Západočeská univerzita v Plzni

Právnická fakulta

DIPLOMOVÁ PRÁCE

Řízení operačních rizik v bankovnictví

Plzeň 2023 Mgr. Petra Lachman

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta právnická
Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Mgr. Petra LACHMAN**
Osobní číslo:	**R18M0220P**
Studijní program:	**M6805 Právo a právní věda**
Studijní obor:	**Právo**
Téma práce:	**Řízení operačních rizik v bankovnictví**
Zadávající katedra:	**Katedra finančního práva a národního hospodářství**

Zásady pro vypracování

1. Úvod diplomové práce
2. Regulace a dohled bankovního sektoru-role ČNB
3. Řízení operačních rizik a nástroje k jejich řízení
4. Specifické druhy mitigace operačních rizik
5. Nejvýznamnější události operačního rizika za posledních 5 let
6. Aktuální operační rizika se zaměřením na Cyber risk
7. Výhled do budoucna v oblasti řízení rizik
8. Závěr diplomové práce

Rozsah diplomové práce:
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná**

Seznam doporučené literatury:

1. BLAHOVÁ, Naďa. Rizika bank a jejich regulace. Jesenice: Ekopress, 2018. ISBN 978-80-87865-47-7.
2. CIPRA, Tomáš, 2015. Riziko ve financích a pojišťovnictví: Basel III a Solvency II. Vydání I. Praha: Ekopress. ISBN 9788087865248.
3. KAŠPAROVSKÁ, Vlasta, 2006. Řízení obchodních bank: vybrané kapitoly. V Praze: C.H. Beck. Beckovy ekonomické učebnice. ISBN 8071793817.
4. NIELSEN Martin Basel IV : the next generation of risk weighted assets Basel IV : the next generation of risk weighted assets / Martin Neisen and Stefan Röth. 2nd edition. Weinheim : Wiley-VCH Verlag GnbH & Co. KGaA, [2018]. 464 stran : ilustrace ; 26 cm (Wiley finance) ISBN:978-3-527-50962--. 2nd edition. Weinheim : Wiley-VCH Verlag GnbH & Co. KGaA, [2018]. 464 stran: ilustrace ; 26 cm (Wiley finance) ISBN:978-3-527-50962
5. Zákon č. 21/1992 Sb., o bankách.
6. Zákon č. 6/1992 Sb., o České národní bance.
7. Opatření ČNB č. 2/2004, k vnitřnímu řídicímu a kontrolnímu systému banky.
8. Opatření ČNB č. 11/2002, kterým se stanoví požadavky na ověření řídicího a kontrolního systému banky včetně systému řízení rizik Směrnice CRD IV, tedy Směrnice 2013/36/ EU ze dne 26.3.2013. Vyhláška č. 163/2014 Sb., o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry.

Vedoucí diplomové práce: **Ing. Mgr. Dana Bárková, Ph.D.**
Katedra finančního práva a národního hospodářství

Datum zadání diplomové práce: **28. března 2022**
Termín odevzdání diplomové práce: **31. března 2023**

Západočeská univerzita v Plzni
L.S.
Fakulta právnická

JUDr. et PhDr. Stanislav Balík, Ph.D.
děkan

JUDr. Petra Hrubá Smržová, Ph.D.
vedoucí katedry

V Plzni dne 8. srpna 2022

Čestné prohlášení

Čestně prohlašuji, že jsem předkládanou diplomovou práci na *téma Řízení operačních rizik v bankovnictví* vypracovala samostatně, všechny použité prameny a literatura byly řádně citovány v poznámkách pod čarou a jsou uvedeny v seznamu použitých zdrojů a literatury.

V Praze dne 29.03.2023 …….

Mgr. Petra Lachman

Seznam zkratek

AML	Anti money loundering, praní špinavých peněz
AML zákon	Zákon č. 25/2000 Sb., zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu
AMA	Advanced Measurement Approaches, pokročilý přístup výpočtu kapitálové přiměřenosti
BCBS	Basel Committee on Banking Supervision, Basilejský výbor pro bankovní dohled
BIA	Basic Indicator Aproach
D&O	Directors and Officers Liability Insurance, pojištění profesní odpovědnosti členu vrcholného managementu
EBA	European Banking Authority, Evropský orgán pro bankovnictví
ECB	Evropská centrální banka
ENISA	The European Union Agency for Cybersecurity, Agentura Evropské unie pro kybernetickou bezpečnost
CEO	Chef Executive Officer, generální ředitel
CHF	Švýcarský frank
COVID 19	Pandemie nemoci COVID 19
CRD	Capital Requirements Directive, směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky
CRR	Capital Requirements Regulation, nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky
CZK	Česká koruna

ČBA	Česká bankovní asociace
ČNB	Česká národní banka
ČNBZ	Zákon č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů
DORA	Digital Operational Resilience Act, Nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru 2022/2554 ze dne 14. prosince 2022
EBA	Evropský orgán pro bankovnictví
ECB	Evropská centrální banka
EU	Evropská unie
EUR	Euro společná evropská měnová jednotka
ERM	Enterprise risk management, systém řízení rizik
IPB	Investiční a poštovní banka a.s.
IKT	Informační a komunikační technologie
KRI	Klíčové indikátory rizika
LDC	Loss data collection, sběr událostí operačního rizika
NIS	Směrnice Evropského parlamentu a Rady 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnost sítí a informačních systémů v Unii
NIS 2	Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice EU 2016/1148
NUKIB	Národní úřad pro kybernetickou a informační bezpečnost
OOP	Opatření obecné povahy
OTP	One time password, jednorázové heslo
RCSA	Risk and Control Self Assesment, proces sebehodnocení úrovně a rizik kontrol

RSTS	Raiffeisen stavební spořitelna
SNB	Švýcarská národní banka
SREP	Supervisory Review and Evaluation Process, proces dohledu a hodnocení orgány dohledu
SA	Stantartised Apprroach, standardizovaný přístup pro výpočet kapitálového požadavku k operačnímu riziku
UBS	Union des Banques Suisses
USD	United States dollar, americký dolar
ZOBa	Zákon č. 21/1992 Sb., zákon o bankách, ve znění pozdějších předpisů

Poděkování:

Tímto bych ráda poděkovala vedoucí mé diplomové práce Ing. Mgr. Daně Bárkové, Ph.D. za odborné vedení mé diplomové práce, cenné připomínky, trpělivost a čas, který mi věnovala.

Poděkování patří mé dceři Mie Elinor, manželovi a ostatním členům rodiny, kteří mě při studiu podporovali.

Obsah

Úvod

Při úvahách nad tématem diplomové práce jsem měla jasno v tom, že nechci volit téma, o kterém bylo již mnoho napsáno. Z různých možností jsem si nakonec vybrala Řízení operačních rizik v bankovnictví. Prvotní myšlenka, psát pouze prakticky o řízení operačních rizik, se ukázala jako neproveditelná. Bez teoretického úvodu se diplomová práce jednoduše neobejde.

Volba tématu nebyla náhodná, souvisela s mou profesní orientací. S operačními riziky se setkávám na denní bázi. Vidím, že bankovní prostředí se zrychluje a vyvíjí mílovými kroky. Operační rizika se dynamicky mění.

Před pár lety trval bankovní převod několik dní. Dnes s instantními platbami je platba připsána na účet příjemce do několika vteřin. Každá mince má však dvě strany. S rychlostí a změnami v procesech se pojí mimo jiné nová operační rizika. Dnes se do popředí výrazně dostávají rizika kybernetická, kterým je v práci zcela záměrně věnován prostor. Jedná se o aktuální rizika, ohrožující klienty i banky. Tato rizika generují také výrazné ztráty.

Diplomová práce je zpracována s cílem přiblížit čtenáři rámcově problematiku řízení operačních rizik v bankovnictví, teoreticky i prakticky. Tedy teoreticky, co stanoví regulátor, prakticky jakými způsoby banka regulatorních cílů dosahuje. Vytčených cílů diplomové práce by nemohlo být dosaženo bez teoretického úvodu. Ve smyslu role regulátora ČNB, jejích cílů a úloh a vysvětlení úlohy regulace a dohledu.

Diplomová práce nemá ambici stát se metodikou pro řízení operačního rizika. Jelikož metodika je vždy vypracovávána s ohledem na specifika konkrétní banky.

Zvolené téma je široké, proto jsme do diplomové práce zařadila z oblasti řízení rizik části, které považuji za zajímavé i pro čtenáře, kteří se s operačními riziky nesetkávají, profesně nezabývají.

Použité metody jsou metody popisné a analytické. V některých kapitolách jsou přidány praktické příklady. Při tvorbě práce byla použita výhradně veřejně dostupná data, která v některých případech byla přetransformována v praktický příklad. V práci se nevyskytují žádné vnitřní informace z bank.

První kapitola práce, která je zcela teoretická, pojednává o České národní bance, její úloze a cílech. Kapitola byla zařazena také z toho důvodu, že diplomová práce je vedena na Právnická fakultě. Dalším důvodem je fakt, že Česká národní banka hraje jakožto regulátor v oblasti operačních rizik významnou roli. Nelze ji tedy opomenout.

Ve druhé kapitole práce, která je rovněž teoretická, dochází k vymezení pojmů regulace a dohled, což souvisí také úzce s řízením operačních rizik. Banky operační rizika řídí, jelikož regulátor jim tuto povinnost stanovil.

Kapitola třetí pojednává o Basilejském výboru pro rizika, který sehrál ve formování pravidel pro řízení operačního rizika nezastupitelnou roli. Bez něj by operační riziko, tak jak jej známe dnes, pravděpodobně nevzniklo. Do kapitoly jsou vybrány základní a nejdůležitější body z historie. Samotné Basilejské dohody by svým rozsahem spolehlivě naplnily rozsah diplomové práce.

Kapitola čtvrtá se věnuje samostatně operačním rizikům, jejich základní definici a členění z pohledu legislativy.

Další kapitola se věnuje v obecné rovině systému řízení operačního rizika, požadavkům na řídící a kontrolní systém, základním fázím procesu řízení operačních rizik, požadavkům na obezřetnost a odbornou péči a další.

Kapitola šestá, sedmá a osmá navazují na kapitolu předchozí. Kapitoly se věnují způsobům identifikace, měření a řízení operačních rizik. Každé téma v kapitole zvolené je obsáhlé. Z tohoto důvodu jsem volila variantu samostatných kapitol.

V kapitole deváté se dostávám k praktickým příkladům selhání některého mechanismu u řízení rizik. Případně v definovaných příkladech dochází k selhání více faktorů najednou. Kapitoly jsou obohaceny o příklady. Co se týče výběru událostí, vybírala jsem ty události, které jsou z mého pohledu signifikantní. To, že jsem příklady vybrala pravděpodobně dobře, ukazuje dynamičnost dění kolem Credit Suisse v posledních dnech.

Kapitola desátá se věnuje aktuálním kybernetickým rizikům, která ohrožují banky i klienty. Problematice kybernetických rizik se věnují každý den i média.

Poslední kapitola navazuje na předchozí. Zamýšlí se nad tím, jak dnes již platné regulatorní změny v oblasti řízení rizik zasáhnou banky samotné. Jedná se o velmi aktuální téma.

1 Vymezení postavení ČNB a její role

Tato kapitola je kapitolou úvodní, klade za cíl definovat Českou národní banku (dále jen ČNB), vymezit její postavení, pravomoci a v neposlední řadě její cíle.

Abychom mohli z hovořit o České národní bance a jejich pravomocech, je třeba určit, jaké má ČNB zakotvení v právním řádu. Faktem je, že samotná existence ČNB je garantována ústavním zákonem č. 1/1993 Sb., dále jen Ústava. ČNB je věnována samostatná hlava. Ústavní zakotvení ČNB akcentuje významnost. Existence ČNB je zakotvena v hlavě šesté Ústavy v článku 98 odst.1, který zní „*Česká národní banka je ústřední bankou státu. Hlavním cílem její činnosti je péče o cenovou stabilitu; do její činnosti lze zasahovat pouze na základě zákona.“* Z tohoto ustanovení, lze vyčíst, hlavní cíle ČNB. Jedná se tedy o banku centrální, jejím hlavním úkolem je péče o cenovou stabilitu. Jedná se o cíl, který se v čase měnil. Péče o cenovou stabilitu nebyl cílem ČNB od počátku účinnosti Ústavy. Tento cíl byl do ustanovení článku 98 odst. 1 Ústavy přidán, a to novelizací provedenou ústavním zákonem č. 448/2001 Sb. Jednalo se o změnu, která souvisela se vstupem České republiky do Evropské unie (dále jen EU), ve své podstatě šlo o změnu vynucenou.[1] Implementace nového cíle ČNB byla obtížná, jelikož vládní návrh novely Ústavy byl zamítnut v Poslanecké sněmovně. Naproti tomu začlenění nově definovaného cíle do zákona o ČNB bylo schváleno.[2] Následně došlo k tomu, že Ústavní soud zrušil hlavní body novely zákona o ČNB pro rozpor s hierarchií právních norem. Hlavní problém tkvěl v tom, že zákon, nikoliv ústavní zákon, změnil a omezoval rozsah úkolů ČNB.[3] Pokud by tedy změna byla provedena ústavním zákonem, tak by takovéto řešení bylo v souladu s ústavním pořádkem.

Co se týče postavení působnosti ČNB, dle 98 odst. 2 Ústavy platí, „*že postavení, působnost a další podrobnosti stanoví zákon.“*[4] Bližší podrobnosti stanoví zákon č. 6/1993 Sb., zákon o České národní bance, (dále jen ČNBZ). V ustanovení § 1 odst.

[1] VOSTRÁ, Zuzana. Ústavní zakotvení České národní banky a bankovní unie. Právněhistorické studie [online]. 2017, vol. 47, no. 2. [cit. 26. 11. 2022]. Dostupné z: https://karolinum.cz/data/clanek/5205/PHS_47_2_0129.pdf.
[2] RYCHETSKÝ, P., LANGÁŠEK, a kol. Ústava České republiky. Ústavní zákon o bezpečnosti České republiky. Komentář. Praha: Wolters Kluwer, a.s., 2015, s.338.
[3] Nález č. 278/2001 Sb., nález Ústavního soudu ze dne 20. června 2001 ve věci návrhu na zrušení části zákona č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů.
[4] Článek 98 odst. 2 Ústavy, ve znění pozdějších předpisů.

1 ČNBZ je stanoveno, že „*Česká národní banka je ústřední bankou České republiky, orgánem vykonávajícím dohled nad finančním trhem a orgánem příslušným k řešení krize.“*[5] Z tohoto ustanovení, již lze vyčíst rámcové pravomoci ČNB. Jedná se o orgán vykonávající dohled nad finančním trhem a také orgán pro řešení krize. Přičemž ČNB je bankou ústřední. Ustanovení § 1a ČNBZ stanoví, že ČNB je součást Evropského systému centrálních bank a podílí se na plnění cílů a úkolů Evropského systému centrálních bank. Jedná se tedy o rozšíření cílů ČNB. § 1 odst. 2 ČNBZ dále uvádí, že „*Česká národní banka je právnickou osobou veřejného práva se sídlem v Praze.“* Zákonodárce definoval jasně ČNB jako právnickou osobu veřejného práva, což je pro její postavení naprosto klíčové. § 2 odst. 3 ČNBZ stanoví, že „*České národní bance jsou svěřeny kompetence správního úřadu v rozsahu stanoveném tímto zákonem a jinými právními předpisy.“* Ustanovení stanoví, ve kterých případech jsou ČNB svěřeny kompetence správního úřadu.

Podstatnou věcně právní úpravou stanovující rozsah pravomocí ČNB je zákon č. 21/1992 Sb., zákon o bankách (dále uváděn jako ZOBa), který konkrétně v ustanovení § 3a stanoví, „*Česká národní banka vykonává funkci příslušného orgánu a je zároveň určeným orgánem podle přímo použitelného předpisu Evropské unie upravujícího obezřetnostní požadavky.“*[6] Toto ustanovení cílí částečně na část šestou tohoto zákona, tedy na dohled ČNB. Dle ustanovení § 25 odst. 1 ZOBa podléhá činnost bank dohledu ČNB, přičemž se tento dohled neomezuje na dodržování pouze zákona o bankách nebo tuzemských právních předpisů.[7] Toto ustanovení upravuje dohled ČNB nad dodržováním CRR (Capital Requirements Regulation), neboli nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky. V tomto ustanovení je ČNB pověřena rolí určeného správce dle CRR.[8]

[5] §1 odst. 2 zákona č. 6/1993 Sb., ČNBZ ve znění pozdějších předpisů.
[6] SMUTNÝ, Aleš. *Zákon o bankách: komentář*. 2. vydání. V Praze: C.H. Beck, 2019. Beckovy komentáře, str.118-119.
[7] Tamtéž.
[8] SMUTNÝ, Aleš. *Zákon o bankách: komentář*. 2. vydání. V Praze: C.H. Beck, 2019. Beckovy komentáře, str.118-119.

Ráda bych zmínila ještě jeden tuzemský právní předpis, který považuji za důležitý z pohledu bank i ČNB, a to zákon č. 25/2000 Sb., zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.

Z pohledu literatury je ČNB definována „*jako ústřední banka státu, která je nezávislá na výkonné moci.*“[9] Důležitý je prvek ústřednosti a nezávislosti na moci výkonné. Cíle a role ČNB rozeberu níže.

1.1 Hlavní cíle ČNB

Co se cílů týče, tak z pohledu literatury je existence centrální banky klíčová k tomu, aby bylo zajištěno řádné fungování peněžní sféry a finanční a bankovní soustavy. Jednou z nejdůležitějších institucí, která se tyto cíle naplňuje je Česká národní banka.[10] S tímto pohledem lze souhlasit. ČNB má skutečně vliv na peněžní sféru a bankovnictví. Z mého úhlu pohledu je ČNB garantem správného, řádného a bezpečného fungování bankovní soustavy v České republice.

V posledních měsících bylo o ČNB slyšet, a to v souvislosti se zvyšováním úrokových, které se promítly do vyšších hypotečních sazeb. Těmito změnami ČNB naplňovala legislativně vytčený cíl. Pečovala o cenovou stabilitu. Je otázkou nakolik se jí to povedlo, to zhodnotíme až s odstupem času.

Hlavní cíl činností ČNB, jak již bylo řečeno výše, je primárně zakotven v Ústavě. Je otázkou, zda definice hlavního cíle právě v Ústavě je krok správným směrem. Názory se v tomto případě rozcházejí. Přikláním se k názoru, že definovat cíle ČNB by bylo možné v zákoně standartní právní síly.

Cíl ČNB je dále specifikován v ustanovení § 2 ČNBZ (zákon č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů) ČNBZ, do kterého se rovněž promítá znění Ústavy. *„Hlavním cílem činnosti České národní banky je péče o cenovou stabilitu. „Česká národní banka dále pečuje o finanční stabilitu a o bezpečné fungování finančního systému v České republice. Pokud tím není dotčen její hlavní cíl,*

[9] BAKEŠ, Milan. Finanční právo. 6., upr. vyd. V Praze: C.H. Beck, 2012. Beckovy právnické učebnice, str. 362.
[10] ŠENKÝŘOVÁ, Bohuslava. Bankovnictví. Praha: Vysoká škola finanční a správní, 2010. Eupress, str.58.

Česká národní banka podporuje obecnou hospodářskou politiku vlády vedoucí k udržitelnému hospodářskému růstu a obecné hospodářské politiky v Evropské unii se záměrem přispět k dosažení cílů Evropské unie. Česká národní banka jedná v souladu se zásadou otevřeného tržního hospodářství.“[11] Sama ČNB uvádí, *„že finanční stabilita a její analýza je jedním z klíčových úkolů ČNB*.“[12] Co se týče cenové stability, zde platí snaha ČNB dosáhnout nízké míry inflace. Inflace je v současnosti cílovaná na 2 %.[13] V roce 2023 se pohybujeme vysoko nad tímto inflačním cílem a dle ukazatelů, lze očekávat, že inflace hranicí tolerančního pásma ČNB bude součástí ekonomiky ještě několik dalších čtvrtletí. Dle prognózy ČNB zveřejněné 02. 02. 2023 se očekává návrat inflace mírně nad 2 % v roce 2024.[14] Domnívám se, že tato prognóza je optimistická.

Mezi úkoly ČNB lze zařadit dle ustanovení § 2 odst. 2 ČNBZ řadíme:

- *„ Určování a provádění měnové politiky.*
- *Vydávání bankovek a mincí.*
- *Řízení peněžního oběhu, platebního styku a zaúčtování bank, zahraničních bank vykonávajících bankovní činnosti na území České republiky prostřednictvím své pobočky a spořitelních a úvěrních družstev, pečuje o jejich plynulost a hospodárnost a podílí se na zajištění bezpečnosti, spolehlivosti a efektivnosti platebních a vypořádacích systémů a na jejich rozvoji.*
- *Výkon dohledu nad osobami působícími na finančním trhu.*
- *Rozpoznávat, sledovat a posuzovat rizika ohrožení stability finančního systému a v zájmu předcházení vzniku nebo snižování těchto rizik přispívat prostřednictvím svých pravomocí k odolnosti finančního systému, omezovat nárůst systémových rizik a udržení finanční stability a vytvářet tak makro obezřetnostní politiku; v případě potřeby spolupracovat na tvorbě makro obezřetnostní politiky s orgány státu, jejichž působnosti se tato politika týká*

[11] § 2 odst. 1 zákona č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů.
[12] Finanční stabilita: Finanční stabilita. *Česká národní banka* [online]. [cit. 04.12.2022]. Dostupné z: https://www.cnb.cz/cs/financni-stabilita/.
[13] Inflační cíl: Inflační cíl. *Česká národní banka* [online]. [cit. 04.12.2022]. Dostupné z: https://www.cnb.cz/cs/menova-politika/inflacni-cil/.
[14] Prognóza ČNB zima 2023. Česká národní banka [online]. 02.02.2023 [cit. 02.02.2023]. Dostupné z: https://www.cnb.cz/cs/menova-politika/prognoza/.

- *Provádět další činnosti, podle ZČNB a dalších právních předpisů.“* [15]

1.1.1 ČNB a její makroekonomické funkce

K tomu, aby ČNB mohla plnit svou funkci, musí mít k dispozici vhodné a efektivní nástroje.

V oblasti měnové politiky ČNB k dosažení svých cílů používá především změny v nastavení základních úrokových sazeb. Změny v nastavení úrokových sazeb iniciuje a schvaluje bankovní rada ČNB po vyhodnocení aktuálních hlavně makroekonomických prognóz. Spolu s prognózami ČNB hodnotí i rizika se změnou sazeb spojená. O výši sazeb ČNB rozhoduje osmkrát ročně.[16] Změna výše úrokových má výrazný vliv na makroekonomické prostředí České republiky. Je však třeba zdůraznit, že efekt změn výše úrokových sazeb se v ekonomice projeví s určitým časovým odstupem.

V oblasti měnové politiky hrají významnou roli devizové intervence. ČNB prostřednictvím devizových intervencí ovlivňuje měnový kurz. Devizové intervence bývají použity v případě, kdy není možno využít změnu v nastavení úrokových sazeb, jelikož tyto již klesly na nulovou úroveň a další snížení je tedy neproveditelné.[17]

V oblasti emisí bankovek mincí ve smyslu hotovostních peněž má ČNB výsadní postavení, jelikož je jediným emitentem, bankovek, mincí a pamětních mincí, což explicitně vyplývá z ustanovení § 12 ZČNB, který stanovuje: „*Česká národní banka má výhradní právo vydávat bankovky a mince, jakož i bankovky a mince pamětní.“*[18] S emisí bankovek a mincí je spjato pravidlo, zakotvené v ustanovení § 16 zákona o ČNB, které stanoví: „*Platné bankovky a mince vydané Českou národní bankou jsou zákonnými penězi ve své nominální hodnotě při všech platbách na území České republiky.“*[19]

[15] § 2 odst. 2 zákona č. 6/1993 Sb., ve znění pozdějších předpisů.
[16] Měnová politika Měnová politika [online]. Česká národní banka, [04.12.2022]. Dostupné z: https://www.cnb.cz/cs/menova-politika.
[17] RÝDL, Tomáš, Josef BARÁK, Luděk SAŇA a Petr VÝBORNÝ. Zákon o České národní bance: komentář. Vyd. 1. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR), str. 167.
[18] § 12 zákona č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů.
[19] § 16 zákona č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů.

Činnost v devizově oblasti je poslední, ne méně důležitou oblastí, které se ČNB věnuje.

1.1.2 ČNB a její mikroekonomické funkce

Prostřednictvím mikroekonomické funkce ČNB také naplňuje legislativně vytčené cíle a úkoly. Mezi mikroekonomické cíle řadíme roli banky bank, roli banky státu, regulaci a dohled.

Role banky bank znamená, že ČNB vystupuje ve vztahu k bankám komerčním jako jejich bankéř.[20] Od bank přijímá vklady, vede jim účty a provádí zúčtovací a platební operace, poskytuje jim úvěry, operuje s cennými papíry mezi centrální bankou a komerčními bankami a další.

Role banky státu je rolí ČNB spočívající v tom, že poskytuje státu a municipalitám bankovní služby.

Problematice regulace a dohledu se bude podrobněji věnovat následující kapitola.

[20] REVENDA, Zbyněk. Peněžní ekonomie a bankovnictví. 5., aktualizované vydání Praha: Management Press, 2015, str 216.

2 Bankovní regulace a bankovní dohled

Tato kapitola má za cíl osvětlit problematiku bankovní regulace a bankovního dohledu, včetně důvodů jejich vzniku.

Na vývoj bankovní regulace a bankovního dohledu mělo historicky zásadní vliv několik událostí. Stěžejní roli hrály krize, které otřásaly bankovním sektorem. Krize daly na mezinárodní úrovni vzniknout Basilejským dohodám, kterým se bude věnovat následující kapitola. Menší vliv na regulaci měly změny geopolitické situace v jednotlivých zemích.

Na vývoj bankovní regulace v České republice měla vliv 90. léta 20 století. Tato éra se vyznačuje pádem několika bankovních domů různých velikostí. Namátkou pád Union banky, Moravia banky. Mezi nejvýznamnější události lze zařadit také nucenou správu IPB banky, která patřila k největším v zemi. Tyto události ukázaly na slabiny bankovního sektoru, začalo se nahlas hovořit o tom, že situaci je třeba napravit. Vyvstala potřeba tvorby intenzivnější bankovní regulace, posílení dohledu nad bankovními ústavy (bankami, kampeličkami, záložnami, družstvy) a finančním trhem.

Je důležité správně vymezit pojmy regulace a dohled. Pojem bankovní regulace může mít v závislosti na chápání jeho smyslu dvě pojetí.

1. Širší pojetí, tedy regulace je činnost upravující podnikání ve sféře finančního trhu.
2. Užší pojetí, kde je regulace prováděna právními předpisy dochází k udílení licencí a k vydávání prováděcích právních předpisů.[21] Regulátor si také prostřednictvím regulace stanovuje své cíle.

V jiných zdrojích můžeme najít odlišné definice pojmu bankovní regulace. Regulace může být definována jako „*vytváření a vydávání specifických pravidel autorizovanými orgány na základě zákona. Tato pravidla se týkají fungování a struktury bankovního sektoru.“*[22] Jak z definice plyne, účelem regulace je vytvořit podmínky pro fungování bankovního sektoru jako takového do budoucna.

[21] JENÍK, Ivo. Dohled a regulace finančního trhu. Praha: Spolek českých právníků Všehrd, 2011, str. 25.
[22] Bankovní regulace [online]. [cit. 10.2.2023]. Dostupné z: cbaonline.cz/bankovni-regulace.

Další definice pojmu regulace, regulaci definuje jako: *„limitování určité činnosti za předem vytyčených pravidel.“*[23]Ať je k vymezení pojmu regulace použita jakákoliv definice, z mého pohledu se vždy potkají v tom, že účelem regulace je stanovit rámec. V tomto rámci se musí subjekty v něm se vyskytující pohybovat. Ve všech definicích panuje shoda na stanovování cíle regulátora prostřednictvím regulace. Pouhé stanovení cílů je nedostatečné. Je třeba zaručit i vynutitelnost regulace. Vynutitelnost je esenciální složkou. Co se základních cílů regulace, respektive regulátora týče, mezi tyto můžeme zařadit:

1. *„Stanovení podmínek pro umožnění samotného výkonu finanční nebo bankovní činnosti. Tedy stanovení rámce pro výkon činnosti.*
2. *Udělení bankovní nebo jiné licence, jakožto oprávnění k výkonu dané činnosti.*
3. *Stanovení pravidel pro výkon bankovní činnosti jako takové.*
4. *Spolupráce a výměna informací s dalšími regulátory ve smyslu regulátorů tuzemských i zahraničních.“*[24]

Velmi důležitou součástí regulace je pravomoc ČNB vydávat podzákonné právní předpisy, na základě zákona a v jeho mezích.[25] Mezi podzákonné právní předpisy můžeme zařadit:

1. Vyhlášky ČNB, přičemž zmocnění k vydávání vyhlášek je obsaženo např. v ustanovení § 22 odst.1 písm. a ZČNB, § 41 odst.3 ZČNB. Vyhlášky jsou podepisovány guvernérem a následně vyhlašovány ve sbírce zákonů.[26]
2. Opatření obecné povahy, např. OOP vydané dle § 45b odst. 1. Tedy Opatření obecné povahy stanovení horní hranice úvěrových ukazatelů, které je podstatné pro oblast poskytování spotřebitelských úvěrů.[27]
3. Úřední sdělení, kterými ČNB dle ustanovení § 49a odst. 3 ZČNB informuje *zejména o rozhodnutích bankovní rady o úrokových sazbách, o výkladových stanoviscích České národní banky, o podmínkách pro provádění obchodů České národní banky a o skutečnostech důležitých pro osoby, které působí na finančním*

[23] ZRŮST, Lukáš. Selhání subjektů finančního trhu. Praha: Wolters Kluwer, 2019. Právní monografie (Wolters Kluwer ČR), str. 48.
[24] JENÍK, Ivo. Dohled a regulace finančního trhu. Praha: Spolek českých právníků Všehrd, 2011, str. 25-27.
[25] Článek. 79 odst. 3 Ústavy, ve znění pozdějších předpisů.
[26] § 8 ZČNB, ve znění pozdějších předpisů.
[27] Opatření obecné povahy ze dne 25.11.2021, ke stanovení horní hranice úvěrových ukazatelů č. I/2021.

trhu.[28]*Úřední sdělení ČNB s podepisuje člen bankovní rady a je vyhlašováno ve Věstníku.*[29]

Co je podstatné zmínit, je fakt, že existence bankovní regulace je žádoucí. Důležitá je míra regulace.

V otázce provádění regulace, je třeba, aby tato byla prováděna nestranně, nezávislými orgány. V neposlední řadě tvorba a provádění regulace nemají podléhat politickým vlivům a tlakům. Cílem regulace by mělo být vytvoření a udržení zdravého, stabilního, konkurenčního prostředí mezi bankovními domy, které bude důvěryhodné a přehledné.[30]

Dalším pojmem, které je třeba definovat je pojem bankovní dohled. Definovat tento pojem není snadné, jelikož na problematiku existuje nepřeberné množství pohledů, které se zásadně odlišují. V nejobecnější rovině lze bankovní dohled charakterizovat jako kontrolu dodržování pravidel bankovní regulace.[31] Tuto definici považuji za velmi obecnou, i když meritorně správnou. Dle odborné literatury lze dohled označit, jako zvláštní druh dozoru, který je vykonáván v samostatné působnosti veřejnoprávním subjektem odlišným od státu.[32] Tato definice je ve své podstatě správná. Z mého úhlu pohledu však může vést k částečnému smísení pojmu dohled a dozor, což není žádoucí.

2.1 ČNB jako orgán dohledu nad bankami

ČNB je od přijetí zákona č. 57/2006 Sb., kterým došlo ke sjednocení dohledu nad finančním trhem jediným dohledovým orgánem.[33]

Co se dohledu týče, ČNB při výkonu dohledu vystupuje jako orgán veřejné moci a vykonává kompetence správního úřadu v souladu s ustanovením § 1 odst. 3 ZČNB,

[28] § 49 a odst. 3 ZČNB ve znění pozdějších předpisů.
[29] § 49 a odst. 4, 5 ZČNB znění pozdějších předpisů.
[30] ZRŮST, Lukáš. Selhání subjektů finančního trhu. Praha: Wolters Kluwer, 2019. Právní monografie (Wolters Kluwer ČR), str 25.
[31] Česká bankovní asociace: Bankovní dohled [online]. [cit. 15.03.2023]. Dostupné z: https://cbaonline.cz/bankovni-dohled.
[32] HENDRYCH, Dušan. Právnický slovník. 3., podstatně rozš. vyd. V Praze: C.H. Beck, 2009. Beckovy odborné slovník, str 154.
[33] BARÁK, Josef. Česká národní banka jako orgán dohledu nad finančním trhem. Právní rozhledy. C.H.Beck, 2006, str. 1-3.

přičemž i na její činnost v tomto postavení dopadá zákon č. 500/2004 Sb., správní řád.[34] Pravomoci ČNB v dohledové oblasti jsou vymezeny v ustanovení § 44 odst. 2 ZČNB, oblast dohledu zahrnuje rozhodování o žádostech o udělení licencí, kontrolu dodržování podmínek stanovených udělenými licencemi a oprávněními, kontrolu dodržování právních předpisů, které jsou součástí platného právního řádu a mnohé další.[35]

Dohled ČNB je prováděn dvěma způsoby, a to na místě nebo na dálku. ČNB v rámci dohledu používá i analytický nástroj, kterým jsou zátěžové testy označované jako stress testy.

Dle dostupných informací ke konci roku 2021 ČNB vykonávala dohled nad 23 tuzemskými bankami (včetně pěti stavebních spořitelen),[36] dohlížela též na družstevní záložny, a v mezích právního řádu i na 20 poboček bank ze zemí EU.[37] Počet dohlížených subjektů byl tedy poměrně vysoký. ČNB v bankovním sektoru v roce 2021 provedla 28[38] kontrol, což není nízký počet, vzhledem k faktu, že v roce 2021 se Česká republika potýkala s pandemií COVID 19.

Ze zkušenosti období COVID mohu konstatovat, že ČNB svůj dohled na dálku zesílila. Banky pravidelně reportovaly větší množství dat než obvykle, zejména stav likvidity a kapitálovou přiměřenost. ČNB hodnotila kapitálovou přiměřenost velmi pečlivě. V květnu 2020[39] bylo vydáno doporučení restrikcí výplaty dividend, které se dotklo celého bankovního sektoru nejen v České republice. Na základě tohoto doporučení se měly finanční instituce zdržet výplaty dividend/podílů na zisku do konce roku 2020. Což u akcionářů vyvolalo vlnu nevole. Toto doporučení bylo novelizováno v prosinci 2020. Horizont zdržení se výplaty dividend/podílů na zisku byl prodloužen o dalších 9

[34] SMUTNÝ, Aleš. Zákon o bankách: komentář. 2. vydání. V Praze: C.H. Beck, 2019. Beckovy komentáře, str.152.
[35] § 44 odst. 2 zákona č.6/1993 Sb., o České národní bance ve znění pozdějších předpisů.
[36] Zpráva o dohledu nad finančním trhem [online]. 2021. Česká národní banka, 2022 [cit. 01.02.2023]. Str 63. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohled-financnitrh/.galleries/souhrnne_informace_fin_trhy/zpravy_o_vykonu_dohledu/download/dnft_2021_cz.pdf.
[37] Tamtéž.
[38] Tamtéž.
[39] Recommendation European Systematic Risk Board: on restriction of distributions duringtheCOVID-19pandemic [online].Dostupnéz:https://www.esrb.europa.eu/pub/pdf/recommendations/esrb.recommendation200608_on_restriction_of_distributions_during_the_COVID-19_pandemic_2~f4cdad4ec1.en.pdf.

měsíců.[40] Po modifikovaném doporučení mohly instituce provádět částečnou výplatu podílů na zisku / dividend, při splnění striktních kritérií. Proč tomu tak bylo? Primárně šlo o kapitálovou přiměřenost, respektive dostatečnou kapitálovou vybavenost jednotlivých bankovních domů. ČNB návrhy na výplatu dividend posuzovala individuálně. Cílem bylo udržení stability jednotlivých bankovních domů i celého bankovního sektoru

U dohledu jako takového je třeba akcentovat jeden aspekt. Tímto je dohledová nezávislost. jelikož poskytuje dohledovým orgánům ochranu před vnějšími tlaky. Dle literatury se jedná o tlaky politické, ale i tlaky ze strany kontrolovaných subjektů.[41] Ve světle dnešních ekonomických událostí si dokážu představit, že by ČNB mohla být vystavena politickému tlaku. Zvyšování úrokových sazeb výrazně prodražuje úvěry. Vzhledem k faktu, že státní rozpočet je v hlubokém deficitu, každé zvýšení sazeb znamená prodražení dluhu. To, že by byla ČNB pod tlakem kontrolovaných subjektů, je těžko představitelné a prakticky nerealizovatelné. Jaký tlak by mohl kontrolovaný subjekt na ČNB vyvíjet, z jakého titulu? ČNB je pro kontrolované subjekty autoritou. Nedomnívám se, že by jakýkoliv subjekt kontroly na ČNB vyvíjel tlak. Riziko zhoršených vztahů s regulátorem je příliš vysoké.

Je třeba dodat, že u nezávislosti dohledu je podstatné, aby rozhodnutí dohledových orgánů byla přezkoumatelná soudy.[42]

2.1.1 Dohled na místě

Dohled na místě je prvním typem dohledu, který je ze strany ČNB v bankách prováděn. Legislativně je dohled na místě zakotven v ustanovení § 25 odst. 1 zákona ZOBa, který stanoví. „*Činnost bank včetně jejich poboček působících na území cizího státu podléhá bankovnímu dohledu vykonávanému Českou národní bankou, včetně kontrol na místě. Činnost poboček zahraničních bank podléhá dohledu vykonávanému orgánem dohledu země sídla zahraniční banky a v rozsahu stanoveném zákonem bankovnímu dohledu*

[40] Recommendation European Systematic Risk Board: Recommendation of the European Systematic Risk Board [online]. 15.12.2020 [cit. 15.02.2023]. Dostupné z: https://www.esrb.europa.eu/pub/pdf/recommendations/esrb.recommendation200608_on_restriction_of_distributions_during_the_COVID-19_pandemic_2~f4cdad4ec1.en.pdf.
[41] JENÍK, Ivo: Dohled a regulace finančního trhu, Všehrd Spolek Českých právníků, 2011, str. 120.
[42] Tamtéž.

vykonávanému Českou národní bankou, včetně kontrol na místě.[43]*“* Další legislativní upřesnění dohledu na místě nalezneme v ustanovení § 45 ČNBZ podle něhož se dohledová činnost na místě řídí zákonem č.255/2012 Sb. Kontrolním řádem. Výsledkem kontroly na místě je dle § 12 zákona č.255/2012 Sb., protokol.[44] Přičemž platí, že v souladu s ustanovením §13 zákona č. 255/2012 Sb., lze proti kontrolnímu zjištění uvedeném v protokolu podat námitky.[45]

Je na místě zmínit, že ČNB považuje v bankovním sektoru optimální dohledovou frekvenci v oblasti dohledu na místě jednou za 4 roky, nejvýše jednou za 5 let.[46] V praxi mohu potvrdit, že ČNB toto dodržuje. V rámci dohledu na místě ČNB neprovádí dohled v celé kontrolované bance. Vždy je vybrána nějaká část, nad kterou dohled provádí např. kreditní riziko, operační riziko.

2.1.2 Dohled na dálku

Dohled na dálku je druhým typem dohledu, který je ze strany ČNB v bankách prováděn. Mám za to, že se jedná o méně náročným typ dohledu.

Banky mají v dle § 24 odst. 1 ZOBa „pravidelně reportovat poměrně rozsáhlé sady dat. Pro banky platí, *povinnost vypracovat a předkládat České národní bance informace a podklady, jejichž formu a způsob předkládání stanoví v souladu s přímo použitelným předpisem Evropské unie upravujícím obezřetnostní požadavky, a nařízením nebo rozhodnutím Evropské komise Česká národní banka vyhláškou. Banka je povinna vypracovat a předkládat České národní bance další informace a podklady potřebné pro výkon dohledu. Obsah těchto informací, formu, lhůty a způsob jejich předkládání stanoví Česká národní banka vyhláškou. Banka je povinna předložit České národní bance na její žádost další doklady a jiné materiály potřebné pro výkon dohledu a podle požadavku České národní banky poskytnout k tomu všechny potřebné informace.“*[47] Toto ustanovení je obecné, pro obsah pravidelného reportingu je třeba nahlédnout do jiných předpisů. Obsah povinného reportingu je zakotven ve vyhlášce č. 163/2014 Sb.,

[43] §25 odst. 1 ZOBa ve znění pozdějších předpisů.
[44] §12 zákona č. 255/2012 Sb., ve znění pozdějších předpisů.
[45] §13 zákona č. 255/2012 Sb., ve znění pozdějších předpisů.
[46] Dlouhodobá koncepce České národní banky [online]. Česká národní banka, 2017 [cit. 10.02.2023]. Dostupnéz:https://www.cnb.cz/export/sites/cnb/cs/dohledfinancnitrh/.galleries/dlohodoba_koncepce_dohledu/dlohodoba_koncepce_dohledu.pdf.
[47] § 24 ZOBa, ve znění pozdějších předpisů.

o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry. Další povinnosti týkající se reportingu jsou zakotveny ve směrnici CRD (Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky) atd.

2.1.3 Dohledové zátěžové testy prováděné ECB

Dohledové a zátěžové testy jsou ukázkou praktické realizace dohledu. Evropská centrální banka (dále ECB) dle článku 97 CRD povinna realizovat dohledové zátěžové testy s roční frekvencí.[48] Výsledky provedených testů jsou využívány v rámci SREPu (Supervisory Review and Evaluation Process, proces dohledu a hodnocení orgány dohledu), který detailně popíšu níže. Cílem testů je ověření finanční stability, identifikování rizik a slabých míst a případně doporučení k nápravě.

Další důležité testy na úrovni celé EU, tentokráte s frekvencí dvou let jsou prováděny EBA (Evropský orgán pro bankovnictví). Cílem celounijních zátěžových testů je zhodnocení celkové odolnosti finančního systému EU. Do těchto testů se zapojuje i ČNB a český bankovní sektor. Pohledem na výklad ČNB zjistíme, že dle její definice je účelem dohledových zátěžových testů zhodnocení odolnosti jednotlivých bank na českém trhu.[49] V dohledovém a zátěžovém testu je přihlédnuto ke specifiku jednotlivé banky. Základní scénáře dohledového zátěžového testu jsou dva.

1. Základní scénář ekonomického vývoje. Pro poslední provedený test v roce 2021 byl založen na makroekonomické prognóze ČNB ze zimy 2021. Předpokládal pokračující hospodářský růst v celém horizontu testu okolo 3 %, odeznívání koronavirové pandemie a počítal s mírou nezaměstnanosti na úrovni 3,8 %. Scénář také počítal s posilováním kurzu CZK/EUR ve prospěch a dynamikou nárůstu mezd kolem 5 %.[50]

[48] § 97 CRD.
[49] Dohledové a zátěžové testy [online]. [cit. 10.02.2023]. Dostupné z: https://www.cnb.cz/cs/financni-stabilita/zatezove-testy/dohledove-zatezove-testy/index.html.
[50] Dohledové zátěžové testy vybraných bank 2021 [online]. Česká národní banka [cit. 10.02.2023]. Dostupnéz:https://www.cnb.cz/export/sites/cnb/cs/financnistabilita/.galleries/zatezove_testy/2021/zatezove_testy_banky_2021_10.pdf.

2. Nepříznivý scénář ekonomického vývoje. V roce 2021 počítal s opakujícími se poklesy zahraniční i domácí ekonomické aktivity z důvodu pokračujících vln koronavirové pandemie. Počítal dokonce s pomalým tempem vakcinace obyvatel, poklesem spotřeby u domácností i firem. Scénář počítal také s poklesem vývozu a oslabováním CZK/EUR.[51]

Přičemž platí, že s výsledky se dále pracuje v rámci pravidelného přezkumu SREP.[52] Zátěžové testy v bankách právě probíhají.[53]

EBA avizovala, že bude dohledovému stress testu podrobeno 99 bank podléhající dohledu ECB. Přičemž 57 z nich budou banky velké. EBA zveřejnila metodiku pro provedení stress testů v roce 2023.[54] Vzhledem k faktu, že u provedení dohledových testů ČNB vychází z EBA metodiky, testy v České republice budou prováděny v souladu se ní. Toto potvrzuje i Compliance table EBA, která označuje ČNB jako dohledový orgán, který avizoval soulad s pravidly.[55]

2.1.4 Proces dohledu a hodnocení SREP

Proces dohledu a sebehodnocení byl zaveden v roce 2004 v rámci BASEL II. Od té doby naznal velkých změn. Primárně je SREP zakotven ve směrnici CRD článku 97 a následujícím. V červenci 2018 vydala EBA Revidované obecné pokyny ke společným postupům a metodikám procesu přezkumu a vyhodnocení zátěžového testování v rámci dohledu. ČNB avizovala, že bude postupovat s účinností od 01. 01. 2019 s těmito

[51] Dohledové zátěžové testy vybraných bank 2021 [online]. Česká národní banka [cit. 10.02.2023]. Dostupnéz:https://www.cnb.cz/export/sites/cnb/cs/financnistabilita/.galleries/zatezove_testy/2021/zatezove_testy_banky_2021_10.pdf.
[52] Tamtéž.
[53] Tamtéž.
[54] 2023 EU-Wide Stress Test: Methodological Note [online]. EBA European Banking Authority, 2023 [cit.10.03.|2023].Dostupnéz:https://www.eba.europa.eu/sites/default/documents/files/document_library/Risk%20Analysis%20and%20Data/EU-wide%20Stress%20Testing/2023/Scenarios/1051436/2023%20EU-wide%20stress%20test%20-%20Methodological%20Note.pdf.
[55] Guidelines compliance table: Guidelines on the revised common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing [online]. European Banking Authority, 2021 [cit. 20.02.2023]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/document_library/963608/Compliance_EBA_GL_2018_03.pdf.

pokyny.[56] SREP je prováděn každoročně. ČNB banky následně banky informuje o jeho výsledcích. Orgány dohledu se v rámci hodnocení SREP zaměřují na:

1. Obchodní model, zda je tento proveditelný a udržitelný.
2. Způsob vnitřního řízení, řízení rizik, kompetentnost managementu banky.
3. Kapitál, zda má banka dostatečné rezervy pro krytí a absorpci potenciálních ztrát.
4. Stav likvidity, likviditní rizika, udržitelnost financování.[57]

CRD v článku 97 a následujícím dále stanovuje, že v rámci SREP je po dohledových orgánech požadováno, aby posoudily mechanismy, procesy, strategie implementované úvěrovými institucemi ve vztahu k rizikům, kterým by instituce mohly být vystaveny. Totéž je třeba hodnotit i ve vztahu k rizikům plynoucím pro celý finanční systém. Hodnotí se také rizika identifikovaná v rámci SREP.

Výsledkem provedeného SREPU rozhodnutí o hodnocení. V tomto rozhodnutí se nacházejí i případná doporučení pro banku. Lhůta pro případnou nápravu je většinou stanovena na jeden rok. Např. MONETA Money Bank, a.s. oznámila, že na základě výsledků SREP kapitálový požadavek pro rok 2023 zůstává pro banku beze změny.[58] Uvádím pouze jako demonstrativní příklad, že se s výsledky testů pracuje.

[56] Sdělení ČNB o obecných pokynech EBA ke společným postupům a metodikám procesu přezkumu a vyhodnocení (SREP) [online]. [cit. 20.02.2023]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/obecne-pokyny-evropskych-organu-dohledu/Sdeleni-CNB-o-obecnych-pokynech-EBA-ke-spolecnym-postupum-a-metodikam-procesu-prezkumu-a-vyhodnoceni-SREP//

[57] Final Report: Guidelines for institutions and resolution authorities to complement the resolvability assessment for transfer strategies (Transferability guidelines) [online]. European Banking Authority, 2022 [cit. 10.02.2023]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2022/EBA-GL-2022-11%20GL%20on%20transferability/1039809/Final%20report%20on%20Guidelines%20on%20transferability.pdf.

[58] Povinně uveřejňovaná informace: Zveřejnění vnitřní informace [online]. 2022 [cit. 2023-03-15]. Dostupné z: https://investors.moneta.cz/documents/12270853/20115959/mmb-srep-pozadavek-2023-cz.pdf.

3 První zmínky o operačním riziku – Basilejské dohody

Považuji za důležité zařadit do diplomové práce tuto kapitolu o Basilejských dohodách. Cílem je vysvětlit, jakým historickým vývojem prošlo vnímání operačních rizik a jaká při tom byla role Basilejského výboru pro bankovní dohled (Basel Committee on Banking Supervision), dále jen BCBS.

BCBS byl založen v roce 1974 na základě iniciativy Banky pro mezinárodní platby. Cílem BCBS je zlepšení finanční stability a zajištění zlepšeného a kvalitního dohledu nad bankovním sektorem. Cíle je dosahováno určením minimální výše standardů pro oblasti regulace a dohledu. Je zde patrná také jasná snaha o mezinárodní spolupráci.[59]

Basilejský výbor z pohledu práva není nadnárodní autoritou. Rozhodnutí Basilejského výboru není právně závazné ani vynutitelné. Závaznost lze částečně dovodit z odpovědnosti vyplývající z členství v Basilejském výboru. Přičemž členové BCBS se zavázaly v článku 5 odst. a-g statutu k tomu, že budou spolupracovat, aby dosáhly naplnění mandátu BCBS, budou dbát na finanční stabilitu, nepřetržitě zvyšovat kvalitu regulace a dohledu, aktivně přispívat k rozvoji standardů aj.[60] Jak si ukážeme níže důležité dohody byly přeneseny do právních řádů členských států BCBS.

Co se týče operačního rizika orgány dohledu se poprvé o operačním riziku, (dále označovaném slovním spojením OpRisk), zmiňují již po roce 1990, v konzultačním materiálu BCBS.[61] Ke vzniku samostatné kategorie operačních rizik však byla od roku 1990 ještě poměrně dlouhá cesta.

Vznik samostatného OpRisku se pojí s Basel II, který operační rizika definoval a zakotvil.

[59] History of the Basel Committee*: At a glance* [online]. [cit. 01.01.2023]. Dostupné z: https://www.bis.org/bcbs/history.htm.
[60] Charter (Statut Basilejského výboru): [online] June 2018, Bank for international settlement [cit. 25.02.2023] dostupné na https://www.bis.org/bcbs/charter.htm.
[61] NIESEL, Martin a Stefan ROTH. Basel IV. 2. Weinhelm: Vilely, 2018, str. 289.

3.1 Basel I

První z Basilejských dohod podepsaná 16. 07. 1988, označovaná také jako Basel I se týká především kapitálu a kapitálové přiměřenosti.[62] Na rozdíl od svých nástupců se vyznačovala relativní jednoduchostí a přehledností. Faktem je, že měla daleko užší zaměření než dohody pozdější.

Cílem Basel I bylo vytvoření minimálních kapitálových požadavků pro banky, což mělo vést k vyšší stabilitě banky. Dalším cílem Basel I bylo zvýšení motivace bank pro držení likvidních a nízkorizikových aktiv. V neposlední řadě měl Basel I zabránit bankám v tom, aby držely nadrozměrná úvěrová rizika.[63]

K dohodě Basel I byl v roce 1996 podepsán dodatek kapitálové dohody o zahrnutí tržních rizik, přičemž je doporučeno, aby banky při výpočtu kapitálového požadavku začaly počítat i s tržními riziky.[64] Tržní riziko je definováno *jako „riziko ze ztráty z rozvahových a mimobilančních pozic, které mohou vzniknout jako důsledek pohybu tržních cen.“*[65] Česká republika nebyla signatářem Basel I, ale k dohodě se připojila.

V České republice jsou pravidla pro kapitálovou přiměřenost platná od 01. 01. 1993, a to na základě Opatření Státní banky československé, kterým se stanoví minimální výše likvidních prostředků č. 97/1992/03 Sb. Stanovení kapitálového požadavku ve výši 8 % bylo povinné pro celý bankovní sektor až od 01.01.1997.

Basel I ani jeho dodatek se nedotknul operačních rizik, jak je známe dnes. Operační rizika byla součástí compliance rizik nebo se řadila do rizik ostatních. Operační riziko je samostatně vydefinováno až v Basel II.

Nedostatky Basel I byly v tom, že při výpočtu kapitálové přiměřenosti zohledňoval pouze dva druhy rizik, úvěrové a tržní riziko. Vyvstala tedy logická potřeba změny v podobě Basel II.

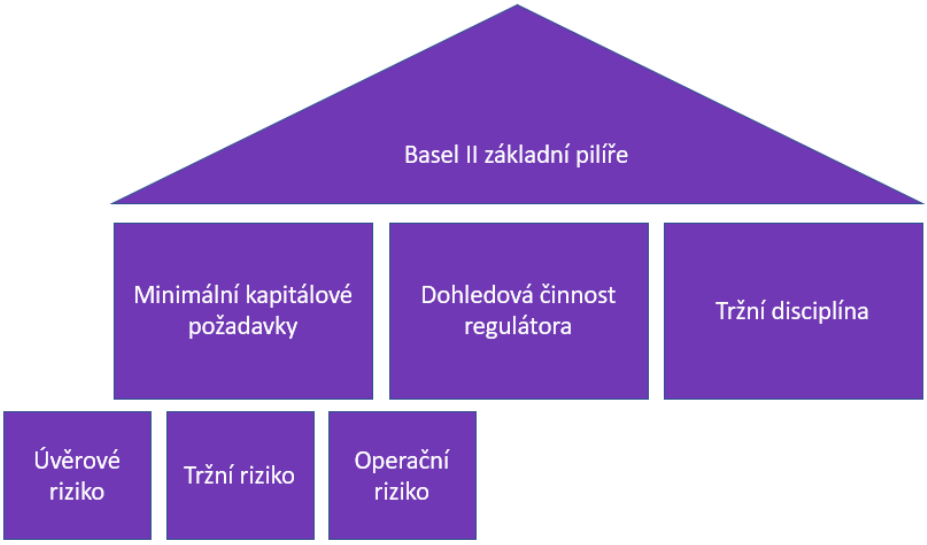
---

[62] Basel Comitee of Banking Supervision: International Governance of Capital Measurment and Capital Standarts [online]. Basel, 1988 [cit. 05.01.2023]. Dostupné z: https://www.bis.org/publ/bcbs04a.pdf.
[63] PETRJÁNOŠOVÁ, Božena Bankovní management. 1. vyd. Brno: Masarykova univerzita. 2004. str. 91.
[64] *History of the Basel Committee: At a glance* [online]. [cit. 01.01.2023]. Dostupné z: https://www.bis.org/bcbs/history.htm.
[65] Amendment to the Capital Accord to incorporate market risks [online]. Str.7 Dostupné z: https://www.bis.org/publ/bcbs119.pdf.

3.2 Basel II

První návrhy na novou podobu Basel II byly představeny v červnu roku 1999. Následoval poměrně složitý a dlouhý proces jednání v členských zemích Basilejského výboru. Vydání další verze dokumentu pod názvem „*A New Capital Adquancy Framework.*“[66] Tato dohoda byla podrobena pro svou obecnost silné kritice.

Druhá verze dohody *International Convergence of Capital Measurement and Capital Standards* označované jako Basel II byla zveřejněna v červnu 2004. Práce na této dohodě byly intenzivní a složité. Cílem dohody bylo zvýšení stability finančního systému a posílení odpovědnosti managementu bank.[67] Následně v letech 2005 a 2006 došlo k revizi Basel II.[68] V roce červnu 2006 byla publikována revidovaná verze a finální verze. Basel II pod názvem *International Convergence of Capital Measurement and Capital Standards.* Basel II je postaven na třech základních pilířích.



Obrázek 1- Basel pilíře, vlastní tvorba

[66] A new Capital Adequancy Framework: Consultative paper issued by the Basel Committee on Banking Supervision [online]. Basel, 1999 [cit. 2023-03-16]. Dostupné z: https://www.bis.org/publ/bcbs50.pdf
[67] NIESEL, Martin a Stefan ROTH. Basel IV. 2. Weinhelm: Vilely, 2018, str. 289.
[68] *History of the Basel Committee* [online]. 2023 [cit. 18.02.2022]. History of the Basel Committee and its Membership. Dostupné z <http://www.bis.org/bcbs/history.htm>.

3.2.1 První pilíř

První pilíř se týká minimálních kapitálových požadavků. Minimální kapitálový požadavek činí 8 %. Do výpočtu kapitálového požadavku nově vstupuje kapitálový požadavek na operační riziko. V důsledku tohoto vstupu dochází ke komplexnějšímu posouzení a stanovení kapitálových požadavků pro konkrétní banku. V souvislosti se zahrnutím operačního rizika do výpočtu kapitálové přiměřenosti dochází také ke změně v přístupu pro výpočet úvěrového rizika.[69]

V tomto pilíři pozorujeme zrod samostatné kategorie operačního rizika, jak jej známe dnes. Basel II přináší i vnímání větší citlivosti rizika, než tomu bylo v předchozí verzi.

Basel II již obsahuje definici pojmu Operační riziko. Operační riziko je definováno jako *„riziko ztráty vyplývající z nedostatečnosti nebo selhání vnitřních procesů, lidí a systémů nebo z vnějších událostí. Tato definice zahrnuje právní riziko.“*[70] Operační rizika přestávají být součástí compliance rizik nebo kategorie ostatních rizik a stávají se samostatnou kategorií. V tomto pilíři pozorujeme zrod samostatné kategorie operačního rizika, jak jej známe dnes. Lze tady pozorovat větší citlivost vnímání rizika, než tomu bylo v předchozí verzi.

Dle Basel II si banka v rámci přístupů k operačnímu riziku vybírá ze tří možných přístupů. Výběr metody výpočtu kapitálového požadavku je podmíněn schválením ze strany regulátora.

1. **Metoda BIA** (Basic Indicator Approach) je první, nejjednodušší metodou, vhodnou pro menší banky s nižším stupněm řízení operačního rizika. Nebyla vnímána jako vhodná metoda pro mezinárodně aktivní banky. Základním indikátorem je průměrný hrubý roční příjem banky za poslední tři roky. Kapitálový požadavek je roven 15 % tohoto indikátoru.
2. **Metoda SA** (Stantartised Apprroach) je druhou o něco složitější metodou. Indikátorem jsou hrubé příjmy stanovené obchodní linie. Kapitálový požadavek v závislosti na obchodní linii (korporátní finance, obchod a prodej, retailové bankovnictví, komerční bankovnictví, finanční vypořádání, agenturní služby, správa

[69] KAŠPAROVSKÁ, VLASTA. Řízení obchodních bank. Praha: C. H. Beck, 2006, str. 82-83.
[70] International Convergence of Capital Measurement and Capital Standards: Revised Framework [online]. Basel: 2004 [cit. 02.03.2023]. Dostupné z: https://www.bis.org/publ/bcbs107.pdf.

investic a retailové obchodování s cennými papíry činí 12 %, 15 % nebo 18 %. Celkový kapitál je tvořen prostým součtem kapitálových požadavků na jednotlivé obchodní linie.

3. **Metoda AMA** (Advanced Measurement Approach) je třetí a nejsložitější metodou pro výpočet kapitálového požadavku. Kapitálový požadavek je stanoven na základě interní kalkulace, respektive vnitřních modelů banky. Vnitřní modely jsou založeny na údajích o ztrátách interních i externích, analýzách rizikových scénářů, faktorech obchodního prostředí, vnitřních kontrolách.[71]

3.2.2 Druhý pilíř

Ve druhém pilíři byl velký důraz kladen na vnitřní řízení rizik ze strany bank. Banky tedy implementace druhého pilíře nevyhnutelně vedla ke stanovení nových vnitřních kontrol. Z pilíře také vyplývá, že metody měření, monitorování a hodnocení rizik musí být správně nastaveny, což je logické.[72] Při špatném nastavení by nefungovaly efektivně. Druhý pilíř stojí na čtyřech klíčových principech:

1. Banky by měly mít vyvinutý proces/metodu pro určování celkové kapitálové přiměřenosti ve vztahu k jejich rizikovému profilu a mít jasnou strategii pro udržení jejich kapitálové přiměřenosti. Což v praxi znamená, banka musí být schopna prokázat, že interně zvolené kapitálové cíle jsou reálné. Je třeba, aby tyto cíle byly v souladu s rizikovým profilem banky. Při stanovování kapitálové přiměřenosti je třeba přihlédnout i k fázi ekonomického cyklu. Nezastupitelnou roli v procesu hraje dohled managementu a vrcholného vedení, monitorování a podávání zpráv, přezkum interních kontrol a procesů atd.[73] Důležitý je tedy i proces řízení operačních rizik.
2. Orgány dohledu by měly kontrolovat a hodnotit proces udržování interní kapitálové přiměřenosti, strategii udržování kapitálu na potřebné výši. Mělo by k tomu docházet stejným způsobem, jako v případě hodnocení regulatorní kapitálové přiměřenosti. Do dohledových opatření můžeme zařadit dohled místě, pohovor

[71] KAŠPAROVSKÁ, VLASTA. Řízení obchodních bank. Praha: C. H. Beck, 2006, str. 139-144.
[72] International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version [online]. Str. 204. Basel, 2006 [cit. 12.02.2023]. Dostupné z: https://www.bis.org/publ/bcbs128.pdf.
[73] Tamtéž str. 204-207.

s managementem banky, pravidelný reporting, kontrolu na dálku, přezkoumání externích auditních zpráv.[74]

3. Orgány dohledu by měly zasáhnout při prvních příznacích poklesu kapitálu pod požadovanou úroveň. Orgány dohledu budou požadovat urychlené kroky směřující k nápravě nedostatečné kapitálové úrovně instituce. Opatření regulátora mohou spočívat ve zvýšení intenzity monitoringu banky, omezení výplaty dividend, požadavek na okamžité navýšení kapitálu.[75] Při volbě dohledového nástroje je třeba ze strany regulátora přihlédnout ke konkrétní situaci v bance.
4. Orgány dohledu očekávají, že banky udržují výši svého kapitálu výše, než kolik stanoví minimální kapitálový požadavek. Orgány dohledu mohou požadovat vyšší minimální kapitálový požadavek, než stanoví pilíř 1.[76]

3.2.3 Třetí pilíř

Třetí pilíř je doplňkový ve vztahu ke dvěma předchozím. Jeho cílem je stanovení povinnosti zveřejňování transparentních informací o podnikání bank. Tyto informace jsou nezbytné pro akcionáře i klienty, jelikož dodávají komplexní obrázek o finanční stabilitě banky, kapitálové přiměřenosti, počtu klientů, počtu zaměstnanců, dodržování obezřetnostních požadavků a dalších.

3.2.4 Transpozice Basel II do právního řádu České republiky

Mezi lezy 2005 až 2010 byly do českého právního řádu transponovány směrnice Evropského parlamentu a Rady 2006/48/ES ze dne 14. června 2006 o přístupu k činnosti úvěrových institucí a o jejím výkonu, směrnice Evropského parlamentu a Rady 2006/49/ES ze dne 14. června 2006 o kapitálové přiměřenosti investičních podniků a úvěrových institucí a směrnice Komise 2007/18/ES ze dne 27. března 2007. Tyto směrnice přímo vycházejí z Basel II. Definici operačního rizika vycházející z Basel II nalezneme v čl. 4 odst. 22 Směrnice Evropského parlamentu 2006/48/ES. Definice je následující: „*operačním rizikem" se rozumí riziko ztráty, které vyplývá z vnějších událostí nebo z nedostatků či selhání vnitřních procesů, osob a systémů a*

[74] International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version [online]. Str. 209-221. Basel, 2006 [cit. 02.01.2023]. Dostupné z: https://www.bis.org/publ/bcbs128.pdf.
[75] Tamtéž, str. 212.
[76] Tamtéž, str. 211.

které zahrnuje právní riziko.[77] Definice byla bez změny textace použita ve vyhlášce č. 123/2007 Sb. O pravidlech obezřetného podnikání bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry, konkrétně v ustanovení § 2 odst. 2 písm. f.

3.3 Basel III

Po vydání Basel II bylo jasné, že budou nevyhnutelně následovat další úpravy. Když v roce 2008 došlo k pádu Lehman Brothers, celý svět se ocitl v šoku a uvědomil si, že bude třeba změnit zažitá pravidla.

BCBS vydal jako reakci na události na finančním trhu v roce 2008 a 2009 doporučení k posílení kapitálové přiměřenosti stanovené Basel II. *Principles for Sound Liquidity Risk Management and Supervision.*[78] Následně začaly práce na nové dohodě Basel III. V roce 2009 Basilejský výbor vydal i další důležitý dokument. Zformuloval totiž principy zátěžového testování tzv. Stress Testing Principles.

Basel III byl vydán v roce 2010. Revidován v roce 2011 pod názvem *Regulatory framework for more resilient banks and banking systems*.[79]

Cílem Basel III je vyšší stabilita a odolnost bankovního sektoru jako celku a zabránění další finanční krizi. Novinkou bylo vytvoření tzv. kapitálových polštářů, tedy vytváření rezerv tzv. na horší časy, které by měly absorbovat možné příchozí šoky. Většina reforem byla implementována v období 2012-2019.

V prosinci 2017 byly představeny finalizují post krizové reformy v podobě Basel III Finalising post crisis reforms.[80] Známější pod pojmem Basel IV, někdy označované jako Basel 3.1, což může působit zmatečně. V bankovním světě se vžilo označení Basel IV.

[77] Článek 4 bod 22 CRR.
[78] *History of the Basel Committee: At a glance* [online]. [cit. 01.01.2023]. Dostupné z: https://www.bis.org/bcbs/history.htm.
[79] Basel III: A global regulatory framework for more resilient banks and banking systems [online]. Basel: Bank for International Settlements [cit. 01.01.2023]. Dostupné z: https://www.bis.org/publ/bcbs189.pdf.
[80] Basel III: Finalising post-crisis reforms [online]. Basel: Bank for International Settlements, 2017 [cit. 01.01.2023]. Dostupné z: https://www.bis.org/bcbs/publ/d424.pdf.

3.3.1 Transpozice Basel III do právního řádu České republiky

Basel III byl do českého právního řádu včleněn nařízením CRR, které je vzhledem ke své povaze přímo účinné. Účinnost většiny ustanovení byla stanovena 01. 01. 2014. S Basel III je spojeno ještě jedno nařízení, a to CRD s účinností od 01. 01. 2014. Basel III si vyžádal následné změny v dalších právních předpisech. Změny byly provedeny změnovým zákonem. Pro OpRisk bylo důležité zrušení vyhlášky ČNB č.127/2007 Sb., kterou nahradila současná vyhláška č. 163/2014 Sb.

3.4 Basel IV

Basel IV je zatím poslední dohoda z BCBS. Původní datum platnosti bylo stanoveno 01.01.2022.[81] V březnu 2020 v souvislosti s pandemií COVID 19 došlo k odložení platnosti na 01.01.2023 se stanoveným pětiletý postupným zaváděním reforem schválených v prosinci 2017.[82]

V souvislosti s Basel IV guvernéři centrálních bank zaslali do Evropské komise dopis, v němž apelují na nutnost dokončení reforem. Apelují tedy na řádné, včasné a koordinované dokončení v definovaných změn.

Faktem je, že 27. 10. 2021 Evropská komise publikovala tzv. bankovní balíček.[83] Dle tohoto balíčku by nová obezřetnostní pravidla měla být účinná od roku 2025. Vzhledem k dynamičnosti současného bankovního prostředí bych toto datum neviděla reálně. Co je zajímavé v rámci tohoto balíčku, kde je Basel IV označen jak Basel III. S označením Agreement, přičemž se má na mysli Basel III Finalising post crisis reforms.[84]

V jakém časovém horizontu proběhne implementace změn si v tuto chvíli netroufám odhadnout. Mohu pouze konstatovat, že bankovní sektor se na tyto změny kontinuálně připravuje.

---

[81] Finalising Basel III In brief [online]. Basel: Bank for International Settlements, 2017 [cit. 01.01.2023. Dostupné z: https://www.bis.org/bcbs/publ/d424_inbrief.pdf.
[82] Finalising Basel III standart adoptation [online]. Basel: Bank for International Settlements, 2017 [cit. 01.01.2023]. Dostupné z: https://www.bis.org/bcbs/implementation/rcap_reports.htm?m=3059.
[83] *Banking package* [online]. European Comission: Bank for International Settlements, 2021 [cit. 01.01.2023]. Dostupné z: https://finance.ec.europa.eu/publications/banking-package_en.
[84] Finalising Basel III In brief [online]. Basel: Bank for International Settlements, 2017 [cit. 01.01.2023. Dostupné z: https://www.bis.org/bcbs/publ/d424_inbrief.pdf.

4 Operační rizika základní definice a členění

V této kapitole dojde definování operačních rizik, z pohledu legislativy. Podíváme se i na to, jak operační riziko definují velké bankovní domy v České republice ve svých výročních zprávách. Následně operační rizika rozdělím do odpovídajících legislativních kategorií, definovaných pro banky.

4.1 Operační riziko

Riziko v nejobecnější rovině můžeme vnímat jako vliv nejistoty na očekávaný výsledek. Tuto definici naplňuje i riziko operační, které má svá specifika.

Operační riziko můžeme vnímat z mnoha různých úhlů pohledu, z pohledu procesního, ekonomického, právního.

Z pohledu literatury je operační riziko „*definováno jako možnost potenciální ztráty v důsledku nedostatků nebo selhání interních procesů, informačního systému nebo možnost ztráty v důsledku externích vlivů.*“[85] Tato definice je značně nepřesná a nepokrývá všechny aspekty operačního rizika. K definování operačního rizika lze využít i definice negativní. Operační riziko je definováno jako riziko, které není kreditní ani tržní.[86] Toto je definice velmi obecná, z mého pohledu spíše rámcová.

V řeči práva můžeme pojem operační riziko zařadit do kategorie neurčitého právního pojmu. Nelze totiž dopředu jednoznačně určit, jakou oblast nebo linii podnikání dané riziko zasáhne. Dopady mohou být napříč bankou.

Je třeba vzít v potaz, že bankovní svět se vyvíjí zejména s ohledem na technologie velmi rychle. Banky nabízejí stálé nové produkty a každý produkt s sebou nese sadu rizik. Některá rizika mohou být zcela nová, dosud neidentifikovaná. Úzká definice pojmu operačního rizika by byla na škodu. Od bankovního světě se očekává, že se při definici operačního rizika bude pohybovat v mezích regulace, ale přizpůsobí jí svým vlastním liniím podnikání.

[85] DUCHÁČKOVÁ, Eva. Principy pojištění a pojišťovnictví. 3., aktualiz. vyd. Praha: Ekopress, c2009, str 98.
[86] CHAPELLE, Ariane. Operational risk management: best practices in the financial services industry. Hoboken: Wiley, 2018, str. 12.

Na definici pojmu operační riziko se podíváme i do legislativy. Definic najdeme více.

1. **Definice Basel** z pohledu Basel je operační riziko „*definováno jako Riziko ztráty vyplývající z nedostatečnosti nebo selhání vnitřních procesů, lidí a systémů nebo z vnějších událostí. Tato definice zahrnuje právní riziko, ale vylučuje strategické a reputační riziko.“*[87] Basel II definuje sedm kategorií operačního rizika, které byly implementovány do CRR, jak ukazuje obrázek níže.[88]

Obrázek 2 - Klasifikace operačních rizik dle CRR, vlastní tvorba na základě CRR

2. **Z pohledu nařízení CRR** platí dle ustanovení článku 4 odst.1 bodu 52, *že operačním rizikem je riziko ztráty, které vyplývá z nedostatků vnitřních procesů, osob a systémů nebo z vnějších událostí a zahrnuje právní riziko.*[89] Dále je v CRR stanoveno, že *„Operační riziko představuje pro instituce významné riziko, a proto musí být kryto kapitálem. Je nutné přihlédnout k různorodosti institucí v unii tím, že se vymezí alternativní přístupy k výpočtu požadavků na krytí operačního rizika, které budou zahrnovat různé úrovně citlivosti vůči riziku a vyžadovat různý stupeň propracovanosti. Institucím by měly být poskytnuty vhodné pobídky, které by je motivovaly k zavádění přístupů citlivějších vůči riziku. Vzhledem k tomu, že techniky měření a řízení*

[87] International Convergence of Capital Measurement and Capital Standards: Revised Framework [online]. Basel: 2004 [cit. 02.03.2023]. Dostupné z: https://www.bis.org/publ/bcbs107.pdf.
[88] Vlastní zpracování na základě podkladu International Convergence of Capital Measurement and Capital Standards: Revised Framework [online]. Basel: 2004 [cit. 02.03.2023]. Dostupné z: https://www.bis.org/publ/bcbs107.pdf.
[89] Článek 4 odst. 1 bod 42 CRR.

operačního rizika byly vypracovány teprve v poslední době, měla by se pravidla průběžně přezkoumávat, popřípadě aktualizovat, přičemž by se měl brát ohled i na náklady různých linií podnikání a na uznávání technik snižování rizika. Zvláštní pozornost u jednoduchých přístupů pro výpočet kapitálových požadavků na krytí operačního rizika by se měla věnovat zohlednění pojištění.“[90] Tato definice a klasifikace je pro banky klíčová.

3. **Dle vyhlášky č. 163/2014 Sb.,** vyhláška sama odkazuje na CRR. Přičemž detailně rozpracovává v příloze č.6 požadavky na řízení operačního rizika.
4. **Z pohledu českých bank** pro účely práce jsou vybrány ty největší na našem trhu.

a) **ČSAS operačním rizikem definuje** *„riziko ztráty vlivem nepřiměřenosti či selhání vnitřních procesů, lidského faktoru nebo systémů či riziko ztráty vlivem vnějších událostí, včetně rizika právního.“*[91]

b) **ČSOB operačním rizikem definuje***: „riziko ztrát vyplývajících z neadekvátnosti nebo selhání interních procesů, lidí a systémů nebo externích událostí. Operační rizika zahrnují rizika právní, riziko podvodu a rizika daňová. Při stanovování náchylnosti k těmto událostem operačního rizika se bere v úvahu i reputační dopad.“*[92]

c) **Komerční banka** operační riziko ve výroční zprávě výslovně definováno nemá. „*Operační riziko řídí na úrovni skupiny Societe Generale KB ve výroční zprávě akcentuje využití kontrol druhé úrovně při řízení operačního rizika*.“[93]

d) **Moneta Money bank** operačním rizikem rozumí *„riziko ztráty vlivem nedostatků či selhání vnitřních procesů, lidského faktoru nebo systémů či riziko ztráty vlivem vnějších skutečností, včetně rizika ztráty v důsledku porušení či nenaplnění právní nebo regulatorní normy nebo ohrožení dobré pověsti Skupiny. Zahrnuje i právní riziko a riziko outsourcingu.“*[94]

---

[90] Bod 52 CRR.
[91] Výroční zpráva Česká spořitelna [online]. 2022, Praha [cit. 05.02.2023]. Str. 53. Dostupné z: https://www.csas.cz/static_internet/cs/Redakce/Ostatni/Ostatni_IE/Prilohy/vz-2021.pdf.
[92] Výroční zpráva ČSOB [online]. 2022, Praha [cit. 05.02.2023]. Str. 180. Dostupné z https://www.csob.cz/portal/documents/10710/444804/vz-csob-2021.pdf.
[93] Výroční zpráva Komerční banka [online]. 2022, Praha [cit. 05.02.2023]. Str. 70. Dostupné z: https://www.kb.cz/getmedia/9aafd6ac-7be2-4808-9060-2feae98f9cd0/Vyrocni-zprava-KB-2021_1.pdf.aspx.
[94] Výroční zpráva Moneta Money bank [online]. 2022, Praha [cit. 05.02.2023]. Str. 116. Dostupné z: https://investors.moneta.cz/documents/12270853/20117788/mmb-vyrocni-zprava-2021-cz.pdf.

e) **Unicredit bank** má definici následující*: „Operační riziko je riziko vzniku ztráty v důsledku nedostatků či selhání vnitřních procesů, lidí a systémů nebo vlivem vnějších událostí. Tato definice zahrnuje právní riziko, nikoli však riziko strategické ani reputační. Právní riziko zahrnuje mj. riziko pokut, sankcí nebo exemplární náhrady škody vyplývající z opatření dohledu a ze soukromoprávního vyrovnání.“* [95]

f) **Raiffeisenbank** definuje operační riziko v souladu s platnou legislativou jako „*riziko ztráty Skupiny vlivem nepřiměřenosti či selhání vnitřních procesů, lidského faktoru, nebo systémů či riziko ztráty Skupiny vlivem vnějších událostí. Skupina tato rizika sleduje, eviduje, pravidelně vyhodnocuje a přijímá opatření za účelem minimalizace ztrát.“* [96]

Banky definují operační riziko buď na úrovni banky nebo na úrovni skupiny. Oba přístupy jsou možné. Při definici vychází z platné legislativy. Z výročních zpráv je patrné, že některé banky si metodiky definici operačního rizika s právními předpisy definici operačního rizika upravují vzhledem k povaze jejich podnikání.

4.2 Základní dělení operačního rizika

Na nejzákladnější úrovni můžeme operační riziko členit do dvou základních kategorií.

1. Interní operační riziko, operační riziko vzniklé uvnitř organizace. Mající na organizaci dopad.
2. Externí operační riziko, operační riziko vzniklé vně organizace. Toto riziko by se za určitých okolností mohlo materializovat i jinde než v původní organizaci.

4.3 Pokročilejší dělení operačního rizika

Operační riziko je tedy riziko v důsledku nedostatků či selhání

- Vnitřních procesů.

[95] Výroční zpráva Unicredit bank [online]. 2022, Praha [cit. 05.02.2023]. Str. 113. Dostupné z: https://www.unicreditbank.cz/content/dam/cee2020-pws-cz/cz-dokumenty/o-bance/vyrocni-zpravy/VZ_2021_CZ_final.pdf.

[96] Výroční zpráva Raiffeisen bank [online]. 2022, Praha [cit. 05.02.2023]. Str. 134. https://www.rb.cz/attachments/zpravy/Raiffeisenbank_a_s_Konsolidovana_vyrocni_zprava_2021_CZ.pdf.

- Lidského faktoru.
- Systémů.
- Externích faktorů/událostí.

Do operačního rizika neřadíme riziko strategické ve smyslu ztráty z důvodu chybného manažerského rozhodnutí a riziko reputační. S reputačním rizikem však pohled není jednoznačný. Samotné operační riziko není rizikem operačním v kombinaci se selháním některého z výše definovaných bodů už o reputační riziko jít může.

4.4 Kategorizace operačního rizika

Při kategorizaci operačního rizika vycházím z kategorizace určené bankám, tedy definice CRR. Jak bylo zmíněno výše, operační riziko pro banky lze dle regulace dělit do kategorií.

Kategorizace sedmi kategorií je využívána v rámci standardizovaného přístupu pro výpočet kapitálového požadavku ke krytí operačních rizik.

Banka se ve vnitřních procesech nemusí striktně držet vydefinovaných sedmi kategorií. Tedy ztráty z operačních rizik může řadit vnitřně i jinak. Reálně je kategorií více, než udává legislativa. Podstatné je, že banka musí být schopna události zařadit do daných sedmi oblastí ve výkazech pro ČNB. Podmínkou je převodník vnitřní klasifikace kategorií operačních rizik s klasifikací CRR. Při přesnější klasifikaci je možné operační rizika efektivněji řídit.

Je třeba mít na paměti, kategorie klasifikace se mohou prolínat. Zařazení operačního rizika do jedné ze sedmi kategorií není v praxi snadné. Ne každá událost má na první pohled jasnou kořenovou příčinu. Navíc se událost v čase vyvíjí. Klasifikace na počátku procesu (Loss data collection sběr událostí operačního rizika, dále jen LDC) se nemusí rovnat klasifikaci závěrečné. Při klasifikaci událostí budeme vycházet z legislativního rámce CRR.

Při klasifikaci událostí operačního rizika je třeba brát v potaz ještě dva faktory, prvním z nich je Risk Apetite limit (RAL), který určuje na základě podkladů management konkrétní banky. Jinou výši RAL bude mít malá banka a odlišnou výši RAL bude mít středně velká a velká banka. Výše RAL následně také dokáže ovlivnit, zda je konkrétní

událost považována za událost operačního rizika nebo ne. V praxi se v interních předpisech velmi často stanovuje dolní hranice události operačního rizika. Což znamená, událost se v procesu LDC zaznamená do interního systému. Na druhou stranu se tato událost neklasifikuje jako událost operačního rizika. Tedy není třeba vyšetřování události, hledání slabých míst atd. Každá banka bude mít tuto hranici jinde, v závislosti na individuálním posouzení a rozhodnutí managementu.

Druhým faktorem jsou rizika plynoucí z outsourcingu, ta mohou být skutečně velmi rozmanitá.

4.4.1 Interní podvody

Interní podvody jsou definovány v CRR článku 324 jako: „*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.“*[97] Půjde o situace, kdy do podvodu je nějakým způsobem zainteresován interní zaměstnanec a bance selžou zcela nebo částečně preventivní, detekční a kontrolní mechanismy. Např. neoprávněně odčerpané finanční prostředky z bankovního účtu klienta, zpronevěření hotovosti na pokladně banky.

4.4.2 Externí podvody

Externí podvody jsou definovány v CRR článku 324 jako: „*ztráty způsobené jednáním třetí strany, jehož úmyslem je podvodně připravit o majetek, zpronevěřit jej nebo obejít zákon.“* Typicky půjde např. o loupež, padělání dokladů a dokumentů nejčastěji za účelem získání bankovního produktu, krádež identity, můžeme tam zařadit i family fraudy[98] atd.

4.4.3 Postupy při zaměstnávání a bezpečnost na pracovišti

Postupy při zaměstnávání a bezpečnost na pracovišti jsou definovány v článku 324 CRR jako: „*ztráty způsobené jednáním, které je v rozporu se zákony nebo dohodami*

[97] CRR článek 324
[98] Family raud podvod finanční povahy v rodině. Např. odcizení dokladů totožnosti otci a načerpání úvěru bez jeho vědomí.

týkajícími se zaměstnávání, ochrany zdraví a bezpečnosti, ztráty způsobené platbami z důvodu újmy na zdraví nebo z důvodu diskriminace či sociální a kulturní odlišnosti.[99] V tomto případě půjde o riziko, které je úzce spjato především s oddělením lidských zdrojů a compliance. Klasifikace nebývá obtížná. Nejčastěji se jedná o rizika spojená s diskriminací, může jít o aktivní právní spory neukončení pracovního poměru v souladu s legislativou. Dalším příkladem může být kompenzace zaměstnancům v případě pracovního úrazu, kdy banka nesplnila legislativní požadavky na ni kladené.

4.4.4 Klienti produkty a obchodní postupy

Klienti produkty a obchodní postupy jsou v CRR článku 324 definovány jako: „*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.*[100] Tady se více než kde jinde akcentuje povinnost banky jednat s odbornou péčí vůči klientovi. Banka také musí nabízet klientovi vhodný produkt pro jeho potřeby, nastavovat klientovi vhodné limity, zejména tedy finanční, aby nedošlo k předlužení. Dále musí dojít k informování klienta o produktu jako takovém o všeobecných obchodních podmínkách, způsobem pro klienta srozumitelným.

Dále je třeba myslet na to, že bankéř, který nabízí klientovi konkrétní produkt musí mít příslušné certifikace, podle povahy nabízeného produktu. Typicky u hypotečního úvěru nebo o spotřebitelského úvěru.

4.4.5 Škody na hmotném majetku

Škody na hmotném majetku jsou dle článku 324 CRR definovány jako: *„ztráty způsobené ztrátou nebo poškozením hmotného majetku přírodní katastrofou nebo jinými událostmi.“* Tato kategorie je jediná z mého úhlu pohledu naprosto jasná. Typicky se bude jednat o rozbité výlohy pobočky, poškozené bankomaty, poškozené služební automobily atd.

[99] CRR článek 324.
[100] CRR článek 324.

4.4.6 Přerušení obchodní činnosti a selhání systému

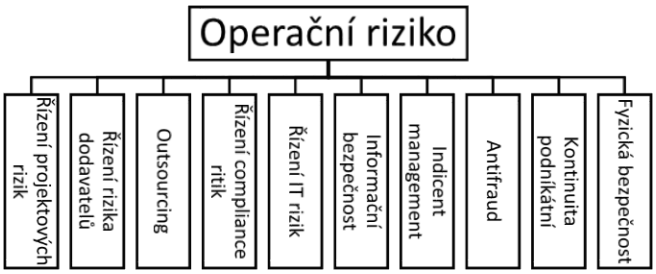
Ztráty způsobené přerušením obchodní činnosti nebo selháním systému dle článku 324 CRR definovány *jako: „ztráty přerušené obchodní činnosti nebo selhání systému.“*[101] Tato kategorie je poměrně široká. Např. špatně fungující datové centrum, nefunkční core systém a mnoho dalšího.

4.4.7 Provádění transakcí, dodávky a řízení procesů

Provádění transakcí dodávky a řízení procesů je v článku 324 *CRR* definováno jako: *„ztráty způsobené chybami při zpracovávání transakcí nebo při řízení procesů, ztráty plynoucí ze vztahů.*[102]*“* Tato kategorie je široká a velmi významná z pohledu regulace. Nalezneme v ní např. incidenty z platebního styku.

4.5 Operační rizika v bance

Kde všude tedy můžeme na operační rizika narazit? Prakticky všude se toto riziko může materializovat.



Obrázek 3 - Operační riziko, vlastní tvorba

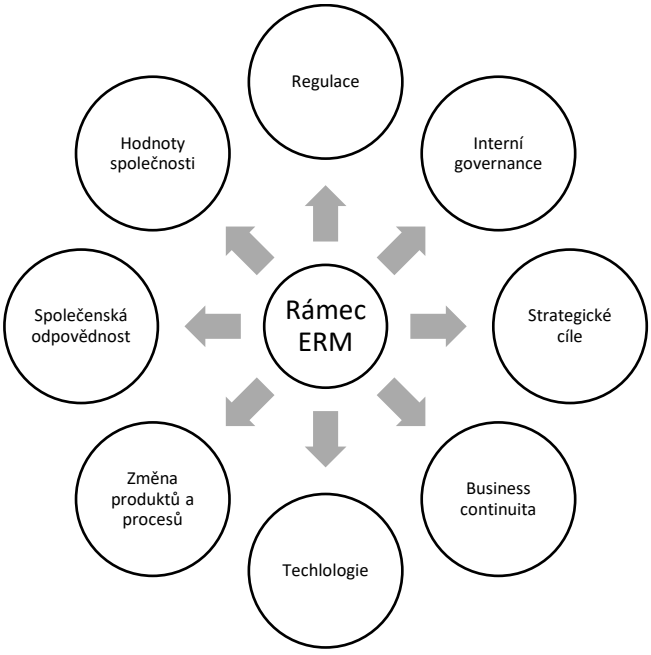
[101] CRR článek 324.
[102] CRR článek 324.

5 Systém řízení operačního rizika

Řízení rizik označované často zkratkou ERM (Enterprise Risk Management), na průběžné bázi komplexně zajišťuje identifikaci, posouzení a vyhodnocení rizik. Dále zavedení prevenčních, detekčních a kontrolních opatření. Stanovuje jasný rámec při řízení rizik v dané společnosti, často označovaný jako Risk Framework.

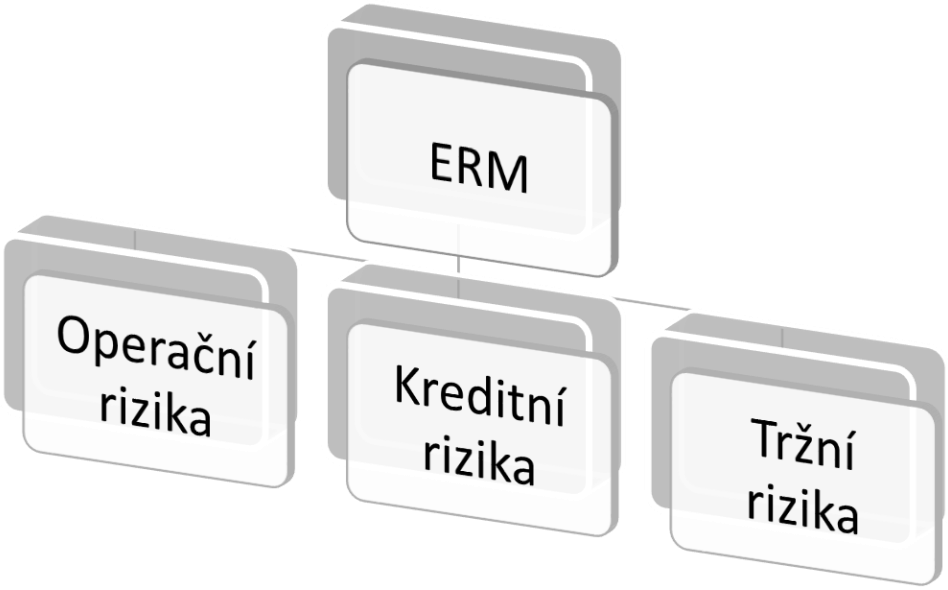
Systém řízení rizik je v každé společnosti jiný v závislosti na:

- Stanovených cílech společnosti.
- Strategickém plánování.
- Známých externích faktorech.
- Významnosti rizik.
- Interní governance.
- Nastavených procesech.
- Apetitu rizika atd.
- Apetitu ke změnám produktů.



Obrázek 4 - Rámec ERM, vlastní tvorba

Co se řízení rizik týče, je možné je řídit centralizovaně nebo decentralizovaně. V bankách dochází v rámci ERM k řízení rizik operačních, kreditních a tržních.



Obrázek 5- Řízení rizika ERM, vlastní tvorba

Při řízení rizik je třeba zohlednit tzv. Best practice. Tedy řídit rizika v souladu s nejlepšími známými poznatky v dané oblasti.

Dle nejobecnějšího pohledu lze řízení rizik rozdělit do tří etap.

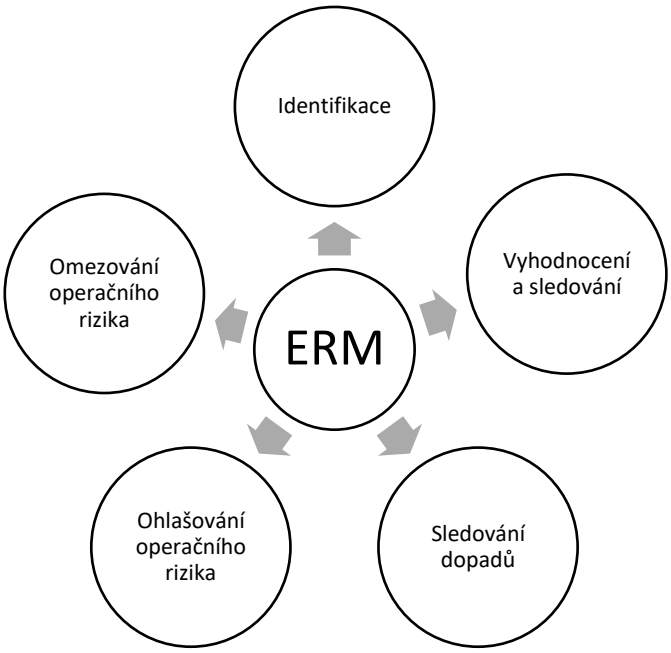
- Identifikace rizika.
- Vyhodnocení rizika.
- Management rizika.

Vyhláška č. 163/2014 Sb., která je pro řízení operačních rizik významná, řízení operačního rizika rozděluje podrobněji.

- Identifikace rizika.
- Vyhodnocování a sledování operačního rizika.
- Sledování dopadů a potenciálních ztrát z operačního rizika.
- Ohlašování operačního rizika.
- Omezování operačního rizika.[103]

[103] Vyhláška č. 163/2014 Sb,

Celý proces řízení operačních rizik můžeme vyjádřit i takto



Obrázek 6 – ERM, vlastní tvorba

5.1 Požadavky na řídící a kontrolní systém

Jasné vymezení pravomocí a odpovědností řídícího a kontrolního systému banky je jedním z důležitých předpokladů účinné vnitřní kontroly a řízení rizik.

Cíle řídícího a kontrolního systému musí být v souladu se strategií banky, právní předpisy. Přičemž požadavky na řídící a kontrolní systém musí být v souladu s legislativou.

Základní požadavek na řídící a kontrolní systém nalezneme v ZOBa. Dle ustanovení § 8b odst. 1 písm. b. ZOBa *„musí mít banka systém řízení rizik, který vždy zahrnuje pravidla přístupu banky k rizikům, kterým banka je nebo může být vystavena, včetně rizik vyplývajících z vnějšího prostředí a rizika likvidity, dále banka musí disponovat účinnými postupy rozpoznávání, vyhodnocování, měření, sledování a ohlašování rizik, a také účinnými postupy přijímání opatření vedoucích k omezení případných rizik.“*[104] Požadavek na řídící a kontrolní systém je dále detailně rozpracován ve vyhlášce č. 163/2014 Sb., která v ustanovení § 9 stanoví: *„povinná osoba splňuje požadavky*

[104] §8 písm. b. ZOBa, ve znění pozdějších předpisů.

stanovené na řídicí a kontrolní systém a jeho součásti s ohledem na svou velikost, model svého podnikání, jeho složitost a s ním spojená rizika, organizační uspořádání, povahu, rozsah a složitost činností, které vykonává nebo hodlá vykonávat.[105] Požadavky na řídící a kontrolní systém lze dle komentářové literatury rozdělit do tří základních kategorií.[106]

1. Vymezení funkcí vedoucích zaměstnanců a nastavení informačních toků ve společnosti. Nastavit řízení společnosti (corporate governance a vnitřní řízení společnosti internal governance).
2. Stanovení pravidel pro řízení, sledování a kontrolu rizik, která banka podstupuje v souvislosti svou podnikatelskou činností.
3. Stanovení pravidel, sledování a kontroly dodržování právních předpisů regulujících činnost banky a požadavky na vnitřní obecný kontrolní systém zaměřený na efektivnost a účinnost ostatních prvků vnitřního řídicího a kontrolního systému (systém vnitřní kontroly).

Pro řídící a kontrolní systém banky a operační riziko je podstatná příloha č. 6 vyhlášky č. 163/2014 Sb. Tato stanoví, *„že povinná osoba zavede a udržuje systém řízení operačního rizika, který je přiměřený povaze rozsahu a složitosti činností a obsahuje alespoň:*

- *Vymezení operačního rizika.*
- *Zásady a cíle řízení operačního rizika.*
- *Postupy řízení operačního rizika.*
- *Působnost, pravomoci a informační toky při řízení operačního rizika na všech řídících a organizačních úrovních.*
- *Informace o významných událostech a ztrátách vzniklých v důsledku operačního rizika.*
- *Míru akceptovatelného operačního rizika.*
- *Způsob případného vyvedení operačního rizika na jinou osobu typicky outsourcing nebo pojištění.*

[105] § 9 Vyhlášky č. 163/2014.
[106] § 9 Vyhlášky č. 163/2014.

- *Limity pro operační riziko.“* [107]

Vyhláška se odkazuje na princip proporcionality při požadavcích na řízení operačního rizika. Tento princip nalezneme zakotven i v ustanovení § 8b odst. 2 ZoBa.

Požadavky na ERM byly zakotveny také na úrovni BCBS. Při řízení je podstatná role na všech úrovních v organizační struktuře banky. Role představenstva je důležitá, nicméně opomenout nelze ani roli vyššího managementu, který pro představenstvo připravuje podklady ke schválení. Zapomenout nelze ani na velmi významnou roli dozorčí rady, která při řízení rizik hraje také významnou roli. Základní principy vydefinovaní BCBS je možné shrnout do následujících bodů.

1. Dostatečná kvalifikace členů představenstva, jasné vymezení role členů představenstva ve vnitřním řízení společnosti.
2. Vyvinout a implementovat a udržovat takový rámec řízení rizik, který bude odpovídat bance samotné, jejímu obchodnímu modelu, ekonomickému prostředí atd.
3. Stanovit, schválit a pravidelně přezkoumávat rámce řízení operačních rizik. Přičemž na tento proces dohlíží jak vrcholný management, tak dozorčí rada.
4. Schválit míru akceptovatelného operačního rizika ze strany představenstva banky. Míru akceptovatelného operačního rizika navrhuje vyšší management banky, zpravidla department řízení operačních rizik.
5. Vypracovat, schválit robustní struktury řízení rizik s dobře definovanou, transparentní a konzistentní linií odpovědnosti ze strany představenstva banky. Nelze zapomenout ani na roli vyššího managementu banky, který vrcholnému managementu připravuje podklady. Mezi významné úkoly řadíme.

    - Zajištění identifikace operačního rizika u nových produktů ze strany vyššího managementu banky, který předkládá rizika ke schválení.
    - Zajištění, aby všechny nové produkty a činnosti byly posouzeny ve vztahu k operačnímu riziku.
    - Zajištění systému kontinuity činností.[108]

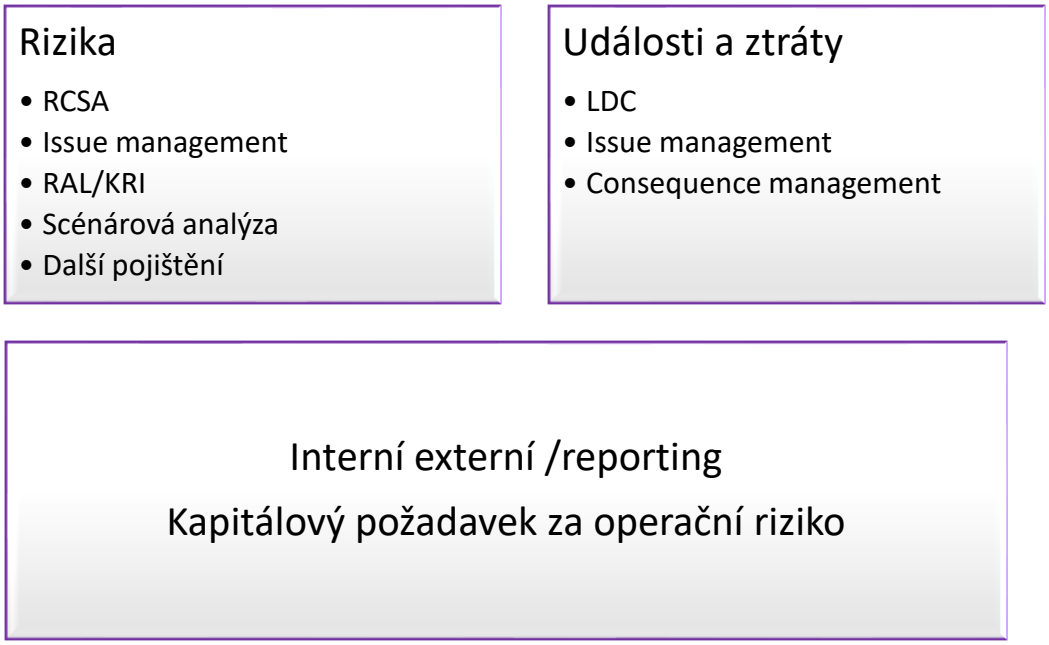
[107] Vyhláška č. 163/2014 Sb. Příloha č. 6.
[108] Principles for the Sound Management of Operational Risk [online]. 2022, Bank for International Settlement [cit. 10.03.2023]. Dostupné z: https://www.bis.org/publ/bcbs195.pdf.

5.1.1 Vymezení operačního rizika

Vymezení a schválení rámce operačního rizika probíhá v souladu s požadavky na řídící a kontrolní systém banky. Je tedy na každé bance, aby si vymezila rámec řízení operačního rizika.

5.1.2 Zásady a cíle řízení operačních rizik

Banka při řízení operačního rizika definuje vlastní cíle řízení operačního rizika. Cíle operačních rizik definovány na úrovni interních předpisů. Cíle jsou schvalovány v souladu s hierarchií banky. Cíle musí naplňovat požadavky na řídící a kontrolní systém banky. Při řízení operačních rizik banka také definuje nejen cíle. Je třeba definovat i postupy při řízení operačního rizika. Tedy odkud mohou rizika přicházet, kde je banka identifikuje? Co nám z rizik hrozí? Jaká je reakce na riziko atd. Postupy při řízení operačního rizika jsou rámcově vyjádřeny na schématu níže.

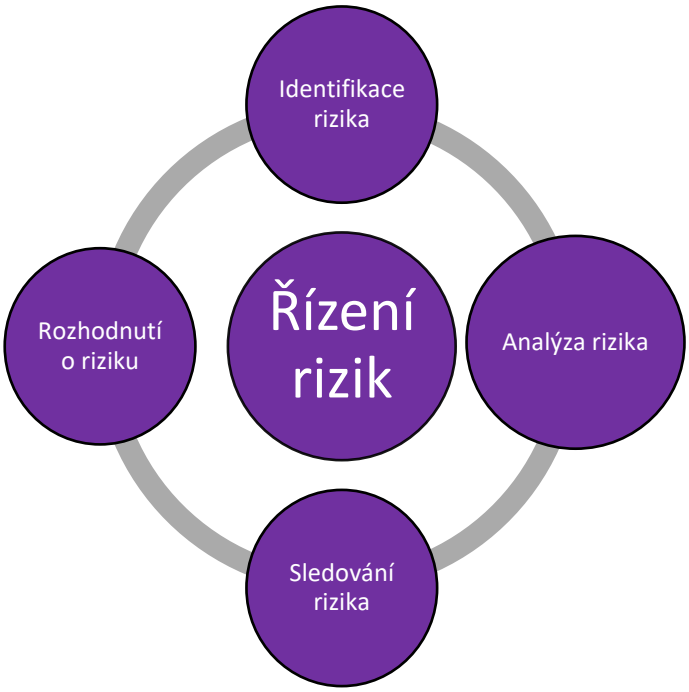


Obrázek 7 - Řízení rizik, vlastní tvorba

5.1.3 Základní fáze procesu řízení operačních rizik

Řízení operačních rizik je soustavný a nikdy nekončící proces. Je vhodné si tento proces rozčlenit do logických, na sebe navazujících celků. Proces lze rozdělit do čtyř základních kroků, které na sebe navazují a tvoří logický celek.

Fáze procesu řízení rizik[109]



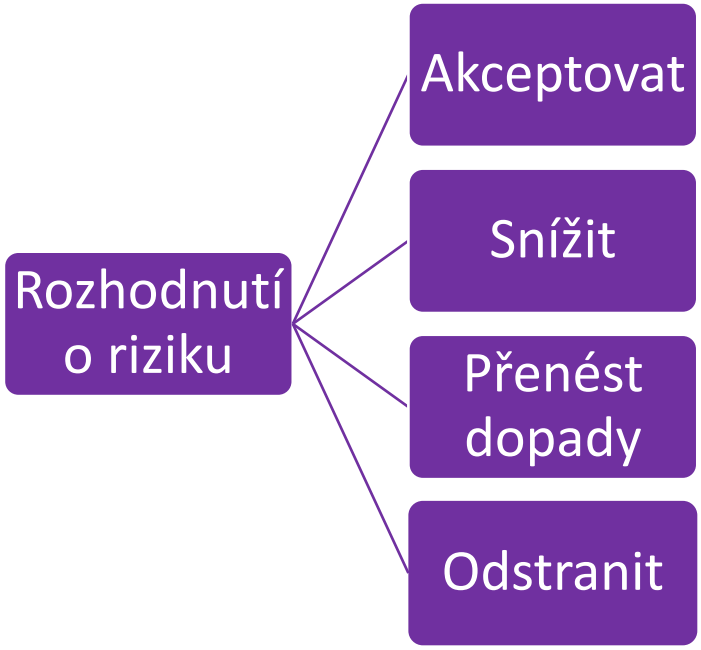
Obrázek 8 - Fáze procesu řízení rizik, tvorba na základě citace podkladu Chapelle Ariane

1. Rozpoznávání/identifikace operačního rizika jedná o soustavnou činnost, která probíhá kontinuálně napříč celou bankou. Cílem tohoto kroku je identifikovat operační rizika, která ohrožují banku a také zdroje těchto rizik. Ty mohou být externí nebo interní.
2. Analýza operačního rizika je navazujícím krokem na bod 1. V tomto bodě dochází k analýzám a hodnocení událostí operačního rizika. Odhadují se možné vzniklé ztráty, a to jak ztráty přímé tzv. direct loss, ztráty nepřímé tzn. Indirect loss, near

[109] CHAPELLE, Ariane. Operational risk management: best practices in the financial services industry. Hoboken: Wiley, 2018, str. 13.

miss tedy ztráta, která mohla vzniknout, ale se štěstím nevznikla a mnohé další. Zjednodušeně řešeno se v tomto kroku riziko kvantifikuje.

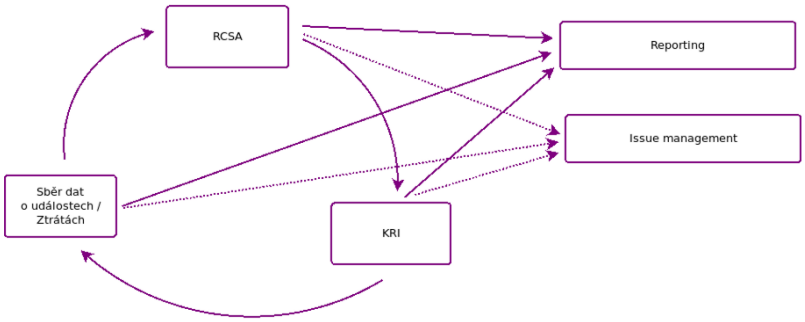
3. Sledování operačního rizika spočívá v pravidelném monitoringu operačních rizik a jeho vyhodnocování. Pro naplnění legislativních požadavků na řídící a kontrolní systém je nutné s rizikem pracovat.
4. Rozhodnutí o riziku, toto můžeme akceptovat, snížit, přenést dopady nebo zavést taková opatření, která riziko zcela odstraní. To, že by se riziko v praxi zcela odstranilo se neděje moc často. Scénář rozhodnutí o riziku je zachycen také na obrázku níže.



Obrázek 9 - Rozhodnutí o riziku, vlastní tvorba

5.1.4 Vztah mezi postupy při řízení operačního rizika

Mezi hlavními postupy při řízení operačního rizika existují na obecné rovině vztahy. Jedná se opět o nikdy nekončící koloběh, kdy jedno navazuje na druhé. Detailní rozpracování jednotlivých složek bude následovat v další kapitole práce.



Obrázek 10 - Vztahy mezi postupy při řízení operačních rizik, vlastní tvorba

5.1.5 Požadavek obezřetnosti a odborné péče při řízení rizik

Každá banka je dle ustanovení § 12 odst.1 ZOBa. *„povinna při výkonu své činnosti postupovat obezřetně, zejména provádět obchody způsobem, který nepoškozuje zájmy jejích vkladatelů z hlediska návratnosti jejich vkladů a neohrožuje bezpečnost a stabilitu banky.“*[110] Jedná se tedy o požadavek obezřetnosti banky při výkonu činnosti, což lze označit jako jeden ze základních požadavků kladených na banku. Do tohoto požadavku bychom tedy mohli zahrnout i požadavek na obezřetné řízení rizik.

5.2 Pojištění jako nástroj k řízení operačního rizika

Pojištění je nástrojem, které může zmírnit dopady ztrát z operačního rizika u některých rizik. Negativní finanční dopad z události operačního rizika je přenesen na pojišťovnu zcela nebo z části. Podle povahy rizika a parametrů pojistné smlouvy. Z povahy operačních rizik nelze uzavřít pojištění na všechny druhy rizik. Už proto, že všechny druhy rizik nemají definovatelný pojistný zájem ve smyslu ustanovení § 2761 a následujících zákona č. 89/2012 Sb.

Nejčastěji se pojišťují rizika spojená s majetkem banky, odpovědností obecnou i profesní. Povinnost mít uzavřenu pojistnou smlouvu může vyplývat i z právních předpisů.

V dnešní době je také často diskutované pojištění kybernetického rizika tzv. Cyber pojištění. Jedná se o pojištění proti rizikům typu, Ransomware, přerušení činnosti z důvodu hackerského útoku, výpadek datového centra, výpadek bankomatové sítě a

[110] §12 ZOBa ve znění pozdějších předpisů.

mnoho dalších kybernetických rizik. Pojištění kybernetických rizik se stává ve světě standartním pojistným produktem. V České republice je možno sjednat pojištění kybernetických rizik. Rozsah pojištění je však užší než u zahraničních pojišťoven. Samotnému uzavření pojistné smlouvy předchází několik zásadních kroků. Důležitá je účast pojišťovny, která si pojišťovaný subjekt pečlivě zkoumá. Často formou testů bezpečnosti. V neposlední řadě je třeba přihlédnout k apetitu pojistitelů pojistnou smlouvu vůbec uzavřít. Což je v současnosti jeden z největších problému. Tím, jak roste počet kybernetických hrozeb, zmenšuje se apetit pojistitelů rizika upisovat a zvyšují se pojistné sazby.

ENISA v roce 2021 provedla šetření na pojištění kybernetických rizik, ze kterého vyplývá, že pouze 26 % dotazovaných subjektů má uzavřenu pojistnou smlouvu kryjící kybernetická rizika.[111] Na první pohled se číslo 26 % zdá jako velmi nízké. Faktem je, že uzavření pojistné smlouvy kybernetického rizika je běh na dlouhou trať

Velmi zajímavým tématem je i pojištění profesní odpovědnosti statutárních orgánů tzv. D&O pojištění (Directors and Officers Liability Insurance). Dle ustanovení § 159 odst. 1 zákona č. 89/2012 Sb., občanského zákoníku platí: „*Kdo přijme funkci člena voleného orgánu, zavazuje se, že ji bude vykonávat s nezbytnou loajalitou i s potřebnými znalostmi a pečlivostí. Má se za to, že jedná nedbale, kdo není této péče řádného hospodáře schopen, ač to musel zjistit při přijetí funkce nebo při jejím výkonu, a nevyvodí z toho pro sebe důsledky.*“[112] S porušením povinnosti péče řádného hospodáře je spojena povinnost nahradit společnosti vzniklou škodu. Právě pro tyto případy je uzavíráno D&O pojištění.

Rozhodnutí, zda je vhodné přenést riziko na pojistitele by měla předcházet důkladná analýza. Tady jako dobrý zdroj informací může posloužit databáze Loss data collection které obsahuje informace o ztrátových událostech. Je třeba kvalifikovaně odhadnout přínos pojištění vzhledem k jeho ceně. Určit cenu není složité, stačí poptat pojišťovnu. Stanovení přínosu je už o něco složitější, je třeba postupovat individuálně.

[111] Demand Side of Cyber Insurance in the EU: Analysis of Challenges and Perspectives of OESs [online]. 1. European Union Agency for Cybersecurity (ENISA), 2023: European Union Agency for Cybersecurity (ENISA), 2023, [cit. 04.03.2023]. ISBN 978-92-9204-586-9. Dostupné z: https://www.enisa.europa.eu/publications/demand-side-of-cyber-insurance-in-the-eu.
[112] § 159 odst. 1 zákona č. 89/2012 Sb., občanského zákoníku ve znění pozdějších předpisů.

Pojištění hraje důležitou roli i při výpočtu kapitálového požadavku metodou AMA, jelikož banka má díky pojištění nižší požadavky na kapitálovou přiměřenost.

Vhodně zvoleným pojistným produktem lze efektivně snížit negativní dopady z událostí operačního rizika. Důležité je, aby pojistné smlouvy byly pravidelně aktualizovány ve vztahu k rizikům, která kryjí.

6 Sběr událostí operačního rizika

Vyhláška č. 163/2014 Sb., bankám ukládá povinnost pravidelně identifikovat, měřit monitorovat, hlásit a pracovat s operačními riziky. Nástrojem, jak těmto povinnostem dostát i LDC.

LDC zahrnuje sběr, evidenci, měření validaci sledování a také reporting událostí operačního rizika. V některých případech je součástí consequence management.

LDC probíhá průběžně, jedná se o nikdy nekončící proces. Většinou dochází v bankách ke sběru událostí bez ohledu na výši ztráty. Následně je událost odpovědnými pracovníky individuálně posuzována. Přičemž při posuzování je třeba ke každé události přistupovat individuálně v souladu s metodikou pro řízení operačních rizik a v neposlední řadě v souladu s best practice.

Sbírat události operačního rizika je možno několika způsoby.[113]

1. Systém sběrných míst pracovníci jsou kromě jiných úkolů pověřeni i sběrem některých událostí operačního rizika a zaznamenávat je do systému banky. Následuje samozřejmě kontrola správnosti a konzistence dat, což už je většinou práce OpRisku.
2. Využití analýzy interních účtů, na které jsou zaznamenány události operačního rizika a dochází k následné analýze účetních záznamů. Tato metoda se v praxi používá spíše jako doplňková.
3. Systém všichni pracovníci zadávají události operačního rizika do databáze. Tato metoda je vhodná spíše pro menší banky. Následuje opět kontrola správnosti a konzistence dat.

Je možné kombinovat metody 1+2, 3+2, což zaručuje vyšší pravděpodobnost záchytu všech událostí do interního systému banky. Při detailním přehledu rizik je možno je efektivněji řídit.

[113] MAZÁNKOVÁ, Věra a Michal NĚMEC. *Operační riziko a jeho dopady do finanční stability* [online].[cit.10.02.2023].Dostupnéz:https://www.cnb.cz/export/sites/cnb/cs/financnistabilita/.galleries/zpravy_fs/fs_2007/FS_2007_clanek_4.pdf.

Obrázek 11 - Proces LDC, vlastní tvorba

6.1 Hlášení událostí operačního rizika

Banka musí mít jasně definovaná pravidla, kdo a jakým způsobem hlásí, případně zadává události do databáze. Důležitou roli hraje i čas, tedy jak rychle po zjištění událostí má tato být zadána do databáze. Detaily je třeba definovat v interních předpisech.

6.2 Zpracování událostí operačního rizika

Zpracování událostí operačního rizika v databázi musí mít předem jasně definovaná pravidla, která budou zakotvena v interních předpisech. Dále je nutné zavést vhodný nástroj ke sběru událostí. Zpravidla jde o některé ze softwarových řešení. Programů je na trhu celá řada. Nástroj je vždy třeba upravit pro potřeby konkrétní banky se zohledněním jejich specifik, zejména organizační struktury, linií podnikání a dalších.

1. Určit, kdo bude mít oprávnění zadávat události do nástroje/databáze.
2. Vydefinovat událost operačního rizika. Tedy jaká událost je považována za událost operačního rizika, kterou se banka bude zabývat ve smyslu vyšetřování a práce s událostí. V praxi bývají stanoveny parametry na základě, kterých je událost považována za událost operačního rizika.
3. Určit, které události operačního rizika mají být reportovány vyššímu managementu a v jakém okamžiku.
4. Určit odpovědné oddělení za validaci události a hlášení vyššímu managementu. Po zadání události do databáze je třeba s událostí pracovat, což může provést vždy jen pověřený pracovník. S událostí je třeba pracovat. Určit a zadat do databáze zejména následující informace.

    - Datum kdy událost vznikla.
    - Datum, kdy jsme se o události dozvěděli.

- Určit kořenovou příčinu události. Ta nemusí být na první pohled patrná. Často se stanoví až v průběhu práce/vyšetřování události.
- Jedná se o OpRisk událost nebo ne?
- Typ události operačního rizika. Klasifikace události do LDC nástroje dle interní metodiky.
- Kde se událost stala? Na jakém oddělení dle organizační struktury?
- Selhaly nějaké vnitřní kontrolní mechanismy?
- Jaké dopady událost má? Jedná se o přímé finanční dopady? Nepřímé finanční dopady, potenciální ztrátu, zisk z události?

Abychom se nepohybovali pouze v abstrakci uvedeme si příklady, které vychází z volně dostupných dat.

6.2.1 Praktický příklad Phishing na klientku banky

Na call centrum banky Čtyřlístek a.s. se dne 11.03.2023 obrací klientka s tím, že jí z účtu záhadně „zmizelo“ 100 000 Kč. Telefonní bankéř ověřuje totožnost klientky v souladu s legislativou. Bankéř se táže klientky, co že se stalo na jejím účtu? Klientka odpoví, že jí z účtu „zmizelo“ 100 000 Kč. Bankéř při pohybu na účtu zjistí, že částka ve výši 100 000 Kč odešla k protistraně Binance, tedy do kryptoměn. Částka je zaúčtovaná, z banky odešla. Stop platby tedy nelze uskutečnit. Bankéř vidí, že transakce byla řádně dvou faktorově autorizována. Při telefonním hovoru vyjde najevo, že klientka prodávala přes inzertní portál dětské boty. Klientce se ozval zájemce o boty a žádal o údaje k platební kartě, aby mohl na kartu poukázat platbu za boty a údajně poslat kurýra pro zboží. Klientka údaje k platební kartě včetně CVV kódu vyplnila. Tím fakticky dala útočníkovi kartu plně k dispozici. Autorizační OTP kódy klientka útočníkovi poslala prostřednictvím aplikace Whats app. Co tedy udělá bankéř? Pravděpodobně okamžitě zablokuje platební kartu pro odchozí platby a totéž provede i s účtem klientky. Klientce je doporučeno změnit jméno a heslo do internetového bankovnictví a znovu vystavena platební karta. V tomto případě se jedná o banku, která nepoužívá bankovní identitu, takže tuto není třeba blokovat. Teď si událost rozebereme z pohledu operačního rizika. Pro zjednodušení počítejme, že jde o malou banku, kde událost do databáze zadává každý zaměstnanec a s událostí pracuje pověřený zaměstnanec.

- Datum kdy událost vznikla. Událost vznikla 11. 03. 2023.
- Datum, kdy jsme se o události dozvěděli 11. 03. 2023.
- Určit kořenovou příčinu události. Na první pohled se zdá, že se jedná o externí událost. Klientka údaje k platební kartě předala dobrovolně útočníkovi. Přičemž byla při převzetí platební karty poučena o tom, že údaje ke kartě nemá nikomu předávat. V autorizačním klíči internetového bankovnictví je navíc upozornění o tom, že citlivé údaje nemají být nikdy nikomu předány.
- Jedná se o OpRisk událost nebo ne? Z prvotního šetření se zdá, že o Oprisk událost nepůjde, jelikož banka nepochybila. Platba byla potvrzena řádně ze strany klientky.
- Je třeba reportovat managementu? V tomto případě podle interní metodiky nikoliv.
- Typ události operačního rizika. Klasifikace události do LDC nástroje dle interní metodiky.
- Kde se událost stala? Na jakém oddělení dle organizační struktury? V tomto se dle organizační struktury jedná o individuální bankovnictví. Jedná se také o podvodnou platbu. Což je třeba při zadání události zohlednit.
- Selhaly nějaké vnitřní kontrolní mechanismy? Z prvotního šetření se zdá, že nikoliv. V průběhu šetření události se opak neprokázal.
- Jaké dopady událost má? Jedná se o přímé finanční dopady? Nepřímé finanční dopady? Na banku nemá přímý finanční dopad. Přímý finanční dopad má na klientku banky.
- Můžeme zavést nějaké mitigační opatření ke zmírnění události? Ne, další transakce patrny nejsou.
- Prevence dalšího útoku ano, změnit přístupové údaje klientky k jejímu účtu. Snížit limity na platební kartě, vydat novou platební kartu.

Nejedná se tedy o událost operačního rizika. Jedná se však o LDC událost. V databázi tedy své místo má. Jedná se také o podvodnou platební transakci, která bude v souladu s legislativou reportována.

6.2.2 Pokuta pro banku neuchování telefonních záznamů s investory

Tento příklad vychází z případu sankce pro Českou spořitelnu a.s. ze strany ČNB, jako orgánu dohledu nad finančním trhem. Česká spořitelně byla vyměřena pokuta ve výši 2 750 000 Kč. [114]

V bance Čtyřlístek a.s. jsou poskytovány klientům investiční služby, které zahrnují přijetí a poskytnutí pokynů zákazníka. V interních instrukcích chybí pokyn, pro zaměstnance, že hovory, týkající se investic lze s klienty uskutečnit pouze prostřednictvím nahrávaných telefonních linek.

Dne 11. 03. 2021 volal investičnímu bankéři Leoši Šťastnému na jeho soukromý mobilní telefon pan Dalimil Kočička, dlouholetý klient. Pánové se dobře znali, již několik let spolu ke spokojenosti obou spolupracovali. Pan Dalimil Kočička volal s pokynem nákupu cenných papírů ve výši 2 000 000 Kč. Pan Leoš Šťastný pokyn přijal a obchod provedl. Obchod však neproběhl v souladu s legislativou, jelikož hovor, respektive pokyn neproběhl přes nahrávaný telefonní hovor. Pan Dalimil Kočička následně 12. 03. 2023 podal písemnou reklamaci do internetového bankovnictví. Reklamoval výši provedeného nákupu cenných papírů. Cenné papíry měly být nakoupeny za částku 1 000 000 Kč. Reklamaci si převzalo reklamační oddělení a začalo ji v souladu s reklamačním řádem banky Čtyřlístek a.s. řešit.

- Datum kdy událost vznikla. Událost vznikla 11. 03. 2023, datum uskutečnění telefonického hovoru.
- Datum, kdy jsme se o události dozvěděli 12. 03. 2023, fakticky datum podání reklamace.
- Určit kořenovou příčinu události. Kořenová příčina události jsou nejasné pokyny v interních předpisech banky, kde není jasně uvedeno, že hovory od klientů mohou být přijímány pouze na nahrávaných, pracovních telefonních číslech. Toto je kořenová příčina. Zda pan Leoš Šťastný pokyn provedl chybně se nedozvíme. Záznam z telefonního hovoru chybí.

[114] Rozhodnutí České národní banky č.j. 2022/85885/570 ze dne 29. srpna 2022, sp.zn. Sp/2019/596/573. https://www.cnb.cz/export/sites/cnb/cs/dohledfinancnitrh/.galleries/prilohy/SSp2019_00596_CNB_573.pdf.

- Jedná se o OpRisk událost nebo ne? Tady o Oprisk událost půjde. Banka nejednala v souladu s legislativou. Měla nejasné interní pokyny směrem k zaměstnancům.
- Typ události operačního rizika. Klasifikace události do LDC nástroje dle interní metodiky. Dle interní metodiky se jedná o chybnou parametrizaci procesu. Dle CRR o kategorii provádění transakcí, dodávky a řízení procesů.
- Kde se událost stala? Na jakém oddělení dle organizační struktury? V tomto se dle organizační struktury oddělení Treasury.
- Selhaly nějaké vnitřní kontrolní mechanismy? Neselhaly, jelikož nebyly nastaveny.
- Jaké dopady událost má? Událost měla přímý finanční dopad na klienta. Rozporoval transakci ve výši 1 000 000 Kč, kurzovní rozdíl se rovnal částce 35 000 Kč, kterou nárokuje po bance. Pro banku v případě uznání reklamace půjde o přímou ztrátu ve výši 35 000 Kč. V případě prokázání pochybení ze strany banky. Eventuální závěr: prokáže se, že banka nepochybila, ale klientovi reklamaci uzná. V takovém případě nepůjde o událost operačního rizika, ale o obchodní rozhodnutí. Událost sice do LDC zadána bude, nebude však považována za OpRisk.

LDC je velmi důležitým zdrojem informací. Výstupy z LDC se hojně užívají při přípravě RCSA, scénářových analýz, KRI a dalších.[115]

6.3 Reporting událostí operačních rizik

Událost může mít natolik závažný dopad, že je třeba ji reportovat. Reporting můžeme rozdělit do dvou základních kategorií.

1. Reporting interní dle závažnosti rizika a jeho dopadu reportovat v souladu s organizační strukturou předem určené linii. Např. Členům představenstva, manažerům atd. Jak znázorňuje tabulka níže.

[115] Operational Loss Events Internal and External Data: Operational Risk Sound Practice Guidance. The Institute of Operational Risk, str. 15.[online]. SWORD: The Institute of Operational Risk, 2019 [cit. 12.03.2023]. Dostupné z: https://www.ior-institute.org/sound-practice-guidance/operational-loss-events/.

Závažnost rizika	Rozhodovací pravomoc
Extrémní	Představenstvo banky BoD
Vysoké	Úroveň B-2
Střední	Úroveň B-1
Nízké	Hodnotitel RCSA

Tabulka 1 Rozhodovací matice hlášení operačních rizik, vlastní tvorba

2. Reporting externí podle typu události reporting např. ČNB, NUKIB atd. U některých druhý událostí je stanoven obligatorní reporting.

6.4 Rozhodnutí o reakci na událost

Na vzniklou událost je třeba reagovat. Tedy událost je třeba řádně prošetřit, rozhodnout o nutnosti nápravné akce a následně událost uzavřít. To vše v souladu s interními předpisy. Při rozhodnutí o nápravné akci je třeba tuto nadefinovat, zadat do systému, sledovat a následně uzavřít. Po realizaci nápravné akce je možné považovat událost za uzavřenou.

7 Risk and Control Self Assesment

Vyhláška č. 163/2014 Sb., bankám ukládá povinnost pravidelně identifikovat, měřit monitorovat a hlásit operační rizika. Nástrojem, jak těmto povinnostem dostát je Risk and Control Self Assesment, (dále jen RCSA).

Hlavním cílem RCSA je identifikace a měření operačních rizik. Co se týče materiality je na bance, jaké operační rizika chce měřit. Většinou se v rámci RCSA identifikují a měří operační rizika, jejichž materialita je finančně ohodnocena částkou. Např. banka identifikuje a měří operační rizika s dopadem nad 25 000 Kč. Jako událost operačního rizika je označena ta, jejíž dopad přesahuje danou hranici.

Příklad 1: Klient pod vlivem alkoholu poškodí bankomat ve vlastnictví banky, jelikož bankomat po chybném zadání pinu nevydal klientovi hotovost. Celková způsobená škoda je 5 000 Kč. Toto je operační riziko, jedná se o poškození majetku banky. V rámci LDC do databáze zadáno bude. O riziko v rámci RCSA se jednat nebude, jelikož není materiální.

Příklad 2: Pět bankomatů banky je napadeno tzv. Black boxingovým útokem. Black boxingový útok spočívá v tom, že pachatelé pomocí softwaru ovládají předmětný bankomat a donutí ho k vydání hotovosti. Tady se také jedná o operační riziko. Toto riziko by již v rámci RCSA identifikováno a zaznamenáno být mělo. Toto riziko je materiální, jelikož se pohybujeme v milionových částkách.

V rámci RCSA se dále identifikuje a posuzuje efektivita kontrolního prostředí. Tedy zda jsou zavedeny kontrolní mechanismy a jak efektivní jsou.

Dále RCSA slouží k rozhodnutí o operačním riziku. Tedy o jeho přijetí, zavedení nápravného opatření vedoucí k jeho snížení. Lze také rozhodnout o vyvedení dopadů nebo odstranění operačního rizika.

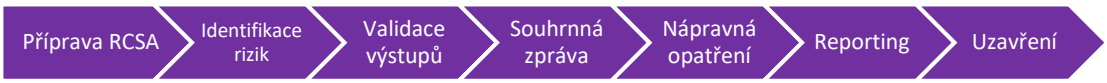
Výsledky RCSA mohou sloužit dále jako podklad pro tvoření klíčových indikátorů rizika.

RCSA probíhá většinou na roční frekvenci nebo v případě, kdy se podstatně změní okolnosti. Způsob provedení je většinou top down nebo bottom up metodou. Záleží na konkrétní organizaci, který model si zvolí. RCSA nejčastěji probíhá dvěma formami.

1. Dotazníkovým šetřením. Méně časové náročné. Vhodné spíše pro větší organizace. Dotazníky jsou odesílány pracovníky operačního rizika ve standardizovaných šablonách.
2. Workshopovou formou. Časově výrazně náročnější. Workshopy metodicky vedou většinou pracovníci operačního rizika, kteří účastníkům workshopu poskytují metodickou podporu. Samozřejmostí je zaznamenávání výsledků workshopů do standardizovaných šablon.

7.1 Fáze RCSA

RCSA probíhá v několika fázích, které na sebe logicky a časově navazují. RCSA se provádí vždy na další kalendářní rok. Např. v roce 2023 provádíme RCSA pro rok 2024. Tedy identifikujeme a dále pracujeme s riziky, se kterými se v roce 2024 může banka potkat.



Obrázek 12 - Fáze RCSA, vlastní tvorba

7.1.1 Příprava RCSA

Příprava RCSA je pro efektivitu provedení velmi důležitá. Je třeba jí věnovat pozornost. Při přípravě RCSA je třeba pracovat s výstupy z LDC, KRI (dále jen klíčové indikátory rizika), scénářových analýz, externích událostí. V rámci přípravy, je dobré se zabývat následujícími otázkami: Podívat se s jakými riziky se banka v uplynulém roce potýkala a porovnat s předchozími obdobími. Je patrný nějaký trend? Z čeho pramení?

1. Jaká je celková ztráta z operačního rizika za předchozí rok?
2. Jaké linie podnikání vygenerovaly nejvyšší ztrátu?
3. Jaká je výše přímých, nepřímých, potenciálních dopadů za předchozí rok?
4. Je na nějakou událost vytvořena rezerva? Jak vysoká?
5. Čeká banku v následujícím roce něco důležitého pro řízení rizik? Např, stěhování, akvizice, změna obchodní strategie?

6. Byla na základě událostí operačních rizik zavedena nápravná opatření? Jsou již splněna?
7. Máme jasně stanovené role a odpovědnosti v rámci RCSA? Pro přehlednost uvádím do tabulky.[116]

Role	Odpovědnosti
Řídící orgán	Jaká je role řídícího orgánu. Např schvaluje celkové výsledky RCSA.
Senior management	Např. schvaluje rizika identifikovaná v RCSA od určité úrovně.
Střední management	Např. schvaluje rizika identifikovaná v RCSA od určité úrovně.
Risk vlastník	Vlastník, kterému je přiřazeno riziko v závislosti na závažnosti. Dohlíží na nápravné kroky k danému riziku.
Vlastník kontroly	Odpovědný za návrh a implementaci nové efektivní kontroly v první nebo druhé úrovni.

Tabulka 2- Role a odpovědnosti v RCSA, vlastní tvorba

7.1.2 Provedení RCSA – identifikace operačních rizik

RCSA lze v praxi provést několika způsoby. Dotazníkovým šetřením, formou workshopů nebo kombinací. U všech forem je důležité řádně připravit časový harmonogram, šablony, podkladová data, krátkou prezentaci na téma RCSA. Podklady je vhodné zaslat účastníkům RCSA v předstihu. Řádné vysvětlení účelu RCSA je velmi důležité, zvyšuje pravděpodobnost přesných a validních výsledků celého RCSA procesu.

V rámci provádění RCSA jsou identifikována rizika. Následně je třeba v rámci RCSA také vyhodnotit dopad a pravděpodobnost. To se děje prostřednictvím matice rizik, která odráží rizikový apetit banky.

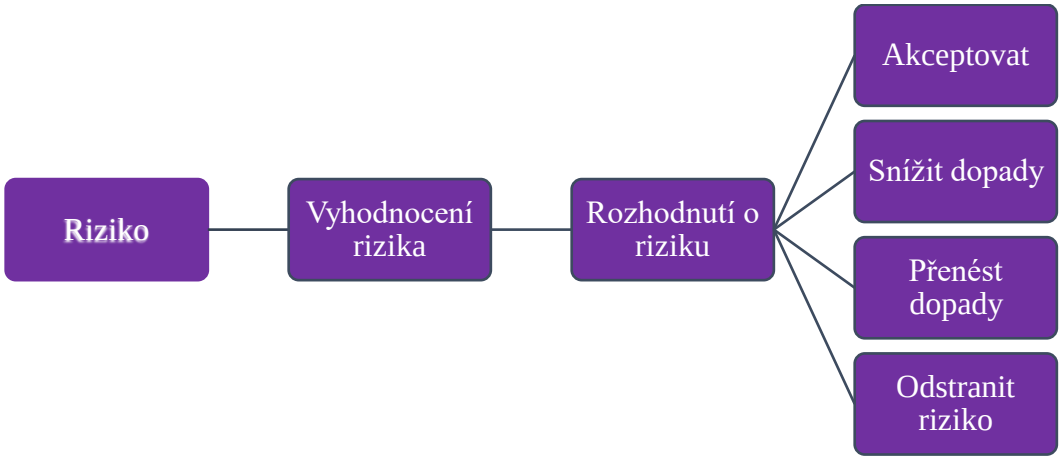
[116] Vlastní zpracování na základě podkladu Risk and Control Self Assessment: Operational Risk Sound Practice Guidance [online]. The Institute of Operational Risk, 2021, ,23 [cit.01.03.2023]. Dostupné z: https://www.ior-institute.org/sound-practice-guidance/risk-and-control-self-assessment/.

Pravděpodobnost					
	Minimálně jednou ročně	Nízké	Střední	Vysoké	Extrémní
	Jednou za 1-5 let	Nízké	Nízké	Vysoké	Extrémní
	Jednou za 5-10 let	Nízké	Nízké	Střední	Vysoké
	Více než 10 let	Nízké	Nízké	Střední	Vysoké
		1-10 mil	10-25 mil	25-75 mil	75 mil

Dopad

Tabulka 3 - Matice rizik, vlastní tvorba

V rámci procesu RCSA je riziko identifikováno, vyhodnocen jeho dopad a pravděpodobnost. Na základě těchto veličin je riziku přiřazena materialista od nízké přes středný po vysokou až extrémní v souladu s maticí rizik.



Obrázek 13 - Reakce v rámci RCSA, vlastní tvorba

7.1.3 Validace výstupů RCSA

Ať už si banka zvolí dotazníkovou, workshopovou nebo jinou metodu k provedení RCSA je třeba výstupy validovat.

Validací výstupů se nemyslí akceptace rizika. O riziku je rozhodováno akceptací, snížením, přenesením dopadů a odstraněním. Validace znamená souhlas s definovanými riziky, kontrolním prostředím a rozhodnutím o riziku. O riziku je rozhodováno v souladu s rozhodovací maticí.

Závažnost rizika	**Rozhodovací pravomoc**
Extrémní	Představenstvo banky BoD
Vysoké	Úroveň B-2
Střední	Úroveň B-1
Nízké	Hodnotitel RCSA

Tabulka 4 - Rozhodovací matice, vlastní tvorba

7.1.4 Souhrnná zpráva o výsledcích RCSA

Jakmile je RCSA provedeno a validováno je třeba informovat management o výsledcích. Nezbytností je vyhotovení zprávy s počtem identifikovaných rizik, jejich závažností dle matice rizik. Dále třeba management seznámit s navrhovanými nápravnými opatřeními. V případech, kdy o reakci na riziko rozhoduje BoD, požádat BoD také o reakci na rizika v jejich gesci. To vše v souladu se strategií banky za použití best practice. Obrázek níže znázorňuje výsledky RCSA v číslech. V tomto případě je třeba BoD požádat o reakci na čtyři rizika s extrémním dopadem, dle výše uvedené matice rizik.

Minimálně jednou ročně	50	5	9	2
Jednou za 1-5 let	10	9	4	2
Jednou za 5-10 let	10	25	14	1
Více než 10 let	14	2	14	41

Tabulka 5- Matice rizik v souhrnné zprávě, vlastní tvorba

7.1.5 Nápravná opatření vzešlá z RCSA

Z RCSA často vychází nutnost zavedení nějakého nápravného opatření. Tato nápravná opatření jsou zadávána a monitorována následným procesem issue managementu. Tento proces navazuje na provedené RCSA a zajišťuje, že nápravná opatření budou řádně implementována. Případně může revizi stávajících klíčových indikátorů nebo definici indikátorů nových.

7.1.6 Uzavření RCSA

Jakmile jsou všechny výše popsané kroky provedeny, RCSA můžeme pro daný rok považovat za uzavřené a začít s přípravou roku následujícího.

8 Další způsoby řízení operačních rizik

Způsobů, jak měřit, řídi, sledovat, snižovat operační rizika je více. Vyberu z mého pohledu nejzajímavější z nich. Přičemž platí, že definovat klíčové indikátory nebo scénářové analýzy není snadné.

8.1 Klíčové indikátory rizika

O klíčových indikátorech jsem se zmínila již v předchozí kapitole. Revize a definice KRI často navazuje na RCSA. Jelikož KRI může částečně ošetřit rizika z RCSA vzešlá.

KRI lze definovat na měřitelná rizika mít na rizika. KRI existují v podstatě dva typy.

1. Prediktivní KRI se v praxi definuje poměrně obtížně. Jedná se o indikátor, který nás dopředu upozorní, že je něco v nepořádku. Máme tedy čas delší čas na reakci.
2. Následný indikátor KRI nám ex post řekne, že k něčemu došlo. Např. KRI indikátor je nastaven školení pro zaměstnance na 15 %. Pokud tedy povinným školením neprojde měsíčně více, než 15 % zaměstnanců, KRI „zčervená.“ Dá nám informaci o tom, že více, než tolerovaná skupina zaměstnanců nesplnila své povinnosti. Následně jsou KRI reportována a přijata nápravní opatření

8.2 Scénářové analýzy

Scénářové analýzy jsou významnou součástí procesu řízení operačního rizika. Jedná se o poměrně významný vstup pro výpočet kapitálového požadavku pro operační rizika u některých metod, zejména AMA.

Scénářová analýza je předem vydefinovaný scénář, kterému může být reálně banka vystavena v případě jeho realizace. Scénář většinou navrhuje ke schválení oddělení operačních rizik. Při jeho definicí vychází z reálného rizika, kterému banka je nebo může být vystavena. Jako podkladová data pro výběr scénářů slouží především externí události, interní ztrátové události vycházející z LDC, výsledky z RCSA, klíčové identifikátory rizika, auditní nálezy atd.[117]

[117] CHAPELLE, Ariane. Operational risk management: best practices in the financial services industry. Hoboken: Wiley, 2018, str 14.

8.3 Fáze scénářových analýz

Fáze scénářových analýz jsou shodné s fázemi RCSA. Nejobtížnější na celém procesu je z mého úhlu pohledu definice proveditelného scénáře. Pro mě osobně je scénářová analýza ta nejzajímavější a nejzábavnější část z řízení operačních rizik.

9 Významné události operačního rizika

Předmětem této kapitoly budou události operačního rizika za posledních pět let.

První tři příklady budou věnovány poškození reputace. Reputační riziko se do operačních rizik samostatně neřadí, v kombinaci se selháním interních procesů, lidského faktoru atd. už o operační riziko půjde.

Ještě, než přistoupím k jednotlivým případům, považuji za důležité vyjasnit si, co to je run na banku. Jelikož s tím to pojmem budu dále pracovat.

Při slovním spojení run na banku si většina z nás představí dlouhé fronty před pobočkami banky, davy snažící se dostat ke svým penězům. Pro veřejnost jde o signál, že v dané bance není všechno v pořádku. Pří runu na banku se klienti domnívají, že banka nebude schopna dostát svým závazkům a hromadně vybírají depozita v krátkém časovém horizontu.[118]

Ztráta důvěry klientů může nastat z rozličných příčin. Nejčastěji se jedná o ztrátu důvěry, která je způsobená negativní reklamou, změnou akcionáře, geopolitickou situací a mnohé další. Podstatnou roli u runu hraje čas. Je důležité, jak rychle a v jakém množství se depozita z banky odlévají.

Výběr depozit může být pomalejší, ale i tak může banku poměrně výrazně destabilizovat.

Nebezpečí runu se skrývá v tom, že se nemusí týkat jedné banky. Může dojít k tomu, že střadatelé pod vlivem emocí začnou hromadně vybírat svá depozita z většího množství bank na trhu. Pád jedné banky může zásadně narušit důvěru klientů v bankovní systém jako celek. To je problém, se kterým se Česká republika v minulosti potýkala. Zejména v souvislosti s pády bankovních domů v 90 letech 20 století. Od té doby však bankovní svět prošel významnou transformací z pohledu regulatorních podmínek, která je daleko přísnější, než tomu bylo v minulosti.

I přes velmi robustní regulaci však run na banku a případný pád vyloučit nelze.

[118] Run (útok na banku).*: Run* [online]. [cit. 07.01.2023]. Dostupné z: https://cbaonline.cz/run-utok-na-banku.

9.1 Run na Sberbank CZ a.s.

Při pohledu do výroční zprávy Sberbank CZ a.s. za rok 2021 zjistíme, že ke dni 31.12.2021 se jednalo zdravou banku s bilanční sumou 84,975 miliardy Kč, tedy menší, stabilní bankovní dům. Kapitálová přiměřenost dosahovala hodnoty 17,42 %, což je velmi dobrý výsledek.[119] Počet úvěrů v selhání byl 2,64 %, tedy nízká míra úvěru v selhání. Počet zaměstnanců 700 také relativně stabilní. Banka byla za rok 2021 zisková s počtem 24 poboček po celé České republice.[120]

Dne 13. 02. 2022 tedy pouhých 11 dní před runem na Sberbank CZ a.s. CEO Sberbank CZ a.s. v rozhovoru pro E15 uvádí, že banka si nechala zpracovat průzkum veřejného mínění, ze kterého vyplývá, že postoj Čechů v bance je spíše neutrální. Což se objektivně neprokázalo. Dále paní ředitelka uvádí. „*Jsme skutečně bankou s ruským kapitálem. Jsme ale zároveň lokální banka, která se řídí regulacemi ze strany České národní banky. Diplomatické vztahy se občas zhoršují nebo naopak zlepšují, to platí pro většinu zemí, Rusko není výjimkou. Měli bychom se ale spíše soustředit na byznysové zájmy.* “[121] Je jasné, že banka se musela řídit českými právními předpisy. V opačném případě by na našem území nemohla podnikat. Co se týče konstatování o vnímání banky Sberbank CZ veřejností, tak se ukázalo, že mediální obraz negativní nebyl. Za necelé dva týdny se ukázalo, že s mediálním obrazem je zcela odlišná od provedeného průzkumu. Když ve čtvrtek 24. 2. 2022 vpadla ruská vojska na Ukrajinu, celý svět byl v šoku. Osud Sberbank CZ a.s., jak se později ukázalo, byl definitivně zpečetěn. Sberbank CZ a.s. byla hned ráno po vpádu vojsk podrobena výraznému negativnímu mediálnímu obrazu. Příčinou byly přímé vazby na Rusko, jak je zobrazeno na obrázku níže.[122] To, že se jednalo o banku s ruským kapitálem banka otevřeně přiznávala.

[119] Výroční zpráva Sberbank [online]. 2022, Praha [cit. 05.02.2023]. Str. 5. Dostupné z: https://www.sberbank.cz/media/files/povinneinformace/vyrocnizpravy/Vyrocni_zprava_2021_CZ.pdf.
[120] Totéž str 12.
[121] WEINBENDER, Kristina. Zvažujeme akvizice menších bank, říká nová šéfka české Sberbank [online]. [cit. 05.01.2023]. Dostupné z: https://www.e15.cz/byznys/finance-a-bankovnictvi/zvazujeme-akvizice-mensich-bank-rika-nova-sefka-ceske-sberbank-1387520.
[122] Vlastní zpracování na základě podkladů ve výroční zprávě Sberbank CZ a.s. dostupné https://www.sberbank.cz/media/files/povinneinformace/vyrocnizpravy/Vyrocni_zprava_2021_CZ.pdf.

Obrázek 14 - Vlastnická struktura Sberbank CZ a.s, vlastní tvorba na základě údajů ve výroční zprávě Sberbank CZ a.s.

Před pobočkami banky se začaly hned ráno po vpádu vojsk tvořit fronty klientů. Media o situaci intenzivně informovala.[123] Vývoj byl velmi rychlý. V pátek 25. 2. 2022, banka pod vlivem runu nebyla schopna plnit své závazky vůči klientům.[124] Pobočky byly od 25. 2. 2022 14.00 uzavřené, internetové bankovnictví nefunkční. Což je samo o sobě problematické. Banka prakticky přestala plnit svou funkci a pro klienty byla nedostupná. Bankovní licence se ocitla v přímém ohrožení. Český bankovní sektor netrpělivě čekal, zda Sberbank CZ a.s. přes víkend zvládne situaci stabilizovat, zastavit odliv likvidity a uklidnit nervózní klienty.

V neděli 27. 02. 2022 projednala bankovní rada ČNB na mimořádném zasedání postup, jaký bude vůči Sberbank CZ a.s. uplatňován.[125] Domnívám se, že už na tomto jednání bylo jasné, že likvidní situace v bance špatná a konec jedné banky je nadohled.

Tehdejší guvernér ČNB Jiří Rusnok uklidňoval veřejnost, když prohlásil: „*Likviditní krize Sberbank CZ byla způsobena externím, geopolitickým vývojem. Jedná se tak o izolovaný a specifický problém banky, která není významná z hlediska tuzemského*

[123] KAHÁNEK, Adam. Klienti ruské Sberbank CZ zahltili pobočky. Ty nakonec zavřely [online]. [cit. 05.02.2023]. Dostupné z: https://www.novinky.cz/clanek/ekonomika-klienti-ruske-sberbank-zahltili-pobocky-ty-nakonec-zavrely-40388375.
[124] ČNB. Tisková zpráva: ČNB odebrala licenci Sberbank [online]. Praha, 2022 [cit. 05.02.2023]. Dostupné z: https://www.cnb.cz/cs/cnb-news/tiskove-zpravy/CNB-odebrala-licenci-Sberbank-CZ/.
[125] ČNB. Tisková zpráva: ČNB zahájila kroky k odejmutí licence Sberbank CZ [online]. Praha, 2022 [cit. 05.02.2023]. Dostupné z: https://www.cnb.cz/cs/cnb-news/tiskove-zpravy/CNB-zahajila-kroky-k-odejmuti-licence-Sberbank-CZ/.

bankovního sektoru. Ten tak i nadále zůstává jedním z nejrobustnějších a nejstabilnějších v Evropě," *Česká národní banka nastalou situaci ve Sberbank CZ od počátku intenzivně řeší a činí vše pro to, aby byl dopad problémů banky na její klienty co nejmenší."*[126] Proč guvernér uklidňoval veřejnost? Důvodů je několik. Prvním z nich je fakt, že bylo třeba zklidnit v tu dobu poměrně rozjitřené emoce. Druhým důvodem byla obava, aby run na Sberbank CZ a.s. nespustil dominový efekt a pod náporem klientů se neocitly i další bankovní domy. To už by nebyl problém izolovaný, ale problém bankovního sektoru.

Odliv depozit se Sberbank CZ a.s. byl tak masivní, že dne 28. 2. 2022 ČNB zahájila kroky k odejmutí licence Sberbank CZ a.s. a to s ohledem na likvidní situaci v bance.[127]

Dne 9. března 2022 začal garanční systém finančního trhu vyplácet náhrady pojištění vkladů.[128] Dne 30 dubna 2022 pozbyla Sberbank CZ a.s. na základě pravomocného rozhodnutí bankovní licenci.[129] Proti rozhodnutí banka opravný prostředek nepodala. Následně na základě usnesení Městského soudu v Praze[130] Sberbank CZ vstoupila dne 2. 5. 2022 do likvidace.

9.1.1 Prevenční detekční a kontrolní opatření

Domnívám se, že situace Sberbank CZ a.s. byla natolik netypickou a nestandartní, že by jejímu pádu nedokázala zabránit ani ta nejlepší opatření od prevence přes detekci. Mitigační opatření v případě, kdy banka run nepřežije smysl nedávají.

U Sberbank CZ a.s. se ukázala materializace geopolitického rizika naprosto jasně. Co by mohlo být prevenční opatření by byla bývala změna akcionáře bez vlivu na Rusko, před invazí. Domnívám se, že pokud by byl akcionář jiný, k pádu banky by pravděpodobně nedošlo.

---

[126] ČNB. Tisková zpráva: ČNB zahájila kroky k odejmutí licence Sberbank CZ [online]. Praha, 2022 [cit. 05.02.2023]. Dostupné z: https://www.cnb.cz/cs/cnb-news/tiskove-zpravy/CNB-zahajila-kroky-k-odejmuti-licence-Sberbank-CZ/.
[127] Tamtéž.
[128] ČNB. Tisková zpráva: ČNB odebrala licenci Sberbank [online]. Praha, 2022 [cit. 05.02.2023]. Dostupné z: https://www.cnb.cz/cs/cnb-news/tiskove-zpravy/CNB-odebrala-licenci-Sberbank-CZ/.
[129] Rozhodnutí ČNB č.j. 2022/38793/570 Praha, 2022 [cit. 05.02.2023]. Dostupné z:https://www.cnb.cz/export/sites/cnb/cs/dohled-financni-trh/.galleries/prilohy/S-Sp-2022_00075_CNB_573.pdf.
[130] Usnesení Městského soudu v Praze č.j. 83Cm 810/2022-7 Praha, 2022 [cit. 05.02.2023]. Dostupné z: https://www.cak.cz/assets/rozhodnuti-o-likvidaci-sberbank.pdf.

Detekční opatření zcela jasná, stav likvidity. Ta, alespoň dle dostupných dat (aktivity ze strany ČNB) z banky odcházela ve velkém množství a rychle. To, že ČNB zasedala v neděli samo o sobě ukazuje, jak vážná situace byla.

V praxi existují nástroje, které do jisté míry dokážou likviditu v krátkém časovém horizontu do banky přivést, ale vyžaduje to čas, a ten Sberbank CZ a.s. prokazatelně pří pohledu na časovou osu neměla.

O mitigačních opatřeních nemá smysl hovořit, jelikož banka jako taková ukončila na území České republiky činnost.

Co nám však pád Sberbank CZ a.s. ukázal? Z mého profesního pohledu zcela jistě jednu věc. Geopolitická situace je významným rizikovým faktorem, kterým je třeba se zabývat více než v minulosti. Je třeba dbát na transparentní akcionářskou strukturu a také jasnou komunikaci směrem ke klientům.

Komunikace je jedna z věcí, kterou Sberbank CZ a.s. nezvládla dobře. Z mého pohledu byla komunikace směrem k veřejnosti pomalá a nedostatečná. Domnívám se, že pokud by komunikace byla zvládnuta lépe, pád Sberbank CZ a.s. by nebyl tak rychlý. To, že by vůbec nenastal si tvrdit netroufám.

Druhá věc, kterou pád ukázal je to, že je třeba se více zabývat reputačním rizikem.

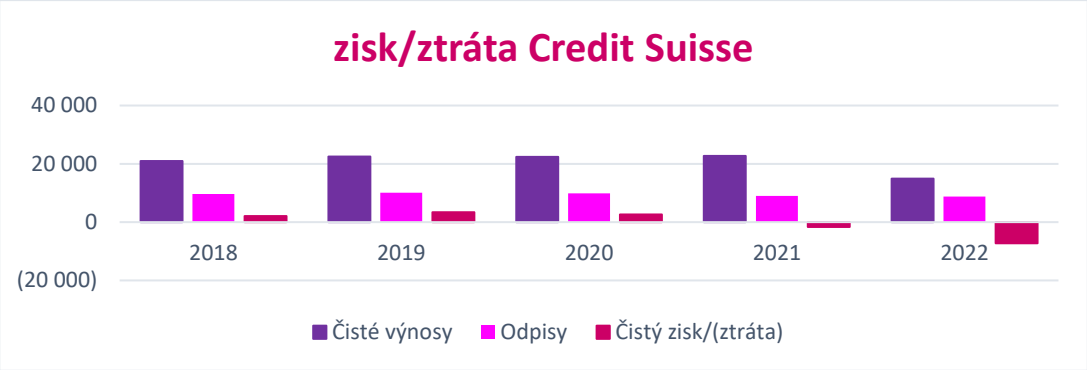
9.2 Credit Suisse

Credit Suisse jsem do diplomové práce zařadila zcela záměrně. V posledních týdnech vzaly události v bance nečekaný obrat.

Credit Suisse je svou velikostí a počtem klientů významná. Z pohledu Švýcarské národní banky se jedná o bankovní instituci velkého významu, a to jak na tuzemském, tak zahraničním trhu.[131] Credit Suisse má z pohledu velikosti, počtu zaměstnanců, odvedených daní vliv i na ekonomiku Švýcarska.[132]

[131] Rapport sur la stabilité financière [online]. Banque Nationale Suisse, 2022 [cit. 10.02.2023]. Str 19. Dostupné z: https://www.snb.ch/fr/mmr/reference/stabrep_2022/source/stabrep_2022.fr.pdf.
[132] Rapport sur la stabilité financière [online]. Banque Nationale Suisse, 2022 [cit. 10.02.2023]. Str 21. Dostupné z: https://www.snb.ch/fr/mmr/reference/stabrep_2022/source/stabrep_2022.fr.pdf.

Při pohledu do výroční zprávy zjistíme, že Credit Suisse je v hluboké ztrátě. V únoru 2023 banka ohlásila, že za rok 2022 je ve ztrátě 7,29 mld CHF.[133] Je na místě podotknout, že se nejedná o exces. Banka je ve ztrátě již po několikáté za sebou. V roce 2021 vykázala ztrátu 1,65 mld CHF.[134] V monitoringu o finanční stabilitě za rok 2021 SNB (Švýcarská národní banka) konstatuje, že v kontextu ekonomického vývoje má banka Credit Suisse relativně nízký provozní zisk,[135] což je první problém. Druhým významným problémem je materializace právních rizik, operačních rizik a také úvěrových rizik.[136] Sečtení všech těchto faktorů najednou je pro banku velký problém.



Obrázek 15 - Credit Suisse zisk a ztráta, vlastní tvorba na základě výroční zprávy Credit Suisse

9.2.1 Příčiny realizace ztrát u Credit Suisse

Při analýze příčin nepříznivých výsledků Credit Suisse vycházím z veřejně dostupných dat. Domnívám se však, že je jich dost na to, abych mohla provést alespoň základní analýzu příčin špatných hospodářských výsledků Credit Suisse. Z veřejně dostupných dat se zdá, že Credit Suisse stojí na pomezí kreditního, operačního, tržního rizika. Převládá riziko kreditní. Operační je ovšem nezanedbatelné. Jaké jsou tedy příčiny realizovaných kreditních ztrát?

[133] Media Release: Credit Suisse makes strong progress on Group strategic priorities; reports net revenues of CHF 3.1 bn and pre-tax loss of CHF 1.3 bn along with a CET1 ratio of 14.1 % in 4Q22 [online]. Zurich, 2023 [cit. 20.03.2023]. Dostupné z: https://www.credit-suisse.com/media/assets/corporate/docs/about-us/media/media-release/2023/02/q4-22-press-release-en.pdf.
[134] Rapport sur la stabilité financière [online]. Banque Nationale Suisse, 2022 [cit. 10.02.2023]. Str 18. Dostupné z: https://www.snb.ch/fr/mmr/reference/stabrep_2022/source/stabrep_2022.fr.pdf.
[135] Tamtéž strana 19.
[136] Tamtéž strana 6.

1. **Příčina první Grensill Capital** byl jedním z důležitých klientů Credit Suisse, který se dostal do insolvence, a to 8. 3. 2021.[137] Banka musela suspendovat 10 mld USD v investicích, spojených s Greensill Capital. Část prostředků ve výši 7,3 mld USD se bance podařilo získat zpět. Zbývající část bude poměrně náročné zpět získat. Sama Credit Suisse ve své výroční zprávě hodnotí, že insolvence Greensill Capital má výrazný negativní dopad na hospodářské výsledky.[138] V roce 2021 skončila Credit Suisse ve ztrátě 1,7 miliardy CHF.
2. **Příčina druhá Archeos Capital Management** Credit Suisse půjčila společnosti Archeos Capital částku ve výši 20 mld USD na nákup akcií. Dle mého názoru je to vysoká riziková expozice i na banku velikosti Credit Suisse. Problémem je vysoká riziková expozice na jednoho klienta. V březnu roku 2021 Credit Suisse investiční banka realizovala ztrátu přibližně 5,5 mld USD v souvislosti s pádem Archeos Capital Managementu, který nebyl již schopen plnit své úvěrové závazky. Tato událost tedy zcela jasně banku poslala do červených čísel. Událost byla tak významná, že nejvyšší management ustanovil speciální nezávislou komisi, jejíž úkolem bylo objasnění důvodů realizace takto významné ztráty. Zpráva čítající 172 stran byla na stránkách Credit Suisse publikována 29. června 2021. Závěry vyšetřovací komise jsou z mého pohledu alarmující a vyplývají z ní následující závěry.

a) Nebrání známých informací v potaz toto je velmi vážné zjištění. Ze zprávy vyplývá, že Credit Suisse měla informace o tom, jak vážná je situace. Mohla podniknout kroky ke zmírnění dopadu, ale neučinila tak. Ignorovala tedy všeobecně známé informace o pozici Archeos. Dopad tedy bylo možno před rozhodným datem zmírnit.[139]

b) Obchod a obchodní model ze zprávy vyplývá, že banka se v oblasti rizik nesoustředila na rizika, i když rizikové indikátory byly skutečně varovné. Oddělení obchodu bylo zaměřeno výrazně pouze na růst objemu obchodů. Indikátory

[137] *Credit Suisse: Annual Report 2022* [online]. Switzerland [cit. 20.02.2023]. Str. 25. Dostupné z: https://www.credit-suisse.com/about-us/en/reports-research/annual-reports.html?aa=rl-onsite-search%2065.
[138] Tamtéž str. 5
[139] Press Release: Le Credit Suisse Group publie le rapport de l'enquête externe indépendante concernant Archegos Capital Management [online]. Zurich [cit. 20.02.2023]. Dostupné z: https://www.credit-suisse.com/about-us-news/fr/articles/media-releases/archegos-202107.html.

úvěrových rizik byly ignorovány. Dalším problémem byla špatná rozhodovací matice a hierarchie v managementu. Platné limity pro úvěrové riziko byly dlouhodobě a výrazně překračovány. Přičemž úvěrové riziko bylo výrazně koncentrováno, což je samozřejmě jev nežádoucí. Úvěrová riziková expozice byla velmi vysoká. Úvěrové riziko nebylo bráno v celém souhrnu.

c) **Risk** ze zprávy vyplývá také pochybení v oblasti operačních a tržních rizik. Riziko z pohledu operačního nebylo dobře řízeno. Jeden z největších problémů byla ignorace koncentrace rizika, která výrazně přesahovala povolené a doporučené limity. Někteří zaměstnanci dlouhodobě upozorňovali na riziko, které Archeos představoval. Nebyly stanoveny lhůty pro nápravu překročených limitů. Překročené limity ve všech oblastech nebyly dlouhodobě a pečlivě sledovány. Operační rizika se spokojila s pouhým velmi jednoduchým spíše obchodním zdůvodněním překročení limitů.
d) **Nedostatečné kompetence a školení managementu** to je další z důvodů realizace obří ztráty Credit Suisse.

Příčin pádu Archeos Capital je samozřejmě daleko více. Je dobré zdůraznit, že nejen Credit Suisse pocítila negativní dopady. Další zasaženou bankou byla japonská Nomura nebo švýcarská UBS.

3. **Příčina třetí** obvinění z praní špinavých peněz poslední skandál, který zmítá Credit Suisse a o kterém nejsou z pochopitelných důvodů k dispozici téměř žádná data.

Tato událost také přispěla k negativnímu obrazu o Credit Susse. K čemu tedy vlastně došlo? U Credit Suisse došlo k úniku osobních údajů, ze kterých je patrno, že banka pravděpodobně prala špinavé peníze drogových dealerů. Jak uvádí Reuters. Bance byla udělena pokuta ve výši 2 milionů CHF v trestním řízení.[140]

Tvrzení Reuters potvrzuje i švýcarský federální trestní soud, který dne 27. 06. 2022 publikoval zprávu pro média ve které uvádí: Soud uznává vinnou bývalou zaměstnankyni Credit Suisse z praní špinavých peněz ukládá jí domácí trest odnětí svobody v délce 20 měsíců a zároveň peněžitý trest. Manažerka v rozmezí od července

[140] Fact box Credit Suisse's scandals - spies, lies and money laundering [online]. Reuters, 2022 [cit. 01.03.2023]. Dostupné z: https://www.reuters.com/business/finance/spies-lies-chairmans-exit-credit-suisses-scandals-2022-01-17/.

2007 do prosince 2008 provedla transakce na pokyn zločinecké organizace, převážně zahraniční bankovní převody, přesto, že měla jasné indicie, že původ prostředků pochází z kriminální činnosti. Tímto jednáním pomohla k tomu, že částka v ekvivalentu 19 milionů CHF unikla spravedlnosti. Co se týče Credit Suisse, soud konstatoval, že v průběhu řízení shledal nedostatky v bance, a to jak v oblasti monitorování a dohledu tak v oblasti hierarchie a compliance. Tyto nedostatky umožnily protiprávní jednání bývalé zaměstnankyně a z tohoto důvodu se banka Credit Suisse odsuzuje dle ustanovení §102 alinea 2 trestního zákona k pokutě ve výši 2 miliony CHF.[141] Z vyjádření trestního soudu je tedy patrné, že v bance byly nedostatečně pokryta rizika compliance, která umožnila praní špinavých peněz. Banka Credit Suisse tedy od soudu odešla s peněžitým trestem ve výši 2 milionu CHF.

Zajímavý pohled na problematiku fondů nabízí The Economist. Ten ve svém článku zdůrazňuje, že banky hledají investiční příležitosti, což ve světle nízkých úrokových sazeb a široké a přísné regulace není snadné.[142] The Economist uvádí, „*že pro banky je příliš drahé, aby obchodovaly na trzích pod vlastním jménem, uchylují se tedy k fondům.*“[143] Neříkám, že s tímto názorem bezezbytku souhlasím. Co mě na něm zaujalo je zamyšlení se nad mírou regulace. Dle mého názoru z článku jasně vyplývá, že příliš regulace může mít i negativní dopad.

Je na místě dodat, že za rok 2022 klienti Credit Suisse vybrali z banky téměř 110 mld CHF.[144]

Dne 15.03.2023 v návaznosti na zveřejnění výroční zprávy Credit Suisse Švýcarská národní banka uklidňuje zveřejňuje prohlášení. V tomto uvádí, že situaci v Credit Suisse monitoruje a není třeba se obávat o její stabilitu.[145] Za pár dní ukázalo, že

[141] Cause Ministère public de la Confédération contre Credit Suisse AG et autres prévenus (SK.2020.62). Tribunale Pénale Federale [online]. 27.06.2022 [cit. 02.03.2023]. Dostupné z: https://www.bstger.ch/fr/media/comunicati-stampa/2022/2022-06-27/1275.html.
[142] Archegos, a family office, brings Nomura and Credit Suisse big losses. The Economist [online]. 2022 [cit. 01.03.2023]. Dostupné z: https://www.economist.com/finance-and-economics/2021/03/31/archegos-a-family-office-brings-nomura-and-credit-suisse-big-losses
[143] Tamtéž.
[144] Credit Suisse: Annual Report 2022 [online]. Switzerland [cit. 20.02.2023] str. 5 Dostupné z: https://www.credit-suisse.com/about-us/en/reports-research/annual-reports.html?aa=rl-onsite-search%2065.
[145] SNB and FINMA issue statement on market uncertainty. [cit. 25:03.2023]. Dostupné z: https://www.snb.ch/en/mmr/reference/pre_20230315/source/pre_20230315.en.pdf.

přichází zásadní obrat. Banka UBS s Credit Suisse spojí své síly. Respektive pokusí se banku zachránit. Tato transakce se neobejde bez asistence státu a SNB. Jaké budou přesně parametry záchranného balíčku se ukáže v následujících týdnech.

9.3 Deutsche Bank

Ekonomická situace v Deutsche bank je jiná než Credit Suisse. Pro rok 2022 ohlásila zisk před zdaněním ve výši 5,6 mld EUR.[146] Banka se tedy nepohybuje v červených číslech.

Deutsche Bank obdržela sérii pokut za usnadňování praní špinavých peněz a nedostatečnou kontrolu nad transakcemi. Tedy společný jmenovatel poškozená reputace, nedostatky v řízení risku a Compliance zde najdeme. Problémů Deutsche bank je několik.

a) **Nedostatečný dohled nad transakcemi** německý regulační úřad BaFin uložil v prosinci 2021 Deutsche bank pokutu ve výši 8,66 milionů EUR. Sankce se týká nedostatečného dohledu nad transakcemi s mezinárodními sazbami. Německý regulační úřad přímo uvádí, že „*banka neměla nastaven efektivní preventivní systém kontrol a vnitřních předpisů*.[147] Toto zjištění je samo o sobě závažné.
b) **Praní špinavých peněz** Deutsche bank byla podezřelou z umožňování transakcí vedoucí k praní špinavých peněz.[148] Mezi podezřelými bylo více bankovních domů. U Deutsche bank byl počet podezřelých transakcí nejvyšší.

9.3.1 Společný jmenovatel

Při pohledu na Sberbank CZ, Credit Suisse a Deutsche bank zjistíme, že banky spojují tři témata. Selhání řídícího a kontrolního systému bank, poškozená reputace, rizikové investice.

Co si lze představit pod pojmem reputační riziko? Dle Basel II lze reputační riziko definovat jako „*riziko, které vzniká negativním vnímáním ze strany části zákazníků,*

[146] Media Release Deutsche Bank [online]. 2022 [cit. 02.03.2023]. Dostupné z https://www.db.com/news/detail/20230202-full-year-results-2022?language_id=11.
[147] https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Massnahmen/40c_neu_124_WpHG/meldung_211229_deutsche_bank_ag_geldbusse_en.html.
[148] https://www.e15.cz/zahranicni/prani-spinavych-penez-obchazeni-sankci-dokumenty-ukazuji-pochybne-transakce-bank-1373436.

akcionářů, investorů, věřitelů, tržních analytiků nebo jiných relevantních protistran, případně regulátorů a může omezit schopnost banky si udržet stávající, případně navázat nové, obchodní vztahy a zajistit trvalé zdroje financování. Reputační riziko je multidimenzionální a odráží vnímání ostatních účastníků trhu. Reputační riziko existuje po celou dobu fungování. Reputační riziko je odrazem toho, jak efektivní řízení interního managementu rizik v bance je.[149] Tato definice je sice téměř vše zahrnující, z mého pohledu šroubovaná. Reputační riziko je možno definovat i jednodušším způsobem. Reputační riziko lze definovat též *jako riziko ztráty nebo poškození dobré pověsti, tedy pozitivního vnímání ze strany zákazníků, dodavatelů a dalších obchodních partnerů. Je spojeno s nějakou negativní publicitou, kdy hrozí, že zveřejnění určité informace může způsobit ztrátu důvěry obchodních partnerů.*[150] Ať vybereme první nebo druhou definici, tak je dobré si uvědomit, že riziko ztráty dobré pověsti s sebou může přinést velké problémy. Ztráta dobré pověsti může vygradovat v run na banku a její následný pád.

9.4 Raiffeisen stavební spořitelna

Společnosti Raiffeisen stavební spořitelna (dále RSTS) byla udělena sankce ve výši 100 000 Kč. Dle zjištění ČNB *„nedisponovala řídicím a kontrolním systémem, který by byl účinný, ucelený a přiměřený charakteru, rozsahu a složitosti rizik spojených s modelem jejího podnikání a činností, a to v oblasti řízení rizik informačních systémů a informačních technologií v těchto oblastech:*

1. Analýza rizik.
2. Bezpečnostní monitoring.
3. Ochrana proti pokročilým kybernetickým hrozbám.
4. Provoz informačních systémů.
5. Elektronické bankovnictví.
6. Pohotovostní plány.

[149] Enhancements to the Basel II framework [online]. Bank for international Settlement [cit. 05.02.2023]. Dostupné z: https://www.bis.org/publ/bcbs157.pdf.
[150] Reputational Risk [online]. [cit. 05.02.2023]. Dostupné z: https://managementmania.com/cs/reputacni-riziko-reputational-risk.

7. Rekonstruovatelnost auditorských spisů.[151]

Pro oblast operačního rizika je podstatný bod 20.ČNB jako správní orgán měla za prokázané, že RSTS nezapracovala do svých vnitřních předpisů požadavky na procesy posouzení rizik, přezkumy, hodnocení a testování bezpečnosti informací vyplývající. Tedy RSTS postupovala v rozporu s požadavkem ustanovení § 27 odst. 1 písm. c) vyhlášky č. 163/2014 Sb.,[152] který stanoví, že povinná osoba, tedy RSTS zabezpečí, že proces rozpoznávání rizik je zajištěn u všech činností a na všech řídicích a organizačních úrovních a umožňuje odhalování nových, dosud neidentifikovaných rizik.[153] S tímto ustanovením vyhlášky souvisí ještě jedna výtka ČNB směrem k RSTS. Nedostatky se týkaly i nenaplnění požadavků citovaného ustanovení u kybernetických hrozeb a nedostatečným prováděním penetračních testů.[154] Provádění kvalitních penetračních testů je v dnešní době zvýšené aktivity hackerů naprostou nutností.

Další dílčí nedostatky, které správní orgán odhalil se týkaly internetového bankovnictví, síly hesel, snadné odhadnutelnosti hesel atd. Vzhledem k výši uložené sankce však zjištění nebyla správním orgánem pravděpodobně považována za závažná.

[151] Příkaz ČNB: Sp/2022/100/573 [online]. [cit. 2023-03-25]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohledfinancnitrh/.galleries/prilohy/SSp2022_00100_CNB_573.pdf.
[152] Tamtéž.
[153] § 27 odst. 1 písm.c. vyhlášky č. 163/2014 Sb.,
[154] Tamtéž

10 Aktuální kybernetická rizika

V této kapitole si nejdříve legislativně zakotvíme kybernetickou bezpečnost a následně se budu věnovat těm nejpalčivějším kybernetickým rizikům, se kterými se banka nebo klient může dnes setkat.

Na úvod je třeba říct, že v posledních letech došlo k velmi výraznému rozvoji informačních technologií, což s sebou nese i nová rizika a potřebu zajištění kybernetické bezpečnosti. Kybernetická bezpečnost je dnes velmi aktuálním tématem, nejen pro banky a finanční instituce, ale i nemocnice, mobilní operátory, elektrárny a další.

Málo kdo z nás si umí život představit bez instantních plateb, mobilní aplikace internetového bankovnictví, mobilního klíče a dalších. Nové technologie však s sebou nesou nejen pozitiva, ale i negativa v podobě různého spektra dosud nepoznaných operačních rizik.

U zajištění kybernetické bezpečnosti nejde jen o bezpečnost bank a jejich klientů, Kybernetická bezpečnost má mnohem širší dopad. Například citlivé údaje uložené v nemocničních systémech, které by se následkem hackerského útoku mohly dostat do nepovolaných rukou. Nefunkčnost IT systému v nemocnici může způsobit nemožnost provedení život zachraňující operace. V takovém případě už kybernetická bezpečnost nabývá zcela jiný rozměr. Už nejde „jen o peníze," ale o lidské životy.

10.1 Právní úprava kybernetické bezpečnosti a její specifika

Oblast kybernetické bezpečnosti je poměrně nové právní odvětví, které však v dnešní společnosti díky rozvoji moderních technologií hraje významnou roli. Jedná se o oblast poměrně širokou. Proto se domnívám, že by nebylo vhodné přistupovat k právní úpravě formou kodexu. Dnešní nastavení kybernetické bezpečnosti v oblasti práva můžeme označit na nastavení spíše rámcové. Velkou roli při tvorbě regulace hrají specializované úřady např. Národní úřad pro kybernetickou bezpečnost – NUKIB.

Problematiku kybernetické bezpečnosti nalezneme zakotvenu jak v mezinárodních, tak vnitrostátních pramenech práva. Z mezinárodních pramenů hraje velmi důležitou roli směrnice NIS, který by měla být od roku 2024 nahrazena směrnicí NIS 2, o tom budu

hovořit v následující kapitole. Ve vnitrostátních pramenech práva zakotvení kybernetické bezpečnosti najdeme v ústavním zákoně č. 110/1998 Sb., který sice v době svého vzniku na kybernetickou bezpečnost jistě nemířil. Naplnění cíle kybernetické bezpečnosti však dle mého názoru naplňuje ustanovení *§ 1 zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot je základní povinností státu.*[155]" V kybernetické bezpečnosti může být objektem zájmu ochrany jak ochrana životů, i když v přenesené formě. Tady například u výše zmiňovaných nemocnic, tak ochrana majetku a majetkových hodnot v případě bank.

Nejdůležitějším a nejobsáhlejším zákonem o kybernetické bezpečnosti je zákon č. 181/2014 Sb., o kybernetické bezpečnosti, mezi jehož cíle patří ochrana existence a funkčnosti prostředí tvořeného informačními systémy a sítěmi i službami elektronických komunikací, a to tak, aby nedocházelo „*k ohrožení práv subjektů na informační sebeurčení, fungování základních společenských funkcionalit chráněných nedistributivními právy České republiky a národní kybernetická infrastruktura nebyla zneužitelná k útokům mimo Českou republiku.*[156]" Je dobré zmínit, že tento zákon v celé šíři prozatím nedopadá na všechny banky na českém trhu, ale pouze na některé z nich. To se v roce 2024 s účinností NIS2 zásadně změní.

Na banky také částečně dopadá zákon č.240/2000 Sb., o krizovém řízení, který definuje prvky kritické infrastruktury státu. Důležité je rovněž nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Toto nařízení určuje kritéria pro určení odvětvových a průřezových kritérií pro určení, zda se jedná nebo nejedná o kritickou infrastrukturu. Z daného nařízení vyplývá, že součástí kritické infrastruktury státu jsou datová centra. Tedy jakési zásobárny informací nejen pro bankovní systémy. V okamžiku, kdy by nebyl funkční datové centrum, mohlo by dojít minimálně k částečnému výpadku bankovních služeb. Zařazení data center pod kritickou infrastrukturu je na místě.

[155] Ústavní zákon č. 110/1998 Sb, ve znění pozdějších předpisů.
[156] Zákon o kybernetické bezpečnosti: Komentář. Praha: Wolters Kluwer, s.5.

Oblasti kybernetické bezpečnosti se věnuje také velké množství podzákonných právních předpisů. Např. vyhláška č.82/2018 Sb., o kybernetické bezpečnosti. Nebo vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích a další.

Mezi důležité prameny práva můžeme zařadit již v práci dříve zmiňovanou vyhlášku č. 163/2014 Sb., která ve své příloze č. 6 bodu 17 povinným osobám stanoví povinnost provést analýzu rizik spjatou s informačními systémy a další povinnosti.

V současné době nebezpečně vzrůstá počet kybernetických útoků v celém světě. NUKIB v listopadu 2022 upozorňoval na zvýšené množství DDoS útoků. V listopadu 2022 ENISA (Agentura Evropské unie pro kybernetickou bezpečnost) upozorňovala na vzrůstající trend kybernetických útoků od Ransomware, přes Malware až po DDOS.[157]

V lednu 2023 NUKIB zveřejnil zprávu o vzrůstající tendenci kybernetických útoků.[158] Vysoký byl především počet DDoS útoků.[159] Kybernetické útoky však nejdou jen DDoS, ale i Phishing, Ransomware a další. Se všemi typy kybernetických útoků se můžeme v praxi setkat. Samozřejmě, že banky i další instituce mají velké množství prostředků nejen k prevenci, detekci, ale i mitigaci rizik. Nicméně riziko nemůže být už ze své podstaty nulové. U kybernetického útoku, když už nastane, tak je třeba co nejefektivněji snížit jeho dopady a také se z rizika poučit a přijmou opatření ke snížení opakování rizika. Budu se zabývat těmi nejpalčivějšími kybernetickými riziky současnosti.

10.1.1 DDoS

DDoS útok neboli Distributed Denial of Service je kybernetický útok, *„mající za cíl omezit nebo vyřadit služby počítačových systémů. Zpravidla se jedná buď o generování velkého množství podvržených požadavků s cílem zahltit systém a/nebo přenosovou cestu nebo jde o sofistikovaný útok na slabá místa v cílovém systému a/nebo přenosové*

[157] Enisa Cyber Security Landscape [online]. 2022 [cit. 05.02.2023]. Dostupné z: https://www.enisa.europa.eu/news/volatile-geopolitics-shake-the-trends-of-the-2022-cybersecurity-threat-landscape.
[158] Kybernetické incidenty pohledem NÚKIB – leden 2023 [online]. 2023 [cit. 05.03.2023]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1934-kyberneticke-incidenty-pohledem-nukib-leden-2023/
[159] Tamtéž.

cestě.[160]*“* V praxi se jedná o případ, kdy útočníci zašlou na internetové stránky poškozeného z několika míst velké množství požadavků s cílem, vyřadit z provozu dané internetové stránky.

Útok patrně typu DDoS proběhl nedávno i na banku ČSOB. Za tímto útokem stála proruská skupina hackerů NoName057.[161] Sama banka uvedla na svých internetových stránkách, že čelí hackerskému útoku, ale, že tento útok nezasáhl interní systémy.[162] U tohoto případu je dobré poukázat na to, že došlo nejen k materializaci kybernetického, ale i geopolitického rizika. Tato skupina útočí převážně na subjekty, kteří podporují v probíhajícím konfliktu Ukrajinu.

10.1.2 Phishing

Phishing je dalším typem kybernetického útoků, který nemíří primárně na instituce, ale na uživatele. Phishingových útoků je v poslední době obrovské množství. Není den, kdy by média o nějakém takovém útoku neinformovala. Co je to phishing? „*Jedná se o techniku sociálního inženýrství, kdy se útočník snaží získat uživatelova důvěrná data nebo spustit do zařízení oběti škodlivý kód*.[163] Phishing má i několik pod typů dle způsobu provedení.

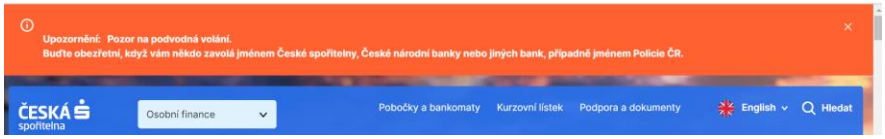
a) **E-mail phishing** v tomto scénáři uživatel nejčastěji obdrží email, kde jsou po něm žádána důvěrná data k platební kartě za nějakým účelem. Tyto typy emailů nebývají adresované. Nejčastěji jsou to podvody typu, k získání velkého dědictví chybí zaplatit daň. Jakmile ji zaplatíte, zpřístupníme vám pohádkové dědictví. Obrana před tímto typem phishingu není složitá. Stačí ostražitost a použití tlačítka spam nebo report phishing v emailu.

[160] Doporučení pro napadení DDOS útokem [online]. [cit. 15.02.2023]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2150-doporuceni-pro-pripad-napadeni-ddos-utokem-jak-se-zachovat-a-jak-postupovat/.
[161] FIŠER, Miloslav. ČSOB ochromili na několik hodin proruští hackeři [online]. [cit. 15.02.2023]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-csob-pod-palbou-hackeru-nektere-sluzby-nefunguji-40424686.
[162] Aktuální výpadek služeb [online]. [cit. 15.02.2023]. Dostupné z: https://www.csob.cz/portal/-/n230303?redirect=%2Fportal%2F.
[163] Phishing [online]. [cit. 15.02.2023]. Dostupné z: https://www.eset.com/cz/phishing/.

b) **Spear phishing** je nebezpečnější druh phishingu, jelikož je adresný.[164] Cílem útočníka je buď vylákat citlivá data uživatele nebo prostřednictvím přílohy nebo odkazu do sítě pustit škodlivý kód. Do kategorie Spear phishingu může zařadit i tzv. CEO fraud. Tedy situaci, kdy zaměstnance obdrží email, který na první pohled vypadá, jako odeslaný nejvyšším manažerem banky. Nejčastěji s prosbou o rychlé zprocesování úhrady faktury. Tento typ útoku je dle mého názoru méně nebezpečný, jelikož mu lze zabránit prevenčním opatřením. Tedy nastavením takových procesů, aby byl tento scénář nenaplnitelný.

c) **Smishing** využívá SMS a MMS zprávy. V tomto případě se útočník obvykle vydává za důvěryhodnou instituci nebo zpráva obsahuje škodlivý kód. Velmi nebezpečný typ smishingu se objevil v České republice v srpnu 2022. Phishingová kampaň cílila na zneužití bankovní identity uživatelů. Jejím cílem bylo získat údaje k bankovní identitě a tím i přístup k bankovním účtům oběti.[165]

d) **Whishing** je velmi nebezpečným druhem phishingu. V tomto scénáři volají útočníci oběti telefonují s tím, že jsou pracovníci banky, na jejich účtu se děje něco nekalého. A jediný způsob, jak peníze zachránit je vybrat je z banky a převést jinam. Což je procesně úplný nesmysl. Banka sama disponuje prostředky ke zmrazení účtu. Těchto útoků v poslední době přibylo. Např. Česká spořitelna má na svých stránkách toto upozornění.[166]



Obrázek 16 - Upozornění na ww.csas.cz

ČSOB reagovala na tyto podvody zavedením speciální telefonní linky, což je velmi dobré řešení, jelikož internetové podvody probíhají velmi rychle a není čas na to, se provolávat hlasovým automatem.

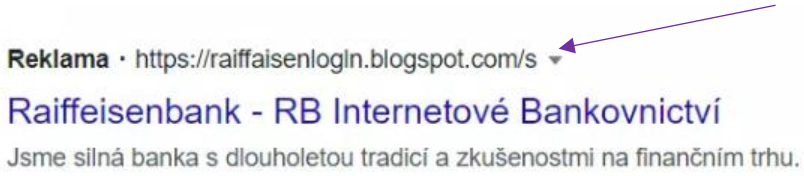
---

[164] Podvodné emaily a zprávy na sociálních sítích na míru spear phishing [online]. [cit. 15.02.2023]. Dostupnéz:https://www.nukib.cz/download/publikace/analyzy/Spearphishing_a_jak_se_pred_nim_chranit.pdf.

[165] Upozorňujeme na phishingovou kampaň s cílem zneužít bankovní identitu [online]. [cit. 15.02.2023]. Dostupné z: https://nukib.cz/cs/infoservis/hrozby/1872-upozornujeme-na-phishingovou-kampan-s-cilem-zneuzit-bankovni-identitu/.

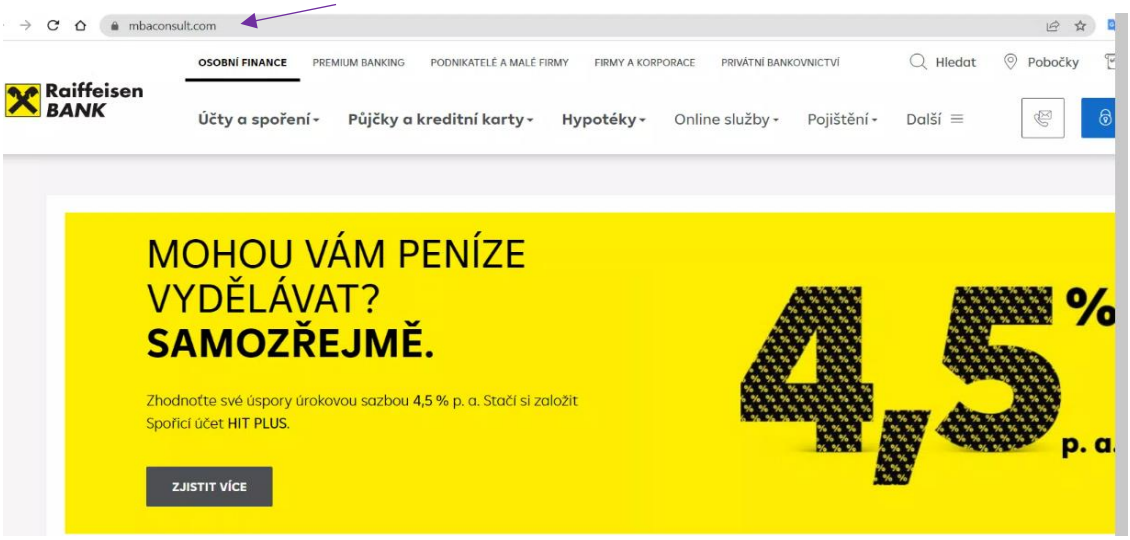
[166]Upozornění [online]. [cit. 15.02.2023]. Dostupné z: https://www.csas.cz/cs/osobni.

e) **<u>Falešné phishingové internetové stránky</u>** jsou také velmi nebezpečným typem phishingu. V srpnu 2022 média informovala o falešných stránkách Raiffeisen bank. V případě, kdy klienti přistupoval k internetovému bankovnictví přes vyhledavač Google, první odkaz, který viděli, byl falešný odkaz na Banku. Podvod bylo možno odhalit v příkazovém řádku. Ostražitost je na místě.[167]



Obrázek 17- Falešný odkaz na bankovní web

V případě, že klient zadal falešné phishingové schránky údaje k bankovnictví, tak útočníci získali všechny potřebné údaje k ovládnutí bankovního účtu. Falešné stránky vypadaly poměrně věrohodně. Podvod bylo možno odhalit opět příkazovém řádku.[168]



Obrázek 18 - Falešný web

10.1.3 Podvodné platební brány

Vyskytují se často u podvodů typu bazar. Postup je většinou následující. Oběť prodává na internetovém bazaru nebo bazarové platformě zboží. Ozve se „kupující“ s tím, že o věc má zájem (velmi často prostřednictvím WhatsApp). Prodávající nabídne, že pošle pro věc kurýra, ale potřebuje od vyplnit údaje k její platební kartě nebo internetovému

[167] Pořízeno print screenem ve vyhledávači Google.
[168] Pořízeno print screenem ve vyhledávači Google.

bankovnictví v zaslaném odkazu. Pokud údaje oběť vyplní velmi často skončí s účtem v lepším případě na nule. V tom horším útočníci stihnou načerpat i předschválené spotřebitelské úvěry.

10.1.4 Ransomware

Ransomware útok je velmi vážným typem útoku. Co se týče jeho mechanismu, jde o škodlivý kód nebo software, který se nějakou dobu v systému nepozorovaně pohybuje. Standartně alespoň několik týdnů. Jeho cílem je znepřístupnit data v systému, a dešifrovací klíč k datům dodat až v okamžiku zaplacení výkupného. Často se škodlivý kód dostane do systému otevřením napadené přílohy emailu nebo otevřením odkazu v emailu.

Jak vyplývá z analýzy NUKIB,[169] pod tímto útokem byly v minulosti dvě nemocnice. Z analýzy rovněž vyplývá, že kybernetické útoky typu Ransomware jsou v cílenější. NUKIB doporučuje zaměřit se na prevenci, což je zcela klíčové. Při dobré segmentaci sítě lze dle mého názoru dopady výrazně snížit. Preventivní opatření lze aplikovat i v oblasti vzdělávání zaměstnanců, tedy provádět pravidelná školení, pravidelné phishingové kampaně, které prověřují ostražitost zaměstnanců a dokážou odhalit případné slabé stránky. Co se týče platby výkupného v případě napadení, tak NUKIB nedoporučuje útočníkům výkupné hradit.[170]

10.1.5 Spyware

Spyware není útok sám o sobě. Ve své podstatě se jedná o druh malwaru, ten se nepozorovaně inkorporuje do operačního systému uživatele a sleduje jeho aktivitu. Shromážděná data jsou následně odesílána třetí straně.[171]

[169] Analýza hrozeb: Útoky jsou stále cílenější [online]. [cit. 02.03.2023]. Dostupné z: https://www.nukib.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf.
[170] Tamtéž.
[171] ENISA Threat Landscape 2022 [online]. 2022 [cit. 02.03.2023]. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

10.2 Opatření před kybernetickými útoky zaměřené na banku

Je na místě poznamenat, že opatření proti kybernetickým rizikům jsou rozmanitá, jako samotné kybernetické útoky. Každá instituce si dle své velikosti a povahy volí vlastní cestu. Obecně lze opatření dělit do tří základních kategorií. Preventivní, detekční a mitigační opatření. Tato opatření lze dle povahy řadit do dalších kategorií.

a) **Bezpečnostní politika** je klíčovou v prevenci, detekci kybernetických útoků. Pro případ kybernetického útoku nebo incidentu je třeba mít srozumitelně a jasně zpracovanou bezpečnostní politiku, která bude součástí interních předpisů. Jedná se o jeden z požadavků vyplývající z vyhlášky č. 163/2014 Sb., která ve svém ustanovení § 10 stanovuje: „*Povinná osoba zajistí, že požadavky stanovené na řídicí a kontrolní systém a jeho součásti a postupy povinné osoby k jejich splnění a při výkonu dalších činností jsou promítnuty do vnitřních předpisů povinné osoby. Povinná osoba stanoví postup při přijímání, změně a uplatňování vnitřních předpisů.“*[172]
b) **Kategorie technické** tedy blokování phishingových stránek a aplikací různými technickými nástroji lze zařadit spíše do opatření preventivních. Automatické filtrování škodlivých emailů slouží k tomu, aby se emaily nedostaly do sféry vlivu uživatele. Dalším velmi užitečným nástrojem je používání automatického správce hesel, segmentace sítě. Další technické nástroje jsou:

- **Firewall pokročilá úroveň** v rámci best practices je třeba také zavádět pokročilé Firewall nástroje. Ty mohou mít jak úroveň preventivní, tak detekční.
- **Antivir a anti-malware řešení** chrání uživatele i firemní síť před viry a škodlivými kódy. Je samozřejmě třeba v rámci řízení rizik nástroje pravidelně aktualizovat. Tyto technické nástroje řadíme do preventivních opatření.
- **Omezení použití externích zařízení** mezí základní preventivní nástroje řadíme omezení nebo zákaz použití technických zařízení ve firemní síti.

[172] § 10 vyhlášky č. 163/2014 Sb.

- **Více faktorové ověřování** je dalším poměrně efektivním prevenčním nástrojem.

c) Kategorie lidských zdrojů

Do této kategorie řadíme primárně kontinuální vzdělávání uživatelů a dalších osob tak, aby byly schopni detekovat potenciální útok. Mezi velmi efektivní edukační nástroje můžeme zařadit např. provádění pravidelných phishingových kampaní. Toto opatření můžeme označit za preventivní i detekční. V závislosti na pracovním zařazení školeného zaměstnance.

10.3 Opatření před kybernetickými riziky zaměřené na klienty

Česká bankovní asociace, (dále jen ČBA) spustila před nedávnem kampaň s názvem „nePINdej!“ Cílem kampaně je seznámení klientů bank s možnými riziky, se kterými se mohou běžně setkat na internetu. Součástí kampaně je i desatero bezpečnosti na internetu a kybernetický test, ve kterém si uživatel může otestovat své znalosti. Sama ČBA uvádí, že průměrná zcizená částka z kybernetického útoku je 165 000 Kč.[173]

Banky klienty kontinuálně vzdělávají v oblasti kybernetických rizik. Velmi často vkládají do svých mobilních aplikací informace o probíhajících útocích. Před potvrzením transakce klient vidí varovná upozornění atd. Jak z banky edukují své klienty? Při porovnání vycházím z veřejně přístupných zdrojů.

a) ČSAS varuje před podvody hned na úvodní stránce. Při rozkliknutí volby bezpečnost dat klient uvidí vysvětleny srozumitelně vysvětleny hrozby typu vishing, vzdálený přístup do počítače, bazarové podvody, Ransomware, CEO fraud a další.[174] ČSAS pro své klienty také vydefinovala bezpečnostní desatero, aneb jak se chovat, aby klient snížil riziko kybernetického útoku na minimum.[175]

[173] Kyber test [online]. [cit. 01.03.2023]. Dostupné z: https://www.kybertest.cz/.
[174] Bezpečnost a ochrana dat [online]. [cit. 01.03.2023]. Dostupné z https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat.
[175] Bezpečnostní desatero[online]. [cit. 01.03.2023] https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bezpecnostni-desatero-obecna-pravidla.

b) ČSOB na úvodní stránce varování před podvody na rozdíl od ČSAS nemá. Varování před podvody však na stránkách nalezneme také, pod záložkou zásady bezpečného chování.[176] Koncept edukace klientů je trochu jiný, bezpečnostní desatero o ČSOB cílí na bezpečné používání platebních karet.[177]

c) KB má na úvodní stránce v záložce bezpečnost umístěno varování před útoky kybernetického rázu.[178] Bezpečnostní desatero na internetových stránkách nalezneme také. Líbí se mi poznámka u bezpečnostního desatera *„nestačí si je přečíst, musíte je mít pod kůží.“*[179]

d) Unicredit bank Pravidla bezpečného chování na internetu nalezneme hned na úvodní stránce. Což je velmi praktické. Desatero obsahuje stejně jako desatera předchozích konkurentů 10 bodů pro klienta, co dělat, aby měl své údaje v bezpečí.

e) Raiffeisen bank u RB na úvodní obrazovce není hned vidět upozornění na bezpečnostní hrozby. Při použití lupy a zadání klíčových slov se k zásadám bezpečnostního bankovnictví dostaneme bez potíží. V bezpečnostních zásadách a pokynech pro RB kladně hodnotím detail zpracování. Na stránkách je velmi srozumitelně vysvětleno, co konkrétně si má klient, u kterého rizika hlídat.

Všechny banky mají materiály pro klienty zpracovány v podobném duchu. Vyzdvihla bych jednu věc. Bezpečnost a bezpečnostní pravidla je třeba mít naprosto zautomatizované. Tím se výrazně snižuje riziko, že se staneme obětí podvodníků. Ti jsou totiž vždy o krok před námi.

[176] Zásady bezpečného chování: Buďte chytřejší, než útočníci [online]. [cit. 02.03.2023]. Dostupné z: https://www.csob.cz/portal/bezpecnost/zasady-bezpecneho-chovani.

[177] Nejčastější dotazy: Platební karty, karty na internetu [online]. [cit. 03.03.2023]. Dostupné z: //www.csob.cz/portal/documents/10710/19255958/nejcastejsi-dotazy-platebni-karty.pdf.

[178] Bezpečnost aktuální hrozby [online]. [cit. 02.03.2023]. Dostupné z: https://www.kb.cz/cs/bezpecnost/aktualni-hrozby.

[179] Bezpečnostní desatero [online]. [cit. 02.03.2023]. Dostupné z: https://www.kb.cz/cs/bezpecnost/desatero.

11 Výhled do budoucna v oblasti řízení rizik

V oblasti řízení rizik nás čeká řada změn. Nejvýznamnější ze změn, která čeká nejen banky je DORA a s ním související nařízení NIS 2. Obě tato nařízení budou mít zásadní dopad do řízení rizik. Zejména rizik informačních a komunikačních technologií. Řízení rizik informačních a komunikačních technologií nabývá na významu i vzhledem ke geopolitickému riziku současnosti.

Oblast informačních a komunikačních technologií (dále jen IKT) se významnou do oblasti řízení rizik promítá a promítat bude, vzhledem ke stále se zvyšujícímu podílu digitalizace v bankovním světě.

Dalším důležitým a významným tématem je Basel IV, o kterém jsem se zmiňovala v kapitole třetí.

11.1 Nařízení DORA

Nařízení DORA (Digital Operational Resilience Act) je součástí sady právních předpisů z oblasti digitálních financí. DORA vychází ze směrnice NIS, přičemž platí, že NIS je lex generalis a DORA lex specialis.[180]

DORA Byla publikována 27. 12. 2022 s platností od 17. 02. 2023 a účinností od 16.01.2025. Implementační lhůta je dvouletá. Což se na první pohled může zdát jako poměrně dlouhá implementační lhůta. Vzhledem ke změnám, které přináší hodnotím implementační lhůtu jako krátkou.

Nařízení DORA se do jisté míry inspiruje již existujícími normami jako např. ISO/IEC 27000, které jsou ve světě kybernetické bezpečnosti již best practices.

Nařízení DORA v důvodové zprávě odkazuje na BASEL II a BASEL III, přičemž akcentuje, že v rámci BASEL dohod nebyla rizikům vyplývajícím z informačních a komunikačních technologií věnována patřičná pozornosti. Svět IKT se však mění tak

[180] Ius Focus: Právní úprava digitální provozní odolnosti finančního sektoru přijata v prvním čtení [online]. C.H.Beck, 2022 [cit. 13.03.2023]. Dostupné z: https://www.beck-online.cz/bo/chapterviewdocument.seam?documentId=nrptembsgjpwszs7gqyti&groupIndex=1&rowIndex=0&refSource=search.

rychle, že v daném čase nebylo možno dnešním rizikům, které v té době ani neexistovaly věnovat pozornost.

Co se týče cílů DORA, ty jsou stanoveny v důvodové zprávě takto:

- „*Harmonizace pravidel pro řízení v oblasti informačních a komunikačních technologií.*
- *Harmonizace hlášení incidentů v oblasti informačních a komunikačních technologií.*
- *Účelem právní úpravy je podpora rozvoje potenciálu se současným ošetřením rizik plynoucích z informačních a komunikačních technologií.*“[181]

11.1.1 Působnost DORA

Působnost je zakotvena v článku 2, který je poměrně obsáhlý. Pro účely této práce uvedu ty nejvýznamnější subjekty.

- Banky, spořitelní a úvěrní družstva.
- Pojišťovny a zajišťovny. Pro ty bude toto nařízení velkou novinkou.
- Obchodníky s cennými papíry.
- Zprostředkovatele pojištění a zajištění.
- Centrální depozitáře.
- Crowfundongové platformy atd.[182]

Oblasti řízení a organizace se věnuje čl. 5, který v bodu 1 uvádí: „*Finanční subjekty musí mít solidní, ucelený a dobře zdokumentovaný rámec pro řízení rizik v oblasti IKT, který jim umožní řešit tato rizika rychle, účinně a komplexně a zajistit vysokou míru digitální provozní odolnosti odpovídající potřebám jejich provozu, jejich velikosti a složitosti jejich struktury.“*[183] Na tento článek navazuje bod 7 DORA, který stanoví, *že Rámec pro řízení rizik v oblasti IKT uvedený v odstavci 1 podléhá pravidelnému auditu auditory IKT s dostatečnými znalostmi, dovednostmi a odbornými zkušenostmi v oblasti*

[181] Nařízení Evropského parlamentu a Rady: Důvodová zpráva DORA [online]. [cit. 23.03.2023] Dostupné z https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020PC0595.
[182] Článek 2 DORA.
[183] Článek 5 bod 1 DORA.

rizik IKT. Četnost a zaměření auditů IKT odpovídají rizikům finančního subjektu v oblasti IKT.[184] Dle článku 5 musí být rámec řízení rizik:

- Solidní, ucelený a dobře zdokumentovaný. Což oproti stávajícímu stavu změna není.
- Rámec řízení rizik musí obsahovat strategie pro oblast IKT
- Zavedení pravidelných školení také není žádnou novinkou.
- Zavedení komunikačního kanálu o jakémkoliv outsourcingu už ale novinkou je. Co si pod tímto pojmem představit je otázkou.

11.1.2 Změny s nařízením DORA

Při pohledu do článku 6 je jasné, že strategie pro řízení rizik bude muset ve společnostech doznat podstatných změn. Co bude třeba ve strategiích definovat?

- Jakým způsobem bude docházet k ochraně hardware, software a know-how. Částečně je to definováno již dnes. DORA však vyžaduje větší detail.
- Strategie řízení IKT rizik podléhá jak internímu auditu. Což rovněž není novinka. Jde opět o míru detailu.

Článek 14 dává tušit, že krizové komunikační plány budou muset být zpřesněny. Komunikační matice při hlášení incidentů bude muset být jasnější a povinnost hlásit incidenty se dotkne širšího okruhu lidí.

Co se týče principu proporcionality, ten je v DORA zakotven v článku 16. Měl by se uplatnit i v těchto okruzích:

- V rámci řízení rizik. Fakticky platí i dnes.
- V oblasti rychlé identifikaci a detekci zdrojů rizika. Z pohledu rizik IKT toto ustanovení dává smysl. Nicméně detekce v případě IKT může být poměrně složitý např. u případu Ransomware.
- Princip proporcionality by se měl uplatnit i u pravidelného testování a přijetí závěrů z testování. Otázka je, jak si princip proporcionality vyložit například u problematiky testování penetračních testů.

[184] Článek 5 bod 7 DORA.

Změny v otázce hlášení incidentů. Hlášení incidentů IKT se změní velmi významně. V čl. 17 DORA je zakotvena povinnost zavést a uplatňovat proces řízení incidentů. Tento proces musí obligatorně zahrnovat detekci, řízení a hlášení incidentů. Lhůty jsou výrazně kratší a proces vyžadován významně detailnější. Proces musí obsahovat:

- Jasné plány komunikace, včetně komunikační matice.
- Jasné rozdělení kompetencí a úloh.
- Postupy ke snížení/zmírnění dopadů.
- Ukazatele včasného varování.
- Postupy vedoucí k identifikaci, evidenci, sledování, klasifikaci a kategorizaci incidentů.

Oblast IKT bude mít fakticky řekněme vlastní sběr událostí plynoucích z rizik IKT. Proces řízení incidentů v DORA je něco významně jiného než dnes.

Významné změny se dotknou také oblasti outsourcingu. Což bude mít významný dopad do řízení operačních rizik.

Ještě jedna věc je z pohledu řízení rizik velmi důležitá. Je třeba tedy brát DORU na zřetel již dnes. Pravidla DORA se totiž nebudou vztahovat pouze na nově uzavírané kontrakty, ale i na ty stávající. Proto je třeba typicky například u outsourcingu požadavky z DORA do smluvního vztahu vhodné zakotvit již dnes.

11.1.3 Následné kroky

Již dnes víme, že implementační lhůta pro DORU je dvouletá. Bylo by tedy dobré vědět, co které organizaci DORA přinese. Co všechno se bude muset změnit. Vhodným nástrojem pro zjištění se jeví rozdílová analýza. Tedy porovnáním současného stavu se stavem žádoucím, tedy v souladu s DORA. Závěry z rozdílové analýzy je třeba následně implementovat do bankovních procesů.

Závěr diplomové práce

Bankovní svět se mění a rozvíjí velmi rychle. S dynamikou bankovního prostředí se stejně rychle mění i operační rizika, která je třeba řídit. Přičemž řízením se rozumí celý proces od identifikace, kvantifikace, mitigační opatření, korekční opatření a další.

Je třeba držet krok s dobou, konkurencí a současně být v souladu se zpřísňující se regulací. Dále jednat jako řádný hospodář, hájit investice, zájmy akcionářů a depozita klientů.

V horizontu dvou let banky a finanční instituce čeká implementace NIS 2 a DORA. Bude se jednat o náročné projekty, který by měly být v bankách koordinovány ideálně z jednoho místa. Rozdílová analýza bude nutností. Dá se očekávat, že implementace bude finančně i časově velmi náročná. Rizika IKT však podceňovat, jelikož jsou a pravděpodobně budou na vzestupu i nadále. Útočníci jsou bohužel vždy o krok před bankami a klienty.

Regulatorní změny nepřijdou jen s výše jmenovanou regulací. Přípravy bude třeba zahájit i na regulatorní změny, které přinese Basel IV. Bankovní sektor tedy čekají velmi zajímavé a snad i trochu zábavné okamžiky u implementace nové regulace.

Co si banky budou muset do budoucna zcela jistě posoudit, pokud tak již neudělaly, je pojištění kybernetických rizik Cyber. Do budoucna si troufám říct, pojištění bude standardem na trhu. Domnívám se, že bude platit, že pojištění bude drahá a těžko sjednatelné.

Je na samotných bankách, jak efektivně vypořádají s materializací operačních rizik.

Resumé

The focus of this thesis is Operational Risk Framework in banking sector. Tho goal is to explain basically what the Operational Risk Framework is.

For the beginning is explained the role of Czech National Bank and supervision of Czech National Bank.

Important is as well the role of BCBS which is significant related the Operational Risk history, definition, categorisation, basic division.

The goal of Operational Risk Framework is to find a balance of risk and reward. It is possible with four steps which are described od this thesis.

Operational Risk significant event are described as an example of materialization of Operational Risk.

Last part is about cyber risk and DORA regulation which is coming to the bank sector in the European Union.

Seznam použité literatury

A. Komentáře

1. RÝDL, Tomáš a Josef BARÁK. Zákon o České národní bance: komentář. 1. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-622-8.344 s.
2. RYCHETSKÝ, P., LANGÁŠEK, T., HERC T., MLSNA, P. a kol. Ústava České republiky. Ústavní zákon o bezpečnosti České republiky. Komentář. Praha: Wolters Kluwer, a.s., 2015. ISBN 978-80-7478-809-3. 1224 s.
3. SMUTNÝ, Aleš. Zákon o bankách: komentář. 2. vydání. V Praze: C.H. Beck, 2019. Beckovy komentáře. ISBN 978-80-7400-764-4. 888 s.
4. Zákon o kybernetické bezpečnosti: Komentář. Praha: Wolters Kluwer. 1. Praha: Aspi, 2015. ISBN 978-80-7478-818-5. 232 s.

B. Monografie

1. BAKEŠ, Milan. Finanční právo. 6., upr. vyd. V Praze: C.H. Beck, 2012. Beckovy právnické učebnice. ISBN 978-80-7400-440-7. 549 s.
2. HENDRYCH, Dušan. Právnický slovník. 3., podstatně rozš. vyd. V Praze: C.H. Beck, 2009. Beckovy odborné slovníky. ISBN 978-80-7400-059-1.1488 s.
3. DUCHÁČKOVÁ, Eva. Principy pojištění a pojišťovnictví. 3., aktualiz. vyd. Praha: Ekopress, c2009. ISBN 978-80-86929-51-4. 224 s.
4. JENÍK, Ivo. Dohled a regulace finančního trhu. Praha: Spolek českých právníků Všehrd, 2011. 1. ISBN 978-80-85305-48-7. 120 s.
5. KAŠPAROVSKÁ, VLASTA. Řízení obchodních bank. Praha: C. H. Beck, 2006. ISBN 80-7179-381-7 339 s.
6. PETRJÁNOŠOVÁ, Božena Bankovní management. 1. vyd. Brno: Masarykova univerzita. 2004. 132 s. ISBN 80-210-3481-5.
7. REVENDA, Zbyněk. Peněžní ekonomie a bankovnictví. 5., aktualizované vydání Praha: Management Press, 2015. ISBN 978-80-7261-279-6. 417 s.
8. CHAPELLE, Ariane. Operational risk management: best practices in the financial services industry. Hoboken: Wiley, 2018. ISBN 978-1-119-54904-8. 272 s.

9. BASEL COMMITTEE ON BANKING SUPERVISION. Basel III: A global regulatory framework for more resilient banks and banking system, Basel, Bank for International Settlements, 2010, 77 s. ISBN 92-9131-859-0.
10. NIESEL, Martin a Stefan ROTH. Basel IV. 2. Weinhelm: Vilely, 2018. ISBN 978-3-527-50962-1,499 s.
11. ŠENKÝŘOVÁ, Bohuslava. Bankovnictví. Praha: Vysoká škola finanční a správní, 2010. Eupress. ISBN 978-80-7408-029-6.253 s
12. ZRŮST, Lukáš. Selhání subjektů finančního trhu. Praha: Wolters Kluwer ČR, 2019. 244 s.

C. Odborné články

1. BARÁK, Josef. Česká národní banka jako orgán dohledu nad finančním trhem. Právní rozhledy. C.H.Beck, 2006, str. 1-3.
2. VOSTRÁ, Zuzana. Ústavní zakotvení České národní banky a bankovní unie. Právněhistorické studie [online]. 2017, vol. 47, no. 2. [cit. 26.11.2022]. ISSN2464689X.Dostupnéz:https://karolinum.cz/data/clanek/5205/PHS_47_2_0129.pdf.
3. MAZÁNKOVÁ, Věra a Michal NĚMEC. Operační riziko a jeho dopady do finanční stability [online]. 111[cit.10.02.2023].Dostupnéz:https://www.cnb.cz/export/sites/cnb/cs/financnistabilita/.galleries/zpravy_fs/fs_2007/FS_2007_clanek_4.pdf..
4. KAHÁNEK, Adam. Klienti ruské Sberbank CZ zahltili pobočky. Ty nakonec zavřely [online]. [cit. 05.02.2023]. Dostupné z: https://www.novinky.cz/clanek/ekonomika-klienti-ruske-sberbank-zahltili-pobocky-ty-nakonec-zavrely-40388375.
5. WEINBENDER, Kristina. Zvažujeme akvizice menších bank, říká nová šéfka české Sberbank [online]. [cit. 05.02.2023]. Dostupné z: https://www.e15.cz/byznys/finance-a-bankovnictvi/zvazujeme-akvizice-mensich-bank-rika-nova-sefka-ceske-sberbank-1387520
6. Ius Focus: Právní úprava digitální provozní odolnosti finančního sektoru přijata v prvním čtení [online]. C.H.Beck, 2022 [cit. 13.03.2023]. Dostupné z:https://www.beconline.cz/bo/chapterviewdocument.seam?documentId=nrptembsgjpwszs7gqyti&groupIndex=1&rowIndex=0&refSource=search.

D. Judikatura

1. Nález č. 278/2001 Sb., nález Ústavního soudu ze dne 20. června 2001 ve věci návrhu na zrušení části zákona č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů Ústavní zákon č. 1/1993 Sb., Ústava České republiky, čl. 98 odst. 1,2.

E. Příkazy, rozhodnutí, usnesení

1. Příkaz ČNB: Sp/2022/100/573 [online]. [cit. 23.03.2023]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohled-financni-trh/.galleries/prilohy/S-Sp-2022_00100_CNB_573.pdf.
2. Usnesení Městského soudu v Praze č.j. 83Cm 810/2022-7 Praha, 2022 [cit. 05.02.2023]. Dostupné z: https://www.cak.cz/assets/rozhodnuti-o-likvidaci-sberbank.pdf.
3. Rozhodnutí České národní banky č.j. 2022/85885/570 ze dne 29. srpna 2022, sp.zn. Sp/2019/596/573. https://www.cnb.cz/export/sites/cnb/cs/dohled-financni-trh/.galleries/prilohy/S-Sp2019_00596_CNB_573.pdf.

F. Ústavní zákony a zákony

1. Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů
2. Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky.
3. Zákon č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů.
4. Zákon č. 21/1992 Sb., zákon o bankách, ve znění pozdějších předpisů.
5. Zákon č. 255/2012 Sb., kontrolní řád, ve znění pozdějších předpisů.
6. Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
7. Zákon č. 181/2014 Sb., o kybernetické bezpečnost
8. Zákon č. 240/2000 Sb., o krizovém řízení, ve znění pozdějších předpisů.

G. Podzákonné právní předpisy

1. Vyhláška č. 163/2014 o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry.
2. Opatření obecné povahy ze dne 25.11.2021, ke stanovení horní hranice úvěrových ukazatelů č. I/2021.

3. Opatření Státní banky československé, kterým se stanoví minimální výše likvidních prostředků č. 97/1992/03 Sb.
4. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

H. Legislativa EU

1. Nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012.
2. Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES.
3. Nařízení Evropského parlamentu a Rady: Důvodová zpráva DORA [online]. [cit. 23.03.2023] Dostupné z https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020PC0595.
4. Digital Operational Resilience Act, Nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru 2022/2554 ze dne 14. prosince 2022.

I. Internetové zdroje

1. Run (útok na banku) *Run* [online]. [cit. 07.01.2023]. Dostupné z: https://cbaonline.cz/run-utok-na-banku.
2. A new Capital Adequancy Framework: Consultative paper issued by the Basel Committee on Banking Supervision [online]. Basel, 1999 [cit. 16.03.2023]. Dostupné z: https://www.bis.org/publ/bcbs50.pdf.
3. Amendment to the Capital Accord to incorporate market risks [online]. Str. 7Dostupné z: https://www.bis.org/publ/bcbs119.pdf.
4. *Banking package* [online]. European Comission: Bank for International Settlements, 2021 [cit. 01.01.2023]. Dostupné z: https://finance.ec.europa.eu/publications/banking-package_en.
5. Bankovní regulace [online]. [cit. 10.2.2023]. Dostupné z: cbaonline.cz/bankovni-regulace.

6. Basel Comitee of Banking Supervision: International Governance of Capital Measurment and Capital Standarts [online]. Basel, 1988 [cit. 05.01.2023]. Dostupné z: https://www.bis.org/publ/bcbs04a.pdf.
7. Basel III: A global regulatory framework for more resilient banks and banking systems [online]. Basel: Bank for International Settlements [cit. 01.01.2023]. Dostupné z: https://www.bis.org/publ/bcbs189.pdf.
8. Basel III: Finalising post-crisis reforms [online]. Basel: Bank for International Settlements, 2017 [cit. 01.01.2023]. Dostupné z: https://www.bis.org/bcbs/publ/d424.pdf.
9. *Credit Suisse: Annual Report 2022* [online]. Switzerland [cit. 20.02.2023]Dostupné z: https://www.credit-suisse.com/about-us/en/reports-research/annual-reports.html?aa=rl-onsite-search%2065
10. ČNB. Tisková zpráva: ČNB odebrala licenci Sberbank [online]. Praha, 2022 [cit. 05.02.2023]. Dostupné z: https://www.cnb.cz/cs/cnb-news/tiskove-zpravy/CNB-odebrala-licenci-Sberbank-CZ/.
11. ČNB. Tisková zpráva: ČNB zahájila kroky k odejmutí licence Sberbank CZ [online]. Praha, 2022 [cit. 05.02.2023]. Dostupné z: https://www.cnb.cz/cs/cnb-news/tiskove-zpravy/CNB-zahajila-kroky-k-odejmuti-licence-Sberbank-CZ/.
12. Demand Side of Cyber Insurance in the EU: Analysis of Challenges and Perspectives of OESs [online]. 1. European Union Agency for Cybersecurity (ENISA), 2023: European Union Agency for Cybersecurity (ENISA), 2023, 2023 [cit. 04.03.2023]. ISBN 978-92-9204-586-9. Dostupné z: https://www.enisa.europa.eu/publications/demand-side-of-cyber-insurance-in-the-eu.
13. *Doporučení pro napadení DDOS útokem* [online]. [cit. 2023-03-25]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2150-doporuceni-pro-pripad-napadeni-ddos-utokem-jak-se-zachovat-a-jak-postupovat
14. Dohledové a zátěžové testy [online]. [cit. 10.02.2023]. Dostupné z:https://www.cnb.cz/cs/financni-stabilita/zatezove-testy/dohledove-zatezove-testy/index.html.

15. Dohledové zátěžové testy vybraných bank 2021 [online]. Česká národní banka [cit.10.02.2023].Dostupnéz:https://www.cnb.cz/export/sites/cnb/cs/financnistabilita/.galleries/zatezove_testy/2021/zatezove_testy_banky_2021_10.pdf.
16. Dlouhodobá koncepce České národní banky [online]. Česká národní banka, 2017[cit.10.02.2023].Dostupnéz:https://www.cnb.cz/export/sites/cnb/cs/dohledfinancnitrh/.galleries/dlohodoba_koncepce_dohledu/dlohodoba_koncepce_dohledu.pdf.
17. Enisa Cyber Security Landscape [online]. 2022 [cit. 25.03.2023]. Dostupné z: https://www.enisa.europa.eu/news/volatile-geopolitics-shake-the-trends-of-the-2022-cybersecurity-threat-landscape.
18. 2023 EU-Wide Stress Test: Methodological Note [online]. EBA European Banking Authority, 2023 [cit.10.03.|2023]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/document_library/Risk%20Analysis%20and%20Data/EUwide%20Stress%20Testing/2023/Scenarios/1051436/2023%20EUwide%20stress%20test%20%20Methodological%20Note.pdf.
19. Fact box Credit Suisse's scandals - spies, lies and money laundering [online]. Reuters, 2022 [cit. 01.03.2023]. Dostupné z: https://www.reuters.com/business/finance/spies-lies-chairmans-exit-credit-suisses-scandals-2022-0.
20. Final Report: Guidelines for institutions and resolution authorities to complement the resolvability assessment for transfer strategies (Transferability guidelines) [online]. European Banking Authority, 2022 [cit. 10.02.2023]. Dostupnéz:https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2022/EBAGL202211%20GL%20on%20transferability/1039809/Final%20report%20on%20Guidelines%20on%20transferability.pdf.
21. Finalising Basel III standart adoptation [online]. Basel: Bank for International Settlements,2017[cit.01.01.2023].Dostupnéz:https://www.bis.org/bcbs/implementation/rcap_reports.htm?m=3059.
22. Finalising Basel III In brief [online]. Basel: Bank for International Settlements, 2017[cit.01.01.2023.Dostupnéz:https://www.bis.org/bcbs/publ/d424_inbrief.pdf.

23. International Convergence of Capital Measurement and Capital Standards: Revised Framework [online]. Basel: 2004 [cit. 02.03.2023]. Dostupné z: https://www.bis.org/publ/bcbs107.pdf.
24. Finanční stabilita: Finanční stabilita. Česká národní banka [online]. [cit.04.12.2022]. Dostupné z: https://www.cnb.cz/cs/financni-stabilita/.
25. FIŠER, Miloslav. *ČSOB ochromili na několik hodin proruští hackeři* [online]. [cit. 2023-03-25]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-csob-pod-palbou-hackeru-nektere-sluzby-nefunguji-40424686.
26. Guidelines compliance table: Guidelines on the revised common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing [online]. European Banking Authority, 2021 [cit. 20.02.2023].Dostupnéz:https://www.eba.europa.eu/sites/default/documents/files/document_library/963608/Compliance_EBA_GL_2018_03.pdf.
27. *History of the Basel Committee: At a glance* [online]. [cit. 01.01.2023]. Dostupné z: https://www.bis.org/bcbs/history.htm.
28. Charter (Statut Basilejského výboru): [online] June 2018, Bank for international settlement [cit. 25.02.2023] dostupné na https://www.bis.org/bcbs/charter.htm.
29. International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version [online]. Basel, 2006 [cit. 02.01.2023]. Dostupné z: https://www.bis.org/publ/bcbs128.pdf.
30. Inflační cíl: Inflační cíl. Česká národní banka [online]. [cit. 04.12.2022]. Dostupné z: https://www.cnb.cz/cs/menova-politika/inflacni-cil/.
31. Media Release: Credit Suisse makes strong progress on Group strategic priorities; reports net revenues of CHF 3.1 bn and pre-tax loss of CHF 1.3 bn along with a CET1 ratio of 14.1 % in 4Q22 [online]. Zurich, 2023 [cit. 2023-03-20]. Dostupné z:https://www.creditsuisse.com/media/assets/corporate/docs/aboutus/media/media-release/2023/02/q4-22-press-release-en.pdf.
32. Měnová politika: Měnová politika: Česká národní banka [online]. [cit 04.12.2022]. Dostupné z: https://www.cnb.cz/cs/menova-politika/.
33. *Kybernetické incidenty pohledem NÚKIB – leden 2023* [online]. 2023 [cit. 05.03.2023]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1934-kyberneticke-incidenty-pohledem-nukib-leden-2023/

34. Operational Loss Events Internal and External Data: Operational Risk Sound Practice Guidance. The Institute of Operational Risk, str. 15.[online]. SWORD: The Institute of Operational Risk, 2019 [cit. 12.03.2023]. Dostupné z: https://www.ior-institute.org/sound-practice-guidance/operational-loss-events/.
35. Povinně uveřejňovaná informace: Zveřejnění vnitřní informace [online]. 2022 [cit. 2023-03-15]. Dostupné z: https://investors.moneta.cz/documents/12270853/20115959/mmb-srep-pozadavek-2023-cz.pdf.
36. Principles for the Sound Management of Operational Risk [online]. 2022, Bank for International Settlement [cit. 10.03.2023]. Dostupné z: https://www.bis.org/publ/bcbs195.pdf.
37. Prognóza ČNB zima 2023. Česká národní banka [online]. [cit. 02.02.2023]. Dostupné z: https://www.cnb.cz/cs/menova-politika/prognoza/.
38. Rapport sur la stabilité financière [online]. Banque Nationale Suisse, 2022 [cit. 10.02.2023]. Str 19 Dostupné z: https://www.snb.ch/fr/mmr/reference/stabrep_2022/source/stabrep_2022.fr.pdf
39. Risk and Control Self Assessment: Operational Risk Sound Practice Guidance [online]. The Institute of Operational Risk, 2021, ,23 [cit.01.03.2023]. Dostupné z: https://www.ior-institute.org/sound-practice-guidance/risk-and-control-self-assessment/.
40. Run (útok na banku).: Run [online]. [cit. 07.01.2023]. Dostupné z: https://cbaonline.cz/run-utok-na-banku.
41. Recommendation European Systematic Risk Board: on restriction of distributions during the COVID-19 pandemic [online]. Dostupné z: https://www.esrb.europa.eu/pub/pdf/recommendations/esrb.recommendation200608_on_restriction_of_distributions_during_the_COVID19_pandemic_2~f4cdad4ec1.en.pdf.
42. Sdělení ČNB o obecných pokynech EBA ke společným postupům a metodikám procesu přezkumu a vyhodnocení (SREP) [online]. [cit. 20.02.2023]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/obecne-pokyny-evropskych-organu-dohledu/Sdeleni-CNB-o-obecnych-pokynech-EBA-ke-spolecnym-postupum-a-metodikam-procesu-prezkumu-a-vyhodnoceni-SREP//.

43. SNB and FINMA issue statement on market uncertainty. [cit. 25.03.2023]. Dostupnéz:https://www.snb.ch/en/mmr/reference/pre_20230315/source/pre_20230315.en.pdf.
44. Výroční zpráva Česká spořitelna [online]. 2022, Praha [cit. 05.02.2023]. Str. 53. Dostupnéz:https://www.csas.cz/static_internet/cs/Redakce/Ostatni/Ostatni_IE/Prilohy/vz-2021.pdf.
45. Výroční zpráva ČSOB [online]. 2022, Praha [cit. 05.02.2023].Str. 180. Dostupné z https://www.csob.cz/portal/documents/10710/444804/vz-csob-2021.pdf.
46. Výroční zpráva Komerční banka [online]. 2022, Praha [cit. 05.02.2023]. Str. 70. Dostupné z: https://www.kb.cz/getmedia/9aafd6ac-7be2-4808-9060-2feae98f9cd0/Vyrocni-zprava-KB-2021_1.pdf.aspx.
47. Výroční zpráva Moneta Money bank [online]. 2022, Praha [cit. 05.02.2023]. Str. 116. Dostupné z: https://investors.moneta.cz/documents/12270853/20117788/mmb-vyrocni-zprava-2021-cz.pdf.
48. Výroční zpráva Unicredit bank [online]. 2022, Praha [cit. 05.02.2023]. Str. 113. Dostupné z: https://www.unicreditbank.cz/content/dam/cee2020-pws-cz/cz-dokumenty/o-bance/vyrocni-zpravy/VZ_2021_CZ_final.pdf.
49. Výroční zpráva Raiffeisen bank [online]. 2022, Praha [cit. 05.02.2023]. Str. 134. https://www.rb.cz/attachments/zpravy/Raiffeisenbank_a_s_Konsolidovana_vyrocni_zprava_2021_CZ.pdf.
50. Výroční zpráva Sberbank [online]. 2022, Praha [cit. 05.02.2023]. Str. 12. Dostupné z:https://www.sberbank.cz/media/files/povinneinformace/vyrocnizpravy/Vyrocni_zprava_2021_CZ.pdf.
51. Zpráva o dohledu nad finančním trhem [online]. 2021. Česká národní banka, 2022 [cit. 15.03.2023]. ISBN 978-80-88424-09-3. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohledfinancnitrh/.galleries/souhrnne_informace_fin_trhy/zpravy_o_vykonu_dohledu/download/dnft_2021_cz.pdf.
52. Podvodné emaily a zprávy na sociálních sítích na míru spear phishing [online]. [cit. 15.02.2023]. Dostupné z: https://www.nukib.cz/download/publikace/analyzy/Spearphishing_a_jak_se_pred_nim_chranit.pdf.

53. Upozorňujeme na phishingovou kampaň s cílem zneužít bankovní identitu [online]. [cit. 15.02.2023]. Dostupné z: https://nukib.cz/cs/infoservis/hrozby/1872-upozornujeme-na-phishingovou-kampan-s-cilem-zneuzit-bankovni-identitu/.
54. Upozornění [online]. [cit. 15.02.2023]. Dostupné z: https://www.csas.cz/cs/osobni
55. Enhancements to the Basel II framework [online]. Bank for international Settlement [cit. 05.02.2023]. Dostupné z: https://www.bis.org/publ/bcbs157.pdf
56. Reputational Risk [online]. [cit. 05.02.2023]. Dostupné z: https://managementmania.com/cs/reputacni-riziko-reputational-risk.

Seznam obrázků tabulek a grafů

A. Seznam obrázků