ČESKÝ INSTITUT INTERNÍCH AUDITORŮ

The Institute of Internal Auditors

4 | 2013

# INTERNÍ AUDITOR

ROČNÍK 17, ČÍSLO 4–2013 (70)
ČTVRTLETNÍK ČESKÉHO INSTITUTU INTERNÍCH AUDITORŮ


## VOLAT S MOBILEM OD ČEZ JE JEDNODUCHÉ. NIC NESKRÝVÁ

Platíte jen to, co skutečně využijete. Tarif „Platím, jak volám“ je fér. Žádný povinný měsíční poplatek ani minimální útrata. Vybrat si můžete i balíčky, se kterými si cenu ještě snížíte, a v síti ČEZ dokonce voláte zcela zdarma. Pokud od nás máte elektřinu nebo plyn, získáte zdarma v síti ČEZ i SMS.

MOBIL

**www.cez.cz | Zákaznická linka 840 840 840**

JSME S VÁMI. SKUPINA ČEZ

## OBSAH



Vážené kolegyně, vážení kolegové v interním auditu,

rok 2013 vstoupil do našich hlav s novým konceptem pod hlavičkou „Interní audit 2.0", který nachází v řadách auditorů své nadšené příznivce i zavilé odpůrce.

Já osobně jsem k němu zpočátku přistupoval se značným despektem. Především proto, že snad až příliš posouval do popředí onu aktivní roli interního auditora při řízení doporučovaných změn, která ihned asociuje porušení standardů. A přitom se ucházel o podporu ČIIA, který je na jejich dodržování založen!

Protagonisté Interního auditu 2.0 však od samého počátku projevovali ochotu jeho koncept dále dopracovávat a zpřesňovat. S tím, že jeho nosnou myšlenkou je především zlepšení vlastního auditu, smysluplné zacílení jeho výstupů a zvýšení užitku pro firmu či organizaci. Tedy i zvýšení prestiže interního auditu u managementu. Zde byl soulad s posláním ČIIA zřejmý, ale zřejmé bylo i to, že institut hlásící se k IIA nemůže připustit odchýlení od standardů.

Důkladná konfrontace s přesnou dikcí standardů a doprovodných doporučení pro praxi ukázala, že i na takový „přešlap" pamatují. Nezapovídají, aby auditor převzal pověření mimo rámec interního auditu (a po dobu takového pověření přestal být auditorem), ale vymezují pravidla a restrikce, kterými se „návrat k řemeslu" auditora musí podřídit.

Podle mého názoru však propagátoři nového konceptu podcenili symboliku toho, že pod značkou „Interní audit 2.0" zastřešili i (byť jen minoritně prováděné) neauditní činnosti.

Po řadě diskuzí jsme nyní společně dospěli ke konsenzu, kterým je redefinice celého konceptu, s novým názvem „Interní audit 2.0+". Názvem, ve kterém část „verze 2.0" vyjadřuje právě jen novou kvalitu auditní činnosti, ale výhradně v mezích standardů. A pro ony „spanilé jízdy" do prostoru neauditních činností, neboť řízení auditorem doporučené změny již mezi auditní činnosti nepatří, je určeno znaménko plus. Jako něco navíc, co tam být může, ale nemusí.

Přál bych si, aby takto redefinovaný koncept „Interního auditu 2.0" přijali za svůj i zastánci striktního udržení činnosti auditorů v mezích standardů jako první stupínek nové kvality. S tím, že pro ty útvary interního auditu, od kterých je vyžadováno více než samotný standardní audit, je určen klon „Interní audit 2.0+".

*Petr Vobořil*
*Prezident ČIIA*

**TÉMATA PRO ROK 2013**

1/2013 NOVÉ FORMY PODVODŮ A JAK NA NĚ

2/2013 BENCHMARKING

3/2013 TRESTNÍ ODPOVĚDNOST PRÁVNICKÝCH OSOB A VÝZVY PRO INTERNÍ AUDIT

INTERNÍ AUDIT A MODERNÍ KOMUNIKAČNÍ TECHNOLOGIE



**Vydává**
Český institut interních auditorů, o.s.
Karlovo nám. 3
120 00 Praha 2
tel.: +420 224 920 332
+420 224 919 361
e-mail: ciia@interniaudit.cz
www.interniaudit.cz

**Redakce INTERNÍ AUDITOR**
Karlovo nám. 3
120 00 Praha 2
Registrace: MK-ČR-E-12322
ISSN 1213-8274

**Redakční rada:**
Vedoucí – Jan Kovalčík, Petr Cerman, Petr Hadrava, Daniel Häusler, Šárka Nováková, Andrea Káňová, Pavla Kostřibová, Petra Škvorová, Kateřina Zonygová

Ilustrace: Jitka Holečková
Foto: archiv ČIIA
Neprodejné, určeno pro Český institut interních auditorů
Náklad: 1 200 výtisků
Pre-press: Viktor Beránek
Tisk: Reproservis, s. r. o.
Distribuce: A.L.L. production, s.r.o.

Ing. Luboš Klečka, CISA,
ředitel odboru audit IT,
Česká spořitelna, a.s.

*Ve svém profesionálním životě se zaměřil na oblast bezpečnosti informačních technologií. Podílel se na realizaci a rozvoji infrastruktury veřejných klíčů, řešil architekturu bezpečnosti přímých distribučních kanálů, působil jako konzultant bezpečnosti IT v rámci projektových aktivit. V současné době je zodpovědný za IT audit v České spořitelně. Podílel se na založení české pobočky organizace ISACA a je členem jejího výboru.*

# AUDIT INFORMAČNÍCH TECHNOLOGIÍ

Potřeba auditu informačních technologií narůstá s rozměrem implementace nových technologií. Organizace si váží informací ukládaných ve svých datech, vnímají je jako konkurenční výhodu a z hlediska ochrany dat jako cenné vlastnictví. Jako k takovému přistupují i k jejich ochraně a zabezpečení. V současné době narůstá potřeba chránit firemní data i v prostředí, jejichž boom nastal v souvislosti s dostupností mobilních technologií – „chytré" telefony, tablety, přenosná média, fotoaparáty, paměťové karty, moderní komunikační technologie (bluetooth, wi-fi). Využívání přináší do organizace nové a nezanedbatelné riziko zneužití dat.

***Motto:*** *Musíš se mnoho učit, abys poznal, že málo víš.*

Z hlediska interního auditu a odborné veřejnosti nemá asi smysl popisovat, co slovo audit znamená a jaký je jeho význam. Jistě se objevily i odborné statě v tomto časopisu, jak auditorské řemeslo vzniklo a jaké kroky učinilo do současnosti. Vzhledem k tématu bych přece jenom připomněl, jakou roli ve vnímání auditu má audit informačních technologií a jak profese IT auditu vznikala.


Z obrázku je zřejmé, jak dlouhý časový úsek před vznikem zmíněné profese musel proběhnout, než byla profese IT audit „akceptována". Od první zmínky auditorského řemesla spojené s panováním krále Daria (pro opakování – ve starověké Persii si počínal velice obratně v získávání informací o stavu společnosti a jejich následném vyhodnocování). Pravděpodobně se interní auditoři k tomuto datu hlásí jako k historickému mezníku vzniku prvních kroků spojených s auditorskou činností. (Starověká Persie 522 před n. l., „Eyes and Ears of the King")

Praktický zrod auditu IT je spojen s rokem 1968, kdy Americký institut certifikovaných účetních definoval tzv. EDP (electronic data processing) standard.

Souvislosti vytvoření takového standardu jsou zřejmé – hromadně se zavádějí prostředky výpočetní techniky, datová centra zpracovávají obrovské množství dat, roste rozsah ukládaných informací na paměťová média. Realizují se audity, které řeší problematiku komplexně, včetně informačních technologií. Plánují se rovněž specializované audity, vytvářejí se auditní týmy, které se zaměřují na zpracování dat, ověřování způsobilosti výpočetní techniky, ověřování správnosti finančních výkazů a dalších pomocných sestav sloužících k řízení firem. Ukazuje se potřeba zapojit do auditních týmů specialisty se znalostí informačních technologií, ukládání dat, ověřování přístupu k datům.

Postupem času se problematikou IT začínají zabývat profesní organizace, které ve svých standardech řeší i informační technologie, např. COSO (The **Committee of Sponsoring Organizations** of the Treadway Commission), ISACA (Information Systems Audit and Control Association), nyní mezinárodní profesní organizace zaměřená na IT Governance. Jako ambasador organizace ISACA, která je již zavedena v podvědomí specialistů řešících problematiku IT, auditu IT, bezpečnosti IT, managementu a governance IT, budu ve svých argumentacích vycházet z jejich zdrojů.

Definice auditu informačních technologií je uvedena zde:

*I když Wikipedie nemusí být vždy považována za seriózní zdroj, přece jenom není od věci pojetí auditu IT zmínit. Je chápán jako druh auditu, jehož cílem je zkoumání kontrolních mechanizmů uvnitř infrastruktury informačních technologií.*

ISACA převzala a doplnila definici od R. Webera, který audit IT charakterizuje jako proces sběru a hodnocení fakt k určení, zda počítačový systém (informační systém) chrání prostředky (aktiva), udržuje integritu dat, je efektivní s účinným využitím dostupných zdrojů.[1]

Účelem auditu IT je zhodnotit danou oblast a poskytnout vedení firmy zpětnou vazbu, ujištění a další náměty ke zlepšení. Setkáváme se zavedenými pojmy z hlediska bezpečnosti IT:

- dostupnost
- integrita
- důvěrnost

Zmíněné kategorie patří ke třem základním oblastem práce týmů zajišťujících audit a bezpečnost informačních systémů.

I z toho důvodu je činnost IT auditu úzce propojena s ověřováním bezpečnosti IT a spoluprací se specialisty bezpečnosti informačních technologií – oba subjekty mají společný cíl – nastavit kontrolní mechanizmy informačních technologií s cílem snížení, minimalizace či vyhnutí se bezpečnostnímu riziku.

1 Weber, Ron, EDP Auditing—Conceptual Foundations and Practise

## ZAMĚŘENÍ AUDITU IT

IT auditor, někde specialista auditu pro informační technologie, je součást auditního týmu. Odpovídá za ověřování kontrolních mechanizmů, které ovlivňují rizika související s informačními technologiemi, resp. informačními systémy. Nejde jenom o detailní ověřování kontrolních mechanizmů technického a programového vybavení, ale i procesního řízení, pravidel a procedur vytvořených v organizaci, majících vliv na zpracování a ochranu dat.

Činnost IT auditora může být plánovaná, z hlediska např. ročních plánů, nebo může být realizovaná na vyžádání – to když klient vyžaduje uskutečnit ověření nějaké skutečnosti, o které se domnívá, že postrádá kontrolní mechanizmy, resp. kontrolní mechanizmy již nejsou, například rozvojem či aktualizací systému, funkční.

Z hlediska plánovaných auditů jde v drtivé většině o audity, jejichž cílem je ověřovat rizika, která jsou významná a která si zaslouží pozornost managementu firmy. Velikost rizika lze stanovit různými způsoby, dvě varianty jsou uvedeny zde:

*V některých společnostech se využívá vyhodnocení rizika formou kalkulace ztráty, kombinace inherentního a reziduálního rizika, někde se používají hodnocení, která používají vyčíslení rizika, například na pětiúrovňové stupnici – od bezvýznamného po závažné na stupnici rizik.*

## PROČ ROSTE ÚLOHA AUDITU IT V SOUČASNOSTI?

Rozvoj mobilních technologií s sebou přináší schopnosti doposud nepoznané. Data je možné uložit např. na karty fotoaparátů, do mobilních telefonů, na přenosné disky, je možné je jednoduše odeslat do technologií, které s sebou přináší cloud řešení, velice rychle zaslat prostřednictvím nových a rychlých komunikačních technologií.

Na jedné straně tyto technologie mohou být velice užitečné a mohou přinést rozvoj obchodních záměrů, umožní rychle a bezbolestně reagovat na potřeby trhu. Na straně druhé může být tento rozvoj zpomalen opatřením z bezpečnostní politiky firmy. Skupina zaměstnanců, odpovědná za bezpečnost a ochranu dat, může mít jiný názor. Připraví pravidla, zavede nové procedury, které mohou tzv. otevřenost mobilních zařízení. Tato chytrá mobilní zařízení mají již implementovány mechanizmy přístupu k internetu, komunikační technologie, z hlediska uživatele se jedná jenom o to, jaké použije;

- uživatelé mohou k přístupu k informacím využívat i vlastní technologie. Roste gramotnost uživatelů, pro firmu může být přínosné, aby zaměstnanci byli více spokojeni s nástroji, které k přístupu používají.

Role bezpečnosti IT a auditorů IT s tímto trendem musí růst. Specialisté zodpovědní za ochranu dat nemohou lpět na zavedeném přístupu tzv. interních perimetrů, kdy je vše pod jejich kontrolou a monitorováním. Měli by vnímat současný rozvoj a hledat řešení, které umožní efektivní ochranu dat. Nejenom technologickým způsobem – využitím moderních komunikačních technologií, které mohou přispět k ochraně dat. Mnohem důležitějším bude organizační a procedurální způsob:

- příprava zaměstnanců na nové technologie a jejich možnosti;
- předání informací o bezpečném používání mobilních technologií.

Ve spolupráci bezpečnosti IT a IT specialistů se musí hledat efektivní řešení, aby se možnosti realizace obchodních požadavků daly splnit co nejlépe. Efektivně, se zaměřením na obchodní cíle firmy.

## A ROLE AUDITU IT?

Nebojme se přiznat, že role auditora IT roste. V průběhu rychlosti zavádění změn, jejich implementací, musí být management firmy informován, zda jsou, či nikoliv, rizika pod kontrolou. Tuto roli musí sehrát auditor, který je obeznámen s kroky, které firma činí, a objektivně zhodnotí úroveň zajištění obchodních cílů a kroky spojené s ochranou a přístupem k datům.

K tomuto účelu mohou sloužit i informace, které přináší zmíněné organizace. V případě cloud řešení se jedná převážně o:

- Cloud Governance: Questions Boards of Directors Need to Ask;
- Security Considerations for Cloud Computing;
- Guiding Principles for Cloud Computing Adoption and Use.

## „Rozvoj mobilních technologií s sebou přináší schopnosti doposud nepoznané“

Navážu na rozhovor s panem Dohnalem o cloud řešení. Implementace cloud řešení s sebou přináší nová rizika a zároveň šance, jak tyto technologie využít ke snížení rizik jiných. Nemíním popisovat typy cloud řešení. Tyto popisy a pomůcky z hlediska infrastruktury, bezpečnosti, způsobů manipulace s daty jsou hojně vydávány v různých publikacích a rovněž technické články jsou dostupné na internetu.

V současné době lze konstatovat, že značná část malých a středních podniků uvažuje o zavedení cloud řešení nebo k němu již přešla. Důvody jsou zřejmé:

- nemusí se starat o interní infrastrukturu, pouze o propojení na internet;
- data jsou dostupná kdekoliv a kdykoliv;
- provoz je efektivnější;
- rozšiřují se možnosti z hlediska

Lze využít i normy ISO:

- ISO/IEC 27017 Information Security Controls for Cloud Services;
- ISO/IEC 27036-4 Guidelines for Security of Cloud Services.

Posledně jmenovaný dokument je výborné východisko pro provedení analýzy rizik a nastínění dalších kroků pro případnou implementaci cloud řešení. V každém případě seznámení se s jedním dokumentem nepostačuje

## „Implementace cloud řešení s sebou přináší nová rizika a zároveň šance“

Popřípadě výsledky výzkumu NIST (National Institute of Standards and Technology):

- Cloud Computing;
- NIST Cloud Computing Security Reference Architecture;
- URL adresu NIST Cloud Computing Program (http://www.nist.gov/itl/cloud/).

Vyznat se v džungli předpisů není snadné. Když k tomu přidáme předpisy Evropské unie, resp. ENISA (European Union Agency for Network and Information Security), a její Cloud Computing Risk Assesment, máme čtení na hodně dlouhou dobu.

k úplnému zvládnutí problematiky cloud. Při provádění přípravných kroků by auditoři měli vnímat ochranu dat jako prvořadý směr dalšího postupu. Upozorní na nedostatky a mohou doporučit další kroky.

Většina organizací si vytvořila i z hlediska zákonů České republiky vlastní předpis, který řeší, jaká data organizace vlastní, uchovává, vytváří nebo s nimi manipuluje a jak se s těmito daty má nakládat – často známý dokument „Klasifikace dat“. V průběhu analýzy je nutné zvažovat rizika spojena:

- s přechodem a zasíláním dat do cloud řešení;
- s přístupem z různých typů zařízení k datům;
- se způsoby ukládání dat do cloud řešení;
- s typy zařízení, která mohou k datům přistupovat, resp. je sdílet (mobilní telefony, tablety, tiskárny apod.).

Firmy na některá rizika, která přicházejí z auditních zpráv, mohou reagovat aktivitami, které omezí přítomnost určitého typu dat v cloud řešení, případně definují, jak se s daty v cloud řešení má nakládat. To vše vyžaduje součinnost zaměstnanců a jejich motivovanost přejít na cloud řešení s vědomím, že vnímají, jaká manipulace s daty je povolena a jaká ne. Rozdíly mezi firmami a jednotlivci se mohou začít stírat, výpočetní středisko může být vnímáno stejně jako osobní počítač. Data tedy budou dostupná všem, je však žádoucí připravit s přechodem na cloud řešení i firemní kulturu.

### ZÁVĚR

Vždy se vyplatí důkladné přípravné kroky, které plní roli preventivních opatření, což jak všichni víme, je nejlevnější řešení. Pozdější detekce problémů, případně jejich oprava si vyžadují dodatečné náklady, které nemusí být brány pozitivně a celé řešení prodraží.

Ing. Pavel Závitkovský, CIA
Partner, Audit,
KPMG v České republice

Ing. Miroslav Šíp, CISA, CRISC
Senior Consultant, Risk Consulting,
KPMG v České republice

# ZABEZPEČENÍ FIREMNÍCH DAT NA MOBILNÍCH ZAŘÍZENÍCH

Vývoj informačních a komunikačních technologií jde nezadržitelně vpřed a pryč je doba, kdy používání notebooku místo stolního počítače bylo považováno za nadstandard. Nemáte-li v dnešní době tablet, chytrý telefon nebo alespoň netbook, stojíte mimo hlavní proud. Většina společností se tomuto trendu přizpůsobuje tím, že pro své zaměstnance vybírá moderní firemní zařízení, ale i tím, že jim nabízí možnost využívat soukromá zařízení pro firemní účely (tzv. BYOD – bring your own device). Ne všechny společnosti a jejich IT manažeři si však uvědomují rizika, která jsou s používáním těchto zařízení spojena, a nutnost zabezpečení stejně jako jakéhokoli jiného zařízení ve firemní síti.

Společnosti používání takovýchto zařízení umožňují také proto, že jim i zaměstnancům přinášejí několik výhod, především:

- zvýšenou produktivitu práce díky možnosti pracovat off-site mimo prostory společnosti;
- lepší zákaznický servis díky možnosti mít vždy a všude aktuální informace o zákaznících, objednávkách atp.;
- zkrácení reakčního času při komunikaci se zákazníky, řešení problémů či stížností – důsledkem je lepší vnímání společnosti ze strany zákazníků;
- propojení soukromého a pracovního života, a tím zlepšení nálady a spokojenosti zaměstnanců.

Rozhodne-li se společnost zpřístupnit firemní data a e-mail v mobilních zařízeních, měla by si uvědomit rizika, která to s sebou nese. Nejlépe k tomu poslouží aktualizace celkové analýzy rizik. Výsledkem bude nejen uvědomění si rizik, ale také ohodnocení jejich výše a důležitosti pro společnost. Hlavními kategoriemi rizik, kterým společnosti čelí, jsou:

- ztráta nebo krádež zařízení vedoucí k úniku citlivých firemních dat;
- možnost instalace aplikací i z nedůvěryhodných zdrojů, která vede ke ztrátě kontroly nad zařízením, třeba kvůli možnému odposlechnutí hesel apod.;
- zavedení škodlivého softwaru či malwaru, který může způsobit vznik bezpečnostních děr, jež umožní hackerovi proniknout do zařízení;
- neomezený přístup k firemním datům a možnost obejít standardní bezpečnostní opatření bránící úniku citlivých dat;
- připojení na nezabezpečenou bezdrátovou síť.

Jsou-li mobilní zařízení soukromým majetkem, který často využívá nejen zaměstnanec společnosti, ale i jeho rodina, musí IT manažeři najít vhodný způsob, jak tato zařízení ochránit a zároveň umožnit jejich používání pro soukromé účely. Existuje k tomu několik opatření, které je třeba zkombinovat a jejichž existenci a efektivnost by měl pravidelně vyhodnocovat interní audit.

### 1. Kvalitní směrnice pro používání mobilních zařízení

Směrnice by měla vycházet ze standardních pravidel pro přístup k firemním datům a být doplněna o pravidla pro nové technologie, jako jsou chytré telefony a tablety. Musí se vztahovat na všechny hardwarové a softwarové prostředky, které mají přístup k podnikovým datům. Je také potřeba ji pravidelně, nejméně jednou ročně aktualizovat, aby odrážela nejnovější technologický vývoj a hrozby.

### 2. Školení zaměstnanců a udržování povědomí o bezpečnosti

Nastavení vztahu se zaměstnancem, zejména při možnosti BYOD, je velmi důležitý, ale často podceňovaný prvek řízení bezpečnosti mobilních zařízení. Než společnost schválí přístup k firemním datům, měla by uzavřít písemnou dohodu, která bude obsahovat minimálně:

- důvod, proč je potřeba připojit zařízení do firemní sítě;
- identifikaci zařízení, včetně používaného operačního systému;
- podmínky centrální správy zařízení;
- zákaz synchronizace s dalšími zařízeními a sítěmi;
- postup v případě ztráty zařízení;
- prohlášení o dodržování stanovených postupů;
- postupy a postihy v případě porušení dohody.

Při dlouhodobém používání by společnost měla u zaměstnanců pravidelně udržovat povědomí o bezpečnosti, provádět školení a průběžně připomínat, co je v rámci využívání zakázáno.

## ANKETA ČIIA

OTÁZKY

**INTERNÍ AUDIT A MODERNÍ KOMUNIKAČNÍ TECHNOLOGIE**

**1. Co vše chápete pod pojmem moderní komunikační technologie?**

**2. Jaké moderní komunikační technologie využíváte při své práci?**

**3. Na co se v budoucnu musí, dle Vašeho názoru, interní audit nejvíce zaměřit při využívání a auditu komunikačních technologií? Kde v současnosti vidíte největší rizika v této oblasti?**

**Jiří Linek**

**Středočeský kraj**
**vedoucí Odboru interního auditu a kontroly**

1. Moderní komunikační technologie jsou nástroje, které by měly přispívat k tomu, že naše činnost bude efektivnější, účelnější a hospodárnější. Domnívám se, že jak svět, tak interní audit spěje stále ve větší míře k používání moderních technologií. Snahou je a bude komunikovat elektronicky, nikoliv papírovou formou, jejíž význam postupně klesá. Ruku v ruce s tím je třeba se zabývat otázkou informační a komunikační bezpečnosti. Informace, a to i ta šířená digitálně, se stává cenným zbožím, a proto je třeba k ní tak přistupovat a chránit komunikační kanály, kterými proudí.

2. Odbor interního auditu a kontroly Středočeského kraje má snahu transformovat současný systém oběhu dokumentů z papírového na digitální formu. V současné době probíhá na půdě krajského úřadu projekt, jehož smyslem je integrovat používané a značně diverzifikované softwarové produkty do společného prostředí. Funguje např. elektronický oběh účetních dokladů, které již nekolují v listinné podobě, ale elektronicky, přičemž je zajištěna elektronická řídicí kontrola těchto účetních dokladů. Kromě toho využíváme standardních komunikačních technologií – telefon,

mobilní telefon, internet, intranet, videokonference atd.

3. Jak jsem již výše uvedl, informace jsou velice cenné zboží a je třeba je chránit. Musí být zajištěna informační a komunikační bezpečnost, nastavena bezpečnostní politika korporací tak, aby bylo minimalizováno riziko zneužití informace, krádeže informací či ztráty informace.

**Jaroslav Barnáš**
**interní auditor**
**OKIN GROUP, a.s.**

1. ERP, internet, intranet, el. fakturace, el. oběh dokladů, el. pošta, Skype, videokonference, Facebook, mms, sms...

2. ERP, internet, intranet, portál, Skype, videokonference...

3. Projektová a změnová řízení, integrace dat, bezpečnost informací, aktuálně na implementaci změn daných rekodifikací k 1. 1. 2014. K rizikům: technokratizmus – z prostředku podpory účel – odtržení od hlavních procesů, mnoho kapacity nadprodukci nevyužitých detailních informací na úkor podstatných, nedostatečná bezpečnost informací, nadměrná závislost na poskytovatelích SW podpory...

**Petr Vobořil**
**ředitel interního auditu**
**ČEZ, a.s.**

1. Vše, co mi dovolí odkudkoli: pracovat s daty, jako bych seděl ve své kanceláři, anebo diskutovat s partnery, jako bych s nimi seděl ve stejné místnosti. A neřešit hardware.

2. Vše, co uvádím v prvé odpovědi, s částečným omezením videokonferencí/videotelefonů (diskuze se vzdálenými partnery) na firemní prostory.

3. Základním rizikem, tedy i tématem pro interní audit, je bezpečnost takové komunikace. V praxi je často opomíjena, přestože obvykle firemní standardy nějaké prostředky nabízejí, nejsou využívány (i proto, že chybí osvěta).

**Ing. Dana Vojíková, MBA**

**senior auditor,**
**interní auditor expert ve VS,**
**Magistrát města Plzně**

1. Za moderní komunikační technologie považujeme v prvé řadě různé nástroje internetu (vyhledávače, e-mail, sociální sítě, apod.) a mobilní telekomunikační sítě. V případě pohledu z úhlu komunikačních zařízení by se zde řadily mobilní telefony, smartphony, tablety, síťové skenery, tiskárny a tak dále.

### 3. Centrální správa mobilních zařízení

Lidé mají tendenci zapomínat a předcházející opatření mají charakter „pouhých" nařízení či pokynů, takže je bezpodmínečně nutné mít nástroj, jehož pomocí může společnost v případě potřeby vzdáleně zasáhnout nebo alespoň zkontrolovat aktuální nastavení přístroje. Tyto nástroje slouží také k informování uživatele o nesouladu se stanovenými pravidly a k nápravě zjištěných odchylek.

Existují dvě hlavní skupiny nástrojů, které tyto požadavky splňují:

- MDM (Mobile Device Management) – robustnější řešení pro větší společnosti nebo firmy s velkým počtem zařízení. Umožňují vzdáleně spravovat dané zařízení, měnit nastavení, upravovat či mazat data v zařízení apod. Tyto nástroje jsou vhodné především pro správu vlastních zařízení společnosti.
- MDA (Mobile Device Audit) – nástroje, které informují o aktuálním nastavení, ale nemají plnou správu nad zařízením. Jsou vhodné pro menší společnosti a BYOD, jelikož je majitelé díky zachování soukromí vnímají lépe.

### 4. Řízení přístupu k firemním datům

Pro správu mobilního zařízení je důležité oddělit privátní data od firemních dat „bez hodnoty" a od firemních dat, která jsou pro společnost citlivá. Existuje několik způsobů, jak tyto skupiny dat odlišit, včetně použití tzv. sandboxu (bezpečnostního mechanizmu, který slouží pro oddělování dat a procesů běžících se stejným oprávněním) pro data či aplikace. Samozřejmou součástí snahy o ochranu dat je šifrování firemních dat na mobilních zařízeních.

Z pohledu monitoringu je v první řadě nutné mít v každém okamžiku přehled, kdo má přístup k firemním datům, které účty mají přístup pouze k firemnímu e-mailu, které mohou přistupovat do firemní sítě pomocí VPN, zda jsou tyto účty přiřazeny zaměstnancům či třetím stranám apod.

### 5. Nastavení základních bezpečnostních prvků

Existuje celá řada bezpečnostních prvků, jejichž nastavení je velice snadné a které oproti implementaci nástrojů MDM/MDA nepředstavují žádné nebo představují jen minimální náklady. Jedná se především o:

- používání zámku obrazovky – jde o základní nastavení každého mobilního zařízení, které ztíží možnost úniku dat nejen při ztrátě zařízení, ale i v případě jeho odložení z dohledu; výběr konkrétního mechanizmu zamykání není klíčový, je pouze potřeba zvážit nevýhody jednotlivých řešení (např. zanechání stopy gesta na dotykovém displeji),
- používání silných hesel pro přístup k firemním datům – další jednoduché, účinné opatření zvyšující zabezpečení, které naráží pouze na omezení uživatelské přívětivosti,
- udržování operačního systému vždy v aktuálním stavu – jak se používání operačních systémů rozšiřuje, i hackeři se učí překonávat slabá místa, a tak je důležité využívat vylepšená zabezpečení, která v sobě nové verze operačních systémů nesou,
- zákaz instalace aplikací z nedůvěryhodných zdrojů – ty mohou zařízení zanést škodlivým softwarem; samozřejmostí je zákaz provedení tzv. jailbreaku neboli prolomení uzavřeného operačního systému, které umožňuje instalovat neoficiální aplikace nebo upravovat systémové soubory,
- zákaz přesměrování,
- zákaz používání otevřených bezdrátových sítí, na kterých je zvýšené riziko odposlechnutí přenášených dat.

### 6. Zálohování dat a řízení bezpečnostních incidentů

I v případě, že jsou nastavena pravidla hry a riziko se snížilo na přijatelnou hodnotu, je vždy vhodné mít připravený havarijní plán. Nejčastější havárií je ztráta nebo krádež mobilního zařízení, instalace škodlivého softwaru, případně napadení hackerem. Havarijní plán by měl být schválen vedením společnosti a měl by obsahovat minimálně informace o tom,

- kdo a jakým komunikačním kanálem má být informován,
- jaké bezprostřední změny v bezpečnostním nastavení se mají provést (vzdáleně prostřednictvím MDM/MDA) – např. zablokování přístupu, smazání dat apod.,
- jaké následné forenzní šetření je potřeba podstoupit, aby se zjistilo reálné postižení.

Uživatelsky fatálním následkům havarijních postupů lze předejít tím, že se uživatelé naučí zálohovat svá soukromá data a nastaví se pravidelné zálohování firemních dat umístěných v mobilním zařízení.

Implementace některých z uvedených opatření bude vyžadovat důkladné plánování a úsilí pracovníků IT. Je proto potřeba, aby si všechny zainteresované strany uvědomily, že se toto úsilí vyplatí, a aby vedení společnosti ocenilo snahu snížit riziko úniku citlivých dat, a tím i reputační riziko. Pokud jsou při volbě opatření zohledněni i samotní majitelé zařízení (v případě BYOD), budou k nim i oni přístupnější. Důležité je také uvědomit si, že řízení bezpečnosti mobilních zařízení není v podstatě nic nového a že se jedná „pouze" o rozšíření stávajících principů a opatření na mobilní zařízení.

Igor Gricinko, MBA, CISA

*Je absolventem Escuela Superior de Marketing y Administración a držitelem certifikace CISA od roku 2011. Pracuje více jak 15 let v IT oborech, z toho 5 let jako auditor IT v Komerční bance. Věnuje se zejména bezpečnosti informačních a komunikačních systémů, řízení IT rizik a problematice Basel AMA.*

# INTERNÍ AUDIT A MODERNÍ KOMUNIKAČNÍ TECHNOLOGIE

Historie auditů sahá do dob mezopotamské civilizace 3500 let před Kristem, kdy jeden písař připravoval součty transakcí a druhý je ověřoval. Od té doby se svět poněkud změnil. Auditoři si postupně zvykali na používání kuličkového počítadla, arithmometru, logaritmického pravítka, kalkulačky (o velikosti půl stolu) a nakonec i počítačů.

Dnes už si práci auditora nelze představit bez laptopu, mobilního telefonu a bez neustálého připojení „někam". Je to realita dnešních dnů: procesy jsou stále složitější, termíny jsou neúprosné, geografické vzdálenosti nehrají roli a auditované mnohdy ani „fyzicky" nepotkáme. K tomu, aby to smrtelník-auditor vše zvládl, se musí spolehnout na technické pomocníky.

Otevřel jsem svůj počítač a zjistil jsem, že denně potřebuji minimálně 17 aplikací pro svou práci. Pojďme si uvést příklady, kdy technika pomáhá auditorům:

| | Typ | Typický příklad |
|---|---|---|
| Základní nástroje | Tabulkový procesor | Excel |
| | Textový editor | Word |
| | Správce souborů | Total Commander |
| | Elektronická pošta | Outlook |
| | Prohlížeč sítě Internet | Internet Explorer |
| | Prezentace | Powerpoint |
| Podpůrné nástroje | Tvůrce PDF | PDF creator |
| | Prohlížeč PDF | Adobe Acrobat |
| | Kompresní program | WinZip, 7-zip |
| | Otisk obrazovek | ScreenHunter, Výstřižky |
| | Kreslení | Visio |
| Sofistikované nástroje | Analýza dat | IDEA |
| | Databáze | SQL, Access |
| | Řízení času | Project |
| | Auditní evidence | TeamMate, Galileo atd. |
| | Synchronizace | BlackBerry, ActiveSync atd. |
| | Připojení | VPN klient |

Výhody použití technologií jsou zřejmé:

- Úspora času (potažmo i nákladů);
- Automatizace všeho druhu (výběry vzorků, předběžná analýza);
- Snadná a rychlá komunikace (jak interní, tak i s auditovanou stranou);
- Urychlení výpočtů nad velkými vzorky;
- Analýza velkého objemu informací;
- Připojení kdykoli, kdekoli a k čemukoli;
- Efektivní práce s textem, prezentace výstupů atd.;

Na druhou stranu jako IT auditor, který více jak 15 let pracuje s počítači, vidím i nevýhody technologií např.:

- Heterogenní prostředí nutí auditora být spíše IT specialistou;
- Žádný počítač nezamění lidský úsudek (alespoň zatím ne);
- Výstupy z počítače/programů musíte interpretovat;
- Po čase začínáme technice bezmezně důvěřovat;
- Programy nejsou dokonalé a obsahují chyby;
- Techniku musíte umět obsluhovat;
- Programy je nutné používat účelově a efektivně;
- Technika vždy selže v nejméně vhodnou chvíli;
- Licenční poplatky jsou nenulové.

Zkusme se na nevýhody podívat ve větším detailu, jelikož jsou méně viditelné než výhody.

Osobně provádím audity ve více jak 30 společnostech. Každá z nich, byť jsou součástí skupiny, používá jiné IT systémy, pracuje s jinými formáty dat. V důsledku, pokud si vyžádám jeden druh auditní dokumentace (např. elementární organigram společnosti), dostanu jej minimálně ve třech různých formátech. K tomu, abych rychle a efektivně vytěžil z balíku dat jejich informační hodnotu, mě heterogenní prostředí nutí často přemýšlet, jaký soubor otevřít čím, převést kam atd.

Počítače a programy mohou být dobrými pomocníky, ale osobně jsem toho názoru,

2. Využíváme internetovou a intranetovou síť, smartphony, síťová zařízení, sdílení dat, dálkové přístupy.

3. Z hlediska využití komunikačních technologií je nutné, aby i audit tzv. nezaspal dobu a držel krok v používání moderních, nejen komunikačních, technologií ve své práci. Stěžejními riziky této problematiky bude zejména riziko zneužití přístupových oprávnění, šifrovacích klíčů, elektronických podpisů, včetně nadměrného či neopodstatněného použití komunikačních prostředků zaměstnavatele, dále riziko nezabezpečení dat před viry a nedodržování autorských práv (copyright). Stále je velkým rizikem neoprávněný zásah z vnějšku (prostřednictvím hackerů) a s tím související možnost zneužití interních informací (často podléhající určité míře utajení, v případě veřejné správy zejména např. osobní údaje).

**Alice Kateřina Visolajská**
**Senior Specialist, interní auditor**
**DAIKIN INDUSTRIES Czech republic, s.r.o.**

1. Pod pojmem „Moderní komunikační technologie" si dovedu představit vše, co umožňuje komunikaci a výměnu informací jiným způsobem, než nutnou osobní účastí daných osob.

2. Pracuji v mezinárodním týmu interních auditorů se sídlem v mateřské společnosti v Belgii, a proto využíváme kromě klasického emailu, telefonů také videokonference.

3. Největší riziko v této oblasti vidím zejména v zabezpečení dat a informací.

**Alena Marcínová**
**vedoucí IA**
**ČEPS, a.s.**

1. Mobil, telefonní linka, mail, sociální sítě, webová komunikace (např. tento dotazník), intranet včetně sdílených složek.

2. Mobil, telefon, web, mail, intranet.

3. Audit – bezpečnost, šifrování využívání – všechny formy s cílem zrušit v co největší míře „papír" riziko – možnost zneužití dat, formy šifrování, úniky informací.

že nedokážou nahradit pestrost lidského myšlení. V mnoha případech mé praxe mě auditní evidence ujišťovala o tom, že v dané oblasti jsou rizika minimální. Kouzlo osobního setkání, pozorování chování lidí i „zdravý selský rozum" mi však pomohly vést analýzu správným směrem a odhalit nedostatky. Technika by se měla chápat jako pomocník, který ledacos napoví. Výstupy z programů (analýza z Excelu, výsledek SQL dotazu atd.) však musí být auditorem správně interpretovány, tj. přeložené z řeči čísel do reálných dopadů, zasazené do kontextu nálezu, použity jako podklad pro jasné argumenty pro zadavatele auditu. A to už je úkol, který počítač nezvládne. Zde je zapotřebí použít analytické myšlení, znalost prostředí, letité zkušenosti a „selský" rozum.

Další nevýhoda, kterou pozoruji, je vztah bezmezné důvěry k technice. Myslím, že existují dva extrémy:

- ten, kdo počítačům, programům a IT do detailu nerozumí. Ten získává pocit respektu, úcty a neomylnosti vůči blikající obrazovce velmi snadno;
- druhým extrémem je IT profesionál, který ví vše, a znalosti jej utvrzují v bezchybnosti IT.

Důležité je být názorově ve středu obou extrémů a uvědomit si, že veškerou techniku vymyslel jen člověk. Technika, programy i jejich výstupy tak mohou být zatíženy chybou. Proto vše, co auditorovi automaticky vyhodnotí nějaký program, je nutné objektivně ověřit (např. v oblasti forenzního auditu). A to jsem neotevřel širokou oblast bezpečnosti IT. Osobně znám 101 způsobů, jak zmanipulovat informace v počítači, a tím i pokřivit realitu. Funguje to v případě, kdy auditor bezmezně propadne důvěře v technologie.

Již jsem hovořil o chybách techniky a o jejich důsledcích. Mohu uvést jeden názorný příklad, který již byl dávno zapomenut. Procesor je srdcem každého počítače a jeho úkolem je provádět matematické výpočty. V roce 1994 byl procesor Intel Pentium 5 modelové řady 1 a 2 postižen chybou zvanou FDIV, neboli chybou v jednotce, která prováděla výpočty v plovoucí řádové čárce. Pokud jste na kterémkoli počítači, který byl osazen tímto procesorem, dali jakémukoli programu vypočítat 4195835/3145727, vrátil vám výsledek 1.333 739068902037589 místo správné hodnoty 1.333 **820449136241002**. Zdánlivá maličkost?

Již na začátku článku jsem uvedl krátký výčet programů/aplikací, které tvoří denní chleba auditora. Domnívám se, že k tomu, abychom z těchto programů vytvořili efektivní pomocníky, a nikoli nepřátele komplikující práci, je nutné s aplikacemi umět pracovat, plně využívat jejich funkcí a vědět o jejich slabinách. Zažil jsem případy, kdy se ve Wordu kapitoly a obrázky číslovaly ručně, text se posouval na střed stránky pomocí mezer atd. Neříkám, že to nejde, ale tím si přidělováme práci a počítač se stává spíše komplikací než pomocníkem. Proč nepožádat zkušené kolegy o školení? Často psané texty nahradit automatickým textem a používat univerzální šablony auditní zprávy?

Dalším bodem je účel použití některých programů v praxi. Často se setkávám s tvrzením, že Excel je všemocný. Používá se mimo výpočtů a analýzy dat také na dlouhé dotazníky, matice 200x200, plánování zdrojů atd. Není to chyba, to rozhodně ne. Výrobce programů se snaží svůj produkt připravit jako univerzální, aby pokryl potřeby většiny zákazníků. Excel se dá přizpůsobit téměř na vše. Spíše je nutné se zamyslet, zda neexistuje pro daný problém lepší, přehlednější, jednodušší nástroj. Příkladem může být plánování zdrojů a auditu. Zde by šel použít i nástroj Project. Navíc každý program má svá omezení daná buď technickými možnostmi, nebo licenční politikou výrobce. Tato omezení limitují i jejich použití v praxi, např. Excel s více jak 64 tis. řádky spolehlivě „spadne"; analýza více jak 1 milionů řádku v Access je téměř nemožná, poznámkový blok neotevře větší textový soubor atd.

Předposlední nevýhoda IT je interpretací Murphyho zákonů v praxi. Co se může pokazit, to se pokazí, a to v nejméně vhodnou chvíli. Připadají vám níže uvedené obrázky povědomé?

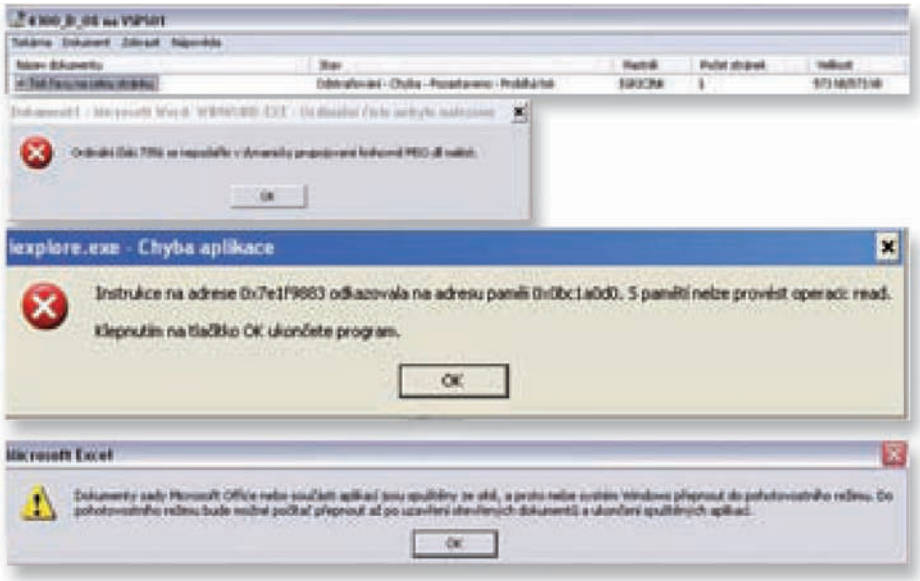
Takové chování počítače dokáže odradit i profesionála. A jak je těžké tiskárnu přesvědčit, aby tiskla prezentaci pro představenstvo, když už stojíte ve dveřích a nechcete přijít pozdě?

A příkladů bych mohl uvést desítky. Důležité je nespoléhat na počítače na 100 % – vždy se pokazí. Na druhou stranu, pokud by technika pracovala perfektně, o práci by přišlo celé IT oddělení.

Poslední nevýhodou, které bych se chtěl věnovat, jsou licenční poplatky. Programy jsou duševním vlastnictvím a výrobci si za ně účtují nemalé poplatky. Některé aplikace jsou sice zdánlivě „zdarma", nicméně pro jejich komerční využití (což audit bezesporu je), je nutné uhradit poplatek. Pro organizaci to může představovat značné náklady a dá se říct neúčelně vynaložené, pokud programy nejsou využity efektivně.

Jako od každého auditora, tak i ode mne se očekává doporučení závěrem. Pokusil jsem se je shrnout do populárního desatera:

1. *Nebojte se používat IT nástroje pro podporu auditu. Dnes jsou nezbytnou součástí práce.*
2. *Nedůvěřujte na 100 % všemu, co vidíte na obrazovce.*
3. *Programové výstupy je nutné interpretovat. Selský rozum je k nezaplacení i v 21. století.*
4. *Najměte do auditního týmu IT specialistu, IT auditora nebo datového analytika.*
5. *Do detailů vyškolte uživatele pro práci se základními programy (elektronická pošta, textový editor).*
6. *Pořádejte interní workshopy podporující výměnu zkušeností mezi auditory (i v oblasti efektivního využívání IT prostředků).*
7. *Používejte IT nástroje účelně a nebojte se změny zaběhnutých postupů. Nechte si poradit.*
8. *Pod tíhou obchodních nabídek nekupujte programy bezhlavě. Nejprve je vyzkoušejte v praxi.*
9. *Nespoléhejte plně na techniku. Určitě selže v nejméně vhodný okamžik. Mějte záložní plán.*
10. *Pokud technika vykazuje perfektní výsledky, není něco v pořádku.*



**Bohuslav Dohnal**
Managing Partner
společnosti netmail

*Působí jako Managing Partner ve společnosti netmail, kde se zabývá architekturou a nasazením veřejných cloud služeb a vývojem cloud aplikací ve středních a velkých organizacích. V současné době spolupracuje se společností Google na několika projektech nasazení tzv. Google Cloud Platform v zemích střední a východní Evropy.*

# Rozhovor s BOHUSLAVEM DOHNALEM

*Rozhovor vede Luboš Klečka ze společnosti Česká spořitelna, a.s.*

***Co si myslíš o cloud technologiích?***

Cloud technologie jsou jednoznačně jedním z nejvýznamnějších konceptů, který se v ICT objevil. Nabízí reálné přínosy pro firmy i jednotlivce.

To, že cloud dnes používáme, je dáno rozvojem mnoha dílčích technologií – internet, mobilní zařízení, internetové prohlížeče, flexibilita zpracování a odbavení požadavků stovek milionů uživatelů v reálném čase. Důvody, proč firmy adoptují cloud řešení, jsou zejména tyto:

- dostupnost informací s cílem zajistit a zjednodušit obchodní příležitosti;
- nové formy spolupráce a interakce v týmech nebo se zákazníky;
- příležitost změnit firemní kulturu;
- kontrola cen, v mnoha případech i snížení cen;
- značná pružnost využitelnosti a vysoký výkon.

Cloud je nicméně součástí širšího konceptu digitalizace – který zasahuje všechny obory, firmy i jednotlivce. Cloud je jedním ze základních kamenů, které tuto digitalizaci umožňují.

***Hovoříš o zjednodušení, dostupnosti, využitelnosti cloud řešení. Není na místě reakce z hlediska ochrany dat?***

Ochrana dat – osobních i firemních je na prvním místě. Bohužel v minulosti tomu tak ne vždy bylo, ale právě cloud vynesl tuto problematiku více na světlo. Používání cloud řešení musí být podmíněno důvěrou mezi poskytovatelem a firmou, na základě vzájemně dohodnutých a odsouhlasených podmínek. Významnou roli hrají také nezávislí auditoři a certifikace, které usnadňují zákazníkům orientaci při výběru cloud poskytovatele.

Musí být zřejmé, jaké možnosti a požadavky firma má z hlediska ochrany dat a bezpečnostní politiky. Tyto požadavky by měly být pečlivě srovnány s možnostmi, které poskytovatel cloud řešení má. Tady hraje značnou roli analýza rizik. Nesmíme ale zapomenout, že každé riziko má příležitosti na straně byznysu a je třeba hledat odpovídající rovnováhu.

„Cloud umožňuje nabídnout zcela nové služby nezávisle na místě, čase nebo zařízení“

***Jak se, dle Tvého názoru, bude cloud řešení vyvíjet?***

Z mého pohledu je cloud významně spojen s trendem „konzumerizace IT“ ve firemním prostředí. V soukromém životě zákazníci preferují snadnost a rychlost používání technologií, na rozdíl od firemního prostředí, kde je uživatel nucen používat složitá řešení s výraznými omezeními (např. omezená dostupnost, kapacita, rychlost). Trendy cloud řešení nejsou ani tak dány z pohledu IT, jako z pohledu běžných uživatelů a toho, co se bude dít v technologiích z pohledu běžného spotřebitele. Další motivací poskytovatelů cloud řešení bude zjednodušení a dostupnost informací v celém širokém spektru. Jsem přesvědčen, že hybatelem budou i obchodní požadavky firem – dostat se blíže k zákazníkovi, využít všech dostupných a rychle zpracovaných informací k zajištění spokojenosti zákazníků. Pro budoucnost cloudu, nebo lépe digitalizace je třeba se dívat na neobvyklé příležitosti, které s největší pravděpodobností přijdou z nečekaných směrů.

***Co je v současnosti hlavní motivací pro přechod ke cloud řešení?***

Jedním z prvních tzv. spouštěčů je snížení nákladů, což si ale řada zákazníků chybně přeložila do snížení výdajů spojených s provozem IT. Cloud umožňuje nabídnout zcela nové služby nezávisle na místě, čase nebo zařízení. Tímto způsobem lze docílit snížení nákladů na neefektivní cestování, schůzky, zjednodušenou komunikaci se zákazníky apod. Principy „pay-as-you-go“ pak tyto přínosy jenom podtrhují.
V současnosti už se již prosazuje u klientů chápání cloud řešení jako příležitosti provést změnu fungování organizace, způsobů komunikace a spolupráce – s důsledkem změny firemní kultury a nástupem digitalizace firem i jednotlivců.

***Zmínil jsi změnu kultury v organizaci. V jakém smyslu?***

Firemní kulturu vytvářejí lidé a ti ji také mohou změnit. Cloud je v prvé řadě způsob, jak se „dělá IT“ a tím, že cloud je dostupný kdekoliv a kdykoliv, přináší nové způsoby komunikace a spolupráce – tak může v organizaci pomoci nastartovat změnu. Videokonference, chat, rychlý přístup k informacím by měly vyústit k novým, efektivním formám spolupráce mezi zaměstnanci, zákazníky nebo partnery. Není možné si myslet, že podnikové systémy nebo aplikace, které vycházejí z konceptů s kořeny v 90. letech (nebo

i dále), mohou naplnit očekávání a rozvoj, která na ně dnešní uživatelé kladou.

Otázku bychom samozřejmě mohli položit v obráceném směru: „Brzdí zastaralé technologie rozvoj organizace?“ Případně: „Je nastavená infrastruktura stále vyhovující pro naplnění obchodních cílů?“

průběžně po celou dobu plánování a využívání cloud služeb. Cloud služby se neustále rozvíjejí a přinášejí nové možnosti, a v některých případech také rizika, která je třeba vyhodnotit a pracovat s nimi. Současně je třeba pracovat i s exit strategií a data portability. Řada cloud poskytovatelů poskytuje vzájemně kompatibilní rozhraní,

## „Používání cloud řešení musí být podmíněno důvěrou mezi poskytovatelem a firmou“

*Jak vnímají dnešní CIO cloud řešení?*

Většina CIO o cloud slyšela, viděla prezentace, diskutovala možnosti cloud řešení. Možná jim bylo od podřízených řečeno, že mají vlastně „privátní cloud“. Bohužel jenom velmi málo z nich má s cloud řešením ve firemním prostředí praktickou zkušenost – i třeba jenom z pilotních projektů. Řada z nich má dnes pocit, že cloud je jenom bublina a ve skutečnosti nepřináší nic nového. Praxe je ale většinou taková, že i když „oficiální stanovisko“ je, že cloud nevyužívají, většinou jsou jejich firemní data dávno v cloudu.

a lze tedy snadno navrhovat architekturu cloud řešení a exit strategii tak, aby bylo možné ve velmi krátkém čase přesouvat aplikace, data, výpočetní výkon mezi cloud poskytovateli. V mnoha případech je velmi výhodné mít více cloud poskytovatelů, zejména pro kritické služby a aplikace.

Implementace cloud řešení v širším kontextu organizace představuje významný projekt a důležitou změnu. Proto je potřeba dobře připravit řízení změny, a především interní komunikaci – proč se tak děje, jaké jsou očekávané přínosy, jak bude projekt probíhat, zajištění ochrany dat atd. Vždy bych volil pro realizaci takový

## „Není možné si myslet, že podnikové systémy nebo aplikace, které vycházejí z konceptů s kořeny v 90. letech, mohou naplnit očekávání a rozvoj“

*Vraťme se, prosím, k problematice bezpečnosti. Jaké doporučuješ kroky před zavedením cloud řešení?*

V první řadě volba plnohodnotného cloud poskytovatele a současně detailní analýza rizik, připravená pro cloud poskytovatele – například ENISA. Určitě se nejedná o jednorázovou událost, naopak – rizika cloud řešení je třeba vyhodnocovat

tým, který má s podobnými projekty zkušenost. Získání vlastní zkušenosti bývá zpravidla draze vykoupeno.

*Má IT bezpečnost reagovat na novou situaci?*

Samozřejmě ano! IT bezpečnost by měla být především mentorem, jak se v cloud a online světě pohybovat. Bohužel ale většinou vidíme spíše restriktivní přístup ve smyslu – uživatel neví, jak s tím pracovat, tak mu to raději zakážeme. Nebo dokonce „můžeme něco zakázat, tak to zakážeme“. S pravidly či nastavením kroků IT bezpečnosti by se uživatelé měli cítit bezpečně, ne omezeně, nebo dokonce ohroženě (například sledováním).

IT bezpečnost, ale i IT jako takové, si musí uvědomit, že doby, kdy lidé v zaměstnání měli nejmodernější techniku a doma nic, je dávno pryč. Není možné uživatele podceňovat nebo podezřívat z „počítačové negramotnosti“. S nástupem digitalizace se v následujících letech významně zvýší množství rizik spojených s „cyber“ prostorem a IT bezpečnost bude čelit zcela novým požadavkům ochrany a zabezpečení.

Národní konference ČIIA – Užitečnost interního auditu aneb audit ve všech barvách; říjen 2013
Pavel Racocha, Komerční banka

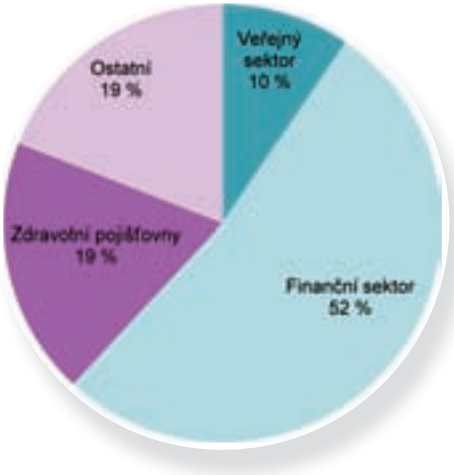
**Ing. Pavel Závitkovský, CIA**
Partner, Audit,
KPMG v České republice

**Ing. Zuzana Kitto, CPA, CISA**
Associate Manager, Risk Consulting,
KPMG v České republice


# HROZBY A PŘÍLEŽITOSTI INTERNÍHO AUDITU IT

- *Jak firmy organizují, plánují a řídí aktivity interního auditu IT?*
- *Má interní audit IT odpovídající zdroje a nástroje?*
- *Pokrývá svou činností klíčová rizika?*

Na tyto i další otázky hledal odpověď průzkum celosvětové sítě poradenských společností KPMG o stavu interního auditu IT. Poprvé proběhl v roce 2009, podruhé na konci minulého roku, kdy se ho zúčastnilo přes 400 organizací z 21 zemí Evropy, Blízkého východu a Afriky (region EMEA). Respondenty byli vedoucí oddělení interního auditu, interního auditu IT nebo řízení rizik. V České republice se zapojilo celkem 21 společností napříč několika sektory, jejichž rozložení znázorňuje následující graf.




Aktuální průzkum auditu IT v regionu přinesl několik hlavních poznatků:

- Audit IT se bude muset stále více zaměřovat na nově vznikající rizika (Sofware jako služba neboli SaaS, kybernetická bezpečnost, Big Data[1] nebo využití cloudu) a bude potřeba zajistit jejich náležité pokrytí z interních nebo externích zdrojů.
- 78 procent společností uvádí jako hlavní důvod nespokojenosti s auditem IT nedostatek znalostí a dovedností, ovšem jen 31 procent společností využívá služeb externích poskytovatelů.
- Mnoho společností rozhoduje o zaměření auditu IT na základě schopností svého týmu interních auditorů a podle rozpočtových omezení, místo aby se zaměřily na svůj rizikový profil.
- Se svým interním auditem IT byla spokojena méně než polovina respondentů, přestože ve většině těchto společností byl plán auditu IT schválen vedením.
- Existuje prostor pro větší sladění činnosti interního auditu IT s ostatními aktivitami správy a řízení společnosti: pouze 53 procent společností se domnívá, že interní audit IT je s těmito aktivitami v náležitém souladu, přičemž 16 procent uvádí limitovanou nebo žádnou koordinaci.
- V řadě dotázaných společností by bylo možné vyšší kvality dosáhnout prováděním kontroly kvality činností interního auditu IT.

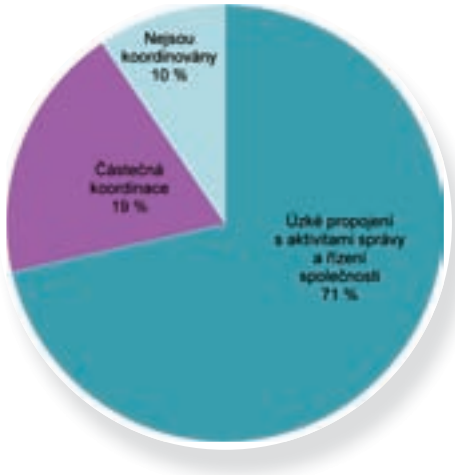
A jak si vedly české společnosti v porovnání s celkovými zjištěními? Výsledky 21 zúčastněných českých firem lze rozdělit do několika oblastí.

## ORGANIZAČNÍ ZAČLENĚNÍ FUNKCE INTERNÍHO AUDITU

Stejně jako v regionu EMEA i v českých společnostech odpovídá vedoucí interního auditu výboru pro audit, představenstvu nebo dozorčí radě. Polovina respondentů uvedla podřízenost interního auditu i generálnímu řediteli společnosti. Z odpovědí lze dovodit, že interní audit je často podřízen liniově generálnímu řediteli či CEO společnosti a funkčně výboru pro audit nebo dozorčí radě.

71 procent českých respondentů se domnívá, že audit IT je dostatečně sladěn s ostatními činnostmi řízení a správy společnosti. To je o poznání lepší výsledek než v celém regionu, kde úzkou koordinaci s ostatními činnostmi řízení a správy společnosti uvádí pouze polovina společností.

V jakém rozsahu jsou plány interního auditu IT koordinované s ostatními aktivitami vedení společnosti? (výsledky za ČR)



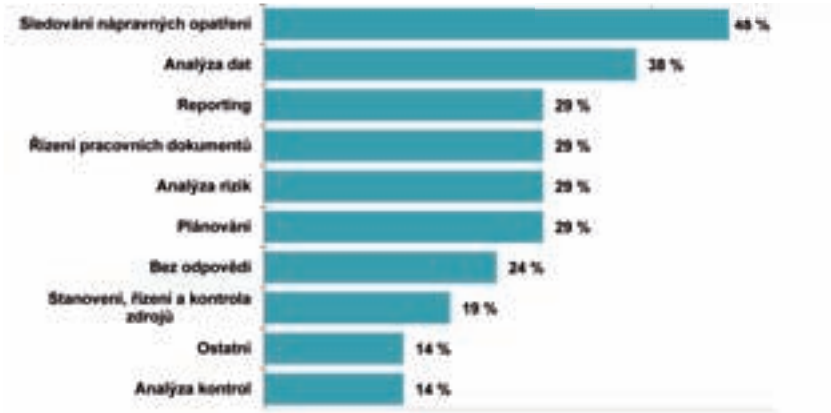

[1] Pojem Big Data označuje data, která jsou moc velká nebo složitá, aby je bylo možno zachycovat, spravovat a zpracovávat běžně používanými softwarovými prostředky v rozumném čase. Například americký řetězec Walmart spravuje milion zákaznických transakcí za hodinu a velikost databází je odhadována na 2,5 petabajtů.

## ORGANIZACE AUDITU IT

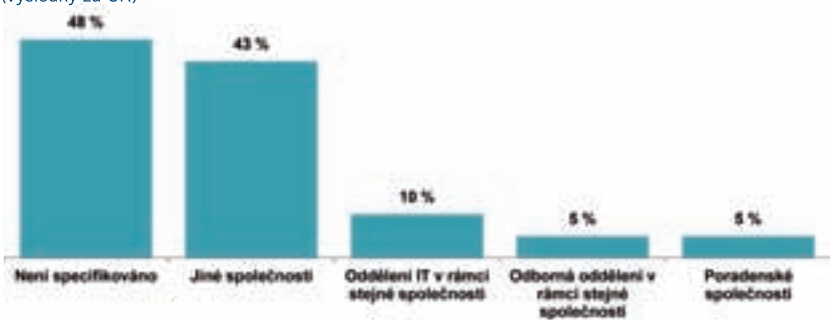
Většina oddělení interního auditu zajišťuje činnost auditu IT z vlastních zdrojů. V Česku jsou v porovnání s ostatními zeměmi více využíváni externí dodavatelé (ČR 34 procent, EMEA 31 procent) a zdroje z ostatních oddělení společnosti (ČR 22 procent, EMEA 13 procent). Může jít o důsledek toho, že větší týmy auditorů IT fungují jen ve velkých bankách a většina společností specializované pracovníky nemá nebo využívá služeb mateřské společnosti. Externí dodavatelé v České republice podobně jako v ostatních zemích regionu nejčastěji poskytují 0–20 procent celkového objemu auditu IT a jsou jim nejčastěji alokovány zdroje ve výši 0–20 procent celkových zdrojů. Hlavními důvody využití externích zdrojů jsou nedostatek technických znalostí a nedostatek kapacit.

„Z odpovědí lze dovodit, že interní audit je často podřízen liniově generálnímu řediteli či CEO společnosti a funkčně výboru pro audit nebo dozorčí radě“

Ve které fázi procesu interního auditu IT jsou používané automatické nástroje? (výsledky za ČR)




Do jakých oblastí odcházejí zaměstnanci interního auditu IT? (výsledky za ČR)




## ROZSAH POKRYTÍ A PŘÍSTUP K AUDITU IT

Rozsah pokrytí se v českých společnostech liší. Ve finančním sektoru je pokrytí jednotlivých oblastí auditem IT poměrně široké a zahrnuje mobilní komunikační technologie, sociální média a cloud, zatímco v ostatních společnostech, kde často nepůsobí specializovaní auditoři IT, je pokrytí podstatně užší a zaměřuje se především na „tradiční“ oblasti, jako jsou bezpečnost IT, kontroly IT prostředí a klíčové IT projekty.

Většina společností využívá při výkonu auditu IT mezinárodně uznávaný rámec jako COBIT, ITIL nebo ISO 27001.

Nejčastěji využívanými automatickými nástroji v rámci auditu IT jsou sledování nápravných opatření a nástroje pro analýzu dat. Pro české respondenty je příznivé, že automatizované nástroje využívají častěji, než je průměr regionu EMEA.

## PLÁNOVÁNÍ INTERNÍCH AUDITŮ IT

Z odpovědí na otázky týkající se plánování bylo nejpřekvapivější zjištění, že u čtvrtiny českých respondentů není zaveden formální cyklus plánování. Na druhou stranu analýzu či vyhodnocení rizik provádějí všechny české společnosti, většinou jednou ročně.

## LIDSKÉ ZDROJE

Auditoři IT v Česku jsou služebně starší, než je průměr regionu. Čeští auditoři IT nejčastěji odcházejí do jiných společností. Do jiných oddělení v rámci jedné společnosti přechází jen necelá čtvrtina českých auditorů IT. Přitom v zahraničí představují přestupy do jiných oddělení přibližně polovinu všech jejich odchodů.

## HODNOCENÍ ČINNOSTI AUDITU IT

V této oblasti české společnosti jednoznačně zaostávají: polovina českých respondentů neprovádí žádné hodnocení kvality auditu IT (v regionu EMEA hodnocení neprovádí pouze jedna třetina firem).

62 procent českých respondentů je spokojeno s úrovní auditu IT, zatímco v celém regionu je to pouze 46 procent. Hlavní důvod nespokojenosti je v Česku i celém regionu stejný – nedostatek znalostí a dovedností.

## CESTA DO BUDOUCNOSTI

Situace v českém interním auditu IT je trochu jiná než v ostatních zemích regionu. Nová IT rizika do českého prostředí pronikají pomaleji a společnosti mají víc času se na ně připravit. Ovšem i tak platí, že se profil IT rizik mění, a je tedy nutné je identifikovat, ohodnotit a přizpůsobit jim náplň činnosti auditu IT. To lze bez formálního plánovacího procesu zajistit jen velmi těžko.

Posledním bodem k zamyšlení jsou lidské zdroje. Neznamená nižší podíl přestupů auditorů IT do jiných oddělení společnosti, že o kolegy z interního auditu nemají ostatní oddělení zájem? Je to důsledek jejich delšího setrvávání v interním auditu, nebo špatného pochopení role interního auditu ve společnosti?


Národní konference ČIIA – Užitečnost interního auditu aneb audit ve všech barvách; říjen 2013

## „Auditoři IT v Česku jsou služebně starší, než je průměr regionu“

Nejčastěji požadovanými profesními certifikacemi jsou CISA (Certified Information Systems Auditor), CIA (Certified Internal Auditor) and CISM (Certified Information Security Manager). Čtvrtina českých respondentů nepožaduje od svých auditorů IT žádnou profesní certifikaci, zatímco v celém regionu nemá žádný takový požadavek pouze šest procent společností.
V rámci regionu EMEA je alarmující, že zatímco většina společností očekává, že v budoucnosti budou potřebovat poměrně specifické znalosti, jenom 16 procent z nich poskytuje svým auditorům IT technická školení. V České republice není tento rozdíl tak velký. Technická školení poskytuje přes 30 procent respondentů a potřeba auditů cloudu a dalších nově vznikajících rizik není tak velká.

V České republice je lepší koordinace auditu IT s ostatními činnostmi řízení a správy společnosti a také spokojenost s úrovní auditu IT je zde vyšší. Nicméně ve společnostech, kde je úroveň auditu IT hodnocena jako nedostačující, je stejně jako ve zbytku regionu potřeba se zaměřit na školení týmu auditorů IT, případně na zajištění externích zdrojů.

V řadě případů je možné dosáhnout zvýšení úrovně auditu IT zavedením systematického rámce pro hodnocení kvality a efektivity interního auditu.

Ing. Jiřina Oleksiaková
Česká spořitelna, a.s.
úsek interního auditu
joleksiakova@csas.cz

# ZKUŠENOSTI S AUDITEM ODMĚŇOVÁNÍ

Ráda bych navázala na předchozí dva články, týkající se odměňování ve finančních institucích v souvislosti s CRDIII, a podělila se s vámi o své praktické zkušenosti při výkonu tohoto auditu.

Náš tým se aktivně účastnil již procesu přípravy a implementace regulatorních požadavků do banky. Od roku 2010 jsme společně se skupinou odborníků z útvaru řízení rizik, lidských zdrojů, kanceláře společnosti právního útvaru a dalších zainteresovaných útvarů a společností podrobně konzultovali jednotlivé požadavky Směrnice Evropského parlamentu a Rady 2010/76/EU, a zejména novelizované Vyhlášky č. 123/2007 Sb., o pravidlech obezřetného podnikání bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry (dále jen Vyhláška č. 123/2007 Sb.), včetně úředního sdělení ČNB ze dne 22. 12. 2010 k výkonu činnosti banky, družstevní záložny a obchodníka s cennými papíry na finančním trhu – odměňování.

Základním záměrem této skupiny bylo zpracovat Zásady odměňování a nastavit systém odměňování v bance tak, aby vyhovoval požadavkům regulátora a motivoval k obezřetnému podnikání s cílem zajistit dlouhodobou finanční stabilitu banky.

Fungování zásad odměňování, zejména plnění schválených zásad a plánů, přiměřenost odměn vzhledem k rizikovému profilu i dlouhodobým cílům instituce a soulad s národními a mezinárodními předpisy a standardy, podléhá nezávislé vnitřní kontrole. V naší bance toto ověření provádí již druhým rokem útvar interního auditu. Nutno však zmínit, že za přijímání opatření k nápravě a zajištění správného fungování systému vždy odpovídá dozorčí orgán.

A nyní již, jak jsme přistoupili k vlastnímu auditu.

Ze všeho nejdříve jsme si stanovili cíl auditu, a tím bylo, poskytnout managementu banky ujištění o tom, že nastavení zásad a postupů odměňování je v souladu s legislativními požadavky dle Vyhlášky ČNB č. 123/2007 Sb., příloha č. 1a. Současně bylo cílem ověřit plnění schválených zásad politiky odměňování a přiměřenosti odměn vzhledem k rizikovému profilu i dlouhodobým cílům banky a souladu s národními a mezinárodními předpisy a standardy.

> „Interní audit aktivně sleduje všechny změny a doporučuje auditovaným útvarům analyzovat dopady nových požadavků“

Mezi auditovanými subjekty byly lidské zdroje, řízení rizik, kancelář společnosti, výbor pro odměňování, dozorčí rada a dceřiné společnosti, kterých se tato legislativní úprava týká.

Informace pro vyhodnocení stanoveného cíle jsme získali zejména studiem obecně závazných právních předpisů, příslušných vnitřních předpisů auditovaných společností a útvarů a v neposlední řadě řízenými rozhovory se zaměstnanci auditovaných útvarů a společností. Současně jsme provedli analýzu nastavených pravidel a procesů, a ověřovali vzájemnou spolupráci příslušných útvarů v oblasti odměňování dle pravidel vyplývajících z vyhlášky ČNB č. 123/2007 Sb. v platném znění.

***Mezi obecně závazné právní a regulatorní předpisy, které byly hlavním předmětem našeho zájmu, patřily zejména:***

- Směrnice evropského parlamentu a rady 2010/76/EU, kterou se mění směrnice 2006/48/ES a 2006/49/ES, pokud jde o kapitálové požadavky na obchodní portfolio a resekuritizace a o dohled nad zásadami odměňování.
- Vyhláška č. 123/2007 Sb., o pravidlech obezřetného podnikání bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry, včetně přílohy č. 1a. Podrobnější vymezení některých požadavků na odměňování.
- Úřední sdělení ČNB ze dne 22. 12. 2010 k výkonu činnosti banky, družstevní záložny a obchodníka s cennými papíry na finančním trhu – odměňování.
- Úřední sdělení ČNB ze dne 28. 3. 2012 k pravidlům obezřetného podnikání bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry – Informace o odměňování.

  Příloha č. 1 – Informace o zaměstnancích s vysokými odměnami.

  Příloha č. 2 – Souhrnné informace o odměnách zaměstnanců.
- Pokyny EBA k nominacím členů řídicích orgánů.
- Obecné pokyny k zásadám řádného odměňování podle směrnice o správcích alternativních investičních fondů – ESMA/2013/232.

Dále jsme si podrobně prostudovali všechny vnitřní předpisy a dokumenty, které se k ověřované problematice vztahují, jako jsou např. Základní zásady odměňování, Mzdový řád, řídicí a kontrolní systém apod. V neposlední řadě jsme se v rámci přípravné fáze auditu seznámili i se všemi ostatními informačními zdroji, jako jsou

např. výsledky dohledového šetření ČNB zaměřeného na odměňování, výstupy z prováděného monitoringu, výsledky z předchozího auditu odměňování CRDIII, karty rizik příslušných útvarů, zápisy ze zasedání představenstev, dozorčích rad a Výboru pro odměňování, otázky a odpovědi ČNB k regulaci odměňování, regulace odměňování v bankách – ČBA, rámec profesní praxe interního auditu, standardy pro profesionální praxi interního auditu, výstupy z implementace CRDIII. Auditorské ověřování bylo realizováno analýzou relevantní dokumentace a řízenými rozhovory s managementem a odpovědnými zaměstnanci auditovaných útvarů a společností.

***Před zahájením práce v terénu jsme vypracovali přehled požadovaných podkladů nezbytných pro auditorské ověření. Jednalo se např. o:***

- platné Zásady politiky odměňování, včetně zápisů o schválení představenstvem, dozorčí radou a výborem pro odměňování;
- jmenný seznam osob a funkcí, na které se vztahují specifické zásady odměňování;
- kritéria pro hodnocení významnosti vlivu zaměstnanců na celkový rizikový profil banky;
- seznam hodnocených zaměstnanců a dosažené hodnoty kritérií;
- politika odměňování ve Strategii;
- jména osob odpovědných za správu, aktualizaci a průběžnou kontrolu platnosti Zásad;
- záznamy z dohlídek dozorčího orgánu, reporty dozorčímu orgánu;
- seznam zaměstnanců ve vnitřních kontrolních funkcích a jejich pravomoci;
- popis konstrukce odměny pro zaměstnance ve vnitřních kontrolních funkcích;
- historie plnění kritérií odměn zaměstnanců ve vnitřních kontrolních funkcích;
- seznam poskytnutých výjimek ze specifických zásad odměňování a jejich zdůvodnění (zásada „comply or explain“);
- dokumentace k nastavení formy a struktury odměn týkající se specifických zásad odměňování;
- dotazník pro ČNB + zpětná vazba z ČNB;
- vyhodnocení výkonnostních kritérií za osoby, na které se vztahují specifické zásady odměňování;
- jména osob odpovědných za sledování úrovně kvality;
- dokumentace k případům opatření souvisejících s nedodržením stanovené úrovně kvality (disciplinární opatření, nepřiznání výkonnostní odměny apod.);
- dokumentace k tvorbě bonusového poolu – protokoly o kontrole postupu;
- seznam zaměstnanců pověřených zpracováním těchto odměn – protokoly o proškolení, protokoly o seznámení / komunikace;
- jména osob odpovědných za předávání informací do ČNB;
- přehled všech reportů do ČNB, včetně veškeré dokumentace z ČNB týkající se auditované oblasti;
- dokument/analýza o srovnání odměn s konkurencí;
- analýzy dopadů zavedení;
- přehled nastavených kontrolních mechanizmů týkajících se naplňování Zásad politiky odměňování;
- dodatky ke smlouvám manažerů, na které se vztahují změny podle Zásad politiky odměňování.

***Ověřování auditorského týmu bylo provedeno s využitím vypracovaných testových otázek, rozdělených do předem identifikovaných oblastí a zaměřených zejména na:***

**Kontrolní prostředí:**

- soulad Zásad odměňování s legislativními požadavky, včetně jejich schválení orgány banky;
- uplatňování zásad na všechny povinné osoby v rámci auditované společnosti;
- nastavení pravidel pro uplatňování Zásad odměňování v rámci regulovaného konsolidačního celku;
- definování vybrané skupiny zaměstnanců, jejichž činnosti mají významný vliv na celkový rizikový profil banky, včetně určení vhodných kritérií pro tuto definici;
- soulad Zásad odměňování se strategií podnikání, cíli, hodnotami a dlouhodobými zájmy FSČS;
- opatření k zamezování střetu zájmů v souvislosti s odměňováním a zajištění předejití možného obcházení účelu regulace odměňování;
- složení a činnost Výboru pro odměňování;
- zpracování a aktualizaci Procesní mapy politiky CRD III.

**Systém vnitřní kontroly:**

- pravidelné vyhodnocování stanovených Zásad odměňování;
- nezávislé prověřování uplatňování Zásad odměňování;
- dohled a dodržování kompetencí dozorčích orgánů;
- nezávislost, pravomoci a odměňování zaměstnanců ve vnitřních kontrolních funkcích;
- dodržování zásad měření a hodnocení výkonnosti v souvislosti s odměňováním;
- zajištění uchování schopnosti banky posílit kapitál;
- odůvodnění výjimek ze specifických zásad odměňování – zásada „comply or explain“;
- vybrané předpoklady, uspořádání systému odměňování a určení vhodného okruhu zaměstnanců podléhajícím Zásadám odměňování;
- formu a strukturu pohyblivé složky odměn, včetně zásad pro její omezení;
- uplatňování pravidel při nedodržování stanovené úrovně kvality;
- dodržení pravidel tvorby bonusového poolu.

**Oblast informací:**

- seznámení příslušných zaměstnanců s pravidly odměňování;
- zajištění procesu předávání informací do ČNB;
- plnění informačních požadavků ČNB.

**Oblast řízení rizik:**

- podpora řádného a efektivního řízení rizik prostřednictvím přijatých Zásad odměňování;
- ustanovení Zásad odměňování k nepodněcování podstupování rizika nad rámec míry rizika akceptované bankou;
- přiměřenost odměn vzhledem k rizikovému profilu a dlouhodobým cílům FSČS;
- nastavení kontrolních mechanizmů v auditované oblasti.

**Oblast monitoringu:**

- ▲ průběžné sledování platnosti Zásad odměňování;
- ▲ zajištění monitoringu významných změn s možným dopadem na aktualizaci Zásad odměňování.

Na základě celkových výsledků provedeného auditu auditorský tým posoudil účinnost nastavených kontrolních mechanizmů a vyhodnotil řídicí a kontrolní systém v auditovaných oblastech z hlediska jeho funkčnosti a přispívání k minimalizaci případných rizik.

Nemusím asi ani zdůrazňovat, že se jedná o audit, který je citlivý z hlediska poskytování velmi důvěrných informací a dat. Z uvedeného důvodu bylo s veškerou poskytnutou dokumentací a rovněž s veškerými získanými informacemi jednáno tak, aby byla důsledně zajištěna důvěrnost a ochrana poskytnutých informací a dat.

Upřímně řečeno, provádění tohoto auditu nebylo procházkou růžovou zahradou. Myslím si, že každý z nás, kdo tuto oblast ověřoval, se setkal s určitými úskalími pramenícími právě z „citlivosti" tohoto auditovaného tématu. Získat ty správné podklady pro objektivní vyhodnocení celé oblasti odměňování leckdy vyžadovalo trochu více auditorské snahy a diplomacie, nežli bývá obvyklé.

Myslím si však, že nakonec dobrý pocit z odvedené práce převládl. Nejlepším vysvědčením za naši práci pro nás byla jednak pozitivní zpětná vazba od vedení auditovaných útvarů a společností a rovněž kladné hodnocení naší práce ze strany České národní banky.

Nyní vzhledem k nově připravené regulatorice v oblasti CRDIII a CRDIV interní audit aktivně sleduje všechny změny a doporučuje auditovaným útvarům analyzovat dopady nových požadavků a včas zajistit úpravu zásad a postupů odměňování tak, aby byly v souladu s požadavky legislativy.

*Co ještě říci závěrem? Že je nutné zejména:*

- ▲ nepodcenit přípravu;
- ▲ důsledně vyžadovat potřebné podklady;
- ▲ průběžně sledovat celý právní rámec regulatorní problematiky;

Ing. Petr Hadrava, ACCA, CIA
Interní auditor, MetLife pojišťovna a.s.

# CO OČEKÁVÁ MANAGEMENT OD INTERNÍHO AUDITORA?

Je to již několik let, co jsem dokončil svůj první interní audit. Generální ředitel si na závěrečné schůzce trpělivě vyslechnul, jaké oblasti pro zlepšení jsem během auditu identifikoval, a řekl mi: „Máte zajímavé nálezy, ale nestřílíte mimo terč?“ Tak studenou sprchu jsem skutečně nečekal. Dnes jsem rád, že přišla. Vedla k tomu, že jsem změnil svůj přístup k auditování a mnohem intenzivněji pracuji s očekáváním managementu.

## „Máte zajímavé nálezy, ale nestřílíte mimo terč?“

Rád bych se s vámi podělil o to, co management v MetLife pojišťovně očekává od interního auditora. Určitě to není „střelba mimo terč“.

Tento článek by vás měl vést k zamyšlení, zda to, co děláte v rámci interního auditu, dává smysl, a to jak pro vás, tak pro společnost. Možná pro vás bude inspirací a pomůže vám identifikovat oblasti pro zlepšení a zvýšit hodnotu interního auditu. Přitom nezáleží na tom, zda se jedná o audit v malé či velké společnosti, nebo v pojišťovně či výrobním podniku. Základní principy jeho činnosti zůstávají stejné.

### VÍTE, JAKÉ JSOU CÍLE SPOLEČNOSTI A JAKÝM ZPŮSOBEM JE PLÁNUJE DOSÁHNOUT?

V MetLife pojišťovně hraje interní auditor aktivní roli při dosahování cílů společnosti. Management od interního auditora očekává detailní znalost strategie a cílů, předmětu podnikání a prostředí, ve kterém společnost působí, a hlavně jasné propojení naplánovaných auditů s riziky, které mohou ohrozit dosažení těchto cílů. Pokud neznáme cíle a strategii společnosti, je zde nebezpečí, že neidentifikujeme skutečná rizika, nesestavíme efektivní plán interního auditu, budeme „střílet mimo terč“ a nepřidáme žádnou hodnotu. Pokud management uvidí jasnou vazbu mezi ***cíli společnosti***, které jsou přes vhodně zvolená KPIs managementu i jejich individuálními cíli, ***riziky ohrožujícími dosažení těchto cílů a plánovanými oblastmi k auditu***, pak pochopí, že interní auditor je vlastně jejich partnerem, který jim může k dosažení cílů výrazně pomoci.

Přístup: „výzva pro management = výzva pro interního auditora“ se mi v praxi velmi osvědčil a pomohl při budování důvěry mezi interním auditem a managementem. Významnou měrou přispěl k tomu, že je interní auditor brán jako partner, a nikoli jako nutné zlo vhodné k maximální izolaci.

### ZAJÍMÁ VÁS, JAKOU ZKUŠENOST MÁ S VAŠÍ FIRMOU, VÝROBKY ČI SLUŽBAMI VÁŠ ZÁKAZNÍK?

Management od interního auditora očekává detailní znalost přání a potřeb zákazníků. Spokojenost zákazníků má zásadní dopad na plnění cílů společnosti, a jak jsem již naznačil, interní auditor má přispívat k plnění těchto cílů. Má se tedy zajímat o to, zda je zákazník spokojen, a pokud není, jaké jsou příčiny jeho nespokojenosti.

Jedna z cest, jak získat zpětnou vazbu od klientů, je návštěva zákaznické linky. Interní auditor v MetLife pojišťovně pravidelně poslouchá hovory operátorek s klienty. Úkolem je identifikovat oblasti ke zlepšení, komunikovat je managementu a získat inspiraci pro budoucí audity. Další možností je analýza dopisů klientů a monitorování diskuzních fór na internetu.

### NECHÁTE MANAGEMENT, ABY VÁM MLUVIL DO PLÁNU INTERNÍHO AUDITU?

Management očekává, že bude přizván do procesu tvorby plánu interního auditu. Co více by si interní auditor mohl přát? Interní audit je tu pro společnost a jakýkoli zaměstnanec má podle mého názoru plné právo navrhovat, jakými oblastmi by se interní auditor měl zabývat. Pro mě jsou pravidelné formální i neformální diskuze s managementem i řadovými zaměstnanci cenným zdrojem informací. Diskutujeme, jaké oblasti by chtěli zauditovat a proč. Získané informace tvoří jeden ze vstupů analýzy rizik před sestavením nebo úpravou plánu interního auditu. Při jakékoli diskuzi je zásadní pokládání správných otázek. Otázky typu: „Co vám nejvíce znepříjemňuje vaši práci?“ nebo „Co vám vadí?“ zní jednoduše, až téměř neprofesionálně, ale divili byste se, kolik podnětů pro plodný audit z odpovědí vzešlo.

### MÁ VÁŠ PLÁN INTERNÍHO AUDITU NĚJAKOU VYPOVÍDACÍ SCHOPNOST?

Již výše jsem zdůraznil důležitost vazby mezi cíli společnosti, riziky a plánovanými audity. Mohu doporučit, aby uvažovaný plán interního auditu nebyl jen výčtem plánovaných auditů, ale aby obsahoval i cestu, jak k těmto oblastem interní auditor dospěl, chcete-li „risk assessment“. Ve srovnání s pouhým výčtem oblastí k auditu má takový dokument o hodně větší hodnotu pro jeho čtenáře, ať už to je management, dozorčí rada, nebo výbor pro audit.

### JE VÁŠ PLÁN INTERNÍHO AUDITU ŽIVÝM, RIZIKOVĚ ORIENTOVANÝM DOKUMENTEM?

Auditní plán má být snadné rychle upravit tak, aby stále reagoval na aktuální klíčová rizika. Pokud se připravuje na jeden rok dopředu, je pravděpodobné, že se objeví nová rizika či se změní pořadí naléhavosti stávajících rizik. V takovém případě je nutné změnit pořadí auditních prací. Plán interního auditu má být rizikově orientovaný, tzn. pozornost auditu je zaměřována tam, kde hrozí společnosti

Národní konference ČIIA – Užitečnost interního auditu aneb audit ve všech barvách; říjen 2013
vystoupení Ivo Středy, RWE Česká republika

největší rizika. Periodické slepé auditování typu „rozdělíme činnosti společnosti do 100 procesů a každý rok auditujeme 10 z nich“ již dávno neobstojí. Kromě toho management očekává, že auditor nebude zkoumat jen minulost či současnost, ale že bude schopen kdykoli přijít a upozornit na rizika, kterým může společnost s vysokou pravděpodobností čelit v budoucnosti.

## INTERNÍ AUDITOŘI, MLUVTE S RISK MANAGEREM!

Management očekává, že klíčová rizika identifikovaná interním auditorem a risk managerem se nebudou zásadně odlišovat, stejně jako hodnocení významnosti jednotlivých rizik. Konzistentnost jejich výstupů směrem k managementu je zásadní. Jinými slovy je důležité zajistit, aby obě tyto funkce společnosti promlouvaly k managementu stejným jazykem.

## JE INTERNÍ AUDITOR POUZE „HLEDAČEM NEPRAVOSTÍ“, NEBO I PROAKTIVNĚ NABÍZÍ ŘEŠENÍ?

V MetLife pojišťovně má interní auditor aktivní roli a jeho úlohou není pouze identifikace auditních nálezů, ale je nedílnou součástí procesu hledání nejlepšího řešení pro odstranění těchto nálezů. Interní auditor má v aktivní diskuzi s managementem nabízet možnosti řešení s tím, že konečné rozhodnutí o přijetí konkrétního opatření dělá management.

Ideální je již v průběhu auditu diskutovat možná řešení auditního nálezu se zaměstnanci a na závěrečnou schůzku s managementem přijít už s návrhy řešení dané situace. Přístup: „Tady je seznam auditních nálezů, co s tím hodláte dělat?“ neodpovídá požadavkům managementu na proaktivní přístup interního auditora.

## MÉNĚ JE NĚKDY VÍCE

Management má nabitý kalendář a chce s auditorem a jeho zprávami strávit jen tolik času, kolik je nezbytné a účelné. Interní auditor má do zprávy auditu uvádět pouze dostatečně významné nálezy. Uvádění nevýznamných nálezů by vedlo k rozředění pozornosti managementu a k jejímu odvádění od řešení skutečně důležitých oblastí pro zlepšení. Kromě toho, uvádění nevýznamných nálezů do zprávy auditu povede k tomu, že management nebude brát interního auditora moc vážně.

## HLAVNÍ ÚKOL INTERNÍHO AUDITORA NEKONČÍ IDENTIFIKACÍ AUDITNÍHO NÁLEZU, ANI SHODOU S MANAGEMENTEM, JAKÝM ZPŮSOBEM BUDE NÁLEZ ODSTRANĚN

Při odstraňování auditního nálezu management opět očekává proaktivní přístup interního auditora, který musí tento proces aktivně monitorovat a být v jakémkoli okamžiku schopen říci, v jaké fázi se odstraňování nálezu nachází. Povinností interního auditora je rovněž pravidelně informovat management o uzavřených a otevřených auditních nálezech, a zejména s předstihem informovat o otevřených auditních nálezech, jejichž odstranění v termínu je, podle jeho názoru, ohroženo.

## MÁ BÝT INTERNÍ AUDITOR PARTNEREM VŠECH ZAMĚSTNANCŮ, NEBO OSOBOU, KTERÉ JE LEPŠÍ SE VYHNOUT?

Osobně volím první variantu. Klíčové je vybudovat silný vztah důvěry mezi zaměstnanci a interním auditorem. Výsledkem je, že sami zaměstnanci přicházejí k auditorovi s otázkou, jak by měli přistoupit k řešení určité situace, a nebojí se, že budou postihováni, když na nějakou nedokonalost upozorní. Naopak, budou oceněni za proaktivní hledání efektivního řešení.

> „Interní auditor je brán jako partner, a nikoli jako nutné zlo vhodné k maximální izolaci“

Management očekává, že interní auditor bude poradcem, který na základě svých znalostí a zkušeností napříč celou společností přinese nezávislý pohled na řešení určitých situací, a přinese tím společnosti skutečnou hodnotu.

A co dodat závěrem? Interní auditor by měl dělat maximum pro to, aby byl schopen proaktivním přístupem a kvalitou své práce svoji existenci ve firmě obhájit. Výše jsem naznačil cestu, na kterou jsem se vydal a která se mi osvědčila, a to s plným vědomím a respektováním principu nezávislosti interního auditora.

A jaké jsou vaše zkušenosti s očekáváním managementu? Budu rád, pokud se o ně se mnou podělíte a zašlete mi své názory na petr.hadrava@metlife.cz nebo se zúčastníte diskuze v rámci skupiny Internal Audit Expectation Gap na www.linkedin.com.

**Ing. Martina Košťálová**
Ministerstvo financí, odbor Kontrola,
oddělení Centrální harmonizační jednotka

# NOVINKY Z KUCHYNĚ CHJ ANEB CO SE U NÁS ZASE UDÁLO…

Tak jako nám Šarlota se Zoe přichystaly hodinku nedělního času navíc, tak i já jsem vám přichystala silně zkondenzovaný výsledek naší metodické činnosti druhé poloviny tohoto roku. Co se legislativní činnosti týká, ta již není v rukou odboru Kontrola, teď bude záležet jen a jen na tom, jak se k ní postaví nová Poslanecká sněmovna.

„Tento Manuál poskytuje podrobnější návod k usměrnění a sjednocení postupů řídicích orgánů a jejich zprostředkujících subjektů“

Tentokrát se ve svém příspěvku zaměřím opět a zase na novinky z kuchyně CHJ. Tento pravidelný reporting naší činnosti vnímám jako přínosný a nezkreslený zdroj informací přímo od „tvůrce“. Dnešní článek rozdělím na dvě části a donutím vás zapojit obě vaše hemisféry, jednak tedy tu auditorskou, jednak tu kontrolorskou.

## MANUÁL K JEDNOTNÉMU POSTUPU PŘI VÝKONU INTERNÍHO AUDITU V ORGÁNECH VEŘEJNÉ SPRÁVY

V jaké fázi se nachází a v čem vidíme jeho přidanou hodnotu? V současné době je ve stadiu kompletace jednotlivých kapitol a brzy bude vpuštěn do závěrečného konzultačního procesu, kdy se k navržené metodice vyjádří auditorská veřejnost.

CHJ přistupovala k tvorbě samotného Manuálu s jedním společným cílem, tedy vytvořit jednotný a srozumitelný metodický rámec pro interní auditory veřejné správy, který bude sloužit k optimálnímu nastavení a zajištění fungování procesů činnosti IA v orgánech veřejné správy. Metodické přístupy procesu auditování v rámci specifických podmínek sdílené správy a řízení jednotlivých operačních programů spolufinancovaných z fondů Evropské unie a státního rozpočtu ČR zůstávají řešeny vlastní metodikou Auditního orgánu Ministerstva financí.

Neustálý vývoj a pokroky na poli IA nás na CHJ vedly k zamyšlení a zodpovězení těchto otázek, které jsme si při tvorbě Manuálu záměrně kladli. Ubrat na míře obecnosti a popustit uzdu praktickým doporučením? Bezpochyby. Účelem Manuálu je jednoznačně poskytnout podrobnější praktický návod pro aplikaci zásad, metod a postupů, které používá současný interní auditor při výkonu své činnosti. Tento Manuál podrobně, a s možností využití vzorových dokumentů činnosti IA, informuje o vlastním výkonu auditorské práce. Přílohy tvoří nezastupitelnou součást Manuálu, je na ně kladen velký důraz a tvoří přidanou hodnotu tím, že dokreslují praktické využití obsahu Manuálu. Oblast hodnocení kvality činnosti IA, resp. předmět interního i externího prověřování kvality práce auditorů, je s tímto Manuálem úzce propojena a mohu konstatovat, že využití vzorů dokumentace činnosti IA jednoznačně přispěje ke sjednocení postupů a výstupů z auditní činnosti, a povede tak ke zvýšení kvality interního auditu ve veřejné správě. Manuál pro IA spolu s přílohami obsahuje všechny klíčové aspekty a kritéria činnosti IA, a představuje tedy dostatečný základ pro následnou nezávislou validaci interního hodnocení kvality činnosti IA.

Obsah předkládaného Manuálu je rozdělen do 5 kapitol, které představují úzce propojené a spolu související celky a já alespoň přiblížím jádro každé z nich.

### Regulační rámec

Oblast regulace obecně definuje, jaké předpisy považují auditoři za klíčové a kterými se při výkonu své činnosti řídí, tj. příslušná legislativa České republiky a Evropské unie, Mezinárodní rámec profesní praxe IA, Statut IA, Manuál pro IA. U mezinárodního rámce profesní praxe IA se trochu pozastavujeme, opíráme se o jeho primární účel, co poskytuje, upevňuje, vytváří a vymezuje. Detailněji se zde zabýváme závaznými a důrazně doporučenými směrnicemi a jejich podskupinami.

### Osobnost auditora

Osobně považuji vlastnosti auditora za stěžejní východisko pro to, aby se systémy řízení ve všech organizacích úspěšně měnily k lepšímu. Obecně zaznamenáváme vzrůstající trend v kvalitě činnosti IA, způsob, jak audit funguje, pracuje a jak je vnímán, se výrazně blíží principu auditor = profesionální rádce, který při práci sbírá informace a poskytuje svá objektivní stanoviska a doporučení, dává věci do kontextu a nezávislé rady vás auditorů chtě nechtě hodnotu vašemu úřadu přidávají. Bez auditorů by bylo těžké manažerskou práci řádně vykonávat. Auditor chce a umí být užitečný, jen je však zapotřebí dát mu možnost využít jeho potenciál a know-how ukryté v tomto lidském kapitálu.

Co tedy vykresluje **odborný profil auditora?** Hlavně fakt, že přistupuje ke své práci otevřeně a se schopností navrhnout optimální řešení v auditovaných oblastech. Jsou na něho kladeny vysoké nároky, spojené především s jeho průběžným vzděláváním, odbornou kvalifikací, profesionální komunikací zahrnující rovněž diplomacii a etické jednání. Jsou-li zmíněné dovednosti auditorovou doménou, tak je více než pravděpodobné, že se projednávání auditorských zjištění či samotné zprávy z auditu obejde bez negativních emocí „dotčených" auditovaných subjektů. Nehledě na fakt, že dobrým marketingem zvyšují povědomí o přínosech IA. A co víc? Když svému vedení naservírujeme (ideálně v číslech), kde a jak přidáváme hodnotu organizaci, děláme reklamu své dobře vykonané práci.

Co definuje **statut IA** – účel, pravomoci, odpovědnosti, povinnosti a hlavní cíle IA, dále vymezuje charakter ujišťovacích a konzultačních činností, určuje postavení IA v rámci naší organizace a nastavuje vztahy mezi útvarem IA a auditovanými subjekty, mimo jiné odkazuje na Etický kodex interního auditora. Poslání interního auditora je zkrátka věcí cti a profesionality. Dodržování etiky je alfou a omegou činnosti interního auditora, která je ve své podstatě založena na důvěře vkládané vedením organizace do jeho objektivního ujišťování (pokud jde o řízení rizik, řídicí a kontrolní procesy a správu a řízení organizace). K tomu, aby tato důvěra mohla existovat, je nutné (a mělo by být samozřejmostí), aby interní auditor dodržoval etický kodex. **Etický kodex** auditora prohlubuje definici IA tím, že do ní zavádí 2 významné složky – principy, vztahující se k profesi a praxi interního auditu, a pravidla jednání, která napomáhají interpretovat výše zmíněné principy a tvoří návod k etickému chování a jednání.

I **odborná příprava** je velmi zásadním aspektem rozvoje každého z nás. Měla by být nepřetržitá a měla by dostatečně postihovat problematiku auditovaného oboru. Pro udržení svého vysokého standardu v rámci své profesní kvalifikace musí auditor využívat v co nejvíce možné míře možnosti sebevzdělávat se. Nemohu tedy nezmínit systém kontinuálního vzdělávání interních auditorů veřejné správy a pestrou paletu vzdělávacích aktivit ČIIA různého kalibru, často šitých na míru. Proto si zvyšujme odbornou kvalifikaci, vzdělávejme se, kde jen to jde, googlíkujme, mějme přehled, a tedy pořád co nabídnout.

### Typy a plánování auditů

Tato kapitola se prodírá definováním a ukázkami auditů demonstrativně uvedených v zákoně o finanční kontrole (finanční audit, audit systémů, audit výkonu) a řadou dalších typů, jako je např. audit shody či audit informačních technologií.

Proces objektivního zhodnocení rizik tvoří bezpochyby základní platformu pro plánování auditů. Rizika a jejich hodnocení vyplývají ze stanovených úkolů organizace s přihlédnutím k výsledku kontrolní činnosti externích kontrolních orgánů, ke zjištění vnitřního řídicího a kontrolního systému a k zajištění následné kontroly opatření přijatých příslušnými vedoucími zaměstnanci na základě oznámených zjištění a doporučení z předchozích auditů.

Střednědobé plány zohledňují cíle a záměry organizace stanovené v dlouhodobé strategii, výsledky analýzy rizik a priority stanovené vedením. Specifické krátkodobé cíle interního auditu jsou obsaženy v ročním plánu auditu vycházející ze střednědobého plánu auditu. Na praktických příkladech následně demonstrujeme výpočty a odhady vhodných zdrojů nezbytných pro uskutečnění interního auditu z hlediska časové a lidské náročnosti.

### Průběh auditů

Tato kapitola je dle mého názoru step-by-step screeningem toho, jak by proces našeho auditování měl správně vypadat. Jsou zde uvedeny informace o činnostech vykonávaných v období od vydání pověření k výkonu auditu až po uzavření spisu, o auditním týmu a používaných dokumentech.

Nastavení postupů pro výkon interního auditu, které budou v souladu s právními normami, vnitřními normami konkrétního orgánu veřejné správy i mezinárodním rámcem profesní praxe IA, je startovací platformou celého budoucího procesu auditování. Kdo a jak stanoví postupy pro výkon auditu? Orgán veřejné správy ve svém vnitřním předpisu. Následuje zahájení auditu a odpovědnost za jeho provedení. Jaké dokumenty si v úvodní části jistě předpřipravit: čestné prohlášení o nepodjatosti, program auditu, oznámení o zahájení, záznam o zahájení auditu, poučení auditované osoby, a hlavně kontrolní listy. Právě ty jsou po vyplnění naším písemným záznamem provedeného šetření a spolu s důkazními materiály též podkladem pro psaní zprávy. Pak přichází samotné auditní šetření a jeho detailní průběh. Opět zde musím vyzdvihnout skutečnost, že průběh auditu může značně ovlivnit auditor svým chováním, svými organizačními a vyjednávacími schopnostmi. U zprávy z auditu mějme na paměti, že se jedná o jediný oficiální výstup, který z útvaru IA jde, takže se zaměřme na typy, rady a doporučení, jak psát a jak raději nepsat. Pokud podlehneme pokušení předvádět našemu vedení, co všechno jsme zjistili a odhalili, moc přátel si neuděláme a věci samotné také moc neprospějeme. Rozlišujme proto věci podstatné od zjištění drobných nedostatků.

Pro mnohé z vás není výstupem z auditní činnosti samotná zpráva z auditu, ale to, jakým způsobem je s jejími zjištěními naloženo. Odpovědnost za plnění opatření

## „Tento Manuál podrobně, a s možností využití vzorových dokumentů činnosti IA, informuje o vlastním výkonu auditorské práce"

Národní konference ČIIA – Užitečnost interního auditu aneb audit ve všech barvách; říjen 2013

k nápravě zjištěných nedostatků a za riziko vyplývající z nepřijetí či odložení realizace doporučení daných v závěrečné zprávě z auditu nese vedoucí auditované osoby.

### Výběr vzorku

Tato část Manuálu je základním doporučením určeným zejména těm zaměstnancům, kteří řídí, organizují a vykonávají kontrolu a interní audit v orgánu veřejné správy, neboť je zcela na místě, aby, kromě znalosti procesů a dat, se kterými pracují, porozuměli také postupům a standardům pro výběr vzorku a dokázali je využít ve své praktické činnosti.

Účelem této části Manuálu je poskytnout přehled hlavních pojmů, zásad a statistických a nestatistických metod výběru vzorku a na spoustě praktických příkladů demonstrovat jejich využití při výkonu kontroly a interního auditu. Dokázat si odpovědět na otázku, jak vůbec interpretovat primární data a výsledky, ke kterým se dopracujeme. Šlo nám jednoduše o to, dostat do textu Manuálu to nejpraktičtější, co by mohli běžní auditoři využít a podle čeho nejčastěji vzorek vybrat. Milovníkům statistiky je určena i rozsáhlá příloha, která doplňuje vybrané pasáže, a dotváří tak komplexní pohled na oblast vzorkování, jejích metod a celkové extrapolace.

## METODICKÝ POKYN PRO NASTAVENÍ A VÝKON KONTROL V ODPOVĚDNOSTI ŘÍDICÍCH ORGÁNŮ PŘI IMPLEMENTACI FONDŮ SPOLEČNÉHO STRATEGICKÉHO RÁMCE PRO PROGRAMOVÉ OBDOBÍ 2014–2020

Žhavou novinkou na scéně metodiky je právě tento materiál. Iniciativa vzešla z Akčního plánu pro implementaci Strategie pro boj s podvody a korupcí v rámci čerpání fondů společného strategického rámce v období 2014–2020 a také ze snahy využít zkušeností z programového období 2007–2013, zabránit zneužití prostředků poskytnutých z fondů EU, předcházet dopadům a minimalizovat dopady takových jednání. Právě promítnutím strategických dokumentů zajišťuje nastavení takových pravidel čerpání podpory z fondů EU, které v sobě budou mít zabudovány prvky zamezující podvodnému a korupčnímu jednání. Tento metodický pokyn je součástí metodického balíčku všech metodických dokumentů, jejichž prostřednictvím je naplňována koncepce jednotného metodického prostředí.

Hlavním cílem metodického pokynu je nastavit systém kontrol u řídicích orgánů tak, aby zaprvé nezatěžoval a aby zajistil dostatečnou míru ujištění, že výdaje a operace byly vynaloženy a provedeny v souladu s pravidly. Tento Manuál poskytuje podrobnější návod k usměrnění a sjednocení postupů řídicích orgánů a jejich zprostředkujících subjektů při provádění administrativních ověřování a kontrol na místě u žadatele/příjemce, který získá dotaci v programovém období 2014+, a jak aktivně bojovat s možným podvodným jednáním.

### Struktura

Jako obvykle zde věnujeme úvodní kapitolu pojmosloví, aby došlo k synchronizaci terminologie nového programového období ve všech metodických dokumentech. Následuje obecné zasazení systému kontrol v rámci vnitřního řídicího a kontrolního systému veřejné správy. Rozlišení typů a fází kontrol z hlediska charakteru, zaměření a časové souslednosti. Jak provádět administrativní ověřování a kontrolu na místě ve všech fázích projektového cyklu, zejména s důrazem na kontrolu ex-ante před uzavřením právního aktu o poskytnutí podpory až do finančního vypořádání a po dobu udržitelnosti, je věnována dostatečná pozornost. Přílohy (vzory, kontrolní listy) jsou zaměřeny především na aktuálnost, praktičnost a optimální rozsah (vzhledem k administrativní náročnosti a kapacitám řídicích orgánů). Bude se jednat o indikativní vzory, které je nutno pro účely kontroly upravit dle specifických podmínek daného operačního programu.

**Elektronizace** kontrolního procesu se nově prolíná obsahem celého metodického pokynu, a tudíž velkou pozornost věnujeme Monitorovacímu systému strukturálních fondů období 2014–2020. Oficiálně by aplikace MS2014+ měla být základním nástrojem pro monitorování využívání finanční pomoci z fondů Evropské unie v programovém období 2014–2020. Tato aplikace bude sloužit orgánům státní správy, samosprávy, jejich příspěvkovým organizacím a dalším subjektům zapojeným do přípravy, administrace, hodnocení a kontrolování poskytování finančních prostředků z fondů Evropské unie. Aplikace bude sloužit uživatelům, jako jsou žadatelé/příjemci podpory, tak pracovníci kontroly na příslušných řídicích orgánech, zprostředkujících subjektech a dále pak NOKu, Auditnímu orgánu, Platebnímu a certifikačnímu orgánu a další části MF. V tomto programovém období je informačních systémů zajišťujících tuto agendu více (např.: pro žadatele Benefit7+, pro ŘO/ZS Monit7+,

centrálním modulem je pak MSC2007), v budoucím programovém období bude pouze jeden informační systém.

**Administrativní ověřování** spočívá v ověřování dokladů a dokumentů předložených žadatelem/příjemcem při příjmu projektu, při kontrole zadávacího řízení, při příjmu žádosti o platbu či při předložení oznámení o změně v projektu.


Národní konference ČIIA – Užitečnost interního auditu aneb audit ve všech barvách; říjen 2013
Miroslav Matej, Ministerstvo financí ČR

Obsahem této kapitoly jsou informace týkající se administrativního ověřování realizace projektů, které průběžně vykonává řídicí orgán v době při příjmu projektů, jejich realizaci a udržitelnosti, neboť řídicí orgán má odpovědnost za to, že projekty, na jejichž realizaci je přidělena finanční podpora, jsou schváleny a realizovány v souladu s platnými právními předpisy EU a ČR a podle kritérií stanovených v rámci pravidel konkrétního operačního programu.

Řídicí orgán ve výzvě k předkládání žádostí o přiznání finanční podpory stanoví, které dokumenty musí žadatel v žádosti předložit, aby na základě jejich posouzení bylo možné rozhodnout, zda danému projektu lze přiznat finanční podporu. V souladu se zákonem o finanční kontrole provede poskytovatel před schválením přidělení finanční podpory ověření všech dokumentů, které předložil žadatel v žádosti o finanční podporu na základě vyhlášené výzvy. Poskytovatel následně ověří, zda žádost o podporu je zpracována v souladu s podmínkami operačního programu, zda žadatel předložil všechny požadované dokumenty, zda je projekt v souladu s právními předpisy a s operačním programem, a následně na základě předem stanovených hodnoticích kritérií rozhodne, zda projektu bude, či nebude přiznána finanční podpora.

Pro úspěšnou realizaci projektů je důležité, aby zaměstnanci vykonávající administrativní ověřování měli takové znalosti, že jsou schopni příjemcům finanční podpory poskytovat metodickou podporu a zjistit případné chyby, jichž se příjemci při realizaci projektů dopustí, a tím zajistit, že budou příjemcům proplaceny pouze způsobilé výdaje. Z uvedených důvodů je důležité, aby tito zaměstnanci dobře znali pravidla operačního programu a současně uměli správně aplikovat právní předpisy vztahující se k projektům. Správnost realizace projektů ovlivňuje poskytovatel vydáváním správných a jednoznačných pokynů a informací příjemcům.

**Kontrola na místě** spočívá v kontrole realizace projektu a porovnává skutečný stav projektu se stavem deklarovaným. Také kontrola na místě se zabývá kontrolou dokladů. Kapitola je strukturována do základních oblastí, které rámcově pokrývají celý průběh kontrolních činností v rámci procesu kontroly na místě, a to optikou nového kontrolního řádu 255/2012 Sb.: tedy plánování a výběr projektů ke kontrole na místě, příprava a výkon kontroly na místě, návrhy vzorových kontrolních listů pro kontrolu na místě, vyhodnocení výsledků kontrol, postupy při zjištění nedostatků a realizace nápravných opatření. Lze popřípadě doplnit i postup při námitkovém řízení, vypořádání námitek proti protokolu z kontroly apod.

Plánování kontrol a tvorba ročního plánu kontrol je v gesci řídicího orgánu, vytváří jej pracovník v oblasti kontroly s příslušnou rolí a všichni pracovníci ŘO/ZS podle něj budou postupovat. Roční plán kontrol bude zahrnovat rozpis plánovaných kontrol, včetně jejich popisu a cílů ve strukturované podobě. Do ročního plánu kontrol bude možné zahrnout další aktuální kontroly nad rámec schváleného ročního plánu kontrol. Analýza rizikovosti projektů vstupuje do generování projektu ke kontrolám a výběru vzorku projektů ke kontrole. Vzorek se může zaměřit na operace o vysoké finanční hodnotě nebo na operace, u nichž byly v minulosti zjištěny problémy či nesrovnalosti nebo u nichž byly při správním ověřování zjištěny určité transakce, které vypadají nezvykle a vyžadují další přezkoumání. Jako doplňující či alternativní postup lze použít výběr náhodného vzorku.

MS2014+ umožní příslušnému pracovníkovi ŘO/ZS podle předem nastavených kritérií automaticky generovat vzorek projektů ke kontrolám na místě. Výhodou tohoto přístupu je zamezení subjektivního ovlivňování výběru projektů ke kontrole. ŘO/ZS bude moci podle předem daných pravidel rozšiřovat seznam projektů ke kontrolám nad rámec vzorků projektů automaticky vygenerovaných IS.

## MANUÁL K JEDNOTNÉMU POSTUPU PŘI HODNOCENÍ KVALITY AUDITNÍ ČINNOSTI ZAJIŠŤOVANÉ ÚTVARY INTERNÍHO AUDITU V ORGÁNECH VEŘEJNÉ SPRÁVY

Výhledově tj. odhadem koncem roku / počátkem roku nového proběhne kompletní aktualizace Manuálu k jednotnému postupu při hodnocení kvality auditní činnosti. Jeho kompletní repasování bude reagovat jednak na změny ve standardech IIA, které se dotýkají samotného textu, a jednak na diskutované impulzy vedoucí k jeho zpraktičtění a lepšímu uchopení. Zapracujeme konstruktivní připomínky využitelné v praxi, které přispějí k lepší aplikaci postupů a metod do prostředí interního auditu v orgánech veřejné správy.

## ZÁVĚR PRO TRPĚLIVÉHO ČTENÁŘE

Kdo z vás nabyl dojmu, že událostí na poli CHJ se činí požehnaně, tak s ním nemohu nesouhlasit. Jak můžete sami posoudit, nezahálíme a bojujeme na všech frontách :))

Těm z vás, kteří vydrželi až do konce, malá poznámka na závěr, kterou si nemohu nechat pro sebe: podzimní konference ČIIA ukázala, že kráčíte správným směrem, rekognoskujete a vnímáte trendy, kterými vaše auditorské poslání prochází, vybíráte z nich vše pozitivní, co ve své profesi bez porušení svých morálních zásad dokážete uplatnit. A hlavně se nenecháte otrávit méně schopnými.

Klid, mír a vše dobré v novém roce přeje a na případnou polemiku se těší Martina.Kostalova@mfcr.cz.

**Ing. Petr Kheil**
Česká spořitelna, a.s.,
Metodika interního auditu, řídicího a kontrolního systému, včetně jeho vyhodnocování

# ČEHO SI PETR POVŠIML
## (nejen) v legislativě

**Vzhledem k tomu, že v poslední době je situace v oblasti nově publikovaných best practice nebo regulatorních norem klidná, pojďme nahlédnout na to, co by interním auditorům nemělo uniknout v nadcházejícím období.**

*Jak jsem již informoval, mezi publikovanými návrhy na změny v české legislativě je, od poloviny června, k dispozici* ***návrh zákona, kterým se mění zákon č. 93/2009 Sb., o auditorech****. Tento návrh reaguje na přijetí právních předpisů jak z EU, tak z českého prostředí. Mezi změnami jsem postřehl zrušení zákonného vymezení výboru pro audit jako orgánu společnosti, požadavek na nezávislost a odbornost většiny členů výboru pro audit a úpravu rozsahu působnosti výboru pro audit.*

*V oblasti finančních trhů dojde ke změně zákonů v souvislosti se stanovením přístupu* ***k činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry a dohledu nad nimi.*** *Tato změna navazuje na koncept kapitálových požadavků tzv. CRD IV / CRR* ***(Nařízení EU č. 575/2013 a Směrnice č. 2013/36 EU k obezřetnostním požadavkům na úvěrové instituce a investiční podniky)****. Konkrétní požadavky budou provedeny tzv.* ***obezřetnostní vyhláškou****, jejímž těžištěm je, mimo jiné, úprava oblasti řídicího a kontrolního systému. V souvislosti s nabytím účinnosti této vyhlášky dojde ke zrušení dosud platné vyhlášky č. 123/2007 Sb., o pravidlech obezřetného podnikání bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry.*

Ing. Šárka Nováková
Všeobecná fakultní nemocnice v Praze

# MÁME ČÍM SE POCHLUBIT
## aneb činnost Sekce veřejné správy ČIIA

Milí čtenáři, když jsem přemýšlela, jak vás hned prvním odstavcem zaujmout a neodradit od čtení dalšího textu, rozhodla jsem se podělit se s vámi o pocity, které mě inspirovaly k napsání tohoto článku.

Ať už si to přiznáme, nebo ne, interní audit ve veřejné správě má svá specifika a nepřekročitelné mantinely. Pro nás, interní auditory z veřejné správy, je alfou a omegou všech v praxi prováděných činností zákon o finanční kontrole a musíme ho ctít bez ohledu na to, jestli působíme ve státní správě, místní samosprávě nebo v příspěvkové organizaci. Stejná pravidla platí pro mě, která provádím interní audity v jedné z největších fakultních nemocnic v ČR, a stejná např. pro šéfa auditu na státní vysoké škole nebo na ministerstvu.

> „Interní audit ve veřejné správě má svá specifika a nepřekročitelné mantinely“

Ani nevím, co přesně ho k tomu vedlo, ale na minulém jednání Výboru sekce veřejné správy shrnul jeho předseda František Beckert v krátké prezentaci to, co jsme společně od září 2010 dokázali, a všem nám za to poděkoval. Hm, řekne si možná někdo z vás. Mě ale v té chvíli napadlo nejen to, že je František fajn chlap a ví, co se sluší, ale i to, že máme být na co pyšní, že odvádíme dobrou práci a že nastal čas se tím i pochlubit a víc se zviditelnit.

A protože vlastně všichni usilujeme o totéž, máme stejné cíle a řešíme podobné problémy, máme zcela pochopitelnou potřebu výměny zkušeností, vzájemného kontaktu a sdílení tzv. dobré praxe.

Členství v ČIIA a aktivní zapojení do činnosti Sekce veřejné správy ČIIA považuji v tomto směru za ideální.

Sekce veřejné správy ČIIA (SVS), jejímž koordinačním orgánem je Výbor SVS, vznikla v září 2010 a od té doby funguje v téměř nezměněném personálním složení až dodnes. Součástí SVS jsou odborné komise zaměřené např. na primární a sekundární systém dohledu, hodnocení kvality interního auditu ve veřejné správě nebo na certifikaci auditorů ve veřejné správě. Další nedílnou součástí SVS jsou zástupci tzv. komunit, reprezentující různé orgány státní správy a samosprávy, jednotlivé regiony ČR, školství, zdravotnictví atp.

V současné době má Výbor SVS 11 členů, jednání Výboru SVS se však pravidelně účastní i cca 8 stálých hostů. Většina členů Výboru SVS má i své náhradníky, kteří je zastupují, nemohou-li se některého jednání zúčastnit osobně. Jednání Výboru SVS se koná zpravidla 1x měsíčně, členové jednotlivých komisí jsou v kontaktu i častěji.

Činnost SVS se řídí dokumenty schválenými Sněmem ČIIA a Radou ČIIA, nicméně detaily vás zde nebudu zatěžovat, protože jsou dostupné na webových stránkách ČIIA. Co bych však ráda uvedla a nejlépe i dvakrát podtrhla, je skutečnost, že výkon veškerých aktivit v rámci SVS a jejích komisích je dobrovolný a nezištný. Věděli jste to?

Smekám před kolegy, kteří neváhají ve svém volném čase přiložit ruku k dílu nebo vyrazit ze všech koutů republiky na pražské Karlovo náměstí věnovat svůj čas a úsilí našim společným aktivitám zaměřeným na podporu interního auditu ve veřejné správě.

Za ty téměř tři roky společné práce jsme se poznali natolik, že si můžeme dovolit být k sobě otevření a maximálně upřímní. A i když se někdy názorově rozcházíme, věcná diskuze rozšiřuje naše obzory, je přínosná a posiluje nás na cestě ke splnění našich společných cílů.

Workshop ČIIA – Aktuální paragrafy pro interní audit a finanční řízení; Pardubice 2013
František Beckert, člen Rady ČIIA a předseda Výboru Sekce veřejné správy

Aktivity SVS jsou orientovány na potřeby interních auditorů působících ve všech typech a úrovních orgánů veřejné správy, a to bez ohledu na to, zda se jedná o členy ČIIA.

*A čím že se to vlastně chceme chlubit?*

Pořádáme kulaté stoly SVS ČIIA (nejen v Praze, ale např. i v Ostravě nebo v Kutné Hoře), zveme auditory z veřejné správy na různě zaměřená klubová odpoledne (např. o efektivním řízení výdajů poskytnutých ze zdrojů EU), nabízíme širokou nabídku zajímavých seminářů (např. o finanční kontrole ve veřejné správě, mezinárodní dobré praxi a slabých místech v ČR atp.).

Podílíme se na zprostředkování efektivní výměny zkušeností formou pořádání tematických workshopů (opět nejen v Praze, ale i v Olomouci, Karlových Varech, Liberci, v Jihlavě nebo v Pardubicích), pořádáme formální i neformální setkání interních auditorů z veřejné správy v rámci jednotlivých komunit (regiony, katastrální úřady, zdravotnictví…).

Workshop ČIIA – Aktuální paragrafy pro interní audit a finanční řízení; Pardubice 2013

## „Máme potřebu výměny zkušeností, vzájemného kontaktu a sdílení tzv. dobré praxe“

V rámci jednotného systému odborné přípravy pracovníků veřejné správy v oboru finanční kontrola a interní audit organizujeme základní kurz akreditovaný Ministerstvem vnitra, který má rozsah 80 vyučovacích hodin a už se ho zúčastnilo více než 280 auditorů.

Rozšířili jsme nabídku atestačních kurzů (např. o program zabezpečení a zvyšování kvality interního auditu ve veřejné správě nebo audit klíčových oblastí veřejné správy).

Auditorům z veřejné správy nabízíme řadu zajímavých kurzů zaměřených například na audit strukturálních fondů EU, audit informačních systémů ve veřejné správě, audit rozpočtu, audit účetní závěrky atp.

Zavedli jsme čtyřstupňový systém certifikace interních auditorů ve veřejné správě (už nás je 200 a zájem o certifikaci sílí mezi asistenty, juniory, seniory i experty/konzultanty), propagujeme tzv. dobrou praxi v interním auditu ve veřejné správě mezi interními auditory a odbornou veřejností (časopis Interní auditor, Veřejná správa atp.), prezentujeme a prosazujeme dodržování mezinárodních standardů pro profesní praxi interního auditu v podmínkách veřejné správy.

## „Aktivity SVS jsou orientovány na potřeby interních auditorů působících ve všech typech a úrovních orgánů veřejné správy“

Aktivně se zapojujeme do připomínkování legislativy v oblasti finanční kontroly a interního auditu, navázali jsme úzkou spolupráci s Ministerstvem financí v oblasti centrální harmonizace finanční kontroly a interního auditu ve veřejné správě, s Ministerstvem pro místní rozvoj a Ministerstvem vnitra (zejména v oblasti vzdělávání). Pro interní auditory z veřejné správy vydáváme kvalitní odborné publikace.

Auditoři z veřejné správy jsou zastoupeni ve všech klíčových orgánech ČIIA (Rada ČIIA, Kontrolní komise, Redakční rada).

Tak a teď už o SVS víte všechno podstatné. Jestli jste opravdu dočetli až sem (přeskočení pro vás nudných pasáží vám budiž odpuštěno), jste členy ČIIA, působíte jako vedoucí útvaru interního auditu ve veřejné správě a máte chuť rozšířit naše řady, ozvěte se, neváhejte a přijďte mezi nás. Věřím, že nebudete litovat a vaše zapojení do práce v Sekci veřejné správy ČIIA bude oboustranně přínosné.

A ještě něco: máte-li při své práci interního auditora ve veřejné správě nějaké konkrétní pracovní starosti, je před vámi úkol, se kterým si tak úplně nevíte rady nebo pochybujete, jestli jeho splněním v pozici interního auditora můžete být pověřeni, neváhejte a obraťte se na nás. Všichni máme bohaté zkušenosti z praxe, víc hlav víc ví, a to by v tom byl čert, abychom společně nenašli řešení.

**Ivana Krůželová**
Expert v oblasti kohezní politiky
působící v Londýně, Velká Británie

# JAK SI (ne)NASTAVIT OPERAČNÍ PROGRAM

Zase jsme na začátku, i když starší, strukturálně moudřejší, a ještě o kousek ostrouhanější než minule. Zase to zkusíme dát na jednu, tu první, implementační dobrou, než si do toho (zase) lehne nějaký politický hroch bez zkušeností, s elánem a vizí, která vypadla z tramvaje. Podívejme se tedy na to, co se dá už na začátku nastavit „úplně blbě“, aby to pak celé fungovalo buď o mnoho pomaleji, nebo vůbec.

Řídicí orgán tedy rozhodl uzavřít tzv. Akční partnerské dohody s obcemi a regiony, které tak samy implementovaly části operačních programů výměnou za více méně potvrzenou část alokace. Vycházelo se z předpokladu, že když byla kontrola veřejných financí v pořádku pro domácí zdroje (tedy například ty obecní), bude i pro evropské. Audit EK však konstatoval nedostatečné pokrytí na úrovni kontrol podle čl. 13 i čl. 16

## „Státní úředníci sice nebojují s politickým vlivem ve smyslu korupce a lobbyingu“

Odmyslíme-li tak neuchopitelný a nekontrolovatelný faktor, jako je nebohý příjemce v programu, měl by se řídicí orgán soustředit na 3 podstatné oblasti. Implementační strukturu, kontroly podle článku 4 (2004–2006), 13 (2007–2013) a nastavení auditu ze strany členské země podle článku 10 (2004–2006) a 16 (2007–2013). Všechno ostatní je v podstatě realizační život sám, lidi mohu školit průběžně, zakázky kontrolovat důsledněji, výzvy opakovat, příjemce nechat napospas vlastním dovednostem a vždycky to nějak dopadne. Pokud ale „zmastím“ implementační strukturu, nikdy nedosáhnu plynulého čerpání, a pokud nenastavím správně vzorky kontrol, na což se pak ani při auditu nepřijde, bůh se mnou, protože pak mám najisto zastavený program a finanční korekce.

V Británii mají zkušenost s tím, jak spolu tyto tři pilíře souvisejí. Státní úředníci sice nebojují s politickým vlivem ve smyslu korupce a lobbyingu, ale ve smyslu snižování stavů. V programovém období 2000–2006 byly programy implementovány Ministerstvem místních samospráv s regionálními kancelářemi, a hlavně limitovaným počtem zdrojů.

a řídicí orgán to stálo 25 milionů EUR. Management řídicího orgánu se tedy poroučel. Vláda se pak rozhodla ustavit regionální rozvojové agentury, které budou fungovat mimo jiné jako zprostředkující subjekt a příjemce pro programové období 2007–2013. Takže se část kompetencí začala přesouvat na tyto agentury už v období 2000–2006.

## „Audit EK konstatoval nedostatečné pokrytí na úrovni kontrol“

Aby to bylo ještě zajímavější, v roce 2010 tyto regionální rozvojové agentury (zase pod heslem úspory státních výdajů) vláda Davida Camerona zrušila a ustanovila jakési skupinky regionálních partnerství (které nemají ani rozpočet ani zkušenost s čerpáním). Nastal tedy problém se spolufinancováním, problém s absorpční kapacitou, a hlavně problém co tedy s neexistujícím zprostředkujícím subjektem.

Odpovědnost za implementaci přešla kompletně do rukou Ministerstva místních samospráv, které bylo ale původně mimo jiné odpovědné i za kontroly podle článku 16. Tedy auditu systému. A znovu stejný problém. Tady je zajímavé, jak změnu implementační struktury jako takové EK, tedy DG Regio, nijak nezpochybnila (luxus, který si ČR pořád ještě dopřát nemůže). Pro auditory EK a EUD však nastala nepřehledná situace v oddělení kompetencí, pochopitelně nedostatek personálních zdrojů pro kontroly jak podle čl. 13, tak následně čl. 16. Navíc vzhledem k přesunu všech doprovodných materiálů z regionů do Londýna, propouštění pracovníků, kteří měli zkušenost, a hlavně paměť jednotlivých procesů byly prováděné audity EK mnohem obtížnější, a došlo tedy OPĚT na zastavení programu a očekávané korekce.

Jak si ustelu, tak si lehnu a pro implementační program to tedy platí rozhodně. Pokud se NEPODAŘÍ nastavit přehlednou, uříditelnou a efektivní implementační strukturu (a ještě ji takhle přehlednou udržet po celé programové období), která mi umožní provádět pravidelné kontroly na dostatečném vzorku, a pokud je mám, v následném auditu systému odhalit nedostatky této struktury, jsem v pořádném auditním a čerpacím loji a zase to bude stát daňové poplatníky spoustu peněz na korekcích, neproplacených projektech, nových volbách, nově nastavených strukturách ministerstev a snech a iluzích o prosperitě a ekonomickém rozvoji, Evropské unii a vůbec...

**Ing. Josef Vincenec**
vedoucí oddělení interního auditu
Krajský úřad Libereckého kraje

# ZPRAVODAJSTVÍ Z DOMOVA (auditorů) I ZE SVĚTA (zvířat)

## aneb národní konference ČIIA v centru Moravy

Ve dnech 16. a 17. října se stalo překrásné moravské město Olomouc domovem pro více než 150 interních auditorů. Sešli se zde na své pravidelné podzimní Národní konferenci ČIIA. Letošní rokování bylo v mnoha ohledech rozdílné. Začalo to už příjezdem. Řada účastníků ze střední a západní části republiky využila služeb oficiálního dopravce, Českých drah, a přijela z Prahy společně konferenčním vlakem. Čas strávený s kolegy se dal už při cestě využít k pracovním schůzkám i k neformálním diskuzím. To byla první, pozitivní změna. Atmosféru domova vytvořilo příjemné prostředí nově zrekonstruovaného hotelového komplexu Clarion. Pocit domova však navodilo především přijetí místních organizátorů. Moravská srdečnost, hanácká bodrost a rodičovská starostlivost byly všudypřítomné. Bylo to patrné i z úvodního projevu ředitele Krajského úřadu Olomouckého kraje pana Libora Koláře. Pan ředitel mnohé překvapil svým zasvěceným hodnocením poslání interního auditu. V tomto úřadě jsou služby interního auditu velmi cíleně využívány a přispívají ke zvyšování efektivity. Zcela nový pohled na realitu přineslo vystoupení dalšího zástupce místních hostitelů. Dveře do jiného světa, světa zvířat, nám pootevřel pan Radomír Habáň, ředitel Zoologické zahrady Olomouc. Pod jeho záštitou se konference konala. I z jeho několika úvodních vět si mohl člověk uvědomit, že nad profesními standardy, legislativou a zavedenými pracovními postupy jsou ještě jiné zákonitosti, vyšší a neoblomné, zákony přírody. Je to svět, který má svůj řád, obejde se bez manažerů i bez auditorů. Je to svět spravedlivý, přímý, postavený na logice, a přitom krásný. Ostatně o tom, jak zvířata vstoupila v Olomouci do života auditorů, bude ještě zmínka.

Zásadní změna, která odlišovala letošní konferenci od všech předešlých, byla možnost všech účastníků aktivně ovlivnit program dlouho před vlastním jednáním. Na webových stránkách konference byla k dispozici anketa o preferovaných tématech i o možných hostech, o vystupujících. Tímto způsobem bylo vybráno 5 témat pro diskuzní kroužky. Požadavky uvedené v anketě ovlivnily také výběr přednášejících.

Novým formátem byla také panelová diskuze na téma Užitečnost a hodnota interního auditu očima bývalých interních auditorů, nyní manažerů. Zaznamenala velký ohlas. Částečně se podařilo splnit přání účastníků internetové ankety a zajistit některé z požadovaných hostů. Podělit se o své zkušenosti přišli: Jana Báčová (ředitelka sekce peněžního a platebního styku ČNB), Marie Bílková (Generální ředitelka Úřadu práce ČR), Eva Janoušková (ředitelka Sekce ekonomiky a podpory Krajského úřadu Kraje Vysočina), Petr Kusebauch (vedoucí odboru prodej tepla v Pražské teplárenské a.s.) a Pavel Vácha (National Security Manager ve společnosti Provident Finacial).

Je třeba zmínit také tematické spektrum dvoudenního jednání. Mottem celé konference byla „Užitečnost interního auditu aneb audit ve všech barvách“. S uspokojením lze konstatovat, že pokud nebyly prezentovány všechny položky duhové palety, pak určitě alespoň ty nejzářivější. Téměř jako kontrast černé a bílé vyzněly diskuze a odborné spory o inovativní přístup k profesi, tzv. audit 2.0 (na konferenci označovaný také jako audit plus). Základem pro živou výměnu názorů byla vystoupení Tomáše Pivoňky s názvem „Přijdu, až nastaví zrcadlo“. Josef Severa, také zástupce společnosti EY, doplnil představu o nové roli auditu v příspěvku s lakonickým názvem „IA 2.0.“ Další zkušenosti z praxe v tuzemsku i v zahraniční přinesl Ivan Foltman (Deloitte). Ve svém příspěvku s názvem „Užitečnost a hodnota interního auditu“ mimo jiné kategorizoval interní audit do tří skupin: historický – mainstreamový – interní audit zítřka. V těchto třech úrovních by se mohla proměňovat zodpovědnost interního auditu, jeho zaměření, perspektiva, cíle i nástroje. Velkým polínkem, které rozpálilo plamen pod kotlem polemik o auditu plus, bylo impulzivní vystoupení Karla Vabrouška ze společnosti Agrofert. Miroslav Mencl ze společnosti Absolook už názvem svého příspěvku „Interní audit 2.0 – evoluce revolucí?“ podpořil myšlenku změnit stávající roli interního auditu. K tématu „Marketing profese interního auditu“ vystoupili také Pavel Racocha z Komerční banky a Ivo Středa ze společnosti RWE. Kdo z nás, interních auditorů, se nikdy nesetkal s úkolem nebo činností, která nepatří přímo do jeho pracovní náplně? Každý má své zkušenosti. Někdy výkon neauditních činností hraničí s porušením zásady objektivity a nezávislosti. O svých vlastních zkušenostech hovořil Petr Kubík ze společnosti T-Mobile Czech Republic a Josef Vincenec z Krajského úřadu Libereckého kraje.

Letošní rokování auditorů mělo ještě jednu zvláštnost, kterou se odlišovalo od jiných konferencí. Již v úvodu jsem zmínil souvislost s jiným světem, světem zvířat. Kromě záštity, kterou nám poskytl ředitel

Národní konference ČIIA – Užitečnost interního auditu aneb audit ve všech barvách; říjen 2013


Národní konference ČIIA – Užitečnost interního auditu aneb audit ve všech barvách; říjen 2013. Josef Vincenec, Krajský úřad Libereckého kraje

olomoucké ZOO, jsme byli ve virtuálním, myšlenkovém spojení se třemi zástupci živočišné říše. Uvažovali jsme, které zvíře je nám nejbližší, osobně i profesně. Které zvíře si zaslouží naši morální, ale především hmotnou podporu, vyjádřenou finančním příspěvkem na péči o ně v následujícím roce. Přemítali jsme, zda je nám blízký lev berberský. Je podobný internímu auditorovi tím, že je velký, silný, spravedlivý a vždy je králem situace? Ale pozor, ve volné přírodě již zcela vyhynul. Všichni potomci původního prapředka pocházejí z chovu marockého krále. Chceme být i my uměle udržovaným profesním druhem? Nehrozí nám v takovém případě ztráta kontaktu s realitou? Druhým kandidátem byl ibis skalní. Středně velký pták, který patří do kategorie kriticky ohrožených druhů. Počet jedinců žijící ve volné přírodě se odhaduje na 500. Důvody, které vedou k dlouhodobému snižování početních stavů, jsou především ztráta přirozeného prostředí, otrava pesticidy a početné lovy. Jaká podobnost s životem interního auditora! Často jsme nuceni se pohybovat v prostředí a plnit úkoly, které jsou velmi vzdáleny vodám auditorským. Někdy se nacházíme v útvarech, které nefungují přirozeně a efektivně. Identifikovat rizika a poukazovat na nezdravá, jedovatá místa, to se od nás také očekává. Posledním zvířetem, které se ucházelo o přízeň auditorů, je surikata. Je to malé, asi třiceticentimetrové zvířátko, žijící v savanách a polopouštích. Je to tvor společenský, žije v třicetičlenné kolonii v podzemních norách. Skupinu vede dominantní pár. Ve chvílích, kdy většina členů rodiny hledá potravu, někteří jedinci z kolonie jsou pověřeni hlídkováním. Jsou známé svým bleskurychlým otáčením hlavy a monitorováním širokého okolí. Mají velmi dobře vyvinutý systém varovných signálů. Surikata dobře vidí do dálky. Živí se kořínky a cibulkami malých rostlin. Loví drobné obratlovce, ale také hmyz, termity, sarančata, kobylky, pavouky a štíry. Jsou proti jejich jedu imunní. Že je vám charakteristika surikat povědomá? Není divu. Převeďte si jejich život do prostředí lidí. V tu chvíli je před vámi parta sehraných odborníků. Má jednoznačně definovanou organizační strukturu s jedním vedoucím. Dokáží se bleskově orientovat, jsou vnímaví a umí spolupracovat. Funguje u nich téměř bezchybný řídicí a kontrolní systém. V případě napadení jsou imunní vůči nezdravým jevům. O našem chráněnci nakonec rozhodlo hlasování v sále. Největší přízeň získala právě surikata, o několik hlasů méně dostal lev. Své obdivovatele si našel také ibis. Vnímám rozhodnutí pléna za spravedlivé. V určitém slova smyslu se máme co učit od všech třech krásných obyvatel přírody.

Já osobně se už teď těším na další republikové setkání interních auditorů, nejen z veřejné správy. Uskuteční se 23. a 24. dubna 2014 v Liberci.

**Ing. Eva Janoušková**
ředitelka Sekce ekonomiky a podpory
Kraj Vysočina
www.kr-vysocina.cz

# 10 + 1 „UČITELSKÝCH“ RAD PRO INTERNÍ AUDITORY

Delší dobu jsem tak trochu zpovzdálí sledovala živou diskuzi ohledně změn ve vnímání poslání interních auditorů. Ano, mám na mysli otázky zejména z oblasti zvyšování jeho hodnoty a užitečnosti, z oblasti změn v profesi interního auditu. Proto jsem uvítala pozvání organizátorů na národní konferenci interních auditorů, která se měla právě tímto tématem zabývat. Bylo to ovšem ono pověstné „něco za něco“. Přislíbila jsem totiž, že účastníkům konference předám svoje zkušenosti a svůj pohled na toto téma optikou současného manažera, bývalého interního auditora. Naštěstí jsem našla i podporu u svého zaměstnavatele a tak jsem díky tomu všemu mohla být v Olomouci.

O tom, že byla konference inspirativní, zajímavá a tvůrčí, a že rozpoutala velmi živou a podle mne i velmi užitečnou diskuzi, se můžete dočíst na jiném místě časopisu. Mým úkolem je – na žádost redakční rady – přiblížit i vám, čtenářům časopisu, nejdůležitější myšlenky mého vystoupení.

Na úvod bych se s vámi ráda podělila o své pocity, které jsem měla, když jsem poprvé přišla na pódium. Moje prezentace se odehrávala v rámci panelové diskuze na téma „Pohled z druhého břehu – Užitečnost a hodnota IA očima bývalých interních auditorů, nyní manažerů“. Panelovou diskuzi moderoval a také byl jejím „duchovním otcem“ můj dlouholetý kolega Tomáš Pivoňka (EY) – už to pro mne bylo zárukou toho, že zažiji něco nového, že to bude profesionální a přitom lidsky příjemné. A alespoň takto bych Tomášovi i dalším chtěla poděkovat za skvělou příležitost být součástí této části programu konference. A možná se sluší i připomenout, že jsem zde stála za mnohé další kolegyně a kolegy, kterým se i ve veřejné správě podařilo postoupit z pozice interního auditora na pozici manažerskou.

Na pódiu prezentovaly svoje rady v rámci panelové diskuze takové osobnosti českého interního auditu, jako je Jana Báčová (ČNB), které si vážím pro její vysokou profesionalitu a noblesu a integritu, Pavel Vácha (Provident Financial), se kterým jsem se svého času potkávala v radě ČIIA a který obohatil můj život o mnoho filozofických zamyšlení a zajímavých pohledů na život i na profesi interního auditu. Vedle mne seděla v křesle na pódiu také Marie Bílková (Úřad práce ČR), se kterou mne spojuje dlouholetá příslušnost k veřejné správě i stejný způsob uvažování o tom, jak by měla fungovat, a také Petr Kusebauch (Pražská teplárenská a. s.), který do diskuze přinesl velmi vtipný pohled na dané téma. Tedy už jenom příležitost být na pódiu s těmito kolegyněmi a kolegy, byla pro mne velkým zážitkem. Mým velkým „aha“ bylo také poznání, které jsem učinila už během konference, a které se potvrdilo i během této panelové diskuze. I když používáme trochu jiné formulace, mluvíme stejným jazykem a velmi podobně také myslíme a uvažujeme. Máme stejné zkušenosti, stejné představy o tom, jak interní audit funguje a jak ho dělat tak, aby na jedné straně přinesl tu nejvyšší hodnotu našim zákazníkům, a na druhé straně interním auditorům uspokojení, pocit seberealizace a profesní hrdosti.

> „Zcela jednoznačně jsem pro to, aby interní auditor radil, pomáhal s řešením, ale aby nepřebíral za tuto část odpovědnost“


Národní konference ČIIA – Užitečnost interního auditu aneb audit ve všech barvách; říjen 2013
panelová diskuze Pohled z druhého břehu – užitečnost a hodnota IA očima bývalých interních auditorů, nyní manažerů – zleva Pavel Vácha (Provident Financial), Marie Bílková (Generální ředitelství Úřadu práce ČR), Eva Janoušková (Krajský úřad Kraje Vysočina), Jana Báčová (Česká národní banka), Petr Kusebauch (Pražská teplárenská)

V následujícím textu se pokusím shrnout to, co ode mne zaznělo na pódiu, a to nejen v rámci předem připravené prezentace, ale i v rámci otázek, které padaly z pléna, a na které jsem reagovala.

Mottem mého příspěvku bylo „10 + 1 učitelských rad pro interní auditory – aneb byla jsem interní auditorka (a také učitelka), a teď jsem manažerka“. Možná se ptáte, proč právě učitelské rady. Je to poměrně jednoduché, dost velkou část profesní kariéry jsem působila jako středoškolská učitelka a v rámci této profese se to radami do života jen hemžilo. Dalším důvodem je i to, že interní audit stále občas „učím“ a sice na ČIIA, a že stejně jako tehdy ve škole, i teď mě tohle předávání teorie, zkušeností a dobrých rad opravdu baví. A poslední důvod je prozaický, chtěla jsem být přece jen trochu originální. A tak jsem si pro svou prezentaci připravila jednu imaginární vyučovací hodinu, její cíl, napsaný na tabuli, byl „Jak zvýšit užitečnost interního auditu“. A na tabuli bylo imaginární křídou napsáno také následujících 10 + 1 rad.

Národní konference ČIIA – Užitečnost interního auditu aneb audit ve všech barvách; říjen 2013

### Rada první: Kdykoli to půjde, vysvětlujte, co je interní audit

Interní audit přišel do veřejné správy jako naprostá novinka v roce 2001. Skoro nikdo nevěděl, co „to“ vlastně je, jak se „to“ liší od kontroly a nikdo netušil, jaká je odpověď na otázku „proč a jak to“ máme dělat. Nejen z těchto důvodů jsme si během interních auditů ověřili, že je dobré zahajovat každý konkrétní audit tzv. „kick-off meetingem“. Jeho cílem je představit interní auditory, představit cíl, rozsah a účel konkrétní auditní zakázky, způsob a pravidla komunikace a zcela na úvod vysvětlit, co je to interní audit. Docela jednoduše jsme k tomu používali definici interního auditu. Zahajování auditů tímto úvodním setkáním nebylo naším vlastním know how. Tuto praxi nám doporučili zahraniční experti, se kterými jsme se my, interní auditoři na krajských úřadech, mohli setkávat v rámci projektu Phare „Posílení vnitřních finančních kontrolních mechanizmů na mezinárodní úrovni“. Tento projekt, vlastně lidé, které jsem v něm potkala, mne v mojí profesní kariéře velmi ovlivnili. A dodnes jsem za tuto možnost velmi vděčná.

### Rada druhá: Buďte aktivní

Nezbytnou podmínkou fungování této rady (a platí to i pro všechny ostatní) je vzájemná rovnováha mezi očekáváním managementu a schopností a možnostmi interního auditu. Když nebude management očekávat, že interní audit bude vykonávat svojí funkci profesionálně, v souladu s legislativou a standardy, pak těžko můžeme internímu auditorovi radit, aby byl aktivní. Nikdo to totiž od něj nebude čekat a nikdo mu k tomu nebude vytvářet podmínky. A co mám konkrétně touto radou na mysli? Například to, aby se interní auditor, resp. vedoucí útvaru, aktivně účastnil porad vedení. Jednak tyto porady slouží jako dobrá platforma pro výměnu názorů, díky jim může také interní auditor získat důležité informace a může si vytvářet potřebné souvislosti. Být aktivní znamená také nabízet pomoc, zejména formou konzultací, radit ostatním a pouštět se do diskuzí.

### Rada třetí: Nabízejte, konzultujte, raďte, pomáhejte s řešením

Tato rada navazuje na tu předchozí. A odráží již zmiňovanou diskuzi ohledně toho, jestli role interního auditora končí odevzdáním auditní zprávy, ve které jsou zjištění a doporučení, nebo zda má interní auditor jít ještě „trochu dál“ a např. se nějakým způsobem podílet na implementaci doporučení. A ten kruciální problém je právě ve způsobu, jakým se interní auditor podílí na této „poauditní“ části. Jak už říká ona zmíněná rada, jsem pro to, aby interní auditor pomáhal s řešením, aby nabízel svoje rady – přece jenom má tu schopnost podívat se na zjištění a doporučení systémově, z ptačí perspektivy a z principu jeho práce také vychází, že je schopen najít souvislosti mezi příčinou zjištění a konkrétním doporučením. Možná jsme všichni z nás zažili poněkud kousavou reakci auditovaných „když jste tak chytří, tak nám řekněte, jak to máme udělat“. Myslím, že můžeme, či dokonce máme říct, jak to mají auditovaní „udělat“, ale myslím, že pokaždé musíme brát v úvahu rozsah odpovědnosti managementu a také velmi tenkou hranici mezi naší nezávislostí a mezi výkonnou rolí při implementaci doporučení. Tedy zcela jednoznačně jsem pro to, aby interní auditor radil, pomáhal s řešením, ale aby nepřebíral za tuto část odpovědnost. Možná se společenská a ekonomická praxe, následně také standardy a třeba i legislativa posune směrem k velkým změnám, a z interních auditorů budou také manažeři změn nebo dokonce ti, kteří odpovídají za implementaci doporučení… Ale v tuto chvíli to jsou vize, úvahy, směry rozvoje a osobně jsem moc zvědavá, jak to celé dopadne.

### Rada čtvrtá: Buďte v centru dění

Také tato rada opět navazuje na tu předcházející. Podle mne je vhodné, když je interní auditor účasten v různých projektových týmech. Mám na mysli např. projektové týmy, které se zabývají implementací různých metod řízení kvality. Sama jsem velmi kvitovala svoji účast

v týmu, který na našem úřadě opakovaně zajišťoval aplikaci sebehodnotícího rámce CAF. Dozvěděla jsem se tak spoustu informací a také jsem se spoustou poznatků mohla přispět. Ale pozor, interní auditor není totéž, co interní auditor kvality, i tady je třeba velmi pečlivě hledat onu dělicí čáru. Stejně tak účast v dalších projektech, které tzv. hýbaly úřadem, pro mne byla nezapomenutelnou a nepřenositelnou zkušeností. Dostala jsem se tak např. k realizaci veřejných zakázek, což bylo pro můj budoucí osobní rozvoj velmi důležité. Vzpomínám si také, jak jsem měla možnost být členkou hodnotící komise na různé služby, zejména z oblasti externího auditu. Také tyto aktivity mi velmi pomohly. Na tomto místě ale musím znovu připomenout, že základním předpokladem pro to, aby tato rada fungovala, je opět ochota managementu do takových aktivit interního auditora „pouštět", či dokonce cíleně nominovat. A je třeba také jmenovat jednu negativní stránku, tedy že tyto aktivity ubírají z celkové časové kapacity interního auditora a jsou mnohem lépe představitelné tam, kde je útvar interního auditu složen z více zaměstnanců.

### Rada pátá: Mluvte a pište stručně a jasně

V tomto bodě se objevuje moje určitá umanutost. Kolegové, kteří se mnou pracovali, anebo dodnes pracují, moc dobře vědí, jak upřednostňuji krátké věty – zejména ve zprávě z interního auditu. Mám na mysli maximálně 10 slov ve větě. Je to opět jedna rada, kterou jsme získali od zahraničních expertů, a věřím, že krátké, stručné věty vedou k přehlednosti textu a k jeho mnohem vyšší srozumitelnosti. Deset slov jistě není dogma, někdy to prostě nejde, ale je velmi dobrým tréninkem alespoň to zkusit, nebo na toto doporučení myslet. Nutí nás totiž psát jen to nejdůležitější a nejpodstatnější. Odpadá tak spousta tzv. slovní vaty a výstupy práce jsou také mnohem stravitelnější pro zákazníky interního auditu, tedy pro manažery, kteří dost často ze všeho nejvíce postrádají právě čas na čtení dokumentů. Myslím, že ke srozumitelnosti a jasnosti textu přispěje také činný rod. Pojďme si každý z nás uvědomit, jak často jsme napsali „bylo prověřeno, bylo konstatováno…". Proč prostě neříct „prověřili jsme", „vedoucí auditovaného útvaru konstatoval" apod. Velmi dobrým nástrojem v této oblasti jsou také manažerská shrnutí. Ta slouží také ke zvýšení hodnoty zprávy z interního auditu, která je jakousi výkladní skříní práce interního auditu. Manažerské shrnutí bychom tedy měli uvádět hned na úvod auditní zprávy a dbát na to, aby respektovalo strukturu zprávy a sdělilo opravdu to nejpodstatnější.

## „Doporučení interního auditu by měla nabízet spíše jednoduchá a účinná řešení"

### Rada šestá: Vzdělávejte se, rozvíjejte se, buďte profesionál

Když jsem tuto radu psala pomyslnou křídou na pomyslnou tabuli, měla jsem na mysli hlavně to, že interní auditor by měl být vždycky „tak trochu o krok napřed". Opět to souvisí s předchozími radami, měl by tedy být aktivní, měl by se stále snažit zlepšovat se, rozvíjet svoje schopnosti, být lepší a lepší. Mnozí mohou namítnout, že zejména ve veřejné správě chybí na osobní rozvoj peníze. Ano, do určité míry je to pravda. Ale mne osobně nepřestává fascinovat internet a jeho možnosti. Interní auditor se tak může velmi dobře připravit na každý konkrétní interní audit, najít si co nejvíc informací k tématu, má možnost dostat se k vědeckým článkům, názorům v různých diskuzích, k literatuře, anebo třeba i ke konkrétním zprávám nebo závěrům z kontrol. Je třeba si vždycky zachovat „zdravý rozum" při hodnocení těchto informací a rozlišovat oficiální a neoficiální zdroje. Ještě bych se chtěla zmínit o tom, co si představuji pod pojmem interní auditor – profesionál. Ostatně padla na to otázka i v diskuzi. Ne, nemám na mysli, že budeme profesionály v dopravní obslužnosti a budeme znát problematiku do všech možných detailů, pokud budeme právě pracovat např. na interním auditu systému úhrad ztrát dopravcům při zajišťování dopravní obslužnosti. Mám na mysli to, že díky nástrojům, které proces interního auditu nabízí, poznáme tento systém do takové hloubky a do takové míry, abychom ho mohli dobře zauditovat. Konkrétně mám na mysli studium legislativy a veřejně i interně dostupných informací, dále popis systému, identifikaci rizik, hodnocení stávajících kontrolních mechanizmů, předauditní šetření apod. Interní auditor profesionál se podle mne vyznačuje také tím, že kromě perfektní znalosti procesu interního auditu, standardů a legislativy,

Národní konference ČIIA – Užitečnost interního auditu aneb audit ve všech barvách; říjen 2013

má výborné komunikační a prezentační dovednosti, je tak trochu psychologem. V neposlední řadě v této souvislosti musím zmínit i velký zápal pro tuto profesi.

### Rada sedmá: Buďte přívětiví, ale rozhodní

Sedmá rada velmi souvisí s osobnostními charakteristikami každého auditora. Se schopností ovládat emoce – ať už máme na mysli ty pozitivní, nebo ty negativní. Podle mého názoru bychom tedy neměli chodit po našich organizacích zamračení, neměli bychom reagovat podrážděně a naštvaně. Ale tahle přívětivost by neměla přerůst do nadstandardních vztahů s auditovanými, neměla by být projevem přílišné ústupnosti a snahy za každou cenu vyhovět. Jde opět o onu již několikrát zmiňovanou rovnováhu, tentokrát tedy mezi vstřícností, přívětivostí, ochotou na jedné straně a neústupnosti, rozhodností a konzistentností.

### Rada osmá: Myslete nejdříve na druhé, pak na sebe

Konkrétní náplň této rady se „vinula jako zlatá nit“ různými příspěvky i diskuzemi na této konferenci. Zcela logicky v ní jde o to, abychom se podívali na naši „službu“ očima toho, komu jí poskytujeme. Jde o to, abychom znali potřeby našich zákazníků, abychom je dokázali respektovat a také jim co nejvíce přizpůsobit naše doporučení. Jde o to, abychom dokázali napsat auditní zprávu tak, aby si čtenář neřekl jen ono pověstné „no a co“, ale aby ho zaujala, aby nastartovala aktivitu, ale především, aby přinesla přidanou hodnotu, zlepšení. Tedy něco navíc, rozvoj, posun dopředu – něco, co by onen zákazník neobdržel, pokud by naši službu nekonzumoval. Doporučení interního auditu by měla nabízet spíše jednoduchá a účinná řešení, bez zbytečné byrokratické zátěže a s vysokou přidanou hodnotou. Ano, uvědomuji si, že toto je jedna z nejtěžších věcí, která se od interního auditora očekává. A co mám na mysli tím, když radím myslet na sebe až v té druhé řadě? Samozřejmě už (anebo později) zmiňovanou aktivitu a pracovitost, která může přinášet určité nepohodlí. Stejně tak jako hledání správných doporučení není snadnou cestou a stojí nemalé úsilí, vyžaduje přemýšlení, kreativitu, syntetické a analytické schopnosti. A to všechno někdy bývá dřina.

Národní konference ČIIA – Užitečnost interního auditu aneb audit ve všech barvách; říjen 2013
Bohuslav Poduška, Česká spořitelna

### Rada devátá: Nevyvyšujte se, ale nebuďte s každým kamarád

Tato rada opět směřuje do tzv. soft skills a osobnostních předpokladů interních auditorů. Domnívám se, že určitá skromnost, zdravá pokora a respektování postavení „těch druhých“ může přispět ke zvýšení užitečnosti interního auditu. Je to ovšem opět velmi závislé na tom, kdo stojí na oné pomyslné „druhé straně“, často jsou auditovaní a priori „nastartovaní“ proti internímu auditu a jsou připraveni mu to dát patřičně najevo (zde by se velmi hodil jeden expresivní výraz, ale netroufám si ho použít). Záleží samozřejmě také na věku a zkušenostech auditora, složitější situaci může mít mladý, nezkušený interní auditor. A pokud má právě on pocit, že on je ten někdo, kdo disponuje velkou mocí jiné auditovat, nebude to zřejmě fungovat. V organizaci, kde si navíc všichni budou myslet, že interní audit je kontrola nebo inspekce a že má velkou „moc“, bude ovšem velmi obtížné ten „správný“ interní audit vykonávat. A jak už bylo řečeno na jiném místě – blízké, přátelské, až kamarádské a nadstandartní vztahy, které jsou dokonce v rozporu s etickými pravidly, nemohou ke zvýšení užitečnosti přispět vůbec, byť to tak na první pohled nemusí vypadat. Pokud bych na tomto místě chtěla uvést poněkud „vědečtější“ vysvětlení, pak je velmi jednoduché. Jde o to, jak je v organizaci a v jejím vnitřním kontrolním a řídicím systému, nastaveno vnitřní (někde také uváděné kontrolní) prostředí.

### Rada desátá: Pracujte tvrdě

Možná můžete namítat, že všichni pracujeme tvrdě, že nemáme čas na svoje rodiny, zdraví, koníčky, přátele… Touto radou jsem ale nemyslela pracovat tak, aby to odnesla naše rodina a zdraví. Jde vlastně jen o jakési shrnutí těch předcházejících rad. Máme-li být aktivní, v centru dění, máme-li být profesionál, máme-li být dobře připravení na každý interní audit a máme-li dělat interní audit tak, aby byl opravdu užitečným, budeme muset pracovat tvrdě. Jinými slovy, dělat interní audit není žádná procházka růžovým sadem, je to práce, při které často musíme řešit konfliktní situace, práce, při které často děláme jednotvárné činnosti a bohužel, někdy se nám může stát, že o naše výsledky zas až tak nikdo moc nestojí. Ale to bych se už dostala do začarovaného kruhu. Možná bych teď ještě vzala imaginární křídu a dopsala na tabuli. Pracujte tvrdě, ale žijte zdravě.

A rada poslední, ta, která rozšiřuje předchozí desatero, zní: Usmívejte se. A k tomu není co dodat :))

Přesto mi na závěr dovolte jedno přání. Přeji vám, abyste ve své práci interních auditorů měli to štěstí, že při ní budete nacházet každodenní rovnováhu: rovnováhu mezi očekáváním vašich zákazníků a tím, jak tato očekávání budete schopni naplnit. Jedině tehdy se pak můžete začít zabývat 10 + 1 radami, které jsem napsala na pomyslnou tabuli.

# NOVÍ ČLENOVÉ ČIIA

- Ing. Marek Prachař, Muzeum umění Olomouc, s.p.o.
- Ing. Irena Wasserbauerová, Fio banka, a.s.
- Michal Vavrek, Generali PPF Holding B.V.
- Jaromír Hošek, Záložna CREDITAS, spořitelní družstvo
- Ing. Lenka Mušková, CIA, ACCA, Individuální členka
- Petr Jurák, MBA, FCCA, CIA, Bellinda Česká republika, s.r.o.
- Ing. Helena Veselá, Ministerstvo práce a sociálních věcí ČR
- Miloslav Havelka, RN, Individuální člen
- Mgr. Katarína Legemzová, Česká národní banka
- Ing. Lenka Dobešová, Telefónica Czech Republic, a.s.
- Ing. Šárka Vostarková, Ernst & Young, s.r.o.
- Bc. Jana Mikošková, Ernst & Young, s.r.o.
- Lucia Sirotková, MA, Ernst & Young, s.r.o.
- Bc. Tomáš Müller, Ernst & Young, s.r.o.
- Jan Zelený, Dopravní podnik hl. m. Prahy, a.s.
- Bc. Lukáš Pečeňa, Dopravní podnik hl. m. Prahy, a.s.
- Ing. Jonáš Fries, AEGON Pojišťovna, a.s.
- Ing. Gabriela Eichlerová, Státní fond životního prostředí ČR
- Ing. Esma Opravilová, SAB Finance a.s.
- Ing. Michal Pelc, Československá obchodní banka, a. s.
- Lic. Věra Janů, Statutární město Kladno
- Ing. Vladimír Jaroš, Individuální člen
- Ing. Tereza Šimůnková, MBA, AMISTA investiční společnost, a.s.
- Ing. Soňa Ptáčková, Záchranný útvar Hasičského záchranného sboru ČR
- Ing. Kateřina Wodaková, Hasičský záchranný sbor Moravskoslezského kraje
- Ing. Michal Hrubý, Individuální člen
- Ing. Martin Šedivý, Individuální člen
- Ing. Eva Žifčáková, MBA, Mondelez Czech Republic s.r.o.
- Ing. Dagmar Čiháková, Všeobecná fakultní nemocnice v Praze
- Ing. Emília Zborovjanová, Všeobecná fakultní nemocnice v Praze

# NOVÍ CERTIFIKOVANÍ *(nejen)* INTERNÍ AUDITOŘI


V současné době evidujeme celkem 286 certifikovaných:

| | |
|---|---|
| 266 | CIA |
| 10 | CGAP |
| 2 | CCSA |
| 3 | CFSA |
| 5 | CRMA |

V měsících srpen–září–říjen 2013 nám řady certifikovaných rozšířili tito:

**Tomáš Hlivka, CIA**
**Ilona Dubová, CIA**
**Michal Čup, CIA**
**Miroslav Šíp, CIA**

GRATULUJEME!

**Upozornění: Kompletní certifikační program je nutné dokončit do 4 let od podání registrace.**
**Pro kandidáty, kteří zahájili certifikační program před listopadem 2011, platí 4 letá lhůta od posledního pokusu realizace zkoušky.**

Vážení čtenáři,
od prvního čísla v roce 2013 nalézáte v časopise Interní auditor stránku s oddychovo-naučnou rubrikou. V každém čísle je pravidelně zveřejněno několik otázek z oblasti interního auditu, které jsou součástí testu na certifikaci CIA, a také křížovka nebo obdobná zábavná hra s tajenkou. Správné odpovědi na otázky, včetně tajenky, jsou slosovatelné o hodnotnou cenu, přičemž odpovědi na otázky a tajenka příslušného čísla, jsou zveřejněny vždy v dalším čísle časopisu Interní auditor.
**Odpovědi na otázky a tajenku je možné vyplnit pouze na webu – www.interniaudit.cz, a to do 10. února 2014.** Výherce bude následně vylosován na nejbližším jednání Redakční rady. Vylosovaný výherce z čísla 4/2013 obdrží jednodenní seminář na ČIIA zdarma dle vlastního výběru.

Přeji hodně štěstí.
*Daniel Häusler*

# S U D O K U

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 3 | | 8 | 2 | 5 | 9 | |
| | | | | | | | 4 | |
| | | | | 5 | 4 | 1 | 7 | |
| 9 | | 5 | | 2 | | 4 | 8 | |
| 1 | 8 | | | 3 | | | 2 | 9 |
| | | | | 9 | | | | 3 |
| 3 | 1 | 2 | 5 | | | 9 | | |
| | 5 | | | | 7 | | | |
| 7 | 4 | 8 | | | | 2 | | 5 |

Výherce z minulého čísla:
**Pavla Heroutová, Česká spořitelna, a.s.**
gratulujeme.

Správná tajenka z minulého čísla:
**Interní audit**

# OTÁZKY INTERNÍHO AUDITORA

**1. Co je nejlepší akcí v případě, že spuštění programu nebo práce v programu trvá nepřiměřeně dlouho?**

a. Spustit antivirový program (antivirus)
b. Otestovat systém spuštěním jiné aplikace či programu
c. Restartovat (znovu-nastartovat) systém
d. Zazálohovat hard-disk

**2. Které z následujících není jedním ze sedmi elementů rizika?**

a. Načasování
b. ROI analýza
c. Nejistota
d. Četnost

**3. Klient odesílá a sdílí svá citlivá data prostřednictvím internetu. Která z následujících kontrol bude nejefektivnějším preventivním opatřením, aby nedošlo ke zneužití dat v případě, že by komunikace byla zachycena neoprávněnou osobou?**

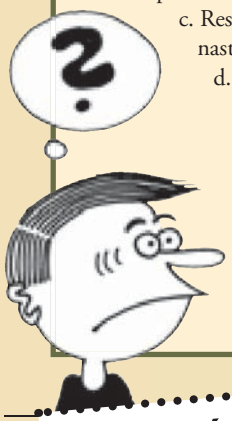
a. Použití hesel
b. Přístupový log
c. Šifrování
d. Firewall

**4. Nejběžnějším problémem při využití počítačů, kterému společnosti čelí, je:**

a. Fraud
b. Narušení počítačového zpracování z důvodu přírodních katastrof
c. Chyby a opomenutí při zadávání dat
d. Špatně fungující hardware

**5. Která z následujících operačních procedur zvyšuje vystavení společnosti počítačovým virům?**

a. Šifrování dat a souborů
b. Časté zálohování dat a souborů
c. Stahování veřejně dostupných programů a aplikací z webových stránek
d. Instalace originálních kopií zakoupených programů a aplikací na hard-disky



## Správné odpovědi z minulého čísla...

*1. Centralizace a decentralizace jsou definované na základě relativního delegování rozhodovacích pravomocí nejvyšším vedením. Mnoho manažerů věří, že decentralizované společnosti mají významnou výhodu před centralizovanými společnostmi. Hlavní výhoda decentralizované společnosti je taková, že decentralizovaná společnost:*

a. Společnost povzbuzuje zvýšenou iniciativu zaměstnanců
b. Strukturují jednotlivé směry ve společnostech a eliminují znásobování zdrojů
c. Společnosti jsou lépe kontrolovatelné
d. Společnosti mají méně manažerů než centralizované společnosti

*Vysvětlení:* Odpověď «A» : Decentralizovaná společnost dovoluje zaměstnancům na nižších úrovních spolupracovat v rozhodovacím procesu. Zvýšené zapojení povzbuzuje iniciativu a kreativní myšlení, zejména v případě komplexního a rychle se měnícího prostředí.

*2. Který z následujících je faktor ovlivňující riziko?*

a. Všechny odpovědi jsou správně
b. Noví zaměstnanec/zaměstnanci
c. Rychlý růst
d. Nový nebo vylepšený informační systém

*Vysvětlení:* Odpověď «A» : Nový zaměstnanec/zaměstnanci, nový nebo vylepšený informační systém i rychlý růst jsou faktory, které ovlivňující riziko.

*3. Interní kontrola může dodat pouze odůvodněné ujištění o tom, že cíle společnosti jsou dosahovány efektivně. Jedním z faktorů limitujících pravděpodobnost dosažení tohoto cíle je:*

a. Náklady interní kontroly by neměly překročit její přínosy
b. Vedení společnosti monitoruje výkonnost
c. Auditní výbor je aktivní a nezávislý
d. Primární odpovědnost interního auditora je detekce fraudu

*Vysvětlení:* Odpověď «A» : Limitujícím faktorem je fakt, že náklady interní kontroly by neměly překročit očekávané přínosy. Z tohoto důvodu, potenciální ztráta související s expozicí nebo rizikem je vážena proti nákladům dané kontroly. Přestože vztah náklady-přínosy je primárním kritériem, které by mělo být zvažováno při designu a implementaci interních kontrol, přesné měření nákladů a přínosů není většinou možné.

*4. Primární odpovědnost za dohled na zřízení a administraci interních kontrol je na:*

a. Správce společnosti
b. Externí auditor
c. Vyšší vedení společnosti
d. Vedoucí pracovník

*Vysvětlení:* Odpověď «C» : Role vyššího vedení společnosti je dohled na zřízení, administraci a hodnocení systému řízení rizik a kontrolu procesů (PA 2130-1).

*5. Které z následujících prvků jsou součástí kontrolního prostředí?*

a. Všechny odpovědi jsou správně
b. Přiřazení pravomocí a odpovědností
c. Organizační struktura
d. Integrita a etické hodnoty

*Vysvětlení:* Odpověď «A» : Jednotlivé prvky kontrolního prostředí zahrnují integritu a etické hodnoty, závazek způsobilosti, účast představenstva nebo auditního výboru, filozofii a manažerský styl, organizační strukturu, přiřazení pravomocí a odpovědností a politiku a praxi řízení lidských zdrojů.

Luboš Klečka

**Audit of Information Technology**
The author describes the role of internal audit and audit of IT and security in the times of quick development of mobile technologies.

Pavel Závitkovský, Miroslav Šíp

**Security of Company Data on Mobile Devices**
The authors deal with possible risks related to use of modern communication technology and define some measures how to prevent realization of the risk.

Igor Gricinko

**IA & Modern Information and Communication Technologies**
Modern information and communication technologies play an important role in auditors practice. Benefits of such approach are usually visible and clear, but do we considering also negative impacts coming from massive technology use? What constraints could significantly devaluate the benefits of modern technologies? As an IT auditor, the author is trying to reveal negative issues in use of technology and its causes. Using less formal style the author is provoking to think about IT in broad range giving the 10 recommendations how to explore more value added from using technology in day-to-day work.

Luboš Klečka

**Interview of Luboš Klečka with Bohuslav Dohnal**
The interview focuses on topics related to cloud technologies, their introduction and opinions on them. The emphasis is put on security issues when using cloud technologies.

Pavel Závitkovský, Zuzana Kitto

**T reats and Opportunities of the IT Internal Audit**
Results of the worldwide research of KPMG companies focused on the IT internal audit.

Jiřina Oleksiaková

**Experience with the Audit of Remuneration**
The author in her article continues with the serie of her articles related to remuneration and focuses now on her experience with the audit of remuneration area in the bank.

Petr Hadrava

**What Management Expects from Internal Auditor**
A proactive approach is expected from the internal auditor in MetLife pojišťovna as well as a detailed knowledge of the company's goals and strategies, wishes and needs of customers and close cooperation of a risk based dynamic internal audit plan. Internal auditor should be a partner for the management who has a sound professional judgement, uses common sense and is prepared to discuss any challange with the management.

Martina Košťálová

**News from the CHJ Kitchen and What New Has Happened**
Next actual information and news from the activity of Ministry of Finance of Czech Republic in the area of internal audit and financial control.

Petr Kheil

**What Peter Noticed (Not Only) in Legislation**
The author mentions in his regular column useful sources of information related to management and control system and internal audit activity. The aim is not the full list of issued laws, bylaws, regulations and other documents.

Šárka Nováková

**We Have Something to Trot Out – the Activity of the Public Sector Section of the CIIA**
The article informs about the activities of the Public Sector Section of the CIIA from its creation until now and challenges the internal auditors from the public sector to use the offered advantages and their active involvement in the Public Sector Section of the CIIA.

Ivana Krůželová

**How (not) to Set Up the Operational Programme**
The author describes system of the structural funds implementation in the UK including experience and issues resolution.

Josef Vincenec

**News from Home (of Auditors) and World (of Animals)**
Information from the CIIA National Conference in the Centre of Moravia.

Eva Janoušková

**T e 10 + 1 "teacher's" recommendations for internal auditors**
The author summarizes her presentation from the national conference of CIIA.

# data pod lupou

## Utvořte si vlastní nezávislý názor na firemní data, ověřte reporty, zvyšte kvalitu interního auditu. Provádějte nezávislá šetření rychle a produktivně.

## Software IDEA®

nová verze IDEA v9 v prodeji

### Nezávislá analýza dat

- **Univerzalita** – schopnost importovat různé formáty dat.
- **Produktivita** – schopnost zpracovávat velké soubory.
- **Nezávislost** – na programech, na strukturách dat.
- **Průkaznost** – intaktnost dat, výpis historie.
- Intuitivní ovládání.
- Výkonné serverové řešení pro velké korporace.

## Smart Exporter

### Snadný přístup k datům SAP®

- Spolehlivý, jednoduchý a rychlý export dat ze systému SAP®.
- Tvorba požadavku na SAP® data přímo ve vašem PC.
- Přístup online i offline.
- Exporty dat lze přesně načasovat (např. noční hodiny, víkend).
- Spolupráce se softwarem IDEA®.

## Smart Analyzer

### Soubor základních auditorských testů

- Doplněk softwaru IDEA®.
- Testy hlavní účetní knihy.
- Analýzy pohledávek a závazků.
- Testy majetku.
- Testy skladů.

## CaseWare™ Monitor

### Kontinuální monitoring

- Efektivní řešení průběžné kontroly vnitřních procesů.
- Univerzální použití, snadná implementace do stávajících systémů.
- Prevence podvodů a neefektivního využití zdrojů.
- Okamžité detekce a reakce.
- Účinné sledování více systémů v rámci organizace.
- Snadná integrace se stávajícími skriptovacími nástroji, jako je IDEA®.

IDEA Software pro analýzu dat

SMART ANALYZER

idea server

CASEWARE MONITOR

**J + Consult, spol. s r.o.**
Čapkova 2/195, 140 00 Praha 4
T: +420 244 118 411, E: idea@jconsult.cz
www.datapodlupou.cz, www.jconsult.cz

jconsult