

INFOTEHNOLOOGIA
Infotehnoloogia valitsemine organisatsioonis

Information technology
Governance of IT for the organization
(ISO/IEC 38500:2024, identical)

EESTI STANDARDI EESSÕNA

See Eesti standard on

- rahvusvahelise standardi ISO/IEC 38500:2024 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 2024;
- eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2024. aasta novembrikuu numbris.

Standardi tõlke koostamise ettepaneku on esitanud tehniline komitee EVS/TK 04 „Infotehnoloogia“, standardi tõlkimist on korraldanud Eesti Standardimis- ja Akrediteerimiskeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

Standardi on tõlkinud TepInfo OÜ, standardi on heaks kiitnud EVS/TK 04.

See standard on rahvusvahelise standardi ISO/IEC 38500:2024 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/IEC 38500:2024. 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 35.020

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.....	VI
SISSEJUHATUS.....	VII
1 KÄSITLUSALA.....	1
2 NORMIVIITED	1
3 TERMINID JA MÄÄRATLUSED.....	1
4 IT HEA VALITSEMINE.....	3
4.1 IT hea valitsemise tulemid	3
4.1.1 Ülevaade	3
4.1.2 Toimiv sooritus.....	3
4.1.3 Vastutustundlik haldamine.....	4
4.1.4 Eetiline käitumine	4
4.2 Põhimõtted, mudel ja raamstruktuur.....	5
5 IT VALITSEMISE PÕHIMÕTTED	5
5.1 Ülevaade	5
5.2 Otstarve.....	7
5.2.1 Põhimõte	7
5.2.2 Valitsemise järelmid IT kasutamisele.....	7
5.2.3 Tulemused	7
5.3 Väärtuse loomine	7
5.3.1 Põhimõte	7
5.3.2 Valitsemise järelmid IT kasutamisele.....	7
5.3.3 Tulemused	8
5.4 Strateegia	8
5.4.1 Põhimõte	8
5.4.2 Valitsemise järelmid IT kasutamisele.....	8
5.4.3 Tulemused	9
5.5 Järelevalve.....	9
5.5.1 Põhimõte	9
5.5.2 Valitsemise järelmid IT kasutamisele.....	9
5.5.3 Tulemused	10
5.6 Vastutus	10
5.6.1 Põhimõte	10
5.6.2 Valitsemise järelmid IT kasutamisele.....	10
5.6.3 Tulemused	10
5.7 Huvipoolte kaasamine	10
5.7.1 Põhimõte	10
5.7.2 Valitsemise järelmid IT kasutamisele.....	11
5.7.3 Tulemused	11
5.8 Juhtimine	11
5.8.1 Põhimõte	11
5.8.2 Valitsemise järelmid IT kasutamisele.....	11
5.8.3 Tulemused	12
5.9 Andmed ja otsused	12
5.9.1 Põhimõte	12
5.9.2 Valitsemise järelmid IT kasutamisele.....	12
5.9.3 Tulemused	13
5.10 Riskivalitsemine	13
5.10.1 Põhimõte	13
5.10.2 Valitsemise järelmid IT kasutamisele.....	13

5.10.3	Tulemused	13
5.11	Sotsiaalne vastutus.....	14
5.11.1	Põhimõte.....	14
5.11.2	Valitsemise järelmid IT kasutamisele.....	14
5.11.3	Tulemused	14
5.12	Kestev elujõulisus ja toimivus	14
5.12.1	Põhimõte.....	14
5.12.2	Valitsemise järelmid IT kasutamisele.....	15
5.12.3	Tulemused	15
6	IT VALITSEMISE MUDEL	15
6.1	Sissejuhatus.....	15
6.2	IT-tavade valitsemine.....	16
6.2.1	Kaasata huvipooled.....	16
6.2.2	Hinnata.....	16
6.2.3	Suunata.....	17
6.2.4	Seirata.....	17
6.3	IT-tava haldus.....	17
6.4	IT valitsemise raamstruktuur	17
7	IT VALITSEMISE RAAMSTRUKTUUR.....	17
7.1	Üldist.....	17
7.2	Raamstruktuuri elemendid.....	19
7.2.1	Üldist.....	19
7.2.2	Suundumus.....	19
7.2.3	Võime	19
7.2.4	Poliitika	20
7.2.5	Delegeerimine	20
7.2.6	Sooritus	21
7.2.7	Vastutus	21
	Kirjandus.....	22

EESSÕNA

ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission) moodustavad ülemaailmse standardimise kohandatud süsteemi. Rahvuslikud organisatsioonid, kes on ISO või IEC liikmed, osalevad rahvusvaheliste standardite väljatöötamisel asjakohase organisatsiooni loodud tehniliste komiteede kaudu, mille eesmärk on tegeleda konkreetsete tehniliste valdkondadega. ISO ja IEC tehnilised komiteed teevad koostööd mõlemale organisatsioonile huvi pakkuvates valdkondades. Selles töös osalevad ka muud ISO-ga ja IEC-ga seotud rahvusvahelised riiklikud organisatsioonid ning vabaihendused.

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

ISO ja IEC pööravad tähelepanu võimalusele, et selle dokumendi rakendamine võib olla seotud patendi (patentide) kasutamisega. ISO ega IEC ei võta seisukohta mis tahes esitatud patendiõiguste tõendamise, kehtivuse ega rakendatavuse eest. Selle dokumendi avaldamise kuupäeva seisuga ei ole ISO ega IEC 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 veebilehtedelt www.iso.org/patents ja <https://patents.iec.ch>). ISO ega IEC 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 kohta ja vastavushindamisega seotud ISO eriomaste terminite ja väljendite kohta ning teave selle kohta, kuidas ISO järgib WTO tehniliste kaubandustöketepingus sätestatud põhimõtteid, on esitatud järgmisel aadressil: www.iso.org/iso/foreword.html. IEC korral vt www.iec.ch/understanding-standards.

Dokumendi on koostanud tehnilise komitee ISO/IEC JTC 1 „Information technology“ alamkomitee SC 40 „IT service management and IT governance“.

Kolmas väljaanne tühistab ja asendab teist väljaannet (ISO/IEC 38500:2015), mis on tehniliselt üle vaadatud.

See väljaanne sisaldab eelmise väljaandega võrreldes järgmisi olulisi tehnilisi muudatusi:

- on detailiseeritud IT valitsemise põhimõtteid ja nende joondumist standardis ISO 37000 esitatud valitsemise põhimõtetega;
- mudelit on ajakohastatud, lisades sellele „kaasata huvipooled“;
- IT valitsemise raamstruktuuri on uuendatud, lähtudes standardist ISO/IEC TR 38502.

Kõikide standardisarja ISO/IEC 38500 osade loetelu on leitav ISO ja IEC veebilehtedelt.

Igasugune tagasiside või küsimused selle dokumendi kohta tuleks suunata dokumendi kasutaja rahvuslikule standardimisorganisatsioonile. Täielik loetelu nende organisatsioonide kohta on leitav veebilehtedelt www.iso.org/members.html ja www.iec.ch/national-committees.

SISSEJUHATUS

Infotehnoloogia (IT) kasutamine on enamiku organisatsioonide edu jaoks elutähtis mitte ainult toetava funktsioonina, vaid ka osana organisatsiooni suutlikkusest ennast ümber kujundada. IT võimaldab uusi ärimudeleid ja võib oluliselt parandada organisatsiooni tulemusi, et vastata ta huvipoolte vajadustele ja ootustele. Kasvavad küberohud ja tärkavatest tehnoloogiatest tulenevad riskid võimendavad sellist tähelepanu keset.

Praeguse ja tulevase IT kasvav potentsiaal nõuab IT valitsemise asjakohast rakendamist, tagamaks, et see täidab organisatsiooni eesmärgi toimival, vastutustundlikul ja eetilisel viisil ning joondub organisatsiooni strateegilise suunaga.

Selle dokumendi eesmärk on anda juhatustele juhiseid IT, andmete ja digivõimete vastutustundliku, uuendusliku, jätkusuutliku ja strateegilise kasutamise kohta, et nende organisatsioonid saaksid täita oma eesmärgi huvirühmade eeldatud viisil. See dokument annab põhimõtetest lähtuvaid juhiseid ega sisalda seetõttu konkreetseid teostuse üksikasju.

See dokument kasutab IT hea valitsemise saavutamiseks juhatuse kolme tööriista ning nendega seotud valitsemise ja halduse tavaid:

- 1) IT valitsemise põhimõtted – nende põhimõtete rakendamine IT vastutustundlikule ja strateegilisele kasutamisele võib viia paindlikuma ja adaptiivsema organisatsioonini.
- 2) IT valitsemise mudel – mudel näitab peamisi valitsemise ülesandeid ja interaktsioone kogu organisatsioonis, mis toob kaasa otsuste tegemise ja vastutuste selguse IT kasutamise kõikides aspektides.
- 3) IT valitsemise raamstruktuur – raamstruktuur kirjeldab elemente, mille kaudu organisatsiooni IT-korralduse valitsemine toimib, aidates tagada, et valitsemise kriitilised tegevused on organisatsiooni poolt IT kasutamisel arvestatud ja rakendatud.

Kuna IT valitsemine on organisatsioonide valitsemise valdkond, joondub see dokument ISO 37000 ja selles toodud valitsemise põhimõtetega. Seda dokumenti saab kasutada ka koos teiste valitsemise koodeksite ja toimiva valitsemise põhimõtetega. Seda dokumenti saab kasutada iseseisvalt või olemasoleva standardi ISO/IEC 38500 eelmisel väljaandel põhineva valitsemise uuendamiseks.

See dokument on suunatud peamiselt juhatusele, kuid see võtab arvesse, et valitsemine toimub kogu organisatsioonis. Seetõttu annab see IT valitsemise praktika juhiseid kogu organisatsioonile, sealhulgas juhiseid kõigi töötajate interaktsiooni ja koostöö kohta, olenemata nende ametijuhenditest.

1 KÄSITLUSALA

See dokument annab juhtpõhimõtted organisatsioonide juhatustele ja neid toetavatele isikutele infotehnoloogia (IT) toimivaks, tõhusaks ja vastuvõetavaks kasutamiseks oma organisatsioonides.

See dokument on rakendatav:

- organisatsiooni praeguse ja tulevase IT-kasutuse valitsemisele;
- IT valitsemisele kui organisatsioonide valitsemise valdkonnale.

Kasutajaskonna seisukohast on see dokument rakendatav:

- kõigile organisatsioonidele, sealhulgas avalik-õiguslikele ja eraettevõtetele, valitsusasutustele ja mittetulundusühingutele;
- igas suuruses organisatsioonidele, vähimatest kuni suurimateni, olenemata nende IT-kasutuse ulatusest.

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 37000. Governance of organizations — Guidance

3 TERMINID JA MÄÄRATLUSED

Selles dokumendis kehtivad standardis ISO 37000 ja allpool esitatud termineid ja määratlused.

ISO ja IEC hoiavad alal standardimisel kasutamiseks olevaid terminoloogiaandmebaase järgmistel aadressidel:

- IEC Electropedia: kättesaadav veebilehelt <https://www.electropedia.org/>;
- ISO veebipõhine lugemisplatvorm: kättesaadav veebilehelt <https://www.iso.org/obp/>.

3.1

suunama (*direct*)

teatavaks tegema soovitud eesmärgid ja tulemusi

MÄRKUS 1 IT valitsemise kontekstis hõlmab suunamine eesmärkide, strateegiate ja poliitikate seadmist, mida organisatsiooni liikmed peavad vastu võtma, et tagada IT kasutamise vastavus ärieesmärkidele.

MÄRKUS 2 Eesmärgid, strateegiad ja poliitikad saab määrata juhtkond, kui juhatus on neile delegeerinud vastavad volitused.

3.2

hindama (*evaluate*)

kaaluma ja tegema informeeritud otsustusi

MÄRKUS IT valitsemise kontekstis hõlmab hindamine hinnangute andmist asjaolude ja võimaluste kohta (sisemised ja välised, praegused ja tulevased), mis on seotud organisatsiooni praeguse ja tulevase IT kasutusega.

3.3

valitsemine (*governance*)

inimpõhine süsteem, mis hõlmab suunamist, järelevalvet ja vastutust