EffiChem, s.r.o.
Purkyňova 649/127 (budova INMEC), Brno – Medlánky 612 00
www.effichem.cz

Výběr dodavatelů a poskytovatelů IT služeb

S postupem elektronizace a digitalizace nabývá výběr dodavatelů a poskytovatelů IT služeb pro SVP regulovaný/farmaceutický průmysl a ISO 17025 akreditované laboratoře na důležitosti, a to jak z hlediska schopnosti splnění farmaceutické legislativy, resp. normy ISO 17025, tak z hlediska plnění požadavků a očekávání samotných zákazníků a uživatelů.

1. Legislativní požadavky

V ČR jsou požadavky SVP dány SÚKL předpisem VYR-32 doplněk 11, ve kterém se specifikuje, že:

3.1 Pokud jsou využívány třetí strany (např. dodavatelé, poskytovatelé služeb), např. pro poskytování, instalaci, konfiguraci, integraci, ověřování, údržbu (např. prostřednictvím vzdáleného přístupu), změnu nebo archivaci počítačového systému nebo související služby, nebo pro zpracování dat, musí existovat formální dohody mezi výrobcem a jakoukoliv třetí osobou, a tyto dohody mají obsahovat jasné prohlášení o odpovědnosti třetích stran. Obdobně se mají brát v úvahu IT oddělení.

3.2 Kompetence a spolehlivost dodavatele jsou klíčovými faktory při výběru produktu nebo poskytovatele služeb. Potřeba auditu má být založena na posouzení rizik.

3.3 Dokumentace dodaná s běžnými komerčními produkty má být přezkoumána regulovanými uživateli za účelem ověření, že jsou splněny uživatelské požadavky.

3.4 Systém jakosti a informace z auditu týkající se dodavatele nebo projektanta softwaru a zavedených systémů mají být zpřístupněny inspektorům na vyžádání.

2. Požadavky na audit

Požadavek 3.1 uvádí, že dohoda musí zahrnovat role a odpovědnosti třetí strany, resp. zúčastněných osob, a nabízené služby. Než může být taková dohoda nebo smlouva uzavřena, je třeba si zodpovědět několik otázek. Základní je:

Je potřeba auditovat dodavatele, resp. poskytovatele IT služeb?

Doplněk 11 říká, že řízení rizik by mělo být uplatňováno po celou dobu životního cyklu počítačového systému s přihlédnutím k bezpečnosti pacientů, integritě dat a kvalitě produktu. Dále v kap. 3.2 se uvádí, že kompetence a spolehlivost dodavatele jsou klíčovými faktory při výběru produktu nebo poskytovatele služeb. Potřeba auditu má být založena na posouzení rizik. Avšak, auditní zprávy musí být na požádání předloženy inspektorovi, viz kap. 3.4.
Z regulatorního pohledu je tedy potřeba u dodavatele provést adekvátní kontrolu/audit. Při něm by neměla být brána v úvahu pouze regulatorní hlediska, ale také obchodní.

Tabulka 1 sumarizuje další požadavky SVP a 21 CFR 11 na IT infrastrukturu:

Doplněk 11 Požadavky na IT Infrastrukturu	**Požadavky 21 CFR Part 11 na IT Infrastrukturu**
• Záznamy a školení: Kvalifikace a životopisy Záznamy o školení včetně • Počáteční a průběžné školení z požadavků GMP a odpovídající kompetence • Zabezpečení • Zálohování a obnova • Řízení změn a správa konfigurace • Pravidelné hodnocení • Správa uživatelských účtů • Dokumentované řízení incidentů a propojení s CAPA	Požadavky na pravidla GMP, např.: • Kvalifikace a životopisy zaměstnanců • Záznamy o počátečním a pravidelném školení, budování GMP povědomí a kompetencí • 11.10 (b) Vytváření přesných a úplných kopií záznamů • 11.10 (c) Ochrana záznamů • 11.10 (d) Omezení přístupu oprávněným osobám • 11.10 (e) Časové razítko (Audit trail)

Shromáždění objektivních informací, že poskytovatel IT služeb s adekvátní mírou jistoty zajistí služby ve shodě s požadavky regulace, spolehlivě a bezpečně, může být skutečnou výzvou.

3. Audit poskytovatele IT služeb:

Při auditu poskytovatele IT služeb je důležité se zaměřit na hlavní cíle a otázky jako:

- zajištění důvěry ve schopnosti poskytovatele IT služeb ve shodě s regulací
- kontrola systému managementu kvality poskytovatele služeb (QMS)
- kontrola zajištění integrity, přístupnosti, čitelnosti a důvěrnost údajů

Protože žádný dodavatel resp. poskytovatel není dokonalý, výsledkem auditu bude obvykle:

- Identifikace nálezů, které nejsou v souladu s předpisy
- Náprava zjištění prostřednictvím CAPA plánu

Pouze v případě, že auditovaná organizace akceptuje zjištění auditu a souhlasí se změnou svého přístupu zavedením nápravných a preventivní/zlepšovacích opatření, může mít audit smysl pro zajištění budoucí spolupráce.

4. Co auditovat?

Tabulka 2 poskytuje přehled hlavních oblastí, které je potřeba vzít v úvahu a auditovat

Tabulka 2: Klíčové oblasti a kritéria pro audit poskytovatelů IT služeb (kromě systému řízení kvality)

Oblast auditu	Kritéria
Zachování integrity dat po celou dobu uchovávání záznamů	• Důvěrnost údajů • Zabezpečení dat • Řízení přístupu a správa uživatelů • Opatření pro uchovávání údajů
Právní požadavky kladené na data uložená v infrastruktuře	• Nároky na duševní vlastnictví • Směrnice EU o ochraně osobních údajů
Kvalifikace infrastruktury, pokud je relevantní (cloud)	• Správně navržená a specifikovaná infrastruktura • Správně instalovaná infrastruktura • Ověřený provoz • Kvalifikované aplikace infrastruktury • Schválené specifikace a návrhy • Instalační plány a záznamy • Ověřená / otestovaná infrastruktura, která prokazuje správnou funkci oproti specifikaci
Správa dat	• Procesy zálohování a obnovení • Kontinuita dat a obnovení po havárii • Archivace
Management změn	• Zahrnuje postup řízení změn vlastníka dat v případě změn infrastruktury? • Zahrnuje postup řízení změn vlastníka dat pro změny provedené v systému, aplikacích a konfiguracích? • Zahrnuje řízení implementace nových verzí
Správa incidentů	• Správa incidentů – zahrnuje popis chyb resp. selhání, určení příčiny, vyhodnocení dopadu a nápravná opatření?

Oblast auditu	Kritéria
Kontinuita činnosti	• Kontinuita činnosti – zahrnuje opatření, která zajistí nepřetržitou podporu kritických procesů v případě poruchy systému (např. manuální nebo alternativní systém), včetně dokumentace a testování těchto opatření. • Kontinuita se neomezuje na dostupnost, ale musí pokrývat přírodní úkazy jako povodně, bouře, výpadky elektřiny, atd.
Znalosti SVP	• Zná poskytovatel služeb předpisy a požadavky na zajištění evidence a dohledatelnosti činností? • Předpisy vyžadují adekvátní kombinaci vzdělání, odborné přípravy a zkušeností • Znalost předpisů SVP, která jim umožní vykonávat jejich práci. • Musí probíhat pravidelné školení o aktualizace znalostí SVP (obvykle jednou ročně). • Formální školicí materiály s hodnocením
QA dohled nad IT aktivitami	Znalosti regulace: • Regulační požadavky na zajištění jakosti dle požadavků SVP • technické znalosti IT infrastruktury

5. Způsoby auditování

Existují tři základní možnosti auditu dodavatele, včetně poskytovatele cloudových služeb:

- Audit formou Dotazníku

- Dotazník a následná telekonference a kontrola dokumentů

- Dotazník a audit na místě s ověřením skutečného stavu

Každá varianta má výhody a nevýhody.

Dotazník

Dotazník je nejrychleji proveditelná varianta auditu, ale dává nejmenší záruku ve skutečnou kvalitu dodavatele. Spoléhá na to, že dodavatel bude při vyplňování dotazníku upřímný a pravdivý. Proto je nutno zajistit, aby zvolené otázky byly dostatečně vypovídající, případně si vyžádat podpůrné informace, např. seznam SOP a seznam specifikací, resp. důkazy o adekvátním systému kvality. Po obdržení vyplněného dotazníku je třeba jej zkontrolovat a vyhodnotit, nikoli pouze založit do šuplíku. Výstupem hodnocení musí být závěr, zda odpovědi jsou přijatelné nebo je třeba dodavatele požádat o další vysvětlení? Nakonec je potřeba učinit rozhodnutí, zda dodavatele využijete, či nikoli, a důvody pro toto rozhodnutí by se měly zdokumentovat v souhrnné zprávě.

Dotazník plus následná opatření

Další možností auditu je forma Dotazníku s přezkoumáním vyplněného dokumentu, jak je uvedeno výše, následované tele/video-konferencí, kde se kromě dokumentů přezkoumají odpovědi a položí doplňující otázky. Nelze očekávat, že dodavatel přesně popíše svůj systém jakosti formou dotazníku, ale musí být ochoten diskutovat o svých politikách a postupech, a ukázat své dokumenty. Podmínkou pro toto obvykle je podpis dohody o mlčenlivosti.

Tele/video-konference vedle dotazníku dává možnost jít do větších podrobností a ověřit si pravdivost odpovědí v dotazníku. Témata lze podrobněji prodiskutovat, potvrdit přístupy k dodržování předpisů a nahlédnout do dokumentace, která nebyla v rámci dotazníku poskytnuta. Některé společnosti uvádějí jako důvod neochoty předvedení dokumentace a interních postupů "duševní vlastnictví". Pokud je uzavřena dohoda o mlčenlivosti, tak tento důvod není relevantní a spíše značí, že společnost nechce informace sdílet, neboť si není jista vlastní kvalitou a systémem jakosti.

Dotazník plus audit na místě

Dotazník se vyplňuje a kontroluje podobně, jak je popsáno výše. Navíc se provádí audit zařízení nebo datového centra a kanceláří společnosti na místě, kde je možno jít do větších podrobností. Je třeba naplánovat termíny návštěvy a dohodnout program a harmonogram. Audit by měl mimo jiné zahrnovat vysvětlení organizačních schémat, záznamy o školení, atd.

Z organizačního schématu by mělo být patrné, kde jsou využíváni subdodavatelé. To je důležité z několika důvodů, např. proto, zda existuje dohoda mezi poskytovatelem služeb a případně využívanou sub-dodavatelskou organizací, která podrobně popisuje role a odpovědnosti a dodržování požadavků SVP.

Záznamy o školení, životopisy a popisy pracovních pozic pracovníků poskytovatele služeb, včetně subdodavatelů, musí být přezkoumány, aby se zjistilo, zda pracovníci mají odpovídající kombinaci vzdělání, školení a zkušeností. Nedostatkem norem ISO je, že nevyžadují životopisy, které jsou vyžadovány ve farmaceutickém průmyslu, a proto musí dodavatel jít dále než k akreditaci ISO.