Avaldatud eesti keeles: märts 2011
Jõustunud Eesti standardina: märts 2011

INFOTEHNOLOOGIA
Turbemeetodid
Infoturbe halduse süsteemi teostusjuhis

Information technology
Security techniques
Information security management system implementation guidance

(ISO/IEC 27003:2010)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

Käesolev Eesti standard:

– on rahvusvahelise standardi ISO/IEC 27003:2010 „Information technology — Security techniques — Information security management system implementation guidance“ ingliskeelse teksti identne tõlge eesti keelde ning tõlgendamise erimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest,

– on kinnitatud Eesti Standardikeskuse 01.03.2011 käskkirjaga nr 45,

– on jõustunud sellekohase teate avaldamisel EVS Teataja 2011. aasta märtsikuu numbris.

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

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

ICS 35.040 Märgistikud ja informatsiooni kodeerimine
Võtmesõnad: infotehnoloogia, arvutivõrk, infoturve, infoturbe haldus
Hinnagrupp V

SISUKORD

EESSÕNA

ISO (Rahvusvaheline Standardimisorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnikakomisjon) moodustavad ülemaailmse standardimise spetsialiseeritud süsteemi. ISO või IEC rahvuslikud liikmeskogud 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 huvipakkuvatel aladel. Selles töös osalevad käsikäes ISO ja IECga ka muud rahvusvahelised riiklikud ja mitteriiklikud organisatsioonid. Infotehnoloogia alal on ISO ja IEC loonud ühise tehnilise komitee ISO/IEC JTC 1.

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

Ühise tehnilise komitee peamine ülesanne on koostada rahvusvahelisi standardeid. Ühises tehnilises komitees vastu võetud rahvusvahelised standardikavandid saadetakse rahvuslikele kogudele hääletamiseks. Avaldamine rahvusvahelise standardina nõuab heakskiitu vähemalt 75% hääletanud rahvuslikelt kogudelt.

Tuleb pöörata tähelepanu võimalusele, et standardi mõned osad võivad olla patendiõiguse subjektiks. ISOt ega IEC-d ei saa pidada vastutavaks mõne või kõigi selliste patendiõiguste identifitseerimise osas.

Standardi ISO/IEC 27003 koostas ISO/IEC tehnilise komitee JTC 1 „Infotehnoloogia“ alamkomitee SC 27 „Turbemeetodid“.

SISSEJUHATUS

Standardi eesmärk on anda praktilisi juhiseid organisatsiooni infoturbe halduse süsteemi (ISMS) teostusplaani väljatöötamiseks kooskõlas standardiga ISO/IEC 27001:2005. Üldiselt rakendatakse ISMSi projektina.

Standardis kirjeldatud protsess on mõeldud aitama rakendada standardit ISO/IEC 27001:2005 (jaotiste 4, 5 ja 7 asjakohaseid osi) ning dokumenteerib:

a) ettevalmistused ISMS teostamisplaani algatamiseks organisatsioonis, projekti organisatsioonilise struktuuri määramiseks ja juhtkonna heakskiidu saamiseks;

b) ISMS projekti jaoks elutähtsad tegevused;

c) näited ISO/IEC 27001:2005 nõuete täitmiseni jõudmise kohta.

Standardi abil suudab organisatsioon välja töötada infoturbe halduse protsessi, andes osanikele kinnitust selle kohta, et infovarade riskid hoitakse pidevalt organisatsiooni määratud vastuvõetavais infoturbepiirides.

Standard ei hõlma käitustegevusi ega muid ISMS tegevusi, kuid hõlmab plaani ISMSi kasutuselevõtust tulenevate tegevuste kavandamiseks. Plaani tulemuseks on lõplik ISMS projekti teostusplaan. ISMS projekti organisatsioonispetsiifilise osa tegelik rakendamine jääb väljapoole selle standardi käsitlusala.

ISMS projekt tuleks sooritada tavalise projektihalduse metoodikatega (lisateavet annavad projektihaldust käsitlevad ISO ja ISO/IEC standardid).

1 KÄSITLUSALA

Standard keskendub olulistele aspektidele, mida tuleb arvestada infoturbe halduse süsteemi (ISMS) edukaks kavandamiseks ja teostamiseks kooskõlas standardiga ISO/IEC 27001:2005. Selles kirjeldatakse ISMSi spetsifitseerimise ja kavandamise protsessi algatamisest kuni rakendusplaanide koostamiseni. Samuti kirjeldatakse protsessi, millega saadakse ISMSi teostamisele juhtkonna heakskiit, määratakse ISMSi rakendamise projekti (mida selles standardis nimetatakse ISMS projektiks) ning antakse juhiseid selle kohta, kuidas plaanida ISMS projekti, mis tuleneb lõplikust ISMS projekti rakendusplaanist.

See standard on mõeldud kasutamiseks ISMSi tegevatele organisatsioonidele. See on kohaldatav igat tüüpi ja iga suurusega organisatsioonidele (näiteks äriettevõtetele, riigiasutustele, mittetulundusühingutele). Iga organisatsiooni keerukus ja riskid on ainulaadsed ning konkreetsed nõuded suunavad ISMSi teostamist. Standardis mainitud tegevused on lihtsustatavad ja neid saab kohaldada ka väiksematele organisatsioonidele. Suuremastaabilised või keerukad organisatsioonid võivad standardis mainitud tegevuste toimivaks haldamiseks vajada mitmekihilist organiseerimis- või haldussüsteemi. Mõlemal juhul aga saab asjakohaseid tegevusi plaanida seda standardit rakendades.

Standard annab soovitusi ja selgitusi ega määra kindlaks mingeid nõudeid. See on mõeldud kasutamiseks koos standarditega ISO/IEC 27001:2005 ja ISO/IEC 27002:2005, kuid mitte ISO/IEC 27001:2005 nõuete ega ISO/IEC 27002:2005 soovituste muutmiseks ega vähendamiseks. Standardile vastavust ei ole vaja deklareerida.

2 NORMIVIITED

Järgmised dokumendid on vajalikud standardi rakendamiseks. Dateeritud viidete korral kehtib üksnes viidatud väljaanne. Dateerimata viidete korral kehtib viidatud dokumendi uusim väljaanne koos võimalike muudatustega.

ISO/IEC 27000:2009, *Information techonology – Security techniques – Information security management systems – Overview and vocabulary*

ISO/IEC 27001:2005, *Information techonology – Security techniques – Information security management systems – Requirements*

3 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse standardites ISO/IEC 27000:2009 ja ISO/IEC 27001:2005 toodud ning järgmisi termineid ja määratlusi.

3.1
ISMS projekt (*ISMS project*)
organisatsiooni sooritatavad struktureeritud tegevused ISMSi teostamiseks

4 STANDARDI STRUKTUUR

4.1 Üldine liigendus jaotisteks

ISMS teostamine on tähtis tegevus ja üldiselt viiakse see organisatsioonis ellu projektina. Standard selgitab ISMSi teostamist, keskendudes projekti algatamisele, plaanimisele ja määratlemisele. ISMSi lõpliku teostamise plaanimise protsess on viiejärguline ja iga järku esitab omaette jaotis. Kõigil jaotistel on ühesugune järgnevalt kirjeldatud struktuur. Need viis järku on:

a) juhtkonna heakskiidu taotlemine ISMS projekti algatamisele (jaotis 5),

b) ISMSi käsitlusala ja ISMSi poliitika määramine (jaotis 6),

c) organisatsiooni analüüsi läbiviimine (jaotis 7),