Avaldatud eesti keeles: jaanuar 2024
Jõustunud Eesti standardina: jaanuar 2024

INFOTURVE, KÜBERTURVE JA PRIVAATSUSKAITSE
Infoturvariskide haldamise juhend

Information security, cybersecurity and privacy protection
Guidance on managing information security risks (ISO/IEC 27005:2022, identical)

EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO/IEC 27005:2022 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 jaanuaris 2024;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2024. aasta jaanuarikuu numbris.

Standardi tõlke koostamise ettepaneku on esitanud tehniline komitee EVS/TK 4 „Infotehnoloogia“, standardi tõlkimist on korraldanud Eesti Standardimis- ja Akrediteerimiskeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

Standardi on tõlkinud Cybernetica AS, standardi on heaks kiitnud EVS/TK 4.

Standardi mõnedele sätetele on lisatud Eesti olusid arvestavaid märkusi, selgitusi ja täiendusi, mis on tähistatud Eesti maatähisega EE.

See standard on rahvusvahelise standardi ISO/IEC 27005:2022 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 27005:2022. 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 35.030

SISUKORD

EESSÕNA V
SISSEJUHATUS VI
1 KÄSITLUSALA 1
2 NORMVIITED 1
3 TERMINID JA MÄÄRATLUSED 1
3.1 Infoturvariski terminid 1
3.2 Infoturvariski halduse terminid 5
4 SELLE DOKUMENDI ÜLESEHITUS 7
5 INFOTURVARISKI HALDUS 7
5.1 Infoturvariski halduse protsess 7
5.2 Infoturvariski halduse tsüklid 9
6 KONTEKSTI LOOMINE 9
6.1 Organisatsioonist tulenev 9
6.2 Huvipoolte põhinõuete piiritlemine 10
6.3 Riskikontrolli rakendamine 10
6.4 Infoturvariski kriteeriumide kehtestamine ja järgimine 10
6.4.1 Üldist 10
6.4.2 Riski aktsepteerimise kriteeriumid 11
6.4.3 Infoturvariski kontrollide sooritamise kriteeriumid 12
6.5 Sobiva meetodi valimine 15
7 INFOTURVARISKI KONTROLLI PROTSESS 16
7.1 Üldist 16
7.2 Infoturvariskide tuvastamine 16
7.2.1 Infoturvariskide tuvastamine ja kirjeldamine 16
7.2.2 Riskiomanike tuvastamine 18
7.3 Infoturvariskide analüüsimine 19
7.3.1 Üldist 19
7.3.2 Potentsiaalsete tagajärgede kontroll 19
7.3.3 Võimalikkuse kontroll 20
7.3.4 Riskitasemete määramine 21
7.4 Infoturvariskide hindamine 22
7.4.1 Riskianalüüsi tulemite võrdlemine riskikriteeriumidega 22
7.4.2 Analüüsitud riskidele prioriteetide andmine riskikäsitluseks 23
8 INFOTURVARISKI KÄSITLEMISE PROTSESS 23
8.1 Üldist 23
8.2 Infoturvariski käsitlemise sobivate variantide valimine 23
8.3 Infoturvariski käsitlemise variantide teostuseks kõigi vajalike meetmete määramine 24
8.4 Määratud meetmete võrdlemine standardi ISO/IEC 27001:2022 lisas A olevatega 27
8.5 Kohaldusmäärangu koostamine 27
8.6 Infoturvariski käsitluse kava 28
8.6.1 Riskikäsitluse kava koostamine 28
8.6.2 Kinnitus riskiomanikelt 29
8.6.3 Jääk-infoturvariskide kinnitamine 30
9 PROTSESSIDE SOORITAMINE 31
9.1 Infoturvariski kontrolli protsessi sooritamine 31
9.2 Infoturvariski käsitlemise protsessi sooritamine 31
10 KAASNEVATE INFOTURBE HALDUSE SÜSTEEMI PROTSESSIDE TOETAMINE 32

10.1 Organisatsiooni kontekst ... 32
10.2 Eestvedu ja kohustumus ... 33
10.3 Teavitus ja konsulteerimine ... 33
10.4 Dokumenteeritud teave ... 35
10.4.1 Üldist ... 35
10.4.2 Dokumenteeritud teave protsesside kohta ... 35
10.4.3 Dokumenteeritud teave tulemuste kohta ... 36
10.5 Seire ja läbivaatus ... 36
10.5.1 Üldist ... 36
10.5.2 Riske mõjutavate tegurite seire ja läbivaatus ... 37
10.6 Juhtkondlik läbivaatus ... 38
10.7 Korrektiivsed toimingud ... 38
10.8 Pidev täiustamine ... 39
Lisa A (teatmelisa) Riskikontrolli protsesse toetavate meetodite näiteid ... 41
Kirjandus ... 65

EESSÕNA

ISO (International Organization for Standardization) 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 ka muud ISO-ga ja IEC-ga seotud rahvusvahelised riiklikud organisatsioonid ning vabaühendused.

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).

Tuleb pöörata tähelepanu võimalusele, et dokumendi mõni osa võib olla patendiõiguse objekt. ISO ja IEC 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) või IEC-le saadetud patentide deklaratsioonide loetelus (vt https://patents.iec.ch).

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 kaubandustõkete lepingus sätestatud põhimõtteid, on esitatud järgmisel aadressil: www.iso.org/iso/foreword.html. IEC korral vt www.iec.ch/understanding-standards.

Dokumendi on koostanud ühendatud tehnilise komitee ISO/IEC JTC 1 „Information technology“ alamkomitee SC 27 „Information security, cybersecurity and privacy protection“.

Neljas väljaanne tühistab ja asendab kolmandat väljaannet (ISO/IEC 27005:2018), mis on tehniliselt üle vaadatud.

Peamised muudatused on järgmised:

— kogu juhendi tekst on viidud kooskõlla standarditega ISO/IEC 27001:2022 ja ISO 31000:2018,

— terminoloogia on viidud kooskõlla standardi ISO 31000:2018 terminoloogiaga,

— jaotiste struktuur on sobitatud standardi ISO/IEC 27001:2022 omaga,

— lisatud on riskistsenaariumi kontseptsioonid,

— varadel põhinevale riskituvastuse metoodikale on vastandatud sündmusepõhine metoodika,

— lisade sisu on läbi vaadatud ja lisad on ümber korraldatud üheksainsaks lisaks.

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

See dokument annab juhiseid alljärgneva kohta:

— infoturvariski alal standardis ISO/IEC 27001 spetsifitseeritud nõuete rakendamine,

— olulised soovitused infoturvariski halduse tegevuste toetuseks ühendatud tehnilise komitee ISO/IEC JTC 1 alamkomitee SC 27 väljatöötatud standardites,

— teabe turvalisuse riskidega tegelemise toimingud (vt standardi ISO/IEC 27001:2022 jaotis 6.1 ja peatükk 8),

— standardi ISO 31000 riskihalduse juhiste rakendamine infoturbe kontekstis.

See dokument sisaldab üksikasjalikke juhiseid riskihalduseks ja täiendab standardi ISO/IEC 27003 juhiseid.

See dokument on mõeldud kasutamiseks

— organisatsioonidele, mis kavatsevad rajada ja ellu viia infoturbe halduse süsteemi (*information security management system*, ISMS) kooskõlas standardiga ISO/IEC 27001;

— inimestele, kes sooritavad infoturvariski haldust või osalevad selles (näiteks ISMS-i spetsialistid, riskiomanikud ja muud huvipooled);

— organisatsioonidele, mis kavatsevad täiustada oma infoturvariskide halduse protsessi.

1 KÄSITLUSALA

See dokument annab juhiseid organisatsioonide abistamiseks

— infoturvariskide käsitlemise toiminguid puudutavate standardi ISO/IEC 27001 nõuete täitmisel;

— infoturvariski halduse tegevuste, eriti infoturvariski kontrolli ja käsitluse sooritamisel.

See dokument on kohaldatav kõigis organisatsioonides sõltumata nende tüübist, suurusest või majandussektorist.

2 NORMVIITED

Allpool nimetatud dokumentidele on tekstis viidatud selliselt, et nende sisu kujutab endast kas osaliselt või tervenisti selle dokumendi nõudeid. 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

3 TERMINID JA MÄÄRATLUSED

Dokumendi rakendamisel kasutatakse standardis ISO/IEC 27000 ning allpool esitatud termineid ja määratlusi.

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

— ISO veebipõhine lugemisplatvorm: kättesaadav veebilehelt https://www.iso.org/obp;

— IEC Electropedia: kättesaadav veebilehelt https://www.electropedia.org/.

3.1 Infoturvariski terminid

3.1.1
väliskontekst (*external context*)
väline keskkond, milles organisatsioon püüab saavutada oma eesmärke

MÄRKUS Väliskonteksti koostises võivad olla

— rahvusvaheline, sisemaine, regionaalne või kohalik sotsiaalne, kultuuriline, poliitiline, õiguslik, regulatiivne, rahanduslik, tehnoloogiline, majanduslik, geoloogiline keskkond;

— organisatsiooni eesmärke mõjutavad kesksed tõukejõud ja tendentsid;

— väliste huvipoolte suhted, tajumused, väärtused, vajadused ja ootused;

— lepingulised suhted ja kohustumused;

— võrkude ja sõltuvuste keerukus.

[ALLIKAS: ISO Guide 73:2009, 3.3.1.1, muudetud – märkust 1 on muudetud]

3.1.2
sisekontekst (*internal context*)
sisemine keskkond, milles organisatsioon püüab saavutada oma eesmärke

MÄRKUS Sisekonteksti koostises võivad olla

— nägemus, missioon ja väärtused;

