VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

INSTITUTE OF FORENSIC ENGINEERING

ODBOR INŽENÝRSTVÍ RIZIK

DEPARTMENT OF RISK ENGINEERING

ŘÍZENÍ OPERAČNÍCH RIZIK V BANKOVNICTVÍ

MANAGEMENT OF OPERATIONAL RISKS IN BANKING

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Tereza Fraitová

VEDOUCÍ PRÁCE
SUPERVISOR

doc. Ing. Radek Doskočil, Ph.D., MSc

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

Zadání diplomové práce

Studentka:	**Bc. Tereza Fraitová**
Studijní program:	Řízení rizik technických a ekonomických systémů
Studijní obor:	Řízení rizik ekonomických systémů
Vedoucí práce:	**doc. Ing. Radek Doskočil, Ph.D., MSc**
Akademický rok:	2023/24
Ústav/odbor:	Odbor inženýrství rizik

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Řízení operačních rizik v bankovnictví

Stručná charakteristika problematiky úkolu:

Na základě zpracované literární rešerše a provedené analýzy identifikovat, analyzovat a vyhodnotit operační rizika ve zvolené bankovní instituci s využitím vhodných metod analýzy rizik a navrhnout opatření směřující k minimalizaci těchto rizik.

Cíle diplomové práce:

Cílem práce je identifikace, analýza a hodnocení operačních rizik ve zvolené bankovní instituci, včetně návrhu opatření vedoucích ke snížení rizik.

Seznam literatury:

ANDERSON, D.R. a kol. Quantitative Methods for Business. Boston: Cengage Learning, 2016. ISBN 978-1-285-86631-4.

SMEJKAL, V. a K. RAIS. Řízení rizik ve firmách a jiných organizacích. Praha: Grada, 2013. ISBN 978-80-247-4644-9.

STAŇKOVÁ, A. Podnikáme úspěšně s malou firmou. Praha: C.H. Beck, 2007. ISBN 978-80-7179-926-9.

TICHÝ, M. Ovládání rizika: analýza a management. Praha: C.H. Beck, 2006. ISBN 80-7179-415-5.

ZUZÁK, R. a M. KÖNIGOVÁ. Krizové řízení podniku. Praha: Grada, 2009. ISBN 978-80-247-3156-8.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2023/24

V Brně, dne

L. S.

prof. Ing. Karel Pospíšil, Ph.D., LL.M.
ředitel

Abstrakt

Tato diplomová práce je zaměřena na řízení operačních rizik v bankovnictví. Hlavním aspektem pro výběr operačních rizik, byl rozsah dopadu ve vybrané bankovní instituci, která se řadí mezi největší finanční instituce v České republice. Identifikace a klasifikace rizika proběhla na základě studia interních dokumentů instituce. Operační riziko je definováno jako riziko ztráty vyplývající z nepřiměřenosti nebo selhání interních procesů a systémů, z lidského selhání, a jako riziko ztráty vzniklé v důsledku externí události. Těmito zmíněnými operačními riziky se bude dále práce zaobírat. Cílem je uplatnit teoretické poznatky získané v průběhu studia a aplikovat je za pomocí nástrojů na měření, zhodnocení rizik do práce. Poté jsou prezentovány dopady a následky za pomoci vybraných analýz. Dále práce obsahuje dílčí návrhy na opatření minimalizace rizika ve vybrané instituci. Výsledky práce obsahují určitý přínos pro vedení společnosti a její risk management v neposlední řadě i pro další rozvoj a opatření rizik ve vybrané bankovní instituci.

Abstract

This thesis focuses on operational risk management in banking. The main aspect for the selection of operational risks was the extent of impact in the selected banking institution, which is one of the largest financial institutions in the Czech Republic. The identification and classification of the risk was based on the study of the internal documents of the institution. Operational risk is defined as the risk of loss arising from inadequacy or failure of internal processes and systems, from human failure, and as the risk of loss arising from an external event. These mentioned operational risks will be dealt with later in the thesis. The aim is to apply the theoretical knowledge acquired during the study and apply it to the work with the help of risk measurement, assessment tools. Then the impacts and consequences are presented using selected analyses. Furthermore, the thesis contains partial suggestions for risk minimization measures in the selected institution. The results of the thesis contain some contribution to the management and its risk management last but not least for further development and risk measures in the selected banking institution.

Klíčová slova

Řízení rizik, bankovní instituce, operační rizika, analýza, dopad.

Keywords

Risk management, banking institutions, operational risks, analysis, impact.

Bibliografická citace

FRAITOVÁ, Tereza. *Řízení operačních rizik v bankovnictví*. Brno, 2024. Dostupné také z: https://www.vut.cz/studenti/zav-prace/detail/153121. Diplomová práce. Vysoké učení technické v Brně, Ústav soudního inženýrství, Odbor inženýrství rizik. Vedoucí práce Radek Doskočil.

Prohlášení

Prohlašuji, že svou diplomovou práci na téma „Řízení operačních rizik v bankovnictví“ jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně .....

.....

Podpis autora

Poděkování

Na tomto místě bych chtěla velice poděkovat svému příteli a rodině za trpělivost a podporu, nejvíce především mému otci za poskytnuté rady, které mě přivedly až do cíle této práce. Dále bych chtěla poděkovat vedoucímu práce doc. Ing. Radku Doskočilovi, Ph.D., MSc za ochotu a odborné vedení. Ráda bych také poděkovala vedení ve vybrané bankovní instituci především za ochotu, vstřícnost a poskytnutí veškerých informací ke zpracování.

OBSAH

OBSAH 8
1 ÚVOD 10
2 SOUČASNÝ STAV/REŠERŠE 11
2.1 Teoretická východiska 11
2.1.1 Riziko 11
2.1.2 Aktivum 12
2.1.3 Hrozba 12
2.1.4 Zranitelnost 12
2.1.5 Protiopatření 13
2.2 Dělení rizik v bankovnictví 13
2.2.1 Úvěrové riziko 13
2.2.2 Tržní riziko 14
2.2.3 Likvidní riziko 14
2.2.4 Operační riziko 15
2.3 Proces řízení rizik 16
2.3.1 Identifikace a sledování rizika 17
2.3.2 Hodnocení analýzy rizik 21
2.3.3 Kvalitativní analýza 21
2.3.4 Kvantitativní analýza 25
2.3.5 Kombinované metody 26
2.3.6 Ošetření rizik 28
2.4 Volby strategie analýzy 29
2.4.1 Strategické nástroje analýzy 29
2.5 Současný stav v bankovnictví 35
2.5.1 Hlavní principy řízení rizik 35
2.5.2 Strategie řízení rizik 36
3 FORMULACE PROBLÉMŮ A STANOVENÍ CÍLŮ ŘEŠENÍ 38
4 POUŽITÉ METODY A JEJICH ZDŮVODNĚNÍ 39
5 VLASTNÍ ŘEŠENÍ VYBRANÉ PROBLEMATIKY 40
5.1 Základní principy řízení operačních rizik 40
5.2 Odpovědnost za řízení operačních rizik ve všech útvarech banky 41
5.3 Identifikace rizik 42
5.3.1 PESTLE analýza 42
5.3.2 McKinseyho model 7 S 49

5.3.3 Metoda RIPRAN 57
5.4 Vyhodnocení operačních rizik 62
5.4.1 Vyhodnocení PESTLE analýzy 62
5.4.2 Vyhodnocení McKinseyho modelu 7 S 63
5.4.3 Vyhodnocení metody RIPRAN 63
5.5 Návrhy opatření k minimalizaci rizik 66
5.6 Návrh strategie operačních rizik 68
5.6.1 Implementace strategie 68
5.6.2 Vymezení odpovědnosti 71
5.6.3 Kontrola a monitoring 72
6 DISKUSE 74
7 ZÁVĚR 75
8 PŘÍLOHA Č. 1 – METODA RIPRAN 77
SEZNAM POUŽITÝCH ZDROJŮ 83
SEZNAM TABULEK 85
SEZNAM GRAFŮ 85
SEZNAM OBRÁZKŮ 85
SEZNAM ZKRATEK 86
SEZNAM PŘÍLOH 86

1 ÚVOD

Tato diplomová práce je zaměřena na řízení operačních rizik v bankovnictví. Primární funkcí systému řízení rizik je přispívat k optimalizaci celkové ziskovosti banky ve vztahu k podstupovanému riziku, a přitom zajišťovat kontinuitu instituce pomocí implementace vhodného přístupu k řízení rizik.

Hlavním aspektem pro zpracování jsou vybraná operační rizika s ohledem na rozsah dopadu ve vybrané bankovní instituci, která se řadí mezi největší finanční instituce v České republice. Identifikace a klasifikace rizika proběhla na základě studia interních dokumentů instituce, jako zaměstnanci mi byl umožněn přístup k interním dokumentům, které obsahují identifikaci jednotlivých rizik s ohledem na její finanční dopad. S ohledem na stupeň utajení těchto dokumentů je zde není možné citovat. Těmito zmíněnými operačními riziky se práce nadále zaobírá.

Z počátku práce jsem stanovila teoretická východiska práce a popsala základní pojmy, týkající se řízení rizik, rozdělení rizik a postup analýzy rizik. Dále je zde popsána strategie analýzy rizik, její nástroje a současný stav v bankovnictví. Tyto pojmy se objevují v bankovních institucích a ve způsobu jejich řízení.

V další části jsem stanovila a popsala hlavní cíl práce, který spočívá ve vyhodnocení operačních rizik vybrané bankovní instituce na základě zpracování dílčích cílů.

Poté jsem se zaměřila konkrétně na operační riziko a použité metody hodnocení, s ohledem na studium interního dokumentu, který identifikuje a ohodnocuje riziko. Zde popisuji základní principy řízení operačních rizik a odpovědnost za jejich řízení. Následně jsem nejprve identifkovala operační rizika pomocí strategických analýz vnějšího a vnitřního prostředí a procesní metody RIPRAN vybrané instituce. Jednotlivé části práce jsem rozdělila v rámci metody RIPRAN dle jejího postupu od identifikace, hodnocení až po výpočet hodnoty rizika a jeho dopadu. Zde jsem navrhla opatření a definovala úseky odpovědné za zajištění minimalizace operačních rizik.

Poslední část práce jsem věnovala návrhu strategie operačních rizik – implementaci řízení, vymezení odpovědnosti, kontrole a monitoringu operačních rizik ve vybrané bankovní instituci.

V závěru práce jsem popsala diskusi výsledků práce s vedením bankovní instituce a její možný přínos pro vedení instituce a její risk management v neposlední řadě i pro další rozvoj a opatření rizik ve vybrané bankovní instituci.

2 SOUČASNÝ STAV/REŠERŠE

Základní vědomostní podklady k teoretické části této diplomové práce, jejímž úkolem je identifikace, analýza a hodnocení operačních rizik ve zvolené bankovní instituci, včetně návrhu opatření vedoucích ke snížení rizik, jsou zejména tyto literární prameny: Quantitative Methods for Business z tohoto literárního pramene jsem popsala kvantitativní rozdělení metod hodnocení analýzy rizika, Řízení rizik ve firmách a jiných organizacích zde jsem využila pro popis základních pojmů, z knihy: Podnikáme úspěšně s malou firmou, byl aplikován základní popis ošetření rizika, Z knihy Ovládání rizika: analýza a management, jsem využila definici hlavního pojmu riziko. Z tohoto literárního pramene: Krizové řízení podniku, jsem popsala podkapitolu, proces řízení rizik.

Při zpracování této práce jsem vycházela z osobní pracovní zkušenosti pro vybranou instituci. Na základě studia interních dokumentů instituce jsem identifikovala a klasifikovala rizika s ohledem na jejich finanční dopad. Na základě této analýzy jsem vyhodnotila operační riziko jako riziko s největším dopadem na vybranou bankovní instituci. S ohledem na stupeň utajení těchto dokumentů, je zde není možné citovat. Specifikace dalších použitých informačních zdrojů je uvedena na konci práce v seznamu použité literatury.

2.1 TEORETICKÁ VÝCHODISKA

V této části práce jsem popsala základní pojmy, které jsou analyzovány a popsány s důrazem na jejich aplikaci v praktické části práce. Tyto pojmy se týkají i řízení rizik v bankovní instituci.

2.1.1 Riziko

Název riziko označuje velmi odlišné kvalitativní pojmy. Pokud přistoupíme k definici rizika, tak zjistíme, že se jedná o významný problém, který není univerzálně řešitelný. Především hodně záleží na oboru, odvětví, a také o jazyku, ve kterém o něm hovoříme či píšeme, abychom věděli, co se právě pod tímto názvem rozumí. Některé vybrané definice považují riziko za pozitivní odchylky od přiřazené hodnoty. Což je logické, protože právě vědomí nebezpečí je nepříznivé pro jednoho člověka a toto může být zároveň příznivé pro druhou osobu. Hovoříme tedy o absolutním riziku a relativním riziku. Naopak především negativní riziko nazýváme výhodou, protože je zde málo rizik, které nemají duální povahu, a právě tyto rizika většinou převažují.

Mnohdy se setkáváme se specifickými definicemi rizik pro konkrétní oblast nebo obor. (Tichý, 2006, s. 15)

2.1.2 Aktivum

Aktivum je cokoli, co má pro analyzovanou společnost hodnotu. Aktiva mohou být hmotné i nehmotné. Základní charakteristikou aktiva je jeho hodnota, vycházející z obecně vnímaného objektivního vyjádření ceny. Působením hrozby může být hodnota aktiva zmenšena, a její citlivost na působení hrozby projevuje zranitelnost. Mezi nejdůležitější aktiva patří například znalosti, data a informace, technické zdroje, software, osobní informace a komunikační zařízení. (Hnilica, 2009, s. 38-39)

2.1.3 Hrozba

Hrozba je událost, síla, činnost nebo osoba, která má negativní vliv na úspěch nebo může způsobit újmu či způsobit poškození celé organizace. Hrozba může být lidského či přírodního zrodu, také může být náhodná nebo úmyslná. Hrozby mohou vycházet zevnitř nebo zvenčí organizace. Hrozbou může být například požár, krádež zařízení, živelná pohroma, získání přístupu ke všem informacím neoprávněnými osobami, chyba personálu, kontrola finančního úřadu nebo i růst kurzu české koruny vzhledem k evropské měně apod.

Poškození nebo ohrožení daného zdroje, které způsobí hrozba, se nazývá dopad hrozby. Dopad hrozby může být odvozen od absolutní hodnoty ztráty, která zahrnuje také náklady na obnovení činnosti aktiva nebo náklady na odstranění následků újmy způsobené subjektem hrozby. (Smejkal, 2013a, s. 82)

2.1.4 Zranitelnost

Zranitelnost je hrozba, znehodnocení nebo stav analyzovaného aktiva (případně subjektu nebo jeho části), které mohou být hrozbou sloužící k vyvolání nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak je aktivum citlivé na působení dané hrozby. Zranitelnost vznikne při interakci mezi hrozbou a zdrojem. Jedním z podstatných rysů zranitelnosti je její úroveň. Úroveň zranitelnosti aktiva se posuzuje na základě těchto faktorů: Citlivost: náchylnost aktiva k poškození danou hrozbou. Kritičnost: důležitost přínosu aktiva pro analyzovaný subjekt. (Smejkal, 2006, s. 83)

2.1.5 Protiopatření

Protiopatření je postup, procedura, proces technická metoda nebo cokoli, co je speciálně navrženo ke snížení dopadu hrozby, snížení zranitelnosti nebo odstranění. Tato protiopatření jsou navrhována s cílem předcházet vzniku újmy nebo s cílem usnadnit odstranění následků vzniklé újmy. V rámci analýzy rizik je protiopatření charakterizováno efektivitou a náklady. Efektivita protiopatření vyjadřuje jak moc, tak i o kolik klesne účinek hrozby. Používá se ve fázi zvládání rizik jako jeden ze dvou hlavních parametrů k zajištění vhodnosti použití určitého protiopatření. Protiopatření se specializují na oblasti snížení úrovně hrozby, snížení následků působení hrozby, snížení úrovně zranitelnosti, detekce nežádoucích vlivů s cílem včasně indikovat dopad hrozby a co nejvíce zabránit jejího plnému použití, dále se soustředí na oblast obnovení činnosti působení hrozby. Náklady na pořízení, zavedení a provozování protiopatření se započítávají do celkových nákladů na protiopatření. Společně s efektivitou protiopatření jsou tyto náklady důležitými parametry při výběru protiopatření. Nalezení adekvátního protiopatření spočívá v optimalizaci, hledá se zde protiopatření, jehož provedení přinese nejmenší náklady. (Smejkal, 2006, s. 83)

2.2 DĚLENÍ RIZIK V BANKOVNICTVÍ

Rizika v bankovnictví v nejjednodušším slova smyslu lze charakterizovat jako rizika, kdy jedna strana finančního nástroje způsobí nesplněním své povinnost finanční škodu druhé straně, nebo protistrana nebude jednat ve finanční transakci v souladu s předem domluvenou smlouvou. Porušení smlouvy, která bance způsobí finanční škodu, může být způsobeno buď neschopností, nebo neochotou protistrany. Pravděpodobnost selhání je pravděpodobnost, s jakou protistrana nedostojí svým závazkům a lze ji přirovnat k pravděpodobnosti, že věřitel (banka) utrpí ztrátu. (Blahová, 2018, s. 84)

2.2.1 Úvěrové riziko

Podstatou úvěrového rizika je neschopnost protistrany dostát svým závazkům. Typ úvěrového rizika se liší v závislosti na finančním nástroji, a také v různých fázích provádění finančních transakcí. Zatímco, u některých typů obchodů (úvěrů) je vystavena riziku celá částka (nesplacená jistina včetně úroků), u jiných typů obchodů (forwardové směnné obchody) sahá míra rizika pouze do výše rozdílu mezi sjednanou cenou úvěru a cenou náhradního obchodu, která je aktuálně dostupná na trhu. V době splatnosti však obchodování s termínovanými obchody zahrnuje období úvěrového platebního rizika pro celou obchodovanou částku. (Blahová, 2018, s. 84)

2.2.2 Tržní riziko

Tržní riziko je pravděpodobnost změny hodnoty společnosti způsobené změnou tržní hodnoty rizikového faktoru. Pro tržní riziko je charakteristické, že je způsobeno rizikovými faktory, které obvykle nabývají určitých hodnot vyplývajících z tržních cen. Tomu se vystavujeme pokaždé, když v budoucnu převezmeme pevnou hodnotu pohledávky nebo závazku. Tržní rizika jsou proto nedílnou součástí finančního plánování.

Aktuální a historická cenová data lze obvykle poměrně snadno získat z veřejných nebo profesionálně dostupných zdrojů (směnné kurzy, burzovní ceny, kotace tvůrců trhu) se vypočítají pomocí známého modelu tržního oceňování.

Podle typu podkladového tržního nástroje, který lze chápat jako rizikový faktor, rozlišujeme základní čtyři kategorie tržního rizika, nazývané akciové riziko, úrokové riziko, měnové riziko a komoditní riziko. Kromě toho jsou zde i odvozená tržní rizika, která ovlivňují ocenění obchodovaných nástrojů, ale samostatně se obchodují pouze ve formě finančních derivátů. (Vlachý, 2006, s. 19)

2.2.3 Likvidní riziko

Každá banka by měla mít dohodnutou strategii pro každodenní řízení likvidity. Tato strategie by měla být komunikována v celé organizaci. Představenstvo musí schválit strategii řízení rizik a mít konečnou odpovědnost za všechny aspekty její implementace a fungování. Ve většině případů se však strategie vyvíjejí ve spolupráci mezi vyššími manažery a ředitelem banky. Výsledky jsou poté předloženy představenstvu ve formě doporučení k formálnímu schválení.

Jedním z nejdůležitějších nároků na strategii řízení likvidity je vymezení rizikových limitů. Strategie řízení likvidity by měla stanovit obecný přístup, který banka při řízení likvidity použije, případně včetně různých kvantitativních a kvalitativních cílů. Představenstvo by mělo podniknout vhodné kroky, aby zajistilo, že limity budou v souladu s tolerancí rizika stanovenou společností. Jak je uvedeno dále v tomto článku, rizikové limity musí být přiměřené povaze, rozsahu a složitosti podnikání banky.

Při určování strategie řízení likvidity musí představenstvo a vedení banky zvážit, jak bude řízení likvidity koordinováno s ostatními strategickými plány a cíli řízení rizik. Například strategické plány na zvýšení zisků prostřednictvím rychlého růstu úvěrů, by měly brát v úvahu riziko likvidity a dopady na financování. Zvláštní pozornost by měla být věnována klíčové

souvislosti mezi rizikem likvidity a reputačním rizikem. Jak poznamenal jeden odborník: „Zničení jména může trvat jen několik týdnů, ale jeho obnovení může trvat roky.“

Než se pustí do velkých obchodních iniciativ, měli by ředitelé a vrcholoví manažeři zvážit důležité otázky, jako například: Jak může provozování nového podniku, jako je subprime půjček, ovlivnit pověst banky, například potenciální problém s novým obchodem, který by mohl mít negativní publicitu v budoucnosti.

Podrobnosti strategie se obvykle odrážejí ve schválených zásadách řízení rizika likvidity představenstvem, což je téma probírané dále. Strategie řízení rizika likvidity by měla zahrnovat specifické aspekty řízení rizika likvidity. V rámci povahy, rozsahu a složitosti vykonávaných činností mohou tyto aspekty zahrnovat: cíle pro řízení krátkodobého a dlouhodobého financování, cíle pro řízení rizik likvidity, způsob řízení likvidity (např. centrální nebo regionální), identifikaci vhodných či nevhodných nástrojů pro řízení rizik, míru koncentrace, která by mohla ovlivnit riziko likvidity a metody řízení celkových potřeb banky v cizích měnách a jejích potřeb v každé jednotlivé měně. (Matz, 2007, s. 67-68)

2.2.4 Operační riziko

K operačnímu riziku můžeme přiřadit v detailním rozlišení následující rizika: Riziko transakcí je rizikem ztráty při provádění operací v důsledku chyb v provedení operací, chyb vyplývajících ze složitosti produktů a neschopnosti současných systémů je kvalitně provádět, chyb v zaúčtování obchodů, chyb ve vypořádání obchodů, při nezáměrném poskytnutí či přijetí komodit a v neadekvátní právní dokumentaci.

V posledních desetiletích dochází ve finančních sektorech, zejména v bankovnictví a pojišťovnictví, k návratu k retailu s rozsáhlým využíváním alternativních prodejních kanálů (bankomaty, internet, GSM bankovnictví – služby pro ovládání bankovnictví za pomocí mobilního telefonu), což s sebou přináší nejen značné výhody pro celý retailový sortiment, ale i řadu nových rizik. V novém regulačním konceptu Solvency II je tato skupina rizik spojených se selháním systému, počítačovými podvody nebo padělaním identity souhrnně označována jako operační riziko. Operační riziko je riziko ztráty v důsledku nedostatečnosti nebo selhání vnitřních procesů, lidí, systémů nebo v důsledku vnějších událostí. Další podskupinou operačních rizik jsou chyby zaměstnanců, výpadky informačního systému nebo výpadky komunikační sítě.
Je zřejmé, že operační rizika jsou velmi závažnou rizikovou kategorií, jejíž důsledky mohou mít v extrémních případech na komerční pojišťovny mnohem větší dopad než jiná rizika.
K operačnímu riziku můžeme v podrobné definici přiřadit tato rizika: Transakční riziko je riziko

ztrát při provádění operací v důsledku chyb při provádění operací, neschopnosti současných systémů jejich řádné provádění a chyb vyplývajících ze složitosti produktů, chyby ve zpracování transakcí, chyby ve fakturačních transakcích, neúmyslné poskytnutí nebo převzetí zboží a nedostatečná právní dokumentace.

Operační manažerské riziko je riziko ztrát v důsledku chyb při řízení činností ve front office a back office. Jedná se o neidentifikované nadlimitní transakce, neautorizované transakce jednotlivých obchodníků, podvodné operace související s obchodováním a zpracováním včetně nesprávného účtování a padělání, praní špinavých peněz, neoprávněný přístup do systému a modelů, závislost na omezeném počtu zaměstnanců a nedostatečná kontrola při provádění obchodů. Systémové riziko je riziko ztrát způsobených poruchami v podpůrných systémech. Patří mezi ně chyby v počítačových programech, chyby v matematických vztazích modelu, nesprávný a pozdní přenos informací o řízení, chyby v jednom nebo více podpůrných systémech, chyby v přenosu dat a nesprávné plánování dopadu nepředvídaných událostí v případě chyby systému nebo přenosu dát. Misselling je prodej výrobku, jehož vlastnosti nebyly zákazníkovi dostatečně vysvětleny nebo jehož vlastnosti neodpovídají potřebám zákazníka. (Vávrová, 2014, s. 65-66)

2.3 PROCES ŘÍZENÍ RIZIK

Cílem vybudování funkčního systému řízení kontinuity podnikání banky je rozvoj organizace, postupů a prostředků, které umožní čelit mimořádným událostem a situacím v podobě neplánovaného přerušení nebo omezení činností banky, haváriím, včetně havárií informačních systémů, selhání pro banku významných třetích osob nebo selhání vnější infrastruktury. Tím bude zajištěna reputace banky, ochrana zaměstnanců a klientů banky, jejích aktiv, nezbytná provozuschopnost a co nejrychlejší obnovitelnost zejména činností významných z hlediska fungování banky. V tomto rámci je obzvlášť důležitým cílem zajištění respektování povinností vyplývajících z právních předpisů a nařízení regulatorních orgánů pro oblast řízení operačních rizik.

Řízení rizik nelze chápat jako jednorázovou či periodickou činnost, ale jako trvalou činnost, která rizika nejen identifikuje a popisuje, ale také je analyzuje, vyhodnocuje a kontroluje. Je součástí krizového managementu chápaného v širším smyslu. Před přípravou podnikových cílů a rozhodnutí musí být řízení rizik realizováno v následujících pěti krocích:

1. Identifikace nebezpečí (zdrojů nebezpečí), např. konkurence, změny v zákoně, potenciální náhradní produkt,

2. Určení rozsahu rizika (např. četnost výskytu, závažnost důsledků pro firmu),

3. Posouzení např. dle níže uvedené matice a provedení rozhodnutí,

4. Zavedení kontrolního systému nad riziky, jehož cílem je identifikace změn rizika (zejména zvýšení rizika),

5. Sledování vývoje rizik, posuzování změn a provádění opatření.

Stanovení úrovně rizika je důležité pro stanovení priorit rozhodnutí a stanovení posloupnosti akcí, pokud společnost přijme cíle. Pokud ve třetím kroku rozhodovatel vyhodnotí riziko pro společnost jako nepřijatelné z hlediska závažnosti důsledků nebo četnosti dopadů rizik, jsou cíle a rozhodnutí přeformulovány a proces se opakuje. (Zuzák, 2009, s. 46-47)

		Frekvence				
		Velmi častá	Častá	Příležitostná	Řídká	Vzácná
Závažnost		A	B	C	D	E
Katastrofální	I	E	E	V	V	M
Kritická	II	E	V	V	M	N
Mezní	III	V	M	M	N	N
Malá	IV	M	N	N	N	N

Obrázek 1: Matice řízení rizik (Zdroj: (Zuzák, 2009, s. 46-47)

2.3.1 Identifikace a sledování rizika

Identifikace rizik (rizikových faktorů) představuje jednu z nejdůležitějších fází řízení rizik, neboť řídit lze pouze ta rizika, která společnost včas identifikovala a připravila vhodné metody pro jejich ošetření. Obsahem této fáze je identifikace všech faktorů, které by mohly ohrozit nebo i pozitivně ovlivnit dosahování cílů podniku (hlavně cílů strategického charakteru) i cílů jednotlivých organizačních jednotek a cílů funkčních oblastí podniku. Identifikace rizikových faktorů je založena na využití znalostí a intuici zaměstnanců společnosti podílejících se na realizaci a řízení jejích činností (identifikace vnitřních rizik), a na pečlivém sledování vývoje podnikatelského prostředí (identifikace vnějších rizik). Při identifikaci rizik by se mělo zapojit co nejvíce zaměstnanců firmy, smysl má i využití externích specialistů. Tato fáze by se však měla vymezit nejen na tradičně chápaná rizika v negativním smyslu, ale i na pozitivní rizika v podobě

příležitostí, doporučujících vytvoření samostatných seznamů rizik a příležitostí. K určité revizi těchto příležitostí dochází po rozpoznání negativních rizik, která mohou přispět k dalšímu nárůstu nalezených příležitostí. K identifikaci rizik se používají tři přístupy, a to:

„Přístup shora dolů“: Identifikace rizik probíhá shora dolů od vedení společnosti. Tento přístup je rychlý a vyžaduje méně komunikace. Protože však neposkytuje hlubší vhled, je nutné identifikovaná rizika postupně zpřesňovat a doplňovat, protože organizace vyžaduje přesnější data pro měření rizik.

„Přístup zdola nahoru“: K identifikaci rizik dochází na nejnižší úrovni řízení společnosti. Získané informace umožňují přesnější a podrobnější pohled. Nevýhodou je velmi náročná komunikace a koordinace.

Procesní přístup: Identifikace rizik se provádí podle linií v organizační struktuře, podle procesů, které jsou navázány na organizační jednotky, nebo i podle produktů. Tento přístup lze kombinovat s oběma předchozími přístupy. Obtížnost tohoto přístupu spočívá v nutnosti zavést a aplikovat jednotnou kategorizaci rizik nutnou pro syntézu získaných dat. (Fotr, 2020, s. 285)

V rámci identifikace rizika lze použít určité nástroje a zdroje informací k identifikaci rizik nebo rizikových faktorů. Nejdůležitější jsou:

Checklist (kontrolní seznam)

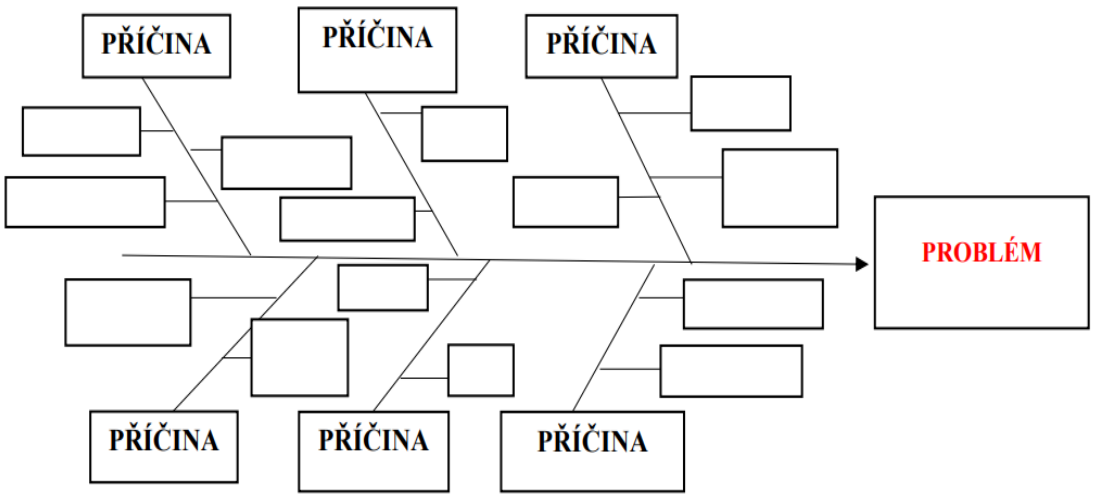
Kontrolní seznamy jsou předdefinované seznamy instrukcí, úkolů, otázek a položek používaných k porovnání produktů, procesů, chování, úkolů, komplexního uživatelského rozhraní atd. Kontrolní seznamy jsou často stručné příručky, podrobné procesní příručky (užitečné, když jsou postupy příliš složité nebo zdlouhavé na zapamatování), nebo jiné základní zdrojové dokumenty. Kontrolní seznamy mohou mít velikost od jednoslovné mnemotechnické pomůcky (např. „AEIOU“), až přes stránku nebo dvě položky ano/ne až po delší texty, jako je celá kniha, manuál nebo velké plány. Kontrolní seznam, bez ohledu na jeho velikost, můžeme považovat za nástroj pro snížení rizika „Čím větší rizika, tím více času budete muset investovat do navrhování a testování svého kontrolního seznamu.“ uvádí autor Atul Gawande. Kontrolní seznamy pomáhají vyhnout se mnoha jednoduchým chybám a také motivují kolegy při práci na složitých úkolech nebo problémech.

Vytváření kontrolních seznamů pro aktivity návrhu zaměřeného na uživatele může být velmi užitečné kontrolu stávajících kontrolních seznamů, abychom zjistili, zda projekt vyžaduje vlastní kontrolní seznam, a pro získání představy o tom, co tvoří dobrý kontrolní seznam. (Wilson, 2013, s. 24)

Ishikawův diagram

V praxi se používá mnoho různých typů kauzálních map, včetně Ishikawových diagramů. Tento diagram je také známý jako rybí kost, diagram příčin a následků, diagramů dopadu (od jedné příčiny k velmi mnoha následkům), stromů hlavních příčin a strategické mapy. Ishikawův diagram byl vytvořen Dr. Kaoru Ishikawa v letech 1943-1969 a je velmi oblíbenou formou kauzální mapy.

Ishikawův diagram poukazuje na vztahy mezi problémem a možnými příčinami problému. Následující obrázek je příkladem. Proces ishikawova diagramu začíná umístěním názvu základního problému na pravý konec diagramu do „hlavy“ hlavní páteře ryby. Hlavní příčinou potíží jsou kosti hlavní páteře.



Obrázek 2:Ishikawa Diagram (Zdroj: Vlastní zpracování)

Mnoho společností identifikuje šest příčin: stroje (technická zařízení), metody, měření, materiály, práce (pracovníci) a matka příroda (životní prostředí). Mnozí však tvrdí, že tento seznam je příliš omezující. Proto se využívá metody Brainstormingu, který se obvykle provádí za účelem přidání možných příčin pro hlavní kosti a specifičtějších příčin pro kosti hlavní páteře. Toto dělení na stále větší specifičnost pokračuje, dokud nelze problémové oblasti dále rozdělit. Reálná maximální hloubka tohoto stromu se obvykle pohybuje kolem čtyř až pěti úrovní.

Ishikawův diagram má velmi mnoho omezení. Lze analyzovat pouze jednu výstupní proměnnou. Tento diagram je obtížné zpracovat, a ještě těžší číst, pokud problém vyžaduje

mnoho vrstev příčinných souvislostí. Kromě psané formy lze vytvořit diagram i na počítači. (50Minutes.com, 2015, s. 8)

Brainstorming

Rozhovory s odborníky a skupinové diskuse. Tyto diskuse mohou mít podobu brainstormingových setkání, kdy skupinu tvoří zaměstnanci společnosti, externí odborníci atd. V diskusi je zakázána kritika vyjádřených názorů. Týmová práce podporuje kreativitu, která je nezbytná pro identifikaci rizik, a umožňuje výměnu informací a zkušeností.

Brainstorming je expertní metoda, jejímž cílem je vygenerovat co nejvíce nápadů na konkrétní téma, protože týmová práce může generovat více nápadů než od izolovaných jednotlivců. Tento proces byl poprvé prosazován reklamním expertem Alexem Faickney Oshornem v roce 1939 a poté byl dále rozvinut jako specifická metoda v knižní podobě. Nejčastěji se používá v managementu, ekonomii, pro hledání optimálních postupů nebo prognózování. Volně se to také překládá jako výměna myšlenek. Brainstorming většinou probíhá ve skupině maximálně dvaceti členů a jde o krátkou diskusi, která se řídí stanovenými pravidly.

Jednotlivá pravidla obsahují:

- Odborníci by měli mít podobné sociální postavení a úroveň vzdělání,
- diskuse musí probíhat v klidném přátelském prostředí a v atmosféře uvolněnosti, neformálnosti a optimismu; účastníci by neměli mezi sebou diskutovat,
- úspěšnost diskuse je ovlivněna formulací otázek; do týmu by se neměli zařazovat skeptici, výsledek nebude optimální.

Prezentované nápady jsou zaznamenány anonymně. Konečnou formulaci a vyhodnocení diskuse provede další skupina odborníků podle písemného záznamu. Brainstorming, jehož výhoda spočívá v rychlosti a použitelnosti, je často určen pouze k překlenutí oblastí, které pak nemůžeme analyzovat pomocí kvantitativních prognostických metod. (Štědroň, 2012, s. 39-40)

Kognitivní (myšlenkové) mapy

Jsou grafickým nástrojem pro zobrazení jednotlivých rizikových faktorů a jejich vztahů. Rizikové faktory jsou napsány na kus papíru a jejich vzájemné vztahy jsou znázorněny pomocí zarovnaných spojnic. Spojnice začíná rizikovým faktorem na straně příčiny a šipka ukazuje na faktor na straně účinku rizika (například překročení investičních nákladů bylo způsobeno navýšením ceny subdodávky, kterou si subdodavatel mohl dovolit z důvodu neodpovídající kvality zakázky). Kognitivní mapa tak ukazuje příčinné vztahy (vztahy příčin a následků) rizikových faktorů

a dopadů rizika. Mezi zdroje informací pro identifikaci rizikových faktorů patří v první řadě informace a znalosti odborníků z oboru, ke kterému se jednotlivé faktory vztahují, výsledky strukturovaných rozhovorů a dotazníků, tuzemské či zahraniční zkušenosti osobního či firemního charakteru, výsledky strukturovaných rozhovorů a dotazníků, výsledky řízených rozhovorů a dotazníků atd. Dále také doporučení externích auditorů, příprava podnikatelského plánu společnosti, výsledky finančního controllingu a interního auditu, periodické rozbory výsledků společnosti, výsledky monitorovacích systémů či systémů včasného varování a v neposlední řadě znalosti a zkušenosti z implementace významných projektů. (Hnilica, 2009, s. 28-30)

2.3.2 Hodnocení analýzy rizik

V mnoha případech se při analýze rizik pracuje s veličinami, které nelze přesně změřit a určení jejich velikosti se často opírá o kvalifikované posouzení odborníka, který se vyjadřuje pouze na základě svých zkušeností (obvykle výrazy jako např. "malé", "střední", "velké" nebo stupnice 1 až 10). Zdá se, že nejrozšířenější výklad pojmu „úroveň rizika“ souvisí s pravděpodobností jeho výskytu. Intuitivně považujeme události s vysokou pravděpodobností ztráty za „rizikovější“ než ty, kde je pravděpodobnost nízká. Tento intuitivní koncept úrovně rizika je v souladu s definicí rizika. Pokud je riziko definováno jako možnost nepříznivé odchylky od požadovaného výsledku, který jsme očekávali nebo v který jsme doufali, je míra rizika mírou pravděpodobnosti této nepříznivé odchylky. Jedinec doufá, že ke ztrátě nedojde, takže pravděpodobnost odchylky od toho, v co doufáme (a co je mírou rizika), se přímo mění s pravděpodobností, že ke ztrátě dojde. U jednotlivce měříme riziko podle pravděpodobnosti nepříznivé odchylky od výsledku, ve který jsme doufali.

Základem měření rizika je vymezení jeho číselných charakteristik v podobě charakteristik variability (rozptylu, pravděpodobnosti ztráty nebo směrodatné odchylky) zvoleného kritéria, např. Hodnota podniku, hodnotící kritéria investičních projektů jako kapitálová hodnota atd. To však vyžaduje jak kvantitativní charakter velikosti (kritéria), podle nichž je riziko určeno, tak znalost jeho rozdělení pravděpodobnosti. V opačném případě není možné numerické měření rizika, ale lze použít určité kvalitativní (verbální měření) charakteristiky. Níže si oba způsoby měření rizik popíšeme podrobněji. (Smejkal, 2009, s. 102-103)

2.3.3 Kvalitativní analýza

Kvalitativní charakteristiky vyjadřují rizika pomocí specifické škály se slovním popisem, které jsou poměrně jednoduché rozpoznat. Stejně jako u hodnocení intenzity přínosů projektu k plnění organizačních cílů je vhodná buď hrubší škála se třemi úrovněmi (nízké, střední a vysoké

riziko), nebo jemnější škála s pěti úrovněmi (velmi nízké, nízké, střední, vysoké, a zvláště vysoké riziko). Pro stanovení rizikovosti projektu v této podobě lze opět použít např. metodu Q-sort. Nejde jen o to, abychom potenciální projekty rozdělili do dvou kategorií (přijatelné a nepřijatelné), ale do tří až pěti kategorií. Kvalitativní znázornění projektového rizika je pro manažery přijatelnější, protože nevyžaduje základní znalosti statistiky a teorie pravděpodobnosti. Hlavním omezením je však to, že na jedné straně nedospíváme ke stanovení dopadu rizika projektu na hodnoty kvantitativních kritérií pro jeho posouzení a na druhé straně je obtížnější stanovit nepřijatelné riziko. Dále jsou popsány některé z metod. (Fotr, 2014, s. 56-57)

Analýza scénářů

Pomocí analýzy scénářů je navržen model budoucího vývoje v souvislosti se zkoumanou nejistotou. Lze jej využít již i při identifikaci rizik, neboť nová rizika lze nalézt zkoumáním různých scénářů budoucího vývoje. Vytvořené scénáře lze také použít jako vstup pro kvantitativní analýzu rizik a rozhodování, kde jsou rizika pro jednotlivé scénáře identifikována pomocí vybraných vhodných metod kvantifikace nebo rozhodování. Scénáře jsou většinou vytvářeny tak, že představují alespoň nejlepší, střední a nejhorší variantu vývoje, vždy však záleží na konkrétní situaci, protože alternativy mohou být pouze dvě, ale může být i více scénářů. Při vytváření a vyhodnocování scénářů je třeba dodržet následující kroky:

1. Sestavení vhodného týmu na základě kontextu problému, který má být řešen.
2. Vyhodnocení události, změny a trendy, které mohou mít dopad na řešený problém (např., vývoj trhu, konkurence změny v technologii, legislativa atd.).
3. Každý z identifikovaných faktorů zohledněný při tvorbě scénářů je nutné posoudit podle velikosti jeho vlivu a míry nejistoty – nejvýznamnější jsou faktory s vysokým vlivem nebo s vysokou nejistotou
4. Každý vytvořený scénář musí mít podobu „příběhu“, který vystihuje, proč a jak k tomuto vývoji může dojít a jaké z toho plynou důsledky.
5. Scénáře je nutné ověřit z hlediska věrohodnosti pomocí otázek „co kdyby“ Je vhodné hned na začátku zvážit možnosti, jak se vypořádat s analyzovanými riziky, aby byl proces hodnocení scénářů efektivnější.
6. Scénáře musí být posouzeny z hlediska jejich pravděpodobnosti výskytu, aby bylo možné se dále zaměřit na ty nejpravděpodobnější.

Scénáře se mohou týkat projektu jako celku nebo jen jeho části, více rizik nebo pouze jednoho rizika. Je však zvláště důležité, aby byl scénář popsán, vysvětlen a prodiskutován se zúčastněnými stranami. Podmínky a události spojené se scénářem musí být zohledněny

a vzájemně koordinovány, takže není možné mechanicky kombinovat různé vlivy na projekt, ale všechny zohledněné faktory musí být ve vzájemném souladu. (Korecký, 2011, s. 314)

Metoda RIPRAN

Metoda RIPRAN™ (RIsk PRoject ANalysis) je empirická metoda pro analýzu rizik projektů, vhodná zejména pro střední a velké projekty. Aktuální třetí verze pracuje s registrem rizik a zaznamenává progresi rizik projektu v čase. Důsledně vychází z procesního pojetí analýzy rizik. Analýza rizik chápe jako posloupnost procesů, z nichž každý má definované vstupy, výstupy a definované procesní činnosti a převádí vstupy na výstupy s konkrétním cílem. (Lacko, 2024)

Skládá ze čtyř základních kroků, označovaných jako

1. Identifikace zabezpečení projektu,

2. Kvantifikace rizika projektu,

3. Reagování na rizika projektu,

4. Celkové hodnocení rizik projektu.

V prvním kroku projektový tým provede identifikaci nebezpečí vytvořením seznamu.

Text řádku můžeme získat buď tak, že hledáme odpověď na otázku:

Co se muže přihodit v projektu nepříznivého, a kdy?

Tedy postup, kdy k hrozbě hledáme možné následky:

HROZBA⇒SCÉNÁŘ

Můžeme však také postupovat opačně a získat kompletní text řádku odpovědi na otázku:

Co může být příčinou, že to, a to nepříznivé v projektu nastane?

Tedy postup, kdy ke scénáři hledáme jeho příčinu:

SCÉNÁŘ⇒HROZBA

Ohrožením rozumíme konkrétní projev nebezpečí. Scénářem rozumíme událost, která nastane v důsledku nastávající hrozby. Je důležité si uvědomit, že příčinou scénáře je hrozba.

Ve druhém kroku se kvantifikuje riziko. Tabulka, kterou vytvoříme v prvním kroku, je rozšířena o pravděpodobnost naplnění scénáře, hodnotu dopadu scénáře na projekt a výslednou hodnotu rizika (v Kč nebo EUR), která se počítá:

Hodnota rizika = pravděpodobnost scénáře x hodnota dopadu.

Metoda RIPRAN umožňuje i tzv. verbální kvantifikaci při použití slovního hodnocení. Kdy hodnotu pravděpodobnosti rizika nad 33 % můžeme slovně ohodnotit jako vysokou hodnotu, a naopak hodnotu pod 10 % jako nízkou hodnotu.

Vysoká pravděpodobnost – VP	nad 33 %
Střední pravděpodobnost – SP	10–33 %
Nízká pravděpodobnost – NP	pod 10 %

Obrázek 3: Verbální hodnoty pravděpodobnosti soustava 3x3 (Zdroj: (Doležal, 2012, s. 92)

Ve třetím kroku se vypracují opatření ke snížení hodnoty rizika na přijatelnou úroveň. Návrhy opatření jsou obvykle zpracovány do tabulky. Pak se místo čísel používají dohodnuté zkratky z jednotlivých tabulek. Typ použitých tabulek musí být dohodnut s projektovým týmem před analýzou rizik. Tým se obvykle před kvantifikací rizik dohodne, zda použije numerickou nebo verbální metodu ke kvantifikaci rizik. Není praktické používat obojí současně, i když je to možné.

Čtvrtým krokem je posouzení celkové hodnoty rizik a vyhodnocení, jak rizikový je projekt a zda je možné pokračovat v realizaci bez zvláštních opatření. Pokud vnímají celkovou úroveň jako velmi vysokou, problém eskaluje na vyšší úroveň řízení. Z výše uvedeného je zřejmé, že metoda RIPRAN vyžaduje práci s detailní analýzou hrozeb, scénářů, hodnot pravděpodobnosti a hodnot dopadu. Proto je komplexnější, složitější a vyžaduje určité znalosti rizikového inženýrství i zkušenosti z předchozích projektů. Poskytuje však přesnější výsledky analýzy rizik pro projekt než skórovací metoda. Kromě toho podporuje tým při hledání opatření ke snížení rizik nabídkou tzv. standardních opatření na snížení rizik, která týmu pomáhají snáze najít konkrétní opatření. (Doležal, 2012, s. 90-93)

FMEA

FMEA je analýza možností vzniku a následků selhání. Patří mezi důležité proaktivní preventivní strategie. Tato metoda je v průmyslu uplatňována více než čtyřicet let a její vznik je spojen s projektem NASA Apollo. Poté se rychle rozšířila do automobilového a leteckého průmyslu jako nástroj ke zlepšování bezpečnosti procesů a výrobků. FMEA je zamýšlena k použití

všemi způsoby především k identifikaci a prevenci potenciálních problémů. Je to metoda, která soustavným způsobem hledá odpovědi na otázky, " jak procesy můžeme učinit bezpečnějšími a proč procesy selhávají". FMEA pomáhá uživatelům najít a implementovat vylepšení dříve, než chyby povedou k poškození majetku nebo zničení pověsti společnosti. Účelem této jednoduché metody je analyzovat všechny komponenty sledovaného systému za účelem odhalení možných zdrojů poruch. Posuzují také možné důsledky poruchy a dopad poruchy na celý systém.

Existují dva typy analýzy FMEA: analýza produktu a analýza procesů. FMEA také řeší některé ze základních důvodů, proč procesy selhávají, jako například: proměnlivé vstupy do procesů, nedůslednost, zbytečná složitost procesů, závislost na lidském faktoru, nereálné časové osy nebo úzká návaznost jednotlivých kroků v procesu. Je zřejmé, že nástroj FMEA se zaměřuje na analýzu těch procesů, které jsou vysoce rizikové a mají vysokou pravděpodobnost selhání a chyb.

Při analýze procesu si klademe následující otázky: Co může v tomto procesu selhat? Jak závažná může být tato chyba, jaké škody může způsobit? Co musíme udělat, abychom předešli případnému selhání? Účelem procesní analýzy je proto zabránit možnosti selhání. Zatímco některé společnosti začínají metodu FMEA uplatňovat retrospektivně (ex post analýza mimořádných událostí), jen málokdo ji využívá správně, tzn. perspektivně jako preventivní analýza. (Škrla, 2008, s. 137)

2.3.4 Kvantitativní analýza

V rámci kvantitativní analýzy rizik projektu, se snažíme poskytnout přesnou analýzu rizik projektu pomocí číselného vyjádření pravděpodobnosti a dopadu ve finančních jednotkách. Tyto numerické metody se také často používají k vyjádření celkového rizika projektu atp. Ne vždy je možné provést kvantitativní analýzu rizik, protože nemusí být k dispozici dostatečně přesné údaje o pravděpodobnosti nebo dopadu jednoho nebo více analyzovaných scénářů (nejsme schopni dosáhnout vyšší úrovně přesnosti než např. uvádějící, že pravděpodobnost je nízká a dopad velký). Vstupní data kvantitativní analýzy rizik mohou být buď v absolutních hodnotách, ale používají se i třímístné odhady, podobně např. při odhadu doby trvání projektových aktivit (tj. např. stanovení hodnoty pro nejnižší, nejvíce pravděpodobný a nejhorší finanční dopad určitého rizika). Pro pozdější možné výpočty a simulace se nejčastěji používá beta rozdělení nebo tzv. trojúhelníkové rozdělení frekvencí. Pokud máme dostatek dat, můžeme implementovat jednu z následujících metod kvantitativní analýzy rizik projektu. (Anderson, 2016, s. 12)

Analýza citlivosti

Analýza citlivosti vyžaduje stanovení některých nejistých předpokladů, které ovlivňují změnu určitých hodnot a tím i změnu souvisejících ekonomických ukazatelů. Obvykle měníme každý z těchto předpokladů postupně o 1 % a vypočítáváme nové hodnoty ukazatelů. Pro každou nově vypočtenou hodnotu ukazatele vyjádříme procentuální změnu výsledného ukazatele (např. pokud se hodnota konkrétního ukazatele změní o 1 %), tak se dané kritérium změní o 5 % atd.) Citlivost analýzy pomáhá ukázat spolehlivost predikovaných hodnot a zároveň informuje schvalovatele o možných dopadech, pokud některé předpoklady nejsou z objektivních důvodů splněny. (Doležal, 2012, s. 98)

Skórovací metoda

Jedná se o velmi jednoduchý způsob analýzy rizik. Tato metoda spočívá v identifikaci měřitelných nebo srovnatelných rizik, které mohou nastat během provádění projektu. Rizikové faktory se pak hodnotí pomocí desetibodové škály. Hlavním kritériem je pravděpodobnost, že příslušný rizikový faktor skutečně nastane a jaký bude mít dopad na průběh projektu. Pro hodnocení jednotlivých rizik se používá desetibodová škála. Celkové skóre se vypočítá jako součin dvou hodnot (pravděpodobnost výskytu a pravděpodobnost dopadu), přičemž výsledná hodnota rizikového faktoru je mezi 1 a 100. Tuto metodu neprovádí jednotlivec, ale tým složený z více lidí (např. tým 8 lidí), přičemž každý člen samostatně posuzuje subjektivně identifikované rizikové faktory. Poté se určí aritmetický průměr odhadů členů týmu a určí se výsledné skóre. (Doležal, 2009, s. 94)

2.3.5 Kombinované metody

Kombinované metody vycházejí z číselných údajů. Cíl je však díky kvalitativnímu hodnocení ve větším přiblížení se realitě oproti předpokladům, ze kterých vycházejí kvantitativní metody. Je ovšem třeba mít na zřeteli, že údaje použité v kvalitativních metodách nemusí vždy odrážet přímo pravděpodobnost události či výši jejího dopadu, ale mohou být ovlivněny měřítkem stupnice, která je v konkrétní metodě použita. (Olsen, 2015)

BASELL II

Nová koncepce pravidel kapitálové přiměřenosti (Basel II) je pokládána za nejznačnější změnu v oblasti regulace finančních institucí v posledních desetiletích. Zásadním rozdílem oproti stávající regulaci (Basel I) z roku 1988 je snaha co nejvíce přiblížit minimální kapitálové hodnoty definované zákonem o dohledu skutečným ekonomickým kapitálovým požadavkům na základě

konkrétních rizikových pozic banky. Těchto cílů bylo možné dosáhnout pouze za cenu opuštění dnešní poměrně jednoduché, ale zobecnitelné metodiky (zejména v oblasti úvěrového rizika) výpočtu kapitálové přiměřenosti a zavedení pokročilejších, ale podstatně složitějších přístupů, které věrněji odrážejí podstatu rizika profilu regulované společnosti.

Basel II nabízí různé metody pro výpočet příslušných kapitálových požadavků pro všechny typy rizik (tržní, kreditní, operační riziko). Metody jsou záměrně navrženy tak, aby použití pokročilejších přístupů vedlo k nižším celkovým kapitálovým požadavkům. To přímo motivuje banky k přijetí pokročilejších metod řízení rizik.

Nová koncepce je proto často vnímána jako příležitost ke snížení kapitálové náročnosti bankovního portfolia. Pro banky, které dosud nezavedly pokročilejší systém měření a řízení rizik (zejména v oblasti kreditního a operačního rizika), je to však především příležitost takový systém vytvořit. Fungující moderní systém řízení rizik se stává důležitým konkurenčním faktorem, a je předpokladem dlouhodobého přežití banky. Koncept Basel II je založen na následujících třech pilířích:

- *Pilíř 1 - Minimální kapitálové požadavky*

První pilíř Basel II se týká stanovení minimálních kapitálových požadavků. Jde o kapitálové požadavky k úvěrovým, tržním a nově i operačním rizikům. Kapitálové požadavky k tržním rizikům zůstávají téměř beze změny. Zcela nové je zavedení kapitálového požadavku k operačnímu riziku. První pilíř se zaměřuje na úvěrové riziko, kde dochází k významným změnám. Hlavní částí prvního pilíře je definice minimálních kapitálových požadavků, která vychází ze tří základních prvků: definice regulatorního kapitálu, rizikově vážených aktiv a minimálního poměru kapitálu k rizikově váženým aktivům.

- *Pilíř 2 - Dohled*

Druhý pilíř Basel II se zabývá procesem kontroly, orgánem dohledu. Jedná se o postup nejvyšší úrovně kapitálové kontroly a bankovního dohledu. Cílem celého procesu kontroly není pouze zajištění dostačující výše kapitálu banky k pokrytí bankou podstupovaných rizik, ale také motivace bank k zavádění lepších technik řízení rizik. Banka by podle návrhu měla odpovídající vnitřní procesy, které by umožnily posoudit přiměřenost jejího kapitálu ve vztahu k rizikům, které banka podstupuje. Regulátor bude oprávněně požadovat vyšší kapitálový požadavek než, s jakým banka kalkuluje. (Kašparovská, 2006, s. 82)

- *Pilíř 3 - Tržní disciplína*

Účelem 3. pilíře je posílení tržní disciplíny a transparentnosti trhu prostřednictvím reportingu a povinnosti komplexního zveřejňování podstatných informací tak, aby všichni účastníci trhu dostávali dostatečné informace, zejména o rizikovém profilu regulovaných osob a o přiměřenosti krytí rizik kapitálem. (Historie ČNB, 2023)

2.3.6 Ošetření rizik

Ošetření rizik označuje proces uchování firemní tržní síly a aktiv při minimalizaci finančních šoků z neočekávaných ztrát. Rozlišujeme tzv. čisté riziko, které je projevem nejistoty, když dojde k nepředvídatelným událostem, které mohou mít za následek ztrátu. Například pravděpodobnost požáru, záplav, krádeže a jiné. Většina těchto rizik se dá analyzovat a předpovídat statisticky, a proto se lze proti nim pojistit. Druhým typem rizika jsou rizika spekulativní, které vyjadřují nejistotu, zda ekonomická činnost prováděná podle naší vůle přinese ztrátu nebo zisk. Investice do navýšení efektivity výrobní linky se ukáže jako přemrštěná, výhodný nákup sezónních zásob se ukáže jako zbytečně velký. Některá spekulativní rizika lze pojistit, jiná nikoli. Doporučují se čtyři způsoby práce se spekulativním rizikem. (Staňková, 2007, s. 141)

Vyhnutí se riziku

Znamená to, že firma ustoupí od určité činnosti nebo odstoupí od projektu s nepřijatelným rizikem (např. uvedení nového produktu nebo technologie, vstup na nové trhy, provedení určité akvizice atd.). Je však třeba si uvědomit, že příliš časté vyhýbání se rizikům zdůrazňuje negativní stránku rizika a často vede k zanedbávání příležitostí, což má negativní dopad na konkurenční pozici firmy (některá rizika jsou tedy nezbytná). (Fotr, 2014, s. 17)

Preventivní ochrana před rizikem, nebo možnou ztrátou

Do první skupiny patří metody, jejichž cílem je působit preventivně tak, aby byl vyloučen (nebo alespoň omezen) vznik rizikových situací – ještě dříve, než dojde k případné škodě. Do druhé skupiny patří metody zaměřené na omezení (snížení) nepříznivých důsledků vzniku nepříznivých situací, kterým se v podnikání nevyhneme. Riziko krádeže lze snížit například nasazením bezpečnostního personálu, preventivními kontrolami elektrických systémů pro prevenci požárů a instalací kamerových systémů pro monitorování skladovacích prostor. (Smejkal, 2013b, s. 173)

Transfer rizika

Jedná se o běžně používaný způsob snižování podnikatelského rizika. Transfer znamená převod na jiné společnosti (odběratele, dodavatele atd.). K přenosu rizika dochází např. uzavíráním dlouholetých smluv na dodávky materiálů a surovin, uzavíráním smluv na prodej služeb a výrobků za předem určených podmínek, pronájmem výrobních prostor formou leasingu a další. (Srpová, 2011, s. 32)

Pojištění

Podstatou pojištění je chránit pojištěnou osobu před následky rizika, které nastalo. Riziko a jeho důsledky fakticky přecházejí na pojišťovnu. Pojistitel těchto služeb přirozeně požaduje odpovídající náhradu. Jedná se tedy především o komerční. (Ostřížek, 2007, s. 106)

2.4 VOLBY STRATEGIE ANALÝZY

Výběr metody analýzy rizik může znamenat použití jednoho ze čtyř hlavních přístupů:

- Základní přístup,
- neformální přístup,
- podrobná analýza rizik,
- kombinovaný přístup.

Obvykle se provádí analýza rizik ve dvou základních krocích:

1. Zaměření analýzy rizik slouží k pozdějšímu rozhodování o volbě metody (strategie) vlastní analýzy rizik konkrétní firmy. Nejprve je provedena indikativní analýza rizik s cílem posoudit, které z objektů (problémy, systémy, aktiva atd.) jsou pro činnost společnosti stěžejní, a které jsou vystaveny významným rizikům.

2. Pro tyto objekty by pak měla být provedena podrobná analýza rizik pomocí jedné nebo obou výše uvedených metod, přičemž kombinace metod je pravděpodobně nejvhodnější, ale zároveň nejdražší a časově nejnáročnější. (Smejkal, 2010, s. 109)

2.4.1 Strategické nástroje analýzy

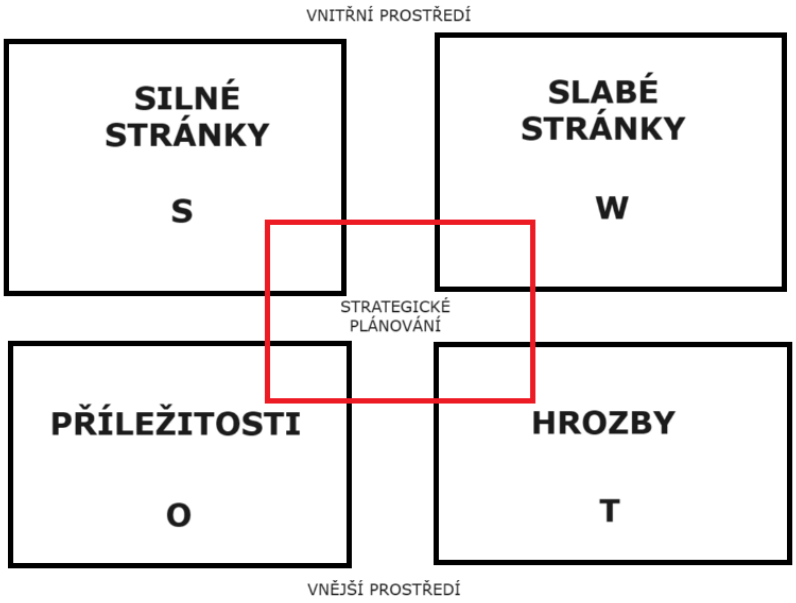
Strategické nástroje analýzy podnikatelského prostředí, jsou například analýza SWOT, SLEPTE analýza, které jsou klíčové pro identifikaci vnějších a vnitřních rizik v podnikatelském prostředí. Kombinace těchto nástrojů poskytuje komplexní přehled o podnikatelském prostředí a umožňuje lepší přípravu na případná rizika. Analýzou těchto aspektů může společnost

identifikovat klíčové faktory, které by mohly ohrozit její stabilitu nebo ziskovost, a přijmout opatření k minimalizaci těchto rizik.

SWOT analýza

SWOT analýza je vícerozměrný nástroj strategické analýzy. Identifikuje vnitřní faktory organizace (silné a slabé stránky) a její vnější faktory ve vztahu k jejímu okolí (slabé stránky a hrozby). Umožňuje také organizacím upřednostňovat faktory z hlediska očekávaného dopadu, ať už pozitivní (silné stránky a příležitosti) nebo negativní (slabé stránky a hrozby). SWOT analýza nemá žádnou vnitřní hodnotu, pokud není použita pro strategické účely.

SWOT analýza zkoumá současnou situaci organizace v určitém okamžiku v budoucnosti, nikoli zpětně. Kromě toho je struktura analyzována s ohledem na budoucí perspektivy. SWOT analýza se zároveň zaměřuje na vnitřní funkčnost (silné a slabé stránky) a vnější prostředí (příležitosti a hrozby) organizace. Silné stránky jsou prvky organizace, které pozitivně ovlivňují její rozvoj a konkurenční pozici. Obecně jsou silné stránky považovány za zvláště důležité, protože neovlivňují konkurenci. SWOT analýza určuje konkurenční výhody podniku oproti jeho konkurentům.



Obrázek 4:SWOT analýza (Zdroj: vlastní zpracování)

Slabé stránky souvisejí také s vnitřním fungováním organizace, ale obecně mají negativní dopad na její rozvoj a konkurenční pozici. Schopnost jasně identifikovat vnitřní slabé stránky organizace je zásadní: umožňuje zlepšit příslušné problémy a nasměrovat práci tak, aby byly

méně zranitelné. Příležitosti organizace závisí na příležitostech dostupných ve vnějším prostředí. Mohou být použity ke zlepšení postupu a konkurenční pozice. Jakmile to udělají, mohou se stát silami, které pozitivně ovlivňují rozvoj organizace. Hrozby přicházejí i z vnějšího prostředí organizace. Jejich identifikace je často výsledkem tradiční strategické práce. Když jsou hrozby odhaleny včas, lze je lépe předvídat a snížit jejich dopad na výkon (a naopak).

Někdy se hrozby mohou stát silnou stránkou. Stejně tak se příležitosti mohou stát slabinami. Protože se organizace nevyvíjí pouze ve svém prostředí, její budoucnost závisí také na rozhodnutích jejích konkurentů. (50Minutes.com, 2015, s. 6-7)

McKinsey model 7 S

McKinseyho model 7 S k integrované strategii rozvíjí sedm témat, z nichž každé začíná písmenem S, jsou to: strategie, struktura, systémy, styl vedení, spolupracovníci, schopnosti, sdílené hodnoty a celkové cíle. Zkušenosti pro velké společnosti naznačují, že strategie založená na těchto otázkách bude komplexní a efektivní.

Strategie

Strategie sama o sobě označuje prostředky, kterými společnost dosahuje svých cílů. Je založena na kombinaci možností založených na zdrojích a trhu. Strategie by měla zohledňovat a být v souladu s tržními podmínkami společnosti, potřebami zákazníků a konkurenčními aktivitami.

Struktura

Struktura se zabývá celkovou organizací společnosti, koordinací jejích funkčních celků a způsobem, jakým zapadá do jejího prostředí. Organizační strukturu ve společnosti dělíme na pět základních forem:

- Liniová – má pouze jeden nadřazený útvar.
- Funkcionální – jsou zde specialisté pro jednotlivé oblasti činnosti. Jedno oddělení má několik oddělení vyšší úrovně.
- Liniově-štábní – zde se spojuje liniová a funkcionální struktura.
- Divizní – člení divize dle zeměpisného umístění, typů kupujících nebo dle výroby.
- Maticová – kombinace divizní a funkcionální struktury.

Systémy

Obchodní systémy jsou postupy a rutiny pro správu a využívání jejich zdrojů. Zahrnuje zde také systémy vyššího řádu. Dále se zde definuje řízení společnosti, pravost a aktuálnost dokumentů a zpětná vazba.

Styl vedení

Styl obecně označuje přístup společnosti, který je ztělesněn v jejím poslání. Obzvláště důležitým prvkem je styl vedení vrcholových manažerů, který řeší pracovní prostředí společnosti, efektivnost vedení, korektnost a rychlost rozhodnutí. Styl vedení rozdělujeme do tří typů:

- Autokratický – kdy absolutní kontrolu má pouze manažer.
- Demokratický – zde mají možnost se vyjadřovat v rámci podnikovém rozhodování i zaměstnanci.
- Laissez-faire – manažer pracovníkům dává volnost a každý dělá, to, co umí.

Spolupracovníci

Do této podkapitoly spadá především specializace pracovníků, motivace a také personální management. Výběr nových zaměstnanců, kvalifikace a možnosti osobního rozvoje zaměstnanců.

Schopnosti

Lidé využívají své dovednosti a znalosti k vytváření, rozvoje a implementace strategie. Tyto schopnosti určují nejsilnější a nejlepší vlastnosti podniku. Měření dovedností zaměstnanců vede ke zjištění dostatečnosti kvalifikace zaměstnanců a zjištění potencionálních cest k jejich zlepšení.

Sdílené hodnoty

Firemní kultura a etika definuje základní hodnoty společnosti, stav a vývoj firemní kultury a povědomí zaměstnanců o vizi a poslání společnosti. (Wickham, 2000, s. 22)

PESTLE analýza

Analýza vnějšího prostředí okolí je považována za obecnou a vztahuje se na všechny organizace. Jedná se o analýzu vzájemně souvisejících společenských trendů, analýzu ekonomických, legislativních, politických a politických trendů, analýzu technických a environmentálních trendů, pokud mají vliv na podnik. PESTLE analýza (někdy označované jako SLEPTE, nebo zkráceně SLEP, PEST. Tento přístup identifikuje klíčové trendy a vlivy a zajímá se o to, jaké vnější vlivy ovlivňují různé organizace a jaké budou rozdíly. Analýza má vyvolat další navazující a podobné otázky a hledat na ně odpovědi: Jaké možné vývojové trendy důležitých

faktorů v základní oblasti životního prostředí jsou v budoucnu možné? Jaké jsou základní impulsy pro změnu, tedy jaké aktéry změnu přivodím? Jaký dopad budou mít v budoucnu? Budou intenzivnější nebo naopak? Jaký možný dopad lze očekávat, že tyto změny budou mít na organizaci? Jaký dopad to bude mít na konkurenční pozici? Jaký dopad budou mít očekávané změny na strategii společnosti?

Analýza PESTLE pokrývá celou řadu vlivů prostředí na organizaci. I když je však možné předvídat určitý směr, často není jasné, jaký dopad bude mít na danou organizaci. V tomto případě je již identifikace vlivů přínosná při přípravě podniku na určité potenciální změny. (Mallya, 2007, s. 41-42)

Politické faktory

Politicko-legislativní (právní) faktory určují pravidla pro podnikatelskou činnost. Jsou to jak instituce, tak zákony. Mezi politické faktory patří především: typ vlády a její stabilita, svoboda tisku, míra byrokracie a korupce. Regulace a deregulace ekonomiky její trendy a pravděpodobné změny politického prostředí. Zákon představuje pravidla, která stát stanovuje a vymáhá. (Dvořáček, 2012, s. 10)

Ekonomické faktory

Ekonomické faktory jsou rozhodující pro úspěch organizace a lze je pokládat za nejpodstatnější. Mezi kritické ekonomické faktory patří faktory související s věkem, věkovou strukturou, úrovní příjmu, disponibilním, aspekty chudoby, příjmem země, mírou zaměstnanosti a nezaměstnanosti, daňovými sazbami, mírou inflace, rozdělením pohlaví, směnnými kurzy, růstem populace a mírou gramotnosti, postoje zákazníků, úroveň vzdělání vnímání a nákupní chování atd. Když jsou ekonomické podmínky příznivé, je zajištěno riziko přežití, a když jsou ekonomické podmínky nepříznivé, průmysl je neatraktivní pro nové investice, růst a přežití. Zákazníci jsou králem byznysu. Nákupy zákazníků určují jádro organizace, cílem je zisk.

Sociální faktory

Je třeba vzít v úvahu tradice, kulturní aspekty, normy, mýty, náboženské hodnoty a náboženské přesvědčení. Je třeba vzít v úvahu etické hodnoty, vnímání a postoje k podnikání a průmyslu na provozním trhu. Například pohřební služby, prostituce a drogy mohou být legální, etické a podporované v podnikatelském prostředí, ale nemůžou být podporovány v jiném. Podnikatelské prostředí je spojeno s kulturními a tradičními hodnotami země, a proto je přizpůsobení se těmto kulturním hodnotám důležité pro vyšší produktivitu, lepší výkon a dosažení cílů růstu. Nákupní a spotřebitelské chování je navíc utvářeno sociokulturními faktory

prostředí, které mají velký význam. Při vývoji mixu produktů nebo služeb by měly být brány v úvahu i environmentální aspekty (Perera, 2018, s. 9-12)

Technologické faktory

Technologické faktory (neboli inovační faktory) představují trendy ve výzkumu a vývoji, je to rychlost technologických změn, výroba, přeprava, skladování, komunikace, informační, sociální technologie atd. Technologické prostředí a jeho změny jsou zdrojem technologického pokroku pro společnosti. To jim umožňuje dosahovat lepších ekonomických výsledků, zvyšovat konkurenceschopnost a humanizovat práci. (Jakubíková, 2013, s. 101)

Legislativní faktory

Právní předpis je soubor obecně závazných právních norem, které jsou součástí právního řádu. Předpisy zahrnují zákony. Právní předpisy jsou výrazem výkonu veřejné moci, jejímž prostřednictvím vzniká nebo se uplatňuje právo. Zákon je obecně závazným předpisem vydaným zákonodárnou mocí, na zákon se však vztahují ústavní zákony a jim rovnocenné mezinárodní smlouvy. Zákon má přednost před předpisy (vyhlášky a nařízení). Obecně závazná nařízení vydávají orgány územní samosprávy, které představují úplný pramen práva, naproti tomu záležitosti vydávané ústředními orgány jsou prováděcími předpisy a jsou omezeni ustanoveními zákona, který provádějí. (Dvořáček, 2012, s. 11)

Environmentální faktory

Faktory ekonomické/environmentální v nynější době nabývají na významu. Jejich relevance se odráží ve vzniku koncepce celkově udržitelného rozvoje, ve vytváření ekologických a dalších standardů souvisejících s kvalitou života. Vliv činnosti firem na životní prostředí je sledován právě proto, že si začínáme uvědomovat nevratnost některých škodlivých zásahů do přírodního prostředí a možnou hrozbu vyčerpání intenzivně využívaných přírodních zdrojů. Zeměpisné
a klimatické podmínky rovněž ovlivňují spotřebitelské a obchodní trhy. (Zamazalová, 2009, s. 52)

2.5 SOUČASNÝ STAV V BANKOVNICTVÍ

V této podkapitole současného stavu jsem popsala aktuální hlavní principy řízení rizik a strategii řízení rizik ve vybrané bankovní instituci.

2.5.1 Hlavní principy řízení rizik

Hlavní funkcí systému řízení rizik ve vybrané instituci je přispívat k optimalizaci celkové ziskovosti banky ve vztahu k podstupovanému riziku a zároveň zajistit kontinuitu implementací vhodného přístupu k řízení rizik. Banka se zabývá různými činnostmi a trhy, často s velmi odlišnými charakteristikami, ale všechny zahrnují převzetí rizika. Proto je důležité zdůraznit základní principy, které by měly být základem všech obchodních rozhodnutí a rozhodnutí o řízení rizik za všech okolností.

Banka pravidelně analyzuje rizika, kterým je vystavena. Systém řízení rizik musí odpovídat povaze, rozsahu a složitosti činností a souvisejících rizik, aby poskytoval nezkreslený obraz podstupovaného rizika. Proces identifikace rizik musí zahrnovat všechny činnosti a všechny úrovně řízení a organizace, aby bylo možné odhalit nová, dříve neidentifikovaná rizika. Řízení rizik musí zohledňovat vnitřní i vnější faktory, včetně budoucí strategie banky, vlivu ekonomického prostředí a cyklů a regulatorních požadavků. Řízení rizik musí brát v úvahu kvantitativní a kvalitativní aspekty rizika, skutečné možnosti kontroly rizik a náklady/přínosy spojené s jejich kontrolou.

Banka nastavuje procesy pro identifikaci, vyhodnocování nebo měření, sledování, vykazování a případně omezování rizik prostřednictvím limitního systému. Banka zavádí systém limitů, které slouží k řízení rizik, včetně procesů a informačních toků při jejich překročení. Všechny strategie, procesy a limity řízení rizik související s řízením rizik jsou pravidelně revidovány a odpovídajícím způsobem upravovány.

Systém limitů pro snižování rizik, včetně požadavků na strukturu aktiv, pasiv a podrozvahových položek, schvaluje představenstvo banky, jím určený výbor nebo v rámci platných schvalovacích delegací v závislosti na povaze rizik. Pro banku se akceptovatelná míra rizika odráží v systému schválených limitů, ve stanovení kritérií pro řízení a omezování jednotlivých typů rizik a v navazujících směrnicích pro řízení kapitálu.

Banka musí zajistit, aby všichni zaměstnanci, jejichž činnost má vliv na řízení rizik, byli dostatečně seznámeni se strategií řízení rizik tak, aby svou činnost vykonávali v souladu s touto strategií, z toho vyplývajícími postupy a omezeními.

Stanovuje zásady kontrolních mechanismů a činností v oblasti řízení rizik k ověřování dodržování stanovených procesů a limitů a k ověřování výsledků hodnocení nebo měření rizik.

Banka musí mít dostatečný kapitál na krytí rizik, kterým je nebo může být vystavena. Strategie a procesy řízení rizik, stejně jako strategie a procesy pro generování a udržování kapitálu k pokrytí rizik, jsou komplexní a vzájemně propojené.

2.5.2 Strategie řízení rizik

Tato strategie platí pro všechny zaměstnance banky, kteří se podílejí na činnostech generujících riziko. Strategie se vztahuje na všechny typy rizik, které banka řídí.

Vybraná bankovní instituce důsledně řídí následující rizika:

Oblast strategie

- strategické riziko a obchodní riziko,
- systémové riziko,

Oblast úvěrování a protistran

- úvěrové (kreditní) riziko, riziko kreditní koncentrace, riziko nákazy,
- riziko spojené se správou zajištění a zatížením aktiv,
- riziko operací, ve kterých je zapojen jiný než členský stát, riziko operací s osobami poskytujícími finanční služby obdobné bankovním, nad nimiž není vykonáván dohled,
- riziko vlivu politického prostředí (kromě rizik politického prostředí ČR) – součást rizika země,

Oblast tržní

- tržní riziko, riziko tržní infrastruktury,
- riziko likvidity,
- riziko spojené se zdroji kapitálu a financováním,
- riziko nadměrné páky,

Oblast operační a compliance

- operační riziko,
- reputační riziko,
- ESG riziko (environmentální, sociální, správní),
- riziko vlivu regulatorního prostředí,

- riziko nestandardních operací, riziko operací, ve kterých je nebo by mohla být zapojena netransparentní nebo jinak potenciálně riziková protistrana nebo zeměpisná oblast,

Strategie řízení rizik zahrnuje všechny činnosti, produkty, procesy a typy zákazníků, protistran či třetích stran – neklienty banky (ručitelé, vkladatelé, dodavatelé, akcionáři atd.), které mohou vést ke vzniku rizik.

3 FORMULACE PROBLÉMŮ A STANOVENÍ CÍLŮ ŘEŠENÍ

Tato diplomová práce řeší řízení operačních rizik v bankovnictví, která jsem vyhodnotila studiem interních dokumentů instituce. Bankovní instituce, kterou jsem si pro zpracování diplomové práce zvolila je právnická osoba se sídlem v České republice, založená jako akciová společnost. V České republice patří mezi jednu z největších bankovních institucí. Vybraná bankovní instituce, je součástí nadnárodní skupiny, která sídlí v zahraničí. Banka svým klientům nabízí následující služby: Přijímá vklady od veřejnosti, poskytuje krátkodobé, střednědobé a dlouhodobé úvěry. Umožňuje svým klientům ukládat jejich finanční prostředky na vytvořené bankovní účty a poskytuje jim přístup k těmto prostředkům pomocí platebních karet či šeků. Klient si zde může uložit své investice na vybrané investiční fondy s jistým zhodnocením. Správa penzijních fondů a pojištění. V rámci pokladních služeb může klient využít, proměnění hotovosti či výměnu bankovek na cizí měnu.

Na základě již zmíněné analýzy interních dokumentů jsem vyhodnotila operační riziko jako riziko s největším dopadem na vybranou instituci. Těmito zmíněnými operačními riziky se práce nadále zaobírá. Problém je řešen pomocí nejvhodnějších metod a postupů a vypracováním navržených opatření k minimalizaci těchto rizik.

Hlavní cíl

Cílem práce je identifikace, analýza a hodnocení operačních rizik ve zvolené bankovní instituci, včetně návrhu opatření vedoucích ke snížení rizik.

Dílčí cíle

K naplnění hlavního cíle jsou definovány následující cíle dílčí práce

- Analýza teoretických východisek práce souvisejících s řízením rizik
- Identifikace hrozeb a scénářů v řízení rizik
- Vyhodnocení operačních rizik
- Návrh opatření k minimalizaci rizik
- Návrh strategie operačních rizik

Zpracováním těchto dílčích cílů v rámci této diplomové práce bude dosáhnuto hlavního cíle. Výsledky práce by měly obsahovat určitý přínos pro vedení společnosti a její risk management v neposlední řadě i pro další rozvoj a opatření rizik ve vybrané bankovní instituci.

4 POUŽITÉ METODY A JEJICH ZDŮVODNĚNÍ

Operační riziko je jakákoliv událost s lidským pochybením, nedostatečností systémů nebo nevhodností nastavených procesů či souvisejících s externí událostí. Identifikace a klasifikace rizika proběhla na základě studia interních dokumentů instituce, které obsahuji identifikaci jednotlivých rizik s ohledem na její finanční dopad. Mezi operační rizika patří obchodní spory, spory s veřejnými orgány, chyby v odhadu rizika nebo ocenění, chyby při provádění pokynů, podvody, nepovolené obchodování, ztráty obchodování, ztráta provozního prostředí či poruchy systémů.

Pro komplexní pohled na vybranou bankovní instituci jsem vypracovala v rámci strategické analýzy metodu Pestle. Tato analýza umožňuje posouzení faktorů, které ovlivňují bankovní instituci z vnějšího okolí. Hodnotí politické, ekonomické, sociální, technologické, legislativní a ekologické faktory. Na analýzu Pestle jsem navázala vypracováním McKinseyho modelu 7 S, která hodnotí především vnitřní faktory. Metoda hodnotí sedm hlavních aspektů: struktura, strategie, systémy, spolupracovníci, schopnosti, styl vedení, sdílené hodnoty. Tato analytická metoda je využita pro hodnocení kritických faktorů organizace.

Pro identifikaci hlavních operačních rizik jsem použila metodu RIPRAN. Tato metoda poskytuje detailnější a komplexní pohled na vybraná operační rizika a jejich možnost řešení. V rámci této metody jsem prvně určila její identifikační číslo a kategorii kam riziko v instituci spadá. Dále jsem popsala jednotlivé hrozby a jejich scénáře, které by mohly nastat. Dle tabulky hodnocení, která je popsána v teorii práce, jsem vypočetla hodnotu možného rizika a dopadu na vybranou bankovní instituci. Následně jsem zhodnotila stav rizik a zpracovala dílčí návrhy na opatření minimalizace rizika ve vybrané bankovní instituci.

5 VLASTNÍ ŘEŠENÍ VYBRANÉ PROBLEMATIKY

Tato kapitola je zaměřena konkrétně na operační riziko a použité metody hodnocení, s ohledem na studium interního dokumentu, který identifikuje a ohodnocuje rizika. Zde popisuji nejprve základní principy řízení operačních rizik vybrané bankovní instituci, a odpovědnost za jejich řízení. Následně jsem za pomocí analýz vnějšího a vnitřního prostředí a metody RIPRAN identifikovala jednotlivé kategorie operačních rizik a jejich nejčastější hrozby. Poté jsem vyhodnotila pravděpodobnost, dopady a celkovou hodnotu rizika. Pro minimalizaci hodnot jednotlivých operačních rizik jsem navrhla opatření a přiřadila odpovědné úseky za zajištění. V neposlední řadě jsem zde zmínila i návrhy strategie operačních rizik pro vybranou instituci. Zmíněné použité metody jsou vypracovány na závěr této kapitoly.

5.1 ZÁKLADNÍ PRINCIPY ŘÍZENÍ OPERAČNÍCH RIZIK

Operační riziko je riziko ztráty vyplývající z nedostatečnosti nebo selhání vnitřních procesů a systémů, lidské chyby nebo důsledku externí události. Operační rizika nezahrnují strategická a obchodní rizika. Spíše se zde počítá i s právními a reputačními riziky.

V kontextu řízení operačního rizika se reputační riziko týká poškození dobrého jména banky v důsledku negativních mediálních zpráv. Reputační rizika mohou mít vnitřní příčinu, např. problematické soudní spory, nebo vnější příčinu, např. pomluvu.

Strategické riziko je riziko vyplývající ze špatného strategického obchodního rozhodnutí. Obchodní riziko je riziko, že banka nebude schopna udržet plánované marže a objemy z důvodu nepříznivých ekonomických podmínek nebo zvýšené konkurence na trhu.

Inherentní operační riziko je považováno za operační riziko procesu (nebo systému, lidské chyby, externí události) před zavedením kontrolních nebo preventivních mechanismů. Jedná se o riziko vlastní danému procesu (nebo systému, lidské chybě, externím událostem). Jediným způsobem, jak toto riziko snížit, je omezit provádění daného procesu (resp. systém nepoužívat, snížit počet pracovníků). Inherentní operační riziko externích událostí nelze zásadně snížit.

Reziduální operační riziko představuje operační riziko, které banka podstupuje po zavedení kontrolních nebo preventivních mechanismů.

Tento přístup předpokládá, že operační riziko je chápáno jako zvláštní kategorie rizik a musí být specificky identifikováno, hodnoceno, sledováno a kontrolováno, aby bylo možné navrhnout vhodná opatření ke snížení tohoto rizika.

5.2 ODPOVĚDNOST ZA ŘÍZENÍ OPERAČNÍCH RIZIK VE VŠECH ÚTVARECH BANKY

Vedoucí útvarů odpovídají za řízení operačních rizik v souladu s vymezením odpovědnosti a zaměření činností útvarů, které vedou, v souladu s příslušnými pokyny nebo jinými vnitřními předpisy.

Mezi jejich povinnosti patří:

- Identifikovat a vyhodnocovat inherentní operační rizika v jejich procesech, postupech, činnostech a systémech sledováním vhodných ukazatelů, jejichž rozsah a povahu určuje každý vedoucí oddělení.
- Navrhovat způsoby, jak snížit reziduální operační riziko: po posouzení závažnosti inherentního operačního rizika musí být vedoucí příslušného oddělení schopen po důkladné analýze zodpovědně a svědomitě rozhodnout, zda lze riziko nějakým způsobem řídit nebo ne.

V případě, že riziko nelze kontrolovat, je třeba rozhodnout o jeho odstranění z banky, nebo omezení činnosti nebo zvážit přijetí daného či souvisejícího rizika.

Pokud lze riziko kontrolovat, je odpovědností vedoucího příslušného oddělení navrhnout a zavést takové kontrolní nebo preventivní mechanismy (tvorba akčního plánu), které účinně snižují riziko bez vynaložení neúměrných nákladů. Mezi tyto mechanismy patří zejména oddělení neslučitelných pravomocí, nastavení a dodržování limitů, chráněný přístup do budov a systémů banky, identifikace neobvyklých výsledků obchodních útvarů, identifikace neobvyklých transakcí na účtech, pravidelná kontrola a odsouhlasení účetních záznamů, školení podřízených zaměstnanců a dalších.

Hlavním zájmem by mělo být dosažení co nejnižší úrovně reziduálního operačního rizika. Každé rozhodnutí o kontrole, odvození nebo přijetí rizika by mělo být jasně zdokumentováno.

- Sledování a vyhodnocování efektivity systému řízení operačních rizik. Rozsah pravidelného monitorování musí být úměrný závažnosti příslušného reziduálního operačního rizika a také zohledňovat možné změny prostředí. Tato činnost musí být úzce propojena s každodenním procesem řízení rizik. Součástí tohoto sledování je i proces permanentní kontroly.

V souvislosti se zaváděním nových procesů, postupů, činností nebo systémů je vedoucí odboru odpovědný za implementaci povinen zajistit vyhodnocení možných operačních rizik.

Pokud dojde ke změně s významným dopadem na velikost operačního rizika, je nutné o této změně informovat výbor pro operační rizika.

U nových produktů a projektů musí být odbor operačních rizik informováno o možných operačních rizicích prostřednictvím popisů nových produktů, které jsou předkládány výboru pro nové produkty v korporátním a retailovém bankovnictví nebo výboru pro nové produkty v investičním bankovnictví.

5.3 IDENTIFIKACE RIZIK

V této části práce jsem zpracovala analýzy vnějšího a vnitřního prostředí vybrané bankovní instituce. Pro analýzu vnějšího prostředí instituce jsem zvolila Pestle analýzu. Tato analýza umožňuje komplexní pohled na vnější faktory, které ovlivňují vybranou bankovní instituci. Tato analýza popisuje šest hlavních faktorů, které ovlivňují vybranou instituci. V rámci analýzy vnitřního prostředí jsem zpracovala metodu McKinseyho modelu 7 S, která popisuje sedm hlavních faktorů strategie řízení uvnitř instituce. Dále za pomocí metody RIPRAN jsem identifikovala a ohodnotila pravděpodobnost, dopad a celkovou hodnotu rizika ve vybrané bankovní instituci.

5.3.1 PESTLE analýza

V Pestle analýze popíši vnější faktory ovlivňující vybranou bankovní instituci a řízení rizik v bankovním sektoru v České republice.

Politické/právní faktory

Dohled nad kapitálovým trhem podle zákona o České národní bance zahrnuje rozhodování o žádostech o vydání licence, povolení, registrace a předchozího souhlasu podle zvláštního právního předpisu, jakož i kontrolu dodržování podmínek uvedených ve vydaných licencích, jakož i kontrolu dodržování podmínek stanovených ve vydaných licencích. Povolení, kontrola dodržování zákonů, které je ČNB oprávněna kontrolovat podle zákona nebo zvláštního právního předpisu, kontrola dodržování předpisů a opatření vydaných ČNB, získávání informací nezbytných pro výkon dohledu a jeho prosazování, kontrola jejich správnosti, úplnosti a včasnost, ukládání opatření k nápravě a sankcí i řízení o přestupcích a správních deliktech.

Poskytovatelé služeb kapitálového trhu vytváří rámec pro podnikatelskou činnost v rámci regulace kapitálového trhu. Jednání účastníků kapitálového trhu upřesňuje zejména zákon č. 240/2013 Sb., o investičních společnostech a investičních fondech, a zákon č. 256/2004 Sb., o podnikání na kapitálovém trhu, ve znění pozdějších předpisů. ČNB na základě zmocnění

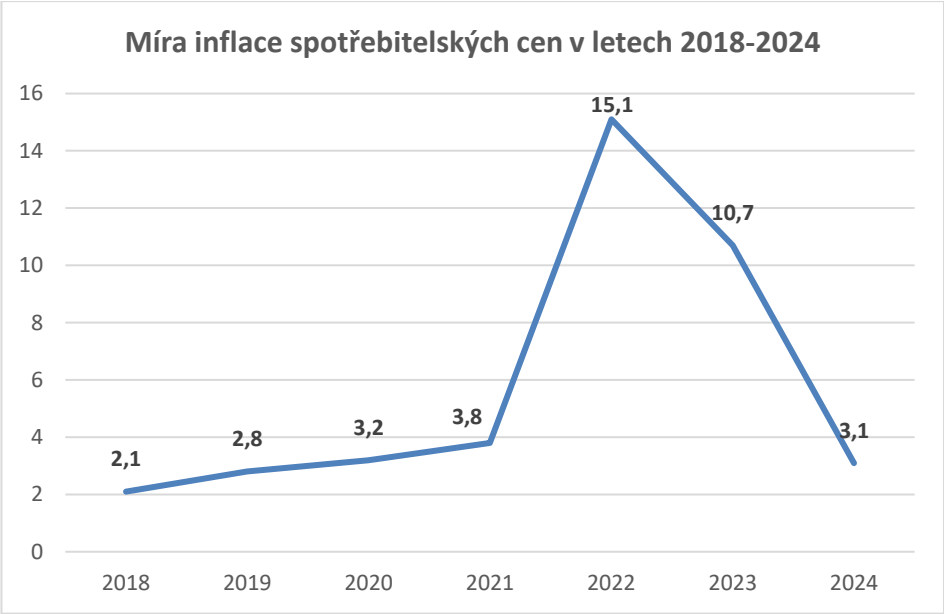
ve zmíněných zákonech vydává vyhlášky, které stanovují především užší podmínky přístupu na kapitálový trh, pravidla dohledu, pravidla pro jednání s investory a zákazníky a pravidla transparentnosti trhu (právní základ). (Česká národní banka, 2022)

Ekonomické faktory

Makroekonomická prognóza je zatížena řadou rizik, která se celkově považují za zkreslená. Ekonomická aktivita, zejména v některých odvětvích hospodářství, může být ovlivněna obnovenými poruchami v dodavatelských řetězcích, například v souvislosti se situací na Blízkém východě. Kromě negativního dopadu na ekonomickou výkonnost by problémy na straně nabídky vytvořily další inflační tlaky. Ty by mohly být způsobeny i zvýšením cen energetických komodit
v případě eskalace geopolitického napětí.

Riziko pro českou ekonomiku představuje také vývoj inflace a inflačních očekávání. Nadhodnocení cen bydlení, na druhou stranu však může mít pozitivní dopad na mimořádný nárůst úspor domácností v posledních letech, který by mohl pomoci působit proti účinkům inflace zmírněním spotřeby.

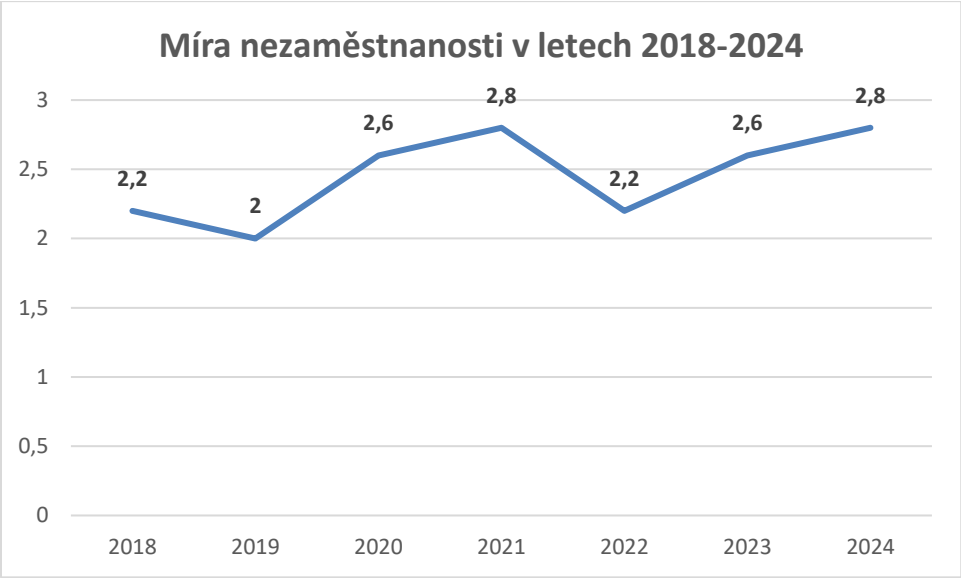
Mírný růst domácí ekonomiky bude v letošním roce tažen především domácí poptávkou. Investiční aktivita v soukromém i veřejném sektoru byla patrná již v loňském roce, přičemž celkové investice v podobě tvorby hrubého fixního kapitálu již v polovině roku 2023 dosáhly úrovně před pandemií. V letošním roce se tempo růstu investic podle odborníků mírně zrychlí, k čemuž pravděpodobně pomůže postupné snižování nákladů na financování v důsledku klesajících úrokových sazeb. Současná slabá výkonnost české ekonomiky se zásadně neprojevuje na trhu práce, předpokládá se, že nárůst nezaměstnanosti bude nízký. To znamená, že tempo růstu nominálních mezd by mělo letos stoupnout na sedm procent, s výrazně nižší inflací.



Graf č. 1:Míra inflace spotřebitelských cen v letech 2018-2024 (Zdroj: Ministerstvo financí ČR)

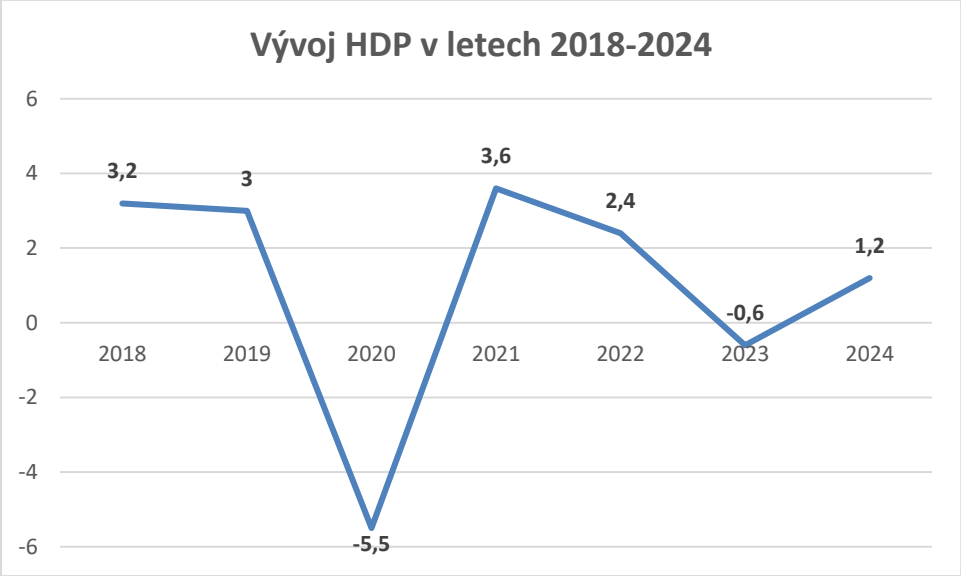
Vysoká inflace minulý rok zbrzdila ekonomický růst a snížila životní úroveň obyvatel. V roce 2023 dosáhla průměrná míra inflace 10,7 %. Ve srovnání s předchozím rokem inflace v loňském roce rychle klesla, ale ve čtvrtém čtvrtletí vzrostla díky srovnávacímu efektu tarifu úspory energie. V letošním roce se očekává meziroční inflace po většinu roku pod 3 %. Zahraniční nabídkové faktory podporující inflaci výrazně oslabily a tlaky domácí poptávky budou v průběhu roku potlačovány vyššími měnově politickými sazbami, k čemuž přispívá i efekt fiskálního konsolidačního balíčku. Průměrná míra inflace by proto měla letos klesnout na 3,1 %.

Od začátku roku 2024 bude inflace meziročně rychle klesat. Prognóza vybrané banky předpokládá, že klesne dokonce pod 3 % a vrátí se tak do tolerančního pásma ČNB. Zůstane však nad 2 % cílem. Po loňských 10,7 % se letos očekává průměrně 2,7 %.



Graf č. 2: Míra nezaměstnanosti v letech 2018-2024 (Zdroj: Ministerstvo financí ČR)

Trh práce nadále vykazuje nerovnováhu v důsledku nedostatku pracovních sil. Proto je nepravděpodobné, že by míra nezaměstnanosti v roce 2024 prudce vzrostla, a to i přes slabou ekonomickou dynamiku. Z odhadovaných 2,6 % v roce 2023 se očekává, že letos vzrostou na 2,8 %. Pokračující napětí na trhu práce nedovolí výrazně zpomalit růst mezd.



Graf č. 3: Vývoj HDP v letech 2018-2024 (Zdroj: Ministerstvo financí ČR)

V roce 2023 poklesl hrubý domácí produkt o 0,6 %. Reálná spotřeba domácností klesala, protože se potýkaly s vysokou inflací. Investiční činnost je ovlivněna ekonomickými spory a restriktivními měnovými podmínkami v zemích eurozóny. Naopak pozitivní dopad mají výdaje státního ústavu a projekty spolufinancované z fondů EU institucionálního sektoru a z předešlé finanční perspektivy. Ekonomiku velmi zbrzdila slabší tvorba zásob při porovnání s předešlým

rokem, zvláště ve spojitosti s ukončením běžné výroby. Odstranění problémů v dodavatelských řetězcích vede ke zvýšení exportu, ale import setrvá potlačený vůči celkové nízké domácí poptávce. V rámci poklesu reálného HDP o 0,4 % v minulém roce, se nyní počítá v letošním roce růst o 0,8 %. Tím by se měla Česká republika dostat na úroveň před pandemií v roce 2019. Hodnot jako v roce 2019 ČR dosáhne jako poslední země z EU. S počátkem letošního roku by měli firmy a domácnosti dosáhnout na vládní konsolidační balíčky. (Ministerstvo financí České republiky, 2024)

Sociální faktory

V rámci sociálních faktorů působících na bankovnictví existuje kampaň, která se zaměřuje na klíčové finanční dovednosti potřebné pro život a zdravé finanční návyky. Především studující a sociálně znevýhodněné skupiny obyvatelstva jsou hlavními cílovými skupinami GMW – (Global Money Week) neboli Globálního týdnu peněz. Zúčastnit se této kampaně může prakticky každý, kdo má o finanční vzdělávání zájem. Národním koordinátorem GMW v ČR je Ministerstvo financí, záštitu nad akcí převzalo Ministerstvo školství, mládeže a tělovýchovy a Česká národní banka.

Tento připravovaný program podporuje společnost yourchance o.p.s. a EFPA ČR, která je akreditovaná ČNB pro pořádání zkoušek odborné způsobilosti pro makléře, osoby, které zajišťují distribuci pojištění, finanční a investiční poradce. Program Globální týden peněz, se uskuteční po celé České republice. Tento program poskytne zájemcům možnost zúčastnit se série přednášek, interaktivních diskusí s odborníky, workshopů, také zde bude možnost zúčastnit se her a soutěží, které budou zaměřeny především na rozvoj zdravých finančních návyků a finanční gramotnosti. Cílem programu je především mladým lidem rozšířit podvědomí o finanční gramotnosti, rozvíjet postoje a dovednosti, které jsou potřebné v každodenním životě, a aby prováděli odpovědná a správná finanční rozhodnutí.

		Index FG	
Rok 2022		56	
Rok 2023		56	Rok 2022
Pohlaví	Muž	58	60
	Žena	55	52
Věk	18 – 34	50	51
	35 – 49	58	56
	50 – 64	58	58
	65 a více let	59	58
Vzdělání	ZŠ, Vyučen/a	47	48
	Maturita	56	56
	VOŠ, VŠ	64	62
Region	Praha	57	59
	Čechy	57	56
	Morava	56	55

Obrázek 5: Index Finanční gramotnosti (Zdroj: (Česká bankovní asociace, 2023))

Na výše vyobrazeném obrázku, vidíme hodnoty indexu finanční gramotnosti rozdělení podle pohlaví, věku, vzdělání, regionu. Index finanční gramotnosti dosáhl v roce 2023 výše 56 bodů, stejně jako v roce 2022. Lidé si své peníze více chrání a projevují zájem je lépe zhodnotit. Častější je převod prostředků na spořicí účty nebo investice. (Ministerstvo financí, 2023)

Technické faktory

Česká národní banka (ČNB) si je vědoma potenciálu inovací založených na využití digitálních technologií zefektivnit fungování všech sektorů finančního trhu, zlepšit poskytování finančních služeb a přispět ke stabilnější a odolnější ekonomice České republiky. ČNB se proto rozhodla zřídit nový specializovaný komunikační kanál pro přijímání dotazů od všech účastníků finančního trhu souvisejících s finančními inovacemi. Jednoduše nazvala tento nový kanál jednotným kontaktním místem pro finanční technologie. Cílem vytvoření kontaktního místa je podpora zavádění inovativních technologií na český finanční trh prostřednictvím aktivnější komunikace s účastníky trhu nebo zájemci o vstup na něj. ČNB v současnosti neplánuje zřízení inovačního centra ani regulačního sandboxu.

Nejdůležitějším způsobem, jak tohoto cíle dosáhnout, je pružněji reagovat na relevantní otázky, které přímo souvisejí s finančními inovacemi. ČNB se obdobně jako v odpovědích na kvalifikované dotazy bude snažit poskytnout pomoc při řešení nejasných regulatorních otázek

(včetně licencování a dohledu) s cílem usnadnit plnění povinností, které jí ukládá regulace finančního trhu. Tazatelé při položení jejich dotazu by měli také vysvětlit, ve kterém konkrétně vidí souvislost mezi svými aktivitami a finančními inovacemi. Zejména by měli vysvětlit, v čem vidí rozdíl mezi popsaným technologickým řešením, obchodním modelem nebo jinými aspekty procesů, produktů nebo služeb, které jsou v daném okamžiku poskytovány nebo používány na tuzemském finančním trhu.

Na digitálních technologiích je nyní stále více závislá moderní společnost. S touto závislostí jsou především spojena rizika, která jsou důsledkem z rostoucí digitalizace. Kybernetické útoky způsobují nebezpečné škody, které paralyzují činnost demokratických států. Chránit informace, data a kritickou infrastrukturu je hlavní povinností České republiky. V rámci kybernetické bezpečnosti musíme věnovat maximální pozornost klíčovým oblastem. Existuje hned několik důvodu pro sestavení nového zákona. Tento zákon by měl odrážet praktické zkušenosti, které NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost získal za deset let práce s nynějším platným zákonem, reaguje na dynamický vývoj bezpečnostního prostředí, které se v posledních letech velmi změnilo, a dále zahrnuje ty změny, které přinesla evropská bezpečnostní směrnice NIS2. (Národní úřad pro kybernetickou a informační bezpečnost, 2023)

Legislativní faktory

Zákon č. 21/1992 Sb. Zákon o bankách

Zákon č. 6/1993 Sb. Zákon České národní rady o České národní bance

Zákon č. 89/2012 Sb. Zákon občanský zákoník

Zákon č. 634/1992 Sb. Zákon o ochraně spotřebitele

Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Zákon č. 370/2017 Sb. Zákon o platebním styku

Vyhláška č. 163/2014 Sb. Vyhláška o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry

Zákon č. 136/2011 Sb. Zákon o oběhu bankovek a mincí a o změně zákona č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů

Vyhláška č. 501/2002 Sb. Vyhláška, kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou bankami a jinými finančními institucemi

Zákon č. 424/2023 Sb. Zákon o požadavcích na přístupnost některých výrobků a služeb

Vyhláška č. 169/2011 Sb. Vyhláška o stanovení pravidel tvorby čísla účtu v platebním styku

Ekologické faktory

Udržitelné financování zohledňuje při investičním rozhodování ve finančním sektoru tzv. ESG faktory, přičemž tyto faktory představují faktory životního prostředí (E), sociální faktory (S) a faktory udržitelného podnikového řízení (G). Rozvoj udržitelného financování se odráží mimo jiné v řadě regulačních iniciativ EU, které mají za cíl přizpůsobit pravidla pro fungování finančních trhů. Téma regulace udržitelných financí přitom prolíná oběma sektorovými právními normami, jde také o nově vytvořenou úpravu, která v té době primárně upravuje oblast transparentnosti s ohledem na udržitelnost vlastností finančních produktů a dopad investiční aktivity společností na finančním trhu na udržitelnost. Pro oblast udržitelných financí jsou uvedeny vybrané relevantní materiály a právní předpisy. (Česká národní banka, 2023)

Do jednotlivých strategií finančních institucí se postupně promítají environmentální faktory. Většina společností při tvorbě firemní strategie zohledňuje environmentální rizika či příležitosti plynoucí z přechodu na ekologicky udržitelnou ekonomiku. V investiční strategii jsou zohledněny i environmentální faktory, kdy většina institucí očekává výrazný nárůst podílu ekologicky udržitelných aktiv ve svých portfoliích. Někteří z nich však vidí překážku v absenci těchto aktiv na trhu. (Česká národní banka, 2022)

5.3.2 McKinseyho model 7 S

Níže jsem vypracovala metodu McKinseyho modelu 7 S. Tato metoda, je založena na zkoumání vnitřního prostředí podniku, a proto rozvíjí sedm témat, z nichž každé začíná písmenem S, jsou to: strategie, struktura, systémy schopnosti, sdílené hodnoty, styl vedení, spolupracovníci.

Strategie

Cílem ve vybrané bankovní instituci je rozvoj organizace, postupů a prostředků, které umožní řešit mimořádné události a situace v podobě neplánovaných přerušení či omezení provozu banky, havárií včetně havárií informačního systému, selhání třetí strany důležité pro banku nebo poruchy externí infrastruktury. Tím je zajištěno dobré jméno banky, ochrana

zaměstnanců a klientů banky, jejího majetku, potřebná funkčnost a co nejrychlejší obnova zejména činností důležitých pro podnikání banky. V této souvislosti je zvláště důležitým cílem zajištění dodržování povinností vyplývajících z právních předpisů a předpisů orgánů dohledu v oblasti řízení operačního rizika. K zajištění těchto cílů banka zpracovává plány krizového řízení, plány kontinuity podnikání, havarijní plány obnovy fyzické infrastruktury a také plány zajištění obnovy informačních a komunikačních technologií nezbytných pro zajištění obnovy a dostupnosti služeb poskytovaných v informačních a komunikačních technologiích ve stanoveném čase. Tyto plány musí být pravidelně testovány, vyhodnocovány a podle potřeby aktualizovány.

Struktura

Struktura vybrané bankovní instituce, zahrnuje rozdělení odpovědností a pravomocí mezi oddělení a úrovně, ve kterých je řízeno operační riziko.

Oddělení operačních rizik předkládá členům výboru výsledky kvantitativního a kvalitativního sledování, které provádí odpovědné úseky, které jsou vyjmenovány výše ve vymezení odpovědnosti. Cílem je seznámit členy s hlavními operačními riziky banky. Stejně tak má každý člen výboru právo informovat ostatní členy o riziku, které považuje za významné.

Výbor se pak může rozhodnout, zda chce riziko projednat. V případě diskuse o riziku je za přípravu reakce na předložené závěry a za předložení těchto závěrů výboru odpovědný člen výboru, do jehož pravomoci příslušné riziko spadá. Tyto odpovědi by měly obsahovat zejména analýzu příčin daného rizika, analýzu nákladů na jeho snížení či odstranění a návrh řešení zohledňující náklady na snížení ve vztahu k výši očekávaných ztrát. Výbor pro operační rizika schvaluje veškerá strategická rozhodnutí související s operačními riziky a předkládá schválená rozhodnutí představenstvu vybrané bankovní instituce.

Odbor operačních rizik pravidelně zpracovává zprávu o operačních rizicích, která obsahuje aktuálně řešenou problematiku operačních rizik, analýzu ztrát banky z operačních rizik, včetně bližšího popisu významných ztrát, jakož i informace o úspěch pojistného programu.

Po schválení výborem, je tato zpráva předložena představenstvu banky, čímž je plněna informační povinnost vůči vedení vybrané bankovní instituce.

Tok informací mezi zaměstnanci útvaru operačního rizika a ostatními útvary banky je definován ve vnitřních předpisech navazujících na tuto politiku. Mezi odděleními postupuje nynějším způsobem:

Odbor operačního rizika spolu s výkonnými řediteli jednotlivých bankovních divizí jmenuje zástupce s koordinačními a komunikačními úkoly v oblastech řízení operačního rizika, tzv. SPOC (Single Point of Contact). Tato role zajišťuje komunikaci, výměnu informací, umisťování kontaktů, koordinaci plnění požadavků řízení operačního rizika včetně ověřování požadovaných výsledků.

Výkonní ředitelé vybraných oblastí banky jsou jednou ročně informováni oddělením operačních rizik o plánech a doporučeních pro budoucí vývoj operačních rizik obchodních oblastí s přehledem všech oblastí, které se jich týkají.

Odbor operačního rizika také pravidelně předem definovaným způsobem informuje mateřskou společnost vybrané bankovní instituce. Možné ztráty z operačních rizik jsou evidovány ve společném interním systému.

Systémy

V rámci systému řízení operačního rizika jsou definovány metody zpětné a prospektivní identifikace a hodnocení operačního rizika. Rizika označená jako podstatná jsou následně projednávána ve výboru pro operační rizika.

Mezi metody hodnocení operačních rizik patří:

- Sběr dat: Jedná se o sběr dat o událostech operačního rizika nad limit stanovený bankou. Rozsah sběru dat se postupně rozšiřuje o rizikové oblasti evidované bankou, které lze identifikovat např. pomocí definovaných KRI (Key Risk Indicators). Způsob sběru dat je definován v interním dokumentu společnosti.
- RCSA (Risk Control Self-Assessment): Cílem je určit úroveň reziduálního operačního rizika v celé bance, napříč všemi procesy a odděleními. RCSA nejprve posuzuje inherentní operační rizika, poté následují kontrolní a preventivní mechanismy, které tato inherentní operační rizika snižují. Hodnocení reziduálního rizika úzce souvisí s ostatními nástroji operačního rizika, tzn. sběr dat, analýzy scénářů, klíčové indikátory rizik, a navíc s výsledky formalizovaných kontrol 1. stupně, které jsou podkladem pro hodnocení kontrolních a preventivních mechanismů v rámci RCSA. Proces je také definován v interním dokumentu vybrané bankovní instituce.
- Analýza scénářů: Účelem analýzy scénářů je získat přehled o méně obvyklých rizicích, jejichž dopad na banku může být významný. Tato metodika se opírá především o dostupná interní data a následně o dostupná externí data

z evropského bankovního sektoru. Každý scénář vyžaduje vlastní ad hoc analýzu zahrnující experty z příslušných oddělení banky. Pokud jsou k dispozici externí data, lze tuto analýzu doplnit o data shromážděná z bankovního sektoru. Proces je definován v interním dokumentu.

- KRI (Key Risk Indicators) jsou definovány jako parametry vyplývající z bankovních činností, které mohou indikovat změnu profilu operačního rizika v určitých procesech nebo oblastech. Příkladem může být počet klientských stížností, počet chyb při zadávání dat, selhání systému, zaplacené pokuty atd. Úzce tedy souvisí s inkasem vnitřních ztrát, které dokážou do určité míry předvídat. Dále do systému formalizovaných kontrol 1. stupně, kde mohou představovat požadovaný výstup těchto kontrol. Vymezení nových monitorovacích oblastí podléhá závěrům kvalitativního sebehodnocení v rámci RCSA.
- Externí data: Banka sleduje externí data, aby identifikovala rizika, která by mohla být příčinou ztráty pro vybranou bankovní instituci. Externí data jsou rovněž využívána v rámci analýz scénářů.

Výše uvedené metody hodnocení operačních rizik tvoří základ pro vytvoření přehledu operačních rizik a pro definování akčních plánů vedoucích ke zmírnění rizik (např. mohou vést ke změnám stávajícího kontrolního prostředí, včetně kontroly úrovně 1 stupně).

Tyto metody definuje mateřská společnost vybrané bankovní instituce a procesy, které tyto metody podporují, jsou definovány na úrovni banky i mateřské společnosti.

Akční plány a jejich monitoring

Akční plány jsou přijímány, pokud dojde k významným událostem operačního rizika nebo jsou identifikovány významné nedostatky v kontrolním prostředí banky. Akční plány lze definovat na základě kterékoli z metod hodnocení operačního rizika uvedených výše nebo kontrolních postupů. Pravidla a kritéria pro závazné stanovení akčních plánů jsou popsána ve vnitřních předpisech pro jednotlivé metody hodnocení operačního rizika.

Termín realizace stanoveného akčního plánu musí být stanoven podle zásady co nejrychlejšího řešení, které omezuje vznik ztráty nebo rizik v budoucnu. Útvar nebo osoba odpovědná za stanovený akční plán je povinna na vyžádání pracovníků odboru operačního rizika poskytnout informace o průběhu plnění akčního plánu a předpokládané načasování realizace akčního plánu. Každé rozhodnutí o zrušení nebo odložení data provedení nápravného opatření musí být doplněno o vysvětlující komentář.

Monitoring akčních plánů a jejich implementaci zajišťuje odbor operačních rizik. Předmětem sledování akčního plánu je dodržování lhůt pro přijetí akčního plánu a způsob jeho realizace na základě informací poskytnutých vlastníkem příslušného akčního plánu.

Výbor pro řízení operačních rizik (ORC) je pravidelně informován o nejdůležitějších akčních plánech. U akčních plánů, které nebudou realizovány včas, bude k jednání ORC připojen vysvětlující komentář. V případě, že se termín stejného akčního plánu posune více než dvakrát, bude o situaci informován kromě ORC také ředitel příslušného odboru nebo člen představenstva pověřený příslušnou agendou, budou vyžádány důvody zpoždění a návrh na další postup.

Hlavní akční plány jsou definovány odborem operačního rizika na základě odhadu míry rizika zmírňovaného příslušným akčním plánem. Předmětem monitoringu je maximálně 10 nejvýznamnějších akčních plánů.

Permanentní kontroly (FLC, SLC)

- FLC – Formalizované kontroly 1. stupně – představují důležitý prvek v procesu monitorování efektivity kontrolního prostředí, jedná se o kontrolní činnosti prováděné z manažerské úrovně a sloužící ke kontrole, zda jsou dodržovány provozní každodenní kontroly a zaměstnanci dodržují předpisy a stanovené postupy. Proces je dále definován v interním dokumentu.
- SLC – Formalizované kontroly 2. úrovně – ověřují definice a efektivní implementaci kontrol 1. úrovně. Cílem je posoudit efektivitu a kvalitu provádění těchto kontrol a zároveň vyhodnotit výsledky kontrol, včetně stanovení nápravných doporučení a jejich pravidelného monitoringu. Principy SLC jsou upraveny v interním dokumentu. Odpovědnost za výkon SLC nenese odbor operačního rizika. Výkon SLC je zajišťován nezávislými týmy, které jsou zapojeny do oblastí řízení rizik, strategie a financí a spadají do odpovědnosti člena představenstva odpovědného za oblast compliance.

Schopnosti

Mezi dovednosti zaměstnanců patří především odborné znalosti v oblasti řízení rizik za účelem analýzy a vyhodnocení vznikajících rizik. Banka zajišťuje, aby zaměstnanci, jejichž činnost má vliv na řízení rizik, byli dostatečně seznámeni se strategií řízení rizik, jejich činnostmi prováděnými v souladu s touto strategií, z toho vyplývajícími postupy a omezeními. Každý zaměstnanec musí splnit školení ohledně zákonů, předpisů a vnitřních direktiv v rámci vybrané

bankovní instituce. Všechny potřebné informace a podklady pro splnění mají k dispozici na intranetu banky.

Představenstvo stanovuje zásady pro kontrolní mechanismy a činnosti v oblasti řízení rizik pro ověřování dodržování stanovených procesů a limitů a pro přezkoumávání výsledků hodnocení nebo měření rizik. Implementace strategie a souvisejících politik řízení rizik je společnou odpovědností představenstva a dalších oddělení. Dále je představenstvo banky odpovědné za vrcholové řízení strategických rizik, finančního a kapitálového rizika, rizika nadměrného zadlužení, systémového, obchodního a operačního rizika. V rámci této konečné odpovědnosti je představenstvo podporováno příslušnými odděleními a divizemi vybrané bankovní instituce. Je-li riziko zvládnutelné, je povinností vedoucího příslušného oddělení navrhnout a zavést takové kontrolní nebo preventivní mechanismy, které umožňují efektivní snížení.

Zaměstnanci musí jasně a efektivně komunikovat s ostatními členy týmu, včetně vedení a dalších oddělení. Efektivní řízení operačních rizik vyžaduje spolupráci a koordinaci mezi různými odděleními a funkcemi v organizaci. Zaměstnanci pracují efektivně jako tým, sdílejí informace a spolupracují při zavádění opatření k řízení rizik.

Sdílené hodnoty

Banka musí udržovat dostatečnou výši kapitálu na pokrytí rizik, kterým je nebo může být vystavena. Strategie a procesy řízení rizik, stejně jako strategie a procesy pro generování a udržování rizikového kapitálu, jsou komplexní a vzájemně propojené.

Při omezování a krytí rizik banka pečlivě zvažuje faktory, které ovlivňují výsledek hodnocení nebo měření podstupovaných rizik, včetně dopadu:

- Tvorba opravných položek a jiných úprav ocenění majetku a tvorba rezerv na podrozvahové položky,
- použití vlastních odhadů a modelů,
- zohlednění výsledků testů, včetně vlivu výsledků úrokových šokových testů a dalších zátěžových testů,
- využití derivátů, zvážení zajištění a dalších technik snižování rizika,
- zvážení efektů z rozložení (diverzifikace) rizik.

V případě, že celková výše podstupovaných rizik není dostatečně kryta kapitálem či jinak, i s přihlédnutím k vlivu vnitřních kontrolních mechanismů (celkový rizikový profil), přijme banka nápravná opatření.

Další důležité zásady:

- Přísné dodržování zákonných a regulatorních požadavků a standardů stanovených ve směrnicích pro řízení rizik skupiny vybrané bankovní instituce.
- Povinnost péče, přesnosti a transparentnosti vůči klientům banky a v souladu s tradicí profesionalitou a integritou.
- Ochota navazovat obchodní vztahy pouze s protistranami, jejichž identita je řádně prokázána a sdílejí stejného ducha integrity a odpovědnosti.
- Dodržování pravidel obezřetnosti a chování, stejně jako kvalita a diverzifikace rizik je nanejvýš důležité, i když to znamená omezení rozsahu činnosti a ziskovosti v krátkodobém horizontu.

Styl vedení

Banka ve spolupráci se všemi relevantními útvary zajišťuje vhodný a cílený systém vzdělávání svých zaměstnanců. Cílem tohoto školení je poskytnout všem dotčeným zaměstnancům banky informace o pravidlech chování a nejnovějším technickém a metodickém vývoji a také podpořit rozvoj obecného povědomí o rizicích v bance.

Pravidla pro implementaci strategie řízení rizik ve vybrané bankovní instituci a její skupině určují odpovědné útvary formou obecných směrnic a procesů, které jsou v případě potřeby dále rozpracovány do podrobnějších provozních postupů. Tyto zásady a postupy pokrývají všechny typy shromažďování, hodnocení, monitorování a kontroly/zmírňování jednotlivých rizik stanovením explicitních odpovědností každého zaměstnance a zajištěním auditní stopy.

Tyto postupy jsou v souladu se strategií banky a příslušnými politikami definovanými v interním dokumentu, s platnou legislativou a příslušnými regulatorními požadavky a odrážejí praxi a standardy dobrého chování a etiky v bankovním odvětví. Postupy a procesy jsou stanoveny individuálními pokyny a pokyny odpovědných útvarů a zpřístupněny všem zaměstnancům prostřednictvím intranetu banky.

Spolupracovníci

Řízení operačních rizik na celkové úrovni celé banky je v kompetenci odboru operačního rizika, které je organizačně začleněno do úseku řízení rizik. Jeho funkce a kompetence jsou definovány v interní směrnici.

Základním úkolem odboru operačních rizik je pomocí standardních metod řízení operačního rizika identifikovat oblasti, kde je zbývající operační riziko stále velmi vysoké, ať už

z důvodu neexistujících nebo nefunkčních kontrolních mechanismů nebo z důvodu vysokého rizika inherentního operačního rizika dané činnosti. Oddělení operačních rizik je povinno o těchto případech informovat výbor pro operační rizika.

Součástí odboru operačních rizik je také koordinace kontroly 1. stupně, jehož úkolem je spolupracovat s koordinátory jmenovanými na úrovni jednotlivých oddělení banky a dceřiných společností. Jejich úkolem je koordinovat nastavení kontrol 1. stupně v souvislosti s nástroji pro hodnocení operačního rizika.

Oddělení operačních rizik v souvislosti s řízením operačních rizik v dceřiných společnostech zahrnutých do regulatorní konsolidace:

- Vykonává dohled nad řízením operačních rizik v dceřiných společnostech,
- kontroluje a případně poskytuje odpovídající metodickou pomoc potřebnou k přiměřené aplikaci metod řízení operačních rizik,
- validuje a schvaluje v odpovídajících případech zásady a postupy řízení operačních rizik uplatňované dceřinou společností.
- Informuje dceřiné společnosti o používaných metodách řízení operačního rizika,
- monitoruje řízení operačních rizik v dceřiných společnostech,
- prověřuje a v případě potřeby poskytuje vhodnou metodickou pomoc nezbytnou pro vhodnou aplikaci metod řízení operačního rizika,
- ověřuje a v odpovídajících případech schvaluje zásady a postupy řízení operačního rizika uplatňované dceřinou společností.

Výbor pro operační rizika

Výbor pro operační rizika schvaluje veškerá strategická rozhodnutí související s operačními riziky a předkládá schválená rozhodnutí představenstvu vybrané bankovní instituce.

Úsek Interní audit

Úlohou úseku interního audit v souvislosti s postupy pro řízení operačních rizik a minimalizaci ztrát z titulu operačních rizik je:

- Ověřovat způsob nastavení kontrolních a preventivních mechanismů u ověřovaných rizik,
- vyhodnocovat efektivitu těchto kontrolních a preventivních mechanismů,
- navrhovat nápravná opatření v případě poruch či nedostatečném nastavení těchto mechanismů.

5.3.3 Metoda RIPRAN

Metoda RIPRAN je empirická metoda pro analýzu rizik projektů, kterou jsem popsala výše v teoretické části. Součásti metody je identifikace rizika, nastavení hrozeb a scénářů daných rizik. Dále jejich hodnocení dle pravděpodobnosti, dopadu, celkové hodnoty rizika, a také návrhy opatření identifikovaných rizik a úseků, které jsou odpovědné za jejich řízení ve vybrané bankovní instituci. Při jejím zpracování jsem vycházela se získaných informací z interních dokumentů a komunikace s vedením.

Identifikace rizik

V této části práce jsem identifikovala hlavní operační rizika, která ovlivňují vybranou bankovní instituci. Na základě informací získaných studiem interních dokumentů vybrané bankovní instituce a také diskuse s vedením jsem vybrala jednotlivá rizika, která jsou identifikovány jako hlavní řešená rizika pomocí metody RIPRAN. Jednotlivá rizika jsou rozdělena do určitých kategorií, kam spadá popis a obsah kategorií je zpracován níže. Následně z těchto rizik byly vybrány nejčastější hrozby a jejich scénáře, které mohou nastat v jednotlivých kategoriích. Následující hrozby a scénáře jednotlivých operačních rizik jsou vyhodnoceny v příloze č. 1 této diplomové práce.

Obchodní spory

Za obchodní spory se považují problémy v obchodním vztahu mezi bankou a třetí osobou (klient, protistrana, prodejce, dodavatel) ohledně typu nabízeného produktu, obchodních zvyklostí, srozumitelnosti a souladu uzavřených smluv s právními předpisy, dodržování smluvních podmínek, nebo obecně vedení vztahu s třetí stranou. Nesprávné provádění pokynů klienta, které banka nerozpoznala a neopravila předtím, než na ně klient upozornil, což má negativní finanční dopad na operace banky. Tyto typy problémů se obvykle řeší buď prostřednictvím soudního sporu, mimosoudního vyrovnání nebo prostřednictvím finančního arbitra. Do této kategorie nepatří případy, kdy se banka dobrovolně, bez nátlaku a bez vlastního pochybení rozhodne odpustit některé závazky klienta v zájmu zachování dobrého obchodního vztahu. Pochybení v oblasti řízení zákaznických stížností. Nejčastější hrozby jsou v rámci této kategorie následující:

- Pochybení v oblasti řízení zákaznických stížností,
- nevhodné obchodní praktiky,
- neadekvátní nabídka produktů,
- neadekvátní péče o klienta,

- další spory s třetí stranou,
- nevymahatelné kontrakty nebo podmínky smluv.

Spory s veřejnými orgány

Tato kategorie zahrnuje neúmyslné porušení jakéhokoli zákona, nařízení, požadavku nebo pravidla stanoveného veřejným orgánem nebo třetí stranou, které musí dodržovat všichni účastníci procesů banky. Záměrné využívání chyb a nejednoznačností v těchto zákonech a nařízeních, i když je v souladu se správným výkladem, neodpovídá myšlence daného zákona nebo nařízení.

Tato část pokrývá veškeré zákony a předpisy, které musí dodržovat všichni účastníci bankovního trhu v České republice. Mezi tyto zákony patří například daňové zákony, pracovní právo, zákony na ochranu životního prostředí, ale i zákony, které se konkrétně vztahují na bankovní sektor, opatření České národní banky, nařízení Ministerstva financí a Komise pro cenné papíry. Příkladem ztrát v této kategorii jsou ztráty vyplývající z nezabránění praní špinavých peněz. Nejčastější hrozby, které mohou nastat, jsou následující:

- Porušení bankovních a finančních zákonů s výjimkou embarg a sankcí,
- porušení zákonů související s ochranou životního prostředí a závazků skupiny k CSR,
- porušení nařízení související s pracovní legislativou,
- porušení bezpečnostních standardů, nebo selhání při ochraně zdraví,
- porušení požadavků/pravidel trhu s výjimkou zneužití trhu
- zneužití trhu,
- nedodržení embarg a sankcí,
- porušení požadavků na regulaci, účetnictví a finanční výkaznictví,
- porušení zákonných opatření v oblasti daňové legislativy,
- porušení pravidel týkajících se boje proti praní špinavých peněz a financování terorismu,
- porušení zákonů o ochraně dat klientů a zaměstnanců,
- nedodržování kodexu chování skupiny včetně nevhodného chování zaměstnanců,
- porušení ostatních vnějších povinností chování.

Chyby v odhadu rizika nebo ocenění

Tato kategorie zahrnuje veškeré nedostatky ve výpočtu míry rizika a v procesu hodnocení nebo přeceňování transakcí. Tato chyba může vzniknout z chybějících informací, chyb v návrhu

modelu, nesprávného použití modelu nebo nesprávného ocenění zajištění. Tato ztráta může nastat v okamžiku dokončení transakce nebo i později při sledování míry rizika konkrétní transakce. Hrozby, které mohou nastat, jsou v následujícím výčtu:

- Nedostatky v procesu řízení a sledování limitů a oprávnění,
- neexistující nebo chybné ocenění pozice,
- špatné informace z trhu,
- chyby v oceňovacích nebo rizikových modelech.

Chyby při provádění pokynů

Zde jsou zahrnuty jakékoli chyby ve zpracování pokynů nebo ztráty vyplývající z přerušení zpracování pokynů. Tyto chyby se mohou vyskytnout v jakékoli fázi zpracování, od dokončení transakce, zadání transakce do účetnictví a reporting až po konečné vypořádání transakce. Příklady možných chyb zahrnují: nesprávné zaznamenání transakce, chyby při potvrzování a zpracování transakce, pozdní nebo neprovedení pokynů klienta, které nějakým způsobem vyžadují finanční kompenzaci, chyby při odsouhlasení, nepřiměřené postupy pro identifikaci a řešení výjimek, neprovedení dodržování důležitých materiálů, smluv a dalších. Patří sem rizika způsobená slabinami v organizační struktuře, nastavení procesů nebo systému kontroly. To se týká zejména důsledků nedodržení základních požadavků na vnitřní kontroly, jako jsou: směšování odpovědností, neadekvátní struktura podávání zpráv, chybějící nebo nedostatečná dokumentace, neefektivní průběžné monitorování. Nejčastější hrozby, které vyplývají z této kategorie, jsou:

- Chyby vznikající v obecné administrativě po dobu trvání transakce,
- chybné zachycení transakce,
- nepřesné informace pro management,
- nevhodná organizační struktura,
- absence nebo selhání kontrolního prostředí,
- nedostatečná ochrana týkající se dokumentů nebo cenných aktiv držených jménem třetích stran,
- selhání dodání sjednané služby třetí stranou nebo outsourcující společností s výjimkou počítačové kriminality,
- chyby při rekonciliaci,
- selhání správy účtů zákazníků / protistran, včetně neoprávněného přístupu na klientský účet,
- selhání reportingu zákazníkovi nebo protistraně,

- trestné činy proti bankovním aktivům od třetí strany s výjimkou počítačové kriminality,
- krádeže, podvody, zpronevěry spáchané třetí stranou s výjimkou počítačové kriminality,
- krádež spáchaná zaměstnancem banky,
- podvodné transakce (provedené přímo zaměstnancem nebo jeho zapojením),
- neoprávněné/nesprávné/nedbalostní použití důvěrných informací interními stranami (zaměstnanci/dodavatelé, kteří jsou zaměstnáni bankou/stážisty),
- počítačová kriminalita na PC systémech zákazníků třetími stranami,
- sabotáž vnitřních IT systémů banky zaměstnanci,
- korupce.

Podvody

Kategorie podvodu zahrnuje jakékoli úmyslné porušení stávajících zákonů, předpisů nebo postupů. Podvodu nebo jiné trestné činnosti se může dopustit zaměstnanec nebo externí subjekt.

Do této kategorie patří zejména krádeže peněz, cenných papírů, movitých věcí a porušování práv duševního vlastnictví, které může být vlastněno nebo může být pouze uschováno členy bankovní skupiny. Například: neoprávněné nebo falešné transakce, neoprávněné použití chráněných nebo omezených informací na určitou skupinu osob, úmyslný útok na IT systém, podvody a další trestné činy namířené proti majetku členů bankovní skupiny. Níže je výčet nejčastějších hrozeb v rámci této kategorie:

- Trestné činy proti bankovním aktivům od třetí strany s výjimkou počítačové kriminality,
- krádeže, podvody, zpronevěry spáchané třetí stranou s výjimkou počítačové kriminality
- krádež spáchaná zaměstnancem banky,
- podvodné transakce (provedené přímo zaměstnancem nebo jeho zapojením),
- neoprávněné/nesprávné/nedbalostní použití důvěrných informací interními stranami (zaměstnanci / dodavatelé, kteří jsou zaměstnáni bankou / stážisty),
- počítačová kriminalita na PC systémech zákazníků třetími stranami,
- sabotáž vnitřních IT systémů banky zaměstnanci,
- Korupce.

Nepovolené obchodování (Rogue Trading)

Rogue trading je anglický termín, který popisuje záměrné nedodržování nebo nerespektování vnitřních a vnějších pravidel obchodníky v souvislosti s transakcemi na finančních a kapitálových trzích. Nejčastější hrozba v rámci této kategorie je:

- Nepovolené aktivity na finančních a kapitálových trzích.

Ztráta provozního prostředí / kapacity

Tato kategorie zahrnuje jakoukoli událost, která má negativní dopad na provozní prostředí nebo kapacitu: zničení zařízení provozovny nebo dalšího vybavení zmizení klíčového dodavatele, zničení dokumentů nebo ztráta transakčních dat, ztráta klíčového člena týmu atd. Vypsané hrozby níže jsou vybrána jako nejčastější.

- Nedostatek pracovníků,
- ztráta dat,
- ztráta výrobních prostředků,
- ztráta klíčové služby.

Poruchy systémů

Tato kategorie zahrnuje všechny funkční nebo technické problémy v IT zařízeních (hardware), operačních systémech nebo aplikacích (software) nebo telekomunikačních zařízeních. Patří mezi ně např.: výběr systému, který nesplňuje požadavky, neodpovídající provoz nebo údržba IT systému, neúmyslné zavedení počítačového viru, poškození způsobené nedostatečnou fyzickou ochranou systému nebo nevhodnou klimatizací prostředí, nevhodné procesní vymezení uživatelského přístupu a uživatelských práv. Nesprávné použití příslušné aplikace uživatelem spadá do kategorie „provádění pokynů, hlášení“. Ztráty způsobené nedostupností IT systému v důsledku zničení budovy, ve které se nachází, by měly být zařazeny do kategorie ztráta provozního prostředí/kapacity.

Z každé této kategorie byly vybrány jednotlivá rizika, které mají největší dopad na řízení operačních riziko ve vybrané bankovní instituci. Identifikace těchto rizik byla podložena komunikací s vedením a nahlédnutím do interních dokumentů oddělení, které je za operační rizika odpovědné. Níže je výčet nejčastější hrozeb v této kategorii.

- Selhání hardware,
- nekonzistentní data,
- špatné řízení projektů,

- chyby v software,
- nedostatečné fyzické zabezpečení.

5.4 VYHODNOCENÍ OPERAČNÍCH RIZIK

V této závěrečné části práce jsem vyhodnotila zvolené analytické metody. Pestle, kterou jsem analyzovala vnější faktory, které dopadají na vybranou instituci. Dále jsem provedla vyhodnocení McKinseyho modelu 7 S, kterým popisuji sedm témat, které řeší vnitřní prostředí vybrané bankovní instituce. V rámci vyhodnocení metody RIPRAN jsem navrhla opatření, které určilo novu hodnotu rizika a odpovědné úseky za zajištění opatření operačních rizik. Příloha se zpracovanou metodou je obsažena na závěr této diplomové práce v příloze č. 1.

5.4.1 Vyhodnocení PESTLE analýzy

Při vyhodnocení vnějších faktorů vybrané bankovní instituce jsem zjistila s ohledem na analýzu politických faktorů, že na riziko porušení bankovních a finančních zákonů s výjimkou embarg a sankcí ve vybrané bankovní instituci největší vliv regulace České národní banky.

Zhodnocením ekonomických faktorů z analýzy vychází, že v nynější době je ekonomická situace instituce nejvíce ovlivněna rizikem poruchy v dodavatelských řetězcích a v souvislosti s celkovým ekonomickým vývojem zahrnující inflaci, vysokou mírou zaměstnanosti a pokles HDP. Rizika vychází z možného porušení zákonných opatření v oblasti daňové legislativy – neočekávaná daňová politika státu. Dále riziko nedostatek pracovníků nemožnost kvalitního vyškolení nových zaměstnanců.

Vnější sociální faktory zahrnují riziko neadekvátní péče o klienta, nedodržování kodexu chování skupiny včetně nevhodného chování zaměstnanců v rámci nedostatečné výchovy k sociálně-finanční gramotnosti.

Vnější technické faktory pro vybranou instituci spočívají v potencionálním riziku krádeže, podvodu, zpronevěry spáchané třetí stranou, neoprávněné/nesprávné/nedbalostní použití důvěrných informací interními stranami zaměstnanci / dodavatelé, kteří jsou zaměstnáni bankou / stážisty, počítačová kriminalita na PC systémech zákazníků třetími stranami.

Při hodnocení vnějších legislativních faktorů je zřejmé, že se jedná o všechny operační rizika, která jsou spojena se spory s veřejnými orgány.

Ekologické vnější faktory jsem vyhodnotila jako rizika ovlivňující porušení zákonů související s ochranou životního prostředí a závazků skupiny k CSR, porušení nařízení spojených s pracovní legislativou.

5.4.2 Vyhodnocení McKinseyho modelu 7 S

V rámci strategie jsem zjistila, že v této souvislosti je zvláště důležitým cílem zajištění dodržování povinností vyplývajících z právních předpisů a předpisů orgánů dohledu v oblasti řízení operačních rizik.

Struktura řízení operačních rizik ve vybrané bankovní instituci zahrnuje odpovědnost a rozdělení mezi oddělení a pravomocí řízení rizik.

Systémy ve vybrané bankovní instituci jsou použity metody: sběr dat, RSCA, analýza scénářů, KRI, externí data. Rizika označena jako podstatná jsou projednávaná a následně instituce uplatňuje akční plány a kontroly prvního a druhého stupně.

Schopnosti v tomto bodu analýzy jsem identifikovala rizika, která řízena v souladu s touto strategií, z toho vyplývajícími postupy a omezeními. Každý zaměstnanec musí splnit školení ohledně zákonů, předpisů a vnitřních direktiv v rámci vybrané bankovní instituce.

Sdílené hodnoty v rámci analýzy vnitřního prostředí instituce mají za úkol snížit operační riziko neadekvátní péče o klienta.

Styl vedení pravidla pro implementaci strategie řízení rizik ve vybrané bankovní instituci a její skupině určují odpovědné útvary formou obecných směrnic a procesů, které jsou v případě potřeby dále rozpracovány do podrobnějších provozních postupů. Tyto zásady a postupy pokrývají všechny typy shromažďování, hodnocení, monitorování a kontroly/zmírňování jednotlivých rizik stanovením explicitních odpovědností každého zaměstnance a zajištěním auditní stopy. Například rizika chybného zachycení transakce a nepřesné informace pro management.

Při zpracování analýzy spolupracovníků, jsem zjistila, že by bylo smysluplné spojit odpovědnost vedení dvou úseků. Neboť několik oddělení/úseků má odpovědnost za řízení operačních rizik.

5.4.3 Vyhodnocení metody RIPRAN

K výše identifikovaným hrozbám a jejich scénářům jsem přiřadila odpovídající třídy hodnocení pravděpodobnosti rizika při zpracování metody RIPRAN, které jsem stanovila procentuálním vyjádřením vůči součtu pravděpodobnosti, z výsledků interních dat z minulých let, operačních rizik výpočtem podle tabulky, která je zpracována v teoretické části práce a také vyobrazena níže.

Tabulka 1: Třídy pravděpodobnosti rizika (Zdroj: (Lacko, 2024) vlastní zpracování)

Vysoká pravděpodobnost - **VP**	Nad 66 %
Střední pravděpodobnost - **SP**	33 až 66 %
Nízká pravděpodobnost - **NP**	Pod 33 %

Třídy dopadu byly nastaveny za daných kritérií, které jsou popsány v následující tabulce. Hodnotu dopadu operačních rizik jsem stanovila, procentuálním výpočtem z celkového finančního dopadu z komplexních ztrát z minulých období kdy: malý nepříznivý finanční má hodnota rizika, která ovlivňuje svým dopadem řízení operačních rizik od 0 – 5 % vůči celkovému součtu, střední nepříznivý dopad na řízení rizik mají rizika s hodnotou dopadu od 6–10 %, velký nepříznivý dopad na finanční stránku vybrané bankovní instituce by měly rizika, které překračují hranici 11-20 %. Určení zásahu při dopadu rizika bylo stanoveno pomocí informací interních dokumentů, kdy vybraná bankovní instituce má stanoveno, že dopady rizik do 250 tis. EUR se považují za zanedbatelné. Střední dopad mají rizika s hodnotou 250–500 tis. EUR. Velký finanční dopad mají rizika s hodnotou 500 tis. EUR a výše. Tyto finanční hodnoty se určují pro celou vybranou bankovní instituci v České republice, je počítáno v eurech vůči měně mateřské společnosti, která sídlí v zahraničí.

Tabulka 2: Třídy dopadu operačních rizik (Zdroj: (Lacko, 2024) vlastní zpracování)

Velký nepříznivý dopad **VD**	Dopad na vybranou bankovní instituci bude významný Dopady vyžadující určité zásahy Hodnota podle metrik z interních dokumentů 11-20 %
Střední nepříznivý dopad **SD**	Dopad na vybranou bankovní instituci bude ke zvážení Dopady vyžadují mírné zásahy Hodnota podle metrik z interních dokumentů do 6-10 %
Malý nepříznivý dopad **MD**	Dopad na vybranou bankovní instituci bude nevýznamný Dopady nevyžadující určité zásahy Hodnota podle metrik z interních dokumentů do 0–5 %

Celková hodnota operačního rizika byla stanovena z níže vyobrazených tabulek, která je dána v rámci hodnocení, které je obsaženo v teorii této práce z použitého literárního pramene.

Tabulka 3: Třídy hodnoty rizika (Zdroj: (Lacko, 2024) vlastní zpracování)

Vysoká hodnota rizika – **VHR**
Střední hodnota rizika – **SHR**
Nízká hodnota rizika – **NHR**

Vyhodnocení operačních rizik jsem provedla pomocí přiřazení třídy hodnoty jednotlivých riziku, s ohledem na hodnotu pravděpodobnosti a dopadu rizik na vybranou bankovní instituci.

Tabulka 4: Přiřazení třídy hodnoty rizika (Zdroj: (Lacko, 2024) vlastní zpracování)

	Velký nepříznivý dopad	**Střední nepříznivý dopad**	**Malý nepříznivý dopad**
Vysoká pravděpodobnost	Vysoká hodnota rizika **VHR**	Vysoká hodnota rizika **VHR**	Střední hodnota rizika **SHR**
Střední pravděpodobnost	Vysoká hodnota rizika **VHR**	Střední hodnota rizika **SHR**	Nízká hodnota rizika **NHR**
Nízká pravděpodobnost	Střední hodnota rizika **SHR**	Nízká hodnota rizika **NHR**	Nízká hodnota rizika **NHR**

Celkové hodnocení jednotlivých operačních rizik vybrané bankovní instituce, zpracované dle jednotlivých tříd jsem vyhodnotila pomocí tabulky č. 4, která je obsažena v příloze č. 1. této diplomové práce.

5.5 NÁVRHY OPATŘENÍ K MINIMALIZACI RIZIK

Návrhy opatření operačních rizik

Jednotlivé návrhy opatření jsem stanovila, pro snížení dopadu vybraných operačních rizik, které byly identifikovány a ohodnoceny v předchozích krocích v metodě RIPRAN. Tím, že operační riziko je definováno jako riziko chyby zaměstnanců, výpadky informačního systému nebo výpadky komunikační sítě. Je zřejmé, že operační rizika jsou velmi závažnou rizikovou kategorií, jejíž důsledky mohou mít v extrémních případech mnohem větší dopad než jiná rizika.

Dvě rizika s nejvyšší celkovou hodnotou jsou následující chybné zachycení transakce, krádeže, podvody, zpronevěry spáchané třetí stranou s výjimkou počítačové kriminality. Rizik se střední hodnotu je šest – neadekvátní péče o klienta, porušení bankovních a finančních zákonů s výjimkou embarg a sankcí, chyby vznikající v obecné administrativě po dobu trvání transakce, nepřesné informace pro management neoprávněné/nesprávné/nedbalostní použití důvěrných informací interními stranami (zaměstnanci / dodavatelé, kteří jsou zaměstnáni bankou / stážisty),

selhání hardware. Opatření, která jsem zpracovala, jsou obsaženy v příloze č. 1. Tyto opatření by měly vybrané bankovní instituci pomoci minimalizovat daná rizika, které jsou následně ohodnocena novou hodnotou rizika.

Nová hodnota rizika

Nové hodnoty rizik jsem stanovila při použití návrhu opatření u zmíněných operačních rizik, které jsou zpracovány v metodě RIPRAN. Vybraná bankovní instituce by měla nízké riziko podstoupit a střední a vysoké řešit pomocí návrhů opatření. Úseky, které jsou zodpovědné za splnění opatření jednotlivých rizik, by měli své návrhy projednat a naplánovat jejich splnění pro minimalizaci finančního dopadu na vybranou bankovní instituci. Při zpracování metody RIPRAN nevyšlo žádné riziko, jako riziko s novou vysokou hodnotou rizika. Se střední hodnotou jsou označeny dvě rizika, a to riziko chybného zachycení transakce, které spadá do kategorie chyb při provádění pokynů a riziko krádeže, podvodů, zpronevěry spáchané třetí stranou s výjimkou počítačové kriminality z kategorie podvodů.

Ostatní zbylé rizika vyšly jako rizika s nízkou hodnotou, tyto rizika jsou pro vybranou bankovní instituci zanedbatelné, protože jejich dopad je roven finančním nákladům na opatření. Vůči reálnému dopadu těchto rizik je málo pravděpodobné že by měli nastat na pravidelné bázi a bylo by potřeba zvážit jejich aplikaci opatření.

Náklady na opatření

Náklady na opatření jsem stanovila podle možného finančního dopadu vybraných operačních rizik. Finanční náklady rizik jsem stanovila pomocí informací získaných z interních dokumentů, kdy má vybraná bankovní instituce stanoveno, že náklady rizik do 250 tis. EUR se považují za nízké. Střední náklady mají rizika s hodnotou 250–500 tis. EUR. Vysoké finanční náklady mají rizika s hodnotou 500 tis. EUR a výše. Tyto finanční hodnoty se určují pro celou vybranou bankovní instituci v České republice, je počítáno v eurech vůči měně mateřské společnosti, která sídlí v zahraničí. Rizika s vysokým dopadem jsou pouze dvě a se střední hodnotou je jich šest z celkového počtu 51 operačních rizik analyzovaných touto metodou.

Tabulka 5: Tabulka přiřazení nákladů na opatření (Zdroj: vlastní zpracování)

Vysoké náklady na opatření	500 tis. EUR a výše
Střední náklady na opatření	250–500 tis. EUR
Nízké náklady na opatření	0–250 tis. EUR

Odpovědné úseky za zajištění

Rozdělení odpovědných úseků jsem stanovila podle vymezení odpovědnosti vybrané bankovní instituce, kam jednotlivé kategorie rizik spadají. Následující procentuální výpočet úseků je vypočítáno z celkového počtu operačních rizik, které mohou nastat a jejich opatření. Dále jsem toto rozřazení komunikovala s vybranou institucí a identifikovala pomocí interních dokumentů.

Úsek Brand Strategy and Communication je přiřazen k zhruba 6 % rizikům. Odbor Compliance zastupuje 28 %, Úsek lidských zdrojů 43 %, Právní oddělení 4 %, Úsek interního auditu 6 %, Odbor Podpůrné služby & facility management 12 %, Úsek spadající pod Chief Digital Officera 18 %. Součet těchto procent nedává dohromady čistých 100 %, protože některé úseky zastupují rizika spolu s dalším úsekem. U těchto rizik potřeba spolupráce, při tvorbě opatření.

5.6 NÁVRH STRATEGIE OPERAČNÍCH RIZIK

V této podkapitole jsem popsala návrh strategie operačních rizik. Zde je možnost, jak by vybraná bankovní instituce mohla řídit rizika – implementaci strategie, vymezení odpovědnosti, kontrola a monitoring vybraných operačních rizik.

5.6.1 Implementace strategie

Implementace strategie a souvisejících politik řízení rizik je společnou odpovědností představenstva a následujících oddělení:

Představenstvo banky je odpovědné za vrcholové řízení strategických rizik, rizika kapitálu a zdrojů financování, rizika nadměrné páky, systémového rizika a obchodního rizika. V rámci této konečné odpovědnosti je představenstvo podporováno odpovědnými útvary a útvary vybrané bankovní instituce. Představenstvo je rovněž odpovědné za celkové riziko (mimo jiné včetně vrcholového managementu kapitálové přiměřenosti).

Oddělení řízení rizik je odpovědné za řízení kreditního rizika, tržního rizika obchodního portfolia, rizika úvěrové koncentrace, rizika spojeného se správou zajištění a rizika transakcí

s bankovními subjekty poskytujícími finanční služby, které nejsou pod dohledem ČNB (z pohledu kreditního rizika), ve kterých je zapojen jiný než členský stát včetně rizika vlivu jejího politického prostředí (riziko země) a rizika nákazy.

Úsek řízení rizik zajišťuje koordinaci implementaci efektivního přístupu k řízení rizik v rámci vybrané bankovní instituce, jakož i tvorbu metodiky a vhodných nástrojů pro výpočet regulatorních kapitálových požadavků s ohledem na úvěrová a tržní rizika vyplývající z činností na finančním trhu a rovněž zajišťuje, aby představenstvo banky pravidelně dostávalo nezávislé informace o vývoji a rozsahu těchto rizik.

Odbor compliance odpovídá za řízení reputačního rizika, rizika nestandardních operací, rizika operací, ve kterých je nebo by mohla být zapojena netransparentní nebo jinak potenciálně riziková protistrana nebo zeměpisná oblast, rizika operací s osobami poskytujícími finanční služby obdobné bankovním, nad nimiž není vykonáván dohled ČNB (z pohledu reputačního rizika) a rizika vlivu regulačního prostředí. Hlavním cílem odboru compliance je minimalizovat riziko neetického chování, porušování zákonů a předpisů, poskytovat vzdělávací programy a školení zaměstnanců, a chránit dobré jméno a integritu organizace.

Oddělení strategie a financí je odpovědné za řízení tržních rizik strukturální knihy (strukturální rizika), rizika likvidity, rizika spojeného s účastí v konsolidačním celku, včetně rizika transakcí se členy stejného konsolidačního celku a rizika majetkové zatížení.

Úsek strategie a financí je odpovědný za tvorbu metodiky a proces její kontroly specificky pro tržní rizika ve strukturní knize (strukturální rizika) a rizika likvidity. Výbor pro řízení aktiv a pasiv, který monitoruje tato strukturální rizika a rizika likvidity schvaluje postupy a limity. V této souvislosti úsek strategie a finance vyvíjí metody a nástroje pro výpočet regulatorního kapitálu vůči podstupovaným rizikům.

Divize transakčních, platebních služeb a investičního bankovnictví zodpovídá za řízení rizik tržní infrastruktury v oblasti platebního styku a transakcí investičního bankovnictví.

Specializovaná oddělení zajišťují některé funkce v rámci systému řízení rizik (provádění analýz, bodování, schvalování, monitorování a řízení), jakož i související provozní funkce (kontrola, zpracování, dokumentace), které mohou podléhat validaci oddělením řízení rizik nebo odborným auditům některými dalšími průřezovými oblastmi. Obecně je možné, že některé úkoly bude plnit buď oddělení řízení rizik, nebo naopak obchodní oddělení, v závislosti na povaze a důležitosti podstupovaných rizik.

Jednotlivá odpovědná oddělení by měli včas a vhodným způsobem komunikovat všem zainteresovaným stranám strategii řízení rizik ve vybrané bankovní instituci a dbát na její správné pochopení a akceptaci. Každý manažer zapojený do procesu řízení rizik musí být jasně informován o cílech, pravomocích a odpovědnostech, které mu byly v rámci systému řízení rizik přiděleny, a také o stanovené formě svého výkonu.

Za nové produkty/služby a nové činnosti/procesy nebo jejich významné změny, zodpovídají příslušná odborná oddělení a jejich předložení ke schválení zřízeným výborům banky: Výboru pro nové produkty investičního bankovnictví nebo výbory pro nové podnikové produkty a retailové bankovnictví v závislosti na povaze a rozsahu pravomocí, které jim byly svěřeny ve vztahu k povaze podstupovaných rizik. Úkolem těchto výborů je mimo jiné zajistit, aby všechna relevantní rizika související s produktem byla řádně kontrolována, změřena, schválena a byly zavedeny vhodné kontrolní procesy před zahájením obchodování. Je zakázáno sjednávat obchody a transakce zahrnující neautorizované produkty.

V rámci ochrany reputačního rizika banky a s ohledem na pravidla stanovená oddělením compliance mají zaměstnanci banky tyto úkoly:

- Před vstupem do vztahu s klientem protistranou, třetí stranou (neklinetem) nebo jinou právnickou osobou a v průběhu tohoto vztahu se musí ujistit, že lze prokázat a ověřit jeho totožnost, důvěryhodnost a právní způsobilost plnit své závazky vůči co největší bezpečnosti.
- Identifikovat všechny případy současných i potenciálních střetů zájmů a okamžitě zajistit, aby byly provedeny nezbytné postupy před získáním nebo poskytnutím informací získaných prostřednictvím finančního poradenství nebo úvěrových aktivit.
- Provádět významné finanční transakce s klientem pouze v případě, že je taková transakce řádně zohledněna v účetních záznamech zákazníka a je tedy dostupná pro externí audit.

Vzhledem k tomu, že banka umožňuje lidem s různými oblastmi odpovědnosti (z hlediska funkcí, trhů atd.) současně vytvářet stejná nebo vzájemně související rizika, je odpovědností jejího managementu spoléhat se na:

- Profesionály se zkušenostmi odpovídající povaze a složitosti rizik, která zpracovávají, a kteří jsou schopni se rozhodovat se vší vážností a citlivostí a kteří jsou schopni konstruktivní vzájemné komunikace mezi sebou nebo se specialisty na správu portfolia – a techniky snižování rizik,

- nejmodernější metody měření rizik pro jednotlivé kategorie rizik, odpovídající typu a objemu podkladových aktiv, jakož i počtu transakcí, poskytující komplexní a jednotné pochopení všech podstupovaných rizik a umožňující koncentraci na rizika, které významně souvisejí s kapitálovými a finančními výsledky banky, včetně projekce dopadu simulací významných změn základních hypotéz,
- informační systémy a standardy řízení, které se zaměřují na kvalitu a konzistenci dat umožňují sledování rizik s optimální pravidelností, na konsolidovaném základě a s dostatečnou úrovní auditní stopy a bezpečnosti,
- zaměstnanci odpovědní za kontrolu nebo validaci aplikace rizikové strategie banky, kteří jsou zcela nezávislí na obchodních oblastech, které kontrolují,
- politika odměňování, která přiměřeně odráží pozitivní a negativní dopady rozhodnutí přijatých v oblasti převzetí a řízení rizik zohledňuje jejich soulad se strategií řízení rizik a standardy stanovenými bankou.

5.6.2 Vymezení odpovědnosti

Úseky a samostatné odbory jsou zodpovědné za vypracování vlastních plánů kontinuity podnikání na základě analýzy dopadů, definované strategie pro udržení nebo obnovení kritických nebo životně důležitých činností a služeb v případě mimořádné situace a za zavedení preventivních opatření přizpůsobených povaze jejich činnosti, možná rizika a význam těchto činností.

Poskytnutí zdrojů nezbytných k udržení nebo obnovení kritických nebo životně důležitých činností a služeb banky musí být součástí smluv o rozsahu poskytovaných služeb uzavřených s dodavateli zdrojů, například jinými útvary vybrané bankovní instituce nebo externími poskytovateli služeb. Dohody o rozsahu také zahrnují opatření k uchování důležitých informací.

Odbor podpůrné služby & Facility Management je odpovědný za zabezpečení zdrojů fyzické infrastruktury nezbytných pro údržbu nebo obnovu kritických nebo životně důležitých činností a služeb banky. Zajišťuje:

- Správu prostor: zahrnuje plánování, organizaci a optimalizace využití prostoru v budovách, včetně skladů, kanceláří, konferenčních místností atd.
- Správu zařízení: řeší správu a údržbu všech systémů, technických zařízení a infrastruktury v budovách, zabezpečovací systémy, klimatizace, výtahy a osvětlení.

- Správu služeb: Zajišťuje koordinaci a kvalitu poskytovaných služeb v budově např. ostrahu, úklid atd.
- Řízení ochrany a bezpečnosti: Zahrnuje provádění bezpečnostních opatření a plánů pro ochranu budovy, zařízení a zaměstnanců.
- Finanční řízení: Hospodaří s prostředky na provoz údržby budovy, zařízení a dále je s tím také spojeno rozpočtování, plánování nákladů a sledování výdajů.
- Projektové řízení: Zahrnuje plánování a provedení projektů souvisejících se správou a údržbou budov a infrastruktury.

Zodpovídá také za zpracování plánů obnovy fyzické infrastruktury v případě jejich zničení mimořádnou událostí. Cílem tohoto odboru je především zajistit bezproblémový a efektivní chod pracovního prostředí, které podporuje produktivitu zaměstnanců.

Úseky podléhající pod Chief Digital Officera jsou odpovědné za zajištění zdrojů informačních technologií nezbytných k udržení nebo obnovení kritických nebo životně důležitých činností a služeb banky. Pod tento úsek spadají například tyto oddělení: Oddělení digitálního marketingu a obchodu, Oddělení IT a technologii, Oddělení digitální transformace. Tento úsek je odpovědný za řízení kontinuity činností informačních a komunikačních technologií v rámci systému řízení bezpečnosti informací banky. Poskytování služeb informačních a komunikačních technologií musí být obnoveno v nezbytném rozsahu a včas na základě uzavřených dohod o rozsahu v případě, že jejich poskytování naruší mimořádná událost.

Oddělení Brand Strategy and Communication je odpovědné za řízení externí a interní krizové komunikace v případě mimořádné události či situace, která může svou povahou vážně poškodit nebo narušit obchodní aktivity banky nebo poškodit její image na veřejnosti.

Oddělení lidských zdrojů odpovídá za vytvoření vhodné politiky řízení lidských zdrojů v případě mimořádných událostí a situací, která respektuje platnou legislativu v České republice a principy stanovené bankou. Kromě toho je ve spolupráci se všemi dotčenými útvary zodpovědný za zajištění vhodného a cíleného pravidelného školení zaměstnanců v oblasti systému řízení kontinuity provozu banky.

5.6.3 Kontrola a monitoring

Za kontrolu systému řízení rizik, jeho rozsahu a přiměřenosti, včetně systému pro nastavení úrovně a souladu s interními předpisy, by měly odpovídat útvary operačního rizika v rámci útvaru řízení rizik nebo další útvary v rámci útvaru strategie a financí nebo útvary

kontroly v rámci odborných oblastí. Zpráva o provedených auditech by měla být pravidelně předkládána představenstvu banky a auditnímu výboru dozorčí rady.

Při zpracování metody McKinseyho modelu 7 S v bodě systémy, již byl zmíněn monitoring a kontrola při zpracování akčních plánu ve vybrané bankovní instituci. Monitoring a jejich implementaci zajišťuje odbor operačních rizik s nezávislými týmy, které jsou zapojeny do oblastí řízení rizik, strategie a financí a spadají do odpovědnosti člena představenstva odpovědného za oblast compliance. Proto bych i nadále doporučovala držet se této permanentní formalizované kontroly 1. stupně a 2. stupně a pravidelného monitorování alespoň jednou ročně i u operačních rizik zjištěných v této diplomové práci.

6 DISKUSE

Při zpracování diplomové práce jsem spatřila přínosy pro vybranou bankovní instituci v následujících úsecích: implementace strategie, vymezení odpovědnosti – zlepšení komunikace jednotlivých oddělení a možná spolupráce při tvorbě opatření k minimalizaci jednotlivých operačních rizik, kontrola a monitoring – pravidelná kontrola i u operačních rizik zjištěných pomocí metody RIPRAN. Tyto jednotlivé úseky spadají pod návrh strategie operačních rizik řízených ve vybrané bankovní instituci.

Tyto návrhy jsem konzultovala s vedením vybrané bankovní instituce a dospěli jsme k závěru, že pro společnost jsou tyto návrhy jistě určitým přínosem, ale v rámci rozsahu společnosti, která má hlavní sídlo v zahraničí je implementace do interních postupů při řízení rizik návrhů velmi nepravděpodobná.

7 ZÁVĚR

Tato diplomová práce si kladla za cíl identifikovat, analyzovat a zhodnotit operační rizika ve vybrané bankovní instituci, včetně návrhu opatření vedoucích ke snížení rizik.

Pro naplnění hlavního cíle byly vypracovány i dílčí cíle práce, které vytváří komplexní propojení této diplomové práce. V úvodu práce jsem stanovila teoretická východiska práce a z těchto jsem dále vycházela při zpracování práce. Identifikaci a klasifikaci rizika jsem provedla na základě studia interních dokumentů instituce, ke kterým mi jako zaměstnanci byl umožněn přístup. Tyto dokumenty obsahují identifikaci operačních rizik s ohledem na jejich finanční dopad.

Na základě komparace zvolených metod vychází operační rizika chybného zachycení transakce a krádeže, podvody, zpronevěry spáchané třetí stranou s výjimkou počítačové kriminality jako rizika s největším potenciálem poškodit vybranou bankovní instituci.

Z analýzy Pestle vyplývá, že vnější technické faktory označili právě operační riziko krádeže, podvody, zpronevěry spáchané třetí stranou s výjimkou počítačové kriminality. Toto riziko se potvrdilo i při analýze metodou RIPRAN, návrh opatření za pomocí implementace bezpečnostních zásad a postupů pro zaměstnance, včetně školení týkajících se rozpoznávání a odhalování prevence podvodů, zpronevěry a krádeží by měl tuto celkovou hodnotu rizika snížit na střední hodnotu, která poté má nižší finanční dopad na vybranou instituci.

McKinseyho model 7 S zachycuje v položce styl vedení riziko chybného zachycení transakce. Tyto zásady a postupy pokrývají všechny typy shromažďování, hodnocení, monitorování a kontroly/zmírňování jednotlivých rizik stanovením explicitních odpovědností každého zaměstnance a zajištěním auditní stopy.

Metodou RIPRAN bylo vyhodnoceno i toto riziko s vysokou celkovou hodnotou. Návrh opatření, které spočívá v důkladném školení zaměstnanců o procesu evidence a provádění transakcí. Toto školení by mělo zahrnovat identifikaci chybových situací a správné postupy k jejich řešení. Zavedení dvojité kontroly, kdy každou transakci kontrolují a schvalují dva nezávislí lidé, aby se minimalizovalo riziko nesprávného provedení příkazu, by mělo tuto celkovou hodnotu rizika snížit také na střední hodnotu, která má finanční dopad na vybranou instituci snížit. Poté jsem zpracovala návrh strategie operačních rizik pro zkvalitnění řízení rizik ve vybrané instituci.

Výsledky práce jsem komunikovala s vedením vybrané bankovní instituce a s ohledem na to, že se jedná o nadnárodní korporaci, je implementace výsledků mé práce velmi nepravděpodobná. Nicméně tímto bych ráda poděkovala vedení společnosti za to, že při

zpracování této diplomové práce jsem si rozšířila svoje znalosti o praktické zkušenosti v oblasti řízení rizik v bankovnictví. Dále jsem zde aplikovala teoretické znalosti získané při studiu, zejména v oblasti řízení rizik. Největším přínosem při zpracování pro mne byla konfrontace s reálným prostředím fungující bankovní instituce.

8 PŘÍLOHA Č. 1 – METODA RIPRAN

Kategorie	ID	Hrozba	Scénář	Pravděpodobnost	Dopad	Hodnota rizika	Návrhy na opatření	Nová hodnota rizika	Náklady na opatření	Zodpovědnost pro zajištění	Poznámka
Obchodní spory	1.	Pochybení v oblasti řízení zákaznických stížností	Neodůvodněné překážky bránící klientovi stěžovat si. Pozdní odeslání potvrzení o přijetí reklamace klienta, nedodržení zákonných lhůt.	Nízká	Malý	Nízká	Pravidelná kontrola procesů vyřizování stížností a reklamací, aby se případné nedostatky nebo zpoždění daly rychleji vyřešit. Klientům by měla také být poskytnuta možnost zpětné vazby v návaznosti na jejich zkušenosti s procesem řešení stížností.	Nízká	Nízké	Úsek Brand Strategy and Communication	Vypracování strategie pro efektivní komunikaci se zákazníky a řešení jejich stížností tak, abyste nepoškodili jméno organizace.
	2.	Nevhodné obchodní praktiky	Příliš agresivní obchodní praktiky, špatně definovaný segment prodeje, nerovné zvláštní výhody určitým klientům, konflikt zájmů.	Nízká	Malý	Nízká	Přísnější kontrola vzdělávání zaměstnanců o etických standardech a důležitosti dodržování pravidel pro zachování integrity v obchodních transakcích. Zaměstnanci by měli být informováni o důsledcích příliš agresivních obchodních praktik a střetu zájmů.	Nízká	Nízké	Odbor Compliance	Sledování a kontrola chování zaměstnanců a řízení etických standardů v organizaci.
	3.	Neadekvátní nabídka produktů	Produkt se nehodí potřebám klienta, (vzniklo nedorozumění ohledně výnosu nebo rizika produktu).	Střední	Malý	Nízká	Personál zapojený do prodeje produktu by měl být plně proškolen o jeho vlastnostech, výnosech, rizicích a vhodnosti pro odlišné typy klientů. Díky tomu mohou klientům poskytnout všechny potřebné informace a odpovědět na jejich dotazy.	Nízká	Nízké	Úsek Brand Strategy and Communication	Vyhodnocení zpětné vazby od klientů a vyvíjení strategie ke zlepšení nabídky produktů, aby lépe vyhovovaly poptávce trhu a očekáváním spotřebitelů.
	4.	Neadekvátní péče o klienta	Nevhodná komunikace s klientem, malá schopnost reagovat na podněty klienta, narušení roviny smluvního vztahu, porušení povinnosti poskytnout klientovi nejlepší služby, neúmyslné chyby banky při provádění klientských pokynů, které banka neodhalila a nenapravila dříve, než na ně byla klientem upozorněna.	Vysoká	Malý	**Střední**	Poskytování školení nebo podpory pro zlepšení schopností zaměstnanců v péči o klienta.	Nízká	**Střední**	Úsek lidských zdrojů	Jestliže dojde k neúmyslným chybám banky, které mají negativní dopad na klienta, měla by za tyto chyby převzít odpovědnost a poskytnout klientovi přiměřenou náhradu nebo nápravu.
	5.	Další spory s třetí stranou	Nedodržení smluvních podmínek z důvodu chyby nebo přehlédnutí ze strany banky, rozpory mezi účastníky smluvního vztahu.	Střední	Malý	Nízká	Smluvní podmínky a jejich změny by banka měla zákazníkům sdělovat jasným a srozumitelným způsobem. To zahrnuje poskytování informací před uzavřením smlouvy a pravidelnou komunikaci po celou dobu trvání smluvního vztahu.	Nízká	Nízké	Právní oddělení	Poskytování právního poradenství, posuzování právních rizik, vyjednávání s protistranami.
	6.	Nevymahatelné kontrakty nebo podmínky smluv	Nejasnosti, chyby, zavádějící podmínky, chybějící dokumentace, protiprávní podmínky, jednání právnické osoby mimo rámec její působnosti.	Střední	Malý	Nízká	Zaměstnanci banky by měli být pravidelně proškolováni o důležitosti dodržování právních předpisů a norem při tvorbě a poskytování smluvních podmínek. Školení by mělo být zaměřeno i na identifikaci a prevenci nejasností nebo protiprávních podmínek.	Nízká	Nízké	Právní oddělení/Úsek lidských zdrojů	Spolupráce při zajištění kvalitního školení zaměstnanců o dodržování právních předpisů banky.

Kategorie	ID	Hrozba	Scénář	Pravděpodobnost	Dopad	Hodnota rizika	Návrhy na opatření	Nová hodnota rizika	Náklady na opatření	Zodpovědnost pro zajištění	Poznámka
Spory s veřejnými orgány	1.	Porušení bankovních a finančních zákonů s výjimkou embarg a sankcí	Porušení např. Zákon o bankách, Vyhlášky ministerstva financí, Opatření ČNB, požadavek na kapitálovou přiměřenost, limity úvěrové angažovanosti.	Vysoká	Malý	**Střední**	Pravidelné revize a audity odpovědným kontrolním oddělení, aby se zjistily a opravily případné nedostatky v dodržování předpisů. Pravidelné seznámení zaměstnanců s důležitými předpisy a povinnostmi a jejich případných změnách.	Nízká	**Střední**	Úsek interního auditu	Minimalizace rizika nedodržení zákonných požadavků a ochrana společnosti před možnými právními důsledky souvisejícími s porušením bankovních a finančních zákonů.
	2.	Porušení zákonů související s ochranou životního prostředí a závazků skupiny k CSR	Nevyhovění zákonům nebo nereagování na změny v zákonech, které zakazují nebo omezují diskriminace dle rasy, pohlaví, věku, schopností, náboženství apod. Porušení právních předpisů v oblasti životního prostředí.	Nízká	Malý	Nízká	Zajištění pravidelných školení zaměstnanců, které by mělo obsahovat informace o aktuálních zákonech týkajících se ochrany životního prostředí a diskriminace. Dále informace o obchodních závazcích a důraz na důsledky nedodržení právních předpisů.	Nízká	Nízké	Úsek Lidské zdroje	Poskytování školení o udržitelnosti a ESG pravidelech skupiny.
	3.	Porušení nařízení související s pracovní legislativou	Nevyhovění zákonům nebo nereagování na změny v zákonech v oblasti pracovního práva (zákoník práce apod.).	Nízká	Malý	Nízká	Provádění pravidelných aktualizací pracovněprávních předpisů a vnitřních postupů v souladu se změnami pracovněprávních předpisů. To by mělo zahrnovat pravidelnou kontrolu právních požadavků a implementaci nezbytných změn.	Nízká	Nízké	Úsek Lidské zdroje	Oddělení je odpovědné za řízení zaměstnanců a zajišťování dodržování pracovněprávních předpisů, provádění školení zaměstnanců a sledování dodržování pracovněprávních předpisů
	4.	Porušení bezpečnostních standardů, nebo selhání při ochraně zdraví	Nevyhovění zákonům nebo nereagování na změny v zákonech. Nesplnění povinností zaměstnavatele v oblasti fyzické a duševní bezpečnosti.	Nízká	Malý	Nízká	Zřízení kontrolního týmu odpovědného za sledování a interpretaci nových a stávajících zákonů. Pravidelné revize interních postupů a zásad tak, aby odpovídaly aktuálním zákonným požadavkům.	Nízká	Nízké	Odbor Podpůrné služby & facility management	Schvalování a udržování pracovního prostředí a zařízení včetně bezpečnostních opatření a zařízení k ochraně zdraví zaměstnanců.
	5.	Porušení požadavků / pravidel trhu s výjimkou zneužití trhu	Nevyhovění zákonům nebo nereagování na změny v zákonech, upravujících obchodování na veřejných trzích.	Nízká	Malý	Nízká	Pravidelný audit a revize interních procesů a kontrolních mechanismů, které zajišťují soulad s právními předpisy.	Nízká	Nízké	Úsek interního auditu	Zajištění, aby společnost splňovala všechny platné právní požadavky, a minimalizovala rizika nedodržení zákonů na veřejných trzích.
	6.	Zneužití trhu	Nevyhovění zákonům nebo nereagování na změny v zákonech.	Nízká	Malý	Nízká	Pravidelně revidovat interní postupy a zásady, aby zajistily, že budou v souladu s aktuálními právními požadavky. Pokud se zákony nebo předpisy změní, měly by být rychle implementovány do interních procesů.	Nízká	Nízké	Odbor Compliance	
	7.	Nedodržení embarg a sankcí	Provádění transakce nebo operace s protistranou zahrnutou v seznamu sankcí a embarga z důvodu selhání, například: - Identifikace zákazníka v procesu; - Před zahájení, operace nejsou přezkoumány seznamy sankcí a embarg.	Nízká	Malý	Nízká	Pravidelné provádění procesů kontroly, které by měly zahrnovat důkladnou identifikaci klientů – tzv. KYC kontrolu. Součástí by mělo být školení zaměstnanců ohledně této kontroly: ověření identity, sledování transakcí, kontrola všech důležitých dokumentů pro banku, aby se identifikovaly potenciální rizikové osoby.	Nízká	Nízké	Odbor Compliance	Implementovat procesy a postupy, které minimalizují riziko provádění transakcí s protistranami uvedenými na seznamu sankcí a embarg.
	8.	Porušení požadavků na regulaci, účetnictví a finanční výkaznictví	Nevyhovění zákonům nebo nereagování na změny v daňových zákonech.	Nízká	Malý	Nízká	Řádné školení zaměstnanců o aktuálních daňových zákonech a jejich změnách. To může zahrnovat závazek banky dodržovat nové daňové předpisy a postupy pro identifikaci a řešení daňových problémů.	Nízká	Nízké	Úsek lidských zdrojů	Minimalizovat riziko nedodržení regulačních požadavků a daňových zákonů a ochrana společnosti před právními a finančními důsledky spojenými s porušením těchto pravidel.
	9.	Porušení zákonných opatření v oblasti daňové legislativy	Nevyhovění zákonům nebo nereagování na změny v daňových zákonech.	Nízká	Malý	Nízká	Zajištění pravidelných školení zaměstnanců v oblasti daňové legislativy a změn daňových zákonů. Toto školení by mělo být povinné a mělo by se zaměřit na konkrétní pracovní oblasti pro jednotlivé zaměstnance.	Nízká	Nízké	Úsek lidských zdrojů	
	10.	Porušení pravidel týkajících se boje proti praní špinavých peněz a financování terorismu	Selhání při vzdělávání zaměstnanců na téma praní špinavých peněz, selhání při identifikaci protistrany/původu peněz, nevedení dostatečné evidence, opomenutí vykazování podezření o praní špinavých peněz.	Nízká	Malý	Nízká	Pravidelná komplexní školení a aktualizace interních postupů, aby byly zaměstnancům poskytovány zásady a a procesy pro identifikaci podezřelých aktivit a řádné hlášení podezření.	Nízká	Nízké	Odbor Compliance/Úsek lidskcých zdrojů	Spolupráve při tvorbě školení zaměstnanců ohledně interních postupů v organizaci.
	11.	Porušení zákonů o ochraně dat klientů a zaměstnanců	Nevyhovění zákonům nebo nereagování na změny v zákonech.	Nízká	Malý	Nízká	Pravidelné školení zaměstnanců o platných zákonech a požadavcích. Zaměstnanci by také měli být schopni rozpoznat a řešit situace, které by mohly vést k porušení zákona.	Nízká	Nízké	Úsek lidských zdrojů	
	12.	Nedodržování kodexu chování skupiny včetně nevhodného chování zaměstnanců	Pomlouvání vedení ze strany zaměstnance na sociální síti.	Nízká	Malý	Nízká	Pravidelná komunikace a udržení otevřené transparentní komunikační kultury by mohlo pomoci úplně odstranit potencionální pobídky k pomlouvání vedení na sociálních sítích a snížit frustraci zaměstnanců.	Nízká	Nízké	Úsek Brand Strategy and Communication	
	13.	Porušení ostatních vnějších povinností chování	Nedodržování pravidel chování na trhu. Porušení zásady jednat se zákazníky spravedlivě a v jejich zájmu.	Nízká	Malý	Nízká	Banka by měla posílit interní monitoring chování zaměstnanců a komunikaci s klienty. Toto opatření může i zahrnovat pravidelné schůzky vedení s obchodními týmy, ohledně etiky a dodržování předpisů.	Nízká	Nízké	Odbor Compliance	

Kategorie	ID	Hrozba	Scénář	Pravděpodobnost	Dopad	Hodnota rizika	Návrhy na opatření	Nová hodnota rizika	Náklady na opatření	Zodpovědnost pro zajištění	Poznámka
Chyby v odhadu rizika nebo ocenění	1.	Nedostatky v procesu řízení a sledování limitů a oprávnění	Nedostatky při vyplňování formulářů na přidělení limitů, neúmyslné porušení metodiky na přidělování limitů, přidělení chybných limitů, nedodání notifikace, různé údaje odsouhlasené klientem a obsažené v notifikaci, nedostatky při sledování limitů, neadekvátní vykazování v této oblasti.	Střední	Malý	Nízká	Pravidelné školení zaměstnanců o zásadách ochrany osobních údajů a jejich povinnostech v souladu s platnými právními předpisy, které by mělo obsahovat i informace o tom, jak správně nakládat s osobními údaji klientů, jak reagovat a rozpoznat na bezpečnostní incidenty, při dodržení interní politiky a postupu v této oblasti.	Nízká	Nízké	Úsek lidských zdrojů	
	2.	Neexistující nebo chybné ocenění pozice	Chybné pozice, nesprávné ceny, chybějící ceny.	Nízká	Malý	Nízká	Provádění pravidelné revize a kontroly obchodních pozic, informací o cenách a obchodních transakcí. Toto opatření by pomohlo identifikovat a odhalit případné chyby nebo nesrovnalosti dříve.	Nízká	Nízké	Úsek lidských zdrojů	
	3.	Špatné informace z trhu	Neexistence přímého přístupu k tržním datům, nedůkladná analýza trhu, nesprávné použití tržních dat.	Nízká	Malý	Nízká	Pravidelná aktualizace analýz trhu na základě nových dat a informací. Seznámení zaměstnanců s metodologiemi analýzy trhu a přesným použitím tržních informací při své práci.	Nízká	Nízké	Úsek lidských zdrojů	
	4.	Chyby v oceňovacích nebo rizikových modelech	Chyby v předpokladech modelu (například pro přidělení ratingu nebo model výpočtu tržní ceny finančního derivátu), chyby v metodologii, nesprávné vstupy nebo výstupy.	Nízká	Malý	Nízká	Zajištění kvality vstupních dat, které by mělo zahrnovat důkladnou kontrolu dat a identifikaci možných chyb či nesrovnalostí. Zkvalitnění procesů kontroly a ověřování vstupních dat a sledování jejich kvality.	Nízká	Nízké	Úsek spadající pod Chief Digital Officera	

Kategorie	ID	Hrozba	Scénář	Pravděpodobnost	Dopad	Hodnota rizika	Návrhy na opatření	Nová hodnota rizika	Náklady na opatření	Zodpovědnost pro zajištění	Poznámka
Chyby při provádění pokynů	1.	Chyby vznikající v obecné administrativě po dobu trvání transakce	Neposlání konfirmace, nepřijetí konfirmace, nekonfirmováni všech parametrů obchodu, nedostatečná rychlost při výměně konfirmací, nesouhlasící konfirmace, zanedbání řešení sporných konfirmací.	Vysoká	Malý	**Střední**	Dodržování postupů pro administrativní práci související s dobou trvání transakce, včetně procesů pro odesílání a přijímání potvrzení. Zlepšení komunikace mezi zaměstnanci a mezi bankou a klienty tak, aby bylo možné rychleji řešit případné problémy či nedorozumění ohledně konfirmací.	Nízká	**Střední**	Odbor Compliance	
	2.	Chybné zachycení transakce	Chyby při manuálním typování, nedostatek znalostí / dovedností / pochopení procesu, špatné použití systému, nedorozumění, přeslechnutí instrukcí, zaměnění buy/sell za sell/buy operaci, chybné provedení příkazu.	Vysoká	Střední	**Vysoká**	Důkladné školení zaměstnanců o procesu evidence a provádění transakcí. Toto školení by mělo zahrnovat identifikaci chybových situací a správné postupy k jejich řešení. Zavedení dvojité kontroly, kdy každou transakci kontrolují a schvalují dva nezávislí lidé, aby se minimalizovalo riziko nesprávného provedení příkazu.	**Střední**	**Vysoké**	Úsek lidských zdrojů	
	3.	Nepřesné informace pro management	Neexistence reportů na vykazování výjimek, chybné vykazování, pozdní vykazování, nevhodné vykazování.	Vysoká	Malý	**Střední**	Pravidelné školení zaměstnanců odpovědných za přípravu a hlášení informací vedení tak, aby byli obeznámeni s požadavky a standardy organizace.	Nízká	**Střední**	Úsek lidských zdrojů/Odbor Compliance	Spolupráce ohledně školení zaměstnanců o nastavených interních standardech organizace.
	4.	Nevhodná organizační struktura	Nedostatečné oddělení funkcí, nedodržování pravidla "čtyř očí", neexistence nezávislého dohledu, nejasně definované zodpovědnosti, chybějící strategie organizace, neadekvátní procedury, neadekvátní stálý dohled.	Střední	Malý	Nízká	Důkladné posouzení stávající organizační struktury a přepracování, aby odpovídala potřebám a cílům organizace. Stanovit jednoznačné odpovědnosti a pravomoci pro každého zaměstnance, aby bylo jasné, kdo je za jaké činnosti a rozhodnutí zodpovědný	Nízká	Nízké	Úsek lidských zdrojů	
	5.	Absence nebo selhání kontrolního prostředí	Nedostatečné oddělení funkcí, nedodržování pravidla "čtyř očí", neexistence nezávislého dohledu, nejasně definované zodpovědnosti, chybějící strategie organizace, neadekvátní procedury, neadekvátní stálý dohled.	Nízká	Malý	Nízká	Pravidelné revize a sledování výkonnosti všech činností organizace. Udržování efektivního kontrolního prostředí, které zahrnuje všechny nezbytné prvky, jako je interní audit, řízení rizik, dodržování předpisů a etických standardů.	Nízká	Nízké	Odbor Compliance	Minimalizace rizika selhání řídícího prostředí pomocí vhodných systémů řízení a sledování souladu s pracovními postupy a zásadami organizace.
	6.	Nedostatečná ochrana týkající se dokumentů nebo cenných aktiv držených jménem třetích stran	Neadekvátní pravidla bezpečnosti, nedostatečné záznamy o uchovávaných cenných papírech, nedbalostí způsobené zničení nebo ztráta klientských aktiv.	Nízká	Malý	Nízká	Přísné dodržování protokolů pro vedení podrobných záznamů o všech držených cenných papírech a klientských aktivitách. Tyto záznamy by měly být pravidelně aktualizovány a uloženy v zabezpečeném a přístupném úložišti.	Nízká	Nízké	Úsek spadající pod Chief Digital Officera	Průběžná kontrola a správa bezpečného a dostatečného uložiště v rámci IT bezpečnost.
	7.	Selhání dodání sjednané služby třetí stranou nebo outsourcující společností s vyjimkou počítačové kriminality	Špatná kvalita služeb, služby nedodané včas, porušení sjednaných pravidel třetí stranou.	Střední	Malý	Nízká	Pravidelné vyhodnocování a aktualizace procesů a postupů pro kontrolu a sledování outsourcovaných služeb s cílem neustálého zlepšování výkonnosti a minimalizace rizik.	Nízká	Nízké	Úsek spadající pod Chief Digital Officera	
	8.	Chyby při rekonciliaci	Nedostatečná rekonciliace, nesprávná rekonciliace, rekonciliace neprovedená včas.	Nízká	Malý	Nízká	Pravidelné a systematické kontroly ze strany interních auditorů nebo speciálně určených týmů, které sledují procesy rekonciliace a identifikují potenciální problémy.	Nízká	Nízké	Úsek interního auditu	Vyhodnocování efektivity kontrolních a preventivních mechanismů.
	9.	Selhání správy účtů zákazníků / protistran, včetně neoprávněného přístupu na klientský účet	Neplatné instrukce, chybné záznamy o klientovi.	Nízká	Malý	Nízká	Provádění komplexních školení pro zaměstnance banky v oblasti řízení zákazníků a procesů souvisejících s příjmem a zpracováním jejich instrukcí. Zaměření se na identifikaci neplatných pokynů a vedení řádných záznamů.	Nízká	Nízké	Úsek lidských zdrojů	
	10.	Selhání reportingu zákaznikovi nebo protistraně	Nerealizování záruky, na kterou má banka právo, zanedbání při vyřizování margin calls, neúmyslné opomenutí uplatnění opce.	Nízká	Malý	Nízká	Zajištění jasné a pravidelné komunikace mezi bankou a klienty ohledně záruk, margin calls a uplatnění opcí. Tato komunikace by měla být písemná a zdokumentovaná.	Nízká	Nízké	Úsek spadající pod Chief Digital Officera	Maximalizace spolehlivosti a efektivity digitálního reportingu a minimalizace rizika nesrovnalostí a nepřesností při komunikaci se zákazníky a protistranami.

Kategorie	ID	Hrozba	Scénář	Pravděpodobnost	Dopad	Hodnota rizika	Návrhy na opatření	Nová hodnota rizika	Náklady na opatření	Zodpovědnost pro zajištění	Poznámka
Podvody	1.	Trestné činy proti bankovním aktivům od třetí strany s výjimkou počítačové kriminality	Útok na pobočku banky, žhářství, sabotáž, terorismus.	Nízká	Malý	Nízká	Vyškolení zaměstnanců v bezpečnostních postupech a reakci na mimořádné události, včetně pokynů v případě útoku, žhářství nebo teroristického útoku.	Nízká	Nízké	Odbor Podpůrné služby & facility management/Úsek lidských zdrojů	Spolupráce ohledně školení o bezpečnostních postupech zaměstnanců.
	2.	Krádeže, podvody, zpronevěry spáchané třetí stranou s výjimkou počítačové kriminality	Falešná identita, nadsazování finančních výsledků, obejití bezpečnostních pravidel, padělané dokumenty, vydírání, neoprávněné vynucování něčeho, defraudace a zpronevěra, loupežné přepadení, krádež.	Střední	Velký	Vysoká	Implementace bezpečnostních zásad a postupů pro zaměstnance, včetně školení týkajících se rozpoznávání a odhalování prevence podvodů, zpronevěry a krádeží.	**Střední**	Vysoké	Úsek lidských zdrojů	Ochrana společnosti před různými formami podvodů a zpronevěry a zajištění dodržování všech příslušných právních a etických norem.
	3.	Krádež spáchaná zaměstnancem banky	Krádež nebo zneužití peněžních prostředků, krádež fyzického nebo duševního vlastnictví banky.	Nízká	Malý	Nízká	Poskytování pravidelných školení zaměstnanců o bezpečnostních postupech, etice a zásadách ochrany duševního vlastnictví banky.	Nízká	Nízké	Odbor Compliance	
	4.	Podvodné transakce (provedené přímo zaměstnancem nebo jeho zapojením)	Úmyslné porušení limitů, zneužití postupů pro oceňování kreditního rizika, fiktivní transakce, padělání záznamů o transakci, obchodování s nepovolenými produkty, obchodování s klienty, s nimiž bylo obchodování zakázáno, opakování obchodu za účelem generování zisku.	Střední	Malý	Nízká	Pravidelní školení zaměstnanců o etických a právních požadavcích obchodování, včetně zdůrazňování dodržování limitů, řádného vedení záznamů a vyhýbání se neoprávněným činnostem.	Nízká	Nízké	Odbor Compliance	
	5.	Neoprávněné/nesprávné/nedbalostní použití důvěrných informací interními stranami (zaměstnanci / dodavatelé, kteří jsou zaměstnáni bankou / stážisty)	Insider trading na účet klienta, porušení politiky čínských zdí (informace získané o klientovi v rámci aktivit na kapitálových trzích by neměly být použity při rozhodování o přidělení úvěru).	Vysoká	Malý	**Střední**	Pravidelné vzdělávání a školení zaměstnancům, smluvním partnerům a stážistům o důležitosti ochrany důvěrných informací, právních a etických povinnostech a důsledcích nedodržování těchto pravidel.	Nízká	**Střední**	Odbor Compliance	
	6.	Počítačová kriminalita na PC systémech zákazníků třetími stranami	Falešná identita, nadsazování finančních výsledků, obejití bezpečnostních pravidel, padělané dokumenty, vydírání, neoprávněné vynucování něčeho, zpronevěra, krádež.	Nízká	Malý	Nízká	Poskytování upozornění o hrozbách počítačové kriminality a postupech pro lepší zabezpečení systému jejich PC např. pomocí e-mailové komunikace či banneru v bankovních aplikacích využívaných klientem. To může zahrnovat seznámení s phishingem, malwarem a dalšími typy útoků.	Nízká	Nízké	Úseky spadající pod Chief Digital Officera	
	7.	Sabotáž vnitřních IT systémů banky zaměstnanci	Úmyslné porušení limitů, zneužití postupů pro oceňování kreditního rizika, fiktivní transakce, padělání záznamů o transakci, obchodování s nepovolenými produkty, obchodování s klienty, s nimiž bylo obchodování zakázáno, opakování obchodu za účelem generování zisku.	Nízká	Malý	Nízká	Pravidelné školení zaměstnanců o dodržování předpisů, etice a rizicích spojených s nezákonnými či neetickými praktikami. Zaměstnanci by měli být upozorněni na důsledky nedodržování pravidel a povinností stanovených v Etickém kodexu banky.	Nízká	Nízké	Odbor Compliance	
	8.	Korupce	Úmyslné porušení limitů, zneužití postupů pro oceňování kreditního rizika, fiktivní transakce, padělání záznamů o transakci, obchodování s nepovolenými produkty, obchodování s klienty, s nimiž bylo obchodování zakázáno, opakování obchodu za účelem generování zisku.	Nízká	Malý	Nízká	Pravidelné školení zaměstnanců o dodržování předpisů, etice a rizicích spojených s nezákonnými či neetickými praktikami. Zaměstnanci by měli být upozorněni na důsledky nedodržování pravidel a povinností stanovených v Etickém kodexu banky.	Nízká	Nízké	Odbor Compliance	
Nepovolené obchodování	1.	Nepovolené aktivity na finančních a kapitálových trzích	Zatajení uskutečněných obchodů, vykazování neuskutečněných obchodů, falšování údajů o transakcích, úmyslné chybné použití nebo zneužití oceňovacího modelu, úmyslné porušení limitů pro tržní riziko a pro riziko protistrany, uzavření transakce se zakázaným klientem, obchodování s nepovolenými produkty nebo na nepovoleném trhu, znovu uzavírání stejné transakce kvůli poplatkům, manipulace s trhem.	Nízká	Malý	Nízká	Pravidelné školení zaměstnanců o dodržování předpisů, etice a dobrých obchodních praktikách. Zaměstnanci by si měli být vědomi rizik spojených s nezákonnými praktikami a důsledků jejich nedodržení.	Nízká	Nízké	Odbor Compliance	

Kategorie	ID	Hrozba	Scénář	Pravděpodobnost	Dopad	Hodnota rizika	Návrhy na opatření	Nová hodnota rizika	Náklady na opatření	Zodpovědnost pro zajištění	Poznámka
Ztráta provozního prostředí/kapacity	1.	Nedostatek pracovníků	Stávka, neflexibilní pracovní trh, nemožnost kvalitního vyškolení nových zaměstnanců, ztráta klíčových osob, nekonkurenční bonusový systém, nepříjemné pracovní prostředí a podmínky, neadekvátní plán na kariérní postup.	Nízká	Malý	Nízká	Revize odměňovacích systémů, poskytnutí flexibilních pracovních podmínek, investice do vybavení a školení v rámci uspokojení a dalšího rozvoje zaměstnanců.	Nízká	Nízké	Úsek lidských zdrojů	
	2.	Ztráta dat	Neadekvátní ochrana dat, nemožnost získat k datům přístup, nevhodná archivace důležitých materiálů.	Nízká	Malý	Nízká	Provádění pravidelné revize a auditů bezpečnostních opatření a postupů pro kvalitní uchovávání a zabezpečení dat.	Nízká	Nízké	Úseky spadající pod Chief Digital Officera	
	3.	Ztráta výrobních prostředků	Přírodní katastrofy (zemětřesení, oheň, záplavy, hurikán), války, nedostatečné plány pro případ katastrofy, občanské nepokoje, znárodnění.	Nízká	Malý	Nízká	Komplexní pojištění proti rizikům ztráty výrobních zdrojů v důsledku přírodních katastrof, a jiných nepředvídaných událostí. Udržovat dostatečné finanční rezervy pro případ, že by po katastrofě byla nutná rekonstrukce a obnova výrobní infrastruktury.	Nízká	Nízké	Odbor Podpůrné služby & facility management	Pojištění je obsaženo ve vnitřních předpisech banky. - odbor zaštiťuje případnou obnovu a rekonstrukci.
	4.	Ztráta klíčové služby	Selhání klíčového dodavatele / smluvního partnera, selhání nebo nedostupnost běžných služeb jako jsou například telekomunikace, elektrická energie, voda, doprava, uzavření trhů během normálních obchodních dní.	Střední	Malý	Nízká	Smluvní ustanovení, která by měli obsahovat doložky, které ukládají povinnost dodavatelů/smluvních partnerů informovat banku o možných problémech či změnách ve svých službách. Zahrnutí ustanovení o náhradním řešení v případě selhání dodavatele, jako je možnost včasného přechodu k jinému poskytovateli služeb.	Nízká	Nízké	Odbor Podpůrné služby & facility management	
Poruchy systémů	1.	Selhání hardware	Nedostatečná kapacita IT (nedostatečný diskový prostor, nebo neadekvátně výkonný stroj), zastarání hardware, pozdě provedené upgrade, nekonzistentní architektura systému, nedostatečná údržba a opravy systému.	Střední	Střední	**Střední**	Stanovení pravidelného plánu pravidelné údržby a oprav IT systémů, který zahrnuje pravidelné aktualizace softwaru, zálohování dat, kontroly výkonu a bezpečnostní audity. Zajištění, aby údržba byla prováděna včas a podle stanovených postupů.	Nízká	**Střední**	Úseky spadající pod Chief Digital Officera	Provádění pravidelné údržby a opravy hardwaru a systémů, aby se snížilo riziko jejich selhání.
	2.	Nekonzistentní data	Neexistence datových standardů, špatná údržba dat (aktualizace, spolehlivost).	Nízká	Malý	Nízká	Pravidelně udržovat a aktualizovat data, včetně pravidelné kontroly a aktualizace záznamů, odstraňování zastaralých dat a doplňování chybějících informací. Stanovení odpovědných pracovníků zodpovědných za správu dat a pravidelné aktualizace.	Nízká	Nízké	Úseky spadající pod Chief Digital Officera/Úsek lidských zdrojů	Spolupráce v rámci zajištění školení a správného výběru odpovědných zaměstnanců v IT.
	3.	Špatné řízení projektů	Neadekvátní projektové plánování, nedostatečná specifikace projektu, pochybení v dodržování jednotlivých fází projektů, nedostatečné výstupy projektu, překročený rozpočet, přerušení projektu či nedostatečné řízení změn.	Nízká	Malý	Nízká	Pravidelné kontroly a hodnocení postupu projektů s cílem identifikovat možné odchylky od plánu a přijmout včasná nápravná opatření. Zajištění školení a rozvoje zaměstnanců odpovědných za projektové řízení a specifikaci požadavků. Zkontrolovat, zda mají potřebné dovednosti a znalosti pro úspěšné řízení projektů.	Nízká	Nízké	Odbor Podpůrné služby & facility management/Úsek lidských zdrojů	Spolupráce při zajištění kvalitně proškolených zaměstnanců při řízení projektů.
	4.	Chyby v software	Nedostatečná funkčnost, chyby v programu, zastarání programu, pozdě provedené aktualizace, nedostatečně integrované jednotlivé programy a aplikace, nedostatečná obsluha.	Nízká	Malý	Nízká	Pravidelná údržba a aktualizace všech programů a aplikací v informačním systému. Instalace nejnovější verzí softwaru a zajištění, aby všechny aktualizace byly prováděny včas. Pravidelné školení zaměstnanců v používání softwaru a aplikací včetně informací o nejnovějších funkcích a postupech.	Nízká	Nízké	Úseky spadající pod Chief Digital Officera/Úsek lidských zdrojů	Spolupráce v poskytování podpory a školení uživatelům s cílem zlepšit jejich schopnost efektivně používat softwarové nástroje. Minimalizace rizik softwarových chyb a zajistit, aby IT systémy podporovaly a usnadňovaly provoz společnosti.
	5.	Nedostatečné fyzické zabezpečení	Neomezení lokálního přístupu k systémům, nedostatečná ochrana proniknutí osob k důležitým systémům, nevhodné umístění zařízení.	Nízká	Malý	Nízká	Provádění pravidelných kontrol a aktualizace bezpečnostních postupů a zásad, aby splňovali nejnovější bezpečnostní standardy. Dále pravidelná školení o bezpečnostních postupech a opatřeních prevence narušení, která by měla zahrnovat školení o rozpoznání podezřelé činnosti, správném zacházení s přihlašovacími údaji a fyzickém zabezpečení prostředí.	Nízká	Nízké	Odbor Podpůrné služby & facility management/Úsek lidských zdrojů	Minimalizace rizika nedostatečné fyzické bezpečnosti a ochrana zaměstnanců, majetku a provozu společnosti před potenciálními hrozbami a neoprávněným přístupem.

SEZNAM POUŽITÝCH ZDROJŮ

50MINUTES.COM, 2015. *The SWOT Analysis* [online]. 1. 50Minutes.com [cit. 2024-01-13]. ISBN 9782806265838. Dostupné z: https://www.50minutes.com/title/the-swot-analysis/

ANDERSON, David Ray, Dennis J. SWEENEY, Thomas Arthur WILLIAMS, Jeffrey D. CAMM, James J. COCHRAN, Michael J. FRY a Jeffrey W. OHLMANN, 2016. *Quantitative methods for business*. 13e. Boston: Cengage Learning. ISBN 978-1-285-86631-4.

BLAHOVÁ, Naďa, 2018. *Rizika bank a jejich regulace*. 1. vydání. Jesenice: Ekopress. ISBN 9788087865477.

ČESKÁ BANKOVNÍ ASOCIACE, 2023. *Finanční gramotnost Čechů 2023* [online]. [cit. 2024-02-12]. Dostupné z: https://cbaonline.cz/financni-gramotnost-cechu-2023

ČESKÁ NÁRODNÍ BANKA, 2022. *Finanční stabilita* [online]. [cit. 2024-02-12]. Dostupné z: https://www.cnb.cz/cs/o_cnb/cnblog/Zohlednovani-environmentalnich-faktoru-ve-financnim-sektoru/

ČESKÁ NÁRODNÍ BANKA, 2022. *Regulace a dohled nad kapitálovým trhem* [online]. [cit. 2024-02-12]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/postaveni-dohledu/regulace-a-dohled-nad-kapitalovym-trhem

ČESKÁ NÁRODNÍ BANKA, 2023. *Udržitelné finance* [online]. [cit. 2024-02-12]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/udrzitelne-finance/

DOLEŽAL, Jan, Pavel MÁCHAL a Branislav LACKO, 2009. *Projektový management podle IPMA*. 1. vyd. Praha: Grada. Expert (Grada). ISBN 978-80-247-.

DOLEŽAL, Jan, Pavel MÁCHAL a Branislav LACKO, 2012. *Projektový management podle IPMA*. 2., aktualiz. a dopl. vyd. Praha: Grada. Expert (Grada). ISBN 8024742756.

DOLEŽAL, Jan, Pavel MÁCHAL, Branislav LACKO a A KOL., 2012. *Projektový management podle IPMA*. 2. aktualizované a doplněné vydání. Praha: Grada Publishing a.s. ISBN 8024780348.

DVOŘÁČEK, Jiří a Peter SLUNČÍK, 2012. *Podnik a jeho okolí: jak přežít v konkurenčním prostředí*. Vyd. 1. V Praze: C. H. Beck. Beckova edice ekonomie. ISBN 8074002241.

FOTR, Jiří a Jiří HNILICA, 2014. *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování*. 2., aktualiz. a rozš. vyd. Praha: Grada. Expert (Grada). ISBN 9788024751047.

FOTR, Jiří, Emil VACÍK, Ivan SOUČEK, Miroslav ŠPAČEK a Stanislav HÁJEK, 2020. *Tvorba strategie a strategické plánování*. 2. Praha: Grada Publishing a.s. ISBN 9788027116324.

Historie ČNB, 2023. In: *ČNB* [online]. [cit. 2024-01-14]. Dostupné z: https://www.cnb.cz/cs/

HNILICA, Jiří a Jiří FOTR, 2009. *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování*. 1. vyd. Praha: Grada. Expert (Grada). ISBN isbn978-80-247-2560-4.

HNILICA, Jiří a Jiří FOTR, 2009. *Aplikovaná analýza rizika*. 1. Praha: Grada Publishing a.s. ISBN 9788024767284.

JAKUBÍKOVÁ, Dagmar, 2013. *Strategický marketing: strategie a trendy*. 2., rozš. vyd. Praha: Grada. Expert (Grada). ISBN 8024746700.

KAŠPAROVSKÁ, Vlasta, 2006. *Řízení obchodních bank: vybrané kapitoly*. Vyd. 1. Praha: C. H. Beck. ISBN 9788071793816.

KORECKÝ, Michal a Václav TRKOVSKÝ, 2011. *Management rizik projektů: se zaměřením na projekty v průmyslových podnicích*. 1. vyd. Praha: Grada. Expert (Grada). ISBN 978-80-247-3221-3.

LACKO, Branislav, 2024. RIPRAN. In: *RIPRAN* [online]. [cit. 2024-01-13]. Dostupné z: https://ripran.cz/

MALLYA, Thaddeus, 2007. *Základy strategického řízení a rozhodování*. 1. vyd. Praha: Grada. ISBN 8024719118.

MATZ, Leonard a Peter NEU, 2007. *Liquidity Risk Measurement and Management*. 1. Hoboken, New Jersey, USA: John Wiley & Sons. ISBN 9780470821824.

MINISTERSTVO FINANCÍ, 2023. *Finanční gramotnost anebo proč se finančně vzdělávat* [online]. [cit. 2024-02-12]. Dostupné z: https://financnigramotnost.mfcr.cz/cs/aktuality/2023/cesko-bude-jiz-osmym-rokem-soucasti-celo-3412/

MINISTERSTVO FINANCÍ ČESKÉ REPUBLIKY, 2024. *Lednová predikce MF* [online]. [cit. 2024-02-12]. Dostupné z: https://www.mfcr.cz/cs/ministerstvo/media/tiskove-zpravy/2024/lednova-predikce-mf-54105

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2023. *Nový zákon o kybernetické bezpečnosti je nezbytností pro Českou republiku, zaznělo ve Sněmovně* [online]. [cit. 2024-02-12]. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/1957-novy-zakon-o-kyberneticke-bezpecnosti-je-nezbytnosti-pro-ceskou-republiku-zaznelo-ve-snemovne/

OLSEN, Birgitte Egelund, 2015. *Carbon Pricing Design, Experiences and Issues* [online]. 1. Velká Británie: Edward Elgar Publishing [cit. 2024-01-14]. ISBN 9781785360237.

OSTŘÍŽEK, Jan, 2007. *Public private partnership: příležitost a výzva*. 1. vyd. Praha: C.H. Beck. C.H. Beck pro praxi. ISBN 9788071797449.

PERERA, Rashain, 2018. *The PESTLE Analysis* [online]. 1. Velká Británie: Independently Published [cit. 2024-01-15]. ISBN 1790845327.

SMEJKAL, Vladimír a Karel RAIS, 2006. *Řízení rizik ve firmách a jiných organizacích*. 2., aktualiz. a rozš. vyd. Praha: Grada. Expert (Grada). ISBN 8024716674.

SMEJKAL, Vladimír a Karel RAIS, 2009. *Řízení rizik ve firmách a jiných organizacích*. 3., rozšířené a aktualizované vydání. Praha: Grada Publishing a.s. ISBN 8024770059.

SMEJKAL, Vladimír a Karel RAIS, 2013a. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada. Expert (Grada). ISBN 8024746441.

SMEJKAL, Vladimír a Karel RAIS, 2013b. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada. Expert (Grada). ISBN isbn978-80-247-4644-9.

SRPOVÁ, Jitka, 2011. *Podnikatelský plán a strategie*. 1. vyd. Praha: Grada. Expert (Grada). ISBN 9788024741031.

STAŇKOVÁ, Anna, 2007. *Podnikáme úspěšně s malou firmou*. Vyd. 1. V Praze: C.H. Beck. C.H. Beck pro praxi. ISBN 978-80-7179-926-9.

ŠKRLA, Petr a Magda ŠKRLOVÁ, 2008. *Řízení rizik ve zdravotnických zařízeních*. 1. vyd. Praha: Grada. ISBN 9788024726168.

ŠTĚDROŇ, Bohumír, 2012. *Prognostické metody a jejich aplikace*. Vyd. 1. Praha: C.H. Beck. Beckova edice ekonomie. ISBN 8071791741.

TICHÝ, Milík, 2006. *Ovládání rizika: analýza a management*. Vyd. 1. Praha: C.H. Beck. Beckova edice ekonomie. ISBN 9788071794158.

VÁVROVÁ, Eva, 2014. *Finanční řízení komerčních pojišťoven* [online]. 1. Praha: Grada Publishing a.s. [cit. 2023-11-03]. ISBN 9788024794051.

VLACHÝ, Jan, 2006. *Řízení finančních rizik*. Praha: Vysoká škola finanční a správní. Eupress. ISBN 8086754561.

WICKHAM, Philip A., 2000. *Financial Times Corporate Strategy Casebook*. 1. London: Financial Times Management. ISBN 9780273643425.

WILSON, Chauncey, 2013. *Credible Checklists and Quality Questionnaires* [online]. 1. Amsterdam: Elsevier Science [cit. 2024-01-15]. ISBN 9780124104495.

ZAMAZALOVÁ, Marcela, 2009. *Marketing obchodní firmy*. 1. vyd. Praha: Grada. ISBN 8024720493.

ZUZÁK, Roman a Martina KÖNIGOVÁ, 2009. *Krizové řízení podniku*. 2., aktualiz. a rozš. vyd. Praha: Grada. Expert (Grada). ISBN 8024731568.

SEZNAM TABULEK

Tabulka 1: Třídy pravděpodobnosti rizika (Zdroj: (Lacko, 2024) vlastní zpracování)..... 64

Tabulka 2: Třídy dopadu operačních rizik (Zdroj: (Lacko, 2024) vlastní zpracování)..... 65

Tabulka 3: Třídy hodnoty rizika (Zdroj: (Lacko, 2024) vlastní zpracování)..... 65

Tabulka 4: Přiřazení třídy hodnoty rizika (Zdroj: (Lacko, 2024) vlastní zpracování)..... 66

Tabulka 5: Tabulka přiřazení nákladů na opatření (Zdroj: vlastní zpracování)..... 68

SEZNAM GRAFŮ

Graf č. 1:Míra inflace spotřebitelských cen v letech 2018-2024 (Zdroj: Ministerstvo financí ČR)..... 44

Graf č. 2: Míra nezaměstnanosti v letech 2018-2024 (Zdroj: Ministerstvo financí ČR)..... 45

Graf č. 3: Vývoj HDP v letech 2018-2024 (Zdroj: Ministerstvo financí ČR)..... 45

SEZNAM OBRÁZKŮ

Obrázek 1: Matice řízení rizik (Zdroj: (Zuzák, 2009, s. 46-47)..... 17

Obrázek 2:Ishikawa Diagram (Zdroj: Vlastní zpracování)..... 19

Obrázek 3: Verbální hodnoty pravděpodobnosti soustava 3x3 (Zdroj: (Doležal, 2012, s. 92)..... 24

Obrázek 4:SWOT analýza (Zdroj: vlastní zpracování)..... 30

Obrázek 5: Index Finanční gramotnosti (Zdroj: (Česká bankovní asociace, 2023))..... 47

SEZNAM ZKRATEK

Atd. – a tak dále

ČNB – Česká národní banka

ČR – Česká republika

EU – Evropská unie

HDP – Hrubý domácí produkt

IT – informační technologie

IT – Informační technologie

Např. - například

Resp. - respektive

Tzv. – takzvaně

SEZNAM PŘÍLOH

Příloha č. 1 – metoda RIPRAN