VKS pohledem interního auditora

Tomáš Pivoňka

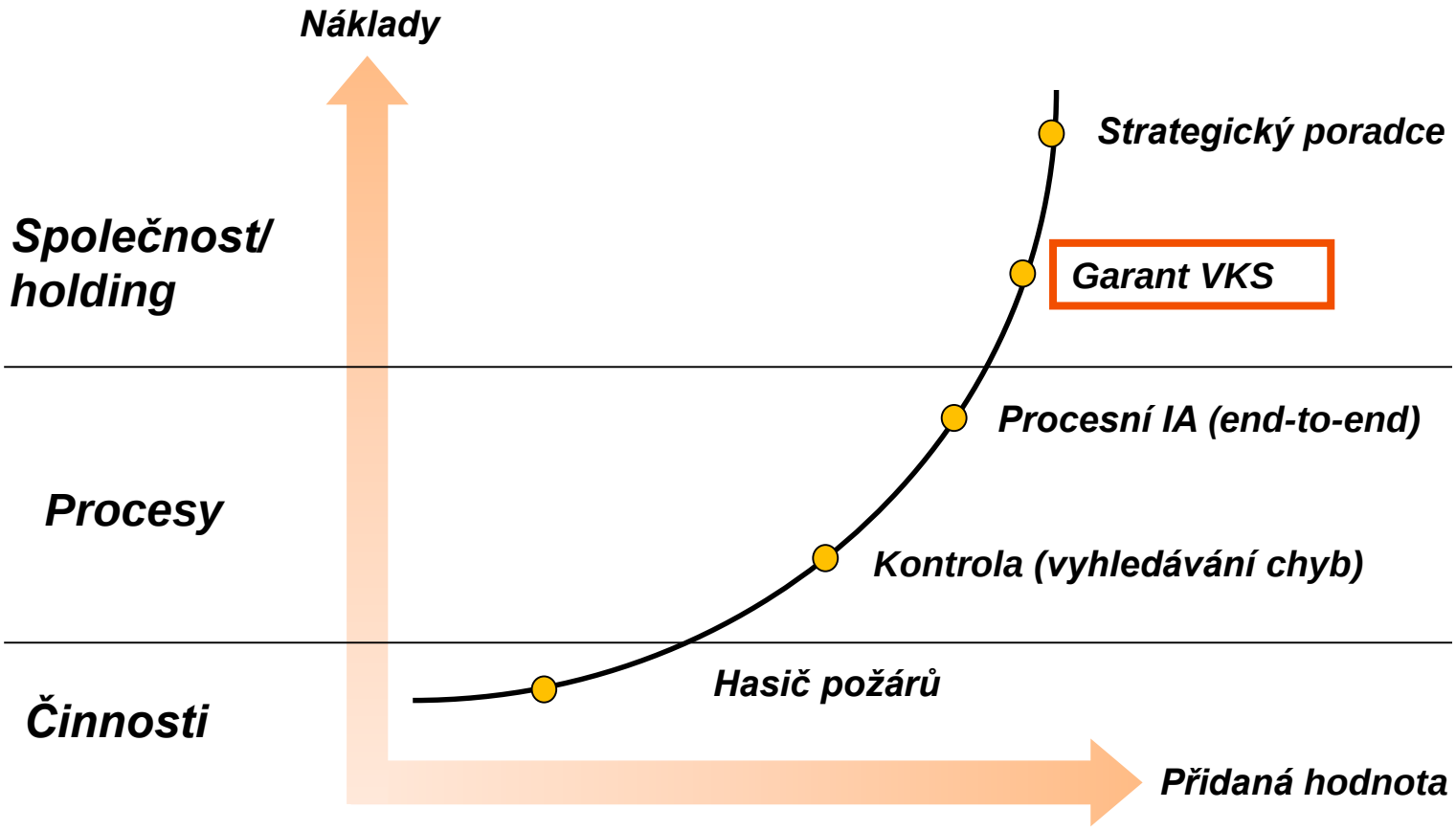
…Ale pane Pivoňko, to je přeci úplně všechno…

- ***COSO – mezinárodní standard více jak 20 let*** *- internal control is broadly defined as a process, effected by an entity's board of directors, management, and other personnel, designed to provide* ***reasonable assurance regarding the achievement*** *of objectives relating to operations, reporting, and compliance*

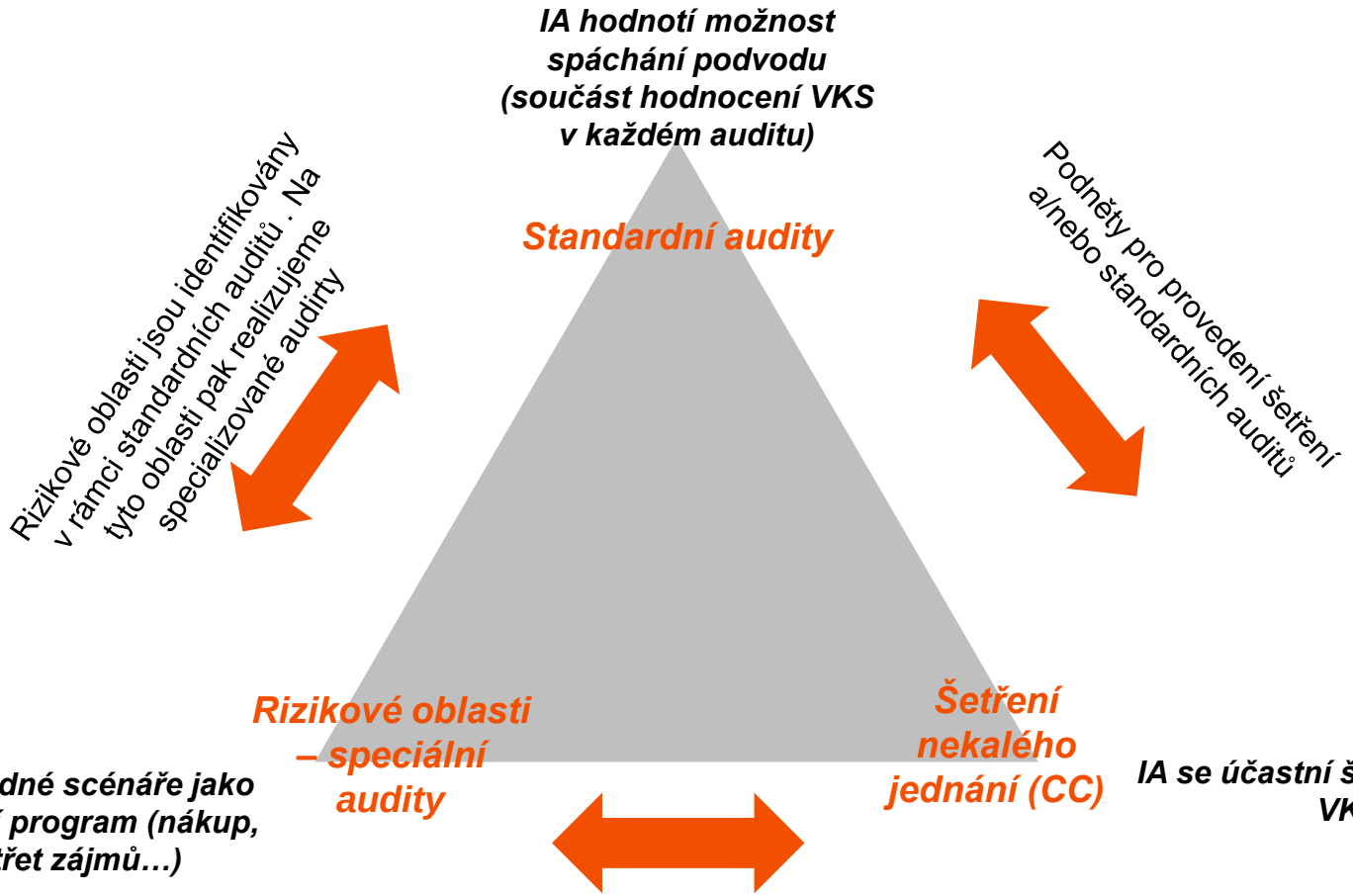
VKS z vrtulníku

- **Extrémně komplexní záležitost, po událostech 2001 a 2008 zvýšená pozornost regulátorů**
  - SOX
  - EBA - Internal Governance
  - EIOPA – Solvency II
  - ČNB – zákon a vyhlášky
- **Obsahuje opravdu všechno, zjednodušeně**:
  - Kostra - Organizace, postupy a pravidla (směrnice), kontroly, IT systémy, monitoring, informace a komunikace
  - Svaly – Lidé
  - Krev – Firemní kultura
- **Interní audit kultivuje kontrolní prostředí ve společnosti/organizaci**
  - Role tzv. ideálního hospodáře
  - Systematický přístup k rizikům a kontrolám

Role IA je výsledkem očekávání vedení a schopností IA



IA jako garant VKS je součástí systému Corporate Compliance ČEZ



Výsledky hodnocení podvodných scénářů jsou předávány do systému Corp. Compliance

IA jako garant VKS

Souhrnné hodnocení VKS v roční zprávě IA (zásadní vstup do hodnocení VpA pro VH)

- **Ujišťovací činnost - hodnocení VKS (80 % kapacit)**
  - Výkon auditů (plánované, mimořádné) - výrok k účinnosti VKS je součástí každé zprávy
  - Účast v systému corporate compliance

- **Konzultační a poradenská – ochrana „dobrého“ VKS (20 % kapacit)**
  - Připomínkování řídící dokumentace
  - Připomínkování materiálů do představenstva
  - Účast v orgánech a komisích – ředitel IA jako stálý host (představenstvo, porada vedení, výbor pro audit, výbor pro řízení rizik, výbor pro bezpečnost)
  - Účast ve strategických projektech formou Quality assurance (zejm. IT projekty a redesign klíčových procesů)

Strategie interního auditu ČEZ
Systematické pokrytí rizik a VKS

Přístup - Systematické pokrytí rizik / klíčových oblastí podnikání

- plní očekávání PAS (nemáme někde zásadní problém ?)
- vtahuje exekutivní vedení „do hry“ (jsou součástí hodnocení rizik – viz dále)
- umožňuje IA se vyjadřovat k účinnosti VKS (Roční zpráva IA, Roční zpráva VpA)

Nástroj - Střednědobý plán IA (Strategie IA)

- Rozdělení (cca 70) hodnocených procesních oblastí (procesní model ČEZ) do tří skupin dle průměrného hodnocení rizika za poslední 3 roky):
  - 20 nerizikovějších procesů,
  - 38 středně rizikových procesů,
  - 11 nejméně rizikových procesů.
- Různá frekvence auditů v rizikových skupinách:
  - skupiny nejrizikovějších procesů v průběhu 3 let (cca 7 procesů ročně),
  - skupiny středně rizikových procesů v průběhu 5 let (cca 7 procesů ročně),
  - skupiny nejméně rizikových procesů v průběhu 10 let (cca 1 proces ročně**).**

Hodnocení rizikovosti procesů
Postup

Expertní - subjektivní hodnocení skupin hodnotitelů:

- vedení společnosti (PAS),
- útvar řízení rizik a členů výboru RMC (D-1),
- útvar interní audit

•na stupnici od 1 (nejnižší riziko) do 5 (nejvyšší riziko)

•vážený průměr skupin hodnotitelů:

- 40% - vedení společnosti (PAS),
- 30% - útvar řízení rizik a RMC (risk),
- 30% - útvar interní audit (audit)

Projednání výstupů na Výboru pro řízení rizik a představenstvu

Back up

COSO Internal Control Framework

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Nejčastější/nejzávažnější nedostatky VKS

- Dle velikosti a maturity firmy/organizace
  - Malé a málo komplexní
    - Chybějící kontroly
    - Nepopsané kontroly
    - Management override
  - Velké a komplexní
    - Nepřehledné/nejasné struktury a odpovědnosti (i vlivem zastarávání)
    - **Přístupová oprávnění a kontroly v IT**
      - Nedostatečné oddělení oprávnění (kritická kumulace odpovědností), chybějící druhá úroveň schvalování,
    - Nefunkční kontroly (lidi nedělají to, co mají, resp. dělají to formálně)