# Cíle a postup informačního auditu

*Informační audit je souhrnný název pro jednorázovou činnost, jejímž výsledkem je obraz, jak skutečně funguje informatika v prověřované oblasti.*

V západní Evropě je povinný pro všechny informační systémy s dopadem na zdraví a bezpečnost občanů a pro všechna výpočetní střediska, která zpracovávají citlivá data pro externí zákazníky. V České republice je povinný pouze pro bankovní systémy. Systém jednotné přípravy informačních auditorů fakticky standardizoval postup auditu a strukturu výsledné zprávy.

Článek popisuje typický průběh auditu od přípravy prověrky až po zpracování a prezentaci zjištění. Důraz článku je kladen na tři stránky prověrky:

- Zjištění, zda existují pravidla a ukazatele pro měření efektivnosti zpracování a jak je prováděno hodnocení efektivnosti zpracování jednotlivých problémových okruhů, respektive jak nákladná je informační podpora jednotlivých obchodních procesů a co přináší těmto procesům.
- Posouzení stavu spolehlivosti a bezpečnosti vlastního zpracování a to nejen ve vztahu ke zneužití chráněných údajů, ale i z hlediska řešení mimořádných a havarijních situací a rizik jejich vzniku.
- Zmapování a posouzení úrovně vnitřního signálního systému, jehož úkolem je signalizovat chyby zpracování a detekovat chybná data.

Závěrem článek na příkladech z České republiky ukazuje, že dobře zpracovaný informační audit slouží nejen pro operativní odstraňování zjištěných nedostatků, ale zpravidla tvoří výchozí základnu pro formulaci cílů informační strategie podniku a současně mění systém vnitropodnikového sledování nákladů na podnikové informační i obchodní procesy. Průhledné sledování nákladů a identifikace a analýza rizik umožňuje kvalifikovaně plánovat investice do informačních technologií a s tím souvisejí restrukturalizaci informační podpory obchodních procesů.

***Informační audit představuje jednorázovou prověrku, jejímž výsledkem je zjištění, jak ve skutečnosti funguje informatika v prověřovaných oblastech. Výsledný protokol informačního auditu je v současné době fakticky standardizován tak, aby vedoucím pracovníkům srozumitelnou formou poskytl verifikovanou informaci, jaké služby (za jakou cenou a s jakým rizikem) informatika poskytuje pro plnění hlavních činností organizace. Výsledek informačního auditu zpravidla navrhuje krátkodobá neinvestiční nápravná opatření a současně slouží jako základ pro formulaci dlouhodobých priorit a věcných cílů informační strategie.***

## Úvod

Pojem "audit" je svým původem kritická analýza vymezené části hospodářských aktivit. Americká asociace auditorů definuje audit jako systematický proces objektivního získávání a vyhodnocování důkazů s cílem zjistit míru souladu mezi informacemi popisujícími zkoumané aktivity a stanovenými kriterii s tím, že výsledky auditu jsou sdělovány zainteresovaným zájemcům. Historicky prvními auditory byli již ve třetím století před Kristem kvestoři jmenovaní římskými vládci, kteří kontrolovali účetnictví ve všech provinciích. V té době byl od latinského slova "audire" (poslouchat) odvozen pojem audit, protože kvestoři výsledky auditu sdělovali slovně vybraným posluchačům. V průběhu let se audity a jejich zaměření specializovaly. Dnes se pojem audit stal faktickým synonymem pro hloubkovou kontrolu, kde přídavné jméno (například finanční, provozní, interní, jakostní atd.) určuje zaměření auditu. Typickým znakem všech auditů je jejich interní charakter. Jsou zpravidla určeny pouze pro vedení podniku (případně zástupce vlastníků) a mají poskytnout objektivní odpověď na jasně formulované otázky. Otázky s výjimkou finančního auditu (tam je jediná otázka a to, zda účetnictví věrně zobrazuje skutečné výsledky hospodaření) zásadně formuluje ten, kdo si audit

objedná. Objednatel auditu také jediný obdrží prezentaci výsledných zjištění, protokol a sumarizující výrok auditora a sám rozhodne o jeho případném zveřejnění.

## Situace vhodné pro informační audit

V praxi se setkáváme s různými pohnutkami pro objednání informačního auditu. Nejběžnější je v poslední době případ, že do organizace nastoupí nový vlastník a zjistí, že není spokojen s existující informační podporou. Obvykle chce provést restrukturalizaci a postrádá věrohodné podklady pro návrh restrukturalizace a zejména údaje pro měření výsledků při jejich realizaci. Pokud tato data požaduje, je tlačen do dalších investic do výpočetní techniky a přitom na skoro každém stole vidí osobní počítač připojený k podnikové počítačové síti. Zpravidla vedlejším produktem dobře provedeného informačního auditu je úspora administrativních "štábních" pracovníků, protože dnešní typický podnik má v počítačích uložen velký objem informací, z nichž využívá pouze část a přitom ekvivalentní údaje zpracovává ručně. Zatím jsme se nesetkali se středním podnikem, kde by některé údaje z účetních systémů neduplikovaly odpovídající údaje vznikající v ostatních provozních systémech a přitom se hodnoty dat z různých zdrojů nelišily. Nepřesné vymezení informačních zdrojů má za důsledek, že řada pracovníků data neustále ručně přepočítává a výkonní pracovníci věří spíše svým ručním záznamům než počítačům. Praxe ukazuje, že odstranění podnikových duplicit při zpracování podnikových dat v různých agendách vede nejen ke sjednocení a zvýšení věrohodnosti účetních a obchodních výkazů, ale současně snižuje personální stavy štábních útvarů.

Druhým typickým případem objednání informačního auditu je snaha vedení jasně formulovat informační strategii a k tomu potřebují objektivní srovnání existujícího stavu s průměrem v podobných podnicích. Pak formulují informační strategii na základě zjištěných silných a slabých stránek vlastní informační podpory.

Třetím případem objednání informačního auditu je případ, kdy některý vedoucí získá podezření, že zpracování není v pořádku anebo bezpečnostní rizika představují vážnou hrozbu pro chod řízených útvarů. Protože podezřívá pracovníky z vlastní organizace či dodavatele, že jsou raněni tzv. provozní slepotou anebo zakrývají vlastní nedostatky, tak objedná externí audit.. V případě nekvalitních dodavatelů tento případ občas končí tendencí k soudnímu řešení, respektive k důvodnému požadavku na slevu anebo bezplatnou nápravu zjištěných nedostatků.

Posledním případem objednání úzce zaměřeného auditu je situace, kdy vedení zjišťuje problémy při realizaci nového informačního projektu (časové skluzy, nárust ceny) a potřebuje nezávislou informaci, v čem je příčina problémů. Někdy je požadavek na audit informačního projektu vyvolán sponsorem projektu, který vyžaduje expertní ocenění vynaložených nákladů v relaci k dosaženým skutečným výsledkům.

## Právní úprava účelu a formy informačního auditu

Z právního hlediska se v České republice poprvé o informačním auditu zmiňuje pouze Opatření České národní banky č. 7/94 v souvislosti s bankovním auditem. V poslední době se situace mění, protože Česká republika přijala Memorandum ke členství v Evropské unii a tudíž se bude přizpůsobovat Směrnicím EU. Například Směrnice č. 95/46/EC týkající se zpracování osobních dat a ochrany soukromí ukládá zajistit periodickou kontrolu dodržování práv jednotlivců. K tomu byla zřízena odborná komise, která technicky zpřesňuje formu periodického auditu. Příslušná pravidla dříve či později akceptuje i český právní řád včetně odvozených pravidel typu Směrnice 97/66 z 12/12/97 o zpracování osobních dat a ochrany soukromí v odvětví telekomunikací.

České procesní právo uznává institut soudních znalců. Pokud by objednatel informačního auditu předpokládal využití výsledku auditu v soudním sporu s obchodním partnerem, je účelné, jestliže je tato partie výsledného protokolu zpracována formou samostatné přílohy ve formě obvyklé pro soudně-znalecké posudky a potvrzena soudním znalcem.

V zásadě lze říci, že právní řád předpokládá interní využití informačního auditu a proto je povinnost informačního auditu právně zakotvena pouze pro případy zpracování informací s dopadem na zdraví,

bezpečnost nebo svobodu občanů. Obsah a struktura informačního auditu se řídí pouze nezávaznými doporučeními odborných komisí. Tato doporučení vycházejí z obvyklého interního využití auditu a doporučují následující formu výsledku:

- jaké úrovně služeb se dosáhlo;
- komu a jaké informace jsou distribuovány;
- standardní a nestandardní informační procesy;
- uspokojení reálných informačních potřeb;
- riziková místa zpracování informací;
- kompetence při řízení informací;
- náklady při zpracování informací.

Jedná se o nezávazná doporučení, která upřesňuje objednatel auditu podle svých potřeb.

## Obecná pravidla postupu při informačním auditu

Aditor při formulaci všech výše uvedených závěrů musí dodržovat obvyklá pravidla kontrolní práce. K nim patří zejména:

- Při zjištění každý údaj použitý pro odvození závěrů verifikuje. To znamená, že je buď potvrzen nezpochybnitelným dokumentem z vnějšího nezávislého zdroje anebo je potvrzen nejméně ze dvou na sobě nezávislých podnikových pramenů.
- Auditor má zpracována pravidla pro odvození a klasifikaci závažnosti závěrů. Odvození je prováděno vždy na základě porovnání s předem stanoveným etalonem. Auditor musí být připraven prokázat věrohodnost použitých etalonů anebo musí upozornit na případné diskutabilní parametry etalonů a tomu přizpůsobit pravidla odvozování závěrů.
- Auditor může postupovat horizontálně (prověřit jedno místo zpracování ve všech obvyklých situacích a pak prověřovat další) anebo vertikálně (vytipovat problém a prověřovat předchozí a následné zpracování až k eliminaci příčin problému a kde se promítají jeho důsledky). Vertikální postup vede zpravidla mnohem rychleji ke zjištění nedostatků a formulaci návrhu nápravných opatření, ale prověřovaní pracovníci se emocionálně často brání poukazem na neobjektivitu prověrky, protože auditor se zabývá pouze nedostatky a nezabývá se tím, co funguje dobře.
- Auditor musí fakta zjišťovat s maximálně možnou objektivitou. Jeho úkolem je zjišťovat fakta a hodnotit je. V žádném případě není jeho úkolem požadovat podrobná vysvětlení, kdo a proč zavinil zjištěné nedostatky. Extrémním případem nevhodného postupu auditora je přístup charakterizovaný úslovím “takové vysvětlení neberu”.
- Auditor musí veškerá zjištění vztahovat k procesům a ne k pracovníkům zapojených do těchto procesů. To vyplývá z toho, že cílem auditu je zlepšit informační procesy a ne poskytovat podklady pro personální čistky. Jasné vysvětlení tohoto pravidla je základem pro dobrou spolupráci pracovníků prověřovaných oblastí.
- Auditor pouze zjišťuje skutečný stav a na základě svých zkušeností navrhuje případná nápravná opatření. Auditor v žádném případě nenahrazuje či nemodifikuje řídící rozhodnutí upravující poměry v prověřované oblasti. Jakékoliv řídící rozhodnutí přísluší pouze kompetentním řídícím pracovníkům. Auditor se nesmí stavět do role řídícího pracovníka, ukládat pracovní úkoly atd.

## Specifika hodnocení nákladů a efektivnosti zpracování

Hodnocení efektivnosti práce s informacemi představuje komplex problémů. Zjednodušeně lze říci, že auditor musí vhodně zvolit ukazatele pro měření nákladů i přínosů.

Měření nákladů představuje kompromis mezi exaktním měřením každé vynaložené koruny a pracnosti tohoto měření. Základní údaje poskytuje účetnictví. Z něj jsme zpravidla schopni zjistit celkové přímé náklady na výpočetní techniku (licenční poplatky, provozní materiál, personální náklady pracovníků odboru informatiky) a odpisy. Mnohem obtížněji se klíčují náklady na jednotlivé agendy. Prakticky nemožné je exaktně zjistit podíl personálních nákladů výkonných pracovníků, které spotřebuje provoz informačních systémů. Elegantní řešení představuje zavedení etalonu, ke kterému ze vztahují zjištěné hodnoty. Pak se problém vhodných ukazatelů redukuje na nalezení a popis relevantního etalonu. Vhodný etalon se snadno najde u agend, jejichž zpracování je obdobné v mnoha organizacích. Typickým příkladem je účetnictví, které je dnes prakticky ve všech účetních jednotkách zpracováváno pomocí počítače. Pak postačuje nalézt několik organizací s podobným počtem vstupních dokladů a podobnou organizační strukturou, zprůměrovat měřitelné parametry (počty pracovních míst, aktuálnost zpracování, počty mimořádných situací, provozní náklady, skladbu a distribuci výsledků) a vznikne etalon umožňující srovnání zjištěného stavu s průměrem.

Horší je situace v případě nestandardních organizací a nestandardních systémů, kde je velmi obtížné najít etalon. Potom nezbývá, než použít expertní odhad. V této situaci si auditor zhusta vypomáhá průměrnými ukazateli pro příslušná odvětví, která jsou k dispozici ze světové ekonomiky. Evropské průměrné ukazatele například dovolují porovnat investiční vybavení hardwarem a softwarem s evropským průměrem, ale většinou nedovolují porovnat přínosy. To souvisí s tím, že podle našich zkušeností z auditu jsou české podniky zpravidly vybaveny více a lepším hardware a novějším systémovým softwarem než je obvyklé v západní Evropě. Ale spolehlivost, stabilita a aplikační software je obvykle na výrazně nižší úrovni. A srovnávat efektivnost zpracování v případě nespolehlivých či neúplných dat je nevěrohodné. Proto v těchto případech je vhodné vždy zjišťovat, zda si pracovníci vedou tzv. ručně údaje paralelní k automatizovanému zpracování, protože existence paralelního ručního zpracování vždy signalizuje problémy automatizovaného zpracování. Druhým obvyklým testem pro ukazatel spolehlivosti a věrohodnosti zpracovávaných dat je porovnání výstupů z účetnictví s ekvivalentními systémy z jiných oblastí. Typickým příkladem je porovnání tržeb z účetnictví a z obchodních systémů, kde tyto údaje zpravidla souhlasí pouze v případě tzv. integrovaných balíků typu SAP/R3.

Z toho vyplývá, že pro stanovení ukazatelů měření efektivnosti je nezbytné nejdříve formou interview zjistit signály ukazující případné kvalitativní problémy zpracování. Pak lze po lokalizaci kvalitativních problémů stanovit ukazatele a zajistit jejich měření včetně hodnot ze srovnatelného etalonu. Následně je možno porovnáním s etalonem hodnotit nákladovou stránku informační podpory a její přínosy pro plnění hlavních úkolů organizace.

## Specifika prověrky bezpečnosti a spolehlivosti zpracování

Problematika bezpečnosti a spolehlivosti zpracování závisí v prvé řadě na požadavcích daných charakterem zpracování. Jiné budou požadavky v bance a jiné v zájmové organizaci. Pravidla bezpečnostních prověrek jsou známá a specifické postupy pro zjišťování bezpečnosti informačních systémů (z technického, organizačního i procedurálního hlediska) mají známá pravidla. V auditech se kromě klasických bezpečnostních problémů setkáváme s podceněním rizik vzniku a řešení mimořádných a havarijních situací. Prakticky v každém systému má některý hardwarový prvek poruchu a občas "spadne" aplikační nebo systémový software. Kromě poruch se běžně setkáváme se situací, kdy byl například zcizen osobní počítač anebo záložní diskety. Zpravidla zjišťujeme neexistenci bezpečnostní politiky, neexistenci pravidel pro řízení přístupu k datům, neexistenci periodických prověrek funkčnosti a správnosti obnovy při havarii systému. Je vyjímečné, pokud mají v podniku zpracovány a prověřeny postupy, co dělat v případě výpadku některého prvku zpracování a kdo nese odpovědnost za provedení nápravy. Jednoduchým testem je zjištění skutečného postupu

rekonstrukce zpracování při posledním výskytu hardwarové poruchy některého paměťového zařízení. Je běžné, že systém byl zprovozněn bez testů úplnosti a správnosti rekonstrukce a že rekonstrukci zajišťovali pracovníci výpočetní techniky bez kontrolních zásahů odborného garanta. I v systémech s vysokými požadavky na bezpečnost typu bankovního zpracování se občas setkáme s tzv. dvojitým anebo "zapomenutým" zúčtováním, které nezjistí vnitřní kontrolní systém banky a klient je nucen reklamovat zpracování. V podnikové sféře je měřítkem nestabilního zpracování například počet tzv. dodatečných přiznání DPH anebo tzv. dohledání skladových zásob, které signalizují problémy informační podpory podnikových procesů. Jiným projevem nepřesné informační podpory je zjištěná náročnost migrace dat při inovaci zpracování některé podnikové agendy, kdy všechny vícepráce vlastně opravují předchozí nedokonalé zpracování. Právě podobným signálům musí auditor věnovat pozornost, protože jejich analýza umožňuje nalézt příčiny nestability zpracování a navrhnout často jednoduchá opatření k jejich nápravě. Navíc škody způsobené nestabilním zpracováním lze poměrně snadno vyčíslit a tím současně objednateli poskytnout protihodnotu za náklady věnované na zpracování informačního auditu.

## Specifika zjištění stavu vnitřního kontrolního systému

Při dobře organizovaném zpracování funguje vnitřní kontrolní systém, který signalizuje problémy při zpracování informací. Součástí dobrého vnitřního kontrolního systému je nejenom signalizace problémů, ale současně "zažité" postupy pro jejich řešení. Dobrý vnitřní kontrolní systém je nejúčinnějším nástrojem pro trvalý růst kvality a spolehlivosti zpracování. Proto auditor musí u každého typu zjištěných problémů při zpracování prověřit, zda tento problém mohl, měl a skutečně zachytil vnitřní kontrolní systém. Analýzám případného nezachycení problému věnuje auditor zvláštní pozornost, protože příčinou nezachycení může být například nevhodná podniková kultura (nepřiznávání chyb), nedostatečná odbornost, nekvalitní hardwarový nebo softwarový produkt anebo celkově nesprávné pojetí a alokace kontrolního systému. Každá z těchto příčin má svá specifika a je úzce svázaná s osobní odpovědností, která často ukazuje až na objednatele auditu. Proto musí auditor zvláště pečlivě verifikovat každé zjištění, jinak zpochybní celý audit. Navíc musí mít auditor při analýze vnitřního kontrolního systému vždy na paměti, že veškerá svá zjištění vztahuje k procesům zpracování a ne k osobám, které toto zpracování zajišťují nebo jsou za něj odpovědné.

## Typické příklady z provedených auditů

V jednom středním podniku zabývajícím se službami občanům bylo zjištěno, že v tzv. předprivatizačním období bylo několik let řízení decentralizováno do jednotlivých závodů, které sídlily v jedné budově. Protože výběr a nákup výpočetní techniky probíhal po jednotlivých závodech, výsledkem byly rozdílné technologie počítačových sítí, rozdílné systémy pro zpracování účetních agend a rozdílné systémy pro zpracování obchodních agend. K tomu přibyla nadstavba slučující data z jednotlivých agend do souhrnného výsledku za podnik. Na základě doporučení vyplývajích z informačního auditu podnikové vedení rozhodlo o používání jediného systému pro účetní a finanční agendy. I když vznikly určité přechodové problémy s převodem dat a přeškolením pracovníků, za několik měsíců nejen klesly náklady na údržbu aplikačních programů (už se udržoval pouze jeden systém), ale odpadnutím slučovací nadstavby se zrychlily výsledky zpracování, kleslo riziko havarijních stavů a celkový stav provozních pracovníků napojených na tyto systémy poklesl o třetinu, protože bylo možno přesouvat špičky zpracování mezi závody. Tento výsledek by nebyl bez externího auditu možný, protože každý závod preferoval své řešení a odmítal přeškolení a převod dat. Úspěch sjednocení finančních agend ukázal výhody integrovaného zpracování a vedení podniku formulovalo informační strategii. Nová informační strategie nepreferovala nákup hardware a systémových prostředků, ale zaměřila se na sjednocení datové základny a její vyšší využití.

Dalším příkladem potřeby informačního auditu byla situace v jedné české dceřinné společnosti zahraničního nadnárodního koncernu, kde zahraniční vlastník prostřednictvím české počítačové firmy instaloval svůj informační systém. Po určité době provozu se systém zhroutil, protože nebyl schopen poskytnout seriozní informaci o skladovém hospodářství, objednávkách a odběratelích, přestože provozní obsluha byla početnější než v ekvivalentních pobočkách v jiných zemích a výkonnost hardware byla neustále posilována. Zahraniční vlastník stál před problémem, zda je systém špatně lokalizován a instalován, nebo je neschopná obsluha. Navíc ode všech českých pracovníků slyšel, že

chyba je v zastaralosti informačního systému, který údajně nešel účinně lokalizovat na nestandardní české hospodářské prostředí a že nákup moderního českého systému by odstranil veškeré problémy. Provedený informační audit zjistil, že systém byl lokalizován a nainstalován takovým způsobem, že například většinu výstupních sestav měla generovat provozní obsluha pomocí cizojazyčného generátoru typu RPG. Ta to nezvládala, takže sestavy pro závěrky a inventury dopočítávala ručně a tím způsobovala chybovost a zpoždění. Po nasazení specialisty, který vygeneroval typové výstupní sestavy se situace bez dalších investic stabilizovala. Kdyby nebyl včas proveden informační audit, docházelo by k zbytečným personálním výměnám provozní obsluhy a k neustálému posilování hardwarových komponent.

Skoro klasickým případem pozdního rozhodnutí o informačním auditu byl případ nefunkční rekonstrukce systému zpracování po havarii. V podniku byla podle vnitropodnikové směrnice archivace dat prováděna na pevné disky pracovních stanic každým uživatelem samostatně podle zásady "za data odpovídá uživatel". Stačil souběh odcizení několika počítačů v účtárně a poruchy disku na serveru a podnik několik týdnů neznal své hospodářské výsledky a jenom opakovaně typoval účetní doklady. Výsledkem byly nejen poruchy v hospodářském styku, ale také odložené přiznání k DPH. Samotná finanční škoda z pozdního uplatnění tzv. vstupního DPH několikanásobně převýšila škodu z odcizené techniky. Kdyby byl informační audit proveden včas, bylo možno této škodě zabránit.

Posledním příkladem úspěšného specializovaného auditu je bezpečnostní prověrka vyhrazené části lokální sítě zpracovávající citlivá data. Protože administrátoři sítě použili standardní názvy systémových funkcí a obsluha navzájem znala svá hesla z důvodu tzv. zastupitelnosti, bylo jednoduché simulovat neoprávněný přístup k datům. Na základě doporučení auditu byla provedena základní opatření pro zvýšení bezpečnosti.

## Závěr

Informační audit je specializovanou službou, která slouží ke zkvalitnění a racionalizaci informační podpory. U velkých organizací může tuto službu provádět oddělení vnitřního auditu za spolupráce odborníků z vlastního útvaru informatiky. U středních a menších podniků je efektivnější tuto službu zadat specializované organizaci, která má zažité postupy, zná etalony pro srovnání a není zatížena provozní slepotou a vnitropodnikovými vazbami. Při výběru vhodné organizace specializované na tento druh služeb je výhodné ověřit reference a garance, ověřit mlčenlivost, nezávislost a objektivitu zjištění. K tomu zpravidla postačuje nahlédnutí do návrhu smlouvy. Odborná způsobilost vhodné organizace je zpravidla doložena akreditací k provádění některého typu analogických prověrek a k poskytování expertních a znaleckých služeb. Pro volbu informačního auditora ale připomínám výše zmíněný právní stav, kdy informační audit, certifikát a expertní posudek může v podstatě vydat kdokoliv. Otázkou zůstává, jakou má provedený audit kvalitu a co organizaci přinese.

Kvalitně provedený informační audit přináší podnikovému vedení srozumitelný a plastický obraz reálného fungování informatiky a jeho srovnání se stavem u konkurence. Znalost skutečného stavu umožní v dalším kroku zadat konkrétní cíle v rámci podnikové informační strategie a současně vymezit optimální objem a strukturu prostředků pro jejich dosažení.

Ing. Zdeněk Vaněk, DCIT