

INFOTURVE, KÜBERTURVE JA PRIVAATSUSKAITSE
Infoturvariskide haldamise juhend

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

EESTI STANDARDI EESSÕNA

See Eesti standard on

- Euroopa standardi EN ISO/IEC 27005:2024 ingliskeelse teksti sisu poolest identne tõlge eesti keelde ja sellel on sama staatus mis jõustumisteate meetodil vastu võetud originaalversioonil. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;
- jõustunud Eesti standardina inglise keeles oktoobris 2024;
- eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2024. aasta oktoobrikuu 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 mõnede sätetele on lisatud Eesti olusid arvestavaid märkusi, selgitusi ja täiendusi, mis on tähistatud Eesti maatahisega EE.

Euroopa standardimisorganisatsioon on teinud Euroopa standardi EN ISO/IEC 27005:2024 rahvuslikele liikmetele kättesaadavaks 07.08.2024.

Date of Availability of the European Standard EN ISO/IEC 27005:2024 is 07.08.2024.

See standard on Euroopa standardi EN ISO/IEC 27005:2024 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 European Standard EN ISO/IEC 27005:2024. 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 35.030

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

English Version

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

Sécurité de l'information, cybersécurité et protection
de la vie privée - Préconisations pour la gestion des
risques liés à la sécurité de l'information (ISO/IEC
27005:2022)

Informationssicherheit, Cybersicherheit und
Datenschutz - Leitfaden zur Handhabung von
Informationssicherheitsrisiken (ISO/IEC 27005:2022)

This European Standard was approved by CEN on 1 August 2024.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

SISUKORD

EUROOPA EESSÕNA.....	4
EESSÕNA.....	5
SISSEJUHATUS.....	6
1 KÄSITLUSALA.....	7
2 NORMIVIITED.....	7
3 TERMINID JA MÄÄRATLUSED.....	7
3.1 Infoturvariski terminid.....	7
3.2 Infoturvariski halduse terminid.....	11
4 SELLE DOKUMENDI ÜLESEHITUS.....	13
5 INFOTURVARISKI HALDUS.....	13
5.1 Infoturvariski halduse protsess.....	13
5.2 Infoturvariski halduse tsüklid.....	15
6 KONTEKSTI LOOMINE.....	15
6.1 Organisatsioonist tulenev.....	15
6.2 Huvipoolte põhinõuete piiritlemine.....	16
6.3 Riskikontrolli rakendamine.....	16
6.4 Infoturvariski kriteeriumide kehtestamine ja järgimine.....	16
6.4.1 Üldist.....	16
6.4.2 Riski aktsepteerimise kriteeriumid.....	17
6.4.3 Infoturvariski kontrollide sooritamise kriteeriumid.....	18
6.5 Sobiva meetodi valimine.....	21
7 INFOTURVARISKI KONTROLLI PROTSESS.....	22
7.1 Üldist.....	22
7.2 Infoturvariskide tuvastamine.....	22
7.2.1 Infoturvariskide tuvastamine ja kirjeldamine.....	22
7.2.2 Riskiomanike tuvastamine.....	24
7.3 Infoturvariskide analüüsimine.....	25
7.3.1 Üldist.....	25
7.3.2 Potentsiaalsete tagajärgede kontroll.....	25
7.3.3 Võimalikkuse kontroll.....	26
7.3.4 Riskitasemete määramine.....	27
7.4 Infoturvariskide hindamine.....	28
7.4.1 Riskianalüüsi tulemite võrdlemine riskikriteeriumidega.....	28
7.4.2 Analüüsitud riskidele prioriteetide andmine riskikäsitlemiseks.....	29
8 INFOTURVARISKI KÄSITLEMISE PROTSESS.....	29
8.1 Üldist.....	29
8.2 Infoturvariski käsitlemise sobivate variantide valimine.....	29
8.3 Infoturvariski käsitlemise variantide teostuseks kõigi vajalike meetmete määramine.....	30
8.4 Määratud meetmete võrdlemine standardi ISO/IEC 27001:2022 lisas A olevatega.....	33
8.5 Kohaldusmäärangu koostamine.....	33
8.6 Infoturvariski käsitlemise kava.....	34
8.6.1 Riskikäsitlemise kava koostamine.....	34
8.6.2 Kinnitus riskiomanikelt.....	35
8.6.3 Jääk-infoturvariskide kinnitamine.....	36
9 PROTSESSIDE SOORITAMINE.....	37
9.1 Infoturvariski kontrolli protsessi sooritamine.....	37
9.2 Infoturvariski käsitlemise protsessi sooritamine.....	37

10	KAASNEVATE INFOTURBE HALDUSE SÜSTEEMI PROTSESSIDE TOETAMINE	38
10.1	Organisatsiooni kontekst.....	38
10.2	Eestvedu ja kohustumus	39
10.3	Teavitust ja konsulteerimine	39
10.4	Dokumenteeritud teave	41
10.4.1	Üldist.....	41
10.4.2	Dokumenteeritud teave protsesside kohta.....	41
10.4.3	Dokumenteeritud teave tulemuste kohta.....	42
10.5	Seire ja läbivaatus.....	42
10.5.1	Üldist.....	42
10.5.2	Riske mõjutavate tegurite seire ja läbivaatus	43
10.6	Juhtkondlik läbivaatus.....	44
10.7	Korrektiivsed toimingud.....	44
10.8	Pidev täiustamine	45
	Lisa A (teatmelisa) Riskikontrolli protsesse toetavate meetodite näiteid	47
	Kirjandus.....	71

EUROOPA EESSÕNA

Dokumendi ISO/IEC 27005:2022 on koostanud Rahvusvahelise Standardimisorganisatsiooni (International Organization for Standardization, ISO) tehniline komitee ISO/IEC JTC 1 „Information technology“ ja selle on standardina EN ISO/IEC 27005:2024 üle võtnud tehniline komitee CEN-CENELEC/JTC 13 „Cybersecurity and Data Protection“, mille sekretariaati haldab DIN.

Euroopa standardile tuleb anda rahvusliku standardi staatus kas identse tõlke avaldamisega või jõustumisteatega hiljemalt 2025. a veebruariks ja sellega vastuolus olevad rahvuslikud standardid peavad olema kehtetuks tunnistatud hiljemalt 2025. a veebruariks.

Tuleb pöörata tähelepanu võimalusele, et dokumendi mõni osa võib olla patendiõiguse objekt. CEN-CENELEC ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest.

Igasugune tagasiside ja küsimused selle dokumendi kohta tuleks suunata dokumendi kasutaja rahvuslikule standardimisorganisatsioonile. Täielik loetelu nende organisatsioonide kohta on leitav CEN-i ja CENELEC-i veebilehtedelt.

CEN-i/CENELEC-i sisereeglite järgi peavad Euroopa standardi kasutusele võtma järgmiste riikide rahvuslikud standardimisorganisatsioonid: Austria, Belgia, Bulgaaria, Eesti, Hispaania, Holland, Horvaatia, Iirimaa, Island, Itaalia, Kreeka, Küpros, Leedu, Luksemburg, Läti, Malta, Norra, Poola, Portugal, Prantsusmaa, Põhja-Makedoonia Vabariik, Rootsi, Rumeenia, Saksamaa, Serbia, Slovakkia, Sloveenia, Soome, Šveits, Taani, Tšehhi Vabariik, Türgi, Ungari ja Ühendkuningriik.

Jõustumisteade

CEN-CENELEC on dokumendi ISO/IEC 27005:2022 teksti muutmata kujul üle võtnud kui EN ISO/IEC 27005:2024.

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 äriiline 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 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 soovitusel 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 käsitlemise sooritamisel.

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

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/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 eesmärged

MÄRKUS Väliskonteksti koostises võivad olla

- rahvusvaheline, sisemine, regionaalne või kohalik sotsiaalne, kultuuriline, poliitiline, õiguslik, regulatiivne, rahanduslik, tehnoloogiline, majanduslik, geoloogiline keskkond;
- organisatsiooni eesmärged 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 eesmärged

MÄRKUS Sisekonteksti koostises võivad olla

- nägemus, missioon ja väärtused;