A
OQT.08	Ověření uživatelských profilů	☐ Ano ☐ N/A
OQT.09	Ověření přístupu	☐ Ano ☐ N/A
OQT.10	Ověření Audit Trail	☐ Ano ☐ N/A
OQT.11	Ověření zálohy a obnovy	☐ Ano ☐ N/A
OQT.12	Ověření archivace	☐ Ano ☐ N/A
OQT.13	Ověření DRP	☐ Ano ☐ N/A
OQT.14	Ověření elektronického podpisu	☐ Ano ☐ N/A
OQT.15	Ověření aktivace metody/receptury	☐ Ano ☐ N/A

Kvalifikace (IQ/OQ/PQ) – vzor test skriptu

Kód testu	OQT.02
Název testu	Ověření data a času
Popis testu	Ověření nastavení a zabezpečení data a času.
Reference na URS	URS-SE.07, URS-ER.06, URS-DI.03
Prerekvizity testu	**Role** s ne-administrátorským oprávněním:_____ **Uživatel**:_____

ID	Popis kroku testu	Kritérium přijatelnosti	Výsledek	ID Přílohy	Komentář
1	**Ověřte datum, čas a časovou zónu.**	Datum, čas a časová zóna je korektně zobrazena a hodnota odpovídá referenčnímu zdroji.	☐ Vyhovuje ☐ Nevyhovuje ☐ N/A	Att.: N/A	
2	**Pokuste se změnit datum, čas a časovou zónu v aplikačním SW.** **Přiložte evidenci.**	Uživatel nemůže změnit datum, čas a časovou zónu v aplikaci. Evidence je přiložena.	☐ Vyhovuje ☐ Nevyhovuje ☐ N/A	Att.: _____	
Tester			**Datum a podpis**		

Kvalifikace (IQ/OQ/PQ) – vzor test skriptu

Kód testu	OQT.02
Název testu	Ověření data a času
Popis testu	Ověření nastavení a zabezpečení data a času.
Reference na URS	URS-SE.07, URS-ER.06, URS-DI.03
Prerekvizity testu	**Role** s ne-administrátorským oprávněním:_____

ID	Popis kroku testu	Kritérium přijatelnosti	Výsledek	ID Př
1	**Ověřte datum, čas a časovou zónu.**	Datum, čas a časová zóna je korektně zobrazena a hodnota odpovídá referenčnímu zdroji.	☐ Vyhovuje ☐ Nevyhovuje ☐ N/A	Att.: N
2	**Pokuste se změnit datum, čas a časovou zónu v aplikačním SW.** **Přiložte evidenci.**	Uživatel nemůže změnit datum, čas a časovou zónu v aplikaci. Evidence je přiložena.	☐ Vyhovuje ☐ Nevyhovuje ☐ N/A	Att.: _
Tester			**Datum a podpis**	

VÝSLEDKY TESTU			
Poznámky:			
Běh #	**Výsledek testu**	**Odchylka**	
_____	Vyhovuje / Nevyhovuje	Ne / Ano	ID Odchylky:_____
	Jméno	**Datum**	**Podpis**
Tester			
Ověřil			
Schválil (QA)			

Kvalifikace (IQ/OQ/PQ)

Kód testu	Název testu	Výsledek	Kód odchylky
IQT.01	Ověření předpokladů pro testování	Vyhovuje	N/A
IQT.02.02	Ověření HW a SW - Stanice/klient	Nevyhovuje	DEV01
IQT.03	Ověření zařízení	Vyhovuje	N/A
IQT.04	Ověření konfigurace ukládání dat	Vyhovuje	N/A
IQT.05	Ověření konfigurace zálohování / archivace dat	Vyhovuje	N/A
IQT.06	Ověření konfigurace zabezpečení systému a Audit Trail	Vyhovuje	N/A
IQT.07	Ověření konfigurace uživatelských rolí a oprávnění	Vyhovuje	N/A
IQT.08	Ověření dokumentace a příruček	Vyhovuje	N/A

- Postupně provedení testů IQ, OQ, PQ podle schválených validačních protokolu.
- Zaznamenání všech výsledků a odchylek.

Kvalifikace (IQ/OQ/PQ)

Kód testu	Název testu	Výsledek	Kód odchylky
IQT.01	Ověření předpokladů pro testování	Vyhovuje	N/A
IQT.02.02	Ověření HW a SW - Stanice/klient	Nevyhovuje	DEV01
IQT.03	Ověření zařízení	Vyhovuje	N/A
IQT.04	Ověření konfigurace ukládání dat	Vyhovuje	N/A
IQT.05	Ověření konfigurace zálohování / archivace dat	Vyhovuje	N/A
IQT.06	Ověření konfigurace zabezpečení systému a Audit		
IQT.07			
IQT.08			

Kód testu	Název testu	Výsledek	Kód odchylky
OQT.01	Ověření předpisové dokumentace	Vyhovuje	N/A
OQT.02	Ověření data a času	Vyhovuje	N/A
OQT.03	Ověření ukládání dat	Vyhovuje	N/A
OQT.04	Ověření neplatných záznamů	Nevyhovuje	DEV02
OQT.05	Ověření posloupnost operací	Vyhovuje	N/A
OQT.06	Ověření tisku a elektronické kopie	Vyhovuje	N/A
OQT.07	Ověření zabezpečení dat a databáze	Vyhovuje	N/A
OQT.08	Ověření uživatelských profilů	Vyhovuje	N/A
OQT.09	Ověření přístupu	Nevyhovuje	DEV03,DEV04
OQT.10	Ověření Audit Trail	Nevyhovuje	DEV05
OQT.11	Ověření zálohy a obnovy	Vyhovuje	N/A
OQT.15	Ověření aktivace metody/receptury	Vyhovuje	N/A

- Postupně provedení testů IQ, OQ, PQ podle schválených validačních protokolu.
- Zaznamenání všech výsledků a odchylek.

Kvalifikace (IQ/OQ/PQ)

Kód testu	Název testu	Výsledek	Kód odchylky
IQT.01	Ověření předpokladů pro testování	Vyhovuje	N/A
IQT.02.02	Ověření HW a SW - Stanice/klient	Nevyhovuje	DEV01
IQT.03	Ověření zařízení	Vyhovuje	N/A
IQT.04	Ověření konfigurace ukládání dat	Vyhovuje	N/A
IQT.05	Ověření konfigurace zálohování / archivace dat	Vyhovuje	N/A
IQT.06	Ověření konfigurace zabezpečení systému a Audit		
IQT.07	(		
IQT.08	(		

Kód testu	Název testu	Výsledek	Kód odchylky
OQT.01	Ověření předpisové dokumentace	Vyhovuje	N/A
OQT.02	Ověření data a času	Vyhovuje	N/A
OQT.03	Ověření ukládání dat	Vyhovuje	N/A
OQT.04	Ověření neplatných záznamů	Nevyhovuje	DEV02
OQT.05	Ověření posloupnost operací	Vyhovuje	N/A
OQT.06	Ověření tisku a elektronické kopie	Vyhovuje	N/A
OQT.07	Ověření zabezpečení dat a databáze	Vyhovuje	N/A
OQT.08	Ověření uživatelských profilů	Vyhovuje	N/A
OQT.09	Ověření přístupu	Nevyhovuje	DEV03,DEV04
OQT.10	Ověření Audit Trail	Nevyhovuje	DEV05
OQT.11	Ověř		
OQT.15	Ověř		

Kód testu	Název testu	Výsledek	Kód odchylky
PQT.01	Dostupnost zavedených procedurálních kontrol	Vyhovuje	N/A
PQT.02	Existence produkčního prostředí.	Vyhovuje	N/A
PQT.03	Ověření procesu	Nevyhovuje	DEV06
PQT.04	Ověření instrumentu a analýzy.	Vyhovuje	N/A

- Postupně provedení testů IQ, OQ, PQ podle schválených validačních protokolu.
- Zaznamenání všech výsledků a odchylek.

Kvalifikace (IQ/OQ/PQ) - odchylky

Popis všech odchylek a jejich vyřešení do souhrnné validační zprávy (VSR).

Fáze	Kód odchylky	Popis	Nápravné opatření	Status
IQT	DEV01	Název stanice uvedené v CDS (DS) neodpovídá názvu stanice systému.	Aktualizace specifikace konfigurace DS	Uzavřeno
OQT	DEV02	Systém nevyžádá vyplnit povinné pole „lot“ v ER2(protokol). Spuštění analýzy proběhne bez vyplnění tohoto pole.	Bez nápravných opatření. Požadavek na zadání pole „lot“ je součástí NO .	Uzavřeno
OQT	DEV03	Systém neumožní přihlášeni uživateli s uzamčeným/deaktivovaným účtem, ale nezobrazí oznámení o uzamčení/deaktivaci.	Do dokumentu SOP bude doplněna informace, že systém nezobrazuje oznámení o uzamčení/deaktivaci účtu.	Uzavřeno
PQT	DEV06	Při tvorbě specifikace uživatelských požadavků (URS) k počítačovému systému byl nesprávně vyžadován požadavek URS-PFR.03 (systém umožňuje vytvářet projekty pro měření a jednoznačně je identifikovat.)	Aktualizace dokumentu (URS)	Uzavřeno

- Pokud odchylky nejsou uzavřeny, musí být převedeny do systému CAPA s jasnou odpovědností a termíne odstranění nedostatku.
- Pokud je odchylka hodnocena jako kritická, musí být odstraněna před uzavřením validace.

Matice dohledatelnosti (TM)

ID požadavku	Popis požadavku	ID testu IQ	ID testu OQ	Reference DS
URS-ITFR.001	Příručka k systému musí být dostupná správcům v tištěné nebo v elektronické verzi (jazyk musí být angličtina nebo čeština).	IQT.08	-	
URS-ITFR.012	Složky stanice pro ER a další data systému musí být přesně vyspecifikovány a zajištěny proti smazání a modifikaci.	IQT.04	OQT.07	
URS-UAC.02	Detailní nastavení práv pro jednotlivé uživatelské úrovně/role musí být uvedeny ve specifikaci konfigurace a návrhu (CDS).	IQT.07	-	DS Příloha 1.

ID požadavku	Popis požadavku	ID testu PQ	Reference DS
URS-PFR.005	Systém umožňuje vytvořit tyto typy metod: ▪ Instrumentová metoda	PQT.03	
URS-PFR.006	Systém umožňuje provádět operace v následujícím pořadí (viz URS-ER.07): ▪ Volba instrumentové metody a protokolu (šablony pro sekvenci) ▪ Analýzy vzorku ▪ Tisk reportu	PQT.04	

Souhrnná validační zpráva (VSR)

Účelem tohoto dokumentu je zhodnotit všechny validační aktivity, které byly provedeny na laboratorním počítačovém systému TOC, položky v inventáři počítačových systémů společnosti TCI, který je nainstalován a bude provozován v laboratořích QC *(oddělení Pharma)* v závodě TCI.

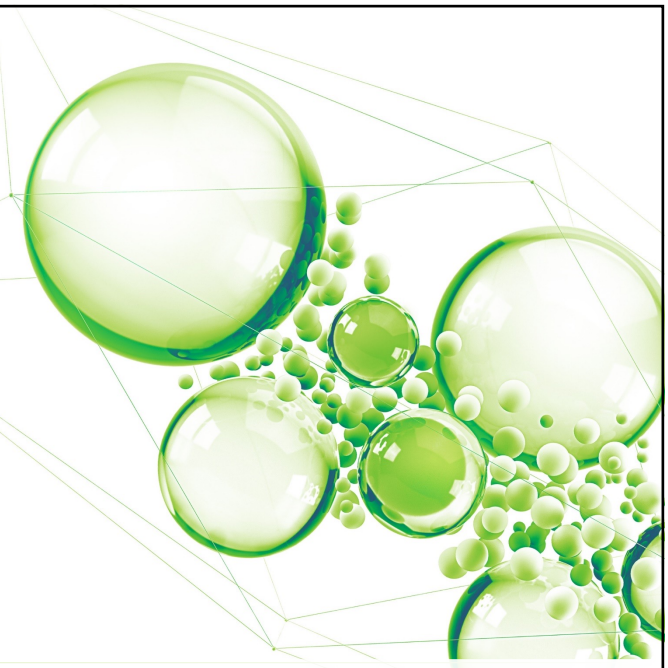
Zpráva musí obsahovat **závěr**, který propouští systém do řádného provozu:

3 Výsledek validace

Výsledky testů byly akceptovány a jsou v souladu se stanovenými požadavky. Vzniklé odchylky během testování byly vyřešeny nebo byla popsána nápravná opatření. Laboratorní počítačový systém DataPro2 je vhodný pro zamýšlený účel a lze jej používat.

- Zpráva by měla dále obsahovat:
  - **Seznam SOP**, které jsou nutné pro řádný provoz počítačového systémů
  - **Seznamy** provedených **testů** pro IQ, OQ a PQ, **hodnocení** všech **odchylek**
  - Master Index – **seznam** vytvořené **validační dokumentace** k danému systému.

Řádný provoz počítačového systému



Řádný provoz počítačového systému

- **Návod na obsluhu**, proškolení uživatelů (předpis, důkaz o proškolení)
- **Fyzické** a **logické zabezpečení**, **řízení uživatelů** a **pravidelná revize** přístupu (předpis, seznamy uživatelů)
- **Řízení změn** (předpis, dokumentace)
- **Plán obnovy, zálohování, archivace** (předpis, záznamy)
- **Mimořádné události** (předpis, záznamy, odchylky)
- **Periodické hodnocení** počítačového systému (předpis, záznamy)
- **Kontrola audit trailu** (předpis, záznamy)
- **Vyřazení počítačového systému** (plán, zpráva)

Kontrola audit trailu

SOP\PQA – Data Integrity

Toto SOP definuje:

- Strategii pro posouzení audit trailu na základě definování rizika počítačového systému a jeho dat
- Metody pro provedení posouzení audit trailu a jeho dokumentování

Jsou rozlišeny dva typy audit trailu a odpovědnosti:

Datový audit trail: část audit trailu, která se týká záznamu vlastníka systému. Kontrola datového audit trailu je předmětem standardní kontroly primárních záznamů analytické dokumentace nebo dat z výrobních zařízení. Za kontrolu datové části audit trailu je obecně odpovědný vlastník počítačového systému.

Systémový audit trail: část audit trailu, která dokumentuje změny prováděné technickým správcem. Systémový audit trail dokumentuje změny nad správou uživatelů a základním nastavením počítačového systému a změnou bezpečnostních nastavení. Za provedení kontroly je zodpovědný technický vlastník procesu.

6.4.1 Vlastník systému (BO)

- U procesu posouzení **datového** audit trailu je vlastník systému odpovědný za:
  - Zajištění provedení hodnocení kritičnosti použití počítačového systému pro stanovení kontroly audit trailu. Typ kontroly, perioda a rozsah kontroly musí být stanovený analýzou rizik a musí být definovaný v návodu na obsluhu počítačového systému.
  - Vlastník systému je zodpovědný za kontrolu **datové** části audit trailu a za dokumentování provedení podle požadavků SOP

6.4.2 Technický správce (TO)

- Pro proces hodnocení audit trailu musí technický správce zajistit, že konfigurace audit trailu je dokumentována a jeho nastavení nelze měnit z nižších uživatelských úrovní než administrátorských.
- Technický správce je zodpovědný za kontrolu **systémové** části audit trailu a za dokumentování provedení podle požadavků SOP

Nastavení požadavků na posouzení datového audit trailu

Rozlišují se tři typy kontroly datového audit trailu:

Typ kontroly audit trailu	Kritéria	Odpovědnost
Kontinuální	Kontrola audit trailu je prováděna v průběhu kontroly analytických výsledků.	Vlastník systému
Periodická	Kontrola audit trailu je prováděna v předem stanovené frekvenci 3 – 12 měsíců (dle kritičnosti).	Vlastník systému
Dle události	Kontrola audit trailu je prováděna v případě potřeby (např. šetření OOS či odchylek)	Vlastník systému

Požadavky na kontrolu datového audit trailu se stanoví na základě:

- Klasifikace kritičnosti měřených GxP dat
- Klasifikace kritičnosti systému z pohledu zajištění integrity GxP dat
- Identifikace kritických operací, které mohou ovlivnit výsledek analýzy nebo integritu naměřených dat.

Posouzení datového audit trailu - metodika

Na základě kritičnosti GxP dat a systému se stanoví požadavek na typ kontroly audit trailu a jeho periodu:

Kritičnost systému	Kritičnost GxP dat: **Vysoká** – GxP data přímo související s procesy stanovení obsahu API nebo nečistot pro FP, bulky a vstupní materiály	Kritičnost GxP dat: **Střední** – GxP data přímo související s ostatními procesy kvantitativního stanovení výsledků pro FP, bulky a vstupní materiály; GxP data přímo související s procesy IPC stanovení obsahu API nebo nečistot.	Kritičnost GxP dat: **Nízká** – GxP data přímo související s procesy kvalitativního stanovení výsledků pro FP, bulky a vstupní materiály; GxP data přímo související s procesy IPC stanovení (kvantitativního nebo kvalitativního). Ostatní GxP systémy QC.
Vysoká – GxP data může ovlivnit uživatel s nejnižší přístupovou úrovní (např. laborant)	**Kontinuální** kontrola AT	**Periodická** kontrola AT: Perioda max. 3 měsíce	**Periodická** kontrola AT: Perioda max. 6 měsíců
Střední – GxP může ovlivnit uživatel s vyšší přístupovou úrovní (např. specialista)	**Periodická** kontrola AT: Perioda max. 3 měsíce	**Periodická** kontrola AT: Perioda max. 6 měsíců	**Periodická** kontrola AT: Perioda max. 12 měsíců
Nízká – GxP data nemůže ovlivnit žádný uživatel	**Periodická** kontrola AT: Perioda max. 6 měsíců	**Periodická** kontrola AT: Perioda max. 12 měsíců	**Revize dle události**

Posouzení datového audit trailu – risk analýza

6.5.2 Identifikace GxP procesů a mapování dat (risk analýza)

Pro stanovení metody kontroly audit trailu se pro každý systém nejprve provádí identifikace všech GxP kritických operací, které mohou ovlivnit výsledek analýzy nebo integritu naměřených dat. V rámci identifikace procesů pro laboratorní počítačový systém je požadováno v rámci mapování zohlednit minimálně následující oblasti procesů:

- Příprava analýzy
- Analýza (včetně možnosti opakování měření)
- Interpretace naměřených dat (procesování)
- Generování výsledku
- Reporting (schválení) výsledku
- Archivace dat

Za kritické činnosti se považují ty činnosti, které mohou vést k porušení integrity dat. Všechny kritické činnosti musí být identifikovány, musí být popsány v risk analýze a musí být stanoveny opatření.

Provádění kontroly datového audit trailu - provádění

Provádění kontroly audit trailu a dokumentace

Kontrola audit trailu se provede podle postupu popsaného v návodech na obsluhu jednotlivých počítačových systémů v periodě a rozsahu, které vyplynuly pro jednotlivé systémy z analýzy rizik podle tohoto SOP.

Návod na obsluhu každého počítačového systému musí obsahovat:

- Stanovení typu kontroly audit trailu a periody periodické kontroly (pokud je požadována).
- Postup stanovení počtů vzorku pro periodickou kontrolu audit trailu.
- Risk analýzu identifikace kritických operací podle požadavků tohoto SOP.
- Přesný postup, jak je kontrola kritických operací prováděna.

Záznam o provedení kontinuální kontroly audit trailu je součástí záznamové dokumentace pro konkrétní laboratorní záznam.

Požadavky na provádění periodické kontroly audit trailu se řídí platným validačním plánem pro počítačové systémy (VMP) a jsou evidovány v modulu gTracking počítačového systému TWH.

Záznam o provedení periodické kontroly audit trailu je vydáván v dokumentačním systému Glorya (vzor viz příloha číslo 1). Po vydání zprávy je vlastník systému zodpovědný za vyplnění záznamu v gTracking a poslání záznamu na uzavření. Odpovědný pracovník QA je zodpovědný za posouzení a schválení záznamu.

Stanovení předmětu a rozsahu kontroly audit trail

Rozsah kontroly GxP dat v audit trailu vychází z typu kontroly:

Typ kontroly audit trailu	Rozsah kontroly
Kontinuální	Provádí se kontrola každého analyzovaného vzorku.
Periodická	Rozsah kontroly je určen dle ČSN ISO 2859-1.
Dle události	Individuální rozsah kontroly.

Počet analýz za hodnocené období (Rozsah dávky dle ČSN ISO-2859-1)	**Minimální rozsah kontroly v audit trailu** (Rozsah výběru při normální kontrole jedním výběrem, obecná kontrolní úroveň II, dle ČSN-ISO-2859-1; v závorce uvedeno kódové písmeno)

Provádění kontroly datového audit trailu – příklad NO (RA)

Návod na obsluhu pro zařízení TOC:

Fáze	GxP Elementy	Kritická operace	Oprávnění	Záznam v AT	Typ kontroly	Komentář
Analýza (měření)	ID instrumentové metody	Ne	N/A	N/A	N/A	Nejedná se o instrumentové metody ale o šablony, které slouží k zahájení analýzy (parametry se nastavují dále)
	Parametry pro analýzu	Ano	Operator/Supervisor	N/A	Kontinuální	Kontrola parametrů na reportu
	ID vzorku	Ano	Operator/Supervisor	N/A	Kontinuální	Kontrola ID vzorku na reportu Struktura ID vzorku je definována v NO
	Jméno analytika	Ne	N/A	N/A	N/A	Nelze změnit
	Opakování měření pro stejné ID vzorku	Ano	Operator/Supervisor	N/A	Periodická	Kontrola opakování analýzy pro dané ID v databázi – počet vzorků (viz Příloha 5)
	Přerušení analýzy	Ano	Operator/Supervisor	Stopped protocol	Periodická	Na reportu je uvedena informace o přerušení analýzy (Incomplete) – postup přerušení analýzy je popsán v NO
	Datum a čas analýzy	Ne	N/A	N/A	N/A	Nelze změnit

Provádění kontroly datového audit trailu – příklad NO (RA)

Návod na obsluhu pro zařízení TOC:

Fáze	GxP Elementy	Kritická operace	Oprávnění	Záznam v AT	Typ kontroly	Komentář
Analýza (měření)	ID instrumentové metody	Ne	N/A	N/A	N/A	Nejedná se o instrumentové metody ale o šablony, které slouží k zahájení analýzy (parametry se nastavují dále)
	Parametry pro analýzu	Ano	Operator/Supervisor	N/A	Kontinuální	Kontrola parametrů na reportu
	ID vzorku	Ano	Operator/Supervisor	N/A	Kontinuální	Kontrola ID vzorku na reportu Struktura ID vzorku je definována v NO
	Jméno analytika	Ne	N/A	N/A	N/A	Nelze změnit
	Opakování měření pro stejné ID vzorku	Ano	Operator/Supervisor	N/A	Periodická	Kontrola opakování
	Přerušení analýzy	Ano				
	Datum a čas analýzy	Ne				

Fáze	GxP Elementy	Kritická operace	Oprávnění	Záznam v AT	Typ kontroly	Komentář
Interpretace naměřených dat (procesování)	ID vzorku	Ne	N/A	N/A	N/A	Nelze změnit
	Parametry metody	Ne	N/A	N/A	N/A	Nelze změnit
	Rekalkulace surových dat	Ne	N/A	N/A	N/A	Neprovádí se
	Mazání dat	Ne	N/A	N/A	N/A	Nelze mazat
	Změna definovaného uložiště	Ne	N/A	N/A	N/A	Je předdefinováno systémem a nelze změnit
Generování výsledku	ID vzorku	Ne	N/A	N/A	N/A	Nelze změnit
	Jméno analytika	Ne	N/A	N/A	N/A	Nelze změnit
	Parametry metody	Ne	N/A	N/A	N/A	Nelze změnit
Reporting (schválení) výsledku	N/A					
Archivace dat	Primární data, protokoly a metody	Ne	N/A	N/A	N/A	Automatické zálohování SW Acronis

Provádění kontroly datového audit trailu – příklad NO

Návod na obsluhu pro zařízení TOC:

8.2 Metoda a četnost kontroly audit trailu

- Kritičnost systému: **Vysoká**
- Kritičnost GxP dat: **Střední**
- Typ kontroly: **Periodická kontrola -** perioda max. 3 měsíce.

8.3 Minimální požadovaný rozsah kontroly

Počet vzorků, na kterých je prováděna periodická kontrola, stanovuje Příloha 5 na základě počtu provedených analýz za hodnocené období. Pro kontrolu jsou vybírány vzorky ze začátku, středu a konce hodnoceného období. ID kontrolovaných vzorků budou přiloženy ke zprávě z kontroly audit trailu.

8.4 Postup periodické kontroly

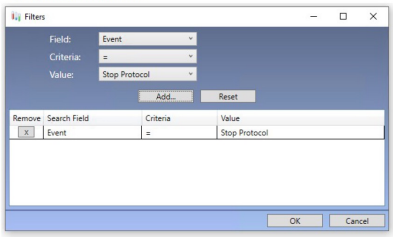
8.4.1 Postup kontroly opakování měření pro stejné ID vzorku

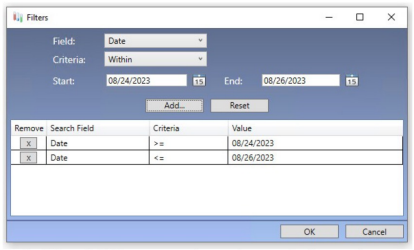
Opakované spuštění analýzy nelze vyhledat v audit trailu. Odpovědná osoba provede kontrolu všech výsledků ±7 dnů od analýzy kontrolovaného vzorku.

8.4.2 Postup kontroly přerušené analýzy

Přerušení analýzy (stop protocol) lze vyhledat v audit trailu:
V SW DataPro2 -> DataGuard, záložka audit trail vyberte „filtred", následně „change".

- V nově otevřeném okně nastavte vyhledávání: Field: „Event"; Criteria: „="; Value: „Stop protocol". Výběr potvrďte tlačítkem „Add".





- V případě, že tato kritická operace nenastala, se na obrazovce zobrazí „No Results".

Provádění kontroly datového audit trailu - zpráva

- Perioda zprávy se řídí definovanou periodou dle návodu na obsluhu.
- Všechny periodické kontroly audit trailu jsem definovány a průběžně kontrolovány v rámci VMP pro počítačové systémy.
- Zpráva z periodické kontroly je vydána c dokumentačním systému.

1 Zpráva periodické kontroly audit trailu

1.1 Úvod

Zpráva periodické kontroly audit trailu hodnotí kritické operace v počítačovém systému za definované období hodnocení. Periodická kontrola je provedena podle požadavků SOP - Data Integrity.

1.2 Hodnocení

V rámci procesu byly provedeny kontroly podle požadavků návodu na obsluhu počítačového systému.

Provedení periodické kontroly audit trailu		
Kód počítačového systému		
Název počítačového systému	***DataPro 2***	
Hodnotící období	***13.09.2023 – 30.11.2023***	
Kontrolu provedl		
Návod na obsluhu		
Přehled testů na posouzení audit trailu	**Výsledek**	
Kontrola opakování měření pro stejné ID vzorku	☒ **OK**	☐ **NOK**
Kontrola přerušení analýzy	☒ **OK**	☐ **NOK**
Poznámky		
Kontrola audit trailu byla provedena od uvedení do provozu dne 13.09.2023 do 30.11.2023. Počet kritických událostí ve sledovaném období: 0 Ve sledovaném období byla provedeno 210 analýz. Pro kontrolu audit trailu bylo vybráno 32 vzorků. Kontrola byla provedena u vzorků: 1857780, 1827224, 1826815, 1827838, 1827839, 1827840, 1827841, 1827842, 1827843, 1827844, 1827845, 1827846 (13.09.2023); 1868823, 1868808, 1868380, 1868381, 1868382, 1868383, 1868384 (24.10.2023); 1898611, 1898612, 1898613, 1898614, 1898615, 1898616, 1898617, 1898618, 1868406, 1868408, 1868409, 1868410, 1868411 (24.11.2023).		

1.3 Závěr

Periodická kontrola audit trailu počítačového systému byla shledána **vyhovující** a počítačový systém včetně předpisové dokumentace je používán podle platných požadavků a **může** být dále používán pro zamýšlený účel.

Příklad – kontinuální kontrola - Empower

Je posuzováno:

1) Analýza nebyla provedena opakovaně

Jedná se o ověření, že daný vzorek charakterizovaný LIMS číslem nebyl analyzován v rámci projektu opakovaně.

Pokud ne, zatrhne se OK.

Pokud byl analyzován opakovaně, zatrhne se NOK a musí být uvedeno číslo šetření (SST, gLIR, ZE, gProtocol, atd.)

2) Ověření shody elektronického záznamu v aplikačním SW a papírového záznamu

Jedná se ověření, zda data v papírovém záznamu jsou ve shodě s elektronickým záznamem v software Empower.

Pokud ano, zatrhne se OK (i v případě, že byla provedena oprava v rámci nestandardní události).

V papírovém záznamu lze opravit: číslo Attachmentu, název produktu, číslo OOS/SST/ZE, stabilitní podmínky. Pokud bude při kontrole nalezena zapsaná hodnota v poli, které není součásti výpočtu, provede se k tomuto poli komentář „ nesouvisí s výpočtem“, tento komentář může provést kontrolor. K opravě je připojen podpis a datum provedení opravy. Na check list je zapsáno NOK.

3) Nebyl proveden zásah do naměřených dat a ověření, jestli byl zásah do dat proveden v souladu s předpisovou dokumentací

Jedná se o ověření, zda je pro dané injection ID pro vzorek na reportu v záložce Result # (System Information) uvedeno více výsledků.

Pokud ne, zatrhne se OK (zatrhne se OK i v případě, kdy je z jednoho nástřiku vyhodnocováno více parametrů např. obsah + nečistoty).

Pokud ano, zatrhne se NOK a musí být uveden důvod reprocesování. Při reprocesování, kdy dochází ke změně hodnoty výsledku je nutno uvést číslo SST z LIMS (Reprocesování – Empower). Doložíme tisk SST.

Manuální integrace musí být provedena ve shodě s SOPG pro HPLC a s SOPG pro GC.

Příklad – kontinuální kontrola - Empower

4) Použití alter running sample set

5) Použití aborted sample set

6) Kontrola ekvilibračního sample setu

7) Kontrola data missing a data incomplete

Acquired By
Processed By ****
Printed By
Project: 21_1\QDP65168_D_21_1

System:
Sample Set Name 210201
Report Method Name: TEVA_SampleSet_checkII

Data Integrity/Kontunualni posouzeni integrity dat

	1) Analyza nebyla provedena opakovane	2) Shoda el/papir	3) Nebyl proveden zasah do vyhodnoceni	4) Nebyl proveden alter running SS	5) Nebyl proveden abort SS	6) Kontrola EQ sample setu	7) Data Missing/ Data Incomplete
1	NOK	✓	✓	✓	✓	✓	

Pokud je nektery z parametru NOK uvede se duvod:

1) kontrola zda byla provedena analýza opakovane, pokud ano, uvede se duvod napr ZE, gLIR, SST

2) vyhodnocení bez manuálního zásahu do vypoctovych hodnot - manualne lze opravit bez prewyhodnocení Attachment, produkt, OOS/SST/ZE, stabilitni podminky, zpiseme NOK duvod není nutno uvadet je provedena oprava podpis + datum

3) komentar k vysledkum #2 pokud se vyhodnocují dva testy z jednoho nastiku nekomentuje se a status je OK

4) kontrola audit trailu

5) kontrola audit trailu

6) zapiseme N/A pokud nebyl EQ spusten

7) kontrala auditrailu

Kontroloval/Datum : 03. 02. 2021

Kontrola systémového audit trailu

- **Provedení kontroly systémového audit trailu**
- Zodpovědnost: technický vlastník systému
- Zaměření:
  - Archivace dat
  - Řízení uživatelských profilů a uživatelů
  - Změny nastavení zabezpečení
  - Mazání dat v systému
- Kontrola vydána formou zprávy: 1x ročně nebo součást periodického hodnocení počítačového systému.

Periodické hodnocení

SOP\PQA - Periodické hodnocení

- frekvence periodického hodnocení pro počítačové systémy:

RAI/ komplexnost počítačového systému	Frekvence periodického hodnocení
Velká a GAMP kategorie 3,4,5	1 x za 2 roky
Malá, střední, velká a GAMP kategorie 5	1 x za 2 roky
Malá, střední a GAMP kategorie 4	1x za 3 roky
Malá, střední a GAMP kategorie 3	1x za 5 let

- 1x za 3 roky periodické hodnocení infrastruktury a periodické hodnocení výpočtových excelovských šablon

Proces hodnocení systémů

Na základě požadavků technického vlastníka hodnotící tým provede revizi minimálně následujících záznamů:

- validační dokumentace (plány, specifikace, analýza rizik, testování, zprávy)
- analýza ER/ES
- návod na obsluhu (NO), záznamy školení
- hodnocení změn, incidentů a odchylek
- definice úrovně přístupů
- platných přístupů uživatelů
- zálohování, archivace, BCP a DRP
- integrity dat, funkčnosti audit trailu
- systémového audit trailu
- nálezy z předchozích periodických hodnocení, auditů a interních auditů

Periodické hodnocení – vzor zprávy

1 Souhrnná zpráva periodického hodnocení počítačového systému

Kód systému	
Název systému	
Verze systému	
Hodnocené období	

1.1 Úvod

Souhrnná zpráva hodnotí validační stav systému ***kód a název systému***. Systém byl uveden do řádného provozu ***datum uvedení do provozu*** a ověřen ***datum provedení periodických hodnocení***. Tento dokument byl vytvořen podle platné verze SOP Periodické hodnocení počítačového systému.

1.2 Hodnotící tým

Hodnocení počítačového systému bylo provedeno následujícím hodnotícím týmem:

Funkce	Jméno
Vlastník systému	
Technický vlastník	
QAV	
Další zúčastněné osoby	

Periodické hodnocení – vzor zprávy

Předmět kontroly	Hodnocení
I. Validační dokumentace (plány, specifikace, analýza rizik, testování, zprávy)	
Kontrola validační dokumentace z pohledu úplnosti a kompletnosti, kontrola schválení	
Odchylky z validací a jejich status	
Hodnocení dodavatele počítačového systému	
II. Analýza ER/ES	
Existence a typy ER	
Existence a typy ES	
Ověření ER/ES	
III. Uživatelský manuál, záznamy školení	
Existence NO	
Kontrola přiřazení NO do školících plánů uživatelů	
Kontrola přiřazení SOP pro administraci (řízení uživatelů, zálohování) do školících plánů TO	
IV. Řízení změn	
Existence SOP na řízení změn	
Seznam změn od posledního PR včetně určení typu změny v souladu s SOP – Řízení změn počítačových systémů	
V. Řízení incidentů	
Existence SOP na řízení incidentů	
Seznam incidentů od posledního PR	
Seznam odchylek od posledního PR	

Periodické hodnocení – vzor zprávy

VI. Hodnocení změn, incidentů a odchylek	
Hodnocení změn, incidentů a odchylek od posledního PR, zejména: Lze pozorovat trend ve vzniku incidentů a odchylek a identifikovat jeho příčinu?	
VII. Definice úrovně přístupů	
Existence SOP s definicí úrovní uživatelských přístupů	
Seznam aktivních uživatelů a jejich přiřazených rolí je aktuální proti výpisu z počítačového systému.	
Pravidelná revize uživatelů proběhla v předepsaném intervalu.	
Uživatelé mají jedinečný uživatelský účet pro přístup do systému.	
Administrátor systému nedisponuje více uživatelskými účty - pro administraci a pro provádění funkcí vlastníka procesu.	
Vlastník systému (BO) a technický vlastník (TO) jsou vzájemně nezávislými.	
Uživatelé systému nemohou provádět změny v metadatech, mazat záznamy nebo s nimi manipulovat a nemohou změnit konfiguraci audit trailu.	
VIII. Data Integrity a ověření funkčnosti datového audit trailu	
Prováděna kontrola audit trailu ve shodě s SOP pro Data Integrity.	
Rozsah a frekvence kontroly audit trailu jsou založeny na zhodnocení rizik.	

Periodické hodnocení – vzor zprávy

IX. Systémový audit trail	
Systémový audit trail je stále aktivní.	
Systémová konfigurace (nastavení rolí uživatelů, nastavení politiky hesel, nastavení audit trailu) je ve shodě se specifikací konfigurace systému.	
Systémový audit trail pro nastavení rolí uživatelů, nastavení politiky hesel, nastavení audit trailu – provedené změny v nastavení za sledované období jsou ve shodě s dokumentací změn k systému.	
Ověření systémového audit trailu pro přiřazení role administrátora - výpis za sledované období musí být ve shodě se změnami v platném seznamu uživatelů.	
Datové uložiště v systému je ve shodě se specifikací konfigurace systému.	
Naměřená data jsou ukládána pouze do uložiště definovaného ve specifikaci konfigurace systému.	
Datum a čas systému synchronizovány s autorizovaným zdrojem (časovým serverem).	
X. Zálohování, archivace, BCP, DRP	
Existence SOP na BCP	
Existence SOP na zálohování a obnovu dat	
Ověření funkčnosti obnovy zálohy, archivace	
Ověření, že probíhá pravidelná kontrola, že zálohovací proces je aktivní,	
Ověření SOP pro archivaci	
Ověření záznamové dokumentace, pokud je archivace dat prováděna manuálně	
Ověření systémového audit trailu pro archivaci dat (ověřit na poslední provedené archivaci, že výpis v audit trailu je ve shodě s dokumentací k archivaci).	
Existence DRP	
Ověření funkčnosti obnovy DRP	

Periodické hodnocení – vzor zprávy

XI. Nálezy z předchozích periodických hodnocení, auditů a interních auditů	
Nálezy z předchozích periodických hodnocení	
Nálezy z auditů	
Nálezy z interních auditů	

1.4 Nálezy z periodického hodnocení počítačového systému

Byly-li během periodického hodnocení zjištěny nedostatky, pak jsou uvedeny níže. Všechny nálezy musí obsahovat ID kód přidělený systémem TrackWise, stručný popis a datum, do kterého musí být nález odstraněn. Rovněž musí obsahovat hodnocení dopadu nálezu na validační status počítačového systému. Nálezem z periodického hodnocení se rozumí zejména:

- Zjištěné odchylky/problémy
- Požadovaná nápravná a preventivní opatření

1.5 Závěr

Počítačový systém byl shledán **vyhovujícím/nevyhovujícím** a **může/nemůže** být dále používán pro zamýšlený účel.

Zkratky

AT	audit trail
BCP	business continuity plan
BO	vlastník systému
DI	data integrity
DRP	disaster recovery plan
EMA	Evropská léková agentura
ER	elektronické záznamy
ES	elektronické podpisy
FDA	Food and Drug Administration (US)
FRA	funkční analýza rizik
IQ	instalační kvalifikace
ISPE	The International Society for Pharmaceutical Engineering
OQ	operační kvalifikace
PDA	Parenteral Drug Association
PIC/S	Pharmaceutical Inspection Co-operation Scheme
PQ	procesní kvalifikace
QA	řízení jakosti
SOP	standardní operační postup
TM	matice dohledatelnosti
TO	technický vlastník
URS	uživatelská specifikace
VP	validační plán, validační protokol
VSR	souhrnná validační zpráva
WHO	Světová zdravotnická organizace
ZŘ	změnové řízení