

Řízení finančních a bankovních rizik



**SLEZSKÁ
UNIVERZITA**

OBCHODNĚ PODNIKATELSKÁ
FAKULTA V KARVINĚ

FIU/BPFPM

Ing. Roman Hlawiczka, Ph.D.

Katedra financí a účetnictví

1. Jaký je rozdíl mezi financovanými a nefinancovanými nástroji transferu úvěrového rizika?
 2. Co znamená zkratka SPV/SPE?
 3. Jak se v případě transferu úvěrového rizika projevuje zastupitelský problém?
 4. Proč není dokončena/uskutečněna významná část prodejů úvěrů na sekundárním trhu?
 5. Jaké jsou možnosti úvěrového posílení cenných papírů emitovaných při sekuritizaci?
-

6. Co je podstatou syntetické sekuritizace?
 7. V čem spočívá riziko toho, že u sekuritizace není dosaženo skutečného prodeje?
 8. Čím se liší swap úvěrového selhání od swapu veškerých výnosů?
 9. Firma ví, že v budoucnu bude potřebovat čerpat úvěr. Obává se však, že dříve, než bude úvěr čerpat, mohlo by dojít k zhoršení jejího ratingu, což by úvěr prodražilo. Jak se proti zdražení může zajistit?
 10. Co se stane s opcí selhání, pokud dlužník řádně splácí? V jaké výši bude mít banka náklady na tuto opci?
-

1. U financovaných nástrojů poskytuje subjekt kupující riziko platbu na krytí tohoto rizika předem, u nefinancovaných nástrojů až poté, co nastane úvěrová událost.
 2. Special purpose vehicle/special purpose entity, speciální jednotka, tj. zprostředko-vatel, který vstupuje mezi kupujícího a prodávajícího u nepřímého transferu úvěro-vého rizika.
 3. Banka sice nadále shromažďuje splátky od dlužníka, ale už má mnohem menší zá-jem na tom monitorovat jeho bonitu.
 4. Proces prodeje úvěrů je velmi komplexní záležitost, trvá dlouho vše připravit a me-zitím se můžou natolik změnit tržní ceny, že původní nabídka je již nezajímavá.
-

5. Vnější úvěrové posílení: neodvolatelná bankovní záruka, pojištění třetí stranou, li-kvidní podpora. Vnitřní úvěrové posílení: účet rozpětí, účet hotovostního kolaterálu, překolateralizace, tranšování.
6. Dochází k převodu pouze úvěrového rizika, nikoliv k převodu vlastnictví původních expozic.
7. Nedojde-li ke skutečnému převodu úvěrového rizika na jiný subjekt, v případě zhoršení kvality aktiv může banka pocítit ztráty, nekryté kapitálem.
8. Swap úvěrového selhání představuje ochranu proti ztrátě v důsledku přesně specifi-kované úvěrové události, swap veškerých výnosů důvody selhání neřeší.



9. Použije call opci úvěrového rozpětí.

10. Banka opci selhání nevyužije, náklady budou rovny opční prémii.



**SLEZSKÁ
UNIVERZITA**
OBCHODNĚ PODNIKATELSKÁ
FAKULTA V KARVINĚ

OPERAČNÍ A TRŽNÍ RIZIKO

Operační a tržní riziko patří vedle úvěrového mezi nejvýznamnější typy rizik, která banka musí řídit.

Zatímco úvěrové riziko vychází ze závazků klientů, **operační riziko** souvisí s vnitřní činností banky a **tržní riziko** s pohyby cen, úrokových sazeb a měn.

Cílem kapitoly je porozumět, jak tyto rizikové faktory vznikají, jak se měří a jakými metodami se řídí, aby neohrozily stabilitu banky.

vymezit podstatu a složky operačního a tržního rizika, ukázat metody měření, rámce řízení a regulatorní požadavky; propojit s aktuálními změnami v EU po roce 2024. V návaznosti na studijní oporu si osvojíte terminologii (VaR, durace, beta, delta), principy limitů a stresových testů, včetně vazby na kapitálovou přiměřenost.

Riziko chápeme jako vyčíslitelnou možnost nepříznivé odchylky od očekávání, kdy alespoň jeden z výsledků je nežádoucí.

V bankovníctví rozlišujeme zejména:
úvěrové, tržní, likviditní a operační riziko; kapitálové riziko pak reflektuje dostatek kapitálu k pokrytí ztrát z těchto rizik.

Trendem je přechod od izolovaného k integrovanému řízení všech rizik napříč transakcemi banky.

Operační riziko: podstata, složky, řízení

Podstata: riziko ztráty vlivem selhání procesů, lidí, systémů nebo vnějších událostí; zahrnuje i porušení právních norem.

Složky (příklady): interní podvody, externí podvody, selhání IT/ICT, výpadky služeb, pochybení v procesech, právní a compliance události, škody z fyzických událostí.

Řízení: jasné pravomoci a odpovědnosti, interní kontrolní systém, limity a tolerance rizika, sběr ztrátových dat, analýza příčin, testování kontinuity, audit a reporting vedení.

Kapitál na krytí operačního rizika vychází z regulatorních přístupů (standardizovaný přístup) a zohledňuje profil banky.

DORA — jednotný rámec digitální provozní odolnosti pro finanční sektor v EU — **platí od 17. 1. 2025**; vyžaduje řízení ICT rizik, testování odolnosti, hlášení incidentů a správu třetích stran (registre smluv s ICT poskytovateli).

Podstata: riziko ztráty z nepříznivého vývoje tržních proměnných.

Složky: úrokové riziko (změna sazeb), měnové riziko (kurzy), akciové riziko (kurzy akcií), komoditní riziko (ceny komodit). Měříme a řídíme pomocí citlivostí (durace, beta, delta), gap analýz, VaR, stresových testů a limitů.

balíček CRR3/CRD6 dokončuje implementaci Basel III v EU od **1. 1. 2025**; tržní riziko (FRTB) má **odloženou závaznou aplikaci do 1. 1. 2027** (EU rozhodnutí 06/2025).

Do té doby běží reporting a příprava modelů/standardizace.

Video „What’s New at CFI | Operational Risk Management in Banks” se zaměřuje přímo na **operační riziko** v bankovníctví – rozděluje jeho hlavní dimenze a dává příklady z praxe.

https://youtu.be/kRA-vQCZ2O0?si=dLV7bLYsJWe_saBp



Téma: „What is Market Risk? | How to Manage Market Risk?“ — pokrývá klíčové složky tržního rizika (úrokové, měnové, komoditní, akciové) a také způsoby, jak jej řídit.

<https://youtu.be/TE8uxeBmzRc?si=fhpPnVFT3iGW8MS->

Měření tržního rizika umožňuje kvantifikovat potenciální ztrátu vyplývající z nepříznivého pohybu tržních faktorů.

Základní přístupy:

- **Metody citlivosti** – měří dopad změny určité veličiny (např. změna úrokové sazby o 1 % → změna hodnoty portfolia).
 - **Value at Risk (VaR)** – pravděpodobnostní metoda udávající maximální možnou ztrátu při dané hladině spolehlivosti (např. 99 %) a časovém horizontu.
 - **Stresové testy a scénářová analýza** – zkoumají dopady mimořádných pohybů (např. prudké zvýšení sazeb, geopolitické šoky).
 - **Backtesting** – porovnává skutečné a modelové ztráty za minulé období.
-

EU rámec FRTB (Fundamental Review of the Trading Book)
rozlišuje standardizovaný a interní modelový přístup; v ČR probíhá
jejich implementace pod ČNB.

Citlivostní analýza měří, jak se mění hodnota portfolia v závislosti na malé změně vybraného faktoru.

Nejpoužívanější ukazatele:

- **Durace** – měří citlivost ceny dluhopisu na změnu úrokové sazby.
- **Delta** – změna hodnoty derivátu při změně ceny podkladového aktiva.
- **Beta** – citlivost výnosu akcie vůči výnosu trhu (systematické riziko).
- **Gamma, Vega, Rho** – druhořadé derivace pro derivátové pozice.

Příklad: pokud durace portfolia = 4, pak růst sazeb o 1 p. b. sníží hodnotu o $\approx 4\%$.

Pozn.: EU doporučení (EBA, 2024) zahrnuje citlivostní analýzu do stress testů pro tržní riziko v bankovní knize.

Definice: VaR = maximální ztráta, kterou portfolio nepřekročí s pravděpodobností $X\%$ během stanoveného období.

Např. VaR = 10 mil. Kč při 95% = pravděpodobnost 5% , že ztráta přesáhne 10 mil. Kč.

Základní metody výpočtu:

1. Historická simulace – využívá reálné historické změny cen.
2. Kovarianční metoda – předpokládá normální rozdělení výnosů a lineární vztahy.
3. Monte Carlo simulace – generuje tisíce náhodných scénářů vývoje trhu.

Význam: banky musí VaR reportovat v rámci kapitálových požadavků (Basel III, CRR3).

EBA v roce 2025 přechází na přísnější standard Expected Shortfall (ES) pro modely FRTB.

Stresové testování a scénářová analýza

Cílem je ověřit odolnost portfolia v extrémních situacích.

Typy testů:

- **Hypotetické scénáře** – např. náhlý růst inflace o 5 p. b., pád akciových trhů o 20 %.
- **Historické scénáře** – např. opakování krize 2008 nebo energetického šoku 2022.
- **Reverse stress testing** – hledání kombinace událostí, která by vedla k insolvenční.

Stresové testy jsou součástí procesu ICAAP a reportingu ČNB.

Od roku 2024 je EBA vyžaduje zahrnout do digitálních odvětví i v rámci rámce DORA – tedy testování odstávky IT, kyberútoku či ztráty dat.

Cílem řízení tržního rizika je minimalizovat pravděpodobnost a dopad ztrát z nepříznivého vývoje tržních proměnných.

Základní kroky v procesu:

1. Identifikace všech pozic v obchodní i bankovní knize.
 2. Měření rizika (především VaR, stres testy a citlivostní analýzy).
 3. Stanovení limitů a tolerancí rizika.
 4. Monitoring a reporting řízení rizika v rámci vnitřního kontrolního systému.
 5. Reakce a úprava pozic – např. hedging, diverzifikace, řízení durace.
-

V praxi jsou limity nastaveny na úrovni portfolioů i celé banky a podléhají schválení řízení rizik a představenstva.

Aktuálně (2025): ČNB požaduje detailní evidence všech pozic v rámci denních reportů o tržních rizicích.

Limity – stanovují maximální povolené ztráty nebo otevřené pozice (např. měnové pozice v USD $\leq 2\%$ kapitálu banky).

Diverzifikace – rozložení aktiv mezi různé třídy (např. akcie, dluhopisy, komodity), země, sektory či měny, aby se snížila korelace výnosů.

Hedging – zajištění pozic pomocí finančních nástrojů (deriváty – forwardy, futures, swapy, opce).

Příklad:

- Firma má úvěr v EUR → zajišťuje se měnovým forwardem na CZK/EUR.
- Banka má portfolia dluhopisů → zajišťuje úrokové riziko pomocí interest rate swapu (IRS).

Poznámka pro praxi: od roku 2025 musí všechny banky v EU reportovat tzv. **hedge effectiveness testing** (EBA ITS 2024) – tj. ověření účinnosti zajištění v modelu VaR.

Příklad řízení tržního rizika v české bance

Příklad – Komerční banka (ČSOB i KB):

- Provádí měření VaR denně – hladina spolehlivosti 99 %, horizont 1 den.
- Provádí měsíční stresové testy scénářů (EBA metodika).
- Řídí úrokové riziko v bankovní knize (IRRBB) pomocí analýzy GAP a durace.
- Měnové riziko řídí prostřednictvím centrálního treasury, včetně zajišťovacích transakcí.
- Tržní limity jsou integrovány do interního systému ORACLE a všechny překročení jsou automaticky hlášena.

Poznámka: ČNB v roce 2025 aktualizovala „Zprávu o finanční stabilitě“ – potvrzuje, že hlavní riziko pro české banky zůstává úrokové a měnové, nikoliv akciové.

Řízení ICT a digitálních operačních rizik (DORA 2025)

Nařízení **DORA (Digital Operational Resilience Act)** platí od 17. ledna 2025 a představuje nový pilíř řízení operačního rizika v EU finančním sektoru.

Zaměřuje se na:

- **Řízení ICT rizik** – požadavek na řízení kybernetické bezpečnosti, identifikaci a prevenci incidentů.
 - **Oznamování incidentů** – do 24 hodin od zjištění kyberútoku.
 - **Testování odolnosti systémů** – povinné red teamingové testy pro kritické subjekty.
 - **Řízení třetích stran** – evidence a kontrola všech externích ICT dodavatelů a smluv.
-

Praktický dopad:

banky musí vytvořit nové pozice CRO/ICT Risk Officer a mít plány kontinuity a obnovy služeb (Business Continuity Plan).

EBA a ČNB v roce 2025 provádějí první přezkum shody DORA v bankovním sektoru ČR.

VaR (Value at Risk)

→ Maximální možná ztráta portfolia při dané hladině spolehlivosti (např. 99 %) a časovém horizontu.

ES (Expected Shortfall)

→ Průměrná ztráta přesahující hodnotu VaR; nový přísnější ukazatel podle Basel III / CRR3.

EBA (European Banking Authority)

→ Evropský orgán pro bankovníctví – vydává standardy a metodiky pro řízení rizik v EU.

CRR3 / CRD6

→ Nařízení a směrnice EU o kapitálových požadavcích bank (Basel III v EU).

FRTB (Fundamental Review of the Trading Book)

→ Reforma měření a řízení tržního rizika v rámci Basel III.

DORA (Digital Operational Resilience Act)

→ Nařízení EU o digitální provozní odolnosti finančního sektoru – platné od 17. 1. 2025.

ICT (Information and Communication Technology)

→ Informační a komunikační technologie; součást řízení operačního rizika a kyberbezpečnosti.

IRRBB (Interest Rate Risk in the Banking Book)

→ Úrokové riziko v bankovní knize – vliv změn sazeb na zisk a kapitál.

CRO (Chief Risk Officer)

→ Vrcholový manažer odpovědný za řízení všech druhů rizik v bance.

BCP (Business Continuity Plan)

→ Plán kontinuity podnikání – zajišťuje obnovu provozu po incidentu nebo výpadku.

Řízení operačního rizika zahrnuje systematický proces, jehož cílem je minimalizovat ztráty způsobené selháním lidí, procesů, systémů nebo vnějšími událostmi.

Základní fáze procesu:

1. Identifikace rizik – mapování činností a procesů, kde může dojít ke ztrátě (např. IT systémy, pokladní operace, platební styk).

2. Měření a hodnocení – klasifikace podle pravděpodobnosti a dopadu; využívají se kvantitativní modely (např. ztrátové databáze, scoring).

3. Řízení a mitigace – návrh kontrol, pojištění, automatizace nebo organizační změny.

4. Monitoring a reporting – pravidelné sledování klíčových ukazatelů a reporting vedení.

5. Zpětná vazba a zlepšení – analýza incidentů, implementace nápravných opatření.

Proces musí být součástí **vnitřního kontrolního systému (ICS)** a **strategie řízení rizik banky (Risk Appetite Framework)**.

Banka si volí způsob výpočtu kapitálového požadavku podle svého profilu a regulatorních možností:

1. Základní indikátorový přístup (BIA)

→ Kapitál = 15 % z průměrného hrubého výnosu za poslední 3 roky.

Jednoduchý, ale nereflektuje rizikový profil.

2. Standardizovaný přístup (SA-OR)

→ Rozděluje výnosy do 8 obchodních linií a používá různé váhy rizika.

Používaný většinou českých bank v současnosti.

3. Pokročilý přístup (AMA – Advanced Measurement Approach)

→ Banka využívá vlastní model založený na interních datech o ztrátách, externích databázích (např. ORX), kontrolním prostředí a scénářové analýze.

Vyžaduje schválení dohledovým orgánem (ČNB).

Aktuálně 2025: EBA schválila zrušení AMA a jeho náhradu **novým standardizovaným přístupem (SMA)** podle Basel III, který kombinuje výnosové a ztrátové ukazatele.

Key Risk Indicators (KRI)

KRI jsou měřitelné ukazatele, které signalizují změnu v úrovni operačního rizika.

Používají se ke sledování trendů, včasnému varování a k rozhodování managementu.

Typické KRI:

- Počet interních a externích incidentů za měsíc.
 - Počet chyb v platbách nebo v účetních zápisech.
 - Výpadky IT systémů (počet hodin nefunkčnosti / rok).
 - Počet nevyřízených reklamací.
 - Počet neautorizovaných přístupů do systému.
 - Počet auditních zjištění nebo nedostatků compliance.
-

Doporučení: KRI musí být pravidelně validovány a propojeny s ukazateli výkonnosti (KPI) – např. pokud roste počet incidentů, má se snížit limit nebo upravit proces.

V roce 2025 EBA doporučuje využívat **automatizované dashboardy** pro monitoring KRI v reálném čase.

Příklady operačních incidentů a ztrát



Typ incidentu	Popis / Příklad	Dopad
IT výpadek	Selhání platebního systému v důsledku aktualizace SW	Finanční ztráta, poškození reputace
Kybernetický útok	Phishing, malware, DDoS na clientský portál	Porušení bezpečnosti dat, náklady na obnovu
Lidská chyba	Chybná platba nebo zadání částky	Náhrady škod, procesní náklady
Právní riziko	Pokuta za porušení GDPR	Sankce, reputační dopad
Externí událost	Povodeň, požár, pandemie	Fyzická ztráta majetku, přerušení činnosti

- Roste počet kybernetických útoků typu *ransomware* na finanční instituce (např. útok na Bank of America, 2025).
 - EBA vyžaduje, aby banky uchovávaly **historii incidentů min. 10 let** a prováděly jejich analýzu v rámci ICAAP.
-

Měření ztrát z operačního rizika

Měření operačního rizika je založeno na sběru dat o historických ztrátách a jejich statistickém vyhodnocení.

Cílem je odhadnout pravděpodobnost a rozsah budoucích ztrát, které mohou nastat.

Typy ztrátových dat:

- **Interní data:** zaznamenané incidenty v rámci banky (např. výpadky, chyby, pokuty).
- **Externí data:** sdílená databáze (např. ORX – *Operational Riskdata eXchange*).
- **Scénářová data:** expertní odhady pro málo časté, ale závažné události (např. pandemie, útoky).

Základní ukazatele:

- **Počet incidentů (frequency)**
- **Výše ztrát (severity)**
- **Kumulovaná ztráta (aggregate loss)**

V roce 2025 banky přecházejí na jednotný systém reportingu ztrát podle nového **EBA Data Dictionary** pro operační riziko.

Model LDA využívá statistické rozdělení pravděpodobnosti k odhadu celkového rizika ztráty.

Používá se zejména u větších bank v rámci pokročilých přístupů.

Základní princip:

1. Odhadni rozdělení počtu incidentů (např. Poissonovo rozdělení).
 2. Odhadni rozdělení výše ztrát (např. log-normální rozdělení).
 3. Vygeneruj simulací možné kombinace událostí → získej **distribuci celkových ztrát**.
 4. Urči hodnotu VaR nebo ES při dané hladině spolehlivosti.
-

Výhoda: umožňuje přesnější kvantifikaci než standardní přístupy.

Nevýhoda: vysoké nároky na kvalitu dat, validaci a dohledový souhlas ČNB.

Aktuálně 2025: přechod z AMA na **SMA (Standardized Measurement Approach)** – hybridní přístup kombinující výnosy a ztráty.

Scénářová analýza operačních rizik

Scénářová analýza doplňuje kvantitativní modely o expertní odhad dopadů extrémních, ale realistických událostí.

Používá se tam, kde chybí dostatek historických dat.

Postup:

1. Identifikace extrémních scénářů (např. výpadek datového centra, ztráta dat klientů).
2. Odhad pravděpodobnosti a finančního dopadu (v mil. Kč).
3. Vyhodnocení kumulovaných dopadů na kapitál a likviditu.
4. Zahrnutí do plánů kontinuity (BCP) a testů odolnosti.

Aktuální trend: integrace scénářů DORA do ICAAP a ILAAP – propojení operačního, IT a likviditního rizika.

EBA 2025 vyžaduje provádění scénářové analýzy alespoň 1× ročně.

Kapitálový požadavek k operačnímu riziku (SMA 2025)

Od roku 2025 se podle Basel III a CRR3 používá **Standardized Measurement Approach (SMA)**:

nahrazuje dřívější přístupy BIA, SA a AMA.

Vzorec:

Kapitálový požadavek = *Business Indicator Component (BIC)* × *Internal Loss Multiplier (ILM)*

- **BIC** – odráží velikost banky (výnosy, úroky, poplatky).
- **ILM** – reflektuje skutečné historické ztráty banky.

Interpretace:

Čím vyšší jsou ztráty z minulých incidentů, tím vyšší je ILM a tedy i kapitálová rezerva.

Praktický dopad pro české banky (2025):

- Banky s kvalitním řízením rizik a nízkými ztrátami dosáhnou snížení kapitálové náročnosti o 5–10 %.
- Instituce s častými incidenty naopak zaznamenají nárůst kapitálového požadavku až o 15 %.

Základní zkratky používané v řízení rizik

VaR (Value at Risk) – maximální možná ztráta portfolia při dané hladině spolehlivosti.

ES (Expected Shortfall) – průměrná ztráta přesahující VaR (Basel III / CRR3).

EBA (European Banking Authority) – evropský orgán pro bankovníctví a dohled.

CRR3 / CRD6 – nařízení a směrnice EU o kapitálových požadavcích bank (Basel III v EU).

FRTB (Fundamental Review of the Trading Book) – reforma měření tržního rizika.

DORA (Digital Operational Resilience Act) – nařízení EU o digitální odolnosti finančního sektoru (od 17. 1. 2025).

ICT (Information and Communication Technology) – informační a komunikační technologie, součást operačního rizika.

IRRBB (Interest Rate Risk in the Banking Book) – úrokové riziko v bankovní knize.

CRO (Chief Risk Officer) – vrcholový manažer odpovědný za řízení rizik.

BCP (Business Continuity Plan) – plán kontinuity podnikání po incidentu.

ICAAP / ILAAP – interní proces hodnocení kapitálové a likviditní adekvátnosti.

KRI (Key Risk Indicator) – klíčový ukazatel rizika.



KPI (Key Performance Indicator) – ukazatel výkonnosti, navázaný na KRI.

BIA / SA-OR / AMA / SMA – různé přístupy Basel k měření operačního rizika (aktuálně SMA od 2025).

LDA (Loss Distribution Approach) – modelování distribuce ztrát z operačního rizika.

ILM / BIC – součásti vzorce SMA (Internal Loss Multiplier / Business Indicator Component).

ERM (Enterprise Risk Management) – integrované řízení všech rizik v organizaci.

ORX (Operational Riskdata eXchange) – mezinárodní databáze incidentů operačního rizika.

ICS (Internal Control System) – vnitřní kontrolní systém banky.

Operační a tržní riziko jsou vzájemně provázané — události v jedné oblasti často vyvolávají dopady v druhé.

Příklady propojení:

- **Selhání IT systému obchodní platformy** → neschopnost uzavřít pozice → vznik tržní ztráty.
 - **Lidská chyba při zadávání obchodního příkazu** → nesprávná expozice na trhu → finanční ztráta.
 - **Porušení limitů v důsledku chybného datového přenosu** → neoprávněné rizikové pozice.
 - **Kyberútok na bankovní infrastrukturu** → výpadky dat a zpožděné zajišťovací operace.
-

Moderní řízení rizik proto sleduje *vazby mezi druhy rizik* a zavádí **integrované modely hodnocení dopadů**.

V roce 2025 EBA doporučuje aplikovat princip "**holistic risk view**", tj. jednotný pohled na všechny rizikové kategorie (EBA/GL/2025/03).

Integrované řízení rizik (Enterprise Risk Management – ERM)



**SLEZSKÁ
UNIVERZITA**
OBCHODNĚ PODNIKATELSKÁ
FAKULTA V KARVINĚ

ERM představuje strategický rámec, který sjednocuje řízení všech druhů rizik – úvěrového, tržního, operačního, likviditního, reputačního i strategického.

Hlavní pilíře ERM:

- 1. Riziková kultura** – odpovědnost všech zaměstnanců, transparentní komunikace.
 - 2. Risk Appetite Framework** – definice míry rizika, kterou je organizace ochotna akceptovat.
 - 3. Governance** – tříúrovňová struktura řízení: představenstvo – CRO – interní audit.
 - 4. Integrované systémy** – jednotná databáze pro všechna rizika, datová analytika, reporting.
 - 5. Strategická vazba** – řízení rizik propojeno s plánováním, rozpočty a výkonností.
-

Cíl ERM: posílit stabilitu, zvýšit důvěru investorů a snížit volatilitu ziskovosti.

V roce 2025 se ERM opírá o rámce **COSO ERM** a **ISO 31000:2018**.

Účinné řízení rizik vyžaduje kvalitní reporting, kontrolu a nezávislý dohled.

Základní principy:

- **Pravidelný reporting** vedení a představenstvu (měsíční / kvartální).
 - **KPI a KRI dashboardy** – přehled trendů a výstražných signálů.
 - **Interní audit** – ověřuje účinnost procesů řízení rizik.
 - **Compliance funkce** – sleduje dodržování legislativních a etických norem.
 - **Whistleblowing kanály** – podporují včasné odhalení pochybení.
-

EBA Guidelines 2024: banky musí zajistit přímé propojení mezi **risk reportingem** a **strategickým řízením** – tedy, že informace o rizicích ovlivňují rozhodování managementu.

V České republice ČNB požaduje, aby součástí každoroční zprávy o řízení rizik bylo i **vyhodnocení incidentů dle rámce DORA**.

Příklad: UniCredit Bank Czech Republic and Slovakia, a.s.

Situace:

V roce 2024 banka čelila výpadku platebního systému způsobenému chybou při aktualizaci software třetí strany.

Událost byla klasifikována jako **operační incident** dle rámce DORA.

Postup řešení:

- Okamžitá aktivace **Business Continuity Plánu (BCP)**.
- Obnovení provozu do 4 hodin, hlášení incidentu ČNB a EBA do 24 hodin.
- Následná interní analýza prokázala nedostatečný testovací proces dodavatele.
- Banka implementovala nový **dodavatelský management systém (Third-Party Risk Management)**.

Výsledek:

- Ztráty 7 mil. Kč → plně pokryty rezervou na operační riziko.

• Incident slouží jako ukázkový případ v rámci školení DORA readiness (2025).

Shrnutí kapitoly

Řízení operačního a tržního rizika je klíčovým pilířem stability každé finanční instituce.
Moderní přístup spojuje měření, prevenci a kulturu odpovědnosti za riziko.

Hlavní myšlenky:

- Operační riziko vyplývá z chyb lidí, systémů, procesů nebo vnějších událostí.
- Tržní riziko vzniká z pohybů úrokových sazeb, kurzů měn, cen akcií a komodit.
- Obě rizika jsou vzájemně provázaná a vyžadují integrovaný přístup (ERM).
- Nové regulatorní rámce (CRR3, DORA, SMA) sjednocují řízení rizik v EU.
- Efektivní reporting a kultura transparentnosti snižují dopady krizových situací.

Cíl banky: vyvážit ziskovost a bezpečnost – přijímat pouze ta rizika, která odpovídají strategii a kapitálové síle.

1. K čemu banka využívá AAA proceduru a jakou část operačního rizika chce tímto snížit?
 2. Co je regulační riziko?
 3. Jaký je rozdíl mezi přímou a nepřímou ztrátou z operačního rizika?
 4. Jak obecně fungují top-down a bottom-up přístupy pro měření operačního rizika?
 5. Co patří do úrokově citlivých aktiv a pasiv a co do úrokově necitlivých aktiv a pasiv?
 6. Jak určíme kumulativní gap?
-



-
7. Proč je důležitá volba časového období při tvorbě úrokového gapu?
 8. Jakou změnu čistého úrokového výnosu můžeme očekávat, pokud má banka více úrokově citlivých pasiv než aktiv a dojde k růstu úrokových sazeb?
 9. Co vyjadřuje durace?
 10. Jakou změnu tržní hodnoty kapitálu banky můžeme očekávat, pokud má banka po-zitivní duraci gap a dojde k růstu úrokových sazeb?
-

1. Uživatel je Autentikován, poté Autorizován pro část sítě nebo činnosti, po celou dobu je Auditována jeho činnost; procedura slouží k snížení rizika selhání informač-ních systémů.
 2. Riziko ztráty banky v důsledku nemožnosti splnit regulační opatření a riziko změny v regulatorních pravidlech.
 3. Přímá ztráta představuje finanční ztráty vznikající přímo na základě operačního selhání, kdežto nepřímá ztráta souvisí s dopadem operačního rizika na jiné druhy rizik.
 4. Metody top-down měří operační riziko komplexně pro celou banku, poté získanou hodnotu potřebného kapitálu alokují na jednotlivé jednotky či transakce. Metody bottom-up změří operační riziko jednotlivých transakcí či procesů, a z nich následně určí, kolik kapitálu na krytí operačního rizika banka jako celek potřebuje.
-



-
5. Do úrokově citlivých aktiv a pasiv patří aktiva a pasiva úročená pohyblivou úrokovou sazbou, nebo aktiva a pasiva úročená sice fixní úrokovou sazbou, avšak ve zvo-leném časovém období dojde ke změně jejich úrokové sazby. Aktiva a pasiva úro-kově necitlivá zahrnují instrumenty s pevnou úrokovou sazbou a dále akcie, podíly, stálá aktiva, kapitál, rezervy či nerozdělený zisk.
 6. Kumulativní gap je součtem periodických gapů.
 7. Při extrémně dlouhém období jsou všechna aktiva a pasiva úrokově citlivá, naopak v extrémně krátkém období úrokově necitlivá.
 8. Čistý úrokový výnos klesne.
 9. Průměrnou dobu vázanosti investice.
 10. Tržní hodnota kapitálu banky klesne.
-

Shrnutí celé kapitoly: Řízení operačního a tržního rizika

1. Vymezení a charakteristiky rizik

- Operační riziko vyplývá z běžných činností banky — selhání procesů, lidí, systémů či externí události.
 - Tržní riziko je spojeno s pohyby tržních proměnných (úrokových sazeb, měnových kurzů, akcií, komodit) a dotýká se jak bankovní kniha, tak obchodní kniha.
 - Obě rizikové kategorie jsou propojené: chyba v procesu (operační riziko) může vést k tržní ztrátě, a naopak tržní šok může vystavit slabiny v operačních procesech.
-

2. Metody měření a modelování

- Pro tržní riziko: citlivostní analýzy (durace, beta, delta), VaR (Value at Risk), stresové testy, scénářová analýza.
 - Pro operační riziko: sběr interních a externích dat o ztrátách, Loss Distribution Approach (LDA), scénářová analýza, KRI (Key Risk Indicators).
 - Nové regulační rámce: např. u operačního rizika přechod na SMA (Standardized Measurement Approach) od roku 2025; u tržního rizika implementace FRTB a posílené požadavky v EU (CRR3, CRD6).
-

Řízení rizik zahrnuje identifikaci → měření/hodnocení → řízení/mitigaci → monitoring/reporting → zpětnou vazbu. Integrovaný přístup (ERM — Enterprise

Risk Management) je klíčový pro to, aby banka nezůstávala ve „silo“ řízení jednotlivých rizik, ale aby měla jednotný pohled na všechny rizikové oblasti. Role orgánů, jako je management, představenstvo, CRO, interní audit, compliance, je kritická pro úspěšné řízení rizik. Reporting rizik (měsíční, kvartální) a KRI/KPI dashboardy pomáhají vedení banky udržet přehled o stavu rizik.

Aktuální trendy a regulační požadavky (r. 2025)

DORA (Digital Operational Resilience Act) – nařízení EU platné od 17. 1. 2025, klade důraz na digitalizaci, ICT rizika, kybernetickou odolnost, outsourcing.

V oblasti tržního rizika – implementace FRTB v EU, posun k přísnějším metrikám jako Expected Shortfall, intenzivnější stresové testování. U operačního rizika – důraz na kvalitu dat, historické ztráty, integraci s IAM modely a transparentnost pro dohledová orgány.

Budujte silnou rizikovou kulturu, kde riziko není vnímáno jen jako hrozba, ale jako nedílná součást řízení banky. Využívejte automatizované nástroje pro monitoring a reporting (např. dashboardy KRI). Pravidelně provádějte stresové testy a scénářové analýzy, včetně těch vyplývajících z DORA.

Udržujte aktuální plány kontinuity podnikání (BCP) a připravenost na ICT incidenty/out-source selhání. Sledujte vývoj regulací a metodik (EBA guidelines, Basel vývoj), aby banka zůstala v souladu a mohla efektivně řídit rizika.



VIDEO k řízení operačního a tržního rizika“

https://youtu.be/XW_274v_9F0?si=UhmfzJ0oSP-gH7RW



**SLEZSKÁ
UNIVERZITA**
OBCHODNĚ PODNIKATELSKÁ
FAKULTA V KARVÍNĚ

DISKUSE
