# iA interní auditor

ČTVRTLETNÍK ČESKÉHO INSTITUTU INTERNÍCH AUDITORŮ
ROČNÍK 21, ČÍSLO 2–2017 (84) 2|2017

## MÝTY O INTERNÍM AUDITU

ČESKÝ INSTITUT INTERNÍCH AUDITORŮ

# GDPR
# NEZÁVISLOST VEDOUCÍHO INTERNÍHO AUDITU
## VÝBORY PRO AUDIT | FINANČNÍ VÝKAZY
## CENA ZA INOVACI


# INOVACE A REGULACE
## v interním auditu

**Rezervujte si termín!**

## BRNO
HOTEL HOLIDAY INN

**14.–15. 11. 2017**

**VIP PŘEDNÁŠEJÍCÍ:**

Angela **WITZANY**
(The IIA – Chairman of the Board), ...v jednání

Lucie **BREŠOVÁ**
(KIWI.COM)

Vladimír **DONÁTH**
(Všeobecná úverová banka)

Zuzana **KITTO**
(UniCredit Bank)

Branislav **KOZMER**
(Allianz – Slovenská poisťovňa)

Radek **NEUŽIL**
(předseda disciplinárního výboru RVDA)

Tomáš **PIVOŇKA**
(ČEZ)

Michal **SVOBODA**
(Ministerstvo financí)

Filip **ZELINGR**
(Český Aeroholding)

WWW.INTERNIAUDIT.CZ

ČIIA ČESKÝ INSTITUT INTERNÍCH AUDITORŮ | IIA The Institute of Internal Auditors | ECIIA

Najít téma pro časopis „Mýty v/o interním auditu“ a najít v něm shodu nebylo tak těžké. Získat přehled mýtů šlo rovněž velmi rychle. Když jsem si sedl se svými kolegy, abych získal jejich pohled na to, jaké mýty v/o interním auditu jsou pro ně zásadní, a tím si doplnil svůj přehled, vznikl v krátké době jejich dlouhý seznam. Stejná diskuze poté proběhla v redakční radě. Nakonec zůstala část nejtěžší – vybrat a oslovit autory, kteří se podělí se svými názory s vámi, čtenáři. Jak to dopadlo, posoudíte vy sami.

Podle mého zařadili autoři mezi mýty mnohé z toho, k čemu jsme i my dospěli v diskuzích. K mýtům byla zaměřena i anketa. I zde se mnohé z mýtů shodují a prolínají. To svědčí o tom, že jsme si mýtů dostatečně vědomi, a možná i víme, jak se k nim ze své strany postavit.

Ve svých článcích autoři uvádějí mýty, zamýšlejí se nad nimi, vysvětlují jejich správné chápání a mýty vyvracejí. Těžší situace by zřejmě nastala v okamžiku, kdy by se nám podařilo na stránky časopisu přivést i zástupce svých klientů. Možná by v některých bodech oponovali, nenechali by argumenty interních auditorů projít jen tak. V tu chvíli by se vysvětlování a dosažení přesvědčení stalo možná daleko těžším. To určitě mnozí z nás znají z každodenní praxe.

Zajisté platí, že je nutné postupy auditu udržovat v rámci standardů, trvale komunikovat se svými klienty a auditovanými, nepřipouštět jejich nereálná očekávání a představy, vysvětlovat poslání a cíle interního auditu, a zejména je naplňovat svojí každodenní prací s kvalitními výstupy.

Nezapomenout, že máme širokou škálu klientů. Každý z nich má své představy, očekávání, nebo je také nemusí mít vůbec. Spolupracujeme s lidmi, kteří svoji práci vykonávají v různých podmínkách, kvalitě, s různou motivací a zápalem. Obecně však neradi slyší kritická slova na svoji práci. I toto může být prostředím, ve kterém se může mýtům dařit.

Určitě je velmi užitečné toto téma otvírat, nad „mýty“ se zamýšlet, střízlivě se dívat na dění kolem sebe a nepřipouštět prohlubování mýtů a jejich bobtnání. Ani těch, které vzbuzují velký pesimizmus, ani těch nekriticky optimistických. Neutvrzovat se v nich, vyvracet je tam, kde je to nutné, a zabraňovat situacím, které by umožňovaly šíření mýtů z našich řad.

*Jan Kovalčík*
*vedoucí redakční rady*

Deloitte.

# Interní audit

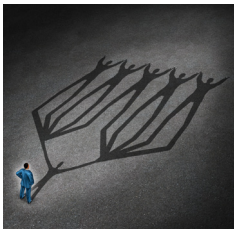
## Spolehlivá business inteligence pro vedení firem



Audit & Assurance

# OBSAH / CONTENTS








ROČNÍK 21, ČÍSLO 2–2017 (84)

2|2017

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

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

Vydavatel nenese odpovědnost za údaje a názory autorů jednotlivých článků.

Redakční rada:
Vedoucí – Jan Kovalčík, Petr Hadrava, Daniel Häusler, Ludmila Jiráňová, Andrea Lukasíková, Šárka Nováková, Petra Škvorová, Eva Štěpánková, Milena Widomská, Kateřina Zonygová

Foto: archiv ČIIA, fotobanka 123RF
Neprodejné, určeno pro Český institut interních auditorů
Náklad: 1 500 výtisků
Pre-press: Viktor Beránek
Tisk: REPRO servis s. r. o.
Distribuce: Mail Step a. s.

iA interní auditor

# MÝTY VS. MODERNÍ PŘÍSTUPY V INTERNÍM AUDITU

MONETA MONEY BANK

**S kolegou jsme dostali nabídku na sepsání článku o mýtech, které provázejí profesi interního auditu nebo samotné auditory. Důležitým úkolem auditních útvarů dnes totiž není jen „syrová“ auditorská práce, ale také dostatečná komunikace s našimi klienty, kdy jim vysvětlujeme roli auditu, a nastavujeme tak vztahy odpovídající firemní kultuře 21. století. K celé problematice totiž nemůžeme přistupovat silou a mýty bořit, ale musíme se jim věnovat s grácií a vysvětlujícím přístupem. Téma nás natolik zaujalo, že jsme se proto rozhodli zde pár mýtů popsat.**

**Ing. Alena Běťáková (Stránská), CIA**
Senior Auditor
MONETA Money Bank, a. s.
alena.betakova@moneta.cz

**Ing. Václav Kupec, Ph.D.**
Senior Auditor
MONETA Money Bank, a. s.
vaclav.kupec@moneta.cz

### AUDIT je nuda

Na úvod tu máme takový pěkný mýtus, a sice, že audit je nuda... Osobně si myslím, že kdo někdy práci v interním auditu vyzkoušel, toho by snad ani nenapadlo si myslet, že audit může být nuda. Naopak však nezainteresovaný člověk může audit vnímat více jako kontrolu, suché odškrtávání pouček a kupu byrokracie. My všichni, kteří již nějaký pátek v interním auditu pracujeme, však víme, že interní audit rozhodně není stereotyp, a nuda už vůbec ne. Každý audit je jedinečný, dozvídáme se při něm spoustu nových informací, máme možnost komunikovat s různými typy osobností a musíme se umět vypořádat s větším či menším množstvím neočekávaných situací, které se čas od času v auditních zakázkách vyskytnou. Každý jednotlivý audit nás tak posunuje kupředu a to, co se zpočátku mohlo zdát jako ne příliš zajímavé téma, se může rázem změnit v napínavý, leckdy až detektivní příběh s překvapivým rozuzlením. Řekněte sami – stalo se vám někdy, že jste auditovali nějaký proces nebo oddělení a nudili se při tom?

### AUDIT je účetnictví

V dřívějších dobách mohl být interní audit vnímám více jako kontrola čísel, a tudíž hojně spojován s účetnictvím. Moderní pojetí interního auditu je však mnohem širší a zahrnuje více oblastí než „pouhé“ finance podniku. V oblasti bankovnictví, v níž pracujeme, jsou to například procesy spojené s úvěrováním klientů, zaváděním nových produktů, dále procesy ovlivňující zákaznickou zkušenost, řízení různých druhů rizik a v neposlední řadě informační technologie a procesy zaměřené na bezpečnost informací a ochranu citlivých údajů. Zdaleka již tedy nejde jen a pouze o čísla, nýbrž o celkový pohled na společnost napříč všemi procesy a na její vnitřní řídicí a kontrolní systém. Vrcholovému managementu poskytuje interní audit své služby jak ujišťovací, tak i poradenské povahy, a je tak nápomocen ve všech oblastech, které ovlivňují podnikání společnosti. Zprostředkovaně tedy máme možnost svou prací ovlivnit i samotný výsledek hospodaření, kdy náprava nedostatků, jež v průběhu auditních zakázek odhalíme, často napomáhá zefektivnit procesy, a ušetřit tak mnohdy i nemalé peníze.

**„Stalo se vám někdy, že jste auditovali nějaký proces nebo oddělení a nudili se při tom?“**

### AUDIT je represe

Stejně tak si můžeme rozebrat mýtus o auditu jakožto represivní složce podniku. Naštěstí jsou pryč doby, kdy se někteří auditoři pohybovali po chodbách společností a úřadů v černých oblecích, lidé se jich báli a auditní zprávy byly přijímány se skřípěním zubů. Tím samozřejmě naivně netvrdíme, že jsou takovéto situace již minulostí všude. Audit každopádně prochází vývojovou etapou, v níž jsou používané techniky auditorů symbioticky doplňovány moderní diplomacií. A pokud uznáme auditorskou diplomacii za umění komunikace v obtížných situacích, otevírají se nám velké možnosti pro uplatnění neoauditních přístupů, kdy jsou auditor a auditovaný na stejné úrovni jednání. Pečlivé naslouchání, přiměřená komunikace a profesionální vystupování nás následně pustí i do oblastí, které nám jinak zůstanou nedostupné. Akce totiž vyvolává reakci, a pokud budeme místo u čtvercového stolu s ostrými rohy jednat u stolu kulatého s nekonečným porozuměním, otevřou se nám mnohé, dosud pevně uzavřené dveře. Je přece rok 2017!


**MONETA MONEY BANK je držitelem Ceny za inovaci 2016 v interním auditu**

### AUDIT je kontrola

Také další představu o auditu, který je pouhou kontrolou, se nám daří pozvolna měnit. Je to však mnohdy sisyfovská práce, protože zejména některá média používají zjednodušující výklad a přiřazují nám pouze kontrolní funkce, aniž by alespoň teoreticky popsala interní audit coby poradce a pomocníka managementu (Schránil, 2010). Tímto rozborem zažitého stereotypu o auditu a kontrole samozřejmě nesnižujeme význam specifických kontrolních funkcí. Je přitom jen na nás, jak dokážeme komplexní úlohu interního auditu odlišit, popsat a vysvětlit co nejširšímu externímu auditoriu. Zaměření do budoucnosti, procesní analytika, ucelené hodnocení a mnohé a mnohé další je totiž to, co nás od ostatních odlišuje. Inovované pojetí auditorských služeb, na které upozorňoval již Dvořáček (2003), tak postoupilo od kontrolních přístupů směrem ke konzultační činnosti mílovými kroky. Dnes stojíme k auditovaným kolegům čelem a týmově se účastníme ujišťovacích nebo poradenských zakázek, což bezesporu přispívá k transparentnosti našeho výkonu.

### AUDIT je postrach

I když ne vždy je to auditovanou protistranou tak vnímáno, interní audit není o strachu a nutném zlu bez přidané hodnoty. U našich kolegů, kteří doposud neměli tu čest projít si interním auditem z pohledu auditovaného, většinou bohužel převažuje vnímání založené na strachu z auditu, z toho, že s auditory nebude rozumná řeč a že budeme auditovaným generovat pouze další nadbytečnou práci s nulovým, nebo zanedbatelným přínosem. Tento mýtus se u nás ve společnosti snažíme eliminovat tím, že děláme své profesi odpovídající marketing. Jednou z aktivit, kterou napříč společností nabízíme, je koncept rotace v rámci programu Guest Reviewer. Kdokoli ze společnosti má tak možnost stát se na omezenou dobu auditorem a účastnit se společně s námi vybrané auditní zakázky. Dáváme tím kolegům možnost nahlédnout pod pokličku interního auditu, a snažíme se tak poodkrýt roucho zahalující naši práci, aby kolegové snáze pochopili, že nejsme ve společnosti jen bičem, ale naopak pomáháme odhalovat slabá místa procesů, a prostřednictvím doporučení tak zlepšovat kontrolní prostředí naší společnosti.

**„Audit každopádně prochází vývojovou etapou“**

**„Interní audit není o strachu a nutném zlu bez přidané hodnoty“**

### AUDIT je „hard skill“

Jistě nejedno z posledních témat, které dnes auditorskou profesi rozšiřuje a posunuje, se týká „hard“ inteligenčního kvocientu (IQ) a „soft“ emočního kvocientu (EQ). Mytická doba, kdy nám pro výkon auditu „stačilo“ znát své řemeslo na úrovni hard skills, se znatelně mění na etapu, kdy po nás zákazníci a prostředí vyžadují rozšiřovat nabízený sortiment služeb také o soft skills. Inteligenční kvocient se totiž stal samozřejmou součástí pracovních nároků, jež jsou na nás kladeny. Aby se náš výkon adekvátně zlepšoval, dostávají se však do popředí auditního výkonu také vlastnosti související právě s emoční inteligencí, tedy s automatickou schopností vycházet s ostatními na osobní i profesionální úrovni (Hasson, 2015). Audit coby mezioborově náročná disciplína je tak stále více o umění přirozené interakce v auditním prostředí a mezi auditovanými subjekty. A pokud přitom využijeme empatii a sebeovládání, dokážeme pochopit analyzovanou problematiku mnohem lépe a rychleji, což následně přinese auditovaným kolegům větší komfort a přidanou hodnotu.

### CO ŘÍCI ZÁVĚREM?

Naší ambicí nebylo na řádcích výše obsáhnout celé široké spektrum mýtů, které kolem interního auditu mohou kolovat, nýbrž jsme se snažili identifikovat ty nejběžnější. Naším záměrem nebylo ani podat jasné závěry, tedy všechny mýty vyvrátit, nebo potvrdit. Naopak jsme vám chtěli vnuknout ideu k zamyšlení, a případně otevřít diskuzi nad tím, jak vy sami vnímáte mýty, které kolem naší profese panují. Budeme rádi za vaše názory, které s námi můžete sdílet prostřednictvím našich e-mailů. ■

# Věříte MÝTU, že auditor je tu od toho, aby ředitel měl vždy pravdu?

*...říká Rodan Svoboda.*

**Ing. Rodan Svoboda, CIA, CICA, CRMA**
jednatel vzdělávací a poradenské společnosti Eurodan, s. r. o.,
konzultant v oblasti VŘKS a IA
svoboda@eurodan.cz

**Pohybuji se v auditní profesi minimálně půlku svého profesního života. Domnívám se, že už jsem pochopil, v čem spočívá kouzlo vnitřního auditingu, jaké je jeho poslání, jakou přidanou hodnotu poskytuje. O to víc mne překvapí, když tu a tam narazím v určité organizaci na obhajování specifické cesty k výkonu auditu s odvoláním na požadavky vedení, na uplatňování vlastních nástrojů a technik k zajišťování operativních závěrů, či přímo na nahrazování auditu kontrolou. Nejsem zas tak naivní, že bych byl přesvědčený, že se pod pojmem interní audit dělá všude jen to samé. Mnohdy se pod audit schovává prakticky všechno, co se nehodí jinam. Ale že by měl auditor na přání vedení jen prošetřovat a kontrolovat, co kdo porušil a nesplnil? Není právě to mýtus, že má být díky auditu úspěšný pouze ředitel a jeho management? Nemá to být celá organizace?**

Není lehké potvrdit či vyvrátit popsané tvrzení. Pokusím se o to v několika následujících bodech tak, jak jsem měl možnost se seznámit s realitou při externích hodnoceních kvality činnosti interního auditu, při konzultacích a rozhovorech s auditory. Pokud se jedná o cílené využívání auditu pro prosazování zájmů nejvyššího vedení, zpravidla se to objeví již ve vymezení role auditu v organizačním řádu, resp. ve statutu interního auditu. Na jedné straně lze zvolit standardní přístup vycházející z rámce profesní praxe interního auditu, zejména z poslání, definice, standardů a etického kodexu. Vždy se bude jednat o podíl na monitoringu správy a řízení, řízení rizik a řídicího a kontrolního systému ve formě objektivního prověřování, zda organizace zná a řídí svá rizika.

Na druhé straně však dochází k tomu, že je interní audit pověřován výkonem široké škály výkonných a kontrolních aktivit s odůvodněním, že právě v tom je přidaná hodnota auditu. Možná v případě zapojení se do řízení rizik, zejména funkce compliance, nebo prověřování ročních výsledků hospodaření, lze tuto strategii auditu za určitých nastavených podmínek přijmout, ale výkon většiny ostatních administrativně kontrolních rolí je už nutné odmítnout. Právě to omezuje audit v uplatňování nezávislosti při hodnocení systému vnitřního řízení a kontroly. Takže pokud útvar auditu nemá ve svém statutu odkaz na rámec profesní praxe auditu, resp. při jeho naplňování se auditoři neopírají o auditní standardy, je to vždy pro případného externího hodnotitele signál, že interní audit nedělá, co má, ale pouze poskytuje účelové služby svému vedení.

**„Není právě to mýtus, že má být díky auditu úspěšný pouze ředitel a jeho management?“**

Dalším bodem, na který se zaměřím, jsou lidé, kteří interní audit vykonávají. Nelíbí se mi až možná nezdravá loajálnost, kdy auditoři vykonávají prakticky vše, co je od nich vedením požadováno. Raději bych vyzdvihl standardní požadavky na etiku jednání auditorů, zejména na integritu, objektivitu, důvěrnost a kompetentnost, které zaručují náležitou odbornost a profesní péči. Pokud tyto požadavky nejsou zakomponovány do vnitřních předpisů pro interní audit, nepromítají se ani do plánu profesního rozvoje a jeho hodnocení, mohu s jistotou tvrdit, že narážím na auditora, který je uzavřen ve své bublině znalostí a dovedností. Zpravidla je nabyl jako dlouholetý kontrolor a nesnaží se je dále rozvíjet v souladu s požadavky profesních auditních standardů. V tom případě se okamžitě seznamuji s výsledky jeho práce a zajímám se o to, k čemu a komu jeho výstupy slouží. Odhadujete dobře, zpravidla převládá šetření incidentů, shromažďování informací o vzniklé škodě a jejím zavinění. Tedy vlastně náboje pro operativní rozhodování managementu.

Vyskytují se organizace, kde jsou oba popsané body ještě do jisté míry v pořádku. Auditor se ve statutu odvolává na rámec profesní praxe a pravidelně se zúčastňuje odborných školení prohlubujících jeho znalosti v auditingu. Kde se však vždy projeví, že audit nepostupuje dobře, je proces střednědobého a ročního plánování. Nejenže se návrh plánu nevytváří v interním auditu na základě každoroční aktualizace mapy rizik, ale navíc si vedení do plánu v míře větší, než je žádoucí, zahrnuje požadavky na operativně vyžádané audity. Čím více mimořádných kontrolních šetření na vyžádání ředitele, tím méně

objektivního a nezávislého ujišťování o účinnosti řídicích a kontrolních systémů pro zřizovatele či orgány organizace.

Co se týká postupů a technik práce interního auditora, tak se zpravidla nedá na první pohled poznat, zda jsou dobré, či nikoliv. Nemluvím teď o pracovníkovi, pro kterého byla pozice auditora zřízena náhradou za to, že byl odsunut z vedení organizace, tam je všechno marné. Od něho se dá očekávat v lepším případě pouze poradenská činnost s minimem přesahu do řízení rizik a kontrolních systémů. Mám teď víc na mysli standardní dosahování výsledků auditu při plnění plánovaných zakázek. Setkávám se s tím, že auditní manuál obsahuje

**„Mnohdy se pod audit schovává prakticky všechno, co se nehodí jinam“**

dostatek pracovních šablon, ale jejich slabinou je, že auditor vždy končí pouze u shromažďování informací. Postrádám v těchto případech návazně dostatečné vyhodnocování podle předem konkrétně stanovených kritérií, a především analýzu zjištění ve vazbě na slabá místa řídicího a kontrolního systému. Vnímáte v tom ten rozdíl? Auditní šetření by nemělo končit kontrolním zjištěním bez doporučení systémových změn, které by snižovaly možnost opakování případných nedostatků. Pravděpodobně o toto není ze strany vedení zájem.

Doposud jsem se zabýval vybranými částmi nastaveného systému interního auditu v organizaci, teď bych se chtěl konečně dostat k výsledkům práce auditora. Na nich se pozná, zda audit v organizaci dělá to, co má, není zneužíván pro operativní účely a vykonávají ho odborně vybavení auditoři s využitím vhodných zásad a postupů.

Zpravidla každé systémové zjištění popsané v auditní zprávě přináší změnu. Možná pro ni nejsou bezprostředně vhodné podmínky a její realizace se proto odloží v čase, ale jednou se opatření týkající se rizika s dopadem v nepřiměřené výši realizovat musí. Vedení sice může takové riziko přijmout, ale v případě, že se následně projeví, je to pro odpovědné osoby ohrožující. Takže se už nedivíte, že raději o tom ředitel nechce vědět? Není z jeho pohledu lepší se pak vymluvit na objektivní vnější vlivy, a případně pak úspěšně řešit následky s extra vyčleněnými zdroji?
Popsaný krátkozraký účelový přístup přímo volá po tom, aby auditoři neauditovali, aby se co možná zabývali jinými agendami a maximálně aby jen kontrolovali to, co už se stalo. Všichni se budou před nimi třást, jen aby náhodou na něco nepříjemného nepřišli, aby probíhající kontrolní šetření zůstalo co možná bez zjištění a pro odpovědné pracovníky bez postihů. V organizaci bude disciplína a ředitel bude mít pořádek. Ale bude mít za takto nastavených podmínek i pravdu? Jsem přesvědčený, že ne.

Vycházím z toho, že posláním interního auditu je zvyšovat a chránit hodnotu organizace objektivním ujišťováním o účelnosti řízení vyhodnocených rizik, poskytováním poradenství a přinášením porozumění podstatě věci. Nic z toho audit, který sám nechce či nemůže implementovat rámec profesní praxe, garantovat nemůže. Nepomáhá rozvíjet řídicí a kontrolní systém a snižovat tak rizika spojená s činností organizace. A pokud pak dojde k negativnímu projevu rizik vlivem nesouladu s předpisy či nízké výkonnosti, ředitel nikdy nemůže mít pravdu. V tom případě je interní auditor k ničemu, byť se držel zásady naplňovat požadavky vedení. Není to tedy správná cesta, je to pouze mýtus. A pro úplnost, pokud se vás to třeba týká, věřte, podobnost v článku je s vámi čistě náhodná. ■

**„Čím více mimořádných kontrolních šetření na vyžádání ředitele, tím méně objektivního a nezávislého ujišťování o účinnosti řídicích a kontrolních systémů pro zřizovatele či orgány organizace“**

# Mýty o interním auditu

**Nejčastější mýty o interním auditu (dále jen IA), to je opravdu zajímavé téma, k němuž je možné přistoupit, jako ostatně u všech věcí, mnoha způsoby a nikdy nebudete mít jistotu, že jste vyčerpali všechny možnosti, které existují. Ale z toho my, interní auditoři, přece strach nemáme, že? My přistupujeme nezaujatě, systematicky a metodicky k jakémukoliv tématu a tímto přístupem vždy dosáhneme objektivního a přesného zhodnocení věci a navržení opatření ke zlepšení práce s mýty o IA… Nebo, že by to byl jeden z řady mýtů o IA? Zatím nevím. Měli bychom se nejdříve podívat na to, co to „mýtus“ vlastně je. A nebude to jednoduché, protože etymologie slova „mýtus“ je poměrně složitá.**

**PhDr. Evžen Mrázek**
Odd. Regulace účetnictví podnikatelů
Vrchní ministerský rada
Ministerstvo financí

**Mýtus** (řecky μύθος, vyprávění) je **„symbolické vyprávění vyjadřující víru v plnost a celistvost nadčasového řádu“**. V tomto smyslu mýty o IA zahrnují vyprávění o IA, o jeho historii, o jeho velikánech, o jeho poslání a samozřejmě i přesvědčení, že tady bude vždy ať se děje, co se děje. Je to víra v to, že člověk (a jeho inteligence), bude vždy v tom složitém systému vzájemně propojených a často protikladných myšlenek a aktivit, jakým svět bezesporu je, potřebovat interní audit. Je to přesvědčení, že podniky a organizace, a především jejich vedení, budou díky rostoucí složitosti jejich motivací, cílů, interakcí a vztahů uvnitř i navenek v prostředí, jehož parametry se neustále mění a jež nelze nikdy se stoprocentní jistotou plně zachytit a pochopit, vždy potřebovat někoho, kdo jim pomocí systematického metodického přístupu k hodnocení a zlepšování účinnosti systému řízení rizik, řídicích a kontrolních procesů a řízení a správy organizace poskytne objektivní ujištění, že jdou (organizace, podnik, vedení) správným směrem. V tomto smyslu je mýtus o interním auditu pravdivý, interní audit má před sebou ještě hodně dlouhou a úspěšnou perspektivu…

Mýtus je však chápán i jako **vyprávění o něčem, co je v rozporu s racionálním poznáním** (dané doby). V soudobém hovorovém jazyce se slovo „mýtus“ používá též pro **všeobecně rozšířenou nepravdu**, vymyšlené tvrzení bez dostatečných důkazů. To je trochu negativní výklad pojmu mýtus, ale v praxi asi bohužel nejčastější.

Každá profese má své mýty a IA nemůže stát bokem, vždyť je to jedna z nejdůležitějších profesí novodobé historie. Alespoň pro nás interní auditory!

Takže se vrhněme po hlavě do některých nejčastějších mýtů o IA. Jsem rád, že předmět článku se netýká nejčastějších mýtů v interním auditu, protože to by bylo téma mnohem složitější a třaskavější…

***Některé příklady mýtů o interním auditu:***

**Interní audit je stejný jako externí audit a externí audit může nahradit interní audit.**

Kdo ho používá a komu slouží? No určitě ho používá ten, kdo ví hodně málo o interním auditu, jeho poslání a o přínosech, které může organizaci dát, pokud je vykonáván v souladu s Mezinárodními Standardy pro profesní praxi interního auditu vydaných IIA (dále jen „Standardy IIA“). Také ho občas používají externí auditoři, aby získali zakázky a při tom zdůrazňují přínosy outsourcingu funkce interního auditu. Je to nepravdivý mýtus. Jedná se o dva odlišné audity s rozdílnou motivací (poskytnout přidanou hodnotu x získat zakázku a realizovat zisk), rozdílnou mírou vnitřní integrity s organizací, rozdílnou nákladovostí atd. Existují situace, kdy je vhodné, aby organizace použila služeb výhradně jednoho typu auditu, nebo aby využívala současně služeb obou auditů.

**Interní audit vše vyřeší.**

Můžeme ho použít na cokoliv. To je zajímavé chápání interního auditu, pravděpodobně vzniklé setkáním s dobrou praxí interního auditu, ale je rovněž v rozporu s realitou a s posláním interního auditu. Interní auditor je specialistou na hodnocení a zlepšování účinnosti systému řízení rizik, řídicích a kontrolních procesů a řízení a správy organizace a není a nemůže být odborníkem na všechno. Odbornou práci by měli dělat odborníci. Interní auditoři nemohou nahrazovat kontrolu, řešení stížností apod. Dělali by práci, která nespadá do jejich působnosti, pro kterou nemají odbornost a kompetence a v níž nemohou nabízet žádná skvělá řešení. Navíc by se dostali do konfliktu zájmů, který by jim znemožnil dobře dělat práci, pro kterou jsou primárně určeni. Interní auditoři nemohou dělat práci za management, který je od toho, aby řídil organizaci, měl pod kontrolou

všechny nejdůležitější faktory jejího úspěchu a řešil problémy, které se objeví. IA systémově nemůže pomáhat manažerům nacházet nová řešení mimo oblast své působnosti tím, že se aktivně zapojí do procesu řízení společnosti například formou hledání obchodních příležitostí a řízení organizačních a procesních změn ve společnosti. To už nebude IA vykonávaný v rámci Standardů IIA, ale externí audit, jehož poslání je jiné.

**„Interní audit a kontrola jedno jsou“**

**Interní audit a kontrola jedno jsou.** To je jeden z nejrozšířenějších mýtů, který občas sami podporujeme tím, že akceptujeme práci na různých, většinou ad hoc ex post kontrolách, v rozsahu, který nám vytíží všechny kapacity pro plánované systémové audity. Audit není kontrola, nejsou to synonyma. Všichni interní auditoři to ví, ale hodně manažerů to nechápe. Ale o tomto mýtu se už napsalo hodně řádků, a proto pojďme k jinému.

**Interní auditor je neomylný.** Auditor je tou největší autoritou. Nikdo není neomylný. Přestože má profese interního auditu, na rozdíl od většiny jiných profesí, prostřednictvím Standardů IIA, vytvořen účinný nástroj pro to, aby výsledky interního auditu byly co nejobjektivnější a aby k chybám docházelo v co nejmenším rozsahu, přesto k chybám dochází a jednou z největších chyb je slabost auditorů otevřeně přiznat vlastní chybu a přijmout odpovídající opatření k tomu, aby se již neopakovala.

**Interním auditorem může být každý.** Stačí, když absolvuje základní auditorský kurz, naučí se, co to je riziko a že se aktiva rovnají pasivům… To je omyl. Interní auditor musí nejen mít poměrně hluboké znalosti o oblasti, kterou audituje, musí nejen zvládnout programování a plánování, realizování a vyhodnocování interních auditů, zabezpečení efektivní komunikace s vedením organizace, on musí především věřit, že to, co dělá, má hluboký smysl a musí být optimista s vytrvalostí Emila Zátopka…

**Interní audit je lepší než kontrola** – nebo naopak – interní auditoři ví, že se jedná o dvě odlišné činnosti, a byť občas sami vykonávají více kontrol než auditů a neuvědomují si, že tím nepřímo přispívají k šíření názoru, že kontrola je lepší než audit, na věci to nic nemění. Kontrola je inherentním prvkem managementu, tj. řízení, a jako taková je v něm vždy obsažena. Existuje i tehdy, když organizace nemá interní audit. Za nastavení a výkon kontrolní činnosti nesou odpovědnost vlastníci jednotlivých procesů. Interní audit nezávisle hodnotí, jak je tato kontrola jako systém úspěšná a jak účinně jako celek přispívá k dosahování cílů organizace. I z tohoto zjednodušeného popisu obou aktivit je zřejmé, že je možné je srovnávat z pohledu jejich zaměření, odpovědnosti za jejich výkon, kvality jejich praktické realizace apod., ale ne z pohledu, co je lepší samo o sobě. Je to jako srovnávat, zda jsou lepší vývojově starší části mozku člověka, které ovlivňují pohyb a základní reflexy, či vývojově mladší části mozku, které ovlivňují duševní činnost člověka včetně schopnosti systematického hodnocení všech kontrol našich funkcí a aktivit. Dnes prostě potřebujeme oboje stejně naléhavě.

**„Interní audit je nudná, monotónní práce s čísly a zákony“**

**Interní audit je nudná, monotónní práce s čísly a zákony** – tento mýtus ani nemusím komentovat. Jen my, kteří děláme interní audit již „nějaký ten pátek“, víme, že interní audit je velké dobrodružství a interní auditor se nikdy nenudí, i kdyby snad někdy chtěl. Auditujeme systémy a oblasti s největšími riziky, tj. s problémy, kde musíme uplatnit své zkušenosti, znalosti, a často i odvahu. Musíme naplánovat audity tak, abychom za určité období pokryli všechny nejrizikovější oblasti činnosti své organizace a rizika jsou téměř ve všech oblastech, takže jednou děláme finanční řízení, poté personální řízení, pak audit kybernetické bezpečnosti. Často nás vedení organizace pověří auditovat operace a procesy, kde něco hoří. Ano, pracujeme s čísly, zákony,

vyhláškami, interními směrnicemi a s doklady, ale především pracujeme s lidmi, a to většinou s hodně zajímavými lidmi, s kterými musíme navázat kontakt, pochopit jejich práci, vysvětlit jim svůj přístup a své závěry. A to nemluvím o konzultačních činnostech, při nichž musíme často uplatnit přímo novátorský přístup k věci, abychom mohli navrhnout „dizajn“ řídicího a kontrolního systému, který odpovídá potřebám 21. století!

**Interní audit je vlastně účetní**
– I když za vším je nějaký přímý či odvozený účetní zápis a my interní auditoři s nimi často pracujeme, protože musíme poznat, zda účetnictví věrně a poctivě zobrazuje skutečnosti a operace, které hodnotíme, není tvrzení pravdivé. Přestože snad v každém druhém auditu auditujeme účetnictví, nevystačíme si jen s účetnictvím, protože náš byznys je o něčem jiném. Naším úkolem, jak bylo v tomto článku již alespoň dvakrát řečeno, je hodnocení účinnosti systému řízení rizik, řídicích a kontrolních procesů řízení a správy organizace a to je práce, která není o „má dáti“ a „dal“. Musíme se primárně zabývat organizací činnosti, procesy v organizaci, kontrolními aktivitami a především lidmi, kteří za tím vším stojí, a to i za účtováním.

**Interní audit je nutné zlo, nikdo ho nemá rád a v podstatě ho nepotřebuje**
– to je jeden z nejrozšířenějších mýtů, kterému občas podlehne i každý z nás. IA není nutné zlo, to by si ho nejúspěšnější organizace samy a dobrovolně nezřizovaly ve všech oborech lidské činnosti. Každý sice někdy trpí masochizmem a dělá věci, které mu nesvědčí, ale o tomto důvodu pro

zřízení interního auditu jsem ještě nikde neslyšel ani nečetl v odborné auditorské či psychiatrické literatuře. Ani v těch organizacích, kde je interní audit zaveden nikoliv dobrovolně, ale na základě regulatorního či zákonného požadavku, není nutným zlem, ale pouze nástrojem, který má velký potenciál, pokud je správně dimenzován a vhodně používán.
Bylo by možné citovat manažerskou literaturu, která obsahuje příklady velmi úspěšných „symbióz“ vedení organizace a interního auditu, nebo prohlášení některých našich politiků, kteří se čas od času dovolávají dobré práce interního auditu ve sdělovacích prostředcích, ale není to potřeba. Stačí, když se zastavíme a s nadhledem se podíváme na svou vlastní práci – určitě najdeme alespoň několik auditů, které pomohly organizaci, za jejíž zájmy kopeme první ligu, aby si nedala „vlastňáka“ a aby vyhrála svůj zápas. Stoprocentně najdeme i několik lidí, kolegů, kterým naše rada pomohla a kteří nám za ni byli vděční. S auditem je to jako s řekou, kdy na začátku její cesty malé praménky a potůčky dávají člověku a krajině relativně malý a na první pohled neviditelný přínos, ale později, dál po proudu, řeka formuje krajinu a dává lidem energii a vodu, bez níž nemohou žít…

Co to je mýtus, jsme si již řekli, některé mýty o IA jsme jmenovali a u některých jsme i nepřímo naznačili, k čemu jsou dobré. Dostáváme se k tomu, jak mýty vznikají. Mýty vznikají jako vyprávění o určitých událostech, které se staly nebo které teprve mají nastat, a vysvětlují je v rámcích představ člověka o tom, jak by svět měl vypadat, aby byl spokojený. Pozitivní mýty jsou navíc symbolickým vyprávěním o něčem, co nám dává víru, že existuje celistvý a nadčasový řád, který nás uspokojí nejen materiálně, ale i duchovně. Mýty tedy tvoříme všichni. Tvoří je interní auditoři i uživatelé a příjemci interního auditu, jeho klienti. Mýty ale tvoří i ti, kteří s interním auditem nemají nebo nechtějí mít nic společného, jen často s jinou než motivací než ti druzí. Takový už je život.

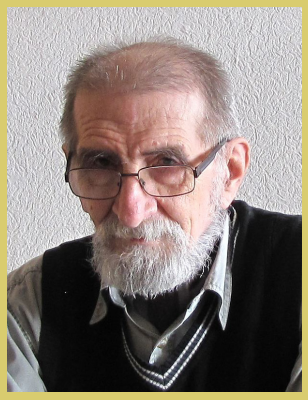
**„Interní audit je nutné zlo, nikdo ho nemá rád a v podstatě ho nepotřebuje“**

Jak tedy s mýty o IA pracovat? Je potřeba je poznávat, monitorovat, vyhodnocovat a reagovat na ně. Mýty byly a jsou součástí našeho života i naší profese. Ty **pozitivní**, které naši profesi posilují, které formou symbolického vyprávění vyjadřují víru v plnost a celistvost „nadčasového řádu“ interního auditu, **je potřeba respektovat a přidávat k nim další příběhy** úspěšných auditů a úspěšných auditorů, kterých není málo, jen se o nich zatím dost málo ví…

Ty **negativní**, které říkají zřejmé účelové nepravdy, jako třeba, že interní audit je zbytečnou nákladovou položkou, že interní audit nepatří do některých typů organizací nebo že s rozvojem ICT interní audit v dnešním slova smyslu nebude potřeba apod., je potřeba **odhalovat jako vyprávění, které je v rozporu s fakty a racionálním poznáním** (naší doby).
A oboje je velmi důležité, protože mýty jsou důležité, mohou vést k mobilizaci velkých skupin lidí i celých národů. ■

# Aby to nebyl mýtus **o Sisyfovi**

***...uvažuje PhDr. Václav Peřich, člen Čestného prezidia ČIIA od roku 1996***



Musím se rovnou přiznat, že jsem na obsah tohoto čísla Interního auditora velmi zvědavý. Slovo ***mýtus*** je totiž samo o sobě trochu zaklínadlem, provokuje představivost a poukazuje na různé roviny možných přístupů k předmětu rozpravy. Už jen ten dnes nejčastěji používaný význam tohoto výrazu – falešná představa – je mimořádně košatý, při čemž jeho rozmanitost ještě vzrůstá se složitostí daného tématu. Ne náhodou prezident IIA Richard Chambers ve svém legendárním článku o pěti mýtech spojovaných s interním auditem[1] napsal, že „*…zázemí auditorů je pravděpodobně právě tak rozmanité jako operace, které auditují*“. A v této souvislosti bych jeho myšlenku o krajním zjednodušování představ o interním auditu rád trochu rozvedl v obecnějším rámci. Zdaleka totiž nejde jen o interní auditory. V obecném povědomí převládá chápání složitosti světa jako důsledku stále pokračující dělby práce, která z nás dělá specialisty omezené na úzký okruh problémů a mající velké potíže se zaujetím nadhledu a porozuměním pro širší souvislosti. Jistě, tento proces stupňované diverzifikace stále pokračuje a v řadě ohledů představuje riziko jakéhosi babylonského zmatení, ale na druhé straně bychom neměli zůstávat nevšímaví ke zcela opačnému trendu, který dělbu práce doprovází. Stále totiž ubývá těch činností, které jsou opravdu jednooborovými specializacemi. Než začne automechanik přistavený vůz rozebírat, připojí jej k testujícímu počítači, kardiolog zvládne díky novým metodám monitorování nesrovnatelně větší okruh pacientů než kdysi, zahradník díky sofistikovaným kapkovým závlahám vystačí s daleko omezenějšími zdroji vody. Každý z nás musí ve větší nebo menší míře porozuměním nebo sdílením některých přístupů vycházet vstříc těm, s nimiž spolupůsobí nebo jejichž produkty a poznatky využívá.

Joseph McCafferty[2] na stránkách IA a IT vzdělávací společnosti MIS TI rozvíjí Chambersovu myšlenku o zjednodušeném pohledu na interní auditory ve spojitosti s velkým průzkumem IIA

ke klíčovým kompetencím interních auditorů[3]. Připomíná, že průzkum se opíral především o názory ze sebehodnocení samotných interních auditorů. Na tom pak ukazuje, že interní auditoři sami přisuzují přední místa v pořadí významnosti těm klíčovým kompetencím, které rozšiřují odborný a vyjednávací obzor interního auditora – jakými jsou komunikativnost, kritické a analytické myšlení , schopnost spolupracovat a chápat problémy vlastní organizace v proměnlivých podmínkách.

Řada dalších autorů zabývajících se dílčími mýty v souvislosti s interním auditem se pak vesměs shoduje v tom, že jsou takové jevy zpravidla odrazem narušených vazeb mezi uživateli a vykonavateli funkce interního auditu. Někdy to jsou dokonce různě zkreslené představy i uvnitř manažerské struktury dané organizace, když vrcholové vedení od interních auditorů očekává a požaduje namísto plnohodnotného plnění nezávislé objektivně ujišťovací a poradenské činnosti pouze posilování vlastních mocenských pozic. V takových situacích se bohužel banální „klasická“ falešná představa stává vážnou překážkou toho, aby interní auditoři mohli poskytovat přidanou hodnotu a plodně přispět ke zdokonalování procesů v organizaci.

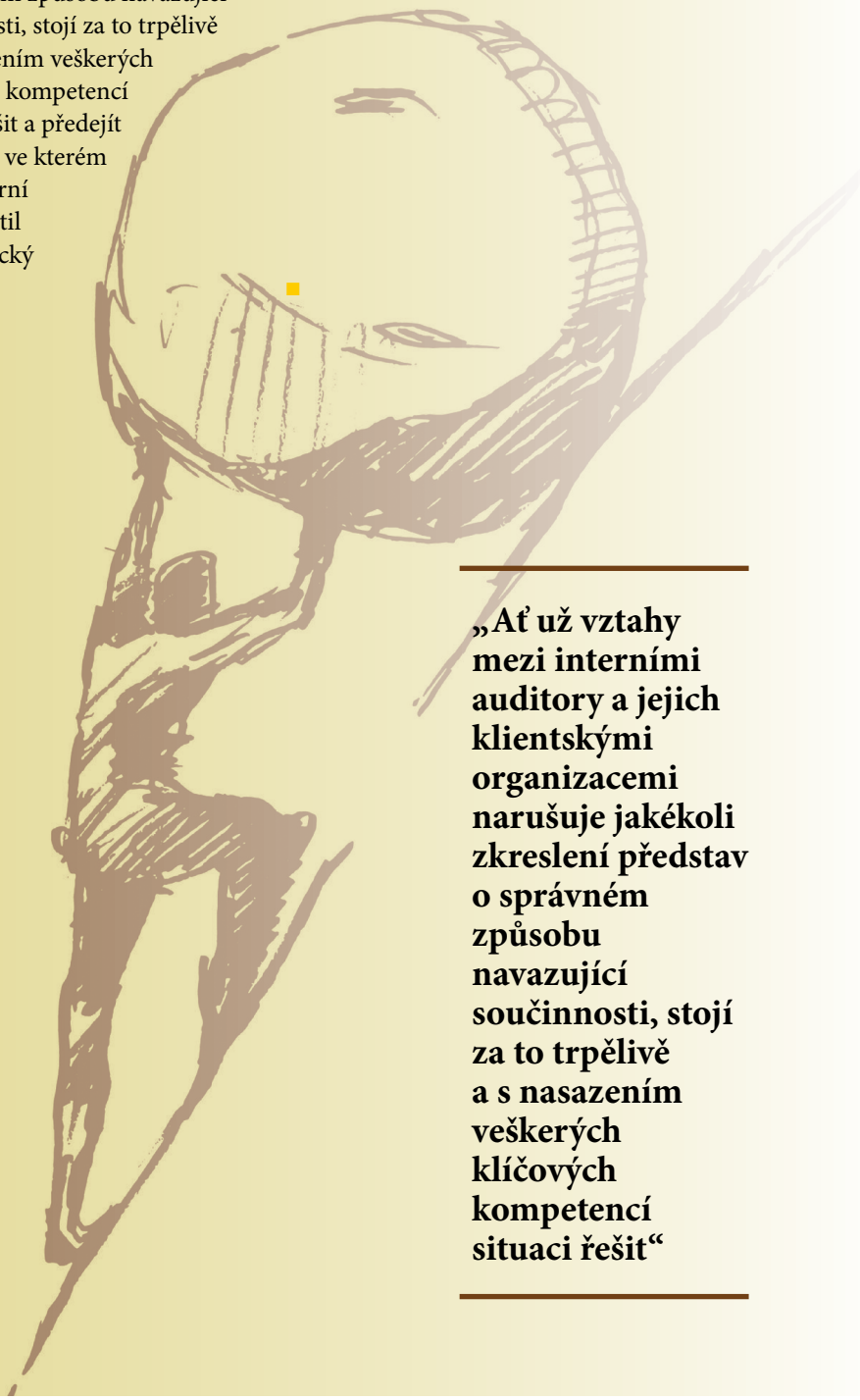
Falešná představa však nemusí být pouze na straně klienta. Za léta svého působení v oboru jsem totiž potkal více jinak dobrých a počestných interních i externích auditorů, kteří trpěli jiným postižením, totiž pocitem, že oni jsou ti „poslední spravedliví“. Měli bychom si někdy přiznat, že k posilování těch pěti mýtů Richarda Chamberse můžeme sami přispívat vlastní rigiditností, neochotou k širšímu porozumění novým podmínkám a situacím nebo snahou za každou cenu uplatnit nějaké zajímavé „zjištění“.

Ať už vztahy mezi interními auditory a jejich klientskými organizacemi narušuje jakékoli zkreslení představ o správném způsobu navazující součinnosti, stojí za to trpělivě a s nasazením veškerých klíčových kompetencí situaci řešit a předejít tak stavu, ve kterém by se interní auditor cítil jako mytický Sisyfos.

[1] CHAMBERS, Richard – Five Clasic Myths About Internal Auditing. iaonline.theiia.org/ 20.6.2012

[2] MCCAFFERTY, Joseph – Dispelling the Myth of the Introverted Internal Auditor. misti.com/internal-audit-insights/ 11.1.2016

[3] BAILEY, James A. Core Competencies for Today's Internal Auditor. The IIA Research Foundation 2010. 107 p.



**„Ať už vztahy mezi interními auditory a jejich klientskými organizacemi narušuje jakékoli zkreslení představ o správném způsobu navazující součinnosti, stojí za to trpělivě a s nasazením veškerých klíčových kompetencí situaci řešit“**

# Five Classic **Myths** About Internal Auditing

**Richard F. Chambers**
Richard F. Chambers, CIA, QIAL, C GAP, CCSA, CRMA, is president and CEO of The IIA. In Chambers on the Profession , he sh ares his personal reflections and insights based on his 40 years of experience in the internal audit profession.

**Myths can tell us a lot about ourselves — or at the least, about how others see the world. But at times it seems that the most inaccurate myths are the most difficult to dispel, particularly if there is a grain of truth buried at the origins of the myth.**

**The modern internal audit profession has been around for less than 100 years. Yet it is amazing how many myths and misperceptions have evolved about the profession in such a relatively short period of time. And while each of the following myths is generally untrue, the fact that these myths are so enduring might be an indicator that each of us needs to take stock of how we are perceived in our own organizations. Do we do things to reinforce these myths? Or, do we need to do a better job of creating awareness of how the profession has changed? You be the judge.**

## Myth #1:

**Internal auditors are accountants by training.**

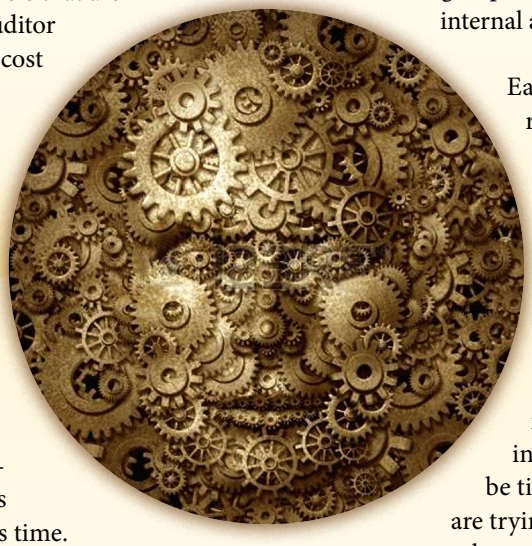
One of the most common misperceptions about internal auditing is that the auditors are all "bean counters" who focus solely on their companies' financial records. There is an obvious grain of truth in this internal audit myth: A solid audit or accounting background can be helpful for a career in internal audit. But internal auditors commonly address fraud risks, compliance issues, and a myriad of operational issues that are unrelated to accounting, and the auditors' backgrounds are likely to be as diverse as the operations they audit. An accounting degree is not the only path for career success, and these days it's not even the most common path: A recent survey by The IIA's Audit Executive Center indicates that audit executives are now recruiting job applicants with analytical/critical thinking ability, data mining skills, business acumen, and IT skills more often than they seek applicants with accounting training.

## Myth #2:

**Auditors are nit-pickers and fault-finders.**

At the heart of several jokes about internal auditors is the misperception that we are dead set on picking apart processes and ruining the reputations of the people who do the "real work." According to the myth, the auditors are viewed as the group who "bayonets the wounded after the battle is over," distracting management from more important responsibilities.

In reality, of course, internal audit's focus is on major risks rather than on nit-picking details. Audit resources are limited, and when auditors focus too much attention on minor issues, they are limiting the time available for addressing the major risks and controls that are at the heart of internal audit. Any auditor would rather report on a $6 million cost savings than on a $6 error!



## Myth #3:

**It's best not to tell the auditors anything unless they specifically ask.**

This myth can be actively damaging, so it is unfortunate the advice has made its way into more than one "How to Survive an Audit" article. Audit clients are sometimes given this advice by well-meaning friends, but it results in less efficient audits and wastes everyone's time. If auditors believe their clients are purposefully hiding information, whether by omission or commission, they normally will increase the scope of the audit to determine whether other important information has gone unreported. The purpose of internal auditing is to add value and improve an organization's operations, and hiding information is against everyone's best interests.

## Myth #4:

**Internal auditors follow a cycle in selecting their audit "targets" and use standard checklists so they can audit the same things the same way each time.**

This myth is less true with each passing year. Our professional standards require risk-based plans to determine our priorities, both in developing audit plans and schedules and in planning individual audits. Obviously some risks justify repeat audits on a regular basis, and there are some types of audits — for example, certain compliance reviews required by regulators — where audit programs and checklists are unlikely to see major changes from year to year. But in general, internal auditing has become a dynamic profession that can change any time an organization's risks change.

## Myth #5:

**Internal audit is the corporate "police function."**

As Lord Justice Topes once said, "The auditor is a watchdog and not a bloodhound." In my experience, the best auditors are almost always those who create a rapport with audit customers. When an auditor's behavior is accusing or aggressive, they are far more likely to be met with resistance than when they treat findings as an opportunity to help accomplish objectives and facilitate improvement. Breaking down this stereotype is so important that most internal audit groups actively encourage clients to think of internal audit as a coach, not a cop.

Each of these myths was closer to reality in the 20th century than today. It's easy to think of a few specific examples where an action that reinforces these stereotypes might be justified — but unfortunately, there are too many cases in which auditors are needlessly perpetuating the myths. Are any of the classic myths true about you or your internal audit group? If so, it might be time to take a good look at what you are trying to accomplish and how you plan to reach your goals.

Changing perceptions takes time, and it often requires the combined effort of many individuals to break down a stereotype. Our profession's image is rapidly improving, but more work is needed to enhance our stakeholders' understanding of the profession. Each of us can help to re-shape these myths and misperceptions, whether through small steps such as passing pertinent news information along to clients, or through larger contributions like sharing audit knowledge at a seminar or conference.

Each audit group is unique, and your perspective on these audit myths might be different from mine. Has your internal audit department recently made changes in any of the areas discussed above? If so, please let us know how it worked for you.

# Mýty v/o interním auditu

**1) S jakými mýty o/v interním auditu jste se během své praxe setkali?**

**2) Které z mýtů považujete za nejrozšířenější v současné době?**

**3) Který z mýtů může ohrozit profesi interní audit?**

**Věra Štembírková**
vedoucí Útvaru interního auditu
Olomoucký kraj

1. Obecné povědomí o práci a vlastním poslání interního auditu v obecné rovině je mizivé. Audit se běžně zaměňuje za kontrolu a jsou po něm požadovány kontrolní, a ne auditní výsledky.
2. Dosti nám uškodila prohlášení vysoce postavených úředníků, politiků či přímo novinářů, kteří za každou možnou kauzou vidí interní audit a tento svůj pohled prezentují v médiích. Prohlášení typu – pošleme tam interní audit, provádí se tam interní audit apod. – je velmi zavádějící a neodpovídá skutečnosti – protože se provádí kontrola. I když to není zrovna vůči MF spravedlivé, tak internímu auditu nepřidalo na dobré pověsti ani zřízení auditního orgánu Ministerstva financí pro oblast evropských finančních prostředků – jeho výslednou činností jsou ve většině případů podněty k finančním represím (vrácení dotace, penále apod.) což taky ovlivňuje pověst klasického interního auditu v obecném povědomí vedení organizací.
3. Zaměňuje se vlastní interní audit organizace (hlavně v územní samosprávě) s kontrolami, ať už veřejnosprávními, nebo vnitřními kontrolami prováděnými v rámci organizace. Hlavně na menších celcích se interní audit zaměňuje za kontroly a vzniká hybrid, který neodpovídá současnému popisu činnosti interního auditu podle zákona o finanční kontrole ve veřejné správě. Jak jsem už zmínila, audit se běžně zaměňuje za kontrolu a jsou po něm požadovány kontrolní výsledky, včetně protokolu a vyčíslení postihu – procesy či nastavené systémy jsou v rámci hledaného výsledku pro zadavatele interního auditu ve veřejné správě vedlejším produktem.

**Jan Brabec**
auditor/konzultant
BA Consulting

1. Interní audit není objektivní – pracovníci IA jsou „teoretici" – výstupy IA nejsou relevantní pro zlepšení situace ve společnosti (firmě).
2. Interní audit je zbytečný.
3. Všechny uvedené – nejvíce ohrožující je přesvědčení, že IA je zbytečný – velmi úzce však váže na kvalitu výstupů IA.

**Hanuš Volf**
Compliance Manager
DPD CZ s.r.o.

1. Interní auditor, pokud najde riziko či zjistí pochybení nám musí přesně říci, co máme dělat (tj. de facto supluje odpovědného manažera). Interní audit nemusí být nezávislý, můžeme auditovat i sám sebe. Kdejaká kontrola se vydává za „audit". Interní auditor musí být expert v každé oblasti, kterou audituje. Auditor má vždycky pravdu.
2. Auditor definuje zjištění i nápravné či preventivní opatření. Když budeme dělat, co auditor říká, zbavujeme se vlastní zodpovědnosti.
3. Za výsledky společnosti odpovídá interní auditor.

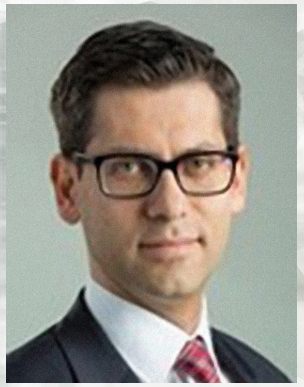
**Josef Černý**
specialista Interního auditu
Metrostav a.s.

1. **Mýtus 1** Interní audit není potřebný. Zatěžuje firmu náklady a nevytváří žádné hodnoty. Manažeři nejlépe vědí, co je třeba dělat.
**Mýtus 2** Doporučení vydaná interním auditem zvyšují administrativní zátěž společnosti. Doporučení není nutno respektovat. (Interní audit vnímán jako nepřátelský prvek hodnotící práci auditovaného subjektu.)
**Mýtus 3** Interní audit vnímán jako kontrola ve společnosti. (Ne jako nezávislý prvek ujišťovacích činností a odborný partner s komplexním náhledem na problematiku vylepšování procesů ve společnosti a ne jako nezávislý poradní názor.)
**Mýtus 4** Interní audit supluje činnost risk managementu, compliance oddělení, a případně dalších oblastí při správě a řízení společnosti.
**Mýtus 5** Program zajištění kvality IA je zbytečný. Pracovníci IA jsou dostatečně odborně vybaveni. Vzdělávání a prohlubování znalostí z oboru IA není potřebné.
2. Mýtus 1, 4, 5
3. Mýtus 1.

**Ludmila Jiráňová**
IAK, nyní již rentiér
ČHMÚ

1. MÝTY o INTERNÍM AUDITU vznikají při komunikaci osob „o interním auditu", kteří nemají základní povědomí v této oblasti. Co je INTERNÍ AUDIT? Jaké normy upřesňují používání této činnosti, jaké může být zaměření, plánování, provádění, a hlavně zpracovávání a vyhodnocení výsledků a k čemu slouží? V naší organizaci o interním auditu hovoří hlavně osoby, které nemají co dělat, jsou málo vytížené a mají volný čas během pracovní doby. MÝTY = interní audit na nic není, výsledky interního auditu se dají zneužít, auditor je ovlivnitelný, interní audit = kontrola...
2. Ani nevím, který z mýtů je nejrozšířenější. Vím, že MÝTY ROZŠIŘUJE NEZNALOST situace a problémů v oblasti INTERNÍHO AUDITU.
3. Každý z mýtů může pozici INTERNÍHO AUDITU, pokud jej budou brát lidi vážně, ohrozit. Jak se říká, na každém šprochu, pravdy trochu. Lepší je neshodám, nesrovnalostem a chybné informovanosti předcházet. Můžeme být rádi, že se o INTERNÍ AUDIT nezajímají média – rozhlas, TV, noviny... to bychom se dozvěděli zajímavosti, kterým bychom se nestačili divit.

# Frequent mistakes within a fraud investigation



**Stevan Villalobos, CFE**
CA MS | Senior Manager | Fraud Investigation & Dispute Services
Ernst & Young Audit, s.r.o.

**Most companies have at some time in the past dealt with asset misappropriation or other types of fraud that has resulted in financial or non-financial damages. Internal auditors as well as forensic auditors or legal counsels are the soldiers in the front line of the battle against fraudulent behaviour. However, has anyone thought about the investigation process retrospectively and asked the question of whether or not anything could have been done better? Could the case have been detected earlier? Could the level of financial losses have been reduced? Has all of the relevant evidence been identified, secured and collected? Have all of the individuals involved in the fraud been identified?**

**The objective of this article is to point out the frequent mistakes that are made in the preinvestigation and investigation process, and that unfortunately all too often end in financial losses being incurred, destruction of relevant evidence or greater harm being caused to a company´s reputation.**

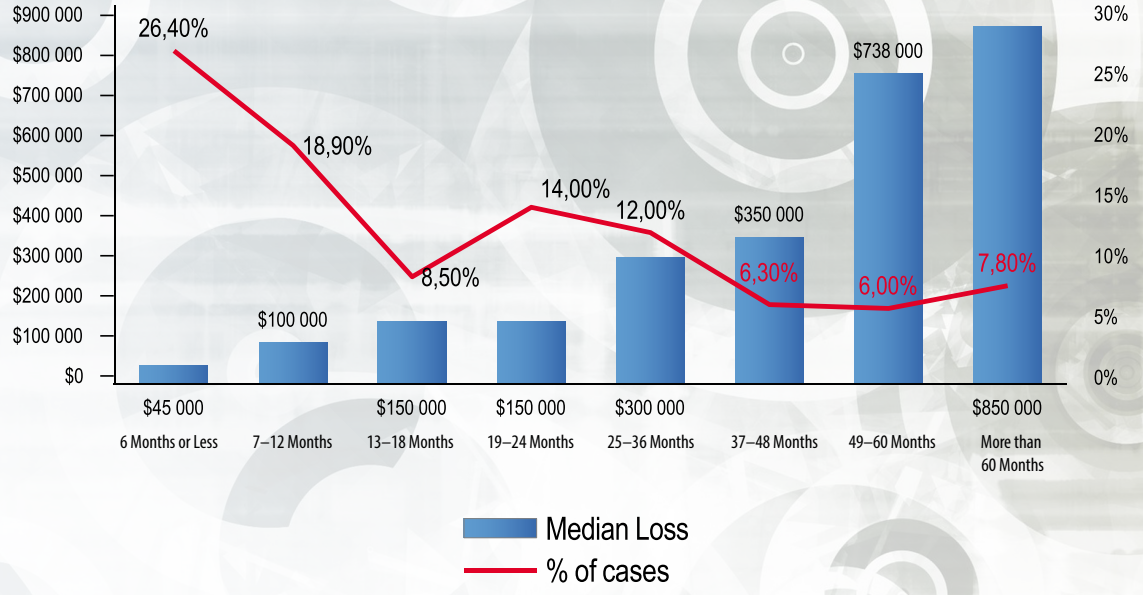
### Over-reliance on internal controls

Sooner or later, in most companies, at least one of the various types of fraud or unethical behaviour will be committed. Of course, you may have heard from many company representatives that they have comprehensive controls in place and fraud cannot happen in their company, but statistics show that this is not the case. In this respect there are simply no perfect companies, because there are no perfect people who are operating within them. So why does fraud frequently remain undetected for such long periods? Should the existing internal controls systems not help companies in early fraud detection and the fight against it? According to the recent Association of Certified Fraud Examiners (ACFE) research, only approximately one quarter of fraud is detected in its early stages, within a period of six months, while the median duration of fraud was 18 months.

Put simply, even if there is a strong internal control system in place, companies need people to perform these controls, which tend to be overlooked in the routine course of an employee's duties. It is also often the case that even if facts are visible and known, these are not spotted or adequately evaluated by employees at source, and thus the controls remain inefficient.

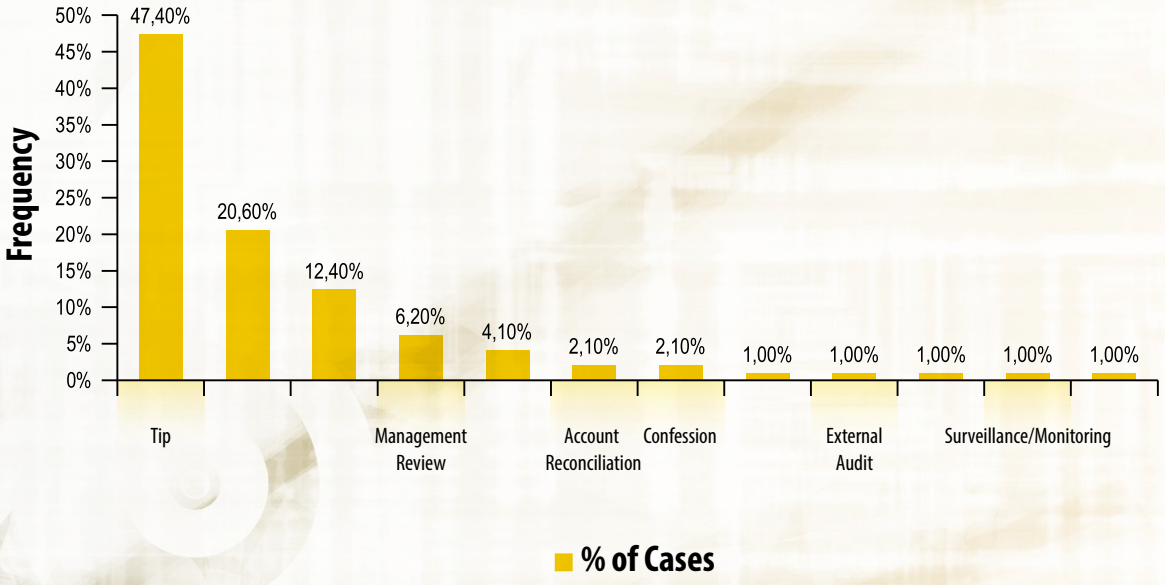
In addition, controls are usually static and not dynamic while the businesses are. In order to meet key business objectives such as profit growth or increasing market share, companies must constantly change in the business environment – develop new products, expand into new industries, hire new employees or simply follow new regulations. It is probably not such a surprise that as per the ACFE research, instead of internal controls, it is instead tips that are the most efficient method in initial fraud detection in Eastern Europe/Western and Central Asia (in 47.40% of cases in 2016) followed by the internal audit function (in 20.60% of cases in 2016). These two methods represent two-thirds of all initial fraud detection.

## Frequency and Median Loss Based on Duration of Fraud




Source: ACFE – 2016 Report to the Nations

## Detection Method by Region – Eastern Europe and Western/Central Asia




Source: ACFE – 2016 Report to the Nations

Company management should therefore not be solely reliant on existing internal controls. Controls should be simple and reasonable, because too many controls in place can turn into routine approvals, and poor control operating effectiveness can harm the actual business. The abovementioned statistics also provide enough support for justifying an internal audit role and offering the opportunity to internal or forensic auditors to periodically review and assess existing controls by issuing recommendations and from time to time adjusting internal controls in order to react to the dynamic business environment.

### Inadequate fraud response plan

Once a suspicion or allegation of fraud exists the key question is what should be the first and second steps in dealing with this. Who has the relevant information and what should they do with it? Many mistakes are made in the initial stages, because companies are often not well prepared for unexpected situations like this which then causes delays in the response and, if the response is prepared, is frequently inadequate for the risks identified.

Have you ever seen a jet pilot face unpredictable situations? the first thing they always do is take the jet emergency mode and follow the emergency manual step by step, because a jet is a complex machine and not doing so could have fatal consequences. It is the same with companies, but how many of you have written rules and procedures for how to handle fraud situations (a 'Fraud response plan'), and do your employees know them all?

Each mid or large sized company should therefore introduce and maintain a fraud response manual which should at least address basic questions such as:

**1. Who should be contacted first?**

**2. Who should evaluate a suspicion or allegation?**

**3. What should be the composition of the fraud response team?**

**4. What should be the scope and what areas should the procedures of fraud response concentrate on?**

**5. What should be the timing of the response?**

Officially appoint someone in your company who will serve as the primary contact – it can be a direct supervisor of the employee, a compliance officer or you could have an anonymous whistleblowing hotline. There is no one perfect solution and each company should assess and select the most appropriate and suitable, because there are still many instances where management is not informed or informed too late, or the information is shared with too many stakeholders and leaks to the suspect.

There can be cases when a suspicion or allegation is raised with the objective of harming the suspect, so once the suspicion or allegation is reported, it should be evaluated for its relevancy. Set up a working group – more brains with different sets of experience (management, legal, forensic, audit or information technology) can come to more qualified conclusions, because you should avoid starting an investigation without simple verification of the key facts.

If the fraud suspicion or allegation is found to be relevant with reasonable grounds, the investigation plan should be put together in cooperation with investigation experts.

## The first 48 hours

The timing of the response is highly relevant as according to historical observations, the first 48 hours after the suspicion or allegation of fraud are crucial for evaluation and investigation planning. As protecting the company's assets is one of the key responsibilities of management boards, key decisions should be made quickly. The more the response is delayed, the higher the risk that the fraudster will destroy any available evidence, continue in malpractices or hide fraud-related proceeds.

Poor investigation planning can discredit the whole investigation process and its benefits. The most frequent mistakes resulting from poor planning can be:

1. **The suspect is informed about being investigated at an early stage**
2. **The relevant sources of evidence are not quickly secured and as a result destroyed**
3. **The investigation scope is too narrow or too complex**
4. **The investigation team digs too deep in irrelevant areas**
5. **The investigation does not consider that the suspect may have accomplices**
6. **The full scale of damages is not determined**
7. **The investigation is assigned to the wrong group, for example when the team does not have enough experience with the specific issues**
8. **The evidence is not gathered in a way that is in compliance with local legislation and would be rejected by the court**

Having reasonable grounds for investigation but losing the opportunity to secure potentially relevant evidence is, together with sharing the suspicion with the suspect too early, probably the worst mistakes that can be made. Relevant evidence can inevitably be damaged when the suspect is informed that they are being investigated and the company will only have a few alternative means of recovering from the damage. The investigation committee should also evaluate where the potential evidence could be found in hard copy or in electronic form, and identify all potential electronic data storage devices (such as laptops, DVDs and USBs, server data or mobile phones) and all locations (such as the suspect's office, archives or regional branches) which may be related to this.

If the investigation's scope did not properly address the suspicion or allegation, the company would probably lose the opportunity to determine all existing damages. On the other hand, an excessive scope can turn out to be too costly compared to the potential damage and can also result in the investigation of areas that are irrelevant from the investigation perspective.

It is very important to identify all of the individuals that were involved directly or indirectly in the fraudulent behaviour. Doing this may significantly contribute to the identification of additional evidence and clarification of the full fraud scheme. Therefore, the investigation team should work with the assumption that the suspect was not alone.

There are situations in which internal teams such as internal auditors or lawyers are leading the investigation process, because they know the company and its environment very well and can efficiently contribute to the smooth closing of the case. On the other hand, if the investigation is too complex, they may need to engage external investigation experts. Assigning the investigation to an inexperienced team can lead to unprofessional performance of the investigation procedures, such as the review of documentation or the interview with the suspect. The gathered evidence should also be collected in line with the existing legislation. By not doing so, it may later appear useless because illegally gathered evidence may not be accepted by the court and can also result in investigation by the authorities. It can then be the company and not the suspect who is punished.

Most of the investigation risks described above can be properly managed, and so setting up an investigation committee may be a good idea. The investigation committee could comprise a responsible board member, internal or external legal counsel, IT specialist, internal and external investigation experts, process owners and others if relevant. The number of internal members involved should be justifiable as the more employees who are informed about the suspicion, the higher the risk of information leakage.

Some investigations can be very complex and planning is essential in efficiently managing the process and protecting the company's assets. There is always a risk that when losses are not recovered, the owners will be challenging the management and their responsibility to act with due care. The task of the investigation committee will be to define the investigation scope and team while taking into consideration the balance between potential losses and investigation costs.

Fraud detection and investigation is not an easy process and many things can simply go wrong.

# Mýty a fakta o deliktní odpovědnosti právnických osob

**Mgr. Bc. Jan Spáčil, LL.M.,**
advokát, vedoucí partner advokátní kanceláře,
Ambruz & Dark Deloitte Legal

**Mgr. Hana Erbsová**
právník, Ambruz & Dark Deloitte Legal

Deloitte. Legal

**Nedávno jsme si mohli připomenout páté výročí účinnosti zákona o trestní odpovědnosti právnických osob a řízení proti nim (zákon č. 418/2011 Sb., „TOPOZ“). Přestože přijetí této normy provázely živé diskuze odborné veřejnosti, samotný zákon vstoupil do života spíše nesměle.**

**Nahlíženo zpětně se však zdá, že ačkoliv nás zřejmě nečeká razantní skok v počtu stíhaných právnických osob (k jakému došlo například ve Francii), *zákon přesto v právním prostředí své místo našel a působí v něm silou oné pověstné tiché vody, která mele břehy*.**

Nedávná novelizace TOPOZ, účinná od prosince 2016, relativně zúžila okruh osob, jejichž jednání je trestně přičitatelné právnické osobě (v některých kategoriích pouze na osoby ve vedoucím postavení). Současně také posílila možnost tzv. vyvinění právnické osoby. Právnická osoba se ve vztahu ke všem fyzickým osobám, jejichž jednání jí lze přičítat, může zprostit trestní odpovědnosti, pokud se jí podaří prokázat, že vynaložila veškeré úsilí, které na ni bylo možno spravedlivě požadovat, aby spáchání protiprávního činu zabránila, a to včetně povinné nebo potřebné kontroly zaměstnanců. Ačkoliv význam této změny byl potvrzen vydáním speciální metodiky Nejvyšším státním zastupitelstvím, z její podstaty je zřejmé, že od ní lze jen těžko očekávat revoluci ve statistikách.

Kolekce trestných činů, za které byly doposud právnické osoby pravomocně odsouzeny, ponechává prozatím v rovině mýtů obavy z účelové kriminalizace nebo ze zneužívání trestních oznámení v konkurenčním boji. Faktem totiž je, že podle statistik Ministerstva spravedlnosti bylo v letech 2012 až 2016 pravomocně odsouzeno za trestný čin sotva 190 právnických osob; přitom jen obchodních společností je evidováno přes 400 000. Celkový počet „usvědčených pachatelů“ sice vykazuje mírně stoupající tendenci, ale roste tempem cca třiceti případů ročně. Vezmeme-li v potaz počet trestně stíhaných právnických osob v letech 2013 až 2015, pak pravomocným odsouzením končí jen sotva polovina zahájených trestních stíhání.

**„Pravomocným odsouzením končí jen sotva polovina zahájených trestních stíhání“**

Zjevně k nejpilnějším oznamovatelům podezření na spáchání trestného činu právnickou osobou patří státní orgány

spravující daně, pojistné a podobné povinné platby do veřejných rozpočtů. Nejčastěji totiž až dosud padaly tresty za zkrácení nebo za neodvedení daně, pojistného na sociální zabezpečení a podobné povinné platby (celkem 92 případů), dále pak za trestný čin podvodu (56 případů) a za zkreslování údajů o stavu hospodaření a jmění (12 případů). Celkem se ve statistikách zatím objevuje méně než 15 skutkových podstat trestných činů, a kromě výše uvedených se jejich četnost počítá v jednotkách případů ročně.

Ukládané tresty odrážejí podstatu stíhaných činů, a mají proto zatím převážně represivní charakter. Nejčastěji byl uložen trest zákazu činnosti (64x), peněžitý trest (61x) a trest zrušení právnické osoby (24x). Posledně zmíněná sankce je však často spíše než trestem jen jakýmsi úklidovým opatřením, jímž je formálně ukončena existence již fakticky nefunkčního subjektu. Zájem na další činnosti právnické osoby, jejíž pověst i majetková podstata je pravomocným odsouzením zásadně dotčena, ze strany jejích členů pochopitelně není valný. Otázkou zůstává, zda i k tomuto účelu byl trest zrušení právnické osoby určen a má být takto užíván (byť nelze v tomto přístupu pominout jistý prvek hospodárnosti).

**„V souvislosti s TOPOZ je stále na místě hovořit spíše o ‚deliktní prevenci' než o hrozbě trestu"**

V aplikaci TOPOZ se projevují i regionální rozdíly, když jednoznačně nejvíce pravomocně ukončených řízení je evidováno v Praze a Jihomoravském kraji, zatímco zbytek republiky, snad s výjimkou Středních Čech, svou aktivitou zaostává.

Z výše uvedeného lze usoudit, že **v souvislosti s TOPOZ je stále na místě hovořit spíše o „deliktní prevenci" než o hrozbě trestu.** Právě v této oblasti pak hraje nezastupitelnou roli interní audit. Jeho význam ještě stoupne, až v červenci letošního roku nabude účinnosti nový zákon o odpovědnosti za přestupky a řízení o nich (**zákon č. 250/2016 Sb.**). Tento zákon totiž **do oblasti správního trestání zavádí princip odpovědnosti právnické osoby za přestupky spáchané fyzickými osobami, jejichž jednání je právnické osobě přičítáno.** Okruh fyzických osob, jejichž jednání může být přičteno k tíži právnické osoby, je dokonce širší, než jak jej vymezuje TOPOZ, a zahrnuje:

- všechny orgány právnické osoby, resp. všechny jejich členy,
- fyzické osoby, které jednají za právnickou osobu (avšak jen pokud právnická osoba výsledku takového jednání využila),

- zaměstnance nebo osoby v obdobném postavení při plnění úkolů vyplývajících z tohoto postavení, a
- fyzické osoby, které plní úkoly právnické osoby nebo které právnická osoba používá při své činnosti.

**„Potřeba investic do prevence, firemní kultury a jejich účinné kontroly je zjevně čím dál naléhavější"**

Výše uvedené osoby nemusí mít v rámci právnické osoby vedoucí postavení ani vykonávat rozhodující vliv na její řízení.

Odpovědnost právnické osoby za přestupek přechází na všechny její právní nástupce, nicméně v odůvodněných případech může dokonce správní orgán v rámci řízení o přestupku zakázat zrušení, zánik nebo přeměnu právnické osoby (což může přicházet

**„Možná, že právě teď přichází doba, kdy bude definitivně zbořen i mýtus, že interní audit a ostatní součásti compliance programu jsou prostě jen další nutná administrativa“**

v úvahu zejména u přeshraničních přeměn, kdy má být právním nástupcem zahraniční osoba).

I zde však zákonodárce umožňuje, aby se právnická osoba své odpovědnosti zprostila, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby přestupku zabránila. Samotná prevence však rozhodně nestačí. Právnická osoba musí také doložit, že vykonávala povinnou nebo potřebnou kontrolu nad fyzickou osobou, jejíž jednání je jí přičítáno, a že učinila nezbytná opatření k zamezení nebo odvrácení přestupku.

Otevírá se tak nový rozsáhlý prostor, v němž se může projevit klíčový význam interního auditu. Zásadním způsobem se totiž rozšiřuje okruh jednání, která mohou být potencionálně přičtena k tíži právnické osoby, a v konečném důsledku ji poškodit. Skrytá záludnost odpovědnosti právnické osoby za přestupky spočívá i v tom, že nejméně do roku 2022 bude stále možné, aby přestupky projednávaly – a odpovědnost právnických osob v této oblasti posuzovaly – úřední osoby bez právnického vzdělání, resp. bez zkoušky odborné způsobilosti v dané oblasti.

Preventivní opatření, předvídaná v TOPOZ i v novém zákoně o odpovědnosti za přestupky, nejen potencionálně umožňují právnické osobě zprostit se odpovědností za přestupek či trestný čin, ale pokud i přes veškerou snahu k trestnému jednání dojde, zvyšují pravděpodobnost, že se podaří dosáhnout zániku této odpovědnosti včasnou následnou reakcí (tzv. účinnou lítostí).

Taková opatření však musí být vždy „šita na míru“ dané právnické osobě a samozřejmě nesmí být jen ryze formální. Stěžejním pojmem je v této souvislosti zejména firemní kultura, resp. tzv. compliance management system, jakožto ucelený soubor norem, opatření a aktivit zajišťujících mimo jiné i deliktní prevenci. Nezbytnou součástí tohoto mechanizmu je také nezávislá kontrola a vyhodnocování jeho funkčnosti, což jsou právě úlohy naplňované interním auditem. Vzhledem k objemu informací, které je nutné v rámci tohoto systému zpracovávat a monitorovat, však **stále významnější roli hraje také automatizace procesů analýzy rizik a compliance.**

**Dovozování odpovědnosti za jednání, jehož se dopustil někdo jiný, není však jen doménou trestního práva.** I v daňovém řízení v poslední době správci daní vyžadují předložení důkazů o tom, že plátce daně přijal veškerá opatření, která po něm lze rozumně vyžadovat, aby se ujistil, zda obchodní vztah, do nějž vstupuje, nemůže být dotčen daňovým únikem. Pokud nechce takový plátce platit znovu daň, kterou nedovedl někdo jiný, musí prokázat, že podmínky dané obchodní transakce byly rozumně vysvětlitelné především legitimními ekonomickými důvody, a nikoliv pouze daňovým únikem. Naštěstí i v této oblasti již existují systémy, které umožňují podstatnou část této agendy provádět automatizovaně.

Výše zmíněný komplex prevence před vznikem deliktní odpovědnosti právnické osoby (jakož i případné odpovědnosti orgánů obchodní společnosti za porušení povinnosti vykonávat funkci s péčí řádného hospodáře), by měl tedy ideálně zahrnovat

- určení rizikových oblastí a odhad míry tohoto rizika,
- stanovení vnitřních norem a opatření k prevenci zjištěných rizik,
- zapojení automatizace do procesů analýzy rizik,
- určení odpovědných osob, nastavení komunikačních procesů (včetně ochrany oznamovatelů protiprávního jednání) a průběžné dokumentace procesů,
- školení členů orgánů i zaměstnanců,
- úpravu příslušné smluvní dokumentace (smlouvy o výkonu funkce, pracovněprávní, ale i obchodní smlouvy atd.),
- kontrolu funkčnosti systému, analýzu nedostatků a zapracování úprav.

Potřeba investic do prevence, firemní kultury a jejich účinné kontroly je zjevně čím dál naléhavější a získává stále reálnější obrysy. Současně s tím roste i poptávka po automatizovaném řešení některých procesů. Možná, že právě teď přichází doba, kdy bude definitivně zbořen i mýtus, že interní audit a ostatní součásti compliance programu jsou prostě jen další nutná administrativa. ■

# BEZPEČNOSTNÍ OPATŘENÍ podle zákona o kybernetické bezpečnosti

## – 2. část – technická opatření

**Pokračování série příspěvků věnovaných problematice kybernetické bezpečnosti z pohledu garanta zaměřené na bezpečnostní opatření dle zákona o kybernetické bezpečnosti. I přes rozdělení tohoto článku na dvě části, věnované v prvním případě organizačním a ve druhém případě technickým opatřením, se nelze vzhledem k rozsáhlosti problematiky bohužel věnovat všem opatřením s takovou mírou detailu, kterou by zasluhovaly.**

**Ing. Lukáš Kintr**
Cyber Security/Policy Specialist, Auditor
Národní bezpečnostní úřad – Národní centrum kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti (dále ZKB či Zákon) prostřednictvím svého prováděcího právního předpisu, vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti (dále VKB či Vyhláška) povinným orgánům a osobám uvedeným v § 3 Zákona ukládá řadu povinností, mezi kterými je mimo jiné zavedení bezpečnostních opatření. Dle ZKB jsou bezpečnostní opatření členěna do dvou základních skupin, a to na **organizační opatření**, která byla předmětem 1. části tohoto článku v čísle 4/2016, a **technická opatření**, na která se zaměřují následující řádky.

### TECHNICKÁ OPATŘENÍ

#### Fyzická bezpečnost

Opatření požadovaná VKB pro zajištění fyzické bezpečnosti vynucují přijetí pravidel a postupů vedoucích k zamezení neoprávněného vstupu do vymezených prostor – prostor ve kterých jsou zpracovávána nebo umístěna aktiva (jinými slovy informace a technické prostředky). Dále, pravidla, která zamezí neoprávněnému nakládání/zásahům, poškození či krádeži těchto aktiv. Po správci KII je dále požadováno uplatňování prostředků fyzické bezpečnosti na úrovni objektu a v jeho rámci. Poněkud obecná formulace však nezastupuje nic jiného než běžně využívané systémy zabezpečení počínaje např. oplocením areálu, vrátným a konče třeba u čidel pro hlášení požárů a v případě serveroven na ně navázaných samočinných hasicích systémů. Praxe ukazuje, že hlavní rozdíl v zabezpečení prvků KII a VIS není ani tak ve škále použitých prostředků, jako spíše v jejich přísnější parametrizaci, samozřejmě vždy s ohledem na možnosti dané povinné osoby.

**„Je třeba uvažovat racionálně a implementovat pouze opatření relevantní vzhledem k zabezpečovanému systému“**

### Nástroj pro ochranu integrity komunikačních sítí

Sousloví „nástroj pro ochranu integrity komunikačních sítí“ může znít poněkud abstraktně. Principy, na kterých stojí opatření v této oblasti, jsou ale zcela konkrétní. Těmi hlavními požadavky jsou zajištění řízení bezpečného přístupu do sítě a její segmentace – rozdělení na více fyzicky či logicky oddělených segmentů, zejména pak zřízením demilitarizované zóny, sloužící pro služby s prostupem z a do vnější sítě. Dalším požadavkem je poté zabezpečení vzdáleného přístupu užitím kryptografických prostředků – šifrování komunikace. Poslední bod tohoto paragrafu pak definuje potřebu na „filtrování“ síťového provozu, respektive odstranění přenášených dat v nevalidním formátu.

### Nástroj pro ověřování identity uživatelů

VKB pro správce IS/KS KII a VIS určuje povinnost užití nástroje pro ověřování identity uživatelů a administrátorů, přičemž pro případy ověřování identity heslem definuje požadavky na komplexnost užívaných hesel (použití různých skupin znaků, minimální délka hesla a jeho expirace). Pouze pro správce IS/KS KII definuje přísnější požadavek na délku hesel administrátorů. Je ale dobrou praxí tento požadavek aplikovat i v případě VIS a podobně je tomu také s dalšími opatřeními definovanými pouze pro systémy KII, kterými jsou zamezení opakovaného použití dříve užitých hesel, omezení možnosti měnit heslo častěji než jedenkrát za 24 hodin a nutnost opětovně ověřit identitu po určité době nečinnosti. Vyhláška počítá také s možností zajištění ověřování identity uživatelů jiným než běžným způsobem (heslem). Klade při tom důraz pouze na to, aby toto ověřování zajišťovalo minimálně stejnou úroveň zabezpečení jako systémy plnící výše popsané principy (v úvahu tedy připadají vícefaktorové autentizace, biometrické systémy aj.).

### Nástroj pro řízení přístupových oprávnění

Povinné osoby (správci systémů KII a VIS) mají v souladu s VKB využívat nástroj pro řízení přístupových oprávnění v několika rovinách. Pro všechny typy systémů mají být řízena oprávnění na úrovni jednotlivých aplikací, dat a dále pro čtení dat, zápis dat a změnu těchto přístupových oprávnění. Výše popsané nástroje musí v případě prvků KII dále zaznamenávat použití těchto oprávnění v souladu s bezpečnostními potřebami správce a výsledky objektivního hodnocení rizik.

### Nástroj pro ochranu před škodlivým kódem

Cílem požadavků na užití nástroje pro ochranu před škodlivým kódem je zajištění ochrany komunikace mezi vnitřní a vnější sítí (v návaznosti na segmentaci aj.), ochrany serverů, sdílených datových úložišť a pracovních stanic. Nedílnou součástí provozu takových nástrojů je jejich pravidelná aktualizace (mj. aktualizace signatur a definic). Praxe ukazuje, že absence aktualizací a kontrola výstupů z těchto a dalších nástrojů (viz další kapitoly) je častým nedostatkem.

**„Většina opatření s sebou přináší také potřebu finančních a jiných prostředků“**

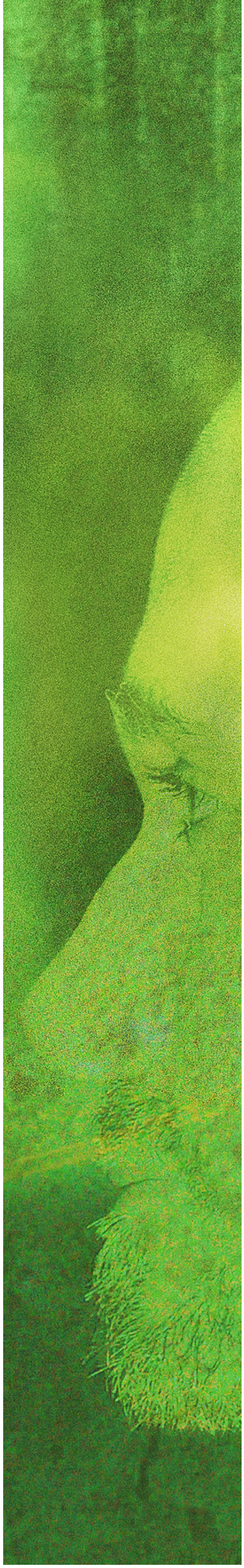
### Nástroj pro zaznamenávání činnosti KII a VIS, jejich uživatelů a administrátorů

VKB shodně pro prvky KII a VIS požaduje nasazení a provozování nástroje pro zaznamenávání zejména následujících činností:

- **systému** – záznam o provozních, konfiguračních a bezpečnostních činnostech,
- **uživatelů a administrátorů** – přihlášení/odhlášení (všeobecně použití mechanizmů identifikace a autentizace, včetně změny přihlašovacích údajů), činnosti provedené administrátory, změny nastavení oprávnění, snaha o činnosti nad rámec přidělených oprávnění atd.,
- **technických aktiv** – zahájení a ukončení činnosti.

Přičemž velice důležitou roli hraje jednak ochrana těchto informací před jejich změnou či smazáním, ale také jejich obsah. Tyto záznamy by v souladu s nejlepší praxí a VKB (navzdory nešikovné formulaci) měly obsahovat minimálně identifikaci uživatele a stroje, ze kterého uživatel přistupuje, činnost a její výsledek (úspěšné/neúspěšné vykonání), identifikaci technického aktiva, které činnost zaznamenalo a datum s časem. Nutné je tedy pravidelně synchronizovat jednotný systémový čas technických aktiv, aby bylo možné pracovat s nimi napříč infrastrukturou a v neposlední řadě také zaznamenávat přístupy k těmto informacím a veškeré pokusy o manipulaci s nimi.

Zvláštní je fakt, že požadavek na dobu uchování výše popsaných záznamů na dobu minimálně 3 měsíců je pouze u systémů KII a pro VIS tato doba není nijak definována.



### Nástroj pro detekci kybernetických bezpečnostních událostí (KBU)

Funkcí výše uvedeného nástroje dle VKB má být ověření, kontrola a případně zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí, avšak to vše v souladu se stanovenými bezpečnostními potřebami a výsledky hodnocení rizik správce. Tuto funkci tak může například plnit systém firewallů a IDS[1]/IPS[2]. Nad rámec toho má správce KII povinnost tento systém používat také v rámci vnitřní komunikační sítě a mezi servery patřícími do rozsahu systémů KII.

### Nástroj pro sběr a vyhodnocení KBU

Zákonná povinnost dopadající pouze na správce systému IS/KS KII cílí na zřízení a provoz nástroje typu SIEM. Tento nástroj má zajistit integrovaný sběr a průběžné vyhodnocování KBU, měl by poskytovat sadu reportů pro jednotlivé bezpečnostní role a na základě průběžného vyhodnocování být schopný včasného varování. Správce má povinnost pravidelně aktualizovat a zdokonalovat pravidla pro automatické vyhodnocování KBU, a minimalizovat tak falešná varování. Pravidelné reporty by poté měly být jedním z podkladů pro zdokonalování celého systému řízení bezpečnosti informací.

### Aplikační bezpečnost

Všeobecnou povinností (platnou jak pro správce KII, tak pro správce VIS) v oblasti aplikační bezpečnosti je provedení bezpečnostních testů aplikací dostupných z vnější sítě před jejich uvedením do provozu a poté v případě zásadních změn. Správce KII musí nad rámec předcházejícího zajistit trvalou ochranu aplikací a informací dostupných z vnější sítě (před jejich neoprávněnou změnou, činností, popřením nebo kompromitací) a také transakcí (před jejich nedokončením, špatným směrováním, změnou, neautorizovaným opakováním či kompromitací).

[1] Intrusion Detection System – systém pro detekci průniku.
[2] Intrusion Prevention System – systém pro prevenci průniku.

### Kryptografické prostředky

Správce KII/VIS musí dle VKB stanovit úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu a pravidla kryptografické ochrany informací v závislosti na typu média pro jejich uložení/přenos. V souladu s výsledky hodnocení rizik (vlastními bezpečnostními potřebami) musí být nasazeny a používány dostatečné kryptografické prostředky, které zajistí ochranu důvěrnosti a integrity předávaných/ /ukládaných dat, včetně identifikace jejich původce. I v této oblasti má správce KII definované další povinnosti. Musí stanovit a provozovat systém správy klíčů, včetně všech jeho náležitostí (generování, distribuci, archivaci, ničení, změn, auditu atp.). Dále má vycházet z vyhláškou definovaného seznamu odolných kryptografických algoritmů a případně řídit rizika související s jinými užitými algoritmy. Vzhledem k dynamickému vývoji v oblasti ICT se však tento taxativní výčet algoritmů jeví jako ne zcela funkční a efektivní řešení.

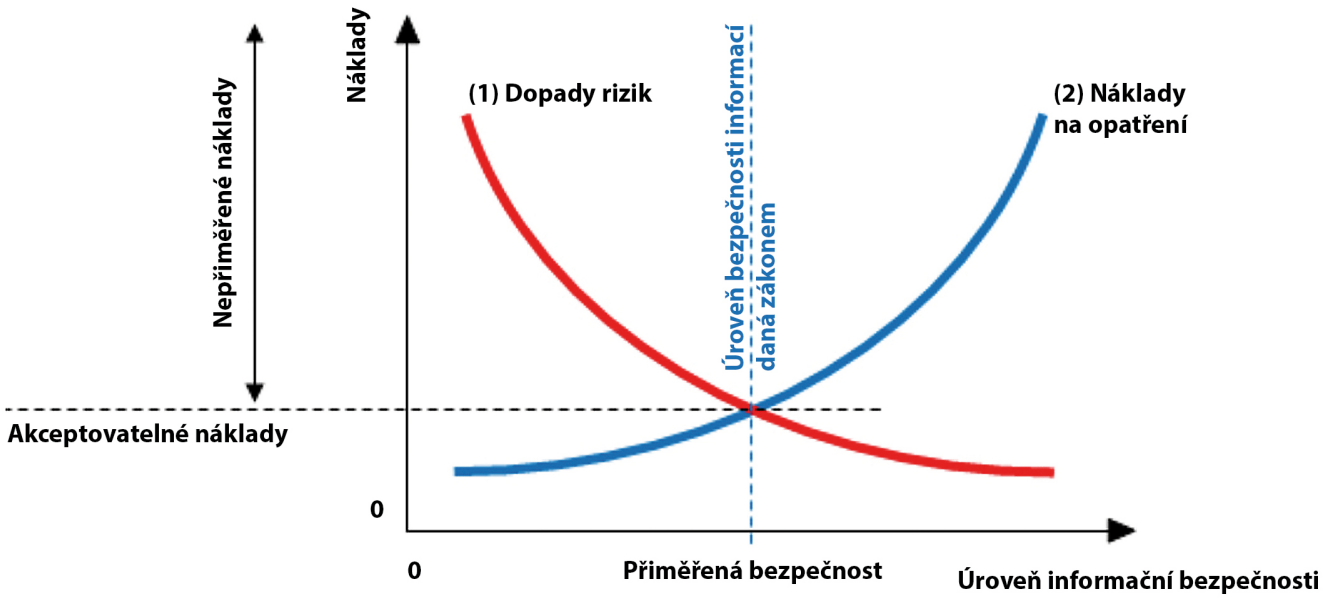
### Nástroj pro zajišťování úrovně dostupnosti

V souladu s výsledky hodnocení rizik musejí správci KII/VIS zajistit úroveň dostupnosti. Nástroj (systém) zajišťující tuto úroveň může představovat například zajištění redundantní infrastruktury, může souviset s mechanizmy na ochranu před DoS útoky apod. Pro prvky KII, respektive jejich správce, jsou v rámci VKB na tento zmiňovaný nástroj definovány konkrétní požadavky. Má být volen tak, aby splňoval potřeby řízení kontinuity činností, zajistil odolnost vůči kybernetickým útokům cílícím na snížení jeho dostupnosti a záložní řešení, ať už formou provozování redundantní infrastruktury, nebo smluvně či jinak zajištěné dostupnosti náhradních komponent v definovaném časovém intervalu.

### Bezpečnost průmyslových a řídicích systémů

Tato oblast opatření je určena pouze pro ICS/SCADA systémy, které jsou prvkem KII nebo jsou jeho součástí. Z mého pohledu v tomto odstavci VKB nepřichází s ničím, co by nebylo pokryto již v předchozích bodech (např. omezení fyzického

## Odvození nepřiměřených nákladů




(Zdroj: *https://www.govcert.cz/download/kii-vis/container-nodeid-738/neprimerenenaklady.pdf*)

přístupu k síti a zařízením nebo havarijních plánů – plánů pro obnovení chodu). Potřeba vytvořit pro tyto systémy samostatný odstavec v rámci VKB pramenila patrně z odlišnosti ICS/SCADA od běžných ICT systémů.

### Shrnutí a doporučení

Kromě celé řady alternativních možností plnění požadavků na zavedení jednotlivých opatření může povinná osoba prokázat plnění opatření podle ZKB (VKB) pomocí certifikace podle ČSN ISO/IEC 27001:2014 za předpokladu, že určený systém KII nebo VIS je zcela zahrnut v rozsahu certifikace.

**Závěrem několik doporučení, jak postupovat a čemu se vyvarovat při implementaci bezpečnostních opatření:**

1. Je třeba uvažovat racionálně a implementovat pouze opatření relevantní vzhledem k zabezpečovanému systému. Jaký má například smysl zavádět politiku mobilních zařízení v případě, že pro přístup k zabezpečovanému systému nelze využít ani notebook, ani žádné jiné mobilní zařízení?
Pro tyto účely má být sestaveno prohlášení o aplikovatelnosti (ve formě definované normou ISO/IEC 27 001), v jehož rámci je možné v relevantních případech zdůvodnit, proč je dané opatření v rámci konkrétního systému neaplikovatelné.

2. Zaváděná opatření by měla vždy vycházet z výsledků analýzy rizik, kterou by měla respektovat. Nicméně většina opatření s sebou přináší také potřebu finančních a jiných prostředků. Při jejich zavádění bychom tedy měli brát v potaz:
a) přiměřenost vynaložených nákladů vzhledem k přínosu pro zabezpečení – vynaložené náklady by měly mít odpovídající přínos po stránce zabezpečení, pokud je tento přínos sporadický, jsou na místě úvahy, zda takové opatření má smysl zavádět (viz graf Odvození nepřiměřených nákladů).
b) V případě omezených možností (zdrojů) postupovat dle kritičnosti a priorit (pracovat s plánem zvládání rizik).

3. Při zavádění jednotlivých opatření se nemusí vždy začínat od začátku.
Je vhodné využít již zavedených a ověřených, byť třeba jen dílčích částí a principů. Ve většině případů lidé snáze přijmou změnu již zavedeného než něco zcela nového. ■

**Ing. Andrea Lukasíková, CIA, CGAP**
kanova.andrea@gmail.com

# Čeho si *Andrea* povšimla *aneb* **co se děje na mezinárodní scéně**

Věděli jste o tom, že květen je měsícem interního auditu? Mezinárodní institut interních auditorů vyzývá své členy, aby v tomto měsíci, ale i po celý rok, informovali o tom, co vlastně interní audit dělá a co to může přinést a jak pomoci všem zainteresovaným stranám. Užitečnou pomůcku s návodem jak úspěšně šířit pozitivní zprávy o interním auditu naleznete zde: *https://global.theiia.org/about/about-internal-auditing/Pages/International-Internal-Audit-Awareness-Month.aspx?utm_source=SilverpopMailing&utm_medium=email&utm_campaign=20170488_Global_LeadersLink_051917%20(1)&utm_content=&spMailingID=15171318&spUserID=NjM5Njg4NjQzODcS1&spJobID=983594412&spReportId=OTgzNTk0NDEyS0*

Porozumění a audit velkých datových souborů je téma nového příručky vydané Mezinárodním institutem interních auditorů. V dnešní době masivního zpracovávání velkého množství dat jistě užitečná pomůcka pro nejednoho interního auditora. Bližší informace naleznete zde: *https://global.theiia.org/about/about-internal-auditing/Pages/International-Internal-Audit-Awareness-Month.aspx?utm_source=SilverpopMailing&utm_medium=email&utm_campaign=20170488_Global_LeadersLink_051917%20(1)&utm_content=&spMailingID=15171318&spUserID=NjM5Njg4NjQzODcS1&spJobID=983594412&spReportId=OTgzNTk0NDEyS0*


Jste účetním expertem, který momentálně pracuje jako interní auditor a přemýšlíte, jak by se vaše znalosti a zkušenosti daly využít pro dobrou věc? IFRS (International Financial Reporting Standards) Foundation spolupracuje se Světovou bankou na zavádění mezinárodních účetních standardů v rozvojových zemích. Nedílnou součástí implementace těchto standardů je také zavedení vnitřních kontrolních systémů a procesů pro zajišťování informací. Zajímavý článek na toto téma si můžete přečíst na tomto odkazu: *https://www.accountingtoday.com/news/ifrs-foundation-teams-with-world-bank-on-aiding-developing-economies*

Dotknul se jeden z posledních celosvětových kybernetických útoků realizovaný v pátek 12. 5. 2017 také vás nebo vaší firmy? Možná tento útok pomohl zdůraznit význam kybernetické bezpečnosti a souvisejících kontrolních mechanizmů, které musí být správně a včas implementovány, aby pomohly ochránit vaše data. Bližší informace naleznete v článku na tomto odkazu: *https://www.nytimes.com/2017/05/14/world/europe/cyberattacks-hack-computers-monday.html*

# Čeští zástupci na **IIA Global Council** v Římě

**„Ty letíš do Říma v únoru? No to děláš chybu, nech to na květen," odrazoval mě od cesty jeden kolega. Ale neodradil a jsem za to ráda. A to nejen díky na únor příjemnému slunečnému počasí, antickým památkám a italské kuchyni…**

**Ing. Zuzana Kitto, CIA, CISA, CPA**
UniCredit Bank Czech Republic a Slovakia, a.s.

Pod pojmem Global Council jsem si představovala zasedání zástupců jednotlivých členských institutů, kde se formalizují rozhodnutí učiněná řídicími orgány IIA. Takže spíše reprezentativní a formální akci. Na stránkách IIA jsem informací ohledně účelu tohoto shromáždění moc nenašla. Nezbývalo než nechat se překvapit. A o překvapení nebyla nouze.

To první čekalo ve formě domácího úkolu, který jsme dostali několik týdnů předem. Stanovy IIA říkají, že Global Council dává vstupy do strategického směřování IIA. Takže cílem tohoto cvičení bylo pomocí strukturovaného dotazníku zrevidovat strategický plán IIA na období 2015–2020. Nic moc zážívného, co by mě do Říma navnadilo.

Další překvapení čekalo hned po příjezdu. Konference se trefila do několikadenní stávky taxikářů proti službě Uber. Ve městě nejezdil jediný taxík. Nejlepší způsob, jak přinutit turisty používat Uber ☺ Nás zachránil pokoutný Alžířan v maličkém Fiatu, který nás, bezradné, oslovil na nádraží. Aspoň jsem si po letech procvičila francouzštinu…

Čtyřdenní program se skládal ze dvou hlavních dnů nabitých přednáškami a workshopy a dvou dnů doplňkových aktivit. Po úvodní řeči Angely Witzany (IIA Global Chairman of the Board) a prezidenta italské IIA Maurizia Bonziho přišla na řadu objevná přednáška hlavního auditora Vatikánu, Libera Miloneho. Tento bývalý partner KPMG je ve Vatikánu prvním svého druhu, protože interní audit zavedl teprve v roce 2014 papež František. Funguje však na velmi podobných principech jako všude jinde. Nejzajímavější bylo „15 nemocí vůdců" papeže

Františka – skvělé spojení křesťanských principů s manažerskými. Vybírám jen některé z 15 jmenovaných nemocí:

- mít nerovnováhu mezi prací a ostatními oblastmi života
- příliš se spoléhat na plány a málo na intuici a improvizaci
- trávit příliš málo času propojováním lidí a stavěním mostů
- nedělit se s ostatními o chválu a odměnu
- dávat svůj vlastní úspěch před úspěch ostatních.

Povedly se také workshopy, ve kterých jsme ve skupinkách po deseti řízeně hodnotili a prioritizovali strategický plán IIA a vyměňovali si zkušenosti. Moji skupinku vedl Larry Harrington, jednotlivé otázky měl pečlivě připravené a předvedl profesionální facilitaci. Bylo velmi zajímavé poznat dílčí aspekty fungování jednotlivých institutů ve skupince – např. Finska, Polska, Singapuru. Ukázalo se, že všichni řešíme podobná témata – členství interních auditorů ze státní správy, poplatky versus podpora ze strany IIA, vzdělávání… Já jsem reprezentovala ČIIA, náš prezident Tomáš Pivoňka přijal roli zástupce ECIIA, vzhledem k tomu, že z Boardu ECIIA nikdo jiný nepřijel. Na podobných akcích je mi vždy velkou ctí prezentovat náš institut, který ve srovnání s podobnými zeměmi zcela vyniká, a to jak počtem členů, tak především škálou aktivit, které úspěšně nabízíme: konference, semináře, kurzy/akademie, kulaté stoly, setkávání auditorů z různých oblastí, klub mladých, quality assurance, časopis, překlady, knihovna… Sklízíme za to obdiv, uznání a prosby o přenos know-how do ostatních zemí.

Na večerním programu mě překvapila možnost vzít všude s sebou drahé polovičky. První večer na střeše majestátního tradičního hotelu, kde celá konference probíhala, odkud byl naprosto jedinečný výhled na celé město. Druhý večer ve staré římské pevnosti s velmi osobitou atmosférou. Náš stůl nemohl být lépe namixován, po levici jsem měla zástupce německého a švýcarského institutu, po pravé potom Jordánsko a Mongolsko.

Celkem se v Římě sešlo 80 zemí reprezentovaných 160 účastníky. Příští rok se zástupci IIA sejdou v Panamě. Uvidíme, jestli se nám podaří se zúčastnit i tam!

# CEE Leadership Meeting 2017 v Bělehradě

Prezident ČIIA, Tomáš Pivoňka, se zúčastnil setkání prezidentů institutů interního auditu ze střední a východní Evropy. Na setkání reprezentoval nejen Český institut interních auditorů, ale také ECIIA (člen The management boardu ECIIA) a IIA (člen výboru pro advocacy). Setkání navazovalo na národní konferenci IIA Srbsko, kde také Tomáš vystoupil s prezentací na téma poradenská činnost interního auditora.








**Setkání s prezidentem IIA Německo p. Berndem Schartmannem (květen 2017)**


**V dubnu 2017 proběhlo 11. setkání interních auditorů z finanční oblasti, tentokrát za podpory společnosti EY.**

**V květnu 2017 jsme přivítali návštěvu auditorů ze Šanghaje. V příjemné atmosféře jsme zejména představili činnost ČIIA, Centrální harmonizační jednotky MF a vzájemnou spolupráci.**

# Výři vířili ve víru LEGISLATIVNÍCH ZMĚN

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

Více než 130 interních auditorů se letos zúčastnilo workshopu ČIIA pro veřejnou správu v Liberci. Tentokrát pod názvem Labyrint legislativních změn. Titulek této reportáže volně navazuje na klasickou hlášku mistrů českého humoru, pánů Smoljaka a Svěráka, z filmu Marečku podejte mi pero. Ústy profesora Hrbolka zazněl pravopisný rébus: „Sveřepí šakali zavile vyli na bílý měsíc.“ V našem případě se nejednalo o šakaly, ale o sovy: „Výři vířili ve víru legislativních změn.“ Alespoň tak to v průběhu workshopu občas vypadalo. Do Liberce se sjely chytré a zkušené hlavy, tak jako se moudré sovy slétají do Atén.

Workshop byl připravován pod záštitou náměstka ministra vnitra pro státní službu Josefa Postráneckého. Ten také přislíbil osobní účast a připravil si podrobnou přednášku o aktuálním stavu Služebního zákona. Víry kolem projednávání novely tohoto zákona byly tak silné, že nedovolily panu náměstkovi osobně se workshopu zúčastnit. Místo toho musel být přítomen v Senátu, kde se právě o tomto zákoně jednalo. V průběhu dne jsme se dověděli, že novela byla schválena. Svou prezentaci pro liberecký workshop předal paní Zuzaně Brüknerové z MV ČR. Ta nejen samotnou prezentaci, ale i doplňující slovní komentář bravurně zvládla. Významnou podporu celé akci poskytlo Ministerstvo financí. Jmenovitě náměstek ministra Tomáš Vyhnánek a tým jeho spolupracovníků.

Výři vířili aktivně a moudře ve čtyřech pracovních skupinách. V první se diskutovalo o aplikaci Služebního zákona. Druhá skupina řešila problematiku registru smluv. Ve třetí skupině se zabývali účastníci auditováním veřejných zakázek. Poslední skupina řešila otázky spojené s kybernetickou bezpečností. Závěry shrnuli členové skupin do prezentace a diskuzního příspěvku v plénu druhý den dopoledne. Zajímavé bylo vystoupení Ondřeje Jaroše ze společnosti Dynatech o aktivních kontrolních mechanizmech interního auditu. Petr Kheil z České spořitelny poutavě prezentoval nové prováděcí směrnice v Mezinárodním rámci profese IA. Dana Ratajská hovořila o novinkách, které připravilo Ministerstvo financí v oblasti metodiky.

Další víření, tentokrát hudební a taneční, si vychutnali účastníci večerního setkání nad číší vína ve společenských prostorách hotelu Babylon. A že se auditoři umí otáčet, to dokázalo nejen na tanečním parketu, ale i s hudebními nástroji. Jedním z členů kapely Angels byl také interní auditor.
Že na vás působí tato reportáž telegraficky, zkratkovitě? Nevěříte, že by se tolik událostí vešlo do dvou půldenních jednacích bloků? Že byste to chtěli jednou prožít na vlastní kůži? Nezbývá, než abyste se příště zúčastnili osobně.


# DĚKUJEME PARTNERŮM

HLAVNÍ PARTNER

DYNA TECHO

PARTNEŘI

Business Institut

IDS Advisory

Ministerstvo financí České republiky

Liberecký kraj

LIBEREC

MEDIÁLNÍ PARTNEŘI

iA interní auditor

Veřejná správa

# Nejen prací živ je interní auditor/kontrolor ☺

Již několikátým rokem se pravidelně setkáváme v rámci moravských měst, resp. napříč celou Moravou. V letošním roce jsme se velmi rády ujaly role hostitelů u nás na městě Šumperku. Jako místo konání jsme zvolily Středisko ekologické výchovy Švagrov, které se nachází v krásném prostředí v srdci Jeseníků. Velmi mile nás překvapil zájem o tuto akci, které se nakonec zúčastnilo na 4 desítky interních auditorů a kontrolorů napříč moravskými kraji, od Olomouckého přes Zlínský až po Jihomoravský. Pro účastníky byl připraven bohatý program zaměřený mj. na veřejnosprávní kontroly a kontrolní řád a na aktuálním téma, a to zákon o registru smluv. Nedílnou součástí byla také vzájemná výměna zkušeností tzv. best practise. A jelikož nejen prací živ je interní auditor/kontrolor, tak i součástí našeho setkání byla neformální část, kdy nám zaměstnanci střediska prostřednictvím zajímavých aktivit přiblížili ekologii. Účastníci si mohli osvěžit své znalosti naší krásné přírody, zejména zvířat v ní žijících, a díky hře zvané „Neviditelná ruka trhu" se mohli setkat s principy a důsledky fungování volného obchodu a porozumět tomu, jak obchod souvisí s prosperitou země. Setkání se podařilo po všech stránkách a dík za to patří nejen organizátorům, ale i všem zúčastněným, kteří vytvořili velmi přátelskou atmosféru. ■

Jaroslava Kopová
vedoucí IAK města Šumperka

# Interní auditoři severní Moravy se sešli na Slezské Ostravě


Pod záštitou starostky MVDr. Barbory Jelonkové a díky podpoře celého vedení městského obvodu Slezská Ostrava se v budově slezskoostravské radnice, která je evidovanou kulturní památkou, konalo pracovní setkání interních auditorů Moravskoslezského kraje. Jednání se uskutečnilo 18. května 2017 a zahájila ho svým krátkým vystoupením místostarostka Ing. Ivona Vaňková. Samotné jednání mělo na programu tři hlavní témata, ale nosným příspěvkem byla určitě prezentace Ing. Blanky Štefankové, která je auditorkou KÚ MSK a také autorkou několika publikací. Její příspěvek na téma „Hodnocení a program kvality interního auditu" byl pro všechny podnětný. Zástupce MF ČR Ing. Dana Ratajská pak seznámila přítomné s novinkami z centrální harmonizační jednotky. Ředitel ČIIA Ing. Daniel Hausler se zaměřil ve svém příspěvku na vzdělávání interních auditorů veřejné správy. Seznámil přítomné s nabídkou stávajících vzdělávacích programů a nastínil nové směry ve vzdělávání. Závěr jednání patřil Slezskoostravské galerii, kam byli všichni účastníci pozváni na expozici spojenou s výročím 750 let města Ostravy.

Ing. Jiřina Halamčáková – Slezská Ostrava
Foto Hana Bončková

# ANTIFRAUD AKADEMIE

## podzimní termín

## 3.–5. 10. 2017

## 17.–19. 10. 2017



## *PwC IT Assurance Services*

Komplexní služby v oblasti řízení rizik vašeho IT

Rostoucí závislost společností na informačních technologiích s sebou nese i zvýšení požadavků na odbornost interních auditorů. Díky každodennímu kontaktu s hrozbami a příležitostmi současného IT vám v PwC umíme pomoci v oblastech, jako jsou:

***IT audity*** - zaměříme se na posouzení odpovídající míry zabezpečení a ochrany dat, informačních systémů a celé IT infrastruktury.

***Ujištění pro třetí strany*** - jste-li odpovědní za správu a provoz systémů využívaných interními či externími klienty, poskytneme jim komplexní ujištění o robustnosti vašeho kontrolního prostředí.

***Hodnocení rizik outsourcingu IT*** - ohodnotíme rizika, procesy a kontroly přímo u vašich poskytovatelů IT služeb.

***Pokročilé metody datových auditů*** - pomůžeme vám lépe využít dostupná data v rámci postupů interního auditu.

***www.pwc.cz/interniaudit***

pwc

# Členové Rady ČIIA a Kontrolní komise ČIIA po zasedání 22. Sněmu ČIIA

## RADA ČIIA

**Ing. František Beckert, CIA**
Ministerstvo financí ČR
**VICEPREZIDENT ČIIA**

**Mgr. Tomáš Pivoňka, CIA, CRMA**
ČEZ, a.s.
**PREZIDENT ČIIA**

**Ing. Zuzana Kitto, CIA, CISA, CPA**
UniCredit Bank Czech Republic a Slovakia, a.s.
**VICEPREZIDENT ČIIA**

**Ing. Michal Čup, CIA, FCCA**
KPMG Česká republika, s.r.o.

**Ing. Miloslav Frumar, CIA**
Česká spořitelna, a.s.

**Ing. Petr Hadrava, ACCA, CIA, CISA**
Sberbank CZ, a.s.

**Ing. Jitka Kazimírová, CIA, FCCA**
Allianz pojišťovna, a.s.

**Ing. Eva Klímová**
Úřad městské části Praha 2

**Ing. Jan Kovalčík, CIA**
Česká spořitelna, a.s.

**Ing. Michaela Kubýová, FCCA**
Raiffeisenbank a.s.

**Mgr. Kateřina Miklošová**
PricewaterhouseCoopers Audit, s.r.o.

**Ing. Dana Ratajská**
Ministerstvo financí ČR

**Ing. Lukáš Wagenknecht**
Good Governace

## KONTROLNÍ KOMISE ČIIA

**Ing. Martin Bubeník, Ph.D.**
ČEZ, a.s.

**Mgr. František Orság, CIA**
Ministerstvo financí ČR
**PŘEDSEDA**

**Mgr. Petr Švub, CIA, CISA**
Česká spořitelna, a.s.

Více o Radě ČIIA zde:

Více o Kontrolní komisi ČIIA zde:



# Certifikovaní **interní auditoři**

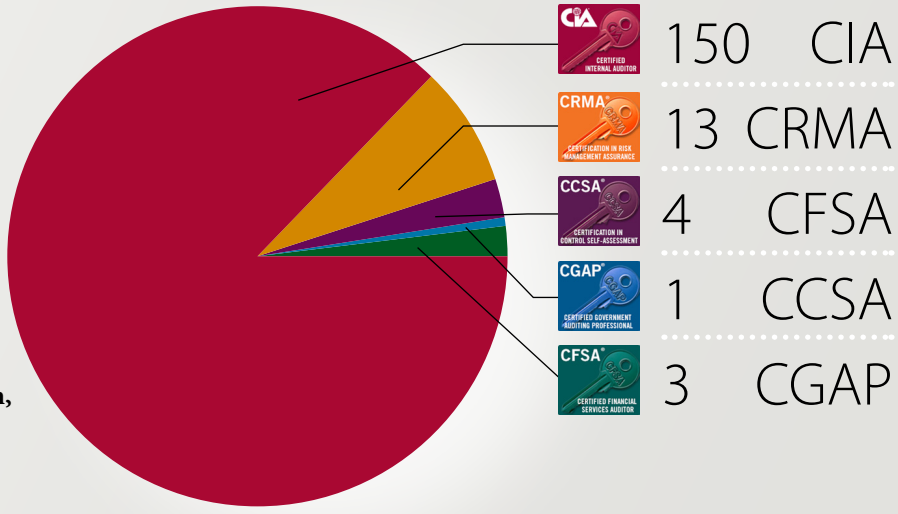
## Nově certifikovaní:

**Ing. Tomáš Babinec, CIA**
**Ing. Irena Kovalčíková (Andělová), CIA**
**Ing. Vadim Beneš, CIA, CRMA**
**Ing. Barbora Jonaštíková, CIA**
**Ing. Lukáš Pečeňa, CIA, CGAP**
**Ing. Petra Šarochová, CIA**

GRATULUJEME!

V současné době evidujeme celkem **154 aktivních certifikovaných, s celkem 171 certifikacemi:**

**Celkem evidujeme 335 udělených certifikací.**



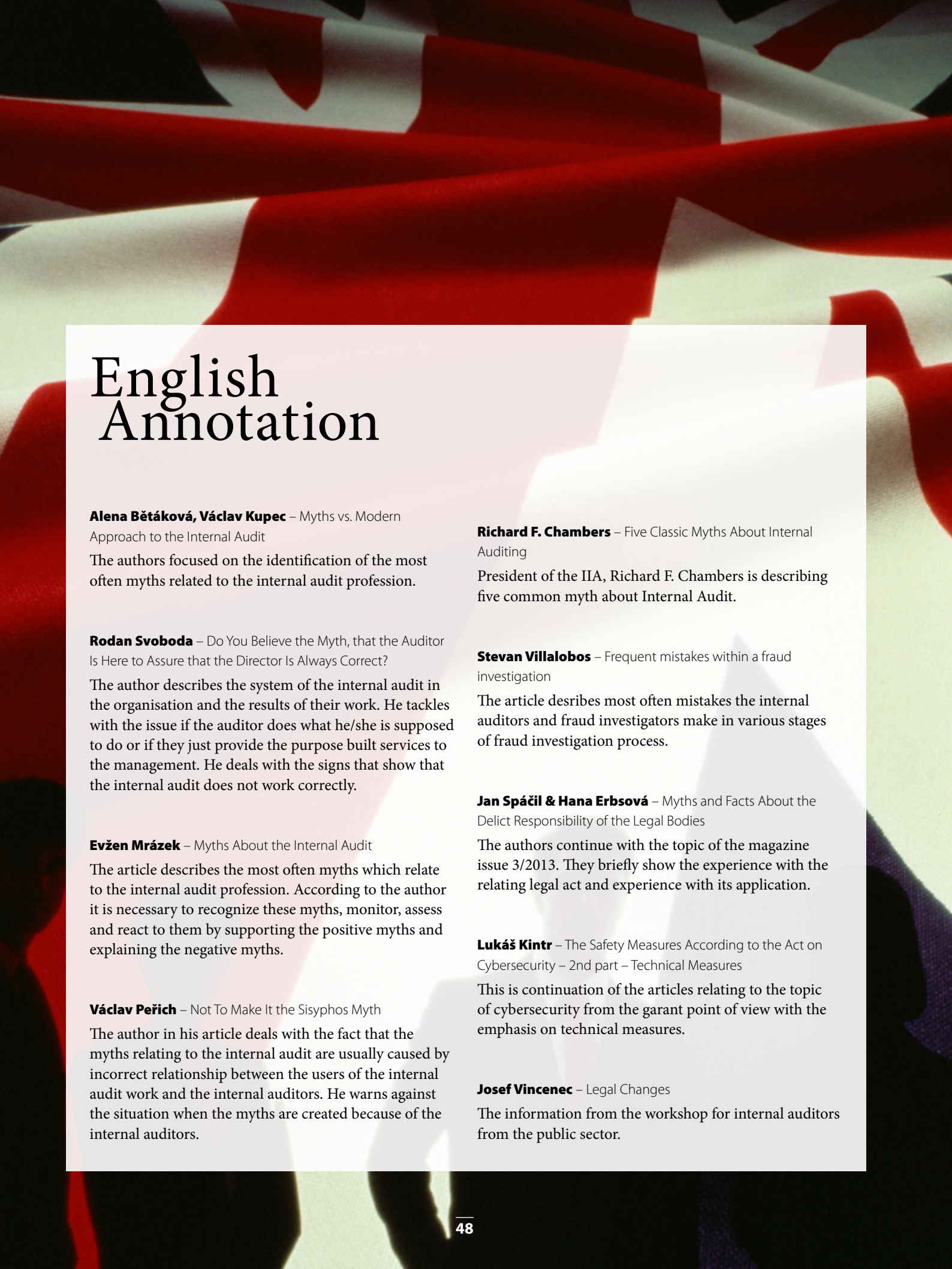

## Certifikace interních auditorů ve veřejné správě

**Počet certifikovaných auditorů ve VS dle oblastí do 31. 1. 2017**

| Oblasti | Počet VIAA | Počet VIAJ | Počet VIAS | Počet VIAK | Počet IA dle oblastí |
|---|---|---|---|---|---|
| Ministerstva, Úřad vlády | 34 | 21 | 52 | 29 | 136 |
| Krajské úřady | 3 | 3 | 3 | 9 | 18 |
| Úřady měst a obcí | 10 | 16 | 27 | 12 | 65 |
| Policie a Hasiči | 6 | 10 | 12 | 5 | 33 |
| Vysoké školy | 1 | 1 | 7 | 3 | 12 |
| Zdravotnictví, lázně | 5 | 2 | 8 | 2 | 17 |
| Ostatní | 33 | 30 | 29 | 18 | 110 |
| **Celkem IA ve VS** | **92** | **83** | **138** | **78** | **391** |

# Noví členové

- Ing. Jan Brabec, MBA, Individuální člen
- Ing. Vladimír Brož, Česká pošta, s. p.
- Mgr. Kateřina Cibulková, Hasičský záchranný sbor Karlovarského kraje
- Ing. Vítězslav Černý, OHL ZŠ, a.s.
- Mgr. Atanas Dandarov, Individuální člen
- Ing. Marcela Fialová, Fakultní nemocnice Ostrava
- Ing. Jana Guregová, Agentura pro podnikání a inovace
- Ing. Richard Hampl, ČEZ, a.s.
- Ing. Jozef Harakaľ, U. S. Steel Košice, s.r.o.
- Ing. Hana Hartmanová, Individuální členka
- Ing. Petr Hranoš, CIA, ČEZ Distribuce, a.s.
- Ing. Sarah Kabanji, Individuální členka
- PhDr. Petr Kroupa, Národní knihovna České republiky
- Jitka Křečková, DiS., Pražská plynárenská Distribuce, a.s., člen koncernu Pražská plynárenská, a.s.
- Ing. Jan Liška, Povodí Vltavy, státní podnik
- Bc. Miroslava Líbalová, DiS., Všeobecná fakultní nemocnice v Praze
- Mgr. Viera Múčková, DipIFR, CIA, NN Životná poisťovňa, a.s.
- Ing. Petr Müller, Agentura pro podnikání a inovace
- Ing. Petra Pánková, Komerční banka, a.s.
- Bc. Ivana Pertlová, Individuální členka
- Ing. Dušana Petelenová, ERGO Poisťovňa, a.s.
- Ing. Michal Plaček, Státní pokladna Centrum sdílených služeb, s.p.
- Ing. Hana Plaňková, Komerční banka, a.s.
- Ing. Mgr. Bc. Ondřej Průcha, Národní agentura pro komunikační a informační technologie, s.p.
- Ing. Arnold Ptasznik, Individuální člen
- Ing. Jan Smejkal, FCCA, Individuální člen
- Ing. Ota Šplíchal, Českomoravská záruční a rozvojová banka, a.s.
- Mgr. Slávka Štefaniková, U. S. Steel Košice, s.r.o.
- Ing. Silvia Vasiľáková, U. S. Steel Košice, s.r.o.
- Ing. Alexandra Vasilová, U. S. Steel Košice, s.r.o.
- Štěpán Vondrášek, ČEZ, a.s.
- Mgr. Lukáš Vymětal, Agentura pro podnikání a inovace
- David Zimandl, FM ČESKÁ, s.r.o.



# English Annotation

**Alena Bětáková, Václav Kupec** – Myths vs. Modern Approach to the Internal Audit

The authors focused on the identification of the most often myths related to the internal audit profession.

**Rodan Svoboda** – Do You Believe the Myth, that the Auditor Is Here to Assure that the Director Is Always Correct?

The author describes the system of the internal audit in the organisation and the results of their work. He tackles with the issue if the auditor does what he/she is supposed to do or if they just provide the purpose built services to the management. He deals with the signs that show that the internal audit does not work correctly.

**Evžen Mrázek** – Myths About the Internal Audit

The article describes the most often myths which relate to the internal audit profession. According to the author it is necessary to recognize these myths, monitor, assess and react to them by supporting the positive myths and explaining the negative myths.

**Václav Peřich** – Not To Make It the Sisyphos Myth

The author in his article deals with the fact that the myths relating to the internal audit are usually caused by incorrect relationship between the users of the internal audit work and the internal auditors. He warns against the situation when the myths are created because of the internal auditors.

**Richard F. Chambers** – Five Classic Myths About Internal Auditing

President of the IIA, Richard F. Chambers is describing five common myth about Internal Audit.

**Stevan Villalobos** – Frequent mistakes within a fraud investigation

The article desribes most often mistakes the internal auditors and fraud investigators make in various stages of fraud investigation process.

**Jan Spáčil & Hana Erbsová** – Myths and Facts About the Delict Responsibility of the Legal Bodies

The authors continue with the topic of the magazine issue 3/2013. They briefly show the experience with the relating legal act and experience with its application.

**Lukáš Kintr** – The Safety Measures According to the Act on Cybersecurity – 2nd part – Technical Measures

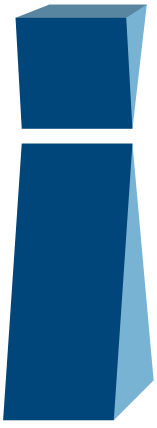
This is continuation of the articles relating to the topic of cybersecurity from the garant point of view with the emphasis on technical measures.

**Josef Vincenec** – Legal Changes

The information from the workshop for internal auditors from the public sector.

# CENA ZA INOVACI V INTERNÍM AUDITU 2017

Český institut interních auditorů vyhlašuje **2. ročník soutěže CENA ZA INOVACI**.
Realizovali jste **inovativní projekt nebo prvek ve své činnosti interního auditu, který představuje nový přístup** a přináší nejen přidanou hodnotu interního auditu, ale také nový pohled na interní audit?
Pak se zapojte do soutěže. Zúčastnit se můžete jako jednotlivec i jako organizace. **Stačí do 15. srpna 2017 zaslat přihlášku včetně popisu projektu.** Odborná porota následně projekty posoudí a tři nejlepší získají **CENU ZA INOVACI 2017!**



CENA
ZA INOVACI
V INTERNÍM
AUDITU

více informací na **www.interniaudit.cz**

# MÝTY V INTERNÍM AUDITU