Třídící znak							
2	0	8	1	1	5	6	0

ÚŘEDNÍ SDĚLENÍ ČESKÉ NÁRODNÍ BANKY

ze dne 27. května 2011

k výkonu činnosti 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 na finančním trhu, pokud jde o kvalitativní požadavky[1] související s operačním rizikem v oblasti informačního systému, kterému je nebo by mohl být poskytovatel finančních služeb[2] 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

[1] Např.:
- banka a spořitelní a úvěrní družstvo jsou ze zákona povinny vytvořit, udržovat a uplatňovat funkční a efektivní řídicí a kontrolní systém včetně systému řízení rizik a informačního systému, přičemž podrobnější kvalitativní požadavky pro dané oblasti jsou stanoveny v části třetí a příloze č. 1 část 3 vyhlášky č. 123/2007 Sb., ve znění pozdějších předpisů (dále jen „vyhláška č. 123/2007 Sb.“);
- pro výkon činnosti centrálního depozitáře cenných papírů jsou některé kvalitativní předpoklady 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 § 12 písm. a) bod 5; pokud centrální depozitář cenných papírů provozuje vypořádací systém, vztahuje se na něj mj. § 83 odst. 9 písm. k) zákona č. 256/2004 Sb. o podnikání na kapitálovém trhu, ve znění pozdějších předpisů (dále jen „zákon o podnikání na kapitálovém trhu“);
- obchodník s cennými papíry je podle zákona o podnikání na kapitálovém trhu povinen uplatňovat řídicí a kontrolní systém, jehož součástí je také řízení rizik; podrobnější požadavky stanoví část třetí vyhlášky č. 123/2007 Sb., kterou se provádějí příslušná ustanovení zákona o podnikání na kapitálového trhu;
- organizátor regulovaného trhu je podle § 48 písm. b) a c) zákona 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., např. v § 9 písm. l);
- pojišťovna a zajišťovna jsou podle § 6 odst. 1 zákona č. 277/2009 Sb., o pojišťovnictví povinny vytvořit a po celou dobu své činnosti udržovat funkční a efektivní řídicí a kontrolní systém, pravidelně z něj vyhodnocovat informace a včas přijímat odpovídající opatření; podrobnější požadavky na řídicí a kontrolní systém, včetně požadavků na řízení rizik a informační systém, jsou stanoveny v příloze č. 1 vyhlášky č. 434/2009 Sb., kterou se provádějí některá ustanovení zákona o pojišťovnictví;
- 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).

[2] Příloha č. 1 bod 1 písm. d) úředního sdělení České národní banky ze dne 10. prosince 2010 k výkonu činnosti na finančním trhu: Kvalitativní požadavky související s výkonem činnosti – základní informace.

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

4. Zrušuje se 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, Věst. ČNB částka 18 ze dne 21. prosince 2010.

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

Příloha
Podrobnější informace České národní banky k výkonu činnosti na finančním trhu, 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:
Ing. Mazánková, tel. 224 412 821
Ing. Rott, tel. 224 412 659

Příloha

Podrobnější informace České národní banky k výkonu činnosti na finančním trhu, pokud jde o kvalitativní požadavky související s operačním rizikem v oblasti informačního systému

Základní cíle, prvky a parametry řízení operačního rizika v oblasti informačního systému

1. Řídící orgán poskytovatele finančních služeb schvaluje a pravidelně vyhodnocuje cíle a hlavní zásady řízení operačního rizika[3] v oblasti informačního systému (dále jen „operační riziko"), a to v rámci strategie řízení rizik, strategie rozvoje informačního systému a bezpečnostních zásad poskytovatele finančních služeb.

   Příklad 1:

   Poskytovatel finančních služeb např. ve strategii rozvoje informačního systému uvede hlavní cíle a konkrétní úkoly rozvoje, rámcový harmonogram jejich realizace a dostatečnou specifikaci finančních a lidských zdrojů pro realizaci strategie včetně vymezení zdrojů, které jsou nutné pro řízení případných souvisejících rizik, vyhodnocuje a případně upravuje strategii při významných změnách v obchodní strategii nebo v organizaci a řídící orgán poskytovatele finančních služeb přijme opatření k implementaci strategie nebo jejích změn.

   Příklad 2:

   Poskytovatel finančních služeb např. na základě analýzy rizik informačního systému (bod 6) a trendů v oblasti bezpečnosti informačních technologií stanoví v bezpečnostních zásadách hlavní cíle a zásady bezpečnosti a metody pro zajištění důvěrnosti, integrity a dostupnosti informací.

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, které jsou promítnuty do interních předpisů,
   c) kontrolní mechanismy řízení operačního rizika a výkonu souvisejících činností.

   Příklad 3:

   Poskytovatel finančních služeb např. promítne do systému řízení operačního rizika hlavní cíle a zásady (strategie, koncepci) své činnosti, zohlední v systému významné operačně rizikové faktory svých činností a procesů a externí rizikové faktory (např. změny stavu právního prostředí), vychází při tvorbě a údržbě systému z analýzy jeho účinnosti a efektivnosti a uplatňuje opatření zaměřená na omezování operačního rizika.

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, zásadami a postupy řízení operačního rizika,
   c) přidělení odpovědností za ochranu aktiv a plnění bezpečnostních zásad v oblasti informačního systému,
   d) zajišťování vývoje informačního systému v logicky i fyzicky odděleném vývojovém prostředí od prostředí produkčního,

[3] 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) oddělené provádění správy informačního systému od vyhodnocování bezpečnostních auditních záznamů, kontroly přidělování přístupových práv a vypracování a aktualizace bezpečnostních předpisů pro informační systém,
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.

Příklad 4:

Poskytovatel finančních služeb např. identifikuje a průběžně sleduje [písm. a)] oblasti, kde existuje možnost vzniku střetu zájmů při řízení operačního rizika a přiděluje odpovědnosti za plnění příslušných úkolů v systému řízení operačního rizika tak, aby bylo dostatečně zamezeno vzniku možného konfliktu zájmů. Odpovědnosti orgánů, pracovníků, útvarů a výborů, pokud jsou zřízeny, stanoví také s ohledem na zajištění účinné komunikace a spolupráce na příslušných úrovních řízení a s ohledem na zajištění funkčního, efektivního, řádného a obezřetného řízení operačního rizika.

Příklad 5:

Poskytovatel finančních služeb např. zabezpečí [písm. b)], aby pracovníci, jejichž činnost má vliv na řízení operačního rizika, byli seznámeni v potřebném rozsahu se schválenou strategií, zásadami a postupy řízení operačního rizika a postupovali v souladu s nimi.

Příklad 6:

Poskytovatel finančních služeb např. zajistí [písm. d)], aby:
(i) pracovník vyvíjející informační systém neměl přístup do provozního prostředí tohoto systému a pokud ve výjimečných a odůvodněných případech má přístup do provozního prostředí, pak musí být zajištěno, že jeho činnost v systému je kontrolována a dokumentována,
(ii) pracovník zajišťující provoz informačního systému neměl přístup do vývojového prostředí,
(iii) při vývoji informačního systému byla používána anonymizovaná provozní data; pokud ve výjimečných a odůvodněných případech je pro splnění cíle nezbytné použití provozních, minimálně časově již neaktuálních dat, je nezbytné přijmout opatření, která zajistí důvěrnost těchto dat včetně opatření zamezujících jejich zpětnému použití v produkčním prostředí.

Příklad 7:

Poskytovatel finančních služeb např. zajistí [písm. e)], aby pracovník zabezpečující výkon správy informačního systému nevyhodnocoval bezpečnostní auditní záznamy, nekontroloval přidělování přístupových práv, nevypracovával a neaktualizoval bezpečnostní předpisy pro jím spravovaný systém a nestanovoval/nerozhodoval o auditování/logování v systému, který věcně nebo technicky spravuje.

Příklad 8:

Poskytovatel finančních služeb např. zabezpečí [písm. f)], aby vyhodnocování bezpečnostních auditních záznamů bylo odděleno od činností souvisejících se zaznamenáváním událostí, které mohou ohrozit nebo narušit bezpečnost informačního systému, a zabezpečí též, aby byla prováděna kontrola této činnosti.

4. Zásady a postupy řízení operačního rizika zahrnují zejména:

a) zásady a postupy 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 souvisejících postupů, způsobu evidence a informačních toků při překročení limitů,
c) zásady a postupy stanovení míry akceptovaného operačního rizika,
d) zásady a postupy omezování výskytu či nepříznivých dopadů výskytu událostí operačního rizika,
e) zásady a postupy případného vyvedení operačního rizika mimo poskytovatele finančních služeb,
f) bezpečnostní zásady a postupy zajištění důvěrnosti, integrity a dostupnosti informací,

g) zásady kontrolních mechanismů a postupy kontrolních 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 postupy fyzické ochrany aktiv poskytovatele finančních služeb v oblasti informačního systému,
i) zásady a postupy zajištění personální bezpečnosti v oblasti informačního systému,
j) zásady a postupy řešení bezpečnostních incidentů v oblasti informačního systému,
k) zásady a postupy řešení operačního rizika při zajišťování dodávek zboží a služeb anebo při vykonávání některých činností v oblasti informačního systému prostřednictvím jiných osob (outsourcing), pokud je uplatňován či zvažován.

Příklad 9:

Poskytovatel finančních služeb stanoví [písm. a)] zásady a postupy pro řízení operačního rizika např. s ohledem na velikost, způsob řízení, počet pracovníků a povahu, rozsah a složitost svých činností. Zásady a postupy promítne do interních předpisů a zajistí seznámení všech příslušných pracovníků s nimi.

Příklad 10:

Poskytovatel finančních služeb např. stanoví [písm. b)] limity pro potřeby řízení, sledování a vyhodnocování operačního rizika a jeho událostí (např. limity v hodnotovém vyjádření pro zahrnování jednotlivých anebo opakujících se událostí operačního rizika do evidence operačních rizik) a předem stanoví postupy pro určení těchto limitů.

Příklad 11:

Poskytovatel finančních služeb např. stanoví [písm. c) až e)] postupy pro analyzování příčin vzniku a dopadu potenciálních a skutečných událostí operačního rizika na poskytovatele finančních služeb, pro porovnání dopadu podstupovaného operačního rizika souvisejícího s vykonávanými nebo plánovanými činnostmi a souvisejících nákladů na opatření k omezování rizika s přínosy příslušných činností a pro rozhodování o akceptaci rizika, vyvedení operačního rizika mimo poskytovatele finančních služeb anebo omezení nebo ukončení činností z důvodu dopadů podstupovaného operačního rizika.

Příklad 12:

Poskytovatel finančních služeb např. definuje [písm. f)] bezpečnostní zásady pro informační systém a jeho jednotlivé významné části. Přitom vychází z vlastní analýzy rizik a vlastní klasifikace (třídění a ohodnocení) aktiv informačního systému a jeho jednotlivých částí (např. jednotlivých informačních subsystémů) a souvisejících procesů.

Příklad 13:

Poskytovatel finančních služeb např. stanoví [písm. i)] postupy pro řízení přístupů pracovníků, klientů a dalších oprávněných osob k jeho hmotnému a nehmotnému majetku v oblasti informačního systému (např. prostor, kde jsou umístěny významné informační technologie anebo jiná aktiva informačního systému) a dále stanoví hmotnou odpovědnost oprávněných osob za poškození, zničení anebo krádež hmotného a nehmotného majetku v oblasti informačního systému.

Příklad 14:

Poskytovatel finančních služeb např. definuje [písm. j)] bezpečnostní incident v oblasti informačního systému a upraví monitorování, vyhodnocování, řešení a reportování o bezpečnostních incidentech a dokumentování těchto procesů.

Příklad 15:

Poskytovatel finančních služeb např. stanoví [písm. k)] v postupech pro řešení operačního rizika při zajišťování činností prostřednictvím outsourcingu pravidla pro výběr a vyhodnocování poskytovatelů outsourcingu (tento je prováděn např. na základě kombinace kriterií cena, kvalita služeb a produktů a důvěryhodnost poskytovatele), způsob vyhodnocování efektivnosti služeb zajišťovaných poskytovateli outsourcingu a také stanoví odpovědnosti a kontrolní a další povinnosti příslušných pracovníků za činnosti, které jsou předmětem outsourcingu.

5. Kontrolní mechanismy řízení operačního rizika zahrnují zejména:
   a) kontrolu dodržování zásad a postupů řízení tohoto rizika na všech řídicích a organizačních úrovních,
   b) přiměřené kontrolní mechanismy pro jednotlivé procesy, včetně outsourcovaných,
   c) fyzickou kontrolu v oblasti informačního systému,
   d) nezávislé prověření systému řízení tohoto rizika a funkčnosti a bezpečnosti informačního systému interním auditem, nebo jiné srovnatelné nezávislé prověření,
   e) vytvoření a udržování systému sledování opatření k nápravě zjištěných nedostatků.

   Příklad 16:

   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 v oblasti přístupů do informačního systému.

   Příklad 17:

   Poskytovatel finančních služeb např. stanoví [písm. b)] kriteria/indikátory pro sledování a vyhodnocování operačního rizika v procesech a liniích řízení v oblasti informačního systému a jejich posuzování začlení do své běžné kontrolní činnosti.

   Příklad 18:

   Poskytovatel finančních služeb např. kontroluje [písm. c)] fyzická omezení přístupu k hmotnému majetku a jiným aktivům informačního systému.

   Příklad 19:

   Poskytovatel finančních služeb např. zavede [písm. e)] evidenci všech přijatých opatření k nápravě zjištěných nedostatků v oblasti informačního systému, sleduje a vyhodnocuje v této evidenci jejich odstraňování a motivuje příslušné pracovníky k odstraňování nedostatků.

Vybrané postupy

6. Poskytovatel finančních služeb provede analýzu rizik spjatých s informačním systémem pro potřeby stanovení bezpečnostních cílů a zásad a přijetí opatření k minimalizaci rizik informačního systému. V analýze zejména definuje aktiva informačního systému[4], 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.

   Příklad 20:

   Poskytovatel finančních služeb např. vypracuje postupy pro provádění analýzy rizik spjatých s informačním systémem a provede vlastní klasifikaci aktiv svého informačního systému. Analýzu rizik aktualizuje např. při významných změnách informačního systému, významných změnách ve vývoji informačních technologií anebo při významných změnách v oblastech souvisejících s jejich bezpečností.

7. Poskytovatel finančních služeb
   a) vytvoří a udržuje plány pro obnovení své činnosti pro případy neplánovaného přerušení nebo omezení svých činností v oblasti informačního systému, zejména pokud jde o případné havárie informačního systému, selhání osoby, prostřednictvím které jsou vykonávány činnosti (outsourcing) v oblasti informačního systému, nebo

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

selhání externí infrastruktury významné pro informační systém, například dodávky energií (dále jen „pohotovostní plány“),

b) zabezpečí, aby pohotovostní plány byly pravidelně testovány, vyhodnocovány a případně aktualizovány,

c) zabezpečí, aby příslušní pracovníci byli s pohotovostními plány seznámeni a postupovali podle nich.

Příklad 21:

Poskytovatel finančních služeb např. stanoví [písm. a)] priority pro obnovení své činnosti v oblasti informačního systému a postupy pro sestavní a úpravy pohotovostních plánů, identifikuje rizikové události ohrožující tyto činnosti a vyhodnotí pravděpodobnost jejich výskytu a dopadu na poskytovatele finančních služeb.

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).

V pohotovostních plánech poskytovatel finančních služeb např. také stanoví konkrétní odpovědnosti útvarů a pracovníků a lhůty pro obnovu činností.

Příklad 22:

Poskytovatel finančních služeb např. vyhodnocuje a případně upravuje [písm. b)] pohotovostní plány při významných změnách v organizaci anebo povaze, rozsahu nebo složitosti činnosti, testuje efektivnost postupů a jejich zajištění v praxi. Výsledky testů dokumentuje.

Příklad 23:

Poskytovatel finančních služeb např. ověřuje [písm. c)] zda příslušní pracovníci mají k dispozici aktuální pohotovostní plány a jsou schopni podle nich postupovat.

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 vysledovatelnost (rekonstruovatetnost) 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 a postupů,

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,
l) pravidelné vyhodnocování a případné upravování zásad a postupů řízení operačního rizika.

Příklad 24:

Poskytovatel finančních služeb např. pořizuje záznamy komunikace s klientem v souvislosti s poskytováním investičních služeb a uchovává [písm. b)] v původní podobě záznamy komunikace s klientem v souvislosti s poskytováním investičních služeb, a to v případě, že ke komunikaci s klientem dochází prostředky komunikace na dálku. Poskytovatel finančních služeb dále používá a spravuje zařízení pro komunikaci s klientem v případě, že ke komunikaci s klientem dochází prostředky komunikace na dálku, přičemž zabezpečuje správu těchto zařízení pouze určeným správcem, má možnost pořídit úplný autentický výstup komunikace z těchto zařízení a zabezpečuje nezměnitelnost záznamu komunikace.

Příklad 25:

Poskytovatel finančních služeb např. identifikuje [písm. c)] zdroje operačního rizika nejen u významných a dalších činností a na příslušných organizačních úrovních poskytovatele finančních služeb, ale zaměřuje se i na odhalování nových, dosud neidentifikovaných operačních rizik v oblasti informačních systémů.

Příklad 26:

Poskytovatel finančních služeb např. zabezpečí [písm. e)] sledování a vyhodnocování:
(i) nadlimitních událostí operačního rizika a jejich dopadu na poskytovatele finančních služeb,
(ii) podílu/významnosti dopadu podlimitních a opakujících se událostí operačního rizika na celkových dopadech operačního rizika na poskytovatele finančních služeb,
(iii) operačního rizika na základě aktuálních, spolehlivých a ucelených informací o událostech a ztrátách vzniklých v důsledku tohoto rizika.

Příklad 27:

Poskytovatel finančních služeb např. zabezpečí [písm. f)] přiměřené informování příslušných pracovníků o:
(i) vyhodnocení událostí a ztrát vzniklých v důsledku operačního rizika, které se vztahují k předmětu jejich činnosti,
(ii) vyhodnocení kriterií/indikátorů operačního rizika v procesech a liniích řízení, které se jich týkají,
(iii) výsledcích analýz a opatřeních přijatých k omezování operačního rizika souvisejícího s jejich činností,
(iv) aktuálních hrozbách, které mohou způsobit výskyt události operačního rizika v jimi zabezpečované činnosti.

Příklad 28:

Poskytovatel finančních služeb např. zabezpečí [písm. h)] aby:
(i) přístupová práva byla uživatelům informačního systému přidělena na základě vymezení činnosti uživatele v informačním systému, klasifikace informací, prověření uživatele (platí pro uživatele, kteří mohou svou činností na základě přidělených přístupových práv významně ovlivnit bezpečnost a provozuschopnost informačního systému), popř. na základě podmínek vyplývajících z písemně uzavřeného smluvního vztahu mezi poskytovatelem finančních služeb a třetí osobou (poskytovatelem outsourcingu, klientem, apod.),
(ii) schvalování přidělení přístupových práv bylo odděleno od technické realizace přístupových práv v informačním systému,
(iii) u významných částí informačního systému byla vždy prováděna kontrola přidělení a odebrání přístupových práv,
(iv) informační systém obsahoval nástroje zajišťující jednoznačnou autentizaci uživatele,
(v) proces autentizace uživatele zajišťoval spolehlivé ověření jeho identity, proces autentizace uživatele byl kontrolován a byla přijata opatření vedoucí k zamezení neautentizovaných přístupů.

Příklad 29:

Poskytovatel finančních služeb např. zabezpečí [písm. i) a j)] aby:
(i) informační systém obsahoval nástroje zajišťující přístup k informacím v informačním systému pouze autorizovanému uživateli,
(ii) přístup uživatelů do významných částí informačního systému byl monitorován a vyhodnocován,
(iii) pokusy o neautorizované přístupy byly evidovány a vyhodnocovány a byla prováděna kontrola této činnosti,
(iv) informační systém obsahoval nástroje zajišťující důvěrnost a integritu autentizační informace,
(v) případy narušení důvěrnosti a integrity autentizační informace byly evidovány a vyhodnocovány a byla prováděna kontrola této činnosti.

Příklad 30:

Poskytovatel finančních služeb např. zabezpečí [písm. k)], aby informační systém podporoval nebo přímo zajišťoval zaznamenávání událostí, které ohrozily nebo narušily bezpečnost informačního systému, do bezpečnostních auditních záznamů, a tyto události byly evidovány a vyhodnocovány a byla prováděna kontrola této činnosti.

Příklad 31:

Poskytovatel finančních služeb např. zabezpečí [písm. l)] pravidelné vyhodnocování a případné úpravy zásad a postupů řízení operačního rizika, a to zejména v souvislosti s významnými změnami ve své obchodní strategii, organizaci řízení interních procesů, pracovníků anebo systémů a také v podmínkách externího ekonomického, právního, technického atd. prostředí.

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 vybavení[5], u kterého výsledky testů prokázaly, že bezpečnostní funkce jsou v souladu se schválenými bezpečnostními zásadami informačního systému; testovací prostředí musí být logicky i fyzicky odděleno od prostředí produkčního a 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,
   g) pravidelné prověřování a vyhodnocování bezpečnosti informačního systému.

Příklad 32:

Poskytovatel finančních služeb např. vypracuje a kontroluje dodržování postupů pro:
(i) provádění změn v informačním systému,
(ii) testování programového vybavení,
(iii) servisní činnost v provozovaném informačním systému,
(iv) zálohování informací a programového vybavení,
(v) schvalování přístupových práv do informačního systému.

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

Tyto postupy jsou pravidelně vyhodnocovány a případně upravovány, a to zejména s ohledem na změny informačního systému a vývoj informačních technologií.

Příklad 33:

Poskytovatel finančních služeb např. vypracuje [písm. a)] návrh na změnu informačního systému, který obsahuje:
(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.

Příklad 34:

Poskytovatel finančních služeb např. zabezpečí [písm. b)] oddělení testovacího a produkčního prostředí, používání fiktivních nebo anonymizovaných dat při testování, dokumentování výsledků testů; pokud ve výjimečných a odůvodněných případech je pro splnění cíle nezbytné použití provozních, minimálně časově již neaktuálních dat, je nezbytné přijmout opatření, která zajistí důvěrnost těchto dat včetně opatření zamezujících jejich zpětnému použití v produkčním prostředí.

Příklad 35:

Poskytovatel finančních služeb např. eviduje a vyhodnocuje [písm. g)] případy narušení bezpečnosti informačního systému.

Příklad 36:

Poskytovatel finančních služeb např. zabezpečí [písm. e)], aby informační systém obsahoval nástroje zajišťující bezpečnost připojení interní sítě k externí komunikační síti, a aby byly evidovány a pravidelně vyhodnocovány případy narušení bezpečnosti připojení a byla prováděna kontrola této činnosti.

Příklad 37:

Poskytovatel finančních služeb např. zabezpečí [písm. f)], aby informační systém obsahoval nástroje zajišťující důvěrnost a integritu informací při jejich přenosu externí komunikační sítí, a to zejména důvěrných informací, a také nástroje zajišťující dostatečně spolehlivou autentizaci komunikujících stran při přenosu informací externí komunikační sítí, a dále zajistí, aby byly evidovány a pravidelně vyhodnocovány případy narušení důvěrnosti a integrity informace při jejím přenosu a byla prováděna kontrola této činnosti.

10. V případě, že poskytovatel finančních služeb vykonává 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.

Příklad 38:

Poskytovatel finančních služeb např. zajistí:
(i) vytváření a poskytování přehledu o svých významných činnostech v oblasti informačního systému, které zajišťuje nebo k jejichž podpoře sjednal outsourcing, relevantním útvarům a osobám včetně dohledu České národní banky; v přehledu uvede charakteristiku outsourcovaných činností a služeb a identifikační údaje o jednotlivých poskytovatelích outsourcingu v oblasti informačního systému,
(ii) uzavírání smluvních vztahů s poskytovateli outsourcingu vhodnou, zpravidla písemnou formou,
(iii) že poskytovatel outsourcingu se ve smlouvě zavazuje: vykonávat činnosti, které jsou předmětem outsourcingu, v souladu s příslušnými právními předpisy a pokyny poskytovatele finančních služeb a zajistit předpoklady pro naplnění všech požadavků na outsourcing i v případě suboutsourcingu (řetězový outsourcing); umožnit a poskytnout součinnost oprávněným/pověřeným pracovníkům poskytovatele finančních služeb nebo třetích osob stanovených poskytovatelem finančních služeb při provedení kontroly outsourcovaných činností; umožnit a poskytnout součinnost České národní

bance při výkonu dohledu; umožnit a poskytnout součinnost při provedení auditu účetní závěrky poskytovatele finančních služeb a dalších ověřeních stanovených právními předpisy týkajících se poskytovatele finančních služeb; zabezpečit, že pracovníci, kteří vykonávají činnosti pro poskytovatele outsourcingu, jsou v adekvátním rozsahu seznámeni také s bezpečnostními zásadami poskytovatele finančních služeb a budou zachovávat mlčenlivost včetně mlčenlivosti o bezpečnostních opatřeních poskytovatele finančních služeb,

(iv) vyhodnocení potenciálních následků selhání či neplnění ze strany poskytovatele outsourcingu v oblasti informačního systému a ve smlouvě se proti této eventualitě adekvátně zajistí.