

Metodický pokyn CHJ č. 2



Centrální harmonizační jednotka  
Ministerstvo financí ČR

# Metodika řízení rizik ve veřejné správě

Verze 1.0

Vydáno dne 4. dubna 2016

# 1 Obsah

1	Obsah.....	2
2	Cíle metodiky .....	3
3	Slovníček.....	3
4	Organizační zajištění řízení rizik organizace.....	4
4.1	Centralizovaný model řízení rizik.....	4
4.2	Decentralizovaný model řízení rizik.....	5
4.3	Obecné předpoklady funkčního řízení rizik v organizaci veřejné správy.....	6
5	Věcný pohled na řízení rizik organizace .....	6
6	Analýza rizik pro účely plánování kontrol a interního auditu .....	10

## 2 Cíle metodiky

Tato metodika je určena pro všechny organizace, které hospodaří s veřejnými prostředky.

Adresáty metodiky nejsou pouze pracovníci útvaru interního auditu, i když lze předpokládat, že právě jejich cestou lze informace obsažené v metodice zprostředkovat osobám, které by v rámci organizace měly rizika řídit nebo se na jejich řízení aktivně podílet. Zejména se jedná o vedoucí pracovníky v rámci řízení rizik vyplývajících z činnosti jim svěřených útvarů, ale i všechny další osoby, které v rámci organizace připravují podklady pro rozhodnutí těchto pracovníků, protože řízení rizik je integrální součástí každého přijímaného rozhodnutí.

Cílem metodiky není stanovit organizacím podrobný návod, co mají dělat, aby byla jejich rizika zaručeně dobře řízena nebo eliminován jejich negativní dopad, ale spíše konkrétně a prakticky vysvětlit, co to vlastně riziko je a jak by mělo jeho řízení probíhat, aby měl takový systém v praxi vůbec šanci fungovat a chod organizace pozitivně ovlivnit (resp. zamezit negativním dopadům).

Sekundárním cílem metodiky je jednoznačně deklarovat, že řízení rizik není a nemá být úkolem útvaru interního auditu nebo jednotlivých interních auditorů. Interní auditor, který se do systému řízení rizik aktivně zapojí nebo jej dokonce v organizaci vytváří a spravuje, ztrácí možnost vykonávat svou primární funkci, tedy podávat vedení organizace nezávislé ujištění o tom, že její řídicí a kontrolní systém (včetně řízení rizik) funguje. Organizace, která svého interního auditora pověří úkoly v rámci řízení rizik, se tím sama připravuje o interní zpětnou vazbu o tom, zda jeden z nejvýznamnějších prvků řízení organizace funguje nebo nikoliv. Výjimku z výše uvedeného tvoří pouze případ, kdy si útvar kontroly či interního auditu vytváří pro vlastní účely vlastní mapu rizik organizace, na základě které sestavuje plány kontrol či interních auditů. Tento proces by však měl být od samotného řízení rizik organizace, které má v praxi vykonávat vedení organizace, oddělen.

Cílem této metodiky naopak není podat či opakovat teoretický výklad problematiky řízení rizik, která je ve své teoretické rovině společná pro veřejnou správu i firemní prostředí a je zcela dostatečným způsobem zpracována v české odborné literatuře. Pro podrobné teoretické vymezení strategie a hlavních zásad řízení rizik, jednotlivých procesů (či fází) řízení rizik, organizace a metodologie řízení rizik a dalších souvisejících oblastí lze v případě hlubšího zájmu využít některou z běžně dostupných publikací, např. Vladimír Smejkal, Karel Rais: Řízení rizik ve firmách a jiných organizacích nebo Doležal Jan, Máchal Pavel, Lacko Branislav a kolektiv: Projektový management podle IPMA.

## 3 Slovníček

**Riziko** – potenciální událost v budoucnosti s negativními následky. Riziko tedy může a nemusí nastat.

Určitá rizika jsou spojená s každou činností, v chodu každé organizace proto rizika vždy byla, jsou a budou přítomna. Cílem proto není všechna rizika eliminovat, ale být si jich vědom a pracovat s nimi (tj. řídit je).

**Řízení rizik** – integrální součást každého rozhodování v organizaci. Soustavná činnost, jejímž cílem je omezit pravděpodobnost výskytu rizik nebo snížit jejich dopad. Účelem řízení rizik je předejít problémům či negativním jevům, tj. zamezit vzniku problémů a vyhnout se tím nutnosti krizového řízení.

**Významnost rizika** – relativní důležitost rizika pro organizaci, která je zpravidla vyjádřena součinem pravděpodobnosti rizika a dopadu rizika.

**Pravděpodobnost rizika** – míra pravděpodobnosti výskytu rizikové události v budoucnosti měřená dle převažující praxe na škále 1-5 (1 nejméně pravděpodobné, 5 nejvíce pravděpodobné).

**Dopad rizika** – rozsah negativního dopadu či ztráty, která organizaci vznikne v případě výskytu rizikové události. Lze do něj zahrnout jak přímé finanční ztráty či dodatečné náklady, tak i dopady nefinančního

charakteru, např. ztrátu dobré pověsti, snížení kvality služeb pro občany atd.). Dopad rizika se dle převažující praxe opět měří na škále 1-5 (1 nejmenší negativní dopad, 5 největší negativní dopad).

**Mapa rizik** – výsledek analýzy rizik; přehled identifikovaných rizik organizace / programu seřazených podle jejich významnosti, který slouží jako jeden z podkladů pro sestavování plánu interních auditů a plánu kontrol. Pro účely sestavování plánu interních auditů a plánu kontrol si útvar kontroly a útvar interního auditu vytváří vlastní mapu rizik organizace / programu – tyto mapy rizik neslouží a nemají sloužit pro účely řízení rizik organizace jejím vedením, ale pro účely plánování kontrol a interních auditů.

**Vrcholové vedení organizace** – 1. a 2. stupeň řízení organizace (v případě ministerstev ministr, státní tajemník a náměstci, v případě ostatních ústředních správních úřadů ředitel a náměstci, v případě krajských úřadů ředitel, tajemník úřadu a ředitelé/vedoucí klíčových odborů, např. ekonomického či finančního odboru, odboru informatiky); u menších úřadů je bezpředmětné jejich vedení rozlišovat na vrcholové a ostatní.

**Vedoucích pracovníků na ostatních úrovních řízení** – ostatní vedoucí pracovníci na nižších stupních řízení organizace (v případě ministerstev a ostatních ústředních správních úřadů ředitelé odborů, vedoucí samostatných oddělení a vedoucí oddělení, v případě krajských úřadů vedoucí oddělení).

## 4 Organizační zajištění řízení rizik organizace

### 4.1 Centralizovaný model řízení rizik

#### Stručný popis

Řízení rizik organizace má na starosti Výbor pro řízení rizik složený z vrcholového vedení organizace. Ke koordinaci činností v oblasti řízení rizik napříč organizací a přípravě podkladů pro jednání a rozhodování Výboru pro řízení rizik je pověřen jeden ze zaměstnanců organizace (tajemník výboru pro řízení rizik / koordinátor řízení rizik / manažer rizik).

#### Předpoklady

Pracovník, který má v organizaci na starosti koordinaci řízení rizik musí mít dostatek znalostí, zkušeností, kompetencí a důvěry ze strany vrcholového vedení organizace i vedoucích pracovníků na ostatních úrovních řízení, aby byl schopen zajistit:

- Aktivní a otevřenou komunikaci s členy Výboru pro řízení rizik
- Přípravu úplných a pravdivých podkladů (ve spolupráci s vedoucími pracovníky na všech úrovních řízení a odbornými útvary) včetně zahrnutí negativních informací a možných dopadů souvisejících s danou operací, které jsou pro rozhodování o dalším postupu relevantní
- Předkládání těchto podkladů Výboru pro řízení rizik a aktivní účast při jejich projednávání

Členové Výboru pro řízení rizik musí být ochotni a schopni existenci rizik u operací ve své gesci akceptovat, nesnažit se je marginalizovat a dále s nimi pracovat, a to nikoliv pouze individuálně, ale i před ostatními členy vrcholového vedení organizace.

#### Výhody

Umožňuje organizaci klást důraz na řízení rizik v podobě samostatných aktivit zaměřených na zjišťování, vyhodnocování, monitorování a vykazování významných rizik v organizaci. Při správném provádění dává vrcholovému vedení organizace přiměřenou jistotu, že klíčová rizika jsou vedoucími pracovníky na příslušných úrovních organizace opravdu důsledně řízena.

## Nevýhody

Mezi nejčastěji identifikované nedostatky řízení rizik ve veřejné správě patří sklon k formalismu, chápání mapy rizik či katalogu rizik organizace jako cíle aktivit v oblasti řízení rizik, nikoliv jako pouhého nástroje pro aktivní řízení rizik vedením organizace, a přílišný důraz na kvantifikaci významnosti rizik, nikoliv na další práci s nimi. Všechny tyto nedostatky zavedení centralizovaného modelu řízení rizik spíše přirozeně podporuje, než aby jim zamezovalo.

Jedná se proto o model v prostředí veřejné správy vhodný spíše jen pro ty organizace, které se skutečně pohybují v rizikovém prostředí a kde je proto fungování systému řízení rizik v podobě samostatných aktivit zaměřených na zjišťování, vyhodnocování, monitorování a vykazování významných rizik klíčové pro jejich úspěšné fungování (např. nemocnice, Energetický regulační úřad, Státní úřad pro jadernou bezpečnost, Státní úřad pro kontrolu léčiv apod.).

V ostatních organizacích, které se pohybují ve standardním prostředí veřejné správy, kde je nejhorším možným negativním dopadem špatného rozhodnutí finanční ztráta, dodatečné náklady či případné správní nebo soudní řízení, není tento model řízení rizik příliš účelný a v praxi mají tendenci se projevovat spíše jeho nevýhody.

## 4.2 Decentralizovaný model řízení rizik

### Stručný popis

Řízení rizik je integrální součástí každého rozhodnutí, které je v rámci organizace jejími vedoucími pracovníky přijímáno. Od určité hladiny významnosti přijímaného rozhodnutí musí mít řízení rizik svou dokumentovanou podobu, aby o něm v organizaci zůstávala auditní stopa. Hladinu významnosti si organizace určí sama ve svých vnitřních předpisech a může, resp. měla by být pro různé typy operací v různých oblastech různá (podle rizikovitosti operací daného typu v dané oblasti pro organizaci obecně<sup>1</sup>).

### Předpoklady fungování

Vedoucí pracovníci na všech úrovních řízení musí chápat, co je to riziko a jak se s ním pracuje a vědomě tyto znalosti uplatňovat v praxi při řízení jím svěřeného útvaru, vždy přiměřeně k operaci, o které rozhodují.

### Výhody

Eliminuje většinu nevýhod centralizovaného modelu řízení rizik. Nepředpokládá existenci centrálního koordinátora rizik, po kterém lze v prostředí veřejné správy přirozeně jen velmi obtížně požadovat takovou míru znalostí, zkušeností a kompetencí, aby byl v diskusi o řízení rizik rovnocenným partnerem vrcholovému vedení organizace.

### Nevýhody

Aby fungoval optimálně, vyžaduje aktivní účast všech vedoucích zaměstnanců na jednotlivých úrovních řízení.

Podmínkou dobrého fungování decentralizovaného modelu řízení rizik však není, aby byl uplatňován hned od prvního okamžiku dokonale plošně napříč celou organizační strukturou. Někde může fungovat lépe a někde hůře, záleží na konkrétních vedoucích pracovnících. Postupně lze napříč organizací sjednocovat formou přenášení dobré praxe z útvarů, kde funguje, na ty ostatní.

---

<sup>1</sup> Typickým příkladem mohou být např. veřejné zakázky zadávané v otevřeném výběrovém řízení versus veřejné zakázky zadávané formou jednacního řízení bez uveřejnění, výdajové operace v běžných provozních oblastech versus výdajové operace v oblasti zdravotnictví či IT apod.

**Proto lze většině organizací veřejné správy, které se pohybují ve standardním a ne příliš rizikovém prostředí, doporučit vydat se právě cestou decentralizovaného modelu řízení rizik.**

### 4.3 Obecné předpoklady funkčního řízení rizik v organizaci veřejné správy

Úspěšnost zavedení kteréhokoliv z výše uvedených modelů řízení rizik v praxi má několik obecně platných předpokladů, mezi které patří v rámci každé organizace veřejné správy zejména:

1. **Jednoznačná organizační struktura<sup>2</sup> a funkční organizační řád**, ve kterém jsou vymezeny přesně, srozumitelně a v souladu se skutečností odpovědnosti jednotlivých organizačních útvarů tak, aby se vzájemně nepřekrývaly a aby naopak nedocházelo k existenci agend či činností, ke kterým nemá odpovědnost stanovenou žádný z organizačních útvarů.
2. **Vhodně definované pracovní náplně** jednotlivých zaměstnanců, které jsou v souladu s organizačním řádem a zároveň odpovídají skutečně vykonávaným agendám a činnostem.
3. **Jasně, srozumitelně a konkrétně formulovaný etický kodex organizace** schválený a podporovaný jejím vrcholným vedením, nejlépe doplněný o proškolení zaměstnanců v této oblasti.
4. **Jasně stanovená pravidla v klíčových oblastech vnitřního chodu organizace, která jsou ve vzájemném souladu** (zejména směrnice o oběhu účetních dokladů; schvalovací postupy a oprávnění; jednací řády poradních a rozhodovacích orgánů; plány, postupy a oprávnění při provádění kontroly; statut, manuál a plány interního auditu).

Jedná se o základní stavební kameny každé organizace, o které se následně může opřít jakýkoliv řídicí a kontrolní mechanismus včetně řízení rizik. Pokud některý z těchto stavebních kamenů chybí nebo je zaveden pouze formálně, opora logicky chybí a nelze na ní proto postavit zcela funkční nastavbu.

## 5 Věcný pohled na řízení rizik organizace

Základním předpokladem řízení každého jednotlivého rizika je schopnost organizace takové riziko identifikovat (uvědomit si, že existuje) a přiměřeně označit či definovat (nikoliv nutně nějak formalizovaně či písemně).

Riziko vždy souvisí s určitou konkrétní operací, na jejíž realizaci se váže. Mělo by být proto vždy formulováno konkrétně a ve vazbě na rozhodování o dané operaci, které se týká. Příliš obecně definované riziko či riziko bez jasně identifikované vazby na nějakou konkrétní operaci či rozhodnutí účinně řídit nelze.<sup>3</sup>

#### Příklady nesprávně formulovaných rizik (příliš obecné):

- Riziko finanční a rozpočtové; příklady vybraných rizikových oblastí/zdrojů:
  - Plánování a rozpočtování
  - Financování

---

<sup>2</sup> Jednoznačná organizační struktura se dá v praxi poznat jednoduše tak, že ji lze nakreslit ve formě organizačního schématu, aniž by vznikly pochybnosti o tom, která řídící linie kam vede nebo aniž by vedlo více těchto řídících linií paralelně.

<sup>3</sup> Dobře formulované riziko se dá v praxi poznat jednoduše tak, že k němu dokážeme definovat konkrétní nápravné opatření (ať již bude nakonec v praxi fungovat či nikoliv). Ke špatně formulovanému riziku konkrétní nápravné opatření ani teoreticky definovat nedokážeme.

- Účetní evidence
- Činnosti pokladní služby
- Čerpání prostředků EU
- Správa a řízení finančních toků
- Inventarizace
- Nepřiměřené náklady
- Správa a ochrana majetku
- Riziko informační a technologické; příklady vybraných rizikových oblastí/zdrojů:
  - Přístupová práva
  - Integrita systémů
  - Fyzické zabezpečení dat a jejich ochrana
  - Dostupnost informačních systémů
  - Spolehlivost informačních systémů
  - Nákup a správa výpočetní techniky
  - Požadavky na HW a jejich hodnocení
  - Programové vybavení
  - Odborné informace
  - Správa síťových aplikací
  - Licenční čistota z hlediska autorských práv
  - Integrita aplikačních systémů

Ve výše uvedených případech se nejedná o formulaci rizik, pouze o výčet možných rizikových oblastí, do kterých lze konkrétní identifikovaná rizika případně třídit a kategorizovat. Konkrétní identifikovaná rizika však již v daném výčtu nenásledují.

**Příklady nesprávně formulovaných rizik (bez vazby na konkrétní operaci či rozhodnutí):**

- Riziko korupční
  - Nestabilita a složitost právních norem, různé iniciativy, lobbying
  - Únik informací nebo jejich neoprávněné poskytnutí
  - Úmyslně zkreslené či zamlčené informace, které mohou neobjektivně ovlivnit rozhodování vedení
  - Zneužití postavení, které je spojeno s porušením principu nestrannosti při rozhodování
  - Ovlivňování plánu a výsledků kontrol
  - Riziko svévolného zvýhodnění jednoho dodavatele oproti ostatním
  - Snaha o získání prospěchu nebo snaha o zneužití prostředků při jejich převodech
  - Nebezpečí potencionálních škod v důsledku nedodržení obecně platných a vnitřních předpisů, zneužití pravomocí, příp. střet zájmů
- Riziko finanční a rozpočtové

- Možnost porušení rozpočtové kázně z důvodu nesouladu legislativy v oblasti účetnictví, daňového zákona, rozpočtových pravidel, stavebního zákona apod.
- Nepozornost při dodržování postupu v rámci stanovené metodické činnosti
- Nevhodně nastavená strategie, která může přinést finanční ztráty a snížení hodnoty svěřených portfolií a ohrožit realizaci rozpočtových priorit
- Nezajištění dostatečné likvidity
- Vystavení souhlasu na základě chybného vyhodnocení
- Špatně připravené podklady
- Porušení postupů podle správního řádu

Ve výše uvedených případech se jedná o reálné a opakující se zkušenosti daných zaměstnanců z praxe, které pro organizaci skutečně znamenají významná rizika. Pokud jsou však rizika formulována takto obecně a bez vztahu ke konkrétní operaci či rozhodnutí, nelze k nim definovat jakékoliv konkrétní nápravná opatření. Ačkoliv si zaměstnanci organizace dali při identifikaci těchto negativních jevů jistě značnou práci, jejich čas pravděpodobně vyjde do značné míry vniveč, neboť takto formulovaná rizika objektivně nelze řídit.

Takto formulovaná rizika lze poměrně dobře využít nikoliv pro samotné řízení rizik, ale pro zpracování mapy rizik organizace pro účely plánování kontrol a interních auditů. Otázkou každé organizace však je, do jaké míry chce věcnou a časovou zátěž spojenou s identifikací rizik pro účely zpracování plánů kontrol a interních auditů takto plošně přenášet na všechny své zaměstnance (tj. nakolik je takový přístup účelný, hospodárný a efektivní). Ve kterých procesech leží klíčová rizika dané organizace, je každý interní auditor či kontrolor se znalostí fungování dané organizace schopen určit poměrně velmi přesně i bez takového plošného cvičení.

#### **Příklady správně formulovaných rizika (rizika zavedení centrálního nákupu státu a navrhovaná opatření k jejich řízení<sup>4</sup>):**

- Riziko monopolizace dodávek pro stát největšími dodavateli na trhu (potenciál pro zlepšení jejich tržní pozice vedoucí k následnému zvýšení tlaku na ceny)

Agregace všech požadavků do jednoho zadávacího řízení, jehož výsledkem by byla smlouva s jedním dodavatelem, by vedla ke značné monopolizaci dodávek pro stát se všemi souvisejícími riziky (možné výpadky dodávek, tlak na zvyšování ceny klíčovým dodavatelem v budoucnu).

Za účelem zachování tržní konkurence a nediskriminačních podmínek pro menší dodavatele je i v případě společné nadresortní veřejné zakázky potřeba rozdělit tuto zakázku na menší části (podle územního členění odběratelů nebo věcných částí plnění).

- Velmi vysoká administrativní náročnost všech fází přípravy a realizace zadávacího řízení v případě nedostatečné IT podpory procesu

Při daném množství zapojených subjektů je bez další technické podpory velmi obtížné organizačně zajistit informace nezbytné pro řádné plnění uveřejňovacích povinností centrálního zadavatele (sledování výše čerpání z jednotlivých rámcových smluv, zajištění nepřekročení sjednaného rámce).

---

<sup>4</sup> Usnesení vlády č. 913/2015 k Informaci o stavu příprav centrálního nákupu státu a k návrhu Rámcového harmonogramu centrálního nákupu státu pro roky 2016-2020, dostupné online na: <http://www.mfcr.cz/cs/verejny-sektor/smart-governance/centralni-nakup-statu/pravidla-cns/usneseni-vlady-c-913-2015>



Zároveň není aktuálně možné pro přípravu zadání využít stávajících IT nástrojů resortů pro elektronické zadávání (zejména pro sběr a agregaci požadavků a následnou realizaci společné veřejné zakázky např. ve formě dynamického nákupního systému), neboť jednotlivými resorty jsou pro elektronické zadávání využívány rozdílné IT nástroje.

Toto riziko je možné eliminovat centralizací IT podpory zadávacích postupů využívané zapojenými veřejnými zadavateli do Národního elektronického nástroje.

- Nutnost dvoustupňového přístupu k organizaci zadávacího řízení, kterou však zákon o veřejných zakázkách nepředpokládá

Příprava veřejné zakázky je organizačně a administrativně realizovatelná pouze za předpokladu, že se jí účastní zástupci jednotlivých resortů, kteří informace přenášejí dále k organizacím v rámci svých resortů a naopak v rámci svých resortů sbírají a agregují za všechny zapojené organizace potřebná data, informace a připomínky (tzv. dvoustupňový přístup). Naopak přímá účast všech zapojených zadavatelů na přípravě veřejné zakázky je po organizační a administrativní stránce představitelná pouze velmi obtížně. Dvoustupňová forma organizace centrálního nákupu (centrální zadavatel – ministerstvo – resortní organizace) však není stávající právní úpravou zadávání veřejných zakázek předpokládána a legislativně upravena.

Bude proto časově i právně náročné vše správně vymezit v rámci smluv o centralizovaném zadávání uzavřených mezi zapojenými resorty (jejich uzavření muselo předcházet uzavření pověřovacích smluv mezi příslušným ministerstvem a resortními organizacemi v rámci jednotlivých zapojených resortů). Tím se však toto riziko eliminuje.

Při rozhodování o riziku je potřeba mít na paměti zejména relativní význam daného rizika pro organizaci. Tomuto ukazateli se obecně říká **významnost rizika** a stanovuje se jako **součin pravděpodobnosti rizika a dopadu rizika, jež se v praxi nejčastěji měří na škále 1-5** (blíže viz Slovníček):

DOPAD	5	S	V	V	V	V
	4	S	S	V	V	V
	3	N	N	S	S	V
	2	N	N	N	N	S
	1	N	N	N	N	N
		1	2	3	4	5
		PRAVDĚPODOBNOST				

V = vysoké riziko  
S = střední riziko  
N = nízké riziko

Při rozhodování o dalším postupu při řízení daného rizika je však nutné zohlednit<sup>5</sup> rovněž další dva faktory, kterými jsou:

- **Schopnost dané riziko řídit** (tj. ovlivnit jeho další vývoj), a to nikoliv pouze já osobně jako jedinec, ale já jako součást dané organizace prostřednictvím všech kroků a nástrojů, které mám jako součást této organizace k dispozici (mohu např. požádat někoho dalšího o součinnost, informovat nadřízené atd.)
- **Náklady spojené s řízením rizika** – cílem jednoznačně je, aby náklady na řízení rizika nepřevyšovaly úspory plynoucí z jeho eliminace

<sup>5</sup> Tyto faktory není nutné nijak přehnaně formalizovaně vyčíslovat či škálovat, stačí je pouze přiměřeně zohlednit v úvaze o dalším postupu při řízení daného rizika.

K řízení rizika lze následně zvolit některý z následujících přístupů:

- **Vyvarování se rizika** (např. neschválení dané operace, zákaz vykonání rizikové aktivity nebo procesu; organizace si však musí dát pozor, zda takovým opatřením nevznikají rizika jiná, která mohou být ještě významnější)
- **Udržování rizika na stávající míře významnosti** (akceptace rizika a sledování jeho vývoje bez dalších opatření k jeho eliminaci; k těm by případně došlo, až pokud by se kriticky zvýšila významnost rizika)
- **Redukce rizika** – přijetí nápravných opatření vedoucích ke snížení pravděpodobnosti výskytu rizika nebo jeho dopadu na přijatelnou mez
- **Přenos / sdílení rizika s někým dalším** – snížení případného negativního dopadu tím, že je částečně přenesen na další osoby (např. na dodavatele v rámci smluvního vztahu, pojištěním rizika apod.; za takovou službu se však zpravidla vždy platí a organizace by si měla dobře spočítat, zda se jí takový postup skutečně vyplatí nebo nikoliv)

Organizace by se měla prostřednictvím svých vedoucích pracovníků soustředit primárně na řízení rizik s vysokou, příp. střední mírou významnosti. U rizik s nízkou mírou významnosti lze doporučit taktiku udržování rizika. Každé riziko by mělo být řízeno subsidiárně na té úrovni řízení, která je k tomu vybavena potřebnými znalostmi a kompetencemi. V opačném případě je potřeba riziko dobře popsat, pokusit se definovat vhodná nápravná opatření a včas jej předat na vyšší úroveň řízení.

Optimálním a přirozeným nosičem takových informací v organizaci je referátník, podklady pro poradu vedení organizace, podklady připravované ke schválení veřejné zakázky, studie proveditelnosti, investiční záměr atd. Pro účely řízení rizik rozhodně není nutné vytvářet nové samostatné dokumenty, stačí úplně a v maximální možné míře objektivní informace o rizicích v přehledné podobě (nejlépe včetně návrhu souvisejících opatření k řízení rizik) zahrnout do podkladů, na základě kterých příslušná osoba či orgán o té které operaci rozhoduje.

## 6 Analýza rizik pro účely plánování kontrol a interního auditu

Jak již bylo uvedeno výše, zcela samostatnou disciplínou v oblasti řízení rizik je analýza rizik pro účely plánování kontrol a interních auditů. Za tímto účelem by měly útvary kontroly a útvary interního auditu každoročně připravit / aktualizovat přehled identifikovaných rizik organizace seřazených podle jejich významnosti, tedy mapu rizik dané organizace. Obecné zásady spojené s kategorizací rizik podle jejich významnosti pro organizaci přitom platí stejně. Zároveň však platí následující základní odlišnosti:

- Při analýze rizik pro účely plánování kontrol a interního auditu se nezohledňují ostatní faktory uvedené v kapitole 5 Věcný pohled na řízení rizik organizace (schopnost organizace dané riziko řídit a náklady spojené s řízením rizika). Vychází se čistě z mapy rizik, která obsahuje přehled všech identifikovaných rizik organizace či programu seřazených podle jejich významnosti.
- Záleží na dané organizaci, zda do identifikace rizik a hodnocení jejich významnosti zapojí všechny zaměstnance dané organizace či zda si mapu rizik zpracuje tento útvar sám vlastními silami na základě svých znalostí a zkušeností o fungování dané organizace a rizikovitosti jednotlivých procesů. Obecně lze doporučit spíše druhý postup, který je efektivnější, účelnější a přináší výsledky na základě odborného posouzení k tomu kompetentních osob, nikoliv pouze souhrn pozorování jednotlivých zaměstnanců organizace, kteří nejsou a ani nemohou být na identifikaci, formulaci a analýzu rizik žádnými odborníky.

Samotný výběr vzorku pro realizaci kontrol a interních auditů je samostatné téma, které přesahuje zaměření této metodiky a bude mu proto v metodické činnosti CHJ věnována samostatná pozornost.