ČESKÁ TECHNICKÁ NORMA

ICS 03.100.01 **Prosinec**
2018

Management rizik – Směrnice

ČSN
ISO 31000

01 0351

Risk management – Guidelines

Management du risque – Lignes directrices

Tato norma je českou verzí mezinárodní normy ISO 31000:2018. Překlad byl zajištěn Českou agenturou pro stan-
dardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO 31000:2018. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO 31000 (01 0351) z října 2010.

Národní předmluva

Změny proti předchozí normě

Hlavní změny proti předchozímu vydání normy jsou uvedeny v předmluvě.

Souvisící ČSN

ČSN EN 31010 (01 0352) Management rizik – Techniky posuzování rizik

Vypracování normy

Zpracovatel: Česká společnost pro jakost, IČO 00417955, Ing. Marie Šebestová

Technická normalizační komise: TNK 6 Management kvality a prokazování kvality

Pracovník České agentury pro standardizaci: Ing. Radmila Foretová

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických poža-

davcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

MEZINÁRODNÍ NORMA

Management rizik – Směrnice

ISO 31000

Druhé vydání

2018-02

ICS 03.100.01

Obsah

Strana

Předmluva ... 5
Úvod ... 7
1 Předmět ... 9
2 Citované dokumenty ... 9
3 Termíny a definice ... 9
4 Zásady ... 11
5 Rámec (struktura) ... 13
5.1 Obecně ... 13
5.2 Vedení a závazek ... 14
5.3 Integrace ... 15
5.4 Návrh ... 16
5.4.1 Porozumění organizaci a jejímu kontextu ... 16
5.4.2 Formulování závazků k managementu rizik ... 16
5.4.3 Přidělování organizačních rolí, pravomocí, povinností a odpovědností ... 17
5.4.4 Přidělení zdrojů ... 17
5.4.5 Ustanovení komunikace a konzultací ... 17
5.5 Implementace ... 18
5.6 Hodnocení ... 18
5.7 Zlepšování ... 18
5.7.1 Přizpůsobování ... 18
5.7.2 Trvalé zlepšování ... 18
6 Proces ... 19
6.1 Obecně ... 19
6.2 Komunikace a konzultace ... 20
6.3 Rozsah, kontext a kritéria ... 21
6.3.1 Obecně ... 21
6.3.2 Stanovení rozsahu ... 21
6.3.3 Externí a interní kontext ... 21
6.3.4 Stanovení kritérií rizika (rizik) ... 22
6.4 Posuzování rizika (rizik) ... 22
6.4.1 Obecně ... 22
6.4.2 Identifikace rizika (rizik) ... 22

Strana

6.4.3 Analýza rizika (rizik) ... 23
6.4.4 Hodnocení rizika (rizik) ... 24
6.5 Ošetřování rizika (rizik) ... 24
6.5.1 Obecně ... 24
6.5.2 Volba možností pro ošetřování rizika (rizik) ... 24
6.5.3 Příprava a implementování plánů ošetřování rizik ... 25
6.6 Monitorování a přezkoumávání ... 26
6.7 Zaznamenávání a podávání hlášení ... 26
Bibliografie ... 28

Contents

Page

Foreword ... 5
Introduction ... 7
1 Scope ... 9
2 Normative references ... 9
3 Terms and definitions ... 9
4 Principles ... 11
5 Framework ... 13
5.1 General ... 13
5.2 Leadership and commitment ... 14
5.3 Integration ... 15
5.4 Design ... 16
5.4.1 Understanding the organization and its context ... 16
5.4.2 Articulating risk management commitment ... 16
5.4.3 Assigning organizational roles, authorities, responsibilities and accountabilities ... 17
5.4.4 Allocating resources ... 17
5.4.5 Establishing communication and consultation ... 17
5.5 Implementation ... 18
5.6 Evaluation ... 18
5.7 Improvement ... 18
5.7.1 Adapting ... 18
5.7.2 Continually improving ... 18
6 Process ... 19
6.1 General ... 19
6.2 Communication and consultation ... 20
6.3 Scope, context and criteria ... 21
6.3.1 General ... 21
6.3.2 Defining the scope ... 21
6.3.3 External and internal context ... 21
6.3.4 Defining risk criteria ... 22
6.4 Risk assessment ... 22
6.4.1 General ... 22
6.4.2 Risk identification ... 22

Page

6.4.3 Risk analysis ... 23
6.4.4 Risk evaluation ... 24
6.5 Risk treatment ... 24
6.5.1 General ... 24
6.5.2 Selection of risk treatment options ... 24
6.5.3 Preparing and implementing risk treatment plans ... 25
6.6 Monittoring and review ... 26
6.7 Recording and reporting ... 26

ISO copyright office
CP 401 · Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Tel.: + 41 22 749 01 11
Fax: + 41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publikováno ve Švýcarsku

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětová federace národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle vypracovávají 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.

Postupy použité při tvorbě tohoto dokumentu a po-stupy určené pro jeho další udržování jsou popsány ve směrnicích ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů ISO. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnicích ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO nelze činit odpovědnou za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržených ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená schválení.

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), jsou uvedeny na tomto odkazu: URL: www.iso.org/iso/foreword.

Tento dokument vypracovala komise ISO/TC 262 *Management rizik*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO 31000:2009), které bylo technicky revidováno.

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO,s adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword

This document was prepared by Technical Committee ISO/TC 262, Risk management.

This second edition cancels and replaces the first edition (ISO 31000:2009) which has been technically revised

Hlavní změny ve srovnání s předchozím vydáním jsou následující:
– revize zásad managementu rizik, které jsou klíčovými kritérii pro jeho úspěch;
– zviditelnění významu vedení ze strany vrcholového vedení a integrování managementu rizik, počínaje správou organizace;
– větší důraz na soustavně se opakující povahu managementu rizik, která upozorňuje na to, že nové zkušenosti, znalosti a analýzy mohou vést ke změně prvků procesů, činností i opatření (pro řízení) v každém stádiu procesu;
– zefektivnění obsahu s větším zaměřením na udržování modelu otevřených systémů tak, aby vyhovoval různým potřebám a kontextům.

The main changes compared to the previous edition are as follows:
– review of the principles of risk management, which are the key criteria for its success;
– highlighting of the leadership by top management and the integration of risk management, starting with the governance of the organization;
– greater emphasis on the iterative nature of risk management, noting that new experiences, knowledge and analysis can lead to a revision of process elements, actions and controls at each stage of the process;
– streamlining of the content with greater focus on sustaining an open systems model to fit multiple needs and contexts.

Úvod

Tento dokument je určen pro použití osobami, které vytváří a chrání hodnoty v organizacích pomocí řízení rizik, rozhodováním, nastavováním a dosahováním cílů a zlepšováním výkonnosti.
Organizace všech typů a velikostí jsou vystavovány působení interních a externích faktorů a vlivů, které vytvářejí nejistotu, zda dosáhnou svých cílů.
Řízení rizik je soustavně se opakující činnost a pomáhá organizacím při stanovování strategie, dosahování cílů a přijímání informovaných rozhodnutí.
Řízení rizik je součástí správy a vedení organizace a je nezbytné pro její řízení na všech úrovních. Přispívá ke zlepšování systémů managementu.

Řízení rizik je součástí všech činností souvisejících s organizací a zahrnuje vzájemné působení se zainteresovanými stranami.
Řízení rizik zohledňuje externí a interní kontext organizace včetně lidského chování a kulturních faktorů.
Řízení rizik vychází ze zásad, rámce (struktury) a procesů, uvedených v tomto dokumentu, jak je zobrazeno na obrázku 1. Tyto součásti mohou již v rámci organizace plně nebo částečně existovat, nicméně mohou být zapotřebí úpravy nebo zlepšení v tom smyslu, aby řízení rizik bylo účinné, efektivní a konzistentní.

Introduction

This document is for use by people who create and protect value in organizations by managing risks, making decisions, setting and achieving objectives and improving performance.
Organizations of all types and sizes face external and internal factors and influences that make it uncertain whether they will achieve their objectives.
Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions.

Managing risk is part of governance and leadership, and is fundamental to how the organization is managed at all levels. It contributes to the improvement of management systems.
Managing risk is part of all activities associated with an organization and includes interaction with stakeholders.

Managing risk considers the external and internal context of the organization, including human behaviour and cultural factors.

Managing risk is based on the principles, framework and process outlined in this document, as illustrated in Figure 1. These components might already exist in full or in part within the organization, however, they might need to be adapted or improved so that managing risk is efficient, effective and consistent.


Obrázek 1 – Zásady, rámec a proces

Figure 1 – Principles, framework and process

1 Předmět normy

Tento dokument poskytuje směrnice pro řízení rizik, kterým jsou organizace vystaveny. Aplikování těchto směrnic může být přizpůsobeno pro jakoukoli organizaci a její kontext.

Tento dokument poskytuje společný přístup pro řízení jakéhokoliv typu rizika a není specifický ani pro průmysl, ani pro sektory.

Tento dokument lze využívat po celou dobu života organizace a může se použít na jakoukoliv činnost, včetně rozhodování na všech úrovních.

1 Scope

This document provides guidelines on managing risk faced by organizations. The application of these guidelines can be customized to any organization and its context.

This document provides a common approach to managing any type of risk and is not industry or sector specific.

This document can be used throughout the life of the organization and can be applied to any activity, including decision-making at all levels.