Tallinna Ülikool

Informaatika Instituut

IT teenuste talitluspidevuse planeerimine avaliku sektori organisatsiooni näitel

Magistritöö

Autor: Kristjan Pedak

Juhendaja: prof Peeter Normak

Kaasjuhendaja: Meelis Karp

Autor: ..... „ ..... „2012

Juhendaja: ..... „ ..... „2012

Kaasjuhendaja: ..... „ ..... „2012

Instituudi direktor: ..... „ ..... „2012

Tallinn 2012

Autorideklaratsioon

Deklareerin, et käesolev magistritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

....
(kuupäev) (autor)

Sisukord

1. Sissejuhatus

1.1 Teema valiku põhjendus ja aktuaalsus

Tänapäeval tagavad paljudes organisatsioonides, sõltumata nende tegevusvaldkonnast, suure osa põhiprotsesside tööst infotehnoloogilised lahendused. Põhiprotsesse toetavad mitmed IT teenused, mistõttu peab olema tagatud nende stabiilne toimimine, eriti juhul, kui teenuseid on palju ja need on üksteisest sõltuvuses (Reiska, 2010).

IT teenuste omavahelise ühendatuse tõttu võib ühe teenuse katkemine mõjutada teiste kättesaadavust. Nende ebapiisav kaitse või puudulik reageerimisvõime suurendab riketest või rünnakutest tulenevate ohtude mõju. Seetõttu nõuab oluliste IT teenuste jätkusuutlikkuse tagamine ja kiire taastamise võimekus erilist tähelepanu (Kaitseministeerium, 2010).

Talitluspidevuse haldus on temaatika, millega varem või hiljem peavad kokku puutuma kõik organisatsioonid. Tavapäraste suurõnnetuste puhul tagatakse operatiivne reageerimis- ja koostöötegevus asutuste osalemisega perioodilistel kriisiõppustel, mille raames harjutatakse riigi võimekust tulla toime erinevate õnnetuste ja ohtudega. Sarnaselt suurõppustele on tähtis, et ka asutusesisestes struktuuriüksustes harjutatakse toimetulekut kriisisituatsioonides ja viiakse läbi õppusi, juhuks kui intsident peaks aset leidma organisatsiooni siseselt. Olukorras, kus IT teenused tagavad suure osa organisatsiooni põhifunktsioonide toimivusest on oluline, et IT struktuuriüksustes harjutatakse regulaarselt läbi erinevaid ohustsenaariumeid. Olukordade läbimängimine eeldab aga toimivat IT talitluspidevuse korraldust koos talitluspidevuse ja taasteplaanidega millele õnnetusjuhtumite korral tugineda. Organisatsioonide valmisolek kriisilukordadeks on pälvinud ülemaailmselt suuremat tähelepanu alates 2001. aastast, mistõttu iga uue kriisi aset leidmine on taas esile tõstnud valmisoleku tähtsuse antud situatsioonideks. (Clas, 2008)

Paljud organisatsioonid on loonud endale ohtliku illusiooni ja leiavad, et suuremat sorti IT teenuste katkestused on nende puhul välistatud või omavad nende jaoks piisavalt väikest mõju (Jaques, 2006). Tänased kliendid nõuavad aga teenuse osutajaid, kellele saab loota nii ööpäeva- kui ka aastaringselt (Clas, 2008).

Chartered Management Institute viis 2008. aastal läbi talitluspidevuse alase uuringu Inglismaal, milles osales 754 vastajat era- ja avalikust sektorist. Tulemustest selgus, et talitluspidevuse plaane pidas „oluliseks“ või „väga oluliseks“ 76% vastanutest, samas kui reaalsed plaanid eksisteerisid vaid 47% organisatsioonides. Muuhulgas oli välja toodud, et suurimaid häireid organisatsioonide töös põhjustab IT (43%) (Chartered Management Institute, 2008).

Olukorda ilmestab ka EMC poolt 2011. aastal Euroopas läbi viidud uuring, milles osales 1750 IT-alaste otsuste vastuvõtjat suurematest era- ja avaliku sektori organisatsioonidest. Uuringu eesmärk oli selgust saada, millisel määral tunnetavad organisatsioonid oma valmisolekut erinevate õnnetusjuhtumitega toimetulekuks. Tulemustest selgus, et 74% organisatsioonidest ei ole kindlad oma võimes katastroofist täielikult taastuda. Muuhulgas selgus, et 54% organisatsioonidest on viimase aasta jooksul kogenud andmete kadu ja kannatanud süsteemide maasoleku tõttu. Samuti toodi välja, et 61% vastanutest peab suurimaks andmete kao ja maasoleku aja põhjustajaks just riistvaralisi rikkeid (EMC, 2011).

Eestis läbi viidud uuringutest võib esile tuua kohaliku infotehnoloogia ettevõtte Net Groupi 2010. aastal läbi viidud IT uuringu, milles osales 200 organisatsiooni. Uuringu eesmärk oli välja selgitada, millisel määral panustavad Eestis tegutsevad keskmise suurusega ettevõtted andmete varundamisse ja kui oluliseks peetakse andmeid ettevõtte jätkusuutliku arengu tagamiseks. Uuringust selgus, et paljudes ettevõtetes pole andmed dubleeritud ja nende taastamiseks puuduvad konkreetsed plaanid. Täpsemalt selgus, et ligi 25% vastanutest puudub tegevusplaan ärikriitiliste andmete varundamiseks ja taastamiseks. Küsitletud ettevõtetest 32% arvab, et andmed on võimalik taastada kahe tunni jooksul; veerand firmadest suudab andmed taastada 6 tunni jooksul. Samas ei oska 18% öelda kui kiiresti suudetakse nende ettevõttes ärikriitilisi andmeid taastada. Uuringust selgus ka, et enamus ettevõtteid hindab ärikriitiliste andmete väärtuseks vähemalt miljon krooni (st ligi 64 000 EUR). Sellest hoolimata puudub paljudel firmadel andmete varundamise või taastamise plaan (Kongo, 2010).

Eelnevalt välja toodud uuringutele tuginedes võib väita, et talitluspidevusega seotud valdkonda peetakse küll üsna oluliseks ja teadvustatakse selle järgi vajadust, mida peegeldab ka paljude organisatsioonide väide plaanide olemasolu kohta, kuid reaalseid varundamis- ja taasteplaane ei oma endiselt märkimisväärne hulk organisatsioone.

Organisatsiooni suurimaks varaks töötajate kõrval on informatsioon ehk olulised äriandmed. Elektrooniliste andmete varundamist ja edukat taastamist võib pidada IT talitluspidevuse põhiosaks, mis võib õnnetusjuhtumi korral päästa organisatsiooni halvimast. Samas probleemid ärikriitiliste andmete taastamisega võivad seisata organisatsiooni töö pikaks ajaks ja halvimal juhul lõpetada organisatsiooni tegevuse. Sellest tulenevalt võib eelpool välja toodud uuringute tulemuste põhjal järeldada, et organisatsioonid, kus vastavaid plaane ei eksisteeri või kus need on olemas, aga regulaarset testimist ei teostata, ebaõnnestuvad kriitilises situatsioonis. Eelnevat järeldust toetab ka Eesti tuntud tehnoloogiaspetsialisti Tõnu Samueli arvamus, mille kohaselt firmades ei tööta vähemalt 50% varunduslahendustest siis, kui neid läheb reaalselt vaja. (Kongo, 2010)

Lisaks võib järeldada, et kui organisatsioonidel puuduvad plaanid andmete varundamiseks ja taastamiseks, siis puuduvad neil ka plaanid talitluspidevuse ja taastamisega seonduva korraldamiseks õnnetusjuhtumi korral.

1.2 Probleemi sõnastus

Magistritöös käsitletavas avaliku sektori organisatsioonis ei ole töö kirjutamise ajal IT teenuste talitluspidevuse haldusega seonduvale pööratud rohkem tähelepanu kui elektroonilise informatsiooni igapäevane varundamine. Aeg-ajalt on ette tulnud erinevate süsteemide üksikute informatsioonielementide taastamise vajadus, mis on taasteprotsessi ka edukalt läbinud, kuid hetkel puudub üldine teadmus ühe või mitme süsteemi eduka taastamise võimalikkuse kohta. Samuti puuduvad ettekirjutatud plaanid ja protseduurid ning varasem kogemus erinevate süsteemide täieliku taastamise kohta IT katastroofide korral.

1.3 Töö eesmärk

Magistritöö peamine eesmärk on välja töötada IT teenuste talitluspidevuse tagamise üldskeem, arvestades vastava temaatika rahvusvahelist tava ja praktikat ning organisatsioonide soovitusi, millele tuginedes on töös käsitletaval avaliku sektori organisatsioonil võimalik talitluspidevuse protsessi planeerimisel juhinduda. Töö alameesmärgiks on organisatsiooni olulisemate IT teenustega seotud süsteemide

taasteprotseduuride loomine, valideerimine ja seeläbi taastamise võimalikkuse väljaselgitamine IT katastroofide korral.

1.4 Uurimismetoodika

Käesolevas töös otsitakse vastust küsimusele „Kuidas korraldada IT teenuste talitluspidevuse halduse protsessi, sealhulgas koostada IT talitluspidevus- ja taasteplaane?“. Sellise küsimusepüstituse korral sobib antud uurimuse läbiviimiseks kvalitatiivne uurimismeetod, millest lähtuvalt valis autor selle läbiviimiseks kirjanduse ja juhtumianalüüsi. Juhtumianalüüs võimaldab nähtust tema loomulikus keskkonnas sügavuti uurida, tuginedes mitmetele erinevatele infoallikatele ja vaatenurkadele. (Kuusk, 2006) Juhtumianalüüsile iseloomulikud tunnused on:

- Uurimuse sügavus/põhjalikkus;
- fookus detailidel mitte üldisel;
- uuritakse suhteid ja protsesse mitte tulemusi;
- reaalsed situatsioonid elust enesest mitte kunstlikult tekitatud (Naaris & Vaidlo, 2010).

Töös tuginetakse elektroonilistele teabeallikatele – kasutatud artiklites, õppematerjalides, raamatutes ja veebilehtedel avaldatud teabe näol on tegemist tunnustatud standardite ning metoodikatega, mistõttu enamus neist on leitavad ametlikel veebilehtedel.

1.5 Töö struktuur

Magistritöö koosneb viiest peatükist. Eraldiseisvateks osadeks on kasutatavad mõisted, mõistete seletused ja lisad.

Esimene peatükk on sissejuhatus, mis annab ülevaate teema valiku põhjendusest ja aktuaalsusest, probleemi sõnastusest, töö eesmärgist, uurimismetoodikast ning töö struktuurist.

Teises peatükis tutvustatakse vajaliku taustainformatsioonina äri talitluspidevuse haldusega seonduvat - antakse ülevaade äri talitluspidevuse haldusest, defineeritakse mõiste ja

kirjeldatakse eesmärke. Samuti esitatakse loend levinumatest metoodikatest, tutvustatakse äri talitluspidevuse halduse elutsüklit ja selle etappe ning seotust IT teenuste talitluspidevuse haldusega.

Kolmandas peatükis käsitletakse lähemalt IT teenuste talitluspidevuse haldust, mille raames antakse ülevaade IT teenuste talitluspidevuse halduse protsessi eesmärkidest, tuuakse välja protsessi elutsükkel ja selles sisalduvad etapid (talitluspidevuse protsessi algatamine, nõuete ja analüüsi etapp, talitluspidevuse juurutamine ning igapäevane haldus).

Neljandas peatükis kirjeldatakse lähemalt IT teenuste talitluspidevuse tagamise üldskeemi, mis sisaldab üksikasjalike tegevuste ja soovituste loetelu, millele tuginedes võiks avaliku sektori organisatsioon talitluspidevuse protsessi planeerimisel juhinduda. Muuhulgas tuuakse välja soovitused projekti algatamiseks, ärimõjude analüüsi ja riskide hindamise läbiviimiseks, strateegia loomiseks, IT talitluspidevus- ja taasteplaanide loomiseks, plaanide testimiseks ning igapäevaseks halduseks.

Viiendas peatükis antakse ülevaade olulisemate IT teenustega seotud süsteemide taasteprotseduuride loomise protsessist avaliku sektori organisatsioonis, sealhulgas vajadusest, eesmärkidest ja tulemustest ning ettepanekutest edaspidiseks.

2. Äri talitluspidevuse haldus

Käesolevas magistritöös on kasutusel termin „äri talitluspidevuse haldus“, milles sisalduva sõna „äri“ all peetakse silmas organisatsiooni ja sellest tulenevalt on termini „äri talitluspidevuse haldus“ all mõeldud „organisatsiooni talitluspidevuse haldust“. Antud mõiste inglisekeelne termin (*Business Continuity Management*) on laialdaselt kasutatav ka välisriikide avaliku sektori organisatsioonidele mõeldud standardites ja parimates praktikates. Seetõttu antud väljendit käesolevas magistritöös ei muudeta ja kasutatakse sellisel kujul ka edaspidi.

Nõudlus äri talitluspidevuse halduse järele on viimastel aastatel suurenenud seoses erinevate sündmustega, mis on häirinud olulisel määral suurte organisatsioonide tööd ja sundinud väiksemaid oma tegevust lõpetama (ENISA, 2012). Katkestused võivad olla tingitud nii personali kaotusest, probleemidest organisatsiooni füüsilise asukoha või taristutega kui ka IT teenuste mittetoimimisest või erinevatest keskkonnaga seotud õnnetustest (Finantsinspektsioon, 2006). See on olnud ajendiks kogu organisatsiooni hõlmava äri talitluspidevuse halduse praktiseerimiseks, eesmärgiga tagada tõsise intsidendi esinemisel kõikide põhiprotsesside jätkusuutlikkus (ITIL and ITSM World, 2010). Toimiv äri talitluspidevuse haldus näitab, et organisatsioon on valmis temast sõltumatutel põhjustel ilmnevateks põhitegevuse katkestusteks ja on suuteline toetuma praktilistele ning usaldusväärsetele plaanidele oma tegevuse jätkamiseks ja potentsiaalsete kahjude vähendamiseks (Finantsinspektsioon, 2006).

Äri talitluspidevuse halduse mõiste puhul ei ole kokku lepitud ühtset definitsiooni. Mitmed allikad on selle sõnastamiseks leidnud erinevaid viise, kuid ühel või teisel juhul on mõiste sisuline pool ja eesmärk ühtne. Siinkohal on välja toodud Inglismaal tegutseva Business Continuity Institute’i definitsioon antud terminist järgnevalt:

- äri talitluspidevuse haldus on terviklik juhtimisprotsess, mis tuvastab potentsiaalsed organisatsiooni ohustavad mõjud ja pakub välja raamistiku vastupidavuse suurendamiseks ning võimekuse efektiivseks reageerimiseks, et tagada võtmetähtsusega osanike huvide, organisatsiooni maine ja väärtust loovate tegevuste kaitse (Business Continuity Institute, 2011).

Äri talitluspidevuse planeerimise peamine eesmärk on võimaldada organisatsioonil kriisiolukorras põhitegevust jätkata ja taastada ettevõtte töö peale erakorralist situatsiooni, kehtestades selle jaoks vastupidavuse suurendamiseks asjakohase strateegia, taastamiseks eesmärgid ja äri talitluspidevuse ning kriisijuhtimise plaanid.

2.1 Äri ja IT talitluspidevuse metoodikad

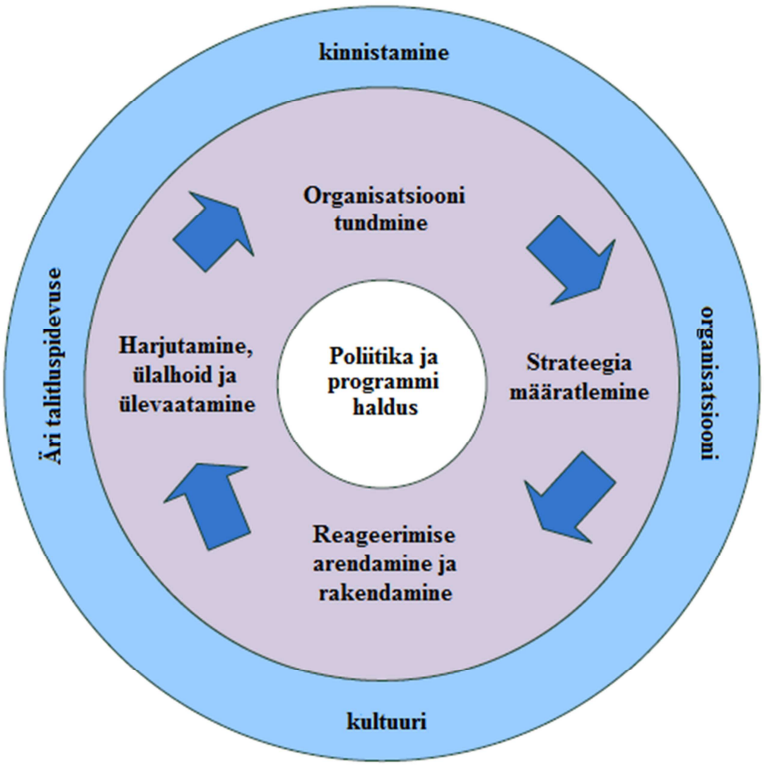
Suurt huvi talitluspidevuse valdkonna vastu näitab mitmete standardite ja parimate praktikate publitseerimine. Kuna metoodikaid on mitmeid ja ainuõiget lähenemist ei eksisteeri, siis valiku tegemisel tuleb leida organisatsiooni jaoks sobivaim. Lõpliku lahenduse ja strateegia väljakujunemisel mängivad olulist rolli nii inimfaktor kui ka tehnoloogilised ja finantsilised piirangud (ENISA, 2012).

Euroopa võrgu- ja infoturbe agentuur (ENISA, 2012) on koostanud nimekirja äri ja IT talitluspidevuse halduse metoodikate kohta, mis on leidnud laialdasemalt rakendust. Siinkohal on mitmed neist välja toodud, millest mõned on leidnud kajastamist ka antud töös:

- HB 292 A Practitioners Guide to Business Continuity Management;
- BS 25999-1 – Business Continuity Management Code of Practice;
- NIST 800-34 Contingency Planning Guide for IT Systems;
- PAS 77 IT Service Continuity Management;
- HB 221 Business Continuity Management;
- BSI 100-2. IT-Grundschutz Methodology;
- FSA BC Management Practice Guide;
- BCI Good Practice Guidelines;
- CobIT 4.0;
- ITIL v2;
- ITIL v3.

2.2 Äri talitluspidevuse halduse protsess

Järgnevalt on välja toodud Business Continuity Institute'i (2007) koostatud joonis (vt joonis 1) äri talitluspidevuse halduse protsessi elutsüklist ja selle põhietappidest.



Joonis 1. Äri talitluspidevuse halduse protsessi elutsükkel

Olenevalt metoodikast võib elutsükli etappe olla rohkem või vähem, kuid ühel või teisel viisil sisaldavad need samu kohustuslikke tegevusi. Äri talitluspidevuse halduse protsessi elutsükli osad, vastavalt juhendis *Business Continuity Institute - Good Practice Guidelines's* (2007) esitatule, võib kirjeldada järgmiselt:

- Poliitika ja programmi haldus – poliitika kirjeldamise kaudu määratletakse äri talitluspidevuse halduse programmi ulatus ja juhtimine, mis peegeldab selle rakendamise vajalikkust organisatsioonis;
- organisatsiooni tundmine – tuvastatakse võtmetähtsusega tooted ja teenused ning määratletakse neid toetavate tegevuste ajakriitilisus. Vajalik informatsioon saadakse ärimõjude analüüsi ja riskide hindamise kaudu;
- strateegia määratlemine – valitakse strateegia, mis vastab talitluspidevuse poliitikale ja organisatsiooni nõuetele, ning sobivaimad meetmed;
- reageerimise arendamine ja rakendamine – etapp, millest sõltub äri talitluspidevuse halduse programmi edu või läbikukkumine. Selle käigus luuakse sobilikud tegevusplaanid jätkusuutlike tegevuste ja tõhusa intsidendihalduse tagamiseks;

- harjutamine, ülalhoid ja ülevaatamine – tagatakse äri talitluspidevuse halduse strateegia, plaanide ja lepinguliste kokkulepete valideeritus ning kaasajastatus;
- kinnistamine organisatsioonikultuuri – eduka äri talitluspidevuse halduse jaoks on oluline selle organisatsiooni integreerimine, olenemata viimase suurusest või tegevusalast.

2.3 Äri talitluspidevuse halduse seos IT teenuste talitluspidevuse haldusega

Traditsiooniliselt on äri talitluspidevuse haldust vaadeldud kui IT üksuse vastutusalasse jäävat kohustust. Seda seetõttu, et äri talitluspidevus on välja arenenud IT avariitaastest (*IT Disaster Recovery*), mille käigus tegeleti üksnes IT taristu avariijärgse taastamise planeerimisega. Infotehnoloogia probleemidest tulenevad tööseisakud on tänaseni organisatsiooni põhitegevuse katkestuste suurimaid põhjustajaid, mistõttu on levinud arvamus, et äri talitluspidevuse haldus peaks toimuma IT üksuse eestvedamisel. Olulised muutused IT arengus on aga muutnud selle rakendamise viise, mistõttu hästi toimiva äri talitluspidevuse halduse planeerimine peab toimuma äripoole eestvedamisel ja olema korraldatud juhtkonna tasemel (Stranack & Cornish, 2009).

Organisatsiooni põhiprotsesside ja tehnoloogia omavaheline sõltuvus on läbi põimunud sellisel määral, et nüüdseks hõlmab äri talitluspidevuse haldus endas nii organisatsiooni põhitegevusega seonduvat, milleks on äri talitluspidevuse planeerimine, kui ka infotehnoloogilist elementi, milleks on IT teenuste talitluspidevuse planeerimine (*IT Service Continuity Management*) (Office of Government Commerce, 2003). Kui äri talitluspidevuse halduse raames määratletakse ootamatute katkestuste korral minimaalsed nõuded IT teenuste tarneks ja vastuvõetavateks töötingimusteks, siis IT teenuste talitluspidevuse halduse kaudu reguleeritakse antud nõuete täitmist (IT-Director, 2007). Kuna IT-süsteemid ja elektroonilised andmed on suure osa põhiprotsesside olulisteks komponentideks, siis nende kaitsmine ja töö õigeaegne jätkumine on eluliselt tähtis (ENISA, 2012).

IT teenuste talitluspidevuse haldusel on hindamatu roll äri talitluspidevuse planeerimise protsessis. Mitmetes organisatsioonides on seda kasutatud just talitluspidevuse ja taastenõuete alase teadlikkuse tõstmiseks ning sageli ka äri talitluspidevuse planeerimise protsessi ja plaanide õigustamiseks ning rakendamiseks. Paljudes organisatsioonides ei ole äri

talitluspidevuse haldus rakendamist leidnud või on sellele pööratud väga vähe tähelepanu. Sageli nõutakse, et mitmed äri talitluspidevuse protsessi raames teostatavad tegevused tuleb läbi viia just IT teenuste talitluspidevuse protsessi käigus. Selleks aga, et tagada efektiivne IT teenuste talitluspidevuse haldus, on oluline tuvastada kriitilised põhiprotsessid ja teostada vajaliku tehnoloogia ning IT teenuste osas analüüs (Office of Government Commerce, 2007).

IT teenuste talitluspidevuse halduse rakendamise kasu organisatsioonile:

- Parendatud põhiprotsessid;
- täiustatud tehnoloogilised vahendid;
- väiksem häirete osakaal;
- kvaliteetsemad teenused (Gregory, 2008).

Järgmises peatükis antakse ülevaade IT teenuste talitluspidevuse haldusest, tutvustatakse IT teenuste talitluspidevuse halduse protsessi elutsüklit ja selle erinevaid etappe.

3. IT teenuste talitluspidevuse haldus

IT teenuste talitluspidevuse haldus on osa äri talitluspidevuse halduse protsessist, mille eesmärk on vähendada miinimumini tegureid, mis takistavad missioonikriitiliste süsteemide tööd. Ühtlasi on antud valdkonna eesmärk määratleda, millised tegevused on vajalikud olukorras, kus teenuse osutamine on häiritud (Hiie, 2009). Antud protsess toetab organisatsiooni jätkusuutlikkust selliselt, et IT teenuste katkemise korral vastaksid taasteajad äripoole nõuetele (Leibur, 2007).

IT teenuste talitluspidevuse halduse raames keskendutakse sündmustele, mille mõju peab äripool katastroofi vääriliseks (Office of Government Commerce, 2007). Selle käigus tegeletakse IT katastroofidega toimetulemise ja nendest taastumise küsimustega. IT katastroofi all mõistetakse teenuse mittetoimimist pikema perioodi jooksul, mistõttu on erandkorras vaja kasutusele võtta alternatiivne süsteem. Talitluspidevuse halduse raames antakse juhiseid olemasolevate süsteemide kaitsmiseks vajalike proaktiivsete meetmete osas ja suuniseid reaktiivsete meetmete arendamiseks (Hiie, 2009). IT teenuste talitluspidevuse halduse edukas rakendamine eeldab juhtkonna pühendumist ja organisatsiooni kõikide liikmete toetust.

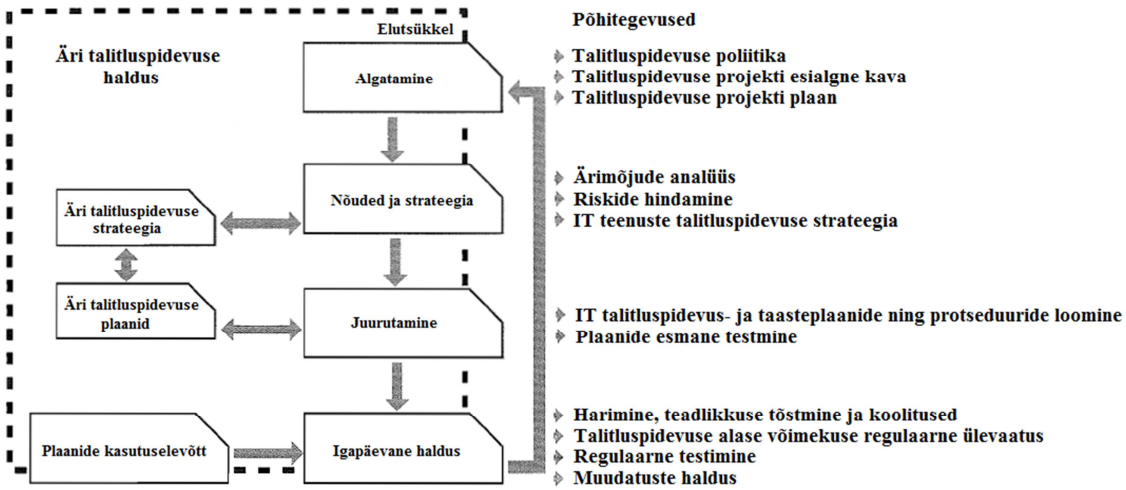
IT teenuste spetsiifilised nõuded ja vajalikud ressursid tagatakse läbi IT teenuste talitluspidevuse halduse ning selle skoop määratletakse lähtuvalt organisatsiooni struktuurist, kultuurist, strateegilistest korraldustest, osutatavatest teenustest ja nende muutumisest aja jooksul (Office of Government Commerce, 2007).

IT teenuste talitluspidevuse põhieesmärk sisaldab järgmisi punkte:

- IT teenuste katkestuste vältimine ja teenuste taastamine katkestuse asetleidmisel;
- talitluspidevuse plaanide koostamine;
- plaanide ja nendega seotud protseduuride regulaarne testimine;
- (uute) töötajate koolitamine seoses talitluspidevusega (Hiie, 2009).

Talitluspidevuse halduse protsessi sisseviimisel ja järgimisel on soovitatav kasutada elutsüklil põhinevat lähenemist vastavalt Office of Government Commerce (2007) parimate praktikate raamistiku *Service Design* publikatsioonis käsitletule (vt joonis 2). Muuhulgas kujutatakse

antud joonisel IT teenuste talitluspidevuse halduse protsessi paiknemist äri talitluspidevuse halduse protsessi sees. Elutsüklil põhinev lähenemine võimaldab peale talitluspidevus- ja taasteplaanide loomist tagada nende joondatavuse äri talitluspidevuse plaanide ja eesmärkidega (Office of Government Commerce, 2007).



Joonis 2. IT teenuste talitluspidevuse halduse protsessi elutsükkel

Talitluspidevuse halduse protsessi elutsükkel koosneb neljast peamisest etapist, millest esimesed kaks moodustavad eelkõige äri talitluspidevuse halduse protsessi osa ja ülejäänud kaks on suuresti IT-spetsiifilised. Allpool on etapid esitatud teostamiseks vajalikus järjekorras:

- Algatamine;
- nõuded ja strateegia;
- juurutamine;
- igapäevane haldus (Office of Government Commerce, 2007).

Järgnevalt on välja toodud protsessi üldine loogika lähtuvalt Office of Government Commerce (2007) parimate praktikate raamistiku *Service Design* publikatsioonist, mis sisaldab järgmisi punkte:

- IT teenuste talitluspidevuse halduse protsessi tegutsemisulatuse ja -poliitika kokkuleppimine;

- IT teenuste katkestusest tingitud kvantitatiivsete ja kvalitatiivsete mõjude väljaselgitamine ärimõjude analüüsi kaudu;
- IT teenustega seotud potentsiaalsete ohtude ja nende esinemise tõenäosuse ning mõju suuruse kindlakstegemine riskide hindamise kaudu;
- talitluspidevuse strateegia loomine;
- IT talitluspidevus- ja taasteplaanide ning taasteprotseduuride koostamine;
- plaanide ja nendega seotud taasteprotseduuride regulaarne testimine;
- plaanide igapäevane haldamine ja hooldamine.

3.1 Algatamine

Algatamine on talitluspidevuse halduse protsessi elutsükli esimene etapp, mille eesmärk on määratleda talitluspidevuse poliitika, koostada talitluspidevuse projekti esialgne kava ja projektiplaan. Talitluspidevuse poliitika on formaalne dokument, mis mängib rolli otsuste vastuvõtmisel ja tegevuste määratlemisel ning muudes talitluspidevusega seotud küsimustes. Poliitika määratlemisel peab lähtuma selle sobivusest organisatsiooni põhiprotsesside iseloomu, ulatuse, keerukuse ja kriitilisusega ning et see peegeldaks organisatsioonikultuuri ja tegutsemiskeskkonda. Poliitika määratlemisel tuleb arvestada lisaks eelarve, ajaliste piirangute, õiguslike aspektide, tähtaegade ja talitluspidevusealase kompetentsi olemasoluga. Poliitika sõnastamine on esmajärguline, kuna see moodustab põhialuse kogu ülejäänud tööle ja tagab talitluspidevuse jätkusuutlikkuse (ENISA, 2012).

IT teenuste talitluspidevuse halduse edukaks rakendamiseks on soovitatav selle algatamisel lähtuda projektijuhtimise põhimõtetest (ENISA, 2012). Projekti algatamise faasis on vaja määratleda selle põhieesmärk ja kujundada selge veendumus projekti vajalikkusest ning teostatavusest (Normak, 2009). Algatamise etapi üheks väljundiks on talitluspidevuse projekti esialgne kava, mille koostamisel tuleb muuhulgas tähelepanu pöörata järgmistele punktidele:

- Eesmärk ja tulemid;
- tähtajad;
- piirangud;
- eelarve;
- ressursianalüüs (ENISA, 2012).

Esialgse kava järgselt algatatakse planeerimise faas, mida on vaja, et koostada projekti täitmise optimaalne skeem (Normak, 2009). Projektiplaan peab muuhulgas sisaldama hästi defineeritud struktuuri, skoopi, eesmärke ja tulemusi, mis on kooskõlas organisatsiooni strateegiaga. Projekti õnnestumiseks on oluline saada sellele juhtkonna kinnitus ja pidev toetus terve projekti vältel (ENISA, 2012).

3.2 Nõuded ja strateegia

Nõuete ja strateegia etapp on IT teenuste talitluspidevuse halduse oluline osa, mille käigus selgitatakse välja organisatsiooni põhitegevuse nõuded teenuste järjepidevuse tagamiseks ning määratletakse organisatsiooni võime katkestusest või õnnetusest taastuda. Kõige olulisemad tegevused käesolevas etapis on ärimõjude analüüs ja riskide hindamine, mille valesti teostamisel või võtmetähtsusega informatsiooni tähelepanuta jätmisel võivad olla tõsised tagajärjed IT teenuste talitluspidevuse efektiivsusele. Lisaks ärimõjude analüüsile ja riskide hindamisele hõlmab antud etapp IT teenuste talitluspidevuse strateegia loomist (Office of Government Commerce, 2007).

3.2.1 Ärimõjude analüüs

Limiteeritud ressursside tõttu on talitluspidevust rakendatavatel organisatsioonidel võimalik teha vaid niipalju kui eksisteerib inimesi, rahalisi ja muid vahendeid. Sellest lähtuvalt ei ole esmase taastevõimekuse loomine kõikide protsesside jaoks optimaalne, mistõttu tuleb keskenduda ainult kõige olulisematele põhiprotsessidele. Kriitiliste põhiprotsesside tuvastamiseks tuleb teostada ärimõjude analüüs (Gregory, 2008).

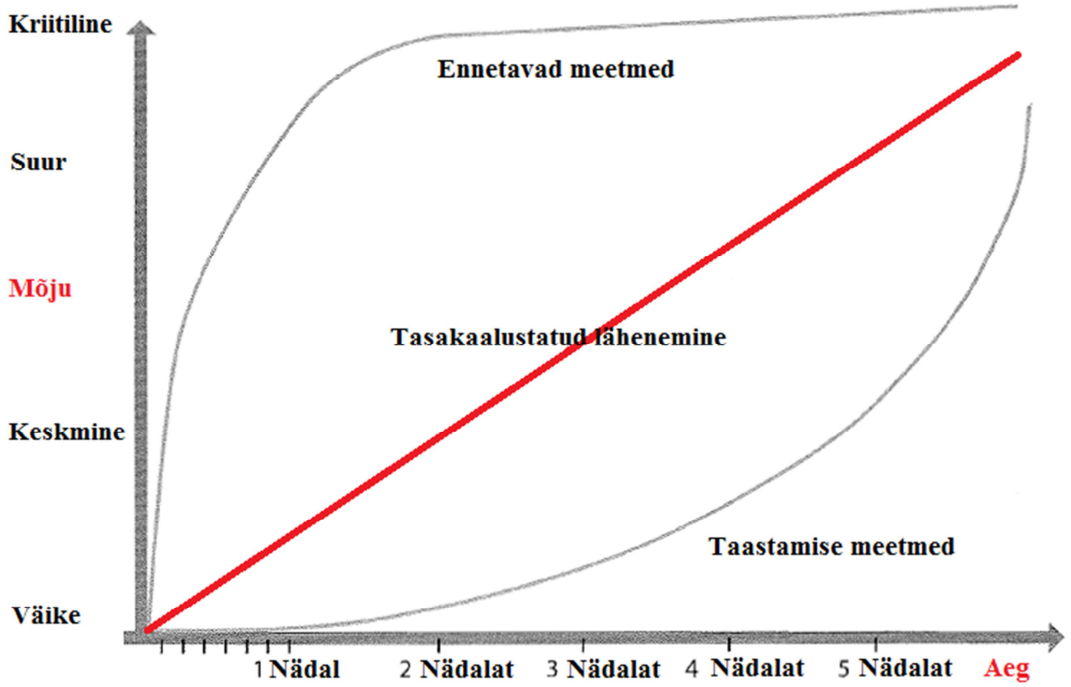
Ärimõjude analüüs on osa äri talitluspidevuse halduse protsessist, mis mängib olulist rolli organisatsiooni talitluspidevuse planeerimisel ja moodustab sellest olulise osa (Business Impact Analysis, 2011). Analüüsi eesmärk on tuvastada, millised protsessid on kõige olulisemad organisatsiooni püsimajäämise seisukohalt, protsesside nõuded ressurssidele ja protsesside mittetoimimisel kvantitatiivsed ning kvalitatiivsed mõjud organisatsioonile (ENISA, 2012). Ressurssideks võivad olla tarnijad, personal, teised protsessid ja IT teenused. (itSMF Estonia, 2010). Analüüsi tulemusel seostatakse ära, millised IT teenused toetavad kõige kriitilisemaid põhiprotsesse (ENISA, 2012). Samuti määratletakse nõuded IT teenuste

taastamise osas, mis puudutavad iga teenuse jaoks taastamisaega ja -kohta (itSMF Estonia, 2010).

Ärimõjude analüüsi kaudu tuvastatakse järgnev informatsioon:

- organisatsiooni kõige olulisemad põhiprotsessid;
- potentsiaalne mõju organisatsioonile põhiprotsessi mittetoimimise korral. Mõjude hindamine toimub kindlate kahjuliikide suhtes, milleks muuhulgas on:
    - finantskahju;
    - maineväärtusega seotud kahju;
    - õigusliku kohustusega seotud kahju;
    - tegutsemisvõimekusega seotud kahju;
    - tervishoiu ja ohutusega seotud kahju;
- mõju hinnanguline eskaleerumine ajas;
- mõju esinemise kõige suurem tõenäosus (päev, nädal, kuu);
- põhiprotsesse toetavad vajalikud ressursid (tarnijad, personal, IT teenused, varad);
- IT teenuste taastamise järjekord lähtuvalt kriitilistest põhiprotsessidest (Office of Government Commerce, 2007);
- maksimaalne lubatud aeg, mille jooksul on taastamine põhjendatud (*Maximum Tolerable Period of Disruption*);
- maksimaalne lubatud aeg süsteemi taastamiseks (*Recovery Time Objective*);
- maksimaalne lubatud andmekadu andmete taastamisel (*Recovery Point Objective*) (Leibur, 2007).

Ärimõjude analüüsi tulemusel kogutud informatsiooni põhjal on iga põhiprotsessi kohta võimalik koostada graafik (vt joonis 3), mis illustreerib üksiku põhiprotsessi mittetoimimisest tingitud võimalikku mõju organisatsioonile ajas. Graafiku alusel on võimalik tuvastada, millisel ajahetkel muutub kriitilise põhiprotsessi või IT teenuse katkestusest tingitud mõju organisatsioonile vastuvõetamatuks. Teenuste puhul, millel on suur mõju lühikese aja jooksul, tuleb kasutada ennetavaid meetmeid nagu riskide vähendamine. Teenuste puhul, mille mõju katkestuse esinemisel on väike ja mis eskaleeruvad pikema aja jooksul, tuleb rakendada taastamisega seotud meetmeid. Teenuste puhul, mille mõju kasvab aja jooksul lineaarselt, tuleb kasutada tasakaalustatud lähenemist ja keskenduda meetmete kombineerimisele.



Joonis 3. Ärimõjude analüüsi graafiline esitus (Office of Government Commerce, 2007)

Ärimõjude analüüsi peamiseks väljundiks on ärimõjude analüüsi aruanne, mis sisaldab üksikasjalikku ülevaadet olulisuse järjekorda reastatud põhiprotsessidest, potentsiaalsetest mõjudest nende mittetoimimise korral ja toimimiseks vajalikke ressursse.

3.2.2 Riskide hindamine

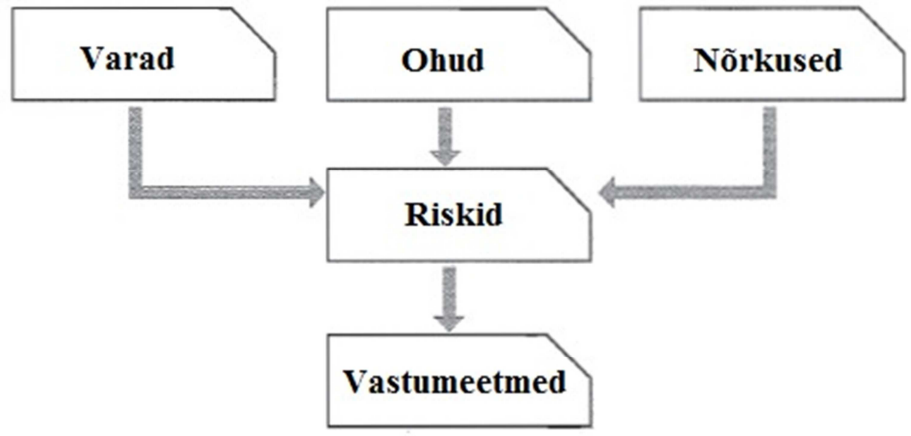
Talitluspidevuse nõuete määratlemisel on oluliseks vahendiks ka riskide hindamine, mis on osa riskihaldusest. Riskide hindamine on protsess, mis kombineerib endas riskide tuvastamise, analüüsi ja evalveerimise. Riskide hindamist kasutatakse potentsiaalsete ohtude tõenäosuse ja mõju suuruse väljaselgitamiseks ning riskide määratlemiseks (Stoneburner, Goguen & Feringa, 2002).

Riskide hindamise puhul on oluline defineerida sellega seotud põhilised mõisted:

- Risk - tõenäosuslik sündmus, mis võib põhjustada kahju või mõjutada võimet saavutada eesmärke. Riski mõõdetakse ohu tõenäosuse, varade haavatavusega ohule ja mõjuga, mis riski realiseerumisel tekib;

- oht - igasugune olukord, sündmus või tegevus, mis võib haavatavuse ära kasutada ja süsteemi kahjustada. Igasugust intsidentide potentsiaalset põhjust tuleb käsitleda ohuna. Iga oht on määratud tasemega, mis näitab võimaliku sündmuse tõenäosust ja mida kasutatakse riskide hindamisel;
- haavatavus – varaga seotud nõrkus või nõrk koht, mida oht võib ära kasutada;
- vara – vara all mõistetakse kõike, mida saab kasutada teenuste osutamiseks nagu juhtimine, organisatsioon, protsess, teadmised, inimesed, informatsioon, rakendused, infrastruktuur ja finantskapital (Saar, 2012).

Paljud riskihindamise ja -halduse metoodikad soovitavad riskide hindamisel järgida joonisel 4 esitatud loogikat.



Joonis 4. Riskide hindamise mudel (Office of Government Commerce, 2007)

Riskide hindamise protsess hõlmab peamiselt järgmisi tegevusi:

- Varade kindlakstegemine;
- ohtude tuvastamine;
- nõrkuste tuvastamine;
- ohtude esinemise tõenäosuse ja mõju suuruse hindamine;
- riski suuruse leidmine (Munipalli, 2005).

Riskide hindamist on keeruline ja mahukas läbi viia kui see hõlmab kogu organisatsiooni. Skoobi määratlemisel on soovitatav fookus suunata ärimõjude analüüsi tulemusel selgunud kriitiliste põhiprotsesside tööd toetavatele ressurssidele, sealhulgas IT teenustele. Selline

lähenemine võimaldab olulisel määral vähendada riskide hindamise ulatust ja osutada tähelepanu peamisele (Business Continuity Institute, 2007).

IT teenuste talitluspidevuse halduse kontekstis on riskide hindamine viis, mis võimaldab tuvastada ja hinnata IT teenustega seotud riske. Riskide hindamise kaudu tuvastatakse mitmed spetsiifilised ohud, mis võivad põhjustada häireid või katkestusi IT teenuste töös. Viimased võivad aga mõjutada kõige kriitilisemate põhiprotsesside toimimist ja sellest tulenevalt organisatsiooni tööd. Riskide hindamise tulemusena on võimalik riske prioritiseerida ja võtta kasutusele sobilikud meetmed (Business Continuity Institute, 2007).

Riskide käsitlemise enamlevinud meetmed on järgmised:

- riskist hoidumine – konkreetse riski põhjuse kõrvaldamine;
- riski vähendamine – riski esinemise tõenäosuse või mõju suuruse vähendamine;
- riski ülekandmine – osaliselt või täielikult riski ülekandmine kolmandale osapoolele;
- riskiga leppimine – riski esinemise tõenäosus või mõju suurus on piisavalt väike, mistõttu ei rakendata täiendavaid meetmeid (Business Continuity Institute, 2007).

3.2.3 IT teenuste talitluspidevuse strateegia

Sobiliku IT teenuste talitluspidevuse strateegia loomise aluseks on ärimõjude analüüsi ja riskide hindamise tulemusena kogutud informatsioon. Kui äri talitluspidevuse strateegia määratlemisel tegeletakse küsimustega nagu kriitiliste põhiprotsesside, personali, ruumide ja hoonete taastamine õnnetusjuhtumi korral, siis IT teenuste talitluspidevuse strateegia loomisel on tähelepanu keskmes IT teenuste taastamisega seonduv. Strateegia loomisel tuleb olenevalt ajahetkest (nt päev, nädal, kuu) võtta arvesse eelisjärjekorras taastamist vajavad IT teenused ja muutused teenuste taastamise järjekorras (Office of Government Commerce, 2007).

Strateegia määratlemisel peab arvestama, et erinevad teenused vajavad erinevaid taastamise meetmeid, mistõttu on oluline jälgida, et valitud lahendus oleks võimalikult kuluefektiivne. Üldine reegel on, et mida kauem suudab organisatsioon ilma teenuseta toimida, seda odavam antud lahendus on (Office of Government Commerce, 2007).

IT teenuste talitluspidevuse strateegia väljatöötamisel tuginetakse järgmistele meetmetele:

- Proaktiivsed meetmed, mille eesmärk on ära hoida teenuste katkestusi ja mis on seotud riskide vähendamisega;
- reaktiivsed meetmed, mille eesmärk on taastada teenuste toimimine vajalikul tasemel ja nõutud aja jooksul ning mis on seotud erinevate taastamise valikutega (Office of Government Commerce, 2007).

IT teenuste talitluspidevuse halduse kontekstis on levinud meetodiks tasakaalustatud lähenemine, mille puhul riskide vähendamise ja taastamise meetmed täiendavad teineteist. Strateegia määratlemisel on oluline arvestada piisavas ulatuses riskide vähendamise meetmetega, et minimeerida ohtude mõju suurust või esinemise tõenäosust. Strateegiaks kujuneb enamasti riskide vähendamise ja taastamise meetmete vahel olev kulude tasakaal, et toetada kriitiliste põhiprotsesside taastamist kokkulepitud ajavahemiku jooksul ning vajalikul tasemel (Office of Government Commerce, 2007).

3.3 Juurutamine

Strateegia määratlemisele ja selles kokku leppimisele järgneb juurutamise etapp, mis hõlmab plaanide loomist ning nende esmast testimist. Käesoleva etapi üheks oluliseks osaks on IT teenuste talitluspidevus- ja taasteplaanide ning taasteprotseduuride loomine, mille kaudu kirjeldatakse vajalik informatsioon kriitiliste teenuste tööshoidmiseks ja taastamiseks vajalikul tasemel ning nõutud aja jooksul (Office of Government Commerce, 2007).

3.3.1 Plaanide loomine

Talitluspidevuse plaanide näol on tegemist dokumentide kogumikuga, mis moodustavad organisatsiooni reageerimistegevused õnnetusjuhtumi algusest kuni tavapärase olukorra taastumiseni (ENISA, 2012). Plaanide loomine on vajalik selleks, et tagada vajalike teenuste tarne organisatsiooni põhitegevusele vastuvõetaval ja otstarbekal tasemel. Plaanid jagunevad:

- IT talitluspidevusplaanid;
- IT taasteplaanid ja –protseduurid (Office of Government Commerce, 2007).

Plaanid sisaldavad kogu informatsiooni ja kajastavad kõiki tegevusi, mis tagavad vajalike teenuste, ruumide ning ressursside tarne organisatsioonile vastuvõetaval tasemel. Sellest tulenevalt hõlmavad plaanid ka vajalikku informatsiooni teenuste omavaheliste seoste kohta, arvestavad vajalikus mahus testimistega ja tagavad taastamiseks vajalike andmete terviklikkuse. Samuti sisaldavad plaanid dokumentatsiooni riskide vähendamise ja taastamist võimaldavate meetmete kohta (Office of Government Commerce, 2007).

3.3.2 Plaanide esmane testimine

Testimine on kogu IT teenuste talitluspidevuse halduse protsessi suhtes kriitilise tähtsusega ja selle abil on võimalik tagada, et valitud strateegia, sõlmitud ooteseisundi lepingud, logistika, plaanid ning protseduurid toimivad ka praktikas. Plaanid, mida ei ole testitud, ei pruugi toimida nii nagu soovitud (Office of Government Commerce, 2007).

IT üksuse ülesanne on vastutada tehnoloogiliste komponentide toimivuse eest. Sellest tulenevalt on vajalik komponentide testimine testkeskkonnas, et tagada nende efektiivne toimimine. Esmased testid, mis on seotud tehnoloogiliste komponentidega, võib teostada ilma organisatsiooni äripoolt kaasamata, kuid järgnevate testide läbiviimseks on mõistlik ka äripoole kaasamine. Antud lähenemine võimaldab tõestada talitluspidevusealast võimekust ja leida äripoolega vajalike tegevuste ning ressursside osas vastastikust mõistmist. Oluline on saavutada ühine eesmärk, milleks on IT teenuste taastamine, mis omakorda võimaldab organisatsiooni tegevuse normaliseerumist (Office of Government Commerce, 2003).

Kõikehõlmav testimine võimaldab plaanide testimist viisil, mis katab ooteseisundi korralduste aktiveerimise, põhiprotsesside taastamise ja kolmandate osapoolte kaasamise. Läbi testimise on võimalik tuvastada plaanide terviklikkus, mis annab kindluse järgmiste punktide osas:

- Ajalised eesmärgid;
- meeskonna valmidus ja teadlikkus;
- kolmandate osapoolte reageerimisvõime, teadlikkus ja efektiivsus (Office of Government Commerce, 2003).

Testide läbiviimisel on oluline, et nende teostamine toimuks kindlate stsenaariumite alusel, mis peegeldaks võimalikult reaalset olukorda (Office of Government Commerce, 2007).

3.4 Igapäevane haldus

Peale talitluspidevuse juurutamist ja plaanide koostamist on vaja talitluspidevuse protsess siduda organisatsiooni igapäevase tegevusega. Muutused on organisatsioonides püsivad ja seetõttu on tähtis tagada, et talitluspidevust võetakse igapäevase töötegemise lahutamatu osana. Uuendused ja muudatused põhiprotsessides, IT teenustes, tehnoloogias, personalis ning teistes valdkondades on talitluspidevusega seotud informatsiooni regulaarse ülevaatamise ja muutmise ajendiks (Gregory, 2008).

Tulenevalt Office of Government Commerce (2007) *Service Design* publikatsioonist sisaldab igapäevase halduse etapp endas järgmisi punkte:

- Harimine, teadlikkuse tõstmine ja koolitused;
- plaanide regulaarne ülevaatus;
- regulaarne testimine;
- muudatuste haldus.

3.4.1 Harimine, teadlikkuse tõstmine ja koolitused

Harimine, teadlikkuse tõstmine ja koolitused peavad talitluspidevusega seotud punktides hõlmama tervet organisatsiooni, eriti IT meeskonda. Selle kaudu tagatakse, et töötajad on teadlikud talitluspidevuse rakendamise vajalikkusest ja võtavad seda kui igapäevast töö osa. Samuti on eesmärk tagada, et kõik plaanidega seotud töötajad on koolitatud tasemel, mis võimaldab neil vajadusel oma oskusi rakendada (Office of Government Commerce, 2007).

3.4.2 Talitluspidevuse alase võimekuse regulaarne ülevaatus

Talitluspidevuse plaanid võivad aeguda väga ruttu ja nende mitteuuendamine võib saada määravaks plaanide efektiivsusele ning asjakohasusele. Peale plaanide esmast testimist on oluline tagada nende regulaarne ülevaatus ja vajadusel uuendamine (ENISA, 2012). Regulaarse ülevaatuse kaudu tagatakse dokumentide kaasajastatus, jätkuv sobivus ja efektiivsus. Dokumentide ülevaatamine on vajalik juhul, kui toimuvad suuremat sorti IT teenuste, varade või nende seoste ja organisatsiooni põhitegevuse, strateegia või IT strateegia

muudatused. Ülevaatus peab aset leidma ka siis, kui lisandub uusi süsteeme, võrke või toimuvad teenusepakkujate osas muudatused (Office of Government Commerce, 2007).

3.4.3 Regulaarne testimine

Peale esmaseid testimisi on oluline luua regulaarsete testimiste läbiviimiseks programm. Plaanide regulaarne testimine võimaldab tagada nende sisu korrektsuse ja kindlustada, et plaanidega seotud töötajad on teadlikud oma rollidest ka praktikas (Business Continuity Institute, 2007).

Regulaarse testimise eesmärgid on järgmised:

- Plaanides sisalduv informatsioon on asjakohane;
- plaanid on läbiharjutatud;
- personal, sh juhtkond on koolitatud (Business Continuity Institute, 2007).

3.4.4 Muudatuste haldus

IT teenused ja nendega seotud süsteemid on pidevas muutumises. Muudatusi võivad põhjustada tehnoloogilised uuendused, muutuvad organisatsiooni vajadused või sisemised ja välised poliitikad. Sellest tulenevalt on oluline, et talitluspidevuse plaanide ülevaatamine ja uuendamine toimub regulaarselt muudatuste halduse protsessi osana. See võimaldab tagada, et igasugune uus informatsioon saab korrektselt dokumenteeritud (Swanson, Bowen, Philips, Gallup & Lynes, 2010).

Muudatuste halduse protsess on vajalik ka selleks, et vajadusel tuvastada informatsiooni varasemalt rakendatud ja tulevikus plaanitavate muudatuste osas ning hinnata nende võimalikku mõju talitluspidevuse plaanidele. Sellest tulenevalt peavad plaanid olema range kontrolli all, kuna ebatäpsed plaanid ja sellest tulenev puudulik taastevõimekus võib põhjustada plaanide ebaõnnestumise (Office of Government Commerce, 2007).

Järgmises peatükis esitatakse IT teenuste talitluspidevuse tagamise üldskeem, milles tuuakse välja soovituslikud punktid talitluspidevuse korraldamiseks.

4. IT teenuste talitluspidevuse tagamise üldskeem

Kui eelnevas peatükis kirjeldati IT teenuste talitluspidevuse halduse protsessi elutsüklit ja selle osasid üldisemalt, siis käesoleva peatüki eesmärk on anda üksikasjalik ülevaade tegevustest, millele tuginedes saab töös käsitletav avaliku sektori organisatsioon talitluspidevuse protsessi planeerimisel juhinduda. IT teenuste talitluspidevuse tagamise üldskeemi väljatöötamisel on lähtutud Office of Government Commerce (2007) parimate praktikate raamistiku *Service Design* publikatsiooni *IT Service Continuity Management* peatükis esitatud struktuurist, mille peamistest osadest anti ülevaade ka eelmises peatükis ja mis hõlmab järgmisi punkte:

- Talitluspidevuse protsessi algatamine (vt punkt 4.1);
    - poliitika loomine (vt punkt 4.1.1);
    - projekti esialgse kava koostamine (vt punkt 4.1.2);
    - projektiplaani loomine (vt punkt 4.1.3);
- organisatsiooni põhitegevuse nõuete tuvastamine ja strateegia loomine (vt punkt 4.2);
    - ärimõjude analüüsi teostamine (vt punkt 4.2.1);
    - riskide hindamise läbiviimine (vt punkt 4.2.2);
    - IT teenuste talitluspidevuse strateegia loomine (vt punkt 4.2.3);
- talitluspidevuse juurutamine (vt punkt 4.3);
    - IT talitluspidevus- ja taasteplaanide ning taasteprotseduuride loomine (vt punkt 4.3.1);
    - plaanide esmane testimine (vt punkt 4.3.2);
- igapäevane haldus (vt punkt 4.4);
    - harimine, teadlikkuse tõstmine ja koolitused (vt punkt 4.4.1);
    - talitluspidevuse alase võimekuse regulaarne ülevaatus (vt punkt 4.4.2);
    - regulaarne testimine (vt punkt 4.4.3);
    - muudatuste haldus (vt punkt 4.4.4).

4.1 Talitluspidevuse protsessi algatamine

Talitluspidevuse protsessi algatamisel on vaja tutvuda selle põhimõtetega (vt punkt 3.1) ja lähtuvalt sellest teostada järgmised tegevused:

- Poliitika loomine (vt punkt 4.1.1);
- projekti esialgse kava koostamine (vt punkt 4.1.2);
- projektiplaani loomine (vt punkt 4.1.3).

4.1.1 Poliitika loomine

Esimese tegevusena on vaja luua selgesti sõnastatud talitluspidevuse poliitika, mille kaudu kirjeldatakse talitluspidevuse korraldamiseks vajalikud põhimõtted ja raamistik. Poliitika tuleb formuleerida kirjaliku dokumendina, mis sisaldab muuhulgas järgmisi punkte:

- Organisatsiooni kontekstis talitluspidevuse definitsioon;
- talitluspidevuse eesmärk;
- talitluspidevuse skoop;
- talitluspidevuse raamistik;
- rollid ja kohustused;
- viited standarditele, eeskirjadele, õigusaktidele ja muudele olulistele dokumentidele, mis määravad talitluspidevuse nõuded;
- tingimused poliitika ülavaatamiseks (Office of Government Commerce, 2007).

Käesoleva punkti väljundiks on talitluspidevuse poliitika dokument, mis tuleb juhtkonnapoolse toetuse tagamiseks lasta allkirjastada juhtkonna liikme või nõukogu poolt. Allkirjastamise järgselt on vaja poliitika avaldada ja levitada, kasutades selleks sobilikku versioonihaldust ning metoodikat.

4.1.2 Projekti esialgse kava koostamine

Järgnevalt on vaja koostada talitluspidevuse projekti esialgne kava, mille kaudu antakse talitluspidevusega seotud töötajatele esmane ülevaade kavandatava projekti põhijoontest. Projekti esialgse kava üheks oluliseks ülesandeks on ka erinevate osapooltega läbirääkimine ja vajadusel kava korrigeerimine ning nõusoleku saavutamine. Selle koostamisel tuleb eelkõige lähtuda organisatsioonis kasutusel olevast projektijuhtimise metoodikast ja sellega seotud põhimõtetest. Projekti esialgne kava peab muuhulgas sisaldama järgmisi punkte:

- Projekti esialgne nimi;
- põhieesmärk;
- skoop;
- vajaduse ja uudsuse lühike põhjendus;
- põhilised tegevused (etapid);
- põhitäitjad ja nende võimalikud põhiülesanded;
- vajalike ressursside hinnang;
- täitmiseks kavandatav aeg (Normak, 2009).

Käesoleva punkti väljundiks on kokkulepitud ja kinnitatud talitluspidevuse projekti esialgne kava, mille alusel on võimalik hakata looma projektiplaani.

4.1.3 Projektiplaani loomine

Tuginedes talitluspidevuse projekti esialgsele kavale, tuleb järgnevalt koostada talitluspidevuse projekti plaan, mis kirjeldab üksikasjalikult projekti eesmärgi saavutamist. Plaani koostamisel tuleb eelkõige lähtuda organisatsioonis kasutusel olevast projektijuhtimise metoodikast ja sellega seotud põhimõtetest, mis peab muuhulgas sisaldama järgmisi punkte:

- Projekti põhiandmed (projekti nimi, põhieesmärk);
- taust (vajadus, põhilised sihtrühmad, hetkeolukord, valdkonna prioriteetsus, täitjate eelnev tegevus antud valdkonnas);
- projektiplaanis kasutatavate mõistete seletused;
- valdkonnas kasutatavatele standarditele vastavus;
- perspektiivid projekti tulemuste edasiarendamiseks;
- projektikirjeldus (põhitulemid, alameesmärgid, vajalikud tegevused);
- ajagraafik;
- projekti haldamine (täitjate iseloomustus, ülesannete jaotus täitjate vahel, töö- ja aruandluse korraldus, riskide käsitlus, kvaliteeditagamine);
- projekti tulemuste rakendamise või levitamise kavad;
- hinnang mõjude osas, mis tulenevad projekti eesmärkide saavutamisest;
- eelarve;
- projekti lühikokkuvõte (Normak, 2009).

Käesoleva punkti väljundiks on kokkulepitud ja kinnitatud talitluspidevuse projekti plaan, mis võimaldab alustada projekti täitmist.

4.2 Organisatsiooni põhitegevuse nõuete tuvastamine ja strateegia loomine

Peale poliitika loomist ja projekti esialgse kava ning plaani koostamist on vaja hakata projekti täitma. Esimeseks tegevuseks on siinkohal nõuete ja strateegia etapi sisuga tutvumine (vt punkt 3.2) ja lähtuvalt sellest järgmiste punktide läbiviimine:

- Ärimõjude analüüsi teostamine (vt punkt 4.2.1);
- riskide hindamise läbiviimine (vt punkt 4.2.2);
- IT teenuste talitluspidevuse strateegia loomine (vt punkt 4.2.3).

4.2.1 Ärimõjude analüüsi teostamine

Ärimõjude analüüsi teostamiseks on esmalt vaja tutvuda selle põhimõtetega (vt punkt 3.2.1) ja teostada järgmised tegevused (Marquis, 2008):

- Andmekogumisviisidega tutvumine ja sobivaima valimine (vt punkt 4.2.1.1);
- andmete kogumise läbiviimine, kasutades valitud andmekogumise meetodit;
- analüüsi teostamine (vt punkt 4.2.1.2);
- tulemuste valideerimine;
- aruande koostamine ja tulemuste levitamine (vt punkt 4.2.1.3).

4.2.1.1 Andmekogumisviisidega tutvumine ja sobivaima valimine

Andmete kogumiseks eksisteerib kolm peamist võimalust:

- Intervjuud – struktureeritud, poolstruktureeritud või struktureerimata kujul intervjuude kasutamine võimaldab koguda väga väärtuslikku informatsiooni, kuid nende läbiviimine on ajamahukas ja väljundid võivad erineda nii formaadis kui detailsuses;
- töötoad - töötubade läbiviimine võimaldab praktilisi tegevusi ja kiireid tulemusi;

- küsimustikud - küsimustikud võivad eksisteerida paberkujul või digitaalselt. Küsimustike kaudu on võimalik kätte saada suur hulk andmeid, kuid nendes sisalduv informatsioon võib olla ebakvaliteetne kui neid ei ole terviklikult täidetud (Business Continuity Institute, 2007).

Parima tulemuse saavutamiseks soovitatakse andmekogumisviisina kasutada kombineeritud meetodit, mis väljendub poolstruktureeritud näost-näkku intervjuude läbiviimises, kasutades selleks eelnevalt koostatud küsimustikku. Kombineeritud meetodi kasutamise eelisteks on:

- Personaalne kohtumine intervjueeritavaga;
- võimalus lisamaterjalide kasutamiseks dokumentide ja jooniste näol;
- küsimustele vastamine etteantud küsimustiku raames;
- võimalus küsimuste täpsustamiseks ja selgitamiseks ning muude oluliste mõtete esiletulemiseks ja läbiarutamiseks (Allaste, 2011).

Ärimõjude analüüsi küsimustiku näidisdokument (ISACA, 2012) asub lisas 1.

Käesoleva punkti väljundiks on sobivaima andmekogumise viisi valimine ja küsimustiku koostamine.

4.2.1.2 Analüüsi teostamine

Analüüsi teostamiseks, andmete võrdlemiseks ja hinnangute andmiseks on vaja esmalt andmed kokku koguda. Selleks sobib hästi mõni üldlevinud tabelitöötlustarkvara, mis võimaldab informatsiooni sisestamist küsimustikest sellisel viisil, et tekib andmete loogiline paiknemine ja ülesehitus. Peale andmete sisestamist on võimalik iga protsessiga seotud kahjude suurused kokku arvutada, mis omakorda võimaldab protsesse järjestada. Järjestamisel tuleb lisaks kahju suurusele jälgida ka seda, millised protsessid põhjustavad kahju kõige kiiremini. Parema ülevaate saamiseks on soovitatav iga protsessi kohta koostada graafik, mis võimaldab mõju suurusi visuaalselt paremini kuvada. Peale protsesside järjestamist on võimalik reastada juba iga konkreetse protsessiga seotud IT teenused vastavalt nende teenuste nõutud taasteajale ja anda hinnanguid ärimõjude analüüsi tulemuste kohta (Marquis, 2008).

Käesoleva punkti väljundiks on kogutud andmete põhjal läbi viidud ärimõjude analüüs ja informatsioon tulemuste kohta.

4.2.1.3 Aruande koostamine ja tulemuste levitamine

Ärimõjude analüüsi aruande koostamisel ja tulemuste levitamisel tuleb silmas pidada järgmisi punkte:

- Tulemuste levitamiseks koostada ärimõjude analüüsi aruanne;
- aruande koostamiseks sobib organisatsioonis kasutusel olev aruande formaat;
- aruanne peab hõlmama ärimõjude analüüsi ulatust, analüüsi tulemusena selgunud kriitilisi põhiprotsesse, nende prioriteete, põhiprotsesse toetavaid IT teenuseid ja püstitatud taaste-eesmärke;
- aruande edastamine kõikidele antud protsessis osalenutele ja nendele, kes analüüsi tulemuste põhjal võtavad vastu edasisi otsuseid;
- tulemuste osas saada juhtkonna või nõukogu kinnitus (Marquis, 2008).

Käesoleva punkti väljundiks on ärimõjude analüüsi aruanne, mille tulemused on aktsepteeritud ja osalistele edastatud.

4.2.2 Riskide hindamise läbiviimine

Ärimõjude analüüsi järgselt tuleb läbi viia riskide hindamine. Selle läbiviimisel tuleb eelkõige lähtuda organisatsioonis kasutusel olevast riskihalduse metoodikast, sealhulgas riskide hindamise põhimõtetest. Käesoleva punkti juures tuleb esmalt tutvuda riskide hindamise läbiviimise põhimõtetega (vt punkt 3.2.2) ja teostada järgmised tegevused (Stoneburner, Goguen & Feringa, 2002):

- IT teenustega seotud informatsiooni kirjeldamine (vt punkt 4.2.2.1);
- sobilike andmekogumise viisidega tutvumine ja sobivaima valimine (vt punkt 4.2.2.2);
- IT teenustega seotud ohtude tuvastamine (vt punkt 4.2.2.3);
- IT teenustega seotud nõrkuste tuvastamine (vt punkt 4.2.2.4);
- olemasolevate või plaanitavate turvameetmete analüüs (vt punkt 4.2.2.5);

- ohu esinemise tõenäosuse määratlemine (vt punkt 4.2.2.6);
- ohu mõju suuruse määratlemine (vt punkt 4.2.2.7);
- IT teenustega seotud riski suuruse määratlemine (vt punkt 4.2.2.8);
- tulemuste dokumenteerimine ja esitamine (vt punkt 4.2.2.9).

4.2.2.1 IT teenustega seotud informatsiooni kirjeldamine

Riskide hindamist tuleb läbi viia ärimõjude analüüsi käigus selgunud kõige kriitilisemaid põhiprotsesse toetavate IT teenuste kohta. Sellest tulenevalt on esmalt vaja tuvastada iga teenusega seotud informatsioon. Lähtuvalt standardist NIST 800-30 (Stoneburner, Goguen & Feringa, 2002) tuleb andmed koguda ja kirjeldada järgmiste punktide kohta:

- Riistvara;
- tarkvara;
- liidesed;
- andmed ja informatsioon;
- kasutajad ja tugiisikud;
- IT teenuse eesmärk;
- IT teenuse ja andmete kriitilisus (IT teenuse väärtus või tähtsus organisatsioonile);
- IT teenuse ja andmete tundlikkus (terviklikkus, konfidentsiaalsus ja käideldavus).

Käesoleva punkti väljundiks on põhjalik loetelu iga IT teenusega seotud komponentidest.

4.2.2.2 Sobilike andmekogumise viisidega tutvumine ja sobivaima valimine

Andmete kogumiseks sobib järgnevalt esitatud meetodite kasutamine üksikult või nende kombineerimine vastavalt vajadusele. Küsimustike ja intervjuude kohta on täpsem informatsioon kirjeldatud ärimõjude analüüsi läbiviimise punktis 4.2.1, mille raames antud soovitused on kohaldatavad ka käesolevas punktis. Andmeid kogutakse punktis 4.2.2.1 kirjeldatud informatsiooni kohta. Andmete kogumise viisid on lähtuvalt standardist NIST 800-30 (Stoneburner, Goguen & Feringa, 2002) järgmised:

- Küsimustikud;

- personaalsed intervjuud;
- dokumentidega tutvumine (nt turva- ja konfiguratsioonidokumendid ning manuaalid);
- tarkvaralised lahendused (nt automaatsed skaneerimistarkvarad).

Käesoleva punkti väljundiks on sobivaima andmekogumise viisi tuvastamine.

4.2.2.3 IT teenustega seotud ohtude tuvastamine

Tuvastada tuleb kõikvõimalikud ohud, mis mõjutavad kriitiliste põhiprotsesside tööd toetavaid IT teenuseid. Lähtuda tuleb enamlevinud ohuallikatest, mis infosüsteemide kolmeastmelise etalonturbe süsteemis (ISKE, 2011) väljatooduna on järgmised:

- Vääramatud jõud (nt personali väljalangemine, äike, kahjutuli, vesi, magnetväljad);
- organisatsioonilised puudused (nt dokumentatsiooni puudumine, volitamatu juurdepääs ruumidesse, failide ja andmekandjate ebaturvaline transport);
- inimvead (nt seadme või andmete hävitamine kogemata, IT-süsteemi väär haldus, väär pääsuõiguste haldus, andmebaasisüsteemi hooletu haldus, koristajad);
- tehnilised rikked ja defektid (nt sisevõrkude katkestus, programmivigade ilmnemine, andmebaasi väljalangemine, andmete kadu andmebaasis, toitevõrgu katkestused);
- ründed (nt IT-seadmete, tarvikute või andmete manipuleerimine või hävitamine).

Käesoleva punkti väljundiks on nimekiri IT teenustega seotud potentsiaalsetest ohtudest. Lisaks on ohtude tuvastamisel võimalik tugineda erinevatele infoturbe materjalidele ja infoturbega tegelevate organisatsioonide veebilehtedel avaldatud informatsioonile.

4.2.2.4 IT teenustega seotud nõrkuste tuvastamine

Järgnevalt tuleb tuvastada IT teenustega seotud nõrkused. Lähtuvalt standardist NIST 800-30 (Stoneburner, Goguen & Feringa, 2002) leiab vajaliku informatsiooni nõrkuste kohta järgmistest allikatest:

- Dokumendid – hõlmab küsimustike abil kogutud andmete analüüsi ja süsteemi konfiguratsiooni, auditi, turvalisuse ning testimiste aruandeid ja dokumentatsiooni;

- turvatestid – hõlmab ründetestide läbiviimist ja süsteemi nõrkuste tuvastamiseks mõeldud skaneerimistarkvarade ning turvaanalüüsi tarkvarade kasutamist;
- turvanõuete loetelu – turvanõuete loetelu ja küsimustikest kogutud andmed võimaldavad tuvastada süsteemi jaoks nõutud turvanõuete vastavuse olemasolevate või plaanitavate turvameetmetega.

Käesoleva punkti väljundiks on nimekiri IT teenustega seotud nõrkustest, mida potentsiaalsed ohud võivad ära kasutada.

4.2.2.5 Olemasolevate või plaanitavate turvameetmete analüüs

IT teenustega seotud riskide hindamisel tuleb arvesse võtta olemasolevaid või plaanitavaid turvameetmeid. Analüüsi teostamisel on abiks eelnevas punktis (vt punkt 4.2.2.4) kirjeldatud turvanõuete loetelu koostamine, mis võimaldab tuvastada olulised lahknevused. Tähelepanu tuleb pöörata nii füüsilistele, infotehnoloogilistele kui ka organisatsioonilistele meetmetele, mis omakorda jagunevad ennetavateks ning avastavateks meetmeteks. Füüsilised meetmed hõlmavad sissepääsu kontrolli- ja valvesüsteeme, infotehnoloogilised meetmed pääsuõigusi, krüptograafiat, varundamist ja viirusetõrjet ning organisatsioonilised meetmed poliitikaid, protseduure, reegleid ja juhiseid. Ennetavad meetmed on vajalikud infoturbe intsidentide ärahoidmiseks. Avastavad meetmed rakenduvad siis kui intsident on aset leidnud või on selles osas kõrgendatud kahtlus (Stoneburner, Goguen & Feringa, 2002).
Käesoleva punkti väljundiks on loetelu IT teenustega seotud olemasolevatest või plaanitavatest turvameetmetest.

4.2.2.6 Ohu esinemise tõenäosuse määratlemine

Ohu esinemise tõenäosuse määratlemisel tuleb arvesse võtta nõrkuse olemust, ohu tüüpi, ajendit ja võimekust ning olemasolevate turvameetmete efektiivsust. Lähtuvalt standardist NIST 800-30 (Stoneburner, Goguen & Feringa, 2002) tuleb tõenäosuse hinnangud anda järgnevalt defineeritud tõenäosuse tasemetele:

- suur – ohuallikas on väga motiveeritud ja piisavalt võimekas ning turvameetmed on nõrkuste ärakasutamiseks ebaefektiivsed;

- keskmine – ohuallikas on motiveeritud ja võimekas, kuid turvameetmed on rakendatud sellisel määral, mis raskendavad nõrkuste ärakasutamist;
- väike – ohuallikal puudub motivatsioon ja võimekus ning turvameetmed on rakendatud määral, mis takistavad või raskendavad oluliselt nõrkuste ärakasutamist.

Käesoleva punkti väljundiks on tõenäosuse tasemed skaalal suur, keskmine, väike ja nende tasemete määratlused.

4.2.2.7 Ohu mõju suuruse määratlemine

Ohu mõju suuruse määratlemisel tuleb vajalik informatsioon tuvastada ärimõjude analüüsi tulemustest. Lähtuvalt standardist NIST 800-30 (Stoneburner, Goguen & Feringa, 2002) antakse mõju suuruse hinnangud järgnevalt defineeritud tasemetele:

- suur – ohu realiseerumine võib põhjustada suures ulatuses materiaalsete põhivarade või ressursside kaotust; võib oluliselt kahjustada, rikkuda või takistada organisatsiooni missiooni, mainet või huve; võib põhjustada inimese surma või tõsiseid vigastusi;
- keskmine – ohu realiseerumine võib põhjustada materiaalsete varade või ressursside kaotust; võib kahjustada, rikkuda või takistada organisatsiooni missiooni, mainet, või huve; võib põhjustada inimvigastusi;
- väike – ohu realiseerumine võib põhjustada osade materiaalsete varade või ressursside kaotust; võib märgatavalt mõjutada organisatsiooni missiooni, mainet või huve.

Käesoleva punkti väljundiks on mõju suuruse tasemed skaalal suur, keskmine, väike ja nende tasemete määratlused.

4.2.2.8 IT teenustega seotud riski suuruse määratlemine

Riski suuruse määratlemiseks tuleb koostada riskimaatriks, riskiskaala ja kirjeldada riskitasemed. Riski suuruse arvutamine tuleb teostada iga oht-nõrkus paari kohta, kus leitav riskitase väljendab järgmisi punkte:

- Ohu realiseerumise tõenäosus;

- mõju suurus ohu realiseerumisel;
- olemasolevate või plaanitavate turvameetmete tõhusus (Stoneburner, Goguen & Feringa, 2002).

Riski suuruse arvutamisel on abiks riskimaatriks, mis on kahemõõtmeline tabel, mille ühel teljel paikneb ohu esinemise tõenäosus (väike, keskmine, suur) ja teisel mõju suurus (väike, keskmine, suur). Vastavalt tasemetele tuleb riskid kanda maatriksile (Stoneburner, Goguen & Feringa, 2002).

Leitavate riskitasemete (väike, keskmine, suur) suuruste paremaks esitamiseks tuleb tõenäosuse ja mõju suuruse tasemetele anda numbrilised väärtused. Näitena esitab standard NIST 800-30 (Stoneburner, Goguen & Feringa, 2002) järgnevad väärtused:

- Ohu esinemise tõenäosuse tasemed (0.1 = väike, 0.5 = keskmine, 1.0 = suur);
- mõju suuruste tasemed (10 = väike, 50 = keskmine, 100 = suur).

Riski suuruse arvutamisel tuleb ohu esinemise tõenäosus korrutada mõju suurusega, mis võimaldab riski paigutada vastavale riskiskaalale, tuvastades seeläbi riskitaseme. Riskiskaala esitatakse järgmisel kujul:

- suur (51-100);
- keskmine (11-50);
- väike (1-10) (Stoneburner, Goguen & Feringa, 2002).

Selleks, et riskide vastu meetmeid rakendada, tuleb kirjeldada riskitasemed. Riskitasemeid võib kirjeldada järgnevalt:

- suur – suure tasemega riskide puhul peab sobilike meetmete kasutuselevõtt toimuma nii kiiresti kui võimalik, rakendades selleks sobilikku strateegiat;
- keskmine – keskmise tasemega riskide puhul on meetmed vaja kasutusele võtta mõistliku aja jooksul, rakendades selleks sobilikku strateegiat;

- madal tase – madala tasemega riskide puhul on vaja otsustada meetmete kasutuselevõtu vajalikkus või leppida antud riskitasemega (Stoneburner, Goguen & Feringa, 2002).

Käesoleva punkti väljundiks on IT teenustega seotud riski suuruste tuvastamine vastavalt riskitasemetele kõrge, keskmine, madal.

4.2.2.9 Tulemuste dokumenteerimine ja esitamine

Riskide hindamise järgselt on vaja koostada formaalne riskide hindamise aruanne, mis kirjeldab ära tuvastatud ohud ja nõrkused ning esitab riski suurused. Aruande põhjal on juhtkonnal võimalik vastu võtta edasisi otsuseid rakendavate meetmete osas.

4.2.3 IT teenuste talitluspidevuse strateegia loomine

Ärimõjude analüüsi ja riskide hindamise järgselt on vaja luua IT teenuste talitluspidevuse strateegia, mis peab tuginema eelpool nimetatud protsesside aruannetel. Strateegia loomisel on vaja otsustada, millised IT teenused vajavad riskide vähendamise meetmeid ja millised taastamise meetmeid. Käesolevas punktis on lähtutud Office of Government Commerce (2007) parimate praktikate raamistiku *Service Design* publikatsioonist. Strateegia loomisel on esmalt vaja tutvuda selle põhimõtetega (vt punkt 3.2.3) ja seejärel teostada järgmised tegevused:

- riskide vähendamise meetmetega tutvumine (vt punkt 4.2.3.1);
- IT teenuste taastamisega seotud meetmetega tutvumine (vt punkt 4.2.3.2);
- strateegia väljatöötamine (4.2.3.3).

4.2.3.1 Riskide vähendamise meetmetega tutvumine

IT teenuste puhul, millel on suur mõju lühikese aja jooksul, tuleb rakendada ennetavaid meetmeid nagu riskide vähendamine, mis hõlmab järgmisi punkte:

- Varutoiteallikate kasutuselevõtt;

- üksikute tõrkeallikate (*Single Point of Failure*) kõrvaldamine;
- kõrgkäideldavate IT süsteemide ja võrkude loomine;
- *RAID* (*Redundant Array of Independent Disks*) ketaste kasutamine serversüsteemides;
- veakindlate süsteemide loomine kriitiliste rakenduste jaoks;
- teenuste sisseostmine rohkem kui ühelt väliselt teenusepakkujalt;
- eelnevalt konfigureeritud varuriistvara säilitamine peamise riistvara rikke korral;
- tõhusamad füüsilised ja IT-põhised turvameetmed, sealhulgas kiipkaardi süsteemid;
- efektiivsemad võimalused, et tuvastada teenuste katkestuste põhjustajaid, sealhulgas tulekahju tuvastamise süsteem koos tule summutamise süsteemiga;
- terviklik andmete varundamise ja taastamise strateegia, sealhulgas majaväline varundus (Office of Government Commerce, 2007).

Käesoleva punkti väljundiks on loetelu meetmetest, mis võimaldavad IT teenustega seotud riske vähendada ja valikute põhjendused.

4.2.3.2 IT teenuste taastamisega seotud meetmed

IT teenuste puhul, mille suurem mõju ilmneb alles mõne aja pärast, tuleb rakendada sobilikke taastamise meetmeid. Võimalikud meetmed lähtuvalt Office of Government Commerce (2007) parimate praktikate raamistiku *Service Design* publikatsioonist on esitatud järgnevalt:

- Käsitsi teostatavad lahendused – lühiajalisi ja käsitsi teostatavaid lahendusi on sobilik kasutada selliste IT teenuste puhul, kus need on praktilised ja mõeldavad (nt kasutajatoe kõnede logimine);
- vastastikused kokkulepped – lepe kahe organisatsiooni vahel teatud ressursside ühiskasutuseks hädaolukorras (nt majavälised varunduslahendused);
- astmeline taastamine – taastamisviis, mida kutsutakse ka „külmaks reserviks“. Eeldatakse, et IT teenuse taastamine toimub enam kui 72 tunni jooksul. Astmelise taastamise korral kasutatakse tavaliselt teisaldatavaid või püsiehitisi, kus on olemas üldine töökeskkond ja sidevõrk, kuid puuduvad arvutisüsteemid. Riist- ja tarkvara paigaldatakse sinna IT talitluspidevusplaani alusel;
- kesktaseme taastamine – taastamisviis, mis on tuntud ka kui „soe reserv“. Eeldatakse, et IT teenus taastatakse 24 kuni 72 tunni jooksul. Kesktaseme taastamisel kasutatakse

tavaliselt teisaldatavaid või püsiehitisi, kus on olemas arvutisüsteemid ja andmesidevõrk. Võib olla vajalik konfigureerida riist- ja tarkvara ning taastada andmeid varukoopiatest, mida tehakse IT talitluspidevusplaani järgi;

- kiire taastamine – taastamisviis, mille puhul eeldatakse, et IT teenus taastatakse kiiresti, tavaliselt vähem kui 24 tunni jooksul. Kiire taastamise korral kasutatakse selleks määratud püsiehitisi, kuhu on paigaldatud arvutisüsteemid ja tarkvara on valmis IT teenuseid jooksutama. Kohene taastamine võib kesta kuni 24 tundi, kui on vaja varukoopiatest andmeid taastada;
- kohene taastamine – taastamisviis, mida kutsutakse ka „kuumaks reserviks". Eeldatakse, et IT teenust saab taastada koheselt ja ilma katkestusteta. Kohene taastamise korral kasutatakse tavaliselt peegeldusi, koormuse jaotust ja topeldatud keskusi (itSMF Estonia, 2010).

Käesoleva punkti väljundiks on loetelu sobilikest meetmetest, mis on vajalikud IT teenuste taastamiseks ja valikute põhjendused.

4.2.3.3 Strateegia väljatöötamine

Strateegia väljatöötamisel ja koostamisel tuleb määratleda kriitiliste IT teenuste jätkusuutlikkuse tagamise üldine lähenemine. Lähtudes Office of Government Commerce (2007) parimate praktikate raamistiku *Service Design* publikatsioonist peab strateegia tuginema järgmistele punktidele:

- Teenuste puhul, millel on suur mõju lühikese aja jooksul, tuleb kasutada ennetavaid meetmeid nagu riskide vähendamine;
- teenuste puhul, mille mõju katkestuse esinemisel on väike ja mis eskaleeruvad pikema aja jooksul, tuleb rakendada taastamisega seotud meetmeid;
- teenuste puhul, mille mõju kasvab aja jooksul lineaarselt, tuleb kasutada tasakaalustatud lähenemist ja keskenduda mõlemate meetmete kombineerimisele.

Taastamisega seotud meetmete valikul peab arvestama järgmiste punktidega:

- Töötajad ja majutus;
- IT süsteemid ja võrgud;

- elutähtsad teenused (elekter, vesi, telekommunikatsioon jms);
- elutähtsad varad (paberdokumendid jms) (Office of Government Commerce, 2007).

Lisaks eelnevale tuleb iga meetme puhul eraldi arvestada järgmiste punktidega:

- Valitud meetme võimekus tagada teenuse taastamine nõutud aja jooksul;
- meetme võimekus tagada kriitiliste andmete taastekoht;
- meetme rakendamise tõhusus riski suurusele;
- meetme rakendamise eeldatav maksumus;
- meetme ülalhoiu, testimise ja plaanide kasutuselevõtu maksumus;
- tagajärjed mittetegutsemisel (ENISA, 2012).

Käesoleva punkti väljundiks on juhtkonna või nõukogu poolt heaks kiidetud ja allkirjastatud IT teenuste talitluspidevuse strateegia dokument, mis sisaldab IT teenustega seotud riskide vähendamise ning taastamise meetmeid koos põhjendustega.

4.3 Talitluspidevuse juurutamine

Peale IT teenuste talitluspidevuse strateegia loomist ja selles kokku leppimist on vaja teostada talitluspidevuse juurutamisega seotud tegevused. Talitluspidevuse juurutamisel on esmalt vaja tutvuda selle põhimõtetega (vt punkt 3.3) ja seejärel lähtuvalt Office of Government Commerce (2007) parimate praktikate raamistiku *Service Design* publikatsioonist teostada järgmised punktid:

- IT talitluspidevus- ja taasteplaanide ning taasteprotseduuride loomine (vt punkt 4.3.1);
- plaanide esmane testimine (vt punkt 4.3.2).

4.3.1 IT talitluspidevus- ja taasteplaanide ning taasteprotseduuride loomine

Plaanide loomisel on esimese tegevusena vaja tutvuda vajalike põhimõtetega (vt punkt 3.3.1), millele järgnevalt on vaja luua plaanid ja protseduurid. Järgnevalt on esitatud nõuded IT talitluspidevusplaani sisule, mille esitamisel on tuginetud Riigi Teataja toimepidevuse plaani

koostamise juhendile (2010) ja Finantsinspektsiooni soovituslikule juhendile talitluspidevuse protsessi korraldamisel (2009):

- Plaani haldus – sisaldab andmeid plaani levitamise, ülevaatuse ja kinnitamise kohta;
- sissejuhatus – esitab selgelt plaani eesmärgi ja oodatava tulemuse;
- plaani kasutuselevõtu tingimused - tuuakse välja katkestuse ulatus, mille ilmnemise korral rakendatakse plaanis kirjeldatud meetmeid ja plaani kasutuselevõtu protseduur;
- töötajate andmed – nimekiri talitluspidevusega seotud töötajate ajakohastatud kontaktandmetest, sealhulgas nimed, aadressid ja kõik telefoninumbrid;
- töötajate ohutuse tagamine – kirjeldatakse protseduurid töötajate ohutuse tagamiseks;
- katkestusest teavitamise korraldus – kirjeldatakse kriisikommunikatsiooni reeglid, so kuidas ja millal teavitatakse töötajaid, kliente ja koostööpartnereid ning avalikkust. Lisaks määratletakse infovahetuse korraldamise eest vastutav isik. Sisaldab ka juhiseid, kuidas käituda, kui sidevahendite kasutamine on häiritud;
- rollid ja kohustused - esitatakse plaani elluviimise eest vastutavate isikute loetelu, ülesanded ning volitused plaani elluviimisel;
- minimaalsed talitluspidevuse nõuded – kirjeldatakse informatsioon kriitiliste põhiprotsesside ja nendega seotud IT teenuste kohta. Hõlmab muuhulgas põhiprotsessi maksimaalset lubatud katkestuse kestust ja nõutavat taasteaega. Lisaks kirjeldatakse iga põhiprotsessiga seotud IT teenuste taasteaeg ja –koht;
- IT teenuste loetelu – kirjeldatakse informatsioon olulisemaid põhiprotsesse toetavate IT teenuste ja nendega seotud ressursside kohta. Käesolevas punktis antakse ülevaade ka riske vähendavatest meetmetest. Sisaldab muuhulgas andmeid oluliste ressursside paiknemise kohta, sealhulgas vajalike lepingute, kliendifailide, operatsioonisüsteemide, rakenduste, andmefailide, kasutusjuhendite ning programmi-, süsteemi- ja kasutajadokumentatsiooni varuasukoht;
- alternatiivasukoht – kirjeldatakse IT teenuste osutamiseks vajalik alternatiivasukoht. Lisaks sisaldab logistikateavet oluliste ressursside, sh töötajad, transportimiseks põhiasukohast alternatiivasukohta;
- viited taasteplaanidele ja -protseduuridele – esitatakse viited IT taasteplaanidele ja üksikasjalikele protseduuridele IT teenuste taastamiseks;
- plaani testimine – määrab, kui tihti plaani testitakse, millises ulatuses ja millised on oodatavad ning saavutatud tulemused.

IT talitluspidevusplaani loomise järgselt tuleb koostada IT taasteplaanid ja -protseduurid. Need peavad olema kirjutatud viisil, mis võimaldab plaane ja protseduure järgida ning täita kogenud spetsialistil, kellel puuduvad konkreetse organisatsiooniga seotud teadmised. Tuginedes Office of Government Commerce (2007) parimate praktikate raamistiku *Service Design* publikatsioonile peab taasteplaanide ja -protseduuride sisu kajastama järgmisi punkte:

- Plaani haldus – sisaldab informatsiooni plaani levitamise, ülevaatuse ja kinnitamisega;
- sissejuhatus – esitab selgelt plaani otstarbe ja oodatava tulemuse ning taastamisega seotud IT teenused;
- taastestrateegia – kirjeldab taastamisega seotud olulise informatsiooni nagu alternatiivasukoht, taastamiseks kuluv potentsiaalne aeg, nõutud taasteaeg ja –koht ning plaani viimane testimine ja tulemus;
- plaani aktiveerimine – loend töötajatest, kellel on volitus plaani kasutuselevõtmiseks;
- seosed teiste plaanidega – seosed teiste talitluspidevus- ja taasteplaanidega ning tingimused nende kasutuselevõtmise kohta;
- üldised juhised intsidendi korral – kommunikatsioon ja tegevuste eskaleerumine;
- seosed teiste teenustega – teenuste järjekord taastamisel ja seosed teiste teenustega;
- kontaktid – loetelu taastamisega seotud sisemistest ja välistest kontaktidest, nende rollidest ja kontakteerumisviisist;
- taastemeeskond – nimekiri taasteprotseduuride täitmisega seotud töötajatest, nende rollidest ja kontakteerumisviisist;
- taastemeeskonna tegevused – loetelu taastamisega seotud peamistest ülesannetest, mis võimaldab märkida iga tegevuse planeeritud ja tegeliku tulemi;
- üksikasjalikud taasteprotseduurid:
    - detailsed juhised ja protseduurid IT teenuste taastamiseks;
    - vajadusel viited teistele juhistele ja protseduuridele.

IT taasteplaani näidisdokument (Office of Government Commerce, 2007) asub lisas 2.

Käesoleva punkti väljundiks on koostatud IT talitluspidevus- ja taasteplaanid ning taasteprotseduurid, mille loomisel on arvestatud eelnevalt loetletud punktidega.

4.3.2 Plaanide esmane testimine

Plaanide esmasel testimisel on vaja tutvuda selle põhimõtetega (vt punkt 3.3.2). Tuginedes ENISA (2012) soovitustele on plaanide esmasel testimisel vaja teostada järgmised tegevused:

- Testkeskkonna loomine (vt punkt 4.3.2.1);
- testi määratlemine (vt punkt 4.3.2.2);
- testi planeerimine (vt punkt 4.3.2.3);
- testi läbiviimine (vt punkt 4.3.2.4);
- testijärgse koosoleku korraldamine ja aruande koostamine (vt punkt 4.3.2.5).

4.3.2.1 Testkeskkonna loomine

Testkeskkonna loomisel on soovituslik kasutusele võtta virtualiseerimistehnoloogial põhinev lahendus, mille eelisteks on selle rakendatavuse lihtsus ja integratsioon. Antud lähenemine mängib taastamisel olulist rolli järgmistes punktides (Dorion, 2008):

- Maksumus – virtualiseerimistehnoloogia võimaldab vähendada testimiseks vajalike füüsiliste serverite arvulist kogust nii peamises kui ka alternatiivasukohas;
- tarnega seotud viivitused – virtualiseerimistehnoloogia võimaldab vähendada sõltuvust füüsilisest riistvarast ja seeläbi riistvara tarnega seotud viivitusi;
- kiire taastamine – virtuaalserverite tõmmiste kasutuselevõtmine ja erinevate füüsiliste süsteemide vahel liigutamine toimub väga kiiresti.

Käesoleva punkti väljundiks on sobiliku virtuaaltehnoloogial põhineva testkeskkonna loomine, mis võimaldab testimiste läbiviimist.

4.3.2.2 Testi määratlemine

Plaanide testimine eeldab sobiva testi meetodi määratlemist. Tuginedes Office of Government Commerce (2007) parimate praktikate raamistiku *Service Design* publikatsioonile on neli peamist testitüüpi järgmised:

- Simulatsiooni test – toimub grupitööna, kus plaani iga etapp arutatakse suuliselt läbi;
- stsenaariumi test – testimine viiakse läbi kindla sündmuse läbimängimiseks;
- osaline test – viiakse läbi üksiku IT teenuse või serveri taastamine;
- kõikehõlmav test – hõlmab kõikide olemasolevate plaane testimist, kuhu kaasatakse organisatsiooni äripool ja sisseostetavate teenuste osutajad.

Käesoleva punkti väljundiks on sobiva testi meetodi tuvastamine, mis võimaldab selle põhjal testi planeerida.

4.3.2.3 Testi planeerimine

Testi läbiviimiseks tuleb koostada testi plaan. Lähtudes standardist NIST 800-34 (Swanson, Bowen, Philips, Gallup & Lynes, 2010), hõlmab testi planeerimine järgmisi tegevusi:

- Määratleda, mida soovitakse testida;
- määratleda testi ulatus ja stsenaarium;
- määratleda testi eesmärgid ja edu kriteeriumid;
- koostada üksikasjalik loetelu tegevustest;
- määratleda tegevuste ajavahemik ja testis osalejad.

Käesoleva punkti väljundiks on sobiva testi meetodi põhjal koostatud testi plaan, mis võimaldab testi läbiviimist.

4.3.2.4 Testi läbiviimine

Tuginedes ENISA (2012) soovitustele, tuleb testi läbiviimisel arvestada järgmiste punktidega:

- Testi läbiviimine peab toimuma võimalikult reaalse stsenaariumi järgi;
- osalejaid tuleb teavitada vajalikust informatsioonist ja anda ülevaade situatsioonist;
- testis osalejad peavad testi läbiviimsel kasutama asjakohaseid plaane;
- testis osalejatel tuleb dokumenteerida iga tegevuse tulem.

Lähtudes Business Continuity Institute (2007) juhendist *The Good Practice Guidelines*, tuleb testi läbiviimisel leida vastused järgmistele küsimustele:

- Tehnika – kas seadmed töötavad;
- protseduurid – kas protseduurid on õiged;
- logistika – kas protseduurid toimivad omavahel loogilises kooskõlas;
- õigeaegsus – kas protseduuride kaudu saavutatakse tegevuste nõutud taasteaeg;
- administratiivne – kas protseduurid on juhitavad;
- personal – kas on kaasatud õiged inimesed vajalike oskuste, volituste ja kogemustega.

Käesoleva punkti väljundiks on sobiva testi läbiviimine, mille juures on arvestatud eelnevalt loetletud punktidega.

4.3.2.5 Testijärgse koosoleku korraldamine ja aruande koostamine

Testimise järgselt tuleb korraldada vastavasisuline koosolek, mis hõlmab ka testiaruande koostamist. Lähtudes ENISA (2012) soovitustest, peab antud punkti juures arvestama järgmiste tegevustega:

- Testimise järgselt tuleb korraldada koosolek niipea kui võimalik;
- osalejatel tuleb anda tagasisidet testi edukuse ja paranduste sisseviimise osas;
- koosolekust peavad osa võtma kõik testis osalejad ja need, kes on seotud plaani haldamisega;
- koosoleku lõpus määratletakse kohustused paranduste sisseviimiseks plaani;
- testi järgselt on vaja koostada testi aruanne, mis sisaldab eesmärki, ulatust, meetodit, toimumise aega, kaasatud ressursse, testi läbiviijat ja tulemusi ning soovitusi parandusteks koos paranduste täitjatega;
- testi mõne osa ebaõnnestumisel tuleb plaanis teostada muudatused ja planeerida uuesti testi läbiviimine.

Käesoleva punkti väljundiks on testijärgselt läbiviidud koosolek, mis hõlmab testiaruande koostamist.

4.4 Igapäevane haldus

Plaanide loomise ja nende esmase testimise järgselt tuleb tagada, et talitluspidevusega seotud temaatikale pööratakse tähelepanu ka edaspidi. See on võimalik igapäevase halduse etapi kaudu (vt punkt 3.4). Tuginedes Office of Government Commerce (2007) parimate praktikate raamistiku *Service Design* publikatsioonile, hõlmab käesolev etapp järgmisi punkte:

- Harimine, teadlikkuse tõstmine ja koolitused (vt punkt 4.4.1);
- talitluspidevuse alase võimekuse regulaarne ülevaatus (vt punkt 4.4.2):
- regulaarne testimine (vt punkt 4.4.3);
- muudatuste haldus (vt punkt 4.4.4).

4.4.1 Harimine, teadlikkuse tõstmine ja koolitused

Harimise, teadlikkuse tõstmise ja koolituste valdkonnas on esmalt vaja tutvuda vastavate põhimõtetega (vt punkt 3.4.1). Tuginedes ENISA (2012) soovitustele on töötajate harimine ja teadlikkuse tõstmine võimalik järgmiste punktide kaudu:

- Koolitused;
- uue töötaja sisseelamisprogramm;
- stsenaariumi harjutused ja testid;
- artiklid organisatsiooni uudiskirjas;
- informatsioon Intranetis;
- päevakorrapunkt koosolekutel.

Lähtudes standardist NIST 800-34 (Swanson, Bowen, Philips, Gallup & Lynes, 2010), tuleb töötajate koolitamisel arvesse võtta järgmiseid punkte:

- Koolitusi tuleb läbi viia vähemalt kord aastas;
- töötajad, kellele on määratud roll mõnes talitluspidevuse plaanis, peavad saama koolituse niipea kui võimalik;
- töötajad peavad olema koolitatud sellisel tasemel, mis võimaldab neil oma rolle ja kohustusi täita ilma plaanita.

- töötajaid tuleb koolitada plaani järgmiste komponentide suhtes:
    - Plaani eesmärk;
    - meeskondade vaheline koordinatsioon ja kommunikatsioon;
    - aruandluse protseduurid;
    - turvakorraldused;
    - meeskonna spetsiifilised tegevused;
    - individuaalsed kohustused.

Käesoleva punkti väljundiks on meetodid, mis võimaldavad organisatsioonil töötajaid talitluspidevusega seotud teemadel harida ja koolitada ning tõsta nende teadlikkuse taset.

4.4.2 Talitluspidevuse alase võimekuse regulaarne ülevaatus

Talitluspidevuse alase võimekuse regulaarsel ülevaatusel on esmalt vaja tutvuda vastavate põhimõtetega (vt punkt 3.4.2). Järgnevalt esitatud soovitustes on tuginetud ENISA (2012) vastavatele juhenditele. Talitluspidevuse plaanide ja muude dokumentide ülevaatamine ja vajadusel täiendamine peab toimuma järgmistel juhtudel:

- Põhiprotsessides või tehnoloogias toimuvate suuremate muudatuste tagajärjel;
- testi või harjutuse järgselt;
- auditist tulenevate soovituste järgselt;
- regulaarse ülevaatuse ajakava kohaselt (ENISA, 2012).

Regulaarse ülevaatuse käigus tuleb tähelepanu pöörata järgmistele punktidele:

- Kõige olulisemad põhiprotsessid ja neid toetavad IT teenused ning nende osad on tuvastatud ja kirjeldatud talitluspidevuse strateegias;
- talitluspidevuse poliitika, strateegia, raamistik ja plaanid kajastavad täpselt prioriteete ja nõudeid;
- talitluspidevuse alane kompetents ja võimekus on efektiivne ning eesmärgipärane ja võimaldab intsidendi juhtimist ning koordineerimist;
- talitluspidevusega seotud meetmed on tõhusad, sobilikud ja täidavad riskitaseme seisukohalt oma eesmärki;

- talitluspidevuse strateegia ja plaanid sisaldavad intsidentide, harjutuste ning regulaarse ülevaatuse käigus tuvastatud parandusi;
- talitluspidevusega seotud protseduurid on edukalt kommunikeeritud olulistele töötajatele, kes teavad oma rolle ja kohustusi;
- talitluspidevuse testimise jaoks on rakendatud sobilik programm;
- muudatuste halduse protsess on rakendatud ja toimib efektiivselt (ENISA, 2012).

Käesoleva punkti väljundiks on talitluspidevusega seotud võimekuse regulaarne ülevaatus, mille läbiviimisel tuginetakse eelnevalt loetletud soovitustele.

4.4.3 Regulaarne testimine

Regulaarsete testide läbiviimiseks tuleb Office of Government Commerce (2007) parimate praktikate raamistiku *Service Design* publikatsioonist lähtuvalt rakendada sobilik programm (vt punkt 3.4.3). Talitluspidevuse plaanide testimist tuleb läbi viia regulaarselt ja vähemalt kord aastas, kuid regulaarsus sõltub ka läbiviidavast testitüübist:

- Simulatsiooni test – üks kord kvartalis;
- stsenaariumi test – üks kuni kaks korda aastas;
- osaline test – üks kord aastas;
- kõikehõlmav test – üks kord aastas (ENISA, 2012).

Vajaduse testimise järele võivad põhjustada ka järgmised punktid:

- Uute töötajate lisandumine;
- oluline muudatus organisatsiooni põhitegevuses;
- muudatused IT teenustes ja infotehnoloogias;
- organisatsiooni nõuded (Office of Government Commerce, 2007).

Käesoleva punkti väljundiks on organisatsioonis rakendatud programm regulaarsete testide läbiviimiseks, mille puhul tuginetakse eelnevalt esitatud soovitustele.

4.4.4 Muudatuste haldus

Talitluspidevusega seotud muudatuste haldamiseks tuleb Office of Government Commerce (2007) parimate praktikate raamistiku *Service Design* publikatsioonist lähtuvalt rakendada organisatsioonis sobilik muudatuste halduse protsess. Muudatuste haldamisel tuleb esmalt tutvuda vajalike põhimõtetega (vt punkt 3.4.4) ja arvestada järgmiste punktidega:

- Talitluspidevuse plaanid peavad olema muudatuste halduse protsessi all (Office of Government Commerce, 2007);
- plaanidega seotud muudatused, mis on tuvastatud harjutuste, testimise ja koolituste käigus tuleb teostada muudatuste halduse protsessi kaudu (ENISA, 2012);
- muudatuste võimalik mõju plaanidele on hinnatud (Office of Government Commerce, 2007);
- muudatused peab heaks kiitma talitluspidevuse eest vastutav isik (ENISA, 2012);
- uute IT teenuste kasutuselevõtmisel või olemasolevate muutumisel olulisel määral, tuleb teostada nende teenuste osas ärimõjude analüüs ja riskide hindamine ning vastavalt uuendada strateegiat ja plaane (Office of Government Commerce, 2007);
- muudatuste liigid, millega peab arvestama:
    - tehnoloogilised muudatused;
    - organisatsioonilised muudatused;
    - personalimuudatused;
    - välised muudatused (Gregory, 2008).

Käesoleva punkti väljundiks on organisatsiooni poolt kasutusele võetud muudatuste halduse protsess, mille juures lähtutakse eelpool loetletud punktidest.

Eelnevalt kirjeldatud muudatuste halduse punkt lõpetab IT teenuste talitluspidevuse tagamise üldskeemi peatüki. Järgmises peatükis antakse ülevaade taasteprotseduuride loomise protsessist avaliku sektori organisatsioonis ja sellest tulenevalt esitatakse soovitused edasiseks.

5. Taasteprotseduuride väljatöötamise analüüs avaliku sektori organisatsioonis

Käesolevas peatükis antakse ülevaade avaliku sektori organisatsiooni olulisemate IT teenustega seotud süsteemide taasteprotseduuride loomise protsessist. Vajadus protseduuride järele tulenes asutusepoolsest nõudest, millega määratleti kindlaks teatud võrgus asuvate süsteemide taasteaeg ja -koht. Sellest tulenevalt oli võimalik antud teema sidumine magistritööga, kuna IT teenuste talitluspidevuse planeerimise üheks osaks on just plaanide loomine (vt punkt 4.3.1) ja testimine (vt punkt 4.3.2), mis hõlmab ka taasteprotseduure.

Antud teema peamine eesmärk sai sõnastatud järgmiselt: „Olulisemate IT teenustega seotud süsteemide taasteprotseduuride väljatöötamine“. Eesmärgi saavutamiseks tuli omakorda püstitada alameesmärgid, mis hõlmasid tegevusi järgmistes punktides:

- Esmane visioon;
- testkeskkonna loomine;
- protseduuride loomine;
- protseduuride testimine;
- igapäevane haldus.

Taasteprotseduuride loomisega seotud esmase visiooni üle arutlesid käesoleva töö autor (IT-spetsialist) ja IT osakonna juht algsel vastavasisulisel koosolekul. See hõlmas punkte nagu vajadus taastekeskkonna loomise järele ja selle üldisem korraldus (nt töö- ja testvõrgu lahutamine), olulisemate süsteemide tuvastamine ning nendega seotud spetsiifilisemad küsimused (nt järjekord taastamisel). Muuhulgas lepiti kokku, et taasteprotseduurid peavad saama dokumenteeritud viisil, mis võimaldab süsteeme mittetundval spetsialistil (nt kasutajatoe töötajal) neid kasutada süsteemide edukaks taastamiseks.

Selgus neli olulisemat süsteemi, milleks olid kaks domeenikontrollerit, failiserver ja e-maili server. Eelneva informatsiooni põhjal soetas IT osakond sobiliku jõudlusega testserveri, mis pidi võimaldama taastekatsete läbiviimist. Töö autor paigutas testserveri küll olemasolevasse võrku, kuid virtualiseerimistehnoloogia abil oli võimalik töö- ja testvõrgu eraldamine. Vajaduse paigutada testserver olemasolevasse võrku tingis asjaolu, et varundusserverit ja

lindiseadet, millega teostati töökeskkonna süsteemide igapäevast varundamist, kasutas autor ka taastamiste läbiviimiseks ja seeläbi protseduuride valideerimiseks testkeskkonnas.

Peale taastekatsete läbiviimiseks sobiliku testkeskkonna loomist hakkas töö autor otsima taastamist vajavate süsteemide dokumentatsioone ja tootjapoolseid juhendeid taasteprotseduuride läbiviimiseks. Iga süsteemi kohta tuli läbi töötada suur hulk materjale, mis kirjeldasid erinevaid taasteprotseduure sõltuvalt kahju tüübist ja ulatusest. Käesoleval juhul lähtus autor nõudest koostada sellised plaanid ja protseduurid, mis võimaldavad süsteemide taastamist juhul, kui olemasolevad süsteemid on täielikult hävinenud ning nende taastamine peab toimuma kasutades alternatiivriistvara ja varunduslinte.

Kui algne mõte protseduuride kirjutamiseks nägi ette dokumentatsiooni tuvastamist, olulise informatsiooni filtreerimist, nende põhjal plaanide kirjutamist ja seejärel testimist, siis tegelikkuses langesid kõik tegevused ühte kokku. Töö autor leidis, et iga süsteemiga seotud taasteprotsessi läbiviimine, protseduuride samaaegne ülesmärkimine ja lisainformatsiooni otsimine andis kõige efektiivsema tulemuse. Sellisel juhul sai taasteprotseduur kirja jooksvalt koos korrektsete tegevustega.

Peale iga süsteemiga seotud protseduuri kirjasaamist oli taasteprotsessi läbiviimine võimalik juba koostatud protseduuri alusel, mis võimaldas koheselt ka selle valideerimist ja vajadusel vigade parandamist, mida ilmnes üsna sageli. Testimiste käigus esines üksikjuhtumeid, kus süsteemi seadistamisel tekkinud või protseduuri märgitud kirjaviga ilmnes alles mõne aja pärast ja tekitas mitme tunni töö jagu kahju ning põhjustas taasteprotsessi uuesti alustamise. Lisaks muudele vigadele tuvastas töö autor vea ka Microsofti juhendis, mis kirjeldas domeenikontrolleri taastamist. Reaalse taasteprotsessi käigus, tuginedes pelgalt eelpool nimetatud juhendile, võib antud vea tuvastamisel sellele lahenduse otsimine põhjustada taas olulist ajakadu. Autor leiab, et vigade ilmnemine ja ajalise kahju tekkimine testimise käigus on igati aktsepteeritav ja normaalne nähtus, kuid eksimuse avastamine pärisolukorras ning sellest tulenevalt probleemile lahenduse otsimine ja selle näol tekkiv ajaline kahju ei ole enam lubatav – oluline on kinni pidada organisatsiooni poolt nõutud taasteaegadest.

Kuna protseduuride loomise ja testimisega seotud periood kestis mitu kuud, siis tuli aeg-ajalt ette, et asutuse teised IT-spetsialistid teostasid mõnes süsteemis olulise muudatuse, mis omakorda tingis taas vajaduse protseduuride valideerimiseks ning vigade parandamiseks.

Eelpool öeldut ilmestab protseduuride loomise ajal toimunud füüsilise failiserveri operatsioonsüsteemi uuendamine ja tulenevalt sellest süsteemi viimine virtuaalkeskkonda, mis tingis antud süsteemiga seotud protseduuride täieliku ümberkirjutamise töö autori poolt. Failiserveri taasteprotseduur asub lisas 3.

Kuna taastamisega seotud valdkond sai antud töös valitud lähtuvalt avaliku sektori organisatsiooni vajadustest, siis magistriõpingute järgselt antud teema autori jaoks ei lõpe ning sellega tuleb igapäevaselt tegeleda ka edaspidi.

Tänase seisuga on avaliku sektori organisatsioonil olemas toimivad ja praktikas läbi proovitud tegevusjuhendid, mille alusel on võimalik kriisiolukorras, kus olemasolevate süsteemide (riist- ja tarkvara) kasutamine ei ole võimalik, olulisemate IT teenustega seotud süsteemide taastamine alternatiivasukohta.

Autori poolt loodud testkeskkond ja süsteemidega seotud taasteprotseduurid ning vastavad testimised on avaliku sektori organisatsioonile toonud lisaväärtust mitmel viisil:

- Olulisemate süsteemide jaoks loodud taasteprotseduurid toimivad praktikas;
- igapäevaselt varundatavate andmete, sh virtuaalsete süsteemide, terviklikkuse regulaarne kontroll;
- kindlus organisatsiooni poolt nõutud taasteaja ja -koha osas kinnipidamisel;
- muudatuste testimine testkeskkonnas enne töösolevaid süsteeme (sh töösolevate süsteemide logides pikalt üleval olnud veateadete põhjuste väljaselgitamine ja muudatuste testimine testkeskkonnas, suurendades seeläbi süsteemide käideldavust);
- uued teadmised taasteprotseduuride koostamisest ja süsteemidest, mis ei kuulu töö autori igapäevase administreerimise alla, mille tulemusel on antud süsteemide peaadministraatoreid võimalik asendada.

5.1 Autoripoolsed soovitused avaliku sektori organisatsioonile

Järgnevalt esitatakse autoripoolsed soovitused koos põhjendustega avaliku sektori organisatsiooni töö paremaks korraldamiseks talitluspidevusega, sh taasteprotseduuridega, seotud valdkonnas.

Asutuse juhtkonna poolt algselt määratletud ja seni kehtiv ajaline nõue süsteemide taasteaja ning -koha osas ei ole põhinenud ärimõjude analüüsi tulemusel, vaid on esitatud subjektiivse hinnanguna – hetkel kehtib üks ajaline nõue kõikide nõutud süsteemide kohta. Taasteprotseduure vajavate süsteemide osas on samuti tuginetud subjektiivsele hinnangule, kuigi nende asukoha võrgus eksisteerib veel teisigi süsteeme. Objektiivse hinnangu saamiseks soovitab töö autor läbi viia ärimõjude analüüsi, millest tulenevalt saab määratleda uued taasteajad ja -kohad ning tuvastada täpselt, millised süsteemid on kõige olulisemad. Ärimõjude analüüsi kaudu on võimalik tuvastada, kas antud süsteemid vajavad väiksemaid ajalisi nõudeid, mis on seotud käideldavuse tõstmisega ja sellest tulenevalt täiendavate kuludega riskide vähendamise ja taastamise meetmete näol või suuremaid ajalisi nõudeid, mis võimaldab ennetada süsteemide ülefinantseerimist ja tagada seeläbi kulude kokkuhoidu.

Teine soovitus seisneb väljatöötatud protseduuride sidumises konkreetse IT taasteplaaniga. Hetkel eksisteerivad küll süsteemidega seotud taasteprotseduurid, kuid ainult nendest ei piisa. Protseduurid tagavad iga süsteemi taastamisega seotud tegevused, kuid ei kirjelda vajalikku lisainformatsiooni nagu alternatiivasukoht, taastemeeskond, kommunikatsioon jmt. IT osakonna poolt on vaja luua kõikehõlmav IT taasteplaan, mille juurde antud protseduurid kuuluvad ja mis kirjeldab kogu informatsiooni, et võimaldada IT teenuste taastamist.

Kolmas soovitus on seotud taasteprotseduuride edasiarendamisega. Käesoleval hetkel eksisteerivad protseduurid, mis on mõeldud süsteemide taastamiseks alternatiivasukohta juhul kui olemasolevate süsteemide kasutamine ei ole võimalik. IT osakonna poolt tuleks protseduurid koostada ka süsteemide eripärast tulenevateks taastestsenaariumiteks (nt e-maili serveri taastamine juhul, kui e-maili rakendusega seotud andmebaasid ei asu mitte serveri peal, vaid mujal nt andmemassiivi seadmel ja seadme töös esineb rike). Erinevate taastestsenaariumite väljatöötamine võimaldab ka väiksematele intsidentidele operatiivselt reageerida ja seeläbi vähendada võimaliku katkestuse ajalist kestust.

Neljanda soovitusena tuleks rakendada muudatuste halduse protsessi. Süsteemidega teostatakse muudatusi igapäevaselt, mistõttu muutuvad nende seadistused pidevalt. Sellest tulenevalt ei pruugi taasteprotseduurid olla vastavuses enam tegelikkusega. Muudatuste halduse protsessi kaudu on võimalik tagada muudatuste registreerimine ja taasteprotseduuride uuendamine, mis võimaldab koheselt nende valideerimist läbi taastekaste. Sellega on tagatud protseduuride kaasajastatus, mis lubab intsidendi esinemisel tugineda nende õigsusele.

Viies soovitus seisneb vajaduses juurutada sobilik testimise programm. Praegusel juhul on testimisi teostanud ainult töö autor, kes on ise ka protseduuride loojaks. Testimised on toimunud ebaregulaarselt ja sõltuvalt sellest, kui palju eksisteerib vaba ajalist ressurssi. Sellest tulenevate probleemide vältimiseks soovitab autor asutuses sisse viia sobilik programm, mille raames saavad testimised toimuda etteantud graafiku alusel. See võimaldab testimisi erinevate stsenaariumite alusel ja teiste töötajate kaasamist lisaks protseduuride loojale. Protseduuride järgi tegutsemine töötajate poolt, kes pole nende väljatöötamises osalenud ja kellel puuduvad konkreetsed teadmised taastatavate süsteemide kohta, võimaldab tagada, et päris intsidendi asetleidmisel on nende sisu arusaadav ka teistele ning nende järgi on võimalik süsteeme edukalt taastada.

Üldisem soovitus on aga organisatsioonis sisse viia kõikehõlmav IT teenuste talitluspidevuse haldus, mis sisaldab ka eelnevalt esitatud soovitusi.

Kokkuvõte

Käesoleva magistritöö peamiseks eesmärgiks oli välja töötada IT teenuste talitluspidevuse tagamise üldskeem, arvestades vastava temaatika rahvusvahelist tava ja praktikat ning organisatsioonide soovitusi, millele tuginedes on töös käsitletaval avaliku sektori organisatsioonil võimalik talitluspidevuse protsessi planeerimisel juhinduda. Töö alameesmärgiks oli organisatsiooni olulisemate IT teenustega seotud süsteemide taasteprotseduuride loomine, valideerimine ja seeläbi taastamise võimalikkuse väljaselgitamine IT katastroofide korral.

Eesmärgi saavutamiseks viidi elektrooniliste teabeallikate põhjal läbi kirjanduse analüüs, kus kasutatud artiklites, õppematerjalides, raamatutes ja veebilehtedel avaldatud teabe näol oli tegemist tunnustatud standardite ning metoodikatega. Alameesmärgi saavutamiseks kasutati uurimuse läbiviimisel juhtumianalüüsi.

Magistritöö olulisemateks tulemusteks olid IT teenuste talitluspidevuse tagamise üldskeemi väljatöötamine ja asutuse peamiste IT teenustega seotud süsteemide taasteprotseduuride loomine, nende valideerimine ja seeläbi organisatsiooni võimekuse suurendamine antud valdkonnas. Magistritöö tulemusena eksisteerivad asutusel toimivad ja praktikas läbiproovitud tegevusjuhendid, mille alusel on kriisiolukorras võimalik süsteemide taastamine alternatiivasukohta. Taasteprotseduuride loomise protsessist tulenevalt esitati soovitused koos põhjendustega asutuse töö paremaks korraldamiseks talitluspidevusega, sh taasteprotseduuridega, seotud valdkonnas.

Eelpool kirjeldatut arvesse võttes leiti, et käesoleva magistritöö eesmärk sai täidetud – välja töötati praktilised juhised IT teenuste talitluspidevuse planeerimiseks ja praktikas toimivad taasteprotseduurid organisatsiooni olulisemate süsteemide taastamiseks.

Kasutatud kirjandus

Allaste, A.-A. (2011). Intervjuude läbiviimine. URL https://www.tlu.ee/files/arts/11383/inter7369fb1e758a3ab0473fd15387051797.ppt. Viimati kasutatud 23.04.2012

Business Continuity Institute. (2007). A Management Guide to Implementing Global Good Practice in Business Continuity Management. Good Practice Guidelines 2008. URL http://www.thebcicertificate.org/pdf/GPG2008-2.pdf. Viimati kasutatud 07.04.2012

Business Continuity Institute. (2011). BCM Statement. Introduction. URL http://www.thebci.org/index.php?option=com_content&view=article&id=62&Itemid=105. Viimati kasutatud 25.10.2011

Business Impact Analysis. (2011). What is a Business Impact Analysis? URL http://www.businessimpactanalysis.org/bia-articles.html. Viimati kasutatud 24.10.2011

Chartered Management Institute. (2008). Business Continuity Management 2008. URL http://www.continuitycentral.com/BCMReport2008.pdf. London. Viimati kasutatud 08.02.2012

Clas, E. (2008). Business Continuity Plans. *Professional Safety*, 53(9).

Dorion, P. (2008). Disaster Recovery Planning in a Virtualized Environment. URL http://searchstorage.techtarget.com/tip/Disaster-recovery-planning-in-a-virtualized-environment. Viimati kasutatud 02.05.2012

EMC. (2011). European Disaster Recovery Survey 2011: Data Today Gone Tomorrow, How Well Companies Are Poised For IT Recovery. URL http://emea.emc.com/microsites/2011/emc-brs-survey/index.htm?pid=press-release-brs-112311. Viimati kasutatud 08.02.2012

ENISA. (2012). IT Continuity Home. URL http://www.enisa.europa.eu/activities/risk-management/current-risk/bcm-resilience. Viimati kasutatud 13.04.2012

Finantsinspektsioon. (2006). Nõuded finantsjärelevalve subjekti talitluspidevuse protsessi korraldamisele. URL http://www.fi.ee/failid/talitluspidevuse_juhend1.pdf. Viimati kasutatud 24.04.2012

Gregory, P. (2008). *IT Disaster Recovery Planning for Dummies*. United States of America: Wiley Publishing, Inc.

Hiie, I. (2009). Infotehnoloogia töökorraldus ja haldamine. Õppematerjal. Viimati kasutatud 03.01.2012

ISACA. (2012). Business Impact Analysis. Tool for BIA. URL http://www.isaca.org/Groups/Professional-English/business-continuity-disaster-recovery-planning/GroupDocuments/Business_Impact_Analysis_blank.doc. Viimati kasutatud 08.03.2012

IT-Director. (2007). Are You Missing Something From Your DR Plan? – itSCM. URL http://www.it-director.com/business/security/content.php?cid=9564. Viimati kasutatud 02.11.2011

ITIL and ITSM World. (2010). Continuity Management. URL http://www.itil-itsm-world.com/itil-8.htm. Viimati kasutatud 02.11.2011

itSMF Estonia. (2010). ITIL v3 terminite, määratluste ja lühendite sõnastik. URL http://www.itsmf.ee/content/images/fbfiles/files/ITIL_V3_Glossary_100313.pdf. Viimati kasutatud 12.04.2012

Jaques, R. (2006). Securing Your IT Continuity. *Financial Director*, 12, 42.

Kaitseministeerium. (2010). Eesti julgeoleku poliitika alused. URL http://mod.gov.ee/files/kmin/nodes/9417_Julgeolekupoliitika_alused_2010.pdf. Viimati kasutatud 09.10.2011

Kongo, P. (2010). Uuring: ettevõtetel puudub äriandmete taasteplaan. URL http://blog.netgroup.ee/uuring-ettevotetel-puudub-ariandmete-taasteplaan/. Viimati kasutatud 04.03.2012

Kuusk, K. (2006). Juhtumiuuring. URL http://www.ngo.ee/arhiiv/www.ngo.ee/orb.aw/class%3Dfile/action%3Dpreview/id%3D11594/Juhtumiuuring.ppt. Viimati kasutatud 22.04.2012

Leibur, G. (2007). IT teenuste talitluspidevuse haldus. Õppematerjal. Viimati kasutatud 08.11.2011

Marquis, H. (2008). How to Win With BIA. URL http://www.itsmsolutions.com/newsletters/DITYvol4iss09.pdf. Viimati kasutatud 23.04.2012

Munipalli, Y. (2005). Measuring The Risk Factor. URL http://www.stickyminds.com/s.asp?F=S9379_ART_2. Viimati kasutatud 03.04.2012

Naaris, K. & Vaidlo, M. (2010). Juhtumianalüüs. Tallinna Ülikool. URL http://www.tlu.ee/files/arts/8070/juhtu38f28320995ca996d970026fd0f3ce1b.docx. Viimati kasutatud 22.04.2012

Normak, P. (2009). Projektijuhtimine. Õppematerjal. Viimati kasutatud 23.03.2012

Office of Government Commerce. (2003). *Service Delivery*. United Kingdom: The Stationary Office.

Office of Government Commerce. (2007). *ITIL version 3 Service Delivery*. United Kingdom: The Stationary Office.

Reiska, R. (2010). ITIL muudatuste halduse protsessi realiseerimisest infohaldussüsteemide abil. Magistritöö. Tallinna Ülikool.

Riigi Infosüsteemi Amet. (2011). Infosüsteemide kolmeastmeline etalonturbe süsteem. ISKE kataloogid. ISKE rakendusjuhendi Lisa 1. Versioon 6.00. URL http://www.ria.ee/public/ISKE/iske_kataloogid_6_00.pdf. Viimati kasutatud 21.04.2012

Riigi Teataja. (2010). Toimepidevuse plaani koostamise juhend. RT I 2010, 33, 180. URL https://www.riigiteataja.ee/akt/13326401. Viimati kasutatud 24.04.2012

Saar, J. (2012). Riskihindamismeetodid. URL http://www.e-uni.ee/e-kursused/eucip/haldus/723_riskihindamismeetodid.html Viimati kasutatud 03.04.2012

Stoneburner, G., Goguen, A. & Feringa, A. (2002). National Institute of Standards and Technology Special Publication 800-30. *Risk Management Guide for Information Technology Systems*. Recommendations of the National Institute of Standards and Technology.

Stranack, T. & Cornish, C. (2009). Business Continuity Management - Bridging The Divide. URL http://www.talkingbusinesscontinuity.com/downloads/pdf/BCM_ID561_WP.pdf. Viimati kasutatud 08.11.2011

Swanson, M., Bowen, P., Philips, A.W., Gallup, D. & Lynes, D. (2010). National Institute of Standards and Technology Special Publication 800-34. *Contingency Planning Guide for Federal Information Systems*.

IT Service Continuity Planning. The Case of a Public Sector Organization

Master's Thesis

Kristjan Pedak

Summary

The main objective of this thesis is to aid a public sector organization in Estonia in planning IT service continuity by developing general guidelines for IT service continuity planning. The sub-goal of the thesis is to develop and validate IT recovery procedures related to the most important IT services within the organization to ensure the recovery capability of the organization during IT catastrophes.

The thesis consists of five chapters. Chapter 1 begins with an introduction giving an overview of the reasons why this topic was chosen, the importance of the topic, the research problem, the objective of the thesis and the research method. Chapter 2 provides an overview of the business continuity management as a necessary background information to the IT service continuity management. It presents a list of business and IT continuity methods, describes the process of business continuity management and gives an overview of the relation between business and IT service continuity management. It is followed by chapter 3, which addresses IT service continuity management more generally. It contains information about objectives, introduces the process lifecycle and gives an overview of its stages including initiation, requirements and strategy, implementation and on going operation. Chapter 4 provides the in depth look of the activities for planning IT service continuity. It lists recommended steps for initiating the project, conducting business impact analysis and risk assessment, producing strategy, developing plans, initial testing and on going operation. Chapter 5 covers the creation and validation of the IT recovery procedures within a public sector organization. It also contains recommendations for future improvements based on the results of the development of the procedures.

The outcome of the master's thesis are the guidelines for planning IT service continuity and IT recovery procedures. The author concludes that the objectives of the thesis were successfully accomplished.

Kasutatud mõisted

Inglise keeles	**Eesti keeles**
Business Continuity Management	Äri talitluspidevuse haldus
IT Disaster Recovery	IT avariitaaste
IT Service Continuity Management	IT teenuste talitluspidevuse haldus
Maximum Tolerable Period of Disruption	Suurim lubatud ajaline katkestus
Recovery Time Objective	Taasteaeg
Recovery Point Objective	Taastekoht
Redundant Array of Independent Disks	Sõltumatute ketaste liiasmassiiv
Single Point of Failure	Üksainus tõrkeallikas

Mõistete seletused

Mõiste	Tähendus
IT avariitaaste	Infotehnoloogias taristu võime taasalustada tööd pärast avariid. Taastumisvõime mõõtmiseks kasutatakse peamiselt kaht hinnangut – taasteaeg ja -koht.
IT teenuste talitluspidevuse haldus	Protsess, mis vastutab IT teenuseid tõsiselt mõjutada võivate riskide haldamise eest.
Suurim lubatud ajaline katkestus	Ajavahemik, peale mille ületamist on IT teenuse katkestusest tingitud mõju suurus organisatsioonile vastuvõetamatu.
Sõltumatute ketaste liiasmassiiv	Mitmest kõvakettast või kõvaketta partitsioonist moodustatud loogiline plokkseade andmete salvestamiseks, kus samad andmed salvestatakse mitmele kõvakettale.
Taasteaeg	Maksimaalne lubatav ajavahemik IT teenuse taastamiseks peale katkestust. Iga teenuse jaoks tuleb RTO läbi rääkida, kokku leppida ja dokumenteerida.
Taastekoht	Maksimaalne andmehulk, mis võib minna kaduma teenuse taastamise käigus. Iga teenuse jaoks tuleb RPO läbi rääkida, kokku leppida ja dokumenteerida.
Äri talitluspidevuse haldus	Äriprotsess, mis tegeleb äritegevusele olulist mõju avaldada võivate riskide haldamisega. Äri talitluspidevuse haldus määrab IT teenuste talitluspidevuse halduse jaoks eesmärgid, käsitlusala ja nõuded.
Üksainus tõrkeallikas	Konfiguratsioonielement, mille tõrge tekitab koheselt intsidendi ja mille puhul vastumeetmeid pole veel rakendatud. Tegemist võib olla isiku, protsessi või tegevuse sammu või IT taristu komponendiga.

LISAD

LISA 1. ÄRIMÕJUDE ANALÜÜSI KÜSIMUSTIKU NÄIDIS

Ärimõjude analüüsi küsimustik

Eesmärk

Ärimõjude analüüsi eesmärk on välja selgitada, millised põhiprotsessid on organisatsiooni püsimajäämise seisukohalt kõige olulisemad. Ärimõjude analüüsi kaudu tuvastatakse, kui kiiresti tuleb taastada kõige olulisemate põhiprotsesside töö õnnetusjuhtumi järgselt. Samuti on ärimõjude analüüsi eesmärk välja selgitada, millised ressursid on vajalikud oluliste põhiprotsesside toimimiseks.

Ärimõjusid hinnatakse halvima stsenaariumi kohaselt, eeldades, et kogu füüsiline taristu, mis on struktuuriüksuste tööks ja põhiprotsesside toimimiseks vajalik, on hävinenud ning kõik dokumendid, seadmed jm ei ole kättesaadavad ja kasutatavad 30 päeva jooksul alates õnnetusjuhtumist.

Ärimõjude analüüsi alameesmärgid on:

- Selgitada välja potentsiaalne kvantitatiivne mõju organisatsioonile iga põhiprotsessi mittetoimimise korral;
- selgitada välja potentsiaalne kvalitatiivne mõju organisatsioonile iga põhiprotsessi mittetoimimise korral;
- tuvastada iga struktuuriüksusega seotud põhiprotsessid.

Poliitika

Ärimõjude analüüsi teostamine on vajalik selleks, et välja selgitada kõikide põhiprotsesside kriitilisus organisatsioonile ja tuvastada mõjud organisatsioonile nende protsesside mittetoimimisel. Oluline on kindlaks teha põhiprotsesside nõutav taasteaeg, suurim lubatud mittetoimimise periood, IT teenuste nõutav taasteaeg ja -koht ning protsesside ja IT teenuste järjekord taastamiseks.

Skoop

Ärimõjude analüüs tuleb läbi viia organisatsiooni kõikides kontorites, mis hõlmab kõiki struktuuriüksusi ja nende poolt teostatavaid protsesse.

Mõõdikud

Järgnevalt on esitatud kahjude mõõdikud, millega määratakse kvantitatiivsetest ja kvalitatiivsetest mõjudest tulenevat kahju suurust organisatsioonile protsessi mittetoimimisel, mis omakorda annab võimaluse tulemuste võrdlemiseks kogu organisatsioonis.

Kvantitatiivsete mõjude hindamise tabel (finantskahjud, regulatiivsed ja õiguslikud kahjud)

Kahju aste	Kahju suurus
0	Kahju puudub
1	< 1000 €
2	1000 - 4999 €
3	5000 - 9999 €
4	10000 - 24999 €
5	25000 - 49999 €
6	50000 - 99999 €
7	100000 - 149999 €
8	150000 - 249999 €
9	250000 - 499999 €
10	> 500000 €

Kvalitatiivsete mõjude hindamise tabel (teenuse osutamise, maine kaotuse, tervishoiu ja ohutusega seotud kahjud)

Kahju aste	Kahju suurus
0	Kahju puudub
2	Väike kahju
4	Keskmisest väiksem kahju
6	Keskmisest suurem kahju
8	Suur kahju
10	Väga suur kahju

Definitsioonid

Mõju kategooria	Definitsioon
Finantskohustused	Kinnisvara kaotus, arvete tasumine, laenud, muud lisakulud
Õiguslikud kohustused	Õiguslikud ja seadusest tulenevad kohustused, trahvid, karistused
Teenuse osutamine	Organisatsiooni tegutsemisvõimekuse vähenemine, juhtkonna kontrolli kadu, isikkoosseisu vähenemine
Maineväärtus	Maine kaotus, usaldusväärsuse kaotus, poliitiline ja meedia poolt häbistamine, kindlustunde vähenemine
Tervishoid ja ohutus	Inimohvrid, turvarisk, terviserisk

Ärimõjude analüüsi küsimustik

Ärimõjude analüüs on protsess, mille kaudu selgitatakse välja teenuste katkestustest tingitud mõju organisatsioonile. Analüüsi abil kogutakse vajalik informatsioon õnnetusjuhtumist tingitud lühi- ja pikaajaliste kvantitatiivsete ning kvalitatiivsete mõjude kohta.

Kogutav informatsioon on vajalik selleks, et luua sobilik talitluspidevuse strateegia. Palun täida käesolev küsimustik võimalikult täpselt, sest Sinu poolt sisestatud informatsioon on aluseks efektiivse talitluspidevuse programmi loomisele.

Struktuuriüksuse nimi: _____

Struktuuriüksuse ülesanne: _____

Struktuuriüksuse juht: _____

Sisesta järgmisse tabelisse kõik põhiprotsessid, mida antud struktuuriüksuses teostatakse ja nende omanikud.

	Põhiprotsess	**Omanik**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

Iga eelnevalt loetletud protsessi kohta täida eraldi ärimõjude analüüsi küsimustik.

Koostaja: _____ Kuupäev: _____

Ärimõjude analüüsi küsimustik

Struktuuriüksuse nimi: _____

Põhiprotsessi nimi: _____

Põhiprotsessi omanik: _____

Protsessi kirjeldus: _____

1. Kas käesolev protsess vajab teostamist mingil kindlal ajahetkel (päev, nädal, kuu, aasta)?

   ☐ Ei ☐ Jah – kirjelda täpsemalt

_____

2. Kasutades alljärgnevas tabelis paiknevaid mõju kategooriaid ja eelnevalt esitatud mõõdikuid, määra põhiprotsessi mittetoimimisest tingitud kahju aste (0–10) organisatsioonile ajas.

	Mõju eskaleerumine ajas									
Mõju kategooria	2h	4h	8h	1p	3p	5p	10p	20p	30p	Kokku
Finantskohustused										
Õiguslikud kohustused										
Teenuse osutamine										
Maineväärtus										
Tervishoid ja ohutus										

3. Kas antud protsess sõltub IT teenustest?

   ☐ Ei ☐ Jah – loetle alljärgnevalt

	IT teenus	**Taasteaeg**	**Taastekoht**
1.			

4. Mis on antud protsessi suurim lubatud mittetoimimise aeg? _____
5. Mis on antud protsessi nõutav taasteaeg? _____

Koostaja: _____ Kuupäev: _____

LISA 2. IT TAASTEPLAANI NÄIDIS

IT taasteplaan

1. Dokumendihaldus

1.1 Dokumendi eesmärk

Käesoleva dokumendi eesmärk on tagada IT taasteplaaniga seotud süsteemide taastamine vastavalt avaliku sektori organisatsioonis kokkulepitud nõuetele.

1.2 Dokumendi levitamine

Koopia	Töötaja ees- ja perekonnanimi	Kuupäev	Ametikoht
1.			

1.3 Dokumendi ülevaatamine

Käesoleva dokumendi ülevaatamine toimub iga 3 kuu tagant.

Käimasolev ülevaatus: ____ . ____ . _____

Järgmine ülevaatus: ____ . ____ . _____

Ülevaatuse kuupäev	Versiooni nr	Kokkuvõte muudatustest

1.4 Dokumendi kinnitamine

Käesoleva dokumendi kinnitamine toimub järgmiste töötajate poolt:

Töötaja ees- ja perekonnanimi	Ametikoht	Allkiri

2. TAUSTAINFORMATSIOON

2.1 Sissejuhatus

Käesolev dokument kirjeldab üksikasjalikud juhised ja protseduurid, mida tuleb järgida, et taastada või jätkata dokumendis kirjeldatud süsteemide töö(d) õnnetusjuhtumi järgselt, tagades teenuse järjepidevuse avaliku sektori organisatsiooni põhipoole nõuetele vastaval tasemel.

2.2 Taastestrateegia

Süsteemide taastamine toimub kasutades järgnevalt loetletud alternatiivsüsteeme:

	Alternatiivsüsteemide loetelu	**Asukoht**
1.		

Käesolevas plaanis kirjeldatud süsteemide taastamine võtab aega ____ tundi.
Käesolevas plaanis kirjeldatud süsteemide lubatud andmekadu ajas (RPO) on ____ tundi.
Käesolevas plaanis kirjeldatud süsteemide nõutud taasteaeg (RTO) on ____ tundi.
Käesolevas plaanis kirjeldatud süsteemide taasteaja ja -protseduuride viimane test toimus ____ . ____ . _____

2.3 Plaani aktiveerimine

Järgnevalt on loetletud töötajad kes on volitatud käesolevat plaani aktiveerima:

	Töötaja ees- ja perekonnanimi
1.	

2.4 Seosed teiste plaanidega

Käesolevas punktis kirjeldatakse seosed teiste avaliku sektori organisatsioonis kasutusel olevate talitluspidevuse ja taasteplaanidega ning nende aktiveerimine.

	Teised talitluspidevuse või taasteplaanid	**Seos**
1.		

2.5 Üldised juhised intsidendi korral

Meediast või muudest allikatest tulenevate informatsiooni päringute korral tuleb tugineda avaliku sektori organisatsiooni kommunikatsiooni protseduurile.

Personali teavitamisel potentsiaalsest või tegelikust õnnetusjuhtumist, tuleb järgida tegevuste eskaleerumise protseduuri. Eriti tuleb tähelepanu pöörata järgmisele:

- Jääda rahulikuks ja vältida pikki telefonikõnesid;
- nõustada töötajaid ootuste ja tegevuste osas (vältida üksikasju, kui vähegi võimalik)
- kui kõnele vastab keegi teine peale kontaktisiku, siis:
    - uurida, kas kontaktisikut on teisiti võimalik kätte saada;
    - kui see ei ole võimalik, siis jätta teade, et kontaktisik võtaks ühendust samal numbril, millelt helistatakse;
    - vältida üksikasjade paljastamist intsidendi kohta;
    - alati märkida üles üksikasjad kõneaja, vastuste ja tegevuste kohta.

Kõikidest tegevustest peab maha jääma selge ja täpne ajalugu. Selle lihtsustamiseks peavad tegevused olema kirjeldatud kontrollnimekirja formaadis, mis võimaldab üles märkida teostaja, tegevuse alguse ja lõpukuupäeva ning kellaaja.

2.6 Seosed teiste süsteemidega

Süsteemide omavahelised sõltuvused tuleb kirjeldada alljärgnevalt olulisuse järjekorras. See on vajalik selleks, et antud taasteplaaniga seotud teised taasteplaanid või -protseduurid on tuvastatud ja neid on vajadusel võimalik kasutusele võtta.

Süsteem	**Viide dokumendile**	**Kontaktisik**

2.7 Organisatsiooni sisemiste ja väliste kontaktide nimekiri

Ees- ja perekonnanimi	**Organisatsioon / roll**	**Ametikoht**	**Kontakteerumisviis**

2.8 Taastemeeskond

Järgnevalt loetletud töötajad vastutavad protseduuride täitmise eest või tagavad protseduuride täitmise ning esinenud probleemide ülesmärkimise. Kontakteerumine toimub tavapärase tegevuste eskaleerumise protseduuri järgi.

Ees- ja perekonnanimi	Ametikoht	Kontakteerumisviis

2.9 Taastemeeskonna kontrollnimekiri

Võtmetegevuste läbiviimise lihtsustamiseks tuleb kasutada järgnevalt esitatud kontrollnimekirja.

Ülesanne	Oodatav tulemus	Tegelik tulemus
Kinnitada plaanide aktiveerimine		
Algatada kutsepuu ja tegevuste eskaleerumise protseduur		
Algatada teiste vajalike taasteplaanide kasutuselevõtt		
Korraldada varundusmeedia ja dokumentatsiooni transport alternatiivasukohta		
Kutsuda kokku taastemeeskonnad		
Algatada taastetegevused		
Tagada tulemuste aruandlus		
Teavitada taastemeeskondi aruandluse nõudest		
Tagada infovahetuse nõue kõikide taastemeeskondadega		
Teavitada juhtkonda taastamisega seotud tegevuste eeldatavast lõpust		

3. TAASTEPROTSEDUURID

Järgnevalt loetleda kõik taastamisega seotud instruktsioonid ja protseduurid või viidata nendele.

LISA 3. FAILISERVERI TAASTEPROTSEDUUR

Failiserveri (FS) taasteprotseduur

Eeldused taastamiseks ja lisainformatsioon

- FSi näol on tegemist virtuaalserveriga, mistõttu toimub taastamine lindilt kasutades selleks .vmdk faili;
- Taastamine eeldab varundusserveri ja NetBackup tarkvara kasutamist ning viimast kõlblikku varundusmeediat.

Taasteprotseduur

- Logi varundusserverisse (VS);
- Ava desktopilt **NetBackup Administration Console**;
- Vali menüüst **File -> Backup, Archive, and Restore**;
- Avanenud aknas vali menüüst **File -> Specify NetBackup Machines and Policy Type…**;
- Uues aknas vali rippmenüüst järgmised väärtused ja vajuta **OK**:
    - Server to use for backups and restores: VS_nimi
    - Source client for restores: FS_nimi
    - Destination client for restores: taaste_esx_serveri_IP
    - Policy type for restores: FlashBackup-Windows
- Järgnevalt vajuta menüüs **Select for Restore** kõrval asuvat allanoolt ja vali rippmenüüst **Restore from Virtual Machine Backup**;
- Avanenud aknas vali **NetBackup History** lahtrist sobiva kuupäevaga backup, tee linnuke **All Folders** lahtris olevasse **FS_nimi.domeeninimi** valikule ja vali menüüst **Actions -> Restore…**;
- Uues aknas tee aktiivseks valik **Recover virtual machine to Alternate location** ja vali **Next**;
- Järgnevalt vali **vCenter Server** rippmenüüst valik **xxx.xxx.x.x**;
- Vajuta **ESX Server** lahtri kõrval olevat **Search…** nuppu ja tee linnuke **taaste_esx_serveri_nimi** valiku juurde ning vajuta **OK**;

- Vajuta **Folder** lahtri kõrval olevat **Browse…** nuppu ja tee linnuke **vm** valiku juurde ning vajuta **OK**;
- Vali **Transfer Type** rippmenüüst valik **nbd**;
- Veendu, et käesolevas aknas on valitud järgmised seaded ja vajuta **Next**:
    - NetBackup Recovery Host: xxxxxxxxx.xxxxx
    - vCenter Server: taaste_esx_serveri_IP
    - ESX Server: taaste_esx_serveri_nimi
    - Datacenter: /ha-datacenter
    - Folder: /(DC)ha-datacenter(DC)/vm
    - Display Name: FS_nimi
    - Resource Pool/vApp: Resources
    - Datastore: datastore1
    - Transfer Type: nbd
- **Storage Destination** aknas vajuta **Next**;
- **Network Connections and other options** aknas vajuta **Next**;
- **Perform Recovery** aknas vajuta **Run Pre-Recovery Check**;
- Veendu, et kontrolli tulemused on märkega **passed** ja vajuta **Start Recovery**;
- Avanenud teavitusaknas vajuta **Yes**, kui soovid taasteprotsessi jälgida;
- Taastamine võtab aega u 30 minutit.
- Sellega on FSi taastamisega seotud tegevused varundusserveris lõppenud.

Taasteprotsessi järgsed tegevused

- Olles **VMware vSphere** klientprogrammiga ESXi serveri peal, tee taastatud FSi peal parem hiireklikk ja vali **Power -> Power On**;
- Tee taastatud virtuaalmasina peal parem hiireklikk ja vali **Open Console**;
- Järgnevalt toimub taastatud virtuaalserveri üleslaadimine ja vajalik seadistamine;
- Peale sisselogimisakna ilmumist avaneb mõne aja pärast **VMware Tools Setup** teavitusaken, mis teavitab restardi vajalikkuse kohta. Taaskäivitamiseks vali **Yes**;
- Peale restarti logi serverisse domeeni administraatori kontoga;
- Ava **Start -> Programs -> Administrative Tools -> Services**;
- Peata järgmised teenused ja muuda nende käivitumise olek **disabled**:
    - Teenus_1

    - Teenus_2
- Sellega on virtuaalse FSi taastamine edukalt lõppenud.

Kettapinna tekitamine FSi failide taastamiseks

- Olles **VMware vSphere** klientprogrammiga ESXi serveri peal, tee taastatud FS peal parem hiireklikk ja vali **Edit Settings...**;
- Avanenud aknas, olles **Hardware** tab'i peal vali **Add...**;
- Tee valik **Hard Disk** aktiivseks ja vali **Next**;
- Tee valik **Create a new virtual disk** ja vali **Next**;
- Määra ketta suuruseks (**Disk Size) xxx GB**, jäta valik lahtisse **Thick Provision Lazy Zeroed** ja **Store with the new virtual machine** ja vali **Next**;
- Jäta **Virtual Device Node** valikusse **SCSI (0:1) Hard Disk 2** ja vali **Next**;
- Veendu, et valitud seaded on korrektsed ja vali **Finish** ja seejärel **OK**.

Kettapinna jagamine loogilisteks ketasteks ja vormindamine

- Logi FSi peale domeeni administraatori kontoga;
- Vali **Start** ja tee **Computer** valiku peal paremklikk ning vali **Manage**;
- Koheselt avaneb aken kettapinna initsialiseerimiseks, jätkamiseks vajuta **OK**;
- Tee **Disk Management** all loodud kettapind **Disk 1 (xxx,xx GB Unallocated)** aktiivseks ja tee sellel hiirega paremklikk ning vali **New Simple Volume...**;
- Avanenud **Welcome to the New Simple Volume Wizard** aknas vali **Next**;
- Määra ketta suuruseks **xxxxxx MB (Simple volume size in MB)** ja vali **Next**;
- Määra esimese loogilise ketta tähiseks **X (Assign the following drive letter)** ja vali **Next**;
- Määra **Volume label** lahtis esimese ketta nimeks **Xx**, vali **Next** ja seejärel **Finish**;
- Järgnevalt tee **Disk Management** all loodud kettapind **Disk 1 (yyy,yy GB Unallocated)** taas aktiivseks ja tee sellel hiirega paremklikk ning vali **New Simple Volume...**;
- Avanenud **Welcome to the New Simple Volume Wizard** aknas vali **Next**;

- Ketta suuruseks jäta kogu pakutud ruum **xxxxxx MB (Simple volume size in MB)** ja vali **Next**;
- Määra teise loogilise ketta tähiseks **Y (Assign the following drive letter)** ja vali **Next**;
- Määra **Volume label** lahtis teise ketta nimeks **Yyyyy**, vali **Next** ja seejärel **Finish**;
- Sulge **Server Management** aken;

Failide taastamine loogilistele ketastele

- Logi varundusserverisse (VS);
- Ava desktopilt **NetBackup Administration Console**;
- Vali menüüst **File -> Backup, Archive, and Restore**;
- Avanenud aknas vali menüüst **File -> Specify NetBackup Machines and Policy Type…**;
- Uues aknas vali rippmenüüst järgmised väärtused ja vajuta **OK**:
    - Server to use for backups and restores: VS_nimi
    - Source client for restores: FS_nimi
    - Destination client for restores: FS_nimi
    - Policy type for restores: MS-Windows
- Järgnevalt vajuta menüüs **Select for Restore** kõrval asuvat allanoolt ja vali rippmenüüst **Restore from Normal Backup**;
- Avanenud aknas vali **NetBackup History** lahtrist sobiva kuupäevaga backup, tee linnuke **All Folders** lahtris olevasse **FS_nimi** valikus olevatele taastamist vajavatele ketastele **(X ja Y)** linnuke ja vali menüüst **Actions -> Restore…**;
- Uues aknas jäta aktiivseks valik **Restore everything to its original location** ja vali **Start Restore**;
- Avanenud teavitusaknas vajuta **Yes**, kui soovid taasteprotsessi jälgida;
- Taastamine võtab aega u 3 tundi.
- Sellega on FSi taastamisega seotud tegevused varundusserveris (VS) lõppenud;

Sellega seoses on ka muud vajalikud taasteprotseduurid FSi peal lõppenud.