

Třídící znak							
2	2	1	1	0	5	6	0

ÚŘEDNÍ SDĚLENÍ
ČESKÉ NÁRODNÍ BANKY
ze dne 10. prosince 2010

**k výkonu činnosti organizátora regulovaného trhu, provozovatele vypořádacího systému
a centrálního depozitáře cenných papírů na finančním trhu – operační riziko v oblasti
informačního systému**

1. Toto úřední sdělení navazuje na úřední sdělení České národní banky ze dne 10. prosince 2010 k výkonu činnosti na finančním trhu: Kvalitativní požadavky související s výkonem činnosti – základní informace.
2. Záměrem České národní banky je poskytnout věcný výklad a další informace k výkonu činnosti organizátora regulovaného trhu, provozovatele vypořádacího systému a centrálního depozitáře cenných papírů (dále také jen „poskytovatel finančních služeb“) na finančním trhu, pokud jde o kvalitativní požadavky¹ související s operačním rizikem v oblasti informačního systému, kterému je nebo by mohl být poskytovatel finančních služeb vystaven. Podrobnější informace České národní banky jsou obsaženy v příloze tohoto úředního sdělení.
3. Česká národní banka při výkonu dohledu kontroluje dodržování příslušných požadavků právních předpisů poskytovatelem finančních služeb. Česká národní banka při výkonu dohledu postupuje individuálně, s přihlédnutím ke konkrétním podmínkám zaměření a uspořádání výkonu činnosti daného poskytovatele finančních služeb. Česká národní banka vychází také z uveřejněných úředních sdělení ke kvalitativním požadavkům souvisejícím s výkonem činnosti na finančním trhu; tím není dotčeno právo poskytovatele

¹ Např. organizátor regulovaného trhu je podle § 48 písm. b) a c) zákona č. 256/2004 Sb. o podnikání na kapitálovém trhu, ve znění pozdějších předpisů (dále jen „zákon o podnikání na kapitálovém trhu“) povinen zavést postupy pro řízení rizik a pro zajištění řádného provozu jeho obchodních a jiných systémů; některé kvalitativní předpoklady pro výkon činnosti jsou dále konkretizovány ve vyhlášce č. 233/2009 Sb., o žádostech, schvalování osob a způsobu prokazování odborné způsobilosti, důvěryhodnosti a zkušenosti osob a o minimální výši finančních zdrojů poskytovaných pobočce zahraniční banky (dále jen „vyhláška č. 233/2009 Sb.“), např. v § 9 písm. l).

Provozovatel vypořádacího systému je mj. podle § 83 odst. 9 písm. k) zákona o podnikání na kapitálovém trhu povinen mít pravidla vypořádacího systému, která stanoví systém řízení rizik; některé kvalitativní předpoklady pro výkon činnosti jsou dále konkretizovány ve vyhlášce č. 233/2009 Sb., např. v § 11 písm. d).

Některé kvalitativní předpoklady pro výkon činnosti centrálního depozitáře cenných papírů jsou konkretizovány ve vyhlášce č. 233/2009 Sb., např. v § 12 písm. a) bod 5; pokud centrální depozitář cenných papírů provozuje vypořádací systém, vztahuje se na něj mj. § 83 odst. 9 písm. k) zákona o podnikání na kapitálovém trhu.

finančních služeb individuálně stanovit a uplatňovat jiné interní postupy (zásada „*comply or explain*“).

Viceguvernér
prof. PhDr. Ing. Vladimír Tomšík, Ph.D. v. r.

Příloha: Podrobnější informace České národní banky k výkonu činnosti organizátora regulovaného trhu, provozovatele vypořádacího systému a centrálního depozitáře cenných papírů, pokud jde o kvalitativní požadavky související s operačním rizikem v oblasti informačního systému

Sekce regulace a analýz finančního trhu
Sekce dohledu nad finančním trhem
Odpovědný zaměstnanec:
Mgr. Gavlas, tel. 224 412 098
Ing. Rott, tel. 224 412 659

Podrobnější informace České národní banky k výkonu činnosti organizátora regulovaného trhu, provozovatele vypořádacího systému a centrálního depozitáře cenných papírů, pokud jde o kvalitativní požadavky související s operačním rizikem v oblasti informačního systému

1. Řídící orgán poskytovatele finančních služeb schvaluje a pravidelně vyhodnocuje cíle a hlavní zásady řízení operačního rizika² v oblasti informačního systému (dále jen „operační riziko“), a to v rámci strategie řízení rizik, strategie rozvoje informačního systému a v rámci bezpečnostních zásad poskytovatele finančních služeb.
2. V souladu s cíli a zásadami dle bodu 1 poskytovatel finančních služeb vytvoří, udržuje a uplatňuje systém řízení operačního rizika. Tento systém zahrnuje vždy zejména tyto prvky a jejich vzájemné vazby:
 - a) organizační předpoklady (uspořádání) řízení operačního rizika,
 - b) zásady a postupy řízení operačního rizika, která jsou v souladu s právními předpisy a jsou promítnuta do interních předpisů, a
 - c) kontrolní mechanismy řízení operačního rizika a výkonu souvisejících činností.
3. Organizační předpoklady (uspořádání) řízení operačního rizika zahrnují zejména:
 - a) přidělení odpovědností útvarům a pracovníkům za řízení tohoto rizika,
 - b) seznámení všech příslušných pracovníků v potřebném rozsahu s cíli, hlavními zásadami a pravidly řízení operačního rizika,
 - c) přidělení odpovědností za ochranu aktiv a plnění bezpečnostních zásad,
 - d) oddělené zajišťování vývoje informačního systému od jeho provozu,
 - e) oddělené provádění správy informačního systému od vyhodnocování bezpečnostních auditních záznamů, kontroly přidělování přístupových práv a vypracování a aktualizace bezpečnostních předpisů pro informační systém, a
 - f) vyhodnocování bezpečnostních auditních záznamů pracovníkem, který nemá možnost upravovat (modifikovat) v informačním systému informace související s činností, o které je bezpečnostní auditní záznam pořízen.
4. Zásady a postupy řízení operačního rizika zahrnují zejména:
 - a) postupy pro rozpoznávání, vyhodnocování či měření, sledování, ohlašování a omezování operačního rizika, kterému je nebo by mohl být poskytovatel finančních služeb vystaven, včetně zohlednění málo častých významných událostí,
 - b) soustavu limitů používanou při řízení operačního rizika, včetně postupů, způsobu evidence a informačních toků při překročení limitů,
 - c) postupy pro stanovení míry akceptovaného rizika,
 - d) postupy pro omezování výskytu či nepříznivých dopadů výskytu událostí operačního rizika,

² Operačním rizikem se rozumí riziko ztráty vlivem nedostatků či selhání interních procesů, lidského faktoru nebo systémů či riziko ztráty vlivem vnějších skutečností, včetně rizika právního; významnou součástí jsou rizika v oblasti informačního systému, včetně rizik outsourcingu a compliance;

- e) postupy pro případné vyvedení operačního rizika mimo poskytovatele finančních služeb,
- f) hlavní zásady a postupy pro zajištění důvěrnosti, integrity a dostupnosti informací,
- g) zásady kontrolních mechanismů a činností při řízení tohoto rizika na všech příslušných řídicích a organizačních úrovních, včetně kontroly dodržování stanovených postupů a limitů pro jeho řízení a ověřování výstupů hodnocení či měření tohoto rizika,
- h) zásady a opatření pro fyzickou ochranu aktiv poskytovatele finančních služeb,
- i) postupy pro řešení bezpečnostních incidentů, a
- j) postupy pro řešení operačního rizika při zajišťování dodávek zboží a služeb a při vykonávání některých významných činností prostřednictvím jiných osob (outsourcing)³, pokud je uplatňován či zvažován.

Příklad 1:

Poskytovatel finančních služeb např. promítne [písm. a)] zásady a postupy pro řízení operačního rizika do interních předpisů a zajistí, aby všichni pracovníci, jejichž činnost má vliv na řízení operačního rizika, byli seznámeni v potřebném rozsahu se schválenou strategií, zásadami a pravidly řízení operačního rizika a postupovali v souladu s nimi.

Příklad 2:

Poskytovatel finančních služeb např. stanoví [písm. b)] limity v hodnotovém vyjádření pro zahrnování jednotlivých anebo opakujících se událostí operačního rizika do evidence operačních rizik.

Příklad 3:

Poskytovatel finančních služeb např. stanoví [písm. h)] postupy pro řízení přístupů pracovníků, klientů a dalších oprávněných osob k jeho hmotnému a nehmotnému majetku v rámci svého informačního systému.

5. Kontrolní mechanismy řízení operačního rizika zahrnují zejména:

- a) kontrolu dodržování pravidel pro řízení tohoto rizika na všech řídicích a organizačních úrovních,
- b) přiměřené kontrolní mechanismy pro jednotlivé procesy,
- c) fyzickou kontrolu,
- d) nezávislé prověření systému řízení tohoto rizika a funkčnosti a bezpečnosti informačního systému interním auditem, a
- e) vytvoření a udržování systému sledování opatření k nápravě.

Příklad 4:

Poskytovatel finančních služeb např. kontroluje [písm. a)] dodržování předpisů pro schvalování přístupových práv do informačního systému, monitorování přístupu do informačního systému, zaznamenávání a vyhodnocování událostí operačního rizika.

Příklad 5:

Poskytovatel finančních služeb např. kontroluje [písm. c)] omezení přístupu k hmotnému majetku, cenným papírům a jiným finančním aktivům.

6. Poskytovatel finančních služeb definuje aktiva informačního systému⁴, hrozby, které na ně působí, zranitelná místa informačního systému, pravděpodobnost realizace hrozeb a odhad jejich následků a protiopatření. Poskytovatel finančních služeb pravidelně provádí aktualizaci analýzy rizik spjatých s informačním systémem.

7. Poskytovatel finančních služeb

³ § 12d zákona o podnikání na kapitálovém trhu

⁴ Aktivem informačního systému se rozumí informační technologie, informace uložené v informačním systému a dokumentace informačního systému,

- a) vytvoří a udržuje plány pro obnovení své činnosti pro případy neplánovaného přerušení nebo omezení svých činností, zejména pokud jde o případné havárie informačního systému, selhání osoby, prostřednictvím které jsou vykonávány významné činnosti (outsourcing) nebo selhání externí infrastruktury, například dodávky energií (dále jen „pohotovostní plány“),
- b) zabezpečí, aby pohotovostní plány byly pravidelně testovány, vyhodnocovány a případně aktualizovány, a
- c) zabezpečí, aby příslušní pracovníci byli s pohotovostními plány seznámeni a postupovali podle nich.

Příklad 6:

Pro řešení obnovy činností jsou v pohotovostních plánech stanovena např. tato opatření:

- (i) činnost následující bezprostředně po vzniku krizové situace zaměřená na minimalizaci škod,
- (ii) činnost následující po vzniku krizové situace zaměřená na likvidaci následků krizové situace,
- (iii) způsob zálohování,
- (iv) způsob zajištění nouzového provozu s uvedením minimálních funkcí, které musí být zachovány,
- (v) způsob obnovy činností včetně činností vykonávaných jinými osobami (outsourcing).

8. Při výkonu své činnosti poskytovatel finančních služeb zabezpečí v oblasti informačního systému zejména:

- a) soulad vykonávaných činností při řízení operačního rizika s právními a interními předpisy,
- b) zpětnou výsledovatelnost (rekonstruovatelnost) veškerých schvalovacích a rozhodovacích procesů a kontrolních činností při řízení operačního rizika, včetně souvisejících odpovědností, pravomocí a interních předpisů,
- c) rozpoznávání zdrojů operačního rizika a začlenění vyhodnocování a sledování tohoto rizika do běžných procesů,
- d) informační toky při řízení operačního rizika na všech příslušných řídicích a organizačních úrovních,
- e) vyhodnocování a sledování informací o významných a opakovaných událostech operačního rizika a dopadech a ztrátách, včetně potenciálních, vyplývajících z těchto událostí,
- f) informování příslušných pracovníků o podstupovaném operačním riziku souvisejícím s jejich činností (ohlašování operačního rizika),
- g) dodržování bezpečnostních zásad,
- h) přidělení přístupových práv uživatelům v informačním systému a jednoznačnou autentizaci (ověření totožnosti) uživatele, která musí předcházet jeho činnostem v informačním systému,
- i) přístup k informacím v informačním systému pouze uživateli, který byl pro tento přístup autorizován,
- j) ochranu důvěrnosti a integrity autentizační informace,
- k) zaznamenávání událostí, které ohrozily nebo narušily bezpečnost informačního systému, do bezpečnostních auditních záznamů, ochranu těchto záznamů před neautorizovaným přístupem, zejména úpravou (modifikací) nebo zničením, a jejich archivaci, a
- l) pravidelné vyhodnocování a případné upravování pravidel řízení operačního rizika.

9. Při provozování informačního systému poskytovatel finančních služeb zabezpečí zejména:

- a) aby jeho změnu bylo možno provést až po vyhodnocení vlivu této změny na bezpečnost informačního systému,

- b) aby bylo používáno pouze otestované programové vybavení⁵, u kterého výsledky testů prokázaly, že bezpečnostní funkce jsou v souladu se schválenými bezpečnostními zásadami informačního systému; výsledky testů musí být zdokumentovány,
- c) aby servisní činnost byla organizována tak, aby bylo minimalizováno ohrožení bezpečnosti informačního systému,
- d) zálohování informací a programového vybavení, významných pro jeho fungování; zálohované informace a programové vybavení jsou uloženy tak, aby byly zabezpečeny proti poškození, zničení a krádeži,
- e) připojení své interní sítě k externí komunikační síti, která není pod jeho kontrolou tak, aby byla minimalizována možnost průniku do jeho informačního systému,
- f) aby při přenosu důvěrných informací externí komunikační sítí byla zajištěna přiměřená důvěrnost a integrita informací a dále spolehlivá autentizace komunikujících stran, včetně ochrany autentizačních informací, a
- g) pravidelné prověřování a vyhodnocování bezpečnosti informačního systému.

Příklad 7:

Návrh na změnu informačního systému obsahuje např.:

- (i) analýzu očekávaných dopadů,
- (ii) návrh postupu zavedení,
- (iii) analýzu rizik včetně návrhů na jejich řízení,
- (iv) identifikaci zdrojů, které je nutno vyčlenit na řádné řízení souvisejícího operačního rizika.

10. V případě, že poskytovatel finančních služeb vykonává významnou činnost v oblasti informačního systému prostřednictvím jiné osoby (outsourcing), uzavře smlouvu upravující outsourcing způsobem, který umožňuje zachycení jejího obsahu, kontrolovatelnost a případnou vymahatelnost, jakož i uchovatelnost (zpravidla v listinné podobě) a nezbavuje se tím žádné ze svých povinností a odpovědností; současně zajistí, aby sjednání outsourcingu neomezilo soulad činností, které jsou předmětem outsourcingu, s příslušnými právními předpisy, možnost jejich kontroly poskytovatelem finančních služeb a výkon dohledu České národní banky včetně případné kontroly skutečností týkajících se outsourcingu u jeho poskytovatele.

⁵ Programovým vybavením se rozumí programy, procedury a pravidla nutné k tomu, aby příslušné technické vybavení plnilo požadovanou funkci;