4|2016

INTERNÍ AUDITOR

ČTVRTLETNÍK ČESKÉHO INSTITUTU INTERNÍCH AUDITORŮ
ROČNÍK 20, ČÍSLO 4–2016 (82)

ČESKÝ INSTITUT INTERNÍCH AUDITORŮ

The Institute of Internal Auditors

TRENDY V INTERNÍM AUDITU

CLOUD OČIMA REGULÁTORA

VÝBOR PRO AUDIT

SVAZEK KLÍČŮ PRO HODNOCENÍ KONTROLNÍCH SYSTÉMŮ

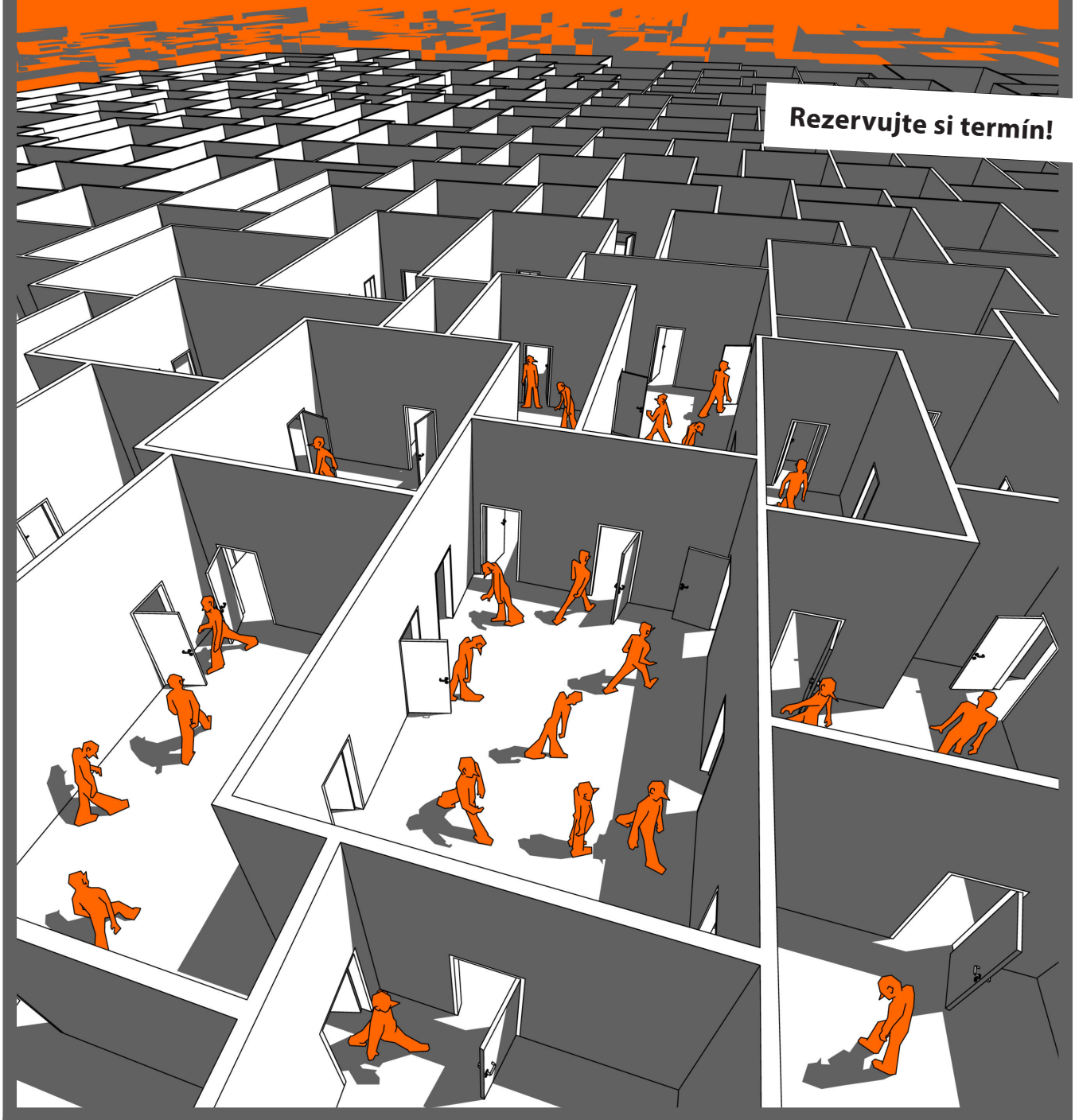
ČESKÝ INSTITUT INTERNÍCH AUDITORŮ

LABYRINT LEGISLATIVNÍCH ZMĚN

19–20/4 2017

LIBEREC

WORKSHOP PRO VEŘEJNOU SPRÁVU



Rezervujte si termín!

ČIIA ČESKÝ INSTITUT INTERNÍCH AUDITORŮ

IIA The Institute of Internal Auditors

LIBEREC

WWW.INTERNIAUDIT.CZ

OBSAH

Vážené čtenářky, vážení čtenáři,

jak už je tak trochu tradicí, rád bych využil prosincového čísla Interního auditora k bilancování letošního roku. S radostí opět začínám tím, že to byl dobrý rok (už si pomalu připadám jako vinař ☺). Podařilo se toho hodně, nicméně rád bych vyzdvihnul tři momenty, které jsou pro mě něčím výjimečné: národní konferenci, soutěž o inovace a aktivity ČIIA na mezinárodním poli.

Z národní konference o IT v interním auditu jsem byl doslova nadšený. Bavila mě uvolněná, přátelská a pracovní atmosféra, která na konferenci panovala. Ti, kteří zažili přednášku Martina Hudečka, mi budou věřit, že mám doživotní zážitek (a jistě si vždy vzpomenou na červenou košili). A opět jsme překročili rekordní počet účastníků na národní konferenci. První ročník soutěže o inovaci v interním audit do písmene naplnil ambice, které Rada ČIIA při vyhlašování soutěže měla. Podařilo se nám rozpoutat diskuzi o inovacích v auditu, členové institutu se soutěže aktivně účastnili v hojném počtu a vyhlášení výsledků bylo důstojné a zároveň zábavné (zdravím do Ostravy). V tomto roce jsme také zúročili několikaletou práci na mezinárodním poli. Naše aktivity vyvrcholily mým zvolením do představenstva ECIIA. Takže opět po dvaceti letech je zástupce ČIIA v nejvyšším vedení ECIIA. Za toto zvolení musím poděkovat vám, členům ČIIA a zejména kolegům v Radě, bez jejichž podpory by se tento úspěch neudál.

A jaké jsou priority pro rok 2017? V rámci institutu se osobně chci zaměřit na dvě skupiny stakeholderů, které jsou pro budoucí úspěch ČIIA a profese klíčové – mladou generaci auditorů a ředitele útvarů IA. Z pohledu profese bude, dle mého názoru, příští rok o kybernetické bezpečnosti, narůstající regulaci a schopnosti auditorů rychle identifikovat nové hrozby a rizika podnikání a ještě rychleji je „proauditovat" (auditing at speed of risk).

Přeji vám klidné prožití adventního času a všechno dobré do nového roku.

Tomáš Pivoňka

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

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

Foto: archiv ČIIA, fotobanka 123RF
Neprodejné, určeno pro Český institut interních auditorů
Náklad: 1 400 výtisků
Pre-press: Viktor Beránek
Tisk: REPRO servis s. r. o.
Distribuce: Mail Step a. s.

AUDIT NIKDY NESPÍ

Angela Witzany, IIA Global Chairman of the Board, říká, že interní auditoři si uchovají svoji relevantnost pouze v případě, že budou neustále věnovat pozornost prioritám organizace, které poskytují auditní služby.

Angela Witzany, CIA, QIAL, CRMA
vedoucí interního auditu ve společnosti Sparkassen Versicherung AG ve Vídni

Žijeme v „neustále připojené“, 24/7 společnosti. Naše chytrá zařízení nám umožňují být neustále online, společnosti jsou dostupné nepřetržitě a velká rychlost cyklů je standardem. Očekáváme nepřetržitý přístup k informacím a rychlé dodávky produktů a služeb. Náš svět je hyperpropojený a je v neustálém pohybu.

Součástí této nové skutečnosti je, že riziko a změny se staly firemními konstantami. Neustále se objevují nová rizika, kterých si musí být interní auditoři vědomi a musí držet krok s nejnovějším vývojem. Musíme si být neustále vědomi toho, co se děje v prostředí naší organizace, jaký je vývoj v legislativě a v naší profesi obecně, a všechno musíme dělat v rámci zrychlujícího se světa kolem nás.

Proto jsem si jako téma mého předsednictví vybrala „AUDIT NIKDY NESPÍ“. V současné době si interní auditoři nemohou dovolit usnout na vavřínech. Musíme nabízet inovativní a proaktivní cesty ke zlepšení a neustále nabízet nová řešení. Měli bychom využít každé příležitosti k posílení naší značky, budování důvěry a kultivaci vztahů. K riziku musíme přistupovat ostražitě a s maximální pozorností. Interní auditoři si uchovají svoji relevantnost pouze v případě, že budou neustále věnovat pozornost prioritám organizace, které poskytují auditní služby.

> „Interní auditoři si uchovají svoji relevantnost pouze v případě, že budou neustále věnovat pozornost prioritám organizace, které poskytují auditní služby“

Moje téma se také úzce váže k místu založení IIA – New Yorku – města, které nikdy nespí. Již od založení IIA v centru Manhattanu před 75 lety interní auditoři pracovali neúnavně a se zapálením, aby plnili neustále se vyvíjející očekávání různých zainteresovaných stran. Na tomto tempu musíme stavět a pokračovat v něm, pokud chceme svým klientům poskytovat kvalitní služby i v období neustálých změn. Zdokonalováním našich komunikačních schopností, uplatňováním uceleného přístupu, děláním správných věcí, zaměřením se na strategii a zaměřením se na budoucnost si můžeme připravit cestu k ještě proaktivnějšímu, firemně orientovanému přístupu.

Správně komunikovat

Efektivní komunikace s různými zainteresovanými stranami je pro práci interního auditora zásadní. Management a výbor pro audit očekávají, že nabídneme svůj vhled do obchodních záležitostí a tento odprezentujeme způsobem, který bude nejen slyšet, ale bude možné mu i jasně rozumět.

Schopnost interního auditu komunikovat závisí částečně na vztazích auditorů v rámci společnosti. Bez silných vztahů ani ta nejlepší sdělení a náš vhled do obchodních záležitostí nemusí zasáhnout cílovou skupinu nebo padnout na úrodnou půdu. Interní auditoři musí investovat do budování vztahů a snažit se dobře poznat své klienty. Nemůžeme se potkávat v kanceláři jenom se svými auditními kolegy. Musíme zavítat i do jiných oddělení a komunikovat s těmi, kterým v naší organizaci poskytujeme služby. Měli bychom využít každé příležitosti nejen k formální, ale i k neformální komunikaci – zejména s našimi klíčovými zainteresovanými stranami – abychom se dozvěděli nové nebo měnící se skutečnosti. Dát si snídani, oběd nebo šálek kávy se zástupcem managementu může být prvním krokem k tomu, aby náš hlas byl slyšet.

Foto: Ian Ehm

CESTA K PŘEDSEDNICTVÍ

2009 Member, IIA–Austria Board of Directors
2010 President, IIA–Austria; Member, IIA Professional Certifications Board
2012 Member, ECIIA Management Board
2013 Treasurer, IIA Global Board of Directors
2014 Senior Vice President, ECIIA; IIA Vice Chairman of the Board–Professional Guidance
2015 Senior Vice Chairman, IIA Global Board of Directors
2016 Chairman, IIA Global Board of Directors

Efektivní komunikace samozřejmě nevyžaduje jen obratnost při sdílení informací, musíme také pozorně naslouchat tomu, co říkají naši klienti. Že je tato dovednost nesmírně důležitá, dokazuje to, že více než 90 procent respondentů průzkumu (IIA 2016 North American Pulse of Internal Audit) uvedlo, že aktivní naslouchání je zapracováno do jejich školicích programů a náborových iniciativ.

Musíme umět naslouchat „mezi řádky", abychom slyšeli podstatná sdělení. Dobrý posluchač správně pochopí to, co klient říká, a ujistí ho o tom. Auditoři, kteří mají tuto schopnost, zlepšují kvalitu shromažďování auditních informací, stejně jako vylepšují obrázek o auditu coby spolehlivého partnera, který si uvědomuje obavy a priority společnosti.

Zaujmout ucelený přístup

Auditoři s uceleným přístupem mají řadu kompetencí. Zatímco zkušenosti s účetnictvím nebo financemi jsou jistě pro auditory cenné, existuje mnoho dalších schopností, které nám umožňují řešit rizika ovliňující naši organizaci.

Kybernetické útoky a otázky bezpečnosti v oblasti soukromí a informací nadále sužují organizace všech typů. Jak ukazují nedávné globální průzkumy, kybernetické riziko je klíčové riziko pro představenstva a management; spolu s velkou rychlostí inovací v oblasti nových technologií jde o hlavní výzvy pro interní auditory v současné době a jsou ve stále větší míře v hledáčku našich zainteresovaných stran. Otázkou pro interní auditory je, zda máme technické znalosti pro posouzení a řešení rizik tohoto typu. Musíme neustále investovat do rozšiřování IT znalostí, abychom byli schopni naplnit očekávání svých zainteresovaných stran, a pro zajištění uceleného souboru dovedností. Jedna cesta vede přes intenzivní školení s cílem vytvořit kvalitní základ znalostí v rámci auditorského týmu. Kromě zapojení IT auditorů, každý interní auditor potřebuje mít základní, nebo i vyšší úroveň IT znalostí. Nicméně pro některé audity nebo vyšetřování v IT oblasti budou organizace neustále potřebovat využití externího dodavatele IT znalostí.

GLOBÁLNÍ PŘEDSEDNICTVÍ

Jako globální předsedkyně IIA pro období 2016–2017 mám v plánu pilně pracovat se svými kolegy na podpoře dlouhodobého strategického plánu Institutu – chci se postarat o to, aby profese interního auditu byla všeobecně považována za nepodstradatelnou pro efektivní řízení, risk management a kontrolu. Tento cíl má pět hlavních částí:
Profesionalita IIA bude řídit profesi interního auditora prostřednictvím včasného rozvoje relevantních znalostí, globálního vedení a návody pro kariérní rozvoj.
Obhajoba (profese interního auditu) IIA zviditelní profesi interního auditu a zvedne poptávku po této profesi a postará se o to, aby interní audit byl považován zainteresovanými stranami za nepostradatelný.
IIA jako vůdce IIA bude uznávan jako vůdce pro interní audit.
Kapacita IIA bude globálně spolupracovat za účelem rozšíření kapacity profese interního auditu.
Udržitelná hodnota IIA nasadí jak finanční, tak obchodní modely, které vytvoří udržitelnou hodnotu pro členy.

Těším se na to, že pomohu Institutu proměnit tuhle vizi v realitu, a na řízení naší profese tak, aby měla v budoucnosti větší relevanci a vliv.

Uplatnění měkkých dovedností (tzv. soft skills) může být pro náš úspěch stejně důležité jako technické znalosti, možná i víc. Auditoři s uceleným přístupem se například obratně orientují v politickém klimatu společnosti a řeší problémy cestou kompromisu. Jsou efektivními vyjednávači oddanými k nalezení společného řešení pro spokojenost všech zainteresovaných stran.

Provádění auditní práce s rozšířenými obzory zahrnuje nejen dovednosti, ale i způsob myšlení – ucelené, integrované myšlení. Auditoři, kteří se na svoji práci dívají z několika perspektiv, budou schopni mnohem lépe posoudit situaci v širším kontextu, a tím poskytnou svojí společnosti cennou hodnotu. Tento holistický přístup se odrazí v hlavním produktu naší práce, v auditním reportu, a v našich poradenských službách. Auditní práce je hodně odlišná a má nižší hodnotu, pokud je použit krátkozraký, jednorozměrný přístup.

Samozřejmě, žádný interní auditor nemůže ovládat všechny znalosti a dovednosti – a to je místo, kde se uplatní tzv. integrované auditování. Auditní tým jako celek potřebuje správné lidi se správnými znalostmi a zkušenostmi. Kromě toho musí auditoři úzce spolupracovat a klást velký důraz na sdílení informací za účelem zvýšení schopnosti týmu využít tohoto integrovaného přístupu. Pokud máme správný mix auditorů v auditním týmu, který efektivně spolupracuje, vytváří to solidní základ pro úspěch.

Dělat správné věci

Při své práci musíme klást velký důraz na etiku. Jenomže etické chování znamená mnohem víc než jen dodržování pravidel a standardů – auditoři musí být při provádění auditů transparentní. Auditní proces by za všech okolností měl být jasný a přesný, dobře zdokumentovaný s dohledatelnými důkazy, a měl by být vykonaný pravdivě a se zdravým úsudkem.

Budování základů transparentnosti zabere nějaký čas. Vyžaduje to nepretržitou komunikaci s našimi zainteresovanými stranami a intenzivní snahu je vzdělávat v oblasti auditního procesu. Také to zahrnuje uvědomění si, že transparentnost znamená víc než jen provádět svou práci čestně. Jinými slovy, člověk může být čestný, aniž by se nutně choval transparentně. Důležité je jasně formulovat naše cíle a přesně ukázat, jak může být naše práce pro organizaci přidanou hodnotou. Tato naše snaha musí být nepřetržitá a uplatňovaná při jednání s každým klientem.
Etické chování také znamená jednat s integritou. Auditoři musí demonstrovat spravné charakterové vlastnosti, profesionalitu a respekt ke klientům.

Musíme dodržovat Etický kodex IIA a za všech okolností udržovat co nejvyšší standard chování. Pokud půjdeme příkladem v oblasti integrity, můžeme podpořit etické chování i mimo auditní profesi a být příkladem pro zbytek organizace. Interní auditoři by měli být nositeli etického přístupu.

Mít strategický přístup

Auditoři musí přistupovat ke své práci s vědomím strategie organizace. Přesto podle nedávné studie (Internal Audit Common Body of Knowledge Study), kterou provedla IIA Research Foundation, až 43 % auditních plánů není dostatečně v souladu se strategií organizace. Toto zjištění představuje významnou příležitost pro auditory ke zlepšení.

Angela na setkání se členem představenstva společnosti Sparkassen Versicherung AG, panem Manfredem Bartalszkym (uprostřed) a finančním ředitelem, panem Manfredem Rapfem. Foto: Ian Ehm

KDO JE ANGELA WITZANY?

Osobní
Celý život žije ve Vídni, Rakousko.

Vzdělání
Titul v oblasti obchodní vědy z ekonomické univerzity ve Vídni. Studovala také angličtinu a francouzštinu.

Aktivity
Lyžování, cestování, poznávání, účast na fotbalových zápasech, čtení na pláži, ochutnávky jídla a vína. Nedávno investovala do restaurace ve Vídni, která se vyznačuje rakouským jídlem z různých oblastí této země.

Odstranění tohoto nedostatku, tedy nedostatečného souladu se strategií organizace, vyžaduje soustředěné úsilí. Je naší povinností ptát se na strategii organizace a ujistit se, že jí rozumíme. Vedoucí interního auditu může například požádat o svolení k účasti na poradách věnovaných strategii organizace – i kdyby měl být pouze hostem bez hlasovacích práv – aby se dozvěděl, o čem se v oblasti strategie diskutuje. Případně by interní auditor mohl dostávat zápisky z těchto porad, pokud jeho účast není možná.

Bez pochopení strategie organizace bude auditní činnost vykonávána naslepo a auditoři nebudou dostatečně v souladu s tím, co dělá organizace. Celý auditní tým si musí být vědom strategie společnosti, protože jim to pomůže při každodenní práci s klienty.

Zaměření na budoucnost

Ruku v ruce s naším strategickým zaměřením, interní auditoři musí být schopni předvídat. Historicky se naše profese zaměřovala na minulé události. Řekli jsme, jaké chyby jsme udělali, a pomáhali jsme organizaci vyhnout se jim v budoucnu. Ale dnes je vyžadováno mnohem víc.

Musíme vzít v úvahu klíčové rizika, kterým naše organizace mohou čelit, a podělit se o tyhle úvahy se svými zainteresovanými stranami. Tímto způsobem se mohou naši klienti lépe připravit na výzvy nebo příležitosti, a to předtím, než se projeví. Dívání se vpřed nám umožňuje varovat před možnými katastrofami, které pramení z nedostatečné pozornosti věnované podnikatelským rizikům, nebo využít nové růstové příležitosti, které mohly uniknout pozornosti managmentu.

Interní auditoři musí aktivně vyhledávat informace, které jim pomohou pochopit, co bude dál. Důležitou součástí tohoto procesu je hledat příležitosti k navázání kontaktu s vedením a managementem za účelem posouzení jejich obav a priorit. V odvětvích, která jsou přísně regulovaná, by auditoři měli udržovat dobrý vztah s regulátorem, aby získali představu, co se chystá v oblasti nových požadavků.

Interní auditoři často mohou vytušit blížící se regulační požadavky a držet krok v oblasti dalších záležitostí, které se chystají, a to výměnou znalostí mezi sebou v rámci svého oboru. Já se například setkávám dva až třikrát ročně s dalšími vedoucími interního auditu v rámci pojišťovnictví, abychom se podělili o nové informace a osvědčené postupy. Na našem posledním setkání jsme diskutovali, jaký vliv mají nové regulace, jako je např. U Solvency II Direktiva, na naši strategii v rámci interního auditu a na naši každodenní práci. Tato setkání mi umožňují odhadnout nadcházející události a pomáhají mi vytvářet přidanou hodnotu při řízení rizik v organizaci.

Zaměstnanci v auditu na všech úrovních musí zůstat naladěni na to, co se bude dít v budoucnu, a to prostřednictvím své práce s jednotlivými odděleními ve společnosti.

Každý týden při setkáních s mým auditním týmem si sdílíme znalosti, které jsme získali při práci s klienty, abychom se ujistili, že všichni máme lepší prozumění současných a budoucích cílů. Taky klademe velký důraz na auditní trénink – další klíčovou část k tomu, abychom zůstali soustředeni na budoucnost. Trénink by neměl být sporadický – měl by se skládat z nepřetržitého a kontinuálního vzdělávání. Znalosti nejnovějších trendů v oblasti interního auditu nám dávají možnost vidět, co se bude v budoucnu dít, a lépe nás připraví na to, abychom zainteresovaným stranám poskytli předpovědi, které po nás požadují.

Reakce na výzvy

V roce 2015 vydal IIA revidovanou verzi IPPF, s cílem pomoci auditorům zorientovat se v změnách a stále rostoucích podnikatelských výzvách. Jako členka týmu, který pomohl s revizí rámce, pevně věřím v jeho poslání pro auditní profesi: „Posílit a chránit hodnotu organizace poskytováním ujištění, rad a vhledů, která jsou objektivní a založená na riziku." Jednoduše řečeno, je naší povinností formovat vnímání interního auditu a pozvednout tuto profesi na ještě vyšší úroveň.

Během mého předsednictví bych s vámi chtěla sdílet své názory, zkušenosti a výzvy, se kterými se setkávám. Nicméně chtěla bych slyšet i váš názor. Existuje několik rozmanitých způsobů, jak dosáhnout naší mise. Bez ohledu na vaše postavení, velikost auditního oddělení nebo odvětví je mým osobním cílem naslouchat interním auditorům z celého světa a získat nejrůznější názory na naši profesi.

Musíme pracovat neúnavně a se zaujetím na naší cestě být co nejlepší a být neustále ve střehu při hledání příležitostí k přidávání hodnoty organizaci. Společně můžeme pozvednout profesi interního auditu a zajistit, aby naše profese byla neustále relevantní. Těším se na vaše příběhy a na naši společnou cestu k dosažení tohoto cíle. ■

Bezpečnostní opatření podle zákona o kybernetické bezpečnosti – 1. část – organizační opatření

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

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.

Zákon o kybernetické bezpečnosti (dále ZKB) povinným orgánům a osobám uvedeným v § 3 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 a technická opatření**. Specifikace jednotlivých opatření a rozsah/úroveň jejich plnění v závislosti na kritičnosti jednotlivých typů určených systémů (prvků KII[1]/VIS[2]), respektive požadavků kladených na jejich správce, jsou dále rozvedeny prováděcím právním předpisem – vyhláškou č. 316/2014 Sb., o kybernetické bezpečnosti (dále VKB).

Jak již bylo naznačeno, vzhledem k podstatě systému nastaveného aktuálně platným zněním ZKB jsou v porovnání s VIS prostřednictvím VKB kladeny na prvky KII přísnější (komplexnější) požadavky. Tzv. přechodné období (někdy označované také jako přechodné lhůty) určené pro zavedení požadovaných opatření je pro oba výše uvedené typy systému stanoveno shodně na jeden rok.

Organizační opatření

Systém řízení bezpečnosti informací

Zavedení systému řízení bezpečnosti informací (dále pouze ISMS, někdy překládané jako SŘBI) lze chápat jako všeobecné bezpečnostní opatření. Jako takové logicky agreguje několik odkazů na jiná opatření, jako jsou řízení rizik, stanovení bezpečnostních politik a jejich udržování. Pro prvky KII je v této oblasti dále vyžadováno zajištění auditu kybernetické bezpečnosti s roční periodou a několik dalších dílčích opatření formou monitoringu a vyhodnocování účinnosti zavedených bezpečnostních opatření a politik. Poněkud nešťastně však definuje požadavek na stanovení rozsahu ISMS a řízení provozu a zdrojů s tímto systémem spojených pouze pro prvky KII. V případě VIS tak nemusí být dle VKB výše zmíněné stanoveno, ačkoli je bez toho téměř nemožné ISMS správně a efektivně provozovat.

Řízení rizik

V rámci řízení rizik a v návaznosti na předchozí bod jsou detailněji rozpracována opatření formou zavedení metodiky pro identifikaci a hodnocení aktiv a rizik, včetně požadavků na hodnocení důležitosti aktiv a na druhé straně zvažování hrozeb a zranitelností při hodnocení rizik. Vše je podložené výčtem bodů, které mají být brány při hodnocení rizik v potaz a odkazem do příloh č. 1 a 2 k VKB, které obsahují vzorové (pouze doporučené) stupnice pro hodnocení. Pochopitelným rozdílem v požadavcích na KII a VIS je rozdílný rozsah zvažovaných aktiv. Zatímco v případě KII mají být hodnocena všechna aktiva a s nimi související rizika (hrozby a zranitelnosti), v případě VIS se tak má dít pouze pro primární aktiva. Pokud však chce organizace získat lepší přehled o svých aktivech a maximalizovat přidanou hodnotu tohoto opatření, lze obecně doporučit plnění tohoto opatření nad rámec povinnosti.

Výstupem řízení rizik má být několik vzájemně provázaných dokumentů. Výchozím dokumentem je zpráva o hodnocení aktiv a rizik a v návaznosti na ni a ideálně na některý z registrů opatření má být sestaveno prohlášení o aplikovatelnosti. Dalším dokumentem navázaným na zprávu o hodnocení rizik je plán jejich zvládání – tyto dokumenty nelze vytvářet a spravovat izolovaně. VKB mimo jiné definuje minimální požadavky na obsah těchto dokumentů. Zcela zásadní je pak uvědomit si, že se jedná o kontinuální proces, a nikoli o jednorázový, jak je někdy mylně chápáno.

[1] Prvky KII jsou myšleny komunikační a informační systémy kritické informační infrastruktury.

[2] VIS jsou myšleny významné informační systémy.

ANKETA

NÁŠ ČASOPIS

1. S jakými tématy byste se rádi setkali v časopise v následujících číslech?

2. Co Vás v minulých číslech časopisu Interní auditor nejvíce zaujalo?

3. Jak jste spokojeni s formou a formátem časopisu?

Tomáš Malchárek
interní auditor ICT a bezpečnosti
Metrostav a.s.

1. Audity IT a kybernetické bezpečnosti.

2. ×

3. Spokojen.

VKB umožňuje plnit, podobně jako ve většině ostatních případů, toto opatření jiným způsobem, než uvádí VKB, za předpokladu že tento jiný způsob zajišťuje stejnou nebo vyšší bezpečnost.

Bezpečnostní politika

I bezpečnostní politiky již byly avizovány v požadavcích na zavedení ISMS. Hlavním opatřením v této oblasti je stanovení bezpečnostní(ch) politik pokrývající(ch) taxativně vyjmenované oblasti v rozdílném objemu pro KII a VIS. Praxe ukazuje, že tento taxativní výčet může být chápán jako seznam jednotlivých politik, opatření však míří především na pokrytí uvedených oblastí a nechává plně v kompetenci správce, zda vytvoří jednu všeobjímající politiku, nebo ji rozdělí do několika dílčích. Stejně tak nejsou důležité názvy těchto politik, ale jejich obsah a úplnost s přihlédnutím, zda je, či není daná oblast pro správce a dotčený systém/prvek relevantní.

Organizační bezpečnost

V oblasti organizační bezpečnosti je definováno bezpečnostní opatření požadující jak pro prvky KII, tak VIS zavedení tzv. výboru pro řízení kybernetické bezpečnosti a další bezpečnostní role, včetně jejich práv a povinností. Tyto role jsou manažer, architekt a auditor kybernetické bezpečnosti a garant aktiva, přičemž tyto role jsou pro správce KII povinné, zatímco pro správce VIS je povinná pouze role garanta aktiv a zavedení ostatních rolí je „dobrovolné" – role mají být dle VKB zavedeny přiměřeně. Na základě dosavadní praxe však lze silně doporučit stanovení alespoň manažera KB. Ve většině případů je totiž lepší, když náplň (povinnosti) této role v rámci organizace vykonává jeden člověk, než když je rozmělněna mezi více osob bez reálné odpovědnosti. V této pasáži VKB jsou dále uvedeny popisy jednotlivých bezpečnostních rolí a všeobecný požadavek na zajištění jejich odborného vzdělávání v souladu s dále popisovaným plánem rozvoje bezpečnostního povědomí.

V reálu se často setkáváme s dotazy na požadovanou tříletou praxi u zástupců bezpečnostních rolí. Její prokazování se může zdát obtížné, nicméně pro splnění tohoto požadavku plně dostačuje čestné prohlášení podložené relevantními zkušenostmi související s oborem, ať už se jedná o audit, návrh sítě, nebo její zabezpečení.

Stanovení bezpečnostních požadavků pro dodavatele

Další z požadovaných bezpečnostních opatření je zaměřeno na řízení vztahů s dodavateli ve smyslu zajištění řízení bezpečnosti informací. Nejde o nic složitějšího než o seznámení dodavatele se stanovenými bezpečnostními politikami, případně dalšími relevantními bezpečnostními požadavky a jejich zanesení do relevantních smluv formou ustanovení o bezpečnosti informací. Situace se komplikuje v případě stávajících (dlouhodobých) smluv, jejichž změna či doplnění nemusí být zcela triviální. Na zcela samostatnou kapitolu by pak byla problematika výběrových řízení. Po správcích KII je navíc požadováno pravidelné hodnocení rizik spojených s dodávkou (dodavatelem) a povinnost smluvně stanovit úroveň poskytovaných služeb (SLA).

Řízení aktiv

Bezpečnostní opatření věnované řízení aktiv dále rozvádí problematiku identifikace a hodnocení aktiv zmíněnou v požadavcích (opatřeních) na řízení rizik. Pro úplnost tedy zopakuji, že jediným rozdílem mezi požadavky na řízení aktiv pro správce VIS a KII je povinnost řídit také podpůrná aktiva a jejich vazby na primární aktiva vyžadovaná u prvků KII. Následující požadavky jako identifikace a hodnocení důležitosti aktiv, určení garantů odpovědných za jejich správu a další rozvoj, jejich hodnocení z hlediska důvěrnosti, dostupnosti a integrity jsou již společná pro všechny kategorie systémů.

> „Na základě dosavadní praxe s VIS však lze silně doporučit stanovení alespoň manažera kybernetické bezpečnosti"

Jednou z oblastí, pro které má být zpracována bezpečnostní politika, související s touto problematikou, je klasifikace aktiv. Ta by měla obsahovat další z požadavků souvisejících s řízením aktiv, a to pravidla pro rozlišování jednotlivých úrovní aktiv a dále pravidla pro manipulaci s nimi, jejich užívání, evidenci a ochranu.

Bezpečnost lidských zdrojů

Oblast bezpečnosti lidských zdrojů je podpořena opatřením, jehož předmětem je zpracování zmiňovaného plánu rozvoje bezpečnostního povědomí, nyní však ne pouze v kontextu bezpečnostních rolí, ale v kontextu celé organizace. Plán má mj. zahrnovat formu, rozsah a obsah školení napříč všemi rolemi, včetně té uživatelské. Kromě sestavení plánu je obsahem tohoto bezpečnostního opatření také požadavek na dohled nad jeho výkonem a vedením záznamů o jeho průběhu. Dále stanovení pravidel a postupů kontroly dodržování všech bezpečnostních politik ze strany uživatelů s důrazem na dodržování pravidel pro manipulaci s aktivy, především vracením svěřených aktiv.

Věra Štembírková
vedoucí ÚIA
Olomoucký kraj

1. Samozřejmě cokoliv se týká změny a dodržování Standardů, veškerých změn v oblasti mezinárodních metodik a doporučení pro interní audit. Nebylo by špatné se podívat na otázku spisové služby, a to jak vedení vlastního spisu auditu a jeho archivace, tak i obecnému vedení spisové služby v návaznosti na změnu zákona o archivní a spisové službě podle nařízení EU a případně i zkušenosti z praxe či interního auditu (třeba ministerstvo vnitra?) nebo příslušný úřad? Tato oblast se také dotýká aplikace (ověřených) elektronických podpisů a práce s digitálními dokumenty – a jsme zase v oblasti kybernetické bezpečnosti (viz otázka č. 3).

2. Opravdu velmi mne zaujalo poslední číslo IA 3/2016, kde je rozpracováno téma kybernetické bezpečnosti srozumitelnou formou pro pracovníky „nepraktikující" v oblasti IT. Naši pracovníci výpočetní techniky si budují postavení nedotknutelných „guru", na které nikdo nemá. Výklad oblasti kybernetické bezpečnosti byla podána ve srozumitelné podobě a je jedním z obrovských kroků k tomu, aby si „ajťáci" uvědomili, že se buď

Podpora zvyšování bezpečnostního povědomí v celém kontextu organizace má velký dopad na zabezpečení jednotlivých systémů a jejich bezpečný provoz. Je jedním z klíčových faktorů v prezentaci důvěrnosti (důvěryhodnosti) celé organizace okolnímu světu. Správce KII (pro správce VIS platí opět přiměřeně v návaznosti na určené bezpečnostní role) zpracuje pravidla pro určení osob zastávajících bezpečnostní role, např. jejich zanesením do organizačního řádu.

Řízení provozu a komunikací

Hlavní motivací pro zavedení opatření v oblasti řízení provozu a komunikací je zajistit integritu, stabilitu a bezpečnost provozu systému. Prvním dílčím krokem k takovému výsledku je stanovení provozních pravidel a postupů. Následně je pak na místě monitoring provozu a detekce kybernetických bezpečnostních událostí s pravidelným hodnocením výstupů a řešením detekovaných událostí v souladu se zavedenými opatřeními v oblasti zvládání kybernetických bezpečnostních událostí a incidentů. K zajištění zmiňované stability pak má přispět pravidelné zálohování doplněné prověřováním funkčnosti provedených záloh.

Nad rámec těchto požadavků VKB správcům prvků KII předepisuje základní body obsahu výše zmiňovaných pravidel a postupů, jako je požadavek na stanovení práv a povinností jednotlivých rolí (od manažera až po uživatele), postupy pro spuštění restartu a ukončení chodu systémů po selhání, komunikační matice pro nestandardní stavy aj., dále potom požaduje také striktní oddělení vývojového, testovacího a produkčního prostředí.

Řízení přístupu a bezpečné chování uživatelů

V rámci opatření pro řízení přístupů a bezpečného chování uživatelů mají byt stanoveny základní principy řízení přístupů (technické parametry jsou stanoveny v technických opatření VKB). Správce systémů KII a VIS má dle aktuálních provozních a bezpečnostních potřeb přidělovat přístupová opatření, přičemž přiděluje každému uživateli jednoznačný identifikátor. U přihlašovacích údajů samozřejmě musí být zachována maximální důvěrnost, musí být přijata opatření, která brání jejich zneužití třetí osobou. V návaznosti na řízení aktiv by zde měl být aplikován princip need-to-know. Správce systému KII musí dále stanovit jasná pravidla pro přidělování privilegovaných uživatelských/ /administrátorských účtů. Dohlíží na výkon a dodržování politiky řízení přístupů a řídí přístupy s ohledem na bezpečné užívání mobilních zařízení.

Akvizice, vývoj a údržba

Nelze opomenout zavedení bezpečnostních opatření souvisejících se změnami zabezpečovaných systémů. Předpokladem pro zabezpečení této oblasti je sestavení bezpečnostních požadavků souvisejících s požadavky na změny a jejich zanesení do změnových projektů, ať už se jedná o změny související s vývojem, nebo údržbou. Pro prvky KII je dále stanoven požadavek směřující k řízení rizik (potřeba řídit rizika spojená s touto problematikou) a také k řízení provozu (oddělení vývojového, testovacího a produkčního prostředí, včetně dat).

Zvládání kybernetických bezpečnostních událostí a incidentů

Pro zajištění maximální možné plynulosti a bezpečnosti zabezpečovaných systémů si další opatření vyžadované VKB staví za cíl nastavení procesu zvládání kybernetických bezpečnostních událostí a incidentů (dále pouze události a incidenty). Logicky první řešenou oblastí musí být zajištění oznamování událostí ze strany uživatelů a administrátorů podpořené výše zmiňovanými detekčními systémy. O těchto oznámeních musí být vedena evidence doplněná o prostředí pro vyhodnocování oznámených/detekovaných událostí a následnou analýzu, jejímž výstupem má být mimo jiné rozhodnutí, zda se jedná o událost, či incident, a jeho případná klasifikace. Pro případ výskytu incidentů mají být stanoveny postupy pro jejich řešení a hlášení dle zákonné povinnosti NBÚ. Dále mají být stanoveny postupy pro sběr věrohodných důkazů a příčin. Provedením analýz nad těmito informacemi pak má dojít ke zdokonalení implementovaných opatření, případně nasazení nových opatření s cílem zamezit opakování řešeného incidentu. Veškeré kroky prováděné v rámci zvládání událostí a incidentů by měly být dokumentovány.

„V reálu se často setkáváme s dotazy na požadovanou tříletou praxi u zástupců bezpečnostních rolí“

Řízení kontinuity činností (Business Continuity Management)

Klíčové pro zavedení opatření v této oblasti je stanovení minimální úrovně poskytovaných služeb pro provoz, užívání a řízení dotčených systémů. Dále mají být připraveny plány zabezpečující obnovení této úrovně služeb (Disaster Recovery Plan), včetně stanovení doby na obnovu chodu – doba, během které bude výše definovaná minimální úroveň opět zajištěna. Aby bylo toto opatření funkční, je nutné v rámci zpracovaných plánů definovat také práva, povinnosti a odpovědnost zainteresovaných osob. Plány by měly korespondovat s pravidly pro řízení provozu.

změní, anebo je někdo vymění. Skokové zvýšení povědomí o jejich práci je neocenitelné.

3. Ano, forma i formát časopisu mi vyhovuje. Písemnou podobu mám často v příručním zavazadle na cestách, jde číst na nástupišti vlaku i v čekárně u lékaře, nebo v dopravním prostředku. Naposledy se mnou cestoval minulý rok do Španělska, kde jsem ho přelouskala od a do z. Kvalitní papír byl odolný i proti mořské vodě – ostatní tiskoviny nevydržely. Elektronickou formu časopisu moc nevyužívám, ale když potřebuji konkrétní tisk, sáhnu i na jeho formát.

Jiří Skoblík
interní auditor
Vysoká škola báňská – Technická univerzita Ostrava

1. Novela zákona č. 320/2006 Sb.

2. Nové standardy.

3. Ano, jsem.

Kontrola a audit KII a VIS

Aby bylo zajištěné neustálé zlepšování úrovně zabezpečení dotčených systémů, definuje VKB jako poslední bezpečnostní opatření požadavek na provádění kontroly a auditu KII a VIS. Konkrétně formou posouzení souladu zavedených bezpečnostních opatření s právními, vnitřními a jinými relevantními předpisy, případně jinými smluvními závazky. Současně má být zajištěna pravidelná kontrola dodržování stanovených bezpečnostních politik, jejíž výstupy jsou brány v potaz při aktualizaci plánu rozvoje bezpečnostního povědomí, a případně plánu zvládání rizik – přesněji řečeno analýzy rizik samotné.

Pro KII je pak toto opatření rozšířeno o požadavek na provádění testů zranitelností technických prostředků opět s výstupem sloužícím jako podklad pro provádění analýzy rizik.

Shrnutí

Důležitým faktorem pro úspěšné zavedení výše popsaných opatření je uvědomění si, že se jedná o komplexní vzájemně provázanou problematiku, kterou je nutné řešit napříč celou organizační strukturou povinné osoby. Smyslem VKB není zavádět jednotlivá opatření, ale funkční systém opatření s cílem budovat bezpečnou, fungující organizaci, a podpořit tak její dobré jméno.

„Podpora zvyšování bezpečnostního povědomí v celém kontextu organizace má velký dopad na zabezpečení jednotlivých systémů a jejich bezpečný provoz“

Pokračování článku věnované technickým opatřením doplněné o několik doporučení při implementaci opatření podle VKB bude v příštím čísle časopisu Interní auditor.

[Kheng Ho Toh] © 123RF.COM

Tomáš Mrkos
interní auditor
Ministerstvo obrany

1. Rád bych se setkal s problematikou podvodů v prostředí veřejné správy (dále VS). Akcentuji právě VS, protože většina podvodů končí šetřením orgánů činných v trestním řízení a zajímala by mne konkrétní úloha interního audiu v těchto případech. Dále mne zajímá možnost využití postupů forenzního auditu interními auditory ve VS.

2. Zaujala mne především problematika kybernetické bezpečnosti a datová analýza.

3. Ano jsem. :-)

Cloud očima regulátora

Ing. Martin Fleischmann, Ph.D.
Česká národní banka,
Sekce dohledu nad finančním trhem

1. Úvod

Neutuchající technický pokrok v oblastech síťové konektivity, disponibilního výpočetního výkonu, kapacity úložišť dat i efektivity jejich zpracování umožňuje nebývalou dostupnost dat a aplikací pro firmy i domácnosti. Data a aplikace jsou dostupná prakticky odkudkoliv, kdykoliv, z mnoha různých oblastí a zdrojů. To vše je umocněno rozmachem stále výkonnějších mobilních zařízení. Není proto divu, že využití informačních a komunikačních technologií je a nadále bude rozpoznáváno jako obchodní příležitost a stále častěji aplikováno v praxi nefinanční i finanční industrie. Jde například o inovace využívající platformy typu cloud computing, big data, blockchain, fundraising (crowd/equity/ /peer-to-peer funding/lending), biometrika, robotika, IoT (internet of things), AI (artificial inteligence) a další.

V souvislosti s poskytováním služeb na finančních trzích jsou tato řešení obvykle zahrnována pod pojmem *„Fintech"*. Kromě využití výše uvedených technických platforem je jejich nasazení spojováno s předpokládanou další personalizací poskytovaných produktů a služeb vyžadující změny obchodních modelů stávajících finančních institucí, včetně další proměny existujících distribučních kanálů. Zároveň jsme v rámci těchto trendů svědky snahy o zapojení dalších dosud neregulovaných subjektů do poskytování finančních produktů a služeb. Řada potenciálních aplikací však prozatím naráží na mnohá omezení v oblasti technické, organizační i legislativní. Navíc je zřejmé, že kromě přínosů představují uvedené důsledky změny rizikového profilu jednotlivých institucí i celého sektoru. To vyžaduje důkladnou přípravu na straně institucí i regulátorů tak, aby všechna rizika byla přiměřeně zvládána.

Z těchto důvodů proto není dosud většina z výše uvedených technologií finančními institucemi ve větším rozsahu využívána. Určitou výjimku z tohoto pravidla představují řešení založená na **cloud computingu**. V této oblasti již některé finanční instituce získávají zkušenosti s jeho praktickým využíváním u vybraných (méně významných) systémů a služeb. Proto je tento článek věnován právě problematice cloud computingu s důrazem na jeho obezřetné využívání.

2. Cloud computing a uplatnění principu přiměřenosti

Obecným přístupem ČNB je nebránit institucím ve využívání technologických inovací. ČNB zachovává v této oblasti důslednou technologickou neutralitu a důraz klade na zvládnutí rizik souvisejících s nasazením konkrétního řešení. Přípustné je tedy použití jakéhokoliv řešení, pokud splňuje požadavky platné regulace a očekávání ČNB.

V uplynulých letech některé finanční instituce zvažovaly nebo se připravovaly na využívání cloud computingu. V reakci na rostoucí počet dotazů a konzultací provedl dohled ČNB v roce 2015 *šetření mapující využívání a záměry aplikace cloud computingu* v sektoru bank, pojišťoven a družstevních záložen. ČNB na tento vývoj reagovala také řadou vystoupení na toto téma na různých fórech a dne 4. 12. 2015 zveřejnila *otázky a odpovědi ke cloud computingu*. Následně se ČNB rozhodla upravit tuto aktuální problematiku ještě komplexněji a dne 19. 8. 2016 *vydala Úřední sdělení k výkonu na finančním trhu – cloud computing*[1].

Toto sdělení obsahuje vymezení cloud computingu[2], věnuje se uplatnění principu přiměřenosti při využívání cloud computingu a upravuje očekávání ČNB v této oblasti. Úřední sdělení neposkytuje *„rule-based"* vyčerpávající vodítka. Jednotlivé případy využívání cloud computingu se totiž natolik liší, že jejich posouzení a vyhodnocení vyžaduje individuální přístup. Nicméně úřední sdělení takovéto posouzení významně metodicky podporuje, a to v mezích stanovených požadavky právních předpisů. Za zmínku dále stojí, že v jeho působnosti nejsou pouze banky a spořitelní a úvěrní družstva, ale také tuzemské pojišťovny a tuzemské zajišťovny. Kromě nich je však využitelné jako metodická pomůcka i pro další poskytovatele finančních služeb podléhajících dohledu ČNB.

Oblast outsourcingu, a tedy i cloud computingu, je standardní součástí kontrol prováděných dohledem ČNB v oblasti řízení rizik informačních systémů a technologií. Průběžně je dále dohled ČNB informován o záměrech sjednat outsourcing ve formě cloud computingu mj. i na základě oznamovací povinnosti stanovené v § 107 Vyhlášky č. 163/2014 nebo v odst. 5, § 7g, zákona

[1] Viz http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/legislativa/vestnik/2016/download/vestnik_2016_08_20816560.pdf

[2] Vymezení pojmu „cloud computing" zohledňuje definici Národního ústavu pro normalizaci a technologie USA NIST (2009), která zní: „Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf).

Ludmila Jiráňová
vedoucí interního auditu a kontroly
ČHMÚ

1. Zkušenosti interních auditorů z různých oblastí auditu, novinky – zákony a dále až po zpracovávání směrnic přímo v organizacích.

2. Kybernetická bezpečnost.

3. Ano, jsem spokojena s výtiskem, který získávám, ale i možností otevření v PC.

Dana Vojíková
senior IA
Magistrát města Plzně

1. Ráda bych poznala praktické příklady metodiky a provádění různých typů auditů od různých auditorů.

2. Vždy mne potěší, když se věnujete tématům z praxe.

3. Uvítala bych „skladnější" provedení časopisu, než je A4, a častější vydání. Elektronická forma je výborná.

č. 277/2009 Sb. o pojišťovnictví. Oznámené záměry cloud computingu pak ČNB posuzuje, vzhledem k značné rozmanitosti jednotlivých aplikací, případ od případu a většinou je konzultuje s příslušnou finanční institucí a eventuálně také s potenciálním dodavatelem. Smyslem této činnosti je na jedné straně seznámit se s hlavními charakteristikami daného řešení a způsobem, jakým hodlá příslušná instituce kontrolovat související rizika, a na druhé straně vyjasnit očekávání regulátora v daném individuálním případě tak, aby daná instituce i poskytovatel měli možnost již v této fázi účinně omezit případná budoucí rizika nebo od outsourcingového záměru včas, a tedy bez větších škod ustoupit. Výsledkem těchto konzultací však není posouzení, a tedy ani schválení příslušného outsourcingového vztahu. Soulad s regulací a očekáváními ČNB je posuzován až prostřednictvím kontrol na místě a případná náprava nedostatků je obvykle požadována na základě výsledků těchto kontrol.

> „Obecným přístupem ČNB je nebránit institucím ve využívání technologických inovací“

Na úrovni regulatorních autorit EU panuje dlouhodobě shoda, že cloud computing je formou outsourcingu, a tudíž podléhá regulaci pro outsourcing. Poněkud odlišná situace je však v názoru na způsob aplikace této regulace. Zatímco některé autority trvají v případě využívání cloud computingu na splnění všech požadavků kladených na outsourcing v plném rozsahu, jiné dospěly k závěru, že je za určitých okolností možné a vhodné uplatnit princip přiměřenosti. Smyslem tohoto přístupu je snaha těchto regulátorů nebránit finančním institucím ve smysluplném a obezřetném využití cloud computingu.

I v tomto případě je sice nezbytné reflektovat všechny požadavky stanovené regulací, avšak způsobem, který odpovídá povaze, rozsahu a komplexnosti dotčených činností, souvisejícím rizikům a dalším relevantním okolnostem konkrétního případu. V souladu s přístupem k využívání technologických inovací zmíněným výše se ČNB řadí mezi tuto druhou skupinu regulatorních autorit, které dospěly k závěru, že úplné splnění všech požadavků kladených na outsourcing je u cloud computingu v některých případech prakticky těžko dosažitelné, a v některých oblastech může být dokonce kontraproduktivní, tj. může paradoxně zvyšovat rizikovou expozici dotčených institucí i finančního sektoru jako celku.[3]

Důležitým předpokladem **uplatnění principu přiměřenosti** je důkladné zhodnocení a zohlednění významu, rizikového profilu a povahy konkrétní aplikace cloud computingu. V této souvislosti ČNB očekává, že „Zmírnění nebo modifikace jsou akceptovatelné např., jde-li o informační a komunikační systémy na podporu spolupráce a sdílení informací pouze v rámci poskytovatele finančních služeb anebo v rámci skupiny, jejímž je členem, nebo o uložení nebo zpracovávání veřejně dostupných dat. Pokud by však byl výsledný stav, i s přihlédnutím k zásadě přiměřenosti, v nesouladu s povinnostmi poskytovatele finančních služeb stanovenými právními předpisy, poskytovatel finančních služeb k využití cloud computingu v dané oblasti by neměl přistoupit.“[4]

Jinými slovy to znamená, že outsourcování jednotlivých částí IS/IT dané instituce formou cloud computingu v současné době není přípustné, pokud by se jednalo o některý z významnějších informačních systémů. Význam jedné každé součásti IS/IT je přitom předurčen řadou kritérií, jako jsou například kritičnost obchodních funkcí podporovaných daným IS/IT či charakter v něm zpracovávaných dat. Praxe zatím potvrzuje, že toto obezřetnostní očekávání ČNB je sdíleno i ze strany finančních institucí, a svědčí tak o jejich racionálním a obezřetném přístupu.

3. Specifika cloud computingu a zvládání rizik s tím spojených

Před tím, než instituce přistoupí k využívání cloud computingu, je třeba, aby ve svých **strategiích** jasně a konkrétně vymezila **celkový přístup a hlavní zásady využívání cloud computingu** a patřičně zohlednila jeho specifika. V těchto dokumentech nesmí chybět upřesnění hlavních zásad a postupů pro zajištění důvěrnosti, integrity a dostupnosti informací. Tato formální vymezení jsou základem pro zavedení postupů pro rozpoznávání a řízení rizik spjatých s využíváním cloud computingu do praxe. Za účelem jejich účinného a efektivního zajištění si finanční instituce potřebuje zachovat dostatečné odborné kapacity v oblasti technické, organizační a právní.

[3] Příkladem tohoto paradoxu může být striktní trvání regulátorů na provádění pravidelných kontrol a auditů u poskytovatele ze strany regulovaných institucí bez jakéhokoliv omezení. V případě globálně působících cloudových poskytovatelů by to představovalo nejenom jejich značnou zátěž v důsledku kontrol velkého množství finančních institucí, ale mohlo vést k situaci, kdy rizika spojená s vyzrazením bezpečnostních opatření aplikovaných poskytovatelem převýší hodnotu ujištění získaného v rámci takové kontroly. Na druhé straně však, jak je vysvětleno v dalším textu, to neznamená rezignaci finanční instituce na právo kontroly či auditu poskytovatele, ba naopak.

[4] Úřední sdělení ČNB ze dne 19. srpna 2016 k výkonu činnosti na finančním trhu – cloud computing, Podrobnější informace o přístupu České národní banky ke cloud computingu, odst. 4.

Jaroslav CHLOUBA
interní auditor, klíčová funkce pojišťovny
Pojišťovna VZP, a.s.

1. Osvěta k úpravám Standardů IIA od 2017 a možná také ještě QAR (kvalita se musí stále zlepšovat).

2. Téma výborů pro audit – i na toto téma lze ještě pokračovat a rozšířit jej s ohledem na aktuálně platnou legislativu, která prošla v poslední době změnami.

3. Určitě ANO. Časopis se stále zlepšuje.

Prostor k vyjádření.

Jak již bylo naznačeno výše, vyplývají z povahy cloud computingu některá specifika, která mohou v určitých případech ovlivňovat rozsah, obsah a rekonstruovatelnost informací o řídicích a kontrolních procesech dodavatelů relevantních pro posouzení rizik souvisejících s poskytovanou službou. Tím může být ovlivněn i **výkon kontroly a auditu nad outsourcovanými procesy ze strany finanční instituce**. Týká se to nejčastěji případů, kdy poskytovatelem je velká globálně působící společnost. v praxi se jedná například o omezení při získávání informací, jejich ověření a při zajištění nezávislého ujištění o úrovni řídicího a kontrolního systému poskytovatele ze strany povinné osoby, a to z hlediska kontrolních mechanizmů na všech 3 liniích obrany tzn. na linii: i) operativní a provozní, ii) řízení rizik a iii) interního auditu.

I v těchto případech ČNB očekává, že finanční instituce disponuje ve všech fázích životního cyklu[5] dostatečnými informacemi o řídicích a kontrolních procesech relevantních pro posouzení všech rizik vyplývajících z využívání cloud computingu a zároveň disponuje právem provést přímo kontrolu a/nebo audit procesů významných pro bezpečnost a dostupnost dat, služeb a outsourcovaných činností na místě u poskytovatele.

Pokud jsou však přesto některé kontrolní a auditní činnosti u poskytovatele zajišťované finanční institucí nebo získávání těchto informací z jeho strany z objektivních důvodů omezeny (ať už z hlediska způsobu provedení, rozsahu, zaměření, místa, nebo času), musí mít finanční instituce **právo zadat důvěryhodné a odborně způsobilé třetí straně kontrolu nebo audit procesů významných pro bezpečnost a dostupnost dat, služeb a outsourcovaných činností na místě u poskytovatele**.

Kromě toho však může v těchto případech finanční instituce využívat cloud computing výhradně s podmínkou uplatnění dalších dodatečných opatření tak, aby měla jistotu, že pracovní postupy v oblasti bezpečnosti informací jsou alespoň na úrovni postupů, kterou by finanční instituce použila, pokud by dané činnosti i nadále zajišťovala sama. To samozřejmě mj. předpokládá, že si insituce zachová **dostatečné odborné kapacity na všech třech liniích obrany**, nejenom při přípravě smluvního vztahu, ale také při jeho zavedení a provozování služby, včetně procesů souvisejících s případným ukončením služby. Pro ilustraci lze jako tato další opatření aplikovaná ze strany finanční instituce uvést následující aktivity[6]:

- Zajistit, aby kontroly a audity[7] u dodavatele poskytovaly aktuální, pravidelné, odborné a nezávislé ujištění o řídicích a kontrolních procesech, a zahrnovaly identifikaci, popis a posouzení všech rizik podstupovaných finanční institucí v souvislosti s využíváním cloud computingu,
- Disponovat zprávami z těchto kontrol a auditů tak, že tyto jsou trvale v držení povinné osoby nezávisle na dodavateli.[8] Zprávy by měly být vypracovávány jednou ročně nebo s periodicitou zajišťující pro finanční instituci adekvátní nezávislé ujištění.

[5] Životní cyklus zahrnuje tyto fáze a prvky: příprava smluvního vztahu, vlastní smlouva – kontrakt, provozování a využívání služby, ukončení smluvního vztahu .

[6] Jedná se o ilustrativní, nikoliv úplný či jediný možný výčet. Konkrétní opatření je třeba vždy přizpůsobit konkrétním podmínkám clooud computingového vztahu.

[7] ČNB v rámci ohlašovací povinnosti dle § 107 Vyhlášky č. 163/2016 očekává sdělení informací o externích auditorech poskytovatele.

[8] Ve fázi přípravy smluvního vztahu může být v odůvodněných případech po přechodnou dobu přípustné, aby zprávy byly v plném rozsahu a bez dalších omezení zpřístupněny (například formou zabezpečeného dálkového přístupu), tedy bez toho, aby je v této fázi životního cyklu outsourcingu měla finanční instituce v přímém držení.

[Dmitriy Shpilko] © 123RF.COM

- Poskytnout na vyžádání tyto auditní zprávy České národní bance tak, aby byly použitelné pro úkony v působnosti ČNB vyplývající z příslušných právních předpisů[9].
- Zajistit, aby práce s auditními zprávami umožňovala zpětnou vysledovatelnost a rekonstruovatelnost.
- Disponovat ve všech fázích životního cyklu outsourcingového vztahu možností průběžně a bez zbytečných omezení kontaktovat určené zaměstnance poskytovatele, kteří jsou plně kompetentní poskytnout vysvětlení a informace ohledně interních procesů a postupů poskytovatele souvisejících s outsourcovanými daty a službami, a to včetně vysvětlení informací, nálezů a nápravných opatření týkajících se auditních zpráv.
- Disponovat, kromě výše uvedeného, ve všech fázích životního cyklu dalšími dokumenty a informacemi, které zajišťují dostatečné doplnění informací o vnitřních postupech a opatřeních zavedených u poskytovatele k omezení rizik a spolu s dalšími dokumenty a informacemi o poskytovateli umožňují průběžnou identifikaci a hodnocení rizik podstupovaných finanční institucí, včetně hodnocení efektivity outsourcingu.

Smlouva o poskytování outsourcingu je zásadním dokumentem upravujícím danou službu. Zároveň je sjednávání smluvních podmínek nejlepší příležitostí k eliminaci celé řady rizik na straně finanční instituce. Pokud tato příležitost není adekvátně uchopena, zakládá si daná instituce do budoucna na vážné komplikace v podobě negativních dopadů na její činnost i finančních ztrát. Aby se smlouva mohla stát efektivním nástrojem řízení outsourcingového vztahu, musí vycházet z provedené analýzy rizik, o které bude ještě řeč. V případě cloud computingu je to o to naléhavější, že smluvní protistranou je většinou partner disponující řádově většími zdroji, prostředky a tedy i vlivem než drtivá většina finančních institucí – jeho potenciálních klientů.

Navíc je třeba vzít v úvahu i následující specifika:
„V případě využití cloudových služeb jsme obvykle postaveni před nutnost vypořádat se s požadavky národních, nadnárodních a zahraničních jurisdikcí, zejména v oblasti ochrany bankovního tajemství a osobních údajů. Vzhledem k charakteru cloud computingu, a s tím související přeshraniční působností jeho hlavních poskytovatelů, je nutné tyto aspekty v celé jejich šíři ošetřit. Umístění outsourcovaných dat a služeb spolurozhoduje o rozsahu legislativních požadavků, které budou pro daný vztah ve hře. To obnáší nejen povinnost zajistit smluvní ustanovení splňující požadavky všech možných příslušných právních a regulatorních norem, ale zajistit také jejich jednoznačnost (eliminovat riziko nejasného vymezení) a praktickou použitelnost (vynutitelnost) stanoveným způsobem, v potřebném čase a rozsahu. … Kromě volby právního řádu je při přípravě outsourcingového vztahu dále třeba důkladně zanalyzovat možnosti a způsoby řešení případných sporů. Mimo to je nutné již ve smlouvě pamatovat na možnost změn, úprav i na možnost ukončení outsourcingového vztahu. O precizním vymezení povinností dodavatele a instituce v oblasti dostupnosti, důvěrnosti a integrity informací nemluvě.“[10]

K tomu je třeba dodat, že velmi důležitá je **srozumitelnost a jednoznačnost smlouvy**. Finanční instituce musí přesně porozumět významu použité smluvní terminologie a přesně jednotlivé pojmy vymezit. Na první pohled jednoznačné pojmy jako například „zákaznická data“, „data centrum“ apod. mohou bez přesného vymezení a pochopení způsobit v budoucnu vážné problémy. Smlouva je také místem, kde má finanční instituce relativně největší prostor eliminovat **riziko nerovného postavení** ve smluvním vztahu. Toto riziko roste s velikostí poskytovatele a naopak klesá s tím, v jaké míře je poskytovatel připraven přizpůsobit se individuálním potřebám a regulatorním požadavkům kladeným na finanční instituce. Z dosavadních zkušeností vyplývá, že v tomto ohledu, jsou mezi dodavateli obdobných produktů a služeb značné rozdíly.

Ještě významnější než dokonalé formulování smlouvy je proto vlastní **výběr poskytovatele**. Proces posouzení a výběru poskytovatele by měl všechna výše uvedená hlediska reflektovat.

> „Přípustné je použití jakéhokoliv řešení, pokud splňuje požadavky platné regulace a očekávání ČNB“

V centru pozornosti dohledových autorit je **analýza rizik** služeb cloud computingu. Její kvalita předurčuje kvalitu všech prvků řízení outsourcingového vztahu na straně instituce, a to ve všech fázích jeho životního cyklu. Jak již bylo řečeno, analýza rizik musí být zohledněna a využita při přípravě smluvního vztahu. Kromě již výše zmíněného rizika nerovného postavení musí identifikovat, zhodnotit a ošetřit **všechna další relevantní rizika, a to v rovině technické, procesní i právní**. Analýzu rizik by měla finanční instituce využívat při řízení rizik IS/IT a při kontrole poskytovatele outsourcingu např. v oblasti bezpečnostních zásad, bezpečnostního monitoringu či řízení bezpečnostních incidentů. Z tohoto důvodu je nezbytné provádět pravidelně a při každé významné změně aktualizaci analýzy rizik. Vypracování kvalitní analýzy rizik vyžaduje získání potřebných informací o relevantních procesech a částech řídicího a kontrolního systému poskytovatele. Například je nutné disponovat informacemi o hrozbách identifikovaných v analýze rizik poskytovatele, a mít tedy jasno v tom, která rizika a jakým způsobem pokrývá a řeší dodavatel, a která již nikoliv. Dále je nutné porozumět obsahu terminologie použité v dokumentaci poskytovatele – jde například o jednoznačné pochopení termínů typu „*data*“ vs. „*metadata*“ apod. Finanční instituce musí být rovněž seznámena s umístěním dat a služeb tak, aby mohla prokazatelně doložit lokaci a řídit rizika umístění svých dat (rizika zemí a jurisdikcí, AML rizika, apod.), a to jak z hlediska fyzické, tak i logické bezpečnosti. Součástí analýzy rizik musí být také oblasti zmíněné níže.

V podmínkách cloud computingu, zejména v případě velkých globálních poskytovatelů, je obvykle obtížnější identifikovat významné subdodavatele, a tedy rozpoznat a kontrolovat **řetězový outsourcing**. Je to dáno velkým počtem často různorodých subdodavatelů a také vlastní povahou cloud computingu, kdy dochází k odstínění nižších technologických vrstev od koncového

[9] Zejména kontrolní řád, správní řád, zákon o bankách, zákon o ČNB.

[10] Fleischmann, Martin, Dohled nad informačními systémy finančních institucí v podmínkách outsourcingu, DSM – data security management číslo 2/2014, červen 2014.

zákazníka. Z uvedeného vyplývá, že je v takových případech racionální zaměřit se na subdodavatele, jejichž činnost pro poskytovatele může mít reálný dopad na schopnost poskytovatele plnit své závazky vůči příslušné finanční instituci, správně je identifikovat a ošetřit všechna rizika a požadavky s tím spojené.

> „Soulad s regulací a očekáváními ČNB je posuzován až prostřednictvím kontrol na místě"

Dalším významným zdrojem potenciálních rizik je oblast **bezpečnosti přístupu k informacím**. Finanční instituce by proto měla disponovat dokumenty a informacemi, které jí umožní se ujistit, že postupy poskytovatele v této oblasti jsou alespoň na úrovni postupů, které by použila finanční instituce, pokud by činnost zajišťovala sama. Velmi důležité je znát podmínky přístupu pracovníků poskytovatele k datům finanční instituce, včetně zavedených kontrolních mechanizmů. Vzhledem k povaze cloud computingu ČNB v této souvislosti očekává, že přístup pracovníků poskytovatele k datům finanční instituce bude minimalizován na základě striktního uplatnění zásady *„need to know"*. Finanční instituce by se měla rovněž ujistit o způsobu, jakým jsou oddělena data a služby jednotlivých klientů využívajících stejnou cloudovou službu. Zároveň je nezbytné ověřit zabezpečení dat nejenom z hlediska jejich uložení v databázích poskytovatele (*„data at rest"*), ale také během jejich zpracování (*„data in use"*) a přenosu (*„data in transit"*).

> „Důležitým předpokladem uplatnění principu přiměřenosti je důkladné zhodnocení a zohlednění významu, rizikového profilu a povahy konkrétní aplikace cloud computingu"

Change management poskytovatele je také jednou z oblastí, s jejímž fungováním musí být finanční instituce v potřebném rozsahu obeznámena. Kromě toho je třeba se s dodavatelem dohodnout na rozsahu a konkrétním způsobu provádění změn. Plánované změny služby musí být komunikovány s dostatečným předstihem, aby nedocházelo k narušení integrity a/nebo dostupnosti dat a služeb. Je tedy nutné vytvořit technické, organizační i legislativní předpoklady zajišťující komplexní připravenost finanční instituce a jejího informačního systému na aktualizace služby prováděné poskytovatelem.

V rámci procesů **monitoringu a incident managementu** je třeba zajistit, aby poskytovatel cloud computingu hlásil finanční instituci všechny události, které ohrozily nebo narušily bezpečnost jejich dat. Příkladem může být situace, kdy dojde k neautorizovanému zpřístupnění dat instituce zaměstnanci poskytovatele, jedná se automaticky o bezpečnostní incident, který musí být rovněž neprodleně finanční instituci ohlášen.

V neposlední řadě je třeba věnovat pozornost **zajištění kontinuity činností**. Důraz by měl být kladen na situace, kdy může dojít k **omezení přístupu k vlastním datům**, a je tedy nutné zajistit přesun dat zpět nebo k jinému poskytovateli outsourcingu. Pro tyto účely by měla finanční instituce vypracovat strategii přesunu vlastních dat zpět nebo k jinému poskytovateli outsourcingu. Je žádoucí, aby finanční instituce věnovala pozornost i rizikům souvisejícím s tzv. vyšší mocí, včetně embarg a dalších geopolitických rizik. Je rovněž nezbytné, aby se finanční instituce ve svých pohotovostních plánech zaměřila i na **případ ztráty dodavatele** služby cloud computingu nebo **jednostranné ukončení outsourcingu**. Z uvedeného vyplývá, že je účelné užívat pokud možno otevřené formáty dat, které jejich případnou migraci usnadní (data portability). Přesun vlastních dat by měl být předmětem reálných testů tak, aby toto „testování návratu" potvrdilo reálnou dobu potřebnou k uskutečnění přesunu dat i adekvátnost prostředků, kterými je třeba pro takovou akci disponovat. Pro případ ukončení služby je třeba zajistit **bezpečné smazání dat**. Asi není třeba zdůrazňovat, že plány kontinuity obchodních činností by měly primárně akcentovat, jak si s výše uvedenými situacemi poradí business finanční instituce.

Z hlediska zajištění kontinuity činností je třeba věnovat zvýšenou pozornost **zálohování dat**. V případě cloud computingu jde totiž obvykle o zálohování na principu „všechna vejce v jednom košíku". Proto je nutné zvážit, zda není nutné některá data zálohovat jinde než u poskytovatele.

4. Závěr

Výše uvedený text odráží zkušenosti dohledu ČNB s aplikací cloud computingu na českém finančním trhu a částečně i zkušenosti dalších evropských dohledových autorit z této oblasti.

Vyplývá z něj, že ČNB za určitých podmínek akceptuje uplatnění principu přiměřenosti pro využívání cloud computingu.

Mezi klíčové a zároveň problematické oblasti spojené s využíváním cloud computingu v této souvislosti spatřuje zejména:

1. Zajištění kontroly a auditu ze strany finanční instituce
2. Smlouva
3. Proces posouzení a výběr poskytovatele
4. Analýza rizik
5. Řetězový outsourcing
6. Bezpečnost přístupu k datům
7. Change management
8. Monitoring a incident management
9. Zajištění kontinuity činností s důrazem na omezení přístupu k vlastním datům
10. Zálohování dat

Upozornění:
Zde uvedené informace vyjadřují názory autora, které se nemusí nezbytně shodovat s oficiálním názorem České národní banky. ■

Změny v přístupu útočníků za posledních pět let a další výhled (2. díl)

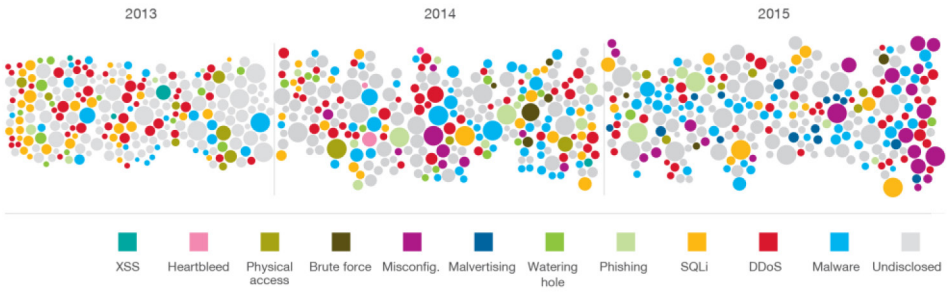
Jiří Slabý
Senior Manager IT & Security Consulting
Deloitte Czech Republic

Historie ukazuje vzorce chování útočníků

V oblasti bezpečnosti je velice těžké vyvozovat trendy, neboť útočníci se již dávno nesnaží ohromit svět kreativitou, ale vydělat kriminální činností peníze, a je jedno, zda použijí deset let starý trik, nebo úplnou novinku. Přesto je možné jisté závěry z minulosti vypozorovat.

Staré přístupy stále fungují

Obrázek 1 ukazuje porovnání posledních tří let z pohledu typu použitého útoku. Velikost kruhu značí závažnost průniku a barva poté typ útoku dle legendy.



Přehled největších útoků v letech 2013 až 2015 a jejich rozdělení podle druhu

Tento přehled ve zkratce prozrazuje několik faktů:

- pro velké úniky dat se již pomalu vytrácí dříve velice hojně využívaný SQL injection útok,
- přes veškerou snahu výrobců bezpečnostních technologií a firem o jejich implementaci existuje značné procento útoků, u kterých se nepodaří zjistit jejich původ a provedení,
- každým rokem roste počet sofistikovaného malware,
- spíše než dlouhodobě plánované akce jsou DDoS útoky sezonního charakteru a reagují na okamžitou situaci,
- útočníci se mnohem více zaměřili na špatně nebo nevhodně nastavené prvky infrastruktury, kdy není třeba vysloveně zneužít zranitelnost, ale kde nepozornost nebo ledabylost administrátorů otevře dveře mnohem snáze,
- klasické phishingové kampaně jsou stále populární, dokonce mírně na vzestupu.

Jiný pohled na trendy v hrozbách poskytuje každoroční zpráva ENISA (2). Jak je vidět, v pořadí prvních pěti kategorií k žádné změně meziročně nedošlo, pouze roste jejich intenzita.

Vlády nestojí stranou

Kromě vlny hacktivismu je jasně patrné rostoucí zapojování států na kybernetickém bojišti, což jde ruku v ruce s vývojem geopolitické situace. Po Snowdenově odhalení je navíc zřejmé, že tito aktéři disponují značnými prostředky a operují mimo rámec běžných zákonů.

Ukrajinská krize naplno ukázala, že kyberprostor je regulérní součástí bojiště a že moderní armády jsou na válku připraveny. Kybernetické útoky se během posledních pěti let staly plnohodnotnou součástí zbrojního arzenálu a propagandy.

Phishing: větší zacílení, chatrnější identita

Pravděpodobně neexistuje e-mailová schránka, do které by nebyl někdy doručen alespoň jeden nigerijský (či podobný) dopis. Tento typ útoku stále přetrvává, ale celkově dochází ke specializaci. Malware Carbanak, za kterým stojí stejnojmenná kriminální skupina a které se připisuje krádež v součtu až 1 miliardy amerických dolarů, je toho příkladem. Nicméně přesnější zacílení a rostoucí kvalita je zjevná i v běžném spamu a také na sociálních sítích. Je to způsobeno i zvětšující se digitální stopou, kterou za sebou jednotlivci nechávají.

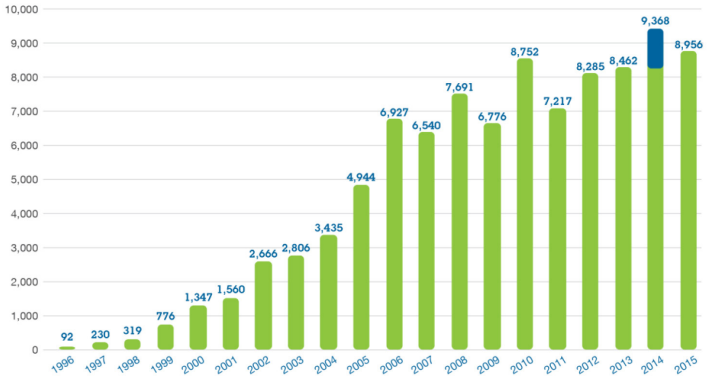
Top Threats 2014	Assessed Trends 2014	Top Threats 2015	Assessed Trends 2015	Change in ranking
1. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
2. Web-based attacks	↑	2. Web based attacks	↑	→
3. Web application /Injection attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Botnets	↓	→
5. Denial of service	↑	5. Denial of service	↑	→
6. Spam	↓	6. Physical damage/theft/loss	→	↑
7. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
8. Exploit kits	↓	8. Phishing	→	↓
9. Data breaches	↑	9. Spam	↓	↓
10. Physical damage/theft/loss	↑	10. Exploit kits	↑	↓

Nejrozšířenější typy hrozeb dle ENISA

Technická zranitelnost se neřeší

Odstraňování zranitelnosti aplikací a infrastruktury se za posledních pět let nikam výrazně neposunulo, využití zranitelnosti tedy stále zůstává nejběžnějším způsobem průniku. Podle studie společnosti Verizon bylo v roce 2015 až 99,9 % zneužitých zranitelností známo více než 1 rok[19]. Z pohledu na Obrázek 3 je patrné, že počet nalezených zranitelností se za poslední léta výrazně nezvýšil, ale ani nesnížil.

Počet zranitelností



Detekce incidentů stále pokulhává

Detekce bezpečnostních incidentů se zlepšuje, avšak velmi pomalu. Podle studie Trustwave z roku 2013 činila průměrná doba odhalení bezpečnostního incidentu 210 dní, v roce 2015 to bylo 188[20].

I v případě, že je incident detekován, je jeho následné řešení mnohdy také problémem. Řada organizací se věnuje primárně běžnému provozu a vyšetřování incidentu, kdy často není ztráta zřejmá ihned, má většinou podřadnou prioritu. Dobrou zprávou je rostoucí používání SIEM systémů a dohledových bezpečnostních center (SOC).

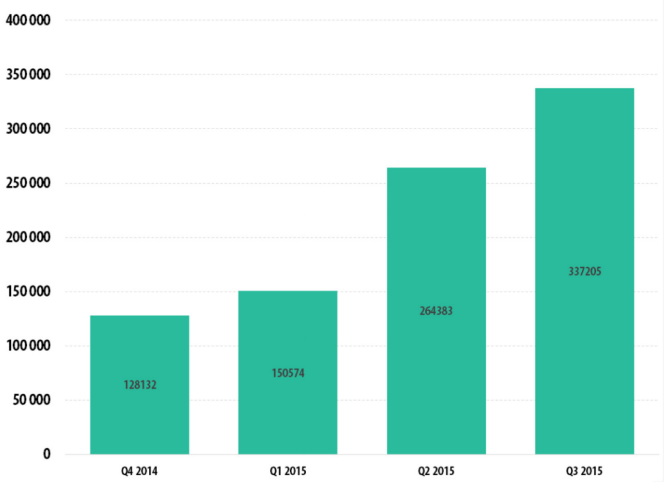
Budete úspěšně napadeni

Pokud vaše společnost nebyla zatím úspěšně napadena, v nadcházejících letech zcela jistě bude. Případně platí v posledních letech velmi skloňovaná verze předchozí věty – pokud ještě nebyla vaše společnost napadena, jen o tom ještě nevíte. Velké úniky dat a informace nejen ze Snowdenova odhalení přispěly k tomu, že se idea neprostupné vrstvené hradby okolo IT prostředků ukazuje být utopickou. Výrobci se již několik posledních let snaží tomuto trendu přizpůsobit a postupně přechází s výrobky ze skupiny pro zamezení napadení (protože je nevyhnutelné) na typ pro detekci napadení (co nejdříve, co nejpřesněji). Je vhodné si uvědomit, že vy nebo vaše organizace nemusí být útočníkovým cílem, ale pouze „přestupným bodem", jak se dostat k informacím.

Ransomware

Ransomware je na silném vzestupu a díky dnes již běžnému využívání velkých úložišť i v domácím prostředí představuje velice úspěšnou formu útoku. V průběhu let vyzrál z triviálního blokování přihlášení do systému v sofistikovaný šifrovací malware a ochrana proti němu je zatím velmi obtížná. FBI dokonce před časem vydala tiskovou zprávu, ve které doporučuje obětem „prostě zaplatit". I přes to, že se objevily varianty, kdy šlo o podvod a ani po zaplacení nedošlo k odšifrování obsahu, tak ve většině případů se jednalo o „legitimní" ransomware, kdy po zaplacení oběť dostala svá data zpět.

Počet uživatelů napadený Trojan-Ransom



Světlá, nebo temná budoucnost? Top trendy pro 2016

Stručný přehled incidentů za uplynulá léta jasně ukazuje, že rozhodně není na místě předpokládat snížení aktivity hackerů. Naopak, úspěšnost úspěšnost řady útoků je dokladem toho, že kybernetický prostor je dnes nejvýdělečnějším odvětvím zločinu a mnohé skupiny dříve operující na černém trhu se zbraněmi, drogami a dalším nelegálním zbožím se dnes přesouvají do online světa. DDoS útoky dnes rutinně překračují 100 Gbps (zatím nepotvrzený rekord drží útok na BBC z ledna 2016 – 602 Gbps[21]). Požadavky na patchování rostou a společnosti stále nestíhají bezpečnostní záplaty aplikovat včas.

Je pravda, že malware se už dnes nešíří pomocí disket a místo USB klíčenek se dnes kradou celé laptopy, ale pro kvalitní zabezpečení je stále platným pravidlem mít základní bezpečnostní opatření v pořádku a používat zdravý selský rozum.

Kybernetická bezpečnost je závodem ve zbrojení, ve kterém jsou „ti dobří" z principu v nevýhodě. Staré hrozby nikam nemizí, s širší paletou útoků a jejich rostoucí kvalitou pouze stoupá „tlak" na bránící se stranu. Je dobrou zprávou, že povědomí o bezpečnosti v kybersvětě roste mezi organizacemi i běžnými uživateli, a proto se s některými typy hrozeb setkáváme méně než dříve, kde typickými představiteli této mizící skupiny jsou:

- SQL injection, session hijacking (penetrační test je prakticky nezbytný krok při publikaci webové aplikace),
- Odposlouchávání odposlouchávání bezdrátových sítí (šifrování WEP již zcela vymizelo, uživatelé využívají end-to-end šifrování),

[19] Verizon. 2015 Data Breach Investigations Report [online]. c2015 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.verizonenterprise.com/DBIR/2015/

[20] Trustwave. 2015 Trustwave Global Security Report [online]. c2015 [cit. 2016-04-05]. Dostupný na World Wide Web: https://www2.trustwave.com/GSR2015.html

[21] KHANDELWAL, Swati. 602 Gbps! This May Have Been the Largest DDoS Attack in History [online]. c2016 [cit. 2016-04-05]. Dostupný na World Wide Web: http://thehackernews.com/2016/01/biggest-ddos-attack.html

- Defaultní defaultní uživatelské účty a jejich hesla (to ovšem však neplatí o používání slabých a odhadnutelných hesel, které jsou stále jedním z nejslabších míst).

To v žádném případě neznamená, že útočníci přestali tyto uvedené možnosti hledat. Pouze je nacházejí méně často.

Ransomware v první lize

Rok 2016 bude rokem ransomware. Dokud IT průmysl nepřijde s široce přijatelným řešením, jedná se pro útočníky o snadný výdělek. Výzkum Cisco poskytl výpočet, který ukazuje, že jen na jednom z rozšířených virů typu ramsomware (Angler) útočníci vydělávají až 34 milionů USD ročně.[22] Ransomware se začne masivněji rozšiřovat na mobilní telefony, kterým uživatelé svěřují stále více cenných dat, a zaměří se také na prostředí cloudových úložišť. První verze ransomware ukázaly i své zranitelné stránky a u některých se výzkumníkům podařilo nalézt klíč k odšifrování bez nutnosti zaplacení, ale útočníci se poučili a již na toto nelze spoléhat.

Doporučení: V případě jednotlivých uživatelů zde pomůže nejstarší opatření – obezřetnost a selský rozum. V mnohých případech se totiž ransomware šíří za pomoci naivních uživatelů, otevírající podezřelé přílohy od neznámých odesílatelů, než konkrétní technickou zranitelností. V korporátním prostředí je vhodnou prevencí především důsledné zálohování a kontrola konzistence.

Mobilní malware

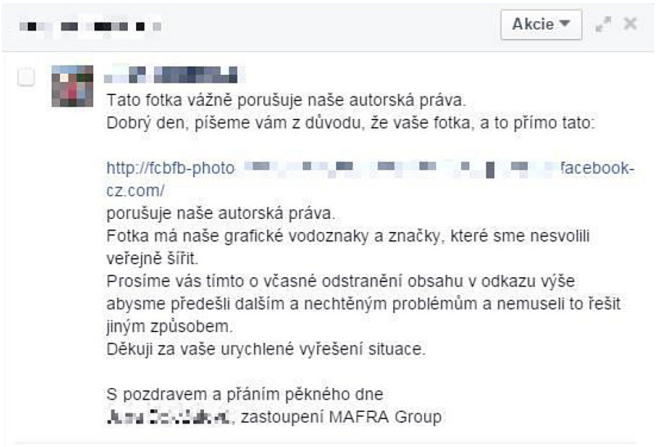
Nárůst mobilního malware je s neuvěřitelně rychlou adopcí chytrých zařízení všeho druhu raketový. Pro následující období předpokládáme rapidní nárůst škodlivých kódů, a to především o dva typy malware – ransomware a sledování uživatelovy aktivity.

Doporučení: Zavést vhodné Enterprise Mobility Management řešení pro snížení rizika úniku citlivých dat, ale pamatovat na potřeby uživatelů. Velmi důležitým krokem také je přepracovat systém sdílení souborů ve společnosti, a to z důvodů, aby uživatelé nemuseli v případě restriktivních omezení hledat nové snazší (a nebezpečné) způsoby, jak sdílet firemní dokumenty, nad kterými nebude mít společnost kontrolu (dropbox, soukromé emaily atp.)

Phishing blíže uživatelům

Phishingové kampaně budou mnohem cílenější. Před lety byly v ČR běžné amatérsky a strojově přeložené e-maily plné pravopisných chyb a nekvalitní napodobeniny webových stránek. Jejich úspěšnost nebyla valná. Poslední dva roky ukázaly, že i malá Česká republika je pro útočníky zajímavým cílem a vyplatí se jim věnovat dostatečnou pozornost lokalizaci. Lze tedy čekat mnohem kvalitnější padělky e-mailů a celých služeb s cílem oklamat i zkušené oko profesionála. Posledním trendem jsou phishing útoky na sociálních sítích. Obchodní význam přítomnosti na těchto sítích pro společnosti roste, bývají i oficiálním komunikačním prostředkem např. pro podporu klientů. Hodnota facebook účtu takové firmy má pro útočníka vysokou cenu. Ve výzkumu Cloudmark 84 % dotazovaných společnosti společností uvedlo, že v posledních 12 měsících zaregistrovaly úspěšný spear phishing.

[22] ČÍŽEK, Jakub. Cisco zmapovalo virus Angler. Záškodníci na něm vydělají až 34 milionů dolarů ročně – Živě.cz [online]. c2016 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.zive.cz/bleskovky/cisco-zmapovalo-virus-angler-zaskodnici-na-nem-vydelaji-az-34-milionu-dolaru-rocne/sc-4-a-181359/default.aspx



Příklad facebook phishingu

Doporučení: Aby bylo toto riziko akceptováno top managementem, je třeba ukázat jeho dopad v podobě provozního rizika. Snažit se vyčíslit škody, které takové kampaně způsobují. Dobrým způsobem je vedení prezentovat příklady malware, který se do instituce dostal kvůli takové kampani. V druhém kroku doporučujeme jednoduchý monitoring v podobě sledování hlaviček protokolu http, které snadno ukáží většinu případů phishingové kampaně.

Multi platformní malware

Uživatelé alternativních operačních systémů již nejsou v pozadí útočníků a drtivá většina moderního malware vzniká paralelně přinejmenším na 2 nebo všechny 3 hlavní platformy (Windows, Linux, MacOS). V roce 2016 se procenta ještě více vyrovnají a především ransomware bude vznikat na platformy Windows a MacOS simultánně.

Doporučení: Bohužel neexistuje jedno doporučení, které tento trend zvrátí, ale máme-li jmenovat, poté v první řadě bezpečnostní školení uživatelů světa Apple výroků, kteří v mnohem větší míře reprezentují skupinu ne-IT vzdělaných uživatelů, spoléhajících na automatiku platformy nastavenou výrobcem.

Přemýšlení jako cílová skupina

Velikým trendem, který se začal objevovat až na konci roku 2015, a je tedy velice čerstvý, je změna přemýšlení útočníků. Starší útoky (libovolnou metodou) měly společný základ v tom, jak útočníci přemýšleli – nalézt velmi kredibilní oběť, vědět, co má smysl od takové zcizit, a to ukrást. Příkladem je dostat se k bankovnímu účtu obsahující miliony korun, a čím více na účtu uloženo, tím lépe. Takové myšlení se mění, protože ukrást takovéto abnormálně veliké množství peněz bude jednak snáze detekováno a bude také výrazně těžší takovou částku dostat do normálního oběhu. Útočníci přešli na přemýšlení uživatelů tím, že přestali být chamtiví a cílí na běžné uživatele. Příkladem je malware, který se vydává za oficiální program policie, usvědčující uživatele z porušování vlastnických práv a požadující zaplacená „pokuty". Taková pokuta se pohybuje v řádu jednotek EUR nebo USD, a je tedy uživateli akceptována a zaplacena. Navíc povahou odrazuje uživatele při takovém incidentu notifikovat policii, že došlo k útoku, neboť předpokládá, že uživatel někdy v historii skutečně vlastnická práva porušil (stažení filmu, seriálu, hry, programu apod.) a nepůjde se dobrovolně udat.

Doporučení: Platí stejné doporučení jako v případě ransomware a obecného malware.

Trendy v interním auditu v České republice – výsledky průzkumu

Mgr. et Ing. Marek Čáp, FCCA, CIA
Director
Risk Consulting,
KPMG Česká republika

Ing. Michal Čup, FCCA, CIA
Associate Manager
Risk Consulting,
KPMG Česká republika

Žijeme v neustále se zrychlující době. Vývoj prostředí (např. regulace, měnící se potřeby a chování zákazníků, konkurence, nové distribuční kanály, IT a nová rizika) klade výrazně vyšší nároky na současné obchodní modely a systémy řízení společností. Tyto změny se odrážejí i v požadavcích na funkci interního auditu. Velký důraz je kladen mj. na oblast spolehlivého řízení rizik a roli interního auditu při identifikaci, předvídání a hodnocení rizik, dále pak na oblast firemní kultury, compliance a etiky obchodu a na přidanou hodnotu interního auditu. Interní audit se dnes neobejde bez detailního IT know-how a využití datové analytiky, které umožňují vyšší efektivitu, detailnější pochopení problémů a efektivnější řízení rizik, včetně těch spojených s informačními technologiemi.

> „Interní audit v České republice se vyvíjí směrem, kterým jdou celosvětové trendy“

Cílem průzkumu KPMG Česká republika bylo zjistit, jak si v tomto měnícím se prostředí stojí útvary interního auditu předních českých společností. Oslovili jsme vedoucí těchto útvarů a zaměřili jsme se zejména na současnou roli interního auditu, na to, jak dnes funguje a jaké je jeho budoucí směřování. Průzkumu se zúčastnilo 39 respondentů z různých odvětví.

Z průzkumu vyplývá, že interní audit v ČR prochází podobným vývojem jako ve světě. Vedoucí útvarů interního auditu považují za stále více klíčová rizika v oblasti IT / IT bezpečnosti a nově přicházející regulace a chtějí se na tyto oblasti v nejbližší době v rámci své činnosti primárně zaměřit. Zároveň přiznávají, že jim v těchto oblastech chybí dostatečná expertiza, kterou není jednoduché na trhu získat.

V obecné rovině průzkum potvrdil rozdílnou zralost funkce interního auditu v jednotlivých oborech a společnostech. Vyspělost konkrétního interního auditu odpovídá míře regulace společnosti, příslušnosti společnosti k lokální nebo mezinárodní skupině, přístupu k řízení rizik a strategii a cílům společnosti. V České republice dosahují zejména regulované společnosti z mezinárodních skupin největší zralosti funkcí interního auditu – ty se blíží úrovni „best practice“. Průzkum zároveň potvrdil, že i pro Česko jsou relevantní trendy ovlivňující vývoj funkce interního auditu popsané v úvodu.

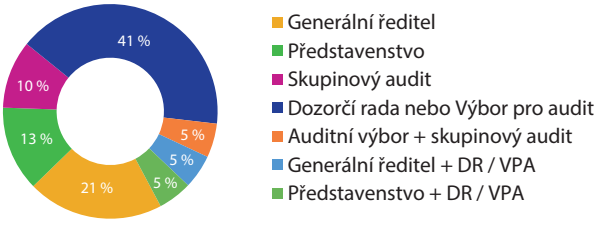
Aby funkce interního auditu v tomto vývoji obstála, musí být postavena na konkrétních základech, jasné a srozumitelně komunikované strategii a musí efektivně přispívat k řízení rizik společnosti. Aby toho dosáhla, musí rozvíjet své základní zdroje, tj. lidi a práci s daty a informacemi.

JAK FUNKCE INTERNÍHO AUDITU V ČESKU OBSTÁLA V KONFRONTACI S CELOSVĚTOVÝMI TRENDY?

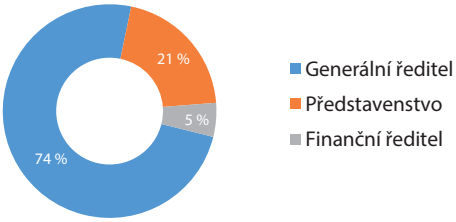
Základy fungování interního auditu

Interní audit v České republice stojí na principech nezávislosti a vychází ze základů postavených na mezinárodních standardech interního auditu. V řadě případů (34 %) je však interní audit stále funkčně podřízen generálnímu řediteli nebo představenstvu. Tento stav nesplňuje požadavky na nezávislost interního auditu a zároveň oslabuje jeho roli v rámci třetí linie obrany. Rozumíme, že důvodem tohoto uspořádání je často pouze formální role dozorčí rady nebo výboru pro audit a s tím související nízká frekvence jejich jednání a interakce těchto orgánů s vedoucím interního auditu. I přesto doporučujeme vedoucímu interního auditu těchto společností otevřít téma s vedením a akcionářem společnosti, podřídit funkčně svou činnost akcionáři, propagovat strukturu tří linií obrany, a posílit tak firemní kulturu a roli interního auditu a jeho přidanou hodnotu.

Komu je IA funkčně podřízen?



Komu je IA administrativně podřízen?



Strategie interního auditu

Základní definice, vymezení role a mise interního auditu jsou obsaženy ve statutu interního auditu. Vedle statutu je vhodné mít rovněž jasně definované konkrétní cíle pro roli interního auditu relevantní pro společnost a jasnou a komunikovatelnou strategii pro dosažení těchto cílů a pro rozvoj interního auditu. V řadě případů jsou však cíle a strategie stanoveny spíše neformálně a „implicitně". Domníváme se, že jasné stanovení cílů a strategie přispívá ke zvýšení kredibility interního auditu a jeho postavení v rámci řádného systému řízení společnosti.

> „Domníváme se, že v dnešní dynamické době je model izolované rizikové analýzy přežitý"

Role interního auditu při řízení rizik

Podle definice interního auditu má interní audit pomáhat společnosti dosahovat jejích cílů tím, že přináší systematický a metodický přístup k hodnocení a zlepšování systému řízení rizik, řídicích a kontrolních procesů a systému řízení společnosti. Tato úloha interního auditu je z našeho pohledu čím dál tím důležitější.

V oblasti řízení rizik náš průzkum ukázal, že v řadě společností v České republice probíhá riziková analýza izolovaně v rámci interního auditu a bez vazby na systém řízení rizik.

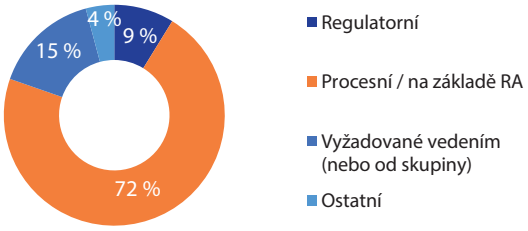
Domníváme se, že v dnešní dynamické době je model izolované rizikové analýzy přežitý. Trendem je naopak posun k systematickému a koordinovanému systému řízení rizik v rámci druhé a třetí linie obrany, zakládání výborů pro řízení rizik a zavádění dynamických modelů řízení rizik zohledňujících korelace mezi jednotlivými riziky. Dalším trendem je přesun ke kontrolování reziduálních rizik, a to pomocí tzv. klíčových rizikových indikátorů.

Klíčová rizika: IT a regulace

Není překvapivé, že v současném globalizujícím se a čím dál více digitálním světě se za klíčová rizika považují IT a regulatorní rizika. Tato rizika patřila mezi tři nejčastěji zmiňovaná v podstatě ve všech odvětvích.

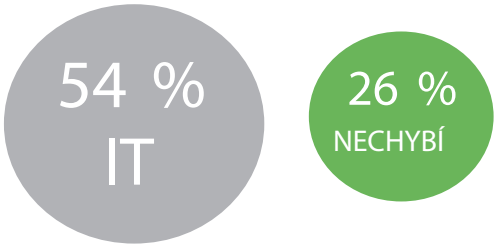
Lze s vysokou mírou jistoty očekávat, že interní auditoři budou pod čím dál větším tlakem, aby svoji činnost zaměřili právě na tato klíčová rizika. Bude proto důležité přizpůsobit strategii a s předstihem si zajistit dostatečnou kapacitu nebo směřovat průběžný rozvoj a vzdělávání k nové obecné a sektorové legislativě a současně ke sledování nových trendů a využívání nástrojů pro efektivní zajištění auditů v IT oblastech.

Jaká je přibližná struktura jednotlivých typů auditních zakázek v procentech?



Jaká rizika vnímá IA pro vaši společnost jako nejzásadnější?

Jaké znalosti či odbornost nejvíce chybí IA jako celku?



Lidé

Základem kvalitního vykonávání funkce interního auditu jsou lidé a efektivní komunikace v rámci společnosti. Obecnými základními a preferovanými požadavky na interní auditory jsou analytické schopnosti a schopnost kritického přemýšlení, komunikační schopnosti, schopnost práce s daty, chápání fungování obchodního modelu a procesů společnosti a IT znalosti. Nalézt kvalitní zaměstnance s odpovídajícími znalostmi a zkušenostmi je však stále těžší a toto téma spolu s tématem rozvoje lidí je jednou z priorit vedoucích interního auditu.

Co ukázal průzkum v oblasti lidských zdrojů?

Téměř tři čtvrtiny vedoucích interního auditu považují velikost svého týmu za dostatečnou. Zároveň přibližně 25 % z nich uvedlo, že personální kapacita útvaru je dostatečná pouze na současný rozsah jeho práce. Dokázali by si jednoduše představit větší tým, který by se mohl více, častěji a hlouběji věnovat klíčovým rizikům a procesům, a tím přidávat větší hodnotu společnosti.

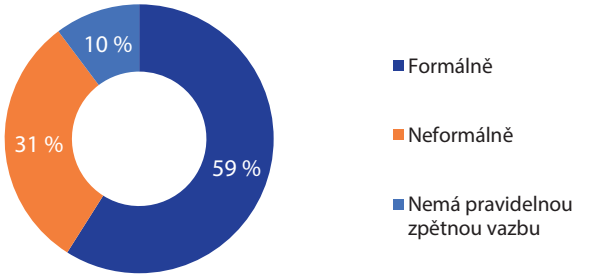
Podle průzkumu je typickým znakem útvaru interního auditu velmi zkušený tým (5 a více let) s velmi dobrou znalostí procesů a byznysu společnosti, kterému se zpravidla nedostává specifických IT znalostí.

Absenci těchto znalostí potvrzuje průzkum i v oblasti nakupovaných externích služeb. Nejčastěji jde o nákup služeb v oblasti IT, datové analytiky a sektorově specifických technických znalostí. Tyto požadované znalosti vzájemně korelují a akceleruje je rozvoj IT technologií, možnosti datových analýz, kybernetická rizika a vývoj digitalizace.

Komunikační schopnosti jsou klíčovou vlastností interního auditora. Jasná a srozumitelná komunikace je důležitá pro efektivní fungování interního auditu a propagování jeho přidané hodnoty. V tomto kontextu je překvapující, že přestože většina respondentů průzkumu uvádí, že mají zpravidla otevřený a flexibilní přístup k vedení společnosti, v 38 % případů není vedoucí interního auditu přítomen při projednávání výsledků auditů na jednání vedení. Zpráva se samozřejmě projednává vždy s auditovaným a obvykle i s členem vedení odpovědným za auditovanou oblast. Přesto považujeme za důležité, aby interní auditor měl možnost (a využíval ji) pravidelně osobně prezentovat klíčové závěry (např. jednou za čtvrtletí) z provedených auditů vedení, a mohl tak prezentovat svoji práci a přínos pro společnost.

Z průzkumu dále vyplynulo, že pouze 59 % respondentů získává pravidelnou formální zpětnou vazbu od auditovaného útvaru nebo od vedení společnosti. Ve světě bývá podíl formální zpětné vazby mnohem vyšší, a to jak prostřednictvím dotazníků po jednotlivých auditech, tak i formou sebehodnocení auditního týmu a neformálních diskuzí s auditovanými, kde jsou závěry z těchto diskuzí zaznamenávány a vyhodnocovány. Proces získávání zpětné vazby považujeme za velmi důležitý pro rozvoj funkce interního auditu.

Jakým způsobem získává IA zpětnou vazbu z jednotlivých zakázek?



Data

V efektivní práci s daty a IT podpoře spatřujeme budoucnost efektivního interního auditu. V průzkumu téměř třetina respondentů uvedla, že začali v posledních třech letech využívat při své činnosti auditní software. V současné době jej využívá téměř 60 % účastníků průzkumu, a to převážně útvarů z mezinárodních společností se skupinovým útvarem interního auditu. Je však nutné si přiznat, že ne všichni respondenti jsou z implementace auditního systému nadšeni a poukazují na „zkostnatělost" systému a ke své práci využívají pouze nutné a skupinovým auditem vyžadované minimum. V těchto případech (přibližně 20 %) je auditní software využíván např. pouze jako úložiště dokumentů nebo jako nástroj pro sledování nápravných opatření.

V oblasti datových analýz poměrně vysoké procento respondentů (44 %) uvedlo, že při své práci datovou analýzu nevyužívají a většina z nich (60 %) ani neuvažuje o jejím zavedení. Překážkou pro tento krok však zpravidla nejsou finanční důvody – z vlastní praxe víme, že data lze efektivně analyzovat pomocí běžných „kancelářských balíčků" nebo s využitím nepříliš nákladných specializovaných softwarů – hlavními důvody jsou nedostatečná odbornost interních auditorů v oblasti zpracování dat a složitý přístup k samotným datům.

Využívání nástrojů Continuous auditing / Continuous monitoring interním auditem je v ČR poměrně vzácné (méně než 20 %) a spočívá zejména v průběžném monitoringu klíčových rizikových indikátorů ve vybraných procesech a automatickém reportingu o neoprávněných přístupech do klíčových systémů. V této oblasti spatřujeme velký potenciál rozvoje.

„Typickým znakem útvaru interního auditu je velmi zkušený tým (5 a více let) s velmi dobrou znalostí procesů a byznysu společnosti, kterému se zpravidla nedostává specifických IT znalostí"

Interní audit v České republice se vyvíjí směrem, kterým jdou celosvětové trendy. Je proto zřejmé, že před námi stojí velké výzvy, jež budou měnit fungování i přístup k práci interních auditorů. Rádi vám se zvládnutím těchto výzev pomůžeme.

Kompletní výsledky průzkumu naleznete na:
https://home.kpmg.com/cz/cs/home/clanky-a-analyzy/2016/10/pruzkum-trendy-v-internim-auditu-v-ceske-republice.html

Prostor k vyjádření.

[PARIWAT INTRAWUT] © 123RF.COM

Co je nového v IPPF?

Dr. Antonín Šenfeld, CIA
manažer operačních rizik
AXA ČR/SK

Na počátku příštího roku k nám přicházejí nové *Standardy*. Pojďme se podívat na nejdůležitější změny, které nové *Standardy* přinášejí.

Rozšíření povinností vedoucího interního auditu

Do Standardu **1110 – Organizační nezávislost** je doplněna povinnost vedoucího IA informovat orgány společnosti v případě, kdy by docházelo k neoprávněným zásahům do oblasti působnosti interního auditu (např. omezení rozsahu zakázky, omezení přístupu k předmětu auditu nebo zásahy do zprávy ze zakázky). Tato eskalace může být užitečná zejména v případech, kdy se management snaží skrývat některé aspekty své činnosti před zraky akcionáře.

Dlouhou dobu nebylo ve Standardech upraveno, zda a za jakých podmínek může IA poskytovat ujišťovací služby tam, kde předtím poskytoval poradenství. Odpovědí je nově zařazený standard **1130.A3**, který říká, že to možné je, ale pouze za podmínky, kdy povaha poradenství nevede k omezení objektivity.

V oblasti zabezpečení a zvyšování kvality IA najdete v interpretacích Standardů **1300** a **1312** nově zařazenou větu požadující po vedoucím IA, aby podporoval orgány společnosti v jejich dohledu nad programem pro zabezpečení a zvyšování kvality a nad externím hodnocením. Jinými slovy tato změna hovoří o vytvoření vyšší zainteresovanosti orgánů společnosti na činnosti IA, která by interním auditu měla přinést vyšší pozornost jeho problémům (např. s odborností, nezávislostí, nedostatkem zdrojů atd.). Zároveň do Standardu **1320 – Podávání zpráv o programu pro zabezpečení a zvyšování kvality interního auditu** bylo doplněno taxativní vymezení typů informací, které vedoucí IA musí předávat orgánům společnosti o programu pro zabezpečení a zvyšování kvality IA.

Oblast předávání zpráv (Standard **2060 – Předávání zpráv vedení a orgánům společnosti**) je obohacena o povinnost vedoucího IA pravidelně předávat vedení a orgánům společnosti informaci o souladu s Etickým kodexem a *Standardy*. Související interpretace nově obsahuje výčet konkrétních položek, o kterých musí vedoucí IA informovat vedení a orgány společnosti:

- Statut IA,
- Nezávislost útvaru IA,
- Plán interního auditu a jeho plnění,
- Požadavky na zdroje,
- Výsledky auditních činností,
- Stupeň souladu s Etickým kodexem a se Standardy a související akční plány,
- Odpovědi vedení na rizika, která jsou dle úsudku IA nepřijatelná.

Úloha vedoucího interního auditu nad rámec působnosti interního auditu

Zcela nově je zařazen Standard **1112 – Role vedoucího IA zastávané mimo interní audit**, který upravuje situace, kdy vedoucí IA zastává v organizace jiné role mimo oblast IA (řízení rizik, funkce compliance). Přijetí dodatečných rolí může narušit organizační nezávislost a z tohoto důvodu musí být zavedena příslušná preventivní opatření. Mezi tato opatření patří dohledové činnosti prováděné orgány společnosti – např. pravidelné hodnocení linií informačních toků a odpovědností, a návrh alternativních procesů určených pro získání ujištění souvisejícího s oblastmi dodatečných odpovědností. Toto ustanovení může mít velký význam pro menší útvary IA, kde často dochází k souběžnému výkonu několika funkcí.

Orientace IA na budoucnost, trendy, strategii, rizika, proaktivní přístup:

Jako červená nit se textem nových *Standardů* vine téma větší orientace IA na strategii, trendy a nově vznikající problémy. Související změny najdete hned v několika standardech (1210, 2000, 2010, 2200, 2201). K významnému doplnění došlo u Standardu **2100 – Charakter práce**, který nyní explicitně vyjadřuje, jak by se interní auditoři měli chovat, aby docházelo k růstu důvěryhodnosti a hodnoty IA (proaktivnost, porozumění podstatě věci atd.). Touto změnou se text Standardů hlásí k nedávno zavedenému prvku IPPF – **Hlavním principům profesní praxe interního auditu**.

Spoléhání se na práci ostatních poskytovatelů ujišťovacích a poradenských služeb

Působnost Standardu **2050 – Koordinace a možnost spolehnutí** je rozšířena i na podmínky, za jakých se může vedoucí IA spoléhat na práci ostatních poskytovatelů ujišťovacích činností. Související interpretace podrobným způsobem poskytuje výčet těchto podmínek. Doposud byly podmínky vztahující se na externí poskytovatele součástí doporučení pro praxi (1210.A1–1). Přesun do Standardů znamená vyšší důraz na povinnost dostát těmto požadavkům.

Úprava definic vybraných pojmů

Ve slovníčku pojmů dochází ke zpřesnění výkladu pojmů *„Board – Orgány společnosti“*, *„Chief Audit Executive – Vedoucí interního auditu“*, nově byl zařazen pojem *„Core Principles for the Professional Practice of Internal Auditing – Hlavní principy profesní praxe interního auditu“*.

Kromě výše uvedených změn, byla ve Standardech provedena celá řada menších změn. Aktuální znění nových *Standardů* platných od 1. 1. 2017 je k dispozici na webových stránkách ČIIA. K dispozici je i verze s vyznačenými změnami.

V tomto čísle časopisu je pro členy ČIIA připraven jako dárek flash disk, na kterém je nahráno aktuální znění nových Standardů – a to i s vyznačenými změnami – k vašemu využití.
Soubory jsou k dispozici v českém i anglickém jazyce.

Můžete se také již těšit na spršku nových prováděcích směrnic (které nahrazují dosavadní Doporučení pro praxi), IIA se zavázalo k vydání všech zbývajících prováděcích směrnic do konce tohoto roku. Na seznámení s nimi se můžete těšit v dalších vydáních časopisu.

V prvním čtvrtletí 2017 ČIIA plánuje vydání celého nového Rámce, a to v grafické podobě, na kterou jste zvyklí z minula – na levé straně původní anglické znění, na pravé straně český překlad.

Příjemné čtení nových Standardů vám přeje,

Antonín Šenfeld

Svazek klíčů pro hodnocení kontrolních systémů

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

Tak se nám opět blíží konec roku, což je pravidelně čas, abychom my, interní auditoři, předvedli svůj majstrštyk. Připravili hodnoticí zprávu o řídicím a kontrolním systému (ŘKS). Víte jak na to? Určitě ano, ale přesto ničemu neublížíme, když se spolu nad různými přístupy zamyslíme. Možná vás mohu inspirovat tím, k čemu jsem se kdy dostal. A začnu vzpomínkou na jeden auditorský workshop v Liberci. Je to již více než dva roky, co se tam v jedné skupině sešlo patnáct auditorů z různých organizací z mnoha koutů České republiky. Účelem bylo vytvořit na základě vlastních zkušeností každého z účastníků určitý benchmark pro hodnocení ŘKS. Využili jsme moderované diskuze přecházející do formulace závěrů vyplývajících z převažující praxe, které by mohly být následovány ostatními jako dobré příklady. Vybavuji si, že mne osobně překvapila odpověď hned na první otázku, jakým způsobem u vás interní audit vyhodnocuje ŘKS. Většina respondentů se přiklonila k tomu, že prověřují řídicí a kontrolní mechanizmy v procesech a aktivitách v rámci dílčích auditních zakázek a následně pak zjištění zobecňují do závěrů pro roční hodnoticí zprávu o stavu ŘKS.

Jak je to u vás? Jdete na to podobným způsobem? Nebo raději plánujete samostatný audit ŘKS? Zatímco o tom budete chvíli přemýšlet, pokusím se dobrat odpovědi z pohledu nezávislého konzultanta, který již více než deset let pomáhá s nastavováním a hodnocením ŘKS u mnoha organizací veřejného, soukromého i finančního sektoru. V každé z těchto organizací je interní audit jinak nastavený, a to i v závislosti na regulatorních požadavcích a modelu řízení, různě odborně a kapacitně obsazený, odlišně praktikovaný a pochopitelně i se specifickou praxí hodnocení ŘKS. Nechci tvrdit na základě toho, s čím jsem se kdy seznámil, že některý z uplatňovaných přístupů k hodnocení ŘKS je špatný, zkrátka každý má své výhody i nevýhody. Pokud auditoři dokážou uplatnit své znalosti a zkušenosti, postupně svůj záběr hodnocení kombinovat a rozšiřovat, určitě budou svými ujištěními přinášet řídicím orgánům či vrcholovému vedení čím dál větší přidanou hodnotu.

Hodnocení souladu ŘKS s právními požadavky

Kdo se pouští do hodnocení ŘKS poprvé, dá mi určitě za pravdu, že kritéria pro hodnocení nejsnáze dohledá v platné legislativě. Týká se to především organizací veřejné správy nebo subjektů finančního sektoru. Obě dvě tyto skupiny mají totiž ŘKS regulatorně vymezený a vlastní hodnocení tudíž vyplyne z posouzení souladu mezi právním požadavkem a jeho aplikací do vlastního systému řízení, resp. jeho uplatňováním v systémech, procesech a operacích. Vlastní compliance grid bude obsahovat posouzení, co vše má ŘKS v organizaci zabezpečovat, kdo nese jak za systém jako takový, tak za jednotlivé jeho oblasti odpovědnost, jak má být v rámci soustavy vnitřních předpisů ŘKS popsán a jak je pak v praxi uplatňován. Odchylka požadavků od skutečného stavu je auditním zjištěním a východiskem pro doporučení ke zlepšení ŘKS v organizaci. Myslíte si, že to je moc snadné? Že není nic lehčího, než aplikovat jeden právní předpis? Zkuste to a sami uvidíte. Ještě jsem nenarazil na organizaci, která by všemu z legislativy vyhověla. Dokonce jsem jedné instituci ani pro zásadní nesoulady s právními požadavky nemohl poskytnout ujištění, že jim nastavený ŘKS účinně brání v projevu rizik…

Soukromé společnosti jsou na tom s compliance auditem hůře. Řízení rizik u nich úzce souvisí s podnikatelskou úspěšností a ve veřejném zájmu jsou regulována jen ta rizika, která se dotýkají pracovníků, zákazníků a dalších zainteresovaných osob, reprezentovaných především státními či místními správními orgány. Je pak tedy na každém subjektu, jak si vlastní ŘKS nastaví, komplexně to pro něho žádný právní předpis neřeší. V tomto případě lze využít jako kritéria pro každoroční hodnocení popsanou úpravu ŘKS z vnitřních předpisů. Možná to nebude připraveno na komplexní systémové hodnocení, ale někde se začít musí, lze nejprve prověřit soulad s dílčími požadavky a postupně doporučovat zdokonalení ŘKS směrem k dobré praxi.

> „Soukromé společnosti jsou na tom s compliance auditem hůře“

Kde hledat dobrou praxi, jak by si organizace měla svůj ŘKS nastavit? Tvrdím, že na špici pomyslného peletonu je finanční sektor. Díky evropským nařízením či směrnicím a práci navazujících autorit typu EBA, ESMA či EIOPA, jsou oblasti zahrnuté pod internal governance či internal control, velmi dobře popsané a lze je přiměřeně využít v libovolné organizaci. Má-li však někdo z jakýchkoliv důvodů problém s aplikací těchto evropských předpisů a doporučení do svých vlastních podmínek, mohu vás nasměrovat ještě dál. Přímo ke standardům upravujícím ŘKS a řízení rizik. Tím nejlepším, co je k dispozici, je v nedávné době aktualizovaný model COSO. Určitě jste pak rovněž zachytili, že tento rámec ŘKS bude během krátké doby doplněn i upraveným modelem ERM pro řízení rizik organizace svázaným právě s COSO zásadami. Bude se to hodit, koneckonců i výše zmíněné evropské předpisy k řízení rizik a vnitřní kontrole z COSO modelu vycházejí.

Hodnocení účinnosti ŘKS dle zásad modelu COSO

V čem stojí za to se důkladněji seznámit s modelem COSO? Právě v tom, že definuje ŘKS, vymezuje jeho cíle, prvky, principy a charakteristiky těchto principů. V souladu s COSO se díváme na ŘKS jako na ucelený soubor procesů a nástrojů umožňujících řádnou správu a řízení organizace (tj. veškerých v ní probíhajících činností) a dosažení dlouhodobých i krátkodobých cílů organizace. Jejich prostřednictvím pak orgány a vrcholový management řídí a kontrolují rizika, která by mohla ohrozit či oslabit cíle a bezpečnost organizace.

Od ŘKS se vyžaduje, aby zajistil dosažení tří skupin cílů. Zejména mám na mysli výkonnostní cíle, tj. soustavné dosahování očekávaných výsledků při naplňování stanovených strategií, cílů a dalších požadovaných výstupů, při současném zajištění funkčnosti a efektivnosti vykonávaných činností a trvalého fungování organizace. Nelze zde opominout ani cíle v oblasti ochrany majetku, tj. majetku vlastního i svěřeného na smluvním základě. Za druhé pak usilujeme o dosažení compliance cílů, tj. soustavný soulad výkonu činností s právními a dalšími relevantními předpisy a pravidly a s podmínkami, za kterých byla organizace založena a které upravují její činnost. Stranou nestojí za třetí ani cíle v oblasti poskytování informací, tj. funkčnost a efektivnost komunikace, získávání, evidování, přenosu, zpracování, aktualizace, využívání, sdílení, ohlašování (reportingu), uveřejňování (či jiného poskytování), zabezpečení, ochrany, uchovávání, rekonstruovatelnosti dat, resp. informací. Ano, neodpustil jsem si trochu teorie, ale lépe pak pochopíte, co se po vás bude při hodnocení chtít.

Model COSO za účelem dosažení všech třech skupin cílů stanoví 17 principů propojených s 5 prvky ŘKS, které jsou vhodné pro všechny subjekty. Každý princip má významný vliv na uplatnění a fungování příslušného prvku. Rámec pro ŘKS navíc popisuje charakteristiky principů jako jejich důležité vlastnosti. Management očekává, že prostřednictvím nich budou uplatněny a fungovat principy, a tím i jednotlivé prvky. Charakteristiky tak pomáhají vedení při navrhování, zavádění a provádění ŘKS a následně hodnocení toho, zda příslušné principy jsou uplatněny a fungují. Rámec nevyžaduje, aby se charakteristiky posuzovaly samostatně, hodnotí se v souvislosti s jejich určením pro daný princip, jsou tak důležitým faktorem pro posouzení přítomnosti a fungování principu. Při navrhování a zavádění řídicího kontrolního systému může vedení rozhodnout, že některé z těchto charakteristik nejsou vhodné či relevantní, a může identifikovat a zvážit další, které jsou založeny na konkrétních okolnostech dané organizace.

Pokud máme definováno, co vše tvoří ŘKS a co v rámci organizace zajišťuje, lze přistoupit k vlastnímu hodnocení ŘKS. Požadované prvky ŘKS, jejich principy a navazující charakteristiky principů představují soustavu metrik, o které je možno se při posuzování souladu s modelem COSO opřít a využít při formulaci závěrů, do jaké míry jsou uplatňovány v systému řízení a kontroly organizace a jak jsou v praxi účinné.

Takový interní audit ŘKS opírající se o požadavky modelu COSO může mít specifikovány například následující auditní cíle:

1. Posoudit naplňování základních požadavků na ŘKS, výkon činností řídicích a kontrolních orgánů a vrcholového vedení organizace, nastavené odpovědnosti za jednotlivé cíle ŘKS;
2. Prověřit účinnost nastaveného ŘKS v procesech a aktivitách organizace z pohledu jednotlivých prvků, principů a charakteristik (tj. kontrolní prostředí, hodnocení rizik, kontrolní aktivity, informace a komunikace, monitoring) s ohledem na identifikovaná rizika těchto procesů;
3. Posoudit systém identifikace a nápravy nedostatků ŘKS z pohledu dosahování požadované úrovně vyzrálosti ŘKS za účelem zvýšení jeho účinnosti.

Všechny tyto auditní cíle pak tým auditorů rozpracuje do programu, který prioritně vychází z porovnání stávající úrovně ŘKS vzhledem k metrikám modelu COSO a přihlíží k modelu vyzrálosti uplatňovaného kontrolního systému. Jde o to vytvořit si opět velký hodnoticí grid požadavků a zjištěného stavu, díky tomu je pak možno identifikovat odchylky od standardizované úrovně a předkládat doporučení ke zlepšení stavu v členění podle naléhavosti.

> „Kde hledat dobrou praxi, jak by si organizace měla svůj ŘKS nastavit?“

Hodnocení souladu s požadavky modelu COSO tak zpravidla probíhá v několika fázích. V první fázi auditoři připraví rozpad jednotlivých prvků ŘKS do principů a jejich charakteristik a stanoví k nim kritéria pro hodnocení. V druhé fázi auditoři připraví model vyzrálosti jednotlivých procesů, který pomáhá jednotným způsobem vyhodnotit míru souladu s požadovanými kritérii hodnocení. Ve třetí fázi jsou pak sbírány relevantní informace nastavení a výkonu ŘKS podle organizační struktury k jednotlivým kritériím hodnocení. V závěrečné čtvrté fázi pak auditoři provedou vlastní zhodnocení souladu, identifikují odchylky a zformulují případná doporučení.

Tento přístup k hodnocení je poměrně dosti pracný, vyžaduje jak odborné znalosti v oblasti ŘKS, tak i zkušenosti s procesní analýzou v organizaci a s aplikací uznávaných principů vyzrálosti sytému. Takto lze obvykle identifikovat slabiny a navrhnout podstatná zlepšení, ale ze své praxe vím, že se pro svou náročnost komplexně využívá především u velkých bankovních domů či u společností s nadnárodním vedením. Nic však nebrání začít, podle mých informací se do toho pouští i auditoři veřejné správy.

> „Tvrdím, že na špici pomyslného peletonu je finanční sektor“

Hodnocení klíčových požadavků ŘKS

Oba popsané přístupy směřují k hodnocení ŘKS samostatným auditem. Pokud si ještě vybavujete to, co jsem zmínil v mém úvodu, drobet to koliduje s většinovou praxí mezi českými auditory, že pro hodnocení využívají závěrů z jednotlivých auditních zakázek. Jak tedy přistoupíte k tomuto celkovému shrnutí účinnosti ŘKS ve své organizaci? Docela by mne to zajímalo, obávám se, že i v roční hodnoticí zprávě budou převládat spíše dílčí zjištění než ujištění o tom, jak se daří řídit rizika a dosahovat stanovených cílů…

Dovolím si i pro tento způsob hodnocení ŘKS nabídnout řešení. V poslední době jsem se setkal s jedním přístupem, který do jisté míry kombinuje oba předchozí s praktickými zjištěními o fungování procesů, činností a operací z pohledu řízení a kontroly. Může mít řadu variant, v obecné rovině lze tento rámec pro formulaci názoru na účinnost ŘKS popsat následujícím způsobem:

Popsaný přístup k hodnocení účinnosti ŘKS je postaven na třech procesech hodnocení. První přináší závěr, zda byla identifikována rizika s ohledem na cíle organizace a právní rámec. Druhý spočívá v posouzení, zda organizace na identifikovaná rizika reaguje přijetím cílů řízení a kontroly (control objectives), a jejich rozpracováním v ŘKS. Ten poslední, třetí hodnoticí proces, pak jde po tzv. klíčových požadavcích. Máme-li určeno, čeho chceme, resp. musíme dosáhnout, lze pak do procesů, činností a operací zabudovat odpovídající řídicí a kontrolní mechanizmy. Požadavky na některé z nich jsou klíčové, bez jejichž fungování nelze systémově zajistit účinné pokrytí rizik organizace.

Vlastní hodnocení ŘKS probíhá odspodu vyhodnocením procesů, činností a operací z pohledu klíčových požadavků, tj. jak v nich funguje kontrolní prostředí a jednotlivé předběžné, průběžné a následné vnitřní kontroly, potřebná dokumentace a monitoring kontrol. Pokračuje přes ujištění o plnění cílů řízení a kontroly zabraňující projevu identifikovaných rizik, až dospívá k závěru, nakolik je ŘKS účinný pro dosahování cílů v souladu s legislativním rámcem. Díky tomuto přístupu lze posuzovat účinnost těchto klíčových řídicích a kontrolních mechanizmů postupně v rámci jednotlivých auditních zakázek a celkový závěr o ŘKS vystavit až po ukončení všech dílčích hodnocení.

Pokud jsem varoval, že využití modelu COSO vyžaduje odborné znalosti o ŘKS a zkušenosti s hodnocením procesů z pohledu zvládání rizik, práce s klíčovými požadavky to moc neusnadňuje. Možná představuje určitou výhodu využití formalizace do hodnocení, což na jedné straně klade vyšší nároky na toho, kdo hodnoticí šablony vytváří, na druhé straně to umožňuje do testování kontrol zapojit i méně zkušené auditory, kteří budou vyplňovat zpracované šablony v jednotlivých procesech.

V následující tabulce se nesnažím o vyčerpávající popis všech klíčových požadavků, spíš se pokusím vybrat pár, které považuji za nejdůležitější a bez nichž bych si fungování ŘKS nedokázal představit.

Klíčové požadavky

Definování funkcí – jasné vymezení, rozdělení a oddělení funkcí, kontrola čtyř očí, organizační schéma, pracovní postupy

Ošetření vstupů – formulace potřeb, kritéria, výběrové řízení, kontrola oprávněnosti, hodnocení, audit trail

Informace a komunikace – dohled díky transparentnímu poskytování informací vhodným komunikačním způsobem

Přiměřené řídicí kontroly – zabudování různých forem předběžné, průběžné a následné řídicí kontroly do procesů

Auditní stopa – dokumentace rozhodování, výkonu a řídicí kontroly jak v procesním, tak finančním řízení

Automatizace kontrol – elektronická podpora kontrol v rámci informačních systémů pro odborné/finanční řízení a výkazy

Preventivní a nápravná opatření – identifikace chyb a nesrovnalostí, předcházení, resp. včasné zachycení a reakce

Určitě bychom mohli nalézt uvedené klíčové požadavky i v rámci principů a jejich charakteristik tak, jak nám to popisuje model COSO. Zde jsme nešli do detailního posuzování, vybíráme si jen ty klíčové požadavky na ŘKS, které by nám měly usměrnit řízení a kontrolu rizik ve všech hlavních oblastech fungování organizace.

Závěrem

Bylo by velmi krátkozraké, pokud bychom na základě jakéhokoliv zvoleného hodnocení účinnosti ŘKS poskytli výrok s ujištěním, k němuž nám daný přístup poskytl informace. Mám teď na mysli třeba ujištění o tom, že ŘKS je nastaven v souladu s příslušným právním předpisem nebo že organizace uplatnila všechny prvky a principy ŘKS podle modelu COSO, případně, že se v posuzovaném procesu uplatňují klíčové požadavky ŘKS. Vždy musíme mít na zřeteli, proč naše organizace vytváří a udržuje účelný a efektivní ŘKS. Formulujeme tudíž závěr z hodnocení, že nastavený ŘKS účinně přispívá k řízení operačních rizik v procesech a aktivitách, zejména k dosažení účelnosti, efektivnosti a hospodárnosti operací, k ochraně majetku, k dodržování právních a vnitřních předpisů a k získávání, evidování, přenosu, zpracování, aktualizaci, využívání, sdílení, předávání zpráv a k zabezpečení dat.

Výbor pro audit – co ještě stojí za povšimnutí

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

Problematice výboru pro audit bylo nedávno věnováno celé číslo našeho časopisu. Přesto, podle mého názoru, existuje ještě několik oblastí, které stojí za povšimnutí – a to jak z pohledu členů výboru pro audit, tak z pohledu tajemníků společností, externích auditorů a v neposlední řadě také interních auditorů.

Za východisko pro následující text považujme poměrně rozsáhlou novelu zákona č. 93/2009 Sb., o auditorech (dále také „ZoA"), která nabyla účinnosti dne 1. října 2016, a Nařízení Evropského parlamentu a Rady (EU) č. 537/2014 ze dne 16. dubna 2014 o specifických požadavcích na povinný audit subjektů veřejného zájmu (dále také „nařízení EU").

Jedním z prvotních kroků výboru pro audit by měla být, podle mého názoru, revize a zřejmě také aktualizace statutu / jednacího řádu výboru pro audit. Ať už jde o nastavení aktualizovaného rozsahu působnosti výboru pro audit o nové požadavky, nebo o zakotvení dalších povinností výboru pro audit. Současně navrhuji provést revizi nastaveného systému a frekvence předávání informací od auditora do výboru pro audit. Konkrétní zásady této spolupráce můžeme najít v mezinárodním auditorském standardu ISA 260.

V dalším textu se pojďme na některé vybrané požadavky aktualizované regulace podívat podrobněji.

Jedním z poměrně často diskutovaných požadavků se může stát problematika procesu určení statutárního auditora nebo auditorské společnosti (dále také „auditor"), kde by měl výbor pro audit již na samotném počátku vnímat svoji významnou úlohu – dle čl. 16 nařízení EU **„výbor pro audit je odpovědný za výběrové řízení"**. V rámci zadávací procedury k výběrovému řízení by neměli být v předkládání nabídek omezeni statutární auditoři nebo auditorské společnosti s malým podílem na trhu na auditorskou zakázku. Auditor je jmenován nejvyšším orgánem subjektu veřejného zájmu, na návrh dozorčí rady. Návrh dozorčí rady by se měl opírat o doporučení od výboru pro audit, které by mělo obsahovat nejméně dvě možnosti auditorské zakázky, s náležitým odůvodněním, kterou možnost výbor pro audit upřednostňuje.

V souvislosti s působením auditora v auditovaném subjektu a k posílení jeho nezávislosti je vymezena maximální možná doba **trvání auditorské zakázky**. Nařízení EU v čl. 17 vymezuje alternativy k prodlužování trvání auditorské zakázky. Za konkrétní návod s uvedením možných kombinací pro určení délky trvání auditorské zakázky můžeme, podle mého názoru, považovat text k § 43 v důvodové zprávě k návrhu zákona č. 299/2016 Sb., kterým se změnil zákon o auditorech.

K výše popsaným požadavkům zbývá ještě doplnit, že výbor pro audit by měl při přijímání rozhodnutí o pokračování zakázky důsledně posuzovat případné ohrožení nezávislosti auditora a také objem celkové výše odměn vyplacených auditorovi („> 15 %"). Podle čl. 6 nařízení EU musí auditor každý rok písemně potvrzovat svoji nezávislost výboru pro audit auditovaného subjektu a projednat s výborem pro audit případná rizika ohrožující nezávislost auditora a záruky přijaté k jejich omezení.

Další diskuze mohou být vedeny k **poskytování služeb auditorem mimo povinné audity (tzv. neauditorské služby)**. Nařízení EU v čl. 5 vymezuje tzv. zakázané neauditorské služby, které nesmí přímo ani nepřímo auditor poskytovat. Avšak při splnění požadavků definovaných nařízením EU může auditor poskytovat jiné neauditorské služby než zakázané. K tomu by měl výbor pro audit vydat pokyny se seznamem „povolených" služeb. A také s podmínkou, že poskytnutí takové služby předchází schválení výborem pro audit (někdy také nazývané jako „předschvalovací proces") pro subjekty v rámci skupiny. Nařízení EU v čl. 4 uvádí limitní omezení pro výši odměn za poskytnuté neauditorské služby auditorem.

> „Jedním z prvotních kroků výboru pro audit by měla být revize a zřejmě také aktualizace statutu / jednacího řádu výboru pro audit"

Dále by členové výboru pro audit neměli opomenout, že nejpozději v den předložení zprávy auditora obdrží tzv. **dodatečnou zprávu auditora určenou výboru pro audit**. Tato zpráva musí být vypracována písemně, s vysvětlením výsledků provedeného auditu. Konkrétní náležitosti této zprávy jsou vymezeny v čl. 11 nařízení EU. Za povšimnutí stojí, mimo jiné, popis povahy, frekvence a rozsahu komunikace auditora s výborem pro audit (zde vnímám vazbu na výše citovaný ISA 260). Dodatečnou zprávu by měl auditor projednat s výborem pro audit a dozorčí radou. V souladu s ustanovením odst. 2, § 44aa zákona o auditorech, výbor pro audit tuto dodatečnou zprávu postoupí na vyžádání dozorčí radě a představenstvu auditovaného subjektu a dále Radě pro veřejný dohled nad auditem (dále také „RVDA") a České národní bance, pokud činnosti auditovaného subjektu podléhají dohledu České národní banky.

V neposlední řadě, v souladu s ustanovením odst. 3, § 44aa zákona o auditorech, jednou ročně **výbor pro audit vyhotoví zprávu o činnosti**, ve které zhodnotí svoji činnost ve vztahu k vymezenému rozsahu působnosti a kterou poskytne Radě pro veřejný dohled nad auditem. Jaké obsahové náležitosti by taková zpráva měla obsahovat, není v regulaci upraveno. Proto v rámci snahy o sjednocení přístupu výborů pro audit k obsahové podobě takové zprávy vydá RVDA metodickou publikaci.

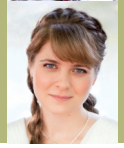
Na závěr stačí už jen neopomenout, že v souladu s ustanovením odst. 7, § 44 zákona o auditorech „subjekt veřejného zájmu zveřejní na svých internetových stránkách **seznam členů výboru pro audit**; u těchto osob uvede takové údaje, které se zapisují u členů kontrolního orgánu do obchodního rejstříku". ■

Prostor k vyjádření.

Analysis of current condition of Internal control in the Russian Federation

Ing. Josef Tyll, Ph.D.
předseda Výboru pro koordinaci vzdělávání a profesní zkoušky Rada pro veřejný dohled nad auditem

Doc. Ing. Stanislava Kontsevaya, Ph.D.
Russian Timiryazev State Agrarian University, Faculty of Economic and Finance, Moscow, Russia



1 HISTORICAL DEVELOPMENT AND CURRENT SITUATION OF INTERNAL CONTROL IN RUSSIAN FEDERATION

History of internal control

It is necessary to estimate current condition of internal control using historical base. The overview isn't complete without retrospective analysis.

Financial control arose simultaneously with starting and developing commodities exchange and finance[1]. China was the first country which used financial control system in 700 B.C. Independent control of assets was practiced in Ancient Rome in 200 B.C. In English speaking countries internal control was first mentioned in 1130. It was a document from Board of Treasury in England and Scotland archives. Financial control as a science and type of economic activity started developing since the beginning of 19th century. The main reason was developing joint-stock company. Owner of this company didn't manage the company and didn't know specificity of work. The owners needed to check working process, employees and managers. In 20th century the evolution of financial control (audit) was associated with developing of stock market. Specific feature of stock market is availability of a big group of people – investors. They are very interested in truthful information about the company and as a result they were interested in audit.[2]

In Russia, before separating to independent science control was investigated only together with accounting. It was complete scientific development in accounting in 1870 year[3]. Since this time control started to look like we know it. It is possible to see history of internal control by Investigating legal texts from different time periods. We can see history of internal control from the end of the 18th century till nowadays in Table 1.

Table 1 Stages of development of internal control

Period	Main legal texts	Internal control description
1870–1917	Directive of government controller Sokolskogo D. about advanced and actual control in Russian Impair[4]	Control was the part of the accounting system. Separation in the independent sphere was required by specificity of joint-stock company
1917–1991	Directive No104 about Revision 13.05.1983 (currently invalid)	Control was based on intradepartmental revision. Inquiry was in case of theft or embezzlement of government property.
1991–2012	Federal law No. 119 about Audit 07.08.2001 (currently invalid)	Extremely high growth of audit firms. These firms executed functions of internal and external audit. Government companies used traditional internal control, according to USSR standards To create internal control department was voluntary decision of each head of the company. Creating internal control department was mandatory only for some sectors (banks, insurance companies and so on).
2012–nowadays	Federal law No. 402 about Audit 06.12.2011	All companies must organize internal control of all facts of activity. The companies that are under obligatory external audit must do internal control for checking accounting statements

Source: authors' construction

Strict regulation of internal control has been implemented since 2012 year. Internal control can be performed by own recourses or using outsourcing. However, outsourcing of internal control is prohibited in a bank.

Internal control in the bank is a separate sphere. The first department of internal control in Russia was established in the bank. The Law No. 242-P about internal control system was published in 2003. Now there is a big base of legal texts about internal control in banks. Review of internal control in banks affects a lot of information and can be the theme of the next research.

[1] Sokolov, Ya.V (2015) History of Accounting (История бухгалтерского учета), Moscow:Magistr, ISBN 978-5-9776-0100-9

[2] Sheremet, A.D., Syuits V.P. (2014) Audit (Аудит), Moscow:Infra-M, ISBN978-5-16-009379-6

[3] Gallagan, A.M. (1927) Historical development of accounting (Счетоводство в его историческом развитии), Moscow: State publishing

[4] http://svk4u.ru/?page_id=663

Internal control definition in the Russian Federation

According to the Law ПЗ-11/2013 Internal control is a process of assuring achievement of a) efficiency and effectiveness of organization's activity, financial and operational figures and soundness of assets b) reliability and timeliness of accounting (financial) and other reports c) compliance with laws in economic and accounting activities. Internal control also helps to achieve organization's objectives. It is expected to prevent or reveal deviations from acting rules and procedures and garbling of data in accounting (financial) and other reports.

The system of internal control is aggregate of organizational structure, policies and procedures adopted by the management of the organization as a means to ensure the effective conduct of economic activity

Reference documents regulating internal control in the Russian Federation and short review of these documents is provided in Table 2. The main document is the Law ПЗ-11/2013. It is similar with the document COSO to some extent.

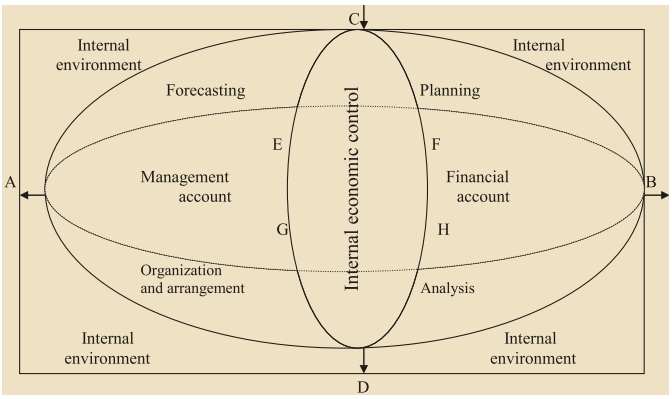
Table 2 The main documents regulating internal control in the Russian Federation

No.	Law	Short review
1.	Federal law about accounting 402 dd 06.12.2011	Article 19. Internal control in accounting 1. An economic entity must establish and execute internal control of performed economic events. 2. The economic entity that accounting (financial) reports are liable to mandatory audit must establish and execute internal control of accounting activity and accounting (financial) reports (except in cases of accounting made by the manager of the economic entity).
2.	The Law ПЗ-11/2013 "Establishment and execution of internal control of economic events, accounting activity and making accounting (financial) reports by an economic entity"	The key aspects of internal control of an economic entity are offered: а) Control environment; б) evaluation of risks; в) internal control procedures; г) information and communication; д) evaluation of internal control. Regulation of keeping records of Internal Control System and its performer.

The source: author's development

Currently, joint stock companies are required to conduct annual external audits and thereby confirm the validity of their public reporting. Upon an initiative of the organization, audits can be carried out more often. Joint stock companies with a state property must also have annual internal revision for checks of financial and economic activity. According to Russian law, the internal auditor (controler) can not combine this post with any more. The exception is a small firm, where the director also performs the duties of the chief accountant.

The elements of internal control system are subject of control, object of control, item of control, technique of control, method and technology of control, process, collection and treatment of initial information for control, informational analysis of results, subject (expert) taking decision on the basis of results and a result of control. In accordance with internal economic control there is a system, a subsystem and an element. Such division allows solving the problems of internal control at any level from the whole business to definite operation. In other words not only managers and specialists are involved in internal control system but controlling persons (control administration) as well. It takes place due to links between internal control and other functions of agricultural activity management **(Fig. 1**).



The source: author's construction

Fig. 1 Position and function of internal economic control in agricultural organization management system.
Legend of pic.1.: A – output information of management accounting, interpreted in control system and implemented in management system; B – transfer of information about financial accounting checked by internal economic control system to outside administrations accepting financial statements; C – input outer information subjected to internal economic control and used in planning and forecasting of risks, uncertainties, market condition etc.; D – information of internal economic control used in management system as an evidence and base of taking decisions; E, G – management accounting information checked in internal economic control system and used in planning, forecasting and taking of management decisions; F, H – financial accounting and economic analysis information checked in internal economic control system and used in process of activity organization, arrangement of economic operations, planning, forecasting, making of accounting (financial) statements and evaluation of survival rate of organizational property.

Organization of professional activity and professional training in audit and internal audit (internal control).

External auditor's activities in the Russian Federation have been under supervision of Self-Regulatory Organization of Auditors. It is non-profit organization based on membership relations. According to the law about Audit, Self-Regulatory Organization of Auditors must have minimum 10 000 individuals or 2 000 commercial organizations as members. It should also have own rules of quality control and professional code of ethics. Self-Regulatory Organization of Auditors guarantees property responsibility for each member to a customer by means of a compensation fund. Each auditors' organization or an individual auditor must be a member of some Self-Regulatory Organization of Auditors, otherwise, It cannot provide audit service. Self-Regulatory Organization of Auditors is authorized to issue a certificate of professional auditor. Availability of the auditor's certificate increases

salary expectations of an employee. To get the certificate is necessary to satisfy the following conditions: work experience not less than 3 years (minimum 2 years of them in auditing organization), higher education in the state universities. Period of validity of the certificate is unlimited. There is a prerequisite – advanced continual training at least 20 hours each year and at least 120 hours during the last 3 years.

Russian agriculture control procedures are regulated by the law No. 193 „Agricultural Cooperatives". Each agricultural cooperative must be a member of Revision Union of Agricultural Cooperatives. This Revision Union of Agricultural Cooperatives should inspect Agricultural Organization annually or biennially. The Revision Union also provides related services such as consulting and outsourcing.

Professional associations of internal auditors are not regulated by law and they are voluntary in the Russian Federation. One of the most famous is the Institute of Internal Auditors[5], based on rules and procedures of the International Institute of Auditors. The Institute of Internal Auditors was found in 2000. Its members are representatives of different Russian and foreign companies from different branches. The main task of the Institute of Internal Auditors in the Russian Federation is to popularize the profession of an internal auditor, development and distribution of ethical and professional standards for internal auditors. It performs a role of an expert in internal auditing, encourages professional development of internal auditors[6]. As well as foreign colleagues, the members of the institute have an exam and get certificates, though, this certificate isn't obligatory for internal audit activity. Its role is similar with advanced training.

2 PRACTICAL EXAMPLES OF INTERNAL CONTROL IN AGRICULTURE OF THE RUSSIAN FEDERATION

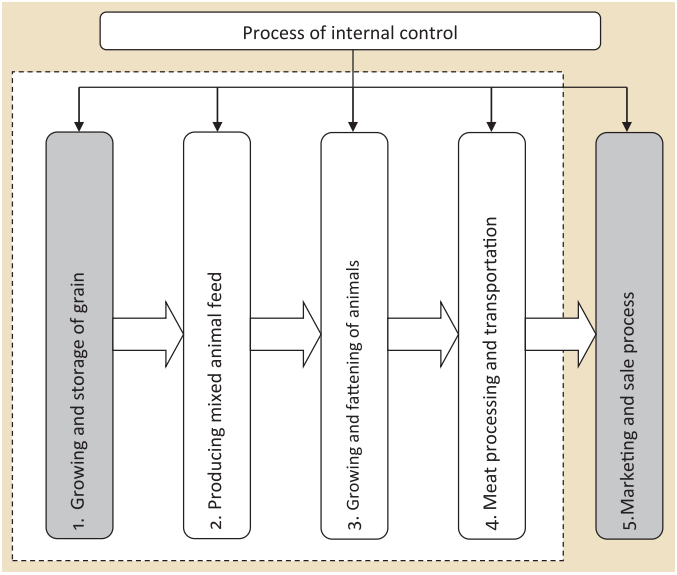
The agricultural holding M. from Russian Federation has been investigated. It has 20 thousand people in 16 regions of the Russian Federation. There are both manufacturing and marketing cycles in meat production (cattle, pig, chicken).
The processes of producing animal feed, growing and fattening animals are sufficiently automated, that causes high safety and protection against fraud. Zone of risk for internal control is growing and storage of grain. The process of control of sales through retailers and own M. shops is quite wide and worth separated investigations.

> "Zone of risk for internal control is growing and storage of grain"

[5] http://www.iia-ru.ru/

[6] Sonin, A.A. (2007) Internal audit: modern approach, Moscow: Finance and Statistics

Fig. 2 Scheme of internal control in M. holding



**A zone of high fraud risk is marked with grey color*
** Zones that take part in the investigation are marked with dotted line*

The base for a fraud is that several parts of the production process are difficult to control or control could be done with big estimated faulty proportion. This fault is the key of the fraud and an embezzlement.

1. Internal control of growing and storage of grain

Growing and storage of grain create the biggest source of the fraud as it is very difficult to find the fraud immediately. The fraud occurs in technological process. For example, results of fertilizer embezzlement in spring could be identified only in autumn, when grain was grown. By this time, a true legend explaining the reason for disappearance of fertilizers could be prepared.

The most popular frauds in growing of grain

- Stealing fuel from agricultural equipment for the purpose of sale or barter exchange.
- Using incomplete useful area of field. For example, the area of a field is 2ha. After annual inventory, in document it would be written, that this field has a problem – some growing trees or partly soil collapse. In this case useful area of this field would be 1,8ha. Expected yield grain for the control is from field 1,8ha. In reality there is 2ha of grain. The difference between the yield from 1,8ha and 2ha goes to the pocket of a violator.
- Cultivation of unrecorded (balance) fields. If productivity of normal field has been decreased, the violator takes lacking grain from these fields.

There is no theft of seed as the result of this theft i.e. empty fields are discovered immediately. There is no changes of seed sorts with low quality as low quality of seeds leads to small growing and fattening of animals. There are extremely big sanctions for decrease in growing and fattening of animals In M. holding.
Control procedures: inspection of timesheet in documents and the actual result in field. All equipment should be furnished with GPS-navigators.

The most popular frauds in storage of grain

- Storage of grain in the best achieved conditions, but on the paper it should be written that rate of grain loss is maximum.
- An estimation of the grain should be done as soon as it is delivered to a storage place. Controlled parameters are density, impurity content and moisture. Laboratory worker does test from 4–6 points from 1 car and gives a conclusion. However, in case of criminal agreement the grain density would be written 600 grams per liter instead of actual density 650 grams per liter. The difference goes to the violator.
- Another criminal agreement is to overstate impurity content. For example, according to the documents an impurity content is 14% instead of actual one 12%. After that, it is decided to decrease impurity content to needed 12% and special procedure should be applied. In fact no procedure is applied. The difference in quantity of grain goes to the violator. This fraud is extremely difficult to control. Especially, when thefts of grain are less than 3–5% of the total amount. It is very expensive to weigh the grain at each storage for control. Calculation by methods of bulk circles gives 15% error. Bulk circles method suggests, that knowing radius, cone height and density of heap grain, it is possible to calculate the quantity of the grain.
- Sell normal grain for cash but in the documents it should be written that this grain is of bad quality (impurity content). Bad quality grain cost is 30% of price of normal grain. The price difference in cash goes to the violator.

Control procedures: recalculate weight of grain and random checks. Not all storage places are equipped with weight scales at entrance and at exit. The price of weight scales is much higher than small fraud. Quick response team that is equipped with fast car and binoculars should be organized. They should selectively check cars with grain at entrance and at exit of the storage.

2. Producing mixed animal feed

M. holding produces animal feed for internal use only. There are no sales of animal feeds outside. In order to resist frauds special color and figure of granules is used in animal feed. If this animal feed with special characteristic appears at the market, the fraud will be immediately recognized and violators will be found.

Control procedures: High level of automation, perfect control of incoming grain, strong technological control of feed production. Minimum use of human labor. There must be sensor checking quality of feed 6–8 time per month and laboratory investigation of feed once per month.

3. Growing and fattening of animals

There is journal to note number of piglets per one pig and number of dying pigs.

The most popular frauds in growing animals

- Number of piglets is underestimated. It is the way to hide a distemper in future. If index of distemper is low, the workers have benefits. Counting by heads and comparing data with the documents is only possible in the end of the feeding cycle. Disposal of the animals is not checked. In paper it is written, that 3 days pig died and in fact it was 6 months pig. The organizations have losses in unaccounted feed costs.
- Number of piglets is overstated. Profit of the fraud is veterinary medicines, used for a non-existing pig. These medicaments are taken away from organization. It is very difficult to control their theft in a little glass tubes. The glass cannot be indicated in metal detector at exit.

Control procedures: Cattle and pig should be checked by weight gained once per month. Weighing is made selectively. The problems with growing grain and preparing feed are identified only at this stage.

4. Meat processing and transportation

This process is characterized by high level of automation, minimum using of manual human labor. A car loaded with corpses is sealed before transportation. There is a weight control before and after transportation.

Fraud

Losses at transportation of meat on distance of 300 km were the same as on distance of 2500 km. A inspector who made an inspection, accompanied a driver during transportation and checked all procedures of loading and unloading. The rate of losses for 300 km was ordinary and normal. Without the inspector the rate of losses was high. After long investigation the answer was found. The construction of the weight scales was illegally changed. If all meat was put on the center of the scales, the result is normal. If meat was near to the end of the scales, the weigh was less about 5 %. So in the presence of the inspector meat was weighing by putting in the center of the scales. Without the inspector employees could make some manipulations. This 5% difference is shown in documents like normal rate of losses. Extra meat was sold by unscrupulous employees.

> "If all meat was put on the center of the scales, the result is normal. If meat was near to the end of the scales, the weigh was less about 5 %"

3 DIFFERENCE BETWEEN INTERNAL CONTROL ORGANIZATION IN THE CZECH REPUBLIC AND THE RUSSIAN FEDERATION

Establishment of internal audit in the Russian Federation has been self-imposed manager's decision so far. The vast majority of the companies didn't use it considering inefficient. The Law about accounting taken in 2012 provides each company to carry out internal control and in some cases internal audit. Nevertheless, an attitude to internal control has not been changed. The vast majority of companies do not consider internal control useful and therefore do not organize internal control departments, fulfilling requirements of the law formally. In other words, a few companies carry out internal control because of own needs and the majority of companies organize internal control formally. Internal control department from the first group of companies comply with legal requirements being independent and high powered etc. Having

position of internal auditor, an employee from the second group of companies is not independent (he may be subordinated to financial department), does not have complete access to all documents and rooms and has no influence at all. There are two different definitions of internal control and internal audit in Russia. Internal audit is the process of checking internal control. Internal control is a control of both documentary and non-documentary activities of the company. But in practice there is confusion between definitions of internal control and internal audit. Also an advantage in recruitment in internal audit department was a certificate of professional external auditor but not a certificate of professional internal auditor.

"Establishment of internal audit in the Russian Federation has been self-imposed manager's decision so far"

The analysis resulted in fact that there is similar situation in Russia regarding the area of internal control and internal audit like in the Czech Republic before 25 years. The Russian banking sector is only the exception namely as regards banks, subsidiaries of the international financial groups where internal audit functions are on comparable level.In the next future this present situation requires

- to deformalize processes and procedures and establish conditions for real development of Internal audit in other sectors than the banking one. One of the most important ways has to be starting and developing cooperation of internal audit departments and exchange of information not only with Group auditors but with the external auditors.
- Further way is learning of international experience (how the internal audit is performed in the different economic environment than that one in Russia).
- The main factor for the development of internal audit are people. It is necessary to hire the right auditors with the respective certificates. Besides, heads of IAD should support the professional development of their auditors.
- Very important issue is transparent communication of IAD with the Management Board, Audit Committee, Supervisory Board and top and line management. IAD should transparently communicate with the auditees, timely announce their quarterly audit plans and audit engagements.
- IAD must permanently focus on increase of their audit quality. They should not only self-control their performance but they should receive feedback from their stakeholders and auditees. Regular control of their audit quality from side of external evaluator appears to be necessary.
- At last but not least the internal audit departments should cooperate with the so called 2nd Defence Line (risk management, compliance).

Conclusion

Internal control in Russia has long and intensive history. However, the problem of organization of high-quality internal control in the company is relevant nowadays. In the Soviet Union period the role of internal control was minimal. But nowadays internal control is experiencing rapid growth. Internal control concept is focused on the COSO concept. But there is still formal organization of obligatory internal control . Most of managers don't understand the importance of the role of control. Similar situation was 25 years ago in the Czech Republic. There are several suggestions in the paper for improving situation in Russia according to Czech experience of developing internal control system – deformalize process and procedures of internal control, to be focused on people and their training, make good vertical communication, to be bearer of changes, to create added value for the stakeholders, to be profitable consultant serving to the management.

"The vast majority of companies do not consider internal control useful"

Acknowledgement

The authors would like to enclose gratitude to Jiří Dvořáček, professor of Business Economics Department of University of Economics, Prague and Ilya Oseev internal control and audit expert with many years of experience of internal control management in agricultural food processing, retail, media business, engineering sphere for help in consulting.

References:

Gallagan, A.M. (1927) Historical development of accounting (Счетоводство в его историческом развитии), Moscow: State publishing

Kontsevaya, S.R. (2014) 'Concept and Arrangement of Internal Economic Control in Agricultural Sector in Terms of Russian Federation' Proceedings of the International Scientific Conference «Agrarian perspectives XXIII — The Community-led Rural Development», Prague: Czech University of Life Sciences, pp. 103–111, [Online], Available: http://ap.pef.czu.cz/static/proceedings/2014/, [Accessed: 03 Nov. 2015], ISBN 978-80-213-2545-6

Sokolov, Ya.V (2015) History of Accounting (История бухгалтерского учета), Moscow:Magistr, ISBN 978-5-9776-0100-9

Sonin, A.A. (2007) Internal audit: modern approach, Moscow: Finance and Statistics

Sheremet, A.D., Syuits V.P. (2014) Audit (Аудит), Moscow:Infra-M, ISBN978-5-16-009379-6

Národní konference ČIIA v Českých Budějovicích

Ing. Šárka Nováková, MBA
Všeobecná fakultní nemocnice v Praze

Letošní národní konference ČIIA se konala 12.–13. 10. 2016 v moderním hotelu Clarion v centru Českých Budějovic a byla zaměřena na audit kybernetické bezpečnosti, resp. IT.

Atmosféra byla příjemně uvolněná, neformální, tvůrčí a dobře zvolené téma nás na oba dny zcela pohltilo. Vystupující své přednášky pojali velmi různorodě a obsahem i zvolenou formou si získali naši maximální pozornost, včetně zpětné vazby ve formě doplňujících dotazů a navazujících neformálních diskuzí.

> „Co se v mládí naučíš, ve stáří rozhodně nebude stačit“

Prezident ČIIA, Tomáš Pivoňka, při zahájení konference

V přednáškách nechyběly výmluvné příklady z praxe, vtipné citace a náměty k zamyšlení, z nichž jsem si řadu i poznamenala.

Náměstek primátora Českých Budějovic Petr Holický citoval v rámci svého úvodního slova Karla Čapka: „Pane, představte si to ticho, kdyby lidé říkali jen to, co vědí“ a v průběhu konference nechyběly ani citáty ze sci-fi seriálu Star Trek nebo knížek Terryho Pratchetta.

Při přednášce Lukáše Mikesky (ISACA Czech Republic Chapter) mě zaujal její podtitul: „Co se v mládí naučíš, ve stáří rozhodně nebude stačit“ a řada překvapivých letopočtů, např. že internet máme od roku 1996 a Facebook až od roku 2004. Zazněla také chvála našeho profesního časopisu Interní auditor, kterou Tomáš Pivoňka (prezident ČIIA) glosoval: „…asi dobrý oddíl“ ☺ (citát z filmu „Jáchyme, hoď ho do stroje“).

Přednášku Jiřího Slabého (Deloitte) zahájilo vtipné video a následovala neúprosná statistika, popis trendů, reálné příklady a nechybělo ani zamyšlení nad dalším vývojem kybernetické bezpečnosti.

Radim Šilhánek (MONETA Money Bank) nám prezentoval IT trendy v bankovnictví a motto že: „Vždy přeceňujeme změnu, která nastane v dalších 2 letech, a podceňujeme změnu, která nastane v dalších 10 letech.“ (Bill Gates)

Následně jsme se rozdělili do šesti pracovních skupin a pilně pracovali, diskutovali a formulovali své společné myšlenky a závěry až do pozdních odpoledních hodin.

Následoval příjemný podvečerní zážitkový program s možností výběru mezi komentovanou prohlídkou pivovaru Budvar a přednáškou na téma „Motivace“.

Vladimír Rohel (NBÚ) při zahájení konference

> „Dobře zvolené téma nás na oba dny zcela pohltilo“

Druhý konferenční den byl zahájen tím, že zástupci každé z šesti skupin výsledky proběhlé diskuze na dané téma prezentovali ostatním, což bylo velmi přínosné a inspirativní.

Martin Hudeček (Orbit) při své přednášce na konferenci

Následně Václav Lukavský (Ministerstvo obrany) při svém vystoupení konstatoval, jak těžké je se preventivně bránit proti něčemu neznámému. Pokračoval výčtem povinností, plynoucích z platné legislativy, a popisem, co konkrétního z toho vyplývá a jaké jsou ve státní správě pro zajišťování kybernetické bezpečnosti podmínky. Posteskl si také, jak obtížné je získat na tuto oblast kompetentní specialisty, a zmínil problematiku pořizování HW, aplikačního a bezpečnostního SW.

Prezentace Martina Hudečka (ORBIT) s podtitulem: „Pochopit budoucnost IT? Naivní představa! Tak co s tím?“ byla velice kreativní, s cílem AHA efektu. Jsem si jistá, že na Tomáše Pivoňku, navlečeného v desítkách vrstev oblečení při demonstrativní scénce, nikdo z účastníků konference jen tak nezapomene.

Konferenci završila panelová diskuze, které se zúčastnili Libor Kovář (EmbedIT), Vladimír Rohel (NBÚ) a Radomír Valica (MF) a závěrečné slovo neměl nikdo jiný než prezident ČIIA Tomáš Pivoňka.

Na závěr si dovolím několik osobních vzkazů:

- Tomáši, Dane, Jitko, Zuzko, Žaneto, Dano…, konferenci jste připravili skvěle a patří vám za to dík,
- Evo, Katko, Pepo…, je škoda, že jste tu tentokrát nemohli být s námi,
- Bohouši, Honzo, Ivo, Vladimíre, Stando, Tomáši, Jirko, Mílo, Laďko, Kájo, Gábino…, je fajn, že jsme se tu spolu sešli, vážím si toho, že mezi vás patřím, a už cestou domů jsem se začala těšit na příští národní konferenci i na všechna naše další setkání při akcích ČIIA.

NBÚ Národní bezpečnostní úřad

Konference je realizována pod záštitou ředitele Národního bezpečnostního úřadu pana Ing. Dušana Navrátila.

ČIIA DĚKUJE VŠEM PARTNERŮM NÁRODNÍ KONFERENCE ZA DOBROU SPOLUPRÁCI PŘI JEJÍ REALIZACI.

GENERÁLNÍ PARTNER

Deloitte.

HLAVNÍ PARTNEŘI

KPMG

pwc

PARTNEŘI

Budweiser Budvar

jconsult

SPOLUPRACUJÍCÍ ORGANIZACE

České Budějovice

ČCA ČESKÁ COMPLIANCE ASOCIACE

ISACA Serving IT Governance Professionals Czech Republic Chapter

Jihočeský kraj

Ministerstvo financí České republiky

Veřejná správa

Panelová diskuse „Implementace požadavků zákona o kybernetické bezpečnosti“. *Zleva* Libor Kovář (EmbedIT), Vladimír Rohel (NBÚ), Radomír Valica (Ministerstvo financí), Tomáš Pivoňka (ČEZ)

Národní konference ČIIA, České Budějovice 2016

Jiří Slabý (zástupce Deloitte Czech Republic - generálního partnera na konferenci ČIIA)

Zástupci z ČR na konferenci ECIIA ve Stockholmu

Snažíme se udržovat a prohlubovat kontakty. S představiteli IIA Lawrence J. Harringtonem a Richardem F. Chambersem byly v letošním roce otištěny v našem časopise rozhovory.

Pavla Víznerová, Jan Kovalčík

Lawrence J. Harrington, Pavla Víznerová, Jan Kovalčík, Richard F. Chambers

Setkáváme se...

Amatéři postavili archu, profesionálové Titanik

PhDr. Václav Peřich
člen Čestného presidia ČIIA od roku 1996

Dnes již okřídlená slova amerického autora sci-fi Davida Drakea sehrála zajímavou úlohu v kampani vedené ve Spojeném království před referendem o vystoupení UK z Evropské unie. V její vrcholící fázi odpůrci Brexitu uveřejnili stanoviska několika ekonomických expertů o pravděpodobných negativních důsledcích vystoupení Británie z EU. Vzápětí však přišla z tábora odpůrců jistkřivá odezva s nesmírně úspěšným ohlasem: „Myslím, že lidé v této zemi už mají expertů dost," prohlásil Michael Gove z iniciativy ***Vote Leave*** (hlasujte pro odchod) a řada vůdců této kampaně si hned parafrázovala Drakeova slova pronesená ve zcela jiné souvislosti na úderný slogan: „Nevěřte expertům, ti postavili Titanik!"

Výmluvný a zdaleka ne jediný příklad krize důvery, jakou můžeme pozorovat po celém světě v nejrůznějších podobách a jaká ve významné míře poškozuje celé společenské prostředí. Za největší část oné všeobecné nedůvěry nepochybně nesou odpovědnost záměrně šířené nepravdy. Ty mají za cíl poškodit konkurenty na všech úrovních mocenských, veřejných i hospodářských soutěží. Podceňovat však nelze ani to, jak k té krizi přispívají – z poněkud jiných pohnutek – všichni ti, kdo do veřejného prostoru šíří matoucí zprávy zakrývající vlastní, ne zcela odpovědné jednání. Sem můžeme počítat jak všechny typy nadbytečných zpravodajských her na straně oficiálních autorit, které si zneužíváním mocenského monopolu vytvářejí neskutečně rozsáhlé soubory sledovacích údajů, tak nejrůznější „vynálezy" v oboru, který jsme si navykli za poslední dekády eufemisticky označovat jako ***kreativní účetnictví***. Obávám se však, že na podkopávání důvěry lidí vůči celkové uspořádanosti poměrů ve společnosti nesou svůj díl odpovědnosti také profesionální zlozvyky v oborech, kterým bychom jinak přičítáním nízkých pohnutek hrubě křivdili.

> „Složitost prostředí prostě postupně narůstá a chtě nechtě na to musíme brát zřetel"

Namátkou tři jednoduché příklady: Nájemní smlouva z roku 1995 má rozsah jedné stránky a po dvaceti letech už se stěží vtěstná na stránky čtyři. Zákon z roku 2001 má 42 paragrafů, má být nahrazen zákonem o 132 paragrafech. Protichůdné znalecké posudky v soudních řízeních. Pravda, nelze z tohoto košatění složitosti vinit jen ty, kdo příliš komplikované a obtížně srozumitelné dokumenty napsali. Složitost prostředí prostě postupně narůstá a chtě nechtě na to musíme brát zřetel. Avšak měli bychom si přitom také uvědomovat, že nelze onomu tlaku vynalézavé nepoctivosti a nárůstu složitosti čelit stereotypními pokusy předcházet všem zkreslením ve výkladu našich textů pouze stupňováním nesrozumitelnosti.

V prvním čísle letošního ročníku tohoto časopisu vyšel článek ***Proč musí umět auditor psát*** Dany Emingerové ve spolupráci s Klárou Dvořákovou. Velmi zajímavě napsaný a příklady výstižně doložený text dobře zapadá to tematického zaměření čísla na METODY A POSTUPY INTERNÍHO AUDITU, avšak jeho význam podle mého mínění tento rámec do značné míry přesahuje. Naznačuje to již podtitul článku: ***Aby mu všichni jeho klienti rozuměli***. Nejde totiž zdaleka jenom o jakousi metodickou dovednost, nýbrž o završení několikafázové soustavné a odpovědné práce, u níž ***porozumění klientů*** má být cílem od samotného počátku. Mnohokrát jsem se totiž za svého působení v oboru setkával s prací „odborníků", jejichž cílem bylo spíše než ***porozumění klientů*** prosté ***vyprodukování nálezů***. A bylo to znát nejen ze závěrečné zprávy samotné, ale už z vymezení oblasti zkoumání a více nebo méně specifikované volby pracovních postupů a metod.

Velký zdroj odborných zkušeností a přítel ČIIA z dob počátků institutu Giovani Grossi zpestřoval svoje přednášky různými půpovídkami a anekdotami. Mezi jinými to byla otázka, jaké jsou v oboru největší dvě lži. Odpověď zněla, že to je uvítání auditora klientem slovy: „Rádi vás tu vidíme!" a auditorova odpověď: „Jsem tu přece, abych vám pomohl." Samozřejmě jsem anekdotě rozuměl jako střízlivému pohledu na reálnou situaci ve vztahu, který má své citlivé stránky. Nemohl jsem se ale zcela upřímně smát, protože anekdota jaksi pomíjela prapůvodní základ, na jakém onen vztah klienta a auditora měl být postaven. Klientem přece má být v zásadě poctivý manažer, který podle svého svědomí a schopností naplňuje obsah svěřené působnosti. Naproti tomu auditor má být nezávislý ověřovatel, ten, kdo o dění pod zkoumanou působností může dát ***přiměřené ujištění***. Pokud na základě své vlastní odbornosti nachází něco, co je takovému ujištění na překážku, musí to učinit předmětem dalšího jednání bez předpojatosti a vlastně v zájmu klienta, jestliže tento zájem není veden úplně jinými pohnutkami.

Jinak řečeno – východiskem onoho základního vztahu má být vlastně oboustranná důvěra podobná té, jaká je obvyklá při bezpečnostních kontrolách na letištích. Pasažér přece má ***rád vidět*** bezpečnostního kontrolora, pasažér sám potřebuje mít, třebaže nepřímo, přiměřené ujištění, že nastupuje do letadla s minimalizovaným rizikem ohrožení plynoucího z přítomnosti ozbrojeného útočníka nebo nebezpečného nákladu. A bezpečnostní kontrolor? Ten je tam také přece proto, ***aby pomohl*** co možná eliminovat riziko, nikoli kvůli uvedení pasažéra do nesnází, byť je pro nás třeba zouvání bot nebo vyvlékání opasků z kalhot také nepříjemné. Toto přirovnání může působit trochu nadsazeně, protože nesrovnalosti v cestovních účtech nebo inventurách nemají brizanci výbušnin nebo střelných zbraní. Neměli bychom však tu

nadsázku vidět jen v té situaci aktuální kontroly. Všechna ta různorodá rizika našich každodenních prostředí a prací se vyskytují a odehrávají v daleko širším rámci. Rizika sama nemáme pokládat za ospravedlnění předem podezřívavého vztahu ke kontrolovaným osobám. Naopak bychom měli objasněním této nadsázky umět navázat lepší vztah mezi auditory a manažery všech úrovní při analýzách a hodnocení rizik, a to dávno předtím, než se vůbec můžeme k prověřování jakékoli agendy vypravit. Toto je ta pravá situace, v níž se mohou auditor a klient s naprostou důvěrou přivítat a vzájemně si pomáhat. Správně nastavené vazby řídicích kontrol, monitorování indikátorů u auditních stop důležitých operací a náležité ohodnocení rizik – to vše má být výsledkem vzájemné součinnosti všech potenciálních kontrolovaných osob a interních auditorů, přičemž bez vzájemné důvěry obou stran by taková součinnost nemohla přinést výsledky odpovídající kvality.

Navíc tu máme ještě tu fázi vzájemných vztahů mezi auditory a jejich klienty, ve které se jedná o vypořádání výsledných nálezů a připomínek z auditů. Nezřídka jsme svědky značně neprůhledných tahanic o to, zda námitky proti obsahu auditních zpráv jsou jenom výmluvami, nebo naopak oprávněnou obranou před podezřívavým vykonstruováním závažně prezentovaného nálezu. Obdobně se řada vysoce postavených manažerů o auditních zprávách vyjadřuje přezíravě a odkrytá slabá místech ve svých agendách s vahou vlastní autority vysvětlují jako chybné porozumění auditorů povaze oněch agend. A tahanice se vlečou tak dlouho, až je postupně zatlačí do pozadí jiné naléhavější problémy. Co nicméně zůstává, je nedořešený konflikt. A ten má bohužel nemalý dopad nejen na jakoukoli další spolupráci mezi auditory a manažery v dané oblasti, avšak také na celé sociální okolí. Není vůbec nadsazené, když si přiznáme, že takové jevy v nemalé míře přispívají k celkové intoxikaci nedůvěrou v širší společnosti.

Titulek tohoto článku rozhodně nemá být chápán jako nadhodnocení amatérské práce nad výkony profesionálů. Daniel Drake to ostatně také tak nemyslel. Velmi pravděpodobně naznačoval, že amatérský stavitel archy myslel s přiměřenou předvídavostí na možné ohrožení, zatímco někdejší profesionálové se při stavbě Titaniku dopustili v setrvačně zaslepené honbě za extrémními výkony ve svém oboru zanedbání důležitých rizik hned v několika ohledech. Ale to není ospravedlnitelný důvod pro paušální nedůvěru k expertům. Naopak je to výzva k prohlubování profesionality právě v tom poslání, jaké má ona naplňovat. Podle mého přesvědčení je správná profesionalita auditorů a manažerů založena nikoli na bravurních odborných hantýrkách, nýbrž na tom, že jsou schopni na jedné straně efektivně organizovat a řídit svěřené agendy a na straně druhé k tomu poskytovat potřebnou součinnost a vydávat o tom přiměřené ujištění. A tím pozitivně přispívat k celkovému obnovování důvěry, jakou každá společnost ke svému vývoji potřebuje. ■

Novinky odboru Centrální harmonizační jednotka za rok 2016

Ing. Milena Widomská, Ph.D., MBA
vrchní ministerský rada
Harmonizace interního auditu
Ministerstvo financí ČR

Vážené kolegyně, vážení kolegové,
jelikož se blíží konec roku, chtěli bychom se pochlubit, a hlavně vás všechny seznámit s výsledky své práce. Tento reporting naší činnosti by měl být vnímán jako přínosný a nezkreslený zdroj informací pro vás všechny, kteří „chtějí být přímo v obraze od tvůrce legislativy" a opravdu chtějí vědět, co je u nás nového a co aktuálně připravujeme na další rok.

Co se metodické činnosti týče, ke dni 18. 3. 2016 vydala Centrální harmonizační jednotka (dále jen CHJ) Ministerstva financí Metodický pokyn CHJ č. 1, který ruší vybrané metodické pokyny a další metodické materiály (*http://www.mfcr.cz/cs/legislativa/metodiky/2016/metodicky-pokyn-kterym-se-rusi-vybrane-m-24375*). Tento metodický pokyn se stal startovací čárou pro další pokyny, které budou každý rok následovat a o kterých vás budeme průběžně informovat.

Metodický pokyn CHJ č. 2 s názvem **Metodika řízení rizik** konkrétně a prakticky vysvětluje, co to vlastně jsou rizika a jak by mělo jejich řízení probíhat, aby měl takový systém v praxi vůbec šanci fungovat a chod organizace pozitivně ovlivňovat. Je určena nejenom pro interní auditory (dále jen IA), ale pro všechny osoby, které by měly rizika řídit nebo se na jejich řízení aktivně podílet.

Metodika veřejného nakupování (Metodický pokyn CHJ č. 3) s podtitulem Naplňování principů 3 E v praxi veřejného nakupování byla vydána 7. 7. 2016 s účinností od 1. 10. 2016. Usnesení vlády ze dne 7. července 2016 č. 620 doporučuje členům vlády, vedoucím ostatních správních úřadů, hejtmanům a primátorce hlavního města Prahy postupovat v souladu s tímto pokynem. Užitečný může být rovněž i pro zadavatele sektorových veřejných zakázek a další subjekty, kteří jsou z různých důvodů různými právními tituly vázány při nákupu zboží či služeb dodržovat zásady účelnosti, hospodárnosti a efektivity.

Dále si CHJ uvědomuje, že jsou v současné době kladeny vysoké nároky na IA, spojené s průběžným vzděláním, odbornou kvalifikací, profesionální komunikací, zahrnující rovněž diplomacii a etické jednání, proto jsme nejdříve připravili a chystáme se zveřejnit ještě v letošním roce na internetových stránkách Ministerstva financí (*www.mfcr.cz/cs/verejny-sektor/kontrola-verejnych-financi/*) **Manuál IA, Statut IA a Etický kodex** – v současné době jsou tyto dokumenty ve stadiu vnitřního připomínkového řízení a budou vpuštěny do závěrečného konzultačního procesu, kdy se k navržené metodice bude vyjadřovat auditorská veřejnost.

Manuál IA poskytuje návod, jak postupovat při výkonu interního auditu (dále jen IA) v souladu s ustanovením § 7, odst. 1 zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů. Nedílnou součástí manuálu jsou rovněž přílohy (vzorové dokumenty), které se týkají vlastního výkonu auditorské práce. Obsahem manuálu jsou všechny klíčové auditní činnosti, a tudíž je zde dostatečný základ pro oblast hodnocení kvality. **Proces hodnocení kvality auditní činnosti zajišťované v útvarech IA veřejné správy** bude upraven v samostatném metodickém pokynu, na kterém se v současnosti pilně pracuje. Plánované vydání je rok 2017.

Statut IA definuje postavení, účel, pravomoci, odpovědnosti, povinnosti, hlavní cíle, charakter ujišťovacích a konzultačních činností a rovněž vztahy mezi útvarem IA a auditovanými subjekty ve veřejné správě. Součástí Statutu IA je rovněž **Etický kodex IA**. Dodržování etiky je nedílnou součástí činnosti IA. K tomu, aby mohla být nastolena důvěra mezi vedoucím orgánu veřejné správy a IA, je nutné, aby tento dodržoval etický kodex.

V současnosti dokončujeme metodiku týkající se **Metod a technik výběru vzorku operací**, jejichž obsahem jsou pojmy, zásady a základní metody a techniky výběrů vzorku operací, praktické příklady a vzorová dokumentace, o kterých si myslíme, že by mohly být využity při výkonu interního auditu a budou dobrou základní praktickou pomůckou pro běžné interní auditory. Plánované vydání tohoto metodického pokynu je rok 2017.

Co se **legislativní činnosti** týče, „Návrh zákona o řízení a kontrole veřejných financí a návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o řízení a kontrole veřejných financí" byl dne 21. 9. 2016 znovu předložen na jednání Legislativní rady vlády.

V rámci legislativních i metodických činností uskutečnilo i připravuje CHJ setkání s připomínkovými místy nejenom k návrhu zákona o řízení a kontrole veřejných financí, ale probíhaly (květen – Smilovice) a budou probíhat metodické dny pro interní auditory rezortů a krajů.

Případné náměty na tvorbu metodik, které by mohly pomoci všem interním auditorům při jejich výkonu, zasílejte na milena.widomska@mfcr.cz.

V novém roce se mějte krásně, a hlavně přeji všem čtenářům hodně zdraví.

Česká Compliance Asociace – nové profesní sdružení odstartovalo

JUDr. Vladimír Valenta
compliance expert
ČEZ, a.s.

JUDr. Roland Jaroš
člen výkonné rady
Česká Compliance Asociace z.s.

Mgr. Zlata Kunešová, LL.M.
manažerka
Česká spořitelna, a.s.

Jak to začalo? Skupinka nadšenců z podnikatelské i veřejné sféry v březnu 2010 založila občanské sdružení Český Compliance Institut, svojí členskou základnou za dobu trvání nepřekračující 10 osob. Díky jednodenní compliance konferenci na podzim 2015 v Praze se slibnou účastí došlo k určitému rozhýbání sdružení.

Restart započal v prosinci 2015, kdy se na několika ideových schůzkách účastníci Roland Jaroš, Zlata Kunešová, Veronika Sedlářová, Juraj Szabó a Vladimír Valenta shodli na společném cíli – oživit toto sdružení a učinit z něho profesní platformu, která bude respektovanou profesní autoritou role compliance v systémech řízení a kontroly organizací a institucí, a zastáncem a podporovatelem compliance profese. Svoji roli také sehrála inspirace historií a zkušenostmi Českého institutu interních auditorů (ČIIA).

Na členské schůzi 10. 3. 2016 proběhla proměna občanského sdružení na zapsaný spolek se změněným názvem Česká Compliance Asociace (ČCA). Schválením nových stanov, jasným zaměřením poslání tohoto profesního sdružení v podobě vize a mise a schválením dalšího klíčového dokumentu – Etického kodex compliance profesionála, sepsaného s využitím tuzemských i zahraničních zkušeností, byly vytvořeny základy pro dynamický rozvoj. V rámci veřejné části členské schůze ČCA se 16 nových zájemců o činnost ČCA seznámilo s výsledky proměny sdružení i zvolenými členy orgánů. Ve výkonné radě ČCA zahájili své funkční období její členové Roland Jaroš, Zlata Kunešová, Veronika Sedlářová a Juraj Szabó, reprezentující podnikatelskou sféru. V kontrolní komisi do funkčního období vstoupili Dušan Uher a Vladimír Kopecký, zastupující sféru veřejných institucí.

Čtyři členové výkonné rady doplnění o řadového člena Vladimíra Valentu v současnosti představují organizační a provozní tým všech následujících aktivit ČCA. Pan Jiří Nápravník pak má zásluhu na tom, že krátce od restartu se společnost o existenci ČCA, jejích cílech a aktivitách začala postupně dozvídat prostřednictvím stránek www.czech-ca.cz.

Restartovací tým začali následně rozšiřovat zástupci dalších společností jako MONETA Money Bank, KPMG, Komerční banka, E.ON ČR, Kinstellar, Český Aeroholding a další, ať už ve formě korporátního členství nebo jako individuální členové. A začali také přispívat k následně pořádaným akcím. Poděkování též patří společnostem ČEZ a Bureau van Dijk, které restart ČCA od počátku značně podporovaly.

> „Restart započal v prosinci 2015“

Všichni, kdo již projevili nebo projevují zájem o působení v ČCA, jsou motivováni a inspirováni posláním tohoto sdružení. Ve své **Vizi** si stanoví *„…prosazování a podporu uplatňování etických principů a compliance v řízení firem a institucí v České republice v souladu s mezinárodními standardy.“*

A smysl svého působení ČCA vidí ve své **Misi** jako: *„…sdružení skupiny lidí, firem a institucí, které je přesvědčené, že nedílnou součástí*

Prezident ČIIA, Tomáš Pivoňka, na konferenci ČCA v Praze v říjnu 2016

efektivního řízení podnikatelských subjektů a veřejných institucí ve prospěch lidského společenství je uplatňování etických principů a dodržování právních norem." A z toho důvodu zaměřených na „…vedení vlastníků podnikatelských subjektů, vedoucích představitelů veřejných institucí, manažerů, compliance profesionálů, dalších odborníků a příznivců oboru k pochopení přínosů compliance funkce a profese pro řízení firem a institucí v České republice a k posilování jejich odbornosti a reputace." A to prostřednictvím *„…vytváření podmínek a využívání dostupných zdrojů ke zpřístupnění, šíření a sdílení mezinárodních zkušeností a postupů v oblasti compliance; se záměrem být garantem vzdělávání compliance profesionálů a dalších zájemců o tento obor, a posilovat povědomí veřejnosti o tomto oboru a profesi. A rovněž využíváním nabytých znalostí a zkušeností v rámci legislativního procesu."*

Za své nosné aktivity ČCA považuje:

- Odborné konference, semináře a workshopy zaměřené na compliance.
- Organizaci systematického profesního vzdělávání.
- Zprostředkování zkoušek k získání mezinárodně uznávaných certifikátů dosažené úrovně odbornosti v compliance profesi.
- Organizaci pracovních a odborných skupin compliance profesionálů a zprostředkování vzájemné komunikace i získávání podnětů k tvorbě legislativy.
- Platformu pro komunikaci se zástupci tuzemských i evropských regulátorů a s významnými domácími i zahraničními odborníky z oboru compliance.
- Spolupráci se zahraničními a mezinárodními profesními sdruženími.
- Zpřístupnění odborných publikací z oblasti compliance, osvědčených nástrojů a postupů pro výkon profesní praxe.

Nově pořádané workshopy jakožto neformální diskuze na předem stanovené téma byly prvním z účinných nástrojů pro setkávání compliance profesionálů mezi sebou. Do poloviny roku 2016 proběhla tři takováto setkání zaměřená na Řízení compliance rizik, Prevenci praní špinavých peněz a financování terorizmu, a Změny právní úpravy trestní odpovědnosti právnických osob, s rostoucím počtem účastníků.

Nejdůležitější aktivitou roku po restartu a současně výzvou, kterou si ČCA sama dala, bylo pořádání první compliance konference s mezinárodní účastí. Tato konference se konala ve dnech 24.–25. 10. 2016 v Praze pod záštitou ministra spravedlnosti pana Roberta Pelikána. Jejím hlavním mottem bylo následující: „Nechcete přijít o firmu? Compliance programy chrání před závažnými dopady porušení práva, včetně možného zrušení."

Úspěchu této konference jistě přispěla účast a vystoupení osobností veřejné i podnikatelské sféry, guvernéra ČNB pana Jiřího Rusnoka, ministra spravedlnosti pana Roberta Pelikána, předsedy Úřadu pro ochranu hospodářské soutěže pana Petra Rafaje, viceprezidenta Svazu průmyslu a dopravy a současně předsedy představenstva a generálního ředitele ČEZ pana Daniela Beneše, člena prezidia České bankovní asociace a současně předsedy představenstva a CEO MONETA Money Bank pana Tomáše Spurného. A rovněž CEO International Compliance Association pana Phila Ryana a Chief Compliance Officera skupiny Siemens pana Klause Moosmayera. Ale také obsazení pěti tematických panelů dalšími osobnostmi, uznávanými odborníky z akademických kruhů, veřejné správy a podnikatelského prostředí z tuzemska i zahraničí. Podrobnosti jsou dostupné na konference2016.czech-ca.cz.

Tato mezinárodní compliance konference byla také vhodnou příležitostí k podpisu Dohody o spolupráci mezi International Compliance Association a Českou Compliance Asociací.

Přestože oficiální komunikace termínu a programu konference začala až koncem srpna, v prostorách hotelu Hilton Prague ji v obou dnech navštívilo téměř 150 osob. Řadu přípravných a organizačních aktivit zajišťovali sami členové výkonné rady ČCA a členové organizačního týmu ČCA s omezenou podporou konferenční agentury. Podle zpětného hodnocení účastníků se to však neprojevilo na velmi pozitivním hodnocení konference. Znovu se potvrdila zkušenost, že nadšení a nasazení pro užitečnou věc dokáže vyrovnat hendikepy časového i finančního omezení.

Ve svém emailovém hodnocení matador corporate governance a compliance českého podnikatelského prostředí Vladimír Brož výstižně uvedl: „…blahopřeji Vám ke skvělé konferenci, která se povedla po všech stránkách a ve svém celku byla lepší než profesionálně připravované akce. Máte můj obdiv, protože ze své vlastní zkušenosti vím, kolik práce a úsilí je potřeba pro pořádání takovéhoto setkání. Je evidentní, že v případě ČCA se dala dohromady správná skupina lidí se zájmem o věc a schopností přidat ruku k dílu, protože „zapálený" jedinec zmůže bez podpory a hlavně reálné pomoci ostatních pouze velmi málo."

Měříme-li úspěch restartu růstem členské základny, pak je i v tomto směru ČCA velmi úspěšná. Za rok 2016 se její členská základna značně rozrostla, a to nejenom v rámci individuálního členství, ale především v počtu korporátních institucí, které se staly nově členy ČCA. Úspěšný průběh konference také vyvolal zájem některých veřejných institucí o spolupráci s ČCA na národních i mezinárodních projektech a činnostech, které jsou tradičně prioritními tématy compliance programů ve firmách i institucích.

> „Proběhla proměna občanského sdružení na zapsaný spolek se změněným názvem Česká Compliance Asociace (ČCA)"

Na tomto místě je nutné zmínit významnou a užitečnou pomoc řady kolegů z ČIIA, kteří cennými radami, zkušenostmi, kontakty, ale i komunikačně a osobně pomohli dovést tuto konferenci k úspěšnému průběhu.

A spolupráce ČCA a ČIIA tím ani zdaleka nekončí, naopak. V běhu již jsou dva odborné compliance semináře, připravované společně na konec listopadu 2016, resp. začátek ledna 2017. Dále zástupci ČCA a ČIIA zahájili diskuzi o dalších formách a příležitostech zejména v oblasti vzdělávání a komunikace. Takže, díky kolegové z ČIIA, a těšíme se na další spolupráci. ■

Čeho si Andrea povšimla aneb co se děje na mezinárodní scéně

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

- Na webových stránkách IIA je v členské sekci ke stažení nová příručka o tom, jak nejefektivněji psát auditní zprávy. Příručka se na psaní auditních zpráv snaží podívat z nového a moderního úhlu pohledu, kdy se klade důraz spíše než na retrospektivní pohled na pohled do budoucnosti. Auditní zprávy by podle ní měly být jasné a stručné a měly by prioritizovat auditní zjištění a doporučení z pohledu jejich celkového dopadu na fungování organizace. Příručka je ke stažení na následujícím odkazu: https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/audit-reports-practice-guide.aspx

- V listopadu 2016 byla vydána příručka k řízení rizik podvodu vydaná COSO (The Committee of the Sponsoring Organisations of the Treadway Commission). Jde o aktualizaci již dříve vydané brožury, která je obohacená o nové případové studie, a aktualizovány jsou také některé termíny ve vazbě na změny ve Standardech. Tuto příručku je možné zakoupit na stránkách IIA a bude jistě zajímavým doplněním knihovničky každého interního auditora zajímajícího se o problematiku podvodů – https://bookstore.theiia.org/fraud-risk-management-guide-2

- 24. října 2016 vyšel v novinách The Wall Street Journal článek Richarda Chamberse, prezidenta IIA o rostoucí roli a významu vedoucích interního auditu ve společnostech a organizacích. Jejich role začala být posilována už s tím, když v USA vstoupil v platnost zákon Sarbanes – Oxley (SOX), který kladl zásadní důraz na funkčnost vnitřního kontrolního systému a ověřování jeho správného nastavení a fungování. V dnešní době přibývají postupně další rizika, která je nutné sledovat, a interní audit má v této oblasti nezastupitelnou úlohu. Článek Richarda Chamberse si můžete přečíst zde: http://www.wsj.com/articles/internal-audit-chiefs-gain-in-clout-compensation-1477339076.

- Stali jste se novým členem výboru pro audit? Nebo máte ve svém výboru pro audit nové členy? Doporučte jim přečtení článku v časopise Interní auditor, který bude určitě zajímavý pro ty, kteří nově přijali roli člena výboru pro audit. https://iaonline.theiia.org/blogs/chambers/2016/Pages/An-Open-Letter-to-Newly-Appointed-Audit-Committee-Members.aspx

Otázky interního auditora

Vážení čtenáři,
stále máte možnost soutěžit s Interním auditorem a odpovídat na otázky z profese interního auditu. Správné odpovědi na otázky z příslušného čísla jsou zveřejněny vždy v dalším čísle časopisu Interní auditor. Odpovědi je možné vyplnit na webu – www.interniaudit.cz, a to do **15. února 2017**. Výherce bude následně vylosován na nejbližším jednání Redakční rady. Vylosovaný výherce z čísla 4/2016 obdrží jednodenní seminář v ČIIA zdarma dle vlastního výběru.

1. Jaký je ekonomický důvod pro vládní intervence v oblasti obchodu?
a) udržení sféry vlivu
b) ochrana mladých odvětví
c) ochrana národní identity
d) obchodovat se spřízněnými zeměmi

2. Vlády mohou v dlouhodobém horizontu omezovat obchodování nejpravděpodobněji kvůli
a) podpoře nových průmyslových odvětví
b) ochraně upadajících průmyslových odvětví
c) zvýšení daňových příjmů
d) podpoře národní bezpečnosti

3. V jaké fázi vývoje bude společnost pravděpodobně hledat financování formou rizikového kapitálu?
a) vznik společnosti
b) rychlý růst společnosti
c) fáze dospělosti
d) fáze poklesu

Správné odpovědi z čísla 3/2016...

1. Co z následujícího tvrzení nejlépe popisuje účel interního auditu?
a) přidávat hodnotu společnosti
b) pomáhat managementu s implementací systému řízení rizik
c) zkoumat a hodnotit účetní systém
d) monitorovat interní kontroly pro externí auditory
(správná odpověď je A)

2. Nejpřesvědčivější informace ohledně hodnoty aktiv získáme
a) dotazem na management
b) pozorováním procesů
c) fyzickým zkoumáním
d) externě vypracovanou dokumentací
(správná odpověď je D)

3. Jaká je přímá odpovědnost jednotlivých uživatelů EUC?
a) nákup HW a SW
b) vedení seznamu používaných EUC
c) strategické plánování v oblasti EUC
d) fyzické zabezpečení vybavení
(správná odpověď je D)

Výherce z minulého čísla:
Ing. Petr Vilimovský,
Český Aeroholding, a.s.
GRATULUJEME

Prostor pro vaše odpovědi.

The European Space Agency (ESA) is seeking an

Internal Auditor (m/f)

in the Internal Audit and Evaluation Service, Director General's Services
to be based at the ESA Headquarters in Paris, France or ESTEC, Noordwijk, Netherlands

The European Space Agency (ESA) is an intergovernmental organisation whose mission is to shape the development of Europe's space capability and ensure that investment in space continues to deliver benefits to the citizens of Europe. ESA employs about 2200 staff members across Europe and has a budget of 5.2 billion euros.

Within the Internal Audit and Evaluation Service, the postholder will conduct audits of the Agency's activities and carry out management consultancy assignments to ensure the effectiveness of ESA's organisation and the adequacy of controls and risk management to achieve the Agency's strategic objective

Applicants for this post should have a Master's degree in auditing, engineering, business administration, or other relevant discipline, with a minimum of three years' experience of internal auditing in an international environment. Candidates should be Certified Internal Auditors or the equivalent. Certified competence in auditing Management Information Systems will be considered a strong asset.

Excellent analytical, organisational and coordination skills and the ability to provide quality summary output against tight deadlines are prerequisites for this post as well as good communication and interpersonal skills.

The working languages of the Agency are English and French. A good knowledge of one of these is required together with a working knowledge of the other.

For a complete job description visit the **http://www.esa.int/About_Us/Careers_at_ESA/Vacancies** or visit the **«Careers at ESA»** webpage. If you wish to apply, please complete the online application form which can be found by clicking on the link within the vacancy notice, reference ESA/VN-HO(2016)019

Closing date: 4 th January 2017

ESA is an equal opportunities employer that offers challenging career opportunities and excellent employment conditions.

Please note that applications are only considered from nationals of one of the following States: Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, the United Kingdom and Canada.

Aktor

inzerce

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

Noví certifikovaní *(nejen)* interní auditoři

V současné době evidujeme celkem **324** certifikací:

292	CIA
11	CGAP
2	CCSA
5	CFSA
14	CRMA

V měsících období

září–listopad 2016

nám řady certifikovaných rozšířila (CIA):

Ing. Linda Babincová, CIA

GRATULUJEME!

Upozornění: Kompletní certifikační program je nutné dokončit do čtyř let od podání registrace.

Certifikace interních auditorů ve veřejné správě

Přehled o počtu žádostí a vydaných certifikátů

Počet žádostí od 1.1.2016	65
Počet vydaných certifikátů	65
Celkový počet žádostí od r. 2011	495
Celkem vydaných certifikátů od r. 2011	473

Upozornění pro certifikované

	VIAS	VIAK
Hlášení CPE do konce roku 2016 pro vydané certifikáty v roce	2013	2012, 2014

Noví členové

- Bc. Martina Benešová, Město Vodňany
- Ing. Marek Hakala, MBA, CIA, CISA, AAA Auto International a.s.
- Ing. Václav Hrstka, Státní pozemkový úřad
- Ing. Irena Krolopová, Krajský úřad Karlovarského kraje
- Ing. Lenka Lucová, Deloitte Audit s.r.o.
- Ing. Petra Mečířová, Státní fond životního prostředí ČR
- Ing. Emanuel Mercl, OKAY s.r.o.
- Mgr. Petr Novák, Pražská plynárenská, a.s.
- Ing. Darja Stará, Individuální členka
- Ing. Drahomíra Stefanovičová, Krajský úřad Karlovarského kraje
- JUDr. Lenka Tesařová, Ph.D., Státní pozemkový úřad
- Ing. Helena Ulrichová, MBA, Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
- Vratislav Vrška, Deloitte Audit s.r.o.

Počet certifikovaných auditorů ve VS dle oblastí do 31.10.2016

Oblasti	Počet VIAA	Počet VIAJ	Počet VIAS	Počet VIAK	Počet IA dle oblastí
Ministerstva, Úřad vlády	35	21	50	27	**133**
Krajské úřady	3	3	3	9	**18**
Úřady měst a obcí	10	15	27	12	**64**
Policie a Hasiči	6	9	11	4	**30**
Vysoké školy	1	0	7	3	**11**
Zdravotnictví, lázně	4	2	7	2	**15**
Ostatní	32	23	29	18	**102**
Celkem IA ve VS	**91**	**73**	**134**	**75**	**373**

Deloitte.

Interní audit

Spolehlivá business inteligence pro vedení firem

Audit

English Annotation

Angela Witzany

Audit never sleeps

Angela Witzany describes in her article, why she selected during her presidency the topic: "Audit never sleeps" and describes how the auditors should keep their relevancy.

Lukáš Kintr

Safety Measures according to the Cybersecurity Act – Part One – Organisational Set-Up

Next part of the series of articles about the cybersecurity from the sponsor point of view focused on the safety measures according to the cybersecurity.

Martin Fleischmann

The Cloud from the Regulator Point of View

The author deals in his Article with the Cloud Computing. He explains and attitude of the regulator to this technology. The text contains the Czech National Bank and other European supresory authorities experience with this area. The author points out the key and problematic areas, which need to be followed.

Jiří Slabý

The Changes in the Approach of the Attackers in the Past Five Years and Future Outlook (Part Two)

The article contains overview of the interesting world and national security incidents.

Marek Čáp, Michal Čup

The Internal Audit Trends in the Czech Republic – Survey Results

Information from the survey of the KPMG about the internal audit in major Czech companies.

Antonín Šenfeld

What are the Novelties in the IPPF?

The articles summarizens major changes of the International Standards. The new Standards reflect new changes and actual problems and the strategy is seen as important. Also the attention is paid to the explanation of the major terms.

Rodan Svoboda

The Keys to the Control Systems' Assessment

The Author desribes in his articles major approaches to the internal control systems'assesment. He explains in more detail the assessment of the effectivity of the internal control system according to COSO and assement of major requirements.

Petr Kheil

The Audit Committee – What Else Needs Also your Attention

The Author adds comments to the topic of the Audit Committes, which was the topic of the issue 2/2016. The article is based on the requirements of the new Act on Auditors and the EU directive.

Josef Tyll, Stanislava R. Kontsevaya

Analysis of current condition of Internal control in the Russian Federation

The author explains historical development and current situation of internal controls in the Russian Federation, provides practical examples of internal controls in agriculture and summarizes differences between internal controls in the Czech Republic and the Russian Federation.

Šárka Nováková

National ČIIA Conference in České Budějovice

Ing. Šárka Nováková, MBA, head of the Internal control and internal audit department in the Faculty Hospital in Prague, shares with our readers her experience and view of the national ČIIA konference focused on cybersecurity.

Václav Peřich

Amateurs Built the Ark, the Professionals the Titanic

The author discusses in his article the relationship between the internal auditor and the client, and the need of the trust in their relationship.

Milena Widomská

Current News from the Department Central Harmonisation Unit in the Year 2016

Information about the current news from the Ministry of Finance in relation to the internal audit and financial control.

Roland Jaroš, Zlata Kunešová, Vladimír Valenta

Czech Compliance Association – the New Professional Organisation Just Started

The Author in his article shows the activities, which shoud accelerate the Czech Compliance Association activities. He introduces the mission and vission, major activities and concrete events in 2016. Important event was the international compliance konference.

Flash disk pro členy ČIIA

FLASH DISK URČENÝ PRO ČLENY ČIIA OBSAHUJE:

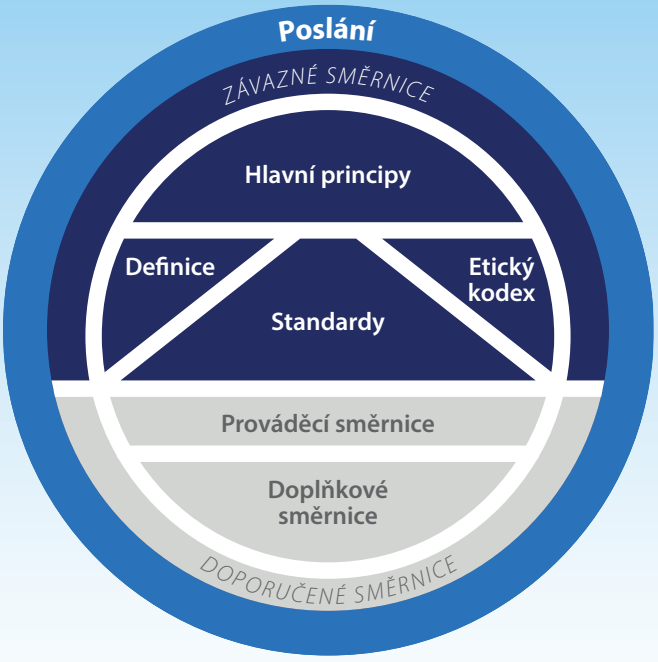
Mezinárodní standardy pro profesní praxi interního auditu platné od 1. 1. 2017
(i s vyznačenými změnami)

■

Vydané časopisy Interní auditor v elektronické podobě v letech 2015 a 2016

■

PF 2017



www.chytremesto.cz

„Se mnou v kapse máte celou radnici pod palcem.“

INOVACE 2: Inteligentní aplikace pro Vaše město

CHYTRÉ MĚSTO

ČESKÁ SPOŘITELNA
Jsme Vám blíž.

Inteligentní nadstavba nad městský portál umožňující jednoduše z pohodlí domova řešit běžné agendy s městem včetně všech plateb od pokut přes správní poplatky až po komunální odpad či vybrané komerční služby. Jedná se o další z řady chytrých řešení, která zlepšují kvalitu života ve městech. Víme, že ve „smart“ projektech je nejen potenciál pro rozvoj českých měst, ale také příležitost pro inovativní české firmy. Proto je tu specializovaný program Chytré město od České spořitelny. Ať už jste zadavatel, nebo dodavatel, dokážeme Vám zajistit finanční prostředky z národních a evropských zdrojů i odborné poradenství při přípravě a realizaci. Vstupte s námi do světa chytrých měst a kontaktujte naše specializované poradce na www.chytremesto.cz.