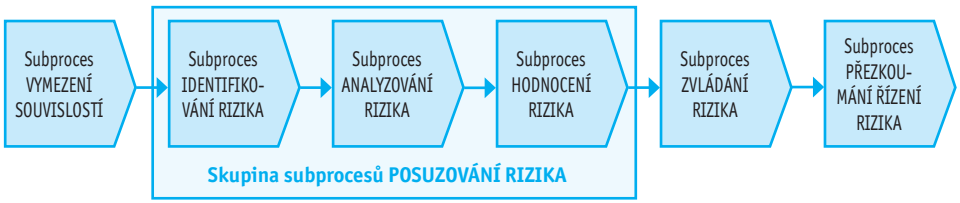
Kapitán Ing. David Řehák, Ph.D., Ing. Monika Grasseová, Ph.D.

Vymezení souvislostí jako součást procesu řízení rizik u organizací ústřední státní správy

Pokud se na organizaci díváme jako na systém vzájemně provázaných a vzájemně souvisejících procesů, [1] pak každý proces má v tomto systému svoji úlohu (účel, cíl). Z hlediska účelu můžeme procesy dělit na hlavní, to jsou ty, které zabezpečují, že organizace poskytuje služby, které jsou smyslem její existence, zabezpečují nám tedy plnění poslání. [2]

Proto, abychom zabezpečili kvalitní plnění poskytovaných služeb, máme procesy řídící (např. plánování, kontrolní procesy). Pro zabezpečení chodu organizace pak máme procesy podpůrné. Jedním z těchto procesů je také proces řízení rizika, [3] který slouží pro včasné rozpoznání, posouzení a následné zvládání rizika a jehož účelem (cílem) je předcházení možným nežádoucím dopadům na aktiva [4] organizace. Realizace tohoto procesu je jedním z velice důležitých předpokladů pro úspěšné plnění poslání a cílů nejen organizací ústřední státní správy.

Z procesního hlediska je tedy možné *řízení rizik* [risk management] charakterizovat jako proces řídící, který se skládá z jednotlivých na sebe navazujících subprocesů (obr. 1).



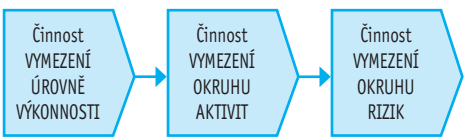
Zdroj: Upraveno dle ISO/IEC Guide 73. *Risk management – Vocabulary*, 2002.

Obr. 1: Průběh procesu řízení rizika

Výchozím a velmi významným subprocesem procesu řízení rizik je *vymezení souvislostí* [establishing the context], které by mělo být managementem organizace provedeno před navazujícím subprocesem identifikace rizik. [5] Zde je ovšem nutno podotknout, že většina odborných publikací [6] nepopisuje problematiku vymezení souvislostí v rámci procesu řízení rizik s patřičnou podrobností a jako výchozí subproces (fázi) tohoto procesu zpravidla považuje identifikaci rizik, případně analýzu rizik (některé publikace [7] nebo normy [8] považují identifikaci rizik jako součást analýzy rizik).

Je však nezbytné upozornit, že pokud nejsou managementem organizace vymezeny souvislosti rizik, je jejich následná identifikace velmi obtížná a mnohdy může být neúplná či zavádějící. Při realizaci subprocesu vymezení souvislostí je nezbytné provést tyto konkrétní činnosti (obr. 2):

- vymezení úrovně výkonnosti,
- vymezení okruhu aktiv,
- vymezení okruhu rizik. [9]



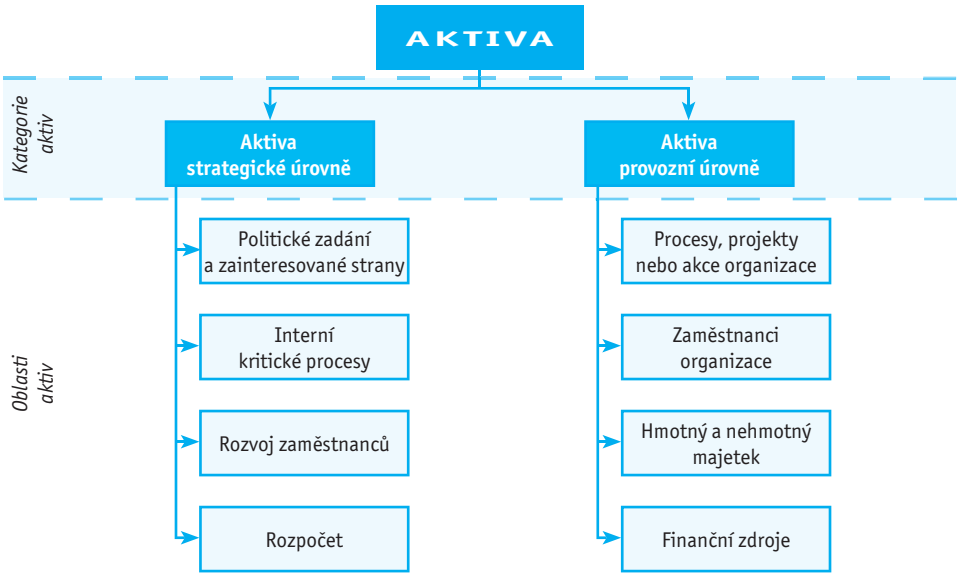
Obr. 2: Průběh subprocesu vymezení souvislostí

Vymezení úrovně výkonnosti

Rizika mohou být u organizací státní správy řízena ve dvou výkonnostních úrovních, a to na úrovni strategické, zde jsou rizika řízena u strategických cílů [10] organizace, a na úrovni provozní, zde jsou rizika řízena u cílů procesů, projektů nebo akcí. Výsledkem této činnosti je určení, zda se budeme zabývat úrovní výkonnosti strategickou nebo provozní.

Vymezení okruhu aktiv

Výsledkem této činnosti je výběr oblasti (případně oblastí) aktiv pro zvolenou úroveň výkonnosti, které budou dále posuzovány. Pro provedení činnosti vymezení okruhu aktiv je možné využít doporučené členění aktiv na jednotlivé kategorie (obr. 3).



Obr. 3: Doporučené členění aktiv do kategorií a oblastí

Rizika mohou u organizací státní správy působit na aktiva ve dvou výkonnostních úrovních. V případě, že byla v předchozí činnosti zvolena úroveň strategická, budeme se dále zabývat kategorií *aktiv strategické úrovně*, přičemž jako aktiva této úrovně budeme chápat organizací definované strategické cíle. Pro členění aktiv této kategorie do oblastí můžeme využít metodu **balanced scorecard (BSC).** [11] Při využití této metody lze jako oblasti aktiv charakterizovat jednotlivé perspektivy BSC, kterými jsou u organizací ústřední státní správy:

- politické zadání a zainteresované strany [12] (jakou politickou zakázku nebo požadavky zainteresovaných stran musíme splnit?),
- interní kritické procesy (které procesy jsou pro nás kritické, respektive klíčové, abychom úspěšně prosadili a dosáhli strategie?),
- rozvoj zaměstnanců (jak dosáhneme schopnosti ke změnám a zlepšování, abychom realizovali strategii?),
- rozpočet (jaký musí být rozpočet, aby byla naše strategie úspěšně realizována?).

V případě rezortu obrany bychom BSC mohli rozšířit o další perspektivu, a to operační schopnosti (jakých operačních schopností jednotlivých druhů ozbrojených sil chceme dosáhnout?).

Pokud byla vymezena úroveň provozní, budeme se dále zabývat kategorií *aktiv provozní úrovně*. U této kategorie lze jako oblasti aktiv u organizací ústřední státní správy charakterizovat:

- Procesy, projekty nebo akce organizace (u tohoto okruhu aktiv nám rizika mohou působit např. na kvalitu výstupů, efektivnost, [13] včasnost, náklady).
- Zaměstnanci organizace (u tohoto okruhu aktiv nám rizika mohou působit např. na jejich zdraví, znalosti či dovednosti).
- Hmotný a nehmotný majetek [14] (u tohoto okruhu aktiv nám rizika mohou působit zpravidla na jejich hodnotu).
- Finanční zdroje (u tohoto okruhu aktiv nám rizika mohou působit zpravidla na jejich hodnotu).

Vymezení okruhu rizik

Výsledkem této činnosti je výběr skupiny (skupin) rizik, které budou dále posuzovány. Pro provedení činnosti vymezení okruhu rizik je možné využít následující členění rizik na kategorie, oblasti a skupiny. Rizika je možno, z hlediska působení zdrojů rizik [15] na organizaci, klasifikovat do dvou kategorií. První kategorii představují *vnější rizika*. Jedná se o rizika neovlivnitelná, proto u této kategorie můžeme tlumit pouze důsledky jejich působení. Vnější rizika je možno členit do šesti oblastí, a to na rizika politická, ekonomická, sociální neboli společenská, technologická, legislativní a ekologická.

Toto členění je provedeno podle faktorů PESTLE analýzy, [16] která slouží pro analýzu vnějšího prostředí. Vedle oblastí rizik vyplývajících z faktorů PESTLE analýzy navrhujeme do kategorie vnějších rizik zahrnout i oblast bezpečnostních rizik.

Druhou kategorií jsou *vnitřní rizika*. Jedná se o rizika ovlivnitelná, jelikož u této kategorie lze příčiny jejich působení minimalizovat či eliminovat. Kategorii vnitřních rizik je možno dále členit do tří oblastí, a to na rizika procesní (projektová), personální a věcná. Členění rizik do kategorií a oblastí je znázorněno na obr. 4.

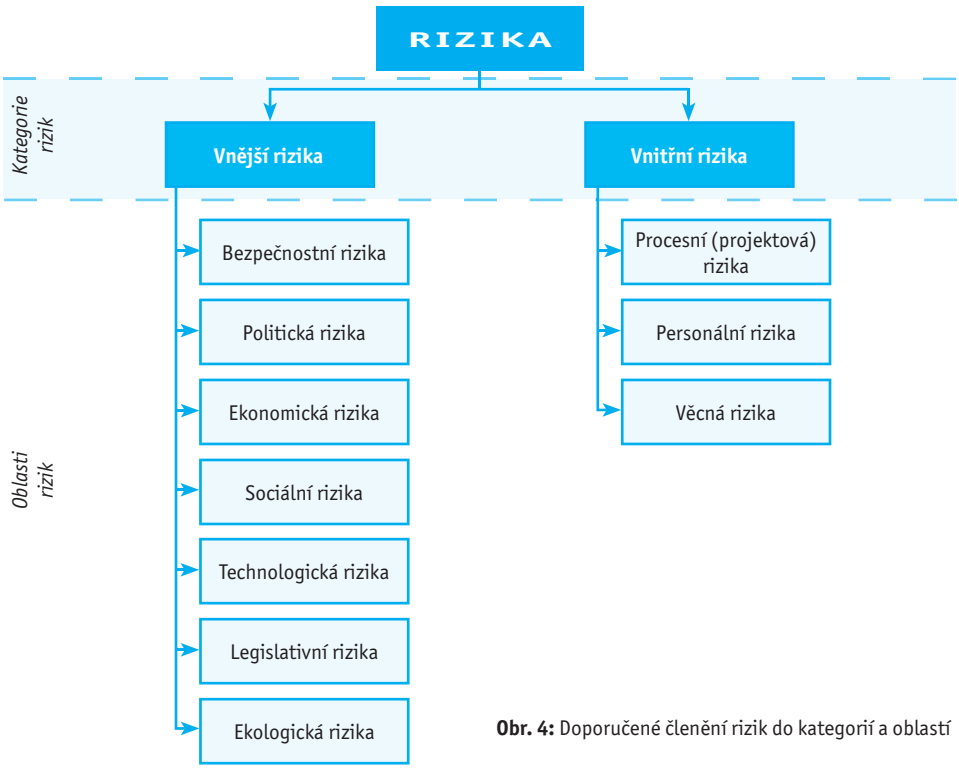
U organizací ústřední státní správy můžeme výše uvedené oblasti vnějších rizik dále na nižší rozlišovací úrovni členit do skupin.

Do oblasti **bezpečnostních rizik** můžeme zahrnout např. skupiny rizik:

- válečná rizika (vojenská rizika),
- režimní rizika (terorismus, extremismus, separatismus),
- kriminální rizika (obchod se zbraněmi, organizovaný zločin),
- proliferační rizika (šíření zbraní hromadného ničení),
- informační rizika (napadení a zneužití kritických informací a systémů informačních technologií).

Do oblasti **politických rizik** můžeme zahrnout např. skupiny rizik:

- intervenční rizika,
- rizika spojená se změnou státního zřízení,
- rizika spojená se změnou vlády,
- rizika spojená s občanskými iniciativami.



Obr. 4: Doporučené členění rizik do kategorií a oblastí

Do oblasti **ekonomických rizik** [17] můžeme zahrnout např. skupiny rizik:
- rozpočtová rizika,
- inflační rizika,
- kurzová rizika,
- rizika správy finančních prostředků (např. kolaps bankovních institucí).

Do oblasti **sociálních rizik** můžeme zahrnout např. skupiny rizik:
- demografická rizika (přelidňování, masová migrace),
- rizika úrovně vzdělání,
- kulturní rizika (národnostní a náboženská nesnášenlivost či diskriminace),
- rizika spojená s nezaměstnaností,
- zdravotní rizika (infekční a neinfekční onemocnění, zoonózy, úrazy aj.).

Do oblasti **technologických rizik** můžeme zahrnout např. skupiny rizik:
- dopravní rizika,
- energetická rizika,
- komunikační rizika,
- softwarová rizika,
- internetová rizika,
- průmyslová rizika.

Do oblasti **legislativních rizik** můžeme zahrnout např. skupiny rizik:
- rizika spojená se zákony, vyhláškami, normami či smlouvami,
- soudní rizika.

Do oblasti **ekologických rizik** můžeme zahrnout např. skupiny rizik:
- rizika přírodních katastrof (živelních pohrom),
- rizika čerpání neobnovitelných zdrojů,
- rizika úbytku ozonové vrstvy,
- rizika navyšování skleníkového efektu,
- rizika globálního oteplování,
- rizika klimatických změn.

U organizací ústřední státní správy můžeme výše uvedené oblasti vnitřních rizik dále na nižší rozlišovací úrovni členit do skupin.

Do oblasti *procesních (projektových) rizik* můžeme zahrnout např. skupiny rizik:
- rizika související s nastavením procesu (např. neexistence nebo složitost pravidel nebo interních normativních aktů pro provádění procesu, neexistující nebo špatně vymezené cíle procesu, nevhodná návaznost procesů, neexistující nebo špatně vymezené kompetence, neefektivnost nebo nepřesnost pracovních postupů),
- rizika související se vstupy do procesu (např. včasnost dodání vstupů, kvalita vstupů),
- rizika související se zdroji procesu (např. nedostatek zdrojů, nízká nebo nevhodná kvalita zdrojů, špatná alokace zdrojů),
- rizika související s výstupy procesu (např. včasnost dodání výstupů, kvalita výstupů).

Do oblasti *personálních rizik* můžeme zahrnout např. skupiny rizik:
- kvalifikační rizika (např. neznalost, neinformovanost, nekompetentnost, špatný výcvik),
- etická rizika (např. úplatnost, střet zájmů, zneužití pravomoci, odcizení, podvod),
- rizika spojená s prováděním činností (např. nepozornost, nedbalost, nesprávná obsluha, nešikovnost).

Do oblasti *věcných rizik* můžeme zahrnout např. skupiny rizik:
- mechanická rizika (např. hluk, vibrace),
- fyzikální rizika (např. teplo, záření),
- chemická rizika,
- biologická rizika.

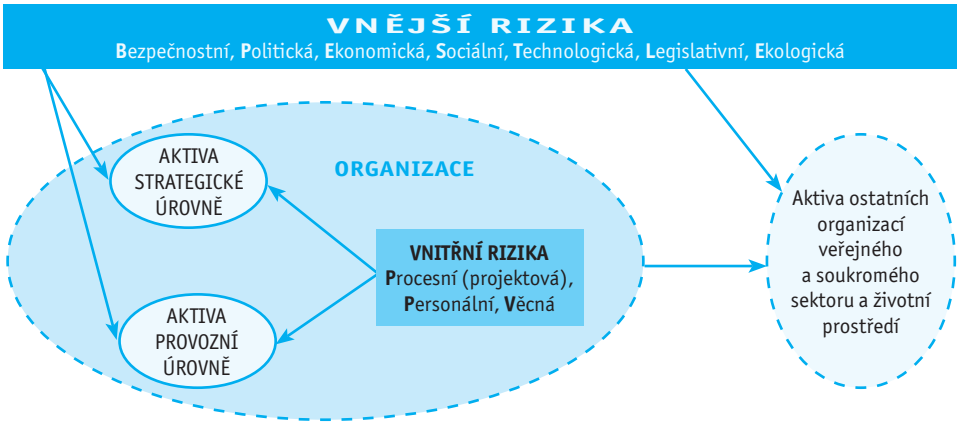
Kromě výše uvedené doporučené klasifikace rizik z hlediska působení zdrojů (tj. na vnitřní a vnější) je možné rizika členit také podle jiných hledisek, která ovšem nejsou pro potřeby subprocesu vymezení souvislostí natolik relevantní.

Některé odborné publikace [18] uvádějí členění např. z hlediska předvídatelnosti (předvídatelná a nepředvídatelná), ovlivnitelnosti (ovlivnitelná a neovlivnitelná), původu (primární a sekundární), systematičnosti (systematická a nesystematická), objektivity hodnocení (subjektivní a objektivní), dynamiky vývoje nežádoucí události (pomalá a rychlá),

pravděpodobnosti vzniku nežádoucí události (pravděpodobná a nepravděpodobná) či z hlediska intenzity dopadu nežádoucí události (rizika s mírným, vyšším a fatálním dopadem).

Závěr: Deskripce působení rizik na aktiva

Z výše uvedeného členění vyplývá, že na organizace ústřední státní správy působí dvě kategorie rizik, a to vnější a vnitřní. Tyto kategorie rizik mohou působit jak na aktiva úrovně strategické, tak i provozní. Současně je ovšem nutné vzít v úvahu, že vnitřní rizika mohou rovněž působit i vně organizace, a to na aktiva ostatních organizací veřejného nebo soukromého sektoru či na životní prostředí. Schéma působení rizik na aktiva je znázorněno na obrázku 5.



Obr. 5: Schéma působení rizik na aktiva

V souvislosti s působením rizik na aktiva je důležité podotknout, že většina prvků organizace (např. procesy, zaměstnanci, nemovitosti) může vystupovat ve dvou rolích. Jednak mohou představovat aktiva, na která působí vnější a vnitřní rizika. Současně ovšem mohou samy negativně působit na ostatní aktiva organizace, přičemž v tento okamžik již vystupují jako vnitřní zdroj rizika.

Tento článek byl zpracován v rámci grantového projektu GA AV ČR KJB606070701 „Metoda preventivního posouzení vlivu vojenského výcviku na životní prostředí“.

Poznámky k textu:

[1] Proces [process] je soubor vzájemně souvisejících nebo působících činností, které přeměňují vstupy na výstup při využití zdrojů (personál, finance, hmotné a nehmotné). Proces můžeme rozkládat na subprocesy, respektive jeho fáze. Každý subproces se poté skládá z jednotlivých na sebe navazujících činností.

[2] Poslání [mission] vyjadřuje smysl (účel) existence dané organizace. U organizací ústřední státní správy musí být poslání stanoveno v souladu se zákonem č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy ČR, ve znění změn a doplňků (tzv. kompetenční zákon).

[3] Riziko [risk] je kombinací pravděpodobnosti výskytu nežádoucí události a jejich následků, respektive dopadů (ISO/IEC Guide 73:2002). Riziko je tedy možnost, že při zajišťování činnosti orgánu státní správy s určitou pravděpodobností nastane určitá událost, jednání nebo stav s následnými nežádoucími dopady na plnění schválených záměrů a cílů tohoto orgánu. Stupeň významnosti rizika se určí jako součin možných nežádoucích dopadů a pravděpodobnosti zapůsobení tohoto rizika (CHJ-6:2004).

[4] Aktivum [asset] je všechno, co má pro danou organizaci hodnotu, která může být zmenšena působením rizika.
[5] Identifikace rizik [risk identification] je subproces zahrnující činnosti nalézání, rozpoznávání a popisování rizik (ISO/IEC Guide 73:2002).
[6] Např. (Smejkal, Reis, 2006) nebo (Tichý, 2006).
[7] Např. (Smejkal, Reis, 2006).
[8] Např. (ČSN IEC 300-3-9:1997).
[9] Autoři jsou si vědomi, že pokud není riziko vyjádřeno kombinací pravděpodobnosti a závažností dopadu na aktivum hovoříme o **hrozbě [threat]**. Ovšem pro potřeby tohoto článku bude nadále používán pouze **pojem riziko,** i když výše zmíněné atributy neobsahuje a jedná se tedy ve své podstatě o hrozbu.
[10] Cíl [objective] vyjadřuje, čeho chce organizace v budoucnu dosáhnout. Popisuje tedy požadovaný stav v budoucnu.
[11] Blanced scorecard (BSC) je metoda sloužící pro převod poslání, vize a strategie organizace do soustavy měřitelných strategických cílů a z nich vyplývajících strategických akcí. Strategické cíle pro účely ústřední státní správy jsou stanovovány pro stanovené perspektivy, kterými jsou politické zadání a zainteresované strany, interní kritické procesy, rozvoj zaměstnanců a rozpočet. Tato metoda tedy slouží jako nástroj strategického řízení, pro komunikaci a pro řízení výkonnosti.
[12] Zainteresované strany [stakeholders] jsou osoby nebo skupiny mající zájem na výkonnosti nebo úspěchu organizace, např. zákazníci/občané, zaměstnanci, společnost, inspekční orgány, média, dodavatelé, ale také například vláda, reprezentovaná volenými (nebo jmenovanými) vedoucími pracovníky, a nadřízené vládní organizace. Zainteresovanou stranou může být také sama organizace nebo její části. Hlavní zainteresovanou stranou jsou občané, kterým jsou primárně určeny poskytované služby stanovené v poslání organizace.
[13] Podle ČSN EN ISO 9000:2001 efektivnost [effectiveness] vyjadřuje vztah mezi realizací plánovaných cílů a dosaženými výsledky (např. cílové hodnoty stanovené v procesu/projektu a skutečně dosažené hodnoty).
[14] Hmotný a nehmotný majetek může být např. nemovitosti, kancelářské vybavení, materiál, technika, autorská práva, know-how.
[15] Zdroje rizik [risk sources] jsou objekty nebo činnosti, které mohou být příčinnou rizik (ISO/IEC Guide 73:2002). Autoři doporučují využívat následující jimi navrženou definici: Zdroje rizik jsou vnější činitelé (např. vnější legislativní prostředí, vnější politické prostředí) nebo vnitřní prvky organizace (např. procesy, zaměstnanci, nemovitosti), které jsou původci rizik, a jejichž vývoj nebo činnost (případně nečinnost) způsobuje možné nežádoucí dopady na aktiva organizace.
[16] PESTLE je akronym a jednotlivá písmena znamenají různé typy vnějších faktorů: P – politické, E – ekonomické, S – sociální, T – technologické, L – legální (legislativní), E – ekologické (environmentální). Podstatou analýzy je identifikovat pro každou skupinu faktorů ty nejvýznamnější jevy, události, rizika a vlivy, které ovlivňují nebo budou ovlivňovat organizaci.
[17] U soukromých firem se v této oblasti rizik objevují specifické skupiny rizik spojených s podnikáním jako např. investiční riziko, tržní riziko.
[18] Např. (Božek, Urban, 2008), (Smejkal, Reis, 2006).

Literatura:

BOŽEK, František, URBAN, Rudolf. *Management rizika – obecná část*. 1. vyd. Brno: Univerzita obrany, 2008, ISBN 978-80-7231-259-7, 145 s.

CHJ-6. *Pokyn k jednotnému uplatňování závazných pravidel a doporučení pro systém řízení rizik v orgánech veřejné správy*, 2004, 37 s.

ČSN EN ISO 9000. Systémy managementu jakosti – základy, zásady a slovník. Praha: Český normalizační institut, 2001.

GRASSEOVÁ, Monika a kolektiv. *Procesní řízení ve veřejném i soukromém sektoru*. 1. vyd. Brno: Computer Press, 2008, ISBN 978-80-251-1905-1, 266 s.

GRASSEOVÁ, Monika. Využití SWOT analýzy pro dlouhodobé plánování. *Obrana a strategie*, 2006, roč. 6, č. 2, ISSN 1214-6463, s. 48-55.

ISO/IEC Guide 73. *Risk management - Vocabulary*, 2002.

SMEJKAL, Vladimír, RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích*. 2. vyd. Praha: Grada Publishing, 2006, ISBN 80-247-1667-4, 296 s.

TICHÝ, Milík. *Ovládání rizika. Analýza a management*. 1. vyd. Praha: C. H. Beck, 2006, ISBN 80-7179-415-5, 396 s.