Novinky nie len zo sveta IT / 03 – 2012

ISACA
Dôvera v informačné systémy a ich prínos
Slovensko Chapter

ISACA NEWSLETTER

Asociácia ISACA, založená v roku 1969, je so svojimi vyše 95 000 členmi vo viac ako 190 krajinách renomovanou profesijnou organizáciou a lídrom v oblasti riadenia, bezpečnosti a kontroly informačných technológií.

ISACA Slovensko vznikla v roku 1999 ako občianske združenie, ktoré úzko spolupracuje s medzinárodnou asociáciou ISACA.

Editoriál

Riziko je nielen hrozba, že utrpíme stratu, ale aj možnosť, že sa nám vráti to, čo sme investovali. A keďže sme s rizikom konfrontovaní každý deň či už v práci alebo v súkromnom živote, mali by sme byť v jeho zvládaní odborníci, ktorí nepotrebujú žiadny návod či usmernenie. Že by sa vám v súkromí nejaký ten recept na riziko predsa len zišiel? Ak taký recept máte, podeľte sa s nami. My sa s vami zase radi podelíme o to, ako pomocou Risk IT zvládať riziko v oblasti informačných technológií.

Jana Pfeifer, CISM, CRISC

ISACA Slovensko pozýva na konferenciu

11. ročník konferencie ABIT
Ochrana súkromia

25.októbra 2012
Hotel Hradná Brána, Slovanské nábrežie 15, Bratislava – Devín
Registrácia na *www.isaca.sk*

ROBÍME IT SVET
BEZPEČNÝM

30. november 2012
Radisson Blu Carlton Hotel, Bratislava
www.itvip.sk

ISACA Slovensko pozýva na spoluprácu zameranú na inováciu a rozšírenie vzdelávacích aktivít a širšie zapojenie odborníkov z praxe. Námety na spoluprácu zasielajte na adresu: *stefanska@isaca.sk*

Rozhovory s ľuďmi inšpirujú

Ing. Kristína Lachová
CISA

3–4 →

Kalendár udalostí 2012

25.10.
Konferencia ABIT 2012

8.12.
Certifikovaná skúška CISA/CISM/CGEIT/CRISC

30.11.
Predstavenie projektu „Robíme IT svet bezpečným“

Redakčná rada

Obsah

Risk IT

Množina riadiacich princípov a prvý rámec, ktorý pomáha podnikom identifikovať, riadiť a efektívne spravovať IT riziká.

V podnikaní dnes hrajú riziká kritickú úlohu. Takmer každé biznis rozhodnutie vyžaduje, aby riadiaci pracovníci vyvažovali súvisiace riziká a prínosy. Efektívny manažment biznis rizík je nutnosťou pre úspech spoločnosti.

Často sa stretávame s prehliadaním IT rizík (biznis riziká súvisiace s využívaním IT). Pritom ostatné biznis riziká ako napríklad trhové, úverové a prevádzkové sa stali súčasťou podnikových rozhodovacích procesov. IT riziká boli preradené technickým špecialistom, mimo zasadnutí správnej rady, napriek tomu, že spadajú pod tú istú kategóriu ako ostatné biznis riziká: čoho dôsledkom je zlyhanie napĺňania strategických cieľov.

Problém je jasný. Riešenie? Nejasné.

Až doteraz: **Predstavujeme Risk IT.**

Čo je Risk IT?

Risk IT je:

- Rámec, ktorý pomáha zaviesť efektívne riadenie a správu IT rizík
- Súčasť produktového portfólia ISACA pre oblasť riadenia IT
- Rámec založený na sade riadiacich princípov pre efektívny manažment IT rizík

Aké sú výhody používania Risk IT?

Výhody používania Risk IT zahŕňajú:

- Spoločný jazyk pri komunikácii medzi obchodnými zložkami, IT, manažmentom rizík a auditu
- End-to-end návod ako manažovať riziká súvisiace s využívaním IT
- Kompletný profil rizík slúžiaci k lepšiemu pochopení rizík a lepšiemu využitiu podnikových zdrojov
- Lepšie pochopenie rolí a zodpovedností vzhľadom na manažment IT rizík
- Súlad s podnikovým systémom manažmentu rizík (ERM)
- Lepší pohľad na riziká súvisiace s využívaním IT a zodpovedajúce finančné implikácie
- Menší počet neželaných prevádzkových situácii a zlyhaní
- Zvýšenie kvality informácii
- Zvýšená istota zúčastnených strán a zmenšené obavy vyplývajúce z regulačných požiadaviek
- Inovatívne aplikácie podporujúce nové obchodné iniciatívy

Čo Risk IT umožňuje?

Risk IT:

- Umožňuje spoločnostiam prispôsobovať komponenty rámca tak, aby vyhovovali ich potrebám.
- Poskytuje end-to-end komplexný pohľad na všetky riziká súvisiace s používaním IT a rovnako dôkladné ošetrenie rizík od vysokoúrovňových oblastí až po prevádzkové otázky.
- Umožňuje spoločnostiam porozumieť a riadiť všetky zásadné typy IT rizík
- Poskytuje hmatateľné obchodné prínosy
- Umožňuje spoločnostiam vykonávať rozhodnutia s uvedomením si zodpovedajúcich rizík
- Vysvetľuje ako zarobiť na investíciách do už zavedeného interného kontrolného systému IT pre manažment IT rizík.
- V rámci hodnotenia a manažmentu IT rizík umožňuje integráciu s celopodnikovými prístupmi pre manažment rizík a regulačných

> Efektívny manažment biznis rizík je nutnosťou pre úspech spoločnosti.

Princípy Risk IT

Rámec Risk IT je o IT rizikách – biznis rizikách súvisiacich s využívaním IT. Prepojenie na biznis sa nachádza v princípoch, na ktorých je rámec postavený. Efektívne podnikové riadenie a správa rizík:

- Vždy súvisí s biznis cieľmi
- Vytvára súlad medzi IT rizikami a celkovým podnikovým systémom manažmentu rizík (ERM) – ak je to možné. Napríklad ak je ERM implementované v rámci spoločnosti
- Vyvažuje náklady a prínosy manažmentu IT rizík
- Podporuje spravodlivú a otvorenú komunikáciu ohľadne IT rizík
- Zavádza správny prístup zhora pri definovaní a vynucovaní osobných zodpovedností za prevádzku, v rámci prijateľných a dobre definovaných úrovní tolerancie.
- Je kontinuálny proces a súčasť každodenných aktivít

Manažment a porozumenie IT rizík

Pre stanovenie priorít IT rizík a ich správu, potrebujú predstavitelia vysokého manažmentu referenčný rámec a jasnú predstavu o funkcii IT a súvisiacich rizikách. Avšak kľúčové zainteresované strany vrátane členov rady a vysokého manažmentu, práve tí ktorí by mali byť zodpovední za manažment rizík v rámci podniku, často túto predstavu nemajú.

IT riziká nepredstavujú len technický problém. Zatiaľ čo experti pre oblasti IT pomáhajú pochopiť a riadiť rôzne aspekty IT rizík, obchodný manažment je najdôležitejšia zúčastnená strana. Obchodní manažéri určujú čo IT potrebuje urobiť pre podporu ich biznisu; nastavuje ciele pre IT a zároveň je zodpovedný za manažment súvisiacich rizík.

Rámec Risk IT vysvetľuje IT riziká, umožňuje spoločnosti vykonávať obchodné rozhodnutia s uvedomením si zodpovedajúcich rizík a tým umožňuje používateľom:

- Integrovať a riadiť IT riziká v rámci celkového podnikového manažmentu rizík (ERM)
- Vykonávať dobre informované rozhodnutia vzhľadom na rozsah rizika, mieru akceptovania a tolerancie rizika v rámci prostredia spoločnosti.
- Porozumieť ako reagovať na riziká
- V súhrne, rámec umožňuje podnikom pochopiť a riadiť všetky závažné typy rizík. Rámec Risk IT poskytuje komplexný end-to-end pohľad na všetky riziká súvisiace s využívaním IT ako aj na samotný manažment rizík. Rámec zapĺňa medzeru medzi všeobecnými systémami riadenia rizík ako napríklad COSO ERM, AS/NZS 4360 (čoskoro nahradený ISO 31 000) a jeho britským ekvivalentom ARMS6 a detailnejšími systémami riadenia rizík (často zameranými na bezpe-čnosť).

Risk IT publikácie

Risk IT pozostáva z dvoch publikácii: Rámec Risk IT (Risk IT Framework) a Praktický sprievodca (Risk IT PractitionerGuide).

Risk IT Framework poskytuje:

- Sadu riadiacich praktík pre manažment rizík
- End-to-end procesný rámec pre úspešný manažment rizík
- Všeobecný zoznam často sa vyskytujúcich, potenciálne nežiaducich IT rizikových scenárov, ktoré môžu negatívne ovplyvniť realizáciu biznis cieľov.
- Nástroje a techniky na pochopenie konkrétnych rizík obchodným operácii, ako protiklad k všeobecným kontrolným zoznamom, alebo požiadavkám na súlad a zhodu.

Rámec poskytuje základné stavebné komponenty, na základe ktorých buduje komplexný procesný model pre IT riziká. Pre používateľov COBIT a Val IT, bude tento prístup určite známy. Návod je poskytnutý pre kľúčové aktivity každého procesu, zodpovednostiach za proces, informačných tokoch medzi procesmi a výkonnostným riadením každého procesu. Model je rozdelený na tri domény – Riadenie rizík, Hodnotenie rizík a Reakcia na riziká – každá z nich obsahuje tri procesy:

- Riadenie rizík
  - Vytvorenie a udržiavanie spoločného pohľadu na riziká
  - Integrácia s podnikovým systémom manažmentu rizík (ERM)
  - Tvorba obchodných rozhodnutí s uvedomením si zodpovedajúcich rizík
- Hodnotenie rizík
  - Zber dát
  - Analýza rizík
  - Udržiavanie profilu rizík
- Reakcia na riziká
  - Šírenie povedomia o rizikách
  - Manažment rizík
  - Reagovanie na udalosti

Risk IT PractitionerGuide

Je podporný dokument pre rámec Risk IT, ktorý poskytuje príklady a možné techniky adresovania problémov súvisiacich s IT rizikami, ako aj detailné návody ako napĺňať koncepty pokryté v procesných modeloch rámca. Koncepty a techniky zahŕňajú:

- Tvorbu scenárov, založenú na sade všeobecných IT rizikových scenároch
- Tvorbu mapy rizík za využitia techník pre popis dopadu a frekvencie jednotlivých scenárov
- Tvorba kritérií dopadu v závislosti od relevantnosti pre biznis
- Definovanie KRI (kľúčové indikátory rizika)
- Použitie COBIT a Val IT na zmiernenie rizika; prepojenie medzi rizikami, COBIT a Val IT kontrolnými mechanizmami a kľúčovými riadiacimi praktikami.

Vaše riešenie pre IT riziká

Použitie osvedčených praktík manažmentu IT rizík podľa Risk IT poskytne značné obchodné výhody, ako napríklad menej prevádzkových chýb a neželaných situácii, zvýšenú kvalitu informácii, väčšiu istotu zúčastnených strán a zníženie obáv z regulácie, inovatívne aplikácie podporujúce obchodné iniciatívy. Rámec Risk IT je súčasťou produktového portfólia ISACA, pre zastrešenie riadenia IT. Napriek tomu, že poskytuje kompletný a samostatný rámec, obsahuje taktiež referencie na COBIT a Val IT. Tie sú obsiahnuté v praktickom sprievodcovi, a je odporúčané aby sa manažéri a odborníci zoznámili so základnými princípmi a obsahom týchto dvoch rámcov. Rovnako ako COBIT a Val IT, Risk IT nie je štandard, ale flexibilný rámec. To znamená, že spoločnosti jeho jednotlivé komponenty môžu/mali by prispôsobiť svojím špecifickým potrebám.

Preklad, **Stanislav Ondac**

PLAUT

Aby služby boli každému bližšie

www.plaut.sk

Plaut Slovensko, s.r.o., Ďurgalova 16, 831 01 Bratislava
Tel.č. 02/321 514 11, Fax: 02/321 514 12, E-mail: info@plaut.sk

Riadenie IT rizík ako súčasť riadenia operačného rizika v bankách.

V tomto článku budeme vychádzať z reálnej situácie riadenia IT rizík v bankovom sektore. Článok nepopisuje všeobecné pravidlá riadenia IT rizík, ale konkrétny spôsob akým jedna z bankových skupín vníma a riadi operačné riziko, ktorého súčasťou je aj riadenie IT rizík.

Riadenie operačného rizika v bankách je len jednou časťou riadenia celkového rizika banky (Obr. 1).

OBR. 1 – ROZDELENIE RIZÍK

Riadenie rizík a operačného rizika pritom vychádza aj z regulácie Basel II.

Operačné riziko sa môže vnímať aj v širšom kontexte ako je len riadenie čisto prevádzkových rizík, pod ktoré spadá aj riadenie IT rizika (Obr. 2).

OBR. 2 – PREVÁDZKOVÉ RIZIKO AKO PODMNOŽINA OPERAČNÉHO RIZIKA.

IT riziko je v tomto prípade zamerané hlavne na riadenie rizík súvisiacich so zlyhaním IT technológií, zlyhaním systémov, zlyhaním IT procesov a zlyhaním ľudského faktora v IT.

Globálny program certifikácie

CISA Certified Information Systems Auditor®
An ISACA® Certification

CISM Certified Information Security Manager®
An ISACA® Certification

CGEIT Certified in the Governance of Enterprise IT®
An ISACA® Certification

CRISC Certified in Risk and Information Systems Control™
An ISACA® Certification

CISA certifikát získalo viac ako 70 000 profesionálov po celom svete.

Viac ako 11 000 osôb z viac ako 80 krajín sveta doteraz získalo certifikáciu CISM.

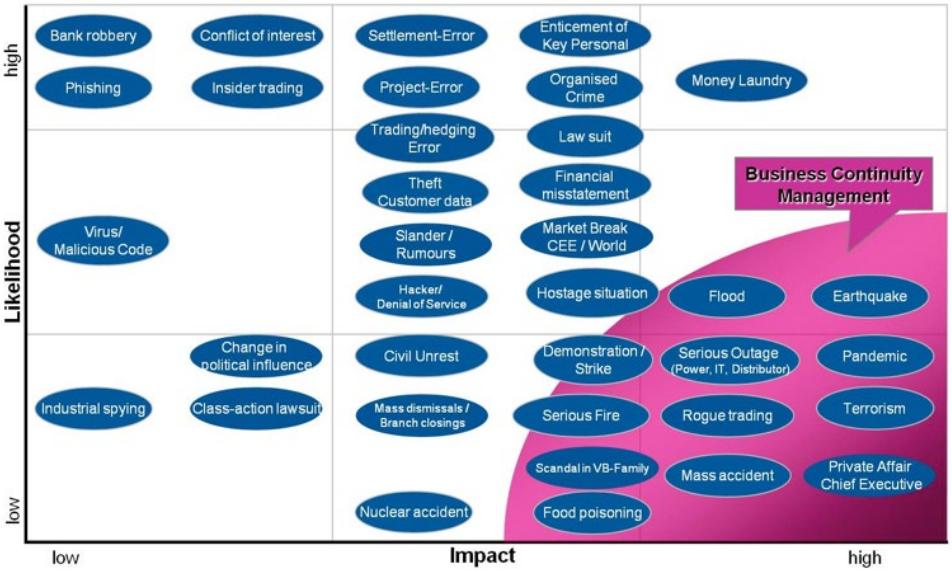
Marketingové oddelenie

Zuzana Kopáčiková – Štefanská, PhD.
Marketing & Communication Manager

E-mail: *stefanska@isaca.sk*
Web Site: *www.isaca.sk*

FOTOGRAFIE KONFERENCIA A WORKSHOP COBIT 5 (2012)

Rozdelenie rizík na základe ich dopadu na banku a frekvencie výskytu, umožňuje adekvátne reagovať na možné hrozby. Rozdelenie rizík môže vyzerať napríklad tak, ako je uvedené na obr. 3.



OBR. 3 ROZDELENIE RIZÍK NA ZÁKLADE ICH DOPADU NA BANKU

Následky rizík z oblasti s vysokým dopadom na banku, sa znižujú vytváraním plánov obnovy v rámci BCM (Business Continuity Management), ktorých súčasťou sú DRP (Disaster Recovery Planning) plány s konkrétnymi opatreniami týkajúcimi sa IT technológií.

Ostatnétypy IT rizík sa riešia adekvátnymi IT prostriedkami, napr. možné napadnutie počítačov vírusmi sa rieši prostredníctvom nasadenia antivírusových programov.

Súčasťou riadenia rizík je aj ich kontinuálne hodnotenie prostredníctvom KRI (Key Risk Indicator). Neexistuje všeobecný návod ktoré KRI a ako vyhodnocovať. Vytvorenie KRI indikátorov je preto veľmi individuálne a závisí od každej banky akým spôsobom ich nastaví. Jeden z príkladov je uvedený na obr. 4 a 5. ↗

Key Risk Indicator Description:

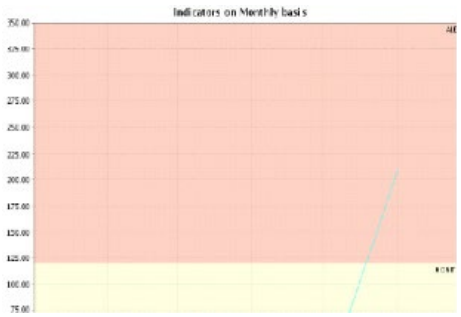
Key Risk Indicator	Description & Format	Thresholds
Non-Availanility Core Banking in minutes	Shows the total number of minutes of downtime per month for core banking system - unexpected downtime (format: number)	< 30 green
		30 - 12 yellow
		> 120 red
Solved finding (Penetration Test) / All Findings	Number of fixed / closed critical findings from last penetration test in respect to number of total critical findings (format: percentage)	> 80% green
		80 - 50% yellow
		< 50% red
Nr. of employees with security training within last 24 months / total number of employees	Number of employees who participated in at least one security awareness training within the last 24 months (either web-based training or physical training) (format: percentage)	> 80% green
		80 - 50% yellow
		< 50 % red

OBR. 4 – DEFINÍCIA KRI V BANKE – PRÍKLAD

Pravidelné vyhodnocovanie KRI umožňuje zamerať včas pozornosť na opakujúce sa hrozby a prijať adekvátne (aj IT relevantné) opatrenia na ich minimalizáciu.

Pripravil **Miroslav Molnár,** CGEIT

Non-Availanility Core Banking in minutes

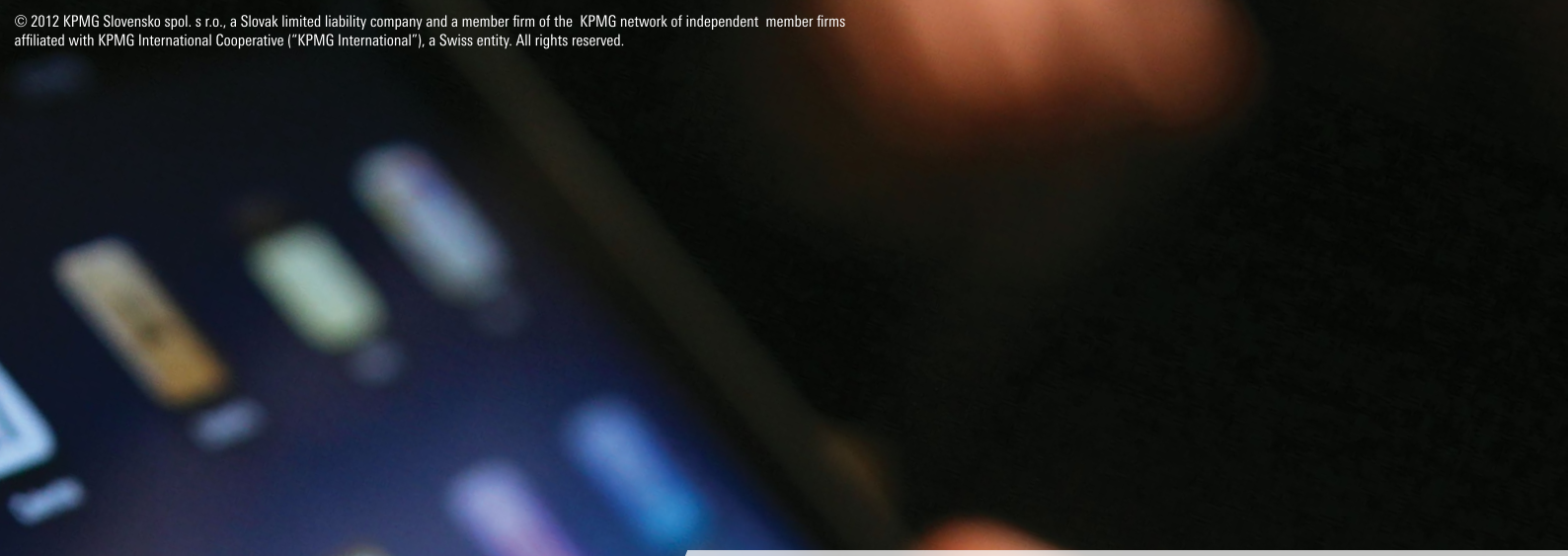


Solved finding (Penetration Test) / All Findings

Nr. of employees with security training within last 24 months / total number of employees

OBR. 5 – PRÍKLAD VYHODNOTENIE KRI

FOTOGRAFIE VÝROČNÁ X. KONFERENCIA ABIT (2011)



Sú Vaše dáta dostatočne zabezpečené?

Opýtajte sa nás!

- Riadenie informačnej bezpečnosti - stratégia, riadenie rizík, organizácia, bezpečnostná politika a procedúry
- Audit IT a informačnej bezpečnosti
- Ochrana osobných údajov a súkromia
- Riadenie kontinuity podnikateľských činností, krízové riadenie a havarijné plánovanie
- Technická bezpečnosť IT – penetračné testy, bezpečnostné previerky konfigurácie, aplikačná bezpečnosť
- Správa používateľov a prístupov
- Poradenstvo a audit v oblasti PKI a elektronického podpisu

Rudolf Sedmina, Partner, rsedmina@kpmg.sk
Erik Saller, Manažér, esaller@kpmg.sk
Michal Bubák, Manažér, mbubak@kpmg.sk

KPMG na Slovensku, Dvořákovo nábrežie 10, 811 02 Bratislava

KPMG
cutting through complexity™

Ing. Kristína Lachová
CISA

„Celý život som sa venovala počítačom. Fascinuje ma, čo sa dosiahlo za tie roky na technologickom poli.“

Aká je Vaša úloha a úloha interného auditu IT v NBS?
Mám na starosti interný audit IT a operačný audit, čiže všetko, čo sa týka procesov vo vnútri banky. V rámci NBS spolupracujeme s ostatnými centrálnymi bankami EÚ. Vykonávame s nimi spoločné audity. Našou prioritou tohto a budúceho obdobia je zjednotiť metodiku hodnotenia rizík IT, auditov v rámci Európskeho systému centrálnych bánk (ESCB).
Interné audity realizujeme na základe plánu schváleného Bankovou radou NBS, kde sú zahrnuté aj audity spoločne koordinované v rámci ESCB. To znamená, že vo všetkých centrálnych bankách EU sa v rovnakom čase, podľa rovnakého programu vykoná rovnaký audit. Z výsledkov týchto dvadsiatich siedmych auditov Výbor interných audítorov, ktorého som členkou, vypracuje spoločnú správu. Okrem toho sa zapájame aj do úzkych pracovných skupín, ktoré riadia konkrétne audity, osobne pôsobím v „taskforce“ pre audity IT.

„Na práci audítora IT je najťažšie udržať si profesijný background.“

Ako by ste zhodnotili úroveň riadenia IT v jednotlivých centrálnych bankách, existujú v niektorých štátoch výraznejšie rozdiely? Alebo je už tento stav vyrovnaný?

Ing. Kristína Lachová
CISA

Pani Ing. Kristína Lachová, CISA pôsobí v Národnej banke Slovenska ako vedúca operačného a IT auditu. Vyštudovala elektrotechnickú fakultu, začínala pracovať ako programátor, vývojár a administrátor. Sama o sebe hovorí: „Celý život som sa venovala počítačom. Fascinuje ma, čo sa dosiahlo za tie roky na technologickom poli. Ale zároveň som smutná, že všetky Orwellove čierne predtuchy o budúcnosti sveta boli už dávno prekročené. Preto sa dnes radšej venujem pestovaniu paradajok (smiech).“

Dostať riadenie rizík a auditov IT na jednotnú úroveň je zdĺhavý proces, pretože centrálne banky hlavne vo väčších európskych štátoch majú dlhoročnú tradíciu a kultúru. Takže to vyžaduje ešte čas. Za týmto účelom sa robia viaceré praktické kroky. Napríklad Výbor interných audítorov ESCB podporuje výmenu audítorov v jednotlivých krajinách EÚ. To znamená, že audítor z jednej centrálnej banky je zapojený do auditu inej centrálnej banky a je priamym členom tímu audítorov. Aj v tomto čase je kolegyňa z operačného auditu na obdobnom audite v inej centrálnej banke.

Vykonávate audity IT aj v komerčných bankách na Slovensku?
Nie, dohliadku komerčných bánk na mieste alebo na diaľku vykonáva Bankový dohľad Národnej banky Slovenska. Náš odbor však audítuje činnosť aj Bankového dohľadu NBS.

Ako vyzerá Váš bežný pracovný deň?
Najskôr si urobím prehľad, čo ma v daný deň čaká, aké mám stretnutia, porady a telekonferencie, ktoré využívame predovšetkým v rámci ESCB. Následne si pozriem najbližšie termíny viac či menej urgentných úloh, čo je v pošte, z ktorej prichádzajú ďalšie úlohy. Veľa času venujem rozhovorom s jednotlivými tímami audítorov, aby som sa informovala, čo preverili, s akými zisteniami a problémami sa stretli, napriek tomu, že elektronicky dokumentujeme stav uskutočnených auditov. Keďže som zapojená do pracovných skupín, ktoré riadia IT audity v rámci ESCB, musím preštudovať veľké množstvo dokumentov, písať správy atď. Často sa stáva, špeciálne v piatok, že si na konci dňa spisujem zoznam úloh, ktoré musím urobiť ešte cez víkend, hlavne, keď ma čaká služobná cesta, ako je meeting vo Frankfurte a pod.

Aké veľké je Vaše oddelenie?
Moje oddelenie má okrem mňa 6 ľudí. Spolu so mnou sa oblasti IT auditu venujeme štyria a traja sú skôr procesne zameraní, nakoľko audítujeme všetky interné procesy banky od prípravy finančnej analýzy trhu po prevoz hotovosti, prevádzku trezorov a pod.

Dá sa povedať, že mávate pravidelné obdobia väčšieho náporu práce?
Tradične býva náročný každý koniec roka, nápor začína už v septembri. Tento rok boli vyčerpávajúce aj letné

prázdniny, nakoľko sme finalizovali niekoľko ESCB auditov. Napriek tomu, že som vedúca, jeden z nich som aj priamo vykonávala. Bol zameraný na technológie sietí v rámci ESCB - IT network operation and security. Mám však pocit, že nápor spolu s novými úlohami stále narastá.

Čo je podľa Vás na práci audítora IT najťažšie?
„Na práci audítora IT je najťažšie udržať si profesijný background." Oblasť IT sa rozvíja obrovským tempom asi ako žiadna iná. Členov do svojho tímu audítorov IT som vyberala aj podľa toho, či majú dlhoročné skúsenosti priamo so správou IT, aby rozumeli problematike a vedeli posúdiť, kde sa v skutočnosti riziká IT nachádzajú. Audítor má časom nevýhodu, že stratí priamy kontakt s informačnými systémami a je pre neho veľmi náročné udržať sa na požadovanej odbornej úrovni.

Kde čerpáte odborné vedomosti zo sveta IT bezpečnosti Vy?
Internet je dnes nekonečná studnica informácií. Zúčastňujeme sa tiež vzdelávacích aktivít Výboru interných audítorov ESCB. Iná možnosť ako vzdelávať sa tu nie je. V niektorých európskych bankách je nastavený mechanizmus točenia ľudí z audítorskej pozície na výkonnú a naopak. Myslím si, že je to výborný spôsob, ako získať skúsenosť s prevádzkou IT, poznať reálne ich problémy, na druhej strane aj vedieť posúdiť, na čo sa audítor zameriava.
„Snažím sa, aby moji audítori boli veľkorysí v maličkostiach a neúprosní vo veľkých veciach."

Cieľom overenia bezpečnosti IS banky je okrem iného poskytnúť primeranú istotu, či bankou spracúvané a uchovávané údaje sú PRIMERANE zabezpečené pred ich zneužitím. Podľa akej metodiky určujete túto mieru primeranosti?
Sú to predovšetkým ISO štandardy, Cobit a niektoré ďalšie. V rámci ESCB bola implementovaná vlastná metodika IRM (Information Risk Management) na riadenie rizík IT vychádzajúca z noriem radu ISO 27000, ktorá je prispôsobená organizácii, zvyklostiam a kultúre ESCB.

Má NBS na riadenie IT rizík implementovanú metodiku RiskIT?
Nie, našou snahou je implementovať predovšetkým spomínanú internú metodiku IRM, nakoľko vznikla v rámci ESCB skôr ako RiskIT. Metodika zahŕňa a tlačí celý realistický životný cyklus posudzovania rizík IT. Detailne sa zaoberá úlohu vlastníka biznisu a jeho rozhodovacími právomocami. Jednotlivé „control objectives" sú rozpracované na konkrétne opatrenia a ich váhu, rozhodujúcu na ich zavedenie a riešenie daného druhu problému a elimináciu rizika. Metodika tak vedie až k úplným a detailným opatreniam vhodným pre konkrétne situácie, aplikácie, systémy a projekty. Zároveň jednoznačne stanovuje základné požiadavky na bezpečnosť IT v závislosti od kritickosti systému. Tie posudzuje vlastník daného biznisu a stanovuje požiadavky na dostupnosť, dôvernosť a integritu. Na metodike IRM vyzdvihujem aj jej praktickosť a biznis pohľad na IT riziká.

„Snažím sa, aby moji audítori boli veľkorysí v maličkostiach a neúprosní vo veľkých veciach."

Je táto metodika verejne dostupná?
Ide o internú metodiku, ale myslím si, že bola vydaná brožúra, s popisom jej obsahu, ktorá by mala byť dostupná na webstránke ECB, nie však v plnom rozsahu. Účastníci konferencie ABIT v r. 2011 sa s ňou mohli oboznámiť na prezentácii šéfa auditu IT z Európskej centrálnej banky.

S akými najčastejšími druhmi problémov zápasia banky pri zabezpečení prevádzky IT?
Niektoré problémy centrálnych bánk sú vyvolané veľmi rýchlym nástupom technológií, ktoré prinášajú používateľom okamžité benefity, ale sú nasadzované bez posúdenia ich rizík. Ako príklad uvediem problémy spôsobené nasadením virtualizácie do siete, ktorá bola pôvodne segmentovaná v závislosti od toho, aké dôležité systémy z pohľadu bezpečnosti v nej bežia. Virtualizáciou sa zrazu vytvoria prepojenia, ktoré znegujú celú bezpečnostnú segmentáciu. Virtualizácia síce prináša úžasne efektívne riešenia z pohľadu dostupnosti a nákladovosti na prevádzku IT, rýchle vytvorenie testovacích a vývojových prostredí, v ktorých sa ale neraz nachádzajú aj ostré dáta, a pri tom vytvára iný druh problémov. Niekedy nie je jasné, kde sa takéto dáta fyzicky nachádzajú, ako tečú, kto k nim má prístup a pod.

V ktorom roku ste získali certifikát CISA?
V roku 1998 v Prahe, nakoľko vtedy ešte ISACA Slovensko neorganizovala skúšky v Bratislave, ako tomu je dnes. Do banky som prišla pracovať v roku 1996 so zámerom rozbehnúť audit IT. Dostala som sa na medzinárodnú konferenciu ISACA, kde sa na mňa zástupcovia ISACA z ústredia doslova vrhli, aby som založila pobočku ISACA na Slovensku. To isté sa v rovnakom čase stalo nezávisle aj pánovi Borákovi, s ktorým sme následne založili ISACA Slovensko.

Čomu sa venujete vo voľnom čase?
Vo voľnom čase sa venujem záhradke a hudbe. Moje najobľúbenejšie kvety sú modré hortenzie, ktoré sa mi ale nedarí vypestovať, lebo potrebujú kyslú pôdu. V mojej záhrade na zásaditej pôde dostávajú nádych do ružova. Nepomáhajú ani dostupné hnojivá, účinkujú len krátkodobo.

Pani Lachovej srdečne ďakujem za príjemný rozhovor a ochotu podeliť sa so svojimi bohatými skúsenosťami. Zároveň jej želám mnoho úspechov v práci i v súkromí.

Zhovárala sa **Erika Slivová**

Osemsmerovka

E	V	A	L	U	A	T	I	O	N
S	E	V	E	R	I	T	Y	R	I
T	N	E	M	T	A	E	R	T	S
I	K	S	I	S	Y	L	A	N	A
M	I	T	I	G	A	T	I	O	N
A	A	M	H	A	Z	A	R	D	A
T	N	T	A	R	T	E	S	S	A
I	G	E	R	M	E	N	A	L	P
O	A	V	O	I	D	A	N	C	E
N	K	S	I	R	X	E	T	N	T

Vyškrtajte pojmy v 8 smeroch, zostávajúce písmená tvoria tajničku.

Virtuálna kancelária

Edit Babincová – Fridrichová
Office Manager

Mobile: +421 918 327 238
E-mail: *fridrichova@isaca.sk*

Kontaktujte kanceláriu v prípade, že ste člen ISACA a máte záujem o:

- Objednávanie študijných materiálov
- Registrovanie na skúšku alebo obnovu členstva

Volajte počas pracovných dní v čase od 8:00 – 18:00 hod.

Pred každým tlačením dokumentu myslite na životné prostredie.