

ČESKÁ TECHNICKÁ NORMA

ICS 03.100.01 **Říjen 2010**

Management rizik – Principy a směrnice

ČSN
ISO 31000
01 0351

Risk management – Principles and guidelines

Management du risque – Principes et lignes directrices

Tato norma je českou verzí mezinárodní normy ISO 31000:2009. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO 31000:2009. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Souvisící ČSN

ČSN EN ISO 9000 (01 0300) Systémy managementu kvality – Základní principy a slovník

ČSN EN ISO 9004 (01 0324) Řízení udržitelného úspěchu organizace – Přístup managementu kvality

ČSN EN ISO 14121-1 (83 3010) Bezpečnost strojních zařízení – Posouzení rizika – Část 1: Zásady

ČSN EN 60812 (01 0675) Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA)

ČSN EN 61025 (01 0676) Analýza stromu poruchových stavů (FTA)

TNI 01 0350 (01 0350) Management rizik – Slovník (Pokyn 73)

Vysvětlivky k textu převzatého dokumentu

K podpoře správného chápání textu je dále uvedeno vysvětlení překladu výrazů, pro které nebylo v normě možné nalézt zcela výstižný český ekvivalent a mohly by být chápány ve zkresleném nebo omezeném významu, než je míněn v anglickém textu normy.

a. **risk**

Pro anglický výraz „*risk*“ lze užívat ekvivalent jak v jednotném, tak v množném čísle. V překladu byly použity obě možnosti. Pokud se jedná o obecnější pohled, překládá se množným číslem, jako

např.: „management rizik“, „hodnocení rizik“, „ošetřování rizik“, pokud se jedná o podrobný postup při provádění konkrétní analýzy, překládá se v jednotném čísle, jako např. „identifikace rizika“, „vyhnutí se riziku“, „sdílení rizika“.

b. risk management framework

V normě jsou uvedeny dva ekvivalenty výrazu „risk management framework“, a to „rámec managementu rizik“ nebo „struktura managementu rizik“, protože různé typy organizací mohou skupinu činností, kterou tento výraz zastřešuje, ve své organizaci řízení nazývat jinak. Oba ekvivalenty jsou pro použití v organizacích srovnatelně vhodné.

c. governance

Pro anglický výraz „governance“ lze užívat ekvivalent „správa“ nebo „správné řízení“, v této normě se však výraz vztahuje především ke způsobu řízení určité organizace, a tak je v některých kapitolách použit také ekvivalent „vedení“.

d. managing

Pro anglický výraz „managing“ je v této normě použit ekvivalent „řízení“. Jedná se o řízení strategické, nikoli operativní.

e. control

Anglický výraz „control“ se v normách pro management rizik opakuje poměrně často. Jako podstatné jméno vyjadřuje soubor aktivit, které se musí realizovat, aby se identifikované riziko snížilo nebo alespoň zůstalo pod kontrolou. Tuto skutečnost dobře vystihuje použitý ekvivalent „opatření“, v některých případech je však výstižnější užití ekvivalentu „řízení“ pro control, jako např. ve spojení „monitorování řízení“.

Vypracování technické normy

Zpracovatel: Fakulta podnikohospodářská Vysoké školy ekonomické v Praze, IČ 61384399, Ing. M. Šebestová, IČ 16112946

Technická normalizační komise: TNK 6 Management kvality a prokazování kvality

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Soňa Húsková

MEZINÁRODNÍ NORMA

Management rizik – Principy a směrnice ISO 31000 První vydání 2009-11-15

ICS 03.100.01

Předmluva	6
Úvod	7
Management rizik – Zásady a směrnice	11
1 Předmět	11
2 Termíny a definice	11
3 Zásady	18
4 Rámec (struktura)	19
4.1 Všeobecně	19
4.2 Mandát a závazek	21
4.3 Návrh rámce pro řízení rizik	21
4.3.1 Pochopení organizace a jejího kontextu	21
4.3.2 Stanovení politiky managementu rizik	22
4.3.3 Odpovědnost	22
4.3.4 Integrace do procesů organizace	23
4.3.5 Zdroje	23
4.3.6 Nastavení mechanismů pro vnitřní komunikaci a hlášení	23
4.3.7 Nastavení mechanismů pro vnější komunikaci a hlášení	24
4.4 Implementování managementu rizik	24
4.4.1 Implementování rámce pro management rizik	24
4.4.2 Implementování procesu managementu rizik	24
4.5 Monitorování a přezkoumávání rámce	25
4.6 Neustálé zlepšování rámce	25
5 Proces	25
5.1 Všeobecně	25
5.2 Komunikace a konzultace	27
5.3 Stanovení kontextu	27
5.3.1 Všeobecně	27
5.3.2 Stanovení vnějšího kontextu	28
5.3.3 Stanovení vnitřního kontextu	28
5.3.4 Stanovení kontextu v rámci procesu managementu rizik	29
5.3.5 Určování kritérií rizik	29
Strana	
5.4 Posuzování rizik	30
5.4.1 Všeobecně	30
5.4.2 Identifikace rizik	30
5.4.3 Analýza rizik	31
5.4.4 Hodocení rizik	31
5.5 Ošetření rizik	32
5.5.1 Všeobecně	32
5.5.2 Výběr možností ošetření rizik	32
5.5.3 Příprava a implementování plánů ošetření rizik	33
5.6 Monitorování a přezkoumávání	34
5.7 Zaznamenávání procesu managementu rizik	34
Příloha A (informativní) Příznaky rozšířeného managementu rizik	35
Bibliografie	37

Odmítnutí odpovědnosti za PDF

Tento soubor PDF může obsahovat vložené typy písma. V souladu s licenční politikou Adobe je přípustné tento soubor tisknout nebo prohlížet, nesmí být však editován, pokud nejsou vložené znaky opatřeny licencí a nejsou nainstalovány v počítači, na kterém se editace provádí. Stažením tohoto souboru na lokální počítač přijímají strany odpovědnost za neporušování licenční politiky Adobe. Adobe je obchodní značka „Adobe Systems Incorporated“.

Foreword	6
Introduction	7
Risk management – Principles and guidelines	11
1 Scope	11
2 Terms and definitions	11
3 Principles	18
4 Framework	19
4.1 General	19
4.2 Mandate and commitment	21
4.3 Design of framework for managing risk	21
4.3.1 Understanding of the organization and its context	21
4.3.2 Establishing risk management policy	22
4.3.3 Accountability	22
4.3.4 Integration into organizational processes	23
4.3.5 Resources	23
4.3.6 Establishing internal communication and reporting mechanisms	23
4.3.7 Establishing external communication and reporting mechanisms	24
4.4 Implementing risk management	24
4.4.1 Implementing the framework for managing risk	24
4.4.2 Implementing the risk management process	24
4.5 Monitoring and review of the framework	25
4.6 Continual improvement of the framework	25
5 Process	25
5.1 General	25
5.2 Communication and consultation	27
5.3 Establishing the context	27
5.3.1 General	27
5.3.2 Establishing the external context	28
5.3.3 Establishing the internal context	28
5.3.4 Establishing the context of the risk management process	29
5.3.5 Defining risk criteria	29
Strana	
5.4 Risk assessment	30
5.4.1 General	30
5.4.2 Risk identification	30
5.4.3 Risk analysis	31
5.4.4 Risk evaluation	31
5.5 Risk treatment	32
5.5.1 General	32
5.5.2 Selection of risk treatment options	32
5.5.3 Preparing and implementing risk treatment plans	33
5.6 Monitoring and review	34
5.7 Recording the risk management process	34
Annex A (informative) Attributes of enhanced risk management	35
Bibliography	37

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. Adobe is a trademark of Adobe Systems Incorporated.

Podrobnosti o softwarových produktech, které byly použity při vytváření tohoto PDF souboru, lze nalézt ve všeobecných informacích vztahujících se k tomuto souboru; parametry pro vytváření PDF souborů byly optimalizovány pro tisk. Veškerá pozornost byla věnována tomu, aby byl soubor vhodný pro používání všemi členy ISO. V případě nepravděpodobné události a zjištění souvisejícího problému zašlete, prosím, informaci Ústřednímu sekretariátu na níže uvedenou adresu.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO 2009

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně fotokopíí a mikrofilmů, bez písemného svolení buď od organizace ISO na níže uvedené adrese, nebo od členské organizace ISO v zemi žadatele.

© ISO 2009

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 · CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org
Vydáno ve Švýcarsku

ISO copyright office
Case postale 56 · CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org
Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětovou federací národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle připravují technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodní organizace, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

Mezinárodní normy se navrhují podle pravidel uvedených ve směrnících ISO/IEC, části 2.

Hlavním úkolem technických komisí je tvorba mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členským orgánům k hlasování. Zveřejnění mezinárodní normy vyžaduje schválení alespoň 75 % hlasujících členů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO není odpovědná za identifikování jakýchkoli nebo všech těchto patentových práv.

ISO 31000 byla vypracována pracovní skupinou Technického řídicího výboru pro management rizik.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 31000 was prepared by the ISO Technical Management Board Working Group on risk management.

Úvod

Organizace všech typů a velikostí jsou vystaveny působení vnitřních a vnějších faktorů a vlivů, které vytvářejí nejistotu, zda a kdy dosáhnou svých cílů. Účinek, který má tato nejistota na dosažení cílů organizace, je riziko.

Všechny činnosti organizace zahrnují rizika. Organizace řídí rizika tím, že je identifikují, analyzují a pak vyhodnocují, zda by rizika mohla být změněna jejich ošetřením tak, aby se uspokojivě vešla do hranic příslušejících kritérií rizik. V průběhu tohoto procesu komunikují a konzultují se zainteresovanými stranami a monitorují a přezkoumávají rizika i opatření, která rizika modifikují, aby se zajistilo, že žádná další ošetření rizik už není zapotřebí. Tato mezinárodní norma podrobně popisuje tento systematický a logický proces.

Zatímco všechny organizace řídí rizika jen do určité úrovně, tato mezinárodní norma stanoví řadu principů, které je třeba naplnit, aby byl management rizik efektivní. Tato mezinárodní norma doporučuje, aby organizace rozvíjely, implementovaly a kontinuálně zlepšovaly rámec, jehož účelem je integrovat proces pro řízení rizik do svého celkového vedení, strategie a plánování, managementu, procesů podávání hlášení, politik, hodnot a kultury.

Management rizik lze aplikovat na celou organizaci, v mnoha oblastech a na mnohých úrovních, v kteroukoli dobu, stejně jako pro specifické funkce, projekty nebo činnosti.

Přestože zavedené postupy managementu rizik byly v průběhu času vyvíjeny v rámci mnoha sektorů pro splnění různých potřeb, zavedení konzistentních procesů v rámci celkové struktury může pomoci zajistit, aby bylo řízení rizik v rámci celé organizace smysluplné, efektivní a koherentní. Generický přístup, popsán v této mezinárodní normě, poskytuje principy a návody pro řízení jakékoli formy rizika systematickým, transparentním a důvěryhodným způsobem a v rámci jakéhokoli rozsahu i kontextu.

Introduction

Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is "risk".

All activities of an organization involve risk. Organizations manage risk by identifying it, analysing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Throughout this process, they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk in order to ensure that no further risk treatment is required. This International Standard describes this systematic and logical process in detail.

While all organizations manage risk to some degree, this International Standard establishes a number of principles that need to be satisfied to make risk management effective. This International Standard recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

Risk management can be applied to an entire organization, at its many areas and levels, at any time, as well as to specific functions, projects and activities.

Although the practice of risk management has been developed over time and within many sectors in order to meet diverse needs, the adoption of consistent processes within a comprehensive framework can help to ensure that risk is managed effectively, efficiently and coherently across an organization. The generic approach described in this International Standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context.

Každý specifický sektor nebo využití managementu rizik přináší s sebou individuální potřeby, uživatele, vnímání a kritéria. Hlavní úlohou této mezinárodní normy je tudíž zavedení „stanovení kontextu“ na počátku generického procesu managementu rizik. Stanovení kontextu zachytí cíle organizace, prostředí, ve kterém usiluje o své cíle, její zainteresované strany a různorodost kritérií rizik – a to všechno pomůže odkrýt a vyhodnotit povahu a komplexnost jejích rizik.

Vztah mezi zásadami pro management rizik, rámcem, pomocí kterého vzniká a procesy managementu rizik, popsanými touto mezinárodní normou, je znázorněn na obrázku 1.

Management rizik, pokud je dobře zaveden a udržován podle této mezinárodní normy, umožňuje organizacím například:

- zvýšit pravděpodobnou možnost dosažení cílů;
- dodat odvalu proaktivnímu vedení;
mít povědomí o potřebě identifikovat a ošetřovat rizika v rámci celé organizace;
zlepšovat identifikování příležitostí a hrozeb;

- být v souladu s příslušnými požadavky zákonů, předpisů a mezinárodních norem;

zlepšit finanční vykazování;

zlepšit organizaci řízení (vedení);

zlepšit důvěryhodnost pro zainteresované strany;

vytvořit spolehlivou základnu pro rozhodování a plánování;

zlepšit řízení;

účinně rozmístit a využívat zdroje pro ošetření rizik;

zlepšit provozní funkčnost i efektivnost;

pozvednout výkonnost bezpečnosti a ochrany zdraví i environmentální ochrany;

zlepšit prevenci ztrát a management incidentů;

minimalizovat ztráty;

zlepšit princip učení se v organizaci; a

zlepšit pružnost organizace.

Tato mezinárodní norma je určena, aby naplnila potřeby širokého rozsahu zainteresovaných stran, včetně:

1. těch, kteří odpovídají za vývoj politiky managementu rizik v rámci své organizace;
3. těch, kteří odpovídají za zajištění efektivního řízení rizik buď v rámci celé organizace, nebo v rámci určité oblasti, projektu nebo činnosti;
4. těch, kteří potřebují vyhodnotit efektivnost organizace v řízení rizik; a
5. zpracovatelů norem, pokynů, postupů a návodů celých nebo jejich částí, které stanovují, jak řídit rizika v rámci specifických kontextů těchto dokumentů.

Současné praktiky a procesy managementu mnoha organizací obsahují součásti managementu rizik a mnoho organizací již také zavedlo formalizovaný proces managementu rizik pro určité typy rizik nebo situací. V takových případech se může organizace rozhodnout provést kritické přezkoumání těchto existujících přístupů a procesů z pohledu této mezinárodní normy.

Each specific sector or application of risk management brings with it individual needs, audiences, perceptions and criteria. Therefore, a key feature of this International Standard is the inclusion of “establishing the context” as an activity at the start of this generic risk management process. Establishing the context will capture the objectives of the organization, the environment in which it pursues those objectives, its stakeholders and the diversity of risk criteria – all of which will help reveal and assess the nature and complexity of its risks.

The relationship between the principles for managing risk, the framework in which it occurs and the risk management process described in this International Standard are shown in Figure 1.

When implemented and maintained in accordance with this International Standard, the management of risk enables an organization to, for example:

- increase the likelihood of achieving objectives;
- encourage proactive management;
- be aware of the need to identify and treat risk throughout the organization;
- improve the identification of opportunities and threats;

comply with relevant legal and regulatory requirements and international norms;

improve financial reporting;

improve governance;

improve stakeholder confidence and trust;

establish a reliable basis for decision making and planning;

improve controls;

effectively allocate and use resources for risk treatment;

improve operational effectiveness and efficiency;

enhance health and safety performance, as well as environmental protection;

improve loss prevention and incident management;

minimize losses;

improve organizational learning; and

improve organizational resilience.

This International Standard is intended to meet the needs of a wide range of stakeholders, including:

1. those responsible for developing risk management policy within their organization;
3. those accountable for ensuring that risk is effectively managed within the organization as a whole or within a specific area, project or activity;
4. those who need to evaluate an organization effectiveness in managing risk; and
5. developers of standards, guides, procedures and codes of practice that, in whole or in part, set out how risk is to be managed within the specific context of these documents.

The current management practices and processes of many organizations include components of risk management, and many organizations have already adopted a formal risk management process for particular types of risk or circumstances. In such cases, an organization can decide to carry out a critical review of its existing practices and processes in the light of this International Standard.

V této mezinárodní normě se používá jak výraz „management rizik“, tak i „řízení rizik“. Za všeobecných podmínek „management rizik“ vyjadřuje architekturu (zásady, rámec a proces) pro efektivní řízení rizik, zatímco „řízení rizik“ vyjadřuje používání této architektury pro konkrétní rizika.

In this International Standard, the expressions “risk management” and “managing risk” are both used. In general terms, “risk management” refers to the architecture (principles, framework and process) for managing risks effectively, while “managing risk” refers to applying that architecture to particular risks.



Obrázek 1 - Vazby mezi principy, rámcem a procesem managementu rizik



Figure 1 - Relationships between the risk management principles, framework and process

Management rizik – Zásady a směrnice

1 Předmět

Tato mezinárodní norma poskytuje zásady a generické směrnice pro management rizik.

Tuto mezinárodní normu mohou využívat všechny veřejné, soukromé nebo státní podniky, sdružení, skupiny nebo jedinci. Proto tato mezinárodní norma není specifická pro žádný průmysl nebo sektor.

POZNÁMKA Pro zjednodušení budou všichni nejrozličnější uživatelé této normy označováni všeobecným termínem „organizace“.

Tuto mezinárodní normu lze používat v průběhu celého života organizace a pro široký rozsah činností, včetně strategií a rozhodnutí, provozu, procesů, funkcí, projektů, služeb a majetku (aktiv).

Tuto mezinárodní normu lze použít pro všechny typy rizik, ať jsou jakékoli povahy, a jak pro pozitivní, tak pro negativní následky.

Přestože tato mezinárodní norma je generickou směrnici, není zamýšlena pro rozvíjení jednotného managementu rizik napříč organizacemi. Návrh a implementování plánů a rámců managementu rizik bude potřebovat zohlednit měnící se potřeby specifických organizací, jejich zvláštní cíle, souvislosti, strukturu, činnosti, procesy, funkce, projekty, produkty, služby nebo vlastnictví a specifické používané zavedené postupy.

Je záměrem, aby tato mezinárodní norma byla využívána k harmonizování procesů managementu rizik v existujících a budoucích normách. Poskytuje to společný přístup v podporování norem týkajících se specifických rizik a/nebo sektorů, aniž by nahrazovala tyto normy.

Tato mezinárodní norma není určena pro účely certifikace.

Risk management – Principles and guidelines

1 Scope

This International Standard provides principles and generic guidelines on risk management.

This International Standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.

NOTE For convenience, all the different users of this International Standard are referred to by the general term “organization”.

This International Standard can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

This International Standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Although this International Standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.

It is intended that this International Standard be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.

This International Standard is not intended for the purpose of certification.

Konec náhledu - text dále pokračuje v placené verzi ČSN.