SLOVENSKI STANDARD

SIST ISO 31000

maj 2018

Obvladovanje tveganja – Smernice

Risk management – Guidelines

Management du risque – Lignes directrices

ICS 03.100.01

Referenčna oznaka
SIST ISO 31000:2018 (en,sl)

Nadaljevanje na straneh 2 do 32

NACIONALNI UVOD

Standard SIST ISO 31000 (sl, en), Obvladovanje tveganja – Smernice, 2018, ima status slovenskega standarda in je enakovreden mednarodnemu standardu ISO 31000, Risk management – Guidelines, 2018.

Ta standard nadomešča SIST ISO 31000:2011.

NACIONALNI PREDGOVOR

Mednarodni standard ISO 31000:2018 je pripravil tehnični odbor ISO/TC 262 Obvladovanje tveganja. Slovenski standard SIST ISO 31000:2018 je prevod angleškega besedila mednarodnega standarda ISO 31000:2018. V primeru spora glede besedila slovenskega prevoda v tem standardu je odločilen izvirni mednarodni standard v angleškem jeziku. Slovensko-angleško izdajo standarda je pripravil SIST/TC VZK Vodenje in zagotavljanje kakovosti.

Odločitev za izdajo tega standarda je dne 26. marca 2018 sprejel SIST/TC VZK Vodenje in zagotavljanje kakovosti.

ZVEZE S STANDARDI

Ta dokument ne vsebuje zvez s standardi.

OSNOVA ZA IZDAJO STANDARDA

– privzem standarda ISO 31000:2018

PREDHODNA IZDAJA

– SIST ISO 31000:2011, Obvladovanje tveganja – Načela in smernice

OPOMBE

– Povsod, kjer se v besedilu standarda uporablja izraz "mednarodni standard", v SIST ISO 31000:2018 to pomeni "slovenski standard".

– Nacionalni uvod in nacionalni predgovor nista sestavni del standarda.

VSEBINA **Stran**

CONTENTS **Page**

Predgovor

ISO (Mednarodna organizacija za standardizacijo) je svetovna zveza nacionalnih organov za standarde (članov ISO). Mednarodne standarde navadno pripravljajo tehnični odbori ISO. Vsak član, ki želi delovati na določenem področju, za katerega je bil ustanovljen tehnični odbor, ima pravico biti zastopan v tem odboru. Pri delu sodelujejo tudi mednarodne vladne in nevladne organizacije, povezane z ISO. ISO v vseh zadevah, ki so povezane s standardizacijo na področju elektrotehnike, tesno sodeluje z Mednarodno elektrotehniško komisijo (IEC).

Postopki, uporabljeni pri razvoju tega dokumenta, in postopki, predvideni za njegovo nadaljnje vzdrževanje, so opisani v Direktivah ISO/IEC, 1. del. Posebna pozornost naj se nameni različnim kriterijem odobritve, potrebnim za različne vrste dokumentov ISO. Ta dokument je bil pripravljen v skladu z uredniškimi pravili Direktiv ISO/IEC, 2. del (glej www.iso.org/directives).

Opozoriti je treba na možnost, da je lahko nekaj elementov tega dokumenta predmet patentnih pravic. ISO ne prevzema odgovornosti za identifikacijo katerihkoli ali vseh takih patentnih pravic. Podrobnosti o morebitnih patentnih pravicah, identificiranih med pripravo tega dokumenta, bodo navedene v uvodu in/ali na seznamu patentnih izjav, ki jih je prejela organizacija ISO (glej www.iso.org/patents).

Morebitna trgovska imena, uporabljena v tem dokumentu, so informacije za uporabnike in ne pomenijo podpore blagovni znamki.

Za razlago prostovoljne narave standardov, pomena specifičnih pojmov in izrazov ISO, povezanih z ugotavljanjem skladnosti, ter informacij o tem, kako ISO spoštuje načela Mednarodne trgovinske organizacije (WTO) v Tehničnih ovirah pri trgovanju (TBT), glej naslednji naslov URL: www.iso.org/foreword.html.

Ta dokument je pripravil tehnični odbor ISO/TC 262 *Obvladovanje tveganja*.

Ta druga izdaja razveljavlja in nadomešča prvo izdajo (ISO 31000:2009), ki je bila tehnično revidirana.

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.html.

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.

Glavne spremembe glede na predhodno različico so naslednje:

- prenovljena načela obvladovanja tveganja, ki so ključna merila za njegovo uspešnost,
- poudarjanje voditeljstva najvišjega vodstva in vključevanja obvladovanja tveganja, začenši z vodenjem organizacije,
- večji poudarek na ponavljajoči se naravi obvladovanja tveganja, pri čemer lahko nove izkušnje, znanje in analize vodijo do revizije elementov procesa, ukrepov in ukrepov za obvladovanje tveganja na posamezni stopnji procesa,
- poenostavitev vsebine z večjo osredotočenostjo na ohranjanju modela odprtega sistema, ki ustreza več potrebam in kontekstom.

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.

Uvod

Ta dokument je pripravljen, da ga uporabljajo osebe, ki z obvladovanjem tveganj, sprejemanjem odločitev, postavljanjem in doseganjem ciljev ter izboljšanjem delovanja ustvarjajo in varujejo vrednost v organizacijah.

Organizacije vseh vrst in velikosti se soočajo z zunanjimi in notranjimi dejavniki ter vplivi, ki jih postavljajo v negotovost, ali bodo dosegle svoje cilje.

Obvladovanje tveganja je ponavljajoč se proces in organizacijam pomaga pri vzpostavljanju strategije, doseganju ciljev in sprejemanju informiranih odločitev.

Obvladovanje tveganja je del vodenja in voditeljstva ter predstavlja podlago za vodenje organizacije na vseh ravneh. Prispeva k izboljšanju sistemov vodenja.

Obvladovanje tveganja je del vseh aktivnosti, povezanih z organizacijo, in vključuje interakcijo z deležniki.

Obvladovanje tveganja upošteva zunanji in notranji kontekst organizacije, vključno s človeškim vedenjem in kulturnimi dejavniki.

Obvladovanje tveganja temelji na načelih, okviru in procesu, opisanih v tem dokumentu, kot prikazuje slika 1. Te komponente morda že obstajajo v organizaciji v celoti ali deloma, vendar jih je morda treba prilagoditi ali izboljšati, tako da je obvladovanje tveganja učinkovito, uspešno in konsistentno.

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.

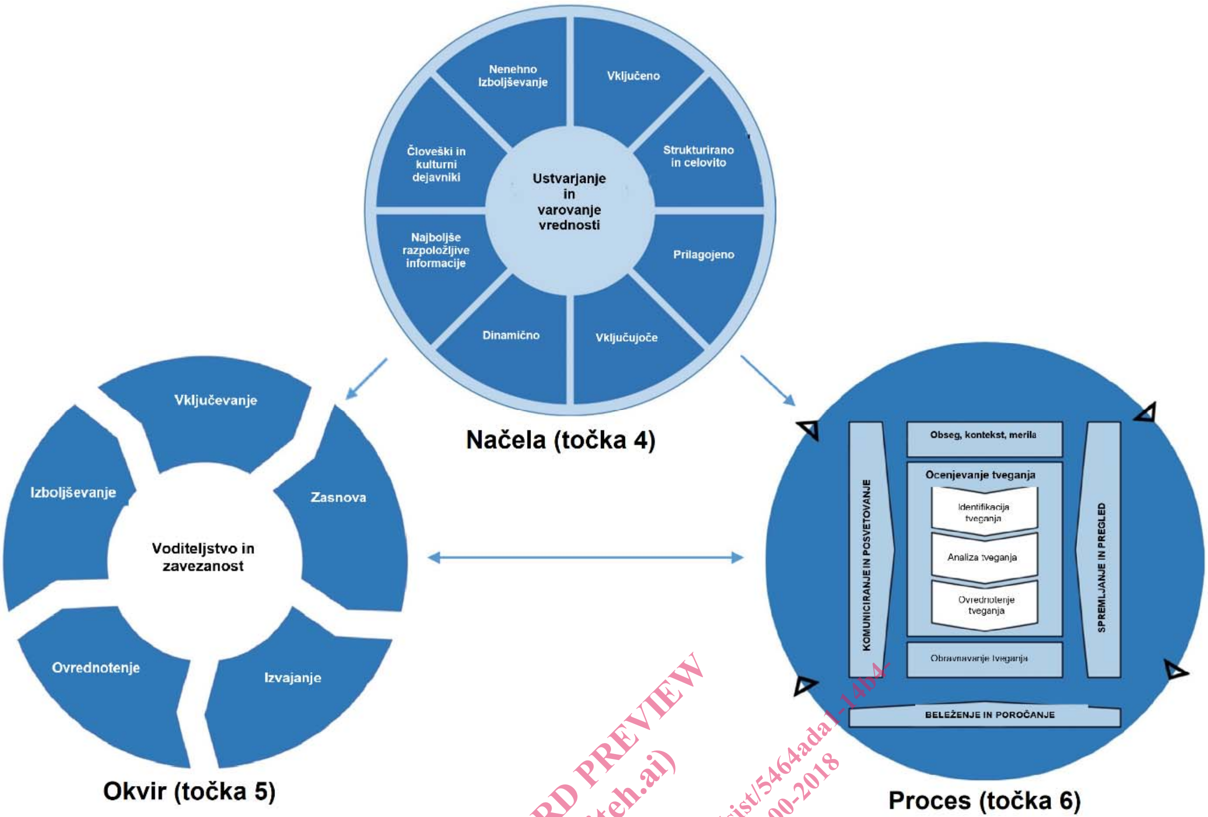
Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions.

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.



Slika 1: Načela, okvir in proces

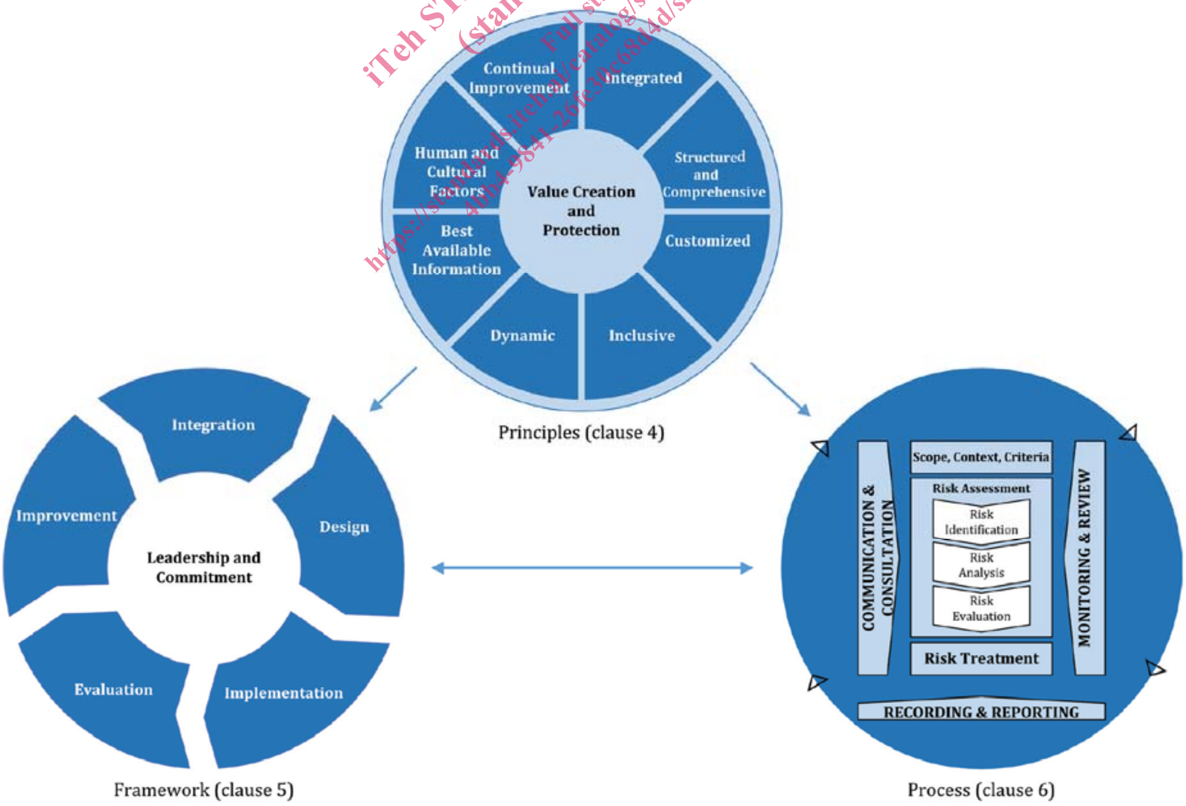


Figure 1 – Principles, framework and process

Obvladovanje tveganja – Smernice

Uvod

1 Področje uporabe

Ta dokument zagotavlja smernice o obvladovanju tveganja, s katerim se soočajo organizacije. Uporabo teh smernic je mogoče prilagoditi vsaki organizaciji in njenemu kontekstu.

Ta dokument zagotavlja splošni pristop k obvladovanju vseh vrst tveganja in ni specifičen za neko industrijo ali sektor.

Ta dokument se lahko uporablja v celotnem življenju organizacije in za katerokoli aktivnost, vključno s sprejemanjem odločitev na vseh ravneh.

2 Zveze s standardi

Ta dokument ne vsebuje zvez s standardi.

3 Izrazi in definicije

V tem dokumentu se uporabljajo naslednji izrazi in definicije.

ISO in IEC vzdržujeta terminološke zbirke podatkov za uporabo v standardizaciji na naslednjih naslovih:

- platforma za brskanje po spletu ISO: dostopna na http://www.iso.org/obp
- IEC Electropedia: dostopna na http://www.electropedia.org

3.1
tveganje
vpliv negotovosti na doseganje ciljev

OPOMBA 1: Vpliv je odstopanje od pričakovanega. Lahko je pozitiven, negativen ali oboje ter se lahko nanaša na priložnosti in grožnje, jih ustvarja ali jih povzroči.

OPOMBA 2: Cilji imajo lahko različne vidike in kategorije ter se lahko nanašajo na različne ravni.

OPOMBA 3: Tveganje je navadno izraženo v obliki **virov tveganja** (3.4), **potencialnih dogodkov** (3.5), njihovih **posledic** (3.6) in njihove **verjetnosti** (3.7).

3.2
obvladovanje tveganja
usklajene aktivnosti za usmerjanje in nadzorovanje organizacije v zvezi s **tveganjem** (3.1)

Risk management – Guidelines

Introduction

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.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at http://www.iso.org/obp
- IEC Electropedia: available at http:// www.electropedia.org

3.1
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of **risk sources** (3.4), **potential events** (3.5), their **consequences** (3.6) and their **likelihood** (3.7).

3.2
risk management
coordinated activities to direct and control an organization with regard to **risk** (3.1)

3.3
deležnik
oseba ali organizacija, ki lahko vpliva na odločitev ali aktivnost ali na katero odločitev ali aktivnost vpliva ali ji daje občutek, da vpliva nanjo

OPOMBA 1: Namesto izraza "deležnik" se lahko uporablja izraz "zainteresirana stran".

3.4
vir tveganja
element, ki je sam ali v kombinaciji z drugimi elementi sposoben povzročiti **tveganje** (3.1)

3.5
dogodek
pojav ali sprememba določenega spleta okoliščin

OPOMBA 1: Dogodek lahko zajema enega ali več pojavov ter ima lahko več vzrokov in več **posledic** (3.6).

OPOMBA 2: Dogodek je lahko tudi nekaj, kar je pričakovano, a se ne zgodi, ali nekaj, kar ni pričakovano, a se zgodi.

OPOMBA 3: Dogodek je lahko vir tveganja.

3.6
posledica
izid nekega **dogodka** (3.5), ki vpliva na cilje

OPOMBA 1: Posledica je lahko gotova ali negotova in ima lahko pozitivne ali negativne neposredne ali posredne vplive na cilje.

OPOMBA 2: Posledice se lahko izražajo kakovostno ali količinsko.

OPOMBA 3: Vsaka posledica se lahko stopnjuje s kaskadnimi in kumulativnimi vplivi.

3.7
verjetnost
možnost, da se bo nekaj zgodilo

OPOMBA 1: V terminologiji **obvladovanja tveganja** (3.2) se beseda "verjetnost" uporablja za označevanje možnosti, da se bo nekaj zgodilo, ki se lahko določi, izmeri ali ugotovi objektivno ali subjektivno, kakovostno ali količinsko ter opiše s pomočjo splošnih izrazov ali matematično (kot verjetnost ali pogostnost v danem časovnem obdobju).

OPOMBA 2: Angleški izraz "likelihood" v nekaterih jezikih nima neposredne ustreznice, namesto njega se pogosto uporablja ustreznica za izraz "probability". V angleščini pa se "probability" pogosto ožje razlaga kot matematični izraz.

3.3
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Note 1 to entry: The term "interested party" can be used as an alternative to "stakeholder".

3.4
risk source
element which alone or in combination has the potential to give rise to **risk** (3.1)

3.5
event
occurrence or change of a particular set of circumstances

Note 1 to entry: An event can have one or more occurrences, and can have several causes and several **consequences** (3.6).

Note 2 to entry: An event can also be something that is expected which does not happen, or something that is not expected which does happen.

Note 3 to entry: An event can be a risk source.

3.6
consequence
outcome of an **event** (3.5) affecting objectives

Note 1 to entry: A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

Note 2 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 3 to entry: Any consequence can escalate through cascading and cumulative effects.

3.7
likelihood
chance of something happening

Note 1 to entry: In **risk management** (3.2) terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is

Zato se v terminologiji obvladovanja tveganja "likelihood« uporablja z namenom, da bi imel enako širšo razlago, kot ga ima izraz "probability" v številnih jezikih, razen v angleškem.

often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

3.8
ukrep za obvladovanje tveganja
ukrep, ki ohranja in/ali spreminja **tveganje** (3.1)

OPOMBA 1: Ukrepi za obvladovanje tveganja med drugim vključujejo vsak proces, politiko, napravo, prakso ali druge pogoje in/ali ukrepe, ki ohranjajo in/ali spremenijo tveganje.

OPOMBA 2: Ukrepi za obvladovanje tveganja mogoče ne bodo vedno imeli nameravanega ali pričakovanega spreminjajočega učinka.

3.8
control
measure that maintains and/or modifies **risk** (3.1)

Note 1 to entry: Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

4 Načela

Namen obvladovanja tveganja je ustvarjati in varovati vrednost. Izboljšuje delovanje, spodbuja inovativnost in podpira doseganje ciljev.

Načela, zapisana na sliki 2, podajajo napotke za značilnosti uspešnega in učinkovitega obvladovanja tveganja, sporočanje njegove vrednosti in razlago njegovega namena. Načela so temelj za obvladovanje tveganja in naj se upoštevajo ob vzpostavljanju okvira in procesov za obvladovanje tveganja v organizaciji. Ta načela naj organizaciji omogočajo obvladovati vplive negotovosti na doseganje ciljev.

4 Principles

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives.

The principles outlined in Figure 2 provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. The principles are the foundation for managing risk and should be considered when establishing the organization's risk management framework and processes. These principles should enable an organization to manage the effects of uncertainty on its objectives.