Auditování založené na rizicích

Milan Trčka, NQA CZ, Jihlava

Zlepšování systémů managementu je povinné, avšak manažeři i auditoři berou požadavky posledního článku ISO 9001 často velmi formálně. Navíc nová norma ISO 9001 je v nedohlednu, mnoho organizací vyčkává nebo volí pohodlnou cestu „udržování systému v certifikovatelném stavu“. Co lze tedy pro zlepšení úrovně interních auditů udělat? Novela ISO 19011 umožňuje auditování založené na rizicích.

Systémy managementu vyžadují systematický a disciplinovaný přístup ke zlepšování. Významnou oblastí pro zlepšování je řízení programu interních auditů a jejich provádění. Příkladem správné praxe jsou dodavatelé v automobilovém nebo leteckém průmyslu či výrobci zdravotnických prostředků. Pro organizace s vyzrálým systémem řízení představují audity systému managementu základ, který následně rozšiřují o produktové audity a audity procesu. Interní auditoři se současně orientují jak na kvalitativní, tak i na kvantitativní výkonnost procesů. Procesně zaměřené audity monitorují a hodnotí dosažené výstupy (KPI), auditoři vyhledávají opakující se problémy, odhalují plýtvání u dodavatelů nebo řeší nízkou úroveň outsourcovaných služeb. Prostor pro zlepšování skýtá **auditování orientované na rizika,** které je nyní velmi aktuálním doplňkem výkonově orientovaných auditů.

Přidaná hodnota auditu rizik

Podstatou auditování založeného na rizicích je *hledání přidané hodnoty v celém systému řízení organizace*. Revidovaná norma ISO 19011 v příloze A nabízí interním auditorům integrovaných systémů řadu alternativ, zejména si mají osvojit:

- metody ošetření rizik (QMS, BCM),
- techniky stanovování rizik (EMS),
- techniky posuzování rizik (QMS, DM),
- řízení rizik nežádoucích událostí (BCM),
- posuzování rizik (identifikace a hodnocení aktiv; identifikace, analýza a hodnocení rizik) a analýzy dopadu (týkající se osob, aktiv a vlivu podnikání na životní prostředí; BCM, EMS, OHSAS),
- management rizik bezpečnosti informací (ISMS),
- určování způsobů řízení a komunikace o riziku (OHSAS),
- metody monitorování expozice a posuzování rizik bezpečnosti a ochrany zdraví při práci a typická nebezpečí a rizika odvětví (OHSAS).

Při provádění auditů systému managementu má být tým auditorů znalý principů managementu rizik, má disponovat dovedností v používání relevantních metod a technik, ale i vyhodnocovat a řídit rizika spojená s realizací programu auditů. Konkrétně audity systému managementu kvality (dále QMS) mají zohledňovat riziko nedodržení právních požadavků, které lze z pohledu ISO 9001 členit na požadavky zákonů a požadavky předpisů – viz tab. 1.

Tabulka 1 Rizika neplnění právních požadavků

Požadavky zákonů	Požadavky předpisů
Při výskytu rizika nejsou událost a její možné následky vyhodnocovány ve vazbě na nedodržení zákonů, vyhlášek a dalších právních norem formálně vydaných a schválených vládou, resp. ostatních legislativních požadavků daných právem (stát, EU).	Riziko představuje neznalost předpisů vyžadujících shodu s technickými požadavky, pravidly, zásadami nebo požadavky na používání.
Partneři a další zainteresované strany nejsou seznamováni s účinkem rozhodnutí vydaných správními orgány.	Není identifikováno riziko či ohrožení organizace týkající se vybavení, aktivit, funkcí, produktů či služeb.
Při auditech třetí stranou (ISO 17021) má být vyžadováno hodnocení souladu s právními požadavky, které se týkají celé organizace, včetně QMS.	Nejsou aktualizovány dokumenty stálé platnosti vydané dalšími institucemi, které k tomu dostaly zákonem oprávnění (inspekční orgány).
Nejsou dodržovány interní postupy organizace zavazující se k plnění požadavků zákonů.	Nejsou dodržovány interní postupy organizace zavazující se k plnění požadavků předpisů.

Management rizik není požadavkem ISO 9001, pouze čl. 0.1 stručně říká, že navrhování a implementace systému managementu kvality jsou ovlivňovány prostředím organizace a riziky spojenými se změnami jejího prostředí. Pokud definice řízení rizik představuje „snižující vliv nejistoty na dosahování cílů“, má vedení organizace v souladu s ISO 19011 zahrnout v programu auditů klíčové charakteristiky kvality produktů a služeb, nebezpečí a rizika bezpečnosti a zdraví a důležité environmentální aspekty a jejich řízení. Při auditu QMS lze dále zohlednit management rizik u následujících požadavků ISO 9001 podle tabulky 2.

Tabulka 2 Rizika v systémech managementu kvality (QMS)			
Požadavek ISO 9001	**Odpovědnost**	**Popis požadavku**	**Potenciální riziko**
5.1 Závazek managementu	Vedení organizace	Vedení se angažuje při uplatňování právních požadavků a stanovování cílů.	Přezkoumání rizik má obsahovat hodnocení požadavků odvětví nebo oboru a jejich srovnání.
5.4 Plánování		Vedení organizace stanovuje měřitelné cíle kvality, zaměřené na produkt.	Cíle nejsou v souladu s politikou kvality. Cíle nezajišťují stabilní kvalitu finálních produktů.
5.6 Přezkoumání vedením		Součástí hodnocení souladu s legislativou má být „posouzení nových a budoucích právních požadavků“.	Vedením není zvažováno předvídání právních požadavků. Aplikace analýzy vlivů a dopadů není důsledná. Nevyhodnocují se negativní události či nehody.
7.1 Plánování realizace produktu	Vlastník procesu plánování	Organizace musí určit cíle kvality a specifické požadavky na produkt.	Po rozpoznání rizik má být pochopena jejich povaha a v souladu s hodnoticími kritérii stanovena úroveň rizika.
		Musí být identifikovány kritické aktivity, procesy, funkce či závazné požadavky.	Proces hodnocení rizik má zvažovat obvyklé nehody či poruchy, které mohou vést k narušení kontinuity podnikání (havarijní či nouzové stavy a situace).
7.3 Návrh a vývoj	Vlastník procesu vývoje	Organizace musí specifikovat výstupy z návrhu a vývoje, tj. charakteristiky produktu, které jsou zásadní pro jeho bezpečné a správné používání.	Bezpečnost produktu – návody, značení, symboly; kapacitní testy a ověřování – zkracování odezvy na nehodu či incident (prevence – FMEA).
		Výsledný produkt musí být schopen plnit požadavky specifikovaného nebo zamýšleného použití.	Hodnocení shody není efektivní, zvyšuje se riziko neplnění požadavků na specifikované nebo zamýšlené použití.
8.5.3 Preventivní opatření	Vlastník problému	Organizace musí určovat potenciální neshody a jejich příčiny.	Není určeno, zda se riziko týká více produktů či produktových skupin, resp. stejného nebo více výrobních míst nebo částí organizace.

Tým auditorů se má při interním auditu ujistit, že vedení organizace ve výstupech z přezkoumání (tab. 2, 5.6) reagovalo na následující okolnosti, představující potenciální rizika:

- Změny strategií a politik.
- Organizační změny a změny řídicích procesů.
- Personální změny (zaměstnanci, dodavatelé).
- Změny v realizačních procesech (technologie).
- Změny v informačním systému (aplikační SW).
- Vliv změn na alternativní a krizové scénáře.

Rizika interních a zákaznických auditů

Nově je zavedena koncepce „auditování založeného na rizicích“, která má být aplikována již od přípravy a plánování programu auditů. Změny v plánování interních auditů vyžadují vyhodnocováni rizik spojených s vytvářením, zaváděním, monitorováním a přezkoumáváním programu auditu, která mohou ovlivnit dosažení cíle auditu. Všechny organizace, které provádějí interní audity v souladu s *Programem auditů*, mají zvážit, nakolik je vhodné přizpůsobit rozsah a četnost auditů dosahovaným výstupům, resp. zda má „osoba řídící program auditů“ (ORPA) doporučit změny programu a rozšířit jej o další neplánované audity. Řízení programu auditů má svá další úskalí:

- Osoba řídící program auditů má v souladu s novelou ISO 19011 doložit své kompetence a má být v postavení, které jí umožní nestrannost a objektivitu rozhodování.
- V malých organizacích neřídí auditor program a nesmí mít odpovědnost za auditovanou oblast.

Při prezentaci *Komentovaného vydání ČSN EN ISO 19011:2012* na semináři ČSJ vznikla procesní mapa nových a změněných požadavků k řízení a realizaci programu interních auditů – viz tab. 3, podtrhující význam ORPA.

Tabulka 3 Analýza procesu interních auditů SIPOC				
Dodavatel (KDO)	**Vstup (CO)**	**Proces (JAK/Aktivita)**	**Výstup (KDE/Monitoring)**	**Zákazník**
Osoba řídící program auditů	Výstupy minulých auditů	ŘÍZENÍ PROGRAMU AUDITŮ • Stanovení rozsahu • Identifikace a hodnocení rizik • Stanovování postupů	Schválený roční program auditů	Představitel vedení, manažer kvality (MK)
Vedoucí auditor, auditor, technický expert	Příručka systému managementu		Cíle systému managementu	
Správce dokumentace	Postupy pro interní audity		Přezkoumání vedením	Vedení organizace
Osoba řídící program auditů	Požadavky na ORPA	KOMPETENCE A HODNOCENÍ AUDITORŮ • Postupy pro hodnocení • Plánování osobního rozvoje auditorů	Kompetence ORPA	Představitel vedení, MK
Osoba řídící program auditů	Požadavky na auditory		Kompetence týmu auditorů	Představitel vedení, MK
Vedoucí auditor	Záznamy z minulých auditů	REALIZACE PROGRAMU • Cíle, předmět a kritéria auditu • Výběr metod • Výběr auditorů • Řízení výsledků auditů a souvisejících opatření (NOPO)	Plán auditu	Osoba řídící program auditů
Osoba řídící program auditů	Formuláře		Monitoring a hodnocení auditů	Představitel vedení, MK
Osoba řídící program auditů	Informace, data		Zprávy z auditu Registr NOPO	Představitel vedení, MK

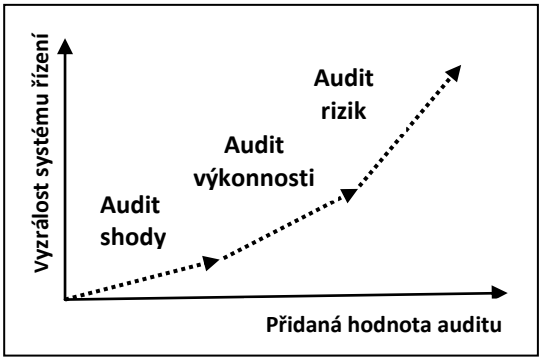
U auditů dodavatelů prováděných 2. stranou musí být určeny rámcové podmínky při plánování a organizování auditu, smluvně mají být vyjasněny podmínky u dodavatele:

- dohoda o ochraně důvěrných informací;
- povolení přístupu na výrobní místa (včetně dislokovaných pracovišť, resp. outsourcingu);
- předání výsledků třetí osobě (např. OEM).

Závěr: Výhledy do budoucna

Tradiční ***„audity shody systému“*** s ISO 9001 nejsou manažery vnímány příliš pozitivně. Otázky auditorů se příliš nemění: týkají se dokumentovaných postupů a souvisejících záznamů. Výsledkem je shoda nebo neshoda; takovéto audity ne vždy poskytují objektivní hodnocení organizace, požadované vedením.

Pokročilé organizace preferují „**auditování výkonnosti organizace**“, postavené na neustálém zlepšování klíčových procesů. Procesně orientované audity se zaměřují na postupy a procesy, výsledkem je ověření správnosti a efektivnosti procesů (KPI). Audity výkonnosti umožňují vedení optimalizovat procesy a více vnímat plnění specifických požadavků zákazníků či právních požadavků.



„**Auditování založené na rizicích**“ nabízí manažerům novou, proaktivní formu hodnocení organizace. Týmem interních auditorů musí být identifikovány výstupy monitorování procesního řízení, navíc však auditoři vyhledávají kritické aktivity, funkce či závazné požadavky. Po rozpoznání rizik může vedení organizace lépe reagovat na úzká místa systému řízení a zaměřit se na rizikové oblasti, které mohou vést k narušení kontinuity podnikání.

Autor:
Ing. Milan Trčka, ředitel a auditor certifikační společnosti NQA CZ, s. r. o.
Kontakt: *mtrcka@nqa.cz*