Třídící znak							
1	0	4	0	6	5	3	0

OPATŘENÍ
ČESKÉ NÁRODNÍ BANKY
Č. 3 ZE DNE 25. KVĚTNA 2006,

K VNITŘNÍMU ŘÍDICÍMU A KONTROLNÍMU SYSTÉMU INSTITUCE ELEKTRONICKÝCH PENĚZ

Česká národní banka podle § 18d odst. 4 zákona č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku), ve znění zákona č. 257/2004 Sb. a zákona č.62/2006 Sb. a § 24 písm. a) zákona č. 6/1993 Sb., o České národní bance, ve znění zákona č. 127/2002 Sb. a 62/2006 Sb. stanoví:

§ 1

Účel opatření

(1) Toto opatření zapracovává příslušné předpisy Evropských společenství[1)] a stanoví požadavky na vnitřní řídicí a kontrolní systém instituce elektronických peněz včetně požadavků na vnitřní audit a řízení rizik.

(2) Požadavky stanovené tímto opatřením naplňuje instituce elektronických peněz s ohledem na svou velikost a způsob řízení, typ, povahu a složitost činností, které vykonává.

(3) Požadavky stanovené tímto opatřením instituce elektronických peněz upraví ve svých vnitřních předpisech.

§ 2

Definice pojmů

Pro účely tohoto opatření se rozumí

a) tržními riziky rizika ztráty instituce elektronických peněz vyplývající ze změn cen, kurzů nebo 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 instituce elektronických peněz vyplývající ze selhání smluvní strany tím, že nedostojí svým závazkům podle podmínek smlouvy, na základě které se instituce elektronických peněz stala věřitelem smluvní strany,

c) operačním rizikem riziko ztráty instituce elektronických peněz vlivem nedostatků nebo selhání vnitřních procesů, lidského faktoru nebo systémů anebo riziko ztráty instituce elektronických peněz vlivem vnějších událostí, včetně rizika ztráty instituce elektronických peněz v důsledku porušení či nenaplnění právní normy,

d) rizikem likvidity se rozumí riziko, že instituce elektronických peněz ztratí schopnost dostát svým finančním závazkům v době, kdy se stanou splatnými nebo nebude schopna financovat svá aktiva,

e) řízením rizik jejich identifikace, měření nebo vyhodnocování, sledování a případné přijímání opatření vedoucích k omezení podstupovaných rizik,

f) vnitřním auditem nezávislá, objektivní, ujišťovací a konzultační činnost zaměřená na přidávání hodnoty a zdokonalování procesů v instituci elektronických peněz,

g) pracovníkem osoba, která se podílí na činnosti instituce elektronických peněz na základě pracovní nebo jiné smlouvy,

h) celkovou strategií soubor dokumentů, který obsahuje hlavní cíle a strategická rozhodnutí v jednotlivých oblastech činnosti instituce elektronických peněz,

[1)] Směrnice Evropského parlamentu a Rady 2000/46/ES ze dne 18. září 2000 o přístupu k činnosti institucí elektronických peněz, o jejím výkonu a o obezřetnostním dohledu nad touto činností.

i) strategií řízení rizik soubor dokumentů, které obsahují strategická rozhodnutí ohledně řízení rizik,

j) informačním systémem funkční celek, který slouží instituci elektronických peněz k získávání, uchování, přenášení, zpracování a poskytování informací pomocí informačních technologií,

k) 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,

l) aktivem informačního systému informační technologie, informace uložené v informačním systému instituce elektronických peněz a dokumentace informačního systému,

m) autentizací uživatele proces ověření jeho totožnosti,

n) důvěrností informace zajištění, že informace je přístupná pouze uživateli, který je k přístupu oprávněn,

o) dostupností informace zajištění, že informace je pro oprávněného uživatele přístupná ve stanovené době,

p) integritou informace zajištění správnosti a úplnosti informace a metody jejího zpracování,

q) likvidní pozicí instituce elektronických peněz stav (přebytek nebo nedostatek) zdrojů v rámci stanovených časových pásem,

r) čistým peněžním tokem rozdíl mezi přílivem a odlivem peněžních prostředků.

§ 3

Základní požadavky na vnitřní řídicí a kontrolní systém

(1) Instituce elektronických peněz vytvoří a udržuje účinný a efektivní vnitřní řídicí a kontrolní systém, který je tvořen zejména těmito prvky a vazbami mezi nimi:
   a) kontrolní prostředí,
   b) kontrolní činnosti,
   c) informace,
   d) řízení rizik,
   e) sledování a vyhodnocování účinnosti a efektivnosti vnitřního řídicího a kontrolního systému a náprava nedostatků včetně vnitřního auditu.

(2) Vnitřní řídicí a kontrolní systém zajistí tyto cíle:
   a) provádění činnosti instituce elektronických peněz v souladu s celkovou strategií instituce elektronických peněz a vnitřní předpisovou základnou,
   b) aktuálnost, spolehlivost a ucelenost informací používaných institucí elektronických peněz pro rozhodovací procesy a poskytovaných institucí elektronických peněz třetím stranám,
   c) soulad činností instituce elektronických peněz s příslušnými zákony a předpisy.

(3) Vnitřní řídicí a kontrolní systém zahrnuje všechny činnosti a organizační složky instituce elektronických peněz.

(4) Veškeré rozhodovací procesy a kontrolní činnosti musí být zpětně rekonstruovatelné (vysledovatelné). K naplnění tohoto požadavku instituce elektronických peněz vytvoří odpovídající systém archivace dokumentů a dat.

Kontrolní prostředí

§ 4

Kontrolní a řídící orgány

Instituce elektronických peněz zajistí, že jsou pro účely udržování účinného a efektivního vnitřního řídicího a kontrolního systému jasně stanovené pravomoci a působnost jejích řídících a kontrolních orgánů .

§ 5

Instituce elektronických peněz zajistí, že dozorčí rada nejméně jednou ročně vyhodnocuje účinnost a efektivnost vnitřního řídicího a kontrolního systému.

§ 6

(1) Instituce elektronických peněz musí mít funkční organizační strukturu, která mimo jiné jasně vymezuje odpovědnosti a pravomoci útvarů a pracovníků a umožňuje efektivní komunikaci a spolupráci na všech úrovních instituce elektronických peněz. Organizační struktura musí zohledňovat požadavky na oddělení neslučitelných funkcí. Funkčnost organizační struktury je pravidelně, alespoň jednou ročně, vyhodnocována představenstvem.

(2) Instituce elektronických peněz zajistí pravidelné informování představenstva o její expozici vůči tržnímu riziku a o likvidní situaci instituce elektronických peněz. Představenstvo musí být informováno o tom, zda jsou řádně kryty závazky z vydaných elektronických peněz a o všech překročeních limitů stanovených právními předpisy a opatřeními České národní banky. V případech, kdy se likvidní situace instituce elektronických peněz výrazně nepříznivě mění, musí být představenstvo informováno bez zbytečného odkladu.

§ 7

Oddělení neslučitelných funkcí

(1) Instituce elektronických peněz zajistí, aby útvarům a pracovníkům instituce elektronických peněz 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 instituce elektronických peněz jsou stanoveny tak, aby omezily možnosti konfliktu zájmů. Oblasti konfliktu zájmů jsou předmětem průběžného nezávislého sledování.

(2) V instituci elektronických peněz 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) Instituce elektronických peněz zajistí oddělené zajišťování vývoje a provozu informačních systémů.

(4) Vnitřní audit musí být vykonáván nezávisle na veškerých výkonných činnostech instituce elektronických peněz.

Kontrolní činnosti

§ 8

(1) Kontrolní činnosti jsou součástí každodenní činnosti instituce elektronických peněz. Kontrolní činnosti zahrnují zejména:
   a) kontrolu po linii řízení,
   b) přiměřené kontrolní mechanismy pro jednotlivé procesy v instituci elektronických peněz,
   c) fyzickou kontrolu.

(2) Instituce elektronických peněz vytvoří postupy pro kontrolní činnost na všech organizačních a řídicích úrovních. Prověřování dodržování stanovených postupů a jejich dostatečnosti je prováděno pravidelně.

Informace

§ 9

Instituce elektronických peněz zajistí, aby dozorčí rada, představenstvo, příslušní pracovníci a útvary měli pro své rozhodování k dispozici informace, které jsou aktuální, spolehlivé a ucelené. Jedná se zejména o informace týkající se dodržování limitů a omezení stanovených právními předpisy a opatřeními České národní banky, míry podstupovaného tržního rizika a reálného vývoje likvidity.

Řízení rizik

§ 10

Obecné požadavky

Vnitřní řídicí a kontrolní systém instituce elektronických peněz je nastaven tak, aby umožňoval soustavné řízení rizik podstupovaných institucí elektronických peněz.

§ 11

Strategie řízení rizik

(1) Instituce elektronických peněz má rozsahu své činnosti odpovídající strategii řízení rizik včetně řízení rizika likvidity, která obsahuje hlavní zásady, jež instituce elektronických peněz uplatňuje při jejich řízení. Instituce elektronických peněz vypracuje konkrétní postupy pro naplňování této strategie. Strategie řízení rizik stanoví zejména:
   a) přijatelnou míru tržního rizika,
   b) metody pro řízení tržních rizik,
   c) metody pro řízení úvěrových rizik,
   d) metody pro měření a sledování rizika likvidity a metody a postupy pro omezení tohoto rizika.

(2) Instituce elektronických peněz 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 instituce elektronických peněz, 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.

§ 12

Řízení tržních rizik

(1) Instituce elektronických peněz má odpovídající systém měření a sledování tržních rizik.

(2) Systém měření a sledování tržních rizik musí zejména:
   a) včasně, přesně a kompletně zaznamenat všechny transakce tak, aby byly podchyceny veškeré expozice vůči tržním rizikům,
   b) správně tyto transakce ocenit,
   c) podchytit všechny významné zdroje tržních rizik,
   d) měřit tržní rizika souhrnně za všechny obchodní jednotky instituce elektronických peněz.

(3) Instituce elektronických peněz dále zabezpečí, že:
   a) pracovníci útvarů odpovědných za řízení tržních rizik a příslušní členové vedení instituce elektronických peněz rozumějí předpokladům, ze kterých systém měření a sledování tržních rizik vychází,
   b) předpoklady, ze kterých systém vychází, jsou dostatečně zdokumentovány.

§ 13

Řízení úvěrového rizika

Instituce elektronických peněz má takový systém měření a sledování úvěrového rizika, který podchytí všechny významné zdroje úvěrového rizika a vyhodnotí jejich dopad na hodnotu jejích aktiv a pasív tak, aby poskytl nezkreslený obraz o míře podstupovaného úvěrového rizika.

§14

Operační riziko

Pro případy neplánovaného přerušení nebo omezení svých činností, havárie informačních systémů, selhání pro instituci elektronických peněz významných třetích stran a selhání vnější infrastruktury zabezpečí instituce elektronických peněz postupy, které vedou k obnovitelnosti činností a informačních systémů významných z hlediska fungování instituce elektronických peněz.

§ 15

Požadavky na řízení rizika likvidity

Pro účely řízení rizika likvidity musí mít instituce elektronických peněz odpovídající postupy měření a sledování čistých peněžních toků a likvidní pozice tak, aby bylo možné určit kroky instituce elektronických peněz potřebné k řízení rizika likvidity.

Požadavky na informační systémy

§ 16

Řízení informačních systémů

(1) Instituce elektronických peněz přijme strategii rozvoje informačních systémů a postupy pro naplňování této strategie.

(2) Instituce elektronických peněz 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) Instituce elektronických peněz zabezpečí, aby strategie rozvoje a bezpečnostní politika informačních systémů byly pravidelně vyhodnocovány a případně upravovány.

(5) Instituce elektronických peněz zabezpečí dodržování bezpečnostní politiky v jednotlivých informačních systémech.

(6) Instituce elektronických peněz uzavře písemné smlouvy s poskytovateli služeb a produktů pro informační systémy.

§ 17

Analýza rizik

(1) Instituce elektronických peněz 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) Instituce elektronických peněz pravidelně provádí aktualizaci analýzy rizik.

§ 18

Bezpečnost přístupu k informacím

Instituce elektronických peněz zabezpečí:
a) přidělení přístupových práv uživatelům v informačních systémech,
b) jednoznačnou autentizaci uživatele, která musí předcházet aktivitám uživatelů v informačních systémech,
c) přístup k informacím v informačních systémech pouze uživateli, který k němu je oprávněn,
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.

§ 19

Bezpečnost komunikačních sítí

(1) Připojení sítě, která je pod kontrolou instituce elektronických peněz, k vnější komunikační síti, která není pod kontrolou instituce elektronických peněz, musí být zabezpečeno tak, aby byla minimalizována možnost průniku do informačních systémů.

(2) Instituce elektronických peněz zabezpečí, aby při přenosu důvěrných informací vnější komunikační sítí byla zajištěna:
a) adekvátní důvěrnost a integrita informací,
b) spolehlivá autentizace komunikujících stran, včetně ochrany autentizačních informací.

§ 20

Fyzická bezpečnost informačních systémů

Na základě analýzy rizik zavede instituce elektronických peněz opatření pro fyzickou ochranu aktiv informačních systémů.

§ 21

Provozovaní 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) Instituce elektronických peněz 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.

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

§ 22

(1) Sledování a vyhodnocování účinnosti a efektivnosti vnitřního řídicího a kontrolního systému je v instituci elektronických peněz prováděno průběžně na všech řídicích úrovních a je předmětem vnitřního auditu.

(2) Nedostatky vnitřního řídicího a kontrolního systému odhalené po řídicí linii, vnitřním auditem, na základě jiné kontroly či jiným způsobem, musí být včas oznámeny příslušné úrovni vedení instituce elektronických peněz a urychleně řešeny. Závažné nedostatky vnitřního řídicího a kontrolního systému musí být oznámeny představenstvu a dozorčí radě, a dále 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.

§ 23

Vnitřní audit

(1) Vnitřnímu auditu podléhají veškeré činnosti instituce elektronických peněz.

(2) Vnitřní audit může být v instituci elektronických peněz zajišťován i externími dodavateli. Instituce elektronických peněz zajistí, aby tato činnost byla prováděna v souladu se standardy platnými pro výkon činnosti vnitřního auditu[2)].

(3) Vnitřní audit musí být vykonáván nezávisle na veškerých výkonných činnostech instituce elektronických peněz.

(4) Prověření vnitřním auditem podléhají zejména:
a) účinnost vnitřního řídicího a kontrolního systému, včetně systému řízení rizik,
b) dodržování zásad obezřetného podnikání,
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 instituce elektronických peněz,
g) funkčnost a bezpečnost informačních systémů,
h) finanční řízení.

(5) Na směrování, plánování a vyhodnocování činnosti vnitřního auditu se podílí dozorčí rada.

§ 24
Účinnost

Toto opatření nabývá účinnosti dnem vyhlášení.

Guvernér

doc. Ing. Zdeněk Tůma, CSc. v. r.

[2)] Standardy pro profesionální praxi interního auditu Českého institutu interních auditorů.