EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

1MT302
Učební text
Část: Operační riziko

Shrnutí

- Postavení operačního rizika v rámci bankovních rizik je specifické. Je obtížně identifikovatelné, kvantifikovatelné a jeho možnost výskytu je významně široká.
- S tím souvisí i specifické postupy jeho měření, které korespondují s regulatorními postupy i řízení, které počítá s angažovaností (zjednodušeně formulováno) všech pracovníků banky.
- Pro operační riziko je specifický jeho „plošný", průřezový výskyt napříč všemi vnitřními procesy.
- Měření operačního rizika je spjato s regulatorními požadavky.
- Postupně jsou analyzovány: přístup základního indikátoru, standardizovaný a alternativní standardizovaný přístup, a nakonec je detailně rozebrána oblast tzv. pokročilých přístupů měření včetně kvalifikačních požadavků a souboru metod, které lze použít k propočtu kapitálového požadavku k operačnímu riziku.

Vymezení operačního rizika

Spolu s nástupem regulatorního konceptu kapitálové přiměřenosti Basel II se do popředí zájmu bank dostalo *riziko operační*, dříve v podmínkách České republiky častěji označované jako *riziko provozní*. Jde o druh rizika, kterému je banka vystavena, jakmile začne provádět operace jakéhokoliv druhu. Formalizovaný přístup k řízení operačního rizika lze vysledovat až s počátkem tvorby koncepce Basel II, kdy byl popsán výchozí stav (blíže BCBS *Operational Risk Management,* Basel*, 1998),* necelý rok před vznikem prvního konzultativního materiálu k Basel II (BCBS 1999*).*

Operační riziko existuje v bankách od počátků jejich fungování, jeho podstata se ale výrazně měnila a mění se změnami vnitřních procesů v bance, se změnami vnějšího prostředí a hrozeb z něj vyplývajících. Významný dopad do podoby operačního rizika má vývoj informačních technologií a s ním korespondující bankami užívané systémy. Změny jsou například výrazně patrné u postupů obchodování, provádění platebních operací, zavádění nových produktů.

Původně se dávalo toto riziko do souvislosti především s lidským faktorem, resp. jeho vědomým či nevědomým selháním a se selháním informačních technologií. Patrně nejpoužívanější a nejznámější vymezení operačního rizika vychází z vymezení Roberta Morrise Associatese[1] (1999) a je v podstatě identické s později formulovanou definicí v rámci Basel II, pouze s tím rozdílem, že Basel II nezahrnuje nepřímé ztráty, resp. členění ztrát na přímé a nepřímé, kvůli obtížné kvantifikaci regulatorního kapitálu. Ztráty přímé, které mají svůj obraz ve finančních výkazech, zahrnují všechny ztráty související s materializací operačního rizika kromě ušlého zisku, nákladů příležitosti. Nutné je také vyčlenit náklady související s realizací postupů cílených na snížení operačního rizika.

Při vymezení operačního rizika lze také vyjít z uplatnění dělení operační riziko na 5 základních kategorií, které se dále detailněji specifikují zavedením 20 podkategorií. Nejde o regulatorní, ani statický pohled na vymezení operačního rizika, ale předpokládá se, že průběžně může docházet ke změnám ve smyslu přiřazení, rozšíření či vyčlenění podkategorií v souladu s přijatými technikami řízení – viz Tabulka č. 1. A konečně tzv. CRR, Nařízení Evropského parlamentu a Rady (UE) č.575/2013 ve znění Nařízení Komise

[1] Operační riziko je přímá nebo nepřímá ztráta, která je výsledkem selhání interních procesů, personálu a systémů nebo následek externí události.

v přenesené pravomoci (EU) 2018/405 chápe operační riziko jako riziko ztráty, které vyplývá z nedostatků či selhání vnitřních procesů, osob a systémů nebo z vnějších událostí, a zahrnuje právní riziko. V této souvislosti jsou banky povinny zavést zásady a postupy pro hodnocení a řízení expozice vůči operačnímu riziku, včetně rizik modelů a pokrytí méně četných, ale vysoce rizikových událostí. Pro účely těchto zásad a postupů instituce jasně zformulují, co tvoří podstatu operačního rizika.

Tabulka č. 1 Kategorie a podkategorie operačního rizika

kategorie	**podkategorie**
Organizace	Struktura
	Firemní kultura
	Firemní komunikace
	Projektový management
	Outsourcing
	Plánování kontinuity podnikání
	Bezpečnost, narušení
Firemní politika a procesy	Interní politika a procesy
	Dodržování interní politiky a procesů
	Produkt
	Klient, pochybení v jednání
Technologie	Komunikace, selhání
	Hardware a software, poruchovost
	IT bezpečnost, narušení
Lidé	Zaměstnanec, vědomé i nevědomé selhání
	Zaměstnavatel, nedostatečné školení
	Konflikt zájmů
Externí události	Fyzické zabezpečení organizace
	Soudní spor
	Podvod, vnější napadení

Zdroj: autor

Lze se setkat s širokým vymezením, kdy se jako operační chápou veškerá rizika, která stojí mimo úvěrové riziko a rizika tržní. Murmann a Otkem (2002) vnímají operační riziko jako všechny typy nekvantifikovatelných rizik. Právě široké pojetí bylo užitečné jako východisko pro konkrétnější vymezení operačního rizika. Zkušenosti z finančních trhů přispěly ke snaze dostat pod kontrolu ztráty, které byly výsledkem materializace rizikových událostí, které nevznikly ani z titulu úvěrového rizika, ani se nejednalo o důsledky rizik tržních. Informace o těchto ztrátách byly poté roztříděny podle příčin jejich vzniku do základních kategorií, které byly základem vymezení jako rizika ztráty z narušení transakce, nedostatků a chyb v kontrole a v důsledku jiných vnějších událostí (blíže Hoffman, 2002). Cílem snah BCBS bylo dosáhnout konsenzu ve vymezení operačního rizika, což se postupným zpřesňováním verzí koncepce Basel II (BCBS 2001 a BCBS 2004).

Specifika operačního rizika a typy událostí

Specifikem rizika je významná destruktivnost, nesnadná možnost předvídatelnosti, a s tím související obtížná identifikace, měření a řízení. Řízení operačního rizika bylo dříve součástí jiných procesů, jeho řízením se nezabývaly samostatné útvary, chyběla koncepce. Banky neměly vypracovány přístupy, které by jim umožňovaly promítnout úroveň operačního rizika do kapitálu. Za hlavní příčinu vzniku událostí charakteru operačního rizika byly považovány neadekvátně nastavené kontrolní mechanismy. Jen velmi málo bank se zabývalo nastavením procesu evidence událostí operačního rizika. S příchodem Basel II je operační riziko vnímáno jako riziko ztrát, způsobených neadekvátností či selháním interních procesů, lidí a systémů anebo vlivem externích událostí a banka je povinna vůči němu držet kapitál (BCBS, 2004). Zatímco u finančních rizik typu úvěrového či rizik tržních je evidentní vztah k portfoliím banky, operační riziko má přímou vazbu na její procesy.

Vymezení zahrnuje *riziko právní*, neobsahuje ale *riziko reputační a strategické*, kde jsou ovšem významné vazby na riziko operační. Riziko právní je rizikem ztráty banky v důsledku porušení nebo neplnění právní normy. Spočívá tedy v nenaplnění právní normy nebo v jejím porušení a má vztah k vymahatelnosti práva. Banky sledují riziko v oblasti compliance – riziko nesouladu se zákony. Riziko reputační souvisí s nezvládnutím některého ze škály rizik, kterému je banka vystavena, nejužší vazbu má na riziko operační. Je hrozbou pro tržní hodnotu banky především jako výsledek materializace operačního rizika, k němuž by měly banky zaujímat postoj nulové tolerance. Tím, že riziko reputační negativně ovlivňuje dobré jméno instituce a banka potřebuje disponovat kredibilitou, může ji ztráta dobrého jména významně poškodit a ovlivnit její postavení na finančních trzích. To je jedním z významných důvodů, proč banky před aplikací Basel II nepřipouštěly možnost výskytu operačního rizika a neinformovaly o postupech, které uplatňují vůči jeho omezení (analogii lze najít například v medicíně, kde také při určitém úhlu pohledu tomuto oboru neprospívá postoj určité míry netransparentnosti a omezeného sdílení nezdarů či nedostatků při uplatňování medicinských postupů). Při řízení operačního rizika je nutné souběžně řešit i riziko reputace, a to včetně vyčlenění ekonomického kapitálu. Strategické riziko souvisí se špatně zvolenou či nevhodně implementovanou strategií. Samo prosazování zvolené strategie, resp. změna dosavadní strategie vyvolává požadavky na nové či modifikované procesy, systémy, a to způsobuje tlak na dovednosti a znalosti zaměstnanců.

Každá banka má možnost vymezit si operační riziko podle svých potřeb, pokud jako výchozí vnímá vymezení dané příslušným regulatorním předpisem. Nutnou podmínkou pro řízení operačního rizika je

transparentně a jednoznačně definovaná organizační struktura a přesně vymezené povinnosti jednotlivých zaměstnanců a orgánů společnosti.

Vymezení operačního rizika konkretizují *typy událostí operačního rizika*. Jde o sedm základních kategorií, které se na začátku platnosti této regulatorní normy dále členily na podkategorie. V současně platných pravidle jsou podkategorie nahrazeny výkladem každé kategorie. Jejich význam spočívá ve snaze zajistit konzistenci při vyhodnocování operačního rizika v různých bankách. Ale i při zavedení typologie není aplikace typů událostí zcela jednoznačná, prvek subjektivity posuzování událostí nelze zcela vyloučit. Mohou existovat události, u kterých nebude kategorizace jasná a banka přistoupí k subjektivnímu posouzení. Jeden typ ztrátové události může mít více příčin. Obtížné je také vymezení ztráty. Kromě přímé ztráty například ve formě poskytnuté kompenzace klientovi, lze předpokládat také ztráty nepřímé ve formě ušlého zisku[2], pokud dotčený klient situaci vyhodnotí tak, že od banky odejde. Tyto ztráty s vysokou pravděpodobností v reakci na projevy operačního rizika mohou nastat, ale regulatorní postupy s nimi nepracují (BCBS, 2006). Vyjádření ztráty z operačního rizika je ve srovnání s vyjádřením ztráty z titulu úvěrového nebo tržního rizika komplikovanější. Lze ji chápat jako dopad do hospodářského výsledku banky z titulu materializace operačního rizika.

Příklady možných událostí operačního rizika, které mohou v bance nastat a které mohou vést k dopadu do hospodářského výsledku banky:

- Nepovolené transakce, nadlimitní obchodování
- Nedostatky v oceňování aktiv
- Prodlení v dodání aktiv spolu s nepříznivým vývojem tržní ceny daného aktiva
- Špatně formulovaná smlouva o vzájemném započtení pohledávek
- Chyba při směrování plateb a následné neúspěšné vymáhání
- Odškodnění klienta z důvodu zpoždění ve vypořádání transakce
- Odpisy hmotného majetku z titulu přírodní pohromy (povodně, požár)
- Špatné právní zajištění poskytnutého úvěru

Tab. č. 2 Typy událostí operačního rizika

Typ události	**Definice**
Interní podvod	Ztráty způsobené jednáním, jehož úmyslem je podvodně připravit o majetek, zpronevěřit jej nebo obejít předpisy, zákony či firemní zásady, vyjma případů diskriminace nebo sociální a kulturní odlišnosti, kterého se účastní alespoň jedna interní strana.
Externí podvod	Ztráty způsobené jednáním třetí strany, jehož úmyslem je podvodně připravit o majetek, zpronevěřit jej nebo obejít zákon.
Postupy při zaměstnávání a	Ztráty způsobené jednáním, které je v rozporu se zákony nebo dohodami týkajícími se zaměstnávání, ochrany zdraví a bezpečnosti, ztráty způsobené platbami z důvodu újmy na zdraví nebo z důvodu diskriminace či sociální a kulturní odlišnosti.

[2] Jde o projev vazby na reputační riziko.

bezpečnost na pracovišti	
Klienti, produkty a obchodní postupy	Ztráty způsobené neúmyslným jednáním nebo nedbalostí, v jejichž důsledku nebyl splněn obchodní závazek vůči některým klientům (včetně požadavků důvěrnosti či přiměřenosti jednání) nebo ztráty způsobené povahou nebo formou produktu.
Škody na hmotném majetku	Ztráty způsobené ztrátou nebo poškozením hmotného majetku přírodní katastrofou nebo jinými událostmi.
Přerušení obchodní činnosti a selhání systému	Ztráty způsobené přerušením obchodní činnosti nebo selháním systému.
Provádění transakcí, dodávky a řízení procesů	Ztráty způsobené chybami při zpracovávání transakcí nebo při řízení procesů, ztráty plynoucí ze vztahů s obchodními protistranami a dodavateli.

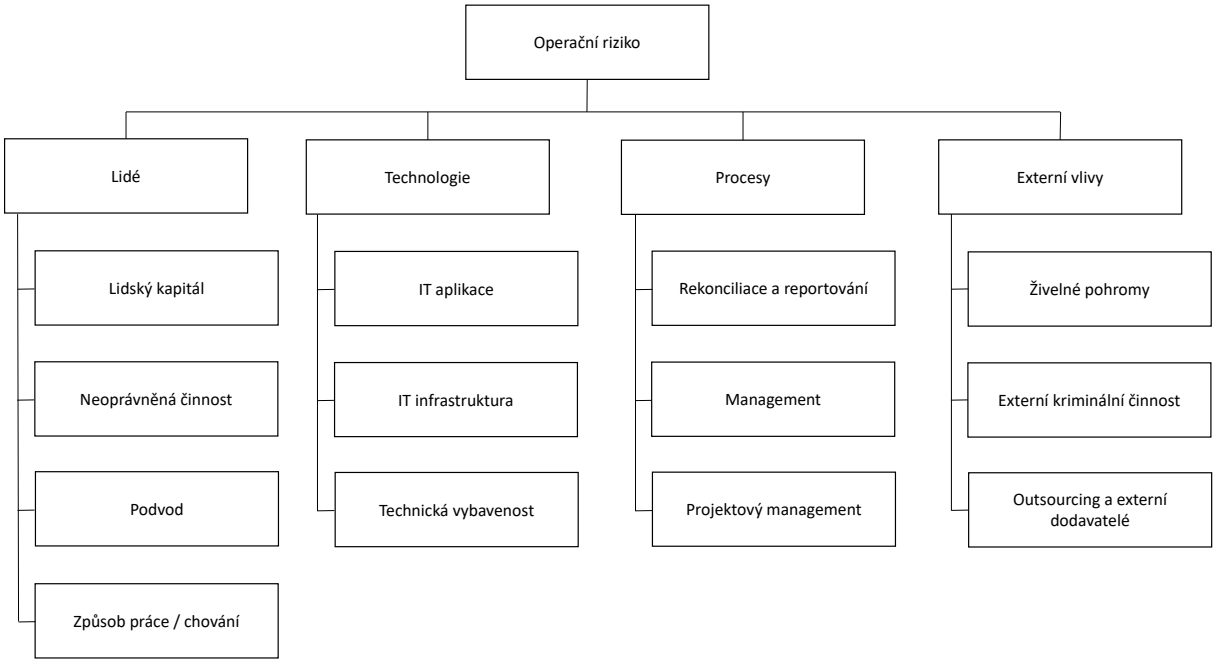
Zdroj: CRR

Hlavní zdroje operačního rizika

Od výše uvedeného vymezení operačního rizika se odvíjí identifikace hlavních zdrojů rizika. Následující text vychází z těchto podkategorií operačního rizika:

- Procesní riziko
- Riziko selhání lidského faktoru
- Riziko systémů
- Riziko externích událostí

Obrázek č. 1: Struktura operačního rizika podle zdrojů rizika



Zdroj: autor

Procesní riziko

Procesní riziko neboli *riziko nedostatku či selhání interních procesů* se projevuje neefektivními nebo nedostatečnými vnitřními procesy, což se manifestuje nekompetentními chybnými rozhodnutími, chybně nastavenými rozhodovacími, realizačními a kontrolními procesy. Míra efektivnosti nastavení vnitřních procesů v bance významně ovlivňuje celkovou úroveň operačního rizika, kterou banka podstupuje. Nevhodně či nedostatečně nastavené procesy nadměrně zvyšují náklady a nevedou k dosažení cílů optimální cestou. Typicky celý transmisní mechanismus procesu tvorby nového produktu nebo služby, výzkum trhu, určení ceny, zhotovení kompletní dokumentace s veškerými vazbami na ostatní činnosti v bance (mj. např. účtování o produktu), prodej produktu, dodržení smluvních podmínek kontraktu. Špatné nastavení procesu může generovat finanční ztráty, vyšší nároky na kapitál, ztrátu klientů, soudní spory, snížení reputace banky.

Pokud se koncipuje nový proces, je důležitým parametrem pokrytí všech fází transmisního mechanismu, adekvátní nastavení kontrolních mechanismů a vhodná návaznost, případně jistá míra překrytí činností tak, aby byl proces zcela pokryt, začleněn.

Do oblasti nedostatků či selhání vnitřních procesů se řadí obchodní spory a nedostatky. Patří sem také oblast bezpečnosti a ochrany zdraví při práci, diskriminace.

Riziko selhání lidského faktoru

Riziko selhání lidského faktoru souvisí zejména s nedodržením nebo porušením ustanovení vnitřních předpisů, úmyslným jednáním zaměstnanců nebo externích osob s cílem poškodit banku nebo její klienty, lze sem zařadit také pracovně právní spory. Selhání může být jak úmyslné, tak neúmyslné.

Škála možných selhání lidského faktoru je poměrně široká. Mezi hlavní faktory spouštějící selhání se řadí nejednoznačná role pracovníka v daném procesu, nejednoznačné vymezení práv a povinností spojených s danou pracovní pozicí, nerespektování principu neslučitelnosti funkcí při tvorbě organizační struktury banky. Významné škody se generují nepovoleným obchodováním na finančních trzích. Firemní kultura, která nezahrnuje prevenci rizikových situací a v případě materializace rizik nemá v adekvátní míře zpracovány postupy jejich řešení, působí rovněž jako spouštěcí mechanismus a může vyvolat řetězení incidentů typu systémové bezpečnosti nebo ohrožení právní odpovědnosti nebo „jen“ snížení produktivity práce.

Omezení vzniku událostí operačního rizika související s rizikem selhání lidského faktoru má úzkou vazbu na kvalitu práce s lidskými zdroji, systémem vstupních a pravidelných interních školení s cílem zvýšit kompetentnost zaměstnanců, jejich znalosti, odpovědnost a profesionalitu. Důležitý je také systém vnitřních kontrol, který významně omezí nepovolené aktivity pracovníků, které mohou vést k nerespektování vnitřních předpisů nebo právních norem. Zde jde o jednání typu krádež, zpronevěra, podvod, zkreslování výkaznictví, kdy se pracovníci banky mohou podílet na takovém konání v kombinaci s jedinci z vnějšího prostředí. Důležité je usilovat o maximální snížení časového zpoždění mezi vznikem události a jejím odhalením. Banky s ohledem na zachování potřebné reputace mají snahu nesdělovat události tohoto typu veřejnosti.

Mezi faktory zvyšující riziko selhání lze zařadit také vyšší míru fluktuace zaměstnanců, která může generovat vyšší přetížení stávajících pracovníků a zvýšení jejich chybovosti. Spouštěčem mohou být i časté organizační změny, přílišný tlak na zaměstnance, nedostatek pracovníků obecný či pouze přechodný (vazba např. na období chřipkových epidemií apod.).

Riziko systému

S rostoucím významem informačních technologií v činnostech banky roste i význam rizika interních technologických systémů, resp. nedostatku nebo selhání technologických systémů. Informační systémy, které banka používá, musí splňovat řadu kritérií. Především musí efektivně podporovat činnost banky, musí být zabezpečené vůči neautorizovanému používání, nesmí omezovat svou kapacitou rozvoj aktivit banky, musí umožňovat plynulost provozu jejích činností. Banky stále sofistikovaněji chrání své systémy, které přesto zůstávají zranitelné. Prolomením bezpečnostního systému banky hrozí neautorizovaný přístup, nedostupnost dat. Může dojít ke zneužití internetového bankovnictví. Jde o neustálý konflikt mezi schopnostmi hackerů a vývojem bankovních systémů. K omezení tohoto rizika je nezbytné, aby zaměstnanci banky striktně respektovali interní předpisy, využívali pouze povolené postupy. Do této kategorie rizika se řadí přerušení dodávky elektřiny, výpadky telekomunikačních systémů, výpadky zabezpečovacích systémů, hackerství, phishing[3], ale také například nesprávně nastavené finanční modely.

Riziko externích událostí

Ve smyslu operačního rizika jde především o události externích podvodů ze strany klientů či obchodních partnerů, napadení pracoviště banky, přírodní katastrofy typu povodní, vandalismus,

[3] Phishing je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci.

terorismus. Svou povahou by se sem dala zahrnout také problematika praní špinavých peněz jako jeden ze způsobů legalizace výnosů z trestné činnosti. Specifickým problémem může být outsourcing, u kterého platí, že banka i nadále nese plnou odpovědnost za služby, které jsou předmětem outsourcingu. Můžeme sem zahrnout nedostatečně ošetřené havarijní plány a krizový management, přímé poškození majetku společnosti), problémy na straně dodavatelů zboží nebo služeb.

Řízení operačního rizika

Řízení operačního rizika je vymezeno Akkizidisem a Bouchereauem (2005) jako systematická aplikace řídících principů, kritérií a nástrojů s cílem optimalizovat veškeré aspekty bezpečnosti v kontextu operační efektivity, času a nákladů, a to průřezově veškerými operačními fázemi. Je vhodné dodat, že tento přístup koresponduje s porovnáváním potenciálních nákladů plynoucích z případné materializace operačního rizika s benefity souvisejícími s absencí řízení operačního rizika. Alvarez (2005) připomíná, že pokud chce banka efektivně řídit celou škálu operačních rizik, aplikuje proces řízení operačního rizika v celé bance a integruje jej o procesy řízení rizik ostatních. To mimo jiné eliminuje nutnost provádění samostatného auditu, banka sníží výskyt událostí operačního rizika, resp. zvýší svou výnosovou marži. Banka musí disponovat strategií řízení rizik, jejíž součástí je i strategie v oblasti rizika operačního, a tato strategie je schválena na nejvyšší úrovni banky. Banka je povinna v souladu s požadavky regulace vytvořit a průběžně udržovat, vyhodnocovat a případně revidovat *systém řízení* operačního rizika, který musí zahrnovat: vymezení, cíle řízení, zásady řízení, postupy řízení, pravomoci, odpovědnosti a informační toky při řízení na všech řídících úrovních, informace o událostech a ztrátách vzniklých jako důsledek operačního rizika, nastavení prahu významnosti, a tím určení akceptované tolerance banky k operačnímu riziku.

Proces řízení operačního rizika je koloběh fází, které lze zjednodušeně popsat následovně: pokud dojde k výskytu a identifikaci operačního rizika, musí dojít k jeho následnému změření, které je vstupem k analýze, monitorování a reportování, a to v závislosti na velikosti a významu rizikové události a při respektování prahů významnosti. Poté je určen kapitálový požadavek a riziko se dále stává předmětem procesu řízení. Procesy řízení lez popsat podrobněji, modifikovaně. Existují minimální standardy řízení operačního rizika od BCBS, které je třeba respektovat.

Identifikace a sběr událostí operačního rizika

Na počátku procesu řízení operačního rizika je nezbytné vybudovat *systém pro identifikaci a sběr událostí* operačního rizika při zahrnutí veškerých relevantní informací vztahujících se k událostem charakteru operačního rizika, který bude sloužit v různých fázích řízení (např. měření, monitorování, reportování) jako databáze. Jde o nutnost formalizovat pravidla této fáze řízení. Vzhledem k tomu, že pro operační riziko je specifický jeho „plošný“, průřezový výskyt napříč všemi vnitřními procesy, je důležité při budování systému sběru událostí dbát na to, aby byl systém uživatelsky příznivý, snadno pochopitelný a fungující s minimálním časovým zpožděním mezi vznikem události a její evidencí. V této souvislosti je nezbytné *uživatele*[4] důkladně *proškolit*, jak se systémem zacházet, jak do něj zadávat

[4] Na rozdíl od ostatních rizik je okruh „uživatelů“ značně široký.

informace o událostech operačního rizika. Nezbytné je vytvořit *motivační program*, který podpoří ochotu spolupracovat a omezí chybovost při vytváření relevantních informací. I tak je vhodné systém z hlediska chybovosti zadávání událostí, resp. jejich správnosti nezávisle a pravidelně kontrolovat. V praktické rovině banka postupuje tak, že využívá auditorské zprávy, názory poradenských firem, komunikuje se zaměstnanci a analyzuje procesy.

Tabulka č.3 Údaje o událostech operačního rizika

Základní údaje	**Doporučené údaje**
Datum zjištění události, resp. jejího záznamu do systému	Druh ztráty podle dopadu do hospodářského výsledku
Popis (stručně, výstižně) a příčina (např. nedostatečná kontrola, informační technologie, selhání zaměstnance…)	Datum případné kompenzace nebo navýšení ztráty
Místo události (obchodní linie), případně bližší lokace (např. potvrzení transakce, stanovení ceny…)	Výše kompenzace nebo navýšení ztráty
Typ události, kategorie	Druh kompenzace/navýšení ztráty
Celková původní výše ztráty	Datum navýšení původně určené ztráty
Případné zajištění rizika (např. pojištění…)	Hodnota navýšení ztráty operačního rizika
Jak a kým (pracovní pozice) byla ztráta zjištěna	Jaký indikátor byl aktivován[5]

Zdroj: autor

Data do databáze lze zadávat manuálně a automaticky. Způsob manuálního zadávání musí eliminovat riziko chybného zadávání, a proto je vhodné připravit pro zaměstnance každé obchodní linie formulář, který je opatřen návodem, je jednoduchý, má přednastavenu škálu hodnot a před uložením do databáze jej prověří a schválí pracovník, který je k této činnosti určen. Automatické zadávání dat vychází z možnosti přístupu do jiných databází. Jde o interní databáze i externí databáze ztrát.

Například je známo, že operační riziko se může zaměňovat za riziko úvěrové. Jednak je třeba napříč bankou zabránit duplicitám při započítávání rizika tudíž nadbytečné alokaci kapitálu, jednak je třeba určit příčinu rizika. Pokud banka na základě nesprávných údajů poskytne úvěr klientovi, který jej následně není schopen jej splácet, pohledávka banky se stane po jisté době pohledávkou v selhání, banka bude nucena (po zohlednění zajištění) k ní tvořit opravnou položku. Negativní dopad do hospodářského výsledku se bude jevit jako následek úvěrového rizika. Na počátku byla ale událost operačního rizika typu podvodného jednání ze strany klienta.

[5] Klíčové indikátory rizika (KRI) popsány blíže na straně….

Identifikace zdrojů rizika

Na rozdíl od řízení jiných bankovních rizik, toto riziko je třeba řídit napříč celou bankou a v podstatě do jeho řízení začlenit všechny pracovníky banky, protože mají ve vztahu k pracovní pozici, kterou zastávají, vazbu na potenciální události operačního rizika. Rozpoznání operačního rizika je soustavnou činností probíhající ve všech útvarech banky a na všech řídících úrovních. Jde o sběr dat událostí operačního rizika, což lze pokládat za základní součást monitoringu operačního rizika. Je potřebné pravidelně hlásit události povahy operačního rizika a v případě, že ve sledovaném období k události nedojde, vystavit negativní hlášení. Pouze tímto důsledným způsobem lze pořídit kompletní dokumentaci událostí. K tomu je potřebné mít nastaven systém monitorování možných operačních rizik v rámci jednotlivých organizačních složek. Banka musí disponovat řádně zdokumentovaným soupisem veškerých událostí OR. Pro systém řízení operačního rizika je třeba nastavit systém vnitřních limitů jako vhodný nástroj řízení. Kromě maximálního limitu ztrát způsobených událostmi operačního rizika je třeba definovat limity pro jednotlivé kategorie událostí OR a stanovit postupy pro případ překročení limitů. Limity je třeba kontrolovat a promítat do nich významné změny interních procesů či produktů. Pouze tak lze identifikovat, měřit a řídit aktuální operační riziko.

Aby byla zajištěna dostatečná identifikace a kvantifikace potenciálních operačních rizik, je vhodné, prospěšné využívat metodu RCSA Risk Control Self Assesment neboli minimálně jedenkrát ročně by vedoucí jednotlivých úseků banky měli provést identifikaci potenciálních problémů operačních rizik pomocí RCSA. Každá identifikovaná událost operačního rizika by měla být vyhodnocena s ohledem na její závažnost, pravděpodobnost výskytu a možnost intervencí.

Tvorba katalogu

Banka si musí vytvořit *katalog operačních rizik*, která ji s různou mírou pravděpodobnosti mohou ohrozit. Katalog by měl být koncipován tak, aby každá riziková událost v katalogu uvedená, byla s potřebnou mírou detailu popsána, rekonciliována na účetnictví, a byl k ní přidělen *původce rizika* a *určeny organizační útvary a procesy*, které jsou tímto rizikem *potenciálně zasaženy*. Banka musí také stanovit prahové hodnoty ztrát z událostí operačního rizika. Při tvorbě katalogu je nezbytné zvažovat pravděpodobnost výskytu událostí operačního rizika a závažnost událostí operačního rizika, resp. jejich potenciální dopad do hospodářského výsledku banky. Výchozí struktura katalogu musí korespondovat s regulatorně vymezeným typem událostí a obchodními liniemi. Katalog je potřebné periodicky validovat a případně navrhovat změny ve struktuře nebo obsahu, které budou reagovat například na zavedení nového produktu nebo změny v organizační struktuře banky.

Analýza a řízení operačního rizika

Je nutné provádět analýzy využívání i využitelnosti informací, které jsou ze systému získávány a případně přistoupit k aktualizaci. Nezbytné je posoudit, jak nezávislý útvar, který odpovídá za řízení operačního rizika v dané bance, má nastaven *práh významnosti* pro další postupy vůči událostem operačního rizika. Oblasti banky, kde byla identifikována vysoká expozice vůči operačnímu riziku, musí být v dalších krocích adekvátně řízeny. Aby byla data dobře využitelná, je požadována jejich vysoká kvalita, konzistence, možná interpretace a vhodnost pro audit. Banka by měla disponovat integrovanou zprávou dat, analytickými nástroji, ale databáze záznamů o ztrátách z událostí operačního rizika se v praxi integrovat nedoporučují. Pro shromažďování velkých objemů dat se využívají datové sklady.

V této souvislosti je nezbytné ověřovat, zda jsou vnitřní předpisy v souladu se systémem řízení operačního rizika v bance, zda pokrývají veškeré oblasti rizika a jsou ve všech fázích řízení operačního rizika využívány. Dále musí být formulováno, jak postupovat při vzniku události operačního rizika. Je vhodné průběžně testovat znalosti vnitřních předpisů zaměstnanci, i dodržování těchto předpisů.

Vybrané nástroje analýzy a řízení

Sebehodnocení

Sebehodnocení, *Risk and Control Self Assessment* (RCSA) je důležitým procesem v rámci řízení operačního rizika. Jeho přínos závisí na kvalitě komunikace, protože záleží na výstupech workshopů, brainstormingů a obdobných aktivit, na aktivní účasti jak vybraných pracovníků řízení rizik, tak i vybraných pracovníků konkrétní zkoumané linie podnikání. Sebehodnocení se zaměří na každou podnikatelskou linii samostatně a v jejímž rámci se identifikují a hodnotí rizika. Současně se posuzuje kvalita kontrolního procesu náležející ke každé konkrétní linii podnikání banky včetně nastavených případných intervencí. Sebehodnocení pomáhá nacházet nejlepší postupy řešení, vytvářet benchmarky mezi obdobnými aktivitami, produkty, službami, nacházet nová rizika. Sebehodnocení lze rozdělit do dílčích fází.

a. Přípravná fáze

Proces sebehodnocení je třeba důkladně připravit. Je třeba, aby všichni účastníci byli dostatečně informováni o celém procesu sebehodnocení, které dílčí procesy budou do sebehodnocení zahrnuty, kterých hlavních rizik se bude týkat, jaké jsou cíle. Vhodné je využít databáze s historickými událostmi operačního rizika, soubor klíčových indikátorů, zprávy vnitřního i externího auditu. Pracovníci řízení rizik si připraví sady základních dotazování tak, aby pokrývaly veškeré předpokládané aktivity zkoumané obchodní linie.

b. Fáze zachycení a identifikace operačních rizik

Pracovníci útvaru řízení rizik vedou rozhovory se zainteresovanými pracovníky, ke kterým využívají připravené dotazníky. Zajímají se o soubor odpovědností jednotlivých pracovních pozic a snaží se v jejich rámci zachytit potenciální operační rizika. Ta se v dalším kroku řadí v souladu s regulací do jednotlivých kategorií podle typu rizikové události. Když se riziková událost vkládá do centrální databáze operačních rizik, musí odpovídat následující struktuře informací: popis rizikové události, ohodnocení rizika z hlediska významu (akceptovatelné, alarmující, kritické), popis současně nastavených kontrol, které mají bránit materializaci rizika, pracovník nebo útvar, který odpovídá za jeho řízení, předchozí zkušenosti s touto rizikovou událostí, klíčové indikátory, které mají signalizovat výskyt události, připravené omezující intervence v případě, že k rizikové události má banka přístup nulové tolerance. Tato fáze by měla být zakončena workshopy, které by měly pomoci zkompletovat potřebné informace.

c. Fáze analytická

V této fázi procesu sebehodnocení je třeba hodně komunikovat, sdělovat si své zkušenosti, přicházet s návrhy, názory. Je důležité pořizovat záznamy z jednání, vracet se k tématům, žádat o postoje k řešení případně i hlasováním o návrzích. Přínosem je zvýšení transparentnosti, lepší

znalosti pracovníků o souvislostech mezi aktivitami, procesy, poskytnutí určitého nadhledu potřebného k chápání vazeb. Poté je vhodné vrátit se k předchozí fázi a provádět zpřesnění, doplnění informací a rozčlenění identifikovaných operačních rizik podle jejich závažnosti, možnosti kvantifikace, popsání kroků vedoucích k ošetření rizik podle stupně akceptovatelnosti.

d. Fáze Reporting

Z výstupů předchozích fází jsou vytvořeny pracovníky řízení rizik reporty, které jsou poté distribuovány na příslušné řídící úrovně jako cenné informace o aktuálním stavu operačního rizika v bance. Důležitá je také formální stránka reportů. Obvykle se přebírá barevný systém semaforů a rizika jsou zařazena do červených, žlutých a zelených polí podle konkrétních kritérií. Barvy signalizují míru důležitosti. Vytváří se soupis nejvýznamnějších rizik, popisují se problémové okruhy, které je třeba akutně řešit.

Klíčové indikátory rizika

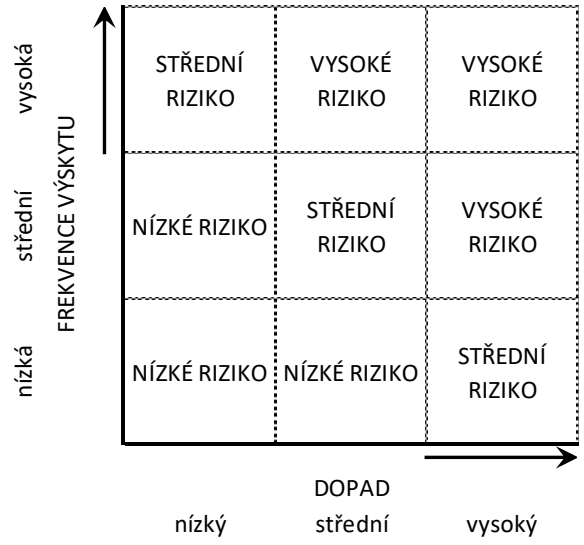
Klíčové indikátory rizika, *Key Risk Indicators* (KRI) jsou vybrané, klíčové ukazatele, které odrážejí expozici banky ve vztahu k významným operačním rizikům v konkrétních procesech nebo konkrétních produktech. Pokud jsou vhodně seskupeny, fungují jako *systém včasného varování* a lze je efektivně využít k řízení operačního rizika. Banka při jejich koncipování musí respektovat určité postupy. Nejprve musí určit procesy, které jsou pro tento způsob řízení operačního rizika, resp. jeho monitorování vhodné. Určení musí předcházet důkladná analýza procesů provedená komplexně v celé bance. Jde o aplikaci tzv. fáze mapování procesů, kdy je snahou identifikovat maximální výskyt operačních rizik, ohodnotit je z pohledu jejich pravděpodobnosti výskytu a potenciálního dopadu do hospodářského výsledku. Poté je třeba určit oblasti, na které se cílí při určování indikátorů. Vhodné je respektovat regulatorní postupy, resp. využít vymezení kategorií operačních rizika a linií podnikání banky. Přitom by banka měla zároveň vycházet ze své individuální situace, kdy pro ni nejsou stejně důležité všechny kategorie a všechny obchodní linie. Své aktivity má například soustředěny jen do užšího výběru linií podnikání, kam musí soustředit svou pozornost a „nasadit“ sem citlivé indikátory. Pokud banka využije regulací vymezené parametry, může její mapa operačních rizik vypadal tak, jak je uvedeno v tabulce č.

Tabulka č. 4 Mapa operačních rizik vycházející z regulatorních pravidel

Obchodní linie / Kategorie rizika	Podnikové financování	Obchodování na finančních trzích	Retailové makléřství	Podnikové bankovnictví	Retailové bankovnictví	Zúčtovací služby pro třetí strany	Služby z pověření	Obhospodařování aktiv
Vnitřní nekalé jednání								
Vnější nekalé jednání								
Pracovněprávní postupy a bezpečnost provozu								
Klienti, produkty, obchodní postupy								
Škody na hmotném majetku								
Narušení činností a selhání systémů								
Provádění transakcí, dodávky, řízení procesů								

Zdroj: *Varadachari, R.: Pitfalls to be avoided in operational risk (2005)* a autor

Obrázek č. 2 Vzor rizikové mapy s využitím kategorizace Basel II



Zdroj: *Varadachari, R.: Pitfalls to be avoided in operational risk (2005)* a autor

Klíčové indikátory by měly být dostatečně citlivé na podstatné změny, chyby, opomenutí, zpoždění v činnostech banky. Při jejich určení by měla být zohledněna i databáze událostí operačního rizika., sebehodnocení, upozornění interního i externího auditu. Jejich soubor je třeba průběžně aktualizovat, zohledňovat organizační změny, nové produkty, změny v nastavení procesů, použití nových informačních systémů. Mohou být impulsem k sestavení scénáře. Ideální by bylo, pokud by banka disponovala výhradně *predikčními indikátory*. V takovém případě by skutečně šlo o signální systém, který by upozornil na potenciální zvýšení výskytu rizika, a tudíž by bylo možné intervenovat ještě před materializací rizika. Banka se ale musí spokojit i s *indikátory koincidenčními*, kde jde o časový souběh mezi vznikem rizika a jeho identifikací pomocí indikátoru a nemusí nutně dojít ke ztrátě. *Detekční indikátory,* kde je přítomno časové zpoždění, i když pouze minimálního rozsahu, bance umožňuje vynaložit minimální náklady na řešení krizové situace. I v bance, kde správně fungují vnitřní kontrolní systémy, se lze setkat se *zbytkovým rizikem* a vůči němu je třeba postavit tzv. *reziduální indikátory*.

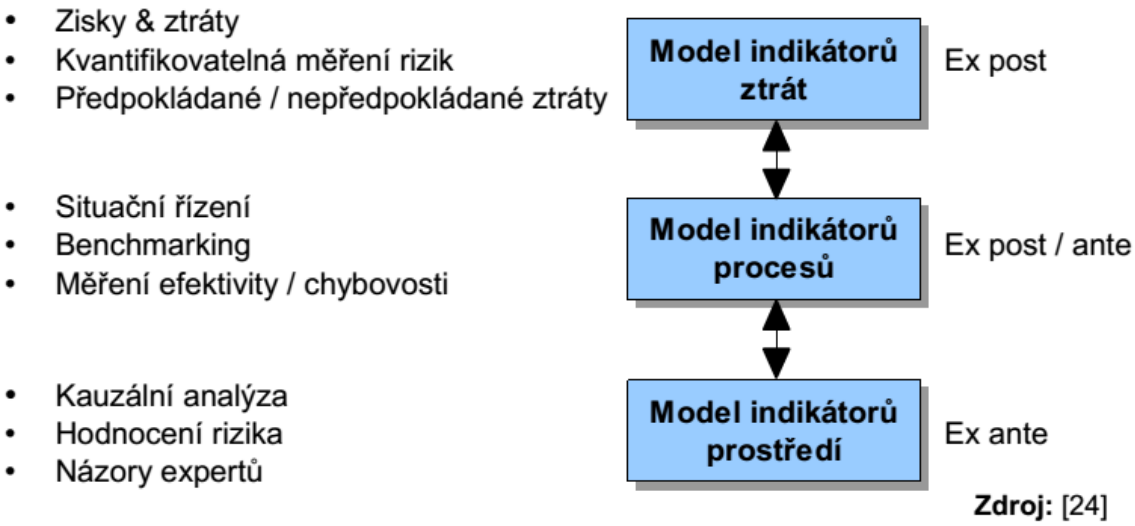
Na výběru vhodných indikátorů pro vybrané procesy by se měli podílet pracovníci daných útvarů[6]. Lze využít potenciál stávajícího manažerského informačního systému, analyzovat vztahy mezi stávajícími statistickými ukazateli, daty a riziky, přistoupit k případné modifikaci ukazatelů nebo navrhnout nové. Vždy je třeba přitom respektovat vypovídací schopnost, frekvenci sběru, zda jsou nastavena oscilační pásma pro pohyb ukazatele, nebo limity akceptovatelnosti. Zjistit, kdo je odpovědný za primární data, tvorbu ukazatele, jeho analýzu. Je možné přistoupit k úpravám ve všech či vybraných sledovaných oblastech s cílem vygenerovat *soubor vhodných indikátorů* za daný proces. Danou problematikou se komplexně zabývali Immaneni, Mastro a Haubenstock (2004). Navrhovali tzv. design matrix, kdy se v prvním kroku určí faktory, které mohou iniciovat vznik události operačního rizika v rámci zkoumaného procesu a těm se v následujícím kroku přiřadí váhy podle výše pravděpodobnosti, s jakou dojde k tomu, že faktor vyvolá rizikovou událost. Jsou předdefinovány čtyři stupně, které určují sílu vztahu mezi faktorem a rizikovou událostí, a to od nuly (žádný vztah), přes jedna (slabý vztah), tři (středně silný vztah) až po devítku (silný vztah).

Na univerzální banku, jejíž činnosti lze rozčlenit na velkou škálu procesů, působí heterogenní operační rizika, a proto se musí snažit vygenerovat dostatečně obsáhlý soubor indikátorů. Musí si být ale vědoma, že jejich nastavení včetně limitů a intervencí a následný monitoring klade nároky na čas. Cílem není pouhé shromažďování dat, ale aktivní analýza a interpretace získaných hodnot. Transparentní, dobře hodnotitelný soubor indikátorů. Než banka spustí provoz sběru dat, musí evidenci indikátorů formalizovat. V databázi musí mít každý indikátor svou identifikaci, název, popis včetně určení účelu použití. Musí být vždy transparentně dohledatelná primární data, provedena kalibrace ukazatelů, popsány postupy výpočtů a frekvence získávání informací. Na výše uvedených dílčích krocích se musí kromě útvaru řízení operačního rizika vždy podílet i předmětný odborný útvar, jehož operační riziko se banka snaží dostat pod kontrolu.

Jeden z možných přístupu uvádí Davies, Haubenstock (2002), kteří vycházejí ze třech druhů indikátorů, tak jak jsou uvedeny na následujícím schématu č. 2.

[6] Zjednodušeně vyjádřeno, útvarů odpovědných za daný proces.

Schéma č. 2 Modely indikátorů



Obrázek 4.5 Přehled typů indikátorů rizika

Zdroj: Davies, Haubenstock (2002)

Soubor indikátorů ztrát soustavně sleduje, vyhodnocuje a kvantifikuje ztráty vzniklé materializací operačního rizika. Ke kvantifikaci může docházet v rámci obchodních linií. Jde o sledování a měření ex-post. Pomocí simulace lze na základě minulých dat provádět i predikce.

Soubor indikátorů procesů je zacílen na měření chybovosti, bezpečnosti, spolehlivosti a v podstatě signalizují kvalitu nastavených procesů, aktivit, transakcí. Lze je využívat, jak vpřed hledící, tak i zpět hledící.

Soubor indikátorů prostředí lze také aplikovat jak o zpět hledící i vpřed hledící. Soustřeďují se na informace vyplývající z reklamací, stížností klientů, spokojenost zaměstnanců, hodnocení kvality interních školení, hodnocení využívaných technologií.

9.1.1 Modelování a měření operačního rizika

Při modelování a měření operačního rizika je třeba postupovat v souladu s požadavky regulace. Zavedení statistických metod kvantifikace operačního rizika může být realizováno buď pomocí tzv. “bottom-up“ nebo „top-down“ přístupu. Bottom-up přístup vychází z analýzy operačního rizika jednotlivých procesů v rámci obchodních linií, identifikuje přítomnost rizika na úrovni jednotlivých procesů. Postupuje se tak, že jsou procesy mapovány podle typů rizikových událostí a událostí ztrát s cílem odhadnout pravděpodobnost výskytu konkrétních scénářů. Poté jsou potenciální změny typů rizikových událostí a událostí ztrát simulovány za účelem vygenerování distribuce ztrát. Přístup je náročný na vstupní informace, ale je vhodnější pro efektivní řízení rizika než přístup top-down, který

pracuje s agregovanými procesy, je nenáročný na vstupní data, ale nelze se na něj spolehnout jako na solidní analytický nástroj. Pro kvantifikaci operačního rizika je důležitá četnost výskytu událostí operačního rizika a jejich závažnost. Podrobně je problematika řešena v kapitole 9.3.

Identifikace zdrojů rizika

Na rozdíl od řízení jiných bankovních rizik, toto riziko je třeba řídit napříč celou bankou a v podstatě do jeho řízení začlenit všechny pracovníky banky, protože mají ve vztahu k pracovní pozici, kterou zastávají, vazbu na potenciální události operačního rizika. Rozpoznání operačního rizika je soustavnou činností probíhající ve všech útvarech banky a na všech řídících úrovních. Jde o sběr dat událostí operačního rizika, což lze pokládat za základní součást monitoringu operačního rizika. Je potřebné pravidelně hlásit události povahy operačního rizika a v případě, že ve sledovaném období k události nedojde, vystavit negativní hlášení. Pouze tímto důsledným způsobem lze pořídit kompletní dokumentaci událostí. K tomu je potřebné mít nastaven systém monitorování možných operačních rizik v rámci jednotlivých organizačních složek. Banka musí disponovat řádně zdokumentovaným soupisem veškerých událostí OR. Pro systém řízení operačního rizika je třeba nastavit systém vnitřních limitů jako vhodný nástroj řízení. Kromě maximálního limitu ztrát způsobených událostmi operačního rizika je třeba definovat limity pro jednotlivé kategorie událostí OR a stanovit postupy pro případ překročení limitů. Limity je třeba kontrolovat a promítat do nich významné změny interních procesů, či produktů. Pouze tak lze identifikovat, měřit a řídit aktuální operační riziko.

Aby byla zajištěna dostatečná identifikace a kvantifikace potenciálních operačních rizik, je vhodné, prospěšné využívat metodu RCSA Risk Control Self Assesment neboli minimálně jedenkrát ročně by vedoucí jednotlivých úseků banky měli provést identifikaci potenciálních problémů operačních rizik pomocí RCSA. Každá identifikovaná událost by měla být vyhodnocena s ohledem na její závažnost, pravděpodobnost výskytu a možnost intervencí.

Příklad výskytu operačního rizika při obchodování na finančních trzích

Operační riziko je přítomno ve všech bankovních činnostech, ale při provádění operací na finančních trzích je toto riziko značné, resp. mohou být značné možné ztráty s ním související. Z toho důvodu je třeba řešit návrh zásad na korektní nastavení příslušných procesů, který by měl omezit vznik operačního rizika u tohoto typu aktivit banky. Základním předpokladem, který vede k omezení operačního rizika, je potřebná kvalifikace příslušných pracovníků, vhodné interní metodiky, které popisují přípustné postupy při obchodování, evidenci a vypořádání obchodů a odpovídající informační systém, který bude svým uživatelům poskytovat potřebný komfort (neumožní udělat chybu).

Konkrétní pracovník – dealer, smí provádět pouze ty operace, které jsou mu povolené, a to pouze na jemu vymezených trzích. Při obchodování se dealer musí pohybovat v rámci povolených limitů. Zde je důležitá informační podpora, která jednak umožní udržovat si v reálném čase přehled o velikosti nečerpaných limitů a také poskytuje přehled o ekonomických výsledcích pozic a portfolií, za které dealer odpovídá. Pokud jsou limity vnitřně strukturované, lze snížit riziko plynoucí z jejich překročení možností simulace transakce a signalizací nepovolených kroků. Pokud přesto dojde k otevření expozice nad stanovenou, resp. akceptovatelnou míru, musí být v bance připraven mechanismus, který umožní

tuto situaci řešit. Dealer je povinen vystavit tzv. ticket, který přesně identifikuje jeho osobu a transakci. Uvádí časový termín včetně hodiny, kdy k operaci došlo, označení nástroje, který byl předmětem operace, uvedení protistrany a instrukce k vypořádání operace. Pro zamezení operačního rizika bylo vždy doporučováno v této fázi pořizovat nahrávky veškerých obchodů uzavíraných po telefonu.

Významný vliv na omezení operačního rizika při obchodování má útvar *back-office***,** který je odpovědný za zavedení veškerých uzavřených obchodů do účetního systému banky. V rámci vypořádání transakcí, které uzavře pracoviště *front-office,* musí zajistit převody peněžních prostředků na peněžních účtech a investičních prostředků na majetkových účtech. Tyto činnosti jsou založeny na komunikaci s back-office útvary, bankami případně depozitáři příslušných protistran vypořádávaných transakcí.[7] Jednotlivé obchodní případy jsou přijímány ve formě validovaných transakcí.[8] Instrukce musí být dodána do dne dohodnutého vypořádání transakce. Pokud je instrukce v pořádku, obdrží back-office potvrzení o přijetí instrukce a v den vypořádání potvrzení o vypořádání. Pokud je instrukce vadná, obdrží back-office hlášení o chybě. Důležitý je faktor času, protože omezením intervalu mezi provedením obchodu a záznamu o jeho provedení se omezuje možnost uzavření dalšího obchodu, který by mohl být již nadlimitní. Minimálně na konci každého obchodního dne je nutné provést kontrolu mezi výstupy dealingu a vstupy back office. V delších časových horizontech potom je vhodné aplikovat kontrolu mimo obě tato pracoviště. Neoprávněné vstupy do systému musí být znemožněny a veškeré opravy údajů musí být zaznamenávány, tj. jde o standardní přístup známý z účetnictví. Především dealeři nemohou manipulovat s daty již uzavřeného obchodu, provádět konfirmace. Za včasné odesílání konfirmací odpovídá back office, který využívá SWIFT. Pokud by teoreticky banka neuskutečňovala konfirmace písemně, muselo by být hlasové párování vždy zaznamenáváno a kontrolováno s tím, že musí být identifikovatelný pracovník konfirmaci provádějící i obchod, který je předmětem konfirmace.

Při obsluze peněžních účtů se používají různé formy elektronického bankovnictví. Nejobvyklejší je používání individuálních systémů jednotlivých bank, vzájemně nekompatibilní. Back-office potřebuje pro svou činnost odesílat platební příkazy a načítat výpisy z účtů a k tomu je třeba mít podporu v informačních systémech. Jediným standardem je SWIFT, který slouží k elektronické výměně informací, a to na mezinárodní i národní úrovni. Výměna zpráv probíhá ve standardním formátu a se zabezpečeným obsahem[9] a zabezpečenou autentizací. Důležitou pozici v rámci podpůrných činností má útvar *middle-office*, který především zajišťuje průběžné kontroly prováděných transakcí a dodržování limitů, resp. kontrolu jejich zpracování tzv. validací, správu statistických dat, oceňování dílčích portfolií, výpočet čisté hodnoty majetku portfolií a výkonnosti portfolií a benchmarkingu. Validace transakcí znamená porovnávání údajů o konkrétním obchodním případu zadaném do informačního systému s ticketem k obchodnímu případu a konfirmacemi protistran. Po přijetí konfirmace od protistrany se porovnávají údaje, které byly zadány do informačního systému s údaji, které jsou uvedeny na ticketu a s údaji, které byly přijaty od protistrany. V případě, že údaje souhlasí, *middle office* potvrdí neboli validuje, danou finanční transakci a předá ji k dalšímu zpracování do útvaru *back office*. Pokud údaje nesouhlasí, je třeba upozornit útvar řízení rizik a nesrovnalosti odstranit.

[7] Náročnost systému vypořádání je dána mimo jiné vysokou četností protistran, z nichž každá může používat svůj specifický způsob výměny informací.
[8] Validaci zajišťuje útvar middle-office, jak vyplyne z následujícího textu.
[9] Předpokladem komunikace je, aby si protistrany vyměnily šifrovací klíče.

Metody měření operačního rizika

Podstata operačního rizika znesnadňuje jeho identifikaci a měření, což jsou v obecné rovině předpoklady pro úspěšné řízení. Na rozdíl od rizika úvěrového a rizik tržních, kde lze vysledovat tvorbu metod měření nezávisle na regulatorních požadavcích a přístup „best practices" ze strany formulování regulatorních požadavků, které v oblasti měření rizik pro potřeby propočtu požadavků na kapitál vycházejí z již známých a ověřených metod formulovaných a používaných bankami pro propočet ekonomického kapitálu, u operačního rizika se s obdobným vývojem nesetkáváme.

Regulatorní pravidla směřují k propočtu kapitálového požadavku k operačnímu riziku a nabízejí jak orientaci na jednoduché postupy měření, které ovšem nevedou k efektivnímu řízení rizika, tak i metody složitější, která jsou v konečném výsledku pro regulované subjekty z pohledu řízení rizika užitečnější. Lze vycházet z předpokladu, že čím náročnější postup banka zvolí, tím méně kapitálu bude vůči operačnímu riziku alokovat a tím lépe bude toto riziko řídit. Regulátor nabízí základní metodu, k jejíž aplikace není nutný souhlas a metody náročnější, na které se musí banka kvalifikovat. Nároky regulátora na kvalifikaci jsou přímo úměrné stupni náročnosti dané metody. U jednodušších metod měření je podstatné určení *relevantního ukazatele*, jako *indikátoru expozice* vůči operačnímu riziku. Jeho hodnota by měla odrážet současnou a případně i budoucí situaci banky a zohledňovat míru operačního rizika, kterému je, příp. bude banka vystavena. Za předpokladu, že se podmínky podstatně nezmění, je stanovená hodnota relevantní po dobu jednoho roku. Regulatorní požadavek stanovil určení relevantního ukazatele u přístupů jednodušších (BIA, TSA a ASA).

Přístup základního indikátoru BIA

Basic Indicator Approach (BIA) nebo také *metoda základního ukazatele* je nenáročnou a nejjednodušší metodou, pomocí které lze vypočítat kapitálový požadavek vůči operačnímu riziku. Banka před zavedením tohoto přístupu nemusí žádat o souhlas regulátora. Přístup byl vyvinut pro menší banky, pro které aplikace náročnějších postupů představuje vyšší náklady než odhadnuté výnosy z ušetřeného kapitálu. Negativem je nízká citlivost kapitálového požadavku na úroveň operačního rizika, kterému je banka vystavena.

Relevantní ukazatel expozice vůči operačnímu riziku, resp. rizikový faktor, který má výnosový charakter a který odráží úroveň operačního rizika, je počítán jako průměr[10] z údajů za poslední tři účetní období[11], které jsou ověřeny auditorem. Struktura ukazatele je patrná z tabulky č. 1, jde o hrubý příjem banky. Kapitálový požadavek k operačnímu riziku podle přístupu BIA se rovná 15 % z hodnoty relevantního ukazatele. V případě, že by banka dosáhla záporné hodnoty relevantního ukazatele a, nebo byl ukazatel

[10] Aplikace průměru zmírní volatilitu hrubého příjmu, a tedy také volatilitu požadavku na kapitál.
[11] Pokud je banka činná méně než tři roky, může k výpočtu relevantního ukazatele použít výhledové obchodní odhady s tím, že jakmile bude mít skutečná data, začne je bez odkladu používat. To platí i pro další přístupy k propočtu kapitálového požadavku.

roven nule, banka nebude tento údaj při propočtu za tříleté období zohledňovat. Jde tedy o součet kladných hodnot dělený počtem kladných hodnot.

Relevantním ukazatelem je součet položek uvedený v tabulce č. 1. Banka počítá ukazatel před odečtením rezerv a provozních nákladů[12].

Tabulka č. 5 Položky vstupující do propočtu hodnoty relevantního ukazatele

POLOŽKY	VLIV NA HODNOTU ZÁKLADU RELEVANTNÍHO UKAZATELE
Úrokové výnosy	+
Úrokové náklady	-
Výnosy z dividend	+
Výnosy z poplatků a provizí	+
Náklady na poplatky a provize	-
Zisk (ztráta) z finančních aktiv a závazků k obchodování	+/-
Zisk (ztráta) z přecenění finančních aktiv a závazků na reálnou hodnotu	+/-
Zisk (ztráta) ze zajišťovacího účetnictví	+/-
Kurzové rozdíly	+/-
Ostatní provozní výnosy	+

Zdroj: autor

Regulátor naopak vymezuje položky, které jsou nepřípustné pro zahrnutí do relevantního ukazatele. Jde o realizovaný zisk/ztrátu z prodeje položek bankovního portfolia, mimořádné a nepravidelné

[12] Do provozních nákladů patří například poplatky za služby outsourcingu prováděné třetí stranou, a to při splnění určitých podmínek.

výnosy, výnosy z pojistných plnění. Lze zahrnout přecenění nástrojů obchodního portfolia, pokud je vykázáno ve výsledovce.

Kapitálový požadavek lze vypočítat podle následující vzorce:

$$K_{BIA} = [\sum(GI_{1..n} \times \alpha)] / n$$

kde

K_{BIA} = výše kapitálového požadavku spočteného podle BIA přístupu

GI = kladný roční hrubý příjem (*gross income*)

n = počet let, ve kterých byl roční hrubý příjem kladný

α = 15 %

Takto nastavený kapitálový požadavek implikuje následující vztah: Čím „větší“ je banka, tím „větší“ bude mít roční hrubý příjem, a tím „více“ ztrát z titulu operačního rizika bude realizovat. Korelace mezi velikostí relevantního ukazatele a velikostí expozice banky vůči jednotlivým typům ztrát z operačního rizika je slabá. Výsledný kapitálový požadavek může být v poměru ke skutečným ztrátám z operačního rizika jak zbytečně vysoký, tak přiměřený nebo nízký. Nelze predikovat, která ze tří variant nastane. Výše kapitálového požadavku, ke které lze dospět pomocí přístupu BIA neodráží úroveň řízení operačního rizika v dané bance.

Standardizovaný přístup STA

Principem přístupu *Standardised approach* (*STA*) je povinnost banky sledovat relevantní ukazatel ne za banku jako celek, ale na úrovni jednotlivých tzv. *obchodních linií*. Každá obchodní linie zahrnuje skupinu obchodních činností se společným zaměřením – viz tabulka č. 6. Relevantní ukazatel zůstává stejný jako u BIA přístupu. Opět se počítá tříletý průměr součtu ročních kapitálových požadavků všech linií podnikání. Roční kapitálový požadavek pro každou linii podnikání se rovná součinu odpovídajícího faktoru β a části relevantního ukazatele přiřazené příslušné linii podnikání. Přístup STA umožňuje na rozdíl od BIA přístupu započítat i záporný relevantní ukazatel[13]. Obchodní linie se od sebe vzájemně liší mírou rizika, která je vyjádřena hodnotou koeficientu β, který je obchodním liniím přiřazen a nabývá tří hodnot – 12 %, 15 % a 18 %. Basilejský výbor nastavil koeficienty β po provedení potřebných simulací tak, aby průměrná banka přechodem na STA přístup snížila kapitálový požadavek oproti tomu, k jakému by dospěla při aplikaci přístupu BIA.

[13] Banka může v kterémkoliv roce vyrovnat záporné kapitálové požadavky, které vyplývají ze záporné části příslušného relevantního ukazatele v kterékoliv linii podnikání kladným kapitálovým požadavkem v ostatních liniích podnikání bez omezení. Pokud je ale souhrnný kapitálový požadavek všech linií podnikání v daném roce záporný, banka použije pro daný rok v čitateli hodnotu nula.

Tabulka č. 6. Vymezení obchodních linií

Linie podnikání	Seznam činností	Parametr
Podnikové finance	Upisování finančních nástrojů nebo umisťování finančních nástrojů na základě neodvolatelného závazku Služby spojené s upisováním Investiční poradenství Poradenství podnikům ve věcech kapitálové struktury, odvětvové strategie a v souvisejících otázkách, poradenství a služby v oblasti fúzí a koupě podniků Investiční výzkum a finanční analýza a jiné formy všeobecných doporučení ohledně transakcí s finančními nástroji	**18 %**
Obchodování na finančních trzích	Obchodování na vlastní účet Peněžní makléřství Přijímání a převody příkazů vztahujících se k jednomu či několika finančním nástrojům Provádění klientských příkazů Umisťování finančních nástrojů bez neodvolatelného závazku Provozování mnohostranných systémů obchodování	**18 %**
Retailové makléřství (činnosti pro fyzické osoby nebo malé a střední podniky, pokud expozice vůči nim splňují kritéria retailových expozic	Přijímání a převody příkazů, vztahujících se k jednomu či několika finančním nástrojům Provádění klientských příkazů Umisťování finančních nástrojů bez neodvolatelného závazku	**12 %**
Komerční bankovnictví	Přijímání vkladů a jiných splatných peněžních prostředků Poskytování úvěrů Finanční leasing Záruky a přísliby	**15 %**
Retailové bankovnictví (Činnosti pro fyzické	Přijímání vkladů a jiných splatných peněžních prostředků	**12 %**

osoby nebo malé a střední podniky splňující kritéria pro kategorii retailových expozic)	Poskytování úvěrů Finanční leasing Záruky a přísliby	
Provádění plateb a vypořádání	Služby týkající se převodu peněžních prostředků Vydávání a správa platebních prostředků	**18 %**
Služby z pověření	Uložení a správa finančních nástrojů na účet klienta, včetně opatrovnictví a souvisejících služeb jako například správa peněžních prostředků či kolaterálu Správa aktiv	**15 %**
Správa aktiv	Správa portfolií Správa v subjektech kolektivního investování Jiné formy správy aktiv	**12 %**

Zdroj: autor

Banka musí respektovat zásahy pro přiřazování k liniím podnikání a musí je mít zdokumentované. Především musí mít jasně určená kritéria, podle kterých přiřazuje relevantní ukazatel příslušné linii podnikání. Při přiřazování činností k liniím nesmí docházet k překrývání, ale je třeba zařadit veškeré činnosti. Pokud vznikne problém, kdy nelze jednoznačně určit přiřazení, je třeba volit linii s vyšším požadavkem na kapitál. Banka může využívat interní oceňovací modely. Je důležité, aby banka respektovala zásadu konzistentnosti neboli přiřazování činností k liniím podnikání pro účely stanovení kapitálového požadavku k operačnímu riziku musí mít vazby na kategorie, které banka využívá pro úvěrové a tržní riziko.

Požadavek na kapitál se počítá podle vzorce:

$$K_{TSA} = \left\{ \sum_{roky\,1-3} \max\left[\sum (GI_{1-8} \times \beta_{1-8}), 0 \right] \right\} / 3$$

kde

K_{STA} = výše kapitálového požadavku spočteného podle STA přístupu

GI_{1-8} = roční hrubý příjem (*gross income*) vytvořený příslušnou obchodní linií

β_{1-8} = koeficient β pro příslušnou obchodní linii (viz Tab. č. 6)

Aplikace tohoto přístupu pro propočet kapitálového požadavku je podmíněna schválením regulátora, resp. banka musí splnit daná kvalifikační kritéria, pokud chce přístup STA používat. Jde především o požadavek na zdokumentované postupy, které určují, jak rozdělovat relevantní ukazatel mezi jednotlivé obchodní linie. Banka musí všechny činnosti zařazovat do linií tak, aby žádná činnost nebyla vynechána a nedocházelo ani k duplicitnímu zařazování. Požadavky regulátora směřují k maximálnímu omezení nepovolených aktivit banky, které by vedly ke zkreslení, resp. podhodnocení kapitálového požadavku a spočívaly v principu preferování linií s nižším koeficientem beta. Proces členění činností a alokace relevantního ukazatele do standardizovaného rámce vymezeného v tabulce č. 6 podléhá nezávislému přezkoumávání.

Banka, jejímž záměrem je používat standardizovaný přístup, musí prokázat, že má zdokumentovaný systém vyhodnocování a řízení operačního rizika vč. systému hlášení, jasně stanovené odpovědnosti, zaznamenává údaje, které se rizika týkají vč. údajů o událostech s významným dopadem. Dále prokázat, že její systém vyhodnocování operačního rizika je přímo začleněn do procesů řízení rizik a výstupy systému jsou součástí procesu sledování rizikového profilu banky.

Expozice jednotlivých obchodních linií vůči operačnímu riziku je významně odlišná, a proto je možnost sledovat relevantní ukazatel na úrovni jednotlivých obchodních linií přínosný. Banky, které své aktivity směřují do linií s vysokým koeficientem beta, jsou tímto přístupem zatíženy. Z toho důvodu regulace nabízí možnost využití tzv. *alternativního standardizovaného přístupu (ASA)*, který je vhodný pro banky, jejichž naprostá většina činností spadá do linie podnikání retailového bankovnictví a podnikového bankovnictví a které prokáží, že významná část činnosti retailového a podnikového bankovnictví je tvořena expozicemi s vysokou pravděpodobností defaultu.

Alternativní standardizovaný přístup ASA

Přístup ASA je modifikací předchozího pojetí STA s tím, že indikátorem expozice vůči operačnímu riziku pro linie podnikání retailového bankovnictví anebo komerčního bankovnictví je *alternativní ukazatel* namísto ukazatele relevantního. Pro obchodní linie retailového a komerčního bankovnictví jde o nominální hodnotu úvěrů a půjček[14] vynásobené koeficientem 0,035. Alternativní ukazatel odpovídá normalizovanému ukazateli výnosu, který se rovná součinu koeficientu 0,035 a dlužné částky poskytnutých úvěrů v linii nebo liniích (retailové, komerční bankovnictví) s tím, že do linie komerční bankovnictví se zařazují také cenné papíry investičního portfolia v nominální hodnotě úvěrů a půjček.

Aby banka mohla aplikovat přístup ASA, musí její retailové nebo komerční bankovní činnosti generovat minimálně 90 % jejích příjmů s tím, že významná část retailových nebo komerčních bankovních činností je tvořena půjčkami, které mají vysoký parametr PD (pravděpodobnost defaultu).

Při použití přístupu ASA se stanoví kapitálový požadavek k operačnímu riziku

$$KRB/PB = ßRB/PB \cdot 0{,}035 \cdot URB/PB$$

kde: metoda ukazatelů

[14] Úvěry a půjčkami se rozumí celková čerpaná částka v odpovídajících úvěrových portfoliích.

ßRB/PB = riziková váha (parametr ß) pro linie podnikání retailové bankovnictví (RB)

anebo komerční bankovnictví (PB)

URB/PB= dlužná částka poskytnutých úvěrů v příslušné linii nebo liniích podnikání.

Při výpočtu hodnoty kapitálového požadavku pro ostatní linie podnikání a celkového kapitálového požadavku postupuje banka jako při přístupu STA. Pokud provedeme komparaci těchto jednodušších přístupů propočtu kapitálového požadavku, je sice STA pokročilejší, ale ve vazbě na reflektování úrovně operačního rizika mezi nimi není podstatný rozdíl.

Pokročilé přístupy AMA

Soubor pokročilých metod měření operačního rizika, které lze shrnout pod tzv. AMA přístup, *Advanced Measurement Approach*, nabízí, na rozdíl od všech předchozích uvedených přístupů, nejen možný postup propočtu kapitálového požadavku, ale zároveň bance umožňuje reflektovat skutečnou úroveň operačního rizika, operační riziko dostat pod kontrolu, efektivně je řídit. V dlouhodobém horizontu lze pracovat s případným pojištěním (na rozdíl od předchozích metod, kde pojištění nelze v propočtu požadavku na kapitál zohlednit). Kapitálový požadavek je výsledkem měření pomocí vlastního modelu banky, k jehož využití pro regulatorní účely se banka musí poměrně náročně kvalifikovat, resp. splnit soubor kvalitativních i kvantitativních požadavků. Kvalifikační proces je náročný nejen pro banku, ale také pro dohledovou instituci, protože každý interně vyvinutý model je jedinečný a je třeba ověřit jeho vhodnost pro účely propočtu kapitálového požadavku k operačnímu riziku, které daná banka podstupuje.

Tabulka č. 7 Kvalifikační požadavky kvalitativní povahy pro používání AMA přístupu

KVALITATIVNÍ POŽADAVKY
Systém řízení operačního rizika je přímo začleněn do každodenních procesů řízení rizik
Funguje nezávislý útvar pro řízení operačního rizika
Existuje pravidelný reporting o expozicích vůči operačnímu riziku, o ztrátách
Banka má postupy pro případné intervence, nápravná opatření
Dokumentace systému řízení rizik, postupy zajišťující respektování pravidel, zásady pro případ porušení
Interní a externí auditor pravidelně provádí přezkum postupů řízení operačního rizika
Interní procesy validace jsou účinné a probíhají řádně
Toky údajů a procesy spojené se systémem pro měření rizik jsou transparentní a dostupné

Zdroj: autor

Kromě kvalitativních standardů musí banka splňovat i standardy kvantitativní, a to jak pro procesy, tak pro interní údaje. Ve vztahu k procesům banka musí do propočtu požadavku na kapitál zahrnovat jak neočekávanou, tak očekávanou ztrátu z titulu operačního rizika. Pouze pokud by byla očekávaná ztráta přiměřeně podchycena v interních obchodních postupech[15] banky, nebylo by třeba ji zahrnout. Při měření musí banka zachytit i potenciální události, které se vyznačují nízkou pravděpodobností výskytu, ale případným významným dopadem do hospodářského výsledku. Přitom banka musí během roku naplňovat standard spolehlivosti, který je srovnatelný s intervalem spolehlivosti 99,9 %. To, co je velmi důležité a co zaručuje vyvážený a komplexní pohled na operační riziko dané banky, je její povinnost zahrnout do propočtu nejen interní data, ale dále také externí data, analýzu scénářů, faktory zohledňující firemní prostředí a vnitřní kontrolu, nástroje zmírňující riziko. Tím, že je výpočet takto strukturován, umožní to bance zohlednit historii ztrát, extrémně vysoké ztráty s malou frekvencí výskytu, transfer rizika na jiné osoby.

Nejvýznamnější složkou jsou *interní data* o ztrátách. Součástí každého záznamu o události operačního rizika musí být obchodní linie, ke které se vztahuje a musí mít přiřazenu jednu z kategorií rizika. Pro výslednou kvalitu je důležité nastavení procesu sběru dat včetně jejich frekvence. Každý záznam o události operačního rizika musí obsahovat informace o případné vazbě na úvěrové nebo tržní riziko. Důvodem je i to, aby nedocházelo ke vzniku duplicit pro propočtu nároků na kapitál, kdy by se jedna událost objevila, jak zahrnuta do propočtu kapitálového požadavku k operačnímu riziku, tak zároveň v propočtu kapitálového požadavku k buď k úvěrovému, nebo tržnímu riziku. Banka musí mít nastaven limit ztrát, jakousi hranici významnosti, od které události eviduje. Pokud by banka shromažďovala veškeré události, zvyšovala by nadměrně náklady.

Pokud chce banka využívat pokročilé postupy k měření operačního rizika, musí shromažďovat interní měření po dobu minimálně pěti let[16].

[15] Banka může prokázat, že očekávanou ztrátu pokrývá průběžným vytvářením rezerv nebo ji zahrnuje do kalkulace ceny produktů.
[16] Pokud přechází na pokročilý přístup nově, může použít data za tříleté období.

Tabulka č. 8 Možný způsob mapování operačního rizika

Tabulka 3.2 Mapování typů rizika na sedm typů rizikových událostí a osm obchodních linií

Obchodní linie	Typy rizikových událostí	Typy rizik
Podnikové finance	Interní podvod	Lidé
Obchodování na finančních trzích	Externí podvod	Externí události
Retailové bankovnictví	Pracovní postupy a bezpečnost provozu	Lidé
Komerční bankovnictví	Klienti, produkty a pracovní postupy	Organizace
Zúčtovací služby	Škody na hmotném majetku	Externí události
Zprostředkovatelské služby	Narušení činnosti a selhání systémů	Systémy
Správa aktiv	Provádění transakcí, dodávky a řízení procesů	Procesy
Retailové makléřství		

Zdroj: [1] str. 138

Zdroj: autor

Externí data je třeba vnímat jako substitut za chybějící data interní. Kapitálový požadavek, který by vycházel pouze z interních dat, by neodrážel komplexní expozici banky vůči operačnímu riziku. Existují sdílené databáze jako www.riskbusiness.com, www.orx.org[17], které je možné využít s tím, že banka musí zohlednit relevanci dat[18], resp. externí data upravit tím způsobem, aby byla porovnatelná s daty interními.

Pro řízení operačního rizika je důležité pracovat s *hypotetickými scénáři* a jejich analýzou. Banka by se měla soustředit na simulování málo četných událostí s velmi vysokým dopadem do hospodářského výsledku, protože to jsou data, kterými banka v potřebném rozsahu nedisponuje[19]. Jde o dopředu hledící stresové testování, které bance pomůže identifikovat slabá místa a iniciovat tvorbu pohotovostních plánů, kde bude popsáno, jak postupovat v případě krizové situace, na jaké procesy a činnosti se soustředit, které aktivity potlačit. Nedostatkem práce se scénáři může být subjektivní prvek, který je v simulaci zastoupen. Je proto třeba využívat expertů, kteří mají s operačním rizikem a jeho projevy zkušenosti. Vést detailní dokumentaci a vytvořit tak podklady pro přesnější rozhodování v budoucnu.

Další složkou zahrnovanou do propočtu kapitálového požadavku je *soubor indikátorů*, který odráží rizikovost vnitřního prostředí banky a případnou neadekvátnost systému vnitřních kontrolních mechanismů. Jde vlastně o signální systém souboru indikátorů, které by měly upozornit na změny

[17] Operational Risk Exchange.
[18] Tzv. scaling.
[19] Banka disponuje v potřebném rozsahu interními daty, která mají nízký až střední dopad do hospodářského výsledku a jejich četnost výskytu je častá.

úrovně operačního rizika s cílem zamezit nárůstu operačního rizika. Výběr indikátorů by měl zohledňovat určitá kritéria. Indikátor by měl být kvantifikovatelný, měl by být citlivý na změny úrovně operačního rizika. Banka může vypovídací schopnost signální soustavy posílit a zpřesnit zpětným testováním. Jako příklad lze uvést fluktuaci pracovníků určitého útvaru banky za určité období. Měl by být nastaven horní limit, který je pro řádné fungování útvaru ještě akceptovatelný. Pokud dojde k překročení nastaveného limitu, musí v co možná nejkratším čase následovat intervence v podobě mimořádných znalostních kurzů pracovníků, interních školení, přesunu bývalých pracovníků útvaru, kteří nyní pracují v rámci jiného útvaru zpět na pomoc zaškolení nově příchozích zaměstnanců.

Mezi *nástroje zmírňující operační riziko* můžeme v krajním případě zařadit i rozhodnutí danou činnost v budoucnu neprovádět. Pokud byl s určitou aktivitou banky spojen vyšší výskyt ztrát z titulu operačního rizika a banka nenachází vhodné řešení, jak tomu v budoucnu zamezit, může přijmout rozhodnutí se danou aktivitou již nezabývat. Zváží náklady, které by souvisely například s pořízením vhodného softwaru, získáním vysoce kvalifikovaných specialistů apod. a porovná s potenciálními výhodami jako například možnost doplnit nabídku produktové škály o strukturovaný vysoce sofistikovaný produkt, který by stabilizoval segment atraktivního segmentu klientů s velkým finančním potenciálem. Banka může postupovat také zdokonalením vnitřní kontroly. Většinou ani posílené vnitřní kontroly nedokáží zcela eliminovat události operačního rizika. Proto banka musí vzniklé ztráty pokrývat průběžně svými příjmy (ztráty očekávané), částečně pojištěním a také kapitálem (především neočekávané ztráty, případně také očekávané, pokud průkazně nedokáže jejich krytí jinými zdroji). Pojištění umožňuje bance využití u speciálních typů událostí operačního rizika jako pojištění proti krádežím, živelným pohromám, havarijní pojištění vozového parku apod.

Banka může zkoumat i korelace mezi jednotlivými kategoriemi ztrát z operačního rizika v rámci jednotlivých predikcí rizika, a to za předpokladu, že disponuje spolehlivými systémy, které měří korelace spolehlivě i v krizových obdobích. Korelace pak může uznat jako nástroj zmírňující operační riziko.

Banka může zohlednit vliv pojištění a dalších postupů transferu rizika na snížení propočtu kapitálového požadavku. Musí ale dohledu jednoznačně prokázat, že ke snížení jednoznačně dochází. Například poskytovatel pojištění musí disponovat ratingem, který deklaruje schopnost vyplácet pojistné plnění. Pojištění musí splňovat regulatorně daná kritéria, mezi která patří:

- Počáteční platnost pojistné smlouvy nesmí být kratší než jeden rok. V případě pojistných smluv se zbytkovou platností kratší, než jeden rok musí banka provést náležité snížení hodnoty, kterým zohlední zkracující se zbytkovou platnost dané pojistné smlouvy; v případě pojistných smluv se zbytkovou platností 90 dní nebo kratší může toto snížení dosáhnout až plných 100 %.
- Výpočty účinků snižování rizika musí zohledňovat pojistné krytí transparentním a konzistentním způsobem ve vztahu ke skutečné pravděpodobnosti a dopadu ztrát použitých při celkovém stanovování kapitálových požadavků k operačnímu riziku.
- Snížení kapitálových požadavků plynoucí ze zohlednění pojištění a jiných mechanismů převodu rizik nesmí přesáhnout 20 % výše kapitálového požadavku k operačnímu riziku před zohledněním technik snižování rizika.

V rámci AMA přístupu lze nalézt *škálu metod*, kterou nelze pokládat za uzavřenou. Naopak lze předpokládat, že se budou generovat metody další. Jde o metody statistické i metody expertních odhadů, případně kombinované.

Metoda rozdělení ztrát

Metoda rozdělení ztrát (*Loos Distribution Approach*, LDA) se pro potřeby propočtu kapitálového požadavku k operačnímu riziku používá poměrně často. Jako vstupy používá interní data o událostech operačního rizika a výši kapitálu stanoví na základě odhadu četnosti výskytu a závažnosti dopadu událostí operačního rizika do hospodářského výsledku banky, k čemuž využívá statistické a aktuárské techniky. Přesnějších výsledků banka docílí, pokud pracuje s obchodními liniemi, protože lze předpokládat, že rozdělení ztrát se bude v rámci jednotlivých obchodních linií lišit. Agregované rozdělení pravděpodobnosti pro kombinaci obchodní linie a typ ztráty lze získat pomocí Monte Carlo simulace. Výstupy se využijí k propočtu kapitálového požadavku přístupem VaR. Pokud vycházíme z předpokladu úplné korelace rozdělení ztrát průřezově kombinacemi obchodní linie a typ události, dá se celkový kapitálový požadavek stanovit jako suma hodnot VaR všech kombinací. Pokud předpokládáme nižší než úplnou korelaci, bude kapitálový požadavek nižší. Nevýhodou metody je přílišné soustředění se na interní data, předpoklad relativně statického prostředí, neschopnost reagovat na nové typy událostí.

Metody analýzy scénářů

Aplikace praktického přístupu tvorby variantních scénářů byla v minulosti bankami používána především při řízení rizika likvidity, které je rovněž do značné míry závislé na empirii. Principem je tvorba scénářů možného budoucího vývoje expozice banky v operačním riziku a jejich analýza. Scénáře v principu popisují hypotetický vývoj s ohledem na události operačního rizika. Jako vstupní data banka využívá jednak konkrétní externí a interní statistická data operačního rizika a externí a interní expertízy prostředí, ve kterém podniká. Vychází z historických údajů, nebo pracuje s hypotézami. Tyto údaje pak využívá jako vstupy vícekriteriálního analytického hodnocení. Scénáře se mohou vytvářet na různě dlouhá časová období, lze uplatnit horizont jednoho roku, ale také kratší či delší, a to pro banku jako celek, pro její vybrané linie nebo pro všechny formulované linie. Horní limit pro počet vytvořených scénářů je závislý především na nákladech a efektivní interpretaci výsledků. Minimálně se tvoří tři scénáře-optimistický, pesimistický a scénář předpokládaného vývoje neboli modální. Na místě je také sestavení stresového testování pro nejhorší možné situace. Důležitou součástí úspěšné aplikace je zpětné testování, které umožní při tvorbě nových scénářů či upřesňování stávajících uplatňovat pravděpodobnější varianty. Přístup je vhodný pro simulaci hypotetických událostí s velmi malou četností výskytu a zároveň významným dopadem do hospodářského výsledku banky.

Analýza scénářů je jednou ze složek, které vstupují do propočtu kapitálového požadavku k operačnímu riziku. Banky mají k dispozici údaje o událostech operačního rizika s častým výskytem, se kterými se převážně pojí nízký až střední dopad do hospodářského výsledku. Data, kterými banky příliš nedisponují, se vztahují k málo četným událostem s vysokým dopadem. Scénáře se musí soustředit především na odhady expozic banky vůči takovýmto událostem. Hlavní nevýhodou scénářů je silné zastoupení subjektivní složky měření. Výhoda spočívá v možnosti používat je jako prediktivní nástroj, případně formulovat jako scénáře zátěžové. Scénáře se také uplatňují při identifikaci slabých míst,

chybějících kontrol a působit preventivně ve smyslu odvrácení významných ztrát s vynaložením nízkých nákladů.

Když banka zvažuje, které oblasti by měly být předmětem tvorby scénářů, může vycházet z výsledků sebehodnocení, ale je žádoucí, aby ke každé kategorii rizika byl vytvořen scénář. Samotná konstrukce scénáře by měla být prováděna s vysokou mírou detailu, veškeré kroky by měly být podrobně popsány. Pouze za tohoto předpokladu lez provést solidní odhady četnosti a dopady do hospodářského výsledku ve struktuře průměrného očekávaného dopadu a maximálně možného dopadu. Součástí popisu scénáře by měl být i popis souboru faktorů, které mohou vést ke změně četnosti výskytu rizikové události. Je žádoucí, aby interní audit posoudil relevanci odhadů a zároveň posoudil, zda veškeré uplatněné postupy v rámci scénáře jsou v souladu s vnitřními předpisy banky i regulatorními požadavky. Scénáře mohou fungovat opakovaně, je možné je aktualizovat nebo je přestat používat a soustředit se formování nových.

Metody ukazatelů

Metody ukazatelů vychází z rozdělení banky na jednotlivé procesy, které se poté seskupí do tzv. *obchodních linií*. Pro každou či každou sledovanou obchodní linii se potom určí soubor ukazatelů (scorecard), který indikuje operační riziko v rámci příslušné obchodní linie, resp. příslušného procesu. Výběr vhodných ukazatelů je rozhodující pro odpovídající hodnocení rizikového profilu dané obchodní linie. Při výběru se postupuje tak, že vedoucí pracovníci jednotlivých obchodních linií formulují sadu otázek, aby označily možné zdroje rizika v dané obchodní linii. Odpovědi jsou potom využity na tvorbu tzv. risk scores normalizací k hodnotě 1 (např. 0,5 - 1,5) pro každou kombinaci obchodní linie a typu rizika s tím, že lepší hodnocení představuje nižší rizikový ukazatel a naopak. Důležité je, aby ukazatele signalizovaly změnu (negativní i pozitivní) v rámci odpovídající linie a tím reagovaly na zvýšení či snížení výskytu operačního rizika. Nemusí jít tedy nutně o přímé měření operačního rizika, ale o indikátory, jejichž sledování zprostředkovaně pomáhá hodnotit výskyt a význam operačního rizika. Určení vhodných indikátorů by mělo být výsledkem důkladné analýzy a v pravidelných časových intervalech by banka měla hodnotit vhodnost výběru a dosahované výsledky. Pro banku je prospěšné brát v úvahu historická data, ale je třeba postupovat obezřetně při snaze extrapolovat minulý vývoj.

Metoda vnitřních měření

Předpokladem statistické metody vnitřních měření (*Internal Measurement Approach, IMA*) je lineární závislost mezi vývojem očekávaných a neočekávaných ztrát. Při analyzování procesů, kde může být přítomno operační riziko, banka zaznamenává náhodné události a čas jejich výskytu. Potom pro určený časový interval, např. jeden rok, hodnotí četnost a významnost sledovaných událostí. Aby se celý postup usnadnil, vychází banka při výpočtu neočekávaných ztrát operačního rizika ze znalosti ztrát očekávaných s tím, že použije parametr, kterým provádí konverzi očekávané ztráty v neočekávanou. Pokud banka tento postup provádí v rámci jednotlivých obchodních linií, vyjadřuje celkové operační riziko následným součtem velikostí neočekávaných ztrát za jednotlivé linie, a tak získá údaj za celou banku.

Kapitálový požadavek je vypočítán na základě očekávané ztráty s tím, že každá obchodní linie má určen indikátor expozice (*Exposure Indicator, EI*), který vyjadřuje pravděpodobnost vzniku ztráty (*Probability*

of Event, PE). V případě, že ztráta nastane, vyjadřuje ji parametr velikost ztráty (Loss Given Event, LGE). Očekávanou ztrátu lze vyjádřit:

$$EI \,.\, PE \,.\, LGE = N\mu \,.\, n/N \,.\, \mu L/\, \mu = EL$$

Kde:
EI je indikátor expozice
PE je pravděpodobnost vzniku ztráty
LGE je velikost ztráty
N je celkový počet transakcí
μL je průměrná velikost ztráty
μ je průměrná částka transakce
n je počet událostí
EL je očekávaná ztráta

Souhrnný požadavek na kapitál získáme jako sumu očekávaných ztrát vynásobenou faktorem identifikujícím každou z obchodních linií.

Kauzální metody

Při aplikace kauzální metody banka musí nejprve formulovat vztahy příčiny a důsledku tím, že hledá vazby mezi procesy a rizikovými projevy. Klíčová je identifikace rizikových faktorů. Pro určení pravděpodobností jednotlivých prvků banka používá Bayesovskou teorii, pro kterou je charakteristické, že dynamicky reaguje na změny. Výsledkem je pravděpodobnostní rozložení operačních ztrát, ke kterému se dospěje na základě zjištění pravděpodobnostního výskytu rizikových faktorů. Výhodou kauzálního přístupu je jednak možnost zahrnovat nové informace a jednak možnost zahrnutí dosti úplného souboru rizikových faktorů. Tento přístup nepracuje s lineárním vztahem mezi změnami rizikových faktorů a změnami dopadu do čistého příjmu banky, což zvyšuje jeho přesnost, ale zároveň složitost konstrukce.