

INFOTEHNOLOOGIA
Turbemeetodid
Infoturvariski haldus

Information technology
Security techniques
Information security risk management
(ISO/IEC 27005:2011)

EESTI STANDARDI EESSÕNA

See Eesti standard on

- rahvusvahelise standardi ISO/IEC 27005:2011 ingliskeelse teksti sisu poolest identne tõlge eesti keelde. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;
- jõustunud Eesti standardina sellekohase teate avaldamisega EVS Teataja 2014. aasta aprillikuu numbris.

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

Standardi tõlkimise ettepaneku on esitanud EVS/TK 4, standardi tõlkimist on korraldanud Eesti Standardikeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

See standard on rahvusvahelise standardi ISO/IEC 27005:2011 eestikeelne [et] versioon. Teksti tõlke on avaldanud Eesti Standardikeskus ja sellel on sama staatus ametlike keelte versioonidega.

This standard is the Estonian [et] version of the International Standard ISO/IEC 27005:2011. It has been translated by the Estonian Centre for Standardisation. 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 35.040 Märgistikud ja informatsiooni kodeerimine

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

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

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:

Aru 10, 10317 Tallinn, Eesti; www.evs.ee; telefon 605 5050; e-post info@evs.ee

SISUKORD

EESSÕNA	V
SISSEJUHATUS.....	VI
1 KÄSITLUSALA	1
2 NORMIVIITED	1
3 TERMINID JA MÄÄRATLUSED	1
4 STANDARDI ÜLESEHITUS	8
5 TAUST	9
6 INFOTURVARISKI HALDUSE PROTSESSI ÜLEVAADE	10
7 KONTEKSTI LOOMINE	13
7.1 Üldisi kaalutlusi	13
7.2 Aluskriteeriumid	13
7.2.1 Riskihalduse meetodika	13
7.2.2 Riski hindamise kriteeriumid	13
7.2.3 Toime kriteeriumid	14
7.2.4 Riski aktsepteerimise kriteeriumid	14
7.3 Käsitlusala ja piirid	15
7.4 Organisatsioon infoturvariski halduseks	15
8 INFOTURVARISKI KAALUTLEMINE	16
8.1 Infoturvariski kaalutlemise üldkirjeldus	16
8.2 Riski tuvastamine	16
8.2.1 Sisseyuhatus riski tuvastamisse	16
8.2.2 Varade identifitseerimine	17
8.2.3 Ohtude tuvastamine	17
8.2.4 Olemasolevate turvameetmete väljaselgitamine	18
8.2.5 Nõrkuste tuvastamine	18
8.2.6 Tagajärgede tuvastamine	19
8.3 Riskianalüüs	20
8.3.1 Riskianalüüsi meetodikad	20
8.3.2 Tagajärgede hindamine	21
8.3.3 Intsidendi võimalikkuse hindamine	21
8.3.4 Riskitaseme määramine	22
8.4 Riski hindamine	22
9 INFOTURVARISKI KÄSITLEMINE	23
9.1 Riskikäsitluse üldkirjeldus	23
9.2 Riski muutmine	25
9.3 Riski säilitamine	26
9.4 Riski vältimine	26
9.5 Riski jagamine	26
10 INFOTURVARISKI AKTSEPTEERIMINE	27
11 INFOTURVARISKIST TEAVITAMINE JA KONSULTEERIMINE	27
12 INFOTURVARISKI SEIRE JA LÄBIVAATUS	28
12.1 Riskitegurite seire ja läbivaatus	28
12.2 Riskihalduse seire, läbivaatus ja täiustamine	29
Lisa A (teatmelisa) Infoturvariski halduse protsessi käsitlusala ja piiride määratlemine	31
Lisa B (teatmelisa) Varade identifitseerimine ja väärtustamine ning toime hindamine	35
Lisa C (teatmelisa) Tüüpiliste ohtude näiteid	44
Lisa D (teatmelisa) Nõrkused ja nõrkuste hindamise meetodid	47
Lisa E (teatmelisa) Infoturvariski kaalutlemise meetodikad	52

Lisa F (teatmelisa) Riski muutmise kitsendused	57
Lisa G (teatmelisa) Erinevused ISO/IEC 27005:2008 ja ISO/IEC 27005:2011 määratlustes	59
Kirjandus	69

See dokument on EVS-i poolt loodud eelvaade

EESSÕNA

ISO (Rahvusvaheline Standardimisorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnikakomisjon) moodustavad ülemaailmse standardimise spetsialiseeritud süsteemi. ISO või IEC rahvuslikud liikmesorganisatsioonid 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 IEC-ga ka rahvusvahelised, riiklikud ja valitsusvälised organisatsioonid. Infotehnoloogia valdkonnas on ISO ja IEC rajanud ühendatud tehnilise komitee ISO/IEC JTC 1.

Rahvusvahelised standardid kavandatakse ISO/IEC direktiivide 2. osas esitatud reeglite kohaselt.

Ühendatud tehnilise komitee põhiülesanne on rahvusvaheliste standardite koostamine. Ühendatud tehnilises komitees vastuvõetud rahvusvahelised standardikavandid saadetakse hääletamiseks liikmesorganisatsioonidele. Avaldamine rahvusvahelise standardina nõuab, et hääletanud liikmesorganisatsioonidest kiidaks selle heaks vähemalt 75 %.

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse subjekt. ISO-t ega IEC-d ei saa pidada vastutavaks sellis(t)e patendiõigus(t)e väljaselgitamise eest.

Standardi ISO/IEC 27005 on koostanud ühendatud tehnilise komitee ISO/IEC JTC 1 „Infotehnoloogia“ alamkomitee SC 27 „Infoturbemeetodid“.

See, teine redaktsioon tühistab ja asendab esimese redaktsiooni (ISO/IEC 27005:2008) ning on selle tehniline uustöötlus.

SISSEJUHATUS

See standard annab suuniseid infoturvariski halduseks organisatsioonis ning toetab muuhulgas ISO/IEC 27001 nõudeid infoturbe halduse süsteemidele (ISMS). See standard ei anna aga infoturvariski halduseks mingit konkreetset meetodit. Organisatsiooni ülesandeks jääb määratleda oma lähenemine riskihaldusele sõltuvalt näiteks ISMS-i käsitusala, riskihalduse kontekstist või majandussektorist. ISMS-i nõuete täitmiseks selles standardis kirjeldatud raamstruktuuris saab kasutada mitmeid olemasolevaid meetodikaid.

See standard puudutab juhte ja töötajaid, kes tegelevad organisatsioonis infoturvariski haldusega, ning asjakohastel juhtudel ka selliseid tegevusi toetavaid väliseid pooli.

1 KÄSITLUSALA

See standard annab suuniseid infoturvariski halduseks.

Standard toetab standardis ISO/IEC 27001 spetsifitseeritud üldkontseptsioone ja on kavandatud aitama infoturbe rahuldavat rakendamist riskihaldusliku lähenemisviisi alusel.

Selle standardi täielikuks mõistmiseks on tähtis tunda mõisteid, mudeleid, protsesse ja termineid, mida kirjeldavad ISO/IEC 27001 ja ISO/IEC 27002.

Standardit saab rakendada igat tüüpi organisatsioonidele (näiteks äriettevõtetele, riigiasutustele, mitetulunduslikele organisatsioonidele), kes kavatsevad hallata riske, mis võivad rikkuda organisatsiooni teabe turvalisust.

2 NORMIVIITED

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

ISO/IEC 27000. Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 27001:2005. Information technology — Security techniques — Information security management systems — Requirements

3 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse alljärgnevalt ja standardis ISO/IEC 27000 esitatud termineid ja määratlusi.

MÄRKUS Erinevused ISO/IEC 27005:2008 ja selle standardi määratlustes on esitatud lisas G.

3.1

tagajärg (*consequence*)

eesmärke mõjutav **sündmuse** (3.3) tulemus

[ISO juhend 73:2009]

MÄRKUS 1 Sündmusel võib olla palju tagajärgi.

MÄRKUS 2 Tagajärg võib olla kindel või määramatu ning infoturbe kontekstis on see harilikult negatiivne.

MÄRKUS 3 Tagajärgi võib väljendada kvalitatiivselt või kvantitatiivselt.

MÄRKUS 4 Esialgsed tagajärjed võivad tekitada tagajärgede ahelreaktsiooni.

outcome of an **event** (3.3) affecting objectives

[ISO Guide 73:2009]

NOTE 1 An event can lead to a range of consequences.

NOTE 2 A consequence can be certain or uncertain and in the context of information security is usually negative.

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

NOTE 4 Initial consequences can escalate through knock-on effects.