TARTU ÜLIKOOL
Arvutiteaduse instituut
Informaatika õppekava

Ilona Peedosk

Euroopa Liidu Digitaalse tegevuskerksuse regulatsiooni DORA võrdlusanalüüs infoturbe standardi ISO/IEC 27001 põhjal

Bakalaureusetöö (9 EAP)

Juhendaja: Sander Saveli, MSc; MBA
Kaasjuhendaja: Heili Orav, PhD

Tartu 2024

Euroopa Liidu Digitaalse tegevuskerksuse regulatsiooni DORA võrdlusanalüüs infoturbe standardi ISO/IEC 27001 põhjal

Lühikokkuvõte:

Bakalaureusetöö eesmärk oli analüüsida Euroopa Liidu digitaalse tegevuskerksuse regulatsiooni DORA nõudeid ISO/IEC 27001 infoturbe standardi põhjal. Analüüsimiseks kasutati võrdlusanalüüsi meetodit. Töös antakse lühiülevaade riskijuhtimisest ja kirjeldatakse digitaalse tegevuskerksuse regulatsiooni. Koostatud võrdlusanalüüs on töös üles ehitatud järgmiselt. Kõigepealt kirjeldatakse kehtima hakkava regulatsiooni nõudeid, millele järgnevalt tuuakse välja ISO/IEC 27001 kontrollide vastavus uue regulatsiooni nõuetega ja tuvastatud puudused. Kokkuvõtvalt esitatakse võrdlusanalüüsi tulemused ja antakse soovitused, kuidas digitaalse tegevuskerksuse regulatsiooni ISO/IEC 27001 infoturbe standardi põhjal rakendada.

Võtmesõnad:

DORA, ISO/IEC 27001, infoturve, IKT-riskijuhtimine

CERCS:

P175 Informaatika, süsteemiteooria

Comparative Analysis of the European Union Digital Operational Resilience Act Based on Information Security Standard ISO/IEC 27001

Abstract:

The purpose of this Bachelor's thesis was to analyze the requirements of the Digital Operational Resilience Act based on the ISO/IEC 27001 information security standard. The comparative analysis method was used for the analysis. A brief overview of risk management and digital operational resilience act is described. The comparative analysis is structured as follows. First, the requirements of DORA are described, then the compliance of the ISO/IEC 27001 controls with the DORA requirements and identified deficiencies. In summary, the results of the analysis are presented and recommendations are given on how to implement the regulation based on the ISO/IEC 27001 information security standard.

Keywords:

DORA, ISO/IEC 27001, information security, ICT risk management

CERCS:

P175 Informatics, systems theory

Sisukord

Sissejuhatus

Finantssektoris on igapäevasel olulisel kohal info- ja kommunikatsioonitehnoloogia, mis toetab ja võimaldab erinevaid tugi- ja äriprotsesse. Digiajastul on finantsettevõtted paljuski digiteeritud, kasutades ettevõttes keerukaid IKT-süsteeme. Lisaks digiteerimisest saadud kasule suurendab digitaalsete teenuste laiaulatuslik kasutamine ettevõtte infotehnoloogia riske (IKT-riske), mis realiseerumisel võivad kahjustada ettevõtte eesmärkide saavutamist. IKT-riskide suurenemisele viitab ka Akmai poolt läbi viidud uuring [1], kus võrreldi Euroopa finantsteenuseid pakkuvate ettevõtete küberrünnakute arvu. Sellest selgub, et 2023. aasta teises kvartalis oli ettevõtete vastu suunatud küberrünnakute arv kasvanud 119% ehk kahekordseks. Eeldatavasti on selle põhjuseks küberkurjategijate rahaline ja poliitiline huvi Euroopa pankade vastu [1]. Seega on oluline, et finantssektori digitaalsed protsessid oleksid vastupidavad ning sektor suudaks kaitsta end küberrünnakute ja teiste IKT-riskide eest.

Alates 2022. aastast on finantssektori IKT-riskijuhtimise valdkonnas aktuaalne Euroopa Liidu uus digitaalse tegevuskerksuse regulatsioon ehk DORA (ingl *Digital Operational Resilience Act*), milles seatud nõudeid tuleb hakata järgima kõikidel Euroopa Liidu liikmesriikidel 2025. aasta algusest [2]. DORA määruse eesmärk on seada nõuded finantssektori digitaalsele tegevuskerksusele ning IKT-riskide juhtimisele. Digitaalne tegevuskerksus on ettevõtte suutlikkus luua ja tagada oma digitaalsete teenuste terviklikkus ja usaldusväärsus [2]. DORA regulatsiooni rakendamiseks, tuleb ettevõttes teha põhjalik eeltöö, et kaardistada püstitatud nõuete sisu ning võrrelda neid juba olemasolevate IKT-riskijuhtimise meetmetega.

Käesoleva bakalaureusetöö eesmärk on analüüsida digitaalse tegevuskerksuse regulatsiooni DORA poolt kehtestatud uusi nõudeid ja anda soovitusi nende rakendamiseks. Eesmärk on tuletatud ühe Eesti finantsettevõtte praktilisest vajadusest olla 2025. aastaks, lähtuvalt seadustest, vastavuses DORA regulatsioonis kehtestatud nõuetega. Regulatsiooni analüüsimiseks kasutatakse võrdlusanalüüsi meetodit, kus võrreldakse DORA nõudeid populaarse ISO/IEC 27001 infoturbe standardi nõuetega. Võrdlemiseks valiti rahvusvaheliselt tunnustatud ISO standard, kuna tegu on sama valdkonda puudutava laia levikuga standardiga [3]. Võrdlus ISO/IEC 27001 standardiga aitab saada praktilist ülevaadet olemasoleva standardi vastavusest uue regulatsiooni nõuetega.

Sellest lähtuvalt uuritakse võrdlusanalüüsis, kas ja mil määral vastavad ISO kontrollimeetmed (edaspidi kontrollid) DORA nõuetele ja kuidas ISO kontrolle täiendada selliselt, et mittevastavusi vähendada. Antud analüüsi aktuaalsust suurendab asjaolu, et DORA

regulatsioon on uus ning valdkonnas puudub varasem praktika (mai 2024) DORA nõuete rakendamisel. Samas tuleneb Euroopa Liidu määrusest kohustus kõigil liikmesriikide finantsvaldkonna ettevõtetel hakata DORA nõudeid 2025. aasta algusest rakendama.

Bakalaureusetöö on jaotatud viieks suuremaks peatükiks. Esimeses peatükis antakse lühiülevaade riskijuhtimisest, selgitades riskijuhtimise protsessi ja IKT-riskijuhtimist finantssektoris. Teises peatükis avatakse digitaalse tegevuskerksuse regulatsiooni DORA, kirjeldatakse DORA eesmärki ja olulisust ning regulatsiooni ülesehitust ja nõudeid. Töö kolmandas peatükis selgitatakse töö metoodikat, põhjendatakse analüüsitavate DORA nõuete, ISO standardi ja analüüsimeetodi valikut. Neljandas peatükis viiakse läbi DORA regulatsiooni võrdlusanalüüs, peatükkide ja artiklite kaupa, kus kõigepealt kirjeldatakse DORA artiklites olevate nõuete sisu, tuuakse välja tuvastatud ISO kontrollid ja nende vastavus DORA nõuetega, kirjeldades tuvastatud puuduseid. Viiendas peatükis esitatakse kokkuvõtvalt võrdlusanalüüsi tulemused ja antakse soovitusi, kuidas ISO kontrolle täiendada, et nad DORA nõuetele vastaksid.

Mõisted ja terminid

DORA (ingl *Digital Operational Resilience Act*): Euroopa Liidu digitaalse tegevuskerksuse regulatsioon [2].

Tegevuskerksus: Ettevõtte suutlikkus luua ja tagada oma tegevuse terviklikkus ning usaldusväärsus [2].

IKT: Info- ja kommunikatsioonitehnoloogia [2].

ISO (ingl *International Organization for Standardization*): Rahvusvaheline standardite organisatsioon [4].

IEC (ingl *International Electrotechnical Commission*): Rahvusvaheline standardite organisatsioon, mis kehtestab elektrooniliste tehnoloogiate standardeid [4].

ISO/IEC 27001: ISO ja IEC ühine infoturbe standard [4].

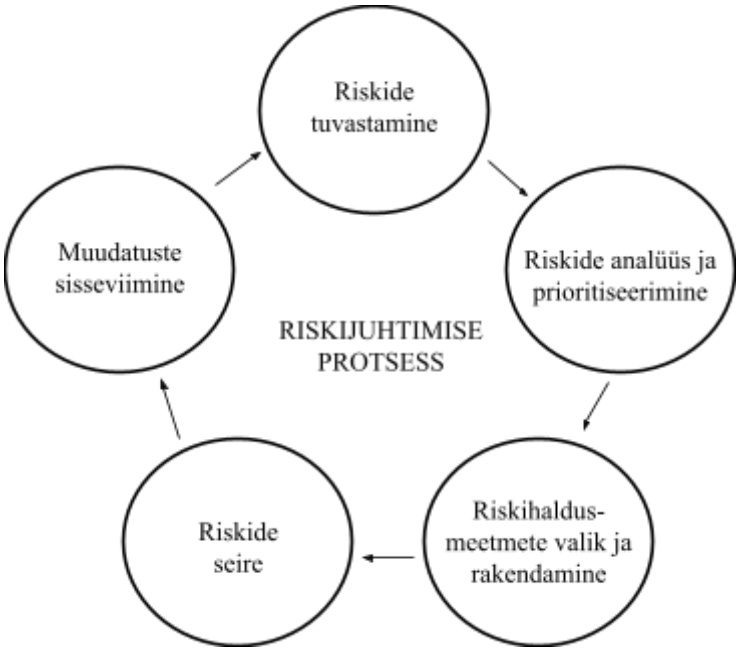
Talitluspidevus (ingl *Business continuity*): Ettevõtte võime säilitada olulised ärifunktisoonid, vältides teenuste katkestusi ja vajadusel taastada nende funktsioonid võimalikult kiiresti [5].

1. Riskijuhtimine

Risk on tõenäoline sündmus, mis võib takistada ettevõtte eesmärkide saavutamist ja millel võib olla negatiivne tagajärg [6]. Selleks, et vältida riskide realiseerumist ja riskidest tulenevat võimalikku kahju on vaja riske juhtida [7]. Selles peatükis kirjeldatakse riskijuhtimise protsessi ja antakse lühiülevaade IKT-riskijuhtimisest finantssektoris.

1.1 Riskijuhtimise protsess

Riskijuhtimise valdkonna eesmärk on tagada asutuse eesmärkide tulemuslik saavutamine [7]. Riskijuhtimine on pidev protsess (joonis 1), mille käigus tuleb esmalt ettevõtte tegevust puudutavad riskid tuvastada, sealjuures välja selgitada riskide põhjus ja päritolu [8]. Seejärel tuleb tuvastatud riske hinnata, analüüsida ja paika panna riskide prioriteedid, vastavalt riski prioriteetsusele saab valida riski käsitlemise strateegia [7]. Kui riski käsitlemise tulemusena otsustatakse, et riski tuleb maandada, rakendatakse riski kontrollimiseks erinevaid kontrolli-meetmeid, mis vähendavad riski esinemise tõenäosust või riski realiseerumise tagajärge [7]. Järgnevalt on vaja riske seirata, et saada teada, kuidas riskijuhtimine toimib ja milliseid muudatusi on protsessis vaja läbi viia [8]. Viimases etapis viiakse sisse muudatused ja vaadatakse kogu protsess üle, et riskijuhtimine oleks piisavalt tõhus [8].



Joonis 1. Riskijuhtimise protsess.

Riskijuhtimise protsess on tsükliline protsess, mis algab uuesti esimesest etapist pärast viimase etapi läbimist [8].

1.2 IKT-riskijuhtimine finantssektoris

Lisaks finantsriskidele on finantssektoris muutumas üha olulisemaks operatsiooniriskide juhtimine [9]. Operatsiooniriskid on riskid, mis tulenevad sisemiste protsesside, inimeste või süsteemide mittetoimimisest oodatud viisil, nende riskide üheks osaks on infosüsteemide poolt põhjustatud riskid ehk IKT-riskid [9].

Laiemalt võib IKT-riski defineerida kui sündmust või olukorda, mis on põhjustatud andmete konfidentsiaalsuse rikkumisest, süsteemide ja andmete terviklikkuse rikkumisest või süsteemide ja andmete kättesaadamatusest [10]. Näiteks on finantssektoris IKT-risk kogemata kliendi andmete jagamine kolmandatele isikutele või näiteks internetipanga käideldavuse probleemid, mille tulemusena ei saa kliendid finantsteenuseid kasutada. Samuti võib IKT-risk olla olukord, mis tekib võimetusest muuta infotehnoloogiat, kui keskkond või ärivajadused seda nõuavad [10]. Lisaks hõlmab IKT-risk turvariske, mis tulenevad ebapiisavatest või ebaõnnestunud siseprotsessidest või välisteguritest [10]. Näiteks kui finantsteenus nagu internetipank, ei ole piisavalt turvaline ja väline osapool suudab ligi pääseda konfidentsiaal-setele andmetele.

Seega saab öelda, et IKT-risk hõlmab kõiki riske, mis on seotud infotehnoloogiaga ning mis riski realiseerumisel võib kahjustada ettevõtet. Kuna IKT-riskid võivad ohustada tugevalt ettevõtte jätkusuutlikkust on oluline IKT-riske juhtida, et asutus oleks võimeline oma strateegilisi eesmärke saavutama [10].

IKT-riskijuhtimises kasutatavad põhimõtted ühtivad eelpool kirjeldatud üldise riskijuhtimise protsessiga. IKT-riskijuhtimises tuleb samamoodi kõigepealt riskid tuvastada, hinnata ja analüüsida ning seejärel neid vajadusel maandada ja seirata kogu protsessi.

2. Digitaalse tegevuskerksuse regulatsioon DORA

Finantssektor on üks rangemalt reguleeritud majandussektoreid [11]. Euroopa Liidu liikmesriikide finantssektorile on Euroopa Liit seadnud mitmeid direktiive ja seadusi, mille eesmärk on reguleerida ja seeläbi edendada ühtset, kuid konkureerivat finantssektorit [12]. Lisaks uutele regulatsioonidele on suurenenud regulatsioonidele mittevastavuse karistus-normid, mis DORA määruse puhul ulatuvad Eestis viie miljoni euroni [13]. Sellest tulenevalt on finantssektoris tegutsevatel ettevõtetel suur kohustus ja stiimul uusi välja töötatud regulatsioone rakendada.

2.1 DORA taust

DORA regulatsioon on Euroopa Liidu määrus nr 2022/2554 [2]. Määruse koostamine sai alguse 2020. aastal, kui Euroopa Komisjon tegi ettepaneku luua nõuded finantssektori digitaalse tegevuskerksuse valdkonnale [14]. DORA määrus anti välja 2022. aastal ja hakkab Euroopa Liidu liikmesriikides kehtima alates 17. jaanuarist 2025 [2]. Selleks tähtajaks peavad kõik finantsasutused, kellele määrus kehtima hakkab, täitma ja järgima määruses olevaid nõudeid. Regulatsiooni on kohustatud järgima liikmesriikide finantsettevõtted, kuhu lisaks krediidiasutustele kuuluvad ka teised finantssektoris tegutsevad asutused: makseasutused, investeerimisühingud, krüptovarateenuste pakkujad jpt [15].

Kuna DORA nõuded kehtivad kõikidele Euroopa Liidu liikmesriikide finantsvaldkondadele, on DORA regulatsiooni kohuslane ka Eesti finantssektor. Kuigi Eesti finantssektorile kohaldub määrus otse, siis on Eesti Rahandusministeerium viinud DORA regulatsiooni vastavusse Eesti seadustega. Rahandusministeerium võttis vastu eelnõu number 23-1460 “Finantskriisi ennetamise ja lahendamise seaduse ning teiste seaduste muutmise seadus”, kus käsitletakse erinevaid finantssektoris kehtivaid seaduseid, kuhu viiakse sisse muudatused eesmärgiga tagada seaduste vastavus kehtima hakkavate DORA nõuetega [13].

2.2 DORA olulisus ja eesmärk

DORA regulatsioon on osa Euroopa Liidu digipaketist, mille eesmärk on finantssektoris toetada digirahanduse innovatsiooni ja konkurentsi ning samal ajal maandada sektoris riske [16]. Finantsvaldkonnas kasutatakse igapäevastes tegevustes keerukaid IKT-süsteeme ja digiteerimist. Kuigi need on loonud sektorisse palju võimalusi, on Euroopa Liidus leitud vajadus suurendada ettevõtete vastupanuvõimet IKT-riskidele, selleks on kehtestatud

järelevalve ja standardid [16]. IKT-süsteemide kasutamine ja digiteerimine on laialt levinud, kuid nende digitaalset tegevuskerksust ehk vastupidavust ei ole käsitletud ja seetõttu pole seda valdkonda piisavalt reguleeritud [2].

DORA regulatsiooniga soovitakse ühtlustada ühetaolist IKT-riskijuhtimist ehk koondada ja ajakohastada IKT-riskidega seotud nõuded, mida varasemalt on käsitletud erinevates määrustes ja direktiivides [16]. Olukorra parandamiseks lõi Euroopa Liit ühise regulatsiooni liikmesriikide finantssektorile, suunates nõuded finantssektori digitaalsele tegevuskerksusele ja IKT-riskide juhtimisele [2]. Täpsemalt kehtestab DORA reeglid IKT-riskijuhtimisele, IKT-intsidentide ehk realiseerunud riskide haldamisele, digitaalse tegevuskerksuse testimisele ja kolmandatest isikutest tulenevale IKT-riskijuhtimisele [2].

2.3 DORA regulatsiooni ülesehitus ja nõuded

DORA määrus koosneb põhitekstist ja eraldi välja antud regulatiivsetest tehnilistest standarditest. Põhitekst on jagatud peatükkideks, mis koosnevad artiklitest. Artiklites on määratud nõuded, mis on iseloomulikud finantssektorile [2].

DORA nõuded on kirjeldatud neljas põhipeatükis. Lisaks on määruses viis peatükki, mis seavad üldiseid sätteid. Põhipeatükkideks on IKT-riskijuhtimine, IKT-intsidentide haldamine ja liigitamine ning nendest teatamine, digitaalse tegevuskerksuse testimine ja kolmandatest isikutest tulenev IKT-riskijuhtimine [17, 2]. Järgnevalt tutvustatakse neid peatükke lähemalt.

IKT-riskijuhtimise peatüki eesmärk on, et finantsettevõttel oleks terviklik IKT-riskijuhtimise raamistik, millega IKT-riske ettevõttes juhtida [17]. Seega esimene peatükk kehtestab nõuded IKT-riskijuhtimise raamistikule [17]. Peatükk on jagatud kaheks osaks, milles kokku on 12 artiklit [2]. Esimeses osas tuuakse välja üldised kriteeriumid IKT-riskijuhtimisele ja selle seosele organisatsiooniga [2]. Teises osas on täpsemad nõuded IKT-riskijuhtimise raamistiku kohta, sisaldades raamistiku põhimõtteid ja nõudeid raamistiku sisule [2].

Teises peatükis kirjeldatakse IKT-intsidentide haldamise põhimõtteid ja nõudeid [17]. IKT-ga seotud intsident on olukord, mis on juhtunud IKT-riski realiseerumisel ehk riski juhtumisel [18]. Need nõuded on jagatud seitsme artikli vahel [2]. Antud artiklid seavad kriteeriumid sellele, kuidas finantsasutused IKT-intsidente haldama peavad, tuuakse nõuded intsidentide haldamisele, liigitamisele ja intsidentidest teavitamisele järelevalveasutustele [2].

Digitaalse tegevuskerksuse testimise peatükk seab nõuded selleks, et digitaalne tegevuskerksus ettevõttes oleks piisavalt tagatud [2]. Digitaalse tegevuskerksuse testimine tähendab ettevõtte digiteenuste vastupidavuse testimist, selgitamaks kui vastupidavad on ettevõttes digitaalsed teenused. Neljas artiklis kehtestatakse nõuded, millele testimine peab vastama, lisaks seatakse nõuded IKT-vahendite ja -süsteemide süvatestimisele [2].

Kolmandatest isikutest tulenev IKT-riskijuhtimise peatükk seab nõuded sellele, milline peab olema IKT-riskijuhtimine, keskendudes IKT-riskidele, mis tulenevad kolmandatest osapooltest, kes pakuvad finantsettevõttele IKT-teenuseid. See peatükk on jagatud kaheks osaks, kus kokku on 17 artiklit [2]. Esimeses osas on kirjeldatud üldised põhimõtted, kuidas kolmandast isikust tulenevat IKT-riski juhtida [2]. Teises osas on spetsiifilisemalt kirjeldatud järelevaatamise raamistik, millega teostada järelevalvet kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele. See osa toob välja erinevad kriteeriumid nii järelevaatamise raamistiku kui ka järelevaatamise asutuste kohta [2].

Eelmainitud nelja põhilise sisulise peatüki järel on regulatsioonis lisaks neli täpsustavat peatükki. Need peatükid seavad üldisemaid nõudeid, mida finantssektoril tuleb seoses DORA regulatsiooniga järgida [2]. Teabe jagamise peatükis tuuakse välja kokkulepped küberohte käsitleva teabe jagamise kohta. Pädevate asutuste peatükis on nõuded erinevate asutustevahelise koostöö teemade kohta. Delegeeritud õigusaktide peatükis on kirjeldatud delegeeritud volituste rakendamise tingimused [2]. Viimane peatükk kehtestab DORA ülemineku- ja lõppsätted, mis koosnevad läbivaatamisklauslist, määruse muudatustest ning määruse jõustumisest ja kohaldamisest [2]. Need peatükid otseseid nõudeid finantsasutustele ei esita.

Peale regulatsiooni väljaandmist koostatakse regulatiivsed tehnilised standardid [14]. Tehnilised standardid väljastatakse peale DORA regulatsiooni ja neid võib nimetada DORA määruse lisadeks [14]. Standardeid töötavad välja Euroopa järelevalveasutused ning standardite eesmärk on tagada DORA regulatsiooni ühtlustamine ja uuendamine [2]. Tehnilisi standardeid peavad finantssektorid järgima samamoodi nagu DORA määrustki [2].

3. Metoodika

Töö eesmärgist lähtudes analüüsitakse Euroopa Liidu regulatsiooni DORA. Analüüsimiseks kasutatakse võrdlusanalüüsi meetodit. Võrdlusanalüüsis võrreldakse DORA regulatsiooni infoturbe standardi ISO/IEC 27001 põhjal. Kuigi DORA nõuete käsitlusala on laiem, valiti nõuete võrdluseks ISO standard, sest antud standardi poolt määratud infoturbe juhtimise süsteem ja selle kontrollimeetmed [19] hõlmavad suurt osa IKT-riskijuhtimise raamistikust ning kattuvad suuresti DORA nõuetega. Teine põhjus ISO standardi valimiseks oli ISO standardi lai levik, mis võimaldas leida ISO rakendamise ja kontrollimeetmete kohta palju praktilist informatsiooni [3]. Selline analüüs pakub suurimat praktilist väärtust, sest ISO standardi laia leviku tõttu on paljud finantsettevõtted seda rakendanud või sellega erinevate teenuste vaates kokku puutunud [3].

3.1 DORA põhitekst

DORA regulatsiooni analüüsimiseks kasutatakse määruse põhiteksti. Lisaks põhitekstile on DORA regulatsioonis regulatiivsed tehnilised standardid, kuid kuna töö koostamise ajal (mai 2024) ei ole kõiki tehnilisi standardeid lõplikus tekstis välja antud, siis piirdutakse selles töös määruse põhitekstis olevate nõuetega. DORA nõuded, mida käesolevas töös analüüsitakse, on jagatud järgmistesse valdkondadesse [2]:

1. IKT-riskijuhtimine,
2. IKT-intsidentide haldamine ja liigitamine ning nendest teavitamine,
3. digitaalse tegevuskerksuse testimine,
4. kolmandast isikust tulenev IKT-riskijuhtimine.

Võrdlusanalüüsi peatükk on jagatud nende valdkondade järgi alapeatükkideks.

3.2 ISO/IEC 27001 standard

ISO/IEC 27001 on ISMS (ingl *information security management system*) standard ehk infoturbe juhtimissüsteemide standard, mis annab ettekirjutuse, millele infoturbe juhtimise süsteem peab vastama [19]. Standard määrab kindlad juhised süsteemi loomiseks, juurutamiseks, jälgimiseks, hooldamiseks ja täiustamiseks [19]. Infoturbe haldussüsteemi eesmärk on kaitsta teabe konfidentsiaalsust, kättesaadavust ja terviklikkust [20]. Konfidentsiaalsuse aspektist ei tohi teave olla kättesaadav volitamata isikutele, kätte-saadavuse aspektist peab teave olema juurdepääsetav volitatud isikutele ning terviklikkuse

aspektist peab teave olema täielik ja täpne [20]. Käesolev ISO/IEC 27001 standard annab ette kontrollimeetmed, mille eesmärk on tagada teabe kaitse eeltoodud kolmest aspektist. Lisaks aitavad kontrollimeetmed organisatsioonil implementeerida, säilitada ja täiustada infoturbe juhtimissüsteeme [21]. Antud standard jagab oma kontrollid nelja kategooriasse [22]:

1. organisatsioonilised kontrollid (ingl *Organizational Controls*),
2. inimeste kontrollid (ingl *People Controls*),
3. füüsilised kontrollid (ingl *Physical Controls*),
4. tehnoloogilised kontrollid (ingl *Technological Controls*).

Standard toob erinevates kategooriates kokku 93 kontrolli [22].

3.3 Võrdlusanalüüs

DORA ja ISO/IEC 27001 võrdlemiseks kasutatakse võrdlusanalüüsi. Võrdlusanalüüs põhineb DORA põhiteksti nõuetel ja nende seostamisel ISO/IEC 27001 2022. aasta versiooni kontrollidega.

Analüüsi alguses tutvuti ISO/IEC 27001 kontrollidega ja nende sisuga, seejärel koostati käesolev analüüs DORA põhiteksti kohta. Kõigepealt töötati läbi põhitekst koos sealsete nõuetega. Seejärel otsiti DORA nõuetele vastavaid kontrolle 2022. aasta ISO kontrollide seast. Lähtuti sellest, et ISO kontroll ei pea täielikult vastama DORA nõuetele, sest vajadusel on võimalus ISO kontrolle vastavalt DORA nõuetele täpsustada. Nõuete ja kontrollide teema kattuvusel seoti ISO kontrollid DORA nõuetega. Kui DORA käsitles teemasid, mida ISO/IEC 27001 standard ei ole käsitlenud, toodi erinevused puudustena välja.

Analüüsi käigus hinnati ISO kontrollide vastavust ja mittevastavust uutele DORA nõuetele. Saadud tulemused annavad ülevaate regulatsiooni ja standardi vastavusest ning aitavad välja selgitada võimalikud puudused. Seejärel saab anda DORA ja ISO kattuvuse kohta hinnangu ja soovitused, milliseid täpsustusi tuleks ISO kontrollide puhul teha, et kontrollid vastaksid DORA regulatsiooni nõuetele. Analüüsi tulemusi saab finantsasutus kasutada DORA rakendamiseks eeldusel, et ISO/IEC 27001 kontrollid on ettevõttes kasutusel.

4. Võrdlusanalüüs

Lõputöö tulemusel valmis võrdlusanalüüs, kus võrreldi DORA regulatsiooni nõudeid ISO/IEC 27001 standardi kontrollidega. Käesolevas peatükis analüüsitakse DORA määruse nelja põhilist teemat ja võrreldakse nõudeid ISO kontrollidega. Antud peatükk jaguneb sarnaselt DORA teemadele neljaks alapeatükiks, kus igas peatükis avatakse DORA artikleid ning tuuakse välja tuvastatud ISO kontrollid ja tuvastatud puudused. Analüüsi eesmärk on välja selgitada, kuidas ISO/IEC 27001 2022. aasta kontrollid vastavad uutele DORA nõuetele ja leida DORA nõuded, millele ISO kontrollid täielikult ei vasta.

4.1 IKT-riskijuhtimine

4.1.1 Artikkel 5 „Juhtimine ja organisatsioon”

Artikli nõuded

Artiklis „Juhtimine ja organisatsioon” (ingl *Governance and organisation*) nõutakse, et finantsettevõttel oleks sisemine juhtimis- ja kontrolliraamistik ning kehtestatakse nõuded juhtorganile ja selle liikmetele. Artiklis määratakse juhtorgani vastutus IKT-riskide juhtimisel ja seatakse nõuded juhtorgani liikmete oskustele ja teadmistele [2].

Tuvastatud kontrollid

ISO kontrollidest vastavad nendele nõuetele järgmised kontrollid [21]:

- 5.1 Infoturbe poliitikad (ingl *Policies for information security*),
- 5.2 Infoturbe rollid ja vastutusalad (ingl *Information security roles and responsibilities*),
- 5.4 Juhtimiskohustused (ingl *Management responsibilities*),
- 5.36 Infoturbe poliitikate, reeglite ja standardite järgimine (ingl *Compliance with policies, rules and standards for information security*).

Tuvastatud puudused

Need kontrollid ei vasta täielikult DORA nõuetele. ISO kontroll 5.2 kehtestab kindlad rollid ja vastutusalad ainult infoturbe valdkonnale, kuid DORA nõuab, et kindlad rollid ja vastutusalad oleksid määratletud laiemalt IKT-riskijuhtimise korraldamiseks. Hõlmates näiteks detailsemalt talitluspidevust ja juhatuse kohustusi riskijuhtimise korraldamiseks. Lisaks käsitletakse selles artiklis kolmanda osapoolega seotud riskijuhtimise ja rollidega

tegevusi ning IKT reageerimis- ja taastamisplaane (ingl *ICT response and recovery plans*), kuid neid tegevusi pole ISO kontrollides kindlalt määratletud.

4.1.2 Artikkel 6 „IKT-riskijuhtimise raamistik”

Artikli nõuded

Artikkel „IKT-riskijuhtimise raamistik” (ingl *ICT risk management framework*) seab nõuded finantsasutuse IKT-riskijuhtimise raamistikule. Raamistik peab sisaldama strateegiaid, põhimõtteid ning IKT-protsesse ja -vahendeid selleks, et ettevõttel oleks võimalus kaitsta oma IKT-varasid. DORA nõuab, et juhtimise raamistik oleks dokumenteeritud, määratleks kindlad vastutusalad ja raamistiku uuendamise tingimused ning sisaldaks digitaalse tegevuskerksuse testimise strateegiat [2].

Tuvastatud kontrollid

IKT-riskijuhtimise raamistiku nõudeid saab siduda järgmiste ISO kontrollidega [21]:

- 5.1 Infoturbe poliitikad (ingl *Policies for information security*),
- 5.29 Infoturve häirete ajal (ingl *Information security during disruption*),
- 5.30 IKT-valmidus talitluspidevuse tagamiseks (ingl *ICT readiness for business continuity*).

Tuvastatud puudused

Teema, mida ISO kontrollides võrreldes DORA nõuetega ei kajastata, on digitaalne tegevuskerksus ja selle testimine. ISO kontrollid 5.29 ja 5.30 kirjeldavad kaudselt tegevuskerksust, kuid keskenduvad kitsamalt IKT-talitluspidevuse juhtimisele. DORA nõuded on põhjalikumad ja käsitlevad ettevõtte tegevuskerksust laiemalt, hõlmates erinevaid talitluspidevuse protsesse.

4.1.3 Artikkel 7 „IKT-süsteemid, -protokollid ja -vahendid”

Artikli nõuded

Artikkel „IKT-süsteemid, -protokollid ja -vahendid” (ingl *ICT systems, protocols and tools*) seab nõuded finantsasutuse IKT-süsteemidele, -protokollidele ja -vahendidele. Artiklis kirjeldatakse, millised peavad olema süsteemid, protsessid ja vahendid selleks, et ettevõte saaks juhtida IKT-riski [2].

Tuvastatud kontrollid

Antud artikli nõudeid saab siduda järgmiste ISO kontrollidega [21]:

- 5.9 Teabe ja muu seotud varade inventuur (ingl *Inventory of information and other associated assets*),
- 5.10 Teabe ja muu seotud varade vastuvõetav kasutamine (ingl *Acceptable use of information and other associated assets*).

Tuvastatud puudused

Selle artikli võrdlemisel ISO kontrollidega puuduseid ei leitud. Tuvastatud ISO kontrollid katavad antud artikli nõudeid.

4.1.4 Artikkel 8 „Kindlaksmääramine”

Artikli nõuded

Artikkel „Kindlaksmääramine” (ingl *Identification*) kehtestab nõuded IKT-riskide määramiseks ehk seab mitmeid juhiseid ja protsesse, kuidas IKT-riske kindlaks määrata ja neid hiljem hallata. Täpsemalt sätestatakse nõuded ärifunktsioonidele, riskipõhjuse tuvastamisele, varade kaardistamisele, asjakohaste andmete säilitamisele, kolmanda isiku teenuste hindamisele ja riskihindamiste läbiviimisele [2].

Tuvastatud kontrollid

Nende nõuetega kattuvad osaliselt järgmised ISO kontrollid [21]:

- 5.7 Ohuluure (ingl *Threat intelligence*),
- 5.9 Teabe ja muu seotud varade inventuur (ingl *Inventory of information and other associated assets*),
- 8.8 Tehniliste haavatavuste haldamine (ingl *Management of technical vulnerabilities*),
- 8.9 Konfiguratsiooni haldus (ingl *Configuration management*).

Tuvastatud puudused

Tuvastatud kontrollid ei vasta täielikult DORA nõuetele. DORA käsitleb põhjalikumalt kolmanda isiku teenuste hindamist ning seab spetsiifilisemad nõuded üldisemale IKT-riski hindamisele.

4.1.5 Artikkel 9 „Kaitse ja ennetus”

Artikli nõuded

Artikli „Kaitse ja ennetus” (ingl *Protection and prevention*) nõuded lähtuvad sellest, kuidas tagada IKT-süsteemide turvalisus ja riskide haldamine. DORA nõuded on kehtestatud IKT-süsteemide seirele ja kontrollile ning üldistele turvalisuse põhimõtetele [2].

Tuvastatud kontrollid

Selleks, et käesolevad DORA nõuded oleksid terviklikult kaetud, tuleb neid siduda paljude ISO kontrollidega [21]:

- 5.1 Infoturbe poliitikad (ingl *Policies for information security*),
- 5.7 Ohuluure (ingl *Threat intelligence*),
- 5.9 Teabe ja muu seotud varade inventuur (ingl *Inventory of information and other associated assets*),
- 5.12 Teabe klassifikatsioon (ingl *Classification of information*),
- 5.14 Infoedastus (ingl *Information transfer*),
- 5.15 Juurdepääsukontroll (ingl *Access control*),
- 5.17 Autentimise teave (ingl *Authentication information*),
- 5.25 Infoturbe sündmuste hindamine ja otsustamine (ingl *Assessment and decision on information security events*),
- 5.26 Infoturbe insidentidele reageerimine (ingl *Response to information security incidents*),
- 5.30 IKT-valmidus talitluspidevuse tagamiseks (ingl *ICT readiness for business continuity*),
- 8.8 Tehniliste haavatavuste haldamine (ingl *Management of technical vulnerabilities*),
- 8.12 Andmelekke vältimine (ingl *Data leakage prevention*),
- 8.16 Seiretegevused (ingl *Monitoring activities*),
- 8.20 Võrkude turvalisus (ingl *Networks security*),
- 8.24 Krüptograafia kasutamine (ingl *Use of cryptography*),
- 8.32 Muutuste juhtimine (ingl *Change management*).

Tuvastatud puudused

Tuvastatud kontrollid vastavad antud artikli nõuetele, seega puuduseid ei tuvastatud.

4.1.6 Artikkel 10 „Avastamine”

Artikli nõuded

Artikkel „Avastamine” (ingl *Detection*) kehtestab nõuded finantssektori ettevõtte protsessidele, mis aitavad tuvastada ettevõttes IKT-intsidente ja seejärel käivitada intsidentidele reageerimise protsessid [2].

Tuvastatud kontrollid

Neid nõudeid katavad järgnevad ISO/IEC 27001 kontrollid [21]:

- 5.24 Infoturbe intsidentide juhtimise planeerimine ja ettevalmistamine (ingl *Information security incident management planning and preparation*),
- 8.16 Seiretegevused (ingl *Monitoring activities*).

Tuvastatud puudused

Enamasti ISO kontrollid katavad artikli nõudeid, kuid DORA lisab mõningaid täpsustusi. Näiteks seab DORA nõuded andmete aruandluse teenuse pakkujate süsteemidele, aga ISO kontrollid seda ei kajasta.

4.1.7 Artikkel 11 „Reageerimine ja taastamine”

Artikli nõuded

Artikkel „Reageerimine ja taastamine” (ingl *Response and recovery*) seab ettevõttele nõuded, kuidas käituda IKT-intsidentide korral ehk kuidas neile reageerida ja vajadusel taastada intsidendile eelnev olukord. Artiklis tuuakse välja talitluspidevuse põhimõtted ja nende rakendamine, nõuded seatakse reageerimis- ja taasteplaanidele ning nende testimisele. Nõuded on kehtestatud talitluspidevuse mõju analüüsimisele, andmete kogumisele ja aruandlusele. Lisaks antakse suunised järelevalveasutustega suhtlemiseks IKT-intidentide teavitamisel [2].

Tuvastatud kontrollid

Selle artikli nõudeid saab siduda kahe ISO kontrolliga [21]:

- 5.26 Infoturbe intsidentidele reageerimine (ingl *Response to information security incidents*),
- 5.30 IKT-valmidus talitluspidevuse tagamiseks (ingl *ICT readiness for business continuity*).

Tuvastatud puudused

Tuvastatud kontrollid vastavad artikli nõuetele, seega puuduseid ISO kontrollides ei leitud.

4.1.8 Artikkel 12 „Varunduspõhimõtted ja -menetlused, ennistamise ja taastamise menetlused ja meetodid”

Artikli nõuded

Artikli „Varunduspõhimõtted ja -menetlused, ennistamise ja taastamise menetlused ja meetodid” (ingl *Backup policies and procedures, restoration and recovery procedures and methods*) nõuete eesmärk on tagada IKT-süsteemide ja andmete ennistamine ning taastamine minimaalse seisuaja ja piiratud katkestuse või kaotusega, olenevalt ettevõtte ärinõuetest. Nõuded sisaldavad kohustust välja töötada varunduspõhimõtted ja -menetlused ning ennistamise ja taastamise menetlused ja meetodid. Lisaks peavad ettevõttel olema varusüsteemid ja eraldatud IKT-süsteemid [2].

Tuvastatud kontrollid

Nendele DORA nõuetele vastavad järgmised ISO kontrollid [21]:

- 5.29 Infoturve häirete ajal (ingl *Information security during disruption*),
- 5.30 IKT-valmidus talitluspidevuse tagamiseks (ingl *ICT readiness for business continuity*),
- 7.10 Andmekandjad (ingl *Storage media*),
- 8.12 Andmelekke vältimine (ingl *Data leakage prevention*),
- 8.13 Teabe varundamine (ingl *Information backup*),
- 8.14 Infotöötlusvahendite koondamine (ingl *Redundancy of information processing facilities*).

Tuvastatud puudused

Tuvastatud ISO kontrollid vastavad artiklis toodud nõuetele, seega puuduseid analüüsi käigus ei tuvastatud.

4.1.9 Artikkel 13 „Õppimine ja areng”

Artikli nõuded

Artikli „Õppimine ja areng” (ingl *Learning and evolving*) nõuded aitavad ettevõttel IKT-intsidentidest õppida. Nõuded seatakse IKT-intsidentide ja IKT-riskijuhtimise protsesside

pidevale uuendamisele ning töötajate koolitamisele, et suurendada teadlikkust IKT ja digitaalse tegevuskerksuse valdkonnas [2].

Tuvastatud kontrollid

ISO kontrollidest katavad neid nõuded järgnevad kontrollid [21]:

- 5.5 Kontakt ametiasutustega (ingl *Contact with authorities*),
- 5.6 Kontakt eri huvirühmadega (ingl *Contact with special interest groups*),
- 5.7 Ohuluure (ingl *Threat intelligence*),
- 5.27 Infoturbe intsidentidest õppimine (ingl *Learning from information security incidents*),
- 8.8 Tehniliste haavatavuste haldamine (ingl *Management of technical vulnerabilities*).

Tuvastatud puudused

Analüüsi käigus puuduseid ei tuvastatud. Tuvastatud ISO kontrollid katavad selle artikli sisu.

4.1.10 Artikkel 14 „Kommunikatsioon"

Artikli nõuded

Artikkel „Kommunikatsioon" (ingl *Communication*) annab ette nõuded selleks, et ettevõttes oleks IKT-riskidega seoses tõhus kommunikatsioon. Täpsemad nõuded seab DORA kriisikommunikatsioonile, üldisele ettevõtteülesele kommunikatsioonipoliitikale ja kommunikatsioonistrateegia rakendamisele [2].

Tuvastatud kontrollid

Selle valdkonna nõuetele vastavad järgmised ISO kontrollid [21]:

- 5.24 Infoturbe intsidentide juhtimise planeerimine ja ettevalmistamine (ingl *Information security incident management planning and preparation*),
- 5.26 Infoturbe intsidentidele reageerimine (ingl *Response to information security incidents*).

Tuvastatud puudused

ISO kontrollid ei nõua ettevõtteülest kommunikatsioonipoliitikat, kuid antud artiklis nõutakse IKT-riskijuhtimise valdkonnaga seotud töötajate vahel kommunikatsioonipoliitikat .

4.1.11 Muud artiklid

IKT-riskijuhtimise peatükis on veel kaks artiklit, artikkel 15 ja 16. Neid artikleid ei võeta võrdlusanalüüsi sisse, sest tegu ei ole niivõrd sisuliste nõuetega, mida käesolevas töös ISO kontrollidega võrrelda. Artikkel 15 kirjeldab edasisi samme Euroopa järelevalveasutuste poolt, et ühtlustada IKT-riskijuhtimise peatükki. Teine artikkel toob lihtsustatult IKT-riskijuhtimise raamistiku nõuded, mis on mõeldud väiksematele finantsasutustele [2].

4.2 IKT-intsidentide haldamine

4.2.1 Artikkel 17 „IKT-intsidentide haldamise protsess"

Artikli nõuded

Artikkel „IKT-intsidentide haldamise protsess" (ingl *ICT-related incident management process*) seab ettevõttele nõuded IKT-intsidentide protsessi haldamiseks, mis sisaldab intsidentide avastamist, haldamist ja teavitamist. Täpsemalt kirjeldatakse, kuidas IKT-intsidente seirata ja järelmeetmeid teostada. DORA nõuab, et ettevõte määratleks kindlad rollid ja ülesanded erinevatele IKT-intsidentidele [2].

Tuvastatud kontrollid

IKT-intsidentide haldamise protsessi nõuetele vastavad järgmised ISO kontrollid [21]:

- 5.5 Kontakt ametiasutustega (ingl *Contact with authorities*),
- 5.6 Kontakt eri huvirühmadega (ingl *Contact with special interest groups*),
- 5.24 Infoturbe intsidentide juhtimise planeerimine ja ettevalmistamine (ingl *Information security incident management planning and preparation*),
- 5.26 Infoturbe intsidentidele reageerimine (ingl *Response to information security incidents*),
- 5.25 Infoturbe sündmuste hindamine ja otsustamine (ingl *Assessment and decision on information security events*),
- 5.27 Infoturbe intsidentidest õppimine (ingl *Learning from information security incidents*),
- 5.28 Tõendite kogumine (ingl *Collection of evidence*),
- 8.16 Seiretegevused (ingl *Monitoring activities*).

Tuvastatud puudused

Selles artiklis on DORA nõuded võrreldes ISO kontrollidega detailsemad. Näiteks on IKT-intsidentide protsessi osas kehtestatud nõuded, kus ettevõte peab lisama protsessi varajased hoiatusindikaatorid ja määratlema rollid ning kohustused, mis aktiveeruvad erinevate IKT-intsidentide stsenaariumite korral. Lisaks tuleb kehtestada kommunikatsiooni-plaanid, mille järgi suheldakse töötajate, väliste osapoolte ja meediaga. Seega vajavad ISO kontrollid DORA nõuete põhjal täiendusi.

4.2.2 Artikkel 18 „IKT-intsidentide ja küberohtude liigitamine"

Artikli nõuded

„IKT-intsidentide ja küberohtude liigitamise" (ingl *Classification of ICT-related incidents and cyber threats*) artikkel seab kriteeriumid sellele, kuidas IKT-intsidente ja küberohte liigitada ja nende mõju hinnata. Täpsemalt kirjeldatakse nõudeid, mis aitavad ettevõttel IKT-intsidente andmete põhjal liigitada. Lisaks seatakse kriteeriumeid küberohtude liigitamiseks [2].

Tuvastatud kontroll

ISO kontrollidest katab osaliselt neid nõudeid järgnev kontroll [21]:

- 5.25 Infoturbe sündmuste hindamine ja otsustamine (ingl *Assessment and decision on information security events*).

Tuvastatud puudused

Selle artikli puhul seab DORA kindlad kriteeriumid, mille alusel liigitada IKT-intsidente ja küberohte. ISO kontrollid seevastu ei sea intsidentide klassifitseerimisele nii täpseid kriteeriume.

4.2.3 Artikkel 19 „Tõsistest IKT-intsidentidest teavitamine ja vabatahtlik teavitamine olulistest küberohtudest"

Artikli nõuded

Artikkel „Tõsistest IKT-intsidentidest teavitamine ja vabatahtlik teavitamine olulistest küberohtudest" (ingl *Reporting of major ICT-related incidents and voluntary notification of significant cyber threat*) toob välja kriteeriumid, millal ja kuidas peab teavitama IKT-intsidentidest ja olulistest küberohtudest. Lisaks kirjeldatakse artiklis, kuidas teavitada kliente tõsiste IKT-intsidentide korral, kuidas esitada järelevalveasutustele raporteid olulistest intsidentidest ja millistel kriteeriumitel edastada teavet teistele asutustele [2].

Tuvastatud kontrollid

Antud artikli nõudeid katavad need ISO kontrollid [21]:

- 5.25 Infoturbe sündmuste hindamine ja otsustamine (ingl *Assessment and decision on information security events*),
- 5.26 Infoturbe intsidentidele reageerimine (ingl *Response to information security incidents*).

Tuvastatud puudused

Selle artikli nõuete juures ISO kontrollides puuduseid ei tuvastatud.

4.2.4 Muud artiklid

DORA selles peatükis on lisaks artiklid 20–23. Neid artikleid võrdlusanalüüsis ei analüüsita, kuna need ei sea otseselt nõudeid finantsasutustele. Seega ei saa neid nõudeid võrrelda ISO kontrollidega [2].

4.3 Digitaalse tegevuskerksuse testimine

4.3.1 Artikkel 24 „Digitaalse tegevuskerksuse testimise üldnõuded”

Artikli nõuded

Artikkel „Digitaalse tegevuskerksuse testimise üldnõuded” (ingl *General requirements for the performance of digital operational resilience testing*) seab nõuded ettevõtte digitaalse tegevuskerksuse testimisele. Täpsemalt seatakse nõuded digitaalse tegevuskerksuse testimise protsessile, mis peab sisaldama erinevaid testimeetodeid ja hindamisi, näiteks nõrkuse hindamine, õhupõhine testimine ja läbistustestimine. Need meetodid aitavad tuvastada ettevõtte tegevuskerksuse tugevusi ja nõrkusi. Lisaks seatakse kriteeriumid läbistustestimise tegevuste läbiviimisele [2].

Tuvastatud kontrollid

Nendele DORA nõuetele vastavad osaliselt järgmised ISO kontrollid [21]:

- 5.30 IKT-valmidus talitluspidevuse tagamiseks (ingl *ICT readiness for business continuity*),
- 8.29 Turvatestimine arenduses ja vastuvõtmisel (ingl *Security testing in development and acceptance*).

Tuvastatud puudused

Kuna ISO kontrollid ei sea tingimusi digitaalse tegevuskerksuse testimisele, siis praegused testimise kriteeriumid kontrollides vajavad suuremaid täiendusi.

4.3.2 Artikkel 25 „IKT-vahendite ja -süsteemide testimine”

Artikli nõuded

Antud artiklis „IKT-vahendite ja -süsteemide testimine” (ingl *Testing of ICT tools and systems*) seatakse nõuded IKT-vahendite ja -süsteemide testimisele. Artikkel annab tervikliku ja süsteemse lähenemise testimisele, tuues välja kriteeriumid, mida testimine peab sisaldama. Näiteks peab testimine sisaldama nõrkuste hindamist, skaneerimist ja läbistustestimist [2].

Tuvastatud kontrollid

Nendele nõuetele vastavad osaliselt järgnevad ISO kontrollid [21]:

- 8.8 Tehniliste haavatavuste haldamine (ingl *Management of technical vulnerabilities*),
- 8.25 Turvaline arenduse elutsükkel (ingl *Secure development life cycle*),
- 8.29 Turvatestimine arenduses ja vastuvõtmisel (ingl *Security testing in development and acceptance*).

Tuvastatud puudused

See artikkel kehtestab põhjalikud nõuded IKT-vahendite ja -süsteemide testimisele. Lisaks tuuakse välja terviklik lähenemine testimisele, kuid sellist lähenemist ISO kontrollides ei ole. Seega on ISO kontrollides puudused testimise kriteeriumites ja nõutud meetodites.

4.3.3 Artikkel 26 „IKT-vahendite, -süsteemide ja -protsesside süvatestimine, mis tugineb ohuteabel põhinevale läbistustestimisele”

Artikli nõuded

Artikkel „IKT-vahendite, -süsteemide ja -protsesside süvatestimine, mis tugineb ohuteabel põhinevale läbistustestimisele” (ingl *Advanced testing of ICT tools, systems and processes based on TLPT*) seab nõuded läbistustestimisele, täpsemalt testimise sagedusele ja sisule. Nõuded on kehtestatud kolmandale osapoolele eeldusel, et nad on testimisse kaasatud. Täpsemad nõuded on määratud tegevustele, mis viiakse läbi pärast testimise etappi, et tõendada testimise vastavust nõuetele. Need tegevused sisaldavad järelduste ja kokkuvõtete tegemist ning tõendite ja lepingute kinnitamist [2].

Tuvastatud kontroll

Antud artikli nõuded saab siduda järgneva ISO kontrolliga [21]:

- 8.29 Turvatestimine arenduses ja vastuvõtmisel (ingl *Security testing in development and acceptance*).

Tuvastatud puudused

Selle artikli juures on ISO kontrollid puudulikud läbistustestimise kriteeriumite juures. Lisaks kehtestatakse nõuded kolmanda osapoole kaasamisele ja koostöö testimisele, kuid need teemad on ISO kontrollides puudu.

4.3.4 Artikkel 27 „Testijatele esitatavad nõuded ohuteabel põhineva läbistustestimise tegemiseks"

Artikli nõuded

Artikkel „Testijatele esitatavad nõuded ohuteabel põhineva läbistustestimise tegemiseks" (ingl *Requirements for testers for the carrying out of TLPT*) seab nõuded testijatele selleks, et testija oleks usaldusväärne ega tekitaks ettevõttesse liigseid riske. Täpsed nõuded seatakse nii sisetestijale kui ka välistestijale [2].

Tuvastatud kontrollid

ISO standardist saab nende nõuetega siduda järgnevad kontrollid [21]:

- 8.29 Turvatestimine arenduses ja vastuvõtmisel (ingl *Security testing in development and acceptance*),
- 8.34 Infosüsteemide kaitse audit testimise ajal (ingl *Protection of information systems during audit testing*).

Tuvastatud puudused

Kontrollides seatakse nõuded testijale, kuid otseselt läbistustestimise testijale nõudeid ei ole.

4.4 Kolmandast isikust tulenev IKT-riskijuhtimine

4.4.1 Artikkel 28 „Üldpõhimõtted"

Artikli nõuded

Artiklis „Üldpõhimõtted" (ingl *General principles*) seatakse üldised nõuded ja põhimõtted kolmandast isikust tulenevale IKT-riskijuhtimisele. Täpsemad nõuded on loodud IKT-teenuste osutajatega seotud lepingutele, kaasa arvatud lepingutest väljumise

strateegiatele. Ettevõtetel tuleb kehtestada kontrolli- ja auditeerimisõigused ning koostada teenusepakkujate kohta riskianalüüsid, et kolmandast isikust tulenev IKT-risk oleks tõhusalt hallatud [2].

Tuvastatud kontrollid

Selle artikli nõudeid saab siduda järgnevate ISO kontrollidega [21]:

- 5.19 Infoturve tarnija suhtes (ingl *Information security in supplier relationships*),
- 5.20 Infoturbe käsitlemine tarnijalepingute raames (ingl *Addressing information security within supplier agreements*),
- 5.30 IKT-valmidus talitluspidevuse tagamiseks (ingl *ICT readiness for business continuity*),
- 5.31 Õiguslik, seadusjärgne, regulatiivne ja lepinguline nõue (ingl *Legal, statutory, regulatory and contractual requirement*),
- 5.35 Infoturbe sõltumatu ülevaade (ingl *Independent review of information security*).

Tuvastatud puudused

Selles artiklis tuvastati puuduseid ISO kontrollides suurel määral. ISO kontrollid kajastavad kolmandatest isikutest tulenevalt riskijuhtimist infoturbe valdkonna vaatest, seega DORA nõuetele need kontrollid täielikult ei vasta. DORA nõuded kolmandast isikust tuleneval IKT-riskijuhtimisel on laiemad, sisaldades riskijuhtimise strateegiat ning erinevaid talitluspidevuse ja teenuse juhtimisega seotud teemasid.

4.4.2 Artikkel 29 „IKT-kontsentratsiooniriski esialgne hindamine”

Artikli nõuded

„IKT-kontsentratsiooniriski esialgse hindamise” (ingl *Preliminary assessment of ICT concentration risk at entity level*) artikkel seab nõuded IKT-ga seotud teenuste lepingute sõlmimise juurde. Ettevõttel tuleb kaaluda alternatiivseid lahendusi ja analüüsida riske, hinnata teenusepakkuja maksejõuetust ning andmete taastamist ja andmekaitsenorme [2].

Tuvastatud kontroll

Selle artikli nõudeid saab siduda järgneva ISO kontrolliga [21]:

- 5.31 Õiguslik, seadusjärgne, regulatiivne ja lepinguline nõue (ingl *Legal, statutory, regulatory and contractual requirement*).

Tuvastatud puudused

See artikkel puudutab kolmandatest isikutest tulevat IKT-riskijuhtimist, kuna ISO kontrollid antud valdkonda piisavalt põhjalikult ei käsitle, tekivad ISO kontrollide juures puudused.

4.4.3 Artikkel 30 „Peamised lepingusätted”

Artikli nõuded

Artikkel „Peamised lepingusätted” (ingl *Key contractual provisions*) seab nõuded ettevõtte ja kolmandate isikute vaheliste IKT-teenuste lepingutele. Artiklis tuuakse välja nõuded, mida peavad sisaldama ja kuidas peavad olema dokumenteeritud nii IKT-teenuste kui ka kriitiliste teenuste lepingud [2].

Tuvastatud kontrollid

Nendele nõuetele vastavad osaliselt järgmised ISO kontrollid [21]:

- 5.20 Infoturbe käsitlemine tarnijalepingute raames (ingl *Addressing information security within supplier agreements*),
- 5.22 Tarnijateenuste jälgimine, ülevaatamine ja muudatuste juhtimine (ingl *Monitoring, review and change management of supplier services*),
- 5.31 Õiguslik, seadusjärgne, regulatiivne ja lepinguline nõue (ingl *Legal, statutory, regulatory and contractual requirement*).

Tuvastatud puudused

DORA on täpsem kriteeriumite juures, mis käsitlevad kolmandaid osapooli. ISO kontrollides seatakse üldisi lepingusätteid ja tingimusi, kuid neid oleks vaja täpsustada kolmandate isikutega seotud riskide seisukohast.

4.4.4 Muud artiklid

Neljandas peatükis on lisaks artiklid 31–44, mis finantsettevõtetele otseselt nõudeid ei sea. Seega käesolevas töös neid nõudeid võrdlusanalüüsis ISO kontollidega ei võrrelda [2].

5. Tulemused

Käesolevas peatükis kirjeldatakse võrdlusanalüüsi tulemusi. Kokkuvõtvad tulemused tuuakse välja DORA põhipeatükkide kaupa, kus kirjeldatakse, kas ja mil määral DORA artiklid ISO kontrollidele vastasid. Lisaks antakse soovitusi, kuidas ISO/IEC 27001 kontrolle täpsustada selliselt, et need kehtiks DORA määrusega.

5.1 Võrdlusanalüüsi tulemused

Järgnevalt on peatükkide kaupa välja toodud võrdlusanalüüsi tulemused. Igas peatükis on kokkuvõttev tabel, mis kirjeldab olulisemaid tulemusi. Tabelites on iga artikli kohta välja toodud, kas analüüsi käigus tuvastati ISO kontrollides puuduseid ja kas ISO kontrollides on vaja teha täpsustusi, et need vastaksid DORA artikli nõuetele.

Küsimusele „Kas tuvastati puudused?” on alltoodud tabelites vastatud kolmel viisil: „Jah, tuvastati”, „Vähesel määral” või „Ei tuvastatud”. Vastus „Jah, tuvastati” näitab, et puudused ISO kontrollides tuvastati ja tuvastatud puudused on suuremamahulised ehk tegemist on suuremate sisuliste mittevastavustega. Vastus „Vähesel määral” tähendab, et puudused tuvastati, kuid tegemist on väikeste puudustega, mida on võimalik ISO kontrollides kergesti täpsustada. Vastus „Ei tuvastatud” tähendab, et ISO kontrollides puuduseid ei tuvastatud.

Küsimusele „Kas on vaja teha täpsustusi?” on vastatud alltoodud tabelites kolmel viisil: „Jah, on vaja teha suuremaid täpsustusi”, „Jah, on vaja teha väiksemaid täpsustusi” ja „Ei ole vaja”. Vastus „Jah, on vaja teha suuremaid täpsustusi” tähendab, et puudused tuvastati ning ISO kontrollides on vaja teha suuremaid sisulisi täiendusi või luua täiesti uued kontrollid, mis vastaksid DORA nõuetele. Vastus „Jah, on vaja teha väiksemaid täpsustusi” näitab, et ISO kontrollides on vaja teha väikesed täiendused, mis tähendavad mõne kontrolli täpsustamist. Vastus „Ei ole vaja” tähendab, et ISO kontrollid vastavad antud artiklile ja ISO kontrolle ei ole vaja täpsustada.

5.1.1 IKT-riskijuhtimise peatüki tulemused

Tabel 1. IKT-riskijuhtimise peatüki tulemused

DORA artikkel	Kas tuvastati puudused?	Kas on vaja teha täpsustusi?
Artikkel 5	Vähesel määral	Jah, on vaja teha väiksemaid täpsustusi
Artikkel 6	Vähesel määral	Jah, on vaja teha väiksemaid täpsustusi
Artikkel 7	Ei tuvastatud	Ei ole vaja
Artikkel 8	Vähesel määral	Jah, on vaja teha väiksemaid täpsustusi
Artikkel 9	Ei tuvastatud	Ei ole vaja
Artikkel 10	Vähesel määral	Jah, on vaja teha väiksemaid täpsustusi
Artikkel 11	Ei tuvastatud	Ei ole vaja
Artikkel 12	Ei tuvastatud	Ei ole vaja
Artikkel 13	Ei tuvastatud	Ei ole vaja
Artikkel 14	Vähesel määral	Jah, on vaja teha väiksemaid täpsustusi

Tabel 1 kirjeldab IKT-riskijuhtimise peatüki artiklite analüüsist saadud kokkuvõtvaid tulemusi. Peatüki analüüsimisel selgus saadud tulemustest, et nendes artiklites kirjeldatud nõuded on ISO kontrollide poolt enamjaolt kaetud. Seega suures mahus puuduseid ISO kontrollides ei tuvastatud. Artiklite 5, 6, 8, 10 ja 14 puhul tuvastati kontrollides puuduseid vähesel määral. Puudused nendes kontrollides ei olnud kuigi mahukad ehk eeldavad väiksemaid täiendusi ISO kontrollide kriteeriumite juurde.

5.1.2 IKT-intsidentide haldamise peatüki tulemused

Tabel 2. IKT-intsidentide haldamise peatüki tulemused

DORA artikkel	Kas tuvastati puudused?	Kas on vaja teha täpsustusi?
Artikkel 17	Vähesel määral	Jah, on vaja teha väiksemaid täpsustusi
Artikkel 18	Vähesel määral	Jah, on vaja teha väiksemaid täpsustusi
Artikkel 19	Ei tuvastatud	Ei ole vaja

IKT-intsidentide haldamise peatükki kirjeldavad tulemused on välja toodud tabelis 2. Selle tabeli kokkuvõtvad tulemused näitavad, et antud artikli peatükkidele ISO kontrollid enamasti

vastavad. Artikli 17 ja 18 puhul tuvastati puuduseid vähesel määral ehk ISO kontrollid vajavad väiksemaid täiendusi, et vastavus DORA nõuetega oleks täielik. Enamasti on IKT-intsidentide haldamise peatüki nõuded ISO kontrollidega kaetud.

5.1.3 Digitaalse tegevuskerksuse testimise peatüki tulemused

Tabel 3. Digitaalse tegevuskerksuse testimise peatüki tulemused

DORA artikkel	Kas tuvastati puudused?	Kas on vaja teha täpsustusi?
Artikkel 24	Jah, tuvastati	Jah, on vaja teha suuremaid täpsustusi
Artikkel 25	Jah, tuvastati	Jah, on vaja teha suuremaid täpsustusi
Artikkel 26	Jah, tuvastati	Jah, on vaja teha suuremaid täpsustusi
Artikkel 27	Vähesel määral	Jah, on vaja teha väiksemaid täpsustusi

Tabel 3 kirjeldab digitaalse tegevuskerksuse testimise peatüki analüüsimisel saadud tulemusi. Kokkuvõtvad tulemused näitavad, et antud teemat ISO kontrollid otseselt ei kajasta ja puudused tuvastati iga artikli juures. Enamasti olid tuvastatud puudused suuremahulised. Selleks, et ISO kontrollid kataksid DORA nõudeid, tuleb kontrollidesse lisada täiendusi, mis kehtestaksid kriteeriumid digitaalse tegevuskerksuse testimisele. Töö autori arvates oleks siinkohal mõistlikum ISO kontrollide juurde lisada uued kontrollid, mis vastaksid antud DORA nõuetele.

5.1.4 Kolmandatest isikutest tuleneva IKT-riskijuhtimise peatüki tulemused

Tabel 4. Kolmandatest isikutest tuleneva IKT-riskijuhtimise peatüki tulemused

DORA artikkel	Kas tuvastati puudused?	Kas on vaja teha täpsustusi?
Artikkel 28	Jah, tuvastati	Jah, on vaja teha suuremaid täpsustusi
Artikkel 29	Jah, tuvastati	Jah, on vaja teha suuremaid täpsustusi
Artikkel 30	Jah, tuvastati	Jah, on vaja teha suuremaid täpsustusi

Tabelis 4 on toodud kolmandatest isikutest tuleneva IKT-riskijuhtimise peatüki tulemused. Kokkuvõtvatest tulemustest on selgelt märgata, et antud artiklite nõuded ISO kontrollidele ei vasta. Selles peatükis on iga artikli juures tuvastatud kontrollides suuremahulised puudused.

Kuna selle peatüki teemasid ja nõudeid ISO standard ei käsitle, on vaja teha suuremaid täpsustusi või luua uusi kontrolle, mis vastaksid spetsiifilisemalt DORA nõuetele.

5.2 Soovitused

Võrdlusanalüüsis tuvastati mittevastavusi ISO/IEC 27001 kontrollide ja DORA nõuete vahel. Analüüsi eesmärk oli kindlaks teha, kuidas ISO kontrollid katavad DORA nõudeid ja tuvastada, millised puudused ISO kontrollides võrreldes DORA nõuetega esinevad. Tulemustest selgus, et teemade kaupa olid ISO kontrollides suuremad ja väiksemad puudused. Selleks, et ISO kontrollid vastaksid DORA nõuetele, vajaksid kontrollid täiendusi.

Esimeses peatükis „IKT-riskijuhtimine" ja teises peatükis „IKT-intsidentide haldamine" olid tuvastatud puudused ISO kontrollides väikesed ja enamjaolt katsid olemasolevad ISO kontrollid antud peatükkide nõudeid. Nende kahe peatüki puhul soovitab töö autor lisada ISO kontrollidesse täpsustusi vastavalt tuvastatud puudustele ehk täiendada puuduseid vastavalt DORA nõuete kriteeriumitele.

Kõige suuremad puudused tuvastati kolmandas peatükis „Digitaalse tegevuskerksuse testimine" ja neljandas peatükis „Kolmandatest isikutest tulenev IKT-riskijuhtimine". Antud peatükke katsid ISO kontrollid kõige vähem. Siinkohal soovitab töö autor luua ISO kontrollide juurde mõned uued kontrollid, mis vastaksid eelpool nimetatud DORA peatükkide sisule. Töö autor leiab, et mõistlikum oleks luua uued kontrollid, sest olemasolevate ISO kontrollidega oli kattuvus pigem väike. Seetõttu oleks vaja tuvastatud kontrolle põhjalikult täiendada. Uute kontrollide loomine oleks eeldatavasti arusaadavam ja lihtsam.

Võrdlusanalüüs annab hea aluse DORA edukaks rakendamiseks ettevõttes, milles on ISO/IEC 27001 infoturbe juhtimissüsteem või selle elemente kasutatud. Sellisel juhul annab töö hea ülevaate DORA mittevastavusest olemasoleva IKT-riskijuhtimise süsteemiga. Lisaks selgusid töö tulemusel DORA nõuded, millega esmajärjekorras tegeleda, et likvideerida suuremad mittevastavused. See aitab ettevõttes tõsta efektiivsust ja hoida kokku ressursse uute regulatsioonidega vastavuse saavutamiseks.

Kokkuvõte

Töös anti lühiülevaade riskijuhtimise protsessist ning IKT-riskijuhtimisest finantssektoris ja kirjeldati uue digitaalse tegevuskerksuse regulatsiooni DORA olemust. Bakalaureusetöö põhieesmärk oli analüüsida digitaalse tegevuskerksuse regulatsiooni. Selle analüüsimiseks kasutati võrdlusanalüüsi meetodit ehk uut regulatsiooni analüüsiti laialdaselt levinud infoturbe standardi ISO/IEC 27001 põhjal. Võrdlusanalüüsis kasutati uute nõuete analüüsimiseks ISO/IEC 27001:2022 standardi kontrolle. Analüüsi eesmärk oli tuvastada puudused ISO kontrollides ja anda soovitusi ISO kontrollide täiendamiseks nii, et need vastaksid võimalikult palju DORA poolt kehtestatud nõuetele.

Analüüsi tulemusel selgus, kas ja mil määral ISO/IEC 27001 kontrollid vastavad DORA nõuetele. Võrdlusanalüüsi tulemustest tuli välja, et DORA kolmas ja neljas peatükk olid võrreldes ISO kontrollidega spetsiifilisemad ning sätestasid nõudeid, mida ISO standard ei kehtesta. Esimeses ja teises peatükis vastasid ISO kontrollid enamjaolt DORA nõuetele, kuid tuvastati puudused, mis eeldavad väiksemaid täiendusi ISO kontrollides. Sellest lähtuvalt soovitab töö autor alustada DORA vastavuse saavutamiseks esmajärjekorras DORA regulatsiooni kolmanda ja neljanda peatüki nõuete analüüsi ja kontrollide täiendamisega, sest seal esineb suuremaid mittevastavusi ISO standardi kontrollidega.

Töö annab hea aluse, kuidas DORA nõudeid konkreetses finantsasutuses rakendada eeldusel, et ettevõttes on kasutusel ISO/IEC 27001 standardi kontrollimeetmed. Käesolevas töös analüüsiti DORA põhinõudeid, kuid regulatiivsed tehnilised standardid jäid analüüsist välja. Töö võimalik edasiarendus võiks olla DORA regulatiivsete tehniliste standardite analüüsimine ISO/IEC 27001 kontrollidega. Samuti võib analüüsida DORA regulatsiooni mõne teise infoturbe standardi ja kontrollimeetmete põhjal.

Viidatud kirjandus

[1] Muncaster P. Attacks on European Financial Services Double in a Year. Infosecurity Magazine 2023. https://www.infosecurity-magazine.com/news/emea-financial-services-attacks/ (08.03.2024)

[2] EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) 2022/2554, 14. detsember 2022, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/101. Euroopa Liidu Teataja 27.12.2022. https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32022R2554 (14.05.2024)

[3] Culot G., Nassimbeni G., Podrecca M., Sartor M. Information security and value creation: The performance implications of ISO/IEC 27001. Computers in Industry 2022. https://www.sciencedirect.com/science/article/abs/pii/S0166361522001415 (10.05.2024)

[4] Loshin P. ISO (International Organization for Standardization). TechTarget 2021. https://www.techtarget.com/searchdatacenter/definition/ISO (27.11.2023) (võib vajada sisse logimist)

[5] Gillis A. S. business continuity. TechTarget 2024. https://www.techtarget.com/searchdisasterrecovery/definition/business-continuity (10.05.2024)

[6] Stanford University. Definition of Risk. https://ocro.stanford.edu/enterprise-risk-management-erm/key-definitions/definition-risk (19.03.2024)

[7] Riskijuhtimise protsessi hindamine. Juhendmaterjal täidesaatva riigivõimu asutustele. Sisekontrolli koordineerimise talitus, Finantskontrolli osakond, Rahandusministeerium. Detsember 2013. https://fin.ee/sites/default/files/documents/2020-10/riskijuhtimise_protsessi_hindamine.pdf (14.05.2024)

[8] Unit21. Risk Management in Banking: Types + Best Practices for Mitigation. 2023. https://www.unit21.ai/blog/risk-management-in-banking (20.03.2024)

[9] Nõuded operatsiooniriski juhtimise korraldamiseks. Finantsinspektsioon 2019. https://www.fi.ee/sites/default/files/2019-08/N%C3%B5uded%20operatsiooniriski%20juhtimise%20korraldamiseks%20uus%20redaktsioon%20ET_0.pdf (08.05.2024)

[10] Final Report: EBA Guidelines on ICT and security risk management. European Banking Authority 2019.
https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/december/guidelines-on-ict-and-security-risk-management.pdf (10.03.2024)

[11] Schick B. GUIDE: How to Market in Highly Regulated Industries. Meshagency 2023. https://meshagency.com/guide-how-to-market-in-highly-regulated-industries/ (10.05.2024)

[12] Casu B., Girardone C., Molyneux P. Introduction to Banking. Pearson Education Limited 2006. https://www.academia.edu/40429609/INTRODUCTION_TO_BANKING (14.05.2024)

[13] Finantskriisi ennetamise ja lahendamise seaduse ning teiste seaduste muutmise seadus. RAM ja EIS number 23-1460. Eelnõude infosüsteem. Rahandusministeerium. 2023. https://eelnoud.valitsus.ee/ (14.05.2024)

[14] Weinberg A. D. 12 Essential Steps to Become Compliant with the DORA Act.
Cybeready 2023.
https://cybeready.com/digital-operations-and-resilience-act-dora/become-compliant-with-the-dora-act (06.03.2024)

[15] DORA määruse mõjud õigus- ja IT-osakondadele. KPMG 2023.
https://kpmglaw.ee/artiklid/dora-maaruse-mojud-oigus-ja-it-osakondadele (08.03.2024)

[16] EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014 ja (EL) nr 909/2014. 24.09.2020. Euroopa Liidu Väljaannete Talitus. 2022.
https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52020PC0595
(08.03.2024)

[17] pwc. DORA: Framework for management of digital risks in Financial Markets. https://www.pwc.com/cz/en/temata/dora-regulation.html (08.03.2024)

[18] Law Insider. ICT-related incident definition. https://www.lawinsider.com/dictionary/ict-related-incident (16.02.2024)

[19] ISO. ISO/IEC 27001:2022. https://www.iso.org/standard/27001 (28.11.2023)

[20] Understanding ISO 27001:2022: People, process, and technology. KPMG 2023. https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2023/understanding-iso27001-2022-people-process-technology_v8.pdf (30.11.2023)

[21] International Organization for Standardization & International Electrotechnical Commission. Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27001:2022). 2022.

[22] Secureframe. ISO 27001 Controls Explained: A Guide to Annex A. https://secureframe.com/hub/iso-27001/controls (14.05.2024)

Litsents

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Ilona Peedosk,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „Euroopa Liidu Digitaalse tegevuskerksuse regulatsiooni DORA võrdlusanalüüs infoturbe standardi ISO/IEC 27001 põhjal", mille juhendaja on Sander Saveli ja kaasjuhendaja on Heili Orav, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Ilona Peedosk
15.05.2024