

See dokument on EVS-i poolt loodud eelvaade

ÜHISKONDLIK TURVALISUS
Talitluspidevuse juhtimissüsteem
Nõuded

Societal security
Business continuity management systems
Requirements
(ISO 22301:2012)

EESTI STANDARDI EESSÕNA

See Eesti standard on

- Euroopa standardi EN ISO 22301:2014 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 septembris 2014;
- eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2016. aasta augustikuu numbris.

Standardi tõlke koostamise ettepaneku on esitanud tehniline komitee EVS/TK 33 „Juhtimissüsteemid ja vastavushindamine“, standardi tõlkimist on korraldanud Eesti Standardikeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

Standardi on tõlkinud OÜ TJO Konsultatsioonid, standardi on heaks kiitnud EVS/TK 33.

Euroopa standardimisorganisatsioonid on teinud Euroopa standardi EN ISO 22301:2014 rahvuslikele liikmetele kättesaadavaks 23.07.2014. **Date of Availability of the European Standard EN ISO 22301:2014 is 23.07.2014.**

See standard on Euroopa standardi EN ISO 22301:2014 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 22301:2014. 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

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega: Aru 10, 10317 Tallinn, Eesti; koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

English Version

**Societal security - Business continuity management systems -
Requirements (ISO 22301:2012)**

Sécurité sociétale - Systèmes de management de la
continuité d'activité - Exigences (ISO 22301:2012)

Sicherheit und Schutz des Gemeinwesens -
Aufrechterhaltung der Betriebsfähigkeit - Anforderungen
(ISO 22301:2012)

This European Standard was approved by CEN on 17 July 2014.

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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, 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

SISUKORD

EESSÕNA.....	3
0 SISSEJUHATUS.....	4
0.1 Üldist.....	4
0.2 Planeeri-Teosta-Kontrolli-Tegutse (<i>The Plan-Do-Check-Act</i> , PDCA) mudel.....	4
0.3 Selles rahvusvahelises standardis olevad PDCA komponendid.....	5
1 KÄSITLUSALA.....	7
2 NORMIVIITED.....	7
3 TERMINID JA MÄÄRATLUSED.....	7
4 ORGANISATSIOONI KONTEKST.....	15
4.1 Organisatsiooni ja selle konteksti mõistmine.....	15
4.2 Huvipoolte vajaduste ja ootuste mõistmine.....	16
4.3 Talitluspidevuse juhtimissüsteemi (BSMS-i) käsitusala kindlaksmääramine.....	16
4.4 Talitluspidevuse juhtimissüsteem.....	17
5 EESTVEDAMINE.....	17
5.1 Eestvedamine ja pühendumus.....	17
5.2 Juhtkonna pühendumus.....	17
5.3 Juhtpõhimõtted.....	18
5.4 Organisatsioonisisese rollid, kohustused ja volitused.....	18
6 PLANEERIMINE.....	18
6.1 Riskide ja võimaluste käsitlemisele suunatud tegevused.....	18
6.2 Talitluspidevusala eesmärgid ja nende saavutamise planeerimine.....	19
7 TUGI.....	19
7.1 Ressursid.....	19
7.2 Kompetentsus.....	19
7.3 Teadlikkus.....	20
7.4 Teabevahetus.....	20
7.5 Dokumenteeritud teave.....	20
8 TOIMIMINE.....	21
8.1 Toimimise planeerimine ja ohjamine.....	21
8.2 Ärimõju analüüs ja riskihindamine.....	22
8.3 Talitluspidevuse strateegia.....	23
8.4 Talitluspidevuse protseduuride sisseadmimine ja ellurakendamine.....	24
8.5 Harjutamine ja katsetamine.....	26
9 TULEMUSLIKKUSE HINDAMINE.....	26
9.1 Seire, mõõtmine, analüüs ja hindamine.....	26
9.2 Siseaudit.....	27
9.3 Juhtkonnapoolne ülevaatus.....	28
10 PARENDAMINE.....	29
10.1 Mittevastavus ja korrigeeriv tegevus.....	29
10.2 Järjepidev parendamine.....	30
Kirjandus.....	31

EESSÕNA

ISO 22301:2012 teksti on koostanud ISO (*International Organization for Standardization*) tehniline komitee ISO/TC 223 „Societal security“ ja standardina EN ISO 22301:2014 üle võtnud tehniline komitee CEN/TC 391 „Societal and Citizen Security“, mille sekretariaati haldab NEN.

Euroopa standardile tuleb anda rahvusliku standardi staatus kas identse tõlke avaldamisega või jõustumisteatega hiljemalt 2015. jaanuariks ja sellega vastuolus olevad rahvuslikud standardid peavad olema kehtetuks tunnistatud hiljemalt 2015. a jaanuariks.

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse subjekt. CEN [ja/või CENELEC] ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise 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, Slovakkia, Sloveenia, Soome, Šveits, Taani, Tšehhi Vabariik, Türgi, Ungari ja Ühendkuningriik.

Jõustumisteade

CEN on standardi ISO 22301:2012 teksti muutmata kujul üle võtnud standardina EN ISO 22301:2014.

0 SISSEJUHATUS

0.1 Üldist

See rahvusvaheline standard määrab kindlaks nõuded mõjusa talitluspidevuse juhtimissüsteemi (*Business Continuity Management System, BCMS*) loomiseks ja juhtimiseks.

BCMS rõhutab järgneva tähtsust:

- organisatsiooni vajaduste ning talitluspidevuse juhtimise juhtpõhimõtete ja eesmärkide vajalikkuse mõistmise,
- organisatsiooni töökätkestusjuhtumite haldamise üldise võimekuse saavutamiseks ohjemeetmete ja mõõdikute elluviimise ja toimimise,
- BCMS-i tulemuslikkuse ning mõjususe seire ja ülevaatuse ning
- objektiivsel mõõtmisel põhineva järjepideva parendamise.

BCMS-il on sarnaselt teiste juhtimissüsteemidega järgmised võtmekomponendid:

- a) juhtpõhimõtted;
- b) inimesed koos kindlaks määratletud kohustustega;
- c) juhtimisprotsessid, mis seostuvad
 - 1) juhtpõhimõtete,
 - 2) planeerimise,
 - 3) elluviimise ja toimimisega,
 - 4) tulemuslikkuse hindamisega,
 - 5) juhtkonnapoolse ülevaatuse ja
 - 6) parendamisega;
- d) dokumentatsioon, mis annab auditeeritava tõenduse ning
- e) mis tahes organisatsiooni jaoks asjakohane talitluspidevuse juhtimise protsess.

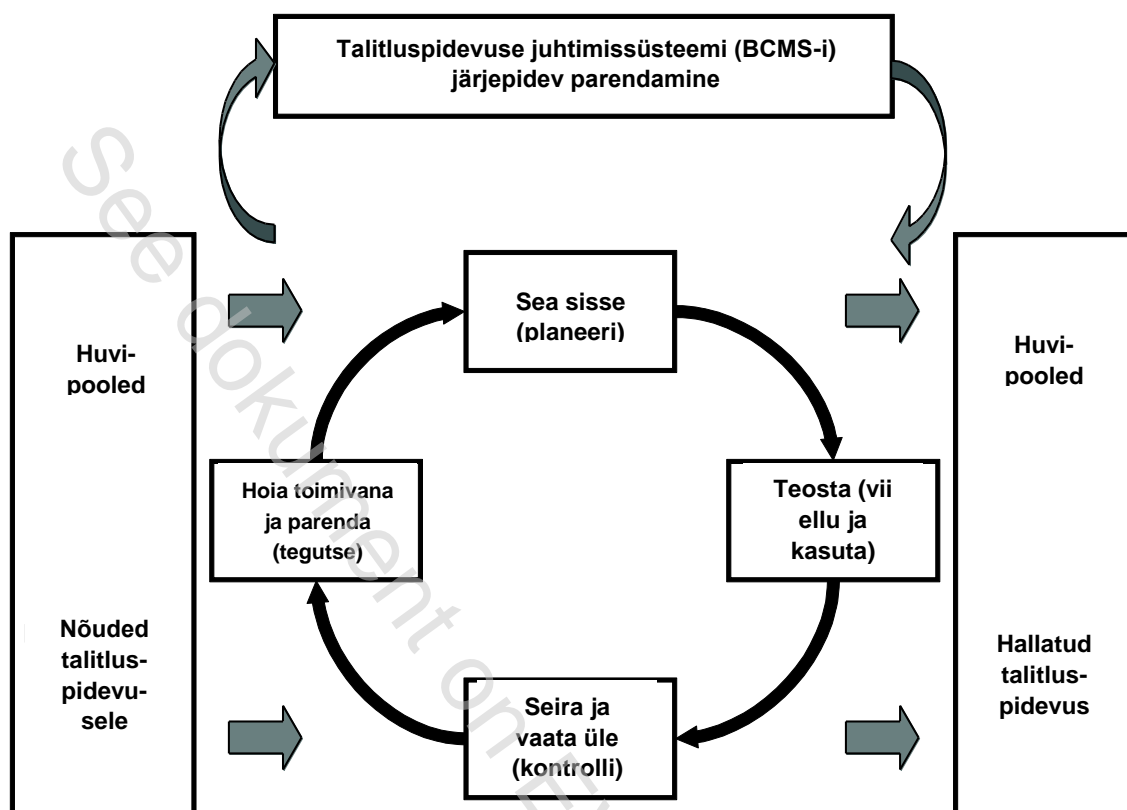
Talitluspidevus aitab kaasa ühiskonna vastupanuvõimelisusele. Taasteprotsessidesse võib olla vaja kaasata laiemat üldsust ja organisatsiooni keskkonna mõju organisatsioonile ja seega ka teisi organisatsioone.

0.2 Planeeri-Teosta-Kontrolli-Tegutse (*The Plan-Do-Check-Act, PDCA*) mudel

See rahvusvaheline standard kohaldab organisatsiooni BCMS-i mõjususe planeerimisele, sisseadmisele, elluviimisele, toimimisele, seirele, ülevaatusele, toimivana hoidmisele ja järjepidevale parendamisele „Planeeri-Teosta-Kontrolli-Tegutse“ (PDCA) mudelit.

Nimetatud mudel tagab teatava koostöökõla teiste juhtimissüsteemide standarditega, nagu ISO 9001 „Kvaliteedijuhtimissüsteemid“, ISO 14001 „Keskkonnajuhtimissüsteemid“, ISO/IEC 27001 „Infoturbe halduse süsteemid“, ISO/IEC 20000-1 „Infotehnoloogia. Teenusehaldus“ ja ISO 28000 „Tarneahela turvalisuse juhtimissüsteemide spetsifikatsioon“, toetades seeläbi seotud juhtimissüsteemidega koostööl olevat ja lõimitud ellurakendamist ning toimimist.

Joonis 1 näitab, kuidas BCMS kasutab sisendina huvipooli, talitluspidevuse juhtimisele esitatavaid nõudeid ning nimetatud vajalike toimingute ja protsesside kaudu toodab nendele nõuetele vastavaid talitluspidevuse väljundeid (st juhitud talitluspidevust).



Joonis 1 — BCMS-i protsessidele kohaldatud PDCA mudel

Tabel 1 — PDCA mudeli selgitus

Planeeri (sea sisse)	Seadke sisse talitluspidevusala juhtpõhimõtted, eesmärgid, ülesanded, ohjemeetmed, protsessid ja protseduurid, mis on vajalikud tulemuste saavutamiseks vastavalt talitluspidevuse parendamiseks, et saavutada tulemuste joendumine organisatsiooni üldiste juhtpõhimõtete ja eesmärkidega.
Teosta (vii ellu ja kasuta)	Viige ellu ja kasutage talitluspidevuse juhtpõhimõtteid, ohjemeetmeid, protsesse ja protseduure.
Kontrolli (seira ja vaata üle)	Seirake protsesse ja vaadake üle tulemuslikkus talitluspidevusala juhtpõhimõtete ja eesmärkide suhtes ning kandke tulemustest ette juhtkonnapoolsel ülevaatusel ning määratlege ja volitage tegevused kõrvaldamiseks ja parendamiseks.
Tegutse (hoia toimivana ja parenda)	Hoidke toimivana ja parendage BCMS-i, rakendades korrigeerivaid tegevusi, mis põhinevad juhtkonnapoolse ülevaatusel ja hindavad ümber BCMS-i käsitusala ning talitluspidevuse juhtpõhimõtteid ja eesmärgid.

0.3 Selles rahvusvahelises standardis olevad PDCA komponendid

Selle rahvusvahelise standardi tabelis 1, peatükkides 4 kuni 10 toodud Planeeri-Teosta-Kontrolli-Tegutse mudel hõlmab järgmisi komponente.

- Peatükk 4 kujutab endast Planeeri komponenti. Selles peatükis tutvustatakse nõudeid, mis on vajalikud BCMS-i konteksti, aga ka vajaduste, nõuete ja käsitusala sisseseadmiseks organisatsioonis kohaldataval kujul.
- Peatükk 5 kujutab endast Planeeri komponenti. See peatükk võtab kokku tippjuhtide rollile esitatavad erinõuded BCMS-is ja määratleb viisi juhtkonnapoolsete organisatsioonile esitatavate ootuste väljendamiseks juhtpõhimõtete avalduse kaudu.

- Peatükk 6 kujutab endast Planeeri komponenti. Selles peatükis kirjeldatakse BCMS-i kui terviku jaoks strateegiliste eesmärkide ja juhtpõhimõtete sisseadmise nõudeid. Peatüki 6 sisu erineb riskianalüüsist ning ärimõju analüüsist (*business impact analysis, BIA*) tuletatud taaste-eesmärkidest tulenevate riskijuhtimisvõimaluste sisseadmisest.

MÄRKUS Ärimõju analüüs ja riskihindamisprotsessi nõuded on täpsustatud peatükis 8.

- Peatükk 7 kujutab endast Planeeri komponenti. See peatükk toetab BCMS-i pädevuse ja korduva / vastavalt vajadusele huvitatud isikutega teabevahetuse sisseadmiseks tehtavaid toiminguid, samaaegselt koostades, ohjates, toimivana hoides ja säilitades nõutavat dokumentatsiooni.
- Peatükk 8 kujutab endast Teosta komponenti. See peatükk määraleb talitluspidevuse nõuded, määrab kindlaks nendega tegelemise viisi ning töötab välja töökatkestusjuhtumite haldamise protseduurid.
- Peatükk 9 kujutab endast Kontrolli komponenti. Selles peatükis on kokku võetud talitluspidevuse juhtimise tulemuslikkuse mõõtmiseks vajalikud nõuded, BCMS-i vastavus sellele rahvusvahelisele standardile ja juhtkonna ootustele ning eesmärk juhtkonnalt ootustele vastamise osas tagasisidet saada.
- Peatükk 10 kujutab endast Tegutse komponenti. Selles peatükis tuvastatakse korrigeerivate tegevuste kaudu BCMS-i mittevastavused ja kasutusele võetavad meetmed.

1 KÄSITLUSALA

See talitluspidevuse juhtimise rahvusvaheline standard sätestab nõuded dokumenteeritud juhtimissüsteemi planeerimiseks, sisseseadmiseks, elluviimiseks, toimimiseks, seireks, ülevaatuseks, toimivana hoidmiseks ja järjepidevaks parendamiseks, kaitsmaks töökatkkestusjuhtumite eest, nende esinemise tõenäosuse vähendamiseks, nendeks valmistumiseks, neile reageerimiseks ja nendest taastumiseks.

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

Selle rahvusvahelise standardi taotluseks ei ole talitluspidevuse juhtimissüsteemi (BCMS) ühetaolisus, vaid organisatsioonipoolne tema vajadustele ning tema huvipoolte nõuetele vastava BCMS-i kavandamine. Nimetatud vajaduste kujundajad on õigusaktid, regulatsioonid, organisatsioonilised ja tööstuse nõuded, tooted ja teenused, rakendatavad protsessid, organisatsiooni suurus ja struktuur ning organisatsiooni huvipoolte nõuded.

See rahvusvaheline standard on kohaldatav igasuguse suuruse ja tüübiga organisatsioonidele, kes soovivad

- a) seada sisse, viia ellu, hoida toimivana ja parendada BCMS-i,
- b) tagada vastavuse sätestatud talitluspidevuse juhtpõhimõtetega,
- c) demonstreerida vastavust teistele,
- d) taotleda oma BCMS-i sertifitseerimist/registreerimist akrediteeritud kolmanda osapoole sertifitseerimisorgani poolt või
- e) teha kindlaks oma tegevuse vastavuse selle rahvusvahelise standardiga ja seda deklareerida.

Selle rahvusvahelise standardi abil on võimalik hinnata organisatsiooni võimet täita oma järjepidevus-alaseid vajadusi ja kohustusi.

2 NORMIVIITED

Alljärgnevalt loetletud dokumendid, mille kohta on standardis esitatud normiviited, on kas tervenisti või osaliselt vajalikud selle standardi rakendamiseks. Dateeritud viidete korral kehtib üksnes viidatud väljaanne. Dateerimata viidete korral kehtib viidatud dokumendi uusim väljaanne koos võimalike muudatustega.

Normiviited puuduvad.

3 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse alljärgnevalt esitatud termineid ja määratlusi.

3.1

tegevus (*activity*)

organisatsiooni poolt (või tema nimel) ühe või mitme toote ja teenuse tootmiseks või toetamiseks läbiviidav protsess või protsesside kogum

NÄIDE Selliste protsesside hulka kuuluvad raamatupidamine, kõnekeskus, IT, tootmine, jaotamine.