

Avaldatud eesti keeles: oktoober 2009
Jõustunud Eesti standardina: oktoober 2009

See dokument on EVS-i poolt loodud eelvaade

Infotehnoloogia valitsemine organisatsioonis

Corporate governance of information technology
(ISO/IEC 38500:2008)

EESTI STANDARDI EESSÕNA

Käesolev Eesti standard:

- on rahvusvahelise standardi ISO/IEC 38500:2008 "Corporate governance of information technology" ingliskeelse teksti identne tõlge eesti keelde ning tõlgendamise erimeelsuste korral tuleb lähtuda ametlikus keeles avaldatud tekstist,
- on kinnitatud Eesti Standardikeskuse 23.09.2009 käskkirjaga nr 167,
- jõustub sellekohase teate avaldamisel EVS Teataja 2009. aasta oktoobrikuu numbris.

Standardi tõlkis Cybernetica AS, standardi tõlke on heaks kiitnud EVS/TK 4 "Infotehnoloogia".

Standardi tõlke koostamistehpaneeku esitas EVS/TK 4, standardi tõlkimist korraldas Eesti Standardikeskus ning rahastas Majandus- ja Kommunikatsiooniministeerium.

ICS 35.080 Tarkvara
Võtmesõnad: haldus, infotehnoloogia, valitsemine
Hinnagrupp H

Standardite reprodutseerimis- ja levitamiseõigus 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

EESSÖNA	IV
1 KÄSITLUSALA, RAKENDAMINE JA EESMÄRGID	1
1.1 Käsitlusala	1
1.2 Rakendamine	1
1.3 Eesmärgid	1
1.4 Kasu selle standardi kasutamisest	1
1.5 Viidatud dokumendid	2
1.6 Määratlused	2
2 ORGANISATSIIONI HEA IT VALITSEMISE RAAMSTRUKTUUR	4
2.1 Printsiihid	4
2.2 Mudel	5
3 JUHISED IT VALITSEMISEKS ORGANISATSIIONIS	7
3.1 Üldist	7
3.2 Printsiiip 1: vastutus	7
3.3 Printsiiip 2: strateegia	8
3.4 Printsiiip 3: hankimine	8
3.5 Printsiiip 4: sooritusvõime	8
3.6 Printsiiip 5: vastavus	9
3.7 Printsiiip 6: inimkäitumine	10

See dokument on EVS-i poolt loodud eelvaade

EESSÕNA

ISO (Rahvusvaheline Standardiorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnikakomisjon) moodustavad ülemaailmse standardimise spetsialiseeritud süsteemi. ISO või IEC rahvuslikud liikmekogud osalevad rahvusvaheliste standardite väljatöötamises tehniliste komiteede kaudu, mis on nendes organisatsioonides rajatud käsitlema tehnilise tegevuse eri valdkondi. ISO ja IEC tehnilised komiteed teevad koostööd mõlemale huvi pakkuvatel aladel. Selles töös osalevad käsikäes ISO ja IECga ka muud rahvusvahelised riiklikud ja mitte-riiklikud organisatsioonid. Infotehnoloogia valdkonnas on ISO ja IEC rajanud ühise tehnilise komitee ISO/IEC JTC 1.

Rahvusvahelised standardid kavandatakse vastavalt ISO/IEC direktiivide 2. osas esitatud reeglitele. Ühise tehnilise komitee pealesanne on rahvusvaheliste standardite koostamine. Ühises tehnilises komitees vastu võetud rahvusvahelised standardikavandid saadetakse liikmekogudele hääletamiseks.

Avaldamine rahvusvahelise standardina nõuab vähemalt 75 % hääletanud liikmekogude heakskiitu.

Tuleb pöörata tähelepanu võimalusele, et mõned selle dokumendi elemendid võivad olla patendiõiguse objektiks. ISO ega IEC ei ole kohustatud mingeid selliseid patendiõigusi välja selgitama.

ISO/IEC 38500 koostas Austraalia Standardiasutus standardina AS8015:2005, mille võttis kiirkäsitlusprotseduuriga üle ühine tehniline komitee ISO/IEC JTC 1 "Infotehnoloogia", paralleelselt selle kinnitamisega ISO ja IEC rahvuslikes liikmekogudes.

ISO/IEC 38500 on printsipi põhine üldtasemel nõustav standard. Lisaks üldiste suuniste andmisele valitsemiskogu rolli kohta õhutab ta organisatsioone toetama oma IT valitsemist asjakohaste standardite kasutamisega.

Selle standardi avaldamise ajal jätkab JTC 1 tööd muude infotehnoloogia valitsemisega seotud dokumentide väljatöötamiseks.

Need dokumendid, mis edaspidi tõenäoliselt avaldatakse ISO/IEC tehniliste aruannetena ja võib-olla standarditena, käsitlevad eeldatavalt laia temaatikat, sealhulgas:

- IT-investeeringut sisaldavate projektide valitsemist,
- igapäevases äritegevuses kasutatava IT valitsemist.

SISSEJUHATUS

Selle standardi eesmärk on anda teatav põhimõtteline raamstruktuur, mida juhatajad saaksid rakendada info-tehnoloogia (IT) kasutamise hindamisel, suunamisel ja seiramisel oma organisatsioonis.

Enamik organisatsioone kasutab IT-d äritegevuse alusinstrumendina ja vähesed suudavad tegutseda ilma selleta. IT on ka oluline tegur paljude organisatsioonide edaspidise äritegevuse plaanides.

Kulutused IT-le võivad moodustada kaaluka osa organisatsiooni rahaliste ja inimressursside kulutustest. Sageli aga ei mõisteta täielikult selle investeeringuga saadavat kasu ja ebasoodsad toimed organisatsioonile võivad olla märkimisväärsed.

Niisuguste negatiivsete tagajärgede peamine põhjus on rõhu asetamine IT-tegevuste tehnilistele, rahalistele ja ajakavalistele aspektidele, mitte aga IT kasutamise kogu ärialasele kontekstile.

See standard annab teatava raamstruktuuri toimivaks IT valitsemiseks, et aidata organisatsiooni kõrgeimal tasemel olijail tunda ja täita oma õiguslaseid, regulatiivseid ja eetikaalaseid kohustusi oma organisatsiooni IT kasutamise suhtes.

Selle raamstruktuuri moodustavad määratlused, printsiibid ja mudel.

See standard on kooskõlas organisatsiooni valitsemise määratlusega, mis avaldati 1992. aastal organisatsiooni valitsemise rahaliste aspektide komisjoni aruandena (Cadbury aruandena). Cadbury aruanne andis ka organisatsiooni valitsemise alusmääratluse OECD organisatsiooni valitsemise printsiipides 1999. aastal (läbi vaadatud 2004. aastal). Käesoleva standardi kasutajail on soovitatav tutvuda Cadbury aruandega ja OECD organisatsiooni valitsemise printsiipidega.

Valitsemine (*governance*) erineb haldusest (*management*) ja segiajamise vältimiseks on need kaks mõistet käesolevas standardis selgelt määratletud.

See standard on küll adresseeritud eeskätt valitsemiskogule, mis võib omakorda määrata, et organisatsiooni juhtkond peab rakendama teatavaid meetmeid, kuid ta võimaldab ka seda, et mõnedes (enamasti väiksemates) organisatsioonides võivad valitsemiskogu liikmetel olla ka kesksed rollid juhtkonnas. Seeläbi on tagatud, et standard on kohaldatav kõigile organisatsioonidele kõige väiksemast kõige suuremani, sõltumata eesmärgist, lahendusest ja omanduse struktuurist.

Standard on mõeldud ka teavitama ja suunama neid, kes tegelevad valitsemist toetavatest poliitikatest, protsessidest ja struktuuridest koosneva haldussüsteemi kavandamise ja teostamisega.

See dokument on EVS-i poolt loodud eelvaade

1 KÄSITLUSALA, RAKENDAMINE JA EESMÄRGID

1.1 Käsitlusala

See standard annab organisatsiooni juhatajatele (sealhulgas omanikele, nõukogu liikmetele, juhatajatele, partneritele, kõrgematele juhtidele jt selletaoliste) suunavaid printsiipe infotehnoloogia (IT) toimiva, tõhusa ja aktsepteeritava kasutamise kohta nende organisatsioonis. Standard kehtib organisatsioonis kasutatavaid info- ja sideteenuseid puudutavate haldusprotsesside ja (-otsuste) valitsemise kohta.

Neid protsesse võivad juhtida organisatsiooni või väliste teenuseandjate IT-spetsialistid või organisatsiooni allüksused.

Standard annab suuniseid ka neile, kes nõustavad, teavitavad või abistavad juhatajaid.

Nende hulka kuuluvad:

- vanemjuhid;
- organisatsioonis ressursse seiravate rühmade liikmed;
- välised tegevusalased või tehnilised spetsialistid, näiteks õiguse või raamatupidamise alal;
- spetsialistid, jaemüügiliidud või erialakogud;
- riistvara, tarkvara, side jm IT-toodete müüjad;
- sisemised ja välised teenuseandjad (sealhulgas konsultandid);
- IT audiitorid.

1.2 Rakendamine

See standard on rakendatav kõigile organisatsioonidele, sealhulgas riigi- ja eraettevõtetele, riigiasutustele ja mittetulunduslikele organisatsioonidele. Standard on rakendatav igasuguse suurusega organisatsioonidele kõige väiksemast kõige suuremani, sõltumata nende IT kasutamise ulatusest.

1.3 Eesmärgid

Selle standardi eesmärk on soodustada IT toimivat, tõhusat ja aktsepteeritavat kasutamist kõigis organisatsioonides:

- veendes riskiosalisi (sealhulgas tarbijaid ja töötajaid) selles, et standardi järgimisel võivad nad usaldada organisatsiooni IT valitsemist;
- teavitades ja suunates juhatajaid IT kasutamise valitsemisel oma organisatsioonis;
- luues aluse organisatsiooni IT valitsemise objektiivseks hindamiseks.

1.4 Kasu selle standardi kasutamisest

1.4.1 Üldist

See standard kehtestab IT toimiva, tõhusa ja aktsepteeritava kasutamise printsiibid. Kui organisatsioon järgib neid printsiipe, saavad sellest abi:

- vanemjuhid;
- organisatsioonis ressursse seiravate rühmade liikmed;
- välised tegevusalased või tehnilised spetsialistid, näiteks õiguse või raamatupidamise alal;
- spetsialistid, jaemüügiliidud või erialakogud;
- riistvara, tarkvara, side jm IT-toodete müüjad;
- sisemised ja välised teenuseandjad (sealhulgas konsultandid);
- IT audiitorid;
- juhatajad, IT kasutamisest tulenevate riskide ja julgustavate soodsate võimaluste tasakaalustamisel.

See standard loob ühe mudeli IT valitsemiseks. Juhatajate risk oma kohustuste täitmisel väheneb, kui nad ülalmainitud printsiipide järgimisel pööravad vajalikku tähelepanu sellele mudelile.

Standard loob IT valitsemise sõnavara.