Avaldatud eesti keeles: detsember 2019
Jõustunud Eesti standardina: detsember 2019

ÜHISKONDLIK TURVALISUS
Talitluspidevuse juhtimissüsteem
Nõuded

Security and resilience
Business continuity management systems
Requirements
(ISO 22301:2019)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— Euroopa standardi EN ISO 22301:2019 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 2019;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2019. aasta detsembrikuu numbris.

Standardi tõlke koostamise ettepaneku on esitanud tehniline komitee EVS/TK 71 „Valveteenused ja -süsteemid“, standardi tõlkimist on korraldanud Eesti Standardikeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

Standardi on tõlkinud OÜ TJO Konsultatsioonid, standardi on heaks kiitnud EVS/TK 71.

Euroopa standardimisorganisatsioonid on teinud Euroopa standardi EN ISO 22301:2019 rahvuslikele liikmetele kättesaadavaks 06.11.2019.

Date of Availability of the European Standard EN ISO 22301:2019 is 06.11.2019.

See standard on Euroopa standardi EN ISO 22301:2019 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 22301:2019. 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 03.100.01; 03.100.70

EUROOPA STANDARD
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO 22301

November 2019

ICS 03.100.01, 03.100.70

Supersedes EN ISO 22301:2014

English Version

Security and resilience - Business continuity management systems - Requirements (ISO 22301:2019)

Sécurité et résilience - Systèmes de management de la continuité d'activité - Exigences (ISO 22301:2019)

Sicherheit und Resilienz - Business Continuity Management System - Anforderungen (ISO 22301:2019)

This European Standard was approved by CEN on 14 October 2019.

CEN 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 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 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, Turkey and United Kingdom.

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

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

Ref. No. EN ISO 22301:2019 E

SISUKORD

EUROOPA EESSÕNA

Dokumendi (EN ISO 22301:2019) on koostanud tehniline komitee ISO/TC 292 „Security and resilience“ koostöös tehnilise komiteega CEN/TC 391 „Societal and Citizen Security“, mille sekretariaati haldab AFNOR.

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

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 22301:2014.

CEN-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 22301:2019 teksti muutmata kujul üle võtnud standardina EN ISO 22301:2019.

EESSÕNA

ISO (International Organization for Standardization) on ülemaailmne rahvuslike standardimis-organisatsioonide (ISO rahvuslike liikmesorganisatsioonide) föderatsioon. Tavaliselt tegelevad rahvusvahelise standardi koostamisega ISO tehnilised komiteed. Kõigil rahvuslikel liikmes-organisatsioonidel, kes on mingi tehnilise komitee pädevusse kuuluvast valdkonnast huvitatud, on õigus selle komitee tegevusest osa võtta. Selles töös osalevad käsikäes ISO-ga ka rahvusvahelised, riiklikud ja valitsusvälised organisatsioonid. 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 tehniline komitee ISO/TC 292 „Security and resilience“.

Teine väljaanne tühistab ja asendab esimest väljaannet (ISO 22301:2012), mis on tehniliselt üle vaadatud. Peamised muudatused võrreldes eelmise väljaandega on järgmised:

— kohaldatud on ISO nõudeid juhtimissüsteemi standarditele, mis on alates 2012. aastast arenenud;

— nõuded on täpsustatud, uusi nõudeid ei ole lisatud;

— distsipliinipõhised talitluspidevuse nõuded jäävad nüüd peaaegu täielikult peatükki 8;

— peatükk 8 on ümber struktureeritud, et saada põhinõuetest selgem ülevaade;

— selguse suurendamiseks ja praeguse mõtteviisi kajastamiseks on muudetud mitmeid distsipliinipõhiseid talitluspidevuse termineid.

Igasugune tagasiside või küsimused selle dokumendi kohta tuleks suunata dokumendi kasutaja rahvuslikule standardimisorganisatsioonile. Täielik loetelu nende organisatsioonide kohta on leitav veebilehelt www.iso.org/members.html.

SISSEJUHATUS

0.1 Üldist

See dokument määrab kindlaks talitluspidevuse juhtimissüsteemi (*Business Continuity Management System*, BCMS) elluviimise ja toimivana hoidmise struktuuri ning nõuded, mis arendavad organisatsiooni talitluspidevust sellise mõju suuruse ja tüübi järgi, mida organisatsioon võib häiringute tagajärjel aktsepteerida või mitte.

BCMS-i toimivana hoidmise tulemusi kujundavad organisatsiooni õiguslikud, regulatiivsed, organisatsioonisatoorsed ja tööstuse nõuded, pakutavad tooted ja teenused, kasutatavad protsessid, organisatsiooni suurus ja struktuur ning huvipoolte nõuded.

BCMS rõhutab järgneva tähtsust:

— organisatsiooni vajaduste ning talitluspidevuse juhtpõhimõtete ja eesmärkide vajalikkuse mõistmine,

— organisatsiooni protsesside, võimekuse ja reageerimisstruktuuride haldamine ning toimivana hoidmine, et tagada organisatsiooni häiringutest taastumine;

— BCMS-i tulemuslikkuse ning mõjususe seire ja ülevaatamine;

— kvalitatiivsetel ja kvantitatiivsetel mõõtmisel põhinev järjepidev parendamine.

BCMS sisaldab nagu ka teised juhtimissüsteemid järgmisi komponente:

a) juhtpõhimõtted;

b) kompetentsed inimesed koos määratletud kohustustega;

c) juhtimisprotsessid, mis seostuvad
   1) juhtpõhimõtete,
   2) planeerimise,
   3) elluviimise ja toimimisega,
   4) tulemuslikkuse hindamisega,
   5) juhtkonnapoolse ülevaatuse ja
   6) järjepideva parendamisega;

d) dokumenteeritud teave, mis toetab operatiivjuhtimist ja võimaldab tulemuslikkuse hindamist.

0.2 Talitluspidevuse juhtimissüsteemi eelised

BCMS-i eesmärk on valmistada ette, pakkuda ning hoida toimivana ohjemeetmed ja võimekus juhtida organisatsiooni üldist võimekust toimimise jätkamiseks häiringute ajal. Selle saavutamiseks organisatsioon

a) äritegevuse vaates
   1) toetab oma strateegilisi eesmärke;
   2) loob konkurentsieelise;
   3) kaitseb ja tugevdab oma mainet ja usaldusväärsust;
   4) suurendab organisatsiooni vastupidavust;

b) finantsvaates
   1) vähendab juriidilisi ja rahalisi riske;
   2) vähendab häiringute otseseid ja kaudseid kulusid;

c) huvipoolte seisukohast

1) kaitseb elu, vara ja keskkonda;
2) kaalutleb huvipoolte ootusi;
3) pakub kindlustunnet organisatsiooni edukuse võimekuse kohta;

d) sisemiste protsesside seisukohast
1) parendab selle võimet püsida häiringute ajal mõjusana;
2) demonstreerib riskide ennetavaid meetmeid mõjusalt ja tõhusalt;
3) käsitleb operatiivseid haavatavusi.

0.3 Planeeri-Teosta-Kontrolli-Tegutse (*The Plan-Do-Check-Act*, PDCA) tsükkel

See dokument kohaldab planeeri (sea sisse), teosta (vii ellu ja käita), kontrolli (seira ja vaata üle) ning tegutse (hoia toimivana ja parenda) (PDCA) tsüklit, et viia ellu, hoida toimivana ja järjepidevalt parendada organisatsiooni BCMS-i mõjusust.

See tagab teatud määral kooskõla muude juhtimissüsteemide standarditega, näiteks ISO 9001, ISO 14001, ISO/IEC 20000-1, ISO/IEC 27001 ja ISO 28000, toetades seeläbi seotud juhtimissüsteemide järjepidevat ja lõimitud elluviimist ning toimimist.

PDCA-tsükli kohaselt hõlmavad peatükid 4 kuni 10 järgmisi komponente:

— Peatükk 4 tutvustab organisatsiooni suhtes kohaldatava BCMS-i konteksti sisseseadmiseks vajalikke nõudeid, samuti vajadusi, nõudeid ja käsitlusala.

— Peatükk 5 võtab kokku konkreetsed nõuded tippjuhtkonna rollile BCMS-is ja kuidas eestvedamine väljendab juhtpõhimõtete kaudu oma ootusi organisatsioonile.

— Peatükk 6 kirjeldab BCMS-i kui terviku jaoks strateegiliste eesmärkide ja suunavate põhimõtete sisseseadmise nõudeid.

— Peatükk 7 toetab BCMS-i toiminguid, mis on seotud kompetentsuse ja teabevahetuse sisseseadmisega huvipooltega korduvaks/vajaduspõhiseks suhtlemiseks, dokumenteerides, ohjates, hoides toimivana ja säilitades samal ajal nõutavat dokumenteeritud teavet.

— Peatükk 8 määratleb talitluspidevuse vajadused, määrab kindlaks, kuidas neid käsitleda, ja töötab välja protseduurid organisatsiooni juhtimiseks häiringute ajal.

— Peatükk 9 võtab kokku nõuded, mis on vajalikud talitluspidevuse tulemuslikkuse ja BCMS-i selle dokumendiga vastavuse mõõtmiseks ning juhtkonnapoolse ülevaatuse läbiviimiseks.

— Peatükk 10 tuvastab BCMS-i mittevastavuse ja rakendab asjakohaseid meetmeid ning järjepidevat parendamist korrigeeriva tegevuse kaudu.

0.4 Selle dokumendi sisu

See dokument vastab ISO juhtimissüsteemi standardite nõuetele. Need nõuded hõlmavad kõrgtaseme ülesehitust, identset põhiteksti ja baastermineid koos põhimääratlustega, mis on loodud abiks kasutajatele, kes rakendavad mitut ISO juhtimissüsteemi standardit.

See dokument ei sisalda muude juhtimissüsteemide erinõudeid, ehkki selle elemente saab viia vastavusse või lõimida teiste juhtimissüsteemide omadega.

See dokument sisaldab nõudeid, mida organisatsioon saab kasutada BCMS-i rakendamiseks ja vastavuse hindamiseks. Organisatsioon, kes soovib näidata sellele dokumendile vastavust, saab seda teha järgmiselt:

— esitades enesemääratluse ja enda koostatud deklaratsiooni; või

— taotledes kinnitust oma vastavusele organisatsiooni huvipooltelt, näiteks klientidelt; või

— taotledes kinnitust enda koostatud deklaratsioonile organisatsiooniväliselt osapoolelt; või

— taotledes oma BCMS-i sertifitseerimist/registreerimist mõnelt väliselt organisatsioonilt.

Selle dokumendi peatükkides 1 kuni 3 on esitatud käsitlusala, normiviited ning terminid ja määratlused, mida selle dokumendi kasutamisel kohaldatakse. Peatükid 4 kuni 10 sisaldavad nõudeid, mida tuleb kasutada sellele dokumendile vastavuse hindamisel.

Selles dokumendis kasutatakse järgmisi sõnalisi vorme:

a) „peab“ tähistab nõuet;

b) „peaks“ tähistab soovitust;

c) „on lubatud“ tähistab luba;

d) „võib“ tähistab võimalust või suutlikkust.

Sõnaga „MÄRKUS“ tähistatud teabe eesmärk on anda juhiseid seonduva nõude mõistmiseks või täpsustamiseks. Peatükis 3 kasutatud „MÄRKUSTES“ on toodud lisateave, mis täiendab terminoloogilisi andmeid ja võib sisaldada sätteid termini kasutuse kohta.

1 KÄSITLUSALA

See dokument sätestab nõuded juhtimissüsteemi elluviimiseks, toimivana hoidmiseks ja parendamiseks, kaitsmaks häiringute eest, nende esinemise tõenäosuse vähendamiseks, nendeks valmistumiseks, neile reageerimiseks ja nendest taastumiseks.

Selle dokumendi nõuded on üldised ja mõeldud kohaldamiseks kõikidele organisatsioonidele või nende osadele nende suurusest, tüübist ja olemusest sõltumata. Nende nõuete kohaldatavuse ulatus sõltub organisatsiooni toimimise keskkonnast ja keerukusest.

See dokument on kohaldatav igasuguse suuruse ja tüübiga organisatsioonidele,

a) kes viivad ellu, hoiavad toimivana ja parendavad BCMS-i,

b) kelle eesmärk on tagada vastavus sätestatud talitluspidevuse juhtpõhimõtetele,

c) kes peavad suutma häiringute ajal jätkata toodete ja teenuste pakkumist vastuvõetavas ettemääratud mahus;

d) kes püüavad BCMS-i mõjusa elluviimise kaudu oma vastupidavust suurendada.

Selle dokumendi abil on võimalik hinnata organisatsiooni võimet täita oma talitluspidevuse vajadusi ja kohustusi.

2 NORMIVIITED

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 22300. Security and resilience — Vocabulary

3 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse standardis ISO 22300 ning allpool esitatud termineid ja määratlusi.

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 http://www.electropedia.org/.

MÄRKUS Allpool esitatud terminid ja määratlused asendavad standardis ISO 22300:2018 esitatud termineid ja määratlusi.

3.1
tegevus (*activity*)
ühe või mitme määratletud väljundiga ülesannete kogum

[ALLIKAS: ISO 22300:2018, 3.1, muudetud – määratlus on asendatud ja näide on kustutatud.]

3.2
audit (*audit*)
süstemaatiline, sõltumatu ja dokumenteeritud *protsess* (3.26) auditi tõendusmaterjali hankimiseks ja selle objektiivseks hindamiseks, et määrata kindlaks auditi kriteeriumide täitmise ulatus