AUDIT ŘÍZENÍ RIZIK

Řízení rizik je nástroj, který umožňuje organizacím nejen lépe chápat své schopnosti a omezení, ale také identifikovat příležitosti k inovacím a posílení své pozice na trhu.
Na dalších řádcích se dozvíte, jak chápeme oblast řízení rizik v bance a jak přistupujeme k jeho auditování v Interním auditu KB. Začněme od začátku, respektive od naší mateřské instituce – IIA.

Ing. Lenka Landa Schejbalová, MBA
Výkonná ředitelka Interního Auditu KB

Po ukončení studií na Vysoké škole ekonomické, fakultě Finance a účetnictví, spojila Lenka svou profesní kariéru s francouzskou finanční skupinou Société Générale (SG). Začínala jako junior auditor v Komerční bance a po dvou letech odjela v rámci mezinárodní mobility do centrály SG v Paříži, kde nakonec strávila šest let na různých pozicích v rámci interního auditu. Nejdříve jako auditor a vedoucí mise pokrývala mezinárodní retailovou síť SG, poté jako auditní supervisor SG centrální funkce se zaměřením na compliance, a především na boj proti praní špinavých peněz a financování terorismu. Po návratu do České republiky vedla v rámci KB korporátního bankovnictví tým middle office strukturovaných transakcí, poté v týmu strukturovaného financování zastávala funkci Chief Operating Officer. V roce 2019 byla jmenována do pozice výkonné ředitelky pro interní audit KB, kde zaštiťuje tuto roli pro všechny společnosti skupiny KB a pro společnosti SG zabývající se specializovaným financováním (ALD, SGEF) ve střední Evropě.

Ing. Helena Raizl Jumrová, CGSS
Chief Operating Officer – Internal Audit KB

Po studiu fakulty Mezinárodních vztahů na VŠE získala své několikaleté profesní zkušenosti v EY, kde se věnovala převážně realizaci auditních zakázek různého charakteru. V Komerční bance pak jako Vedoucí auditor vybudovala tým se zaměřením na compliance rizika, především pak na praní špinavých peněz a financování terorismu. Je autorkou řady metodik, procesních změn a školí auditní praxi v Interním auditu KB, včetně uplatňování postupů Lean Six Sigma, jakožto držitel Green Belt. Na současné pozici COO navíc zastává organizaci chodu celého útvaru Interního auditu KB.

V této oblasti se dle IPPF – IIA Standardů od nás auditorů očekává, že zhodnotíme účinnost procesů, které mají řízení rizik ve společnosti zajišťovat. Půjdeme-li dál, nutnou součástí této oblasti je stanovení cílů společnosti, identifikace a hodnocení souvisejících rizik, stanovení opatření pro jejich řízení, a to vše doprovázeno získáváním a sdělováním informací napříč společností. A tím vzniká komplexní téma obzvlášť v systémové bance, jakou Komerční banka je.

„KB řídí všechna rizika nejen jako izolované jevy, ale jako součást celkového bankovního ekosystému“

Tak jako při provádění každé auditní zakázky si pojďme nejprve oblast zmapovat, a to v prostředí celosvětového bankovního domu Société Générale (SG). Pro tyto účely musíme zdůraznit interní instrukci tzv. SG Code, který reflektuje požadavky dané regulací v této oblasti a má za cíl stanovovat rámec pro veškeré činnosti spojené s řízením rizik ve všech svých dceřiných společnostech po celém světě. KB je tak členěna do tzv. tří linií obrany, jejichž jednotlivé struktury a procesy slouží k napomáhání dosahování cílů právě prostřednictvím optimálního nastavení řízení rizik. Uvedené vychází z „EBA Guidelines on Internal Governance“, který stojí na obdobných principech jako náš známým „The Three Lines Model“ z dílny IIA.

Podíváme-li se na oblast tzv. seshora, od cílů společnosti, najdeme jejich stanovení v rámci každoročně publikovaných dokumentů, které pro KB popisují klíčové strategické obchodní cíle a na ně navazující strategii řízení rizik.

KB uplatňuje **holistický přístup k řízení rizik**, což znamená, že KB řídí všechna rizika nejen jako izolované jevy, ale jako součást celkového bankovního ekosystému a řadí ho v rámci organizační struktury pod zodpovědnost jednoho člena představenstva. KB se, jako ostatně i další banky, potýká s typy rizik, jako jsou úvěrové, tržní, likvidity, operační – včetně IT, compliance atd. Důležitým úkolem této strategie řízení rizik je podpora obchodních aktivit banky, udržování a posilování její tržní pozice při zachování zdravé bilance.

Strategie řízení rizik je vypracována na základě principů uvedených v dokumentech Risk Appetite Statement a Risk Appetite Framework, které dále zpřesňují přístup a apetit k jednotlivým rizikům, včetně jejich konkrétního řízení a definice rolí a zodpovědností v rámci relevantních procesů v bance. Toto jsou tedy stěžejní a závazné dokumenty, ze kterých v rámci auditů týkajících se (nejen) řízení rizik auditní tým vychází.

Snahou je mít jednotnou terminologii a přístup k identifikaci a měření rizik. Pro identifikaci a měření rizik tak používá KB systém kategorizace činností/procesů, odpovídajících taxonomii rizik a kontrol, se kterými pracuje. Každá skupina rizik používá pro její hodnocení specifické nástroje a metody.

„Klíčovým atributem pro řízení rizik v bance je tzv. stress testing,“

Rizika jsou identifikována jak na bázi každodenního řízení procesů (sledování jejich klíčových indikátorů, limitů a prahových hodnot) a prostřednictvím specificky zaměřených výborů nebo v rámci zavádění/změny produktů či procesů.

Dále pak dochází k identifikaci a měření rizik prostřednictvím každoročních hodnocení jednotlivých skupin rizik napříč bankou, jako je například pro kapitálovou přiměřenost Internal Capital Adequacy Assessment Process (ICAAP), pro likviditu Internal Liquidity Adequacy Assessment Process (ILAAP), Risk Control Self-Assessment (RCSA) pro operační rizika, podobné cvičení banka provádí také nad riziky Compliance.

Klíčovým atributem pro řízení rizik v bance je tzv. stress testing, který má za cíl kvantifikovat veškerá materiální rizika pro KB a celou skupinu SG. Podstatou je modelování (extrémně) rizikových scénářů (např. související se změnou ekonomického prostředí) a určení úrovně daného rizika. Jsou pak významným zdrojem pro stanovování opatření k jeho snížení, např. nová rozhodnutí týkající se skladby portfolia.

Důležitým aspektem pro auditní činnost je správné určení **„ultimátních vlastníků rizik“**, jelikož komplexnost procesů v bance, které prostupují napříč organizací, vyžaduje nezbytnou spolupráci a koordinaci skrz banku, a to jak její „run“ částí, tak její částí „change“.

Interní audit Komerční banky kopíruje z velké části organizaci řízení rizik v bance, jednotlivé auditní týmy jsou specializované na nejmateriálnější rizika, se kterými banka pracuje. Tedy auditní tým specializující se na řízení kreditních rizik, jiný tým zaměřující se na rizika compliance s dalším specifických zaměřením např. na rizika spojená s praním špinavých peněz a financování terorismu, tým IT expertů, tým pokrývající operační rizika či rizika spojená s investičním bankovnictvím. Tyto týmy budují expertizu nejen dle jednotlivých rizik, ale také dle specifických aspektů těchto rizik v jednotlivých společnostech Skupiny KB, jako např. KB Penzijní společnost, ESSOX, SGEF, ALD nebo Faktoring KB. Auditor se tak postupně stává odborníkem znalým jak regulace, tak i její aplikace v praxi, a navíc v různých obchodních modelech.

Ve své podstatě se každý audit zaměřuje na řízení rizik v bance. Audit řízení rizik může mít mnoho podob, může probíhat přes různé řídicí linie, může se zaměřovat na kontrolní body

Lenka Landa Schejbalová

v konkrétních procesech, může pokrývat nastavení celkového řídicího rámce. Obecně v Interním auditu KB využíváme následující přístupy, pomocí kterých dosahujeme potřebného pokrytí:

- **Celkové tzv. governance řízení rizik** v bance anebo nastavení řízení konkrétního významného rizika, a to nejen v rámci banky, ale také v rámci celé finanční skupiny. Jako příklad můžeme uvést audit zaměřený na samotný model tří linií obrany v KB a jeho soulad s regulatorikou, s nejlepší praxí, jeho reálným fungováním a jeho vyspělostí. Dalším příkladem je audit řízení kreditního rizika, kdy se zaměřujeme na nastavení pravidel pro řízení kreditního rizika, jejich soulad s regulatorními požadavky, jejich nasazení na nižších úrovních řízení a v jednotlivých společnostech skupiny. Auditní činnosti se dále mohou zaměřit na další detailní nastavení a funkčnost dílčích klíčových pravidel a kontrolních mechanismů jako například na kvalitu datových toků nebo monitoring a reporting klíčových ukazatelů zásadních pro přijímání informovaných rozhodnutí managementu banky.

- **Procesní audit**, který se může zaměřovat na celý proces (tzv. „end-to-end“) nebo jen na jednu jeho např. specificky rizikovou část. Klíčové je zde detailní pochopení kontextu a celkového fungování daného procesu. Na těchto auditech máme často možnost nejvíce využít pro tyto účely nástroje Lean Six Sigma, které nám pomáhají se lépe zaměřit na rizika související s kvalitou a výkonností daného procesu. Příkladem může být procesní audit produktového charakteru, třeba poskytování bankovní záruky, kde hodnotíme veškerá rizika v procesu, tedy ze všech kategorií (operační riziko, riziko udržitelnosti procesu, související IT rizika používaných systémů atd.), přičemž z charakteru produktu je nejvýznamnějším riziko kreditní. Nebo audit pokrývající klíčový bankovní proces, jako je například přijetí klienta do banky a jeho proces z bankovního pohledu tzv. KYC („poznej svého klienta“). V tomto případě bude audit zaměřen především na řízení rizika compliance.

- **Tematické či post-implementační audity** uplatňujeme v případě implementace nové regulace zasahující do řízení významného rizika, např. GDPR ovlivňující řízení a monitoring compliance rizik nebo v případě Zákona o kybernetické bezpečnosti by se jednalo o audit řízení rizik spojených s informačními systémy. K takovýmto auditům přistupujeme i v případě, že dochází k zavedení nových systémů a nástrojů v jednotlivých procesech banky, které jsou pro daný proces zásadní změnou, která je nositelem možných rizik.

„Důležitým aspektem pro auditní činnost je správné určení ‚ultimátních vlastníků rizik‘.“

Nutno dodat, že významnost jednotlivých naplánovaných auditů v daném roce vychází z každoročního hodnocení rizik (risk assessment).

Klíčová je pro nás pravidelná komunikace s managementem banky, tzv. pravidelný monitoring, který nám umožňuje získávat informace i mimo audity, jehož prostřednictvím můžeme reflektovat změnu v navrženém systému pokrytí pro daný auditní rok na základě změny rizikového profilu banky.

Při realizaci již konkrétního auditu pak postupujeme standardním způsobem, kdy po tzv. diagnostické fázi, jejíž součástí je vyhodnocení námi identifikovaných rizik v rámci auditované oblasti, stanovení cílů, rozsahu ověření za použití jednotlivých auditních metod, které vycházejí z IIA Standardů, při použití pokročilé datové analýzy či datové vědy, bez ohledu na odvětví, ve kterém auditujeme. Naším konečným výstupem je tradiční závěrečná zpráva hodnotící silné a slabé stránky v řízení oblasti, a konečně názor na účinnost řízení rizik.

Řízení rizik v bance je jako pohled na skládanku, kde jednotlivé dílky tvoří součásti většího obrazu. Banka, a ostatně i my, auditoři, se snažíme pochopit, jak tyto dílky spolu souvisejí a interagují, a jak mohou ovlivnit celkovou stabilitu a obchodní úspěšnost banky. ■

Helena Raizl Jumrová