



ia
interní auditor

ČTVRTLETNÍK ČESKÉHO INSTITUTU INTERNÍCH AUDITORŮ

ROČNÍK 27, ČÍSLO 3|2023 (109)

3|2023

ŘÍZENÍ RIZIK

Aktuality

z tábora INTERNÍHO AUDITU

1.–2. listopadu 2023, Tábor

LH Hotel Dvořák Tábor ****



program

Záštitu nad konferencí poskytli **Ing. Štěpán Pavlík**, starosta města Tábor. Konference je realizována ve spolupráci s MF ČR.

1. listopadu 2023

- 8:30–9:30 Registrace
- 9:30–9:50 Zahájení
Tomáš PIVOŇKA, prezident Českého institutu interních auditorů
Jiří FOJTÍK, vrchní ředitel Sekce Finanční řízení a audit (Ministerstvo financí ČR)
- 9:50–10:50 **Jana BÁČOVÁ**
„Nové standardy pro interní audit“
- 10:50–11:20 Přestávka
- 11:20–12:30 Panelová diskuse na téma:
WHISTLEBLOWING – NOVÁ PRÁVNÍ ÚPRAVA A DOBRÁ PRAXE

- Štěpánka ČERNÁ**, manažerka útvaru compliance (ČEZ)
- Jiří JELÍNEK**, ředitel interního auditu (CPIPG)
- Hana ŽUFANOVÁ**, vedoucí oddělení interního auditu (MŠMT)
- 12:30–13:30 Oběd
- 13:30–15:30 **PRACOVNÍ SEKCE**

SEKCE A

- 15:30 Ukončení odborného programu prvního dne konference
- 15:45–18:00 **Zážitkový program**
 - Komentovaná prohlídka tábořského podzemí (včetně muzea).
 - Komentovaná vycházka historickým centrem Tábora.
 - Únikové hry.
 - Muzeum pivovarnictví a Pivovar pod Besedou.

Více o zážitkovém programu: **ZDE**.

- 19:00 Večerní program „Číše vína“
LH Hotel Dvořák Tábor ****
Congress & Wellness

2. listopadu 2023

- 8:30–9:00 Registrace
- 9:00–10:15 Přednášky a panelová diskuse na téma:

CYBER SECURITY – PŘÍPRAVA NA IMPLEMENTACI NIS2
Martin DLOUHÝ, manažer bezpečnosti (GasNet)
Tomáš GRZNÁR, bezpečnostní expert (ČEZ)
Tomáš KUDĚLKA, Director, Management consulting (KPMG)
Martin ŠVĚDA, vedoucí Oddělení regulace soukromého sektoru (NÚKIB)
Iva VONDROVÁ, Associate Manager, Risk Consulting (KPMG)

- 10:15–10:45 Přestávka
- 10:45–11:45 **Jiří ČIHÁK**, Interní audit IT (T-Mobile Czech Republic)
„Umělá inteligence a interní audit“
MUDr. František KOUKOLÍK, DrSc.
„Temná trojice“
- 11:45–12:55 Ukončení konference
Tomáš PIVOŇKA, prezident Českého institutu interních auditorů
- 12:55–13:00 Oběd

SEKCE A

FRAUD RISK MANAGEMENT A INTERNÍ AUDIT
Petr BARÁK, předseda Komise pro bankovní a finanční bezpečnost (Česká bankovní asociace)
Kateřina HALÁSEK DOSEĐELOVÁ, vice-president (ACFE Czech republic Chapter)
Tomáš PIVOŇKA, ředitel útvaru audit a compliance (ČEZ)
Filip ZELINGR, ředitel útvaru Interní audit, Řízení rizik a Compliance (Letiště Praha)

SEKCE B

VEŘEJNÁ SPRÁVA
Tomáš VYHNÁNEK, vedoucí oddělení Revize výdajů, sekce Finanční řízení a audit (Ministerstvo financí ČR)
„Výsledky mezinárodního srovnání v oblasti interního auditu“



Vážené čtenářky, vážení čtenáři, přátelé interního auditu,

vítejte u nového čísla časopisu Interní auditor. Hned v úvodu se s vámi chci podělit o novinku, kterou s vámi sdílíme od srpna. Máme nový design webových stránek a věřím, že je v mnoha ohledech moderní a inovativní. Nová je nejen grafika, ale i celkové uspořádání informací, a to tak, aby pro vás bylo více intuitivní a přehledné. Věřím, že se nám to povedlo. Když už jsme v úvodníku časopisu, tak nezapomeňte, že na webu je prostor pro online vydání Interního auditora. Jsou tam volně k dispozici všechna čísla od roku 2008.

A co naleznete zajímavého v tomto vydání? Zejména se zaměřujeme na široké spektrum témat spojených s řízením rizik. Od obecných principů řízení rizik, konkrétních přístupů a osvědčených postupů z dobré praxe až po audit řízení rizik. Věříme, že každý z vás zde najde něco užitečného, ať už jste auditorem v oblasti řízení rizik, zkušeným profesionálem v ní, nebo teprve začínáte objevovat její kouzlo. Vydání jsme doplnili o další články, které vás mohou inspirovat a motivovat.

Děkujeme vám za vaši podporu a zájem o naše služby. Nezapomeňte sledovat náš nový web a přihlásit se na naši konferenci, která se uskuteční v krásném prostředí historického města Tábora.

Pohodový podzimní čas vám za Institut přeje



Daniel Häusler
ředitel kanceláře ČIIA

OBSAH

Hrozí riskařům zakrnění? Michal Němec	4
Historie řízení rizik u Správy železnic Karel Peška	7
Dobrá praxe v řízení rizik Lucia Rončáková, Michaela Lenochová, Jana Štubňová	9
Řízení rizik ve veřejné správě – bez odhodlání vrcholového managementu to nepůjde Valdemar Adamiš	12
Rizika v podnikání, význam a formy jejich řízení Jiří Dvořáček	15
Interní audit v pojišťovnách z pohledu České národní banky Karla Voráčková, Martina Höferová	19
Rizika spojená s využíváním AI z pohledu IA a auditovaných Jiří Čihák	23
Audit řízení rizik Lenka Landa Schejbalová, Helena Raizl Jumrová	27
Auditors in the Hot Seat Alexander Heggen	30
Jak začít s AI? Jiří Čihák	36
Nové Standardy jsou skoro na světě – pokračování (3. část) Jana Báčová	37
Jakou sílu má mysl Alena Jáchimová	42
Vztahy? Rodina? Někdy to není jen tak Radka Moricová	45
Noví členové	

3. strana obálky

ROČNÍK 27, ČÍSLO 3|2023 (109)

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 (Print)
ISSN 2787-9798 (Online)
Náklad: 1400 kusů

Redakční rada:
Předseda – Jan Kovalčík
Jiří Čihák, Daniel Häusler,
Ludmila Jiráňová, Šárka Nováková,
Ladislava Slancová, Petra Škvorová,
Eva Stěpánková, Milena Wídomská

Editorka: Jana Mikešová

Grafika: Viktor Beránek

Vydavatel nese odpovědnost za údaje
a názory autorů jednotlivých článků

Foto: archiv ČIA, fotobanka 123RF

Neprodejné, určeno pro Český institut
interních auditorů

ia
interní auditor

NIS 2 jako služba

Jste připraveni na NIS 2?

Směrnice NIS 2 ukládá povinnost zavést opatření v oblasti kybernetické bezpečnosti, se kterou máme jako dodavatel letité zkušenosti. Svěřte své starosti profesionálům a mějte klid v nebezpečném kybernetickém prostředí.

- pomůžeme vám se zavedením a splněním podmínek **dle směrnice NIS2**
- provedeme nezávislý **audit kybernetické bezpečnosti**
- **poskytneme nástroj** – aplikaci dTASK pro digitální vedení agendy auditu kybernetické bezpečnosti
- **SECaaS – bezpečnost jako služba** - ucelená sada bezpečnostních opatření
- nezávislé konzultace & poradenství

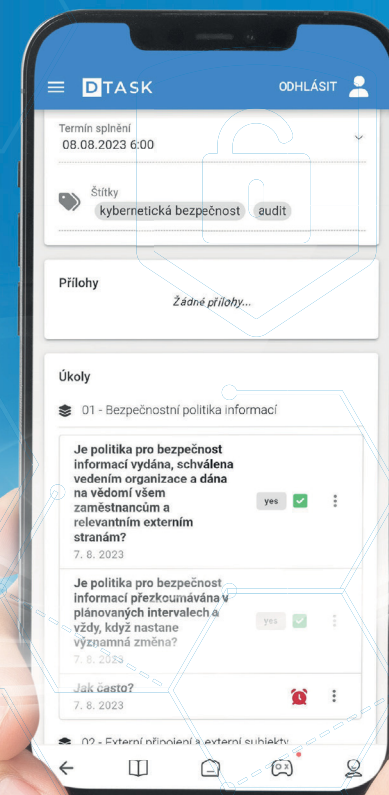
Kdo jsme?

Poskytujeme komplexní služby a řešení v IT, dlouhodobě se specializujeme na oblast kybernetické bezpečnosti. Jsme stabilní a léty prověřený hráč s více než 30ti letou působností. Máme vlastní silné technologické zázemí a tým čítající více než 50 certifikovaných odborníků a specialistů. Sami jako dodavatelé procházíme náročnými externími a interními audity a rádi pomůžeme i vám.

Neváhejte se na nás obrátit.

+420 255 772 148, +420 728 444 152, www.its.cz

Získejte potřebnou úroveň zabezpečení bez investic!





HROZÍ RISKÁŘŮM ZAKRNĚNÍ?

Když jsem byl požádán o příspěvek zaměřený na vyhodnocení změn v oblasti řízení rizik za posledních deset let, nevěděl jsem si ihned základní zádrhel, který je způsoben omezením paměti. Jen obtížně se mi přesně vybavuje, zda mé vzpomínky sahají do období před třinácti, nebo osmi lety. Jak z tohoto omezení vybruslit? Jednoduše, až na jednu výjimku se vyhnu jakémukoliv přesnému datování. Zároveň s ohledem na mé dlouhodobé působení v oblasti nefinančních rizik se budu věnovat primárně této části rizik a oblast úvěrových či tržních rizik ponechám stranou.

Mgr. Michal Němec

Česká spořitelna
ředitel Řízení nefinančních rizik

Michal je ředitelem řízení nefinančních rizik v České spořitelně, kde se aktuálně zabývá oblastí prevence praní špinavých peněz, řízením operačních rizik, prevencí podvodů a oblastí GDPR. Má zkušenosti i z oblasti compliance, fyzickou bezpečnosti, řízením vnitřního kapitálu i krizovým řízením. Na počátku pracovní kariéry získal zkušenosti i na různých pozicích v rámci bankovního dohledu České národní banky.

Přestože základní principy řízení rizik se za posledních deset let příliš nezměnily (stále se řídíme obezřetností vyhláškou ČNB č. 163 z roku 2014), byla vydána řada doplňujících technických standardů, doporučení, které tyto principy dále rozpracovávají či upřesňují. Nevnímám však, že by došlo k výraznému posunu z hlediska celkového konceptu pojetí nefinančních rizik. Byly však vydány nové regulace, které zvyšují přístupnost veřejnosti k některých službám (jako příklad mohu uvést regulaci v oblasti platebního styku, která umožnila vstup na trh novým licencovaným subjektům), zabývají se zcela novými oblastmi (např. regulace související s udržitelností) nebo dále zvyšují ochranu spotřebitele. Ale jelikož v rámci tohoto příspěvku bych se chtěl spíše zaměřit na dopady na způsob řízení rizik v obecnější rovině, nebudu se detailně zabývat uvedenými regulacemi a jejich přínosem pro ochranu klientů, společnosti či bankovního systému jako celku. Zamyšlení

budu věnovat spíše rozdílům v práci specialistů řízení rizik, kde vnímám za posledních deset let velkou změnu.

Již před deseti lety jsem považoval bankovníctví za komplexní odvětví, a i mezinárodně uznávaní znalci či hlavní metodici České národní banky již připouštěli, že téměř není v lidských silách pojmout veškeré souvislosti vycházející z regulatorních požadavků na banky. Přesto se mi komplexita aktuálních požadavků a nároků na řízení rizik zdá být neporovnatelná.

Můžeme začít vnitřním organizačním uspořádáním některých bank, i když se nejedná o oblast, která přímo souvisí s legislativními požadavky. Spíše reaguje na stále se zrychlující vývoj externího prostředí, které nutí banky k větší flexibilitě a akceschopnosti, než tomu bylo v předcházejících letech. To zvláště platí pro banky, které nechtějí jen pasivně sledovat a reagovat na probíhající změny, ale chtějí se přímo

na nich aktivně podílet, a přispívat tak k samotnému určování nových trendů.

Příklad uvedu na fungování týmů, které se podílejí na akceptaci nových produktů nebo ještě obecněji jakýchkoliv změnových procesů. Jako zástupce takového týmu mohu použít operační rizika, která byla jednou z prvních oblastí mého zaměření. Ještě před dekadou byla operační rizika vnímána poměrně odděleně jako úzce specializovaný tým, který se do značné míry věnoval plnění požadavků regulátora. Za tímto účelem se operační rizika zabývala vyhodnocováním řady nástrojů, které byly používány pro dlouhodobé monitorování vývoje tohoto rizika nebo přispívala expertním hodnocením při zavádění nových produktů. Některá z těchto cvičení byla ročně aktualizována, přičemž často se jednalo jen o pouhé drobné korekce, protože mezi jednotlivými roky nedocházelo k výrazným dramatickým změnám. Jednotlivé změny v procesech nebo systémech byly závislé na pravidelných a s velkým předstihem naplánovaných termínech pro nasazování novinek do produkce. Tradiční banky byly rovněž často velmi hierarchické a jednotlivé změny v produktech či procesech procházely schvalovacím procesem na úrovni řídicích pracovníků, ať už na úrovni celého představenstva, či jeho poradních orgánů. Z toho důvodu bylo poměrně jednoduché nastavit a udržovat si přehled o změnových požadavcích podléhajících schvalovacímu procesu banky. Postačovalo udržovat kontakty s poměrně úzkou skupinou kolegů, aby příslušné týmy zapojené do posuzování rizik měly jistotu o zapojení do všech relevantních procesů.

V dnešním pojetí vnímám výrazný odklon od tohoto hierarchického uspořádání k větší autonomii jednotlivých týmů, které se zabývají procesy ve svěřené oblasti definované podle typů produktů, klientských segmentů či potřeb klientů. Zároveň v souvislosti s rychlejšími požadavky na nasazování nových funkcionalit dochází často k uvádění nových verzí systémů nebo produktů, jakmile jsou dané novinky

vyvinuty a příslušně otestovány. Cílem nejedné společnosti tak může být v podstatě průběžná kontinuální aktualizace používaných aplikací. Tímto rostou požadavky na operační rizika či další obdobné týmy na průběžný sběr informací o chystaných změnách, jelikož vlastní odpovědnost za vývoj a nasazování novinek je často delegována na jednotlivé týmy. Zvláště u menších změn tak není dodržován dříve častěji využívaný centralizovaný systém schvalování, což právě přináší nové výzvy pro kontrolní funkce.

„vlastní odpovědnost za vývoj a nasazování novinek je často delegována na jednotlivé týmy.“

Jak na tuto změnu mohou operační rizika reagovat? Mohou se vydat cestou průběžných a detailnějších kontrol, pomocí kterých se mohou ujišťovat, že jim pod rukama neprobíhají změny bez patřičného vyhodnocení rizik. Tím se však snadno dostanou do vleku událostí a případné dodatečné požadavky se jim budou obtížněji prosazovat. Alternativou je větší specializace členů tohoto týmu, užší zapojení do projektů již při jejich vývoji a do průběžného přispívání k nastavení výsledného produktu. A právě díky větší specializaci může docházet k vyšší přidané hodnotě těchto specialistů. Ta v optimálním případě může přispět i k přímému oslovování těchto funkcí vlastníky nových produktů, protože sami budou více rozpoznávat přidanou hodnotu specialistů z risku.

To ale není jediná změna. Zároveň roste požadavek na vyšší efektivitu využívání jednotlivých nástrojů pro řízení rizik, jelikož dnes už málokoho uspokojí tvrzení, že se jedná o regulatorní požadavek. Přestože je regulace stále významným argumentem, je jednotlivými obchodními týmy vyvíjen větší tlak na její uchopení způsobem, který bude pro všechny

účastníky srozumitelný a přínosný. Tento trend vnímám z dlouhodobého hlediska jako velmi pozitivní, protože vede k hlubšímu zamyšlení se nad jednotlivými požadavky. Výstupy z těchto závěrů pak nekončí čistě v týmech řízení rizik za účelem naplnění očekávání regulátora, ale jsou častěji prakticky využívány. Zde vnímám i velmi pozitivní vliv mladé generace, která nemá zábrany upozorňovat na věci, které jí nedávají smysl, a mnohem častěji proaktivně přichází s alternativními návrhy.

Další významnou změnou je, že bankovníctví přestalo být úzce izolovaným odvětvím, které poskytovalo pouze základní služby vyplývající z původní bankovní licence. Dříve v podstatě záleželo na strategii banky, které produkty nabídne klientům a jaké parametry u těchto produktů nastaví. Díky tomu bylo jednodušší i řízení souvisejících rizik. V dnešní době, kdy dochází k výrazné digitalizaci nejen v komerčním, ale i státním sektoru, jsou banky stavěny před nové výzvy. Příkladem mohou být nástroje pro ověření identity klienta, které byly dříve vydávány každou institucí výhradně pro jejich vlastní potřebu. Dnes je prostřednictvím Bank ID využívána identita klienta jako nástroj nejen k otevírání produktů či jejich obsluze v jiných bankách, ale i pro přistupování ke státním službám či různým dalším komerčním účelům. V této souvislosti se otevírají nová rizika například v situaci, kdy banka nedostatečně identifikuje klienta, kterému vydává vlastní identitu. Takto získaná identita může být následně využita k různým nežádoucím účelům, např. k neoprávněnému uzavření smlouvy či neautorizovanému přístupu k osobním údajům jiného klienta. Tím se banka vystavuje novým typům rizik, kterými se dříve vůbec nemusela zabývat.

Trendu rostoucí digitalizace a různého využívání bankovní identity nenahrává ani situace stále pokročilejších útoků na klienty jednotlivých bank. Tyto útoky již nesměřují jen k přímému obohacení útočníků prostřednictvím jednorázového převodu peněz či majetku klientů,

ale objevují se i případy pokusů o neoprávněné ovládnutí klientské identity. Tyto pokusy kladou výrazně zvýšené nároky na monitoring i netransakčních aktivit klientů a detekci jakýchkoliv anomálií při využívání identity jako takové. Již tedy nepostačuje sledovat pouze převody prostředků či výběry hotovostí, byt se stále jedná o silné rizikové indikátory. Situaci značně ztěžuje pokročilá manipulace klienty ze strany útočníků, kdy i na přímé dotazy zástupců banky reagují klienti kvůli jejich manipulaci ze strany útočníků úmyslně nepravdivými informacemi. Operátorům tedy již nepostačují prosté dotazy, zda klient prováděl danou operaci, či nikoliv, ale je potřeba využívat aspoň základů psychologie a pokusit se klienta vymanit ze zajetí útočníka. Není výjimkou, když klienti až po delším rozhovoru s řadou otázek, ale i popisu historických zkušeností banky s různými typy útoků připustí, že i oni mohou být obětmi útoku útočníka. Ano, mohlo by být konstatováno, že v této oblasti jdou banky již daleko nad rámec svých povinností, ale na druhou stranu není v zájmu bank zpochybnění bezpečnosti elektronických služeb ze strany jejich klientů, kdyby se tyto typy útoků staly úspěšnějšími. Naštěstí v tomto boji nejsou banky osamocené, ale mohou využívat úzké a prospěšné spolupráce s policejními složkami či přímo s Českou národní bankou.

Nedílnou součástí změn v posledním desetiletí je i oblast využívání nových cloudových technologií, kdy dochází ke stále častějšímu využívání služeb vyvinutých třetími stranami a jejich použití ve vlastních aplikacích. Tento přístup bezesporu urychluje práci vývojářů, na druhou stranu je opět v této oblasti potřeba zvyšovat míru jistoty kvality a bezpečnosti využívaných služeb a nástrojů. Proto je žádoucí nový způsob vývoje podpořit zvýšeným důrazem na testování výsledných řešení, včetně penetračních testů zaměřených na bezpečnost řešení. A to se zatím nezmiňuji o nových modelech stále výrazněji se prosazujících, např. algoritmech založených na principech zpracovávání a vyhodnocování obrovského množství textových informací typu Chat GPT.

Přestože se bezesporu jedná o perspektivní oblast, která má potenciál usnadnit práci v mnoha oblastech, je opět před masovějším využíváním těchto technologií potřebné jim detailně porozumět a vyhodnotit nejen jejich přínosy, ale i nová rizika. Mimochodem sám jsem tuto technologii použil zkušebně pro porovnání rozdílů v jednotlivých vyhláškách ČNB zaměřených na obezřetnostní principy platných pro banky a výsledky byly poměrně uspokojivé, aniž by mi to zabralo mnoho času.

„je žádoucí nový způsob vývoje podpořit zvýšeným důrazem na testování výsledných řešení“

Výše uvedená rizika bych zařadil spíše do kategorie provozních rizik, ale nechtěl bych zároveň opomenout charakteristiku, kterou pro bankovní sektor považuji za naprosto zásadní. Tou je důvěra klientů v danou instituci, kterou z pohledu řízení rizik lze zahrnout do kategorie reputačních rizik neboli velmi jednoduše pod riziko ztráty důvěry v danou instituci.

Zde si dovolím zaspekulovat a vyjádřit velmi osobní názor, že dříve se klienti zaměřovali především na stabilitu dané společnosti, tedy, zda banka je dostatečně silná a zdravá na to, aby klientům vyplatila jejich prostředky, kdykoliv je budou potřebovat. V dnešní době, s ohledem na míru stability našeho bankovního sektoru, začala řada klientů stabilitu banky vnímat jako automaticky garantovanou věc, o kterou se v podstatě nemusí zajímat.¹ Klienti tak začali rozlišovat další řadu parametrů, které jsou z jejich pohledu důležité. A tím může být míra dostupnosti jednotlivých klientských řešení, složitost používání bankovních aplikací, včetně jejich instalace, množství informací poskytovaných k jednotlivým produktům či službám nebo rychlost zpracování klientských požadavků, včetně potenciálních reklamačních řízení.

Z pohledu klienta jistě oprávněná očekávání opět mají dopad na pracovníky řízení rizik, kteří stále více musí zohledňovat klientské potřeby a jejich očekávání. A to i v případech, kdy daná opatření mohou být spatřována jako opatření na úkor kvality či bezpečnosti poskytovaných služeb. Cílem je tedy nacházet řešení, která budou uživatelsky stále akceptovatelná, ale na druhou stranu budou stále splňovat požadavky na bezpečnost identifikace klienta, zajištění dané služby či naplnění regulačních povinností ve vazbě na informační povinnosti. Při hledání cílových řešení se opět vyplácí velmi úzká spolupráce mezi obchodními či produktovými týmy bank a řízením rizik.

Tyto selektivně vybrané ukázky jsem vybíral se záměrem ukázat, jak se i pro zástupce risk managementu významně mění rozsah jejich práce a jak je pro ně podstatné udržovat se ve střehu a vstřebávat celou řadu novinek. Jak jsem uvedl výše, záměrně jsem se nezabýval změnami, které bankám přináší nové regulační požadavky.

Přestože bychom jako risk manažeři měli být zvyklí uvažovat o rizicích, které mohou nastat s velmi malou pravděpodobností, netroufám si odhadnout, kam se naše práce posune nejen za dalších deset let, ale i ve výrazně kratším období. Proto za jednu ze základních dovedností pro risk management považuji otevřenost novým směrům a zapálenost pro seznamování se s čerstvými myšlenkami. Zároveň bychom se měli snažit jim porozumět a dokázat nejen rozpoznat významná rizika, ale i vidět budoucí perspektivní využití. Takové nastavení nás, pevně věřím, udrží relevantními partnery pro byznys. Jsem přesvědčen, že náplň práce risk manažera bude sice stále náročnější, ale zároveň i velmi pestrá a zajímavá.

Ať už jste risk manažerem, či kolegou v jiné kontrolní funkci, nebo jste dokonce zástupcem byznysu, přeji vám, aby vás práce naplňovala a nacházeli jste si v ní i krásné poslání. ■

Historie řízení rizik u Správy železnic



Mgr. Karel Peška, MBA

Je absolventem Univerzity Karlovy v Praze. Titul MBA získal studiem na Central European Management Institutu. Zastával manažersko-ekonomické pozice ve veřejné správě na úrovni okresu, kraje i ústředních orgánů státní správy. Působil jako vrchní ředitel sekce ekonomiky a provozu na Ministerstvu vnitra ČR. Několik let pracoval ve funkci vrchního ředitele na Ministerstvu dopravy ČR. V roce 2012 nastoupil na Generální ředitelství tehdejší SŽDC na odbor interního auditu, kde se v roce 2017 stal ředitelem. Tento útvar poté výrazně transformoval, na Správě železnic vybudoval centralizovaný systém řízení rizik a spolupodílel se i na zavádění programu compliance v rámci organizace. K výrazným počínům patřila i implementace integrovaného informačního systému pro interní audit a řízení rizik, jakož i zřízení oddělení IT a kybernetické bezpečnosti.

Organizace Správa železnic zaujímá nezastupitelné místo v zajištění provozuschopnosti železniční dopravní cesty a organizování a řízení železniční dopravy v ČR. V rámci plnění tohoto úkolu je nutné vykonávat a zajišťovat mnoho procesů. Ohrožení některého z nich by mohlo znamenat řetězení problému s dopadem do plynulosti a bezpečnosti dopravy či rozvoje železniční infrastruktury.

Z těchto důvodů se vedení organizace v roce 2018 rozhodlo pro zavedení centralizovaného systému řízení rizik. Jeho hlavním úkolem je zajistit včasnou identifikaci hrozeb a rizik, jejich neustálé sledování a vyhodnocování, následně pak realizaci opatření k minimalizaci dopadu rizik na plnění hlavních úkolů a dosažení strategických cílů organizace.

Na odboru interního auditu tak v roce 2018 vzniklo nové oddělení rizik vedené manažerem rizik, jehož náplní je zejména koordinovat systém řízení rizik.

V první fázi zaměstnanci oddělení vypracovali interní dokumenty vycházející z normy ISO 31000 Management rizik, na jejichž základě bylo možné postupně implementovat a integrovat nový systém řízení rizik do celkového vedení a strategie organizace. Začátkem roku 2019 jmenoval

generální ředitel členy Výboru pro řízení rizik (VŘR).

Výběr vhodného IS

Pro zajištění efektivního fungování celého procesu řízení rizik bylo rovněž nutné pořídit sofistikovaný IS. Zásadním kritériem pro výběr systému bylo, aby fungoval jako jednotný elektronický nástroj pro podporu klíčových činností zajišťovaných odborem interního auditu, tj. pro vlastní výkon činnosti interního auditu, pro řízení rizik a evidenci externích kontrol, v samostatných modulech s možností jejich propojení a získání maximálních synergických efektů. S tím, že IS bude umožňovat postupné doplňování dalších modulů např. pro řízení kybernetických či korupčních rizik.

V rámci průzkumu trhu jsme nenalezli software, který by splňoval naše požadavky, a rozhodli jsme se pro vypsaní výběrového

řízení na implementaci softwaru na klíč. Na jaře 2019 byla soutěž vypsaná a v květnu uzavřena smlouva s vybraným dodavatelem.

Implementace

V roce 2019 tým manažera rizik shromažďoval potřebné informace pro sestavení katalogu rizik, komunikoval a konzultoval navržená rizika s jejich vlastníky a stanovoval kritéria a ukazatele pro jejich hodnocení. Návrhy koncepce a způsobu řízení rizik byly průběžně předkládány VŘR k projednání. Současně probíhala spolupráce s dodavatelem IS na zavedení a spuštění jeho testovací verze. Komunikovali jsme zejména obsah karty rizika a katalogu rizik, import historických dat, možnost a způsob aktualizace parametrů k rizikům, práci s opatřeními, přístup jednotlivých účastníků procesu, a samozřejmě způsob reportování. V neposlední řadě jsme kladli důraz na možnost tvorby různých přehledů pro analytickou činnost a zjišťování trendu vývoje rizik. Současně tým manažera rizik zpracoval podrobný pracovní manuál k IS AURIS.

Testování probíhalo i v průběhu roku 2020, souběžně jsme školili všechny účastníky procesu centralizovaného řízení rizik, aby byli plně seznámeni s prací související s příslušnou rolí v IS. S velkou pečlivostí jsme testovali jednotlivé postupy a funkcionality a ve spolupráci s dodavatelem odstraňovali zjištěné nedostatky.

Vlastní řízení rizik od roku 2019 do konce roku 2020 probíhalo elektronickým způsobem, ale pouze formou excelovských tabulek a formulářů. V závěru roku 2020 byl již do systému nahrán aktuální katalog rizik Správy železnic.

Zahájení ostrého provozu

Produkční prostředí jsme spustili ve dvou fázích. Moduly pro externí kontroly a interní audit byly zprovozněny od poloviny roku 2020. Centralizované řízení rizik však představovalo v organizaci zcela nový proces a modul pro tuto činnost musel zvládnout zapojení většího

počtu uživatelů napříč celou organizací, proto bylo jeho vytvoření a zprovoznění časově náročnější. Chtěli jsme mít co největší jistotu, že všechny možné počáteční neduhy systému budou v maximální možné míře odstraněny. Delší testování a příprava všech zainteresovaných se vyplatily. První ostré reportování za 1. čtvrtletí 2021 proběhlo úspěšně a bylo přijato pozitivně. Od uživatelů jsme si vyžádali hodnocení a podněty na vylepšení, které vyústily v následné úpravy směřující k zefektivnění, zjednodušení a zpřehlednění procesu.

Následný rozvoj

Spuštěním ostré verze práce na IS neskončila. S dodavatelem jsme uzavřeli smlouvu na rozvoj a pustili se do realizace vylepšení, rozšiřování a doplňování funkcionalit. Jako první jsme rozšířili evidenci opatření k rizikům, která jsou důležitou částí procesu řízení rizik. Dále jsme se zaměřili na postupné zpřístupnění systému pro analytiku z organizačních jednotek. V rámci úprav byl kladen důraz na zajištění ještě většího komfortu pracovního prostředí pro jeho uživatele. Byly doladěny i statistické výstupy – přehledy o stavu a vývoji rizik pro běžné uživatele i manažera rizik.

Co systém umí

AURIS je webovou aplikací, uživatelům je k dispozici přes webový prohlížeč s využitím SSO (jednotné přihlašování). Aktuálně máme zprovozněny čtyři moduly – pro interní audit, externí kontroly, řízení rizik a kybernetickou bezpečnost. V modulu rizik evidujeme katalog strategických rizik, přičemž každé riziko je samostatným případem s kartou rizika obsahující jeho popis, historii hodnocení, evidenci sledovaných indikátorů a historii práce s rizikem. Prostřednictvím IS pravidelně čtvrtletně spouštíme reportování o řízení rizik. K jednotlivým rizikům evidujeme přijatá opatření, u nichž sledujeme jejich včasné plnění, účinnost a dopad na hodnocení příslušného rizika. Samozřejmostí je generování různých přehledů, třídění rizik dle zadaných kritérií a grafické zobrazení vývoje rizik.

Přístup a funkcionality jsou řízeny přidělenými rolemi. Nezanedbatelnou výhodou je automatické zaslání notifikací uživatelům do jejich e-mailů v případě přidělení úkolu, včetně živých odkazů. Současně AURIS upozorňuje na nesplněné úkoly, případně může průběžně zasílat požadované přehledy. IS komunikuje rovněž se spisovou službou.

Modul rizik je napojen na modul interního auditu a umožňuje např. přenos aktuálního katalogu rizik pro potřeby tvorby ročního plánu činnosti interního auditu.

Co plánujeme dále

V roce 2023 jsme pokračovali v propojování modulů řízení rizik a interního auditu v oblasti nápravných opatření. Pro management bude zpřístupněn souhrnný report opatření evidovaných v jednotlivých modulech. Rovněž probíhají práce na implementaci nového modulu pro business kontinuitu procesů. A čerstvě jsme ukončili aktualizaci modulu pro kybernetickou bezpečnost, který byl zprovozněn v roce 2021.

V následujících letech, v závislosti na finančních zdrojích, připravujeme např. doplnění modulu pro detailní sledování rizik v oblasti compliance či v systému bezpečnosti provozování dráhy a drážní dopravy. Počítáme s využitím rozšířeného grafického zobrazování.

Shrnutí

Na závěr mohu konstatovat, že spuštění provozu IS AURIS, jakožto hlavního nástroje pro náš útvar, významně napomohlo a podpořilo úspěšné zavedení centralizovaného způsobu řízení rizik v naší organizaci. Díky němu došlo k podstatnému zefektivnění řídicí kontroly a zásadně se nám podařilo rozšířit povědomí o rizicích a podpořili jsme práci s riziky u jejich vlastníků. To dokládá i úspěšné získání certifikace dle normy ISO 9001:2015 pro oblast řízení rizik na Správě železnic, kterou jsme obdrželi v květnu 2023. ■



Lucia Rončáková
Senior Manager | Deloitte Risk Advisory
lroncakova@deloitteCE.com



Michaela Lenočhová
Senior Consultant | Deloitte Risk Advisory
mlenochova@deloitteCE.com



Jana Štubňová
Specialist Lead | Deloitte Risk Advisory
jstubnova@deloitteCE.com

DOBŘÁ PRAXE V ŘÍZENÍ RIZIK

Řízení rizik. Toto sousloví může znít jako magické zaklínadlo, které je s oblibou používáno v názvech firemních dokumentů a v reportech předkládaných managementu. Rozumíme však jeho podstatě a významu? Každý zaměstnanec, který působí v oddělení compliance či interního auditu, nám pohotově odvětlí, že řízení rizik představuje proces identifikace, hodnocení a zmírňování potenciálních rizik, která by mohla organizaci negativně ovlivnit. Tato definice řízení rizik je samozřejmě zcela v pořádku. Poskytuje nám však dobrou představu, co je od nás očekáváno, proč bychom se řízením rizik měli zabývat a jak by vlastně měla taková dobrá praxe řízení rizik vypadat?

Rizika, se kterými organizace nepracují, lze přirovnat k černé díře, která pohlcuje zdroje i potenciál. Nezáleží na tom, zda se jedná o mezinárodní společnost, startupovou firmu, nebo neziskovou organizaci. Všechny mají jednu společnou potřebu: chránit své podnikatelské zájmy a zajišťovat růst a prosperitu. Současná praxe dokládá, že absence v oblasti řízení rizik znemožňuje efektivně tuto potřebu naplňovat, a právě proto je řízení rizik klíčovým prvkem úspěchu pro jakoukoli organizaci.

V tomto článku se podrobněji podíváme na dobrou praxi v oblasti řízení rizik a jaké by měly být její klíčové prvky.

Tři linie obrany – jakou cestu zvolit?

V běžné praxi se pro řízení rizika jako jeden z nejčastěji využívaných modelů uplatňuje tzv. model tří linií obrany (the three lines of defence model). Samotné linie jsou přitom uvnitř firmy dělené následovně: První linii tvoří manažeři a jejich zaměstnanci, druhou linii představuje funkce řízení rizik a dodržování předpisů („compliance“) a třetí linie zastává formu nezávislé kontroly, zpravidla interního auditu. Tento koncept je inspirován vojenským modelem obrany a aplikuje se na proces řízení rizik tak, aby byl zajištěn efektivní a koordinovaný přístup k identifikaci, hodnocení a zmírňování rizik. Byť je tento koncept považován odbornou veřejností za jeden z pilířů dobré praxe řízení rizik a za určitý doporučený rámec, je potřeba si uvědomit, že jeho aplikace v praxi nemusí vždy a za každých okolností a podmínek vyhovovat potřebám všech organizací.

Z tohoto titulu je třeba brát v potaz následující aspekty, které mají vliv na jeho efektivní fungování v praxi. Míra formálnosti implementace modelu by se měla lišit v závislosti na povaze podnikatelského záměru a velikosti organizace, přičemž by měl být brán ohled na její rizikový profil. Ve skutečnosti tak nemusí být role a odpovědnosti mezi jednotlivými liniemi vždy jasně vymezené a může docházet k prolínání funkcí napříč jednotlivými liniemi obrany. Prakticky je možné konstatovat, že organizace disponují značnou mírou flexibility v otázce implementace tohoto modelu a záleží na vyhodnocení specifických potřeb organizace, zda se přikloní k jeho rigidnější, nebo naopak volnější formě. **V každém případě však dobrá praxe řízení rizik vyžaduje integraci interního systému řízení rizik do celkové organizační struktury organizace a jejich aktivit a procesů.**

Výhody a úskalí lidského potenciálu

Zvolený přístup k řízení rizik v rámci organizace musí vždy počítat se závislostí na lidském faktoru, který má významný vliv i na výše popsany model tří linií obrany. Lidský faktor zastává v rámci procesu řízení rizik významnou roli a má jak pozitivní, tak negativní dopad na efektivitu celého systému. Tam, kde se lidský faktor stává výhodou, např. zkušenost a správný úsudek, schopnost přizpůsobit se nebo porozumět kontextu, se může při nedostatečné míře vzdělávání a pracovní odbornosti stát brzdicím prvkem. Organizace by proto měly s lidským potenciálem pracovat a rozvíjet ho tak, aby zaměstnanci podílející se na procesu řízení rizik disponovali dostatečnou pracovní kvalifikací a měli odpovídající pracovní schopnosti a zkušenosti. Důraz a podpora této oblasti ze strany organizace spolu se zavedením vhodných kontrol významně přispívá ke zmírňování výskytu lidských chyb, které mohou narušit kvalitu procesů v rámci jednotlivých linií obrany. Neodpovídající hodnocení, neefektivní monitoring nebo špatná rozhodnutí mohou vést k selhání systému interní kontroly. K eliminaci lidských chyb přispívá i definování

procesů v oblasti řízení rizik. Srozumitelně popsané postupy a procesy jsou prospěšným vodítkem i pro méně zkušené zaměstnance.

Spolupráce v řízení rizik – alfa a omega

I za předpokladu, že je model tří linií obrany dobře navržený a strukturovaný, závisí jeho efektivita na tom, jak dobře se tyto faktory integrují do každodenních procesů organizace. Především v oblasti komunikace a spolupráce mezi jednotlivými liniemi obrany je sdílení potřebných informací klíčové pro efektivní řízení a může přispět k nastavení centrálního systému pro evidenci rizik. Jednotný a centrální systém pro evidenci rizik umožňuje soustředění veškerých relevantních informací týkajících se řízení rizik a dodržování předpisů na jednom místě, přičemž umožňuje transparentní přístup všem zúčastněným stranám. To zajišťuje vyšší efektivitu procesu hodnocení, přesnost a aktuálnost využívaných informací a minimalizuje možnost vzniku nedorozumění a nepřesností v komunikaci.

„Rizika, se kterými organizace nepracují, lze přirovnat k černé díře, která pohlcuje zdroje i potenciál.“

Integrace systému řízení rizik by měla probíhat i na datové úrovni za účelem minimalizace potenciálních duplicit informací a rizika chyb způsobených ručním zadáváním dat. V závislosti na vyspělosti interního systému řízení rizik by organizace měly zvážit implementaci automatizovaných nástrojů a pracovních postupů (tzv. workflows), které zvyšují efektivitu hodnocení rizik, podporují pravidelný monitoring a pomáhají sledovat klíčové ukazatele (key performance indicators, key risk indicators nebo key control indicators). Ty jako celek napomáhají rychle odhalit potenciální problémy a přijmout

preventivní opatření. Automatizované nástroje při správné technické a businessové implementaci mohou významně podpořit jednak spolupráci napříč liniemi obrany, a taktéž integraci řízení rizik s ostatními aktivitami organizace.

Dynamičnost a kontinuita procesu řízení rizik

Řízení rizik je kontinuální a nikdy nekončící proces. Nejen finanční krize, ale v nedávné době i pandemie onemocnění covid-19 nebo válka na Ukrajině ukázaly, jak signifikantně je možné ovlivnit vývoj obchodního prostředí. Během pandemie byly organizace nuceny čelit novým a neočekávaným rizikům, jako je přerušování dodavatelských řetězců, snížená poptávka po produktech nebo službách, technologické výzvy při zavádění práce na dálku (tzv. home office) nebo kybernetické hrozby. Konflikty a války mohou mít rozsáhlé dopady na regionální i globální obchodní a politické prostředí. Řízení rizik tak musí v každém případě zohledňovat tato specifická rizika a organizace musí být připraveny na ně dynamicky reagovat, mj. revidovat a aktualizovat své plány kontinuity podnikání a krizového řízení.

Zvýšené povědomí o rizicích a nároky na dodržování předpisů ze strany vlád a orgánů dozoru mohou řízení rizik v organizacích ovlivnit. Zpřísnující se regulace mohou vyžadovat důkladnější monitorování rizik, zlepšení interních kontrol a postupů a vyšší transparentnost v podnikání. Organizace musí být schopny se přizpůsobit novým právním požadavkům a zajistit, aby všechny aspekty řízení rizik byly v souladu s přicházejícími regulacemi.

Environmentální a geopolitické události, jako jsou pandemie nebo vojenské konflikty, a nově přicházející regulatorní požadavky mají potenciál významně ovlivnit strategie a postupy řízení rizik v organizacích. Přístup k řízení rizik musí být proto pružný a musí být schopen se rychle přizpůsobit novým výzvám a podmínkám. Důležité je pravidelně revidovat a aktualizovat strategii

řízení rizik, aby organizace mohly adekvátně reagovat na aktuální a budoucí události.

Situace v České republice

V České republice se setkáváme jak s vysokou úrovní řízení rizik, která přejímá mezinárodní standardy v této oblasti a je zpravidla patrná u nadnárodních společností působících v tuzemsku, tak s méně rozvinutým systémem pro řízení rizik, který je typický pro malé nebo středně velké organizace, které svým oborem podnikání působí v méně regulovaných odvětvích. Tyto organizace se také zpravidla potýkají s omezenými zdroji, které mají pro tuto oblast k dispozici. Výše uvedený vývoj událostí má však za následek zvyšující se nároky na interní systém řízení rizik dopadající i na tyto společnosti. Tyto organizace by si měly uvědomit, že nově přicházející požadavky nepředstavují pouze zátěž z pohledu nutné počáteční investice, ale také benefit, který jim umožní znát svoje rizika, začít s nimi pracovat a efektivně je řídit.

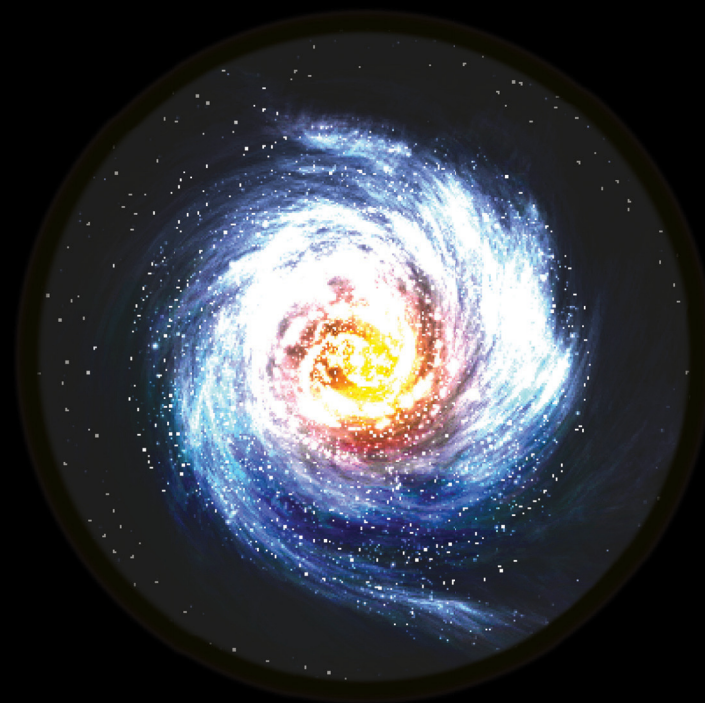
Shrnutí

Závěrem lze konstatovat, že dobrá praxe řízení rizik zahrnuje nejen zavedení modelu tří linií obrany, který odpovídá specifickým potřebám konkrétní organizace, ale i kontinuální vzdělávání a rozvoj lidského kapitálu v oblasti řízení rizik a podporu vzájemné spolupráce napříč liniemi obrany, která je nezbytným předpokladem pro efektivní fungování celého systému.

Dynamická povaha řízení rizik vyžaduje pružný přístup a schopnost rychle reagovat na nové výzvy a změny v obchodním a regulačním prostředí. Efektivitu řízení rizik lze v tomto ohledu významně posílit pomocí integrovaných nástrojů, jako jsou governance, risk and compliance („GRC“) systémy. GRC systém umožňuje organizaci sjednotit a automatizovat procesy související se správou, řízením rizik a dodržováním předpisů, výrazně zvyšuje účinnost řízení rizik a poskytuje komplexní pohled na rizikový profil organizace, přičemž usnadňuje spolupráci mezi jednotlivými liniemi obrany. Ať již organizace v rámci řízení rizik využívají interních systémů, nebo se rozhodnou pro implementaci komplexního GRC řešení, je zřejmé, že správné řízení rizik je klíčem k dlouhodobému úspěchu a odolnosti organizace v rychle se měnícím prostředí, a proto by mělo patřit mezi hlavní strategické cíle každé organizace.

Celkově lze tvrdit, že řízení rizik není pouze frází, ale klíčovým prvkem pro úspěch a udržitelnost každé organizace. Důkladné a efektivní řízení rizik umožňuje organizacím nejen minimalizovat negativní dopady neočekávaných událostí, ale také využívat příležitosti pro růst a inovace. Zavedení modelu tří linií obrany přináší strukturovaný rámec pro řízení rizik, přičemž je důležité vzít v úvahu specifika a potřeby konkrétní organizace. ■

Deloitte.



Risk Advisory Poradenství v oblasti řízení rizik

Kybernetické a strategické riziko | Operační riziko a vnitřní kontrolní systém | Regulatorní a právní riziko | Farmaceutický průmysl a zdravotnictví | Udržitelnost a ESG | Finanční kriminalita

**Proměňte potenciální hrozby
v konkurenční výhodu!**



ŘÍZENÍ RIZIK VE VEŘEJNÉ SPRÁVĚ — BEZ ODHODLÁNÍ VRCHOLOVÉHO MANAGEMENTU TO NEPŮJDE



Zákon o finanční kontrole¹ (dále jen „zákon“), metodický pokyn k řízení rizik², vzorová směrnice k řízení rizik³. Na první pohled by se mohlo zdát, že veřejná správa v České republice má ty nejlepší předpoklady správně řídit rizika při svých činnostech, pro zjednodušení myšleno jakékoliv finanční operaci příjmové i výdajové.

Ing. Valdemar Adamiš

Vedoucí oddělení Harmonizace finančního řízení

Na Ministerstvu financí působí na Centrální harmonizační jednotce, kde se věnuje kontrole evropských fondů, principům 3E a řízení rizik ve veřejné správě.

Minimálně tedy z pohledu teoretického, kdy se jistě nenajde organizace, která by ve svých vnitřních předpisech neměla zmínku, nebo celou oblast řízení rizik, neměla správně procesně upravenou a neměla zavedeny nástroje na řízení rizik. Nakonec zákon tuto činnost má mezi svými základními cíli⁴. Bohužel textace obou ustanovení umožňuje kreativní výklad toho, jaké konkrétní činnosti mají zajistit dodržování těchto ustanovení. Právě proto, že zákon dává vedoucímu organizace relativně velkou volnost v tom, jak má nastavit vnitřní kontrolní systém, zejména s odkazem na jeho přiměřenost a účinnost, je nastavení procesu řízení rizik oblastí, kterou jde velmi snadno

organizovat procesně správně, avšak bez konkrétní věcné náplně. To, že tím nebude naplněna ani povinnost vycházet při zavádění a řízení finanční kontroly z mezinárodně uznávaných standardů⁵, je nasnadě.

„Dokud nebude mít vedoucí organizace chuť se rizikům věnovat, samotní manažeři na nižších pozicích tu vůli mít tuplem nebudou.“

Věcný pohled na řízení rizik, tj. tlak vedoucího organizace nebo vrcholového managementu na to, aby každý zaměstnanec⁶, který přijde

¹ Zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole)

² Metodický pokyn CHJ č. 2, Metodický pokyn CHJ č. 2 – Metodika řízení rizik | 2016 | Ministerstvo financí ČR (mfc.cz)

³ Metodický pokyn CHJ č. 11, Metodický pokyn CHJ č. 11 – Vzorová směrnice o řízení rizik | 2020 | Ministerstvo financí ČR (mfc.cz)

⁴ Ustanovení §4 odst. 1 písm. b) a ustanovení §25 odst. 1 písm. b) zákona o finanční kontrole

⁵ Komponenta č. 2 standardu COSO – Zhodnocení rizik

⁶ Například vedoucí zaměstnanec v roli příkazce operace

do styku s veřejnými prostředky, znal nejen proces řízení rizik, definici a formu opatření k minimalizaci rizik, ale především dokázal zacílit své myšlenky a skutečně vidět rizika, umět je správně popsat, odhadnout jejich významnost, a zejména přijmout vhodné opatření k nápravě a předat tuto informaci vrcholovému vedení, je podmínkou nutnou. Dokud nebude mít vedoucí organizace chuť se rizikům věnovat, samotní manažeři⁵ na nižších pozicích tu vůli mít tuplem nebudou. Samotná vůle ani znalost těchto podřízených vedoucích zaměstnanců toho, jak k rizikům přistupovat, není ani podmínkou postačující, aby byla rizikům v organizaci věnována dostatečná pozornost.

„Hlavním problémem tak stále zůstává zamyslet se, správně definovat a popsat riziko a navrhnout příslušné opatření, jehož plnění bude vymáháno.“

Postupná degradace vůle reportovat o rizicích, když chybí jakákoliv odezva nebo jsou reportovaná rizika a opatření k jejich minimalizaci využívána pro zcela jinou potřebu, vede k tomu, že procesně se děje sice správně, ale činnosti všech zaměstnanců, kteří takto postupují, jsou vlastně zbytečné. S odkazem na účelný, hospodárný a efektivní výkon veřejné správy je nasnadě, že vynaložení výdajů na nevyužívané činnosti by nemělo být považováno za souladné s principy 3E. Samotné řízení rizik, byť procesně a formálně správné, se tak vlastně stává inherentním rizikem pro samotnou organizaci.

Zcela nerelevantní pro výše uvedené je úvaha o zavedení centralizované nebo decentralizované formy řízení rizik. Tato forma opět řeší pouze samotný proces a ukotvení odpovědností v organizační struktuře, nedokáže ale

vyřešit přístup těchto odpovědných osob. Pokud se ustanoví centrální forma s nominovaným manažerem řízení rizik, může to přispět ke skutečnému řízení rizik pouze v případě, že je zde opět vůle vedení organizace jeho výstupy nejen akceptovat, ale i aktivně využívat a jeho činnost podporovat. Hlavním problémem tak stále zůstává zamyslet se, správně definovat a popsat riziko a navrhnout příslušné opatření, jehož plnění bude vymáháno. Pokud není k riziku přiřazeno opatření k jeho řízení nebo není jeho plnění vymáháno, není možné na řízení rizik pohlížet jako na správně zavedený mechanismus. V decentralizovaně pojetém řízení rizik mají úplně stejnou pozici vedoucí zaměstnanci jako manažer řízení rizik v centralizovaném modelu. S tím rozdílem, že mají, nebo by měli mít, stoprocentní znalost své agendy, a tedy i rizik, která se na jejich úrovni vedení vyskytují. A opět, funkční proces nemusí znamenat funkční řízení rizik.

Nefunkčnost řízení rizik se mnohdy snaží napravit interní audit. Je to zcela správně, pokud je to v roli doporučení navazujícího na audit některé z vykonávaných činností organizace nebo konzultace. Praxe řady ústředních orgánů, ale i územních samosprávných celků zdá se však býti odlišná. Mnohdy je to útvar interního auditu, který navrhuje směrnice, a tedy proces řízení rizik a nástroje k jeho řízení. Důvodem, proč tomu tak je, není těžké porozumět. Interní auditoři mnohdy bývají v organizaci jediní, kteří rizika aktivně využívají pro zpracování plánu auditu, a dokážou je tedy věcně správně vnímat. Interní audit by však v žádném případě do volby modelu, konkrétního nastavení procesů řízení rizik, nebo snad odpovědností vedoucích zaměstnanců zasahovat neměl. To je výlučným právem, a jak jsem uvedl výše, povinností vedoucího organizace.

Kdo by ale tedy kromě interního auditu měl poskytovat dovnitř organizace servis k řízení rizik ve smyslu vysvětlování toho, proč je řízení rizik důležité. Nakonec,

nebo možná na začátek, poslední tři roky ukázaly, jak je řízení rizik důležité, a pokud není v orgánech veřejné správy nastaveno správně, jaké může mít dopady. Ztráta peněžních prostředků na bankovních účtech, zpoždování vyplácní podpory nebo proplacení faktur nekomunikujícím obchodním partnerům z Číny by mělo být mementem připomínajícím vedoucím organizací důležitost práce s riziky. Vše tedy začíná od vedoucího organizace, který musí tlačit (A) své podřízené k tomu, aby s riziky aktivně pracovali. Zároveň musí dát jasně najevo, že identifikovaná rizika nebudou podkladem například pro špatné služební hodnocení a že navržená opatření jsou zavedena a jejich dodržování vymáháno.

„Ztráta peněžních prostředků na bankovních účtech, zpoždování vyplácní podpory nebo proplacení faktur nekomunikujícím obchodním partnerům z Číny by mělo být mementem připomínajícím vedoucím organizací důležitost práce s riziky.“

Schválně jsem použil slovo tlačit, protože proces to bude dlouhodobý a nebude jednoduché věcnou podstatu řízení rizik podřízeným vedoucím zaměstnancům vštípit. Samozřejmě onu vzdělávací a osvětovou činnost musí dělat někdo jiný než vedoucí organizace. Kromě manažera řízení rizik v rámci centralizovaného modelu se nabízí role koordinátora a metodika řízení rizik (B). Jeho práce je však mnohdy úkolem nevděčným. Pokud ale platí (A), pak bude mít mnohem jednodušší pozici a nebude muset pouze neefektivně reportovat. Skutečně pak dojde k přenosu znalostí a navnímání důležitosti řízení rizik nad každým rozhodnutím

⁵ Komponenta č. 2 standardu COSO – Zhodnocení rizik

o veřejném výdaji či příjmu. Samozřejmě ani tato pozice není nutná. Je to ale vhodný prostředník mezi vrcholovým vedením organizace, vedoucím organizace, a v uvozovkách řadovými vedoucími zaměstnanci, které jistě nebude školit ani směřovat sám vedoucí organizace. Vrcholové vedení organizace však dá řízení rizik váhu, kterou prostředník může vhodně přetransformovat v každodenní operativní pomoc všem vedoucím zaměstnancům v organizaci nad jakýmkoliv rozhodnutím, vyhlášením veřejné zakázky nebo podáním žádosti o dotaci. To jsou totiž aktivity, kde všechna rizika vznikají a kde je vhodné, ať už úvahu, nebo záznam k riziku, a hlavně přijatému opatření k jeho minimalizaci vést. Proto není nutné zavádět žádné nové speciální nástroje nebo například informační systém. Ty již většinou nad stávajícími rozhodnutím v organizaci běží a jsou zavedeny.

„Bez navržení kvalitního opatření k ošetření rizika, informování vedení a jeho zájmu o rizika a skutečného zavedení takového opatření do praxe nad rozhodnutími v organizaci zůstane řízení rizik jen prázdným procesem.“

Vedoucí zaměstnanci, kteří pak v rámci své agendy budou rizika řídit věcně, nikoliv pouze formálně a procesně správně, mohou předejít závažným škodám nebo zajistit dlouhodobě úspěšné fungování organizace. Jak jsem již uvedl, pak lze na jejich činnost nahlížet jako na činnost účelnou, hospodárnou a efektivní (C). Tím je pak zcela naplněna dílčí část zákona a minimálně dva ze čtyř jeho základních cílů. Tedy ona v textu zmíněná

písmena vyjadřující rovnici $A + B = C$ beze zbytku budou platit a přinesou kýžený synergický efekt v ochraně veřejných prostředků.

Skvěle vymyšleno, ale jak to převést do praxe. Jak donutit vrcholové vedení a vedoucího organizace k tomu, aby řízení rizik dali potřebnou váhu a tlak? Příklady, které jsem uvedl v textu, mohou sloužit jako připomínka toho, co se může vše stát, když vnitřní kontrolní systém na rizika přestane reagovat, respektive je identifikovat a přijímat přiměřená opatření k jejich minimalizaci. Osobní odpovědnost za chybné finanční operace, které neměly ošetřena rizika, může být dalším nástrojem, ale ideálně až té poslední instance. Jakékoliv volání po osobní odpovědnosti by mělo následovat až poté, co jsou všechna ostatní možná řešení vyzkoušena a v praxi se ukážou jako nefunkční. V opačném případě by pouhé zavedení osobní odpovědnosti mohlo znamenat jen větší odpor vedoucích zaměstnanců se o rizika být jen zajímat.

Z těchto důvodů ani příslušné metodické vedení v této oblasti nemůže a nesmí skončit pouze u nastavení procesů. Směrem, kterým je potřeba se vydat, je řízení rizik přizpůsobit činností organizace a prakticky ho vykonávat nad každým výdajem, příjmem nebo rozhodnutím. To mimo jiné znamená konkrétně odhalená rizika popsat a co nejlépe se s nimi vypořádat a zajistit, že s nimi bude pracovat vrcholový management orgánů veřejné správy. Zde nezbývá než konstatovat. Je skvělé rizika identifikovat a přiřadit jim významnost v grafu. Bez navržení kvalitního opatření k ošetření rizika, informování vedení a jeho zájmu o rizika a skutečného zavedení takového opatření do praxe nad rozhodnutími v organizaci, zůstane řízení rizik jen prázdným procesem. To, aby se tak nestalo, je úkol, před kterým stojím nejen já sám v rámci své činnosti na Ministerstvu financí, ale každý, kdo to s riziky ve své organizaci myslí vážně. ■

S autorem článku se můžete setkat na seminářích ČIIA

REGISTRUJTE SE NA SEMINÁŘE

Lektor: **Ing. Valdemar Adamiš**

STANDARDSY COSO – INTEGROVANÝ RÁMEC PRO VNITŘNÍ KONTROLNÍ SYSTÉM (20. listopad 2023)

Obsah:

- Standardy COSO úvod.
- Komponenty.
- Principy.
- 3 linie obrany.
- Případová studie aplikace standardu v českém právním prostředí.

PŘÍSTUPY KE VZORKOVÁNÍ V RÁMCI INTERNÍHO AUDITU (6. prosinec 2023)

Obsah:

- Základní pojmy a obecný postup.
- Rozdělení postupů a metod šetření vzorku.
- Statistické výběry.
- Výběry při testech vlastností.
- Výběry při testech proměnných.
- Nestatistické výběry.
- Hodnocení procesů z výsledků získaných ze vzorků.

Objednávejte na webu ČIIA (www.interniaudit.cz) nebo na prihlasky@interniaudit.cz

Rizika v podnikání, význam a formy jejich řízení

Podnikatelské a manažerské rozhodování se může uskutečňovat za jistoty, tj. za situace, při které víme s určitostí, jaké budou výsledky rozhodnutí. Mnohem častější je však rozhodování za nejistoty, při které neznáme pravděpodobnost, jaká budoucnost nastane při konkrétním rozhodnutí. Pokud tuto pravděpodobnost známe, hovoříme o rozhodování za rizika. Riziko je tedy spojeno s pravděpodobností, tj. možností, že budoucnost bude jiná, než jsme očekávali. Rozeznáváme tzv. riziko čisté, což je pravděpodobnost, že určitá událost či jev bude mít negativní vliv na organizaci, která rozhoduje. Vedle takto chápaného rizika však existuje i riziko podnikatelské, které spojuje možnost neúspěchu s nadějí na úspěch.

prof. Ing. Jiří Dvořáček, CSc.

Katedra strategie

Fakulta podnikohospodářská

Vysoká škola ekonomická v Praze

Riziko je budoucí událost, a proto existuje možnost riziko řídit. Pokud riziko nebylo řízeno, představuje tato nežádoucí událost pro organizaci problém. Každé riziko má tři rozměry, a to možnost (že určitá událost nastane), významnost (jaké důsledky tato událost může znamenat) a četnost (některá rizika se vyskytují pravidelně, souvisejí např. se sezonním charakterem činnosti, jiná se vyskytují sporadicky).

Rizika lze třídit i podle jejich charakteristických vlastností, což je důležité pro vlastní řízení rizik. Kromě kategorizace rizik na tzv. čisté riziko a riziko podnikatelské lze hovořit o riziku systematickém (postihuje v různé míře všechny podnikatelské subjekty a nelze ho snižovat diverzifikací – patří sem např. daňová legislativa) a nesystematické (je specifické pro každý podnikatelský subjekt a lze ho diverzifikovat – např. změna dodavatele). Další kategorizací rizik může být jejich dělení na rizika vnitřní a rizika vnější. Vnitřní rizika vyplývají z charakteru organizace (např. selhání zaměstnance,

kteří vede k možnému podvodu), vnější rizika ve vztahu k okolí podniku (např. vývoj poptávky). Rizika lze dále členit např. na ovlivnitelná a neovlivnitelná, primární a sekundární, rizika vyskytující se v různých fázích realizace projektu apod.

„Riziko je budoucí událost, a proto existuje možnost riziko řídit.“

Podnikatelé či manažeři mohou k riziku zaujmout některý z následujících postojů:

- neutrální, kdy ochota riskovat přímo úměrně souvisí s pravděpodobností úspěchu,
- averze k riziku, při které je ochota k riskování menší než pravděpodobnost úspěchu,
- sklon k riziku, kdy ochota riskovat je větší než pravděpodobnost úspěchu.

Úroveň přijatelných rizik závisí na očekávaném prospěchu.

Největší riziko a největší prospěch se musí vyplatit. Riziko, které je vyšší než prospěch, nemá cenu podstupovat. U vysokého rizika podnikatelé a manažeři očekávají vysoký prospěch (užitek) a samozřejmě preferují nízké riziko s vysokým užitekem.

Proces řízení rizika přibližuje obrázek č. 1.

Řízení rizika (risk management) zahrnuje:

- strategické cíle organizace,
- zhodnocení rizika (analýza rizika, identifikace rizika, popis rizika, posouzení rizik, ohodnocení rizika),
- reportování o riziku (hrozby a příležitosti),
- rozhodnutí,
- řízení rizika,
- reportování o reziduálním riziku (interní a externí reportování),
- monitorování.

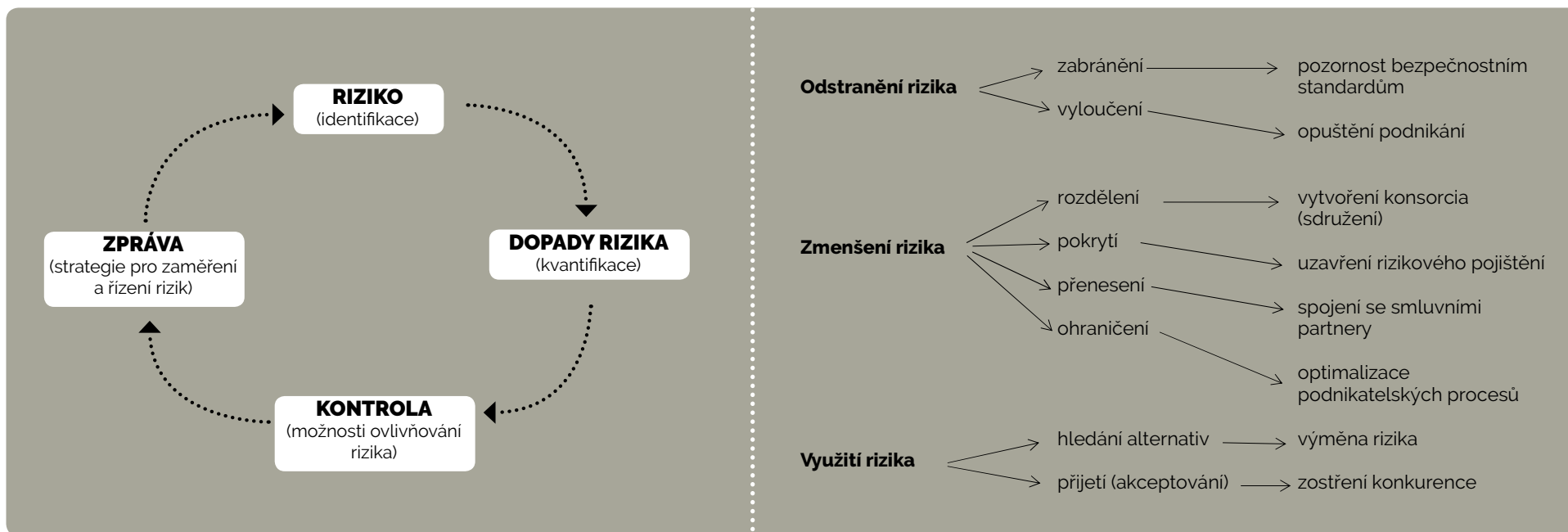
K technikám identifikace rizika zejména patří:

- brainstorming,
- dotazníky,
- podnikatelské studie, v nichž každá činnost popisuje a analyzuje vnitřní a vnější faktory, které na tuto činnost působí,
- analýzy scénářů,
- workshopy na posuzování rizika,
- vyšetřování nehod,
- audity a inspekce.

Velikost rizika lze vyjádřit buď prostřednictvím kvantitativních (číselných) charakteristik rizika, nebo pomocí kvalitativních (popisných) charakteristik rizika.

Kvantitativními charakteristikami rizika se rozumí číselné stanovení velikosti rizika určité podnikatelské aktivity. To vyžaduje kvantitativní charakter veličiny (kritéria), vzhledem ke kterému se riziko určuje, a znalost rozdělení jeho pravděpodobnosti.

Kvalitativní charakteristiky rizika lze k popisu rizika a jeho velikosti



Obrázek č.1 Proces řízení rizika

Obr. č. 2 Možné způsoby řízení rizika

použit zejména tehdy, pokud nejsou k dispozici charakteristiky kvantitativní (není známé např. rozdělení pravděpodobnosti).

„Řízení rizik je spojeno s náklady, které je nutné kvantifikovat.“

Tyto charakteristiky mají podobu verbálních (slovních) popisů a vytvářejí stupnice kvalitativního vyjádření rizika. Nejčastěji se v této souvislosti využívají popisy, posudky nebo názory odborníků v dané oblasti, které jsou získávány aplikací specifických metod.

Možné způsoby řízení rizika přibližuje obrázek č. 2 na předchozí straně.

Řízení rizik je spojeno s náklady, které je nutné kvantifikovat. Celkové náklady jsou představovány jak náklady na prevenci (ty se mohou v čase zvyšovat), tak náklady na likvidaci potenciálních či skutečných ztrát (ty mohou, v souvislosti s růstem nákladů na prevenci, v čase klesat). U celkových nákladů je možné hledat jejich optimum, resp. posuzovat jejich vývoj v čase ve vztahu k tržbám, aktivu, počtu zaměstnanců apod.

Pro řízení rizik lze využít normu ČSN ISO 31000 Management rizika – Principy a směrnice, která je z let 2009 a 2018, a její podsložku ISO IEC 31010 Risk assessment techniques. Na ošetřování rizik se zaměřuje norma ČSN EN 62198 z roku 2014.

K řízení rizik na firemní úrovni je také k dispozici rámec COSO ERM (Enterprise Risk Management) z roku 2004 a novelizovaný v 2014. Rámec má přispět k dosažení dvou cílů:

1. Identifikace kritických rizik, kterým je organizace vystavena, včetně dobrého jména, etiky nebo zdravotních, bezpečnostních a environmentálních rizik (nikoliv pouze finančních či pojistitelných rizik).
2. Řízení a optimalizace portfolia rizik, která jsou vlastní všem činnostem s dopadem na zisk organizace.

COSO ERM přináší širší pohled na řízení rizik, viz tabulka 1.

Novela z roku 2014 reaguje jednak na nová rizika, ale hlavně spojuje proces řízení rizika s firemní strategií, čemuž odpovídá i nový název rámce „Řízení podnikových rizik – integrace se strategií a výkonností“.

„Bez využívání (podstupování) rizika by nebyly inovace, nebyl by žádný pokrok.“

Jinou pomůckou pro řízení rizik je materiál, který v roce 2013 vydal Mezinárodní institut interních auditorů pod názvem The Three Lines of Defense in Effective Risk Management and Control. V 1. a 2. linii je management odpovědný za dosažení cílů organizace. Přitom v 1. linii jsou vymezena přijatelná rizika a provádí se dohled nad jejich řízením. Ve 2. linii

System risk managementu se rozvíjí

OD → → → → → **K**

- | | |
|---|---|
| ■ rizik jako jednotlivého nebezpečí | ■ riziku v kontextu podnikové strategie |
| ■ identifikace a posouzení rizik | ■ vytvoření „portfolia“ rizik |
| ■ zaměření na všechna rizika | ■ zaměření na kritická rizika |
| ■ zmírnění rizik | ■ optimalizaci rizik |
| ■ omezení rizik | ■ strategii řízení rizik |
| ■ rizik, která nemají žádného vlastníka | ■ odpovědnostem za definované riziko |
| ■ kvantifikace náhodného rizika | ■ monitorování a měření |
| ■ rizika, které není mojí odpovědností | ■ riziku, které je odpovědností každého |

Tab. 1 Chápání rizik podle COSO ERM

management zabezpečuje neustálé zlepšování postupů pro řízení rizik. Ve 3. linii působí interní audit, který poskytuje ujištění, že rizika jsou známa a jsou pod kontrolou. Pojem „obránné linie“ je poněkud zavádějící, neboť odporuje chápání podnikatelského rizika jako využívání příležitosti. Bez využívání (podstupování) rizika by nebyly inovace, nebyl by žádný pokrok.

Svět podnikatelských rizik se neustále mění. Evropská federace rizikových manažerů (FERMA) ve svém reportu zveřejněném v roce 2023 uvádí jako současná tato nejvýznamnější rizika:

- kybernetické hrozby, což je spojeno s rostoucím využíváním home office a pokračující digitalizací operací v organizacích,
- selhání dodavatelských a odběratelských řetězců, jako důsledek pandemie, kdy docházelo k omezení, resp. i zastavování řady výroby,
- geopolitické nejistoty, zejména situace na Ukrajině a protiruské sankce,
- nejistoty týkající se ekonomického růstu, což souvisí s inflací a rostoucími náklady,
- přílišná regulace ekonomiky, např. zavádění ESG (viz dále).

„Pojem ‚obránné linie‘ je poněkud zavádějící, neboť odporuje chápání podnikatelského rizika jako využívání příležitosti.“

V horizontu příštích tří let průzkumy FERMA uvádějí tato kritická rizika:

- změny spotřebitelského chování,
- kybernetické hrozby,
- nejistoty kolem ekonomického růstu.

Pro horizont příštích deseti let jsou za kritická považována následující rizika:

- klimatické změny,
- změny spotřebitelského chování,
- přírodní pohromy.

Podnikatelé a firmy se již setkávají s novými riziky, která jsou spojena s prostředím, ve kterém firmy působí, a s důrazem na tzv. udržitelný rozvoj. Nejprve to byla dobrovolně zaváděná Společenská odpovědnost organizací (CSR – Corporate Social Responsibility). Dobrovolnost se však začíná nahrazovat povinností, a ta je spojena s ESG, kde E je environmentální politika firmy, S představuje sociální odpovědnost firmy a G se týká řízení firmy a celého jejího dodavatelského řetězce. ESG souvisí s celkovou strategií firmy a je zaměřena na monitorování jejich aktivit v uvedených oblastech. K monitorování ESG slouží CSRD (Corporate Sustainability Reporting Directive), což je směrnice zaměřená na nefinanční reportování, které má mít podobnou formu jako reportování u finančních výkazů. Nejprve má být toto reportování (od roku 2024) povinné u firem s více než 250 zaměstnanci nebo u firem kótovaných na burze, postupně se má rozšiřovat i na firmy menší velikosti, a to nejpozději od roku 2028. Zpráva o udržitelnosti budoucího rozvoje má mít jednotnou podobu a bude ověřována statutárním auditorem. Úspěšnost řízení rizik bude posuzována proti benchmarku, obsaženému v CSRD. Firmy, které se s riziky úspěšně vyrovnají, budou mít lepší vyjednávací pozici např. ve vztahu k bankám, investorům, dodavatelům i odběratelům. Mohou zvyšovat svou reputaci i před širokou veřejností.

Každý podnikatelský subjekt je zranitelný a riziko je součástí podnikání. Riziko je předpokladem pro inovace, a bez nich žádný podnikatel neuspěje. Z řízení rizik musí podnikatel profitovat, chápat je jako příležitost a být vždy připraven předcházet možným krizím, které jsou důsledkem nezvládnutého rizika. ■



Interní audit v pojišťovnách z pohledu České národní banky



Ing. Karla Voráčková získala své pracovní zkušenosti týkající se sektoru pojištnictví během své dlouholeté auditorské praxe ve společnosti KPMG. Od roku 2002 je statutárním auditorem zapsaným v seznamu Komory auditorů ČR. Od svého nástupu do České národní banky v roce 2015 působí v sekci dohledu nad finančním trhem. V současné době vede odbor dohledu nad pojišťovnami a penzijními společnostmi zabývající se dohledem obezřetnosti. Ve své dohledové činnosti se tak zaměřuje na otázky týkající se solventnosti a finanční situace tuzemských pojišťoven v kontextu jejich rizikového profilu a obchodního modelu. Důležitou oblastí, která je předmětem dohledu ČNB, je řídicí a kontrolní systém pojišťoven s důrazem na problematiku řízení rizik.

Od roku 2016 se tuzemské pojišťovny musí řídit pravidly, která přinesla evropská legislativa v podobě směrnice Solventnost II¹ (dále též jen „Směrnice SII“) a dále nařízení Komise v přenesené pravomoci², a jejímž smyslem bylo mimo jiné posílit rizikově orientovaný přístup a nastavit robustní systém řízení rizik a tomu odpovídající účinný řídicí a kontrolní systém (dále též jen „ŘKS“). Směrnice SII klade v rámci všech oblastí činnosti pojišťoven zcela zásadní důraz na včasnou identifikaci rizik a jejich odpovídající řízení tak, aby byla zajištěna rovnováha mezi strategickými a obchodními cíli pojišťovny a mírou jí podstupovaných rizik.

¹ Směrnice Evropského parlamentu a Rady 2009/138/ES o přístupu k pojišťovací a zajišťovací činnosti a jejím výkonu (Solventnost II).

² Nařízení Komise v přenesené pravomoci (EU) 2015/35, kterým se doplňuje Směrnice SII (dále též jen „Nařízení“).



Ing. Martina Höferová má více než 20leté zkušenosti z oblasti pojištnictví. Většinu své profesní kariéry působila na manažerských pozicích a ve vedení pojišťoven a několik let též ve společnosti KPMG, kde bylo její hlavní pracovní náplní poskytování poradenských služeb pro pojišťovny v oblasti regulace. Od svého nástupu do České národní banky v roce 2018 působí v sekci dohledu nad finančním trhem a zabývá se obezřetnostním dohledem nad činností a solventností a finanční situací tuzemských pojišťoven.

Tento přístup k řízení rizik, založený na třech pilířích obrany s **vyčleněním interního auditu** (dále též jen „IA“), resp. nově zavedené **klíčové funkce interního auditu, jako samostatné úrovně kontrolního systému,** tak **výrazně posílil důležitost role IA** v celkovém ŘKS v pojišťovnách. Důležitost IA dále roste i v současné době, kdy v důsledku velmi dynamického vývoje zejména externího prostředí dochází k neustálým změnám, které přinášejí nejen nové příležitosti, ale též řadu nejistot a nových rizik.

„Funkce IA musí být zcela nezávislá, aby její hodnocení mohlo být nestranné, nezaujaté, a tedy objektivní.“

Klíčové proto je, aby pojišťovny měly schopnost flexibilně reagovat na měnící se prostředí nejen identifikací a využitím nových obchodních příležitostí, ale také z hlediska obezřetného řízení rizik. Důležitým úkolem IA je poskytovat kvalitní zpětnou vazbu vedení společnosti v podobě posouzení, zda je ŘKS (včetně druhé linie obrany, kterou tvoří kontrolní klíčové funkce pojistně-matematická, funkce řízení rizik a funkce compliance) nastaven vhodně a spolehlivě.

Viz Směrnice SII – čl. 47, odst. 1:

Vnitřní audit

Pojišťovny a zajišťovny zřídí účinnou funkci vnitřního auditu. Funkce vnitřního auditu zahrnuje hodnocení, zda jsou systém vnitřní kontroly a další prvky řídicího a kontrolního systému vhodné a efektivní.

Funkce IA musí být nastavena, vykonávána a v rámci společnosti organizačně začleněna tak, aby byly naplňovány **hlavní zásady, principy a regulatorní požadavky** pro její výkon, které lze v zásadě shrnout do **následujících klíčových oblastí:**

Objektivita a nezávislost

Aby mohl IA plnit svoji roli **objektivní ověřovací funkce**, musí být zcela **nezávislý a prostý jakéhokoli střetu zájmů**. Nesmí být pod kontrolou nebo vlivem žádné jiné funkce ve společnosti a musí mít dostatečnou míru autonomie v rozhodování o svých aktivitách.

Funkce IA musí být nezávislá na všech činnostech, které kontroluje. Nesmí se tedy podílet na žádných provozních ani ostatních kontrolních činnostech, aby nemohlo docházet ke střetům zájmů, a aby její hodnocení mohlo být zcela nestranné, nezaujaté, a tedy objektivní.

Nezávislost je nezbytné zohlednit i při nastavování reportovacích linek v pojišťovně a v rámci systému odměňování. Dokonce i při vhodném organizačním zařazení funkce IA může její nezávislost či objektivitu omezovat to, dle jakých kritérií je držitel funkce IA odměňován, případně kdo tato kritéria stanovuje a vyhodnocuje jejich naplňování.

Viz Nařízení – čl. 271, odst. 1.

Osoby vykonávající funkci vnitřního auditu nesmí přijímat žádné povinnosti vyplývající z jakékoli jiné funkce.

Zdroje, kapacity a odborná způsobilost

Aby mohla funkce IA v plném rozsahu, účinně a efektivně dostát své roli, musí mít k dispozici vhodné nástroje, a zejména dostatečné personální kapacity vybavené potřebnou expertizou, tedy potřebnými odbornými znalostmi a zkušenostmi.

Za zajištění naplňování požadavků na odbornou způsobilost osob vykonávajících IA odpovídá představenstvo pojišťovny. Posouzení odborné způsobilosti nesmí být jen formální záležitostí, a není proto možné se omezit jen na „pouhé“ posouzení toho, zda jsou splněny základní kvalifikační předpoklady, například certifikace interního auditora.

Viz Nařízení – čl. 273, odst. 2.

Požadavky na způsobilost a bezúhonnost

Posouzení, zda je osoba způsobilá, musí zahrnovat posouzení odborné a formální kvalifikace této osoby, jejich vědomostí a příslušné praxe v odvětví pojišťovnictví, v jiných finančních odvětvích nebo v jiných oborech, a musí vzít v úvahu příslušné povinnosti, které byly této osobě uloženy, a případně i její pojistné, finanční, účetní, pojistněmatematické a řídicí dovednosti.

Pojišťovna by měla stanovit i další požadavky, především takové, které zohledňují specifika její činnosti. Pro kvalitní výkon IA je důležitým předpokladem nejen samotná znalost IA jako takového, ale rovněž dostatečné praktické zkušenosti a poměrně komplexní znalost problematiky pojišťovnictví, včetně příslušné regulace, a to jak na obecné úrovni, tak rovněž z hlediska specifík činnosti dané pojišťovny. To zahrnuje mj. i porozumění strategii společnosti a jejímu rizikovému profilu. Klíčové je též alespoň základní porozumění i vysoce odborným činnostem, jako je např. pojistně-technická oblast, investiční činnost a ALM či IT/IS problematika.

Samozřejmostí by mělo být průběžné kontinuální vzdělávání interních auditorů obnášející soustavné prohlubování a rozšiřování odborných znalostí tak, aby tyto osoby byly schopny flexibilně reagovat na změny a dynamický vývoj prostředí.

Při nedostatku interních personálních kapacit či při potřebě specifické expertizy může být relevantním řešením využití externího zajištění (dále též jen „outsourcing“) části nebo celého výkonu IA. A to jak prostřednictvím nezávislých externích subjektů, tak případně v rámci skupiny, jíž je pojišťovna součástí. Případné využití skupinového outsourcingu IA může přispět k posílení nezávislosti a umožnit přístup ke specifické odbornosti či přenos zkušeností ohledně „best practices“ v různých oblastech činnosti. V každém případě však **odpovědnost za klíčovou funkci IA vždy zůstává na pojišťovně**, konkrétně na interním držiteli této klíčové funkce přímo v pojišťovně a na jejím představenstvu.

Plánování interních auditů

Funkce IA musí mít nastavený jasný plánovací proces, zdokumentovaný a schválený plán své činnosti a pravidelně podávat zprávy o svém postupu vrcholovému vedení pojišťovny.

Nezávislý plán auditů musí vycházet z objektivní analýzy rizik. Užitečným zdrojem informací pro plánování IA mohou být mimo jiné výstupy z ORSA procesu. Plán by se měl zaměřovat zejména na důležité oblasti činnosti pojišťovny, především pak na ty, které mohou být zdrojem významných rizik. Dostatečná pozornost tak musí být věnována například činnosti upisování pojistných rizik, likvidaci pojistných událostí, investování, řízení rizik a kapitálu a dalším klíčovými oblastem, včetně IT/IS. A to i za situace, kdy by v rámci vlastního útvaru IA chyběly potřebné personální kapacity nebo dostatečná expertiza pro specifické zaměření auditu. V tom případě může být řešením využití outsourcingu, jak bylo zmíněno výše.

Důležité je, aby se plán auditů zaměřoval nejen na jednotlivé oblasti činnosti pojišťovny a příslušné procesy, ale aby docházelo k ověřování i jejich vzájemného propojení. **Hlavním cílem by vždy mělo**

být kritické posouzení, zda ŘKS pojišťovny funguje jako celek efektivně a smysluplně.

Viz Nařízení – čl. 271, odst. 3, písm. a), b) a c).

Funkce vnitřního auditu musí zahrnovat všechny tyto úkoly:

- a) vytvořit, zavést a udržovat plán auditů, který stanoví auditní práci, již je třeba vykonat v nadcházejících letech, se zohledněním všech činností a celého řídicího a kontrolního systému pojišťovny nebo zajišťovny;
- b) při rozhodování o svých prioritách uplatňovat přístup vycházející z rizik;
- c) o plánu auditů informovat správní, řídicí nebo kontrolní orgán.

V případě potřeby může funkce vnitřního auditu provádět i audity, které nejsou zahrnuty do plánu auditů.

Identifikace nedostatků, doporučení nápravných opatření a kontrola jejich implementace

Úkolem IA je **identifikace nedostatků a slabých míst**, jak v kontrolovaných procesech, tak v **ŘKS jako celku**, a **doporučení možných nápravných opatření k jejich odstranění** adresovaných vrcholovému vedení společnosti.

Aby činnost IA přinášela pojišťovně skutečnou přidanou hodnotu, je zcela zásadní, aby pojetí IA nebylo jen v podobě formálních „compliance“ auditů, které sice pokrývají základní činnosti, procesy a rizika, ale zaměřují se primárně na kontrolu formálního dodržování souladu činnosti pojišťovny s požadavky regulace, či dokonce jen s požadavky stanovenými interními předpisy.

Pokud útvar IA dobře rozumí nejen kontrolovaným procesům a celkovému prostředí, ale především je dobře obeznámen se strategickými cíli pojišťovny, měl by být

schopen relevantního kritického posouzení, nakolik je nastavení kontrolovaných procesů vhodné, funkční, a přispívá k celkové funkčnosti ŘKS pojišťovny. Opatření ke včas identifikovaným nedostatkům v interních procesech pak mohou být doporučována tak, aby nejen dostatečně refletovala rizika, kterým je či může být pojišťovna vystavena, ale **aby byla v souladu s celkovou strategií pojišťovny, a to včetně strategie řízení rizik a rizikového apetitu, a přispívala tak k jejímu obezřetnému řízení.**

Viz Nařízení – čl. 271, odst. 3, písm. d) a e).

Funkce vnitřního auditu musí zahrnovat všechny tyto úkoly:

- d) vydávat doporučení, jež vycházejí z výsledku práce vykonané v souladu s písmenem a), a o svých zjištěních a doporučeních alespoň jednou ročně podat písemnou zprávu správnímu, řídicímu nebo kontrolnímu orgánu;
- e) na základě těchto doporučení uvedených v písmenu d) ověřovat dodržování rozhodnutí přijatých správním, řídicím nebo kontrolním orgánem.

V návaznosti na navržená nápravná opatření a doporučení ke zlepšení musí pojišťovna nastavit i **následný proces kontroly implementace, tedy monitorování průběžného plnění opatření** schválených vedením společnosti. I v tomto případě je zásadní, aby kontrola nebyla formální, ale aby docházelo zejména k vyhodnocení, zda byla opatření implementována efektivně, jsou funkční, a zda bylo skutečně dosaženo požadovaného účelu.

Zkušenosti ČNB z dohledové činnosti

ČNB se při své dohledové činnosti setkává s tím, že ne vždy jsou výše uvedené principy pro optimální

fungování IA v praxi naplňovány, a u některých pojišťoven vnímá nedostatky jak v samotném nastavení IA, tak při jeho výkonu.

„Vhodně nastavená funkce interního auditu může pro pojišťovnu představovat zásadní přidanou hodnotu a významně přispívat k naplňování strategie a cílů pojišťovny.“

Typickým nedostatkem z hlediska nastavení funkce IA bývá střet zájmů, který může být na úkor naplnění podmínky nezávislosti. U menších pojišťoven identifikovala ČNB tento problém nejčastěji v takových případech, kdy se u osoby zastávající funkci IA kumuluje další klíčová funkce.

U větších pojišťoven se ČNB setkává se vznikem střetu zájmů v případech, kdy je funkce IA v gesci některého z členů představenstva, který zároveň odpovídá za jinou oblast činnosti, v rámci níž dochází k významnému nabírání rizik. Dalším nedostatkem bývá nedostatečné zabezpečení potřebných kapacit či odborností, a to zejména pro audit specializovaných činností.

V rámci samotného výkonu IA pozoruje ČNB u pojišťoven nedostatky jak z hlediska oblastí, na které se IA



zaměřuje, tak z hlediska způsobu, jakým jsou audity vykonávány. Příkladem může být nedostatečný soulad mezi oblastmi, na které se IA zaměřuje, a oblastmi či procesy, které jsou přirozeným zdrojem hlavních rizik pro pojišťovnu. Nedostatečná pozornost bývá věnována samotnému řízení rizik. Častým nedostatkem bývá též situace, kdy jsou audity zaměřeny na formální soulad s interními předpisy, aniž by docházelo ke skutečnému posouzení, zda dochází k naplnění základního účelu kontrolovaného procesu.

Závěr

Je zřejmé, že rozsáhlá regulace v oblasti pojištnictví týkající se činnosti interního auditu a požadavky z ní vycházející představují pro pojišťovny a útvary IA nemalou zátěž. A to jak z hlediska finančního, organizačního, kapacitního, tak i procesního zatížení.

Klíčové je zejména udržení nezávislosti a objektivity, dostatek personálních zdrojů disponujících potřebnými zkušenostmi a znalostmi, kvalitní plánování a výkon IA zohledňující

komplexnost činnosti pojišťovny i její specifika s ohledem na schválenou strategii a rizikový apetit pojišťovny, a to vše v kontextu dynamicky se měnícího externího prostředí.

Pokud jsou tyto požadavky naplňovány tak, že v praxi vedou k funkčnímu a efektivnímu nastavení činnosti interního auditu, může být IA schopen skutečně kritického pohledu na kontrolované procesy z hlediska jejich vhodnosti nastavení, a díky tomu přinášet užitečná doporučení na zlepšení.

„Jedním z klíčových předpokladů pro kvalitní výkon IA je též porozumění celkové strategii pojišťovny a jejímu rizikovému profilu.“

Závěrem tak nezbyvá než konstatovat, že vhodně nastavená funkce interního auditu představuje pro pojišťovnu zásadní přidanou hodnotu a velmi účinný a efektivní nástroj nejen pro řízení rizik, ale i pro celkové řízení společnosti, a díky tomu významně přispívá k naplňování strategie a krátkodobých i dlouhodobých cílů pojišťovny. ■

RIZIKA SPOJENÁ S VYUŽÍVÁNÍM AI Z POHLEDU IA A AUDITOVANÝCH

V dnešní době je umělá inteligence (AI), ať již v jakékoli své podobě, stále více integrována do různých míst organizací i našich běžných životů, což přináší nejen mnoho výhod, ale také řadu rizik. A to i pro interní audit (IA). Zapojení AI do jakýchkoli činností otevírá nové možnosti výsledků práce či zábavy, ale také právě celou škálu nových rizik. V tomto článku se podíváme na vybraná rizika spojená s AI z pohledu interního auditu a auditovaných a naznačíme, jak tato rizika, ve vztahu k technickému vývoji poloviny roku 2023, minimalizovat.

PhDr. Ing. Jiří Čihák
Interní a forenzní audit IT

V současné době pracuje pro významnou mezinárodní telekomunikační společnost v oblasti interního auditu IT. Předchozí zkušenosti získal v jedné z českých bank v oblasti auditu IT nebo ve společnosti tzv. velké čtyřky, kde se věnoval externímu foreznímu auditu, či v instituci veřejné správy v oblasti IT.

Pohledy na tuto problematiku je možné v úvodu teoreticky rozdělit na přinejmenším dva. A to z pohledu na AI jako objekt auditu a na AI jako nástroj pro audit. Pro ilustraci rizik spojených s AI tyto pohledy pro účely tohoto článku spojíme a podíváme se komplexně na rizika spojená s využíváním AI obecně. Jako vzorový typ AI, na kterém si můžeme konkrétní rizika ilustrovat, si zvolíme v současnosti nejspíše nejznámější typ AI, a to jazykový/textový model umělé inteligence (někdy také nazývaný zjednodušeně AI chatbotem), a stranou nechme všechny jiné typy AI.

Lze zobecnit, že pro AI platí základní triáda: Jak model funguje? – Jak chrání svěřená data? – Jak je používán?

Podíváme se na konkrétní příklady. Co lze zařadit mezi rizika a problémy spojené s využíváním AI? Uvedené příklady ilustrované na prostředí IA lze aplikovat i na jiné útvary či použití jednotlivcem. Zohledňují totiž více charakteristiky AI než charakteristiky IA.

AI modely mohou být či jsou skutečně složité a obtížně interpretovatelné. To způsobuje jakýsi **nedostatek transparentnosti**. Modely jsou často založené na složitých konceptech nejrůznějších typů učení, rozhodování apod., které mohou být obtížně srozumitelné a vysvětlitelné. Nedostatek transparentnosti může vést k neschopnosti odhalit chyby nebo předpojatosti ve výsledcích AI, nepochopení, jakým způsobem dochází k vlastním rozhodnutím a vysvětlením, jak samotná AI dospívá k určitým rozhodnutím. To může vést k nedostatečné transparentnosti procesu rozhodování a ztížit schopnost ověřování auditních výstupů a zjištění.

K eliminaci uvedeného by mohl pomoci přístup interního auditu k důkladným popisům fungování AI modelů, což není vždy dostupné a možné. Nebo nemusí být vždy efektivní tyto modely studovat.

AI modely jsou závislé na **tréninkových zdrojových datech**, a pokud jsou tato data zkreslená nebo obsahují bias, může to vést k nepřesným výsledkům

nebo nesprávným či nespravedlivým rozhodnutím. Je to způsobeno tím, že AI modely se obvykle učí z velkého množství dat, která jsou jim zpřístupněná. To znamená, že jejich odpovědi mohou být ovlivněny neaktuálními, nepřesnými nebo zaujatými informacemi, které byly v těchto datech a byly použity k vycvičení a natrénování modelu. To ve výsledku může ohrozit kvalitu a důvěryhodnost výstupů, včetně auditního procesu, a může se promítnout v **nepřesnost či nespolehlivost**. Při použití zavádějících informací se mohou vyskytnout chyby, které by mohly ovlivnit kvalitu provedeného auditu. Na místě je tak opatrnost při používání informací generovaných AI a nutnost ověření poskytnutých výsledků i z jiných zdrojů, je-li to možné. Což však zpětně umazává časovou úsporu získanou případným využitím AI.

„AI modely mohou být či jsou skutečně složité a obtížně interpretovatelné.“

Dále se mohou objevit i návody k neetickému chování, kdy AI může případně poskytnout **neetické rady** nebo podporovat neetické chování při auditu. Řešením by mohla být prokazatelně prověřená kvalita a reprezentativnost tréninkových dat, což nemusí být vždy možné.

Poskytnutí nepřesných, zavádějících nebo jen povrchních informací může být způsobeno také použitím nesprávného modelu pro daný účel. Tedy pokud je používán nevhodně zvolený typ AI, který má například omezenou specializaci nebo specializaci na něco jiného, než uživatel potřebuje nebo co je pro výsledek auditního použití důležité.

O několik odstavců výše padlo slovo **bias**. **Bias, předsuděk, tendence, sklon, předpojatost**. To je spojené zejména s rizikem nerovnosti a diskriminace. AI může zesilovat určité nežádoucí prvky, jako například sociální stereotypy a nerovnosti obsažené v datech, protože může být ovlivněna právě předsudky dat, na kterých je vycvičena. AI tak může generovat informace, které jsou předsudkové, diskriminační nebo jinak nevhodné. Auditóři, a obecně všichni uživatelé, by si měli být vědomi potenciálu předsudků, resp. biasu. To se přeneseně týká například i historických faktů.

„AI modely se obvykle učí z velkého množství dat, která jsou jim zpřístupněná.“

Závislost na zdrojových datech může vést k nespravedlivým rozhodnutím a k posilování sociálních nerovností, či přímo k diskriminaci. Proto mohou vývojové týmy AI zahrnovat skupiny reviewerů, kteří sledují poskytované výsledky a dávají zpětnou vazbu na nevhodný bias či jiné zaujetí. V zájmu korektnosti mohou být některé odpovědi uhlazené či rovnou neposkytované. Představme si to například tak, že pokud budou tréninková data pojednávat o určité skupině osob určitého geografického původu či stáří, je možné, že právě tento profil osob se následně promítne do generovaných odpovědí. Tj. nemusí dojít ke zohlednění osob ze skupin jiného geografického původu či jiného stáří. V detailech se tak může promítat například do nechtěných opomenutí minoritních skupin, a tedy nedostatku diverzity či diskriminace, do zesilování či opakování nevhodného jazyka, názorů či stereotypů. To vše na základě toho, že tyto aspekty byly zahrnuty ve zdrojových datech použitých k nacvičení modelu. Problematika biasu je jedním z výrazných témat spojených se spravedlivým rozvojem AI.

A samozřejmě, bias mechanismus v AI může být taktéž zneužit k manipulaci s informacemi nebo k šíření dezinformací.

AI modely pracují s velkým množstvím dat od uživatelů, které jsou do nich nahrány jako uživatelské vstupy. To zvyšuje riziko narušení důvěrnosti při zneužití poskytnutých citlivých informací a vystavuje zvýšené nároky na **bezpečnost svěřených dat**. Jakákoli AI, ať již online (cloud), nebo offline, je zranitelná vůči **kybernetickým útokům** a zneužitím, což může ohrozit citlivá data a způsobit škody. Lze tak odůvodněně očekávat rizika krádeže nebo zneužití citlivých informací, se kterými je pracováno, ale také rizika implementace nevhodného kusu kódu, a to s nejrůznějšími účely, včetně například právě krádeže dat, zavlečení cíleného biasu, chybovosti či poskytování tendenčních výsledků.

„Poskytnutí nepřesných, zavádějících nebo jen povrchních informací může být způsobeno také použitím nesprávného modelu pro daný účel.“

Při využívání AI, a zejména při implementaci AI systémů do prostředí organizací, musí proto být pečlivě zvažována **bezpečnostní opatření**. Použití AI totiž může vyžadovat sdílení citlivých interních dat s třetí stranou (například s provozovatelem AI). To může zvýšit riziko úniku či zneužití důvěrných informací. Je důležité zajistit, aby byla zajištěna odpovídající ochrana dat a zachování jejich důvěrnosti, či případně bylo definováno, jaké typy dat lze a které nelze do daného AI nahrávat.

Je vhodné pracovat také s rizikem **nepředvídatelného chování** a chyby, kdy AI mohou občas reagovat nepředvídatelným způsobem. To může mít vliv na kvalitu poskytnutých výsledků, může způsobit nedorozumění či škody případně i většího rozsahu, zejména u aktivních AI, v jejichž možnostech je vykonávání úkolů či předávání pokynů k takovým úkolům.

„Jakákoli AI, ať již online (cloud), nebo offline, je zranitelná vůči kybernetickým útokům a zneužitím.“

I zde je tedy namístě role IA, aby hodnotil zabezpečení datových procesů AI a ověřoval, že jsou dodržovány všechny příslušné normy ochrany dat. Náležitá analýza rizik, spojených s využíváním AI, se taktéž jeví jako výrazně vhodná.

„Používání AI může vyvolávat také široká právní rizika.“

Z pohledu organizací hraje důležitou roli také **lidský faktor**, tedy uživatelé. Ti by měli být při práci s AI adekvátně obezřetní. To z pohledu organizace znamená správně je proškolit a nastavit vhodný dohled, resp. pravidla v podobě interních předpisů. Jinak může snadno docházet k chybám při používání i implementaci těchto technologií. I zde se může uplatnit IA jako kontrolní linie toho, zda jsou správně nastavena pravidla používání a implementace (včetně technického řešení) technologie, zda existuje efektivní dohled nad provozem AI systémů a zda jsou uživatelé dostatečně vyškoleni.

Opět i zde platí omílané, že samotný člověk, uživatel, může být nejslabším článkem řetězu.

Kontrola nad provozem AI, ať již automatizovaná, nebo manuální, je důležitá, neboť některé AI systémy mohou být schopny operovat autonomně a bez lidského dohledu, a poskytovat i aktivní operace. To může zvýšit riziko chyb nebo nežádoucích výsledků.

Alespoň prozatím, k polovině roku 2023, lze uvést, že AI zatím postrádá širší rozpětí jakéhosi lidského uvážení, a zejména **lidské intuice**. Což může být důležité při analýze komplexních situací (ne zcela založených na datech) a zjišťování nepřímých důkazů. AI tak nemusí vždy správně chápat specifický kontext interního auditu, což může vést k nesprávným závěrům nebo přehlédnutí klíčových informací. Některé AI modely již dnes excelují v úkolech založených na analýze obřího množství dat, ale mohou mít stále ještě určité obtíže s vykazováním kreativity, empatie a s porozuměním složitým lidským kontextům. Nicméně opět platí, že již za několik měsíců může být toto zcela jinak.

„Při využívání AI, a zejména při implementaci AI systémů do prostředí organizací, musí proto být pečlivě zvažována bezpečnostní opatření.“

Používání AI může vyvolávat také široká **právní** rizika a otázky týkající se odpovědnosti za rozhodnutí AI, autorských práv atd. Může také vyvolat širší **etická** témata a dilemata ohledně toho, zda a jak má AI přijímat etická rozhodnutí.

Právě rychlý vývoj AI může znamenat, že **regulace a standardy** nejsou dostatečně připraveny na řešení

všech jeho aspektů, což může vést k právním a bezpečnostním nejistotám, rizikům a rizikům dalších či zmařených investic.

Nad rámec tohoto, v kontextu **ESG**, může mít rozšíření AI v některých odvětvích za následek přeskládání struktury pracovních míst, zejména v rutinních a opakujících se činnostech. Nemusí zcela automaticky vést ke snížení pracovních míst, ale nejspíše povede k diverzifikaci mezi těmi zaměstnanci, kteří umí využívat možností AI, a kteří nikoli.

Dále, velmi přeneseně, mohou být i jisté environmentální dopady spojené s tím, že rychlý nárůst využívání AI může vyžadovat velké množství výpočetního výkonu, což může zvýšit spotřebu energie v datacentrech, a mít tak negativní dopad na životní prostředí.

„Kontrola nad provozem AI, ať již automatizovaná, nebo manuální, je důležitá.“

Na závěr shrňme, že nejen z pohledu IA je důležité si uvědomit, že AI by ve svých rozličných podobách měla být používána jako **podpůrný nástroj** při interním auditu a jiných aktivitách, a nikoli zcela jako náhrada za lidskou odbornost a rozsáhlé zkušenosti auditorských týmů. Prozatím. Minimálně pro výkon interního auditu je klíčové zachovávat kritické myšlení, provádět ověření informací a používat technologii AI s obezřetností a zodpovědností, a to jak při využívání AI, tak při jejím auditování.

Navzdory rizikům může být AI jednoznačně cenným nástrojem pro organizace i interní audit. Při používání AI je však důležité být si vědom rizik a přijmout opatření k jejich snížení.

Pro minimalizaci nejen uvedených rizik je vhodné zvážit:

- Zavedení správného využití AI jako nástroje podpory, nikoliv jako jediného zdroje informací.
- Implementaci opatření pro zajištění bezpečnosti dat (technická, uživatelská).
- Pravidelnou aktualizaci a ověřování dat použitých pro učení modelu, je-li to možné.
- Vytvoření dokumentace, která popisuje, jak AI používáte, co je povoleno a co není a jaká jsou rizika spojená s jejím používáním ve vašem prostředí.
- Explicitní definování odpovědnosti za výsledky práce, do kterých byly použité jako vstupy výstupy AI.
- Pravidelné monitorování a sledování vývoje AI, např. novinky v nově implementovaných verzích, jsou-li, a návazné přijímání opatření ke snížení nových rizik.
- Zajištění vhodných školení a dohledu pro správné a efektivní používání AI uživateli.
- Faktor kritického posouzení, interpretace a ověření výstupů AI lidskými auditory a uživateli.

Výhody AI mohou být velké, pokud jsou správně využity, nicméně je velmi důležité pečlivě zvažovat všechny aspekty jejího použití. Interní audit může zaujmout i v této oblasti jakousi klíčovou roli při minimalizaci rizik spojených s využíváním AI v organizacích. Je proto i v této oblasti důležité, aby auditoři byli dobře seznámeni s AI, jejími možnostmi a měli schopnosti identifikovat a adresovat potenciální rizika ještě o něco málo dříve, než skutečně přijdou.

Napiš mi, prosím, 20 rizik spojených s výkonem interního auditu.

„Samozřejmě, zde je seznam 20 rizik spojených s výkonem interního auditu:

- Nepřiměřená nezávislost auditorského týmu a možnost vlivu managementu na auditní proces.
- Konflikty zájmů, které by mohly snížit objektivitu a integritu auditu.
- Nedostatečně kvalifikovaný personál interního auditu.
- Nedostatečná znalost a porozumění procesů, postupů a rizik organizace.
- Nedostatečné pokrytí klíčových oblastí auditního plánu.
- Neefektivní plánování a alokace zdrojů pro audity.
- Nedostatečná spolupráce zaměstnanců a manažerů při auditu.
- Nedostatečná transparentnost auditních postupů a zjištění.
- Nepřiměřená dokumentace auditorských prací a závěrů.
- Nevyhovující sledování a monitorování implementace doporučení auditu.
- Nerespektování příslušných právních a regulačních požadavků.
- Nedostatečná ochrana a bezpečnost auditních dat.
- Neadekvátní kontrolní mechanismy a dohled nad auditními procesy.
- Chybějící nebo nedostatečně aktualizovaný interní auditorský manuál.
- Neúčinné hodnocení rizik a identifikace nových rizikových oblastí.
- Neadekvátní komunikace s vedením a dalšími zúčastněnými stranami.
- Nepřiměřené závěry a doporučení auditorského týmu.
- Neefektivní sledování a posuzování pokroku při implementaci auditorských doporučení.
- Nedostatečné posílení schopností a rozvoj dovedností interního auditu.
- Neodhalení závažných rizik a nedostatečných interních kontrol.

*Paměť si prosím, že některá z těchto rizik lze minimalizovat správným plánováním, striktním dodržováním standardů a etických principů, stejně jako kvalitním řízením interního auditu.**

Generováno pomocí jazykového modelu
OpenAI GPT-3.5. @ chat.openai.com; červen 2023.

Tak a je to. Trochu s překlepy, jedno riziko se opakuje dvakrát, ale kdo z nás by toto vyjmenoval za cca 6 vteřin?

À propos, v článku jsou použity inspirace ze zdrojů AI. ■

S autorem článku se můžete setkat na seminářích ČIIA

Lektor: **PhDr. Ing. Jiří Čihák**

REGISTRUJTE SE NA SEMINÁŘE

■ Audit IT pro non-IT auditory

1. prosinec 2023

■ Praktický průvodce

začínajícího auditora: aneb od programu, přes zajišťování důkazů, po prezentaci zprávy interního auditu

8. prosinec 2023

■ Trendy v IT

13. prosinec 2023

Objednávejte na webu ČIIA
(www.interniaudit.cz) nebo
na prihlasky@interniaudit.cz

AUDIT ŘÍZENÍ RIZIK



Řízení rizik je nástroj, který umožňuje organizacím nejen lépe chápat své schopnosti a omezení, ale také identifikovat příležitosti k inovacím a posílení své pozice na trhu. Na dalších řádcích se dozvíte, jak chápeme oblast řízení rizik v bance a jak přistupujeme k jeho auditování v Interním auditu KB. Začneme od začátku, respektive od naší mateřské instituce – IIA.

Ing. Lenka Landa Schejbalová, MBA

Výkonná ředitelka Interního Auditů KB

Po ukončení studii na Vysoké škole ekonomické, fakultě Finance a účetnictví, spojila Lenka svou profesní kariéru s francouzskou finanční skupinou Société Générale (SG). Začínala jako junior auditor v Komerční bance a po dvou letech odjela v rámci mezinárodní mobility do centrály SG v Paříži, kde nakonec strávila šest let na různých pozicích v rámci interního auditu. Nejdříve jako auditor a vedoucí mise pokrývala mezinárodní retailovou síť SG, poté jako auditní supervisor SG centrální funkce se zaměřením na compliance, a především na boj proti praní špinavých peněz a financování terorismu. Po návratu do České republiky vedla v rámci KB korporátního bankovního týmu middle office strukturovaných transakcí, poté v týmu strukturovaného financování zastávala funkci Chief Operating Officer. V roce 2019 byla jmenována do pozice výkonné ředitelky pro interní audit KB, kde zaštiťuje tuto roli pro všechny společnosti skupiny KB a pro společnosti SG zabývající se specializovaným financováním (ALD, SGEF) ve střední Evropě.

Ing. Helena Raizl Jumrová, CGSS

Chief Operating Officer – Internal Audit KB

Po studiu fakulty Mezinárodních vztahů na VŠE získala své několikaleté profesní zkušenosti v EY, kde se věnovala převážně realizaci auditních zakázek různého charakteru. V Komerční bance pak jako Vedoucí auditor vybudovala tým se zaměřením na compliance rizika, především pak na praní špinavých peněz a financování terorismu. Je autorkou řady metodik, procesních změn a školí auditní praxi v Interním auditu KB, včetně uplatňování postupů Lean Six Sigma, jakožto držitel Green Belt. Na současné pozici COO navíc zastává organizaci chodu celého útvaru Interního auditu KB.

Vtéto oblasti se dle IPPF – IIA Standardů od nás auditorů očekává, že zhodnotíme účinnost procesů, které mají řízení rizik ve společnosti zajišťovat. Půjdeme-li dál, nutnou součástí této oblasti je stanovení cílů společnosti, identifikace a hodnocení souvisejících rizik, stanovení opatření pro jejich řízení, a to vše doprovázeno získáváním a sdělováním informací napříč společností. A tím vzniká komplexní téma obzvláště v systémové bance, jakou Komerční banka je.

„KB řídí všechna rizika nejen jako izolované jevy, ale jako součást celkového bankovního ekosystému“

Tak jako při provádění každé auditní zakázky si pojdme nejprve oblast zmapovat, a to v prostředí celosvětového bankovního domu Sociétés Générale (SG). Pro tyto účely musíme zdůraznit interní instrukci tzv. SG Code, který reflektuje požadavky dané regulací v této oblasti a má za cíl stanovovat rámec pro veškeré činnosti spojené s řízením rizik ve všech svých dceřiných společnostech po celém světě. KB je tak členěna do tzv. tří linií obrany, jejichž jednotlivé struktury a procesy slouží k napomáhání dosahování cílů právě prostřednictvím optimálního nastavení řízení rizik. Uvedené vychází z „EBA Guidelines on Internal Governance“,

který stojí na obdobných principech jako náš známým „The Three Lines Model“ z dílny IIA.

Podíváme-li se na oblast tzv. seshora, od cílů společnosti, najdeme jejich stanovení v rámci každoročně publikovaných dokumentů, které pro KB popisují klíčové strategické obchodní cíle a na ně navazující strategii řízení rizik.

KB uplatňuje **holistický přístup k řízení rizik**, což znamená, že KB řídí všechna rizika nejen jako izolované jevy, ale jako součást celkového bankovního ekosystému a řadí ho v rámci organizační struktury pod zodpovědnost jednoho člena představenstva. KB se, jako ostatně i další banky, potýká s typy rizik, jako jsou úvěrové, tržní, likvidity, operační – včetně IT, compliance atd. Důležitým úkolem této strategie řízení rizik je podpora obchodních aktivit banky, udržování a posilování její tržní pozice při zachování zdravé bilance.

Strategie řízení rizik je vypracována na základě principů uvedených v dokumentech Risk Appetite Statement a Risk Appetite Framework, které dále zpřesňují přístup a apetit k jednotlivým rizikům, včetně jejich konkrétního řízení a definice rolí a zodpovědností v rámci relevantních procesů v bance. Toto jsou tedy stěžejní a závazné dokumenty, ze kterých v rámci auditů týkajících se (nejen) řízení rizik auditní tým vychází.

Snahou je mít jednotnou terminologii a přístup k identifikaci a měření rizik. Pro identifikaci a měření rizik tak používá

KB systém kategorizace činností/procesů, odpovídajících taxonomii rizik a kontrol, se kterými pracuje. Každá skupina rizik používá pro její hodnocení specifické nástroje a metody.

„Klíčovým atributem pro řízení rizik v bance je tzv. stress testing,“

Rizika jsou identifikována jak na bázi každodenního řízení procesů (sledování jejich klíčových indikátorů, limitů a prahových hodnot) a prostřednictvím specificky zaměřených výborů nebo v rámci zavádění/změny produktů či procesů.

Dále pak dochází k identifikaci a měření rizik prostřednictvím každoročních hodnocení jednotlivých skupin rizik napříč bankou, jako je například pro kapitálovou přiměřenost Internal Capital Adequacy Assessment Process (ICAAP), pro likviditu Internal Liquidity Adequacy Assessment Process (ILAAP), Risk Control Self-Assessment (RCSA) pro operační rizika, podobné cvičení banka provádí také nad riziky Compliance.

Klíčovým atributem pro řízení rizik v bance je tzv. stress testing, který má za cíl kvantifikovat veškerá materiální rizika pro KB a celou skupinu SG. Podstatou je modelování (extrémně) rizikových scénářů (např. související se změnou ekonomického prostředí) a určení úrovně daného rizika. Jsou pak

významným zdrojem pro stanovování opatření k jeho snížení, např. nová rozhodnutí týkající se skladby portfolia.

Důležitým aspektem pro auditní činnost je správné určení **„ultimátních vlastníků rizik“**, jelikož komplexnost procesů v bance, které prostupují napříč organizací, vyžaduje nezbytnou spolupráci a koordinaci skrz banku, a to jak její „run“ částí, tak její částí „change“.

Interní audit Komerční banky kopíruje z velké části organizaci řízení rizik v bance, jednotlivé auditní týmy jsou specializované na nejmateriálnější rizika, se kterými banka pracuje. Tedy auditní tým specializující se na řízení kreditních rizik, jiný tým zaměřující se na rizika compliance s dalším specifickým zaměřením např. na rizika spojená s praním špinavých peněz a financování terorismu, tým IT expertů, tým pokrývající operační rizika či rizika spojená s investičním bankovníctvím. Tyto týmy budují expertizu nejen dle jednotlivých rizik, ale také dle specifických aspektů těchto rizik v jednotlivých společnostech Skupiny KB, jako např. KB Penzijní společnost, ESSOX, SGEF, ALD nebo Faktoring KB. Auditor se tak postupně stává odborníkem znalým jak regulace, tak i její aplikace v praxi, a navíc v různých obchodních modelech.

Ve své podstatě se každý audit zaměřuje na řízení rizik v bance. Audit řízení rizik může mít mnoho podob, může probíhat přes různé řídicí linie, může se zaměřovat na kontrolní body



Lenka Landa Schejbalová

v konkrétních procesech, může pokrývat nastavení celkového řídicího rámce. Obecně v Interním auditu KB využíváme následující přístupy, pomocí kterých dosahujeme potřebného pokrytí:

■ **Celkové tzv. governance řízení rizik** v bance anebo nastavení řízení konkrétního významného rizika, a to nejen v rámci banky, ale také v rámci celé finanční skupiny. Jako příklad můžeme uvést audit zaměřený na samotný model tří linií obrany v KB a jeho soulad s regulatorikou, s nejlepší praxí, jeho reálným fungováním a jeho vyspělostí. Dalším příkladem je audit řízení kreditního rizika, kdy se zaměřujeme na nastavení pravidel pro řízení kreditního rizika, jejich soulad s regulatorními požadavky, jejich nasazení na nižších

úrovních řízení a v jednotlivých společnostech skupiny. Auditní činnosti se dále mohou zaměřit na další detailní nastavení a funkčnost dílčích klíčových pravidel a kontrolních mechanismů jako například na kvalitu datových toků nebo monitoring a reporting klíčových ukazatelů zásadních pro přijímání informovaných rozhodnutí managementu banky.

■ **Procesní audit**, který se může zaměřovat na celý proces (tzv. „end-to-end“) nebo jen na jednu jeho např. specificky rizikovou část. Klíčové je zde detailní pochopení kontextu a celkového fungování daného procesu. Na těchto auditech máme často možnost nejvíce využít pro tyto účely nástroje Lean Six Sigma, které nám pomáhají se lépe zaměřit na rizika související s kvalitou a výkonností daného procesu. Příkladem může být procesní audit produktového charakteru, třeba poskytování bankovní záruky, kde hodnotíme veškerá rizika v procesu, tedy ze všech kategorií (operační riziko, riziko udržitelnosti procesu, související IT rizika používaných systémů atd.), přičemž z charakteru produktu je nejvýznamnějším riziko kreditní. Nebo audit pokrývající klíčový bankovní proces, jako je například přijetí klienta do banky a jeho proces z bankovního pohledu tzv. KYC („poznej svého klienta“). V tomto případě bude audit zaměřen především na řízení rizika compliance.

■ **Tematické či post-implemenční audit** uplatňujeme v případě implementace nové regulace zasahující do řízení významného rizika, např. GDPR ovlivňující řízení a monitoring compliance rizik nebo v případě Zákona o kybernetické bezpečnosti by se jednalo o audit řízení rizik spojených s informačními systémy. K takovýmto auditům přistupujeme i v případě, že dochází k zavedení nových systémů a nástrojů v jednotlivých procesech banky, které jsou pro daný proces zásadní změnou, která je nositelem možných rizik.

„Důležitým aspektem pro auditní činnost je správné určení ‚ultimátních vlastníků rizik‘.“

Nutno dodat, že významnost jednotlivých naplánovaných auditů v daném roce vychází z každoročního hodnocení rizik (risk assessment).

Klíčová je pro nás pravidelná komunikace s managementem banky, tzv. pravidelný monitoring, který nám umožňuje získávat informace i mimo audit, jehož prostřednictvím můžeme reflektovat změnu v navrženém systému pokrytí pro daný auditní rok na základě změny rizikového profilu banky.

Při realizaci již konkrétního auditu pak postupujeme standardním

způsobem, kdy po tzv. diagnostické fázi, jejíž součástí je vyhodnocení námi identifikovaných rizik v rámci auditované oblasti, stanovení cílů, rozsahu ověření za použití jednotlivých auditních metod, které vycházejí z IIA Standardů, při použití pokročilých datové analýzy či datové vědy, bez ohledu na odvětví, ve kterém auditujeme. Naším konečným výstupem je tradiční závěrečná zpráva hodnotící silné a slabé stránky v řízení oblasti, a konečně názor na účinnost řízení rizik.

Řízení rizik v bance je jako pohled na skládku, kde jednotlivé dílky tvoří součásti většího obrazu. Banka, a ostatně i my, auditoři, se snažíme pochopit, jak tyto dílky spolu souvisejí a interagují, a jak mohou ovlivnit celkovou stabilitu a obchodní úspěšnost banky. ■



Helena Raizl Jumrová

Auditors in the Hot Seat

Could internal auditors be fined or face enforcement action for failing to address risk?

Late last year, the U.S. Office of the Comptroller of the Currency (OCC) Office of Financial Institution Adjudication released a report and recommendations related to the consumer account and cross-selling failures at Wells Fargo Bank. The report recommends fines for three former internal audit and risk management executives at the bank ranging from \$1.5 million to \$10 million. Although there have been cases where organizations were fined because of weaknesses related to internal auditing, it is extremely rare to hear of an individual internal auditor being fined.

The OCC report contains allegations related to deficiencies and weaknesses in governance, risk, and control (GRC) activities, with emphasis on the risk management and internal audit functions. The fines are just recommendations for now. However, if the OCC decides to pursue them, there could be significant implications for CAEs, internal auditors, and risk management professionals. Regardless of the outcome, there are takeaways from the report for all CAEs and internal audit functions to consider.



REPORT HIGHLIGHTS

The report notes five specific conditions that led to the potential enforcement action (see “Fuel to the Fire,” on page 43). The first being that employees engaged in sales practice misconduct, with most of the report summarizing the failures that led to those charges. The second, third, and fourth conditions relate to the accused parties not determining the root cause of the sales misconduct. The fifth being engaging in unsafe and sound banking practices, which in this case relates to “failing to identify and effectively address known issues of risks.”

According to the report, Wells Fargo’s internal auditors were required to:

- Recognize The IIA’s definition of internal auditing and adhere to The Institute’s International Standards for the Professional Practice of Internal Auditing and Code of Ethics.
- Maintain an audit charter with language indicating that internal audit would provide the board assurance that business lines comply with policies and procedures and would bring a systematic and disciplined approach to evaluating and improving the effectiveness of enterprise governance, risk, and compliance processes.
- Determine whether the governance system is adequately designed and that the board receives timely information.
- Provide assurance of governance functions and processes.

- Ensure an appropriate culture, including risk culture, is established, understood, and consistently complied with throughout the bank.
- Ensure that effective correction actions are timely.
- Provide assurance related to the compensation program.

The chief auditor participated on at least five committees — Operating, Enterprise Risk Management, Team Member Misconduct, Ethics, and Incentive Compensation — and may have had voting authority. The Ethics committee is responsible for significant ethical and business conduct issues. Sales misconduct violations and deceptive practices along with overly aggressive sales goals appear to fit this definition.



Based on the report, the main issue was how the risks were disseminated and escalated throughout the organization. There appears to be little to no responsibility taken for risks related to sales practice misconduct and no upward reporting to the highest levels of governance: the audit committee and the board. In 2015, the OCC issued a report detailing five specific “Matters Requiring Attention” related to sales practices. However, there appeared to be no process for follow-up, reporting, and corrective action.

Interestingly, the report notes that the bank used the Three Lines risk management system throughout the relevant period. However, the OCC questions how well the first line created controls related to incentives and sales practices, how the second line being the risk function operated, and how the internal audit function fulfilled its responsibilities as the third line.

The IIA Three Lines Model demonstrates the need for clear communication and reporting among all three lines, which might be the biggest surprise in the report. The information either did not reach the highest level or it was decided that the information did not need to reach those levels, which indicates a failure to fully understand the risk.

OPPORTUNITIES FOR INTERNAL AUDIT

The report provides CAEs with the opportunity to turn the magnifying glass on their own operations, teaches some important lessons, and offers guidance for internal audit activities and oversight.

Tone at the Top. The report noted numerous charters that guided Wells Fargo’s internal audit, risk groups, and various committees. Corporations can be complex with international operations, affiliates, subsidiaries, holding companies, and various levels of operations. If an organization has multiple governing charters, internal audit should make sure they do not conflict.

„Audit should review its charter and ensure it covers internal audit responsibilities at every entity and level.“

The charter should note that, based on the Standards, internal audit must include the evaluation and reporting of all aspects of GRC, but should not be responsible or have primary oversight of these functions, as that could impair independence and objectivity when performing assurance audits.

Committee Responsibilities. CAEs or other internal auditors who participate on



a committee of any kind must ensure that those responsibilities do not conflict with the audit charter and the independence of the internal audit function. A CAE who provides assurance for compensation, ethics, or risk management as part of the audit plan should not be a voting member of a committee that designs or administers any of these activities. Internal auditors need to be careful when a significant portion of an internal audit bonus plan is based on financial results. This could impair independence and objectivity. The committee meeting minutes or the committee policy should clearly state that any internal audit participation is in an advisory capacity and the auditor has no ability to vote.

Audit Plan. Audit plans do not need a major overhaul based on this report. Internal audit cannot audit every operation and transaction. However, internal audit should be meeting with the board, senior management, and key department managers. In addition, internal audit should meet with any leaders in risk management, compliance, or a fraud-inspection group to at least coordinate efforts and ensure clear communication and reporting. From here, the function should audit to business objectives. For example, if sales goals are a key business objective, internal audit should include this in the audit plan. For community banks with branch and retail locations, these operations are a significant part of the business. In many companies, customer interactions and sales are critical for growth. Internal audit

needs to understand the major revenue and expense streams, understand key lines of business, and make sure these areas have appropriate audit coverage.

Policies and Procedures. Internal audit policies and procedures should be reviewed annually, and that includes more than just changing the last review date. If it is not in the internal audit charter, a policy needs to clearly delineate the reporting lines within internal audit, the supervision of engagements, and communication of results. The CAE can assign these responsibilities to other experienced internal auditors, but the policy needs to address how the CAE will be informed of audit results and any significant findings.

Policies need to further address procedures to communicate and document increasing risks or significant concerns noted by other areas within the organization. Do audit, management, and committee reports clearly identify key or increasing risks or ineffective controls in a way management can understand and take corrective action? If reports are numerous and long, key concerns may go unread. The Standards state that communication is required, but the form of communication is open-ended. Internal audit should be creative and urgent when it comes to key risks. If necessary, internal auditors can send a text message, voice mail, or record a video. Internal audit should not rely on the first line, or even the second line, to escalate material risk issues. Internal audit should document any potential risks or concerns and follow up to ensure they are reported

and addressed. The audit function should not be limited to reporting only the risks it identifies.

Quality Assurance and Improvement Program (QAIP). The Standards state the internal audit function must have an external review every five years. A QAIP demonstrates to regulators, external auditors, senior management, and the board that internal audit is operating in accordance with the Standards and Code of Ethics. A QAIP can highlight areas where risk, communication, and oversight need to be strengthened. It is not, however, a get-out-of-jail free card.

Fraud. To reach elevated sales goals, employees resorted to fraudulent activities. The Standards require internal auditors to evaluate the risk of fraud and how the organization manages fraud risk. Internal auditors need to understand the fraud triangle and be aware of where within the organization there could be the opportunity and the pressure for fraud to occur. Identifying the rationale for fraud could be difficult, but it might become evident through other audits, interactions with employees, and discussions with management. CAEs can assess whether the organization has a reasonable process to manage fraud risk including a review of the organization fraud risk assessment, channels for reporting fraud, and procedures to address potential fraud.

FUEL to the FIRE

5 Alleged Conditions Leading to the Charges

1. **Wells Fargo Community Banking Group team members** engaged in sales practices misconduct that threatened the safety, soundness, and reputation of Wells Fargo Bank, N.A.
2. **The chief auditor**, serving as the head of the bank's third line, failed to: timely identify the root cause of sales practices misconduct in the Community Bank; provide credible challenge to risk control managers; evaluate the effectiveness of risk management controls; and identify, address, and escalate risk management control failures.
3. **The group risk officer** failed to: timely identify the root cause of sales practices misconduct; exercise credible challenge to the Community Bank's head regarding risk management controls relating to sales practices; timely and independently evaluate the effectiveness of risk management controls; and identify, address, and escalate risk management control failures.
4. **The executive audit director** failed to: timely identify the root cause of sales practices misconduct; provide credible challenge when evaluating the effectiveness of the risk management controls; and identify, address, and escalate risk management control failures.
5. **The three audit and risk executives** failed to identify, address, and escalate inadequate controls over known issues of risks related to sales goals pressure. They misled regulators regarding the efficacy of controls over risks related to sales goals pressure, thereby advancing their individual pecuniary interests over the interests of Wells Fargo and breaching fiduciary duties each owed to the bank. Further, the group risk officer's efforts to restrict material information from being disseminated among the bank's senior leaders, board, and regulators violated federal statutes and regulations.

SOURCE: U.S. DEPARTMENT OF THE TREASURY OFFICE OF THE COMPTROLLER OF THE CURRENCY REPORT AND RECOMMENDATION – EXECUTIVE SUMMARY (DEC. 5, 2022)

Removing Controls. Internal auditors frequently issue reports that highlight controls to implement or improve. It is less common to suggest removing a control. In these cases, internal audit needs to clearly document the benefit of the suggestion and why it is being made. In the Wells Fargo report, the OCC notes the audit group recommended removing a control that required customer account approval overrides with the reason being that the employees did not consistently follow the requirements. Internal audit needs to understand how key controls operate and why employees are circumventing or ignoring requirements. They should tread lightly when making these recommendations.

WHAT'S NEXT?

The former head of Wells Fargo's retail banking division, who is listed in the report, pleaded guilty to obstructing a government examination in April. She will pay a \$17 million fine and serve up to 16 months in prison.

The OCC report is a cautionary summary of the risk management events related to the Wells Fargo sales practices misconduct scandal. Banking has more regulations than most industries, and its internal auditors tend to have additional oversight. The lessons in this case, however, are a reminder that all internal auditors have a responsibility to protect organizational value and provide assurance to help reach strategic objectives.

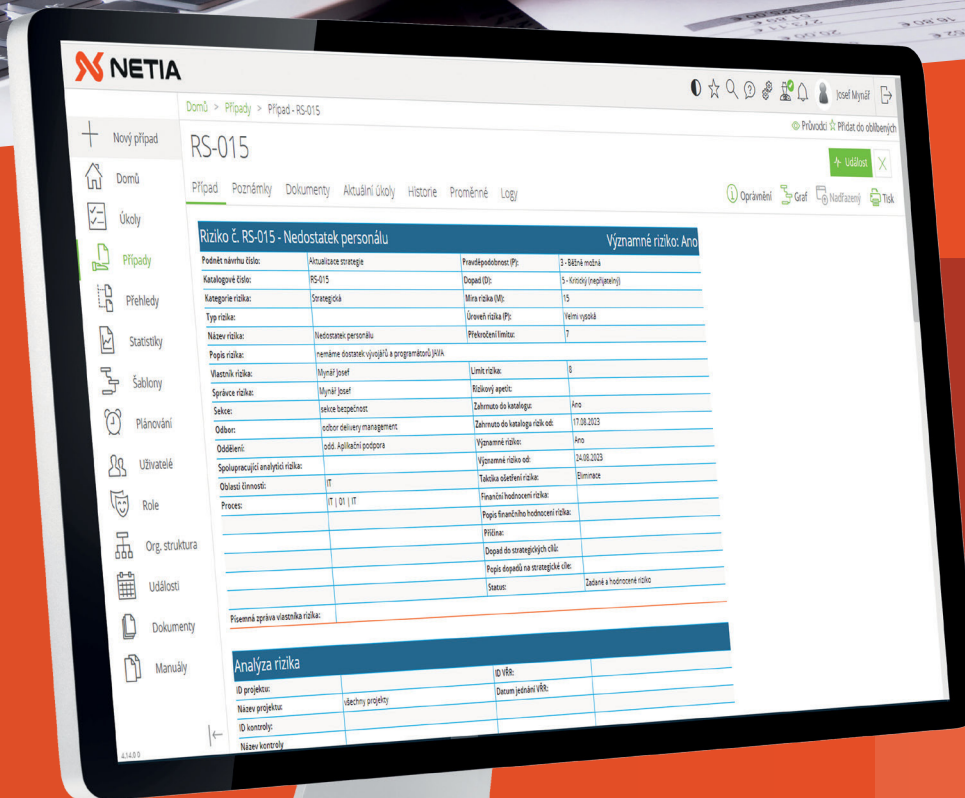
Internal auditors are fallible, and that is partly why assurance is only reasonable and not absolute. Even so, the profession should always be improving. Just because something has not happened yet, doesn't mean it can't happen. ■

Alexander Heggen, CIA, CISA, CMA, spent 20 years as a financial services examiner and internal auditor. He currently is a teaching assistant professor of Accounting at West Virginia University, in Morgantown, W.Va.

„The lesson in this case is that all internal auditors have a responsibility to protect organizational value.“



This article was reprinted with permission from the June 2023 issue of Internal Auditor, published by The Institute of Internal Auditors, Inc., www.theiaa.org.



Moderní softwarové řešení navržené s ohledem na nejnovější směrnici NIS2. **Výkonný nástroj** pro práci s maximální bezpečností a efektivitou.

Uspadněte si interní audity a řízení rizik

Plná shoda s novou směrnici NIS2

Komplexní analýzy & reporty

Jednoduché ovládání & spolehlivé výsledky

Nové Standardy jsou skoro na světě – pokračování (3. část)

Ing. Jana Báčová, CIA

V minulých dvou číslech časopisu jsme představili základní strukturu nového Rámce a Globálních standardů interního auditu a podrobněji se věnovali prvním dvěma doménám a změnám oproti současné profesní úpravě. Nyní se zaměříme na další domény, konkrétně na charakteristiku a změny ve standardech třetí a čtvrté domény.

Pro připomenutí a uvedení do kontextu si zopakujeme strukturu Globálních standardů a jejich 5 domén a 15 principů:

Doména č. III – Interní audit a řízení a správa společnosti je částí, která je věnována auditu a jeho interakci s vrcholovým vedením společnosti. Proto je tato část určena především pro nejvyšší vedení, výbory pro audit a vedoucí útvarů interního auditu. Sami autoři nového Rámce považují tuto doménu za oblast, kde

5 domén a 15 principů



dochází k nejrevolučnějším změnám. Dochází zde nejen ke zdůraznění role vedení a orgánů společnosti (Board), ale je poprvé přímo stanoveno, jaké má/musí mít vedení ve vztahu k internímu auditu pravomoci a odpovědnosti.

I když v této doméně nedochází k významným faktickým změnám oproti současné úpravě a vnímání rolí jednotlivých subjektů (nové jsou některé požadavky v rámci standardů 6.2, 8.1 a 8.4), již jen jinak formulované požadavky samy o sobě posouvají v nových Standardech roli vedení do mnohem akčnější a jednoznačnější polohy. Namísto někdy neadresných formulací v současných standardech je totiž nyní přímo v jednotlivých standardech uvedeno, co Board musí ve vztahu k internímu auditu udělat – co nastavit, přijmout, schválit, o co se zajímat a na co a jak často se ptát. A tak je v jednotlivých standardech principů č. 6 a 7 uvedeno např., že: Board musí chránit nezávislost interního auditu, schválit jeho mandát a jednou ročně ho ověřit, musí s interním auditem a jeho vedoucím nastavit přímé reportovací vztahy, zajistit, že šéf interního auditu má dostatečnou kvalifikaci a kompetence pro efektivní výkon své činnosti a musí schválit jeho role a odpovědnosti v rámci společnosti.

Board též musí podporovat funkci interního auditu a jeho vnímání a uznání ve společnosti. **K tomu nový standard 6.2 pak uvádí, co taková podpora Boardu obnáší.** Stejně jako u Boardu jsou ve standardech této domény

stanoveny povinnosti též vedoucímu interního auditu (CAE). Ten připravuje a poskytuje Boardu potřebné informace k plnění jeho rolí, potvrzuje minimálně jednou za rok vedení společnosti nezávislost funkce interního auditu, popř. prezentuje záležitosti, které by mohly jeho nezávislost narušit. Nic nového pod sluncem, ale každopádně větší jednoznačnost, podrobnost a provázanost.

„je poprvé přímo stanoveno, jaké má/musí mít vedení ve vztahu k internímu auditu pravomoci a odpovědnosti“

Princip č. 8 rozpracovává dohled vedení a orgánů společnosti nad interním auditem v zájmu zajištění jeho účinnosti.

Sem patří nejen péče o dostatečné zdroje interního auditu, ujištění o kvalitě vedoucího interního auditu a celého útvaru, ale též dostatečná vzájemná komunikace a interakce. **V tomto ohledu je zcela nový standard 8.1 Interakce s vedením a orgány společnosti.** Standard nejdříve stanoví povinnost Boardu spolupracovat s interním auditem tak, aby došlo k pochopení governance, řízení rizik a řídicích a kontrolních procesů. Dohled vedení musí zahrnovat průběžnou komunikaci s vedoucím interního auditu, mj. o strategii, cílech

Doména č. III. - Interní audit a řízení a správa společnosti 3 principy, 9 standardů

Board/Výbor pro audit a vedoucí interního auditu

6. Zmocnění vedením a orgány společnosti (Board)

Board zřizuje interní audit, schvaluje a podporuje pravomoci, roli a odpovědnosti funkce interního auditu.

6.1 Mandát interního auditu

6.2 Podpora vedení a orgánů společnosti

7. Nezávislé postavení

Board stanoví a chrání nezávislost funkce interního auditu.

7.1 Organizační nezávislost

7.2 Role, odpovědnosti a kvalifikace vedoucího interního auditu

7.3 Ochrana/zachování nezávislosti

8. Dohled vedení a orgánů společnosti

Board dohlíží na funkci interního auditu za účelem zajištění její účinnosti.

8.1 Interakce s vedením a orgány společnosti

8.2 Zdroje

8.3 Kvalita

8.4 Externí hodnocení kvality

a rizicích společnosti a k určení priorit funkce interního auditu, přičemž je to Board, kdo musí nastavit frekvenci komunikace s CAE a kritéria a proceduru pro eskalaci záležitostí na úroveň Boardu. Vedoucí interního auditu pak musí Boardu recipročně poskytovat takové informace, aby Board mohl svůj dohled nad auditem účelně plnit.

„již jen jinak formulované požadavky samy o sobě posouvají v nových Standardech roli vedení do mnohem akčnější a jednoznačnější polohy“

Obdobně je tomu u standardu 8.2 Zdroje – Board musí zajistit dostatečné zdroje pro plnění funkcí interního auditu a minimálně jednou ročně se dotazovat vedoucího interního auditu, zda jsou zdroje dostatečné pro plnění mandátu a plánu interního auditu. CAE musí zase navrhnout strategii, jak zdroje získat a včas signalizovat, pokud jsou zdroje nedostatečné.

Standardy ke kvalitě, které jsou v současných základních standardech zahrnuty pod číslem 1300 a v podstatě neadresně pojednávají o zajištění kvality interního auditu jsou nyní rozděleny do dvou částí. Obecné požadavky na kvalitu a externí hodnocení kvality

jsou obsaženy v doméně č. III, interní hodnocení kvality pak v doméně č. IV., která stanoví povinnosti pro vedoucího interního auditu. Rozdělení je to logické, protože vrcholové vedení společnosti a výbory pro audit mají při externím hodnocení kvality nezastupitelnou úlohu a bez spolupráce s nimi nemůže sám vedoucí interního auditu toto hodnocení v podstatě získat. Interní hodnocení kvality je naopak v plné kompetenci a odpovědnosti šéfa auditu.

Požadavky na kvalitu se v nových standardech příliš nemění, jsou však opět jednoznačně rozděleny kompetence mezi vedením a vedoucím interního auditu. Od vedení se v této oblasti očekává větší aktivita. Standard 8.3 stanoví, že vedení společnosti musí zajistit, aby CAE vytvořil, implementoval a udržoval program pro zajištění a zvyšování kvality interního auditu. Musí to tedy po šéfovi auditu vyžadovat. Board musí též (minimálně jednou ročně) schválit pro vedoucího interního auditu výkonnostní cíle (ukazatele výkonnosti budou nově rozpracovány ve standardu 12.2 – viz dále) a současně Board sám řídí nebo se účastní na hodnocení jeho výkonu.

Standard 8.4 dává jednoznačně povinnost na zajištění externího hodnocení kvality na úroveň Boardu s tím, že musí být provedeno minimálně jednou za pět let, Board určí jeho zaměření a frekvenci provádění. CAE vypracuje plán pro externí ověření kvality, a ten je poté vedením společnosti posouzen a schválen. **Zcela nový je ve standardu**

8.4 požadavek, že sebehodnocení s nezávislou validací nebude plně nahrazovat externí hodnocení kvality a bude ho možné místo externího hodnocení použít jen jednou za 10 let.

Souhlasím s autory Globálních standardů, že doména č. III. představuje revoluční změnu, ale nikoli co do obsahu či množství nových požadavků, nýbrž revoluční je svým novým pojetím, jednoznačností přiřazování odpovědností a pravomocí konkrétnímu subjektu. Je to doména podtrhující partnerství mezi vedením společnosti a interním auditem, a nejen proto v ní najdeme nejvíce kompetencí přiřazených jednomu ze subjektů, ale též odpovědnosti, které musí být mezi vedením a orgány společnosti a vedoucím interního auditu diskutovány a sdíleny. **Doména č. III je tou správnou částí, ve které je možné hledat a najít inspiraci pro komunikaci s vedením společnosti a využít ji pro nastavení či doladění toho, co doposud ve vzájemné spolupráci pokulhávalo.**

„Board též musí podporovat funkci interního auditu a jeho vnímání a uznání ve společnosti“

Doména č. IV – Řízení funkce interního auditu je určena primárně pro vedoucí útvarů interního auditu.

Tato doména systematicky řadí stěžejní odpovědnosti CAE od porozumění principům governance, risk a compliance (tzv. GRC) přes strategické plánování k ročnímu plánu a k dalším navazujícím povinnostem a aktivitám při řízení útvaru interního auditu. Podrobněji než doposud se pak standardy věnují řízení zdrojů, budování vztahů s ostatními stakeholdery, komunikaci výsledků interního auditu a kvalitě a výkonnosti v procesu provádění auditních činností. V této doméně nalezneme též větší počet zcela nových standardů (9.2, 9.4, 10.1, 10.2, 10.3, 11.1, a 12.2).

„vedení společnosti a výbory pro audit mají při externím hodnocení kvality nezastupitelnou úlohu“

Pod principem č. 9 jsou ve standardu 9.1 modifikovaným způsobem uvedeny požadavky ze současných standardů 2100–2130 (Charakter práce, Řízení a správa společnosti, Řízení rizik, Řízení a kontrola). Aby mohl CAE splnit požadavky tohoto principu, tj. naplňovat mandát a dosahovat úspěchu, vytvořit strategii, statut a plán interního auditu, musí nejdříve pochopit zásady GRC dané společností. Standard 9.1 uvádí mj., co vše musí v tomto ohledu CAE znát a vzít v úvahu.

Doména č. IV. – Řízení funkce interního auditu

4 principy, 17 standardů

Pro vedoucího interního auditu (CAE)

9. Strategicky plánuje

CAE strategicky plánuje, aby zajistil, že funkce interního auditu naplňuje svůj mandát a je umístěna tak, aby dosahovala dlouhodobého úspěchu.

9.1 Porozumění procesům GRC

9.2 Strategie interního auditu

9.3 Statut interního auditu

9.4 Metodika

9.5 Plán interního auditu

9.6 Koordinace a spolehnouti se

10. Řídí zdroje

CAE řídí zdroje tak, aby realizoval strategii interního auditu, splnil plán a naplnil mandát funkce interního auditu.

10.1 Řízení finančních zdrojů

10.2 Řízení lidských zdrojů

10.3 Technologické zdroje

11. Účinně a efektivně komunikuje

CAE zajistí, že interní audit komunikuje se svými stakeholdery účinně a efektivně.

11.1 Budování vztahů a komunikace se stakeholdery

11.2 Účinná a efektivní komunikace

11.3 Komunikace výsledků

11.4 Chyby a omyly

11.5 Komunikace přijetí rizika

12. Zvyšuje kvalitu

CAE zajistí soulad s Globálními standardy interního auditu™ neustále zlepšuje výkonnost a interního auditu.

12.1 Interní hodnocení kvality

12.2 Ukazatele výkonnosti

12.3 Zajištění a zvyšování kvality při provádění zakázek

Navazující zcela nový standard 9.2 Strategie interního auditu požaduje, aby CAE vytvořil, a poté realizoval strategii interního auditu, která podpoří – v souladu s očekáváními Boardu, managementu a dalších stakeholderů – strategické cíle a úspěch společnosti. Tato strategie musí být minimálně jednou ročně posouzena a vyhodnocena ve spolupráci s vyšším managementem a Boardem.

Standard 9.4 se nově věnuje metodice interního auditu, za jejíž tvorbu, vyhodnocení a aktualizaci je zodpovědný

CAE a uvádí 12 oblastí, které musí metodika pokrývat.

Standards pod principem č. 10 nově upravují řízení zdrojů a postupně se zaměřují na zdroje finanční, lidské a technologické. Za řízení zdrojů ve všech oblastech je zodpovědný CAE, který navrhuje rozpočet, plán rozvoje lidských zdrojů a dostatečnou technologickou podporu. V každé oblasti musí zdroje pravidelně vyhodnocovat a včas signalizovat jejich nedostatečnost.

V oblasti komunikace je zcela nový standard 11.1 Budování vztahů a komunikace se stakeholdery (tj. zejm. Boardem, senior managementem, provozním managementem, regulátorem a interními a externími poskytovateli služeb). Důraz je kladen jak na formální, tak neformální komunikaci, aby došlo k vzájemnému porozumění, pochopení rolí a odpovědností jednotlivých stran a možností jejich spolupráce, např. v oblasti řízení rizik, naplňování regulatorních požadavků, a v neposlední řadě též v konkrétních oblastech zájmů dané společnosti, jejich procesů a finančního reportingu.

V principu č. 12 týkajícího se kvality a výkonnosti interního auditu zajišťované vedoucím interního auditu bude kvalita uvedena komplexněji a konkrétněji než je tomu v současných standardech nebo přesněji řešeno, mnohé z toho, co bylo nyní obsaženo v prováděcích směrnicích, se stane závazným požadavkem standardů – např. povinnost jednou ročně komunikovat výsledky hodnocení kvality s vedením, nutnost při pravidelném interním hodnocení vyhodnocovat každý standard, povinnost stanovit metodiku pro měření výkonnosti. Cílem tohoto principu je průběžné zlepšování kvality a výkonnosti funkce interního auditu ve společnosti.

„sebehodnocení s nezávislou validací nebude plně nahrazovat externí hodnocení kvality“

V tomto ohledu je zde zcela nový standard 12.2 Ukazatelé výkonnosti ukládající CAE povinnost stanovit po dohodě s vedením společnosti cíle interního auditu, za které bude zodpovědný a které budou pravidelně vyhodnocovány. Současně musí CAE vyvinout metodiku pro měření výkonnosti funkce interního auditu, stanovit kritéria výkonnosti a způsob měření. Standard 12.2 též uvádí 15 oblastí, na které je vhodné ukazatele výkonnosti zaměřit.

Celkově je možné konstatovat, že povinnosti vedoucího interního auditu jsou pojaty v současných standardech dosti obecně. V nových Globálních standardech je role CAE konkretizována od vrcholových strategických odpovědností přes jeho povinnosti při řízení útvaru interního auditu a komunikaci s vedením až po konkrétní nástroje, např. právě v oblasti výše uvedeného měření výkonnosti.

„v nových Globálních standardech je role CAE konkretizována“

Pro obě zde uváděné domény je relevantní skutečnost, že mnohé požadavky, které jsou nyní součástí prováděcích směrnic, nebo dokonce Manuálu kvality IIA, se dostávají přímo mezi povinnosti do standardů. Dále jsou pak podrobněji rozpracovány v navazujících přístupech pro realizaci daného standardu. Takže, jak bylo uvedeno již v prvním článku ke standardům – vše k jednomu určitému standardu, jak povinnosti, tak i praktické návody k realizaci a k prokázání

souladu se standardem, budou dohledatelné na jednom místě, včetně provazeb na další související standardy.

„mnohé požadavky, které jsou nyní součástí prováděcích směrnic, nebo dokonce Manuálu kvality IIA, se dostávají přímo mezi povinnosti standardů“

Doposud jsme se v jednotlivých číslech časopisu věnovali obecně charakteristice nového Rámce a představení prvních čtyř domén Globálních standardů. V posledním letošním čísle časopisu si představíme poslední pátou doménu – V. Provádění auditních služeb – určenou všem interním auditorům.

Pozn.: Veškeré novinky lze průběžně sledovat na webových stránkách Mezinárodního institutu: theiia.org.

Inzerce

Digitalizace, datová analýza a blockchain v interním auditu?

Pojďte s námi tvořit interní audit budoucnosti

Jsme lídrem v inovacích interního auditu a kontrol. Nastavujeme trendy v technologické transformaci se zaměřením na lidi, procesy a nástroje.

Více na ey.com/cs_cz/risk



JAKOU SÍLU MÁ MYSL

VĚŘÍTE TOMU, ŽE MYŠLENKY A POCITY OVLIVŇUJÍ NÁŠ ŽIVOT?



Alena Jáchimová
lektorka a koučka
Power Coaching

Vše, co jsme jako lidé vytvořili, vzniklo z myšlenky a z našeho zánícení pro ni. Svět kolem nás je takový, jak o něm přemýšlíme. I svůj život si často nevědomě svými myšlenkami utváříme. Přesto se nám stává, že nesebereme odvahu splnit si to, co si z hloubi duše přejeme. Naše mysl dopředu staví mentální zdi tam, kde se ani nepokusíme selhat, a to z banální představy, že úspěch je zcela nemožné. Minulé zkušenosti, které ani nemusí být naše vlastní, podvědomý, strach z neúspěchu a blamáže, nás limitují. A i to má svůj důvod.

Pokud chcete být charismatičtí musíte se umět dostat do žádoucího duševního stavu. Součástí toho je uvědomovat si své myšlenky, pocity, nálady a umět s nimi efektivně zacházet.

Kde se berou myšlenky?

Myšlenky se rodí v těle, stejně jako víra ve vlastní pravdu. Tato pravda, nebo jinými slovy lidská přesvědčení o vlastní hodnotě a smyslu, utváří naši identitu, která zase souvisí s tím, do jakého těla, rodiny, třídy, etnika, kultury atd. jsme se narodili.

„Existují myšlenky, které námi projdou bez povšimnutí, a existují ty, které se v nás zabydlí, a některé z nich nám dokážou zamotat hlavu i život.“

Myšlenky se objevují. Objeví se jedna, za ní druhá, třetí a postupně přicházejí další a další. Časové rozmezí mezi nimi je tak nepatrné, že je sotva postřehneme. Představte si, že myšlenky jsou dav, který se skládá z individualit. Jestli se seskupí více individualit, vzniká síla přesvědčení. Existují myšlenky, které námi projdou bez povšimnutí, a existují ty, které se v nás zabydlí, a některé z nich nám dokážou zamotat hlavu i život.

Jak je to možné?

Podívejme se na následující situaci. Je pozdě večer. Jdete sami temnou částí města. Máte pocit, že za vámi někdo jde. Myšlenka je stále neodbytnější,

přepadne vás strach a vy začnete utíkat. Ten někdo je váš stín. Čím jste rychlejší, tím rychlejší je i stín. Když ještě dokážete ovládnout svůj strach a podívat se na stín, zjistíte, že je jen důsledkem nepřítomnosti světla a spouštěčem jedné staré zkušenosti, která nejspíš ani nebude vaše. Avšak zastavit ve svém mozku tento sebezáchovný proces není vůbec snadné. Proč? Naše tělo je zranitelné a smrtelné. Prvořadou úlohou našeho mozku je chránit život, a tak „nasává“ z prostředí, do kterého jsme se narodili, to, jak svět funguje, jakými zákony se společnost řídí a kde jsou skrytá nebezpečí. Během několika málo let je „nastavení“ hotové a náš mozek má návod na to, jak být v životě „úspěšný“. Kde je tedy háček? Je jich hned několik:

1. Svět se mění opravdu rychle; vzorce, které jsme přijímali v dětství, kdy naše učení bylo nejintenzivnější, jsou nyní již značně zastaralé. A stáhnout si novější verzi sama sebe není tak snadné jako aktualizovat program ve svém PC. Stojí to úsilí a čas.

2. Často děláme rychle, jednostranné závěry, soudy a svým pozitivním a negativním emocím přisuzujeme příliš velkou váhu. Všimněte si, jak snadné je zapřísahat se, že už „nikdy“ nebo spoléhat na naše „vždycky“.

3. Mozek je „negativně předpojatý“. Jedním z jeho klíčových úkolů je chránit náš život, fyzické bytí, zkrátka přežít. Proto preferuje zapamatovat si negativní věci, zážitky, abychom se jim příště vyhnuli, a neohrožovali tak svůj život. Dnes je téměř nemožné potkat na ulici šavlozubého tygra, ale pocity ohrožení jsou v nás stále přítomné. A naše představivost pak dokáže vidět ony pomyslné šavlozubé tygry a prožívat „boj o život“ v každé překážce, který nám náš šéf, partner či život přichystá.

4. Naše racionální mysl a ego těžko nesou, když neví, neorientují se. Ztráta jistoty a chaos vzbuzují často nepříjemné pocity. A tak k tomu, co pozorujeme v okolním světě, si neustále vymýšlíme příběhy

a interpretace, které ale nemusí mít vůbec nic společného s realitou. Často jde o příběhy z „černé kroniky“. Vycházejí totiž z naší úzkosti, obav a strachu.

5. Vyhýbáme se bolesti, nepohodě. Osvojujeme si celou řadu přesvědčení a vzorců chování, které nás utvrzují, že něco není možné, nejde, nefunguje, nezdaří se nám, nezvládneme. Každý z nás v dětství a dospívání zažil něco bolestivého, něco, co nás zranilo, tyto staré rány a pocity oživuje mnohdy nevědomě každá zdánlivá podobnost. Naše tělo nezapomíná. Panikaříme, soudíme a vytváříme si nepřátele.

„máme silnou tendenci si vytvářet domněnky a dáváme vysokou hodnotu našim myšlenkám a pocitům, které jsou s nimi spojeny.“

Zkrátka máme silnou tendenci si vytvářet domněnky a dáváme vysokou hodnotu našim myšlenkám a pocitům, které jsou s nimi spojeny. Faktem je, že tyto myšlenky nemusí být pravdivé, ale pokud jim uvěříme, jsou mocné.

Ať už si svých přesvědčení jsme, nebo nejsme vědomi, silně ovlivňují naše jednání, naše životy a to, zda doopravdy získáme to, co chceme.

Vědci vyzkoumali, že člověk má za den asi 60 tisíc myšlenek – což je dost početný dav. To, co mnozí děláme, když se domníváme, že myslíme, není nic jiného než volné přehrávání si „starých mentálních gramodesek“. Vědci také tvrdí, že až 95 procent myšlenek je stejných jako ty, které jsme měli včera a přede včirem. Opakují se nám v hlavě každý den. Jen zbývajících pět procent věnujeme myšlenkám tvůrčím.

Můžu svoje myšlenky nějak ovládat, nebo absolutně ne?

Myšlenky námi proudí, jako proudí dav lidí ulicemi. Objevují se a mizí do svých domovů, a ulice se tak stávají tichými a prázdnými. Myšlenky se objevují a zase mizí v prázdnotě, v tichu. Pokud si toto uvědomujeme, stáváme se pozorovatelem, svědkem celé této myšlenkové promenády. Tím myšlenky dostáváme pod kontrolu a můžeme je kultivovat, šlechtit a rozvíjet zcela vědomě. Najednou se stáváme vlastníky existujících myšlenek, a tudíž ne ony námi, ale my jimi můžeme vládnout.

„Změníme-li náš vysvětlovací styl ohledně selhání, výrazně snížíme riziko depresí a zvýšíme naši životní spokojenost.“

Můžeme pak objevit různé myšlenky, pocity a vzorce chování, které jsme přijali z prostředí, ve kterém jsme vyrůstali, a dnes nám už neslouží.

Fixní, nebo růstové myšlení

Se zajímavými objevy přišla Carol Dweck. Výzkumy jejího týmu ukazují, že to, jak bude náš život vypadat, je opravdu z velké části v našich hlavách. **Změníme-li myšlení z „fixního“ na „růstové“, náš život se výrazně promění.**

Carol Dweck ve svém výzkumu vzala 128 dětí v rozmezí 10–11 let a rozdělila je na dvě skupiny. Nechala je řešit matematické problémy a pak dětem v první skupině řekla: „Daří se ti, musíš být hodně chytrý.“ Druhé skupině řekla: „Daří se ti, určitě jsi se hodně snažil.“ V další části výzkumu jim dala řešit těžší problémy, dokonce tak těžké, že je skoro nikdo nevyřešil. Do třetice dostaly děti opět lehké zadání.

Výsledek byl takový, že ve třetím testu děti chválené za intelekt (něco daného = fixed) skončily o téměř 25 % hůře než děti chválené za snahu (něco změnitelného = growth).

Lidé s fixním myšlením (fixed mindset) věří, že jsou karty rozdány. Že jejich intelekt a schopnosti jsou dané. Věří například, že pokud jsou introverti, budou vždy introverti. Zkrátka nic se s tím nedá dělat. Růstově přemýšlející lidé (growth mindset) věří tomu, že jsou věci změnitelné, že to mají ve svých rukou. Aktuální výzkumy lidského mozku ukazují, že pravdu má spíše druhá skupina. Mozek je neuroplastický, tj. můžeme ho posilovat podobně jako naše svaly. **Vlastnosti jako kreativita, síla vůle, odvaha, pečlivost či komunikativnost nejsou vrozené, ale spíše naučitelné.**

Jak přesně se tyto dva zmíněné typy myšlení projevují? Typickým rysem fixního myšlení je vzdávání se před překážkou, neschopnost přijímat zpětnou vazbu, špatný pocit z úspěchu ostatních, vyhýbání se výzvám a negativní postoj k úsilí jako takovému. Naopak růstové myšlení se projevuje vřelým vztahem k výzvám, vytrvalostí při čelení překážkám, pozitivním vztahem ke kritice. Růstově myslící člověk vnímá úsilí jako cestu k mistrovství a v úspěchu druhých vidí inspiraci.

Výzkumy dalšího psychologa, Martina Seligmána dokonce dokazují, že i optimismus a pesimismus

nejsou věci vrozené, ale naučitelné. To, jak si vysvětlujeme naše selhání, takzvaný vysvětlovací styl, zásadně ovlivňuje také riziko depresí. Pokud selže pozitivně laděný člověk, řekne si, že **příště se mu bude dařit**. Pokud selže negativně laděný člověk, říká si, že **tak to bude vždy**. Přesně opačně reagují obě skupiny na úspěch. Pokud pozitivní člověk uspěje, říká si, že **tak to bude vždy**. Pokud uspěje negativní člověk, řekne si, že **příště to zase zkaží**. Změníme-li náš vysvětlovací styl ohledně selhání, výrazně snížíme riziko depresí a zvýšíme naši životní spokojenost.

„Pokud věříte, že to půjde, i když věříte, že to nepůjde, tak v obou případech máte pravdu.“
Henry Ford

Sebenaplnující proroctví

Velký problém přináší dělení lidí do škatulek a různých typologií. Ať už jde o dělení na choleriky, sangviniky, introverty, extroverty, či berany a blížence. Pokud někomu řeknete, že je „nějaký“, často to vezme jako nezměnitelný fakt (fixed). A díky takovému nastavení mysli se to opravdu stane pravdou. Mluvíme o takzvaném **sebenaplnujícím proroctví**.

V jednom výzkumu učitelé ve škole dostali tipy na obzvlášť šikovné děti, které ale byly úplně průměrní a normální žáci. Za rok se těmto dětem výrazně zlepšil prospěch. Jak se to stalo? Tato malá lež změnila nastavení

a očekávání učitelů. Ze skrytých záznamů experimentátoři zjistili, že se učitelé chovali k vybraným dětem jinak – častěji je vyvolávali, více je chválili apod.

Podobný výzkum dělali vědci s krysami. Účastníci experimentu měli naučit chodit krysy bludištěm. Dozvěděli se, že zvířata pocházejí ze dvou různých populací – „chytré“ a „hloupé“. V realu byly krysy rovnoměrně rozděleny do dvou smíšených skupin, což ale studenti nevěděli. Krysy, které pokládali za chytré, se naučily projít bludištěm mnohem rychleji, protože s nimi studenti komunikovali mnohem intenzivněji než s těmi, které považovali za hloupé.

Oba výzkumy mluví o tom, jak silně nás dokážou ovlivňovat naše myšlenky a postoje, jak mocné mohou být vyslovené soudy. I staré přísloví zmiňuje: „Stokrát vyslovená lež se stává pravdou.“ Neodsoudil vás také takto někdo v dětství? Neřekl vám například, že na matematiku nemáte hlavu nebo vám chybí pohybové nadání či že jste „věčný smolař a nic pořádného z vás nevyroste“? Možná jste takoví nebyli, ale mohli jste této myšlence uvěřit. Pak nezoufejte a **změňte si své myšlení z fixního na růstové. Jde to, jak ukazují zjištění Carol Dweck. Ta přinášejí naději a možnost učít se svůj potenciál využít naplno.**

Váš vnitřní stav, vaše naladění je z hlediska charismatu klíčové – ovládněte tedy svou mysl. Poznejte své negativní myšlenky,

sabotéry, kteří vám často „házejí klacky pod nohy“. Jako jsou například: „nejsem dost dobrá...“, „to nezvládnou“, „vždycky to nakonec pokazím“. Nepouštějte do svého života a do své hlavy myšlenky, které nechcete žít. Učte se s nimi pracovat tak, aby neničily vaši (sebe)důvěru a neodháněly od vás zajímavé příležitosti a ostatní lidi. **Charisma zkrátka začíná v hlavě.**



Mgr. Radka Moricová

specialista PR
Centrum pro rodinu a sociální péči z. s.

Vztahy? Rodina? Někdy to není jen tak

Péči o vztahy a rodinu se ostravské Centrum pro rodinu a sociální péči z. s. věnuje už 30 let. Za tu dobu se podařilo nasbírat zkušenosti, poučit se z chyb a nahlížet na problémy mnoha různými úhly pohledu. Stále nacházíme nové možnosti, přicházejí rozliční lidé a my je doprovázíme na jejich cestě životem.

S těžejními pilíři naší práce je **podpora rodiny, manželství a péče o děti a mladé lidi se zdravotním postižením.** Významnou aktivitou je také **vzdělávání dětí, rodičů i seniorů.** Všechny aktivity realizujeme prostřednictvím dvou středisek.

„Stěžejními pilíři naší práce je podpora rodiny, manželství a péče o děti a mladé lidi se zdravotním postižením. Významnou aktivitou je také vzdělávání dětí, rodičů i seniorů.“

Středisko **RODINA** podporuje fungování rodin, poskytuje poradenství zaměřené

na vztahy a rodinu, doprovází pěstounské rodiny a také realizuje přednáškovou a vzdělávací činnost. Spokojená rodina není samozřejmostí a naši odborníci jsou připraveni pomoci.

Řešit problémy, až když nastanou? Není lépe se potíží vyhnout a předejít trápení? My jsme přesvědčeni o tom, že nejdůležitější je právě prevence. Proto nabízíme svou pomoc všem napříč různými věkovými kategoriemi.

Dětem a mladým, žákům základních škol a studentům středních se věnujeme ve **Škole osobního života.** Soustředíme se na formování postojů a hodnot, a tím na zlepšení přijetí sebe samého. Přicházíme za nimi přímo do škol a ukazujeme jim, jakými způsoby lze nahlížet na život.

Mladým, kteří uvažují o manželství nebo se na něj už připravují, nabízíme několik možností:

- nejobsáhlejší je program pěti víkendů zvaný **Škola partnerství** naplněný přednáškami, diskusemi, prací ve skupinách, ale také prostorem pro společně strávený čas a zážitkové aktivity,
- několik druhů kurzů různého trvání s večerí při svíčkách, povídaním a řešením úkolů, jako je **Než do toho vletíš, Na svatbu byl pozván...**, **Příprava na Manželství**,
- jako inspirace či motivace k další práci na vztahu poslouží **Vyjmenovaná slova**,
- nebo také videokurs jako doplněk pro dvojice, pro které je osobní účast nemožná **Distanční příprava na manželství**.

Pro manžele je velkým povzbuzením zúčastnit se, prožít si a mít možnost sdílet své radosti či starosti na těchto akcích:

- užít si rande i v manželství nabízíme v programu osmi setkání s inspirací, jak budovat zdravé a trvalé manželství s názvem **Manželské večery**,
- týdenní letní setkání manželů na **Velehradě s obohacujícím programem Škola rodičovských a rodinných kompetencí nebo Studia manželství a rodiny**.

Pro všechny, kteří mají zájem na sobě pracovat a dozvědět se více o komunikaci a rodičovství, nabízíme tyto kurzy:

- **Kurz efektivního rodičovství** pro rodiče dětí různého věku,
- kurz o komunikaci jako cestě k vzájemnému porozumění a lepším vztahům **Cesta efektivní komunikace**,
- podpora párů k odpovědnému **plánování rodičovství Plánování rodičovství pevně pod kontrolou**.

I senioři si u nás přijdou na své. Už 15 let pořádáme přednášky s diskusí **Akademie pro třetí věk**.

Od loňského roku jsme se přímo v terénu seznamovali s kulturním a historickým dědictvím v **Akademii pro třetí věk – cestách za poznáním**. Během celého roku pořádáme pro seniory spoustu přednášek, setkání a aktivit.

V průběhu celého roku pořádáme různá setkání dětí a rodin, expedice pro otce a jejich děti, rodinný festival i další kurzy a semináře.

Jestliže problémy nastanou a lidé jsou ochotni je řešit, nabízíme jim pomoc v obtížných rodinných i vztahových situacích formou **mediací, vztahového poradenství či komplexního poradenství na podporu rodiny a rodičovství**.

„Dětem a mladým, žákům základních škol a studentům středních se věnujeme ve Škole osobního života.“

V rámci pověření k výkonu sociálně-právní ochrany dětí **doprovázíme pěstounské rodiny**.

A také podporujeme, provázíme a pomáháme zvládat život v **rodinách s dětmi a mladými lidmi se zdravotním postižením**. Prostřednictvím Střediska **VÝZVA** poskytujeme tyto čtyři sociální služby: osobní asistence, odlehčovací služba pro pečující rodiče,



odborné poradenství a sociálně aktivizační službu. Mimo oblast sociálních služeb nabízíme půjčování pomůcek pro osoby se zdravotním postižením a rehabilitační asistenci. Pomáháme rodinám v jejich nelehké situaci překonávat překážky a žít „běžný“ život.

„Centrum sídlí v Ostravě-Vítkovicích, v areálu Lékařské fakulty Ostravské univerzity.“

To vše naše Centrum nabízí. Sídlíme v Ostravě-Vítkovicích, v areálu Lékařské fakulty Ostravské univerzity. A právě tady se odehrává většina aktivit a nabízených služeb. Ale nebude tomu tak

i do budoucna. Pracujeme na tom, abychom se mohli přestěhovat do větších prostor v centru města. Nová budova v areálu Městské nemocnice Ostrava tak bude dostupnější a naše služby se budou moci rozšířit.

Níže uvádíme komentáře *Jana Zajíčka*, dlouholetého předsedy Centra pro rodinu a sociální péči, v současnosti rodinného konzultanta, mediátora a předsedy Rodinného svazu ČR.



Jak poznám, že já, můj vztah, má rodina potřebuje mediaci či rodinnou konzultaci?

Zůstanu nejprve u toho páru. Když jsme schopni si povídat o věcech srdečných, jak já říkám o věcech, co máme za hrudní kostí, tak to znamená, že jsme zdraví. Znamená to, že jsme pro sebe čitelní, že jsme si bezpeční, tudíž, že jsme milovatelní. Pokud o tohle přijdeme, tak to je velmi vztyčený prst. Protože každý z nás ze své podstaty, ze své přirozenosti potřebuje a touží být milován a milovat. Ale pokud nejsem schopen mluvit o svých niterných věcech s protějškem, tak to je znakem, že se necítím bezpečně. Při ztrátě tohoto pocitu je nutno buď to zkusit napravit sami, ale pokud se to nedaří, tak vyhledat třetí osobu. Byl mnoho lidí má předsudek, co si budeme své špinavé prádlo prát před někým třetím. Ale já bych to velmi doporučil. Protože pak se ten hovor sníží pouze na provozní rovinu, fungující a funkční, a i tam se postupně začnou projevovat vlivy různých alergií na sebe navzájem. A to už je pak velmi pozdě a trvá potom spoustu času takový vztah očistit od všech těch nánosů a závaží.



V rodině je to dosti podobné, protože největší touhou dětí je vidět milující se rodiče. Pokud děti tohle ztratí, tak začnou svou nejistotu, neklid vyjadřovat směrem k rodičům. Rodiče říkají, že děti takzvaně zlobí. A chování dítěte umravní namísto toho, aby upravili své chování mezi sebou, aby se dítě mohlo zklidnit. A mnohdy to přechází v to, že své dítě dovedou k psychologovi a do různých odborných poraden, a přitom zdrojem toho, co se v dítěti odehrává, jsou oni sami.

„Pomáháme zvládat život v rodinách s dětmi a mladými lidmi se zdravotním postižením.“

Takže tohle platí pro celý systém. Je-li mezi námi láska, pohoda, důvěra, tak jsme schopni překonat i různé potíže, starosti, překážky, neúspěchy, havárie. Protože pokud si o nich můžu s důvěrou popovídat a mám k tomu ty příslušné dovednosti, tak přece platí zásada, že chyba není důvod ke kritice, ale k růstu. A my skrze chyby můžeme růst. A je to jedno, jestli jsem dítě,





nebo rodič, protože i rodiče rostou svými chybami v rovině vztahové či rodičovské.

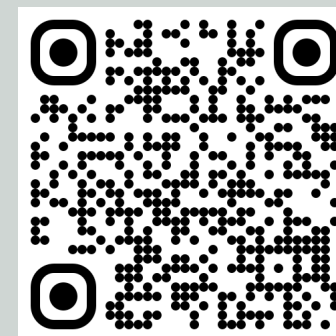
Co je podle Tebe pro úspěšné partnerství nebo manželství důležité?

Já si myslím, že existují tři klíčové dovednosti pro to, aby lidé mohli prožít svůj vztah. Přestože budou doživotně chybovat, tak aby vztah mohl růst, a přesto, že jejich fyzické a mentální síly budou slábnout, aby se mohli cítit stále lépe a šťastněji. To znamená, musíme se naučit dobře zvládnout lidsky úplně odpuštění. Což je velký rozdíl, protože mnoho lidí, říká, my si odpouštíme, a pak mluví o věcech starých pět, deset let s hořkostí, bolestí, zlobou, a to je jasný signál, že odpuštění buď neproběhlo, anebo je v průběhu, ale ne moc zdárném. Samo odpuštění ale nestačí. Protože i kdybychom odpustili, ale na druhou stranu kvůli svým nedokonalostem jsme na hromadu svých ublížení přidávali další, tak ta hromada bude stále stejná. Takže další věcí je naučit se velmi dobře zvládat prevenci, ať už dopředu, nebo dozadu. A ta třetí dovednost, také velmi důležitá, tou je umění být nedokonalý. Netrvat na dokonalosti, protože dokonalosti nejsme schopni. Dokonalost je nemožná, ale zdokonalování je možné.

„Mladým, kteří uvažují o manželství, připravujeme program Škola partnerství, kurzy Než do toho vletíš, Na svatbu byl pozván...; pro manžele program Manželské večery aj.; pro seniory přednášky s diskusí Akademie pro třetí věk a Akademii pro třetí věk – cesty za poznáním aj.“

Jestliže zapojíme všechny tyhle tři prvky, a ještě nějakou sadu dovedností, tak přestože celoživotně budeme chybovat, budeme ubližovat svými chybami a chybami druhých nám bude ubližováno, tak můžeme zvládnout prožít krásný společný život a na konci té cesty řekneme „děkuji Ti, bylo to krásné, nic bych neměnil“.

Podpora je možná zde:



Noví členové

- Denisa Bartošová, Ernst & Young, s.r.o.
- Elena Belugina, Edwards Lifesciences AG, organizační složka
- Ing. Eva Borecká, Národní památkový ústav
- Olga Faierman, individuální členka
- Ing. Silvia Groeneveld, individuální členka
- Ing. Kateřina Abou Chahine, Hlavní město Praha
- Mgr. Karla Chromá, individuální členka
- Kibria Kareem, individuální člen
- Ing. Jan Kořínek, Česká spořitelna, a.s.
- Bc. Richard Laluha, Krajské ředitelství policie hl. m. Prahy
- Kinga Laszczkowska, individuální členka
- Ing. Alena Levina, individuální členka
- Ing. Vlastimil Macháček, Nemocnice Kyjov, příspěvková organizace
- Mgr. Alena Matušová, Centrum pro regionální rozvoj ČR
- Bc. Nikola Opravilová, Fio banka, a.s.
- Bc. Andrij Popil, Fio banka, a.s.
- Ing. Iva Rendová, Český statistický úřad
- Ing. Martin Schwarz, ČEZ, a. s.
- Ing. Kateřina Sobotková, SCHEJBAL & PARTNERS s.r.o., advokátní kancelář
- Mgr. Zdeňka Sokolová, individuální členka
- Ing. Ondřej Sova, Fio banka, a.s.
- Tomáš Šandor, Československá obchodní banka, a. s.
- Bc. Irena Šípová, Hlavní město Praha
- Tatiana Škerlíková, individuální členka
- Mgr. Miroslav Tkáč, LL.M., individuální člen
- Ing. Miluše Tykalová, Státní tiskárna cenin, s. p.
- Jakub Tymočko, Ernst & Young, s.r.o.
- Petra Valentová, BBA, Státní tiskárna cenin, s. p.
- Ing. Vladimír Zejdl, MBA, Krajská nemocnice T. Bati, a. s.





1. blok: **23.–25. října 2023**
2. blok: **6.–8. listopadu 2023**



1. blok: **27.–29. listopadu 2023**
2. blok: **7.–8. prosince 2023**

