Dohled a regulace IS/IT ve finančních institucích z pohledu ČNB

Ing. Martin Fleischmann, Ph.D.

Česká národní banka

Sekce dohledu nad finančním trhem

ČIIA - setkání IA finančních institucí

2.10.2014, PWC , Hvězdova 1734 , Praha 4

Obsah

1. Cíl dohledu, přístup a hlavní principy dohledu IS/IT
2. Regulace v oblasti IS/IT
3. Kontrolované oblasti a očekávání ČNB (benchmarky)
4. Zkušenosti - nejčastější zjištění

Dohled ČNB v oblasti IS/IT

Sekce dohledu nad FT

- Odbor kontroly obezřetnosti (on-site) – 4 referáty
  - **Referát kontroly operačních rizik**
    - Řízení operačního rizika
    - **Řízení rizik IS/IT**
    - Validace pokročilých přístupů (operační riziko)
    - Zásady a postupy odměňování
    - Opatření proti legalizaci výnosů z trestné činnosti a financování terorismu

Operační riziko vs. Riziko IS/IT

- Obchody na FT = práce s informacemi (o peněžních hodnotách)
- IT stále více proniká do obchodních procesů (produkty, modely, …)
- Trendy: e - Banking (klient = uživatel IS/ICT), integrace IS/ICT v rámci FS, outsourcing, cloud computing, ….

☑ IT = kritické pro zajištění obchodu a jeho kontinuity

☑ IT = klíčový nástroj obchodní úspěšnosti

☑ Přesun rizik z manuálních do automatizovaných procesů

→ **Roste význam IS/IT v rámci ORM**

Poslání ČNB

Bezpečné fungování finančního systému

- Regulace finančního trhu
- Dohled nad osobami působícími na finančním trhu

Cíle dohledu v oblasti OR resp. IS/IT

- **minimalizace dopadů OR a rizik IS/IT na jednotlivé subjekty resp. na celý FT**
- adekvátního pokrytí rizik kapitálem

- Předpoklad = odpovídající řízení OR v bankách

Zásady dohledu a regulace OR a IS/IT

1. **Orientace na rizika (ani povrchní, ani příliš detailní)**
2. Principle based požadavky & očekávání
3. Technologická / metodologická neutralita
4. Proporcinalita = ohled na velikost, rozsah a povahu aktivit,…
   ⟷ *Comply or explain*
5. **Přednost obsahu nad formou** ⟷ *Comply or explain*
6. Nepřímý přístup k dohlíženým systémům a zařízením
7. Různý „jazyk“ na různých místech / úrovních
8. **Prezentace a vyjasnění zjištění**
9. **Nápravná opatření a jejich monitoring**
10. Follow up kontroly (dohledová šetření)

Dohled OR a IS/IT ve finančních institucích – přehled

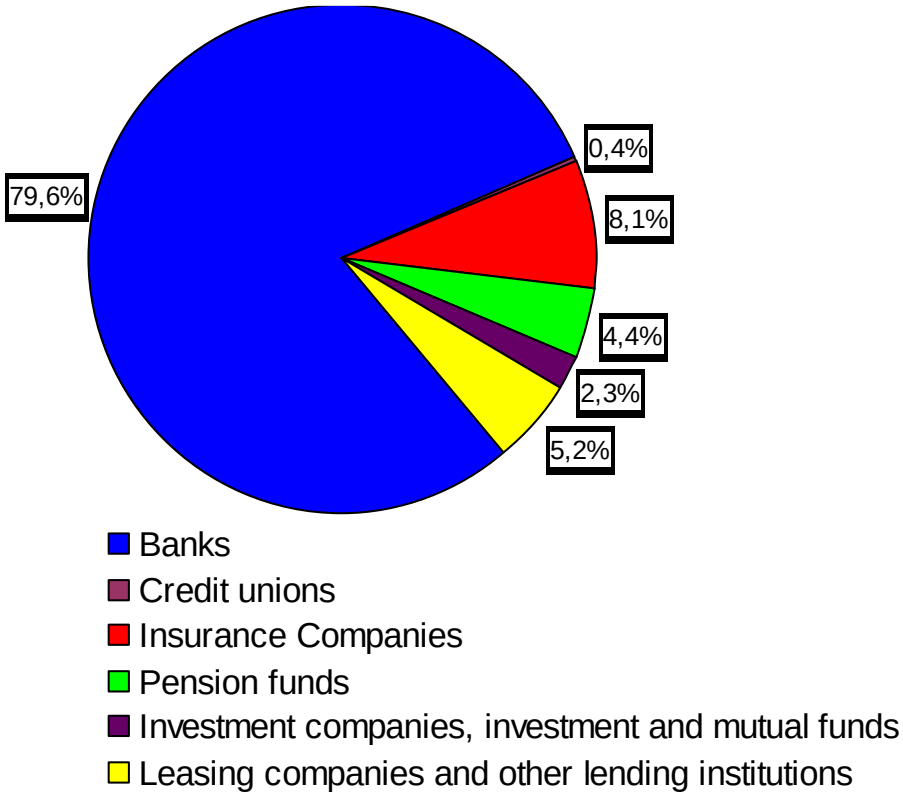
Dohled ČNB v oblasti OR :

- 23 bank
- 13 družstevních záložen
- Pojišťovny s ambicí interních modelů OR

Dohled ČNB v oblasti IS/IT :

- 23 bank
- 13 družstevních záložen
- 35 pojišťoven
- 10 penzijních fondů
- BCPP

Struktura finančního sektoru v ČR



Národní legislativní rámec – základní přehled

Zákony

- č. 21/1992 Sb., o bankách
- č. 87/1995 Sb., o spořitelních a úvěrních družstvech
- č. 277/2009 Sb., o pojišťovnictví
- č. 256/2004 Sb., o podnikání na KT

Vyhlášky

- Vyhláška č. 163/2014 Sb. o pravidlech obezřetného podnikání bank, spořitelních a úvěrních družstev a OCP (z 30.7.2014)
- Vyhláška č. 434/2009 Sb., kterou se provádějí některá ustanovení zákona o pojišťovnictví

Úřední sdělení České národní banky

- z 18.7.2007 – outsourcing - zrušeno (nahrazeno přílohou 7 vyhlášky 23/2014)
- z 10.12.2010 - Kvalitativní požadavky související s výkonem činnosti – základní informace
- z 29.12.2010 - Měření operačního rizika, stanovení kapitálového požadavku k operačnímu riziku
- z 29.12.2010 - Žádost o předchozí souhlas s používáním speciálního přístupu - zrušeno
- **z 27.5.2011 k výkonu činnosti na finančním trhu – operační riziko v oblasti informačního systému**

Shrnutí zákonných a regulatorních požadavků

- **Banky a DZ** - ze zákona povinny vytvořit, udržovat a uplatňovat funkční a efektivní řídicí a kontrolní systém včetně systému řízení rizik a informačního systému,
  - **podrobnější požadavky v části druhé a příloze č. 6 a 7 vyhlášky č. 163/2014 Sb.,**
- **Pojišťovny a zajišťovny** - podle § 6 odst. 1 zákona č. 277/2009 Sb., o pojišťovnictví povinny vytvořit a udržovat funkční a efektivní řídicí a kontrolní systém,
  - **podrobnější požadavky** na řídící a kontrolní systém, řízení rizik a informační systém, jsou v příloze č. 1 **vyhlášky č. 434/2009 Sb.**
- **Obchodník s cennými papíry** je podle ZPKT (č. 256/2004 Sb.) povinen uplatňovat řídicí a kontrolní systém, jehož součástí je také řízení rizik;
  - **podrobnější požadavky v části druhé vyhlášky č. 163/2014 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;
- **Provozovatel vypořádacího systému** je mj. podle § 83 odst. 9 písm. k) ZPKT povinen mít systém řízení rizik;
- **Centrální depozitář cenných papírů** - vyhláška č. 233/2009 Sb., např. v § 12 písm. a) bod 5;

Regulace pojišťoven (příklady)

Zákon č. 277/2009 Sb., o pojišťovnictví

§ 7: (1) Řídicí a kontrolní systém zahrnuje

a) předpoklady řádné správy

b) řízení rizik

c) systém vnitřní kontroly

Vyhláška č. 434/2009 Sb., kterou se provádějí některá ustanovení zákona o pojišťovnictví z 24.11.2009, **Příloha 1**

- Představenstvo zodpovídá za:
  - Strategii rozvoje IS + strategie pro **outsourcing**
  - Bezpečnostní zásady vč. IS/IT
- Systém řízení rizik
  - **Strategie a metody ŘR včetně OR**
  - Zásady pro sestavení a úpravy **pohotovostních plánů**
  - ŘR včetně řízení **OR**
- Interní audit pokrývá řízení rizik včetně bezpečnosti IS/IT

Regulace bank a DZ (příklady)

Vyhláška č. 163/2014 Sb. (z 30.7.2014)

§ 12: Outsourcing (§ 107 – Informace o outsourcingu)

§ 18: Řídící orgán (tj. představenstvo) schvaluje a pravidelně vyhodnocuje mj.:

- strategii řízení rizik (dle §30 vč. strategie řízení OR)
- strategii rozvoje informačního a komunikačního systému
- bezpečnostní zásady včetně bezpečnostních zásad pro informační systém
- akceptovanou míru rizika mj. pro OR
- vymezení a zásady přístupu povinné osoby k outsourcingu

Regulace bank a DZ (příklady)

Vyhláška č. 163/2014 Sb. (z 30.7.2014)

§ 22: Neslučitelné funkce v IS/IT

- Vývoj informačních systémů je zajišťován odděleně od provozu těchto systémů.
- Správa informačních systémů je prováděna odděleně od:
  - vyhodnocování bezpečnostních auditních záznamů,
  - kontroly přidělování přístupových práv
  - vypracování a aktualizace bezpečnostních předpisů pro tyto systémy.

Regulace bank a DZ (příklady)

Vyhláška č. 163/2014 Sb. (z 30.7.2014)

Informace a komunikace

§ 23, odst. 5

- podmínky přístupu zaměstnanců k informačnímu systému
- podmínky nakládání s daty a zajištění snadné zjistitelnosti jejich původního obsahu a provedených úprav,
- ochrana informačního systému před přístupem a zásahy ze strany neoprávněných osob

Regulace bank a DZ (příklady)

Vyhláška č. 163/2014 Sb. (z 30.7.2014)

§§ 27 – 33: Základní požadavky na Řízení rizik

§ 40

- Zásady a postupy pro vyhodnocování a ovlivňování míry podstupovaného **operačního rizika**
- Pohotovostní plány pro mimořádné situace

§ 49: Výkon vnitřního auditu (vč. OR a bezpečnosti IS/IT)

Regulace bank a DZ (příklady)

Vyhláška č. 163/2014 Sb. (z 30.7.2014)

Příloha č. 6 - Podrobnější požadavky na řízení operačního rizika

I. Systém řízení operačního rizika

II. Rozpoznávání, vyhodnocování, sledování a ohlašování operačního rizika

III. Omezování operačního rizika

IV. Kontinuita činností a pohotovostní plánování

V. Informační systémy a technologie

Regulace bank a DZ (příklady)

Vyhláška č. 163/2014 Sb. (z 30.7.2014)

Příloha č. 7 - Podrobnější požadavky na řízení rizika outsourcingu

I. Systém řízení rizika outsourcingu

II. Obecné zásady a postupy řízení rizik při outsourcingu

III. Zásady a postupy řízení rizik při realizaci outsourcingu

IV. Zásady a postupy řízení rizik ve vybraných případech outsourcingu

Celkem 8 stran

Srovnání regulace v oblasti OR & IS/IT, banky vs. pojišťovny - shrnutí

Z hlediska:

- obsahu – srovnatelné
- rozsahu– nesrovnatelné
  - (viz předchozí slidy)

Řešení = harmonizace prostřednictvím:

- **ÚS ČNB z 27.5.2011 k výkonu činnosti na finančním trhu – operační riziko v oblasti informačního systému**

Společný jmenovatel – napříč FT

- Úřední sdělení ze dne 27. května 2011 k výkonu činnosti na finančním trhu – operační riziko v oblasti informačního systému
- http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/legislativa/vestnik/2011/download/v_2011_05_20811560.pdf
- Záměrem ÚS – poskytnout věcný výklad a další informace k oblasti IS/IT

ÚS ČNB z 27.5.2011 k výkonu činnosti na finančním trhu – operační riziko v oblasti informačního systému (příklady)

3. Rámec řízení

…

c) Přidělení odpovědnosti za bezpečnost IS/IT,…;

d) Oddělení vývoje IS/IT od produkčního prostředí;

e) Správa IS/IT je oddělena 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 informace související s činností, o které je záznam pořízen.

ÚS ČNB z 27.5.2011 k výkonu činnosti na finančním trhu – operační riziko v oblasti informačního systému (příklady)

4. Zásady a postupy zahrnují:

f) zajištění důvěrnosti, integrity a dostupnosti IS/IT

h) fyzickou ochranu aktiv IS/IT

i) personální bezpečnost v oblasti IS/IT;

j) řešení bezpečnostních incidentů IS/IT

k) řízení rizik souvisejících s outsourcingem & třetími stranami

ÚS ČNB z 27.5.2011 k výkonu činnosti na finančním trhu – operační riziko v oblasti informačního systému (příklady)

6. Analýza rizik IS/IT:

- Definuje aktiva IS/IT,
- Identifikuje hrozby, kterým jsou aktiva vystaveny
- Identifikuje zranitelnosti
- Stanoví pravděpodobnost uplatnění hrozeb
- Odhaduje dopady
- Stanoví protiopatření

ÚS ČNB z 27.5.2011 k výkonu činnosti na finančním trhu – operační riziko v oblasti informačního systému (příklady)

7. BCM

a) plány pro obnovení činnosti, zejména pro případ:

- Havárie IS/IT,
- Selhání poskytovatele IS/IT
- Selhání externí infrastruktury

b) pravidelné testování, přehodnocování a aktualizaci pohotovostních plánů

c) seznámení relevantních zaměstnanců s pohotovostními plány

ÚS ČNB z 27.5.2011 k výkonu činnosti na finančním trhu – operační riziko v oblasti informačního systému (příklady)

8. Bezpečnost přístupu

…..

h) Autentizace uživatele

i) Přístup k IS/IT pouze autorizovaným uživatelům

j) Ochrana důvěrnosti a integrity autentizační informace

k) **Incident management** & ochrana bezpečnostních auditních záznamů proti neautorizovanému přístupu, modifikaci nebo zničení

ÚS ČNB z 27.5.2011 k výkonu činnosti na finančním trhu – operační riziko v oblasti informačního systému (příklady)

Odstavec 9.

- řízení změn
- zálohování
- síťová bezpečnost
- pravidelné prověřování a vyhodnocování bezpečnosti informačního systému (PDCA)

10. Outsourcing

- Zodpovědnost za outsourcované aktivity
- Soulad s právními předpisy
- Možnost auditu a výkonu dohledu u poskytovatele

Změny regulace

- Vydání nové vyhlášky 163/2014 souvisí s transpozicí Evropské směrnice (CRD IV) a vydáním nařízení (CRR)
  - V podstatě přebírá ustanovení Vyhlášky 123/2007, která byla zrušena
  - Nová příloha č. 7- **Podrobnější vymezení některých požadavků na outsourcing** (nahradila původní ÚS o outsourcingu)

    = posílení úpravy outsourcingu v rámci regulace

Kontrolované oblasti – vztah mezi OR a rizikem IS/IT

1. Strategie řízení operačního rizika
2. Řízení operačního rizika
3. **Strategie rozvoje informačních systémů**
4. **Bezpečnostní zásady informačních systémů**
5. **Řízení bezpečnosti informací (včetně AR a klasifikace aktiv)**
6. ***Události operačního rizika a bezpečnostní incidenty***
7. ***Fyzická bezpečnost***
8. **Bezpečnost přístupu k informačním systémům (vč. komunikačních sítí a monitoringu)**
9. **Provoz informačních systémů**
10. **Elektronické bankovnictví**
11. **Rozvoj informačních systémů**
12. ***Kontinuita činností a pohotovostní plánování***
13. Právní riziko
14. ***Outsourcing a smluvní vztahy***
15. ***Nezávislé ujištění (audit** operačního rizika a **rizik IS/IT)***
16. Kapitálový požadavek k OR

Kontrolované oblasti (pouze IS/ICT)

Systém řízení Bezpečnosti resp. Rizik IS/ICT

- Strategie rozvoje IS/ICT
- Organizace a oddělení neslučitelných funkcí
- Audit IS/ICT
- Bezpečnostní politika
- Klasifikace a řízení aktiv IS/ICT
- Hodnocení a řízení rizik
- Bezpečnostní incidenty
- Outsourcing a přístup třetích stran
- Personální bezpečnost
- Fyzická bezpečnost
- Vývoj a údržba systémů
- Řízení přístupu
- Monitorování používání a přístupu k systému
- Řízení komunikací a provozu
- E - banking
- Řízení kontinuity

Řízení a organizace IS/ICT

Bezpečnost IS/ICT

Provoz IS/ICT

Strategie rozvoje informačních systémů

- vychází z potřeb finanční instituce stanovených v její obchodní strategii
- obsahuje:
  - výčet priorit a hlavních úkolů rozvoje informačních systémů,
  - harmonogram
  - specifikaci finančních a lidských zdrojů pro realizaci strategie.
- jsou stanoveny odpovědnosti za plnění strategie informačních systémů a se strategií jsou seznámeni příslušní pracovníci.
- strategie je schválena a přehodnocována představenstvem.

Bezpečnostní zásady IS/IT

- Bezpečnostní zásady obsahují:
  - cíle bezpečnosti informačních systémů,
  - hlavní zásady a postupy pro zajištění důvěrnosti, integrity a dostupnosti informací,
  - odpovědnosti za ochranu aktiv a plnění bezpečnostních zásad.
- pokrývají všechny významné informační systémy a vycházejí z analýzy rizik informačních systémů.
- jsou stanoveny postupy a odpovědnosti jednotlivých útvarů a pracovníků za plnění bezpečnostních zásad.
- pracovníci jsou v potřebném rozsahu seznámeni s bezpečnostními zásadami.
- jsou schváleny a přehodnocovány představenstvem.

Řízení bezpečnosti informací

- odpovědnosti a pravomoci za řízení bezpečnosti informací jsou jednoznačné
- do řízení je zapojeno vrcholové vedení (včetně představenstva)
- je zamezeno vzniku možného střetu zájmů.
- bezpečnostní manažer disponuje odpovídajícími pravomocemi, zdroji a nezávislostí.
- existují postupy pro výběr zaměstnanců na klíčové pozice (požadavky na osobní integritu), jejich kontrolu a zastupitelnost.
- je k dispozici aktuální analýza rizik, výsledkem analýzy jsou opatření k omezení rizik a stanovení vědomě akceptovaných rizik.
- analýza rizik a klasifikace aktiv jsou východiskem pro stanovení vlastníků jednotlivých aktiv.
- kontrola shody s bezpečnostními zásadami a na ně navazujícími standardy.
- systém řízení bezpečnosti informací je pravidelně přehodnocován.

Události operačního rizika a bezpečnostní incidenty

- *události operačního rizika a bezpečnostní incidenty jsou vymezeny,*
- *jsou stanoveny odpovědnosti a postupy zajišťující jejich rozpoznávání, zaznamenávání (sběr), vyhodnocování, řešení (odezvy) a ohlašování.*
- *postupy jsou začleněny do běžných procesů instituce*
- *jejich vyhodnocování zohledňuje zejména možné dopady a ztráty.*
- *je zajištěna adekvátní integrita a dostupnost informací o událostech a bezpečnostních incidentech*

Fyzická bezpečnost

- *bezpečnostní perimetry*
- *zavedena technická a organizační opatření zohledňující hodnotu a význam hmotných i nehmotných aktiv*
- *opatření zajišťují fyzickou ochranu aktiv před jejich poškozením, zničením či zcizením v důsledku vnějších skutečností (například živelná událost) nebo lidského faktoru (krádež, vloupání).*
- *řízení přístupu zaměstnanců, klientů a dalších osob k hmotnému a nehmotnému majetku instituce včetně fyzické ochrany bankomatů, komunikačních sítí, nosičů dat a výpočetních center.*

Bezpečnost přístupu k informačním systémům

- Systém přístupu k informačním systémům
  - zohledňuje význam (hodnotu a citlivost) informací v nich uložených
  - vychází z provedené analýzy rizik.
  - stanovuje odpovědností a postupy pro přidělování, změny, odebírání, rušení, evidenci a archivaci přístupových práv a souvisejících informací.
- autentizace a autorizace jednotlivého uživatele
- kontrolní mechanismy včetně postupů pro monitorování přístupu k informacím a zaznamenávání událostí, které ohrozily nebo narušily bezpečnost informačních systémů,
- logy jsou kontrolovány v souladu s požadavky na oddělení neslučitelných funkcí.
- opatření k zajištění bezpečnosti vnitřní sítě,
- vnitřní síť banky je od vnějších bezpečně oddělena.
- provoz na sítích významný pro bezpečnost je zaznamenáván do logů.
- autentizace komunikujících stran a ochrana autentizačních informací.

Provoz informačních systémů

- Závazné postupy a odpovědnosti za řízení, správu a kontrolu prostředků zpracovávajících informace zajišťující:
  - správný a bezpečný provoz informačního systému,
  - minimalizují riziko selhání,
  - integritu programů a dat,
  - požadovanou dostupnost a důvěrnost informací
  - zohledňují požadavky na oddělení neslučitelných funkcí a na zastupitelnost klíčových zaměstnanců.
- Činnosti související se správou a změnami konfigurace (HW, OS, sítě, aplikace) jsou dokumentovány, archivovány a kontrolovány.
- Změny konfigurace jsou testovány v neprovozních systémech.
- Postupy dále upravují alespoň provádění patchů, plánování kapacity a vytíženosti systému, zálohování a archivaci dat, ochranu proti škodlivým programům, SLA s dodavateli a podporu koncových uživatelů.

Elektronické bankovnictví

Požadavky na internetové bankovnictví z pohledu:

- ČNB
  - Dodržování obezřetnostních pravidel
  - Řízení rizik (operační včetně právního, reputační, strategické)
- Bank
  - Dosažení obchodních cílů
  - Optimalizace poměru náklady/výnosy
  - Hodnocení a řízení rizik
- Z pohledu klienta:
  - Jednoduchá obsluha a nízká cena
  - …
    - Bezpečnost

Elektronické bankovnictví

Součásti eB (zdroje rizik)

- Použité technologie
- Infrastruktura banky
- Zaměstnanci, pravidla a postupy banky

- Klient (s různým přístupem, znalostmi a IQ)
- Zařízení na straně klienta

- Klient = významný zdroj rizik

Elektronické bankovnictví

Protiopatření :

- Použité technologie
  - Vývoj nových prvků zabezpečení
- Infrastruktura banky
  - Zdokonalování procesů autentizace
  - Fraud detection system
- Zařízení na straně klienta
  - Vzdělávání klienta
  - Snižování požadavků na technické znalosti klienta

Elektronické bankovnictví

Očekávání ČNB v oblasti eB / iB:

- Opatření a postupy k zabezpečení elektronické komunikace z hlediska:
  - autentizace a autorizace
  - podpora klientů (přiměřeně dle technického řešení)
- Sledování, vyhodnocování a řešení bezpečnostních incidentů
  - monitorování provozu
  - připravenost na incidenty (scénáře, krizové štáby, zapojení PR)
- Zajištění dostupnosti (havarijní plány, BCP – alternativní řešení, komunikace s klienty a jejich podpora
- Smluvní vztahy s klienty (ošetření rizik, srozumitelnost)
- Zajištění informovanosti klientů (průběžně)

Rozvoj informačních systémů

- postupy a odpovědnosti za vývoj, údržbu a provádění změn informačních systémů, které zajišťují:
  - oddělení neslučitelných funkcí.
  - realizaci rozvoje informačního systému v souladu se strategií rozvoje a navazujícími realizačními plány
  - implementaci bezpečnostních požadavků stanovených bezpečnostními zásadami a navazujícími předpisy
  - adekvátní testování systémů a jejich uvolňování do provozu (dokumentace, oddělené prostředí, apod.)
  - dostatečnou účast koncových uživatelů a subjektu zodpovědného za bezpečnost IS/IT.
- V případě dodavatelského způsobu jsou zavedeny postupy pro řízení a kontrolu dodavatelů.

Kontinuita činností a pohotovostní plánování

- *Business impact analysis / analýza rizik / scénáře a opatření*
- *Plány pro obnovení činností a havarijní plány IS/IT*
  - *postupy a odpovědnosti pro případ přerušení činností (obchodní síť, havárie IS/IT, selhání významných třetích osob, vnější infrastruktury)*
  - *Plány jsou testovány a výsledky testů dokumentovány a vyhodnocovány*
  - *Plány jsou pravidelně aktualizovány.*
- *Účast a jasné role obchodu i IT*

Outsourcing a smluvní vztahy

- *Strategie outsourcingu*
- *Postupy a odpovědnosti zajišťují:*
  - *přípravnou fázi včetně analýzy rizik*
  - *účinnou a efektivní kontrolu outsourcovaných činností*
  - *soulad s příslušnými právními předpisy,*
  - *Splnění regulatorních požadavků na předmětné činnosti*
  - *umožňují výkon dohledu ČNB včetně případné kontroly na místě u poskytovatele.*
- *Základní princip = za outsourcing zodpovídá povinná osoba*
- *ŘKS minimálně na úrovni, jakoby nedošlo k outsourcingu*

Rizika spojená s CC z pohledu regulátora – 2 strany téže mince

- **Poskytovateli CC služeb jsou většinou dobře technicky, organizačně, odborně i finančně vybavené nadnárodní společnosti**

- **CC přináší nová specifika, která v určitých ohledech zvyšují rizika.**
- **Účinnost opatření na omezení těchto rizik není dostatečně ověřena praxí.**

Rizika spojená s CC z pohledu regulátora (1/3)

- právní riziko
  - ochrana bankovního tajemství + ochrana osobních údajů
  - rizika vyplývající z uplatnění zahraničního práva
  - roste složitost a nároky na strukturu a obsah smluvního vztahu
- compliance riziko
  - obtížné zajištění souladu s požadavky různých národních legislativních a regulatorních požadavků
  - Možnost auditu/dohledu pro zákazníka/dohled nad FT
- regulatorní riziko
  - Nesplnění požadavků na outsourcing, (e.g.možnost výkonu kontroly ČNB u poskytovatele, nedostatečná kontrola outsourcovaných činností ze strany FI)
  - Neplnění regulatorních požadavků na IS/IT (FI je povinna zajistit ať už jsou předmětem outsouringu či nikoliv)

Rizika spojená s CC z pohledu regulátora (2/3)

- riziko ztráty správy (Loss of Governance)
  - ztráta schopnosti účinné kontroly outsourcovaných činností
  - **FI se nezbavuje své zodpovědnosti za outsourcované činnosti (a to ani částečně)!!!**
    - (According to **European data protection legislation** the cloud user always stays responsible for the data and fulfillment of all data protection requirements, irrespective of where the data is processed).
- riziko omezení auditovatelnosti (nezávislého ujištění)
  - ze strany IA - viz požadavek v § 33 Vyhlášky 123/2007

Rizika spojená s CC z pohledu regulátora (3/3)

- riziko nerovného postavení
  - neschopnost být rovnocenným (stejně silným) partnerem ve smluvním vztahu vůči některým poskytovatelům CC
- reputační riziko
  - např. z titulu některých kauz: Snowden
- riziko závislosti na poskytovateli (exit strategy risk)
  - obtížná zpětná migrace dat a služeb zpět do vnitřního IT prostředí
  - obtížný přechod k jinému poskytovateli
- riziko koncentrace
  - důležité z hlediska stability finančního trhu
  - výpadek dominantního dodavatele negativně ovlivní fungování celého finančního trhu.

Změny regulace outsourcingu

- § 107 **Informace o outsourcingu**
  - Pokud povinná osoba pro zajištění svých významných činností nebo k jejich podpoře **sjednává** outsourcing, informuje o tom **v dostatečném předstihu** Českou národní banku. Součástí této informace je přehled takto vykonávaných činností a základní identifikační údaje o poskytovateli outsourcingu.
- navrhovaná úprava reflektuje praxi některých regulátorů i doporučení CEBS/EBA - **GUIDELINES ON OUTSOURCING (**14 December 2006) kde se k informování dohledového orgánu uvádí:
- „An *outsourcing institution should adequately inform its supervizory authority on any material activity to be outsourced. Such information should be made available in a timely manner in order for the supervisor to evaluate the proposal or to allow him to consider whether the proposal raises prudential concerns and to take appropriate action if required.“*

- http://www.eba.europa.eu/documents/10180/104404/GL02OutsourcingGuidelines.pdf.pdf

Přístup ČNB k problematice CC
- Shrnutí -

- CC považujeme za outsourcing
  - 1 z forem outsourcingu s určitou přidanou hodnotou, ale také specifickými riziky
- OR vs. outsourcing
  - Řízení rizik spojených s outsourcingem je součástí ŘKS finanční instituce
  - Rizika outsourcingu jsou podmnožinou OR
- ČNB momentální necítí potřebu doplnit regulaci o specifické požadavky na CC

Nezávislé ujištění (audit rizik IS/IT)

- Řízení rizik IS/IT je předmětem auditu v potřebné míře a rozsahu.
- Audit je prováděn osobami dostatečně způsobilými (zejména oblast IS/IT).
- Jednotlivé akce vycházejí s plánu auditu zohledňujícího rizikovost, jsou prováděny způsobem zohledňujícím auditorské zásady (nezávislost).
- Výstupy auditu jsou příslušným způsobem reportovány a zjištěné nedostatky jsou odstraňovány.

Nezávislé ujištění (audit rizik IS/IT)

Očekávání ČNB na činnost interního auditu:

- Jeho aktivity budou pokud možno průběžné
- Postihnou změny procesů a systémů, fluktuaci klíčových zaměstnanců, legislativu, regulaci atd.
- Pravidelně komunikuje se senior managementem
- Zajišťuje konzultační roli
- Účastní se vybraných projektů
- Připomínkuje vnitřní předpisy

Nezávislé ujištění (audit operačního rizika a rizik IS/IT)

Další požadavky kladené na interní auditory:

- Kvalifikace
  - Toretická **znalost** této **rozsáhlé oblasti** (standardy, guidelines, papers)
  - **Speciální znalosti a schopnosti** (IS/IT)
- Provádění auditu
  - **Komplexní záběr s přiměřenou hloubkou**
  - **Odpovídající periodicita**
  - **Důslednost a systematický přístup k odstranění zjištěných nedostatků**
- Interní auditor = „vztahový“ manager (nikoliv pouhý kontrolor), avšak s tím, že si musí zachovat svou nezávislost

---

- If the internal audit does not possess sufficient prerequisites, the assessment should be performed by qualified independent third party

Nejčastější zjištění

Nejčastější kontrolní zjištění z oblasti řízení rizik IS/IT **napříč segmenty finančního trhu**:

- **Analýza rizik informačních systémů neslouží jako východisko** ke stanovení bezpečnostních politik a dalších opatření pro zajištění důvěrnosti, integrity a dostupnosti informací
- Nesoulad vnitřních předpisů a v praxi vykonávaných činností
- Nedostatky ve smlouvách o outsourcingu, např.:
  - nejednoznačné stanovení odpovědností za vykonávané činnosti
  - nezajištění možnosti výkonu dohledu nad outsourcovanými činnostmi)

Nejčastější zjištění

Příklady zjištění v segmentu **bank**:

- Neaktuální či neúplná předpisová základna (*substance over form*)
- Nejednoznačná nebo chybějící klasifikace informačních aktiv
  - chybějící identifikace aktiv a jejich vlastníků
- Nedostatky v AR, např.:
  - chybějící identifikace hrozeb působících na aktiva či analýza dopadů
- Strategie rozvoje informačních systémů není pravidelně aktualizována, plnění strategie není vyhodnocováno
- Nedostatečné řízení a kontrola outsourcingového vztahu
- Neproaktivní a neefektivní monitoring informačních systémů
- Chybějící ověření/kontrola zařízení připojených do počítačové sítě banky

Nejčastější zjištění

U **družstevních záložen** se obecně jedná o závažnější a systémovější nedostatky než v segmentu bank:

- Nedostatky při definici a dodržování bezpečnostních zásad
- Neúplná nebo chybějící Analýza rizik informačních systémů
- Souběh neslučitelných funkcí
- Neúplná a neaktuální předpisová základna
- V oblasti outsourcingu informačních technologií není dostatečně smluvně ošetřeno určení odpovědností za vykonávané činnosti a zajištění bezpečnosti informací

Nejčastější zjištění

Příklady zjištění v segmentu **pojišťoven**:

- Nedůsledné oddělení vývoje od provozu informačních systémů
- Přidělování přístupových práv k IS mimo standardní proces
- Nedostatečná kontrola privilegovaných účtů u poskytovatelů outsourcingu
- Nedostatečné vymezení odpovědností v souvislosti s procesem havarijního plánování, neidentifikovány klíčové procesy pro sestavení havarijních plánů
- Neprovedeno nezávislé ujištění v oblasti provozu a bezpečnosti IS/IT,
- Absence plánu auditu pro oblast IS/IT
- Absence kontroly připojených periferií, zejména USB zařízení

Řízení rizik IS/IT – příklady zjištění 1

- Nedostatečná podpora vedení
- Nestanovení „vlastníků“ informačních aktiv
- Nejasné přidělení zodpovědnosti za bezpečnost resp. ŘR IS/ICT
- ISO resp. útvar BIT - nedostatečné pravomoci, závislost na vedení ICT)
- Nedostatečná kontrola klíčových pozic
- Absence zastupitelnosti klíčových pozic

Řízení rizik IS/IT – příklady zjištění 2

Řízení kontinuity obchodních činností (BCM)

- Absence BIA (Business Impact Analysis) nebo nedostatečná BIA!
  - absence BIA = neexistuje základní předpoklad pro BCM organizace
- Nedostatečná BIA – příčiny:
  - chybí potřebná odbornost (pro vypracování i implementaci BIA)
  - absence podpory vedení organizace a nedostatečné zapojení relevantních útvarů
- Nedostatečná BIA – důsledky = nedostatky v oblasti BCM:
  - BCM nepokrývá všechny kritické činnosti
  - chybí provázanost manuálních a automatizovaných činností
- Plány kontinuity podnikání
  - nemají dostatečnou vazbu na BIA (výsledky BIA nejsou využity)
  - nejsou dostatečně provázány s DRP pro IT systémy
  - neprovádí se jejich testování
  - nejsou vůbec zpracovány !

Řízení rizik IS/IT –příklady zjištění 3

Řízení outsourcingu

- Nerozpoznání outsourcingu
  - banka nevyhodnotí vztah s externím dodavatelem jako outsourcing
  - nepřijme opatření požadovaná regulací (vč. oznamovací povinnosti)
- Nedostatky ve smlouvách o outsourcingu
  - chybí předpoklady pro řízení a kontrolu outsourcovaných činností
  - neobsahuje ustanovení požadovaná regulací
- Nedostatečná kontrola outsourcovaných činností a řízení rizik v době trvání outsourcingového vztahu
  - široká škála nedostatků
- Oznamovací povinnost a komunikace s regulátorem
  - oznamování ex post i v případech velmi významného outsourcingu (méně časté)
    - instituce podstupuje regulatorní riziko

Řízení rizik IS/IT – příklady zjištění 4

Nezávislé ujištění

Nedostatečné nezávislé ujištění o outsourcovaných aktivitách

- Outsourcované aktivity nejsou předmětem IA vůbec nebo nedostatečně
  - Typicky IS/IT
  - Obvykle ve spojení s nedostatečnou kontrolou outsourcingu ze strany instituce
- V případě nedostatečných kapacit IA může vykonat EA – interní auditor musí zaručit adekvátní kvalitu (scope, periodicitu, výstupy, nápravu nedostatků, etc.)
  - Je nutná znalost outsourcovných aktivit

Očekávání ČNB:

- Outsourcované aktivity jsou pokryty interním auditem (interním auditem skupiny nebo externím auditorem) jakoby outsourcovány nebyly

Řízení rizik IS/IT – příklady zjištění 5

- Řízení přístupu:
  - nedostatečná vazba na AR a KA
  - schvalovací proces (absence formalizace, rekonstruovatelnosti, …)
  - absence komplexní správy (evidence) přístupových práv
  - neostatečná kontrola (zda skutečná práva odpovídají schváleným)
  - nejsou zjišťovány fiktivní účty
  - realizace přístupových práv
    - při zadávání práv do systému chybí princip 4 očí
    - Proces není
  - skupinové účty! (dosti časté)
  - hesla (špatná heslová politika, nedodržování heslové politiky)

Řízení rizik IS/IT – příklady zjištění 6

- Monitorování používání a přístupu:
  - politika (přístup) k monitoringu
    - chybí analýza, které IS mají být auditovány
    - chybí analýza, co má být obsahem auditních záznamů
    - chybí pravidla pro nakládání s auditními záznamy
  - není prováděna kontrola auditních záznamů
  - auditní záznamy nejsou archivovány
  - absence proaktivní kontroly auditních záznamů (nástroje)
  - není sledováno používání silných přístupových práv
  - absence kvalifikovaného posouzení (např. konfigurace FW)
  - podceňování vnitřních hrozeb - spoléhání se na oddělení vnější a vnitřní sítě (FW, IDS, IPS, DMZ)

???

Děkuji za pozornost

www.cnb.cz

Martin Fleischmann

martin.fleischmann@cnb.cz