Avaldatud eesti keeles: november 2022
Jõustunud Eesti standardina: november 2022

TURVALISUS JA KERKSUS
Turvalisuse juhtimissüsteemid
Nõuded

Security and resilience
Security management systems
Requirements
(ISO 28000:2022, identical)

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO 28000:2022 ingliskeelse teksti sisu poolest identne tõlge eesti keelde ja sellel on sama staatus mis ümbertrüki meetodil vastu võetud originaalversioonil. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina inglise keeles novembris 2022;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2022. aasta novembrikuu numbris.

Standardi tõlke koostamise ettepaneku on esitanud tehniline komitee EVS/TK 33 „Juhtimissüsteemid ja vastavushindamine“, standardi tõlkimist on korraldanud Eesti Standardimis- ja Akrediteerimiskeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

Standardi on tõlkinud OÜ TJO Konsultatsioonid, standardi on heaks kiitnud EVS/TK 33.

See standard on rahvusvahelise standardi ISO 28000:2022 eestikeelne [et] versioon. Teksti tõlke on avaldanud Eesti Standardimis- ja Akrediteerimiskeskus ning sellel on sama staatus ametlike keelte versioonidega.

This standard is the Estonian [et] version of the International Standard ISO 28000:2022. It was translated by the Estonian Centre for Standardisation and Accreditation. It has the same status as the official versions.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 03.100.01; 03.100.70

SISUKORD

EESSÕNA

ISO (International Organization for Standardization) on ülemaailmne rahvuslike standardimis-organisatsioonide (ISO rahvuslike liikmesorganisatsioonide) föderatsioon. Tavaliselt tegelevad rahvusvahelise standardi koostamisega ISO tehnilised komiteed. Kõigil rahvuslikel liikmes-organisatsioonidel, kes on mingi tehnilise komitee pädevusse kuuluvast valdkonnast huvitatud, on õigus selle komitee tegevusest osa võtta. Selles töös osalevad käsikäes ISO-ga ka rahvusvahelised ja riiklikud organisatsioonid ning vabaühendused. Kõigis elektrotehnika standardimist puudutavates küsimustes teeb ISO tihedat koostööd Rahvusvahelise Elektrotehnikakomisjoniga (IEC).

Selle dokumendi väljatöötamiseks kasutatud ja edasiseks haldamiseks mõeldud protseduurid on kirjeldatud ISO/IEC direktiivide 1. osas. Eriti tuleb silmas pidada eri heakskiidukriteeriumeid, mis on eri liiki ISO dokumentide puhul vajalikud. See dokument on kavandatud ISO/IEC direktiivide 2. osas esitatud toimetamisreeglite kohaselt (vt www.iso.org/directives).

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse objekt. ISO ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest. Dokumendi väljatöötamise jooksul väljaselgitatud või selgunud patendiõiguste üksikasjad on esitatud peatükis „Sissejuhatus“ ja/või ISO-le saadetud patentide deklaratsioonide loetelus (vt www.iso.org/patents).

Mis tahes selles dokumendis kasutatud äriline käibenimi on kasutajate abistamise eesmärgil esitatud teave ja ei kujuta endast toetusavaldust.

Selgitused standardite vabatahtliku kasutuse ja vastavushindamisega seotud ISO eriomaste terminite ja väljendite kohta ning teave selle kohta, kuidas ISO järgib WTO tehniliste kaubandustõkete lepingus sätestatud põhimõtteid, on esitatud järgmisel aadressil: www.iso.org/iso/foreword.html.

Selle dokumendi on koostanud tehniline komitee ISO/TC 292 „Security and resilience“.

Teine väljaanne tühistab ja asendab esimest väljaannet (ISO 28000:2007), mis on tehniliselt üle vaadatud, kuid säilitab olemasolevad nõuded, et tagada järjepidevus eelmist väljaannet kasutavatele organisatsioonidele. Peamised muudatused on järgmised:

— peatükki 4 on lisatud soovitused põhimõtete kohta, et tagada parem kooskõla standardiga ISO 31000;

— peatükki 8 on lisatud soovitused parema kooskõla tagamiseks standardiga ISO 22301, mis hõlbustab lõimimist, sealhulgas

  — turvastrateegiad, protseduurid, protsessid ja käsitlusmeetmed;

  — turvaplaanid.

Igasugune tagasiside või küsimused selle dokumendi kohta tuleks suunata dokumendi kasutaja rahvuslikule standardimisorganisatsioonile. Täielik loetelu nende organisatsioonide kohta on leitav veebilehelt www.iso.org/members.html.

SISSEJUHATUS

Enamik organisatsioone kogeb julgeoleku keskkonnas kasvavat ebakindlust ja muutlikkust. Selle tulemusena seisavad nad silmitsi turvaprobleemidega, mis mõjutavad nende eesmärke ja mida nad soovivad oma juhtimissüsteemis süstemaatiliselt käsitleda. Ametlik lähenemine turvalisuse juhtimisele võib otseselt kaasa aidata organisatsiooni ärisuutlikkusele ja usaldusväärsusele.

See dokument määrab kindlaks turvalisuse juhtimissüsteemi nõuded, sealhulgas need aspektid, mis on tarneahela turvalisuse tagamise seisukohast olulised. See nõuab organisatsioonilt

— julgeoleku keskkonna hindamist, milles ta tegutseb, sealhulgas tarneahelas (sealhulgas sõltuvusi ja vastastikust sõltuvust);

— kindlaks tegemist, kas turvalisusega seotud riskide mõjusaks juhtimiseks on sisse seatud piisavad turvameetmed;

— seadusjärgsete, regulatiivsete ja vabatahtlike kohustuste, millega organisatsioon on liitunud, vastavuse juhtimist;

— turvaprotsesside ja -ohjemeetmete ühtlustamist, sealhulgas asjakohaste eelnevate ja järgnevate protsesside ning tarneahela ohjemeetmete asjus, et täita organisatsiooni eesmärke.

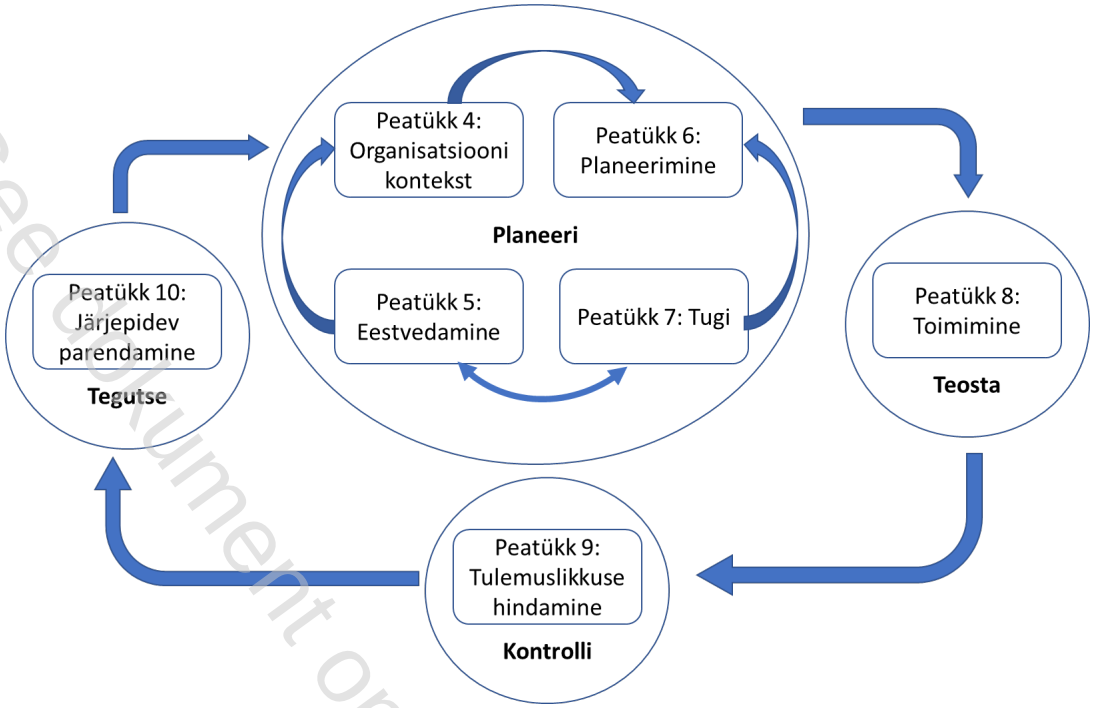
Turvalisuse juhtimine on seotud paljude ärijuhtimise aspektidega. Need hõlmavad kõiki tegevusi, mida organisatsioonid ohjavad või mõjutavad, sealhulgas, kuid mitte ainult, neid, mis mõjutavad tarneahelat. Kaalutleda tuleks kõiki tegevusi, talitusi ja toiminguid, mis mõjutavad organisatsiooni turvalisuse juhtimist, sealhulgas (kuid mitte ainult) selle tarneahelat.

Tarneahela osas tuleb arvestada, et tarneahelad on oma olemuselt dünaamilised. Seetõttu võivad mõned mitut tarneahelat haldavad organisatsioonid turvalisuse juhtimise nõuete täitmiseks eeldada, et nende tarnijad täidavad seotud turvastandardeid, mis on sellesse tarneahelasse kaasamise tingimus.

See dokument kohaldab planeeri-teosta-kontrolli-tegutse (PDCA) mudelit organisatsiooni turvalisuse juhtimissüsteemi planeerimisel, sisseseadmisel, elluviimisel, toimimisel, seiramisel, ülevaatamisel, toimivana hoidmisel ja mõjususe järjepideval parendamisel, vt tabel 1 ja joonis 1.

Tabel 1 — PDCA mudeli selgitus

Planeeri (Sea sisse)	Seadke sisse turvalisuse juhtpõhimõtted, eesmärgid, sihtväärtused, ohjemeetmed, protsessid ja protseduurid, mis on olulised turvalisuse parendamiseks, et saavutada organisatsiooni üldiste juhtpõhimõtete ja eesmärkidega kooskõlas olevad tulemused.
Teosta (Vii ellu ja kasuta)	Viige ellu ja kasutage turvalisuse juhtpõhimõtteid, ohjemeetmeid, protsesse ja protseduure.
Kontrolli (Seira ja vaata üle)	Seirake ja vaadake üle tulemuslikkust turvalisuse juhtpõhimõtete ja eesmärkide suhtes, esitage tulemused juhtkonnale ülevaatamiseks ja määrake kindlaks ning volitage parandus- ja parendustegevused.
Tegutse (Hoia toimivana ja parenda)	Hoidke toimivana ja parendage turvalisuse juhtimissüsteemi, rakendades korrigeerivaid tegevusi, lähtudes juhtkonnapoolse ülevaatuse tulemustest ning turvalisuse juhtimissüsteemi käsitlusala ning turvalisuse juhtpõhimõtete ja -eesmärkide ümberhindamisest.



Joonis 1 — Turvalisuse juhtimissüsteemile kohaldatud PDCA mudel

See tagab teatava kooskõla teiste juhtimissüsteemide standarditega, nagu ISO 9001, ISO 14001, ISO 22301, ISO/IEC 27001, ISO 45001 jne, toetades seeläbi järjekindlat ja lõimitud elluviimist ning toimimist seotud juhtimissüsteemidega.

Organisatsioonidel, kes seda soovivad, võib turvalisuse juhtimissüsteemi vastavust sellele dokumendile tõendada välis- või siseauditi protsessiga.

Taotluslikult tühjaks jäetud

1 KÄSITLUSALA

See dokument määrab kindlaks turvalisuse juhtimissüsteemi nõuded, sealhulgas tarneahelaga seotud aspektid.

See dokument kehtib igat tüüpi ja suurusega organisatsioonidele (nt äriettevõtted, valitsus- või muud riigiasutused ja mittetulundusühingud), mis kavatsevad sisse seada, ellu viia, toimivana hoida ja parendada turvalisuse juhtimissüsteemi. See pakub terviklikku ja ühtset lähenemisviisi ning pole tööstus- ega sektorispetsiifiline.

Seda dokumenti saab kasutada kogu organisatsiooni eluea jooksul ja seda saab kohaldada mis tahes tegevusele, nii sisemisele kui ka välisele, kõigil tasanditel.

2 NORMIVIITED

Allpool nimetatud dokumentidele on tekstis viidatud selliselt, et nende sisu kujutab endast kas osaliselt või tervenisti selle dokumendi nõudeid. Dateeritud viidete korral kehtib üksnes viidatud väljaanne. Dateerimata viidete korral kehtib viidatud dokumendi uusim väljaanne koos võimalike muudatustega.

ISO 22300. Security and resilience — Vocabulary

3 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse standardis ISO 22300 ning allpool esitatud termineid ja määratlusi.

ISO ja IEC hoiavad alal standardimisel kasutamiseks olevaid terminoloogilisi andmebaase järgmistel aadressidel:

— ISO veebipõhine lugemisplatvorm: kättesaadav veebilehelt https://www.iso.org/obp/;

— IEC Electropedia: kättesaadav veebilehelt https://www.electropedia.org/.

3.1
organisatsioon (*organization*)
isik või inimeste grupp, kellel on olemas talitused koos kohustuste, volituste ja suhetega oma *eesmärkide* (3.7) saavutamiseks

MÄRKUS 1 Organisatsiooni mõiste hõlmab üksikettevõtjat, äriühingut, korporatsiooni, firmat, ettevõtet, ametiasutust, partnerlust, heategevusfondi või institutsiooni või nende osa või kombinatsiooni nendest, juriidilise isikuna registreeritud või registreerimata, eraõiguslikku või avalikku, kuid ei piirne nendega.

MÄRKUS 2 Kui organisatsioon on osa suuremast olemist, viitab termin „organisatsioon“ ainult suurema olemi osale, mis jääb *turvalisuse juhtimissüsteemi* (3.5) käsitlusalasse.

3.2
huvipool (*interested party*) (eelistatud termin)
sidusgrupp (*stakeholder*) (lubatud termin)
isik või *organisatsioon* (3.1.), kes võib mõjutada, võib olla mõjutatud või tajub ennast mõjutatuna otsusest või tegevusest

3.3
tippjuhtkond (*top management*)
isik või isikute grupp, kes suunab ja ohjab *organisatsiooni* (3.1) kõrgeimal tasemel

MÄRKUS 1 Tippjuhtkonnal on võim organisatsioonisiseselt volitusi delegeerida ja ressursse jaotada.

