iA
interní auditor
ČTVRTLETNÍK ČESKÉHO INSTITUTU INTERNÍCH AUDITORŮ
ROČNÍK 23, ČÍSLO 1–2019 (91) 1|2019

WORKSHOP PRO INTERNÍ AUDITORY Z VEŘEJNÉ SPRÁVY

10.–11. 4. 2019

Hradec Králové, hotel Černigov

DAATOVÁNÍ

aneb práce s daty nuda je,
má však cenné údaje

Workshop je realizován za podpory náměstka ministra financí České republiky **PhDr. Tomáš Vyhnánka** a generálního ředitele sekce auditu a kontroly Ministerstva financií Slovenskej republiky **Ing. Vladimíra Urmaniče**.

10. dubna 2019

8:30–9:30	Registrace
9:30–9:45	Zahájení
9:45–10:30	**Tomáš VYHNÁNEK**, Ministerstvo financí ČR *„Supervizor a Cityvizor: zkušenosti s aplikacemi nad otevřenými daty“*
	David SLÁMA, Ministerstvo vnitra *„Využívání dat ve veřejné správě pro analytickou činnost MV“*
10:30–10:50	Přestávka
10:50–12:50	Panelová diskuse na téma: **KYBERPROSTOR** **Petr GREŠL**, Rogit **Dominik MAREK**, Kraj Vysočina **Vladimír ROHEL**, NAKIT **Aleš ŠPIDLA**, Generální finanční ředitelství **Milan ZOLICH**, Ministerstvo spravedlnosti
12:50–14:00	Oběd
14:00–16:30	**PRACOVNÍ SKUPINY**
16:30	Ukončení odborného programu
19:00	Večerní program „Číše vína“, Hotel Černigov

SKUPINA A
TÉMA: *„Interní audit založený na datové analytice“*
LEKTOR: **David KORNIET**, Deloitte
Gabriela TVRDÍKOVÁ, Deloitte

SKUPINA B
TÉMA: *„Praktické využití MS Excel a dalších nástrojů firmy Microsoft (PowerPivot, Power BI) v datových analýzách“*
LEKTOR: **Alex VINŠŮ**

SKUPINA C
TÉMA: *„Finančná kontrola a dodržiavanie princípu kontroly štyroch očí“*
LEKTOR: **Kristína DURAJ CHOCHLÍKOVÁ**, Ministerstvo financií SR
Viera RUMANKOVÁ, Ministerstvo financií SR

SKUPINA D
TÉMA: *„GDPR rok poté, jak jsme na tom ve veřejné správě a co dál“*
LEKTOR: **Rodan SVOBODA**, Eurodan
Eva KLÍMOVÁ, Městská část Praha 2

11. dubna 2019

9:00–9:30	Registrace
9:30–10:15	**Martina SMETANOVÁ**, Rada pro veřejný dohled nad auditem *„RVDA – představení činnosti, častá zjištění“*
10:15–10:50	**Miloslav KVAPIL**, DYNATECH *„Prevence trestní odpovědnosti právnických osob ve veřejné správě“*
10:50–11:10	Přestávka
11:10–11:50	**Štěpánka CVEJNOVÁ**, Ministerstvo vnitra *„Interní audit pro řízení kvality“*
11:50–12:50	*„Potřebuje interní auditor ve veřejné správě znát metody a nástroje řízení?“* **Tomáš DOMECKÝ**, Hlavní město Praha **Ivana GÖTTINGEROVÁ**, Statutární město Brno **Eva JANOUŠKOVÁ**, Kraj Vysočina **Blanka ŠTEFANKOVÁ**, Moravskoslezský kraj
12:50–13:00	Ukončení workshopu
13:00	Oběd

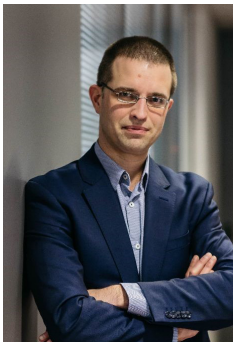
ORGANIZÁTOR

HLAVNÍ PARTNER

PARTNER

MEDIÁLNÍ PARTNER

sli.do



Milí členové,
dostáváte do rukou číslo Interního auditora věnované roli interního auditu ve třech liniích obrany. Téma již delší dobu diskutované a stále aktuální. A pro mne velmi důležité, protože je pro mne tématem osobním a také příslovečným lakmusovým papírkem naší profese. Osobním proto, že od tohoto roku řídím vyjma interního auditu i jiné kontrolní funkce. Lakmusový papírek proto, že na tomto tématu se podle mého názoru ukáže, jak naše profese dokáže reagovat na vývoj byznysového prostředí a na očekávání našich stakeholderů.

Do doby tzv. finanční krize z let 2008/2009 si auditoři žili poměrně v klidu, měli svoji práci, občas ne zcela dobře pochopenou nebo uchopenou, a když jim bylo nejhůř, stačilo vytáhnout zkratky jako VKS, SOX a bylo zas dobře. Jenže krize změnila mnohé. Firmy přestaly tolik vydělávat, jejich vedení se dostalo pod silný tlak a zcela pochopitelně (i když někdy zbytečně) firmy začaly silně osekávat náklady. Tehdy se ukázalo, že interní audit může být velmi rychle zařazen do škatulky „zbytná funkce" (vyjma regulované odvětví finanční a veřejné instituce). Interní audit začal bojovat o své místo na slunci s jinými kontrolními a poradenskými funkcemi (compliance, zlepšování procesů, řízení rizik apod.). Osobně znám několik příběhů, kdy interní audit tento konkurenční boj vyhrál, ale i několik příběhů, kdy prohrál. V čem spočívá klíč v úspěchu v tomto boji? Jde o už stokrát řečené klišé – přidaná hodnota. A v čem spatřují naši stakeholdeři hodnotu?

Dle mých zkušeností to je v prvé řadě ve schopnosti rychle identifikovat relevantní rizika (signifikantní rizika, která se ještě nestihla materializovat). A ještě rychleji je „proauditovat" a zajistit, že se odehraje pozitivní změna. V druhé řadě to je byznysový přínos z realizovaných auditů. Konkrétně to znamená předložit praktická doporučení, která přinesou, zejména pro exekutivní vedení, hmatatelné dopady – úsporu nákladů, vyšší výnosy, udržení tržního podílu apod. Nejdůležitější ze zmíněných aspektů je rychlost. Rychlost, kterou se dokáží rizika materializovat je obrovská (viz kauza WannaCry), fundamentální změny v byznysu se dějí snad stejně rychle (nová konkurence, nová regulace). S touto rychlostí jde ruku v ruce složitost. Žijeme v globalizovaném, extrémně složitém světě. Proto je posledním důvodem, proč exekutivní vedení spojuje kontrolní a poradenské funkce, zjednodušení. Zkrátka, generální ředitel chce mít jednu mapu rizik, jeden rizikový jazyk a jednoho člověka, s kterým se o tom baví. Toto neplatí pro interní audit ve finančním a veřejném sektoru, kde je audit normován legislativou a regulátor do specifické role.

Jsem rád, že tyto změny reflektuje i IIA, který právě ohlásil, že provede revizi modelu tří linií obrany tak, aby co možná nejlépe vyhovoval současnému podnikatelskému prostředí. Já osobně na spojení ujišťovacích funkcí do jednoho celku (pod vedení ředitele IA samozřejmě ☺) vnímám plusy i minusy. Plusy jsou hlavně na straně firmy – je to levnější, rychlejší, jednodušší. Minusy jsou hlavně na straně vedoucího IA. Pracuje v mnohem komplexnějším prostředí, musí velmi dobře hlídat nezávislost a objektivitu interního auditu, což vyžaduje kontinuální sebereflexi a intenzivní debatu s vedením a orgány společnosti. Nicméně i vedoucího interního auditu nakonec platí firma a měl by dělat to, co je nejlepší pro firmu.

Přeji vám vše dobré.

Tomáš Pivoňka,
prezident Českého institutu interních auditorů

Nejste si jisti při uveřejňování závazků do Registru smluv?

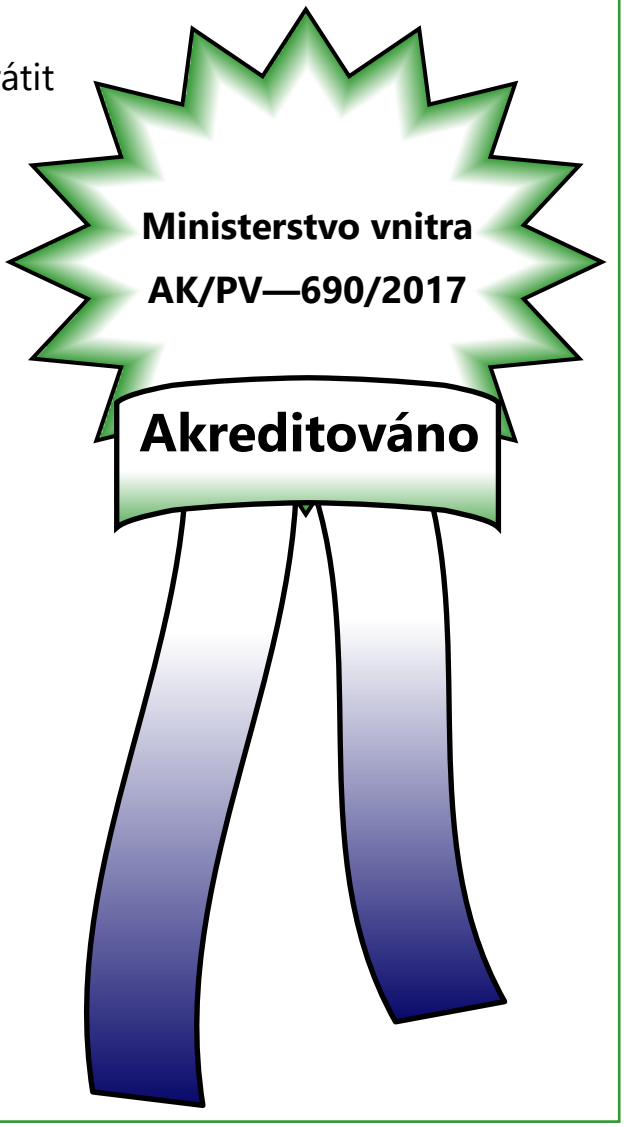
Nechce se vám platit za drahá, celodenní a neosobní školení?

Máte nového zaměstnance, který nezná problematiku Registru smluv?

Využijte našich akreditovaných e-learningových kurzů!

Proč zvolit akreditovaný e-learningový kurz:

1. dostupná cena,
2. čas strávený kurzem se započítá do průběžného vzdělávání,
3. snadné objednání přes internet,
4. bez nutnosti cestovat,
5. při řešení obtížného případu se můžete obrátit na naše certifikované interní auditory ve veřejné správě.



E-learningové kurzy naleznete na:

www.dynatech.cz/vzdelavani

DYNA® TECH

OBSAH / CONTENTS

ROČNÍK 23, ČÍSLO 1–2019 (91)

1|2019

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

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

Vydavatel nenese odpovědnost za údaje a názory autorů jednotlivých článků.
Redakční rada:
Vedoucí – Jan Kovalčík, Petr Hadrava, Daniel Häusler, Ludmila Jiráňová, Andrea Lukasíková, Šárka Nováková, Petra Škvorová, Eva Štěpánková, Lucie Veselá, Milena Widomská, Kateřina Zonygová

Foto: archiv ČIIA, fotobanka 123RF
Obálka: 123RF (dkidpix)
Neprodejné, určeno pro Český institut interních auditorů
Náklad: 1500 výtisků
Pre-press: Viktor Beránek
Tisk: REPRO servis s. r. o.
Distribuce: Mail Step a. s.

iA interní auditor

Tři linie obrany

Pavel Vácha
vedoucí útvaru interního auditu
skupiny ČEPS

Vybráním tématu „Tři linie obrany“ jako prvku správy a řízení organizací (corporate governance) za nosné téma tohoto čísla Interního auditora redakční rada definovala významný milník v českém interním auditu. Ne že bychom se správou a řízením nezabývali, ale vždy to byly izolované články. Zasvětit celé číslo plastickému zobrazení interního auditu, jeho pozici v organizaci, roli, kterou hraje, to vše v kontextu „organicky nepominutelné součásti správy a řízení organizace“, to představuje skutečně výrazný milník.

„Model Tři linie obrany je jakýmsi průmyslovým standardem v oblasti správy a řízení organizací.“

Ale k věci. Model „Tři linie obrany“ je jedním z možných pohledů na roli interního auditu ve správě a řízení organizací. Je to pohled, který existuje již pár let a (do blízkého nedávna) byl přijímán jako základní standard popisu role interního auditu v organizaci. V našem prostředí to ale není zcela všeobecně známý terminus technicus, u něhož každý ví, o co jde a dokáže ho aplikovat ve svých podmínkách.

Jak jsme na tom v publikační aktivitě na toto téma ve srovnání se světem naznačuje následující tabulka. Jsou v ní uvedeny výsledky počtu odkazů, které dodal prohlížeč Google. Objektivita těchto čísel určitě nesnese přísná objektivní měřítka, ale jako jistý odhad posloužit může.

Google 1. 2. 2019

	ČR	Svět	Poměr
„interní audit“	103 000	23 200 000	0,44 %
„správa společnosti“	36 200	290 000 000	0,01 %
„tři linie obrany“	383	197 000	0,19 %
„tři linie obrany” &„interní audit”	65	75 500	0,09 %
počet členů ČIIA/IIA	1 100	175 000	0,63 %

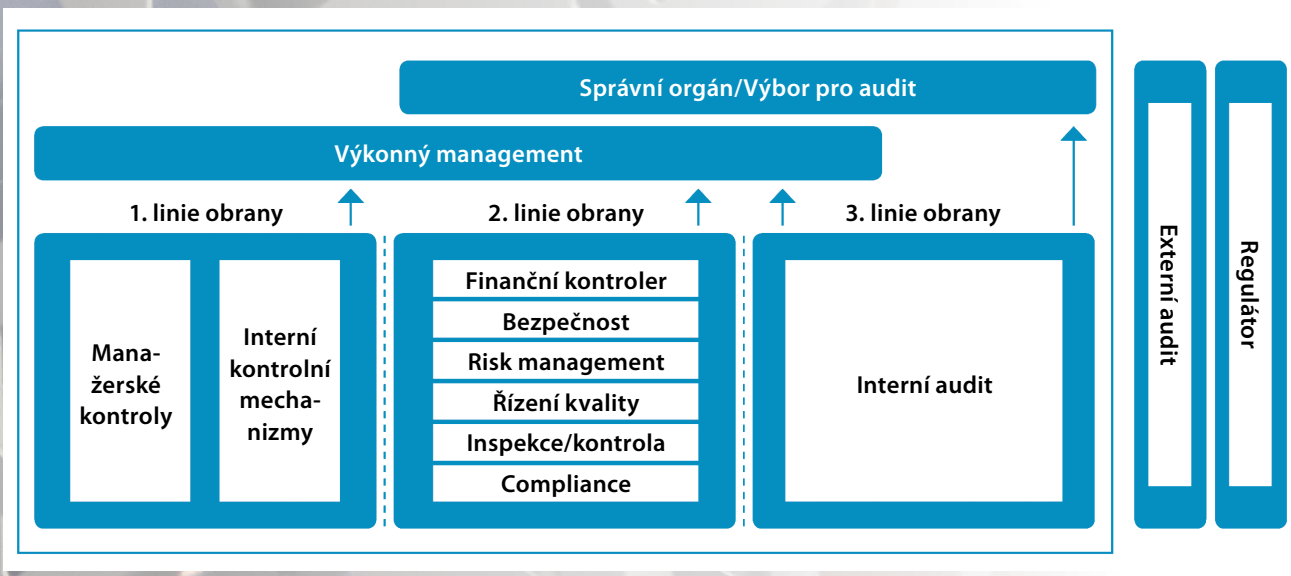
Přisoudíme-li těmto datům alespoň takovou validitu, že je možné z nich vyvodit nějaký závěr, tak jeden z možných by mohl být, že publikační aktivita v našem prostředí na téma „Tří linií obrany“ je sice několikrát nižší vzhledem k relativnímu počtu interních auditorů, ale pořád vyšší než další tématika spojená s interním auditem. Bližší zkoumání vybraných odkazů však jen ukáže, že monopol na sousloví „tři linie obrany“ interní audit rozhodně nemá. Z tohoto cvičení pro mne vyplývá, že jak ve veřejných zdrojích, tak v mém okolí se tento modelu správy a řízení příliš nevyskytuje.

Co to znamená, když se řekne „model Tři linie obrany“, („Three Lines of Defense“).

Mezinárodní institut interních auditorů (IIA) vydal v roce 2013 Position paper „THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL“. Tedy Tři linie obrany v efektivním řízení rizik a řízení. Tato studie konstatuje, že v organizacích se etablovaly samostatné role, které se zabývají řízením rizik (rozuměj jejich aktivním snižováním na akceptovatelnou mez) z dílčích úhlů. K efektivní koexistenci těchto rolí nebo funkcí je nutná jistá míra vzájemné koordinace, aby nedocházelo k vynechání některých aktivit či k duplicitě vynaložené řídicí práce. Model Tři linie obrany (dále jen 3LO) přináší jednoduchou a efektivní strukturu do vzájemného působení organizačních útvarů v organizaci. Rozděluje je do tří „linií“.

- Funkce, které „vlastní“ a řídí rizika.
- Funkce, které „dohlížejí“ na rizika.
- Funkce, které poskytují nezávislé ujištění.

Následující obrázek názorně tuto strukturu zobrazuje.



První linie obrany: výkonné vedení (Operational management)

První linii tvoří ti pracovníci, jejichž role je identifikace rizik a výkon takových aktivit, které mají za cíl riziko řídit, tzn. zmenšit jeho potenciální negativní dopad. Tyto aktivity pak vykonávají na každodenní bázi. Existují názory, že určitá vrstva managementu již není „vlastníkem rizika" a má zejm. dohlížitelskou funkci. Model takovou situaci neřeší a ponechává dosti prostoru pro vlastní přístup každé organizaci.

Druhá linie obrany: kontrolní funkce

Tuto linii reprezentují ti, jejichž úlohou je definování standardů, jimiž se řídí činnost operativních pracovníků, nebo ti, kteří dozorují provádění některých aktivit v organizaci. Tyto útvary lze rozdělit na tři podskupiny. První podskupinou je řízení rizik. Druhou podskupinu tvoří role, které sledují soulad s externími standardy. Typicky právní útvary, problematika BOZP, efektivních nákupních praktik, kvalita, compliance. Třetí podskupinou jsou útvary controllingu zabývající se skupinou finančních rizik a finančním reportingem. Obvykle jsou všechny tyto podskupiny odpovědné za vytváření interních norem, směrnic, postupů a z logiky věci mají dozorovat plnění jimi daných standardů – dohled nad první linií.

„V malých organizacích může docházet ke kombinování jednotlivých linií či jejich částí."

Třetí linie obrany: nezávislé ujištění

Interní audit poskytuje správním orgánům a vrcholovému managementu komplexní ujištění, založené na maximální nezávislosti a objektivitě v rámci organizace. Právě ta nezávislost je něco, co druhá linie postrádá. Vytvoření profesionální funkce interního auditu by měla být ambice každé organizace. To je důležité nejen pro velké a střední organizace, ale může být stejně důležitá i pro ty malé. I ony se totiž pohybují ve stejné komplexním prostředí, ale mají méně formalizovanou a zranitelnější organizační strukturu a je pro ně obtížnější zajistit dostatečně efektivní správu a procesy řízení rizik.

Externisté

Samozřejmě, že nelze opomenout externí subjekty. Externí auditoři, regulátoři a ostatní externí orgány mají

důležitou roli v celkové správní a řídicí struktuře organizace. Lze je považovat za další dodatečnou linii obrany, která má prvky druhé (nastavení kritérií pro řízení rizik) i třetí linie (ujištění). Jejich výstup je však obvykle méně rozsáhlý a specifický než výstupy poskytované „vlastními liniemi" organizace. Také se obvykle zaměřuje pouze na určitou část činnosti té které organizace.

Vrchol pyramidy

I když model 3LO nehovoří ani o vrcholovém vedení (managementu), ani o správních orgánech (governing bodies), z podstaty věci je nelze vynechat. Jsou příjemci výstupů jednotlivých linií a mají největší možnost zajistit, že model 3LO je zapracován do řídicích procesů organizace.

Koordinace všech linií

Tento aspekt je z celého modelu možná tím nejdůležitějším. Přes rozmanitost organizačních typů by všechny tři „linie" měly existovat v každém typu organizace. Jejich podoba a funkčnost se však může lišit. Zejména v malých organizacích může docházet ke kombinování jednotlivých linií či jejich částí. Například Interní audit může být pověřen funkcí řízení rizik. Z této organizační nejednotnosti pak vyplývá rozmanitost přístupů ke koordinaci jednotlivých funkcí zabývajících se řízením rizik. Vrcholové vedení ovšem očekává, a mělo by to i jasně komunikovat, že všechny funkce zabývající se nějakou formou řízení rizik budou sdílet navzájem informace a koordinovat svá úsilí. Interní audit je připraven. Standard 2050 Koordinace říká, že „Vedoucí interního auditu by měl sdílet informace a koordinovat činnosti s ostatními poskytovateli relevantního ujištění...".

Shrneme-li předchozí řádky, tak model Tři linie obrany je jakýmsi průmyslovým standardem v oblasti správy a řízení organizací. Datum jeho vzniku je určitě starší, než je zmíněný Position Paper. Nicméně IIA téma jasně utřídil, dal mu formu a poměrně exaktně definoval role v oblasti řízení rizik a vymezil jejich kompetence. Takže dnes je termín „3LO" (v originále 3LOD) rozšířenou a uznávanou normou, kterou řada organizací přijala za svou a snaží se svoje vnitřní uspořádání strukturovat podle principů 3LO. Důkazem jsou zmínky v řadě výročních zpráv.

Budoucnost modelu Tři linie obrany

Tento model ale nemá jen věrné zastánce. Hlasy, že, mírně řečeno, má své limity, se ozývají již několik let. Norman Marks už před čtyřmi lety kritizoval pasivní zaměření modelu na „obranu". Ptá se: „Proti čemu se bráníme?" A pokračuje: „Když nebudeme riskovat, jsme odsouzeni k zániku. Jediná možnost uspět je riskovat. Praktiční manažeři řízení rizik pomáhají operativním manažerům s nástroji, procesy, informacemi, aby podstoupili právě tu správnou míru rizika." A uzavírá: „Potřebujeme model, který je mnohem pozitivnější a musíme mluvit o tom, jak má výkonný management, risk management a interní audit spolupracovat, aby pomohl organizaci uspět". Na těchto slovech je hodně pravdy. A dnes jistě výrazně více než v roce 2015. Časy se ale mění. I v interním auditu. Standardy z 2017 už mantru nezávislosti neakcentují s takovým důrazem, jak tomu bylo dříve. IIA zavelel k novému strategickému plánu, který deklaruje, že interní audit má kriticky mířit na „zvyšování a ochranu hodnoty organizace". Aby tak byl i skutečně vnímám, musí představovat více než jen třetí linii obrany. Naohiro Mouri (rozhovor s ním obsahuje předchozí číslo našeho časopisu) koncem loňského roku oznámil ambiciózní projekt redesignu tříliniového konceptu správy a řízení organizací, který „by měl zahrnovat současné jemné valéry odlišností mezi jednotlivými organizacemi, aby (ty organizace) se mohly navzájem strategicky a efektivně učit a podporovat". Naohiro rovněž prohlásil, že musíme akceptovat koncept, kdy riziko přesahuje hranice obrany, že nejistota, jako zdroj rizika, vytváří i příležitosti. A obě tyhle strany rizikové mince musí firemní manažeři a stratégové brát v úvahu, když rozhodují a plánují.

Organizace projektu na aktualizaci 3LO není podstatná. Pro nás v České republice je důležitější, že výstup práce těch nejexpertnějších expertů na správu společností napříč zeměkoulí bude předložen k formálnímu celosvětovému připomínkovému řízení. Asi lze očekávat obdobný přístup, jaký byl aplikován na poslední verzi Standardů. K tomuto veřejnému komentování by mělo dojít někdy v 2. čtvrtletí letošního roku. Když vše klapne, tak nový Tříliniák by měl být slavnostně představen po prázdninách. Máme se nač těšit.

Ing. Eva Janoušková
zástupce ředitele – ředitel sekce ekonomiky a podpory
Krajský úřad Kraje Vysočina

PRVNÍ LINIE OBRANY v praxi krajského úřadu – včetně napojení na interní audit

Model „Tří linií obrany“ přináší jiný, specifický pohled na problematiku vnitřního řídicího a kontrolního systému. Zaměřuje se zejména na problematiku řízení rizik a také na zpřesnění odpovědnostních rolí v systému řízení a kontroly každé organizace. Základním principem modelu je identifikace tří linií, které se v organizaci podílejí různým způsobem na řízení rizik. Určitě je dobré připomenout – a sami autoři této metodiky to i připouštějí – že v některých případech není hranice mezi jednotlivými liniemi ostrá, tzn. že se linie mohou i překrývat. A je také dobré podotknout, že při aplikaci modelu je třeba respektovat typ organizace, velikost, předmět činnosti, organizační strukturu, přístup k řízení rizik atd. Ostatně tyto „nevýhody“ modelu „Tři linie obrany“ nastartovaly odbornou diskuzi k jeho inovaci.[1] Pojďme se teď podívat na konkrétní příklad použití tohoto modelu v prostředí Krajského úřadu Kraje Vysočina.

1 https://iaonline.theiia.org/blogs/chambers/2018/Pages/Will-The-IIA-Redraw-the-Lines-of-Defense.aspx

První linie obrany

První linie obrany je reprezentována vlastníky těch nejzákladnějších procesů. Vlastníci těchto procesů jsou zároveň vlastníky rizik. V souladu s přístupy k řízení rizik by tedy měli rizika nejen identifikovat a hodnotit, ale také následně řídit, tj. implementovat adekvátní, efektivní a funkční řídicí a kontrolní mechanizmy.

Na této úrovni řízení najdeme řadové zaměstnance, případně oddělení a jejich vedoucí, tzn. že se jedná o řízení na denní, operativní, provozní bázi. Identifikace a hodnocení rizik a přijímání opatření ke snížení jejich dopadu nebo pravděpodobnosti probíhá s ohledem na cíle těchto činností. Jako konkrétní řídicí a kontrolní mechanizmy – které přispívají ke snížení nebo eliminaci rizik na této úrovni řízení, nejčastěji identifikujeme např.:

- pracovní náplně, stanovení odpovědnosti a pravomoci, popisy práce, manuály;
- směrnice, metodiky, příkazy, řády, statuty a další nástroje tzv. vnitřní legislativy, včetně etického kodexu, standardů chování a nástrojů pro předcházení podvodům;
- autorizační procedury a hesla, řízení přístupů, chybová hlášení, nástroje k zajištění bezpečnosti, přesnosti a úplnosti informací a k ochraně citlivých dat a nakládání s nimi. Patří sem také všeobecné i aplikační kontroly v IT systémech;
- limity, oprávnění, kritéria 3 E, rozpočty – pokud se jedná o finanční operace;
- kontrolní součty, inventarizace, křížové součty, odsouhlasování (rekonciliace) – pokud se jedná o účetnictví;
- stanovení kvalifikačních předpokladů, vzdělávání zaměstnanců, hodnocení jejich výkonu, programy mentoringu a stabilizační programy – pokud se jedná o řízení lidských zdrojů;
- nástroje manažerského řízení na denní bázi podle principu „kdo řídí, kontroluje“ a také zásadu čtyř očí a dvou podpisů, která patří k těm nejzákladnějším kontrolním mechanizmům;

Výše uvedený seznam není rozhodně vyčerpávající, ale zahrnuje takové řídicí a kontrolní mechanizmy, které jsou běžné v každém typu organizace.

V podmínkách krajského úřadu, který má běžnou liniově štábní strukturu, najdeme kromě výše uvedených řídicích a kontrolních mechanizmů i takové, které reagují na specifická rizika konkrétní organizace veřejné správy, tedy Krajského úřadu Kraje Vysočina. Namátkově jde o:

- řídicí a kontrolní mechanizmy, implementované pro pokrytí rizik nesouladu se zákonem o finanční kontrole. Jde např. o elektronická pověření k výkonu funkce příkazce operace, správce rozpočtu, hlavní účetní, individuální a limitované přísliby, schvalovací postupy v procesu nákupu (objednávky, smlouvy), v procesech projektové řízení, schvalovací postupy v rozpočetnictví i v účetnictví, při nakládání s hotovostí, podpisové vzory atd.;
- řídicí a kontrolní mechanizmy, které snižují pravděpodobnost výskytu a významnost dopadu rizik, vznikajících u vybraných procesů: např. Metodika pro proces nepřítomnosti zaměstnance, včetně elektronicky zpracovaného workflow a v něm zabudovaných elektronických formulářů a schvalovacích a informačních postupů, dále např. Metodika pro proces zadávání veřejných zakázek, na kterou opět navazují schvalovací postupy, autorizační postupy (elektronické podpisy), automatické kontroly naplnění zveřejňovacích povinností a vazby na příslušný software apod.);
- řídicí a kontrolní mechanizmy, implementované prostřednictvím HelpDesku krajského úřadu. Zde můžeme najít různé typy např. schvalovacích postupů, postupy vytváření rezervací objektů nebo událostí a školení, postupy k zajištění přístupů do informačních systémů, hlášení incidentů apod. Tyto mechanizmy pokrývají různé typy rizik, např. riziko neoprávněného nakládání s veřejnými prostředky, riziko neoprávněných přístupů, riziko zařazení zaměstnance do nesprávného typu školení apod.;
- řídicí a kontrolní mechanizmy, zajišťující předávání informací a komunikaci na této řídicí úrovni. Zde je to zejména intranet – nejen jako informační, ale i aplikační nástroj (např. Portál strategického řízení, Evidence týmů, přístup do datového skladu, přístup do personálního systému, včetně docházky). Intranet také umožňuje řadovým zaměstnancům vznést připomínku či námět, nebo zveřejnit aktuální informaci pro všechny zaměstnance a jednoduše informuje každého zaměstnance o stavu různých procesů, které se ho bezprostředně týkají. Řadový zaměstnanec může využít i fyzickou schránku důvěry pro sdělení důvěrných a anonymních připomínek. Tato opatření snižují rizika např. nedostatečné informovanosti, nesprávných informací, rizika nevyužité příležitosti ke zlepšení, rizika zneužívání docházkového systému apod.;

- řídicí a kontrolní mechanizmy v oblasti informačních systémů a jejich bezpečnosti – ty pokrývají zejména rizika v oblasti bezpečnosti informací, rizika nesouladu s legislativou nebo normou. Protože krajský úřad implementuje ISO normu 27001, najdeme v této oblasti např. zjednodušená a pro řadového zaměstnance přeformulovaná pravidla kybernetické bezpečnosti a řízení bezpečnosti informačních systémů, řízení přístupů a identit (IDM) v informačních systémech, softwarové audity, nastavení pravidel pro přidělování určitého typu výpočetní techniky, nástroje pro aplikaci a dodržování heslové politiky, historii přístupů do informačních systémů, monitoring a řešení bezpečnostních incidentů apod.;

„První linie obrany je reprezentována vlastníky těch nejzákladnějších procesů.“

- celá řada řídicích a kontrolních mechanizmů na krajském úřadě je implementována i v oblasti účetnictví a rozpočtu s respektem k typu používaného software, stanovené organizační struktuře, rozhodovacím a schvalovacím pravomocem i osvědčené praxi. Namátkou jde např. o kontrolní sestavy drobných výdajů pro kontrolu „čerpání“ limitovaných příslibů, přehledy o plnění rozpočtů v analytické struktuře, výstupy z datového skladu, např. ke kontrole správného zaúčtování na účtu 042, podklady z operativních evidencí atd. I v této kategorii jde o pokrytí různých druhů rizik;
- stanovení cílů každému zaměstnanci – jde o cíle na principu SMART, které vycházejí z cílů útvaru a hodnocení plnění těchto cílů v rámci ročního hodnocení zaměstnance. Díky systému těchto cílů „od shora dolů“ je zajištěno, že jsou rizika identifikována s ohledem na cíle;
- v neposlední řadě bychom v této první linii obrany našli i spoustu řídicích a kontrolních mechanizmů v oblasti objektové bezpečnosti (zabezpečený vstup do vyhrazených prostor), kamerové systémy, klíčové hospodářství – ty pokrývají rizika neoprávněného vniknutí do prostor úřadu, riziko poškození majetku, riziko úniku citlivých dat z informačních systémů apod.

Výše uvedený seznam tedy uvádí pouze vybrané kontrolní mechanizmy. Po pravdě si neumím představit, jak dlouhý by byl seznam úplný… Nemusíme ale takový seznam vymýšlet – máme totiž k dispozici funkci interního auditu (zde

„Nemusíme ale takový seznam vymýšlet – máme totiž k dispozici funkci interního auditu.“

třetí linii obrany). Stejně jako v ostatních dobře fungujících útvarech interního auditu i u nás při provádění svých auditních zakázek auditoři nejprve identifikují rizika, pak hledají existující řídicí a kontrolní mechanizmy a následně ověřují, zda jsou tyto řídicí a kontrolní mechanizmy funkční, účinné a efektivní. Nemusím připomínat, že během jednotlivých auditů se neaudituje celý úřad, ale vybrané procesy, jejich části, někdy v kombinaci s organizačním přístupem, tj. na vybraných útvarech. Oddělení interního auditu během svých auditů ověřuje nejenom „první linii obrany“, kterou jsme blíže popsali, ale zaměřuje se také na to, zda jsou zavedeny a zda fungují řídicí a kontrolní mechanizmy ve druhé linii obrany.

Závěrem si dovolím problematiku modelu „Tři linie obrany“ shrnout. Podle mého názoru jde o model, který přináší jen trochu odlišný pohled na věci, které už známe a se kterými jsme se potkali, i když z trochu jiného úhlu pohledu: ať už se jedná o metodiku COSO a v ní zahrnutý integrovaný systém řízení rizik, nebo o teorii primárního a sekundárního systému dohledu, nebo o filozofii řídicí kontroly, jak ji známe ze zákona o finanční kontrole, vždy jde v principu o totéž: V každé organizaci máme vnitřní řídicí a kontrolní systém. Interní audit poskytuje ujištění o tom, že je funkční, účinný, efektivní a dynamický. Součástí vnitřního řídicího a kontrolního systému je i interní audit, který ověřuje, jak systém funguje a přidává hodnotu svými doporučeními, která vedou ke zlepšení systému. To vše směřuje k tomu, aby byly naplňovány cíle organizace. ■

Bezpečnost v modelu „Tří linií obrany“

Model „Tří linií obrany“ popisuje a shrnuje, jaké jsou úrovně kontroly, ale i jejich spolupráci a vazby v organizaci. Každá organizace má svůj vlastní systém řízení, který je vždy založený na principech zodpovědnosti za jednotlivé oblasti a činnosti. Někdo řídí a určuje strategické směrování společnosti, někdo se stará o vnitřní chod, o finance, o bezpečnost atd., a pochopitelně i o kontrolu. Pokud není správně fungující oblast kontroly, ztrácí společnost zpětnou vazbu a jistotu, že vše, co dělá, dělá dobře a podle všech pravidel – vnitřních i vnějších. Kontrola musí být zavedena a fungovat ve všech oblastech, které organizace vykonává. Od majetku, financí, dodržování zákonných norem, a pochopitelně se dotýká i správného fungování bezpečnosti. Bez dobře fungující bezpečnosti organizace není schopna existovat, stejně jako se neobejde bez fungujícího účetnictví a dalších oblastí.

Mgr. Vladimí Rohel
Ředitel sekce Bezpečnost
Národní agentura pro komunikační a informační technologie

Každá společnost má něco, co potřebuje chránit. Jde například o majetek, zdraví a životy zaměstnanců, své know-how a všechny další informace související s její činností. Musí chránit data svých zaměstnanců, informace o všech svých obchodech, o výzkumu, který dělá a do něhož investuje své prostředky a v neposlední řadě také informace o svém systému fungování a nastavení bezpečnosti, včetně konkrétních výsledků testů a návrhů opatření. Bezpečnost se tak potkává se vším, co organizace dělá, a její úloha je poskytnout všem ostatním účinnou ochranu a jistotu, že je vše v pořádku a zabezpečeno. Proto je nutné a důležité, aby bezpečnost uživatelé, administrátoři i vedení společnosti brali jako jednu z priorit, důvěřovali jí a řídili se jejími nařízeními, doporučeními, a aktivně se tak podíleli na ochraně společnosti.

Zde se nabízí otázka, co vše musí organizace nebo firma v bezpečnosti dělat? Musí řešit vše? Musí investovat velké peníze do své bezpečnosti? Odpověď na tyto i další otázky je i není jednoduchá.

Začněme trochu zeširoka. Bezpečnost je vždy nutné brát jako celek a jako celek ji stavět, hodnotit, ověřovat i kontrolovat. Jednotlivé oblasti bezpečnosti se vzájemně doplňují, podporují a pomáhají přijímat účinná opatření k pokrytí všech hrozeb a souvisejících rizik, které společnosti hrozí. Zní to možná hodně složitě, ale nejde o nic jiného, než co děláme v běžném životě denně. Při přecházení přes ulici automaticky vyhodnotíme, co se nám může stát a jak je to pravděpodobné. K tomu přijmeme odpovídající opatření. Rychle se blížící

vůz by mohl znamenat srážku a úraz, tak buď zrychlíme krok, nebo se zastavíme a počkáme. To, jak se zachováme a co uděláme, je vždy po vyhodnocení celkové situace. Takovýchto rozhodnutí děláme stovky každý den.

„Každá společnost má něco, co potřebuje chránit.“

Na stejném principu funguje bezpečnost obecně. Některými situacemi a problémy se zabýváme proto, že nám to něco nebo někdo nařizuje. V takovém případě nemusíme přemýšlet, zda se nás to týká, nebo ne. Prostě se daným problémem musíme zabývat a své počínání „nějak popsat“. Jak ale zjistíme, že postupujeme správně? Že jsou naše opatření správně navržena? Že jsme na něco nezapomněli, nebo naopak nejdeme s kanonem na vrabce? Jak zjistí budoucí kontrola, že jsme vše udělali správně, efektivně, ekonomicky atd.? K tomu všemu nám slouží rizika a práce s nimi. Rizika jsou výborný nástroj a pomůcka pro řízení nejen bezpečnosti, ale i ostatních oblastí v organizaci. Bez správné analýzy a vyhodnocení rizik nám hrozí, že buď naše opatření nebudou dostatečná, nebo budeme zbytečně investovat velké prostředky, které bychom mohli využít jinak. I k tomu slouží systém kontrol a auditů. Má za úkol prověřit, zda byla správně ohodnocena rizika, opatření jsou adekvátní a navržena v kontextu a s přihlédnutím ke všem dalším oblastem a možnostem řešení. Zároveň je nutné posoudit, zda se tím vším naplňuje základní zadání a požadavek nejvyššího vedení.

Každá organizace by si v souvislosti s tím, čím se zabývá a co je její hlavní činností, měla stanovit, co je pro ni nejdůležitější, a co tak potřebuje nejvíce chránit. Zde si dovolím tvrdit, že po detailním posouzení téměř v každé organizaci dospějeme k tomu, že tím nejcennějším, co máme, jsou naše informace. Majetek si pořídíme nový, seženeme i peníze, odešlé zaměstnance nakonec nahradí noví, ale pokud nám někdo ukradne naše informace, může to znamenat konec našeho bytí. V celé historii lidstva byly vždy informace cennou komoditou. Kdo měl informace, měl výhodu. Stejně je tomu tak i nyní a bude to platit vždy.

Jak ale systém bezpečnosti v organizaci nastavit? Kdo by to měl celé řídit a kontrolovat?

Odpověď na tuto otázku je vcelku jednoduchá a logická – nejvyšší vedení. Zde se určuje, co bude organizace dělat, čím se bude zabývat, jaká bude její strategie, a je nezbytně nutné, aby se na této úrovni vedla i diskuze k bezpečnosti. Není nezbytně nutné, aby ve strategickém vedení byli samí odborníci na bezpečnost, a není k tomu ani důvod, ale je bezpodmínečně nutné, aby jeho členové toto téma vnímali a aktivně ho řešili. Aby se neustále ujišťovali, že jejich informace jsou v bezpečí, že konkurence levně nezíská jejich draze nabyté a získané informace, a nebude tak mít klíčovou výhodu atd. Nejvyšší vedení se musí samozřejmě zabývat tím, jak si vede jejich produkt, jaká je finanční situace firmy, jak pokračují projekty.… Pokud se ale nezajímá o bezpečnost svých informací, hrozí to nejhorší – ztráta nebo narušení jejích informací. Bezpečnost bude mít v organizaci takové slovo, postavení, úroveň a prioritu, na jaké úrovni řízení organizace se řeší. V organizacích, kde je téma bezpečnosti řešeno i nejvyšším vedením, je předpoklad, že tato bude řešena správně a v souladu s politikou organizace. Základní podmínka – podpora vedení je tedy splněna. V souvislosti s bezpečností je nutné, aby se vedení zabývalo klíčovými riziky společnosti, což se dnes běžně děje, a aby požadovalo mezi ně zařadit a vyhodnocovat i rizika související s bezpečností informací.

Dalším stupněm výstavby, provozování a kontroly bezpečnosti je střední management. Zde je třeba klíčová zadání z nejvyššího vedení i v oblasti rizik uchopit a rozvést do všech oblastí v organizaci. Rizika jsou klíčovým pojmem. Těch několik málo vrcholových rizik je nutné rozpracovat a doplnit o další operační rizika navázaná na konkrétní aktiva. Ploché nastavení rizik na všechna aktiva organizace ale není vhodné. Někdy je dobré, a doporučuji to, přejít přes několik vrstev aktiv skupinových a až v poslední úrovni se dostat na konkrétní aktivum. S aktivy

se tak bude lépe pracovat, lze tak nastavovat opatření pro více aktiv najednou a lze jednoduše vytvářet reporty pro kontroly nebo jednotlivé garanty. Správné navržení a práce s aktivy, skupinami aktiv a riziky nad nimi je tak další klíčový bod pro efektivní a rychlé fungování bezpečnosti. Navíc při optimálním nastavení systému řízení rizik lze vzájemně provázat rizika z více oblastí, a usnadnit tak vyhodnocování dopadů navrhovaných opatření. Ve chvíli, kdy je možné řešit problém vícero způsoby, je třeba přesně vědět, co který způsob do detailu znamená, čeho všeho se daná varianta řešení dotkne a kolik to bude společnost stát. Snadno se tak dostanete k hodnotě TCO, která je pro správné rozhodnutí vedení nezbytná. Dobře navržený systém řízení operačních i skupinových rizik, jejich vazba na vrcholová rizika a vzájemné provázání rizik mezi sebou, vám umožní dělat ta nejlepší rozhodnutí a téměř v reálném čase.

Pro to, abyste dokázali navrhnout optimální opatření v oblasti bezpečnosti, je nutné, aby všechny druhy bezpečnosti byly řízeny společně, jednotně a provázaně, a aby tak byly i kontrolovány. Pro ošetření rizika můžete totiž často učinit opatření i v jiné oblasti. Např. riziko úniku informací ze systému můžete eliminovat drahým a složitým softwarem nebo se již na začátku při výběru zaměstnanců zaměříte více na jejich bezpečnostní povědomí a spolehlivost a tím riziko plošně snížíte. Pokud bezpečnost řídíte centrálně a jednotně, docílíte tak maximální synergie a provázanosti navržených opatření, která se budou vzájemně vhodně doplňovat. Dobře je to například vidět v oblastech kybernetická bezpečnost a GDPR. V organizacích, kde tyto oblasti řeší jeden útvar, nutně museli dospět k závěru, že díky kybernetické bezpečnosti již řadu opatření pro GDPR mají splněných a soustředili se pouze na doplnění několika málo detailů a vypořádání pár dalších úkolů, které jsou pro GDPR specifické. Bezpečnost se tak v těchto organizacích staví více logicky, efektivně a jako mozaika, kde každý nový kousek těží z již vybudovaného obrazu a dále ho doplňuje a rozšiřuje. Časem se tak nutně dostanete do situace, kdy každý nový problém v oblasti bezpečnosti informací bude znamenat téměř žádné nebo jen velmi malé náklady a krátký čas na řešení. S tím pochopitelně souvisí i náklady, čas a další požadavky na kontroly a audit.

„Bezpečnost bude mít v organizaci takové slovo, postavení, úroveň a prioritu, na jaké úrovni řízení organizace se řeší.“

Ne nepodstatnou částí bezpečnosti je osvěta, školení a dokumentace. Zde se výhodně opět projeví, pokud bezpečnost je zastřešována a řízena z jednoho místa. Koordinací a synergiemi se tak docílí jednotného přístupu, pohledu na problém ze všech směrů a vzájemného propojení, které má pozitivní dopad na všechny uživatele v organizaci. Je dobré, pokud administrátoři i uživatelé vnímají bezpečnost jako celek a řešení jednoho problému jako komplex opatření z různých oblastí. Takto to totiž funguje i v běžném životě. S tím běžný člověk umí pracovat, snáze to chápe a řídí se tím. Pokud uživatel nerozumí problému a nepochopí ho, nebude dodržovat nezbytná opatření, byť by byla povinná a vynucovaná. Příkladem může být situace, že nikdo si nepověsí klíče od domu na hřebík na plotě, ale spousta lidí si bez problému nalepí své heslo na kalendář nebo monitor na stole. Uživatel musí rozumět podstatě problému, čehož dosáhneme permanentní osvětou, školeními, testy a cvičeními. Dokumentace se musí doplňovat a musí z ní být jasné, na co předepsané povinnosti reagují a jaký problém řeší.

Celý systém bezpečnosti je pochopitelně nutné doplnit o oblast, kterou jsem lehce zmínil na začátku článku – zákonné a jiné povinnosti, které je třeba dodržovat a plnit. K tomu je třeba, aby organizace měla přesně zmapováno, které povinnosti na ni mají vliv a co z toho na ni dopadá. V oblasti bezpečnosti je to jasný základ, kolem kterého by se měl stavět celý systém. Tuto oblast je třeba neustále sledovat a vyhodnocovat. Úkoly pro bezpečnost mohou totiž vyplynout i z oblastí, které s bezpečností nijak nesouvisejí. Už jsem zde uvedl, že naprostá většina toho, s čím v organizaci pracujeme, jsou její informace a ty musíme chránit.

A důležitá věc na závěr. Je vhodné, aby princip výstavby systému bezpečnosti chápali i lidé zajišťující kontrolu a audit. Oni budou nakonec ti, kteří budou poskytovat zpětnou vazbu i nejvyššímu vedení společnosti, upozorňovat ho na chyby v nastavení systému, dávat doporučení a navrhovat úkoly osobám zodpovědným za výstavbu a řízení systému bezpečnosti, a tím tak pozitivně podporovat jeho úspěšné provozování a fungování v organizaci.

Michal Němec
ředitel Řízení nefinančních rizik
a compliance v České spořitelně

Michal Němec působil na různých pozicích v oblasti řízení operačních rizik v bankách, kde dokázal navázat na svoji předcházející zkušenost v bankovním dohledu ČNB. V posledních letech je ředitelem útvaru řízení nefinančních rizik a compliance v České spořitelně, kde usiluje o holistický přístup v řízení těchto rizik.

Existovala by druhá kontrolní linie, kdyby nebyla vyžadována regulátorem?

Role druhé kontrolní linie v bankovnictví má oporu v řadě regulatorních požadavků, ve kterých je její pozice pevně zakotvena a v posledních letech stále posilována. Řada těchto požadavků vychází z významných skandálů, jejichž svědky jsme byli v několika posledních letech. Cílem regulatorních úprav je tak vytvořit, či alespoň ovlivnit vnitřní prostředí ve společnostech způsobem, který by zajistil, že nebude docházet k dalšímu opakování obdobných událostí, nebo aspoň ne v takovém rozsahu. Nicméně zabíhání do detailní analýzy jednotlivých požadavků, včetně zamýšlení se nad motivací pro jejich stanovení, efektivitou těchto požadavků či možným způsobem jejich naplnění v podmínkách konkrétní instituce, by vyžadovalo řadu stránek textu, možná dokonce několik celých čísel tohoto periodika. I tak by s ohledem na včlenění těchto požadavků do různých regulací, doporučení, vyhlášek, reakcí na dotazy či ostatních dokumentů více či méně závazných pro celý sektor, bylo obtížné zajistit úplnost přehledu, nezkreslenost pohledu či odhadnout přesně záměr regulátora. Zároveň jsem přesvědčen, že všichni, kdo se zabývají danou problematikou profesionálně a působí v druholiniových útvarech, mají nastaveny vlastní procesy pro sledování vývoje regulace, proto by takové pojetí příspěvku nebylo ničím více než pouhým výčtem sloužícím pro ověření úplnosti tohoto seznamu. Z těchto důvodů se domnívám, že by mohlo být zajímavější pokusit se zaměřit spíše na přiblížení druhé linie jako nedílného článku celého vnitřního řídicího a kontrolního systému z praktického pohledu.

Protože regulace je v této oblasti spíše založená na principech, a nikoliv detailním výčtu konkrétních požadavků, počet způsobů praktického úspěšného naplnění požadavků může být blízký počtu společností, které se nad zvolením vhodného přístupu aktivně zamýšlejí. Přestože se tedy cesty k dosažení cíle mohou v jednotlivých společnostech lišit, cíl a role druholiniových útvarů by měla zůstávat obdobná. Jedná se nejen o ujištění souladnosti interních procesů s regulatorními požadavky pro vedení společnosti, ale zároveň o podporu vrcholového vedení společnosti a rozvojových aktivit obchodních útvarů, a tím významně přispívat k bezproblémové, rychlejší a co nejefektivnější implementaci nových pravidel.

Přesto mezi požadavky regulátora patří, aby byla oddělena funkce řízení rizik a compliance, je-li to z pohledu velikosti a komplexity konkrétní instituce žádoucí. Konkrétní požadavek je uveden v § 21 odst. 5 tzv. obezřetnostní vyhlášky[1], podle které by tyto funkce měly být vzájemně odděleny, ledaže by takové uspořádání bylo nepřiměřené povaze, rozsahu a složitosti činností zajišťovaných konkrétní společností. Obdobný požadavek je uveden i v obecných pokynech k vnitřnímu systému správy a řízení[2], ve kterých je speciálně v kapitole 19.3 uvedeno, že funkci řízení rizik a compliance lze sloučit s přihlédnutím ke kritériím proporcionality.

V rámci funkce řízení rizik je možné provést další rozklad, který funkci rozděluje na kvantitativní

„Role druhé kontrolní linie v bankovnictví má oporu v řadě regulatorních požadavků.“

Z praktického pohledu se do druhé linie primárně zahrnují útvary, které zajišťují funkci řízení rizik a funkci compliance. část funkce řízení rizik zajišťující primárně vývoj a správu různých matematických modelů, včetně následného

[1] Vyhláška č. 163/2014 Sb., o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry, ve znění pozdějších předpisů.

[2] EBA Obecné pokyny k vnitřnímu systému správy a řízení (EBA/GL/2017/11).

reportingu a ověřování souladu těchto výstupů se systémem limitů stanovených celkovou strategií řízení rizik. Tyto části jsou využívány především při řízení celé škály tržních rizik, úvěrového rizika či rizika likvidity a stanovování souvisejících kapitálových požadavků. Druhá část se zabývá především kvalitativními metodami používanými pro řízení rizik a míří primárně do oblasti řízení rizika operačního, reputačního rizika či dalších kategorií rizik, jejichž kvantifikace je založena spíše na odborném úsudku konkrétních expertů než na matematicky odvozených modelech.[3]

rizika compliance využívá detailní znalosti procesů v bance při zapojení příslušných manažerů banky, například při průběžném hodnocení rizika compliance v jednotlivých útvarech společnosti. Tento přístup je velmi blízký technikám, které jsou uplatňovány funkcí řízení rizik zaměřených na hodnocení kvalitativních rizik, včetně rizika operačního. Proto i u komplexních institucí spatřuji výhody částečného propojení těchto funkcí, minimálně v rovině vzájemné spolupráce při sběru podkladů pro jejich další činnost a vyměňování si zkušeností s využíváním těchto typů expertního hodnocení.

„Regulace je v této oblasti spíše založená na principech, a nikoliv detailním výčtu konkrétních požadavků.“

Považuji za zcela přirozené, že kvantitativní metody vyžadují velmi specifické znalosti, a proto by měly být koncentrovány na jednom místě, aby mohly být v plném rozsahu využity synergické efekty modelářů, ze kterých se stává stále vzácnější zboží s rostoucí poptávkou i mírou jejich uplatnění. Na rozdíl od těchto exaktně odvozených nástrojů se při hodnocení

Bude-li při této spolupráci či výměně názorů zachována nezávislost útvaru compliance v jeho primární roli, tedy ověřování souladu konkrétních činností s vnitřními předpisy a procesy společnosti a zároveň kvality implementace externích předpisů a norem (mimo jiné tedy i právě v oblasti operačních rizik či dalších spolupracujících útvarů), domnívám se, že spolupráce v oblasti získávání informací či jejich vzájemné sdílení je jenom přínosné. Tento závěr je platný samozřejmě pouze za předpokladu, že ve společnosti je vytvořeno takové prostředí, které minimalizuje potenciální konflikt zájmu vycházející z tohoto propojení, např. ve formě možné eskalace ze strany vedoucího týmu compliance, nebyl-li by hlas compliance upozorňující na rozpor s regulací v rámci probíhající spolupráce dostatečně vyslyšen.

Dovolil bych si i mírně provokativní podnět – zkuste se dotázat kolegů, se kterými nepřicházíte pravidelně do styku, jaké jsou role a odpovědnosti útvaru řízení operačních rizik, compliance nebo právního útvaru. A když budete odvážní, můžete do dotazu zahrnout i útvar interního auditu. Já jsem si podobný dílčí průzkum udělal a jasně se ukázalo, že vnímají maximálně rozdíl v základních rolích uvedených útvarů, ale při diskuzi o bližších detailech již nevnímají hranice tak ostře. K tomuto nejasnému vymezení může při odděleném zjišťování informací relevantních pro operační rizika nebo compliance přispívat i podobnost některých otázek, což jsou právě důvody, které mohou vést ke společnému sběru informací.

Nicméně při hodnocení spolupráce se nemusíme zastavit pouze u útvarů naplňujících funkci řízení rizik a compliance, tedy tzv. druholiniových útvarů. V České spořitelně máme dlouhodobou a velmi pozitivní zkušenost i při spolupráci mezi útvary řízení rizik a interním auditem, a to především při plánování kontrolních aktivit nebo při identifikaci rizik napříč celou společností. Standardním nástrojem využívaným pro tento účel je rizikové sebehodnocení, známé rovněž pod zkratkou RCSA, které je standardně zastřešováno útvarem řízení operačních rizik. Tento nástroj slouží pro vytipování oblastí s největším potenciálním rizikem vzniku ztráty či jiného rizika (např. reputačního) pro konkrétní společnost a přijetí následných opatření pro snížení rizikovosti konkrétní činnosti či následné akceptaci rizika ze strany nejvyššího vedení. Obdobný rizikově vážený pohled je využíván i interními auditory při plánování jejich aktivit na následující období. Proto jsem rád, že se nám podařilo spojit úsilí a toto zjišťování provádět ve vzájemné koordinaci, a často dokonce formou společné účasti na jednáních s jednotlivými útvary při diskuzi o jimi podstupovaných rizicích. Opět je však celá spolupráce možná pouze za předpokladu, že nedojde k prolomení základních principů rozlišujících útvary v druhé a třetí linii obrany. Speciálně v našem případě dochází pouze ke společnému sběru informací s využitím stejného nástroje/aplikace, ale v dalším kroku již dochází

[3] Pro zjednodušení se v textu zaměřuji pouze na vybrané činnosti v rámci funkce řízení rizik, na kterých lze ukázat výhody spolupráce s dalšími útvary.

k samostatnému a nezávislému zpracování a využití společně získaných informací. Z vlastní zkušenosti jsem přesvědčen, že ani tento společný přístup ke sběru informací nebrání internímu auditu provést ucelený audit procesu řízení operačního rizika, včetně způsobu vyhodnocení získaných informací v rámci RCSA procesu a jejich dalšího promítnutí do celkového rámce řízení operačního rizika.

Naopak útvary, které jsou předmětem tohoto sběru informací, vzájemnou spolupráci zúčastněných útvarů vnímají velmi pozitivně, jelikož s ohledem na podobnost zjišťovaných informací vnímají úsporu času a kapacit při tomto úzce koordinovaném, či dokonce společném postupu. Předpokladem tohoto společného postupu a jeho akceptace ze strany ostatních manažerů je ale vytvoření takového vnitřního prostředí, ve kterém nebudou mít obavy otevřeně diskutovat problematické otázky či přímo upozorňovat na nedostatky ve vlastním kontrolním prostředí. Dosažení tohoto cíle však není jednoduché, jde o běh na dlouhou trať nebo možná trefněji spíše o extrémní ultramaraton s neustálým trpělivým vysvětlováním přínosů celého cvičení a způsobu vyhodnocení získaných informací.

Pojďme se ale podívat i na druholiniové útvary v právě se transformujícím bankovním prostředí. S rostoucí komplexitou služeb i zvyšováním regulatorní zátěže dospěly tradiční finanční instituce do stadia, ve kterém již nedokáží dostatečně aktivně reagovat na rychle se měnící prostředí a rostoucí konkurenci v podobě nových hráčů na trhu. Těmto třetím stranám se díky nové regulaci otevírá přístup k operacím a informacím do nedávné doby dominantně vlastněných původními institucemi. Jednou z reakcí na tento trend je tak bližší provázání obchodních útvarů s vývojáři klientských či vnitřních aplikací či dalšími podpůrnými útvary. A to bez ohledu na termín, kterým se tento proces označuje, byť ve finančním sektoru v české kotlině aktuálně

převládá pojem agilní transformace.

Tato změna organizace práce a celkového smýšlení o nových strategiích jednotlivých společností staví kontrolní útvary, a především compliance před nové úkoly, které donedávna byly považovány za dávno vyřešené. Jako konkrétní příklad lze uvést organizační uspořádání jednotlivých nových týmů, které často mají pozici blížící se samostatné firmě. Ano, úzké propojení obchodních útvarů na IT vývojáře je z mnoha pohledů prospěšné, především v rovině snazšího vzájemného porozumění a zrychlení dodávek očekávaného produktu, ale na druhou stranu tato uspořádání pozapomínají na specifické funkce, které by z obezřetnostních důvodů měly zůstat vzájemně oddělené. Konkrétně lze uvést funkce vývojářů, testerů, správců aplikací či dalších funkcí souvisejících s vývojem a provozem IT aplikací. V této oblasti je od compliance očekáváno, že nestranně vyhodnotí navržené uspořádání především z pohledu možného konfliktu zájmů (např. rychlá dodávka vs. akceptační testy nebo znalosti vývojáře vs. požadavky na nezávislé prověření před nasazením do produkčního prostředí jako prevence chyb nebo v extrémním případě i detekce nežádoucí částí kódu s cílem budoucího obohacení se na úkor klienta či společnosti), a případně navrhne řešení, které stále bude vyhovovat požadavkům nového funkčního uspořádání a zároveň nebude otevírat společnost nežádoucím rizikům.

„V počátečních úvahách o organizační transformaci měli někteří kolegové poměrně ‚pankáčskou' představu o organizaci práce."

Další výzvou pro kontrolní funkce může být schopnost zaznamenat a dostatečně rychle zareagovat na průběžně se měnící prostředí v těchto nových organizacích, způsoby vývoje nových produktů s důrazem na rychlý vývoj prototypů, jejich otestování na vzorku klientů, stanovení nejvhodnějších řešení a jejich následné dokončení a nasazení do ostrého provozu. V tomto případě je nutné nastavit si nejen informační kanály, které umožní udržovat si i v kontrolních útvarech průběžně aktuální informace. Tohoto cíle lze dosáhnout například účastí kontrolních funkcí na fórech, kde se diskutují a formulují nové cíle na nadcházející období. Náročnější, ale o to přínosnější, je pracovat způsobem a dodávat stanoviska s tak vysokou přidanou hodnotou pro kolegy v nové transformované organizaci, že sami budou tyto kontrolní funkce oslovovat s žádostí o konzultaci ve vhodném okamžiku – tedy ani ne příliš brzy, kdy se teprve formulují základní ideje, ze kterých následně vykrystalizuje pouze zlomek myšlenek s potenciálem na uplatnění v praxi, ale ani příliš pozdě, aby případné úpravy dodávky na poslední chvíli vyžadované kontrolními funkcemi neprodražovaly konečnou dodávku nebo ji časově významně neprodlužovaly. Konzultace by se neměly omezovat jenom na upozorňování na novou legislativu, zajišťování stanoviska regulátorů u nejednoznačných částí regulace či poskytování vlastních výkladů umožňující efektivní naplnění požadavků, ale i průběžné upozorňování na rizika u nově navrhovaných produktů, včetně návrhů na snížení těchto rizik. Neméně významným cílem je i aktivní předcházení nežádoucím efektům při návrhu nových procesů – nebavíme se pouze o předcházení nekalého jednání klientů, zaměstnanců či třetích stran, ale i upozorňování na potenciální systémové či procesní problémy. Tato cesta ale není jednoduchá, zvláště v počátečních úvahách o organizační transformaci měli někteří kolegové poměrně „pankáčskou" představu o organizaci práce, nicméně tyto představy již můžeme komentovat pouze s úsměvem a nemyslím si, že je potřeba je příliš rozebírat. Ve skutečnosti transformovaná společnost klade na organizaci práce a odpovědnost jednotlivých lidí mnohem vyšší nároky než v klasickém hierarchickém uspořádání.

Jak je patrné, kontrolní funkce jsou dále vystavovány většímu tlaku na rostoucí odbornost, a to především se stále rozsáhlejším využíváním automatizace procesů, digitalizace, pokročilých rozhodovacích algoritmů (včetně často zmiňovaných tzv. samoučicích algoritmů apod.) a obdobných postupů. Toto vše jsou důvody, proč je rostoucí tlak na specializaci jednotlivých kolegů v týmech a opuštění kdysi propagované univerzálnosti zaměstnanců v kontrolních funkcích. A právě i díky této postupně zvyšující se odbornosti mohou být zástupci kontrolních útvarů přirozenými partnery pro obchodníky a další útvary banky a nebýt jen trpce akceptovanou přítěží chráněnou regulatorními požadavky. Zároveň tento aktivní přístup činí práci v kontrolních týmech stále pestřejší a zajímavější, přináší neustále nové výzvy a nedovoluje ustrnout v zavedených kolejích.

Příspěvek vyjadřuje autorův soukromý názor, a neodráží tak oficiální stanovisko instituce, pro niž autor pracuje.

Druhá linie obrany – řízení rizik

Eva Štěpánková
ředitelka odboru rozpočtu
Ministerstvo pro místní rozvoj

Ústřední téma tohoto vydání časopisu se nazývá „Linie obrany“. Redakční rada časopisu se snaží shrnout poznatky týkající se efektivního řízení společností podle liniových funkcí, které má management těchto společností k dispozici a na jejichž ujišťovací služby se spoléhá. Ať už všechny linie obrany chápeme v užším, nebo širším slova smyslu, vždy je třeba správně charakterizovat, proti čemu stavíme obranu. A to lze jednoduše shrnout do pojmu „rizika“.

Pokud první linií obrany proti rizikovým událostem je přímo výkonný management, je zřejmé, že tato linie řídí hlavní směry prováděných činností, a samozřejmě vidí i dopady rizik, která nejsou dostatečným způsobem zohledňována a eliminována. První linie stojí na začátku i konci celého procesu odpovědnosti za řízení rizik.

K tomu, aby se rizika vhodným způsobem identifikovala, aby se s nimi operativně pracovalo a sledovala implementace všech opatření, včetně následného hodnocení, slouží druhá linie. Druhá linie obrany sleduje a vyhodnocuje detaily při výkonu činnosti. Zajišťuje faktickou správu organizace. Slouží pro nejvyšší management ke zkvalitnění celkového systému řízení, a to zejména v oblastech compliance, koordinace rizik, řízení kvality, vnitřní kontroly. Tato linie obrany pomáhá organizaci poskytováním dostatečných informací, výsledků interních analýz a vlastním hodnocením.

Dodatečným ověřovacím a ujišťovacím metodám a návrhům systémových opatření se věnuje třetí linie obrany – interní audit. Tato linie obrany funguje nezávisle a podle míry a významnosti rizik audituje oblasti, které jsou pro management nejzásadnější. V celkovém přístupu k hodnocení auditovaných oblastí by neměl interní audit opomenout se zaměřit, mimo jiné, i na úroveň řízení rizik ze strany samotného managementu.

Ve svém článku bych se chtěla více věnovat druhé linii obrany, a to koordinaci a řízení rizik. Nebudu proklamativně uvádět základní známé definice, právní úpravu nebo výčet oblastí, podle

kterých rizika rozlišujeme a v jakých oborech činností se s nimi setkáme, nýbrž bych ráda tuto velice sofistikovanou agendu popsala z pohledu praktického využití pro řízení organizace a její význam v liniích obrany.

Zaměřím se zejména na řízení rizik v organizacích veřejné správy, kde základním právním rámcem pro vymezení hlavních kategorií rizik je zákon o finanční kontrole, který ukládá povinnost zajištění ochrany veřejných prostředků proti rizikům, nesrovnalostem nebo jiným nedostatkům způsobeným zejména porušením právních předpisů, nehospodárným, neúčelným a neefektivním nakládáním s veřejnými prostředky nebo trestnou činností, která je jedním z cílů finanční kontroly.

Kde by měl takový koordinátor spolu s každým vlastníkem rizika začít? Domnívám se, že pro zavedení jednotné evidence rizik i sledování účinnosti opatření je třeba vymezit základní a hlavní působnosti organizace, nikoli detailní aktivity, které neumožní vidění organizace jako celku. Je tedy vhodné vidět tzv. agregovaná rizika, a ta podle jejich významnosti případně řídit i z pohledu dílčích aktivit.

K takovémuto rozdělení je nutná důkladná znalost procesů, které v organizaci probíhají, systému rozdělení odpovědnosti, kompetencí a postupů vyplývajících z interních předpisů, zákonů a vnějších norem, které procesy organizace ovlivňují. Koordinátor velice úzce spolupracuje s vlastníky rizik, ověřuje jejich vstupy pro stanovení přehledu hlavních činností a možných rizik s organizačním uspořádáním, sjednocuje a nastavuje kvantitativní a měřitelné hodnoty pro měření míry dopadu a četnosti výskytu. Vedle toho koordinátor porovnává evidenci významných rizik se skutečnou situací organizace, sleduje případy činností, u kterých dochází k pochybením nebo jiným selháním, k faktickým finančním ztrátám, k negativním výsledkům kontrol, k provozním poruchám, nevhodné medializaci apod. Toto mapování a důsledné sledování chodu organizace je praktickým odrazem stavu řízení rizik.

Pro prvotní sběr informací slouží karty rizik, které v dnešní době lze vést elektronicky a vhodně sledovat vývoj rizika v časové řadě a porovnávat se skutečně řešenými problémy.

Z karet rizik vytváří koordinátor katalog a mapu nejvýznamnějších rizik. Tyto dva dokumenty by měly ležet na stole každého manažera, aby věděl, kterým činnostem je třeba se dlouhodobě věnovat, jak systémově rozdělit odpovědnosti za dílčí aktivity, nastavit dostatečnou personální kapacitu na jejich výkon a sledovat finanční náročnost jejich výkonu. V praxi tedy nejde jen o to, aby se jedenkrát ročně zpracoval katalog velmi podrobně členěných rizik a mnoha opatření, ale aby bylo zejména z mapy rizik na první pohled patrné, kam má manažer zaměřit pozornost.

Příklad karty rizik

Karta právních rizik k datu 30. 4.

Název rizika	**Nedodržování právních norem**		
Kód	**xx/PRÁ/yy/2.1**		
Vlastník rizika – číslo a název odboru			
Agenda – číslo a popis konkrétní dílčí činnosti odboru			
Dopad (D) stupnice 1–3			
Pravděpodobnost (P) stupnice 1–3			
Stupeň významnosti (V) = D x P			
Přijatá opatření – nastavené kontrolní a řídicí mechanizmy ke zmírnění rizik			
Popis	Odpovědná osoba	Termíny realizace	Dokumentování
Monitoring – sledování účinnosti kontrolních mechanizmů			
Popis	Odpovědná osoba	Nastavená frekvence	Datum provedení
Poznámka			

Vhodnou zpětnou vazbou pro koordinátora i pro vlastníka rizika je možnost skutečného měření a kvantifikování dopadů. Částky měřitelné např. u finančních rizik v korunách nebo u právních rizik např. v počtu prohraných soudních sporů, jsou dostatečně výmluvné pro další práci a stanovení potřebných opatření.

„Katalog a mapa rizik by měly ležet na stole každého manažera.“

Níže uvádím variantu mapy finančních a právních rizik vybraných útvarů.

Z celkového přehledu údajů, vedeného v mapách, a z elektronických podkladů propojených z dílčích karet a dalších zdrojů, lze provádět mnoho analýz jak pro vlastníky rizik, tak nejvyšší management, tj. pro první linii obrany. Příkladem může být např. přehled o nejpočetnějším zastoupení vybraných druhů rizik v členění podle organizačních útvarů organizace.

Výsledkem může být např. následující závěr – z celkového počtu identifikovaných rizik vykazují nejpočetnější zastoupení rizika informační a komunikační (219), následují rizika právní (198), provozní (197), finanční (166) a rizika ostatní (52).

RIZIKA

Skupiny rizik	finanční			právní			provozní			informační a komunikační			ostatní			CELKEM rizik za sekce
významnost rizik	6–9	3–4	1–2	6–9	3–4	1–2	6–9	3–4	1–2	6–9	3–4	1–2	6–9	3–4	1–2	
Přímo řízené útvary	0	2	7	3	4	5	2	3	5	4	11	3	0	4	0	53
Sekce 02	1	10	19	2	11	15	10	9	23	5	16	19	1	4	1	146
Sekce 03	14	1	2	22	8			16	10	4	17	9	1	3	2	109
Sekce 04	0	11	42	2	18	37	2	22	29	7	17	32	4	7	4	234
Sekce 05	0	1	24	0	6	22	0	9	25	3	10	29	4	5	8	146
Sekce 06	1	15	11	6	6	13	4	15	8	3	7	9	0	4	0	102
Sekce ST	2	0	3	4	4	10	4	0	1	5	3	6	0	0	0	42
	18	40	108	39	57	102	22	74	101	31	81	107	10	27	15	
CELKEM dle skupin rizik	166			198			197			219			52			832

Odbor			FINANČNÍ RIZIKA					PRÁVNÍ RIZIKA				
			Nedodržení pravidel při využívání veřejných prostředků a prostředků EU (např. porušení rozpočtové kázně)	Nedostatečné nastavení kritérií pro sledování 3E	Nedostatečné dodržování 3E	Nedostatečné zajištění řídicí kontroly ve všech jejích fázích	Nedostatečné plánování finančních zdrojů na příští období v rámci rozpočtové skladby	Nedodržení právních norem	Nedodržování schválených postupů – pracovní činnosti jsou usměrňovány velkým množstvím právních norem, riziko nepochopení a nepřesného výkladu, nezachycení potřebných informací	Nesoulad vnitřních norem s vnějšími právními normami a předpisy EU	Neaktuálnost, neprovázanost vnitřní předpisové základny, nezapracování vnějších právních změn do vnitřního systému	Nesoulad s koncepcemi a strategiemi
č.	zkratka	agenda	1.1	1.2	1.3	1.4	1.5	2.1	2.2	2.3	2.4	2.5
1	AA	1	4	1	2	2		3	6	2	4	1
2	AB	1	4	2	2	2	2	4	4	2	2	2
3	AC	1						9	6			
4	AD	2				9			6			
5	AE	3								4	6	
6	AF	1	3	3	3	1	1	2	1	1	1	1
7	AG	2	4	4	4	4	1	2	2			
8	AH	3	3	3	3	3	2	1	2			
9	AI	1										
10	AJ	2					2					
11	AK	1	4				4	6				

Vizuální přehled např. o počtu konkrétních typů rizik se zohledněním významnosti samozřejmě nejrychleji podávají grafy.

Přestože druhá linie obrany disponuje mnohými moderními metodami, má-li být konkrétně řízení rizik objektivním nástrojem sloužícím k usnadnění práce managementu, je nezbytné vnímat řízení rizik jako průběžnou činnost všech vedoucích zaměstnanců, spočívající ve včasné identifikaci a aktualizaci rizik, vhodném a objektivním nastavení stupně významnosti, monitoringu kontrolních mechanizmů, přijetí vhodných opatření, ve včasném předávání informací koordinátorovi rizik, včetně provádění komplexního vyhodnocování v návaznosti na konkrétní dění v organizaci.

„Řízení rizik není statistická činnost, ale průběžná komunikace uvnitř organizace.“

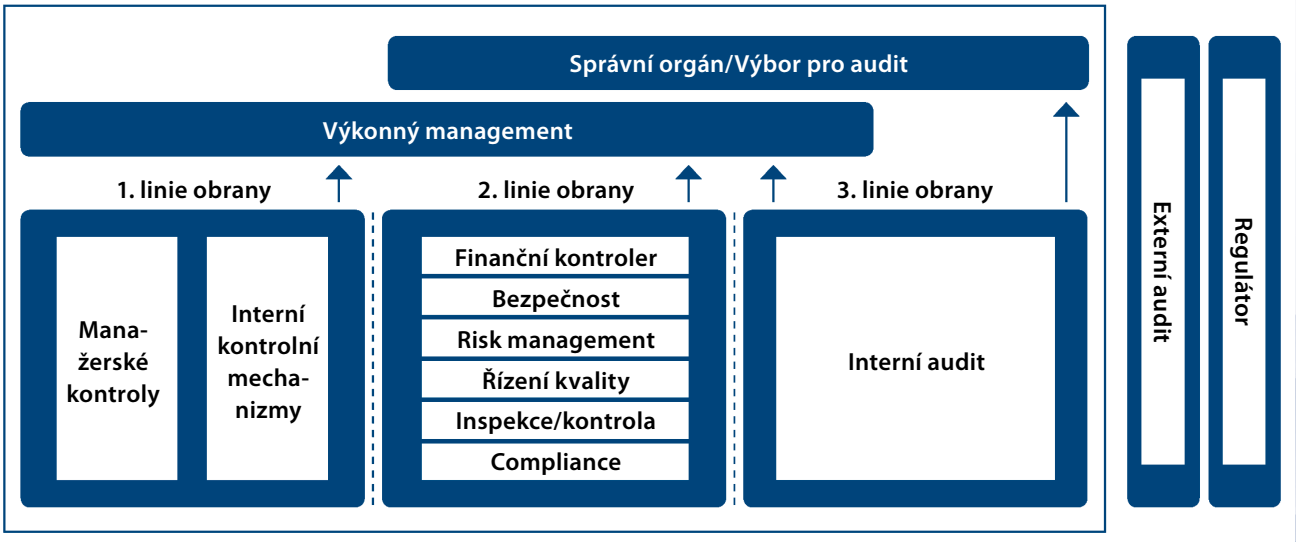
K tomu je nutné, aby všechny procesy při práci s riziky, byly vhodně nastaveny a výsledky dostatečně komunikovány. Pokud organizace sice zpracovává katalog rizik, pravidelně ho aktualizuje, statisticky ověřuje plnění opatření a číselně hodnotí významnost rizik, nedojde-li k důsledné komunikaci a přenesení informací do první linie, na management, stává se činnost pouze teoretickou a samotná organizace spíše „hasí“ okamžité problémy, než systémově využívá včasných varování prostřednictvím nashromážděných informací.

Linie obrany z pohledu státu

Ing. Ladislava Slancová
ředitelka odboru interního auditu,
Nejvyšší kontrolní úřad

Model tří linií obrany je velmi rozšířený, ale způsob, jakým je aplikován v jednotlivých organizacích, se liší. Při plnění úkolů zaměstnanci vstupují do vztahů, které se realizují množstvím procesů a podprocesů. Vlastník procesu je v první řadě zodpovědný za dosahování cílů, jeho rozvoj, popř. zlepšení, a současně musí podléhat kontrolám od osob na vyšším stupni řízení. Kontroly potom musí na sebe efektivně a kontinuálně navazovat, čímž by měl být zabezpečen vnitřní kontrolní systém. **Při implementaci by měl být nápomocný interní audit, který je rozhodující pro hodnocení nastaveného systému ve vztahu k navrhovaným doporučením, která vydává s ohledem na přínosy a náklady pro danou organizaci.**

Model systému tří linií obrany:
Zdroj: IIA Position Paper (2013): The three lines of defense in effective risk management and control



Pohled státu na linie obrany představuji pohledem Nejvyššího kontrolního úřadu (NKÚ) jako externí auditní instituce českého státu. A pokud se ptáte, proč zrovna pohledem této instituce, níže uvádím odpověď.

Zákon č. 166/1993 Sb., o Nejvyšším kontrolním úřadu, vstoupil v účinnost dnem 1. 7. 1993. Při jeho zpracování zákonodárce vycházel, jak uvádí důvodová zpráva: *„z demokratických principů výstavby státu a jeho nejvyšších orgánů, ze zkušeností při uskutečňování vrcholné kontroly v politicky a ekonomicky vyspělých státech a z tradic našeho zřízení.“*

„NKÚ jako externí auditní instituce státu má za úkol prověřovat účinnost interního auditu.“

Základním požadavkem bylo vytvoření takových podmínek, aby nově vznikající vrcholná kontrolní instituce byla schopna poskytovat nezávislé a odborné informace, které Parlament České republiky potřebuje pro plnění své kontrolní funkce ve vztahu k hospodaření s veřejnými prostředky státu.

Charakteristika NKÚ jako kontrolního orgánu znamená, že jeho úkolem je výkon kontroly, ale v právním řádu není NKÚ jediným kontrolním orgánem a jeho označení za „nejvyšší“ nelze vůči ostatním kontrolním orgánům považovat ve smyslu nadřízeného postavení.

NKÚ je nezávislý orgán. Je samostatnou státní institucí – není součástí ani moci zákonodárné, ani moci výkonné, ani moci soudní. Díky své nezávislosti je označován za „čtvrtý pilíř demokracie“ a je zřízen přímo Ústavou (hlava pátá, čl. 97). Požadavek nezávislosti NKÚ, jakož i jeho orgánů a členů, plyne z dokumentů INTOSAI[1], jež je nevládní organizací se zvláštním statutem při Hospodářské a sociální radě OSN, jejímiž členy jsou vrcholné orgány jednotlivých států s působností v oblasti kontroly hospodaření s veřejnými prostředky. Garanci takové nezávislosti pro nejvyšší kontrolní instituce („Supreme Audit Institution neboli SAIs“) požaduje ve své preambuli Limská deklarace směrnic o principech auditu, přijatá v říjnu 1977 na IX. Kongresu INTOSAI v Limě.

Od svého vzniku NKÚ přináší objektivní a nezávislý pohled na nakládání s veřejnými prostředky, které jsou kontrolovaným subjektům svěřeny státním rozpočtem a příslušnými zákony. NKÚ informuje o stavu dodržování právních předpisů a upozorňuje na případy nehospodárného, neúčelného či neefektivního hospodaření se státními prostředky, s cílem přispět ke zlepšení hospodaření státu jako celku.

„Interní audit je z pohledu státu nejdůležitějším partnerem pro externí audit – NKÚ.“

Jako dobrou praxi při výkonu kontroly uplatňuje NKÚ Mezinárodní standardy nejvyšších auditních institucí (ISSAI), přijaté INTOSAI.

1 Mezinárodní organizace nejvyšších kontrolních institucí, mezi jejíž členy patří mimo jiné většina evropských států, včetně České republiky.

Tyto standardy tvoří ucelený systém dokumentů ve čtyřech úrovních:

1. Limská deklarace směrnic o principech auditu (ISSAI 1), která tvoří základní úroveň stanovením zásad auditu ve veřejném sektoru;

2. dokumenty upravující základní předpoklady pro práci nejvyšších kontrolních institucí ve veřejném sektoru, k nimž patří mimo jiné Mexická deklarace o nezávislosti (ISSAI 10), principy nezávislosti (ISSAI 11), Principy transparentnosti (ISSAI 20), Etický kodex (ISSAI 30) a Kontrola kvality nejvyšších kontrolních institucí (ISSAI 40);

3. dokumenty obsahující principy výkonu kontrolní činnosti, jimiž jsou Audit veřejného sektoru (ISSAI 100), Finanční audit (ISSAI 200), Audit výkonnosti (ISSAI 300) a Audit shody (ISSAI 400);

4. metodické materiály (kontrolní či implementační směrnice) poskytující kontrolním institucím praktickou pomoc při zavádění standardů v jejich konkrétních podmínkách, a to pro audit finanční, audit výkonnosti a pro kontrolu legality.

Z třetí úrovně standardů INTOSAI vycházejí Kontrolní standardy NKÚ. Na organizační úrovni zahrnují požadavky na kontrolu veřejného sektoru, zatímco na úrovni jednotlivých kontrolních akcí je jejich účelem poskytovat kontrolujícím podporu při vývoji vlastního profesního přístupu v souladu s působností NKÚ a s právními předpisy. NKÚ uplatňuje tyto standardy z důvodu zajištění věrohodnosti, kvality a profesionální úrovně kontroly veřejného sektoru.
Limská deklarace směrnic o principech auditu **v Článku 3. Interní audit a externí audit** požaduje:

1. „Útvary interního auditu jsou zřizovány v rámci státních úřadů a institucí, kdežto orgány externího auditu nejsou součástí organizační struktury institucí, které mají být auditovány. Nejvyšší auditní instituce jsou orgány pro externí audit.

2. Útvary interního auditu jsou nutně podřízeny vedoucímu úřadu, v jehož rámci byly zřízeny. Mají však být v rámci příslušné organizační struktury funkčně a organizačně tak nezávislé, jak je to jen možné.

3. Jako externí auditor má nejvyšší auditní instituce za úkol prověřovat účinnost interního auditu. Jestliže je interní audit ohodnocen jako účinný, je potřebné dosáhnout co nejvhodnějšího rozdělení úkolů a vzájemné spolupráce mezi nejvyšší auditní institucí a útvarem interního auditu, aniž by tím bylo dotčeno právo nejvyšší auditní instituce provést celkový audit.“

NKÚ je tedy v rámci České republiky nejvyšší auditní institucí a je orgánem pro externí audit. **Jako externí auditor má nejvyšší auditní instituce za úkol prověřovat účinnost interního auditu.** Jestliže je **interní audit ohodnocen jako účinný, je potřebné dosáhnout co nejvhodnějšího rozdělení úkolů a vzájemné spolupráce mezi nejvyšší auditní institucí a útvarem interního auditu**, aniž by tím bylo dotčeno právo nejvyšší auditní instituce provést celkový audit. Úlohou NKÚ je mimo jiné i podpora a přispívání ke zlepšování účinnosti vnitřního kontrolního systému u orgánů veřejné správy a zhodnocení fungování vnitřního kontrolního systému jako celku.

Externí audit veřejného sektoru (státní audit) prováděný NKÚ rozvíjí integrální přístup ve svém rozsahu práce, což znamená poskytnutí osvědčení Parlamentu České republiky a občanům státu, že veřejné prostředky jsou využívány efektivně, účelně a hospodárně a že účetní závěrky a činnosti subjektů veřejného sektoru jsou v souladu s profesními a právními předpisy (důraz je kladen na audit shody a audit výkonu).

„V rámci vzájemné spolupráce interních auditorů a kontrolorů NKÚ dochází ke sdílení znalostí, k lepšímu porozumění rizikům kontrolované organizace a ke snížení překryvů činností.“

Interní audit uživatelů veřejných financí se kromě poskytování ujišťovacích činností stále více zaměřuje na poradenské služby s cílem poskytnout managementu podporu při zlepšování řízení veřejných zdrojů a rizik, efektivnosti vynakládání veřejných prostředků a poskytování kvalitních veřejných služeb. **Jako „třetí linie“ ujištění, interní audit hodnotí správné fungování systémů kontrolujících rizika, které byly implementovány „první linií“, ale také způsob fungování monitorovacích funkcí ve „druhé linii“.**

Ze zásad a postupů doporučených *Mezinárodními standardy nejvyšších kontrolních institucí* (ISSAI) a *Kontrolními standardy NKÚ*, vyplývá, že vyhodnocení vnitřního kontrolního systému by mělo být součástí první fáze kontrolní akce, tj. přípravy kontroly. Kontrolující posoudí, jaký vliv může mít vnitřní kontrolní systém kontrolované osoby na předmět jím prováděné kontroly, a vyhodnotí vnitřní kontrolní systém v příslušném rozsahu tak, aby mohl provést počáteční vyhodnocení kontrolního rizika spojeného s kontrolovanou činností a navrhnout rozsah a strukturu dalších postupů kontroly.

Jestliže tedy vezmeme v úvahu specifický rozsah a cíle externího a interního auditu, je důležitá jejich vzájemná odpovídající a účinná koordinace, aby nedocházelo k duplikacím a vzájemné využití výstupů obou subjektů bylo optimální. **Účinný interní audit tedy umožňuje NKÚ věnovat pozornost oblastem, které nebyly předmětem interního auditu.** V rámci vzájemné spolupráce interních auditorů a kontrolorů NKÚ dochází ke sdílení znalostí, k lepšímu porozumění rizikům kontrolované organizace a ke snížení překryvů činností.

„Využívejme potenciál ‚třetí linie obrany – interního auditu' s dopadem na správu veřejných prostředků a kontrolu hospodaření s nimi."

Vnitřní kontrolní systém v rámci jednotlivých organizací by měl zabezpečit tři hlavní pilíře, **z nichž tedy interní audit je z pohledu státu nejdůležitějším partnerem pro externí audit – Nejvyšší kontrolní úřad.** I když mají různé a jasně definované role, obecným účelem externího a interního auditu ve veřejném sektoru je přispívat k řádnému řízení veřejných financí, to znamená k efektivitě, účelnosti a hospodárnosti daného státu. ■

Schéma: Systém standardů ISSAI

Úroveň 1 – Základní principy	**Úroveň 2** – Předpoklady pro fungování SAI	**Úroveň 3** – Principy pro výkon kontrolní činnosti	**Úroveň 4** – Kontrolní směrnice
ISSAI 1 Limská deklarace	ISSAI 10 Mexická deklarace ISSAI 11 Principy nezávislosti ISSAI 12 Význam a přínosy SAIs ISSAI 20 Principy transparentnosti ISSAI 21 ISSAI 30 Etický kodex ISSAI 40 Kontrola kvality SAI	ISSAI 100 Audit veřejného sektoru ISSAI 200 Finanční audit ISSAI 300 Audit výkonnosti ISSAI 400 Audit shody	ISSAI 1000–2999 pro finanční audit ISSAI 3000–3999 pro audit výkonnosti ISSAI 4000–4999 pro kontrolu legality

PROPOJOVÁNÍ PILÍŘŮ OBRANY V PRAXI

Spojování činností patřících do různých pilířů léta tesaného tříliniového systému obrany vnímáme ve světě interního auditu zejména v posledních letech jako velké téma. Nejprve se spojování takových činností zdálo prakticky nepřekročitelné, později směřujíc k novému standardu mezinárodního rámce profesní praxe interního auditu 1112 jako možná až kontroverzní, a v poslední době naopak snad až jako velká příležitost pro rozšiřování našich zájmů. Jedná se tedy o otázku, ve které pravděpodobně teprve až dobrá praxe ukáže, kde jsou hlavní úskalí, anebo výhody.

Mgr. Filip Zelingr
výkonný ředitel, audit, řízení rizik, compliance
Letiště Praha, a.s.

Další úvahy vychází tedy zejména z naší osobní letité zkušenosti s budováním a provozováním tzv. ARC útvaru, který od již roku 2014 „pod jednou střechou“ spojuje útvary interního auditu, řízení rizik a compliance, včetně prevence nekalých jednání. Při budování našeho ARC modelu kooperace útvarů 2. a 3. pilíře obrany jsme vycházeli z domněnky, že vhodným propojením činností těchto složek lze výrazně posílit efektivitu vnitřního kontrolního systému, aniž by byla narušena nezávislost a objektivita interního auditu.

VÝCHODISKA ÚSPĚCHU

Je nutné si uvědomit, že každá společnost je jiná tím, že její činnost a procesy reflektují například oborová specifika, legislativní či regulatorní rámec, velikost firmy či vliv mateřské nebo jiné spřízněné společnosti. Sada klíčových kritérií pro vyhodnocování očekávané přidané hodnoty spojení prvků 2. a 3. pilíře se tedy pravděpodobně velmi různí. Aby bylo takové spojení nejen v souladu se standardy, ale zároveň přinášelo dostatečnou přidanou hodnotu, považujeme z vlastní zkušenosti za klíčové se již při přípravě důkladně zamýšlet nad následujícími oblastmi.

Předpoklady IPPF standardu 1112

Nezbytným předpokladem je zamezení možného střetu zájmů vedoucího interního auditu (CAE), a tedy zajištění jeho nezávislosti a objektivity. Při výkonu jiných než auditních činností se totiž podílí na řízení provozních či kontrolních činností, které na rozdíl od interního auditu funkčně podléhají exekutivnímu managementu společnosti. Ačkoliv při vzniku ARC byl standard 1112 ještě tzv. v plenkách, došli jsme v diskuzích s vedením společnosti k následujícím opatřením, která později vydanému standardu vyhověla:

- Činnosti compliance a řízení rizik jsou zcela mimo rámec interního auditu a v případě potřeby auditního ujištění si orgány společnosti tuto činnost zajišťují externě.
- Odpovědnosti a pravomoci vedoucího interního auditu pro oblast interního auditu jsou odlišné od compliance a řízení

rizik a jsou separátně stanoveny ve statutu ARC, který je pravidelně revidován.
- Stav činností compliance a řízení rizik, hodnota a stav rizik vyplývajících z jejich činností je projednávána dedikovaným výborem za účasti vedení společnosti.
- Nad všemi činnostmi ARC, včetně interního auditu, probíhá navíc pravidelná dohledová činnost ze strany orgánů společnosti, včetně výboru po audit.

„Nezbytným předpokladem je zamezení možného střetu zájmů vedoucího interního auditu (CAE), a tedy zajištění jeho nezávislosti a objektivity.“

Funkčnost výše uvedených opatření byla v nedávné době potvrzena i nezávislým externím hodnocením kvality interního auditu (QAR) se závěrem, že činnost interního auditu je plně v souladu s Mezinárodními standardy pro profesní praxi interního auditu.

Kvalifikace CAE

Dalším předpokladem je naplnění očekávání standardu, že CAE dostatečně zná a pochopí činnosti mimo interní audit, aby dokázal dostatečně vyhodnotit rizika spojená s možným střetem zájmů. Mimo požadavky standardu by měl ovšem CAE také disponovat potřebnými znalostmi, a především zkušenostmi ve všech oblastech, které zastřešuje. Nemělo by se však jednat o pouhé formální převzetí oblastí s dedikovanými specialisty. CAE by měl totiž naopak být díky své praxi ve všech oblastech schopen maximalizovat možné metodické i provozní synergie.

Pochopení rolí 2. linie obrany

Pochopení rolí 1. linie obrany bývá poměrně jednoduché. Správné pochopení 2. linie obrany však může být složitější. Často je zjednodušeně označována jako dohledová, tj. s cílem zajišťovat, že v rámci 1. linie jsou zavedeny odpovídající procesy řízení rizika a procesy jsou účinné. Ve skutečnosti je však náplň 2. linie obrany mnohem různorodější, a navíc obvykle odlišná v každé společnosti. Často se tak v činnostech 2. linie promítají jak prvky z 1. linie (např. tvorba či adopce metodiky, prvky samotného výkonu, operativní či manažerské kontroly), tak prvky 3. linie (např. různé formy auditů shody často vyplývajících ze systémů kvality řízení). Důsledné pochopení specifik jednotlivých částí 2. pilíře je pak při propojování s 3. pilířem klíčové k hledání a následnému využití všech synergií obou pilířů.

Vztah s managementem

V neposlední řadě je nutné, aby si orgány společnosti byly vědomy cíle, kterého tímto spojením chtějí dosáhnout, včetně výhod i omezení, které s sebou spojení nese. Motivací dlouhodobého koncepčního řešení by tedy mělo být především zvyšování přidané hodnoty, nikoliv pouze řešení personálních otázek. Tak tomu bylo i v naší společnosti, kde spojení interního auditu, řízení rizik a compliance bylo taženo nejen potřebou pokrytí konkrétních oblastí, ale i sjednocením a posílením celého VKS.

SPOJENÍ V PRAXI

Každý prvek VKS má ve společnosti své místo a postavení, každý používá svou metodiku a postupy. Primární smysl všech těchto procesů je však stejný, a to podporovat vedení při řízení společnosti na vytyčené cestě. V našem případě jsme implementaci realizovali ve společnosti, která je silně regulována řadou národních i mezinárodních pravidel a řízení regulatorních rizik je automatickou a léty ověřenou součástí. Toto prostředí s sebou přináší jejich kvalitní řízení, ale na druhé straně i mnoho druhopilířových procesů a útvarů, které se všechny zabývají jejich prevencí a řízením. Setkávali jsme se tak s řadou různých jazyků, kterými o rizicích mluví, hodnotí je a reportují o nich.

Jak je již uvedeno výše, založili jsme tedy útvar ARC, kde CAE kromě auditu řídí i compliance, prevenci nekalých jednání a korporátní řízení rizik.

S ohledem na cíl sjednocení VKS jsme vytvořili společnou metodiku řízení rizik a jednotný informační systém, díky kterým došlo i k propojení s dalšími druhopilířovými útvary. Přidanou hodnotu spolupráce tedy nespatřujeme pouze v organizačním spojení ARC, ale i synergických efektech propojování jednotlivých pilířů VKS, jako např.:

Ošetření rizika podvodů

Standard 2120.A2 dává internímu auditu povinnost hodnotit možnost výskytu podvodu a způsob, jakým společnost řídí riziko podvodu. Díky vzájemnému sdílení informací o těchto rizicích i výstupech jednotlivých šetření interní audit například v každé zakázce poměrně snadno tato rizika hodnotí. Významně flexibilní je i sdílení know-how například formou spolupráce s compliance specialisty, se kterými interní audit diskutuje konkrétní podoby rizika podvodů, jeho možné dopady a případně v testovací fázi detailně ověřuje podvodné aspekty auditovaných procesů. Tato spolupráce na jedné straně pomáhá compliance s pochopením rizika podvodů v širším kontextu ověřovaných procesů, o kterých má interní audit detailní povědomí, a auditu naopak umožňuje flexibilní rozšíření kapacit zakázky a vyšší specializaci, což má pozitivní dopad na kvalitu hodnocení a doporučení v této oblasti.

„Pochopení rolí 1. linie obrany bývá poměrně jednoduché. Správné pochopení 2. linie obrany však může být složitější.“

Datové analýzy

Ačkoliv jsme poměrně velká společnost, nevyužili bychom v každém týmu dedikované odborníky v oblasti datových analýz. Sdílené využití kapacit datových analytiků ARC umožňuje provádět např. vybrané auditní testy na celé populaci, nikoli pouze na vzorku, a zesiluje tak vypovídací schopnost auditních závěrů – ať už ve formě ujištění, tak zjištění o nedostatcích. Prezentace výsledků na datových řezech z různých pohledů auditovaných procesů pomáhá i srozumitelnosti těchto závěrů pro management společnosti. Podobné synergické efekty jsou realizovány i v týmech řízení rizik i compliance.

Kontinuálního monitoringu

Jedním z posledních trendů je za pomocí softwarových nástrojů sledovat kvalitu a výkonnost procesů v reálném čase na 100 % vybraných činností. V naší praxi se jedná o informace, které průběžně zpracovávají a dále analyzují týmy řízení rizik a compliance. Jde především o výstupy tzv. „early warning systému“, ve kterém compliance provádí automatizované datové kontroly například nad riziky podvodných jednání, nebo evidenci incidentů, které vlastníci rizik zaznamenávají v systému řízení rizik. Interní audit, na základě výsledků takových kontrol, zejména ve 2. pilíři, identifikuje možná rizika, případně vyhodnocuje potřebu mimořádného nebo plánovaného auditu.

Dynamického řízení rizik

Vzájemná spolupráce všech útvarů používajících stejnou metodiku k hodnocení rizik přispívá k aktuálním informacím o rizicích a stavu jejich řízení. Jedná se jak o průběžnou aktualizaci rizik v návaznosti na provedené interní audity a compliance šetření, tak o auditní vyhodnocování mimořádných událostí řešených týmy compliance i řízení rizik. Zároveň to umožňuje managementu společnosti pracovat se vždy aktuální a integrovanou informací poskytovanou ve stejné metrice, např. formou reportu, který v každém daném okamžiku poskytuje aktuální informaci o rizikové expozici jediného procesu či celé společnosti.

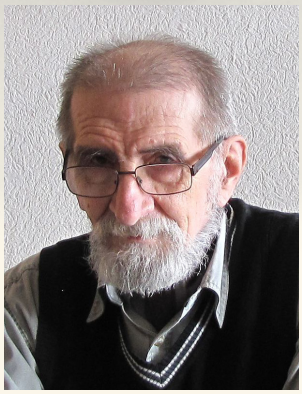
ZÁVĚREM

Věříme, že spojením vybraných prvků jednotlivých pilířů v našem případě došlo k výraznému posílení VKS, a to nejen z pohledu interního auditu, ale i jednotlivých útvarů ostatních pilířů VKS. Posílení vidíme nejen v samotné efektivitě jejich výstupů, ale i srozumitelnosti VKS pro management díky srovnatelnému hodnocení rizik. Zároveň nedošlo k žádnému narušení nezávislosti či objektivity interního auditu, což bylo potvrzeno i nezávislým posouzením kvality interního auditu, uvedeným výše.

Ačkoliv se může zdát, že spojení činností jednotlivých pilířů je prakticky bez omezení a univerzální, není tomu tak. Věříme jednak, že je nutné zvažovat otázky, jaké jsme si vytyčili jako východiska úspěchu, ale i zvažovat omezení, která spojení přináší. Konkrétně lze říci, že míra zefektivnění VKS musí být větší než míra omezení míry pokrytí společnosti interním auditem. V extrémním případě by totiž klidně mohlo dojít k integraci celého 2. pilíře pod vedením CAE, ten by však musel celý interní audit outsourcovat. ■

Filip Zelingr a kolektiv autorů ARC

Neponechávat mezery a předcházet duplicitám



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

„Metafora o třech liniích by v nás ale neměla vyvolávat představy o parkánových hradbách, vodních příkopech a padacích mostech.“

Jeden někdejší manažer po letech úspěšné kariéry zažil poměrně strmý pád nejen na profesním žebříčku. Byl nakonec odkázán na zaměstnávání ve značně neatraktivních pozicích a při snaze zůstat v jakž takž důstojné pozici vůči svému synovi, který byl právě na vzestupné cestě své kariéry, rozšafně přemítal o tom, jakou úlohu mají ve výchově a v životě vůbec povzbudivé, a naopak odstrašující příklady. „Ty dobré příklady sice táhnou, ale ne moc silně. Jsou na nich přitažlivé ty výsledky, ale ne tak už ten každodenní obsah. Soustavnost, ukázněnost, ostražitost a nekonečná pracovitost. Oproti tomu příklady odstrašující – jako ten můj – mají šanci působit daleko výchovněji. Poskytují silnou motivaci k tomu, aby se člověk ‚udržel v lajně‘ a předcházel těm nesčetným příležitostem ke kopancům vedoucím k úpadku.“

Čas od času se mi mudrování starého přítele živě připomene. Nemusí to být jen u osobních příběhů. Také organizace mívají své rozmanitě dramatické osudy úspěchů a pádů. Vezměme jen namátkou pár klíčových slov od 90. let: Cadburyho zpráva, COSO model, Baring Bank, Turnbullova zpráva, Enron, Sarbans-Oxley, Lehman Brothers – „díky“ ponaučením z těchto varovných příběhů a na ně navazujících zpráv jsme nabyli mnoha daleko působivějších poznatků, než bychom získali obdivným (ale poklidným) seznamováním se s perfektním chodem úspěšných firem. Přirozeně by bylo neblahé, kdyby si někdo poslední věty vykládal v tom smyslu, že podceňuji vzdělávání a výměnu poznatků o osvědčené praxi. Rád bych právě naopak zdůraznil, že příklady osvědčené praxe daleko výrazněji vyniknou na pozadí obeznámenosti s oněmi

případy odstrašujícími. Nemálo let opakujeme mantru o ***risk based auditing***, tj. o auditu založenému na znalostech o příslušných rizicích – a ta se nejzřetelněji ukazují na případových studiích podobných událostí, jaké byly zmíněny výše. Koneckonců jeden z nejpřínosnějších vývojových modelů řádné správy a řízení organizací, tzv. COSO model, má ve svých obou výkladových rámcích (Integrovaný rámec vnitřního řízení a kontroly, pět komponent; a Řízení podnikových rizik, osm komponent) klíčové popisy komponent věnovaných riziku.

„To, že je pozice IA nazývána ‚třetí', neznamená časovou posloupnost, není tu žádné ‚předtím' nebo ‚potom', ‚venku' nebo ‚uvnitř'."

Také poziční dokument IIA ke třem liniím obrany[1] zdůrazňuje orientaci na rizika až do takové míry, že hlavní činitele jednotlivých linií charakterizuje v tabulce na str. 6 jako: 1. vlastníci rizik; 2. zvládání rizik; 3. ujištění o riziku. Překlad těchto výrazů může být diskutabilní, avšak odlišnost činitelů v jednotlivých liniích obrany je vcelku zřejmá a z ostatního textu pozičního dokumentu dobře srozumitelná. Metafora o třech liniích by v nás ale neměla vyvolávat představy o parkánových hradbách, vodních příkopech a padacích mostech. Není tomu tak, že by „třetí linie" – tedy interní audit – zůstávala jako poslední útočiště obránců poté, až potencionální „nepřítel" zdolá obě linie předcházející. V našem případě by měla být obranná strategie v určitém ohledu obrácená. Ten, kdo celkovou obranu rozvrhuje, musí počítat s co možná dokonalou znalostí terénu, silnými stránkami protivníka a možnými taktickými nástrahami, jakých by mohlo být využito v náš neprospěch. A pro potřebu takové obeznámenosti je nezbytné poskytovat k budování a trvalému udržování obrany co nejdokonalejší systém účinného zpravodajství o obecných ohrožených i o aktuální situaci právě jednajících činitelů. To, že je pozice IA nazývána „třetí", neznamená časovou posloupnost, není tu žádné „předtím" nebo „potom", „venku" nebo „uvnitř". Rizika jsou působící stále a vně i uvnitř. A v tomto ohledu je tak důležitá přiměřená oddělenost „třetí linie" od těch ostatních. Aby mohla naplňovat to, co se od ní očekává, musí být při vší své propojenosti s celým systémem nezávislá na těch, o jejichž funkční způsobilosti má poskytovat ujištění.

Výše zmiňovaný poziční dokument IIA o třech liniích obrany z roku 2013 při znázornění žádoucího modelu vychází ze staršího dokumentu připraveného ve spolupráci FERMA (Federace evropských sdružení pro řízení rizik) a ECIIA (Evropská konfederace institutů interního auditu) již v roce 2010[2]. Ten je pod názvem „Monitorování účinnosti vnitřního řízení a kontroly, interního auditu a systémů řízení rizik" označen jako **Příručka pro řídicí orgány a výbory pro audit**. Poziční dokument IIA pak pod schématem modelu výslovně uvádí: „Ačkoli ani řídicí orgány, ani vrcholový management nejsou do modelu tří linií obrany zahrnuty, nelze hovořit o celkovém systému řízení rizik, aniž bychom nejprve vzali v úvahu naprosto zásadní úlohu obou orgánů vrcholné správy (tj. řídicí orgány jako představenstvo nebo odpovídající orgán) a vrcholový management. Ty představují prvotní zainteresované partnery spolupůsobící s „liniemi" – a jsou v nejlepším postavení, aby pomáhaly zajistit náležité uplatnění a rozvržení modelu tří linií obrany ve struktuře procesů řízení rizik a ovládacích prvků v organizaci. Řídicí orgány a vrcholové vedení mají kolektivní odpovědnost a musí skládat účty ohledně nastavení cílů organizace, definování strategií k dosahování těchto cílů a ustavení struktur a postupů, jak nejlépe zvládat rizika při dosahování oněch cílů. Model tří linií obrany je nejlépe uplatněn s aktivní podporou a vůdčí účastí řídicích orgánů a vrcholového vedení organizace."

„Model tří linií obrany je nejlépe uplatněn s aktivní podporou a vůdčí účastí řídících orgánů a vrcholového vedení organizace."

Pokud dnes diskutujeme o místu a roli interního auditu, odborná diskuze by nejspíš měla vycházet z principiální shody nad modelem a dalším vývojem jeho aplikací, jak lze mj. sledovat na webovém portále www.ferma.eu. Hlavním dějištěm takových diskuzí by však měl být trvalý dialog o účinnosti příslušných liní obrany mezi vedením útvarů interního auditu a vrcholovými orgány správy dané organizace. ■

1 IIA Position Paper: THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL, JANUARY 2013

2 Guidance on the 8th EU Company Law Directive, article 41, FERMA–ECIIA, Brussels 2010, 19 s.

Vývoj finančního sektoru v ČR a makroobezřetnostní politika ČNB ve světle současného ekonomického vývoje

Libor Holub
náměstek ředitele sekce finanční stability
Česká národní banka

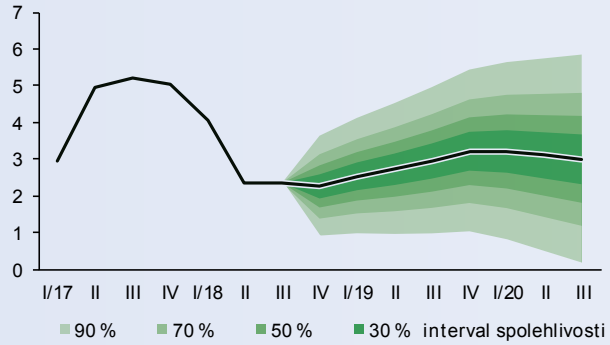
K auditorské profesi mám velice blízko, v archivu auditorský dekret (č. 1165) a během dlouholeté praxe převážně ve finančním řízení průmyslového podniku či banky jsem pravidelně a intenzivně spolupracoval s externími i interními auditory. Velice si vážím jejich práce, která napomáhá k efektivnímu fungování tržní ekonomiky a kultivaci řízení soukromých i státních institucí.

Růst domácí ekonomiky se bude pohybovat blízko 3 %

Robustní růst HDP (graf 1) z minulých let by měl pro letošní a příští rok podle únorové prognózy ČNB[1] zvolnit na úroveň blízko 3 %. Inflace se bude v letošním roce pohybovat poblíž 2% cíle a klíčová měnově-politická úroková sazba (dvoutýdenní repo sazba; 1,75 % od 20. 12. 2018) by neměla doznat významných změn.

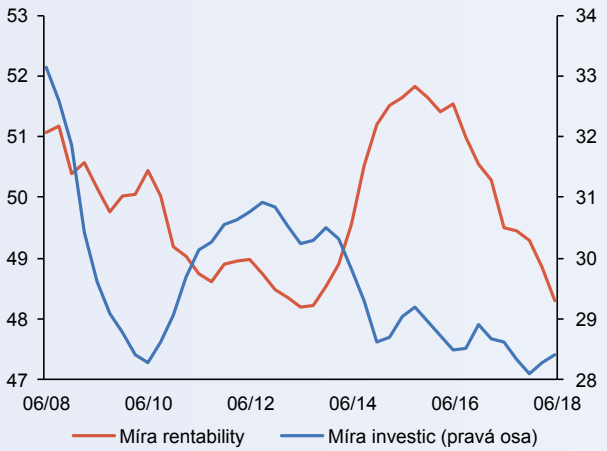
Růst domácí ekonomiky se projevuje napětím na trhu práce. Výrazně rostou reálné příjmy domácností a v návaznosti na to jejich spotřeba i investice (hypotéky, investiční fondy). Zároveň dochází k posilování optimistických očekávání ohledně budoucího vývoje příjmů. Mzdové tlaky se však současně projevují ve vysokém tempu růstu nákladů sektoru nefinančních podniků, a působí tak na snižování jejich ziskovosti (graf 2).

Graf 1
Prognóza růstu HDP
(meziroční změny v %, sezonně očištěno)



Poznámka: Intervaly spolehlivosti prognózy růstu HDP odrážejí predikční schopnost minulých prognóz. Jsou symetrické a lineárně se rozšiřující.

Graf 2
Míra rentability a míra investic v sektoru nefinančních podniků
(v % hrubé přidané hodnoty)



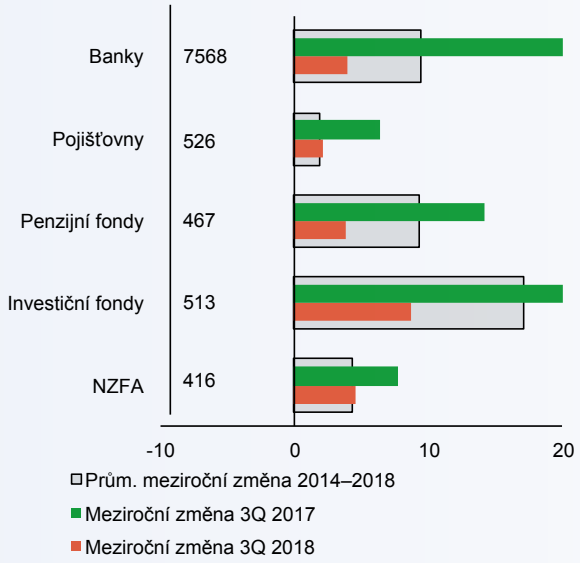
Pramen: ČSÚ
Pozn.: Míra rentability představuje hrubý provozní přebytek k hrubé přidané hodnotě sektoru. Míra investic odpovídá tvorbě hrubého fixního kapitálu k hrubé přidané hodnotě sektoru. Počítáno z ročních klouzavých úhrnů.

1 Prognóza ČNB z února 2019, blíže viz Zpráva o inflaci I/2019), http://www.cnb.cz/cs/menova_politika/zpravy_o_inflaci/2019/2019_I/index.html.

Příznivá makroekonomická situace se promítá i do vývoje ve finančním sektoru…

Objem aktiv spravovaný finančním sektorem roste ve všech jeho částech, nejdynamičtěji potom u investičních fondů (graf 3). Spolu s penzijními fondy se tak stávají stále významnějšími jako správci a uchovatelé hodnoty části úspor obyvatelstva, jejich dlouhodobé úsporné složky.

Graf 3
Dynamika růstu jednotlivých segmentů finančního sektoru
(v %, k 3Q 2018)



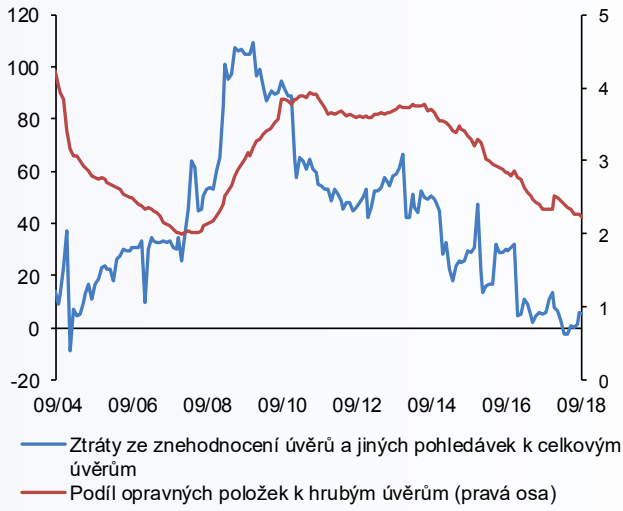
Pramen: ČNB

Bankovní sektor jako nejvýznamnější součást domácího finančního systému (80 % aktiv) vykázal za rok 2018 historicky absolutně nejvyšší úroveň zisku. Příznivě působil růst objemu úvěrů, současně vnímané nízké očekávané ztráty úvěrového portfolia[2] (graf 4), udržování relativně nízké nákladovosti (cost/income, průměr ČR 47 %, EU 63 %) a růst úvěrových marží související též s postupným zvyšováním úrokových sazeb ČNB.

…a přispívá k posunu v růstové fázi finančního cyklu

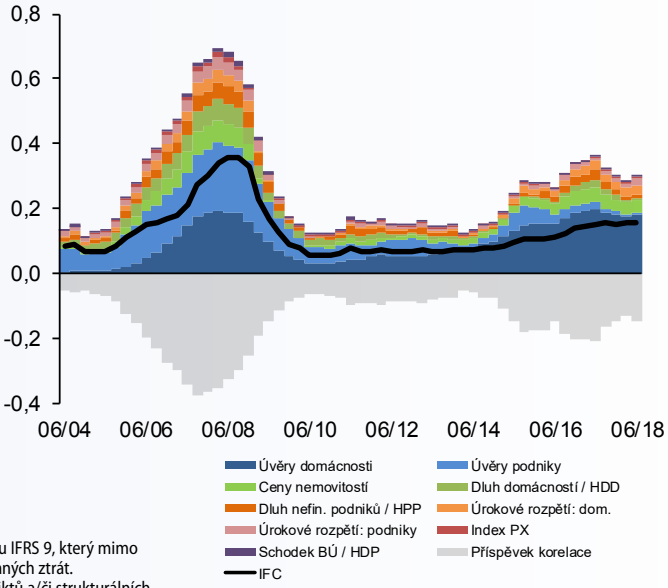
Domácí ekonomika se v minulém roce posunula dále v růstové fázi finančního cyklu (graf 5), což přispívá ke zvýšení zranitelnosti bankovního sektoru vůči případnému zhoršení ekonomického vývoje v budoucnu.[3]

Graf 4
Ztráty ze znehodnocení aktiv a opravné položky k úvěrům
(v b.b.; pravá osa: v %)



Pramen: ČNB

Graf 5
Indikátor finančního cyklu (IFC) a jeho rozklad na složky
(0 minimum, 1 maximum)



Pramen: ČNB, ČSÚ
Pozn.: HDD značí disponibilní důchod domácností, HPP označuje hrubý provozní přebytek nefinančních podniků. Úrokové rozpětí je rozdíl mezi klientskou sazbou na nové úvěry a sazbou 3M PRIBOR. Negativní příspěvek korelační struktury k hodnotě indikátoru IFC (ztráta vlivem nedokonalé korelace subindikátorů) je dán rozdílem mezi jeho aktuální hodnotou a horní mezí, která předpokládá perfektní korelaci mezi všemi indikátory. Slabá korelace mezi subindikátory se projevuje nárůstem negativního příspěvku k celkové hodnotě IFC.

2 Jejich současnou výši podstatně neovlivnilo ani zavedení nového účetního standardu IFRS 9, který mimo jiné nově upravuje účtování o úvěrových ztrátách a je založený na konceptu očekávaných ztrát.
3 Zhoršení může být mimo jiné důsledkem eskalace mezinárodních obchodních konfliktů a/či strukturálních změn v některých odvětvích, které mají významný vliv na tvorbu HDP v české ekonomice.

K tomuto posunu napomáhají finanční podmínky, které zůstávají i přes postupný nárůst úrokových sazeb i nadále uvolněné.[4]
Optimistická očekávání ohledně budoucího vývoje příjmů a cen aktiv podporují svižnou úvěrovou dynamiku. Ceny bydlení přes zvolnění tempa růstu úvěrů nadále rostou a zůstávají podle odhadu ČNB nadhodnocené. Mimořádně nízké ztráty ze znehodnocení aktiv bank nejsou z dlouhodobého hlediska udržitelné, cyklicky podmíněný je i pokles rizikových vah, a tedy relativně nižší potřebná výše kapitálu u některých typů úvěrů.

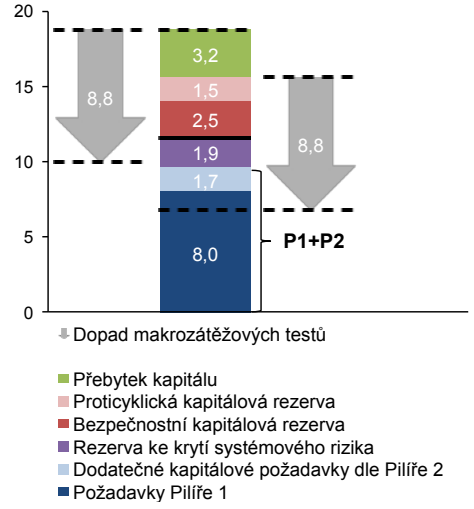
Banky i pojišťovny, které tvoří hlavní části finančního systému, zůstávají i nadále vysoce odolné vůči případným nepříznivým šokům

ČNB pravidelně posuzuje odolnost jednotlivých částí finančního systému, resp. jejich schopnost v případě nepříznivého ekonomického vývoje i nadále poskytovat bez podstatných omezení příslušné služby (úvěry, vklady, pojištění, investiční služby). Odolnost je testována za využití tzv. hypotetického nepříznivého scénáře, který by měl být nastaven dostatečně přísně, avšak realisticky. Výsledky zátěžových testů bank a pojišťoven ukazují, že i v případě naplnění nepříznivého scénáře zůstávají banky i pojišťovny dostatečně kapitalizované a jako celek naplňují minimální regulatorní kapitálové požadavky (banky, graf 6).[5] Odolnost bank je významně podmíněna výší jejich kapitálového přebytku a velikostí požadovaných kapitálových rezerv, které jsou proto jedním z významných nástrojů makroobezřetnostní politiky ČNB.

ČNB reaguje na cyklická rizika v bankovním sektoru stanovením proticyklické kapitálové rezervy

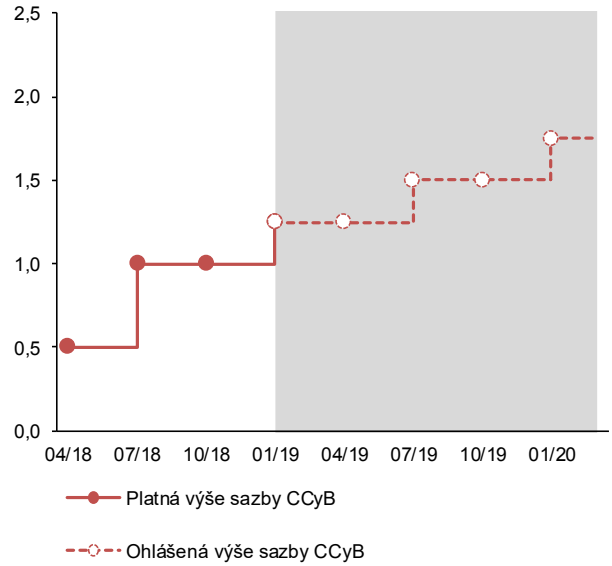
Proticyklická kapitálová rezerva (CCyB) zajišťuje, aby úvěrová rizika nahromaděná v příznivé fázi finančního cyklu byla dostatečně kryta kapitálem a banky mohly i v nepříznivé fázi cyklu poskytovat úvěry bonitním soukromým nefinančním podnikům a domácnostem. Sazbu proticyklické kapitálové rezervy ČNB v posledních více než třech letech zvyšovala postupně. V současnosti činí 1,25 % z objemu rizikově vážených aktiv a od 1. ledna 2020 by měla činit 1,75 % (graf 7). Stanovení sazby proticyklické kapitálové rezervy nevedlo u převážné většiny bank k potřebě navýšení kapitálu, k jejímu pokrytí využily existujícího přebytku kapitálu drženého nad celkovými kapitálovými požadavky (graf 6, zelená složka). ČNB je připravena rezervu neprodleně rozpustit, pokud by došlo k nepříznivému ekonomickému vývoji, který by se přenesl do zhoršení kapitálových poměrů bankovního sektoru. Obdobnou roli jako proticyklická kapitálová rezerva plní také bezpečnostní kapitálová rezerva, která je však regulatorně určena v trvale pevné výši 2,5 % z rizikově vážených aktiv a její dodržování je povinné od roku 2014.

Graf 6
Struktura kapitálových požadavků bank v ČR a dopad makrozátěžových testů s 5letým horizontem
(průměr za sektor ke třetímu čtvrtletí 2018 v p.b.)



Pramen: ČNB
Pozn.: Ilustrace předpokládá aktuálně platnou plnou výši proticyklické rezervy, ač je platná až od poloviny roku 2019.

Graf 7
Aktuálně platná a ohlášená výše sazby CCyB v ČR
(v % celkového objemu rizikové expozice)



Pramen: ČNB

4 Úrokové sazby zůstávají pod svou dlouhodobou neutrální úrovní.
5 5letý makrozátěžový test bank prováděný na datech k 30.9.2018 zveřejněný v publikaci ČNB Rizika pro finanční stabilitu a jejich indikátory – prosinec 2018, blíže http://www.cnb.cz/cs/financni_stabilita/zatezove_testy/zatezove_testy_bankovni_sektor.html.

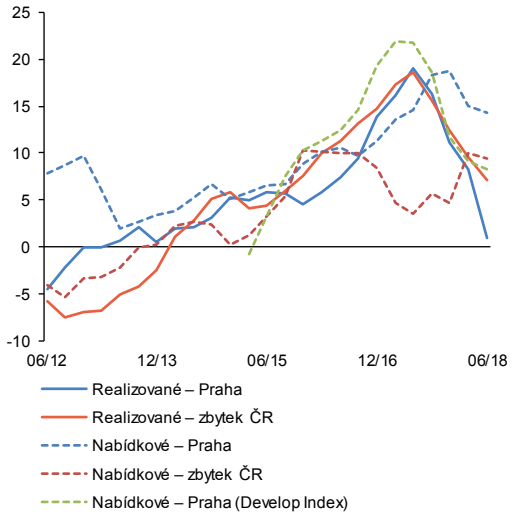
Odolnost systémově významných bank podporuje také kapitálová rezerva ke krytí systémového rizika

Páteř domácího finančního systému tvoří systémově významné banky a jiné systémově významné instituce. Pět největších systémově významných bank je povinno udržovat kapitálovou rezervu ke krytí systémového rizika ve výši 1–3 % ze svých rizikově vážených aktiv (Česká spořitelna, ČSOB, Komerční banka 3 %, Raiffeisenbank 1 % a UnicreditBank 2 %). ČNB přezkoumává seznam systémově významných bank i výši rezervy nejméně jednou za dva roky. Účelem této kapitálové rezervy je podpořit stabilitu fungování rozhodující části bankovního sektoru v případě systémových poruch ve fungování domácí ekonomiky. Společně s tím ČNB každoročně určuje seznam jiných systémově významných institucí, kterých je v současnosti sedm (vedle skupin systémově významných bank se jedná také o skupinu PPF a J&T), nicméně pro ně nyní z tohoto titulu nestanovuje kapitálovou rezervu.

Na rizika spojená s úvěrovým financováním bydlení reaguje ČNB stanovením horních hranic ukazatelů LTV, DTI a DSTI pro všechny poskytovatele hypotečních úvěrů

Déletrvající růst cen nemovitostí (graf 8) projevující se v jejich nadhodnocení a zhoršení příjmové dostupnosti[6], vytváří podmínky pro růst systémových rizik spojených s trhem rezidenčních nemovitostí a úvěry na bydlení. Svoji roli hrají i uvolněné finanční podmínky a vysoká tržní konkurence.

Graf 8
Růst realizovaných a nabídkových cen bytů
(meziroční růst v %)



Pramen: ČSÚ, Cenová mapa/Deloitte
Pozn.: Realizované ceny podle výběrového šetření starších bytů ČSÚ. Z důvodu publikování Develop Indexu ve dvouměsíční frekvenci jsou údaje za březen a září získány jako průměr meziročního růstu v únoru a dubnu, resp. v srpnu a říjnu.

Východiskem k omezování rizik je sada pravidel obsažená v úředním sdělení ČNB *Doporučení k řízení rizik spojených s poskytováním retailových úvěrů zajištěných rezidenční nemovitostí* (dále jen Doporučení)[7], poprvé zveřejněném v roce 2015 (LTV) a aktualizovaném v letech 2016 (LTV), 2017 (LTV) a 2018 (DTI, DSTI). Vedle řady kvalitativních doporučení v oblasti řízení úvěrového rizika stanovuje zejména limity pro horní hranice ukazatelů, které jsou v současnosti stanoveny takto:

- poměr úvěru k hodnotě nemovitosti (LTV, graf 9) – max. 90 %, mezi 80–90 % – max. 15 % produkce
- poměr hodnoty všech úvěrů k výši příjmů po zdanění (DTI, graf 10[8]) – max. 45 % a
- poměr hodnoty splátek všech úvěrů k výši příjmů po zdanění (DSTI, graf 11) – max. 9.

Stanovené limity přispívají ke snížení zranitelnosti poskytovatelů úvěrů (snižují úvěrové ztráty při selhání dlužníka), ale i dlužníků (snižují riziko nadměrného zadlužení a dluhové služby) v případě nepříznivého ekonomického vývoje doprovázeného poklesem cen nemovitostí (LTV, graf 9) či příjmů dlužníků, resp. růstu nezaměstnanosti (DTI, DSTI). Pro zohlednění specifického profilu některých dlužníků je poskytovatelům umožněna výjimka do objemu 5 % poskytnutých úvěrů u každého z ukazatelů.

8 ČNB má k dispozici údaje o poměru poskytnutého hypotečního úvěru a jeho dluhové služby k příjmům (LTI/LSTI).
6 Růst cen nemovitostí v některých lokalitách přesahuje růst příjmů.
7 Zveřejňované na webových stránkách ČNB, viz http://www.cnb.cz/cs/financni_stabilita/makroobezretnostni_politika/doporuceni_k_rizeni_rizik/index.html

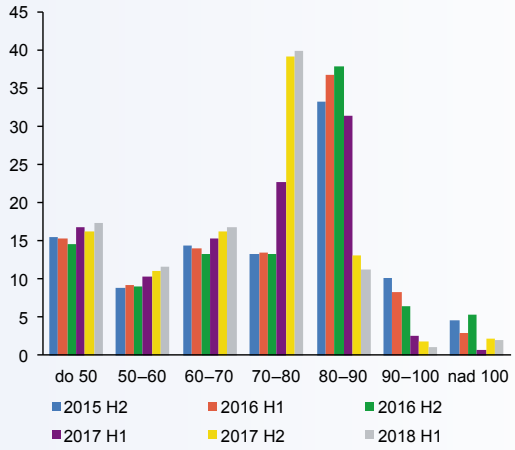
ČNB svými kroky aktivně a transparentně naplňuje zákonný mandát péče o finanční stabilitu…

ČNB analyzuje systémová rizika pro finanční stabilitu průběžně a v návaznosti na výsledky analýz uplatňuje nástroje, které nejúčinněji působí na omezení zjištěných rizik. Veřejnosti jsou analýzy i využívané nástroje představovány pravidelně formou publikací Zpráva o finanční stabilitě (červen)[9] a Rizika pro finanční stabilitu a jejich indikátory (prosinec)[10]. Tyto dokumenty přispívají k transparenci při naplňování jednoho ze zákonných úkolů ČNB – péče o finanční stabilitu. ČNB přistupuje k naplňování tohoto mandátu s cílem omezovat systémová rizika pro finanční stabilitu preventivně a včas, neboť obvykle vznikají v dobrých časech, kdy často nejsou plně vnímána nebo nejsou bezprostředně zřejmá. Přitom využívá i některé mezinárodně doporučované a uznávané nástroje, jejichž zakotvení v právním řádu ČR se teprve připravuje (např. ukazatele z výše zmíněného Doporučení).

…a na účinnosti jeho naplňování může mít svůj podíl i přístup auditorské profese

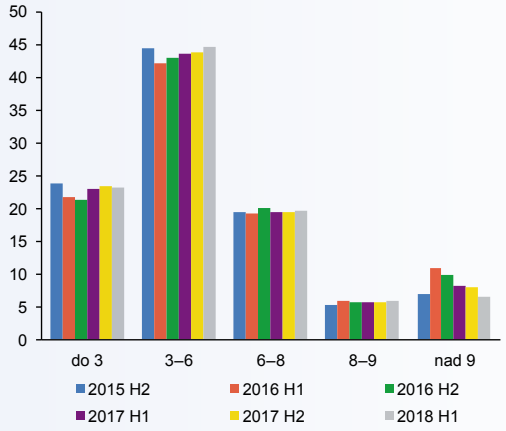
S ohledem na právní nezávaznost některých nástrojů využívaných ČNB může být pro jejich dodržování důležitý i přístup auditorské obce. Auditoři mohou významně napomáhat kultivaci tržního prostředí aktivním prosazování dodržování nástrojů doporučených ČNB v rámci dotčených institucí i v situaci, kdy nejsou dosud právně závazná.

Graf 9
Rozdělení nových úvěrů podle LTV
(osa x: LTV v %; osa y: podíl úvěrů na objemu v %)



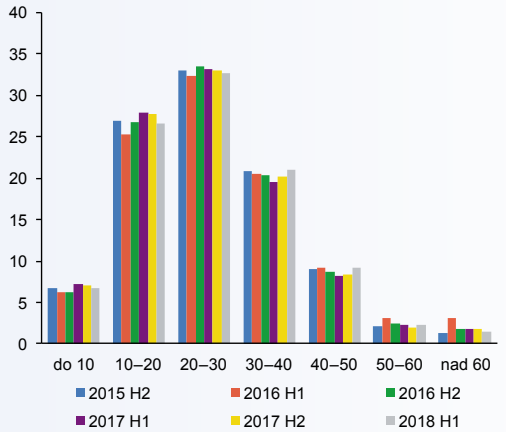
Pramen: ČNB
Pozn.: Interval zprava uzavřen.

Graf 10
Rozdělení nových úvěrů podle LTI
(osa x: LTI v letech; osa y: podíl úvěrů na objemu v %)



Pramen: ČNB
Pozn.: Vztaženo k objemu úvěrů, u kterých jsou k dispozici informace o LTI. Interval zprava uzavřen.

Graf 11
Rozdělení nových úvěrů podle LSTI
(osa x: LSTI v %; osa y: podíl úvěrů na objemu v %)



Pramen: ČNB
Pozn.: Vztaženo k objemu úvěrů, u kterých jsou k dispozici informace o LSTI. Interval zprava uzavřen.

LTI je poměr poskytnutého hypotečního úvěru (L) k ročním čistým příjmům (I) dlužníka.
LSTI je poměr roční dluhové služby z poskytnutého hypotečního úvěru (LS) k ročním čistým příjmům (I) dlužníka.

9 Viz http://www.cnb.cz/cs/financni_stabilita/zpravy_fs/fs_2017-2018/index.html
10 Viz http://www.cnb.cz/cs/financni_stabilita/rizika_pro_fs/.

Noví členové

- Mgr. Miroslav Báňa, MBA, Krajská správa a údržba silnic Vysočiny, příspěvková organizace
- Ing. Taťána Barabášová, Město Rožnov pod Radhoštěm
- Mgr. Veronika Bauerová, Český telekomunikační úřad
- Mgr. Jana Benešová, Dopravní podnik hl. m. Prahy, akciová společnost
- Ing. Jakub Beránek, Česká spořitelna, a.s.
- Ing. Linda Bitomská, Česká průmyslová zdravotní pojišťovna
- Ing. Lukáš Bonko, Individuální člen
- Ing. Petr Bubeník, Zebra Technologies CZ s.r.o.
- Ing. Martin Burjánek, MONETA Money Bank, a.s.
- Ing. Klára Čermáková, Stavební spořitelna České spořitelny, a.s.
- Ing. Ludvík Dvořák, Gardner Denver CZ + SK, s.r.o.
- Ing. Mgr. Renata Dvořáková, Plzeňský Prazdroj, a. s.
- Ing. Michal Ďuriš, Individuální člen
- Zsuzsanna Eifert, Slovak Telekom, a. s.
- Ing. Temuulen Erdenebat, Deloitte Audit s.r.o.
- Ing. Dana Francová, Národní knihovna ČR
- Ing. Monika Goryczková, ArcelorMittal Ostrava a.s.
- Ing. Bc. Lucie Hadynová, Česká spořitelna, a.s.
- Ing. Stanislav Heller, Ministerstvo pro místní rozvoj ČR
- Martina Hokeová, DiS., Státní pozemkový úřad
- Ing. Marián Ivančík, Raiffeisen stavební spořitelna a.s.
- Bc. Karolína Janhubová, Gardner Denver CZ + SK, s.r.o.
- Miroslav Jetleb, Česká spořitelna, a.s.
- Ing. Mgr. Věra Kašparová, Ministerstvo práce a sociálních věcí ČR
- Ing. Bohdana Kloudová, Centrum pro regionální rozvoj ČR
- Ing. Milan Kment, Správa železniční dopravní cesty, státní organizace
- Ing. Lenka Knolová, Komerční banka, a.s.
- Ing. Robert Komendát, U. S. Steel Košice, s.r.o.
- Ing. Eliška Kotoučková, PPF banka a.s.
- Ing. David Kotrba, Fio banka, a.s.
- Ing. Alžběta Kováčová, Bizlink Technology (Slovakia) s.r.o.
- Ing. Radana Krulišová, Raiffeisenbank a.s.
- Bc. Simona Malínská, Hlavní město Praha
- Ing. Marek Maňásek, Město Otrokovice
- Ing. Tomáš Marinka, Správa železniční dopravní cesty, státní organizace
- Nikol Medunová, MSc, Deloitte Audit s.r.o.
- Ing. Monika Mikulecká, Individuální členka
- Vít Müller, Stavební spořitelna České spořitelny, a.s.
- Ing. Mgr. Eva Nachtmannová, Statutární město Plzeň
- Ing. Jiří Nevřela, České dráhy, a.s.
- Mgr. Jan Němec, MBA, Individuální člen
- Ing. Lada Patáková, Česká spořitelna, a.s.
- Ing. Eva Pavelková, Ph.D., Gardner Denver CZ + SK, s.r.o.
- Ing. Petr Pavlas, Komerční banka, a.s.
- Ivana Pavlíčková, Česká spořitelna, a.s.
- Ing. Lenka Petrovićová, Exportní garanční a pojišťovací společnost, a.s.
- Ing. Šárka Petrů, Úřad průmyslového vlastnictví
- Ing. Petra Pírek, Exportní garanční a pojišťovací společnost, a.s.
- Ing. Zuzana Podhradayová, Ministerstvo zdravotníctva SR
- Ing. Martin Pořízek, Česká spořitelna, a.s.
- JUDr. Tomáš Procházka, Individuální člen
- Pavel Prokop, Grant Thornton Advisory s.r.o.
- PaedDr. Verona Prokšová, Česká správa sociálního zabezpečení
- Alena Přibylová, Deloitte Audit s.r.o.
- Petr Ptáček, MONETA Money Bank, a.s.
- Ing. Tomáš Rajtora, Česká spořitelna, a.s.
- Ing. Alena Reichel, Hlavní město Praha
- Ing. Jana Sedláčková, E.ON Česká republika, s.r.o.
- Bc. Martin Štěnička, Fio banka, a.s.
- Ing. Daniela Tichá, Správa železniční dopravní cesty, státní organizace
- Ing. Martin Tocimák, U. S. Steel Košice, s.r.o.
- Ing. Norbert Török, ACCA, CISA, Individuální člen
- Ing. Iva Tučková, NN Management Services, s.r.o.
- Mgr. Hana Vakrmanová, Equa bank a.s.
- Ing. Zdeněk Větrovec, ČD Cargo, a.s.
- Ing. Veronika Volná, MONETA Money Bank, a.s.
- Ing. Bc. Michaela Vrbová, Česká spořitelna, a.s.
- Ing. Libor Všetečka, Fio banka, a.s.
- Mgr. Ivana Vysušilová, Česká správa sociálního zabezpečení
- Ing. Tomáš Zikeš, Česká národní banka
- Ing. Jan Zrůbek, Česká spořitelna, a.s.

ZMĚNY V CERTIFIKACI

Vážené interní auditorky, vážení interní auditoři,

počátek nového roku s sebou přinesl několik avizovaných změn v mezinárodní certifikaci, se kterými bychom vás rádi blíže seznámili.

Mezinárodní institut interních auditorů (dále jen IIA) se rozhodl provést změny v následujících certifikacích: Certified Internal Auditor (CIA), Certification in Risk Management (CRMA), Certified Financial Services Auditor (CFSA), Certification in Control Self-Assessment (CCSA) a Certified Government Auditing Professional (CGAP).

Pokud jste držitelem některé z těchto certifikací, jste právě v certifikačním procesu nebo o certifikaci teprve uvažujete, doporučujeme věnovat následujícím informacím zvýšenou pozornost.
Od počátku ledna 2019 již není možná registrace ke zkouškám CGAP a CFSA. Trvale ukončena byla také registrace ke zkoušce CCSA, jejíž obsah bude sloučen se zkouškou CRMA.

U nejžádanějšího programu CIA došlo k aktualizaci jeho struktury v anglickém jazyce. Čeština bude počátkem ledna roku 2021 ve zkouškách CIA trvale ukončena. Stručný přehled o provedených změnách poskytuje tabulka č. 1.

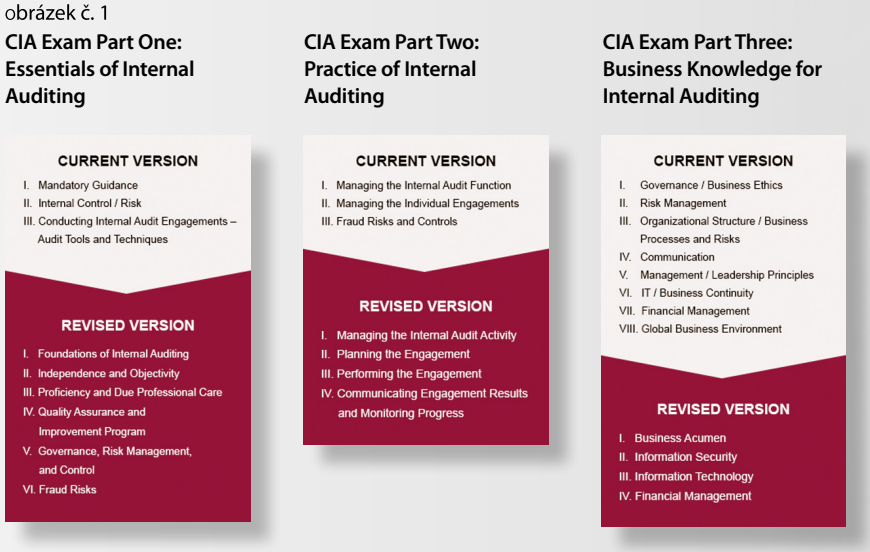
Tabulka č. 1:

CERTIFIKACE	2019	2020
CIA	Změna struktury zkoušky v AJ a ostatních jazycích, které IIA zachová po roce 2020.	Do konce roku 2020 možno složit v českém jazyce s podmínkou registrace do 12/2019. Od 1/2021 bude ukončena čeština ve zkouškách.
CRMA Certification in Risk Management Assurance	Změna obsahu zkoušky, sloučení s CCSA	
CGAP Certified Government Auditing Professional	Zrušení. Registrace od roku 2019 již není možná.	
CFSA Certified Financial Services Auditor	Zrušení. Registrace od roku 2019 již není možná.	
CCSA Certification in Control Self-Assessment	Součást CRMA	

CIA

V roce 2017 provedl IIA rozsáhlou analýzu, jejíž výsledky potvrdily, že je potřeba inovovat stávající strukturu zkoušek CIA tak, aby jejich obsah odpovídal současným požadavkům na znalosti a schopnosti interních auditorů.
Z tohoto důvodu tak od ledna 2019 probíhají zkoušky v anglickém jazyce dle nového sylabu 2019. Více informací o rozdílech mezi původní a novou strukturou zkoušek zjistíte z přiloženého obrázku č. 1.

obrázek č. 1



Zásadní změnou pro uchazeče o certifikaci CIA je ukončení českého jazyka ve zkouškách CIA dne 31. prosince 2020. Poslední možnost konat zkoušky v češtině (dle sylabu 2013) tak mají uchazeči pouze do konce roku 2020, avšak jen za předpokladu, že se registrují do 16. prosince 2019. Pokud kandidát nestihne vykonat všechny tři části zkoušky CIA do konce roku 2020, ať už z důvodu neúspěchu, nebo neúčasti na naplánované části zkoušky, bude muset chybějící část, případně části, vykonat v anglickém jazyce dle aktualizovaného sylabu 2019. Předchozí splněné části v češtině budou uznány.
Uchazeči, kteří se registrují po 16. prosinci 2019 budou zkoušky CIA konat již v anglickém jazyce dle sylabu 2019.
Pokud máte zájem konat zkoušky CIA v českém jazyce, apelujeme na vás, abyste se k nim přihlásili včas, neboť pozdější registrace po výše zmíněném datu již nebude možné administrativně zpracovat.

CRMA

Zkouška CRMA bude spojena se zkouškou CCSA a dojde k rozšíření požadavků na znalosti kandidátů. Bližší informace poskytne IIA v průběhu 4. čtvrtletí roku 2019 a my vás o nich budeme neprodleně informovat.

CIA Challenge Exam

CIA Challenge exam byla vyvinuta na základě rozdílů mezi požadavky ke zkouškám CCSA, CGAP a CFSA a požadavky ke zkoušce CIA s důrazem na Mezinárodní rámec profesní praxe IA (IPPF). Dává možnost získat certifikaci CIA jednoduše složením jediné zkoušky. Určena je však pouze pro ty kandidáty, kteří do 31. 12. 2018 získali certifikaci CGAP, CFSA nebo CCSA a ještě nedisponují CIA certifikací.

CIA Challenge exam bude dostupná v anglickém jazyce a dále také ve španělštině, portugalštině, turečtině, čínštině a japonštině. Registrace bude možná od 1. dubna 2019 do 15. prosince 2020. Samotnou zkoušku pak budou moci registrovaní kandidáti vykonat v termínu od 1. července 2019 do 31. prosince 2020.

Podmínkou je, aby zájemce o CIA Challenge exam zůstal certifikovaný v době, kdy se na zkoušku přihlásí, a i tehdy, kdy ji posléze bude vykonávat.

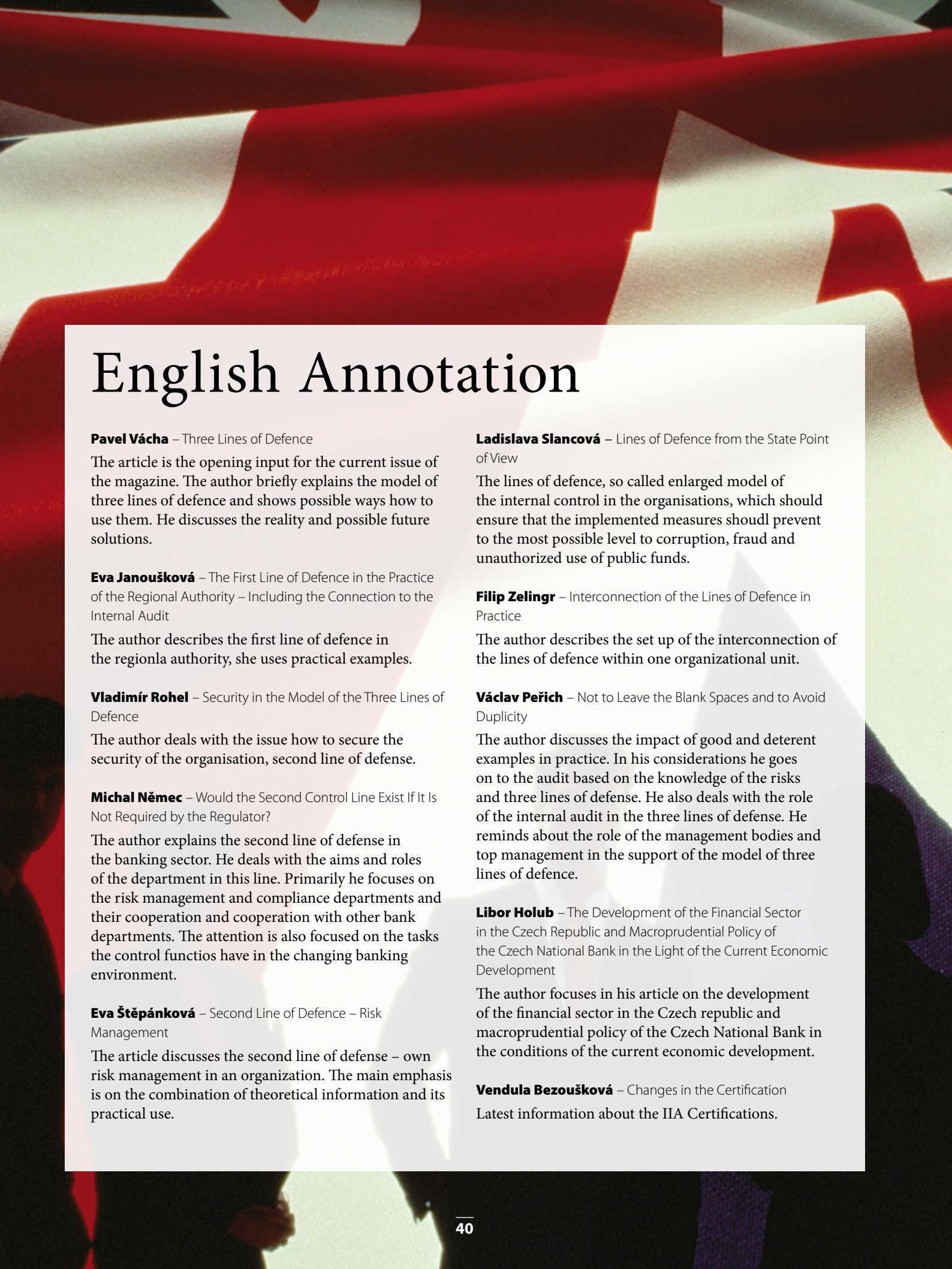
CIA Challenge exam mohou vykonávat i ti kandidáti, kteří se již do certifikačního programu CIA registrovali, včetně těch, kteří již úspěšně absolvovali 1 či více částí zkoušky CIA.

Zkouška bude složena z celkového počtu 150 otázek, na jejichž splnění budou mít kandidáti 3 hodiny. V případě neúspěchu je možné zkoušku za poplatek opakovat, avšak nejdříve za 90 dní od předchozího neúspěšného pokusu. Posledním dnem roku 2020 končí možnost CIA Challenge exam vykonat. Pokud se registrovanému kandidátu nepovede úspěšně do tohoto termínu zkoušku složit, dostane posléze možnost splnit všechny 3 části zkoušky CIA ve lhůtě 4 let od data registrace ke zkoušce CIA Challenge exam.

Pevně věříme, že poskytnuté informace shledáte užitečnými. V případě vašich dalších dotazů ohledně mezinárodní certifikace se můžete obrátit na kancelář ČIIA.

Přejeme hodně štěstí ve vašem procesu certifikace.

Za kancelář ČIIA
Mgr. Vendula Bezoušková



English Annotation

Pavel Vácha – Three Lines of Defence

The article is the opening input for the current issue of the magazine. The author briefly explains the model of three lines of defence and shows possible ways how to use them. He discusses the reality and possible future solutions.

Eva Janoušková – The First Line of Defence in the Practice of the Regional Authority – Including the Connection to the Internal Audit

The author describes the first line of defence in the regionla authority, she uses practical examples.

Vladimír Rohel – Security in the Model of the Three Lines of Defence

The author deals with the issue how to secure the security of the organisation, second line of defense.

Michal Němec – Would the Second Control Line Exist If It Is Not Required by the Regulator?

The author explains the second line of defense in the banking sector. He deals with the aims and roles of the department in this line. Primarily he focuses on the risk management and compliance departments and their cooperation and cooperation with other bank departments. The attention is also focused on the tasks the control functios have in the changing banking environment.

Eva Štěpánková – Second Line of Defence – Risk Management

The article discusses the second line of defense – own risk management in an organization. The main emphasis is on the combination of theoretical information and its practical use.

Ladislava Slancová – Lines of Defence from the State Point of View

The lines of defence, so called enlarged model of the internal control in the organisations, which should ensure that the implemented measures shoudl prevent to the most possible level to corruption, fraud and unauthorized use of public funds.

Filip Zelingr – Interconnection of the Lines of Defence in Practice

The author describes the set up of the interconnection of the lines of defence within one organizational unit.

Václav Peřich – Not to Leave the Blank Spaces and to Avoid Duplicity

The author discusses the impact of good and deterent examples in practice. In his considerations he goes on to the audit based on the knowledge of the risks and three lines of defense. He also deals with the role of the internal audit in the three lines of defense. He reminds about the role of the management bodies and top management in the support of the model of three lines of defence.

Libor Holub – The Development of the Financial Sector in the Czech Republic and Macroprudential Policy of the Czech National Bank in the Light of the Current Economic Development

The author focuses in his article on the development of the financial sector in the Czech republic and macroprudential policy of the Czech National Bank in the conditions of the current economic development.

Vendula Bezoušková – Changes in the Certification

Latest information about the IIA Certifications.

AKADEMIE ÚSPĚŠNÉHO VEDENÍ
INTERNÍHO AUDITU II.

Jak prodávat interní audit ve vlastní firmě?
Aneb budování značky interního auditu.

Termín konání:
14.–16. května 2019

Druhý díl úspěšného konceptu postaveného na:

Interaktivních workshopech.

Případových studiích, cvičeních, experimentech.

Sdílení praktických zkušeností.

Individuálním přístupu, maximálně 10 účastníků.

Propojení zkušeností z vedení interních auditorů a z koučování manažerů.

ČESKÝ INSTITUT INTERNÍCH AUDITORŮ