Aktuality

z tábora INTERNÍHO AUDITU

1.–2. listopadu 2023, Tábor

LH Hotel Dvořák Tábor ****

Český institut interních auditorů

WWW.INTERNIAUDIT.CZ

Antifraud/anticorruption management system
Blueprint ☺

PANELOVÁ DISKUSE

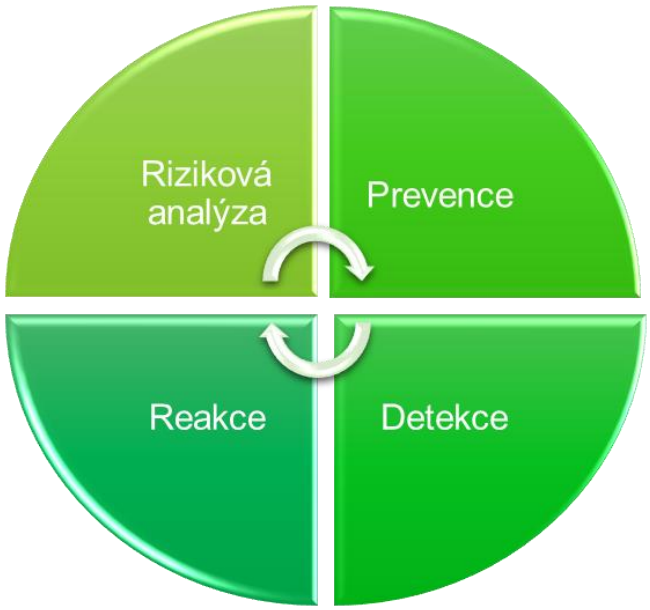
Petr Barák, předseda Komise pro bankovní a finanční bezpečnost (Česká bankovní asociace)

Kateřina Halásek Dosedělová, vice-president (ACFE Czech Republic Chapter)

Tomáš Pivoňka, ředitel útvaru audit a compliance (ČEZ)

Filip Zelingr, ředitel útvarů Interní audit, Řízení rizik a Compliance (Letiště Praha)

Anti Corruption/fraud components



Blueprint sestaven na základě požadavků ISO norem (např. 37001) a podnikové praxe

Antifraud management system je soubor analytických, preventivních, detekční a reakčních opatření, který zajišťuje efektivní identifikaci rizik podvodného (a šířeji – nekalého) jednání a jejich adekvátní prověření/řešení. Můžeme ho rozdělit na 4 části:

- **Riziková analýza**
  - Down top a Top down (periodiky)
  - Výsledek schvalován nevyšším vedením
- **Prevence**
  - Vnitřní pravidla
  - Komunikace (pravidelná a kampaně) a školení (standardní i fokusovaná)
  - Interní audity (hodnocení VKS a podvodné scénáře)
  - Externí audity, certifikace
  - Prověřování zaměstnanců a obchodních partnerů/ třetích stran
- **Detekce**
  - Etická linka
  - Compliance kontroly a interní audity
  - Automatizované kontroly (on-line auditing)
- **Reakce a zlepšování**
  - Šetření a forenzní audity (vč. formulace nápr. opatření a následných kroků)
  - Kontrola plnění nápravných opatření
  - Zlepšování specifické oblasti, ale i celého systému

1. Riziková analýza

- **Komplexní, pravidelná, strukturovaná a celopodniková**
- Identifikace **právní požadavků a relevantních etických principů** a zhodnocení pravděpodobnosti jejich porušení a dopadu takového porušení
- Informace z činnosti **interního auditu** (hodnocení VKS a podvodné scénáře) a **externího auditu** (mng letter)
- Informace z **ERM** (a vlastně celé firmy – BoD, Výbory, Komise)
- Diskuze **s vedením a bratry v triku** (právní, bezpečnost, ….)
- Výsledky jsou **schváleny nejvyšším vedení** a slouží jako prioritizace pro zaměření aktivit

2. Prevence

- **Jasná pravidla, jejich jasná komunikace, sponsorship a tone on the top**
- **Aktivní komunikace - internet a intranet, firemní časopis, výroční zpráva, zpráva o UR**
  - Pravidelná a kampaně
- **Interní audit** (hodnocení VKS a podvodné scénáře)
- **Externí audity, certifikace**
- **Prověřování zaměstnanců a obchodních partnerů/ třetích stran** (různé úrovně prověření dle hodnocení rizikovosti)
- **Nastavení compliance KPI / hodnocení a schvalování obchodních KPI**
- **Compliance kontroly** (kontroly střetu zájmů, kontroly dodavatelů, kontroly souladu s pravidly)
- **Konzultace (formální i neformální)** – připomínky k materiálů BoD, připomínkování ŘD, obchodních strategií, konkrétních transakcí

3. Detekce

- **Pasivní**
  - **Etická linka / vnitřní oznamovací systém** – různé kanály a zdroje (vč. zákazníků a obchodních partnerů), garantovaná ochrana oznamovatelů (dnes již legislativní povinnost)
  - **Incidenty** (systém řízení rizik)
  - **Interní audit** (hodnocení VKS, hodnocení a testování možných podvodných scénářů a konkrétní zjištění) a jiné **kontrolní útvary**
  - **Externí audity**
  - **Management**
- **Pouze pasivní detekce je nedostatečná**
- **Aktivní**
  - **Compliance kontroly** (kontrola střetu zájmů, kontrola dělení zakázek, prověrky KYC/S, background check zaměstnanců, …)
  - **Automatizované kontroly rizikových procesů** (continuous auditing) – „Early Warning System“: risk assessment, analýza scénářů, implementace kontrol

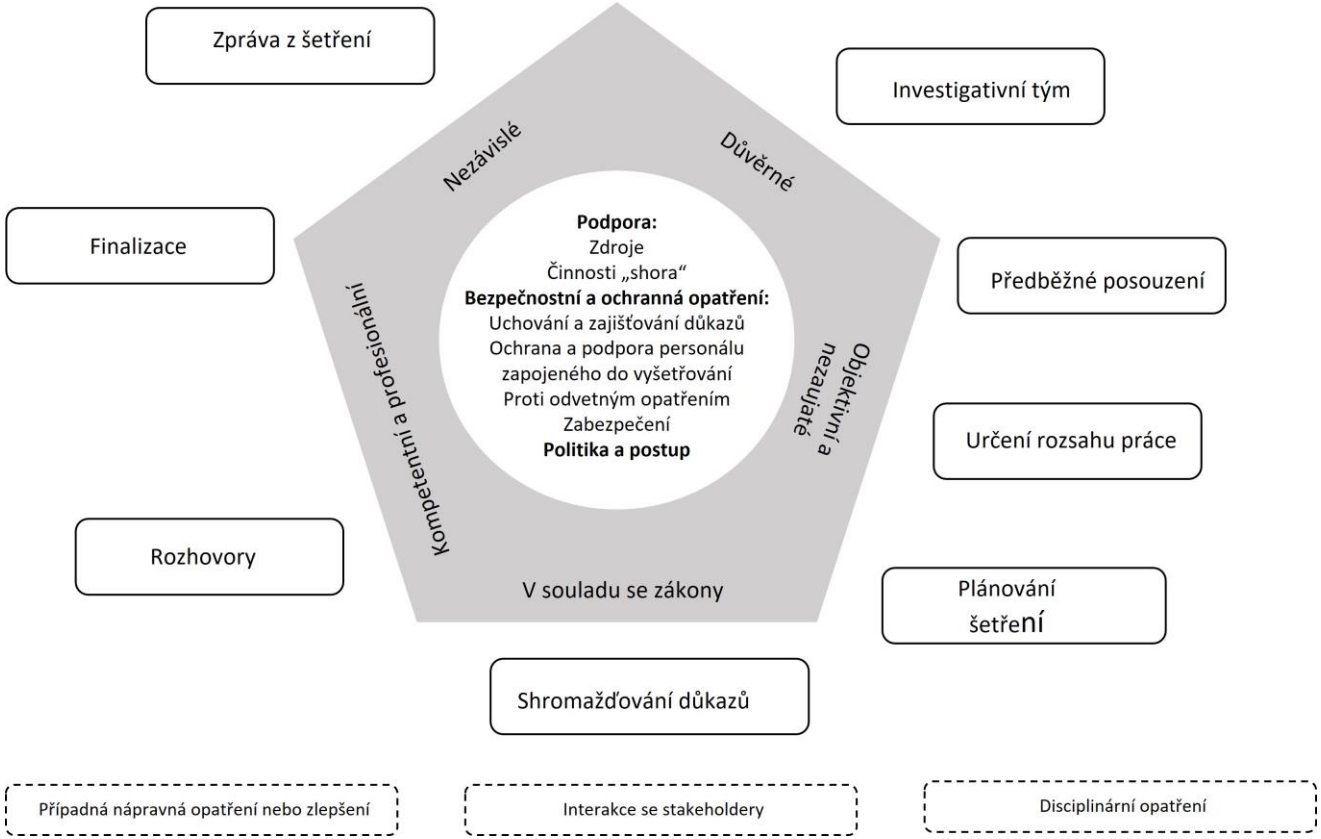
Early Warning System - Dashboard

Název kontroly	Období	Popis výsledku	Frekvence	Závažnost
Kontrola obratového nájemného	11/2021	OK - shodná hodnota	M	1
Fakturace služeb autopůjčovnám	11/2021	OK - fakturovaná částka se shoduje	M	1
	11/2021	OK - hodnota je v toleranci	M	1
Počty kód. lístků půjčovny	11/2021	OK - hodnoty v toleranci	M	1
Kódované lístky firemní účely	11/2021	Evidence je nedostatečná - rozdíl mezi 20 až 100 ks	M	3
Počet smazaných služeb	11/2021	OK - hodnota je v toleranci	M	1
Ruční zvedání výjezdových závor	11/2021	Chybí záznamy v rozsahu 3% - 10%	M	2
Kódované lístky mimo rozsah	11/2021	Lístky kodované korektně se směrnicí PAR	M	1
Kontrola zneužití průkazu ZTP	11/2021	Žádné duplicity čísla průkazů ZTP	M	1
Významné změny v nabídkách	11/2021	Nalezeny nabídky s výraznými posuny v pozicích či nabídkách mezi koly VŘ	M	2
Podobné nabídky soutěžících	11/2021	Vyskytují se dodavetelé s podobnými cenami	M	3
Koluze mezi soutěžícími	11/2021	Výskyty koluzí ve VŘ mezi dodavateli	M	2
Kontrola karty JACKPOT	11/2021	OK	M	1
Záměny check-in za manipulace	11/2021	Informativní charakter	M	1
Vazby mezi dodavateli ve VŘ	11/2021	Vazby nenalezeny	M	1
Záměny check-in za technik	11/2021	Informativní charakter	M	1
Neefektivní tendr či odhad ceny	11/2021	Nalezeny neefektvní tendry nebo nepřesné určení tržní ceny	M	2
Doba kola VŘ a špatný postup	11/2021	Alerty nenalezeny	M	1
Týdenní kontrola zvedání závor	11/2021	Nadsazené množství záznamů v evidenci dispečerů	T	4

4. Reakce a zlepšování

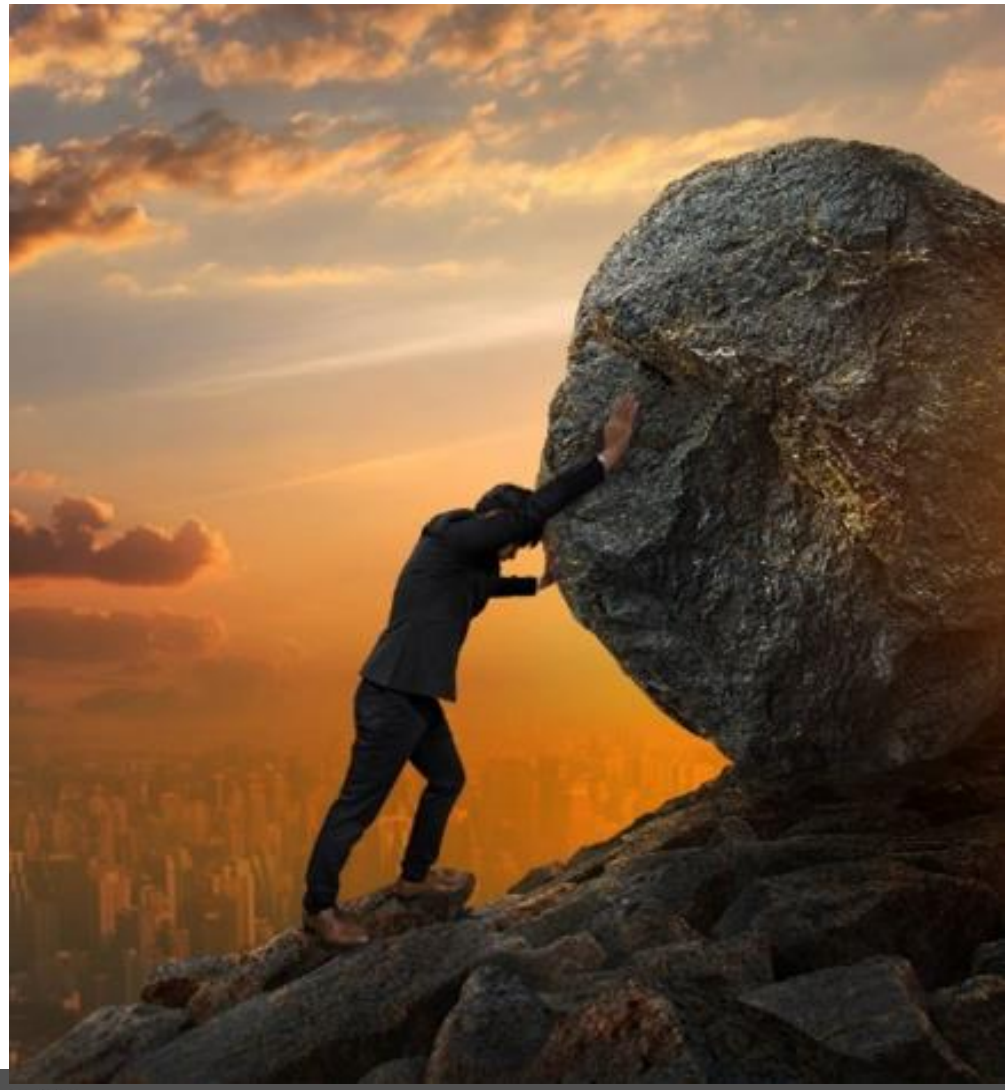
- **Šetření**
  - **Podnět** (interní – externí)
  - **Interně vs outsourcovat** (částečně či plně - forenzní audity)
    - Nový mezinárodní standard: ISO/TS 37008:2023 (Internal Investigations of organizations)
  - **Cíl:**
    - Zjistit skutečnosti a zajistit podklady pro další právní kroky
      - Kdo? – Co? - Kdy? - Proč? - Jak? - Kde? - Jak?
    - Objektivně posoudit zjištěné skutečnosti a jejich provazby
    - Zhodnotit, zda jsou podezření podložená
  - **Výsledek:**
    - Zpráva obsahující faktická zjištění a identifikované podklady
    - Formulace nápravných opatření
- **Právní kroky**
  - pracovní, obchodní a trestní právo na základě výsledků šetření a forenzních auditů
  - oznamovací povinnost TČ a očekávání OČTŘ v kontextu TOPO)
- **Vymáhání náhrady škody**
- **Zlepšování specifické oblasti, ale i celého systému (kontrola plnění nápravných opatření)**

Proces interního šetření dle ISO/TS 37008:2023



5. Aktuální trendy (výzvy) 1

- Trvale probíhající regulatorní změny
- Extenzivní nástup technologické inovace a digitalizace (změna chování a požadavky klientů, např. na tzv. „chytrá řešení“ vs ochrana identity)
- Kybernetická bezpečnost (bezpečnost fin. prostředků, citlivých dat / důvěra a soukromí)
- Nástup AI / etická dilemata (otázky odpovědnosti, rozhodování založeného na algoritmech, transparentnosti a důvěryhodnosti technologií)
- Schopnost rozpoznání reálného světa od virtuálního (např. deep fakes, deep voice fakes)
- Schopnost akceptovat AI nástroje i ve směru od klientů
- Nové informace a schopnost jejich efektivního / zákonného / využití a sdílení
- Změna chování útočníků (sociální inženýrství, stoupající obliba virtuálních měn
- …



5. Aktuální trendy (výzvy) 2

Vlastní vzdělávání

- Legal & Compliance znalosti
- Znalost všech produktů a služeb
- Znalost všech interních procesů
- Komunikační schopnosti
- Integrita (bezúhonnost)
- Znalost vlastních rizik a způsobů jejich řízení
- Analytické schopnosti / kritické myšlení
- Schopnost řešit problémy / krizový management
- IT znalosti (nástup AI)
- Schopnost se dál profesně rozvíjet
- Manažerské schopnosti / vedení týmu
- …