EESTI STANDARD EVS-ISO 31000:2010

Avaldatud eesti keeles: september 2010
Jõustunud Eesti standardina: september 2010

# RISKIJUHTIMINE
# Põhimõtted ja juhised

# Risk management
# Principles and guidelines

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

## EESTI STANDARDI EESSÕNA

Käesolev Eesti standard:

– on rahvusvahelise standardi ISO 31000:2009 “Risk management – Principles and guidelines” inglisekeelse teksti identne tõlge eesti keelde ning tõlgendamise erimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest,

– on kinnitatud Eesti Standardikeskuse 31.08.2010 käskkirjaga nr 170,

– jõustub sellekohase teate avaldamisel EVS Teataja 2010. aasta septembrikuu numbris.

Standardi tõlkis ja ekspertiisi teostas Kvaleks OÜ, käesoleva standardi on heaks kiitnud tehniline komitee EVS/TK 33 “Juhtimissüsteemid”.

Standardi kavandi kohta esitasid arvamusi Elcoteq Tallinn ja TJO Konsultatsioonid esindajad. Saadud arvamuste põhjal koostati kavandi lõppredaktsioon.

Standardi tõlke koostamisettepaneku esitas EVS/TK 33, standardi tõlkimist korraldas Eesti Standardikeskus ning rahastas Majandus- ja Kommunikatsiooniministeerium.

**Käesolev standard on eestikeelne [et] versioon rahvusvahelisest standardist ISO 31000:2009. Teksti tõlke avaldas Eesti Standardikeskus ja see omab sama staatust ametlike keelte versioonidega.**

**This standard is the Estonian [et] version of the International Standard ISO 31000:2009. It was translated by Estonian Centre for Standardisation. It has the same status as the official versions.**

See dokument on EVS-i poolt loodud eelvaade

ICS 03.100.01 Ettevõtte organiseerimine ja juhtimine üldiselt
Võtmesõnad: riskijuhtimine, riskihindamine, riskikäsitlus
Hinnagrupp M

**Standardite reprodutseerimis- ja levitamisõigus kuulub Eesti Standardikeskusele**

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse poolt antud kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, palun võtke ühendust Eesti Standardikeskusega:
Aru 10, 10317 Tallinn, Eesti; www.evs.ee; telefon: 605 5050; e-post: info@evs.ee

## SISUKORD



See dokument on EVS-i poolt loodud eelvaade

## EESSÕNA

ISO (Rahvusvaheline Standardiorganisatsioon – International Organization for Standardization) on ülemaailmne rahvuslike standardimisorganisatsioonide (ISO rahvuslike liikmesorganisatsioonide) föderatsioon. Tavaliselt tegelevad rahvusvahelise standardi ettevalmistamisega ISO tehnilised komiteed. Kõigil rahvuslikel liikmesorganisatsioonidel, kes on mingi tehnilise komitee pädevusse kuuluvast valdkonnast huvitatud, on õigus osa võtta selle komitee tegevusest. Selles töös osalevad käsikäes ISO-ga ka rahvusvahelised, riiklikud ja valitsusvälised organisatsioonid. Kõikides elektrotehnika standardimist puudutavates küsimustes teeb ISO tihedat koostööd Rahvusvahelise Elektrotehnikakomisjoniga (IEC).

Rahvusvahelised standardid kavandatakse vastavalt ISO/IEC direktiivide 2. osas esitatud reeglitele.

Tehniliste komiteede peamine ülesanne on koostada rahvusvahelisi standardeid. Tehnilistes komiteedes vastuvõetud rahvusvahelised standardikavandid saadetakse hääletamiseks rahvuslikele liikmesorganisatsioonidele. Avaldamine rahvusvahelise standardina nõuab heakskiitu vähemalt 75% hääletanud rahvuslikelt liikmesorganisatsioonidelt.

Tuleb pöörata tähelepanu võimalusele, et mõned selle rahvusvahelise standardi elemendid võivad olla patendiõiguse objektiks. ISO ei ole kohustatud mingeid või kõiki selliseid patendiõigusi välja selgitama.

ISO 31000 valmistas ette ISO Tehnilise Juhtimise Nõukogu riskihalduse töögrupp.

See dokument on EVS-i poolt loodud eelvaade

## SISSEJUHATUS

Mistahes liiki ja suurusega organisatsioonid puutuvad kokku nii sisemiste kui väliste tegurite ja mõjutustega, mis teeb ebaselgeks, kas ja millal nad oma eesmärgid saavutavad. Sellist organisatsiooni eesmärkide suhtes esinevat määramatust nimetatakse “riskiks”.

Kõik organisatsiooni tegevused on seotud riskidega. Organisatsioonides juhitakse riske neid tuvastades, analüüsides ning tehes kindlaks, kas riski tuleks muuta tema käsitlemisega nii, et rahuldada oma riskikriteeriume. Kogu selle protsessi ajal nad suhtlevad ja peavad nõu huvipooltega, jälgivad ja vaatavad üle riski ning riski muutva ohje, et ei oleks vaja edasist riskikäsitlust. Käesolev rahvusvaheline standard kirjeldab detailselt kogu seda süstemaatilist ja loogilist protsessi.

Kuigi kõik organisatsioonid juhivad riske teatud astmeni, kehtestab käesolev rahvusvaheline standard hulga põhimõtteid, mida tuleb rakendada selleks, et riskijuhtimine[1] oleks mõjus. Käesolev rahvusvaheline standard soovitab organisatsioonidel välja töötada, ellu viia ja pidevalt parendada raamstruktuuri, mille eesmärgiks on integreerida riskijuhtimise protsess organisatsiooni üldisesse haldamisse[2], strateegiasse ja plaanimisse, juhtimisse, aruandluse protsessidesse, poliitikatesse, väärtustesse ja kultuuri.

Riskijuhtimist saab rakendada nii terves organisatsioonis, tema paljudes valdkondades ja erinevatel tasemetel, igal ajahetkel kui ka spetsiifiliste funktsioonide, projektide ja tegevuste juures.

Ehkki riskijuhtimise praktikat on pikka aega ja paljudes sektorites arendatud selleks, et rahuldada mitmesuguseid vajadusi, võib kindlas raamistikus olev järjekindlate protsesside rakendamine aidata tagada, et riskid on hallatud kogu organisatsioonis mõjusalt, tõhusalt ja selgelt. Käesolevas rahvusvahelises standardis kirjeldatud üldine lähenemine annab põhimõtted ja juhised mistahes riski haldamiseks süstemaatilisel, läbipaistval ja usaldusväärsel viisil ning mistahes tegevusulatuses ja kontekstis.

Iga riskijuhtimise spetsiifiline sektor või rakendus toob kaasa selle individuaalsed vajadused, osalised, arusaamad ja kriteeriumid. Seega, peamine käesolevat rahvusvahelist standardit iseloomustav joon on “konteksti loomise” kui tegevuse kaasamine üldise riskijuhtimisprotsessi alguses. Konteksti loomisega fikseeritakse organisatsiooni eesmärgid ja nende saavutamise keskkond, huvipooled ja riski kriteeriumide mitmekesisus – kõik need aitavad esile tuua ja hinnata organisatsiooni riskide loomust ja keerukust.

Riskijuhtimise põhimõtete vahelised suhted, raamstruktuur, milles see avaldub, ning käesolevas rahvusvahelises standardis kirjeldatud riskijuhtimisprotsess on kujutatud joonisel 1.

Organisatsioonis, kus riskijuhtimine on käesoleva rahvusvahelise standardiga vastavuses ellu viidud ja toimivana hoitud, on võimalik näiteks:

— suurendada eesmärkide saavutamise võimalikkust;

— soodustada ennetavat juhtimist;

— olla teadlik kogu organisatsiooni riskide tuvastamise ja käsitlemise vajadusest;

— parendada võimaluste ja ohtude tuvastamist;

— täita asjakohaseid õiguslikke ja normatiivseid nõudeid ja rahvusvahelisi norme;

— parendada kohustuslikku ja vabatahtlikku aruandlust;

— parendada haldamist;

[1] EE MÄRKUS: *Risk management* on tõlgitud “riskijuhtimiseks” teiste juhtimissüsteemide standardite alusel (näiteks EVS-EN ISO 9001, EVS-EN ISO 14001).

[2] EE MÄRKUS: *Governance* eestikeelse vastena on kasutatud terminit “haldus”.

See dokument on Evsi poolt loodud eelvaade

— parendada huvipoolte kindlustunnet ja usaldust;

— luua usaldusväärne baas otsuste tegemiseks ja plaanimiseks;

— parendada ohjemeetmeid;

— paigutada ja kasutada tõhusalt ressursse riskikäsitluseks;

— parendada tegevuste mõjusust ja tõhusust;

— täiustada nii tervishoiu ja ohutuse alast jõudlust kui ka keskkonnakaitset;

— parendada kadude ennetamist ja intsidentide haldamist;

— viia kaod miinimumini;

— parendada organisatsiooni õppimisharjumusi; ning

— parendada organisatsiooni paindlikkust.

Käesolev rahvusvaheline standard on ette nähtud täitma laia huvipoolte ringi vajadusi, sealhulgas:

a) need, kelle kohustus on arendada riskijuhtimispoliitikat oma organisatsioonides;

b) vastutajad, kes tagavad, et risk on mõjusalt hallatud organisatsioonis tervikuna, spetsiifilises valdkonnas, projektis või tegevuses;

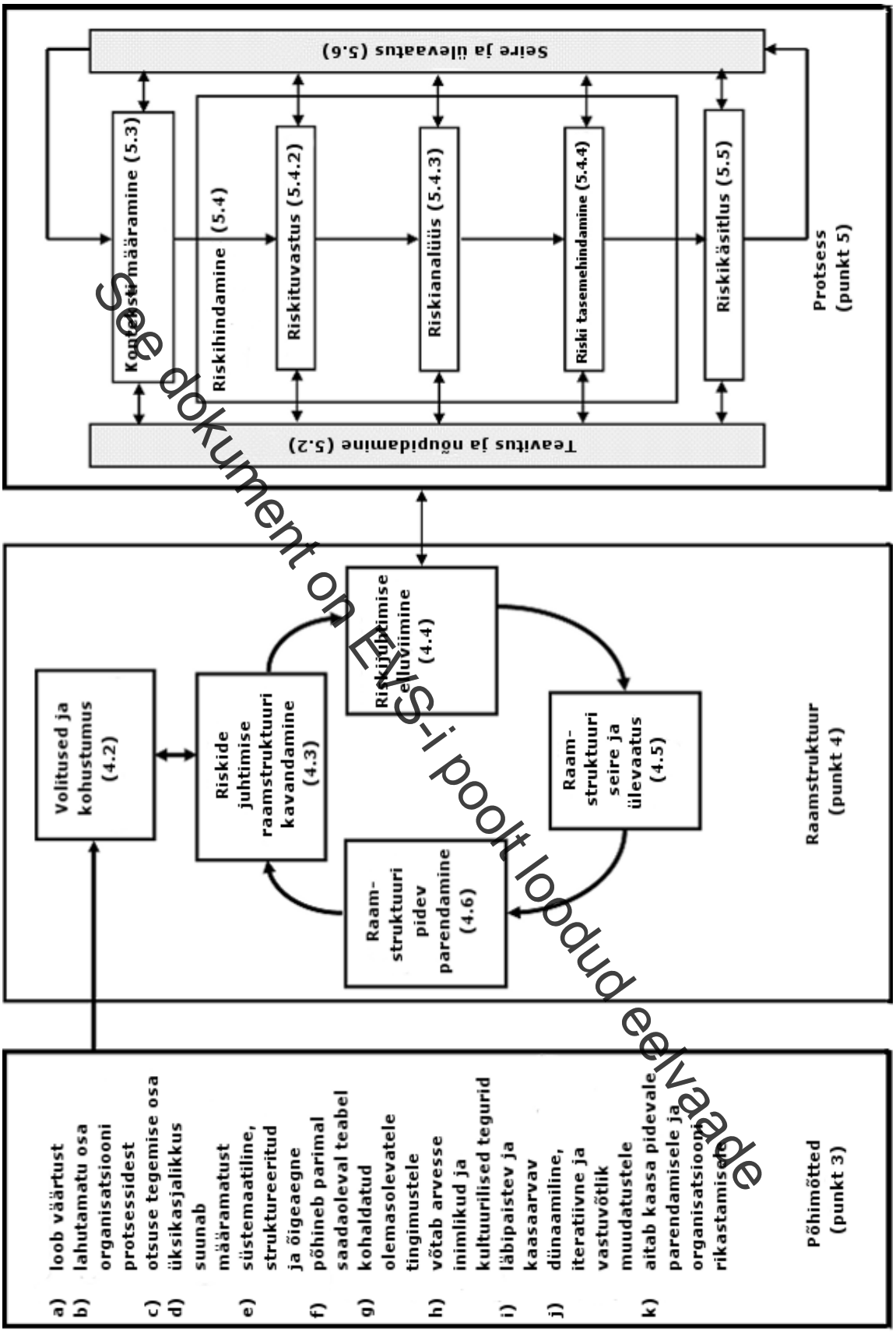
c) need, kes peavad hindama organisatsiooni riskijuhtimise mõjusust; ja

d) standardite, juhiste, protseduuride ja tavakoodeksite arendajad, kes kehtestavad tervikuna või osaliselt riskijuhtimisviisid tulenevalt nende dokumentide spetsiifikast.

Paljude organisatsioonide käibelolevad juhtimise praktikad ja protsessid sisaldavad riskijuhtimise komponente ning paljudes organisatsioonides on juba juurutatud formaalne riskijuhtimisprotsess teatud riskitüüpide või asjaolude jaoks. Sellisel juhul võidakse organisatsioonis otsustada läbi viia olemasoleva praktika ja protsesside kriitiline ülevaatus, mille käigus pööratakse erilist tähelepanu käesoleva rahvusvahelise standardi nõuetele.

Käesolevas rahvusvahelises standardis leiavad kasutust mõlemad väljendid – nii “riskijuhtimine” kui ka “riskide juhtimine”. Üldiselt viitab “riskijuhtimine” riskide tõhusa haldamise struktuurile (põhimõtted, raamstruktuur ja protsess), samal ajal kui “riskide juhtimine” viitab struktuuri kohaldamisele vaadeldava riski suhtes.

See dokument on EVS-i poolt tasuta eelvaade




**Joonis 1 — Suhted riskijuhtimise põhimõtete, raamstruktuuri ja protsessi vahel**

See dokument on EVS-i poolt loodud eelvaade

# 1 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.

# 2 TERMINID JA MÄÄRATLUSED

Käesolevas standardis kasutatakse järgmiseid termineid ja määratlusi.

**2.1**
**risk** *(risk)*
määramatuse toime eesmärkidele

MÄRKUS 1 Toime on positiivne ja/või negatiivne kõrvalekalle oodatavast.

MÄRKUS 2 Eesmärkidel võib olla eri aspekte (näiteks rahalisi, tervishoiu- ja ohutusalaseid ning keskkonnasihte) ja nad võivad kehtida eri tasemetel (näiteks strateegilisel, üleorganisatsioonilisel, projekti, toote ja protsessi tasemel).

MÄRKUS 3 Sageli iseloomustatakse riski võimalike **sündmuste** (2.17) ja **tagajärgede** (2.18) või nende kombinatsiooni kaudu.

MÄRKUS 4 Sageli iseloomustatakse riski mingi sündmuse tagajärgede (sealhulgas asjaolude muutuste) ja selle sündmuse toimumise **võimalikkuse** (2.19) kombinatsiooniga.

MÄRKUS 5 Määramatus on niisuguse teabe puudumine või vaegus, mis on seotud mingi sündmusega, selle tagajärjega või selle võimalikkusega või nende mõistmise või teadmisega.

[ISO Guide 73:2009, määratlus 1.1]

**2.2**
**riskijuhtimine** (*risk management)*
kooskõlastatud tegevused organisatsiooni suunamiseks ja ohjamiseks **riski** (2.1) suhtes

[ISO Guide 73:2009, määratlus 2.1]

See dokument on EVS-i poolt loodud eelvaade