RISKIJUHTIMINE
Põhimõtted ja juhised

Risk management
Principles and guidelines

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

Käesolev Eesti standard EVS-ISO 31000:2010 "Riskijuhtimine. Põhimõtted ja juhised" sisaldab rahvusvahelise standardi ISO 31000:2009 "Risk management -- Principles and guidelines" identset ingliskeelset teksti.	This Estonian Standard EVS-ISO 31000:2010 consists of the identical English text of the International Standard ISO 31000:2009 "Risk management -- Principles and guidelines"
Standard EVS-ISO 31000:2010 on kinnitatud Eesti Standardikeskuse 31.08.2010 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.	This standard is ratified with the order of Estonian Centre for Standardisation dated 31.08.2010 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from Estonian Centre for Standardisation.

Käsitlusala

Käesolev rahvusvaheline standard sätestab riskijuhtimise põhimõtted ja üldised juhised.

Käesolevat rahvusvahelist standardit võib kasutada avaliku sektori, era- või ühiskondlik organisatsioon, ühing, grupp või eraisik. Seetõttu ei ole see rahvusvaheline standard ühegi tööstusharu või sektori spetsiifiline.

MÄRKUS Mugavuse mõttes on kõigi käesoleva rahvusvahelise standardi erinevate kasutajate osas viidatud üldisele mõistele – "organisatsioon".

Käesolev rahvusvaheline standard võib olla rakendatud kogu organisatsiooni eluea jooksul laiale tegevusalade ringile, sealhulgas strateegiad ja otsused, talitlused, protsessid, ülesanded, projektid, tooted, teenused ja varad.

Käesolev rahvusvaheline standard võib olla rakendatud igale riskitüübile sõltumata tema loomusest ja sellest, kas tema tagajärjed on positiivsed või negatiivsed.

Ehkki käesolev rahvusvaheline standard sätestab üldised juhised, ei ole selle eesmärgiks soosida organisatsioonides ühetaolist riskijuhtimist. Riskijuhtimise kavandamise ja elluviimise plaanid ja raamstruktuurid peavad arvesse võtma erinevaid spetsiifilise organisatsiooni vajadusi, tema eripäraseid eesmärke, konteksti, struktuuri, talitlusi, protsesse, ülesandeid, projekte, tooteid, teenuseid või varasid ja kasutatavat praktikat.

Käesolev rahvusvaheline standard on mõeldud kasutamiseks olemasolevates ja tulevikus koostatavates standardites riskijuhtimise protsesside ühtlustamisel. See loob ühtse lähenemise nende standardite toetuseks, mis käsitlevad spetsiifilisi riske ja/või sektoreid ja ei asenda neid standardeid.

Käesolev rahvusvaheline standard ei ole mõeldud sertifitseerimise alusena.

ICS 03.100.01 Ettevõtte organiseerimine ja juhtimine üldiselt

Contents

Page

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.

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 mandatory and voluntary 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:

a) those responsible for developing risk management policy within their organization;

b) those accountable for ensuring that risk is effectively managed within the organization as a whole or within a specific area, project or activity;

c) those who need to evaluate an organization's effectiveness in managing risk; and

d) 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.

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.

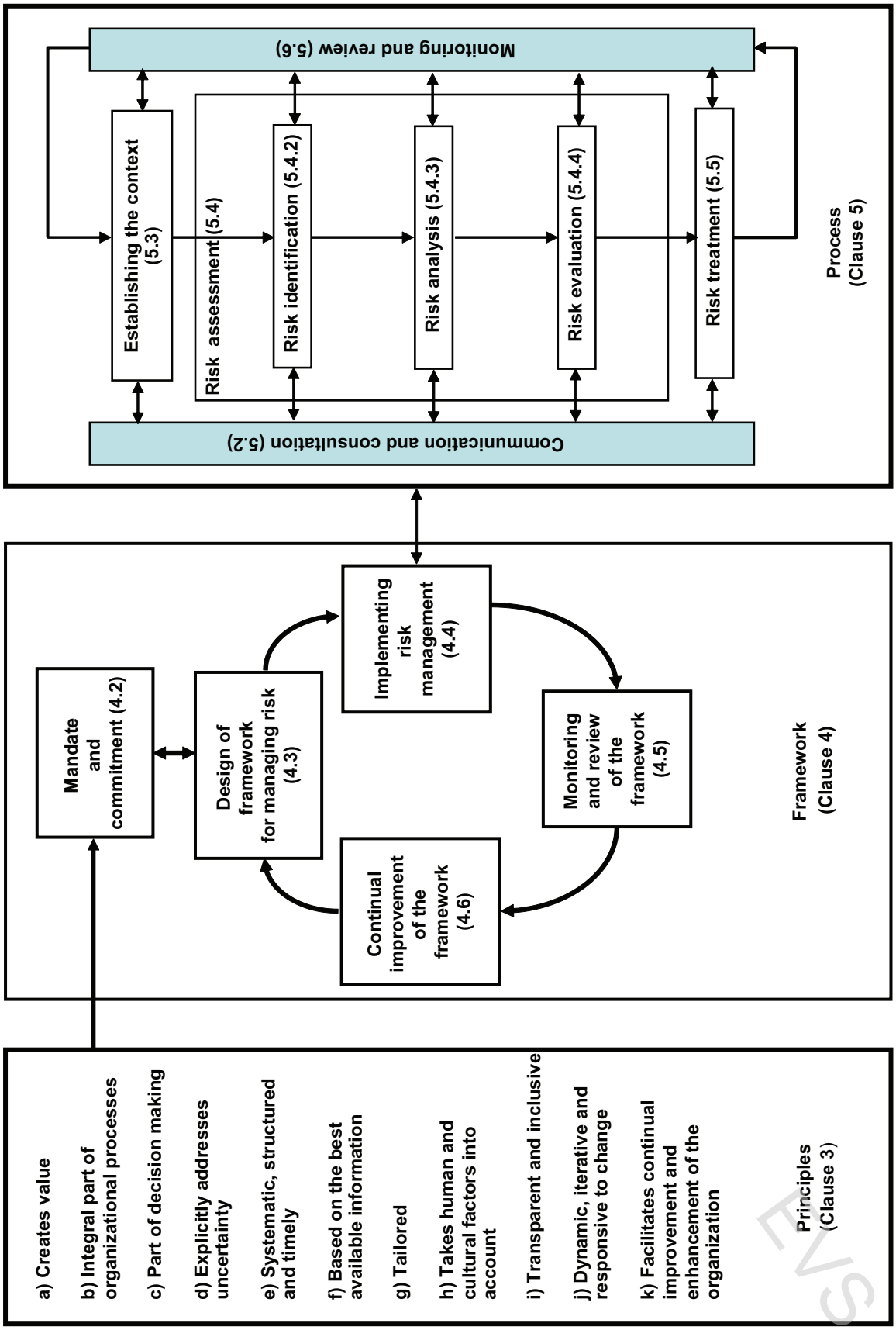

Figure 1 — Relationships between the risk management principles, framework and process

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.

2 Terms and definitions

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

2.1
risk
effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected — positive and/or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3 Risk is often characterized by reference to potential **events** (2.17) and **consequences** (2.18), or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** (2.19) of occurrence.