

Avaldatud eesti keeles: oktoober 2024
Jõustunud Eesti standardina: november 2022
Muudatus A1 jõustunud Eesti standardina: oktoober 2024

TURVALISUS JA KERKSUS
Turvalisuse juhtimissüsteemid
Nõuded

Security and resilience
Security management systems
Requirements
(ISO 28000:2022, identical
+ ISO 28000:2022/Amd 1:2024, identical)

EESTI STANDARDI EESSÕNA

See Eesti standard on

- rahvusvahelise standardi ISO 28000:2022 ja selle muudatuse Amd 1:2024 ingliskeelsete tekstide sisu poolest identne konsolideeritud tõlge eesti keelde ning sellel on sama staatus mis ümbertrüki meetodil vastu võetud originaalversioonidel. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;
- jõustunud Eesti standardina inglise keeles novembris 2022;
- eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2024. aasta oktoobrikuu 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.

Standardimuudatuse tõlkimist on korraldanud Eesti Standardimis- ja Akrediteerimiskeskus.

Standardimuudatuse on heaks kiitnud tehniline komitee EVS/TK 33 „Juhtimissüsteemid ja vastavushindamine“.

Sellesse standardisse on muudatus Amd 1 sisse viidud ja tehtud muudatused tähistatud sümbolitega  .

See standard on rahvusvahelise standardi ISO 28000:2022 ja selle muudatuse Amd 1:2024 eestikeelne [et] konsolideeritud versioon. Teksti tõlke on avaldanud Eesti Standardimis- ja Akrediteerimiskeskus ning sellel on sama staatus ametlike keelte versioonidega.

This standard is the consolidated Estonian [et] version of the International Standard ISO 28000:2022 and its Amendment Amd 1:2024. 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

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardimis- ja Akrediteerimiskeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardimis- ja Akrediteerimiskeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autoriõiguse kaitse kohta, võtke palun ühendust Eesti Standardimis- ja Akrediteerimiskeskusega: Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

SISUKORD

EESSÕNA.....	V
▣ ^{A1} MUUDATUSE AMD 1 EESSÕNA ▣ ^{A1}	V
SISSEJUHATUS.....	VII
1 KÄSITLUSALA.....	1
2 NORMIVIITED	1
3 TERMINID JA MÄÄRATLUSED.....	1
4 ORGANISATSIOONI KONTEKST	4
4.1 Organisatsiooni ja selle konteksti mõistmine	4
4.2 Huvipoolte vajaduste ja ootuste mõistmine	4
4.2.1 Üldist.....	4
4.2.2 Õigusaktide, regulatiivsed ja muud nõuded	4
4.2.3 Põhimõtted	5
4.3 Turvalisuse juhtimissüsteemi käsitusala kindlaksmääramine	6
4.4 Turvalisuse juhtimissüsteem.....	6
5 EESTVEDAMINE	6
5.1 Eestvedamine ja pühendumus	6
5.2 Turvalisuse juhtpõhimõtted.....	7
5.2.1 Turvalisuse juhtpõhimõtete sisseseadmine	7
5.2.2 Turvalisuse juhtpõhimõtete nõuded	7
5.3 Rollid, kohustused ja volitused	8
6 PLANEERIMINE	8
6.1 Riskide ja võimaluste käsitlemisele suunatud tegevused.....	8
6.1.1 Üldist.....	8
6.1.2 Turvalisusega seotud riskide kindlaksmääramine ja võimaluste tuvastamine.....	8
6.1.3 Turvalisusega seotud riskide käsitlemine ja võimaluste ärakasutamine.....	9
6.2 Turvalisuse eesmärgid ja nende saavutamise planeerimine.....	9
6.2.1 Turvalisuse eesmärkide sisseseadmine	9
6.2.2 Turvalisuse eesmärkide kindlaksmääramine	9
6.3 Muudatuste planeerimine	10
7 TUGI.....	10
7.1 Ressursid.....	10
7.2 Kompetentsus	10
7.3 Teadlikkus.....	10
7.4 Teabevahetus.....	10
7.5 Dokumenteeritud teave	11
7.5.1 Üldist.....	11
7.5.2 Dokumenteeritud teabe koostamine ja kaasajastamine.....	11
7.5.3 Dokumenteeritud teabe ohjamine.....	11
8 TOIMIMINE.....	12
8.1 Toimimise planeerimine ja ohjamine.....	12
8.2 Protsesside ja tegevuste tuvastamine	12
8.3 Riski kaalutlemine ja käsitlemine	12
8.4 Ohjemeetmed	13
8.5 Turvalisuse strateegiad, protseduurid, protsessid ja käsitusmeetmed.....	13
8.5.1 Strateegiate ja käsitusmeetmete tuvastamine ning valik	13
8.5.2 Nõuded ressurssidele.....	14
8.5.3 Käsitusmeetmete elluviimine.....	14

8.6	Turvaplaanid.....	14
8.6.1	Üldist.....	14
8.6.2	Reageerimisstruktuur.....	14
8.6.3	Hoiatamine ja teabevahetus.....	14
8.6.4	Turvaplaanide sisu.....	15
8.6.5	Taastamine.....	16
9	TULEMUSLIKKUSE HINDAMINE.....	16
9.1	Seire, mõõtmine, analüüs ja hindamine.....	16
9.2	Siseaudit.....	16
9.2.1	Üldist.....	16
9.2.2	Siseauditi programm.....	16
9.3	Juhtkonnapoolne ülevaatus.....	17
9.3.1	Üldist.....	17
9.3.2	Juhtkonnapoolse ülevaatus sisendid.....	17
9.3.3	Juhtkonnapoolse ülevaatus väljundid.....	18
10	PARENDAMINE.....	18
10.1	Järjepidev parendamine.....	18
10.2	Mittevastavus ja korrigeeriv tegevus.....	18
	Kirjandus.....	20

EESSÕNA

ISO (International Organization for Standardization) on ülemaailmne rahvuslike standardimisorganisatsioonide (ISO rahvuslike liikmesorganisatsioonide) föderatsioon. Tavaliselt tegelevad rahvusvahelise standardi koostamisega ISO tehnilised komiteed. Kõigil rahvuslikel liikmesorganisatsioonidel, 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 ärid nimed 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 kaubandustökete 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 käsitusmeetmed;
 - 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.

[A₁] MUUDATUSE AMD 1 EESSÕNA

ISO (International Organization for Standardization) on ülemaailmne rahvuslike standardimisorganisatsioonide (ISO rahvuslike liikmesorganisatsioonide) föderatsioon. Tavaliselt tegelevad rahvusvahelise standardi koostamisega ISO tehnilised komiteed. Kõigil rahvuslikel liikmesorganisatsioonidel, kes on mingi tehnilise komitee pädevusse kuuluvast valdkonnast huvitatud, on õigus selle komitee tegevusest osa võtta. Selles töös osalevad ka ISO-ga seotud rahvusvahelised 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).

ISO pöörab tähelepanu võimalusele, et selle dokumendi rakendamine võib olla seotud patendi (patentide) kasutamisega. ISO ei võta seisukohta mis tahes esitatud patendiõiguste tõendamise, kehtivuse ega rakendatavuse eest. Selle dokumendi avaldamise kuupäeva seisuga ei ole ISO saanud teateid patendi (patentide) kohta, mida võib vaja minna selle dokumendi rakendamiseks. Dokumendi kasutajaid on siiski hoiatatud, et siin esitatu ei pruugi olla uusim teave, mis võib olla saadud patendiandmebaasist (kättesaadav veebilehelt www.iso.org/patents). ISO ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest.

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.

Dokumendi on koostanud ISO Tehnikanõukogu otsuse 75/2023 kohaselt tehniline komitee ISO/TC 292 „Security and resilience“.

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 eesmärgi 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 eesmärgi.

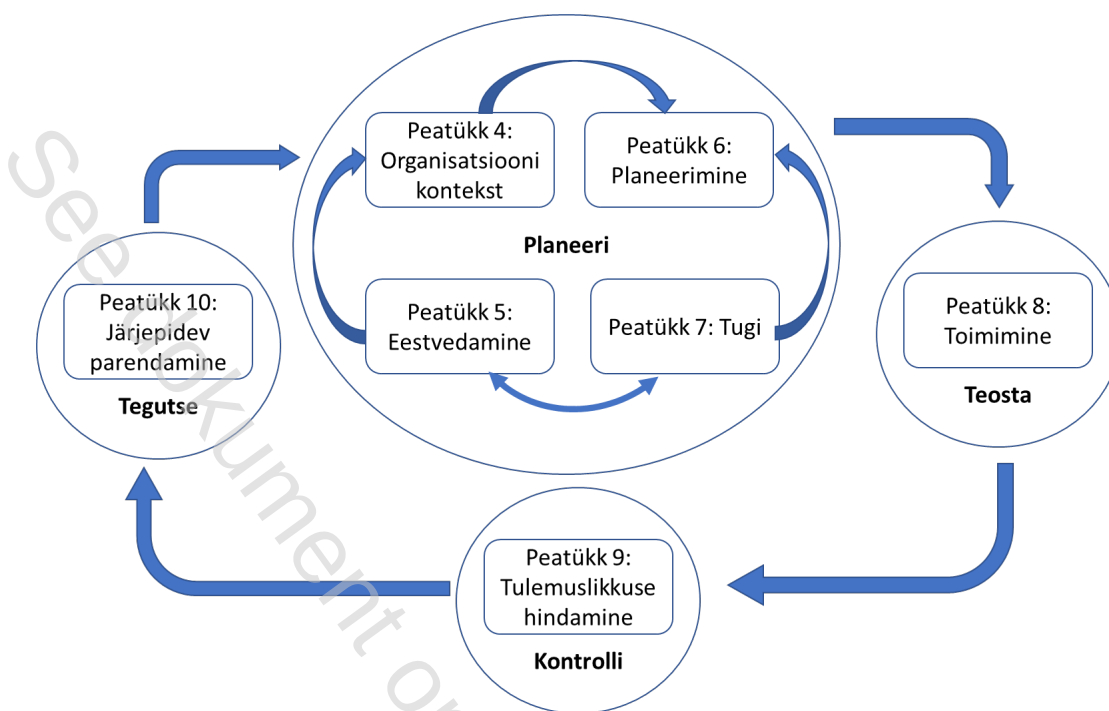
Turvalisuse juhtimine on seotud paljude ärijuhtimise aspektidega. Need hõlmavad kõiki tegevusi, mida organisatsioonid ohjavad või mõjutavad, sealhulgas, kuid mitte ainult, neid, mis mõjutavad tarneahelat. Kaalutleda tuleks kõiki tegevusi, talitusi ja toiminguid, mis mõjutavad organisatsiooni turvalisuse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

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 terveniisti 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) käsituslusalasse.

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 organisatsioonisiselt volitusi delegeerida ja ressursse jaotada.