EESTI STANDARD EVS-EN ISO/IEC 27000:2017

Avaldatud eesti keeles: märts 2017
Jõustunud Eesti standardina: märts 2017

INFOTEHNOLOOGIA
Turbemeetodid
Infoturbe halduse süsteemid
Ülevaade ja sõnavara

Information technology
Security techniques
Information security management systems
Overview and vocabulary
(ISO/IEC 27000:2016)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— Euroopa standardi EN ISO/IEC 27000:2017 ingliskeelse teksti sisu poolest identne tõlge eesti keelde ja sellel on sama staatus mis jõustumisteate meetodil vastuvõetud originaalversioonil. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina inglise keeles märtsis 2017;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2017. aasta märtsikuu numbris.

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

Standardi on tõlkinud AS Cybernetica, 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 27000:2017 rahvuslikele liikmetele kättesaadavaks 22.02.2017.

Date of Availability of the European Standard EN ISO/IEC 27000:2017 is 22.02.2017.

See standard on Euroopa standardi EN ISO/IEC 27000:2017 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 European Standard EN ISO/IEC 27000:2017. It was 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 01.040.35; 03.100.70; 35.030

EUROOPA STANDARD
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27000

February 2017

ICS 01.040.35; 03.100.70; 35.030

English Version

Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2016)

Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Vue d'ensemble et vocabulaire (ISO/IEC 27000:2016)

Informationstechnik - Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Überblick und Terminologie (ISO/IEC 27000:2016)

This European Standard was approved by CEN on 26 January 2017.

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 of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN ISO/IEC 27000:2017 E

SISUKORD

EUROOPA EESSÕNA

Dokumendi (ISO/IEC 27000:2016) on koostanud Rahvusvahelise Standardimisorganisatsiooni (*International Organization for Standardization*, ISO) ja Rahvusvahelise Elektrotehnikakomisjoni (*International Electrotechnical Commission*, IEC) tehniline komitee ISO/IEC JTC 1 „Information technology“ ning see on üle võetud standardina EN ISO/IEC 27000:2017.

Euroopa standardile tuleb anda rahvusliku standardi staatus kas identse tõlke avaldamisega või jõustumisteatega hiljemalt 2017. a augustiks ja sellega vastuolus olevad rahvuslikud standardid peavad olema kehtetuks tunnistatud hiljemalt 2017. a augustiks.

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

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

Jõustumisteade

CEN on standardi ISO/IEC 27000:2016 teksti muutmata kujul üle võtnud standardina EN ISO/IEC 27000:2017.

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. ISO/IEC JTC 1 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 ISMS-i standardipere

ISMS-i standardipere (vt peatükk 4) on mõeldud abistama igat liiki ja igas suuruses organisatsioone ISMS-i teostamisel ja käigushoiul ning koosneb järgmistest rahvusvahelistest standarditest üldpealkirjaga „Information technology — Security techniques“ („Infotehnoloogia. Turbemeetodid“) (loetletud alljärgnevalt numberjärjestuses):

— ISO/IEC 27000. Information security management systems — Overview and vocabulary (Infoturbe halduse süsteemid. Ülevaade ja sõnavara);

— ISO/IEC 27001. Information security management systems — Requirements (Infoturbe halduse süsteemid. Nõuded);

— ISO/IEC 27002. Code of practice for information security controls (Infoturbemeetodite tavakoodeks);

— ISO/IEC 27003. Information security management system implementation guidance (Infoturbe halduse süsteemi teostusjuhis);

— ISO/IEC 27004. Information security management — Measurement (Infoturbe haldus. Mõõtmine);

— ISO/IEC 27005. Information security risk management (Infoturvariski haldus);

— ISO/IEC 27006. Requirements for bodies providing audit and certification of information security management systems (Nõuded infoturbe halduse süsteeme auditeerivatele ja sertifitseerivatele asutustele);

— ISO/IEC 27007. Guidelines for information security management systems auditing (Infoturbe halduse süsteemide auditeerimise juhised);

— ISO/IEC TR 27008. Guidelines for auditors on information security controls (Juhised audiitoritele infoturbe meetmete kohta);

— ISO/IEC 27009. Sector-specific application of ISO/IEC 27001 — Requirements (ISO/IEC 27001 sektorispetsiifiline rakendamine. Nõuded);

— ISO/IEC 27010. Information security management for inter-sector and inter-organizational communications (Sektoritevahelise ja organisatsioonidevahelise suhtluse infoturbe haldus);

— ISO/IEC 27011. Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (Standardil ISO/IEC 27002 põhinevad infoturbe halduse juhised sideala organisatsioonidele);

— ISO/IEC 27013. Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 (Juhised ISO/IEC 27001 ja ISO/IEC 20000-1 integreeritud rakendamiseks);

— ISO/IEC 27014. Governance of information security (Infoturbe valitsemine);

— ISO/IEC TR 27015. Information security management guidelines for financial services (Infoturbe halduse juhised finantsteenuste alal);

— ISO/IEC TR 27016. Information security management — Organizational economics (Infoturbe haldus. Organisatsiooniökonoomika);

— ISO/IEC 27017. Code of practice for information security controls based on ISO/IEC 27002 for cloud services (Standardil ISO/IEC 27002 põhinev pilvteenuste infoturbe meetmete tavakoodeks);

— ISO/IEC 27018. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (Isikutuvastusteabe töötlejaiks olevates avalikes pilvedes isikutuvastusteabe kaitse tavakoodeks);

— ISO/IEC TR 27019. Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry (Standardil ISO/IEC 27002 põhinevad energeetikaspetsiifiliste protsessijuhtimissüsteemide infoturbe halduse juhised).

EE MÄRKUS Eestikeelses standardis on standardi tähist korrigeeritud.

MÄRKUS Üldpealkiri „Information technology — Security techniques“ („Infotehnoloogia. Turbemeetodid“) näitab, et ühise tehnilise komitee ISO/IEC JTC 1 „Infotehnoloogia“ alamkomitee SC 27 „Infoturbe meetodid“ on koostanud need rahvusvahelised standardid.

ISMS-i standardiperesse kuulub ilma selle üldpealkirjata järgmine standard:

— ISO 27799. Health informatics — Information security management in health using ISO/IEC 27002 (Tervishoiuinformaatika. Infoturbe haldus standardiga ISO/IEC 27002 tervishoiualal).

0.3 Selle standardi eesmärk

See standard annab ülevaate infoturbe halduse süsteemidest ja määratleb nendega seotud terminid.

MÄRKUS Lisa A selgitab, kuidas ISMS-i standardiperes kasutatakse verbivorme nõuete ja/või juhiste väljendamiseks.

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;

d) käsitlevad ISMS-i vastavuse hindamist.

Selles standardis kasutatud terminid ja määratlused

— hõlmavad ISMS-i standardiperes üldkasutatavaid termineid ja määratlusi,

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

— ei piira uute terminite määratlemist ISMS-i standardiperes kasutamiseks.

1 KÄSITLUSALA

See standard annab ülevaate infoturbe halduse süsteemidest ning ISMS-i standardiperes kasutatavatest ühistest terminitest ja määratlustest. See standard on rakendatav igat liiki ja iga suurusega organisatsioonides (nt äriettevõtetes, riigiasutustes, mittetulunduslikes organisatsioonides).

2 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse alljärgnevalt esitatud termineid ja määratlusi.

2.1
pääsu reguleerimine (*access control*)
vahend, millega tagada, et juurdepääs varadele on volitatud ning töö- ja turva**nõuete** (2.63) põhjal kitsendatud

means to ensure that access to assets is authorized and restricted based on business and security **requirements** (2.63)

2.2
analüütiline mudel (*analytical model*)
algoritm või arvutus, mis kombineerib üht või mitut **alusnäitajat** (2.10) ja/või **tuletatud näitajat** (2.22) nendega seotud **otsustuskriteeriumidega** (2.21)

algorithm or calculation combining one or more **base measures** (2.10) and/or **derived measures** (2.22) with associated **decision criteria** (2.21)

2.3
rünne (*attack*)
katse hävitada, paljastada, muuta, blokeerida või varastada mingit vara või saada sellele volitamatu juurdepääs või kasutada seda volitamatult

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

2.4
atribuut (*attribute*)
objekti (2.55) omadus või karakteristik, mida inimene või automatiseeritud vahend saab kvantitatiivselt või kvalitatiivselt eristada

[Allikas: ISO/IEC 15939:2007, 2.2, muudetult – „olem“ on määratluses asendatud „objektiga“.]

property or characteristic of an **object** (2.55) that can be distinguished quantitatively or qualitatively by human or automated means

2.5
audit (*audit*)
süstemaatiline, sõltumatu ja dokumenteeritud **protsess** (2.61) auditi asitõendite saamiseks ja nende objektiivseks hindamiseks eesmärgiga teha kindlaks, millises ulatuses on auditi kriteeriumid rahuldatud

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

MÄRKUS 2 „Auditi asitõendid“ ja „auditi kriteeriumid“ on määratletud standardis ISO 19011.