



Information Security Management  
Information Risk Management  
Business Continuity Management  
Information Forensic Analysis



RISK ANALYSIS CONSULTANTS

# A Risk Management Standard

Překlad a interpretace pro české prostředí



© 2002 by The Institute of Risk Management (IRM),  
The Association of Insurance and Risk Managers (AIRMIC),  
ALARM - The National Forum for Risk Management in the Public Sector  
© 2007, Risk Analysis Consultants

TATO STRANA JE PONECHÁNA PRÁZDNÁ ÚMYSLNĚ

## Important information / Důležité informace

Poděkování náleží následujícím organizacím, které spolupracovaly při tvorbě tohoto dokumentu.

*Acknowledgment is given to the following organizations that participated on the development of this publication.*

### **The Institute of Risk Management**

6 Lloyd's Avenue

London EC3N 3AX

020 7709 9808

020 7709 0716

[enquiries@theIRM.org](mailto:enquiries@theIRM.org)

[www.theIRM.org](http://www.theIRM.org)

### **ALARM The National Forum for Risk Management in the Public Sector**

Queens Drive, Exmouth

Devon, EX8 2AY

01395 223399

01395 223304

[admin@alarm.uk.com](mailto:admin@alarm.uk.com)

[www.alarm-uk.com](http://www.alarm-uk.com)

### **The Association of Insurance and Risk Managers**

6 Lloyd's Avenue

London EC3N 3AX

020 7480 7610

020 7702 3752

[enquiries@airmic.co.uk](mailto:enquiries@airmic.co.uk)

[www.airmic.com](http://www.airmic.com)

Tuto publikaci je možné zdarma získat v anglickém originále u výše uvedených organizací z jejich příslušných internetových stránek. Pokud si přejete zakoupit více kopií této normy řízení rizik v tištěné podobě, kontaktujte prosím jednotlivé organizace.

*This publication is available from the above organisations for download from their respective websites free of charge. Please contact the individual associations if you wish to purchase more copies of this Risk Management Standard in printed form*

### **Statut dokumentu / Document status**

Tento dokument je překlad A Risk Management Standard do češtiny provedený organizací Risk Analysis Consultants. Překlad je šířen se souhlasem The Institute of Risk Management (IRM),

Velká Británie. IRM neodpovídá za správnost překladu. Ve sporných případech je směrodatný anglický originál.

*This document is a translation of A Risk Management Standard into the Czech language by Risk Analysis Consultants. It is reproduced with the permission of The Institute of Risk Management (IRM), United Kingdom. IRM takes no responsibility for the accuracy of this translation. In any cases of dispute the English original shall be taken as authoritative.*

## **Autorská práva / Copyright**

Autorská práva © 2002 anglického originálu vlastní The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) and ALARM - The National Forum for Risk Management in the Public Sector. Autorská práva překladu vlastní Risk Analysis Consultants, s. r. o.

*Copyright © 2002 by The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) and ALARM - The National Forum for Risk Management in the Public Sector. Czech language edition arranged with Risk Analysis Consultants, Prague, Czech Republic. All rights reserved.*

Jakékoliv použití tohoto dokumentu nebo jeho částí pro účely další distribuce, kopírování, rozmnožování nebo jiného způsobu šíření je dovoleno pod podmínkou, že bude bezplatné a že budou uváděni všichni vlastníci autorských práv.

Jakékoliv použití tohoto dokumentu nebo jeho částí pro účely prodeje, jakož i překladu do jiného jazyka není možné bez souhlasu vlastníků autorských práv.

## **Informace / Information**

Společnost Risk Analysis Consultants, s.r.o. si vyhrazuje právo na změny v dokumentu bez oznámení subjektům, které dokument užívají.

*Risk Analysis Consultants, s.r.o. reserves the right to make amendments to this document at any time without prior notice.*

Připomínky a návrhy na změnu obsahu české verze tohoto dokumentu, požadavky na informace o aktuální verzi dokumentu je možno zasílat na níže uvedenou adresu.

*We also welcome suggestions for improvement of the Czech version of this document, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities.*

Risk Analysis Consultants, s. r. o.

Španělská 2, 120 00 Praha 2, CZ

Tel. +420 221 628 400, fax +420 221 628 401

rac@rac.cz, www.rac.cz

## **Poznámka k českému vydání**

Pro práci se soubory je doporučeno používat nejnovější verzi aplikace Adobe Acrobat Reader 7.0 CE.

***U některých typů tiskáren nemusí být kvalita tištěné verze, zejména u obrázků, plně srovnatelná s její elektronickou předlohou.***

## Obsah

Statut dokumentu / Document status	3
Autorská práva / Copyright	4
Informace / Information	4
Poznámka k českému vydání	4
Úvod	6
Riziko	7
1. Řízení rizik	7
1.1. Vnější a vnitřní faktory	7
1.2. Proces řízení rizik	9
2. Hodnocení rizik	9
3. Analýza rizik	10
3.1. Identifikace rizik	10
3.2. Popis rizika	10
3.3. Odhad rizika	11
3.4. Metody a techniky analýzy rizik	12
3.5. Profil rizika	12
4. Vyhodnocení rizik	13
5. Hlášení rizik a seznámení s riziky	13
5.1. Interní hlášení	13
5.2. Externí hlášení	13
6. Zvládání rizik	14
7. Monitorování a přezkoumávání procesu řízení rizik	15
8. Role a odpovědnosti při řízení rizik	15
8.1. Politika řízení rizik	15
8.2. Úloha představenstva	15
8.3. Úloha organizačních jednotek	16
8.4. Úloha útvaru pro řízení rizik	16
8.5. Úloha interního auditu	16
8.6. Zdroje a zavedení	16
ISO/IEC Guide 73	21
1. Působnost	21
2. Přehled termínů a definic řízení rizik	21
3. Termíny a definice	21

## Úvod

Tato norma je výsledkem práce skupiny sestavené významnými organizacemi zabývajícími se řízením rizik ve Velké Británii - *The Institute of Risk Management (IRM)*, *The Association of Insurance and Risk Managers (AIRMIC)* a *ALARM The National Forum for Risk Management in the Public Sector*. Skupina prostřednictvím konzultací a diskusních fór dlouhodobě shromažďovala pohledy a názory celé řady profesních uskupení a odborníků v oblasti řízení rizik.

Řízení rizik je rychle se rozvíjející obor a existuje mnoho různých pohledů a přístupů, jak a proč rizika řídit. Právě proto je z dlouhodobého hlediska potřebné zavést určitou normu, aby se zajistil soulad:

- ☒ terminologie, která se vztahuje k používaným pojmům;
- ☒ procesů, jejichž prostřednictvím se řízení rizik může provádět;
- ☒ organizační struktury pro řízení rizik;
- ☒ cílů a náplně řízení rizik.

Je důležité, aby takováto norma vystihla jeden podstatný prvek a to, že také rizika mají své výhody i nevýhody.

Řízení rizik se netýká pouze komerčních společností nebo veřejné správy, ale v podstatě každé krátkodobé nebo dlouhodobé činnosti. Zisky a příležitosti by neměly být posuzovány pouze v kontextu činnosti samotné, ale také ve vztahu ke všem zainteresovaným stranám, které mohou být rizikem ovlivněny.

Je mnoho způsobů a postupů vedoucích k dosažení cílů řízení rizik a není možné je všechny popsat v jediném dokumentu. Proto také záměrem tohoto dokumentu nebylo vytvořit předpisovou normu, která by požadovala plnění jednotlivých konkrétních kroků, ani zavést certifikovatelný postup. Po splnění jednotlivých částí této normy, a to i odlišnými způsoby, mohou organizace deklarovat soulad s normou. Tato norma představuje sbírku nejlepších praktik, kterými se organizace mohou řídit a proti kterým mohou měřit zavedený proces řízení rizik.

Všude, kde je to možné, používá norma terminologii pro rizika zavedenou Mezinárodní organizací pro normalizaci (*International Organization for Standardization, ISO*) ve vydaném standardu *ISO/IEC Guide 73, Risk Management - Vocabulary – Guidelines for use in standards*.

*S ohledem na rychlý vývoj v této oblasti by autoři ocenili zpětnou vazbu od organizací, které normu používají v praxi (adresy se nalézají na začátku této normy). Kvůli udržení aktuálnosti normy jsou plánovány její pravidelné úpravy.*

## Riziko

Riziko je možné definovat jako kombinaci pravděpodobnosti události a jejích následků (*ISO/IEC Guide 73*).

Všechny druhy podnikání jsou ovlivněny možnými událostmi a následky, které přinášejí příležitosti k zisku (výhody) nebo ohrožují úspěch (nevýhody).

Stále více se nahlíží na řízení rizik jako na činnost, která se zabývá jak kladnými, tak i zápornými aspekty rizik. Proto tato norma posuzuje rizika z obou hledisek.

V oblasti bezpečnosti jsou následky obecně považovány za nepříznivé, a proto se řízení bezpečnostních rizik zaměřuje především na prevenci a zmírnění škod.

### 1. Řízení rizik

Řízení rizik je důležitou součástí každého strategického řízení organizace. Je to proces, jehož prostřednictvím se organizace metodicky věnuje rizikům spojeným s činnostmi organizace s cílem dosáhnout trvalého prospěchu z každé jednotlivé a souhrnně ze všech činností organizace.

Správné řízení rizik se zaměřuje na identifikaci a zvládnutí těchto rizik. Jeho cílem je dodat co nejvyšší trvalou hodnotu všem činnostem organizace. Přispívá k pochopení možných výhod a nevýhod všech faktorů, které organizaci ovlivňují. Zvyšuje pravděpodobnost úspěchu a snižuje pravděpodobnost neúspěchu, stejně tak i nejistotu v dosahování obecných cílů činností organizace.

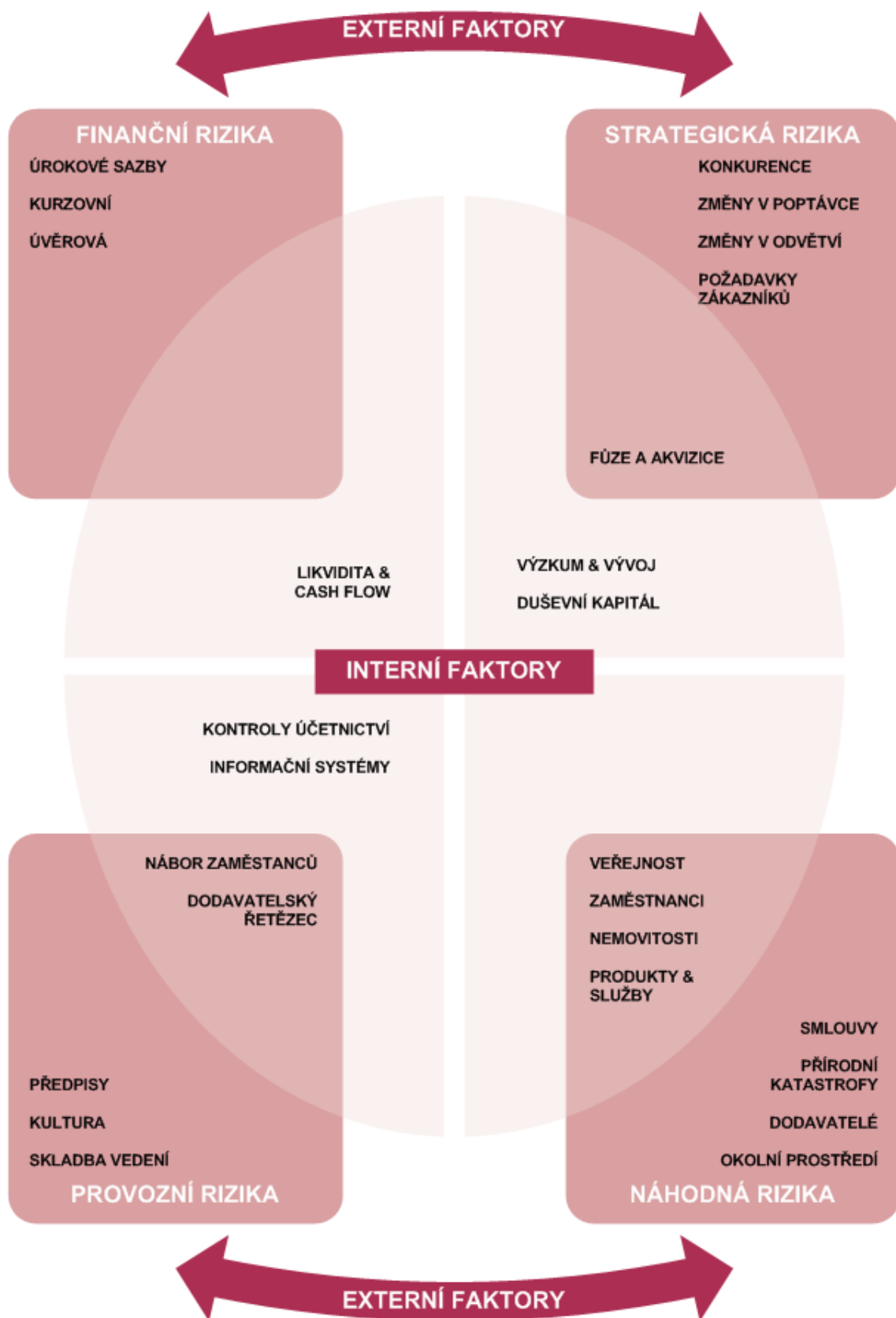
Řízení rizik by mělo být nepřetržitým a stále se zdokonalujícím procesem začleněným do strategie organizace a do jejího prosazování. Mělo by se metodicky zabývat všemi riziky, které se vztahují k minulosti, přítomnosti a především budoucnosti organizace a jejích aktivit. Musí být začleněno do kultury organizace spolu s účinnou politikou a plánem přijatým většinou vyššího managementu organizace. Musí převádět strategii do taktických a provozních cílů a rozdělovat odpovědnost v organizaci tak, aby řízení rizik bylo součástí náplně práce každého manažera a zaměstnance. Musí podporovat odpovědnost, měření a odměňování výkonu a tím přispívat k vyšší efektivitě na všech úrovních.

#### 1.1. Vnější a vnitřní faktory

Rizika, kterým je vystavena organizace a její činnosti, mohou vyplývat z vnějších nebo vnitřních faktorů.

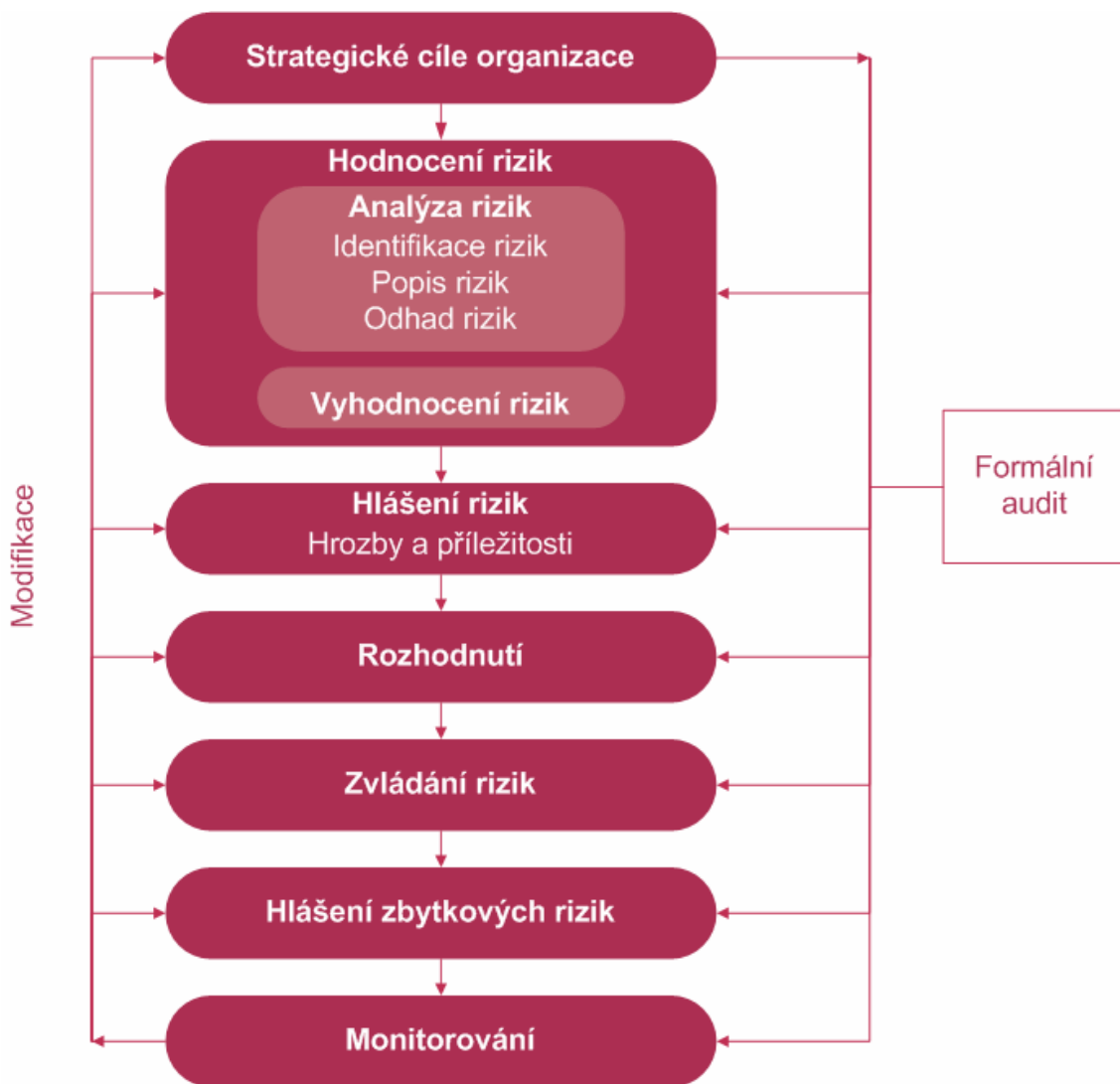
Obrázek na následující straně shrnuje příklady nejpodstatnějších rizik z různých oblastí a ukazuje, že příčiny některých konkrétních rizik leží vně i uvnitř organizace. Rizika mohou být rozdělena podle jejich druhu, jako například rizika strategická, finanční, provozní, náhodná (vyšší moc)<sup>1</sup> atd.

<sup>1</sup> Rizika, kterým se nelze vyhnout; přírodní katastrofy, ozbrojené konflikty a války, stávky, sociální nepokoje, nehody, zranění, virové epidemie, atd.



Obrázek 1 příklady vlivů klíčových rizik

## 1.2. Proces řízení rizik



Obrázek 2 proces řízení rizik

Organizace, která řídí rizika chrání svá aktiva a aktiva všech zainteresovaných stran a zároveň zvyšuje jejich hodnotu zejména tím, že:

- ☒ poskytuje organizaci rámec, který umožní provádět veškeré budoucí činnosti konzistentním a transparentním způsobem;
- ☒ zlepšuje proces rozhodování, plánování a určování priorit pomocí obsáhlého a strukturovaného posouzení jednotlivých činností organizace, posouzení míry nejistoty a příležitostí / hrozeb projektů;
- ☒ přispívá k účinnějšímu využívání / přidělování finančních prostředků a zdrojů organizace;
- ☒ snižuje nejistotu v oblastech, které nejsou pro organizaci zásadní;
- ☒ chrání a zhodnocuje aktiva a dobré jméno organizace;
- ☒ rozvíjí a podporuje znalosti zaměstnanců a znalostní základnu organizace;
- ☒ zvyšuje efektivitu činností organizace.

## 2. Hodnocení rizik

Hodnocení rizik je definováno ve standardu *ISO/IEC Guide 73* jako souhrnný proces analýzy a vyhodnocení rizik (podrobnosti jsou uvedeny v příloze).

### 3. Analýza rizik

#### 3.1. Identifikace rizik

Identifikace rizik slouží k určení míry nejistoty, které je organizace vystavena. Toto vyžaduje podrobnou znalost organizace, tržního, právního, sociálního, politického a kulturního prostředí ve kterém organizace působí, stejně jako důkladné porozumění strategickým a provozním cílům organizace, včetně zásadních faktorů úspěchu, hrozeb a příležitostí spojených s dosahováním těchto cílů.

K identifikaci rizik by se mělo přistupovat metodickým způsobem, aby bylo zabezpečeno, že budou identifikovány všechny podstatné činnosti organizace a určena rizika z těchto činností vyplývající. Dále je třeba identifikovat a ohodnotit veškerou související nejistotu vztahující se k těmto činnostem.

Činnosti organizace a rozhodnutí je možné uspořádat mnoha různými způsoby, příkladem může být rozdělení na:

- ☒ *Strategické* – Týkají se dlouhodobých strategických cílů organizace. Mohou být ovlivněny faktory, jakými jsou dostupnost kapitálových prostředků, rizika spojená s výkonnou mocí a politická rizika, zákonné a regulatorní změny, pověst organizace a změny ve fyzickém prostředí;
- ☒ *Provozní* – Týkají se každodenních problémů, kterým organizace čelí, když usiluje o dosažení svých strategických cílů;
- ☒ *Finanční* – Týkají se efektivní správy a kontroly finančních prostředků organizace, a působení vnějších vlivů, jakými jsou dostupnost úvěrů, směnné kurzy zahraničních měn, pohyb úrokových sazeb a další podmínky na trhu;
- ☒ *Správa znalostí* – Týkají se efektivní správy a kontroly znalostí a jejich zdrojů, jejich vytváření, ochrany a sdělování. Vnější faktory mohou zahrnovat neoprávněné použití nebo zneužití duševního vlastnictví, vnější výpadky elektrické energie, konkurenční technologie apod. Vnitřními faktory mohou být selhání systému nebo odchod důležitého personálu;
- ☒ *Soulad s požadavky* – Zahrnuje záležitosti jakými jsou bezpečnost a ochrana zdraví při práci, otázky životního prostředí, obchodní procesy, ochrana zákazníků, ochrana dat, postupy a zvyklosti při najímání nových pracovníků a regulatorní požadavky.

Přestože identifikaci rizik mohou provádět externí konzultanti, vlastní přístup se srozumitelnými, konzistentními a koordinovanými procesy a nástroji (popsanými v příloze) bude ve většině případů účinnější. Je nezbytné, aby proces řízení rizik „vlastnila“ sama organizace.

#### 3.2. Popis rizika

Cílem popisu rizika je znázornit identifikovaná rizika ve strukturované podobě, například prostřednictvím tabulky. Uvedenou tabulku popisu rizika 4.2.1 lze použít k usnadnění popisu a hodnocení rizik. K zabezpečení důkladného procesu identifikace, popisu a hodnocení rizik je nutné zavést dobře navržené uspořádání. Posouzením následků a pravděpodobností každého z rizik uvedených v tabulce by mělo být možné určit nejzávažnější rizika, která musí být podrobněji analyzována. Identifikace rizik spojených s činnostmi organizace a rozhodováním může být rozdělena jako strategická, projektová/taktická, provozní. Je důležité uplatnit řízení rizik jak v přípravné fázi projektů, tak po celou dobu trvání konkrétního projektu.

1. Název rizika	
2. Rozsah rizika	Kvalitativní popis událostí, jejich významu, druhu, počtu a závislostí
3. Povaha rizika	Např. strategické, provozní, finanční, týkající se znalostí nebo souladu s požadavky
4. Zainteresané strany	Zainteresané strany a jejich očekávání
5. Kvantifikace rizika	Závažnost a pravděpodobnost

6. Tolerance vůči rizikům/ ochota akceptovat rizika	Možnost ztráty a finanční dopad rizika Hodnota ohrožená rizikem Pravděpodobnost a míra možných ztrát/zisků Cíle pro zvládnání rizika a požadovaná úroveň výkonu
7. Zvládnání rizika a kontrolní mechanizmy	Základní prostředky, kterými je riziko obvykle spravováno Úrovně spolehlivosti stávajících opatření Určení záznamů pro monitorování a přezkoumání
8. Možné postupy pro zlepšení	Doporučení ke snížení rizika
9. Vývoj strategie a politik	Určení funkce zodpovědné za vývoj strategie a politik

Tabulka 3.2-1 Popis rizika

### 3.3. Odhad rizika

Odhad rizika, vyjádřený v termínech pravděpodobnosti výskytu a možných následků, může být kvantitativní, polokvantitativní nebo kvalitativní.

Například následky jak hrozeb (nepříznivá rizika), tak příležitostí (příznivá rizika) mohou být velké, střední nebo malé (srovnej tabulku 4.3.1). Pravděpodobnost může být vysoká, střední nebo nízká, ale vyžaduje rozdílné definice pro hrozby a příležitosti (viz tabulky 4.3.2 a 4.3.3). Příklady jsou uvedeny v následujících tabulkách. Různé organizace mohou zavést různá měřítka následků a pravděpodobností, která budou nejlépe vyhovovat jejich potřebám.

Například pro potřeby mnoha organizací celkem postačuje ohodnocení následků a pravděpodobností slovy velké, střední nebo malé a mohou tak být uspořádány do matice 3×3.

Jiným organizacím bude lépe vyhovovat ohodnocení následků a pravděpodobností pomocí matice 5×5.

Velké	Finanční dopad na organizaci pravděpodobně překročí <b>x</b> Kč Významný dopad na strategii a provozní činnosti organizace Značné obavy zainteresovaných stran
Střední	Finanční dopad na organizaci se bude pravděpodobně pohybovat mezi <b>x</b> a <b>y</b> Kč Střední dopad na strategii a provozní činnosti organizace Mírné obavy zainteresovaných stran
Malé	Finanční dopad na organizaci bude pravděpodobně nižší než <b>y</b> Kč Malý dopad na strategii a provozní činnosti organizace Nízké obavy zainteresovaných stran

Tabulka 3.3-1 Následky – Hrozby a příležitosti

Hodnocení	Popis	Indikátory
Vysoká (pravděpodobná)	Vyskytuje se většinou každý rok nebo pravděpodobnost výskytu je vyšší než 25%.	Možnost opakovaného výskytu v určitém časovém období (např. 10 let). Vyskytla se nedávno.

Hodnocení	Popis	Indikátory
Střední (možná)	Nejspíše se vyskytne v časovém období deseti let nebo pravděpodobnost výskytu je nižší než 25%.	Mohla se vyskytnout více než jednou v určitém časovém období (například 10 let).  Hrozbu je obtížné kontrolovat vzhledem k některým vnějším vlivům.  Vyskytla se v minulosti?
Nízká (nepředpokládaná)	Neočekává se výskyt hrozby v časovém období deseti let nebo pravděpodobnost výskytu je nižší než 2%.	Dosud se nevyskytla.  Výskyt je nepravděpodobný.

Tabulka 3.3-2 Pravděpodobnost výskytu – Hrozby

Hodnocení	Popis	Indikátory
Vysoká (pravděpodobná)	Příznivých výsledků je možné dosáhnout do jednoho roku nebo pravděpodobnost výskytu je vyšší než 75%.	Jasná příležitost, na kterou se lze spolehnout s přiměřenou jistotou a kterou je možné využít v krátké době pomocí stávajících procesů řízení.
Střední (možná)	Nadějné vyhlídky na příznivé výsledky do jednoho roku nebo pravděpodobnost výskytu se pohybuje mezi 25% a 75%.	Příležitosti, které lze využít, ale vyžadují opatrné zacházení.  Příležitosti, které se mohou objevit nečekaně a nad plán.
Nízká (nepředpokládaná)	Jisté vyhlídky na příznivé výsledky ve střednědobém čase nebo pravděpodobnost výskytu je nižší než 25%.	Možné příležitosti, které vedení organizace ještě plně neprozkoumalo.  Takové příležitosti, u kterých je pravděpodobnost úspěchu nízká vzhledem k stávajícím zdrojům řízení.

Tabulka 3.3-3 Pravděpodobnost výskytu – Příležitosti

### 3.4. Metody a techniky analýzy rizik

K analýze rizik je možné využít řadu technik, které mohou být použitelné jen pro příznivá nebo nepříznivá rizika, nebo jsou aplikovatelné na oba případy (příklady jsou uvedeny v příloze).

### 3.5. Profil rizika

Výsledek procesu analýzy rizika je možné použít k vytvoření profilu rizika, který udává míru závažnosti každého rizika a poskytuje nástroj pro seřazení činností zvládnání rizik podle jejich důležitosti. To umožňuje roztřídit a uspořádat všechna identifikovaná rizika podle jejich relativního významu.

Tento proces dovoluje spojit určité riziko s činnostmi organizace jím ovlivněnými, určuje základní opatření, která je nezbytné provést, a ukazuje oblasti, ve kterých je třeba zvýšit, snížit nebo přerozdělit náklady na řízení rizik.

Rozdělení odpovědnosti pomáhá zajistit, že „vlastnictví“ rizik je jasně stanovené a že byly vyčleněny příslušné zdroje řízení.

## 4. Vyhodnocení rizik

Po dokončení procesu analýzy rizik je nezbytné porovnat odhadnutá rizika s měřítky rizik, která příslušná organizace zavedla. Měřítko rizik mohou zahrnovat přidružené náklady a zisky, právní požadavky, socioekonomické a environmentální faktory, zájmy zainteresovaných stran, atd. Proto vyhodnocení rizik slouží k rozhodnutí o závažnosti rizik pro organizaci a jestli konkrétní riziko akceptovat nebo jej zvládat.

## 5. Hlášení rizik a seznámení s riziky

### 5.1. Interní hlášení

Různé úrovně v organizaci vyžadují různé informace o procesu řízení rizik.

Představenstvo by mělo:

- znát nejzávažnější rizika, kterým je organizace vystavena;
- znát možné dopady odchylek od očekávaného výkonu na hodnotu akcií;
- zajistit přiměřenou úroveň povědomí o rizicích v celé organizaci;
- vědět, jak bude organizace zvládat krizi;
- uvědomovat si důležitost důvěry zainteresovaných stran v organizaci;
- znát vhodný způsob komunikace s investory, je-li to relevantní;
- zajistit efektivní průběh procesu řízení rizik;
- zveřejnit jasnou politiku řízení rizik zahrnující obecný přístup k řízení rizik a rozdělení zodpovědností.

Organizační jednotky by měly:

- mít povědomí o rizicích, která spadají do jejich oblasti odpovědnosti, o možných dopadech těchto rizik na další oblasti a o následcích, jaké z toho pro ně mohou plynout;
- zavést ukazatele výkonu, které jim umožní sledovat zásadní obchodní a finanční činnosti organizace, dosahování cílů a určit procesy, které vyžadují zásahy (např. předpovědi a rozpočty);
- mít systémy, které dostatečně často upozorňují na odchylky od rozpočtů a předpovědí, aby bylo možné podniknout příslušné kroky;
- systematicky a pohotově hlásit vyššímu vedení organizace jakákoliv nová rizika nebo selhání stávajících opatření.

Jednotlivci by měli:

- chápat jejich odpovědnost ve vztahu k jednotlivým rizikům;
- vědět, jak mohou pomoci stálému zlepšování řízení rizik;
- chápat, že řízení rizik a povědomí o rizicích je podstatnou součástí kultury organizace;
- systematicky a pohotově hlásit vyššímu vedení organizace jakákoliv nová rizika nebo selhání stávajících kontrolních opatření.

### 5.2. Externí hlášení

Každá organizace musí pravidelně informovat všechny zainteresované strany o vytvořených politikách řízení rizik a o efektivitě dosahování stanovených cílů. Zainteresované strany stále více požadují po organizacích důkazy o správném řízení chodu organizace nejen z finančního hlediska, ale také z hlediska společenských událostí, lidských práv, zaměstnávání, bezpečnosti a ochrany zdraví při práci a životního prostředí.

Dobré řízení a správa společnosti vyžadují, aby společnosti zavedly metodický přístup k řízení rizik, který:

- ☒ chrání zájmy zainteresovaných stran;
- ☒ zabezpečí, že představenstvo splní své povinnosti stanovit strategii, vytvářet hodnoty a sledovat výkon organizace;
- ☒ zajistí, že opatření ke zvládnání rizik jsou zavedena a provádějí se správně.

Ustanovení o formálním hlášení o řízení rizik by měla být jasně stanovena a dostupná všem zainteresovaným stranám. Formální hlášení by se mělo věnovat:

- ☒ způsobům kontroly – zvláště odpovědnosti vedení za řízení rizik;
- ☒ procesům užívaným k identifikaci rizik a způsobům, jak systémy řízení rizik s těmito procesy zacházejí;
- ☒ základním opatřením, která byla zavedena ke zvládnání podstatných rizik;
- ☒ zavedenému systému monitorování a přezkoumání rizik.

Jakékoliv zásadní nedostatky odhalené systémem, nebo nedostatky v systému samotném, by měly být hlášeny spolu s kroky provedenými k jejich nápravě.

## 6. Zvládnání rizik

Zvládnání rizik je proces výběru a zavedení opatření vedoucích ke změně rizik. Jeho základním prvkem je regulace/zmírnění rizik, ale zvládnání rizik zahrnuje dále například vyvarování se rizik, sdílení rizik, financování rizik, atd.

*POZNÁMKA: V této normě označuje financování rizik mechanismy krytí finančních následků rizik (např. pojištění). Zajištění prostředků ke krytí nákladů na zavedení procesu zvládnání rizik není obecně považováno za financování rizik (jak je definováno v ISO/IEC Guide 73, strana 17).*

Libovolný systém zvládnání rizik by měl přinejmenším zabezpečovat:

- ☒ efektivní a výkonný provoz organizace;
- ☒ účinné vnitřní kontrolní mechanismy;
- ☒ soulad se zákony a předpisy.

Proces analýzy rizik přispívá k efektivnímu a výkonnému provozu organizace tak, že odhaluje ta rizika, která vyžadují zvláštní pozornost vedení organizace. Opatření ke zvládnání rizik musejí být seřazena podle priorit z hlediska jejich přínosu organizaci.

Účinnost opatření je vyjádřena mírou, se kterou bude riziko buď odstraněno nebo sníženo zavedením navrhovaného kontrolního opatření.

Nákladnost opatření závisí na porovnání výdajů na zavedení takového opatření s očekávanými zisky souvisejícími se snížením rizika.

Navrhovaná opatření je třeba hodnotit srovnáním možného ekonomického dopadu, jestliže nebude provedena žádná akce, a nákladů potřebných na realizaci navrhovaných opatření. Takováto rozhodnutí vždy vyžadují podrobnější informace a předpoklady než jsou v daném okamžiku dostupné.

Nejprve je nutné zjistit náklady na zavedení opatření. Náklady je třeba spočítat s určitou přesností, protože jsou základním měřítkem, podle kterého se posuzuje finanční náročnost a účinnost opatření. Dále je třeba odhadnout předpokládané ztráty, nebudou-li podniknuty žádné kroky, a teprve na základě výsledků může pak vedení rozhodnout, jestli zavést nebo nezavést navrhovaná opatření ke snížení rizik.

Soulad se zákony a regulatorními požadavky je naprosto nezbytný. Organizace musí znát příslušné zákony a musí zavést soubor opatření, která umožní dosáhnout souladu s těmito zákony. Jen ve výjimečných případech je povolena určitá volnost a to v případech, kdy náklady na snížení rizika jsou naprosto nepřiměřené samotnému riziku.

Jedním ze způsobů, jak si zajistit finanční ochranu proti následkům rizik je financování rizik, tento způsob zahrnuje pojištění. Přesto je třeba si uvědomit, že některé ztráty nebo částečné ztráty nejsou pojistitelné, například náklady spojené s bezpečností a ochranou zdraví při práci nebo jinými událostmi, které mohou vést k narušení pracovní kázně zaměstnanců nebo pověsti organizace.

## 7. Monitorování a přezkoumávání procesu řízení rizik

Účinné řízení rizik vyžaduje soustavu hlášení a přezkoumávání celého procesu tak, aby se zajistila účinná identifikace rizik, odhad rizik a zavedení přiměřených opatření a reakcí. Je vhodné provádět pravidelné audity postupů a souladu s normami kvůli nalezení možností ke zlepšení. Je třeba pamatovat i na to, že organizace se stále vyvíjejí a působí v měnícím se prostředí. Změny v organizaci a v prostředí, ve kterém organizace působí, je nutné důsledně sledovat a následně provádět odpovídající změny v systému.

Proces monitorování by měl poskytovat záruky, že jsou zavedena vhodná opatření pro činnosti organizace a že postupy řízení rizik v organizaci jsou srozumitelné a dodržují se.

Změny v organizaci a v prostředí, ve kterém organizace působí, je nutné sledovat a následně provádět příslušné úpravy v systému.

Každý proces monitorování a přezkoumávání rizik by měl také určit, zda:

- přijatá opatření splnila zamýšlený účel;
- přijaté postupy a informace získané k provedení hodnocení rizik byly správné;
- by důkladnější znalosti pomohly dosáhnout lepších rozhodnutí a určit, jaká ponaučení si vzít pro příští hodnocení a řízení rizik.

## 8. Role a odpovědnosti při řízení rizik

### 8.1. Politika řízení rizik

Politika organizace pro řízení rizik by měla vymezit vztah k rizikům, ochotu rizika podstupovat a celkový přístup organizace k řízení rizik. Politika by také měla jasně stanovit odpovědnosti za řízení rizik ve všech částech organizace.

Mimoto by měla poukázat na všechny legislativní požadavky, např. na bezpečnost a ochranu zdraví při práci.

Proces řízení rizik poskytuje komplexní sadu nástrojů a technik, použitelných v různých fázích existujících procesů organizace. Proces řízení rizik potřebuje k efektivnímu chodu:

- podporu vrcholového a výkonného vedení organizace;
- rozdělení zodpovědností za řízení rizik v rámci organizaci;
- vyhrazení příslušných zdrojů na školení a zvyšování povědomí zaměstnanců a ostatních zainteresovaných stran o rizicích.

### 8.2. Úloha představenstva

Představenstvo je zodpovědné za vytyčení strategického směřování organizace a za vytvoření prostředí a struktur pro efektivní chod řízení rizik.

Může se tak stát prostřednictvím výkonné skupiny, poradní komise, komise pro audity nebo jiného takového útvaru, který vyhovuje způsobu fungování organizace a může vystupovat jako „sponzor“ řízení rizik.

Představenstvo by při hodnocení opatření mělo přinejmenším zvážit následující:

- povahu a rozsah nepříznivých rizik, která je organizace ochotna akceptovat a unést;
- pravděpodobnost, se kterou taková rizika nastanou;
- způsob jak zacházet s nepřijatelnými riziky;
- schopnost organizace snižovat pravděpodobnost rizik a dopad na jednotlivé činnosti;
- náklady a zisky spojené s riziky a prováděné kontrolní činnosti;
- účinnost celého procesu řízení rizik;
- rizika plynoucí z rozhodnutí představenstva.

### 8.3. Úloha organizačních jednotek

Tato zahrnuje následující:

- ☒ jednotlivé organizační jednotky nesou odpovědnost za každodenní řízení rizik;
- ☒ vedení organizačních jednotek je zodpovědné za zvyšování povědomí o rizicích ve svých provozech; mělo by začlenit řízení rizik do svých činností;
- ☒ řízení rizik by mělo být pravidelnou položkou na poradách vedení, aby bylo zajištěno posouzení zranitelnosti a případně upraveny priority s ohledem na výsledky analýzy rizik;
- ☒ vedení organizačních jednotek by mělo zajistit, že se řízení rizik stane součástí jak přípravné fáze projektů, tak celého jejich trvání.

### 8.4. Úloha útvaru pro řízení rizik

V závislosti na velikosti organizace může být odpovědnost za řízení rizik přidělena členu vedení, zabývajícím se riziky, přes manažera pro řízení rizik na částečný úvazek, až po plnohodnotné oddělení pro řízení rizik. Úloha útvaru pro řízení rizik by měla zahrnovat následující:

- ☒ vytvoření politiky a strategie řízení rizik;
- ☒ základní podporu řízení rizik na strategické a provozní úrovni;
- ☒ vytvoření povědomí o rizicích v rámci celé organizace, včetně programu vzdělávání;
- ☒ zavedení vnitřních postupů a struktur týkajících se rizik v organizačních jednotkách;
- ☒ procesy navržení a přezkoumání řízení rizik;
- ☒ koordinaci různých činností organizace, které řeší otázky řízení rizik;
- ☒ vytvoření postupů pro reakci na rizika včetně programů kontingence a kontinuity činností organizace;
- ☒ přípravu hlášení o rizicích pro představenstvo a všechny zainteresované strany.

### 8.5. Úloha interního auditu

Úloha interního auditu se bude pravděpodobně lišit od jedné organizace ke druhé. V praxi může interní audit plnit některé nebo všechny následující funkce:

- ☒ zaměření interního auditu na závažná rizika určená vedením organizace a provádění auditu procesů řízení rizik v organizaci;
- ☒ poskytnutí záruky řízení rizik;
- ☒ zajištění aktivní podpory a angažovanosti v procesu řízení rizik;
- ☒ zjednodušení identifikace/hodnocení rizik a vzdělávání zaměstnanců ve věci řízení rizik a vnitřních kontrolních mechanismů;
- ☒ koordinace hlášení rizik představenstvu, komisi pro audit, atd.

Při určování nejvhodnější role pro konkrétní organizaci by mělo být podmínkou, že interní audit zabezpečí splnění požadavků na nezávislost a objektivitu.

### 8.6. Zdroje a zavedení

Zdroje potřebné k zavedení politiky řízení rizik v organizaci by měly být jasně stanoveny na každé úrovni řízení a v každé organizační jednotce.

Kromě dalších provozních funkcí, které mohou plnit, je pro role spojené s řízením rizik nutné jasně vymezit jejich odpovědnosti v politice/strategii řízení rizik. Stejně vymezení je potřebné i u rolí spojených s auditem a přezkoumáváním kontrolních opatření.

Řízení rizik by se mělo stát součástí strategických rozhodnutí a sestavování rozpočtů organizace. Důraz by se na něj měl kladen v rámci školení a vzdělávacích programů, stejně jako v procesech, jakými jsou např. vývoj nových produktů a služeb.





## Příloha A

### Příloha A.1 Techniky identifikace rizik – příklady

- ☒ *Brainstorming*
- ☒ *Dotazníková šetření*
- ☒ *Případové studie, které posuzují každý proces v organizaci a popisují jak vnitřní procesy, tak vnější faktory, které mohou tyto procesy ovlivnit*
- ☒ *Srovnávací výkonové testy (benchmarking)*
- ☒ *Analýza možných scénářů*
- ☒ *Semináře o hodnocení rizik*
- ☒ *Vyšetřování incidentů*
- ☒ *Audity a inspekce*
- ☒ *Studie nebezpečí a provozuschopnosti (Hazard and Operability Studies, HAZOP)*

### Příloha A.2 Postupy a techniky analýzy rizik – příklady

#### Příznivá rizika

- ☒ *Průzkum trhu*
- ☒ *Zjišťování poptávky*
- ☒ *Zkušební marketing*
- ☒ *Výzkum a vývoj*
- ☒ *Analýza obchodních dopadů*

#### Příznivá i nepříznivá rizika

- ☒ *Modelování závislostí*
- ☒ *Analýza silných a slabých stránek, příležitostí a hrozeb (SWOT analysis)*
- ☒ *Analýza „stromu“ událostí (event tree analysis)*
- ☒ *Plánování kontinuity činností organizace*
- ☒ *Analýza tržních, politických, ekonomických, sociálních a technologických podmínek (BPEST analysis)*
- ☒ *Modelování reálných možností*
- ☒ *Rozhodování v rizikových a nejistých situacích*
- ☒ *Statistická odvození*
- ☒ *Zjištění hlavního směřování a rozptylu*
- ☒ *Analýza politických, ekonomických, sociálních, technických, právních a environmentálních podmínek (PESTLE)*

#### Nepříznivá rizika

- ☒ *Analýza hrozeb*
- ☒ *Analýza „stromu“, negativních událostí (fault tree analysis)*
- ☒ *Analýza způsobu a následků selhání (FMEA)*



**Následující strany přinášejí výtažky z dokumentu PD ISO/IEC Guide 73:2002 reprodukované se souhlasem British Standards Institution (BSI) pod licenčním označením 2002SK/0313. Britské normy je možné získat ve středisku služeb zákazníkům BSI na adrese BSI Customer Services, 389 Chiswick High Road, London W4 4AL. (Telefon +44 (0) 20 8996 9001).**

## ISO/IEC Guide 73

Řízení rizik – Slovník – Návody pro použití v normách

### 1. Působnost

Tato příručka poskytuje tvůrcům norem obecné definice termínů vztahujících se k řízení rizik. Je zamýšlena jako výchozí obecný dokument pro přípravu nebo přezkoumání norem, které obsahují hlediska řízení rizik. Cílem této příručky je podporovat koherentní přístup k popisu činností řízení rizik a k používání terminologie řízení rizik. Jejím záměrem je přispět k vzájemnému porozumění mezi členy ISO a IEC spíše než poskytnout návod ke způsobům a metodám řízení rizik.

Bezpečnostními hledisky se zabývá *ISO/IEC Guide 51*.

*POZNÁMKA 1: Pojem „norma“ používaný v této příručce zahrnuje technické zprávy a příručky (technical reports and guides).*

*POZNÁMKA 2: Takové normy se mohou věnovat výhradně řízení rizik nebo mohou obsahovat kapitoly zabývající se řízením rizik.*

### 2. Přehled termínů a definic řízení rizik

Vztah mezi termíny a definicemi řízení rizik ukazují obrázky 1 až 3 normy *ISO/IEC Guide 73*. Řízení rizik je částí obecnějších procesů řízení organizace. Proces řízení rizik závisí na konkrétních souvislostech a podmínkách, ve kterých je použito. Výrazy a pojmy užívané v různých souvislostech se tedy mohou lišit.

Pokud jsou termíny vztahující se k řízení rizik použity v normě, je nezbytné, aby jejich zamýšlený význam v kontextu normy nebyl chybně vysvětlen nebo pochopen. Proto tato příručka zavádí definice pro různé významy, které každý termín může mít, se zvláštním ohledem na to, aby si definice navzájem neodporovaly. Organizace stále více využívají procesy řízení rizik ke zlepšení správy možných příležitostí. Tím se liší od procesu hodnocení rizik popsaného v *ISO/IEC Guide 51*, v jehož pojetí přináší riziko pouze nepříznivé následky. Protože však obchodní společnosti stále více posuzují rizika v širším smyslu, věnuje se tato příručka oběma situacím. Definice zavedené v této příručce jsou obecnější než definice z *ISO/IEC Guide 51*. Ve všech záležitostech týkajících se bezpečnosti platí definice uvedené v *ISO/IEC Guide 51*. *ISO/IEC Guide 73*, příloha A, obsahuje abecední seznam těchto definic a termínů v angličtině a francouzštině.

*POZNÁMKA: Pokud se definice odkazuje na termín zavedený jinde v této příručce, je termín uveden kurzívou spolu s křížovým odkazem. U termínů citovaných v poznámkách nejsou křížové odkazy.*

### 3. Termíny a definice

#### 3.1 Základní termíny

##### 3.1.1 riziko (*risk*)

spojení *pravděpodobnosti* (3.1.3) *události* (3.1.4) a jejich *následků* (3.1.2)

*POZNÁMKA 1: Pojem „riziko“ se obecně používá pouze pokud existuje alespoň možnost negativních následků.*

*POZNÁMKA 2: V některých případech riziko vzniká z možnosti odchylky od očekávaného výsledku nebo události.*

*POZNÁMKA 3: Otázky spojené s bezpečností probírá ISO/IEC Guide 51.*

### **3.1.2 následek (consequence)**

výsledek události (3.1.4)

*POZNÁMKA 1: Jedna událost může vyvolat více následků.*

*POZNÁMKA 2: Následky mohou sahát od kladných po záporné, ale z bezpečnostních hledisek jsou následky vždy záporné.*

*POZNÁMKA 3: Následky mohou být vyjádřeny kvalitativně nebo kvantitativně.*

### **3.1.3 pravděpodobnost (probability)**

míra možnosti s jakou událost (3.1.4) nastane

*POZNÁMKA 1: ISO 3534-1:1993, definice 1.1, uvádí matematickou definici pravděpodobnosti jako „reálné číslo v rozsahu 0 až 1 přiřazené náhodné události. Může se vztahovat k dlouhodobé relativní frekvenci výskytu nebo stupni přesvědčení, že daná událost nastane. Pro vysoký stupeň přesvědčení je pravděpodobnost blízká 1.“*

*POZNÁMKA 2: Při popisu rizika může být použita frekvence výskytu spíše než pravděpodobnost.*

*POZNÁMKA 3: Stupeň přesvědčení o pravděpodobnosti je možné uspořádat do tříd nebo stupnic, jako řídké/nepravděpodobně/průměrně/pravděpodobně/téměř jisté nebo nereálné/nepravděpodobně/zřídka/příležitostně/pravděpodobně/často.*

### **3.1.4 událost (event)**

výskyt konkrétního souboru okolností

*POZNÁMKA 1: Událost může být určitá nebo neurčitá.*

*POZNÁMKA 2: Událost se může vyskytovat osamoceně nebo v řadě dalších událostí.*

*POZNÁMKA 3: Pravděpodobnost spojenou s událostí lze odhadnout pro daný časový úsek.*

### **3.1.5 zdroj (source)**

věc nebo činnost schopná způsobit následek (3.1.2)

*POZNÁMKA: Z pohledu bezpečnosti je zdroj nebezpečím (srovnej přílohu A a ISO/IEC Guide 51:1999).*

### **3.1.6 měřítko rizik (risk criteria)**

referenční údaje, pomocí kterých se hodnotí závažnost rizik (3.1.1)

*POZNÁMKA: Měřítko rizik mohou zahrnovat přidružené náklady a zisky, právní a zákonné požadavky, socioekonomická a ekologická hlediska, zájmy zainteresovaných stran, priority a další vstupy hodnocení.*

### **3.1.7 řízení rizik (risk management)**

koordinované činnosti sloužící k řízení a kontrole organizace s ohledem na rizika (3.1.1)

*POZNÁMKA: Řízení rizik zpravidla zahrnuje hodnocení rizik, zvládnání rizik, akceptaci rizik a seznámení s rizikem (komunikace rizik).*

### 3.1.8 systém řízení rizik (*risk management system*)

soubor prvků ze systému řízení organizace, který se týká řízení rizik (3.1.1)

*POZNÁMKA 1: Prvky systému řízení organizace mohou zahrnovat strategické plánování, rozhodování a další procesy pro nakládání s riziky.*

*POZNÁMKA 2: Kultura organizace se odráží také v jejím systému řízení rizik.*

## 3.2 Termíny týkající se lidí a organizací ovlivněných rizikem

### 3.2.1 zainteresovaná strana (*stakeholder*)

jednotlivec, skupina nebo organizace, kteří mohou ovlivnit, být ovlivněni, nebo se cítit ovlivněni rizikem (3.1.1)

*POZNÁMKA 1: Ten, kdo rozhoduje, je také zainteresovanou stranou.*

*POZNÁMKA 2: Pojem „zainteresovaná strana“ zahrnuje „zájmovou skupinu“ (která je definovaná v ISO 9000:2000), ale má širší význam.*

### 3.2.2 zájmová skupina (*interested party*)

osoba nebo skupina se zájmem na výkonu nebo úspěchu organizace

*PŘÍKLADY: Zákazníci, vlastníci, lidé v organizaci, dodavatelé, banky, odbory, partneři nebo společnost.*

*POZNÁMKA: Skupina může obsahovat organizaci, její část nebo více než jednu organizaci.*

*[ISO 9000:2000, definice 3.3.7]*

### 3.2.3 vnímání rizik (*risk perception*)

způsob, jakým zainteresovaná strana (3.2.1) nahlíží na riziko (3.1.1), založený na souboru hodnot nebo zájmů

*POZNÁMKA 1: Vnímání rizik závisí na potřebách, názorech a znalostech zainteresované strany.*

*POZNÁMKA 2: Vnímání rizik se nemusí shodovat s objektivními údaji.*

### 3.2.4 seznámení s rizikem (*risk communication*)

výměna nebo sdílení informací o riziku (3.1.1) mezi těmi, kdo rozhodují o riziku, a ostatními zainteresovanými stranami

*POZNÁMKA: Informace se mohou vztahovat k existenci, povaze, podobě, pravděpodobnosti, závažnosti, akceptovatelnosti, způsobu zvládnání nebo dalším vlastnostem rizika.*

## 3.3 Termíny týkající se hodnocení rizik

### 3.3.1 hodnocení rizik (*risk assessment*)

celkový proces analýzy rizik (3.3.2) a vyhodnocení rizik (3.3.6)

### 3.3.2 analýza rizik (*risk analysis*)

systematické používání informací k odhadu rizika (3.1.1) a určení jeho zdrojů (3.1.5)

*POZNÁMKA 1: Analýza rizik poskytuje základ pro vyhodnocení rizik, pro rozhodnutí o postupu zvládnání rizik a pro akceptaci rizik.*

*POZNÁMKA 2: Informace mohou zahrnovat údaje z minulosti, teoretické analýzy, odborné názory a zájmy zainteresovaných stran.*

*POZNÁMKA 3: ISO/IEC Guide 51 obsahuje posouzení analýzy rizik v kontextu bezpečnosti.*

### **3.3.3 identifikace rizik (risk identification)**

proces nalezení, zaznamenání a popsání složek rizika (3.1.1)

*POZNÁMKA 1: Složky mohou zahrnovat zdroje nebezpečí, události, následky a pravděpodobnosti.*

*POZNÁMKA 2: Identifikace rizik může také brát v úvahu zájmy zainteresovaných stran.*

### **3.3.4 identifikace zdrojů (source identification)**

proces nalezení, zaznamenání a popsání zdrojů (3.1.5)

*POZNÁMKA: V kontextu bezpečnosti se identifikace zdrojů nazývá identifikací nebezpečí (blíže ISO/IEC Guide 51).*

### **3.3.5 odhad rizik (risk estimation)**

proces používaný k přiřazení hodnot pravděpodobnostem (3.1.3) a následkům (3.1.2) rizik (3.1.1)

*POZNÁMKA: Odhad rizik může brát v úvahu náklady, zisky, zájmy zainteresovaných stran a další proměnné potřebné k vyhodnocení rizik.*

### **3.3.6 vyhodnocení rizik (risk evaluation)**

proces posuzování odhadnutého rizika (3.1.1) podle zavedených měřítek rizik (3.1.6) kvůli určení závažnosti rizika

*POZNÁMKA 1: Vyhodnocení rizika napomáhá při rozhodování o akceptaci nebo způsobu zvládnutí rizika.*

*POZNÁMKA 2: ISO/IEC Guide 51 popisuje vyhodnocení rizik v souvislosti s bezpečností.*

## **3.4 Termíny týkající se zvládnutí a regulace rizik**

### **3.4.1 zvládnutí rizik (risk treatment)**

proces výběru a provádění opatření, která mění rizika (3.1.1)

*POZNÁMKA 1: Termínem „zvládnutí rizik“ se někdy označují samotná opatření.*

*POZNÁMKA 2: Opatření ke zvládnutí rizik mohou zahrnovat vyhnutí se riziku, změnu, přenesení nebo podstoupení rizika.*

### **3.4.2 regulace rizik (risk control)**

činnosti spojené s prováděním rozhodnutí o řízení rizik (3.1.7)

*POZNÁMKA: Regulace rizik může zahrnovat monitorování, přehodnocování a kontrolu prováděných činností.*

### **3.4.3 optimalizace rizik (risk optimization)**

proces minimalizace nepříznivých a maximalizace kladných následků (3.1.2) a jejich odpovídajících pravděpodobností (3.1.3) spojených s určitým rizikem (3.1.1)

*POZNÁMKA 1: V kontextu bezpečnosti se optimalizace rizik zaměřuje na zmenšení rizik.*

*POZNÁMKA 2: Optimalizace rizik závisí na měřítkách rizik, včetně nákladů a právních požadavků.*

*POZNÁMKA 3: Je možné zvážit rizika spojená s regulací rizik.*

#### **3.4.4 redukce rizik (risk reduction)**

úkony provedené ke snížení *pravděpodobnosti* (3.1.3) a/nebo *nepříznivých následků* (3.1.2) spojených s nějakým *rizikem* (3.1.1)

#### **3.4.5 zmírnění (mitigation)**

omezení jakýchkoli *nepříznivých následků* (3.1.2) určité *události* (3.1.4)

#### **3.4.6 vyvarování se rizika (risk avoidance)**

rozhodnutí nepodílet se na rizikové situaci nebo se z ní stáhnout

*POZNÁMKA: Rozhodnutí může být učiněno na základě provedeného vyhodnocení rizik.*

#### **3.4.7 sdílení rizika (risk transfer, risk sharing)**

sdílení ztrát nebo zisků příslušných konkrétnímu *riziku* (3.1.1) s další stranou

*POZNÁMKA 1: Právní nebo zákonné požadavky mohou omezovat, zakazovat nebo nařizovat sdílení některých rizik.*

*POZNÁMKA 2: Sdílení rizik je možné uskutečnit prostřednictvím pojištění nebo jiných dohod.*

*POZNÁMKA 3: Sdílení rizik může zavádět nová rizika nebo měnit stávající rizika.*

*POZNÁMKA 4: Přemístění zdroje není přenosem rizika.*

#### **3.4.8 financování rizik (risk financing)**

poskytnutí peněžních a kapitálových prostředků k pokrytí nákladů na zavedení *zvládnutí rizik* (3.4.1) a souvisejících nákladů

*POZNÁMKA: V některých oborech se financováním rizik míní pouze krytí finančních následků vztahujících se k riziku.*

#### **3.4.9 podstoupení rizika (risk retention)**

akceptování ztrát nebo zisků spojených s určitým *rizikem* (3.1.1)

*POZNÁMKA 1: Podstoupení rizik obsahuje také přijetí zatím neznámých rizik.*

*POZNÁMKA 2: Podstoupení rizik nezahrnuje opatření využívající pojištění nebo přenesení rizik jinými způsoby.*

*POZNÁMKA 3: Může se lišit podle míry akceptace ztrát nebo zisků a závislosti na měřítkách rizik.*

#### **3.4.10 akceptace rizika (risk acceptance)**

rozhodnutí akceptovat (přijmout) *riziko* (3.1.1)

*POZNÁMKA 1: Slovo „akceptovat“ bylo vybráno s ohledem na to, že akceptace má svůj základní slovníkový význam.*

*POZNÁMKA 2: Rozhodnutí o akceptaci rizika je závislé na měřítkách rizik.*

### **3.4.11 zbytkové riziko** (*residual risk*)

*riziko* (3.1.1) zbývající po uplatnění zvládnání rizik (3.4.1)

*POZNÁMKA: ISO/IEC Guide 51 popisuje aplikace vztahující se k bezpečnosti.*





Information Security Management  
Information Risk Management  
Business Continuity Management  
Information Forensic Analysis



Risk Analysis Consultants is an independent Czech based provider of professional services and solutions in all areas of information security.

Risk Analysis Consultants is first Czech company NATO BOA partner.

Risk Analysis Consultants is registered in part I. of the Czech government list of institutes qualified for forensic expertise in the area of cybernetics and computer systems.

Risk Analysis Consultants  
Spanelska 2  
120 00 Prague 2  
Czech Republic

tel: +420 221 628 400  
fax: +420 221 628 401  
e-mail: [rac@rac.cz](mailto:rac@rac.cz)  
[www.rac.cz](http://www.rac.cz)

RISK ANALYSIS CONSULTANTS

