Avaldatud eesti keeles: veebruar 2022
Jõustunud Eesti standardina: märts 2020



# INFOTEHNOLOOGIA
# Turbemeetodid
# Infoturbe halduse süsteemid
# Ülevaade ja sõnavara

# Information technology
# Security techniques
# Information security management systems
# Overview and vocabulary
# (ISO/IEC 27000:2018)

## EESTI STANDARDI EESSÕNA

See Eesti standard on

— Euroopa standardi EN ISO/IEC 27000:2020 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 märtsis 2020;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2022. aasta veebruarikuu numbris.

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

Standardi on tõlkinud Jaak Tepandi, 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.

**Euroopa standardimisorganisatsioonid on teinud Euroopa standardi EN ISO/IEC 27000:2020 rahvuslikele liikmetele kättesaadavaks 19.02.2020.**

**Date of Availability of the European Standard EN ISO/IEC 27000:2020 is 19.02.2020.**

**See standard on Euroopa standardi EN ISO/IEC 27000:2020 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 27000:2020. 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 01.040.35; 35.030

EUROOPA STANDARD
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

# EN ISO/IEC 27000

February 2020

ICS 01.040.35; 35.030

Supersedes EN ISO/IEC 27000:2017

English Version

## Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2018)

Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Vue d'ensemble et vocabulaire (ISO/IEC 27000:2018)

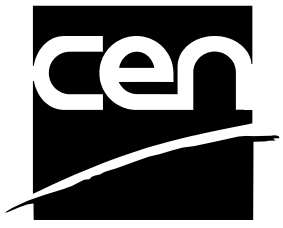
Informationstechnik - Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Überblick und Terminologie (ISO/IEC 27000:2018)

This European Standard was approved by CEN on 20 October 2019.

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, Turkey and United Kingdom.



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



Ref. No. EN ISO/IEC 27000:2020 E

## SISUKORD

## EUROOPA EESSÕNA

Dokumendi ISO/IEC 27000:2018 teksti on koostanud Rahvusvahelise Standardimisorganisatsiooni (International Organization for Standardization, ISO) tehniline komitee ISO/IEC JTC 1 „Information technology“ ja selle on standardina EN ISO/IEC 27000:2020 üle võtnud tehniline komitee CEN/CLC/JTC 13 „Cybersecurity and Data Protection“, mille sekretariaati haldab DIN.

Euroopa standardile tuleb anda rahvusliku standardi staatus kas identse tõlke avaldamisega või jõustumisteatega hiljemalt 2020. a augustiks ja sellega vastuolus olevad rahvuslikud standardid peavad olema kehtetuks tunnistatud hiljemalt 2020. a augustiks.

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

See dokument asendab standardit EN ISO/IEC 27000:2017.

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 on standardi ISO/IEC 27000:2018 teksti muutmata kujul üle võtnud standardina EN ISO/IEC 27000:2020.

## EESSÕNA

ISO (International Organization for Standardization) on ülemaailmne rahvuslike standardimisorganisatsioonide (ISO rahvuslike liikmesorganisatsioonide) föderatsioon. Tavaliselt tegelevad rahvusvahelise standardi koostamisega ISO tehnilised komiteed. Kõigil rahvuslikel liikmesorganisatsioonidel, kes on mingi tehnilise komitee pädevusse kuuluvast valdkonnast huvitatud, on õigus selle komitee tegevusest osa võtta. Selles töös osalevad ka ISO-ga seotud rahvusvahelised riiklikud organisatsioonid ning vabaühendused. Kõigis elektrotehnika standardimist puudutavates küsimustes teeb ISO tihedat koostööd Rahvusvahelise Elektrotehnikakomisjoniga (IEC).

Selle dokumendi väljatöötamiseks kasutatud ja edasiseks haldamiseks mõeldud protseduurid on kirjeldatud ISO/IEC direktiivide 1. osas. Eriti tuleb silmas pidada eri heakskiidukriteeriumeid, mis on eri liiki ISO dokumentide puhul vajalikud. See dokument on kavandatud ISO/IEC direktiivide 2. osas esitatud toimetamisreeglite kohaselt (vt www.iso.org/directives).

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse objekt. ISO 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).

Mis tahes selles dokumendis kasutatud äriline käibenimi on kasutajate abistamise eesmärgil esitatud teave ja ei kujuta endast toetusavaldust.

Selgitused standardite vabatahtliku kasutuse 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.

Dokumendi on koostanud tehnilise komitee ISO/IEC JTC 1 „Information technology“ alamkomitee SC 27 „IT Security techniques“.

Viies väljaanne tühistab ja asendab neljandat väljaannet (ISO/IEC 27000:2016), mis on tehniliselt üle vaadatud. Peamised muudatused võrreldes eelmise väljaandega on järgmised:

— sissejuhatus on ümber sõnastatud;

— mõned terminid ja määratlused on eemaldatud;

— peatükk 3 on ühildatud MSS-i ülataseme struktuuriga;

— peatükki 5 on ajakohastatud, et kajastada asjakohaste standardite muudatusi;

— lisad A ja B on välja jäetud.

# 0 SISSEJUHATUS

## 0.1 Ülevaade

Haldussüsteemide rahvusvahelised standardid annavad mudeli, mida järgida haldussüsteemi rajamisel ja käitamisel. See mudel sisaldab neid aspekte, mida ala asjatundjad peavad üksmeelselt ala praeguseks rahvusvaheliseks arengutasemeks. Tehnilise komitee ISO/IEC JTC 1 alamkomitee SC 27 juures tegutseb ekspertkomisjon, mis on spetsialiseerunud haldussüsteemide rahvusvaheliste standardite väljatöötamisele infoturbe alal; need standardid moodustavad infoturbe halduse süsteemide (*Information Security Management System*, ISMS) standardipere.

ISMS-i standardipere abil saavad organisatsioonid välja töötada ja realiseerida raamstruktuuri, mille abil hallata oma infovarasid, sealhulgas rahandusteavet, intellektuaalset omandit, töötajate isikuandmeid, klientidelt või kolmandatelt pooltelt organisatsioonile usaldatud teavet. Neid standardeid saab kasutada ka selleks, et valmistuda saama sõltumatut hinnangut oma teabe kaitseks rakendatava ISMS-i kohta.

## 0.2 Selle dokumendi eesmärk

ISMS-i standardiperesse kuuluvad standardid, mis

a) määratlevad nõuded ISMS-ile ja selliste süsteemide sertifitseerijaile;

b) annavad otsest tuge, detailseid juhiseid ja/või tõlgendusi kogu ISMS-i rajamise, evituse, käigushoiu ja täiustamise protsessi tarbeks;

c) arvestavad ISMS-i puhul sektorispetsiifilisi juhiseid ning

d) käsitlevad ISMS-i vastavuse hindamist.

## 0.3 Selle dokumendi sisu

Selles dokumendis kasutatakse järgmisi verbivorme:

— „peab/tuleb“ näitab nõuet,

— „peaks/tuleks“ näitab soovitust,

— „võib/tohib“ näitab luba,

— „saab“ näitab võimalikkust või võimet.

Teave tähisega „MÄRKUS“ on juhis nõude mõistmiseks või selgitamiseks. Peatükis 3 kasutatud „MÄRKUSED“ annavad lisateavet, mis täiendab terminoloogilisi andmeid ja võib sisaldada termini kasutamisega seotud sätteid.

# 1 KÄSITLUSALA

See dokument annab ülevaate infoturbe halduse süsteemidest (ISMS). Ta esitab ka ISMS-i standardiperes kasutatavad ühised terminid ja määratlused. See dokument on rakendatav igat liiki ja iga suurusega organisatsioonides (nt äriettevõtetes, riigiasutustes, mittetulunduslikes organisatsioonides).

Selles dokumendis toodud terminid ja määratlused

— hõlmavad ISMS-i standardipere üldkasutatavaid termineid ja määratlusi,

— ei hõlma kõiki ISMS-i standardiperes kasutatavaid termineid ja määratlusi ning

— ei piira ISMS-i standardiperet uute terminite määratlemisel.

# 2 NORMIVIITED

Selles dokumendis ei ole normiviiteid.

# 3 TERMINID JA MÄÄRATLUSED

ISO ja IEC hoiavad alal standardimisel kasutamiseks olevaid terminoloogilisi andmebaase järgmistel aadressidel:

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

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

**3.1**
**pääsu reguleerimine** (*access control*)
vahend, millega tagada, et juurdepääs varadele on volitatud ning töö- ja turva*nõuete* (3.56) põhjal kitsendatud

means to ensure that access to assets is authorized and restricted based on business and security *requirements* (3.56)

**3.2**
**rünne** (*attack*)
katse hävitada, paljastada, muuta, blokeerida või varastada mingit vara või saada sellele volitamata juurdepääs või kasutada seda volitamatult

attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

**3.3**
**audit** (*audit*)
süstemaatiline, sõltumatu ja dokumenteeritud *protsess* (3.54) auditi asitõendite saamiseks ja nende objektiivseks hindamiseks eesmärgiga teha kindlaks, millises ulatuses on auditi kriteeriumid rahuldatud

MÄRKUS 1 Audit võib olla siseaudit (sooritab esimene osapool) või välisaudit (sooritab teine või kolmas osapool) ning ta võib olla liitaudit (kaht või enamat distsipliini ühendav).

MÄRKUS 2 Siseauditi korraldab organisatsioon ise või väline pool tema nimel.

MÄRKUS 3 „Auditi asitõendid“ ja „auditi kriteeriumid“ on määratletud standardis ISO 19011.

systematic, independent and documented *process* (3.54) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled