

Třídící znak							
1	0	2	0	4	5	1	0

OPATŘENÍ
ČESKÉ NÁRODNÍ BANKY
Č. 2 ZE DNE 3. ÚNORA 2004

K VNITŘNÍMU ŘÍDICÍMU A KONTROLNÍMU SYSTÉMU BANKY

Česká národní banka podle § 12, § 14 a § 15 zákona č. 21/1992 Sb., o bankách, ve znění zákona č. 126/2002 Sb., a § 24 písm.a) zákona č.6/1993 Sb., o České národní bance, ve znění zákona č. 127/2002 Sb. stanoví:

ČÁST PRVNÍ Úvodní ustanovení

§ 1 Účel opatření

- (1) Toto opatření stanoví požadavky na vnitřní řídicí a kontrolní systém banky včetně požadavků na interní audit a řízení rizik, zejména požadavky na řízení tržních rizik, úvěrového rizika, operačního rizika a rizika likvidity.
- (2) Požadavky stanovené tímto opatřením naplňuje banka s ohledem na svou velikost a způsob řízení, typ, povahu a složitost činností, které vykonává.
- (3) Požadavky stanovené tímto opatřením přiměřeně upraví banka ve své předpisové základně.
- (4) Tímto opatřením se přiměřeně řídí i pobočky zahraničních bank.

§ 2 Definice pojmů

Pro účely tohoto opatření se rozumí

- a) tržními riziky rizika ztráty banky vyplývající ze změn cen, kurzů a sazeb na finančních trzích. Jedná se o souhrnný pojem pro úrokové, měnové, akciové riziko a jiná rizika spojená s pohybem tržních cen,
- b) úvěrovým rizikem riziko ztráty banky vyplývající ze selhání smluvní strany tím, že nedostojí svým závazkům podle podmínek smlouvy, na základě které se banka stala věřitelem smluvní strany,
- c) operačním rizikem riziko ztráty banky vlivem nedostatků či selhání vnitřních procesů, lidského faktoru nebo systémů či riziko ztráty banky vlivem vnějších událostí, včetně rizika ztráty banky v důsledku porušení či nenaplnění právní normy,
- d) rizikem likvidity se rozumí riziko, že banka ztratí schopnost dostát svým finančním závazkům v době, kdy se stanou splatnými nebo nebude schopna financovat svá aktiva,
- e) řízením rizik jejich identifikace, měření/vyhodnocování, sledování a případné přijímání opatření vedoucích k omezení podstupovaných rizik,

- f) interním auditem nezávislá, objektivní, ujišťovací a konzultační činnost¹⁾ zaměřená na přidávání hodnoty a zdokonalování procesů v bance. Pomáhá bance dosahovat její cíle tím, že přináší systematický metodický přístup k hodnocení a zlepšování efektivnosti řízení rizik, řídicích a kontrolních procesů a správy a řízení organizace,
- g) interním auditorem osoba vykonávající v bance interní audit,
- h) pracovníkem osoba, která se podílí na činnosti banky na základě pracovní nebo jiné smlouvy,
- i) vrcholovým vedením obvykle vedoucí pracovníci přímo podřízení členům představenstva (s výjimkou vedoucího útvaru interního auditu). V případě, že se představenstvo nekryje s výkonným vedením banky, jedná se obvykle o vedoucí pracovníky přímo podřízené vedoucím pracovníkům na nejvyšší úrovni výkonného vedení. V odůvodněných případech může banka vymezit vrcholové vedení odlišně,
- j) celkovou strategií soubor dokumentů, který obsahuje hlavní cíle a strategická rozhodnutí v jednotlivých oblastech činnosti banky,
- k) strategií řízení rizik soubor dokumentů, které obsahují strategická rozhodnutí ohledně řízení rizik,
- l) obchodním útvarem útvar, v důsledku jehož činností vzniká bance přímo tržní či úvěrové riziko,
- m) informačním systémem funkční celek, který slouží bance k získávání, uchování, přenášení, zpracování a poskytování informací pomocí informačních technologií,
- n) informační technologií technické a programové vybavení. Technickým vybavením se rozumí hmotné technické prostředky výpočetní a komunikační techniky. Programovým vybavením se rozumí programy, procedury a pravidla nutné k tomu, aby příslušné technické vybavení plnilo požadovanou funkci,
- o) aktivem informačního systému informační technologie, informace uložené v informačním systému banky a dokumentace informačního systému,
- p) autentizací uživatele proces ověření jeho totožnosti,
- q) autorizací uživatele proces ověření jeho přístupových práv na základě autentizace,
- r) důvěrností informace zajištění, že informace je přístupná pouze uživateli, který je k přístupu oprávněn,
- s) dostupností informace zajištění, že informace je pro oprávněného uživatele přístupná ve stanovené době,
- t) integritou informace zajištění správnosti a úplnosti informace a metody jejího zpracování,
- u) pohotovostním plánem plán pro řešení mimořádných situací včetně situací havarijních,
- v) likvidní pozicí banky stav (přebytek nebo nedostatek) zdrojů v rámci stanovených časových pásem,
- w) čistým peněžním tokem rozdíl mezi přílivem a odlivem peněžních prostředků,

¹⁾ Konzultační činností se rozumí poskytování poradenství v otázkách vnitřního řídicího a kontrolního systému a/nebo v otázkách zavádění vnitřních řídicích a kontrolních mechanismů v činnostech banky interním auditorem.

- x) scénářem pro řízení rizika likvidity soubor vnitřních předpokladů (např. struktura aktiv a pasív) a vnějších předpokladů (např. vývoj na mezibankovním trhu, vývoj platební schopnosti jednotlivých zemí), na jejichž základě banka odhaduje očekávaný čistý peněžní tok a dále souhrn následných aktivit přijatých bankou za účelem pokrytí tohoto čistého peněžního toku.

§ 3

Základní požadavky na vnitřní řídicí a kontrolní systém

- (1) Banka vytvoří a udržuje účinný a efektivní vnitřní řídicí a kontrolní systém, který je zejména tvořen těmito prvky a vazbami mezi nimi:
- kontrolní prostředí (Část druhá),
 - kontrolní činnosti (Část třetí),
 - informace (Část čtvrtá),
 - řízení rizik (Část pátá), a to:
 - tržních rizik (Příloha 1),
 - úvěrového rizika (Příloha 2),
 - operačního rizika (Příloha 3) včetně požadavků na informační systémy (Příloha 4)
 - rizika likvidity (Příloha 5),
 - sledování a vyhodnocování účinnosti a efektivnosti vnitřního řídicího a kontrolního systému a náprava nedostatků (Část šestá) včetně interního auditu (Příloha 6).
- (2) Vnitřní řídicí a kontrolní systém zajistí tyto cíle:
- provádění činnosti banky v souladu s celkovou strategií banky a vnitřní předpisovou základnou,
 - aktuálnost, spolehlivost a ucelenost informací používaných bankou pro rozhodovací procesy a poskytovaných bankou třetím stranám,
 - soulad činností banky s příslušnými zákony a předpisy.
- (3) Vnitřní řídicí a kontrolní systém zahrnuje všechny činnosti a organizační složky banky.
- (4) Veškeré rozhodovací procesy a kontrolní činnosti musí být zpětně rekonstruovatelné (vysledovatelné). K naplnění tohoto požadavku banka vytvoří odpovídající systém archivace dokumentů a dat.

ČÁST DRUHÁ

Kontrolní prostředí

§ 4

Kontrolní a řídicí orgány

Banka pro udržování účinného a efektivního vnitřního řídicího a kontrolního systému zajistí, aby orgány banky a její vrcholové vedení naplňovaly požadavky stanovené v § 5, 6 a 7.

§ 5

Dozorčí rada

- (1) Dozorčí rada dohlíží na účinnost a efektivnost vnitřního řídicího a kontrolního systému banky jako celku a nejméně jednou ročně je vyhodnocuje.

- (2) Dozorčí rada se podílí na směřování, plánování a vyhodnocování činnosti interního auditu. Dozorčí rada k naplnění uvedených požadavků zvaží zřízení výboru pro audit, jehož členové jsou nezávislí na veškerých výkonných činnostech banky a mají odpovídající znalosti a zkušenosti v oblastech vnitřního řídicího a kontrolního systému a interního auditu, a vymezí jeho postavení a předmět činnosti.
- (3) Jmenování a odvolání vedoucího útvaru interního auditu je možné pouze po předchozím souhlasu dozorčí rady banky.
- (4) Dozorčí rada stanoví zásady odměňování členů představenstva a vedoucího útvaru interního auditu, pokud toto není v pravomoci valné hromady.

§ 6

Představenstvo

- (1) Představenstvo zodpovídá za vytvoření, udržování a vyhodnocování účinného a efektivního vnitřního řídicího a kontrolního systému banky.
- (2) Představenstvo schvaluje a pravidelně vyhodnocuje:
 - a) celkovou strategii banky,
 - b) strategii řízení rizik,
 - c) strategii rozvoje informačních systémů,
 - d) bezpečnostní politiku informačních systémů.
- (3) Představenstvo schvaluje funkční organizační strukturu, která mimo jiné jasně vymezuje odpovědnosti a pravomoci útvarů, pracovníků a výborů a umožňuje efektivní komunikaci a spolupráci na všech úrovních banky. Organizační struktura musí zohledňovat požadavky na oddělení neslučitelných funkcí. Představenstvo zodpovídá za pravidelné vyhodnocování funkčnosti organizační struktury.
- (4) Představenstvo zřídí útvar interního auditu²⁾, schválí jeho statut a předmět činnosti, včetně personálního a technického vybavení. Představenstvo dále schvaluje strategický a periodický plán interního auditu.
- (5) Představenstvo zodpovídá za stanovení zásad personální a mzdové politiky. Součástí těchto zásad je též požadavek, aby veškeré činnosti banky prováděli kvalifikovaní pracovníci s odpovídajícími znalostmi a zkušenostmi.
- (6) Představenstvo zodpovídá za prosazování vysoké úrovně etiky a mravní integrity pracovníků banky. K tomuto účelu stanoví pravidla, která jednoznačně formulují etické principy a předpokládané modely správného etického chování a jednání pracovníků banky. Dále představenstvo zajistí, aby všichni pracovníci banky rozuměli své úloze ve vnitřním řídicím a kontrolním systému a aktivně se do tohoto systému zapojili.
- (7) Představenstvo s vrcholovým vedením pravidelně jedná o záležitostech, které se týkají účinnosti vnitřního řídicího a kontrolního systému, a včas vyhodnocuje pravidelné zprávy i mimořádná zjištění, která jsou předkládána vrcholovým vedením, interními a externími auditory a orgány bankovního dohledu. Na základě těchto vyhodnocení přijímá představenstvo přiměřená opatření, která jsou realizována bez zbytečného odkladu.
- (8) Představenstvo banky je pravidelně informováno o expozici banky vůči tržnímu a úvěrovému riziku a o likvidní situaci banky. Představenstvo musí být informováno o všech překročeních limitů ohrožujících dodržení bankou akceptované míry tržních a

²⁾ § 8 odst. 6 zákona č. 21 / 1992 Sb.

úvěrových rizik. V případech, kdy se likvidní situace banky výrazně nepříznivě mění, musí být představenstvo informováno bez zbytečného odkladu.

§ 7

Vrcholové vedení

- (1) Vrcholové vedení zodpovídá za realizaci celkové strategie banky schválené představenstvem, za udržování funkční a efektivní organizační struktury, včetně jednoznačného vymezení odpovědností a pravomocí, a za vytvoření a udržování účinného a efektivního systému sdílení informací.
- (2) Vrcholové vedení zajistí, aby byly uplatňovány takové postupy řízení, které vedou k zamezení nežádoucích činností, kterými jsou zejména upřednostňování krátkodobých výsledků a cílů, které nejsou v souladu s naplňováním celkové strategie banky, systém odměňování, který je nepřiměřeně závislý na krátkodobém výkonu, nebo jiné postupy, které umožňují zneužití zdrojů nebo zakrývání nedostatků.

§ 8

Oddělení neslučitelných funkcí

- (1) Banka zajistí, aby útvarům, pracovníkům a jednotlivým výborům banky byly přidělovány odpovědnosti a pravomoci tak, aby bylo dostatečně zamezeno vzniku možného konfliktu zájmů. Oblasti, kde existuje možnost vzniku konfliktu zájmů, musí být včas identifikovány. Postupy banky jsou stanoveny tak, aby omezily možnosti konfliktu zájmů. Oblasti konfliktu zájmů jsou předmětem průběžného nezávislého sledování.
- (2) V bance je prováděno nezávisle na obchodních útvarech:
 - a) schvalování limitů,
 - b) schvalování oceňovacích systémů a modelů používaných pro měření a sledování tržních rizik,
 - c) schvalování systémů a metod pro oceňování zajištění,
 - d) oceňování transakcí uzavřených na finančních trzích,
 - e) oceňování zajištění,
 - f) vypořádání a rekongilace³⁾ obchodů uzavřených na finančních trzích,
 - g) uvolňování poskytnutých prostředků,
 - h) řízení tržních a úvěrových rizik (včetně kontroly dodržování limitů),
 - i) vytváření kvantitativních a kvalitativních informací o tržních a úvěrových rizicích vykazovaných členům vrcholového vedení a představenstvu,
 - j) měření a sledování likviditní pozice banky a její vykazování členům vrcholového vedení a představenstvu.
- (3) Členům představenstva⁴⁾, jimž jsou organizačně podřízeny obchodní útvary, nesmí být organizačně podřízeny útvary, které zodpovídají za:
 - a) řízení tržních rizik,
 - b) řízení úvěrových rizik,
 - c) vypořádání a rekongilaci obchodů uzavřených na finančních trzích.
- (4) V bance je prováděna odděleně správa informačních systémů od vyhodnocování bezpečnostních auditních záznamů, kontroly přidělování přístupových práv a vypracování a aktualizace bezpečnostních předpisů pro tyto systémy.

³⁾ Kontrola souladu údajů.

⁴⁾ V případě, že se představenstvo nekryje s výkonným vedením banky, oddělení musí být provedeno až do nejvyšší úrovně výkonného vedení.

- (5) Banka zajistí oddělené zajišťování vývoje a provozu informačních systémů.
- (6) Interní audit musí být vykonáván nezávisle na veškerých výkonných činnostech banky.

ČÁST TŘETÍ Kontrolní činnosti

§ 9

- (1) Kontrolní činnosti jsou součástí každodenní činnosti banky. Kontrolní činnosti zejména zahrnují:
 - a) kontrolu po linii řízení,
 - b) přiměřené kontrolní mechanismy pro jednotlivé procesy v bance⁵⁾,
 - c) fyzickou kontrolu⁶⁾.
- (2) Banka vytvoří postupy pro kontrolní činnost na všech organizačních a řídicích úrovních. Prověřování dodržování stanovených postupů a jejich dostatečnosti je prováděno pravidelně.

ČÁST ČTVRTÁ Informace

§ 10

- (1) Banka zajistí, aby dozorčí rada, výbor pro audit, pokud je zřízen, představenstvo a příslušní pracovníci, útvary nebo výbory měli pro své rozhodování k dispozici informace, které jsou aktuální, spolehlivé a ucelené.
- (2) V bance jsou k dispozici informace o:
 - a) míře podstupovaných tržních a úvěrových rizik,
 - b) srovnání míry tržních a úvěrových rizik s interními a regulačními limity,
 - c) srovnání předchozích odhadů míry podstupovaného rizika se skutečnými výsledky (zpětné testování), v případě, že banka používá metody založené na odhadu míry tržního rizika,
 - d) výsledcích stresových testů,
 - e) výsledcích analýz úvěrového portfolia,
 - f) výsledcích měření likvidity (na denní bázi, ve stanovených časových pásmech, v jednotlivých hlavních měnách, souhrnně za všechny měny),
 - g) srovnání reálného vývoje likvidity s příslušným scénářem a limity pro řízení rizika likvidity.

⁵⁾ Např. kontrola dodržování limitů, kontrola schvalování a autorizace transakcí nad stanovené limity, kontrola průběhu transakcí a činností, ověřování detailů transakcí a výstupu modelů řízení rizik používaných bankou, pravidelná reconciliace (kontrola souladu údajů).

⁶⁾ Fyzická kontrola se zaměřuje na omezení přístupu k hmotnému majetku, cenným papírům a jiným finančním aktivům a na pravidelné inventury majetku.

ČÁST PÁTÁ Řízení rizik

§ 11

Obecné požadavky

- (1) Vnitřní řídicí a kontrolní systém banky je nastaven tak, aby umožňoval soustavné řízení rizik podstupovaných bankou.
- (2) Proces identifikace rizik je zajištěn u všech činností a na všech organizačních úrovních banky a musí umožňovat odhalování nových, dosud neidentifikovaných rizik.
- (3) Proces řízení rizik zohledňuje vnitřní a vnější faktory, měřitelné a neměřitelné aspekty rizik, reálné možnosti jejich řízení a náklady a výnosy vyplývající z řízení rizik.

§ 12

Strategie řízení rizik

- (1) Banka má rozsahu své činnosti odpovídající strategii řízení rizik včetně řízení rizika likvidity, která obsahuje hlavní zásady, jež banka uplatňuje při jejich řízení. Banka vypracuje konkrétní postupy pro naplňování této strategie.
- (2) Banka zajistí, aby strategie řízení rizik a veškeré postupy a limity týkající se řízení rizik byly pravidelně vyhodnocovány a případně upravovány.
- (3) Se strategií řízení rizik musí být dostatečně seznámeni všichni pracovníci banky, jejichž činnost má vliv na řízení rizik, a kteří musí tyto činnosti vykonávat v souladu s přijatou strategií a z ní vyplývajícími postupy a limity.
- (4) Strategie řízení rizik stanoví zejména:
 - a) přijatelnou míru tržních a úvěrových rizik,
 - b) metody pro řízení tržních rizik, včetně stresového testování,
 - c) metody pro řízení úvěrového rizika,
 - d) soustavu limitů, kterou banka bude používat pro omezení tržních a úvěrových rizik,
 - e) metody pro měření a sledování rizika likvidity,
 - f) metody a postupy pro omezení rizika likvidity, včetně
 - fa) požadavků na strukturu aktiv a pasív,
 - fb) soustavy limitů, které banka bude používat,
 - g) zásady pro řízení rizika likvidity v jednotlivých hlavních měnách (tj. měnách pro banku významných z hlediska objemu),
 - h) zásady pro sestavení a úpravy pohotovostního plánu pro případ likvidní krize,
 - i) vymezení operačního rizika banky,
 - j) zásady pro řízení operačního rizika,
 - k) zásady pro vymezení povolených produktů, měn, zemí, regionů, trhů a smluvních stran.

§ 13

Nové produkty

- (1) Banka identifikuje rizika spjatá s novými produkty a aktivitami (včetně využití nových trhů či obchodování s nástroji denominovanými v jiných než dosud používaných měnách či měnových párech).
- (2) Banka zajistí, aby předtím, než se s novými produkty začne obchodovat, byly tyto produkty prověřeny přiměřenými schvalovacími a kontrolními postupy v zájmu rozlišení jejich rizikovosti a zařazení do procesu řízení rizik.
- (3) Banka stanoví postupy pro zavedení nových produktů, včetně definice, kdy se jedná o nový produkt.
- (4) Banka stanoví náležitosti, které obsahuje návrh nového produktu, a to zejména:
 - a) popis tohoto produktu,
 - b) analýzu dopadů navrhovaného produktu na banku,
 - c) identifikaci technických a lidských zdrojů, které je nutno vyčlenit na kvalitní řízení rizika tohoto produktu (včetně požadavků na informační systém),
 - d) postupy, které budou použity pro řízení rizika navrhovaného produktu,
 - e) oceňovací postupy,
 - f) definici nebo seznam povolených smluvních stran,
 - g) způsob vypořádání,
 - h) účetní, daňové a právní aspekty (včetně potřeby regulatorního souhlasu).
- (5) V bance jsou jednoznačně stanoveny pravomoci a odpovědnosti při schvalování nových produktů.
- (6) Banka zajistí, aby bylo zakázáno uzavírat transakce s neschválenými produkty.
- (7) Nové produkty mající pro banku zásadní význam schvaluje představenstvo, případně výbor, na který představenstvo tuto pravomoc delegovalo.

ČÁST ŠESTÁ

Sledování a vyhodnocování účinnosti a efektivnosti vnitřního řídicího a kontrolního systému a náprava nedostatků

§ 14

- (1) Sledování a vyhodnocování účinnosti a efektivnosti vnitřního řídicího a kontrolního systému je v bance prováděno průběžně na všech řídicích úrovních a útvarem interního auditu.
- (2) Nedostatky vnitřního řídicího a kontrolního systému odhalené po řídicí linii, útvarem interního auditu, na základě jiné kontroly či jiným způsobem, musí být včas oznámeny příslušné úrovni vedení banky a urychleně řešeny. Závažné nedostatky vnitřního řídicího a kontrolního systému musí být oznámeny představenstvu, dozorčí radě a výboru pro audit, pokud je zřízen.
- (3) Systém odhalování nedostatků vnitřního řídicího a kontrolního systému je nastaven tak, aby umožňoval jejich včasnou nápravu. Účinnost přijatých nápravných opatření musí být následně ověřována.

ČÁST SEDMÁ
Závěrečná ustanovení

§ 15
Zrušovací ustanovení

Zrušují se:

- 1) Opatření ČNB č. 2 z 27. 4. 2001 o standardech řízení likvidity bank,
- 2) Opatření ČNB č. 3 z 30. 7. 2002 o řízení úvěrového rizika v bankách,
- 3) Opatření ČNB č. 4 z 30. 7. 2002 o řízení tržních rizik v bankách,
- 4) Opatření ČNB č. 12 z 11. 12. 2002 k vnitřnímu řídicímu a kontrolnímu systému banky.

§ 16
Přechodná ustanovení

Všechny nově zaváděné informační systémy musí splňovat podmínky uvedené v příloze č. 4, čl. VI, odst. 3. Informační systémy zakoupené či instalované před platností tohoto opatření, které nevyhovují požadavku přílohy č. 4, čl. VI, odst. 3 banka upraví nebo nahradí vyhovujícími nejpozději do tří let od platnosti tohoto opatření, ČNB může na žádost banky tuto lhůtu prodloužit na pět let.

§ 17
Účinnost

Toto opatření nabývá účinnosti dnem vyhlášení, s výjimkou

- a) přílohy č. 6, která nabývá účinnosti 1.8. 2004, s výjimkou odst. 6 čl. IV, který nabývá účinnosti 1.1. 2005
- b) § 6 odst. 2 písm. c) a d), § 8 odst. 4 a 5 opatření a přílohy č. 4, které nabývají účinnosti 1.8. 2004
- c) § 8 odst. 2 písm. j) opatření, který nabývá účinnosti 1.8. 2004,
- d) § 12 odst. 4 písm. i) a j) opatření a přílohy č. 3, které nabývají účinnosti 1.1. 2005.

Guvernér
doc. Ing. Zdeněk Tůma, CSc. v.r.

Přílohy: č. 1 - 6

Sekce bankovní regulace
Odpovědný zaměstnanec:
D. Zeman, tel. 224 413 895
L. Snížková, tel. 224 412 117
E. Kozelková, tel. 224 412 126

Požadavky na řízení tržních rizik

I) Systém měření a sledování tržních rizik

- (1) Banka má takový systém měření a sledování tržních rizik, který odpovídá rozsahu aktivit banky a který podchytí všechny významné zdroje tržních rizik a vyhodnotí dopad změn v tržních sazbách a kurzech na výnosy a náklady banky a hodnotu jejích aktiv a pasív tak, aby poskytl nezkrácený obraz o míře podstupovaných rizik.
- (2) Systém měření a sledování tržních rizik musí zejména:
 - a) včasné, přesné a kompletně zaznamenat všechny transakce tak, aby byly podchyceny veškeré expozice vůči tržním rizikům,
 - b) správně tyto transakce ocenit. Pro účely oceňování je nezbytné používat ceny stanovené nezávisle na obchodních útvarech. Banka má stanoveny postupy pro oceňování včetně:
 1. detailní identifikace zdrojů dat pro přecenění,
 2. způsobu stanovení tržní ceny¹⁾ včetně použitých aproximačních metod a algoritmů použitých pro výpočet ceny v případě strukturovaných produktů,
 - c) podchytit všechny významné zdroje tržních rizik ze všech aktivit banky a vyhodnotit vliv změn v tržních mírách a kurzech způsobem konzistentním s rozsahem aktivit banky,
 - d) stanovit způsob agregace jednotlivých pozic tak, aby při agregaci nedošlo k výraznějšímu zkrácení podstupovaných rizik (např. stanovení počtu a délky gapů při gap analýze) a aby všechny významné pozice a peněžní toky citlivé na tržní riziko byly komplexně a včas systémem podchyceny,
 - e) měřit tržní rizika souhrnně za všechny obchodní jednotky banky a porovnávat velikost těchto rizik se schválenými limity ve vhodné časové periodě s ohledem na povahu podstupovaného rizika,
 - f) měřit úrokové riziko v každé měně, ve které má úrokově citlivé pozice, samostatně. Pokud je úrokové riziko měřeno ve dvou či více měnách společně, je nutné tento postup zdůvodnit (např. významnou korelací, či tím, že banka má v těchto měnách zanedbatelnou aktivitu) a jasně stanovit podmínky, za kterých je takovýto postup možný.
- (3) Banka dále zabezpečí, že:
 - a) pracovníci útvarů odpovědných za řízení tržních rizik a příslušní členové vrcholového vedení banky rozumějí předpokladům, ze kterých systém měření a sledování tržních rizik vychází,
 - b) předpoklady, ze kterých systém vychází, jsou dostatečně zdokumentovány.

¹⁾ mid, bid/ask, closing, fixing atd.

II) Limity

- (1) Banka vytvoří a dodržuje soustavu limitů pro řízení tržního rizika a postupů pro jejich využívání zajišťující, aby nebyla překročena míra tržního rizika stanovená představenstvem nebo regulatorem. Za tímto účelem banka zejména:
 - a) zajistí, aby dílčí limity tržních rizik byly využívány tak, aby nebyla překročena celková bankou akceptovaná míra tržních rizik,
 - b) zajistí, aby soustava limitů byla v souladu s postupy používanými pro měření a sledování tržních rizik a brala v úvahu ostatní rizika, kterým je banka vystavena (úvěrové, likvidity atd.),
 - c) zajistí přiměřenost soustavy limitů vzhledem ke své velikosti a způsobu řízení, komplexnosti a kapitálové přiměřenosti. V závislosti na těchto faktorech stanoví dílčí limity, např. na jednotlivé obchodní jednotky, portfolia či specifické instrumenty,
 - d) při stanovování limitů zohlední jak pozice vyplývající z denního obchodování, tak i pozice vyplývající z celkové struktury aktiv a pasív (jak rozvahových, tak i podrozvahových),
 - e) limity konstruuje tak, aby omezily dopad potenciálních změn v tržních rizikových faktorech na výnosy i na hodnotu aktiv a pasív, přičemž bere do úvahy rychlost, s jakou je schopna své pozice uzavřít.
- (2) Banka dále
 - a) zajistí, aby byly stanovené limity útvarem nebo útvary odpovědnými za řízení rizik pravidelně a při významných změnách podmínek na trhu přehodnocovány tak, aby byly v souladu s tržními podmínkami a celkovou strategií banky,
 - b) zajistí, aby soustava limitů podléhala schválení a pravidelnému přehodnocování představenstvem, případně výborem, na který představenstvo tuto pravomoc delegovalo,
 - c) u každého limitu stanoví přiměřené postupy při jeho překročení, včetně informačních toků.

III) Stresové testování

- (1) Banka provádí stresové testování pro posouzení dopadů extrémně nepříznivých tržních podmínek na banku. Banka bere tyto výsledky do úvahy při stanovování postupů a limitů pro tržní rizika tak, aby ztráty, které banka utrpí v důsledku negativních prudkých změn v tržních podmínkách, nezpůsobily její platební neschopnost či nesnížily její kapitálovou přiměřenost pod minimální hranici stanovenou regulatorem.
- (2) Stresové testování je prováděno na základě stresových scénářů. Při tvorbě stresových scénářů banka zohledňuje rizikovou charakteristiku banky, zejména faktory, vůči jejichž změně je banka nejzranitelnější.
- (3) Banka zajistí:
 - a) pravidelné provádění stresového testování, minimálně jednou za tři měsíce,
 - b) pravidelné prověřování platnosti předpokladů stresových scénářů s ohledem na měnící se podmínky na trhu nebo uvnitř banky. Změny předpokladů jsou podnětem pro úpravu scénářů a následné provedení stresových testů,
 - c) předkládání výsledků stresových testů členům vrcholového vedení banky odpovědným za řízení tržních rizik.

Požadavky na řízení úvěrového rizika

I) Systém pro provádění obchodů

- (1) Banka vypracuje systém pro provádění obchodů tak, aby byly omezeny ty subjektivní aspekty rozhodovacího procesu, které nepříspívají kvalitě tohoto procesu.
- (2) Banka zajistí, aby obchody s osobami se zvláštním vztahem k bance¹ (fyzickými nebo právníckými) byly uzavírány na základě podmínek obvyklých na daném trhu.
- (3) Banka zajistí, aby měla k dispozici informace, které jí umožní zhodnotit bonitu smluvní strany, a to i v případě syndikátních úvěrů.
- (4) Banka zajistí, aby byl každý obchod posouzen s ohledem na jeho výši a složitost.
- (5) V rámci systému pro provádění obchodů musí být v závislosti na druhu produktu a typu smluvního partnera posouzeny zejména následující aspekty:
 - a) bonita smluvní strany,
 - b) účel provedení obchodu,
 - c) zdroje splácení,
 - d) kvalita a dostatečnost zajištění,
 - e) situace v ekonomickém odvětví smluvní strany,
 - f) navrhované podmínky pro provedení obchodu.
- (6) Banka při řízení úvěrového rizika používá techniky a nástroje omezující toto riziko (např. zajištění) s tím, že použití těchto technik a nástrojů nemůže nahradit vyhodnocení bonity smluvní strany.

II) Systém měření a sledování úvěrového rizika

- (1) Banka má takový systém měření a sledování úvěrového rizika, který odpovídá rozsahu aktivit banky a který podchytí všechny významné zdroje úvěrového rizika a vyhodnotí jejich dopad na výnosy a náklady banky a hodnotu jejích aktiv a pasív tak, aby poskytl nezkreslený obraz o míře podstupovaného úvěrového rizika.
- (2) Systém měření a sledování úvěrového rizika musí zejména:
 - a) včasné, přesně a kompletně zaznamenat všechny obchody tak, aby byly podchyceny veškeré expozice banky vůči úvěrovému riziku,
 - b) vyhodnotit všechny významné zdroje úvěrového rizika,
 - c) stanovit způsob sledování expozic banky vůči ekonomicky spjatým skupinám,
 - d) měřit úvěrové riziko souhrnně za všechny obchodní jednotky banky a porovnávat velikost těchto rizik se schválenými limity ve vhodné periodě s ohledem na povahu podstupovaného rizika.
- (3) Systém měření a sledování úvěrových rizik vyplývajících z uzavřených obchodů dále musí zajistit zejména:
 - a) sledování finanční a ekonomické situace smluvní strany s ohledem na typ obchodů uzavřených s touto smluvní stranou,
 - b) sledování plnění podmínek smlouvy smluvní stranou,
 - c) sledování ocenění hodnoty zajištění,

¹⁾ § 19 zákona č. 21/1992 Sb.

- d) sledování aktuálních problémů, jež vyžadují okamžitá nápravná opatření,
 - e) sledování přiměřenosti výše opravných položek a rezerv.
- (4) Banka dále zabezpečí, že:
- a) pracovníci útvarů odpovědných za řízení úvěrového rizika a příslušní členové vrcholového vedení banky rozumějí předpokladům, ze kterých systém měření a sledování úvěrového rizika vychází,
 - b) předpoklady, ze kterých systém vychází, jsou dostatečně zdokumentovány.

III) Limity

- (1) Banka vytvoří a dodržuje soustavu limitů pro řízení úvěrového rizika a postupů pro jejich využívání zajišťující, aby nebyla překročena míra úvěrového rizika stanovená představenstvem nebo regulátorním orgánem. Za tímto účelem banka zejména:
- a) zajistí, aby dílčí limity úvěrového rizika byly využívány tak, aby nebyla překročena celková bankou akceptovaná míra úvěrového rizika,
 - b) zajistí, aby soustava limitů byla v souladu s postupy používanými pro měření a sledování úvěrového rizika a brala v úvahu ostatní rizika, kterým je banka vystavena (tržní, likvidity, atd.),
 - c) zajistí přiměřenost soustavy limitů vzhledem ke své velikosti a způsobu řízení, komplexnosti a kapitálové přiměřenosti. V závislosti na těchto faktorech stanoví dílčí limity, např. pro jednotlivé smluvní strany, jednotlivé státy a zeměpisné oblasti či pro jednotlivé činnosti,
 - d) při stanovování limitů zohlední pozice vyplývající z celkové struktury aktiv a pasív, jak rozvahových, tak i podrozvahových.
- (2) Banka dále:
- a) zajistí, aby byly stanovené limity útvarem nebo útvary odpovědnými za řízení rizik pravidelně přehodnocovány tak, aby byly v souladu s celkovou strategií banky,
 - b) zajistí, aby soustava limitů podléhala schválení a pravidelnému přehodnocování představenstvem, případně výborem, na který představenstvo tuto pravomoc delegovalo,
 - c) u každého limitu stanoví přiměřené postupy při jeho překročení, včetně informačních toků.

IV) Provádění analýz úvěrového portfolia

- (1) Banka provádí analýzy úvěrového portfolia, včetně odhadů jeho budoucího vývoje, a výsledky těchto analýz bere do úvahy při stanovování a ověřování objektivitu postupů a limitů pro řízení úvěrového rizika.
- (2) Banka přizpůsobí postupy upravující provádění analýz úvěrového portfolia podle odstavce 1 rozsahu svých úvěrových aktivit.
- (3) Banka zajistí
- a) pravidelné provádění analýz úvěrového portfolia,
 - b) pravidelné prověřování platnosti předpokladů, z nichž se při zpracování analýz vycházelo,
 - c) pravidelné předkládání výsledků analýz úvěrového portfolia členům vrcholového vedení banky odpovědným za řízení rizik.

Požadavky na řízení operačního rizika

I) Systém řízení operačního rizika

- (1) Banka vytvoří a udržuje systém řízení operačního rizika. Tento musí minimálně obsahovat:
 - a) vymezení operačního rizika,
 - b) cíle a zásady řízení operačního rizika,
 - c) postupy pro řízení operačního rizika,
 - d) pravomoci, odpovědnosti a informační toky při řízení operačního rizika na všech řídicích úrovních,
 - e) informace o významných událostech a ztrátách vzniklých v důsledku operačního rizika,
 - f) akceptovanou toleranci banky k operačnímu riziku,
 - g) způsob případného vyvedení operačního rizika mimo banku.
- (2) Banka pravidelně vyhodnocuje a případně upravuje systém pro řízení operačního rizika.

II) Identifikace, vyhodnocování a sledování operačního rizika

- (1) Banka identifikuje zdroje operačního rizika.
- (2) Banka pravidelně vyhodnocuje a sleduje možné dopady a potenciální ztráty vyplývající z událostí operačního rizika.
- (3) Sledování a vyhodnocování operačního rizika banka začlení do běžného zpracování operací.
- (4) Banka zabezpečí pravidelné informování příslušných pracovníků o podstupovaném operačním riziku souvisejícím s jejich činností.

III) Omezování operačního rizika

- (1) Banka upravuje svoji expozici vůči operačnímu riziku uplatňováním vhodných postupů omezování výskytu či negativních dopadů výskytu událostí operačního rizika.
- (2) Banka posoudí jak rizika ovlivnitelná, tak rizika stojící mimo její přímý vliv, a rozhodne, zda rizika přijme, omezí jejich případné dopady, či zda omezí nebo zcela ukončí příslušnou aktivitu. Banka pro omezování operačního rizika zavede postupy pro:
 - a) řízení přístupů pracovníků, klientů a dalších oprávněných osob k hmotnému a nehmotnému majetku banky,
 - b) řešení odezvy na případný výskyt bezpečnostních incidentů,
 - c) řešení operačních rizik při zajišťování dodávek zboží a služeb a při outsourcingu, je-li bankou uplatňován či zvažován.

IV) Kontinuita provozu a pohotovostní plánování

- (1) Pro případy neplánovaného přerušení nebo omezení svých činností, havárie informačních systémů, selhání pro banku významných třetích stran a selhání vnější infrastruktury zabezpečí banka postupy, které vedou k obnovitelnosti činností a informačních systémů významných z hlediska fungování banky.
- (2) Banka přijme pohotovostní plány pro obnovení své činnosti pro případy uvedené v odstavci 1. Pro řešení obnovy činností banky a informačních systémů musí být v plánech stanovena minimálně tato opatření:
 - a) činnost následující bezprostředně po vzniku krizové situace zaměřená na minimalizaci škod,
 - b) činnost následující po vzniku krizové situace zaměřená na likvidaci následků krizové situace,
 - c) způsob zálohování,
 - d) způsob zajištění nouzového provozu banky a informačních systémů s vyjmenováním minimálních funkcí, které musí být zachovány,
 - e) způsob zajišťování servisní činnosti informačních systémů, způsob obnovy činnosti banky a informačních systémů.
- (3) Pohotovostní plány musí být pravidelně testovány a aktualizovány.
- (4) Banka zabezpečí, aby příslušní pracovníci byli s pohotovostními plány seznámeni a postupovali podle nich.

Požadavky na informační systémy

I) Řízení informačních systémů

- (1) Banka přijme strategii rozvoje informačních systémů a postupy pro naplňování této strategie.
- (2) Banka přijme bezpečnostní politiku informačních systémů.
- (3) Bezpečnostní politika informačních systémů obsahuje:
 - a) cíle bezpečnosti informačních systémů,
 - b) hlavní zásady a postupy pro zajištění důvěrnosti, integrity a dostupnosti informací,
 - c) odpovědnosti za ochranu aktiv a plnění bezpečnostní politiky informačních systémů.
- (4) Banka zabezpečí, aby strategie rozvoje a bezpečnostní politika informačních systémů byly pravidelně vyhodnocovány a případně upravovány.
- (5) Banka zabezpečí dodržování bezpečnostní politiky v jednotlivých informačních systémech.
- (6) Banka uzavře písemnou formou smluvní vztahy s poskytovateli služeb a produktů pro informační systémy.

II) Analýza rizik

- (1) Banka musí provést analýzu rizik spjatých s informačními systémy. V ní definuje aktiva informačních systémů, hrozby, které na ně působí, zranitelná místa informačních systémů, pravděpodobnost realizace hrozeb a odhad jejich následků a protiopatření.
- (2) Banka pravidelně provádí aktualizaci analýzy rizik.

III) Bezpečnost přístupu k informacím

Banka zabezpečí:

- a) přidělení přístupových práv uživatelům v informačních systémech;
- b) jednoznačnou identifikaci a autentizaci uživatele, které musí předcházet aktivitám uživatelů v informačních systémech,
- c) přístup k informacím v informačních systémech pouze uživateli, který byl pro tento přístup autorizován,
- d) ochranu důvěrnosti a integrity autentizační informace,
- e) zaznamenávání událostí, které ohrozily nebo narušily bezpečnost informačních systémů, do bezpečnostních auditních záznamů, ochranu těchto záznamů před neautorizovaným přístupem, zejména modifikací nebo zničením, a jejich archivaci,
- f) vyhodnocování bezpečnostních auditních záznamů pracovníkem, který nemá možnost modifikovat v informačních systémech informace související s činností, o které je bezpečnostní auditní záznam pořízen.

IV) Bezpečnost komunikačních sítí

- (1) Připojení sítě, která je pod kontrolou banky, k vnější komunikační síti, která není pod kontrolou banky, musí být zabezpečeno tak, aby byla minimalizována možnost průniku do informačních systémů.
- (2) Banka zabezpečí, aby při přenosu důvěrných informací vnější komunikační síti byla zajištěna:
 - a) adekvátní důvěrnost a integrita informací,
 - b) spolehlivá identifikace a autentizace komunikujících stran, včetně ochrany identifikačních a autentizačních informací.

V) Fyzická bezpečnost informačních systémů

Na základě analýzy rizik zavede banka opatření pro fyzickou ochranu aktiv informačních systémů.

VI) Provozování informačních systémů

- (1) Při provozování informačních systémů musí být pravidelně prověřována a vyhodnocována jejich bezpečnost.
- (2) Změnu v informačních systémech je možno provést až po vyhodnocení vlivu této změny na bezpečnost informačních systémů.
- (3) V provozovaných informačních systémech může být používáno pouze otestované programové vybavení, u kterého výsledky testů prokázaly, že bezpečnostní funkce jsou v souladu s bezpečnostní politikou informačních systémů. Výsledky testů musí být dokumentovány.
- (4) Servisní činnost v provozovaných informačních systémech se musí organizovat tak, aby bylo minimalizováno ohrožení jejich bezpečnosti.
- (5) Banka zabezpečí zálohování informací a programového vybavení informačních systémů významných pro její fungování. Zálohované informace a programové vybavení musí být uloženy tak, aby byly zabezpečeny proti poškození, zničení a krádeži.

Požadavky na řízení rizika likvidity

I) Měření a sledování čistých peněžních toků

- (1) Pro účely řízení rizika likvidity musí mít banka odpovídající postupy měření a sledování čistých peněžních toků a likvidní pozice tak, aby bylo možné určit kroky banky potřebné k řízení rizika likvidity.
- (2) Postupy měření a sledování čistých peněžních toků a likvidní pozice umožňují zejména:
 - a) měření a porovnání přílivu a odlivu peněžních prostředků,
 - b) sledování čistých peněžních toků na denní bázi pro období nejméně pěti pracovních dní dopředu, sestavení kalendáře splatností a propočtu likvidní pozice. Pokud banka zařazuje aktiva do pásem s kratší splatností než by odpovídalo skutečným splatnostem těchto aktiv, musí stanovit k těmto aktivům systém diskontů, které budou odrážet tržní riziko související s rychlým odprodejem jednotlivých aktiv. Pokud banka zařazuje pasíva do pásem s delší splatností než by odpovídalo skutečným splatnostem těchto pasív, musí být banka schopna prokázat oprávněnost takovýchto přesunů.

II) Řízení rizika likvidity v jednotlivých hlavních měnách

- (1) Pro účely řízení rizika likvidity v jednotlivých měnách má banka postupy umožňující měření, sledování a kontrolu likvidity banky v každé z hlavních měn, se kterými pracuje.
- (2) Financuje-li banka aktiva držená v jedné měně pasívy drženými v jiné měně, musí analyzovat tržní podmínky, které mohou ovlivnit její přístup na devizový trh, možné podmínky směny jedné měny za jinou při různých situacích a další podmínky, jež mohou ovlivnit její přístup ke zdrojům v požadované měně.
- (3) V závislosti na objemu aktivit v jednotlivých měnách by banka měla stanovit limity pro řízení rizika likvidity, a to jak souhrnně za všechny měny, tak i jednotlivě pro každou hlavní měnu, se kterou banka pracuje.
- (4) Při stanovování limitů banka zohlední dopad možných nestandardních podmínek nebo mimořádných krizových okolností. Limity musí zohlednit velikost banky, její finanční situaci, typ a složitost vykonávaných činností banky.

III) Řízení přístupu na trh

Banka dostatečně stabilizuje a diverzifikuje své finanční zdroje. Za tímto účelem zejména:

- a) vytvoří a udržuje pravidelné kontakty s významnými věřiteli, s korespondenčními bankami a dalšími významnými klienty a obchodními partnery,
- b) prověřuje míru spolehlivosti jednotlivých finančních zdrojů,
- c) sleduje různé možnosti financování svých aktiv a vývoj těchto možností,
- d) sleduje a udržuje možnost přístupu na trh za účelem prodeje svých aktiv.

IV) Scénář pro řízení rizika likvidity

- (1) Pro účely řízení rizika likvidity banka sestavuje scénář pro řízení tohoto rizika.
- (2) Banka stanoví předpoklady vývoje objemu a struktury aktiv, pasív, podrozvahových položek a dalších důležitých předpokladů pro scénář řízení rizika likvidity.
- (3) Předpoklady vývoje objemu a struktury aktiv pro scénář řízení rizika likvidity zahrnují především odhad:
 - a) objemu splatných aktiv, které banka hodlá a je schopna obnovit,
 - b) předpokládaného nárůstu objemově nejvýznamnějších aktiv,
 - c) kategorizace jednotlivých aktiv z hlediska jejich likvidnosti.
- (4) Předpoklady vývoje objemu a struktury pasív pro scénář řízení rizika likvidity zahrnují především odhad:
 - a) vývoje objemu pasív včetně vymezení obvyklé úrovně obnovení splatných pasív a obvyklého růstu nových vkladů,
 - b) průměrné splatnosti vkladů a obdobných nástrojů na viděnou založený na historické zkušenosti.
- (5) Předpoklady vývoje objemu a struktury podrozvahových položek pro scénář řízení rizika likvidity zahrnují především prověření odlivu finančních toků prostřednictvím úvěrových příslibů, záruk a akreditivů, pevných termínových kontraktů a opcí.
- (6) Další důležité faktory, které je třeba zohlednit při ověřování scénáře řízení rizika likvidity, zahrnují především likvidní potřeby spojené s některými obchodními aktivitami banky a aktivitami jejích klientů (korespondenční bankovní služby, vypořádání obchodů klientů, apod.).
- (7) Banka zajistí pravidelné prověřování správnosti předpokladů scénáře řízení rizika likvidity s ohledem na měnící se podmínky uvnitř banky nebo mimo banku. Změny předpokladů jsou podnětem pro úpravu scénáře.

V) Pohotovostní plán

- (1) Pro účely řízení rizika likvidity za mimořádných krizových okolností má banka pohotovostní plán.
- (2) Pohotovostní plán obsahuje zejména:
 - a) zajištění přesného a včasného toku informací v rámci banky,
 - b) jasné vymezení pravomocí a zodpovědností v rámci banky,
 - c) možné způsoby ovlivnění vývoje aktiv a pasív,
 - d) způsob komunikace s významnými věřiteli, obchodními partnery, dalšími klienty a veřejností při realizaci této strategie,
 - e) specifikaci záložních finančních zdrojů
- (3) Banka zajistí pravidelnou aktualizaci pohotovostního plánu s ohledem na měnící se podmínky uvnitř banky nebo mimo banku.

VI) Dodržování ukazatelů likvidity

Česká národní banka je v odůvodněných případech oprávněna požadovat po bance dodržování ukazatelů k zabezpečení likvidity (např. poměr rychle likvidních aktiv vůči krátkodobým pasívům) stanovených Českou národní bankou.

Interní audit

I) Základní ustanovení

- (1) Internímu auditu podléhají veškeré činnosti banky.
- (2) Interní audit je v bance zajišťován útvarem interního auditu.
- (3) Některé činnosti související s výkonem interního auditu mohou být zajišťovány též útvary interního auditu společností finanční holdingové společnosti, jejímž členem je banka, nebo externími dodavateli. Banka zajistí, aby tyto činnosti byly prováděny pouze subjekty, jejichž předpoklady k výkonu interního auditu odpovídají požadavkům tohoto opatření.
- (4) Útvar interního auditu banky však musí vykonávat přinejmenším následující činnosti:
 - a) sestavení analýzy rizik,
 - b) sestavení plánů interního auditu,
 - c) zpracování písemného souhrnného vyhodnocení funkčnosti a účinnosti vnitřního řídicího a kontrolního systému,
 - d) zavedení a udržování funkčního a efektivního systému sledování nápravných opatření.
- (5) Interní audit musí být vykonáván nezávisle na veškerých výkonných činnostech banky.
- (6) Vedoucí útvaru interního auditu je podřízen takovému organizačnímu stupni v bance, který útvaru interního auditu umožní plnění všech jeho funkcí.

II) Statut útvaru interního auditu

- (1) Banka vymezí statut útvaru interního auditu, kterým upraví zejména:
 - a) postavení útvaru interního auditu,
 - b) jeho odpovědnosti a pravomoci,
 - c) předmět interního auditu,
 - d) charakter ujišťovacích a konzultačních služeb poskytovaných útvarem interního auditu,
 - e) proces plánování interního auditu,
 - f) způsob sdělování výsledků interního auditu,
 - g) způsob vypořádání připomínek ohledně závěrů interního auditu a řešení případných sporů,
 - h) způsob ukládání opatření k nápravě.
- (2) Banka dále vymezí odpovědnosti a pravomoci útvarů interních auditů společností finanční holdingové společnosti, jejímž členem je banka, při provádění interního auditu v bance a způsob jejich kooperace s útvarem interního auditu banky.
- (3) Při provádění své činnosti musí mít útvar interního auditu zajištěn přístup ke všem dokumentům banky.
- (4) Útvar interního auditu má dále možnost zúčastnit se zasedání všech poradních a rozhodovacích výborů/orgánů banky. V případech hodných zvláštního zřetele může být toto právo útvaru interního auditu jednotlivě omezeno odůvodněným rozhodnutím představenstva banky.

III) Plánování interního auditu

- (1) Plánování interního auditu je založeno na analýze rizik, prováděné útvarem interního auditu alespoň jednou ročně. Při přípravě plánu vedoucí útvaru interního auditu vyžaduje a vyhodnocuje podněty dozorčí rady, představenstva a vrcholového vedení. Zároveň bere v úvahu činnost a požadavky útvarů interního auditu společností finanční holdingové společnosti, jejímž členem je banka, externího auditora a regulatorních orgánů.
- (2) Útvar interního auditu své kapacity rozvrhuje v závislosti na míře rizik spojených s jednotlivými činnostmi banky.
- (3) Analýza rizik musí zohlednit pravděpodobnost selhání vnitřního řídicího a kontrolního systému v činnostech banky a velikost možné ztráty z tohoto selhání vyplývající. Interní audit zpracovává písemný výstup z provedené analýzy rizik. Tento výstup je předkládán představenstvu a dozorčí radě (případně jejímu výboru pro audit, pokud je zřízen) k projednání. Odlišné názory představenstva nebo dozorčí rady (případně jejího výboru pro audit, pokud je zřízen) na výstup z analýzy rizik jsou zdokumentovány.
- (4) Útvar interního auditu sestavuje periodický a strategický plán činnosti. Plány činnosti útvaru interního auditu jsou před schválením představenstvem projednány dozorčí radou (případně výborem pro audit, pokud je zřízen). Důvody případných změn plánů útvaru interního auditu jsou zdokumentovány.
- (5) Strategický plán je sestavován na období 3-5ti let. Strategický plán zajišťuje, aby činnost interního auditu byla efektivně rozvržena na příslušné období (3-5ti let), byla zohledněna strategická rozhodnutí orgánů banky, rizikovitost jednotlivých činností banky a určena předpokládaná perioda jejich prověření. Strategický plán je v návaznosti na provedenou analýzu rizik aktualizován.
- (6) Periodický plán je sestavován na období jednoho roku (případně na kratší časový úsek). Periodický plán určuje cíl, předmět a termín plánovaných auditů. Periodický plán dále rozvrhuje kapacitu útvaru interního auditu na plánované audity, mimořádné audity, vzdělávání a další činnosti interního auditu.

IV) Výkon interního auditu

- (1) Pro výkon činnosti musí útvar interního auditu jako celek mít nebo získat takové znalosti, dovednosti a další schopnosti, které jsou nezbytné pro plnění jeho odpovědností. V případě, že k provedení plánovaného auditu nemá útvar interního auditu dostatečné schopnosti nebo by bylo jeho provedení útvarem interního auditu společnosti finanční holdingové společnosti, jehož členem je banka, nebo externím dodavatelem.
- (2) Vedoucí útvaru interního auditu banky zajistí, aby výkon interního auditu byl efektivně koordinován a prováděn ve spolupráci s útvary interních auditů společností finanční holdingové společnosti a interním auditem prováděným externími dodavateli. Zároveň vedoucí útvaru interního auditu při koordinaci činnosti zohlední ověřování zadaná představenstvem nebo dozorčí radou a/nebo ověření dle požadavku regulátora.
- (3) Prověření interním auditem podléhají zejména:
 - a) účinnost vnitřního řídicího a kontrolního systému, včetně systému řízení rizik,
 - b) dodržování zásad obezřetného podnikání bank,
 - c) úplnost, průkaznost a správnost vedení účetnictví,

- d) spolehlivost účetních, statistických a provozních informací,
 - e) spolehlivost informací předávaných představenstvu a dozorčí radě,
 - f) dodržování záměrů, plánů a strategie stanovených vedením banky,
 - g) funkčnost a bezpečnost informačních systémů,
 - h) finanční řízení.
- (4) Při výkonu konzultační činnosti musí být zajištěno, aby nebyla omezena schopnost útvaru interního auditu podávat nezávislé a objektivní ujištění o účinnosti a efektivnosti vnitřního řídicího a kontrolního systému.
- (5) Pokud se ve výjimečných případech podílí na poskytování ujištění o činnosti interní auditor, který tuto činnost vykonával nebo na jejímž zavádění se podílel před méně než 12 měsíci, musí být tato skutečnost uvedena ve zprávě o provedeném auditu a zároveň musí být zajištěna maximální objektivita této zprávy.
- (6) Útvar interního auditu vypracovává písemné postupy pro provádění auditů a pravidelně je aktualizuje.
- (7) Auditorický spis je veden pro každou jednotlivou auditní akci. Auditorický spis musí být veden takovým způsobem, aby byl kompletně rekonstruovatelný postup při provedeném auditu a obsahoval takové informace, aby na jejich základě přiměřeně uvážlivá a kompetentní osoba došla ke stejným závěrům jako interní auditor¹⁾. Auditorické spisy jsou prověřovány vedoucím útvaru interního auditu, případně jím zmocněným interním auditorem.
- (8) O provedeném interním auditu je vypracovávána zpráva. Zpráva obsahuje zejména cíl, předmět, rozsah interního auditu a zjištění spolu s návrhem nápravných opatření. Zpráva dále obsahuje názor interního auditora na míru rizik obsažené v auditované činnosti včetně zbytkového rizika (tj. rizika spojeného s určitou činností banky s ohledem na zavedené kontrolní mechanismy) a jeho přijatelnost. Zpráva je přístupna představenstvu, dozorčí radě, případně jejímu výboru pro audit, pokud je zřízen, a vedoucím věcně příslušných útvarů banky.
- (9) Nedílnou součástí činnosti útvaru interního auditu je funkční a efektivní systém sledování nápravných opatření. Tento systém sleduje, zda jsou nápravná opatření efektivně zavedena. V případě, že vedoucí útvaru interního auditu dojde k závěru, že je stupeň zbytkového rizika v důsledku nezavedení efektivních nápravných opatření pro banku nepřijatelný, projedná tuto skutečnost s představenstvem banky. Jestliže není otázka zbytkového rizika vyřešena, předá tuto informaci dozorčí radě banky.

V) Informace útvaru interního auditu

- (1) Útvar interního auditu pravidelně informuje o svých zjištěních, návrzích k jejich odstranění a jejich plnění představenstvo a dozorčí radu, příp. její výbor pro audit, pokud je zřízen.
- (2) Útvar interního auditu zpracovává pravidelně (nejméně však jednou ročně) zprávu o své činnosti a předkládá ji představenstvu a dozorčí radě, příp. jejímu výboru pro audit (pokud je zřízen) k projednání.
- (3) Vedoucí útvaru interního auditu informuje představenstvo a dozorčí radu (případně výbor pro audit, pokud je zřízen) o možných dopadech zapříčiněných omezenými zdroji útvaru interního auditu.

¹⁾ Ve smyslu „dostatečné informace“ dle standardu pro výkon činnosti interního auditu č. 2310 Identifikace informací ze Standardů pro profesionální praxi interního auditu Institutu interních auditorů.

- (4) Útvar interního auditu minimálně jednou ročně zpracovává písemné souhrnné vyhodnocení funkčnosti a účinnosti vnitřního řídicího a kontrolního systému banky. Toto hodnocení se týká zejména spolehlivosti a integrity finančních a provozních informací, funkčnosti a účinnosti procesů, ochrany aktiv a dodržování zákonů, předpisů a smluv. Interní audit dále ověřuje do jaké míry vedení banky zavedlo adekvátní kritéria, prostřednictvím kterých lze určit, zda byly stanovené úkoly a cíle splněny. Toto vyhodnocení předkládá představenstvu a dozorčí radě, příp. jejímu výboru pro audit (pokud je zřízen) k projednání.
- (5) Útvar interního auditu poskytuje své výstupy orgánům banky včas a tyto výstupy musí být aktuální, spolehlivé a ucelené.

VI) Zabezpečení a zvyšování kvality interního auditu

Vedoucí útvaru interního auditu vypracuje a pravidelně aktualizuje program pro zabezpečení a zvyšování kvality interního auditu, který zahrne všechny aspekty interního auditu a průběžně monitoruje jeho efektivnost. Činnost útvaru interního auditu je prověřena nejméně jednou za pět let na bance nezávislým externím hodnotitelem²⁾.

VII) Spolupráce interního auditu s externím auditorem

- (1) Vedoucí útvaru interního auditu konzultuje s externím auditorem otázky vnitřního řídicího a kontrolního systému banky.
- (2) Útvar interního auditu se pravidelně hodnotí kvalitu činnosti externího auditora, zejména pak:
- a) zda rozsah prací externího auditora odpovídá uzavřené smlouvě,
 - b) zda provedená práce externího auditora je adekvátní ve vztahu k závěrům přijatým externím auditorem,
 - c) zda není narušena nezávislost externího auditora,
 - d) zda činnost externího auditora přinesla bance přidanou hodnotu.

²⁾ V souladu se základním standardem č. 1312 Externí hodnocení ze Standardů pro profesionální praxi interního auditu Institutu interních auditorů.