

# **Dynamické řízení rizik skrze integrovaný systém kontrolního prostředí**

Cena za inovaci v interním auditu

Cílem projektu je implementovat dynamické řízení rizik, tedy dosáhnout stavu, kdy informace obsažené v systému řízení rizik poskytují v každou chvíli aktuální a ucelený obrázek o expozici rizika, úrovni jeho řízení a management je reálně využívá při operativním i strategickém rozhodování. To vše s vizí nestavět dva paralelní světy, nýbrž prostřednictvím sjednocení pohledu jednotlivých útvarů kontrolního prostředí na vlastní výstupy a jejich napojením na „živé“ procesy společnosti zajistit sblížení řídicích (výkonných) a kontrolních činností a jejich vzájemnou synergii.

Projekt předpokládá realizaci následujících inovativních přístupů:

- Jednotná metodika hodnocení rizik všemi klíčovými útvary kontrolního prostředí
- Jednotné řízení nápravných opatření ve společnosti

## Metodika „one-risk“

- Dynamický proces aktualizace rizik ve společnosti
- Kontinuální proces revize auditního plánu

## Rizika „on-line“

- Komplexní reporting rizik
- Komplexní reporting nápravných opatření

## One-page reporting

- Propojení informací prostřednictvím integrovaného systému

## Systémová integrace

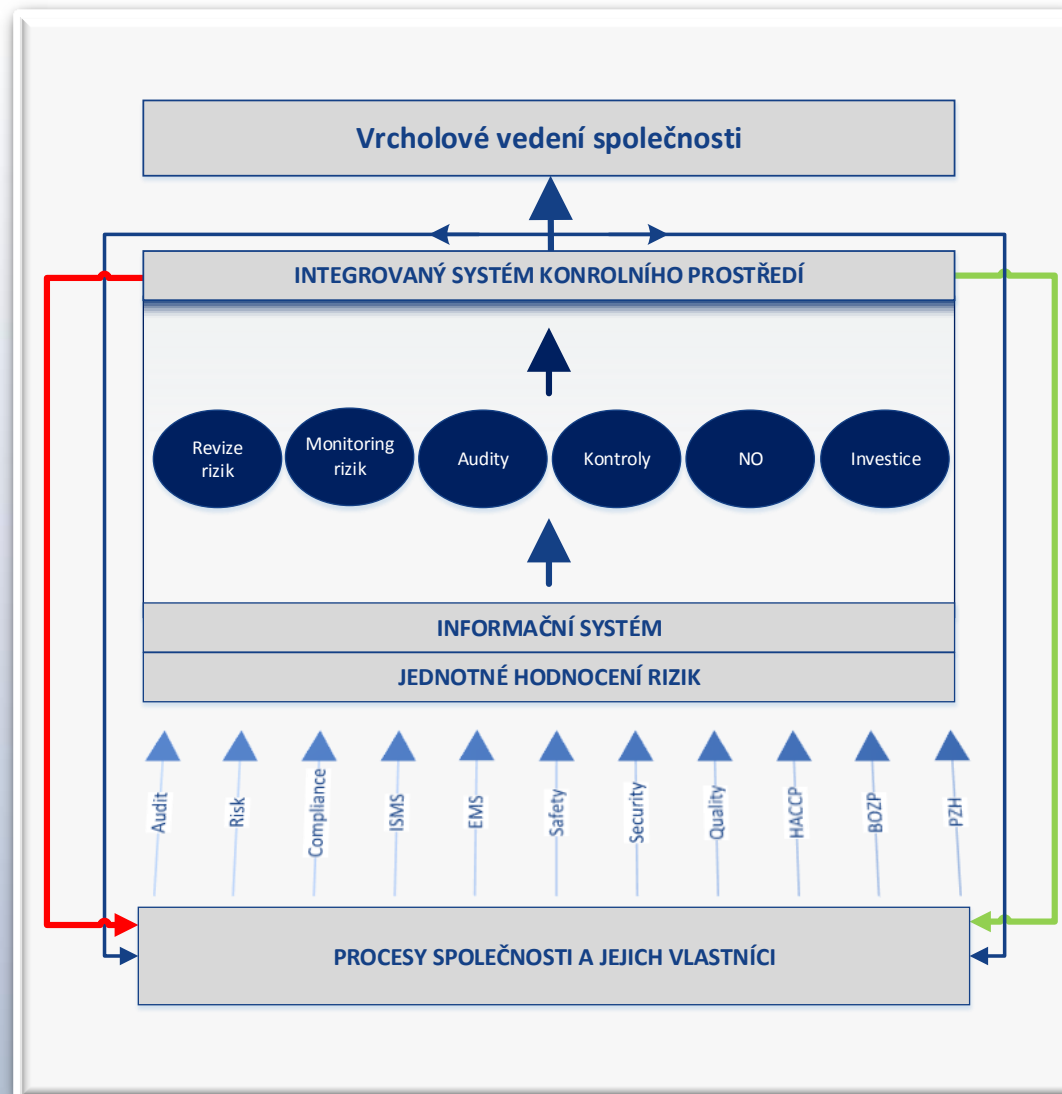
## Metodika „one-risk“

⇒ Implementace jednotné metodiky v rámci společnosti

- ❑ Metodika korporátního hodnocení rizik umožňující integraci výstupů dílčích systémů řízení rizik
- ❑ Jeden integrovaný seznam rizik
- ❑ Jednotná metodika pro nápravná opatření různých kontrolních útvarů
- ❑ Jednotná interpretace a reporting rizik

**INOVACE**

Jeden společný a úplný seznam rizik za celou společnost. Sjednocení jednotlivých principů z řady používaných metodik ve společnosti (např. ISMS, EMS, Safety, BOZP, PZH).



## Rizika „on-line“

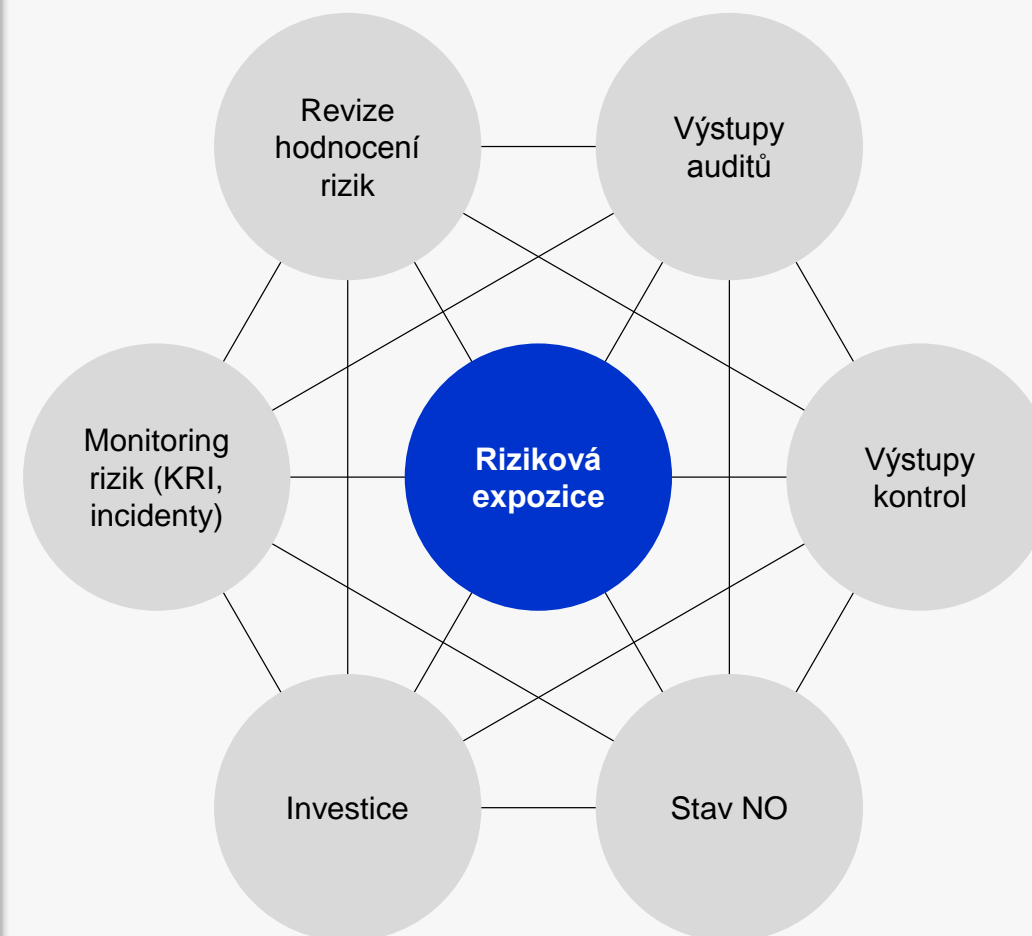
➔ Rizika jsou dynamicky hodnocena a aktualizována v bezprostřední návaznosti na:

- Pravidelná revize hodnocení rizik
- Výstupy auditů a šetření
- Aktuální stav plnění nápravných opatření (NO)
- Realizaci investičních akcí s dopadem na mitigaci rizik
- Výstupy kontrol
- Monitoring rizik (KRI, incidenty)

➔ Rizika v každém okamžiku zobrazují skutečnou expozici

**INOVAČE**

Propojení informací z různých zdrojů s vlivem na expozici rizik do jednotného dynamického systému (technicky i procesně) okamžitě zobrazující aktuální rizikovou expozici.



## „One-page“ reporting rizik

- ➔ Jednoduchý ale komplexní reporting vždy stejnou formou:
  - ❑ Od reportu jediného významného rizika obsahujícího jeho popis, expozici, význam, efektivitu jednotlivých mitigačních opatření i míru kontroly nad ním
  - ❑ Po přehledový report vybrané skupiny či všech rizik dané společnosti
  
- ➔ Na jedné straně A4 stejně využitelný jak jednotlivým vlastníkem rizika, tak vedením společnosti

INOVACE

Na jediné straně A4 komplexní informace o jednom či více rizicích stejně použitelné na všech úrovních vedení nebo vlastníkem rizika.

ID: KZ a název rizika		99999 Vzorové riziko	
Subjekt	CAH	Dopad do reputace	2
Název OJ	TST - Testovací	Dopad na zákazníka	1
Vlastník	František Letecký	Dopad vlivem regulace	3
Risk koordinátor	František Letecký	Dopad - finanční ztráta	1
Č/PR	František Letecký	Dopad do cílů	2
Riziková oblast	VŘKS	Pravděpodobnost - náročnost a komplexnost	2
Procesní oblast (Emonst)	Vzorová karta	Pravděpodobnost - četnost výskytu	1
Kategorie rizika (výběr z možností)	Operační / Nedostatek ve výkonu činnosti	Index rizika	2
Definice a popis rizika		Vzorové riziko	

KVANTIFIKACE		0		
Zdroje / příčiny nastoupení rizika		0		
Důsledky nastoupení rizika		0		
		Brutto	Netto	Rozdíl / Síla mitigace
Dopad (Kč)		0 Kč	0 Kč	0 Kč
Pravděpodobnost (%)		0,00%	0,00%	0,00%
Roční expozice		0 Kč	0 Kč	0 Kč
Základní hodnoty, komentář	0	0	0	0

ŘÍZENÍ		0			
Strategie řízení rizika		0			
Popis existujícího způsobu řízení rizika		0			
Typ mitigačního opatření	Podíl na mitigaci rizika (%)	Síla mitigace (Kč)	Náklady na MO (%)	Náklady na MO (Kč)	
Přenesení na externí subjekt	0%	0,00 Kč		0	
Operativní kontrola	0%	0,00 Kč		0	
Monitoring KR	0%	0,00 Kč		0	
Technickoorganizační opatření	0%	0,00 Kč		0	
Institucionální (Safety, Quality, EMS, CMP...)	0%	0,00 Kč		0	
Ostatní	0%	0,00 Kč		0	
	Přímý vplyv	Nepřímý vplyv	Celkový vplyv		
Předpokládaný vývoj rizika	0	0	0 Kč		

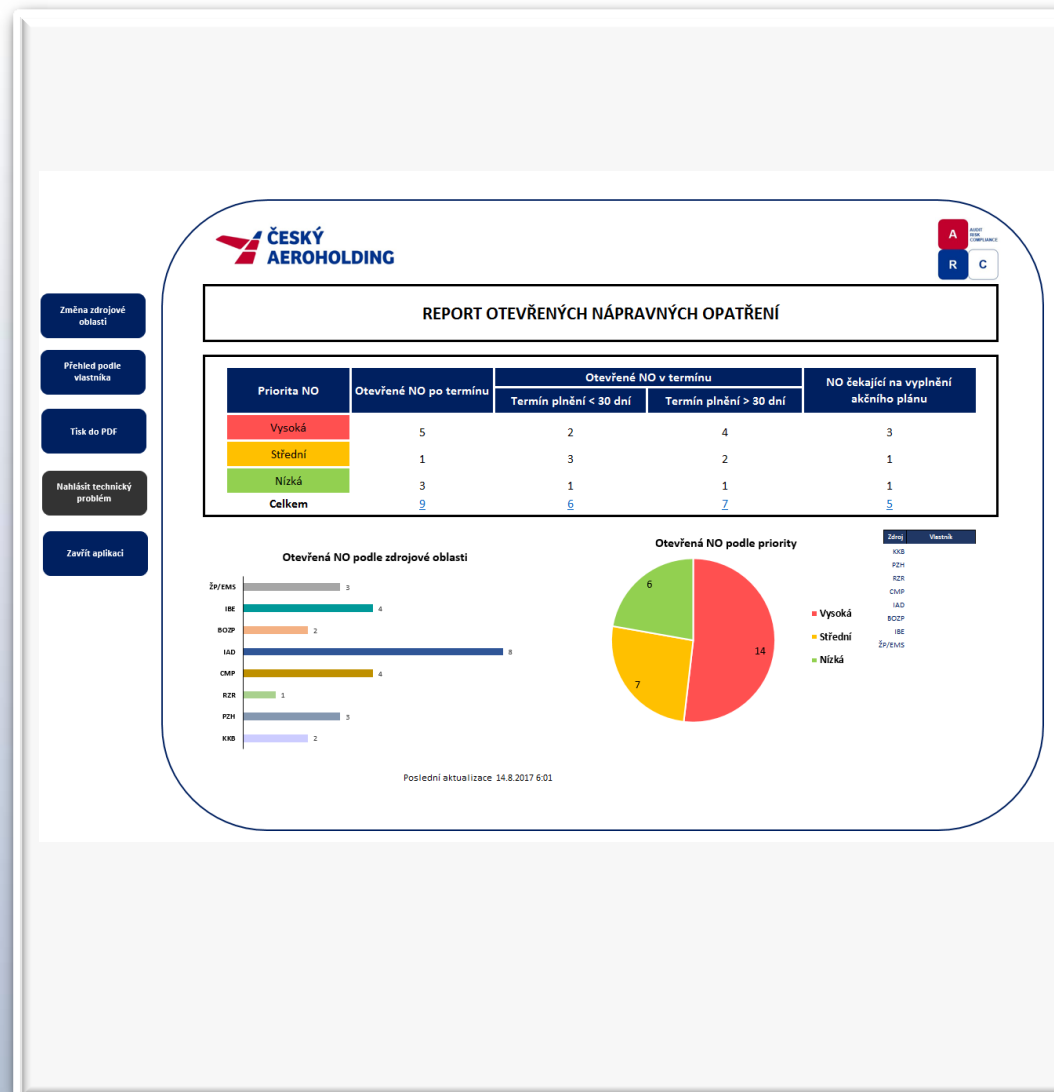
MO - Mitigační opatření (síla řízení rizika)			
Počet MO	Pokrytí rizika MO (síla mitigace v %)	Pokrytí rizika MO (síla mitigace v Kč)	Nákladovost (%)   Náklady na MO (Kč)
0	0,00%	0 Kč	0,00%
MK - Manažerské kontroly (dohled nad řízením rizika)			
Počet MK	Pokrytí počtu MO (síla mitigace v %)	Pokrytí síly mitigace MK (Kč)	Nepokrytí síly mitigace MK (%)   Kč
0	0%	0 Kč	0,00%
Hodnocení manažerských kontrol			
	Vlastníkem (počet)	SRR (počet)	
Efektivní (dosahující pokrytí MO manažerskou kontrolou)	0	0	
Inefektivní (prováděná a neefektivní (nedosahující pokrytí MO manažerskou kontrolou))	0	0	

## „One-page“ reporting NO

- ➔ Vlastník NO má dostupný komplexní report všech otevřených NO v jeho odpovědnosti bez ohledu na útvar, který je vydal
- ➔ Vedení společnosti či jeho člen má k dispozici report umožňující flexibilně vybrat a zobrazit NO
  - po vybraných kontrolních útvarech (např. IA, Compliance, Informační bezpečnost, BOZP, Životní prostředí atd.)
  - po vybraných vlastnících NO

INOVACE

Přehledný report A4, zobrazující stejnou formou všechna NO z různých zdrojů, dostupný kdykoliv, reagující flexibilně na uživatele, který si jej generuje.





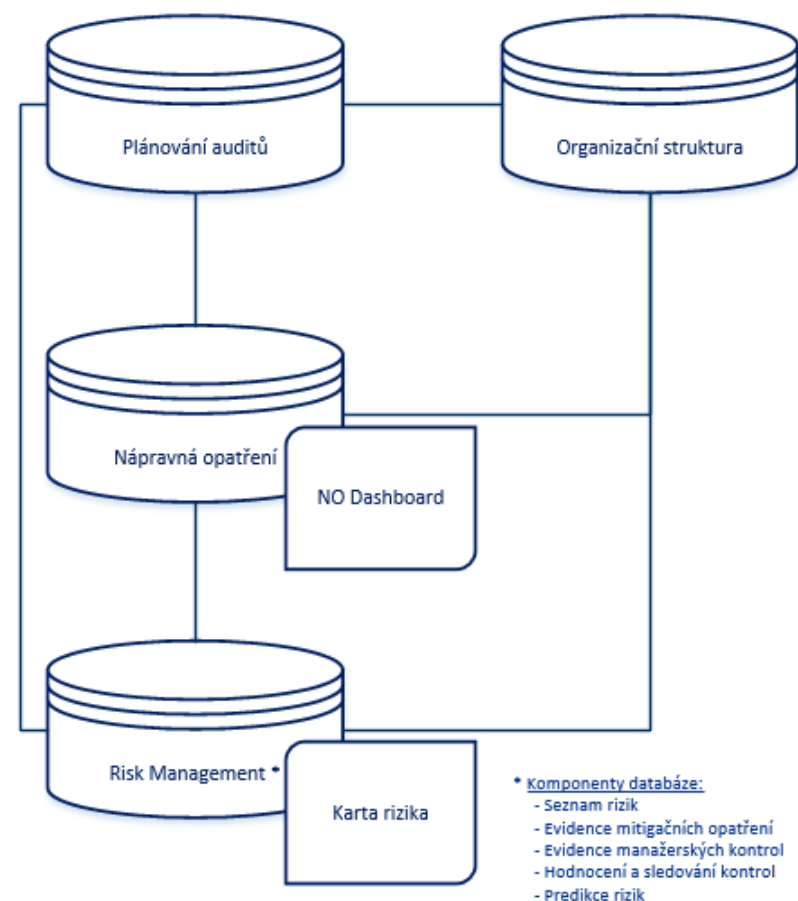
## Systemová integrace

### ⇒ Integrovaný informační systém

- ❑ Implementace jednotného systému pro hodnocení rizik a výstupů auditů/šetření pro všechny útvary společnosti
- ❑ Aktualizace relevantních údajů v systému po ukončení auditu/šetření, realizaci investiční akce, implementaci opatření s dopadem na mitigaci rizika

**INOVACE**

Sdílení informací související s rizikem z různých útvarů ve sdíleném informačním systému.



## Přínosy

### ➔ Přínosy pro vedení společnosti

- Včasná reakce na existující hrozby díky kontinuálně aktualizovaným informacím
- Komplexnost a přehlednost informací
- Podpora pro rozhodování (srovnatelnost investic, podpora plánování)
- Úspora nákladů a administrativy (sdílené zdroje, IS, jednotný reporting)

### ➔ Přínosy pro vlastníky procesů a rizik

- Komplexní pohled na rizika vlastních procesů a možnost porovnání s riziky z různých zdrojů
- Dostupnost porovnání vlastních rizik se srovnatelnými riziky ve společnosti
- „User friendly“ proces
  - Jednotný proces řízení rizik a NO
  - Snížení administrativy

## Realizace

### ➔ Projekt byl realizován v následujících fázích:

1. Vybudování nutného prostředí společnosti
  - Sjednocení metodik řízení rizik a výstupů klíčových útvarů kontrolního prostředí
  - Ustanovení týmu řízení rizik, následné vybudování komunity vlastníků rizik, jejich koordinátorů a tvorba povědomí o rizicích
  - Postupná implementace integrovaného IS (SharePoint) pro relevantní útvary
2. Vytvoření jednoho seznamu významných rizik pro společnost (sběr rizik a jejich konsolidace s existujícími seznamy)
3. Zajištění dynamické aktualizace dat systému jejich napojením na „živé“ procesy společnosti (investice, NO, auditní a kontrolní výstupy atd.)
4. Postupný vznik reportingu vedení společnosti