Avaldatud eesti keeles: september 2023
Jõustunud Eesti standardina: detsember 2022

INFOTURVE, KÜBERTURVE JA PRIVAATSUSKAITSE
Infoturvameetmed

Information security, cybersecurity and privacy protection
Information security controls
(ISO/IEC 27002:2022)

EVS • EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— Euroopa standardi EN ISO/IEC 27002:2022 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 detsembris 2022;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2023. aasta septembrikuu 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 AS Cybernetica, standardi on heaks kiitnud EVS/TK 4.

Euroopa standardimisorganisatsioon on teinud Euroopa standardi EN ISO/IEC 27002:2022 rahvuslikele liikmetele kättesaadavaks 09.11.2022.

Date of Availability of the European Standard EN ISO/IEC 27002:2022 is 09.11.2022.

See standard on Euroopa standardi EN ISO/IEC 27002:2022 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 European Standard EN ISO/IEC 27002:2022. 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

EUROOPA STANDARD
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27002

November 2022

ICS 35.030

Supersedes EN ISO/IEC 27002:2017

English version

Information security, cybersecurity and privacy protection - Information security controls (ISO/IEC 27002:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée - Moyens de maîtrise de l'information (ISO/IEC 27002:2022)

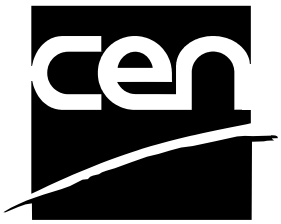
Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022)

This European Standard was approved by CEN on 30 October 2022.

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 and CENELEC members are the national standards bodies and national electrotechnical committees 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

Ref. No. EN ISO/IEC 27002:2022 E

SISUKORD

EUROOPA EESSÕNA

Dokumendi ISO/IEC 27002:2022 on koostanud Rahvusvahelise Standardimisorganisatsiooni (International Organization for Standardization, ISO) tehniline komitee ISO/IEC JTC 1 „Information technology“ ja selle on standardina EN ISO/IEC 27002:2022 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 2023. a maiks ja sellega vastuolus olevad rahvuslikud standardid peavad olema kehtetuks tunnistatud hiljemalt 2023. a maiks.

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.

See dokument asendab standardit EN ISO/IEC 27002:2017.

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 27002:2022 teksti muutmata kujul üle võtnud kui EN ISO/IEC 27002:2022.

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 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“.

Kolmas väljaanne tühistab ja asendab teist väljaannet (ISO/IEC 27002:2013), mis on tehniliselt üle vaadatud. Samuti sisaldab see tehnilisi parandusi ISO/IEC 27002:2013/Cor. 1:2014 ja ISO/IEC 27002:2013/Cor. 2:2015.

Peamised muudatused on järgmised:

— pealkirja on muudetud;

— dokumendi struktuuri on muudetud, meetmed esitatakse lihtsa taksonoomia ning sellega kaasnevate atribuutide abil;

— mõned meetmed on omavahel ühendatud, mõned aga on kustutatud ja mitu uut meedet lisatud. Täieliku vastenduse võib leida lisast B.

See standardi ISO/IEC 27002:2022 parandatud versioon sisaldab järgmisi parandusi:

— mitteavanevad hüperlingid on dokumendis läbivalt taastatud;

— jaotise 5.22 sissejuhatavas tabelis ja tabelis A.1 (rida 5.22) on „#Teabe turvalisuse tagamine“ viidud veerust, mille pealkiri on „Turbealad“, veergu, mille pealkiri on „Võimealad“.

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

0.1 Taust ja kontekst

See dokument on kavandatud igat liiki ja igas suuruses organisatsioonidele. Seda tuleb kasutada võrdlusalusena meetmete määramisel ja teostamisel infoturvariski käsitlemiseks infoturbe halduse süsteemis (ISMS), mis põhineb standardil ISO/IEC 27001. Seda saavad organisatsioonid kasutada ka juhenddokumendina üldtunnustatud infoturvameetmete määramisel ja teostamisel. Peale selle on dokument mõeldud kasutamiseks tegevusala- ja organisatsioonispetsiifiliste infoturbe halduse juhiste väljatöötamiseks, võttes arvesse nende spetsiifilisi infoturvariski keskkondi. Selles dokumendis olevaid erinevaid korralduslikke ja keskkonnaspetsiifilisi meetmeid saab vajaduse korral määrata riskikontrolli kaudu.

Igat liiki ja igas suuruses organisatsioonid (sealhulgas avalik ja erasektor, ärilised ja mittetulunduslikud) loovad, koguvad, töötlevad, talletavad, edastavad ja kõrvaldavad teavet mitmesugusel kujul, sealhulgas elektroonilisel, füüsilisel ja verbaalsel (näiteks vestluste ja ettekannetena).

Teabe väärtus ulatub kirjasõnast, arvudest ja piltidest kaugemale: teadmus, kontseptsioonid, ideed ja tootemargid on näited teabe ainetutest kujudest. Kokkuühendatud maailmas väärivad või nõuavad teave ja kaasnevad varad kaitset mitmesuguste riskiallikate eest, olgu need looduslikud, juhuslikud või sihilikud.

Teabe turvalisus saavutatakse sobiva meetmestiku teostamisega, sealhulgas poliitikate, eeskirjade, protsesside, protseduuride, korraldusstruktuuride ning tarkvara- ja riistvarafunktsioonidega. Oma spetsiifiliste turva- ja ärieesmärkide saavutamiseks peaks organisatsioon neid meetmeid vajaduse korral määratlema, teostama, seirama, läbi vaatama ja täiustama. Selline ISMS, mis on spetsifitseeritud standardis ISO/IEC 27001, vaatleb terviklikult ja koordineeritult organisatsiooni infoturvariske, et otsustada ja teostada kõikehõlmav infoturvameetmestik ladusa haldussüsteemi üldraamistuses.

Paljud infosüsteemid ning nende haldus ja käit ei ole kavandatud turvalistena sellise ISMS mõttes, mis on spetsifitseeritud standardis ISO/IEC 27001 ja selles dokumendis. Turvatase, mis on saavutatav pelgalt tehniliste meetmetega, on piiratud ja seda peaksid toetama asjakohased haldustegevused ning korraldusprotsessid. Piiritlemist, millised meetmed peaksid olema rakendatud, tuleb riskikäsitluse sooritamisel hoolikalt kavandada ja pöörata tähelepanu üksikasjadele.

Edukas ISMS vajab organisatsiooni kogu personali tuge. Ta võib nõuda ka muude huvipoolte, näiteks aktsionäride või tarnijate osalemist. Vajalikuks võivad osutuda ka alade asjatundjate nõuanded.

Sobiv, adekvaatne ja toimiv infoturbe halduse süsteem annab organisatsiooni juhtkonnale ja muudele huvipooltele kindlust selles, et nende teave ja kaasnevad muud varad püsivad mõistlikult turvalistena ning kaitstuna ohtude ja kahjustuste eest, võimaldades organisatsioonil seeläbi saavutada ettemääratud tegevuseesmärke.

0.2 Infoturvanõuded

On oluline, et organisatsioon määraks oma infoturvanõuded. Peamisi infoturvanõuete allikaid on kolm:

a) organisatsiooni riskikontroll, mis arvestab organisatsiooni üldist tegevusstrateegiat ja -eesmärke. Seda saab edendada või toetada infoturvaspetsiifilise riskikontrolliga. Tulemuseks peaks olema selliste meetmete määramine, mis tagaksid, et organisatsiooni jääkrisk vastaks ta riski aktsepteerimise kriteeriumidele;

b) juriidilised, põhikirjalised, regulatiivsed ja lepingulised nõuded, mida organisatsioon ja ta huvipooled (äripartnerid, teenustajad jt) peavad täitma ning nende sotsiaalkultuuriline keskkond;

c) kogum põhimõtteid, eesmärke ja ärinõudeid kõigiks teabe elutsükli sammudeks, mis organisatsioon on oma tegevuse toetuseks välja töötanud.

0.3 Meetmed

Meede on määratletud kui abinõu, mis muudab või säilitab riski. Mõned meetmed selles dokumendis on sellised, mis muudavad riski, teised aga säilitavad seda. Näiteks saab infoturvapoliitika ainult säilitada riski, vastavus sellele poliitikale saab aga riski muuta. Peale selle nimetavad mõned meetmed üht ja sama üldist abinõud erinevates riskikontekstides. See dokument esitab ühe korralduslike, personalipõhiste, füüsiliste ja tehniliste infoturvameetmete üldistatud segu, mis on tuletatud rahvusvaheliselt tunnustatud headest tavadest.

0.4 Meetmete määramine

Meetmete määramine sõltub organisatsiooni otsustest, mis selgelt määratletud käsitlusalaga järgnevad riskikontrollile. Tuvastatud riskidega seotud otsused peaksid põhinema organisatsioonis rakendatavail riski aktsepteerimise kriteeriumidel, riskikäsitluse variantidel ja riskihalduse metoodikal. Meetmete määramine peaks arvestama ka kõiki asjakohaseid riiklikke ja rahvusvahelisi õigusakte ja eeskirju. Meetmete määramine sõltub ka sellest, milline on meetmete vastastikune toime sügavuti kaitse andmiseks.

Organisatsioon võib vastavalt vajadusele meetmed kavandada või need suvalisest allikast piiritleda. Selliste meetmete spetsifitseerimisel peaks organisatsioon arvestama meetme teostuseks ja käigushoiuks vajalikke ressursse ja investeeringut võrreldes saadava ärilise väärtusega. ISMS-i investeerimist puudutavate otsuste kohta ning võistlevate ressursinõuete kontekstis nende otsuste majanduslike tagajärgede kohta annab juhiseid ISO/IEC TR 27016.

Meetmete teostuseks kulutatud ressursid peaksid olema tasakaalus potentsiaalse äritoimega, mis tuleneb turvaintsidentidest nende meetmete puudumisel. Riskikontrolli tulemused peaksid aitama suunata ja määrata asjakohaseid haldustoiminguid, infoturvariskide halduse prioriteete ja nende riskide eest kaitsmiseks vajalikena määratud meetmete teostamist.

Mõningaid meetmeid selles dokumendis võib lugeda infoturbe halduse suunavateks põhimõteteks, mis on kohaldatavad enamikus organisatsioonides. Lisateavet meetmete määramise ning muude riskikäsitluse variantide kohta annab ISO/IEC 27005.

0.5 Organisatsioonispetsiifiliste juhiste väljatöötamine

Seda dokumenti võib pidada organisatsioonispetsiifiliste juhiste väljatöötamise lähtepunktiks. Kõiki selles dokumendis esitatud meetmeid ja juhiseid ei saa kohaldada kõigile organisatsioonidele. Organisatsiooni erivajaduste ja tuvastatud riskide katmiseks on võib-olla vaja lisameetmeid ja -juhiseid, mida selles dokumendis ei ole. Lisajuhiseid või -meetmeid sisaldavate dokumentide koostamisel on ehk kasulik tulevase alusena lisada viiteid selle dokumendi peatükkidele.

0.6 Elutsüklikaalutlused

Teabel on elutsükkel loomisest kõrvaldamiseni. Teabe väärtus ja ta riskid võivad selle elutsükli kestel varieeruda (näiteks ei ole firma finantsaruannete lubamatu avalikustamine või vargus pärast nende avaldamist oluline, kuid nende terviklus on endiselt tähtis), seega on infoturve mingil määral tähtis kõigis ta järkudes.

Infosüsteemidel ja muudel infoturbesse puutuvail varadel on elutsüklid, mille kestel neid algatatakse, spetsifitseeritakse, kavandatakse, testitakse, teostatakse, kasutatakse, hooldatakse ning lõpuks võetakse kasutuselt ja kõrvaldatakse. Igas järgus tuleks arvestada infoturvet. Uute süsteemide väljatöötamise

projektid ja seniste süsteemide muudatused annavad võimalusi turvameetmete täiustamiseks, võttes arvesse organisatsiooni riske ja intsidentidest saadud õppetunde.

0.7 Kaasnevad rahvusvahelised standardid

See dokument pakub juhiseid laia valiku kohta infoturvameetmetest, mida üldiselt rakendatakse paljudes organisatsioonides, muud ISO/IEC 27000 standardipere dokumendid aga esitavad lisanõuandeid või -nõudeid infoturbe halduse kogu protsessi muude aspektide kohta.

ISMS-i ja nimetatud dokumendipere kohta annab üldise sissejuhatuse ISO/IEC 27000, mis esitab ka sõnastiku, määratledes enamiku terminitest, mida kasutatakse kogu ISO/IEC 27000 dokumendiperes, ning kirjeldab selle pere iga liikme käsitlusala ja eesmärke.

On ka sektorispetsiifilisi standardeid lisameetmetega, mis on suunatud käsitlema spetsiifilisi alasid (näiteks ISO/IEC 27017 pilvteenuste, ISO/IEC 27701 privaatsuse, ISO/IEC 27019 energeetika, ISO/IEC 27011 sideorganisatsioonide ja ISO/IEC 27799 tervishoiu tarbeks). Sellised standardid on võetud peatükki „Kirjandus“ ning mõningaile neist on viidatud juhistes ja muudes teabelõikudes dokumendi peatükkides 5 kuni 8.

1 KÄSITLUSALA

See dokument esitab võrdlusalusena ühe komplekti üldistatud infoturvameetmeid koos teostusjuhistega. Dokument on kavandatud kasutamiseks organisatsioonides

a) standardil ISO/IEC 27001 põhineva infoturbe halduse süsteemi (ISMS) kontekstis,

b) infoturvameetmete teostamiseks rahvusvaheliselt tunnustatud heade tavade põhjal,

c) organisatsioonispetsiifiliste infoturbe halduse juhiste väljatöötamiseks.

2 NORMVIITED

Selles dokumendis ei ole normviiteid.

3 TERMINID, MÄÄRATLUSED JA LÜHENDTERMINID

3.1 Terminid ja määratlused

Dokumendi rakendamisel kasutatakse 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/.

3.1.1
pääsu reguleerimine (*access control*)
vahend, millega tagada, et füüsiline ja loogiline juurdepääs *varadele* (3.1.2) on lubatav ning töö- ja infoturvanõuete põhjal kitsendatud

3.1.2
vara (*asset*)
miski, millel on organisatsiooni jaoks väärtus

MÄRKUS Infoturbe kontekstis saab eristada kaht liiki varasid:

— primaarvarad:
  — teave;
  — äri*protsessid* (3.1.27) ja -tegevused;

— igat liiki tugivarad (millest primaarvarad sõltuvad), näiteks:
  — riistvara;
  — tarkvara;
  — võrk;
  — *personal* (3.1.20);
  — tegevuskoht;
  — korraldusstruktuur.

3.1.3
rünne (*attack*)
edukas või edutu lubamatu katse hävitada, muuta, blokeerida *vara* (3.1.2), pääseda selle juurde või igasugune katse vara paljastada, varastada või lubamatult kasutada