Sisekaitseakadeemia

Sisejulgeoleku Instituut

Maarja Vesi

INFO- JA KOMMUNIKATSIOONITEHNOLOOGIA KATKESTUSE MÕJU HINDAMISE METOODIKA POLITSEI- JA PIIRIVALVEAMETI NÄITEL

Magistritöö

Juhendaja:
Raul Savimaa, PhD

Tallinn 2011

ANNOTATSIOON

Sisejulgeoleku instituut	Kuu ja aasta: Mai 2011
Töö pealkiri: Info- ja kommunikatsioonitehnoloogia katkestuse mõju hindamise metoodika Politsei- ja Piirivalveameti näitel	
Töö autor: Maarja Vesi	Olen nõus oma lõputöö kättesaadavaks tegemisega elektroonilises keskkonnas. Allkiri:
Lühikokkuvõte: Magistritöö eesmärgiks on luua metoodika IKT katkestusest tekkiva mõju hindamiseks asutuse põhitegevusele Politsei-ja Piirivalveameti näitel. Töö eesmärgi saavutamiseks on püstitatud järgmised uurimisülesanded: analüüsida IKT valdkonna katkestuse mõõtmise põhimõtteid; määratleda mõjurid IKT katkestuse hindamiseks; töötada välja IKT katkestuse hindamise metoodika Politsei- ja Piirivalveameti jaoks. Töö koosneb kahest peatükist. Esimene peatükk on teoreetiline osa, mis keskendub esimese uurimisülesande lahendamisele. Teine peatükk on empiiriline osa, kus kajastatakse juhtumiuuringu (*case study*) tulemusi ning selle alusel saadavaid mõjureid IKT katkestuse mudeli väljatöötamiseks. Intervjueeritavate ja PPA ekspertide hinnangul sai selliseid mõjureid kokku üheksa, mis mõjutavad põhitegevust. Autor jagas need kaheks: rahalised ja mitterahalised mõjurid ning viimaseid kasutatakse taustainformatsioonina kokkuvõtete tegemisel. Metoodika koosneb kahest osast, mitterahalised mõjurid IKT katkestuse hindamiseks ning mudel katkestusest tekkinud kulutuste arvutuseks. Töös välja pakutud mudelis on kajastatud IKT katkestusest tingitud otsesed kulud ning kaudsed kulud, mis on tingitud tööde kuhjumisest, kuna infosüsteemi kasutaja(te)l ei ole võimalik selleks ettenähtud ajal tööd teha. See on produktiivsuse kaotusega seotud kulu ning seda tuleb mudelis arvestada, kuid kulu ülehindamise riski maandamiseks korrigeeritakse seda ärikriitilisuse koefitsiendiga. Autori hinnangul on mudel PPA-s lihtsalt rakendatav eeltäidetud Exceli tabelit kasutades. Metoodikat tervikuna rakendades (koos mitterahaliste mõjuritega) saab kasutada ülevaadete või kokkuvõtete tegemisel ning see oleks abimaterjalina kasutatav eelarve planeerimisel ja läbirääkimistel SMITiga ning juhtkonnale ülevaadete tegemisel. Väljatöötatud metoodika on rakendatav ka teistes Siseministeeriumi valitsemisala asutustes ning vajadusel oleks võimalik kasutada kõigis avaliku sektori asutustes.	
Võtmesõnad: IKT, IT, IKT katkestus, seisva süsteemi kulud, ITIL, COBIT, teenustaseme kokkulepe, intsidendihaldus, riskihaldus, toimepidevus, avalik sektor, tasakaalus tulemuskaart, mõõdik	
Võõrkeelsed võtmesõnad: ICT, IT, ICT interruptions, downtime costs, ITIL, COBIT, service level agreement, incident management, risk management, continuity, public sector organizations, balanced scorecard, metric	
Säilitamise koht: Sisekaitseakadeemia raamatukogu	
Kaitsmisele lubatud Sisejulgeoleku instituudi juhataja	Allkiri:
Vastab lõputöö nõuetele Juhendaja:	Allkiri:

SISUKORD

MÕISTETE JA LÜHENDITE LOETELU

COBIT - IT haldamise parim praktika (*Control Objectives for Information and Related Technology)*

ISO - Rahvusvahelise Standardi Organisatsioon

HOS - Hädaolukorra seadus

IKT - info- ja kommunikatsioonitehnoloogia

IT - infotehnoloogia

ITIL - IT haldamise parim praktika (*Information Technology Infrastructure Library)*

PPA - Politsei- ja Piirivalveamet

RIK - Registrite ja Infosüsteemide Keskus

SLA - teenustaseme kokkulepe (*service level agreement*)

SMIT - Siseministeeriumi infotehnoloogia- ja arenduskeskus

SISSEJUHATUS

Info- ja kommunikatsioonitehnoloogia (edaspidi IKT) on käesoleval ajal Eestis kasutusel kõigis asutustes ning sisuprotsessid on seotud tehnoloogia arenguga. Inimesed on muutunud järjest mugavamaks ning harjunud, et paljud asjad saab kodus ära teha laua tagant tõusmata. Eestis saavad inimesed oma tulud deklareeritud, e-hääletatud ning maksed tehtud arvuti taga ning võivad asjaajamisest järelejäänud aja endale meelepärastele tegevustele kulutada. Seda enam ollakse üllatunud, kui mõni päev on arvuti- või sidesüsteemis tõrge ja ei saa oma harjumuspäraseid tegevusi teha ning ollakse sunnitud seetõttu ametiasutusse kohale minema või ootama, kuni viga saab parandatud.

Eelmise aasta lõpus oli Eestis kaks suurt üleriigilist sideteenuse katkestust. 17.11.2010 toimus katkestus Elion Ettevõtted AS võrgus ning 01.12.2010 kogeti terve päeva kestnud tõsiseid häireid AS EMT mobiilsides. Need kaks lähestikust katkestust näitasid, kui harjunud ollakse oma tänase eluga ning haavatavad, kui mõni harjumuspärane teenus ei tööta. Samas IKT ei ole asi iseenesest, vaid see toetab vajalikke tööprotsesse, et saaks tööd tõhusamalt ja efektiivsemalt korraldada. Seega peab sisuline protsess paigas olema ja alles seejärel saab IKT-d rakendada töökorralduse paremaks muutmiseks.

IKT valdkonnaga seotud kulutuste pidev kasv, IKT osatähtsuse kiire suurenemine kogu ettevõtte funktsioneerimises ja rahulolematus infosüsteemide mõjuga ettevõtte äriprotsessidele on viinud üha kasvava vajaduseni leida mõõtmissüsteem, mis võimaldaks IKT valdkonna tegevust mõõta ja hinnata järgmistest aspektidest: kas ja kui palju on mõistlik IKT-sse investeerida, kuidas hinnata investeeringu tasuvust ning mismoodi mõõta katkestuse mõju põhitegevusele, kui süsteem ei tööta. IKT valdkonna mõõtmissüsteemi loomisel on rohkem uuritud IKT investeeringute tasuvust nii rahvusvahelisel tasemel kui ka Eestis. Katkestuse mõju põhitegevusele laiemalt uuritud ei ole. Katkestuse mõju

äriprotsessile hindavad eraettevõtted üldjuhul tekkinud kuluna või kahjuna, kui tulu jääb saamata.

Avalik sektor (sh Politsei- ja Piirivalveamet) täidab ühiskonna tellimust ja pakub avalikku hüve ning seega on keeruline hinnata rahaliselt tekkinud kahju avaliku teenuse pakkumisel, kui mõni infosüsteem ei tööta. Samas oodatakse avaliku sektori asutustelt kulude läbipaistvust ning järjest enam ka efektiivsust tööprotsesside korraldamisel. Magistritöö autori hinnangul tuleb hakata avaliku sektori asutustel hindama kulusid, mis takistavad neil avalikku teenust pakkumast, et läbi selle muutuks teadlikumaks ja lihtsamaks eelarve planeerimine ning juhtimisotsuste tegemine.

IKT katkestustest tekkiva kulu hindamine on muutunud Siseministeeriumi valitsemisalas aktuaalseks, kuna asutuste IKT tegevused on konsolideeritud ning teenust pakub Siseministeeriumi infotehnoloogia- ja arenduskeskus (edaspidi SMIT). See on viinud Siseministeeriumi haldusalas kogu IKT valdkonna käsitlemise teenusepõhisele lähenemisele, mis annab selgema aluse nii teenuse kvaliteedi hindamisele kui ka katkestuste mõju arvessevõtmise rakendamisele. Varasemalt, kui IT süsteeme haldas asutuse enda infotehnoloogia (edaspidi IT) osakond, ei rakendatud valdkonnas teenuse kontseptsiooni ning asutuse struktuuriüksuste toimimise efektiivsust ja tulemuslikkust ei mõõdetud.

Magistritöö eesmärgiks on luua metoodika IKT katkestusest tekkiva mõju hindamiseks asutuse põhitegevusele Politsei-ja Piirivalveameti näitel.

Töös kasutatakse katkestuse mõistet ainult IKT katkestuse kontekstis, kus sisuteenuse tagamiseks vajalikus infosüsteemis on katkestus ning kasutajad ei saa teenust kasutada. Ajalist piirangut ei ole katkestusele seatud, va kui tekstis ei ole teistmoodi öeldud. Autor peab vajalikuks täiendavalt märkida, et töös uuritakse IKT katkestuste mõju tervikuna, mitte ainult IT seisukohast ning mõisteid IT ja IKT kasutatakse sünonüümidena.

Töö eesmärgi saavutamiseks on püstitatud järgmised uurimisülesanded:

- analüüsida IKT valdkonna katkestuse mõõtmise põhimõtteid;

- määratleda mõjurid IKT katkestuse hindamiseks;
- töötada välja IKT katkestuste mõju hindamise metoodika Politsei- ja Piirivalveameti näitel.

Töö koosneb kahest peatükist. Esimene peatükk on teoreetiline osa, mis keskendub esimese uurimisülesande lahendamisele. Töö fookus on IKT katkestuse mõõtmisel, paraku ei ole antud valdkonnas laialdast ja üheselt aktsepteeritud teoreetilist baasi. Seetõttu pidas autor vajalikuks analüüsida teoreetilises osas elemente, mis kombineerituna võimaldaksid parimal viisil uurimisülesannet täita. Peatükis vaadeldakse esmalt IKT valdkonna tulemuslikkuse mõõtmise aluseid ja sellega seotud finantsnäitajaid, seejärel käsitletakse IT parima praktika raamistikku katkestuse mõõtmiseks ning, arvestades Politsei- ja Piirivalveameti (edaspidi PPA) tegevusvaldkonda ja ülesandeid, uuritakse ka elutähtsa teenuse toimepidevuse tagamiseks tehtava riskianalüüsi metoodika põhimõtteid. Selline kombinatsioon on vajalik, et terviklikult katta IKT katkestuse mõõtmise erinevaid aspekte politseiorganisatsioonis ning leida kasutatud teoreetilistest lähtekohtadest sobiv sisend väljatöötatavasse metoodikasse.

Teine peatükk on empiiriline osa, kus kajastatakse juhtumiuuringu (*case study*) tulemusi ning selle alusel saadavaid mõjureid IKT katkestuse mudeli väljatöötamiseks. Juhtumiuuring oli vajalik teooria kinnitamiseks ning täpsustamiseks konkreetses keskkonnas ja praktikas. Peatükis tutvustatakse ka PPA IKT valdkonna toimimise põhimõtteid ning autor pakub välja IKT katkestuse mõju hindamise metoodika nimetatud organisatsiooni näitel. Teine peatükk kirjeldab teise ja kolmanda uurimisülesande lahendamist. Töös on kasutatud ka Estonian Business Schoolist Marlen Tamme (2006) magistritöö „Infotehnoloogia valdkonna tulemuslikkuse mõõtmine“ ja Tallinna Tehnikaülikoolist Evelin Kasenõmme magistritöö „IT teenuste haldamise parimad praktikad (ITIL): raamistik avaliku halduse reformide kontekstis ja rakendamine Siseministeeriumi haldusalas“ tulemusi.

Magistritöö raames väljatöötatava metoodika alusel saab hinnata katkestusest tingitud kahju põhitegevusele ning see oleks aluseks investeeringuvajaduste hindamisel ja põhjendamisel eelarve koostamisel.

1.TEOREETILINE RAAMISTIK IKT KATKESTUSE MÕÕTMISEKS

1.1. IKT valdkonna tulemuslikkuse mõõtmine

Juhid teavad, et kaks kõige olulisemat ressurssi, mida tuleb juhtida, on inimesed ja raha. Viimastel aegadel on järeldusele jõutud, et organisatsiooni[1] edukuse seisukohalt mängib kriitilist rolli informatsioon, sellega omakorda on lähedalt seotud infotehnoloogilised kulud. Peaaegu kõik kaasaegsete organisatsioonide tegevused sõltuvad pidevalt keerukamateks ja integreeritumateks muutuvatest IKT lahendustest. Varem peeti IKT-d üksnes organisatsiooni eesmärkide saavutamise tõhusaks vahendiks, samas vaadeldi organisatsiooni eesmärke eraldi olemasolevast tehnoloogiast. Tänapäeval ei ole IKT enam omaette nähtus ning see on tihedalt seotud organisatsiooni eesmärkide ja toimimisega ning kui lakkab töötamast mõni infosüsteem, avaldab see mõju ka asutuse poolt pakutavatele teenustele. Seega peab magistritöö autor vajalikuks IKT katkestuse mõju hindamise metoodika välja töötamiseks uurida organisatsiooni eesmärkide seost IT eesmärkidega ning nendega seotud olulisi mõõdikuid. Väljapakutava metoodika üheks osaks on organisatsioonile tekkinud kulutuste hindamine ning seega huvitab autorit, milliseid kulutusi mudelis kajastada.

Uuringuasutus Harvardi Poliitika Grupp on jõudnud järeldusele, et viimastele aastatel on IKT vallutanud avaliku sektori sellises ulatuses, et sellega tuleb arvestada strateegilise otsustuse protsessis. Seega pole küsimus enam selles, et kas juhid peaksid või ei peaks osalema IKT-ga seotud tähtsate strateegiliste otsuste tegemise protsessis. Küsimus on pigem selles, kuidas nad peaksid seal osalema. (Vintar 2003: 349)

[1] Magistritöös kasutatakse organisatsioon, ettevõtte ja asutus sünonüümidena.

Valk (2003, 15-17) väidab, et avaliku sektor organisatsioonid on loodud riigi ja valitsuse erinevate eesmärkide ja ülesannete täitmiseks. Avaliku organisatsiooni tegevust iseloomustab suurem ettevaatus ja väiksem innovatiivsus, samuti on seal enam bürokraatiat ja formaalsust kui erasektori ettevõtetes.

Eeltingimused organisatsiooni tegevuses eduka tulemuse saavutamiseks on järgnevad:

- organisatsioonil peavad olema strateegilised eesmärgid;
- eesmärgid peavad olema selgelt sõnastatud ja defineeritud;
- eesmärke peab olema vähe ning kergesti juhitavad;
- peab olema üleüldine arusaam organisatsioonis nende vajalikkusest;
- eesmärgid peavad olema mõõdetavad (Waheed, Mansor & Ismail 2010).

Eelpool nimetatud loetelu on eesmärgi põhine ning see keskendub pigem tulemusele kui tegevusele, antud käsitluse kasutamine on raskendatud avaliku sektori puhul, kes alati eesmärke ei sätesta ning pigem keskendub protsessile.

Tulemuslikkuse mõõtmine avalikus sektoris on keeruline ning samuti vähem uuritud valdkond võrreldes erasektoriga, mille põhjused on järgnevad: avalikus sektoris ei ole eesmärgid selgelt defineeritud ning esineb nende paljusus; nad on keskselt juhitavad; neil ei ole üldtunnustatud tulemuse indikaatoreid; nende vastutusala on hajutatud ja killustatud vastastikuse sõltuvuse tõttu (Waheed et al 2010).

Avaliku sektori asutuste tulemuslikkuse mõõtmine on olnud komplitseeritud õigete mõõdikute valimise ja suurema avaliku huvi puudumise tõttu. Samas on viimastel aastakümnetel sellega aktiivselt tegeletud. Näiteks töötati 2000. aastal Suurbritannias välja *best value* kontseptsioon kohalike omavalitsuste moderniseerimiseks. Selle eesmärk oli suurendada teenuse kvaliteeti ja kontrollida kulusid avaliku sektori organisatsioonides (McAdam & Maguire 2004). Tänaseks iseseisval kujul enam *best value* mõistet ei kasutata, kuid need põhimõtted on endiselt kaetud Suurbritannias avaliku sektori kohta tehtavates iga-aastastes ülevaadetes. Tulemuslikkust saab mõõta ka tasakaalus tulemuskaardi abil, mida käsitletakse edaspidi.

Eduka tulemuse saamiseks ainult planeerimisest ja organiseerimisest ei piisa, peab olema ka kontrollsüsteem tulemuste mõõtmiseks. Juhtimise kontrollsüsteemide ülesehitust ja vajalikkust kirjeldavad teooriad tekkisid juba 20. sajandi esimesel poolel. Umbes samast ajast on pärit ka terminid nagu mõõdik ja tulemusnäitaja, mis algselt olid kasutusel peamiselt finantsaruannetes (Buytendjik ja Geishecker 2004). Juhtimise infosüsteeme hakati tutvustama 1970-ndatel aastatel ja tasakaalus tulemuskaardi teooria pärineb aastast 1992. Tulemuste mõõtmist ja mõõtmissüsteemide juurutamist on eriti aktiivselt hakatud kasutama just viimastel aastakümnetel, kuna konkurents on muutunud tihedaks ning organisatsiooni püsimiseks on oluline sätestada õiged eesmärgid ning hinnata nende eesmärkide saavutamist ja vajadusel teha ka korrektuure parima tulemuse saavutamiseks.

Varem peeti IT-d üksnes organisatsiooni eesmärkide saavutamise tõhusaks vahendiks, samal ajal vaadeldi organisatsiooni eesmärke eraldi olemasolevast tehnoloogiast. IT ei toonud kaasa mingeid olulisi muutusi organisatsiooni struktuuris, töömeetodites või tegevusprotsessides. Kuna IT nõudis sügavamat tehnoloogia mõistmist, siis leiti, et see peaks jääma inseneride ning arvutispetsialistide pärusmaaks. Seega võeti varem IT-d kui paratamatut kuluartiklit ning juhtkond ei vaidlustanud nimetatud valdkonna kulutuste suurust. (Vintar 2003: 339)

Tänapäevases turbulentses keskkonnas on peamine põhjus kahtlemaks IT investeeringute väärtuses asjaolu, et väga raske on hinnata pikaajalisemat saadavat kasu ning investeeringute tasuvust. Saadavat tulu tahetakse panna ROI-vääringusse (Drysdale, Bonanni & Shuttlewood 2010), et võrrelda seda teiste konkureerivate investeeringutega, kuid see ei anna vajalikku infot otsuse tegemiseks.

Marlen Tamm on oma magistritöös „Infotehnoloogia valdkonna tulemuslikkuse mõõtmine“ (2006) defineerinud tulemuslikkuse mõõtmise - see on protsess, mis võimaldab analüüsida ettevõtte eesmärkide täitmist ehk tulemuslikkust ja selle saavutamiseks vajalikke tegevusi, kasutades erinevaid finants- ja mittefinantsmõõdikuid.

IT tulemuslikkuse hindamise mõõtmissüsteemi ülesehitamisel tuleks aru saada, mida IT valdkonnalt tegelikult oodatakse. Sageli võib erineva taseme juhtidel olla IT rollist erinev nägemus. Tamm (2006: 28) soovitab enne IT mõõtmissüsteemi loomist selgusele ja üksmeelele jõuda järgmistes küsimustes:

- Kui suur on IT osatähtsus ettevõtte eesmärkide saavutamisel?

Näiteks: kas IT aitab suurendada ettevõtte konkurentsieeliseid, kas IT toetab ettevõtte missiooni täitmist, kas IT suurendab töötajate kompetentsust?

- Milline on IT osalus äriprotsessides?

Näiteks: kas IT on aktiivne või passiivne osaleja äriprotsessides, kas IT toetab või takistab äriliste eesmärkide saavutamist?

- Kuidas mõjutab IT ettevõtte tulemuslikkust?

Näiteks: kas IT on aidanud kulusid vähendada, kas IT on aidanud tulusid suurendada, kas IT on aidanud tõsta klientide rahulolu?

Kui on selge, mida IT valdkonnalt oodatakse, siis on vaja IT tulemuslikkuse mõõtmiseks leida õiged finants- ja mittefinantsmõõdikud. Tihti kasutatakse tulemuslikkuse mõõtmiseks just finantsnäitajaid, kuna ettevõtetes on endiselt kesksel kohal kvartali ja aasta finantsaruanded, kuid finantsnäitajad annavad ülevaate vaid möödunud aja sündmustest ning ei võimalda hinnata immateriaalset ja intellektuaalset vara. Neid asjaolusid püüdsid Kaplan ja Norton arvestada tasakaalus tulemuskaardi (*balanced scorecard*) loomisel, mida tutvustati esmakordselt 1992.aastal ajakirjas *Harvard Business Review*.

Tasakaalus tulemuskaart täiendab eelnevat tegevust kajastavaid rahalisi indikaatoreid näitajatega, mis mõõdavad tulevase edu saavutamiseks vajalikke tegureid. Tasakaalus tulemuskaardi eesmärgid ja näitajad lähtuvad organisatsiooni tulevikupildist (visioonist) ja strateegiast. Süsteem mõõdab ettevõtte tulemuslikkust neljast aspektist: finantsid, kliendid, äriprotsessid ning õppimine ja areng. (Kaplan ja Norton 2003: 9)

Tasakaalus tulemuskaart on rakendatav ka avaliku sektori asutustes mõningate kohandustega. Reeglina on rahaline perspektiiv oluline äriettevõtetel, kuid avaliku sektori asutuste kohta see ei kehti. Grasseova (2010) toob välja, et avaliku sektori asutused peavad

maksimaliseerima konkreetset hüve etteantud eelarve ulatuses ning seega esmane peaks olema sätestada missioon, kuna see väljendab asutuse eksisteerimise eesmärki.

IT tulemuslikkuse mõõtmisel saab kasutada tasakaalustatud tulemuskaarti, kuid selleks peab ettevõte määrama IT sektori eesmärgid ja kriitilised edufaktorid ning leidma nende faktorite vahelised põhjus-tagajärg ahelad.

Epstein ja Rejc (2005) on kohandanud Kaplani ja Nortoni väljatöötatud tulemuskaarti IT tulemuslikkuse mõõtmiseks ning toonud välja faktorite vahelised põhjus-tagajärg ahelad. Nende hinnangul sõltub organisatsiooni edukus IT kasvu ja arenguga seotud elementidest: näiteks vajalik ressurss (kapital ja inimesed), organisatsioonis üldiselt kasutusel olevad süsteemid ja protsessid (koolitus, informatsioon, kasutatavad tulemuslikkuse mõõtmissüsteemid, organisatsiooni kultuur ja kliima). IT kasvu ja arenguga seotud elemendid mõjutavad IT sisemisi protsesse, näiteks standardiseerimine, konsolideerimine, turvalisus ja üleüldine IT-protsesside, toodete ja teenuste kvaliteet. Nii arengu- ja kasvuga seotud tegurid kui ka sisemised protsessid mõjutavad klientide rahulolu. Kuna IT tegevus puudutab nii sise- kui ka väliskliente, siis jagasid Epstein ja Rejc tasakaalustatud tulemuskaardi kliendiperspektiivi vaate kaheks. Sisekliendi rahulolu peegeldub tema suurenenud produktiivsuses, loovuses ja töö kvaliteedi tõusus. Vastukaaluks väliskliendi rahulolu väljendub suuremas lojaalsuses, uute klientide saamises või suuremas müüginumbris. Finantsilisest vaatenurgast viivad mõlemad kliendisegmendid tulude kasvule või kulude vähenemisele.

Tasakaalus tulemuskaardi väljatöötamisest kasu saamiseks tuleb eesmärgid siduda mõõdikutega. Pole olemas täpset reeglit, kui palju mõõdikuid peaks olema, kuid oluline on organisatsiooni jaoks välja selgitada võtmemõõdikud. Epstein ja Rejc (2005) rõhutavad, et mõõta võib kõike, kuid juhtimisotsuste tegemiseks pole kõik mõõdikud vajalikud.

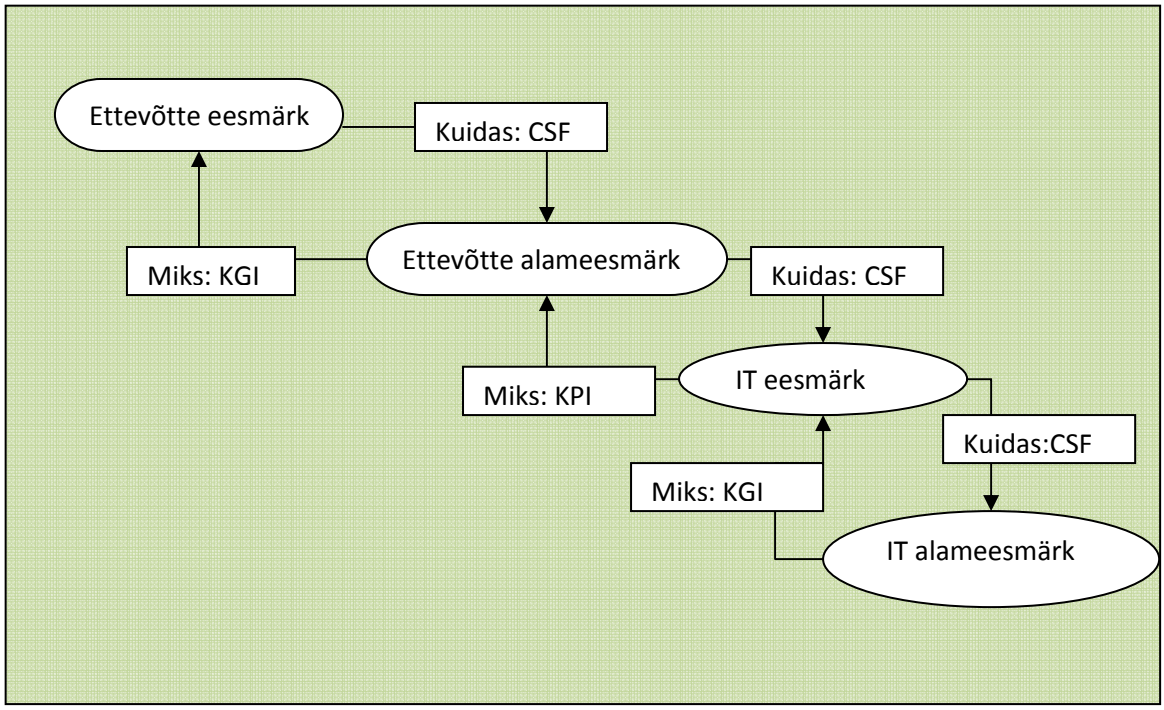
IT valdkonna tulemuslikkuse mõõtmise aluseks on õigete mõõdikute valik. IT eesmärke ei saa vaadelda eraldi organisatsiooni omadest, vaid need on osa sellest.

Eesmärkide täitmist aitavad mõõta õiged mõõdikud ning magistritöö autori hinnangul on maailmas levinumatest olulisemad kolm järgmist:

- **CSF** (*critical success factor*)- faktor, mis töötati välja 1960ndatel ning Rockart ja Bullen sõnastasid selle definitsiooni: võtmeala, kus asjad peavad minema õigesti, et saavutada edukalt sätestatud eesmärgid (Tan, Cater-Steel, Toleman 2009). Smith (2008:29) nimetab näitajat kriitiliseks edufaktoriks, mis reguleerib olulisi tegevusi, mida on vaja saavutada, kontrollida ja juhtida, et saavutada ettevõtte eesmärke.
- **KPI** (*key performance indicator*)- võtmemõõdik, mis on oluline eesmärkide ja tulemuste mõõtmiseks ja hindamiseks (Smith 2008:29).
- **KGI** (*key goal indicator*)- näitaja, mis kinnitab eesmärgi saavutamist (Smith 2008:29).

IT strateegia on sellest, kuidas IT aitab ettevõttel võita. IT strateegia on ühtne tervik äri-strateegiga ning loogiliselt sellega seotud. On olemas neli põhidokumenti, mis on IT strateegia tuumaks: valdkonna ülevaade, 20-leheküljeline strateegia dokument, IT strateegia plaan ja IT tegevusplaan. Eduka dokumendi koostamise võti on läbi mõelda, miks kirjutada IT strateegiat ning seejärel jälgida, et see läheks kokku ettevõtte üldiste eesmärkidega. (IT Strategy…12.03.2011)

IKT toetab ettevõtte strateegiat, mitte ei määra seda. Allpool toodud Joonis 1 näitlikustab ettevõtte eesmärkide seost IT eesmärkidega ning kuidas mõõdetavate alameesmärkide kaudu on võimalik eesmärkide saavutamist kontrollida.



Joonis 1. Seosed eesmärgi ja alameesmärgi vahel
(allikas: Smith 2008: 17)

Eelpool kirjeldati, kuidas IT tulemuslikkust mõõta ning mismoodi seda ettevõtte eesmärkide ja finantsnäitajatega siduda. Finantsnäitajatest on veel kasutatavad investeeringu tasuvus ROI (*return on investment)* ja omamiskulu TCO *(total cost of ownership).*

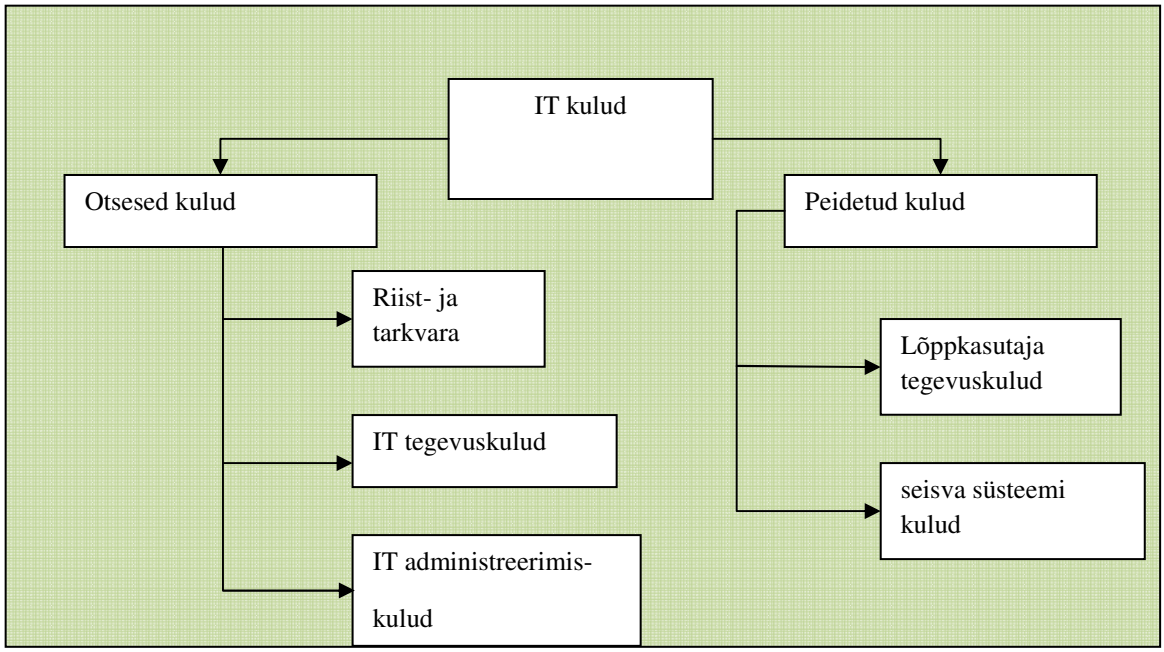
TCO analüüs loodi, et hinnata IT süsteemi elutsükli kulusid, mis on seotud omandamise, kasutamise ja muutmisega ning kulude jaotuse aluseks on infosüsteemiga seotud otsesed ja kaudsed (ka peidetud) kulud (Ciuhureanu 2009). TCO mudel on keskendunud eelkõige kulupositsioonile ning kuidas IT kulusid paremini mõõta, juhtida ja vähendada, tõstmaks IT investeeringute tulusust. Infosüsteemide omamiskulu näitab organisatsiooni poolt infotehnoloogiale tehtavate kulutuste olemust ja struktuuri. Omades selget ülevaadet, kui palju organisatsioon kulutab infosüsteemide loomisele, kui palju kulutatakse selle igapäevasele käigushoidmisele ning kui palju kasutajate koolitusele, on võimalik kujundada tuleviku jaoks õige investeerimis- ja tegevusplaan. Ciuhureanu (2009) rõhutab, et äärmiselt oluline on õigete juhtimisotsuste tegemiseks välja tuua kaudsed kulud, kuna need võivad ulatuda kuni 60% TCO kogukulust.

ROI on lihtne näitaja, mida ettevõtted kasutatavad kaalumaks või hindamaks kapitali tehtavaid kulutusi, eriti siis, kui see võiks vähendada tuleviku kulutusi. Näitaja on oodatav rahaline juurdekasv investeeringult, mis võib sisaldada uut hüve või olemasolevate kulude vähenemist. (Drysdale et al 2010)

ROI arvutamise eelduseks on võimalikult täpne ülevaade kuludest ja tuludest. Selleks väljendatakse need näitajad (st kulud ja tulud) rahas, mitte ajas vms. Samas on Kramer (2005) öelnud, et kui ROI oleks ainus IT mõõdik, jääksid paljud IT projektid tegemata.

IT-sse investeerimine tähendas varem peamiselt tegevuse ratsionaliseerimist ja kulude kärpimist. Tänapäeval on rõhuasetus kaldunud pigem tulude suurendamise poole. Investeeringud IT-sse peavad kiirendama otsuste tegemist, tõstma teeninduse kvaliteeti ja teenuste/toodete arendustempot. Et saada IT investeeringutelt häid tulemusi, on vaja selget teadmist, kus ollakse täna ja kuhu soovitakse jõuda homme. Vajalik on selgete strateegiate olemasolu, eesmärkide püstitus ning tegevusplaanide koostamine. IT investeeringute juhtimisvastutus on ettevõtte juhtkonnal, kes vastutab firma stabiilse arengu, kasvu ja otstarbekate kulutuste eest. (Praust, Kumar, Leis ja Kivimaa 1999: 8)

IKT uuringufirma Gartner Group, toetudes TCO mudelile, jagab IT kulud kahte gruppi: otsesed kulud ja peidetud kulud (Praust jt 1999: 8). Joonisel 2 on toodud kulude jaotus skemaatiliselt.



Joonis 2. IT kulude jaotus (allikas Praust jt: 1999, 8.2)

Otsesteks kuludeks on riist- ja tarkvarakulud (soetus- ja liisingkulud, amortisatsioonikulud), IT tegevuskulud (nt tehnilised teenused, *helpdeski* kulud) ja IT administreerimiskulud (nt IT spetsialistide ja lõppkasutajate koolitus, finants- ja haldusteenused IT infrastruktuuridele).

Peidetud kulud ei ole tavaliselt raamatupidamislikult fikseeritud ja eelarvestatud ning neid on raske määratleta ja mõõta. Peidetud kulude alla kuuluvad eelkõige lõppkasutajaga seotud tegevuskulud ja orienteeruvad kulud seoses arvutisüsteemide tõrgete ja ajalise seiskumisega. (Ciuhureanu 2009)

Praust jt (1999: 8.2) toovad välja lõppkasutaja tegevuskulude alla järgmised orienteeruvad/planeeritavad kulutused: kolleegide abistamine IT kasutamisel, juhuslikud IT-alased õpped, andmefailide haldamine, ajakulu seoses ebaotstarbeka tegevusega (nt arvutimängud, surfamine veebis), omaalgatuslike ja mittevajalike programmiosade või kasutajaliideste loomine. Antud kulutusi on võimalik mõõta kasutajate intervjuude, üleettevõtteliste küsitluste ja koolitusjuhi aruannete abil.

Seisva süsteemi kulud on kaotatud produktiivsusega seotud kulutused, mis on põhjustatud arvutivõrgu, töökohaarvuti, serverite, printerite jms riketest. Siia alla kuuluvad ka olukorrad, kus lõppkasutaja ootab abi oma probleemide lahendamiseks (ei saa niikaua oma ülesandeid täita), IT süsteemile tehtavad planeeritud hooldustegevused (vajalikud teostada tööajal), planeerimata tõrked e-posti süsteemis või andmebaasidesse ligipääsu katkemine. Seega saab seisva süsteemi kulud jagada kaheks: planeeritud ja planeerimata. Infot selliste seisakute kaudu on võimalik saada *helpdeski* aruannetest, arvutivõrgu administreerimisinfost, lõppkasutajate tegevusuuringutest ja IT juhtimisest. (Praust jt 1999: 8.2)

Autor nõustub Ciuhureanuga (2009), et seisva süsteemi kulud tekitavad ebaefektiivsust ja probleeme teenuse pakkumisega ning sellega tekkiv ajakulu, koos teiste kulusid tõstvate elementide mõjuga asutusele, on jäänud tihti hindamata.

Kokkuvõtvalt saab väita, et IKT valdkonna kulutuste ja tulemuslikkuse mõõtmine on edukas siis, kui selleks luuakse vastav mõõtmissüsteem, mis arvestab nii finants- kui ka mittefinantsnäitajaid. Selle eelduseks on IT eesmärkide sidumine ettevõtte eesmärkidega ning selle kaudu on võimalus hinnata ettevõttele vajalike kulutuste mahtu. IKT kulusid saab küll tinglikult kaheks jagada: otsesed ja peidetud kulud, kuid samas peidetud kulusid eelarves ei kajastata ning suurusjärgu määramine on subjektiivne ja hinnanguline (näiteks küsitluste kaudu) ning pigem võimaldab ainult ettevõtte siseseid trende määrata. Kahjuks ei käsitle teadaolevad IKT tulemuslikkuse mõõtmise teooriad piisavalt katkestuse mõju hindamist, mistõttu on vajalik nende kombineerimine teiste teooriatega.

IKT katkestuse metoodika väljatöötamisel on kõige keerulisem seisva süsteemi kulude hindamine. Nagu eelpool mainitud, tihtipeale neid eelarves ei kajastata ning kulu suuruse määramine on subjektiivne. Seega tuleb magistritöö autoril antud asjaoluga arvestada ning otsida võimalusi subjektiivsuse vähendamiseks katkestuse hindamise mudelis. Otsesed kulud on mõõdetavad ja reeglina seotud tark- või riistvara ostuga ning nende määramise aluseks on konkreetselt tekkinud kulud.

1.2. IKT katkestuse mõõtmine IT haldamise parima praktika raamistikus

IKT katkestuste mõju hindamise metoodika väljatöötamiseks peab magistritöö autor vajalikuks uurida IT haldamise parimaid praktikaid ning seal välja pakutavat katkestuse mõju hindamise mudelit. Kahjuks keskenduvad IT haldamise parimad praktikad rohkem IT pakkujale ja tema tegevuse mõõtmisele, mitte niivõrd sisupoolele tekitatud kahju hindamisele. Eraettevõtted saavad näiteks lepinguliste suhetega reguleerida kahjude hüvitamist, kui ostetakse IKT teenust sisse. Siseministeeriumi valitsemisalas pakub nimetatud teenust SMIT ning riigiasutused omavahel leppetrahve ei määra ning seega katkestusest tingitud kahjude järel asutused kulude hüvitamist omavahel ei tee. Sellegi poolest peab magistritöö autor vajalikuks IT haldamise parima praktika uurimist, et kasutada mudelis IT poole väljatöötatud katkestuse/intsidentide hindamise põhimõtteid.

Eelmisest alapeatükist järeldus, et IT tulemuslikkuse hindamiseks tuleb asutuse eesmärkidest lähtuvalt sätestada IT eesmärgid ning välja valida eesmägi saavutamiseks sobilikud mõõdikud. IT teenuste paremaks haldamiseks on välja töötatud mitmeid erinevaid standardeid ja praktikaid. Seega peab organisatsioon välja valima endale sobiliku standardi, et tema eesmärgid oleksid selle abil saavutatavad ning IT protsessid toimiksid.

Magistritöös leiavad käsitlemist kolm levinuimat IT haldamise praktikat: ITIL (*Information Technology Infrastructure Library)*, ISO27002 ja COBIT (*Control Objectives for Information and Related Technology*). Lühiülevaadete järel on valitud täpsemaks uurimiseks katkestuse hindamise seisukohalt kõige sobilikum.

ISO 27002 on rahvusvaheline IT turvalisuse standard, mis on välja antud ISO ja IECi tehnilise komitee ISO/IETC JTC 1 poolt. Selle eesmärk on tagada organisatsioonis infomatsiooni levik õigete osapoolte vahel. Seda saab vaadata kui parimat praktikat arendamaks ja säilitamaks turvalisuse standardit, et suurendada usaldusväärsust informatsiooni turvalisel kasutusel organisatsioonide vahelistes suhetes. Informatsiooni turvaline kasutus sisaldab ka informatsiooni nõuetekohast kättesaadavust ehk siis vajadust tagada infosüsteemide käideldavus. Standard defineerib 133 turvalisuse kontrolli strateegiat, mis on koondatud 11 peamisesse nimetusse. Standard rõhutab riskihalduse

olulisust ja selgitab, et ei ole vajalik rakendada igat juhendit, vaid ainult neid, mis on asjakohased. (Nastase, P., Nastase, F., Ionescu 2009)

Standardi positiivseks küljeks on ka lähenemine, et see ei rõhuta kindlaid lahendusi või tehnilisi konstruktsioone, vaid rõhutab IT süsteemide nõuetekohase toimimise eesmärkide läbimõtlemist. Standardi põhiselt kontrollitakse, kas süsteemide loomisel on silmas peetud erinevaid aspekte, mis mõjutavad süsteemi usaldusväärsust ja loodetavat toimimist. Standard baseerub omaaegsel Suurbritannia standardil BS7799, mille rahvusvahelist aktsepteerimist ISO standardi alusena saab lugeda üheks tunnustuseks parimast praktikast. IKT katkestuste mõõtmise ja hindamise seisukohalt on ISO 27002 heaks eeskujuks võimalike mõjurite nimistu koostamisel ja tervikvaate hindamisel. Siiski ei ole ISO 27002 sobilik otseseks rakendamiseks katkestuste mõju hindamisel ainsa teoreetilise allikana.

COBIT on parima praktika raamistik IT haldamisele, mis tagab juhtkonnale, välistele audiitoritele ja IT kasutajatele asjakohased protsessid, mõõdikud ja indikaatorid, et hõlbustada IT haldamist ja kontrolli organisatsioonis (Knahl 2009). COBIT ei sisalda protsessi samm-sammulist kirjeldust, kuigi see on orienteeritud IT protsessidele, COBIT on pigem kontrolli ja juhtimise raamistik, kui protsessi raamistik (Nastase et al 2009). COBIT keskendub sellele, mida ettevõte peab tegema, mitte kuidas seda teha.

COBIT on tihti peamine allikas IT haldamise auditeerimisel sõltumatute audiitorite poolt. IKT katkestuste ja nende mõõtmise osas sätestab COBIT teatud hindamisstandardid, kuid oma üldistuse astme juures ei anna tegelikkuses vajaminevat otsest mõõtmisjuhist. Seetõttu saab magistritöö raames COBIT-it vaadelda kui allikat täiendavate aspektide arvessevõtmisel (näiteks IKT katkestuste kaudsete mõjude määratlemisel), ent ta ei ole piisav katkestuste mõju täpseks määratlemiseks organisatsioonis.

ITIL võeti esmakordselt kasutusele Inglismaal 1980. aastal. Selle eesmärgiks oli parendada IT teenuste pakkumise ja ressursside haldamise kvaliteeti. Raamistik töötati välja Ühendkuningriigi *Office Of Government Commerce* (OGC) poolt riigiasutustele, mis levis kiiresti erasektorisse. See oli vastuseks IT suuremale iseseisvusele ning samal ajal

suurenevale vajadusele tõhususe ja efektiivsuse järele. (Galup, Dattero, Quan, Conger 2009)

ITIL on kogumik raamatutest, mis kirjeldab IT haldamise protsesse, funktsioone, rolle ja vastutust, mis on seotud teenuse pakkumise ja hilisema toega (Pollard & Cater-Steel 2009). Lisaks kirjeldab ITIL esmakordselt teenuse jätkupidevust kui võtmetegevust, mis on oluline väärtus kliendile (Nastase et al 2009). Teenuse jätkupidevus omab erilist väärtust politseiorganisatsioonis, mis peab tagama oma põhitegevuse jätkusuutlikkuse, vaatamata muutuvatele välis- ja sisetingimustele.

Tabelis 1 on toodud kolme standardi võrdlus, kust selgub iseloomustavad näitajad ning rakendusvaldkond.

Tabel 1. Võrdlus COBIT, ITIL ja ISO 27002 (allikas: Priandoyo 2009, autori kohandus)

Nimetus	COBIT	ITIL	ISO 27002
Funktsioon	IT protsesside kaardistamine	IT teenuste tasemel protsesside kaardistamine	IT turvalisuse raamistik
Valdkond	4 protsessi ja 34 valdkonda	26 protsessi ja 4 funktsiooni	10 valdkonda
Väljaandja	ISACA	OGC	ISO standard
Rakendus	IT audit	Teenuste haldus	Vastavus turva standardile
Konsultant	Audiitorfirma, IT konsultatsiooni firma	IT konsultatsiooni firma	IT konsultatsiooni firma, turvafirma

ITIL on suhteliselt sarnane COBIT-iga, kuid põhierinevus nende vahel on järgnev: COBIT sätestab standardi, mis keskendub protsessi põhisele süsteemile ja riskidele, mida põhjustab IT rakendamine, kuid ITIL seevastu keskendub IT põhiteenustele (Nastase et al 2009). Antud olukorras käsitletakse IT põhiteenuseid kui teenuseid, mis on vajalikud IT

süsteemide toimimiseks ning seega toetavad asutuse (käesolevas töös politseiorganisatsiooni) põhitegevusi.

Valiku tegemisel mõne eelpool nimetatud standardi kasuks tuleb otsustajatel keskenduda esmalt sellele, et millisest standardist lähtuvalt on lihtsam teha muutusi ja võtta üle parendusi ning astuda üks samm korraga. Kindlasti tuleb valiku tegemisel mõelda ka juhtkonna ootustele, kuna enamikes ettevõtetes võtab korraliku ülevaate saamine IT-st aega ning see on pidev täiustamise protsess. (Nastase et al 2009)

Konkreetset ühest vastust ei saa asutusele anda, et millist IT haldamise parimat praktikat rakendada, kuna see sõltub organisatsiooni omapärast ja IT protsesside keerukusest. Paljud asutused alustavad COBIT-ist, mis on kõige üldisem ja koondab teised parimad praktikad enda alla ja aitab neid siduda äripoole nõuetega. Pärast selle rakendamist kaaluvad mõned ettevõtted ka ITILi ja ISO 27002 rakendamist, juhul kui eelarve seda lubab.

Käesoleva töö autor nõustub Nastase (et al 2009) ja Priandoyo (2009) arvamusega, et kõige lihtsam on eelpool nimetatud kolmest praktikast rakendada ITIL-it, kuna seda saab rakendada ka osaliselt, kui kõikide protsesside väljatöötamiseks eelarvelisi vahendeid ei jätku, või kui soovitaksegi ainult ühte moodulit rakendada, siis see ei avalda lõpptulemusele negatiivset mõju. See asjaolu selgitab ka ITILi laialdast levikut.

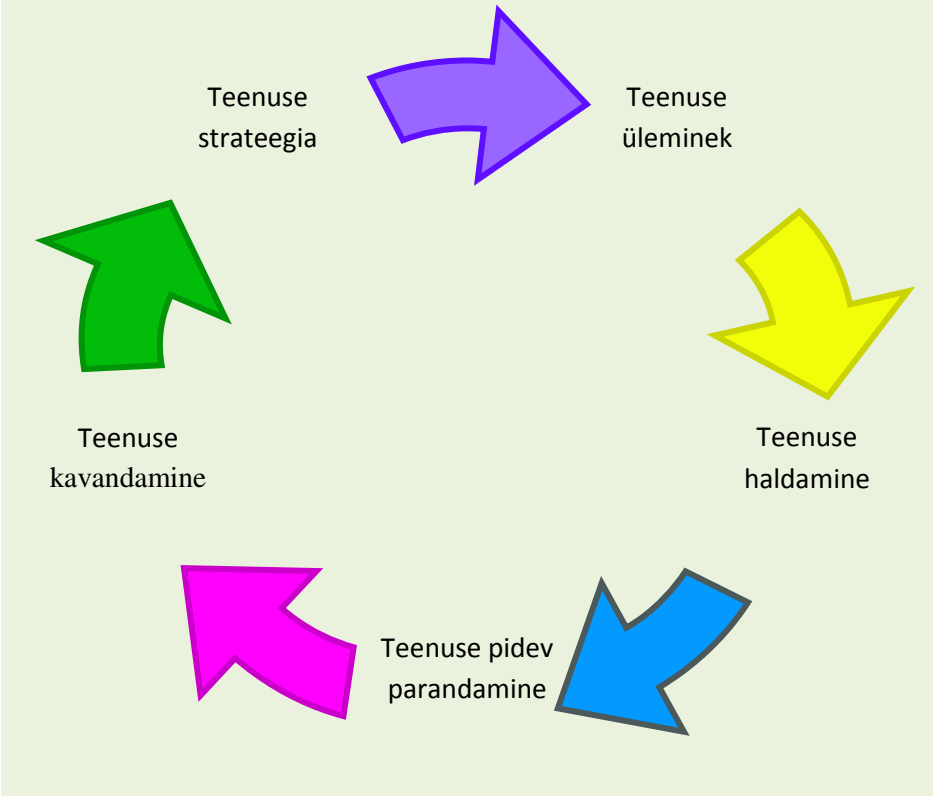
Magistritöö raames väljapakutava IKT katkestuste hindamise metoodika jaoks teoreetilise baasi loomiseks otsustas autor eelpool toodud kolmest parimast praktikast uurida täpsemalt ITILi põhimõtteid ja intsidendihalduse protsessi, kuna see on kõige lähemalt seotud katkestuse mõõtmisega. ITIL vaatleb küll intsidendihaldust IT teenuse pakkuja lähtekohast, kuid magistritöö autor saab neid põhimõtteid kohandada ja kasutada IKT katkestuse mõju hindamise mudeli väljatöötamisel. Valiku üheks argumendiks on asjaolu, et ITILi põhimõtteid rakendab ka Siseministeeriumi valitsemisalale IKT tuge pakkuv SMIT.

Eelmisel aastal magistritööd kaitsnud Evelin Kasenõmm jõudis oma töös „IT teenuste haldamise parimad praktikad (ITIL): raamistik avaliku halduse reformide kontekstis ja

rakendamine Siseministeeriumi haldusalas“ järeldusele, et olenemata avaliku halduse diskursuses toimunud suurtest muudatustest ajast, mil ITIL välja töötati, on ITIL-i näol jätkuvalt tegemist sobiva raamistikuga, millest lähtuda avaliku sektori IT-teenuste arendamisel, nii üldiselt kui ka Eestis. Selle kasuks räägib eelkõige asjaolu, et ITIL-i mehhanismid pole mitte niivõrd IT-põhised, vaid just teenusepakkumise olemuse kesksed, seega ei takista ITIL-i rakendamine avaliku sektori organisatsiooni tõhusamaks ja tulemuslikumaks muutumist.

Tänane ITIL kirjeldab IT parimaid praktikaid läbi protsessi, rolli ja realisatsiooni juhise, mida saab jälgida iga IT organisatsioon, et tõhustada IT teenuste toimimist (Knahl 2009).

Viimane versioon ITIL-ist (versioon 3) avaldati 2007. aasta mais ning see koosneb viiest raamatust. Kõik raamatud katavad IT teenuste haldust ning seda tehakse läbi teenuse elutsükli. IT teenus on teenus, mida tagatakse ühele või mitmele kliendile IT teenuse pakkuja poolt. IT teenus baseerub IT kasutusel ning see toetab kliendi äriprotsesse. IT teenus on kombinatsioon inimestest, protsessidest ja tehnoloogiast ning see on defineeritud teenustaseme kokkuleppes (*service level agreement*). (OGC 2007c: 243)



Joonis 3. Teenuse elutsükkel
(allikas: OGC 2007c: 8, autori kohandus)

Joonisest 3 nähtub, et kõige aluseks on teenuse strateegia kohandamine. Seejärel juba järgmise tasandi protsessidele edasi liikumine, milleks on teenuste kavandamine, teenuste üleminek ja teenuste haldus. Kogu nende teenuste elutsüklite rõngaks on järjepidev teenuste parendamine ja teenuste mõõtmine ning teenuste raporteerimine. ITIL kontsentreerub eelkõige protsessidele ning nende efektiivsemaks muutmisele, koostööle ja kirjeldamisele.

ITIL-i eesmärk on pigem toetada, mitte dikteerida kliendi organisatsioonis toimuvaid protsesse. ITIL-i roll on kirjeldada lähenemist, funktsioone, rolle ja protsesse, millele organisatsioon saab üles ehitada praktika neile sobilikul kujul ja anda juhiseid madalaimal rakendataval tasemel. (Nastase et al 2009)

Käesolevas magistritöös uuritakse katkestuse mõju põhitegevusele ning seega on vajalik avada teenustaseme halduse protsessi ITIL-i mõistes. Teenustaseme halduse eesmärgiks on

- määrata, dokumenteerida, monitoorida ja mõõta pakutava IT teenuse taset;
- hoida ja parendada kommunikatsiooni ettevõtte ja kliendi vahel;
- tagada spetsiifiliste ja mõõdetavate eesmärkide seadmine kõikidele IT teenustele;
- monitoorida ja parandada kliendi rahulolu pakutava teenuse kvaliteediga;
- tagada, et IT ja klient saavad teenustaseme kokkuleppest ühtemoodi aru;
- kindlustada, et kuluefektiivne teenuse kvaliteet on säilinud või järk-järgult paranenud. (OGC 2007a: 65)

Teenustaseme halduse protsessist kasvab välja teenustaseme kokkulepe (*service level agreement*), mis on kirjalik dokument IT teenuse pakkuja ja kliendi vahel. Dokumendis defineeritakse võtmeeesmärgid ja mõlema osapoole kohustused. Parema koostöö nimel on põhirõhk osapoolte vahelisel kokkuleppel. Teenustaseme kokkulepe peab olema selge ja konkreetne ning mitte jätma võimalust kaheti mõistmiseks. Seega tuleks vajadusel lisada ka mõistete seletus kindlustamaks kõigi osapoolte ühist arusaama. Teenustaseme kokkuleppeid saab sõlmida teenuse põhiselt (näiteks e-maili teenus), kliendi põhiselt (üks organisatsioon) ja mitmetasemelise kokkuleppena (näiteks korporatsioonitase, kliendi ja teenuse tase). (OGC 2007a: 66-69)

Hartley (2005) rõhutab, et teenus ei ole aineline nagu on toote valmistamine ning selletõttu võib teenuse hindamine olla subjektiivne. Vältimaks seda subjektiivsust, tuleb teenused selgelt defineerida, kuid mitte ainult teenuse tehnilisest aspektist lähtuvalt, peavad olema määratud ka mõõdikud, mis väljendavad teenuse efektiivsust.

Lähtudes eeltoodust on kvaliteetse IT teenustaseme halduse puhul olulisemad komponendid teenustaseme kokkulepe ja võtmemõõdikud, et saavutada edu IT teenuse pakkumisel (Knahl 2009). Korrektselt sõnastatud teenustaseme kokkulepped soodustavad partneritevahelise koostöö laabumist, samal ajal kui valed või ebaõigete mõõdikutega teenustaseme kokkulepped on sama hea kui nende puudumine (Hartley 2005).

Selle saavutamiseks ei ole autori hinnangul teenustaseme kokkuleppesse mõtet panna mittehinnatavaid näitajaid ning tingimuste täitmise jälgimisega tuleb alustada koheselt peale kokkuleppe sõlmimist. Raportite vormistamise intervall tuleb kliendiga eraldi kokku leppida.

ITIL-i protsessidest on kasutajatugi määratud kliendi vaates võtmefunktsiooniks. Kasutajatugi on kontaktpunkt (*singel point of contact*) vastastikuses suhtluses IT teenuse kasutajaga, mille eesmärk on rahuldada nii kliendi (näiteks soov tellida teenust) kui ka IT teenuse pakkuja (näiteks soov pakkuda IT teenust) eesmärke. Intsidendihalduse protsess läbi kasutajatoe on olulisemaid ITIL-i protsesse hõlbustamaks suhtlust IT kasutaja ja IT teenuse pakkuja vahel. (Knahl 2009)

ITIL-i versioon 3 järgi on intsident planeerimata IT teenuse katkestus või teenuse kvaliteedi vähenemine. Intsident on ka ebaõnnestumine konfiguratsiooni esemega, mis ei ole mõjutanud teenust. Intsidendi haldus on protsess, mis tegeleb kõikide intsidentidega: tõrked, kasutajate (tavaliselt läbi kasutajatoe) ja tehnilise kaadri esitatud küsimused ning päringud või automaatselt läbi monitooringusüsteemi avastatud ja raporteeritud sündmused. (OGC 2007b: 46)

Intsidendihalduse eesmärgiks on tagada normaalne teenuse tase nii ruttu, kui see on võimalik. Normaalse teenuse taseme määratlus tuleb teenustaseme kokkuleppest. Antud magistritöö raames huvitab autorit katkestuse/intsidendi mõju mõõtmine põhitegevusele. ITIL-i raamistik hindab intsidendi olemasolu ja selle kõrvaldamise kiirust ning kõik intsidendid prioritiseeritakse. Eelkõige on määratluse aluseks intsidendi kriitilisus (kui kiiresti vajab äripool lahendust) ja selle mõju ulatus äripoolele (täpsemalt toodud Tabelis 2). Täiendavalt võivad lisanduda järgmised näitajad: oht elule, mõjutatud teenuste hulk, finantsilise kaotuse ulatus, mõju äri mainele ja seadusest tulenevad nõuded.

Tabel 2. Intsidendi kriitilisuse määramine (allikas: OGC 2007b: 51)

			Mõju	
		Kõrge	Keskmine	Madal
	Kõrge	1	2	3
Kriitilisus	Keskmine	2	3	4
	Madal	3	4	5

Järgmiseks soovitab ITIL (vastavalt kriitilisuse astmele) määrata intsidendi lahendamise aja ning üks võimalik ettepanek selleks on toodud Tabelis 3.

Tabel 3. Prioritiseerimise koodi süsteem (allikas: OGC 2007b: 51)

Prioriteetsus	Kirjeldus	Lahenduse aeg
1	Kriitiline	1 tund
2	Kõrge	8 tundi
3	Keskmine	24 tundi
4	Madal	48 tundi
5	Planeerimine	Planeeritud

Selline prioritiseerimine eeldab, et intsidendi vastuvõtja tunneb süsteemi, et määrata vastavat koodi, mis tähendab, et vastav koodisüsteem tuleb teenustaseme kokkuleppe juures läbi arutada ning pärast kasutajatoe meeskonnale selgeks teha.

Alati tuleb rõhutada, et intsidentide prioriteetsus on dünaamiline ja ajas muutuv. Seega kui olukord muutub või intsident ei ole etteantud ajas lahendatud, tuleb ka selle prioriteetsuse tase üle vaadata. Kui kasutajatugi on veendunud, et nad ei suuda ise intsidenti lahendada, tuleb see suunata eskaleerimisse. Eskaleerimise võib tinglikult jagada kaheks: funktsionaalne (kasutajatoe nn teine tase) või hierarhiline (IT juhi teavitamine). Eskaleerimise tasemed ja nende ajamõõtmed määratakse teenustaseme kokkuleppes. Kasutajatugi peab hoidma klienti informeerituna ning jälgima, et intsidendi andmed oleks süsteemis uuendatud, et tagada kogu ajaloo säilimine. Peale intsidendi lahendamist tuleb sellest samuti klienti teavitada ning seejärel intsident sulgeda. (OGC 2007b: 51-53)

Autor leiab, et korrektselt sõnastatud ning mõõdikutega seotud teenustaseme kokkulepe on eduka partnerlussuhte aluseks ning aitab edaspidi vältida vaidlusi teenuse kvaliteedi osas. Mõõdikud, mida intsidendihalduses kasutatakse, on valdavalt suunatud IT teenuse pakkuja sisemiste protsesside tõhustamisele ja tulemuslikkuse mõõtmisele vastavalt teenustaseme kokkuleppes toodud näitajatele. ITIL-i intsidendihalduse protsessi raames prioritiseeritakse intsidendid lähtuvalt selle mõjust sisupoolele. Magistritöö autor peab põhjendatuks analoogset prioritiseerimist kasutada ka väljatöötatavas mudelis, kuna ärikriitilise teenuse katkestuste puhul on selle mõju tervele organisatsioonile suurim (sh ka tekkiv kulu), millega võib kaasneda avalikkuse tähelepanu, kus peab reeglina sekkuma PPA juhtkond ning suuremate katkestuste puhul Siseministeerium.

1.3. IKT katkestuse hindamine toimepidevuse riskianalüüsis

Organisatsiooni jaoks kriitilised tegevused on otseselt või kaudselt seotud IKT komponendiga ning selle mõju ei saa alahinnata. Seega peab autor vajalikuks avada toimepidevuse mõistet läbi riskihalduse ning selle hindamise aluseid, et oleks võimalik saada sisendit magistritöö raames väljatöötatavasse metoodikasse. Toimepidevuse arvestamine IKT vaates on oluline just pidevalt toimivates (ajakriitilistes) organisatsioonides (sh politseiasutustes).

Eelnevalt kajastatud ITIL-i intsidendihalduse põhimõtted on käesolevas alapeatükis seotud toimepidevuse tagamisega, kuna katkestuse prioritiseerimise aluseks on mõju organisatsioonile ning vastavalt sellele määratakse ka reageerimise aeg. Toimepidevuse tagamine üldiselt, nagu vaadeldakse käesoleva alapeatüki alguses, ei ole otseselt seotud IKT teenuste ja nende toimepidevusega, ent magistritöö vaates ja püstitatud ülesannete lahendamiseks küllaltki hästi nendega kombineeritavad.

Äriettevõtted on hakanud järjest enam hindama toimepidevuse tagamist ja selle haldust. Selle eesmärgiks on tagada katkematu toimimine kõikidele võtmeressurssidele, mis on

vajalikud toetamaks kriitilist äritegevust katkestuse korral ning kiirendama tagasipöördumise aega nn tavategevuste juurde. (Tammineedi 2010)

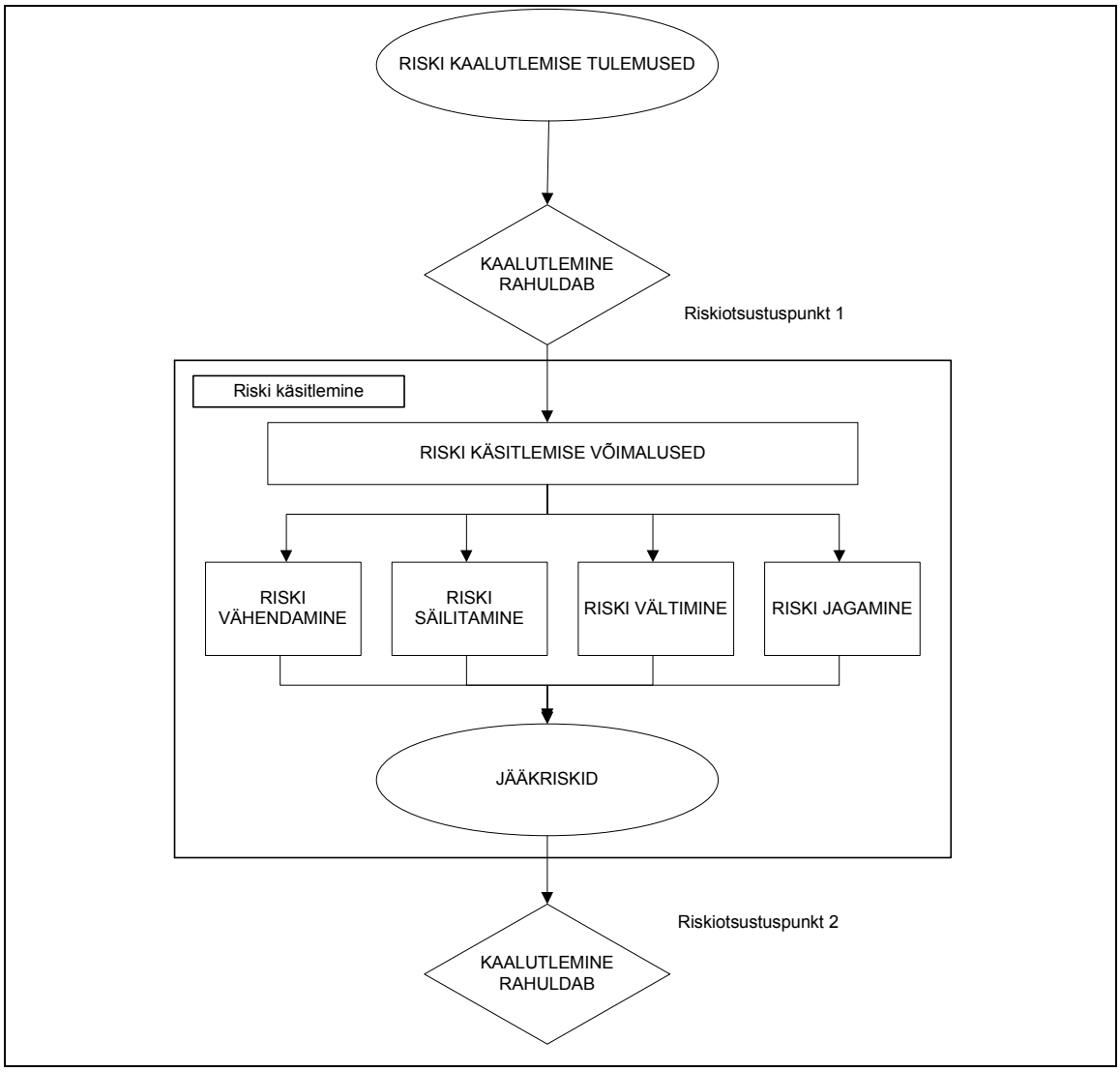
Samas see ei ole omane ainult äriettevõtetele, kuna toimepidevuse mõiste on sisse toodud ka Eesti julgeolekupoliitika alustes, mis sätestab, et ühiskonna ja riigi toimivuse tagamiseks hädavajalikke teenuseid käsitatakse elutähtsate teenustena. Elutähtsa teenuse toimepidevus tagamiseks arendatakse teenuse järjepideva toimimise suutlikkust, taastamise võimet pärast teenuse katkestust, tagatakse piisav tegevusvaru ja koostatakse tegevusplaanid (Eesti julgeolekupoliitika alused, vastu võetud Riigikogu 12.05.2010 otsusega).

Rahvusvahelise Standardi Organisatsioon (edaspidi ISO) andis 2009. aastal välja riskihalduse standardi ISO 31000:2009, mis sätestab igat tüüpi organisatsioonis kohandatavad rakendamise põhimõtted, raamistiku ja haldamise protsessi. See ei määra, et üks lähenemine sobib kõigile, vaid pigem rõhutab fakti, et riskihaldust tuleb kohandada spetsiifilistest vajadustest ja organisatsiooni struktuurist lähtuvalt. (Knight 2010)

Eelpool toodust lähtuvalt on ISO 31000:2009 praktiline dokument, et asutused saaksid juurutada oma lähenemist riskihaldusele. Standardi rakendamisel ei saa organisatsioonid endale sertifikaati taotleda, vaid pigem saavad võrrelda enda riskihaldust rahvusvaheliselt tunnustatud põhimõtetega.

Riskihalduse mõistel on erinevaid tõlgendusi ning Stulz (2009) märgib, et see sisaldab endas mineviku teadmise baasilt ennustamist, et antud risk realiseerub. ISO 31000:2009 seevastu sätestab, et see on kooskõlastatud tegevus organisatsiooni suunamiseks ja ohjamiseks riski suhtes (ISO… 15.04.2011). Chitakornkijsil (2010) nimetab riskihaldust protsessiks, mis osundab organisatsiooni võimalikele kahjudele ning kõige sobilikematele tehnikatele nende kahjudega toimetulekuks.

Seega tuleb riskihalduses defineerida risk ning määrata maandamismeetmed võimaliku tagajärje leevendamiseks või ärahoidmiseks. Joonisel 4 on näidatud klassikaline riski käsitlemise võimalus ning kujutatud riskiotsustuspunkte.



Joonis 4. Riski määramise alused
(allikas: Tomik ja Aben 2010)

Joonisest 4 nähtub, et tuleb kaalutleda, mida riskiga teha ning kas asutuse juhtkonnale on risk vastuvõetav või tuleb otsida siiski riski maandamistegevusi. Kuid alati eksisteerib jääkrisk, mis on asutusele aktsepteeritav ning selle maandamine ei ole enam otstarbekas.

Riski hindamisel ei tasu hinnata tervet organisatsiooni tervikuna, vaid püüda siiski piiritleda mingi valdkond/teenus, mida hakatakse hindama. Saadud analüüsi tulemus on reeglina sisendiks tasuvuse hinnangule - riski tekitatav võimalik kahju vs meetme rakendamise kulu. (Tomik ja Aben 2010)

Chitakornkijsil (2010) toob välja, et riskihalduses jagatakse eesmärgid kaheks: kahju-järgsed ja kahju-eelsed ning seletab neid järgnevalt:

- Kahju-järgsed eesmärgid. Riskihaldus hindab konkreetseid eesmärke pärast kahju toimumist. Sellised eesmärgid on ellujäämine, sisetulekute stabiilsus, jätkusuutlikkuse tagamine jne. Mõnede ettevõtete jaoks on võime tegutseda peale kahju toimumist väga oluline, siia alla käivad ka avaliku sektori asutused, kes peavad elutähtsat teenust tagama.
- Kahju-eelsed eesmärgid. Kriitilised tegurid, mis ilmnevad enne kahju ning reeglina tingitud välistest asjaoludest (majandus, õiguslikud kohustused) ning asutus peab hakkama tegelema nende maandamisega või tegema tegevusi, et võimalik kahju oleks minimaalne.

Eestis kehtima hakanud Hädaolukorra seaduse (edaspidi HOS) neljas peatükk sätestab uued põhimõtted elutähtsate teenuste korraldusele (Hädaolukorra seadus, 15.06.2009). Seaduses kirjutati elutähtsad valdkonnad teenuste tasandil lahti ning määratleti asutuste ja ettevõtete kohustused teenuste toimepidevuse tagamisel. Elutähtsa teenuse osutajal on kohustus koostada teenuse toimepidevuse riskianalüüs ning toimepidevuse plaan. Reeglina on riskianalüüsi osaks ka ärianalüüs, kus tuuakse välja katkestuse ajalise ulatuse hindamine ja vajalike mõjude tuvastamine. Saadud tulemused on sisendiks tasuvuse hinnangule, seega toob autor antud peatükis ära toimepidevuse riskianalüüsi koostamise põhimõtted, et sealt saaks sisendit magistritöö raames väljatöötatavasse metoodikasse.

HOS § 34 lg 1 sätestab, et elutähtsa teenuse toimepidevus on elutähtsa teenuse järjepideva toimimise suutlikkus ja järjepideva toimimise taastamise võime pärast katkestust. Seaduse mõistes peab toimepidevuse riskianalüüsi koostama asutus, kes korraldab elutähtsa teenuse toimepidevust. Siseministeerium korraldab järgnevate elutähtsate teenuste toimepidevust:

- avaliku korra tagamise toimimine
- päästetöö toimimine
- hädaabi õnnetusteadete menetlemise toimimine
- lennu- ja merepääste toimimine
- merereostusseire ja -tõrje toimimine
- operatiivraadiosidevõrgu toimimine

- Riigikogu, Vabariigi Valitsuse ja Vabariigi Presidendi töö toimimise tagamine

Siseminister on määrusega kehtestanud toimepidevuse riskianalüüsi ja toimepidevuse plaani koostamise juhendid. Vabariigi Valitsuse määrusega tuleb täiendavalt kehtestada elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed, mida siiani tehtud ei ole.

Toimepidevuse riskianalüüsi koostamise juhendis reguleeritud toimepidevuse riskianalüüsi koostamise korraldus ning defineeritud seal kasutatavad mõisted (Toimepidevuse riskianalüüsi koostamise juhend, vastu võetud siseministri määrusega 08.06.2010) (edaspidi Toimepidevuse riskianalüüs) ning magistritöö autor toob ära valiku neist, mis on antud töö mõistes olulisemad

- katkestus- negatiivne kõrvalekalle teenuse eesmärgi- ning plaanipärasel osutamisel, mis on põhjustatud kas prognoositavast (nt streik) või ootamatust (elektrikatkestus, torm) sündmusest;
- oht – sündmus või asjaolu, mis võib põhjustada katkestust;
- risk– hinnang asjaoludele, mis võivad takistada asutuse või ettevõtte võimekust osutada elutähtsat teenust tähtajaliselt, ettenähtud kvaliteediga või planeeritud mahus;
- riskimaatriks– maatriks elutähtsa teenuse kriitilise tegevuse katkemise tagajärgedest ning tõenäosusest, mille alusel määratakse riskiklass;
- riskiklass– elutähtsa teenuse katkestuse tähtsuse sõnaline kirjeldus, mis sõltub katkestuse tõenäosusest ja selle raskusastmest ning mille abil järjestatakse riskid;
- maksimaalne katkestuse lubatud kestus– kriitilise tegevuse katkemise periood, mille möödumisel pole juriidiline isik või asutus võimeline osutama elutähtsat teenust seadustes või nende alusel kehtestatud õigusaktides või lepingutes sätestatud tingimustel;
- nõutav taasteaeg – teenuse osutaja poolt määratud aeg kriitilise tegevuse jätkamiseks ja taastamiseks.

Riskianalüüs sooritatakse järgmiste sammudega: elutähtsa teenuse kirjeldamine, kriitiliste tegurite väljaselgitamine, vara olulisuse hindamine, ohtude ja nõrkuste määratlemine,

turvariskide tõenäosuse hindamine ja oodatava kahju hindamine. Riske on võimalik hinnata kvalitatiivselt ja kvantitatiivselt.

Kvantitatiivse riskianalüüsi korral taandatakse kõik rahale: hinnatakse ohtude suhtelisi sagedusi ja raha suurust, st kasutatakse võimalikult täpset statistikat ja kahjude rahalisel väärtusel põhinevat metoodikat.

Kvalitatiivne riskianalüüs on ohtude toime hindamine, kus väärtuste asemel kasutatakse väärtuste tinglikke ja jämedaid astmikke. Tavaliselt on kasutusel 3-4 astet (näiteks suur-keskmine-väike) ning teadaolevad täpsed rahalised väärtused viiakse sellisele kujule.

Toimepidevuse riskianalüüs sätestab, et hinnatakse ainult riske, mis põhjustavad elutähtsa teenuse mittetoimimist. Seega rakendatakse riskianalüüsiks kvalitatiivset riskianalüüsi ning katkestuse ajaline mõõde ja ulatus tuuakse välja 5-astmelisel skaalal. Elutähtsa teenuse tegevuse kriitilisus saadakse kahe näitaja korrutisel.

Elutähtsa teenuse tegevuse kriitilisus = katkestuse ajaline mõõde x katkestuse ulatuse mõõde

Konkreetsed vahemikud on toodud Lisas 1. Saadud tulemused, kus kriitilisuse punktid on üle kuue, siis tuleb jätkata riskianalüüsi koostamist. Toimepidevuse riskianalüüsi lisas 5 on eraldi välja toodud ka infotehnoloogiliste süsteemide hindamise tabel (Lisa 2), kuid selle üldpõhimõte on sama, mis kõikide kriitiliste tegevuste hindamisel. Määruse põhimõte on ka see, et kriitiliste teenuste puhul peaksid olema välja pakutud taasteplaanid ning varuplaanid. Taasteplaanide koostamist ning kriitilisemate süsteemide puhul varuplaanide koostamist näeb ette ka IT parimad praktikad (sh ITIL).

Ärimõju analüüs on toimepidevus planeeringu alus ning need neli sammu on järgmised: määrata võimalik mõju organisatsioonile katkestuse korral; identifitseerida kriitilised protsessid/tegevused ning maksimaalne lubatud katkestuse aeg, taasteaeg ning taastepunkt; määrata taastatavate äriprotsesside ja andmete järjekord katkestuse korral ning taasteplaanid, minimaalsed ressursivarud (Tammineemi 2010).

Need vajalikud sammud on kaetud elutähtsa teenuse toimepidevuse riskianalüüsi määramisel ning seega jälgib juhend üldtuntud riskianalüüsi koostamise põhimõtteid, kuigi määruses on tehtud kohandusi ja lihtsustusi (eeltäidetud tabelid), et asutustel oleks lihtsam analüüsi koostada.

Seega ei ole toimepidevuse riskianalüüs midagi uut, kuna riskianalüüse tuli riigiasutustel teha ka varem. PPA teeb kogu asutust hõlmava riskianalüüsi ning edastab tulemused ministeeriumile. Riskide hindamise protsessi raames tuvastatakse politseiasutuste tegevusriskid, hinnatakse vastavaid riske ning töötatakse välja maandamismeetmed, sh määratakse maandamismeetmete rakendamise eest vastutavad struktuuriüksused. Vastav riskide hindamine täidab oma olemuselt vähemalt osaliselt elutähtsa teenuse toimepidevuse riskianalüüsi funktsiooni.

Kuna 2010/2011 tuli asutustel Siseministeeriumi välja töötatud metoodika alusel riske hinnata esmakordselt, siis on vajalik politseiasutuste analüüside koostamise eest vastutavate struktuuriüksuste koolitamine elutähtsa teenuse toimepidevuse korralduse küsimuses.

Kindlasti tasuks edaspidi kaaluda tegevusriskide ja elutähtsate teenuste toimepidevuse riskianalüüside koostamise ühildamist metoodiliselt ja/või protseduuriliselt, kus ühe tervikliku protsessi raames saadakse sisend asutuste tegevusriskide aga ka asutuste poolt osutatavate teenuste toimepidevuse osas.

Toimepidevuse riskianalüüsi koostamise osas toob autor välja järgnevad asjaolud:

- riskianalüüs tuleb teha ainult elutähtsate teenustega seotud kriitiliste tegevuste osas, mis tähendab, et see ei hõlma tervet organisatsiooni (sh infosüsteeme);
- juhend näeb ette, et riskianalüüs koosneb järgnevatest osadest: sisukorrast ja riskianalüüsi koostanud isikute loetelust; analüütilisest osast; analüüsi tegemiseks koostatud vajalikest tabelitest ja joonistest; riskimaatriksist; ja riskianalüüsi kokkuvõttest. Seega kogu protsessi läbikäimine on aeganõudev ning seda ei saa rakendada kiiresti ja operatiivselt toimunud katkestuse mõõtmiseks;

- hindamise metoodika rõhuasetus on kriitilistel teenustel ja nende toimepidevuse taastamisel, kuid sellega ei hinnata organisatsioonile tekkivat kulu (sh seisva süsteemi kulusid);
- riskide hindamisel hinnatakse juhtumi esinemise tõenäosust, kuid IKT katkestuse hindamise metoodika peaks tuginema juba olnud andmetel, st oleks võimalik hinnata asutusele tekkinud kulu.

Autor saab kokkuvõtvalt väita, et IKT katkestuse hindamise metoodika loomisel saab kasutada ITIL-i intsidentide prioritiseerimise ja elutähtsa teenuse toimepidevuse kriitilisuse määramise põhimõtteid. Mudeli loomisel on oluline arvestada infosüsteemi kriitilisuse astet, kuna ärikriitiliste infosüsteemide mõju on organisatsioonile suurem kui vähemkriitiliste süsteemide puhul. Infosüsteemide ärikriitilisuse määramise põhimõtted (seatakse vastavalt IT eesmärkidele) peavad olema loogilises seoses organisatsiooni eesmärkidega ning IKT süsteem peab toetama nii avaliku teenuse kui ka siseteenuse toimimist. Teistest magistritöö raames vaadeldud teoreetilistest alustest on mudeli praktilise koostamise jaoks väga oluline TCO-s käsitletav otseste ja peidetud kulude jaotus (käsitletud alapeatükis 1.1) ning sellest tulenevalt ka katkestuste hindamisel võimalik kulude jaotus. Samuti on tähtis COBIT-is rõhutatav vajadus määratleda uuritavas valdkonnas konkreetsed ja täpsed mõjurid ning ISO 27002 standardi alusel soovitus mudeli koostamise järgselt läbi viia kontroll, kas valitud mõjurid ja mudel katavad uuritava probleemi tervikvaates (mõlemad käsitletud peatükis 1.2). Käsitledes IKT katkestust kui riski põhitegevuse toimepidevusele, saab autori poolt väljatöötatava metoodika koostamisel toetuda ka ISO 31000:2009 riskihalduse standardile, mis rõhutab lähtumist organisatsiooni spetsiifilistest vajadustest. Seega on IKT katkestuse mõju mõõtmise metoodika loomine erinevaid teoreetilisi aluseid kombineerides antud kujul uudne ning taoline lähenemine on kooskõlas ka vaadeldud enamlevinud teoreetiliste käsitlustega.

2. IKT KATKESTUSE MÕJU HINDAMISE METOODIKA VÄLJATÖÖTAMINE

2.1. Uuringu läbiviimise alused

Magistritöö esimesest peatükist järeldus, et olemasolev teooria ei anna piisavalt konkreetset juhist probleemi lahendamiseks ja sobiva mudeli koostamiseks ning selleks on vaja uurida konkreetseid praktilisi lahendusi sarnastes tingimustes toimivates organisatsioonides. Autor valis uurimisstrateegiaks juhtumiuuringu ning uuringumeetodiks juhtumianalüüsi.

Juhtumiuuring on uurimisstrateegia, mis keskendub mingi probleemi, sündmuse, tegevuse, protsessi, indiviidi või indiviidide grupi detailsele ja terviklikule tundmaõppimisele. See on nähtuste sügavuti uurimine nende loomulikus keskkonnas tuginedes mitmetele erinevatele infoallikatele ja vaatenurkadele. Andmete kogumisel ja analüüsimisel toetutakse eelnevalt välja töötatud teoreetilistele eeldustele. (Laherand 2008: 74)

Juhtumiuuring on eelistatud uurimisstrateegia juhul kui on püstitatud „kuidas?“ või „miks?“ küsimus (Kuusk 2006: 3). Juhtumianalüüsi peamine ülesanne on anda uuritavast juhtumist või situatsioonist laiahaardeline ülevaade. Kui ankeetküsimustikul põhinevad uuringud toetuvad numbrilise tõendusmaterjali kogumisele ja interpreteerimisele läbi statistiliste üldistuste, siis juhtumianalüüs toetub situatsiooni süvauuringutele, mida hinnatakse läbi analüütiliste üldistuste. Juhtumianalüüs võib käsitleda ainult ühte juhtumit, kuid võib käsitleda ka mitut. Juhtumianalüüsi puuduseks võrreldes ankeetküsitluse läbiviimisega on väiksema valimi kasutamine – juhtumianalüüsi tulemuste põhjal saab üldjuhul teha järeldusi vaid konkreetse valimi kohta, laiemad kogu üldkogumit puudutavad järeldused ja üldistused ei ole võimalikud (Laherand 2008: 83). Kindlasti tuleb

juhtumiuuringu puhul arvestada riskina, et antud meetod esitab suuremaid nõudmisi ka uurijale tema teadlikkuse osas.

Autor valis andmekogusmeetodiks intervjuu, kuna tema eelis teiste meetodite ees on paindlikkus, võimalus andmekogumist vastavalt olukorrale ja vastajale reguleerida. Intervjuus võib näiteks varieerida käsitletavate teemade järjekorda, samuti on vastuste tõlgendamiseks hoopis rohkem võimalusi kui näiteks postiküsitluse puhul. Intervjuu eeliseks on ka see, et vajadusel on intervjueeritavaid võimalik kergesti kätte saada, ka siis kui soovitakse andmeid täiendada. (Hirsijärvi, Remes, Sajavaara 2005: 192-193)

Avatud intervjuude läbiviimiseks koostati eelnevalt küsimused ning saadeti need intervjueeritavatele enne intervjuu toimumist tutvumiseks. Küsimustik annab intervjuudele raamistiku, kuid magistritöö autorile jäi võimalus esitada täiendavaid ning suunavaid küsimusi saamaks uuritavast teemast võimalikult laia ja täpse ülevaate. Lisaks sai uurida intervjueeritavate isiklikke seisukohti, nende soove ja ootusi.

Juhtumiuuringu valim koostati teoreetilistel, mitte statistilistel põhjustel. Valimisse kaasati võimalikult erinevaid juhtumeid saamaks situatsioonist laiema ja ülevaatlikuma pildi. Kuigi valimi väiksuse tõttu kõigi tegevusalade esindajaid valimisse kaasata ei olnud võimalik, eelistati magistritöö jaoks olulisemaid valdkondi. Samuti tuleb täheldada, et kõik ettevõtted, kellega autor kontakteerus, ei olnud huvitatud uuringus osalemisest.

Valimis on neli avaliku sektori asutust (Justiitsministeerium, Registrite ja Infosüsteemide Keskus, Maksu- ja Tolliamet, Häirekeskus) ja kaks eraettevõtet (telekommunikatsiooni ettevõte ja G4S) ning nende esindajatega viidi läbi intervjuud, va Maksu- ja Tolliameti esindajaga, kes vastas küsimustele kirjalikult ning edastas need e-mail teel magistritöö autorile. Avaliku sektori asutused valiti talitluspidevuse olulisuse või sisejulgeolekule lähedaste toimimispõhimõtete järgi. Kuna IKT katkestuse mõju põhitegevusele ja äriprotsessidele mõõdavad kindlasti erasektori ettevõtted, siis autor pidas põhjendatuks ka neid valimisse kaasata. Autori hinnangul avaliku sektori asutused ei panustada IKT katkestuse mõõtmisse kindlasti niipalju, kui teeb seda erasektor. Seega ei pruugi ainult avaliku sektori asutuste kaasamine anda piisavat infot järelduste tegemiseks ning saadud

tulemus võib jääda ühekülgseks. Magistritöö autor peab oluliseks kaasata erasektorit, olenemata sellest, et viimane on rahale orienteeritud, ei saa välistada nende kogemuse ja praktika kasutamist peale vajalike kohanduste tegemist avaliku sektori asutustes.

Valimisse kaasatud asutused ja nende valiku põhjendus on toodud alljärgnevalt:
Justiitsministeeriumi peamine ülesanne on kavandada ja viia ellu riigi õigus- ja kriminaalpoliitikat, mis aitaks tagada avatud ja turvalist ühiskonda, kus inimesed on oma õigustest teadlikud ning võivad nende kaitses kindlad olla. Ministeeriumi haldusala asutused on järgnevad: maa- ja halduskohtud ning ringkonnakohtud; prokuratuur; vanglad; registrite ja infosüsteemide keskus; Eesti kohtuekspertiisi instituut; andmekaitse inspektsioon ja kohtute raamatupidamiskeskus. Ministeeriumi haldusalas töötab kokku üle 3900 inimese, neist 170 ministeeriumis. IKT teenust pakub Registrite ja Infosüsteemide Keskus. (Justiitsministeerium…15.03.2011)

Justiitsministeerium kaasati valimisse, kuna on mitme sisejulgeoleku valdkonna jaoks olulise infosüsteemi (näiteks e-Toimik, kinnipidamiskohtades kasutatavad infosüsteemid) sisuline omanik ja tellija ning seetõttu sarnases positsioonis PPA-ga.

Registrite ja Infosüsteemide Keskus (edaspidi RIK) on Justiitsministeeriumi haldusala asutus, mille tegevusvaldkonnaks on Justiitsministeeriumi valitsemisala info- ja sidesüsteemide tehniline arendamine ja haldamine ning info- ja sidetehnoloogiaalaste teenuste pakkumine. RIK haldab ja arendab mitmeid riigile ja kodanikule olulisi registreid ja infosüsteeme. Sealhulgas on nii e-Äriregister, e-Notar ja e-Kinnistusraamat kui ka mitmed õigusalased infosüsteemid (kohtuinfosüsteem, elektrooniline järelevalve ennetähtaegselt vanglast vabanenutele, kriminaalhooldusregister, riiklik kriminaalmenetlusregister, kinnipeetavate register, e-Toimik, e-RT jt). RIKi kulud kaetakse riigieelarvest ja majandustegevusest laekuvast tulust. Asutuses töötab ca 160 inimest. RIK valiti valimisse, kuna pakub sisejulgeoleku valdkonnaga puutumuses olevaid talitluspidevuskriitilisi teenuseid.

Häirekeskus on Siseministeeriumi valitsemisalas asuva Päästeameti halduses olev valitsusasutus, mille ülesanne on hädaabiteadete ning abi- ja infoteadete menetlemine.

Häirekeskuse põhiülesanne on siiski vastata ja reageerida üleriigilisele hädaabinumbrile 112, mis peab olema alati kättesaadav. Häirekeskuse koosseisus on 173 ametikohta. (Häirekeskus… 15.03.2011)

Alates 2010 aastast pakub Häirekeskusele IKT teenust SMIT. Häirekeskus on valimis oluline, kuna sarnaselt PPA-le peab põhitegevuses tagama katkematu töö ning infosüsteemid on olulisel määral seotud tööprotsessiga.

Maksu- ja Tolliamet on Rahandusministeeriumi valitsemisala asutus, kelle seadusjärgne roll ühiskonnas on tõhus ja täpne maksude haldamine, ettevõtluse hõlbustamine ning ühiskonna ja seadusliku majandustegevuse kaitsmine (Maksu- ja Tolliamet… 15.03.2011). Maksu-ja Tolliametil on neli piirkondlikku regiooni. IT haldust sisse ei osteta ning hooldustöid ja *helpdeski* teenust pakub asutus ise. Maksu- ja Tolliamet on valimis, kuna analoogselt PPA-le on ka neil kriitilisi IKT teenuseid, mis peavad 24/7 toimima, et amet saaks oma põhiülesannet täita.

G4S kuulub rahvusvahelisse kontserni, mille põhitegevusalaks on turvateenuste osutamine. G4S Eesti esindused asuvad Tallinnas, Tartus, Pärnus ja Jõhvis. G4S Eesti kontserni aastakäive on ligi üks miljard krooni ja töötajate arv ligi 3100. G4Sil on üle 45 000 püsikliendi. G4Sile kuulub hinnanguliselt 49% Eesti turvaturust ja 65,1% Eesti valveteenuste turust. (G4S… 15.03.2011)

G4S ostab sisse osaliselt IKT teenust, ise pakuvad esmast IT abi oma inimestele ehk *helpdeski* teenust. G4S on valimis, kuna põhitegevus on ajakriitiline ja seetõttu peab kasutatavate infosüsteemide talituspidevus olema tagatud. Töö katkemine tähendab otseselt klientide usalduse vähenemist ning majanduslikku kahju.

Telekommunikatsiooni ettevõte[2] ca 350 töötajaga. IKT haldust pakuvad valdavalt ise, kuid suuremad arendused ostetakse sisse. Talitluspidevus baseerub toetaval taristul ja

[2] Intervjueeritav ei soovinud ettevõtte nime magistritöös kajastada. Kohtumise ülestähendused ja helisalvestis on magistritöö autori valduses. Viitamaks ettevõttele kasutatakse magistritöös läbivalt telekommunikatsiooni ettevõte ja konkreetselt intervjueeritavale IT juht.

infosüsteemidel ning nende töö katkemine tähendab samuti klientide arvu vähenemist ja majanduslikku kahju.

Intervjueeritavate andmed on toodud Tabelis 4. Intervjuud viidi läbi veebruaris- märtsis 2011. Intervjuu küsimused on toodud Lisas 3.

Tabel 4. Intervjueeritavate nimed ja ametikohad (allikas: autor)

ETTEVÕTE	INTERVJUEERITAVA NIMI	INTERVJUEERITAVA AMETIKOHT
Justiitsministeerium	Hettel Varik	Infosüsteemide ja tööprotsesside talituse juhataja
RIK	Martti Allingu	Sisekontrolli ja infoturbe talituse juhataja
Häirekeskus	Eva Rinne	Arendusosakonna juhataja
Maksu- ja Tolliamet	Katrin Holm	Süsteemihooldusosakonna tugi- ja monitooringu talituse juhataja
G4S	Andrus Jauk	Infotehnoloogia divisjoni direktor
Telekommunikatsiooni ettevõte	XX	IT juht

2.2. IKT katkestuse hindamise mõjurid

Magistritöö eesmärgi saavutamiseks, ning arvestades teoreetilises peatükis saadud tulemusi, grupeeris autor intervjuude käigus esitatud küsimused nelja põhikategooriasse

- kas protsessid on kaardistatud ning neile omanikud määratud? kas on sõlmitud teenustaseme kokkulepped (SLA)?
- kas ettevõttes on võimalik tööd ümber korraldada, kui infosüsteem ei tööta?
- kas ja kuidas mõõdab asutus IKT katkestuse mõju põhitegevusele? kuidas ettevõte saadud tulemusi kasutab?

- kas asutused peavad IKT katkestuse hindamise metoodikat vajalikuks? Mis on/oleksid olulised mõõdikud IKT katkestuse mõju hindamiseks?

Empiirilise uuringu esimese sammuna uuris magistritöö autor asutuste IKT toimimise põhimõtteid, kuna katkestuse mõju ei saa vaadelda ilma taustsüsteemi tundmata.

Justiitsministeerium ja Häirekeskus tellivad nii IKT halduse kui ka arenduse teenust sisse selleks loodud riigiasutustelt, mis on vastavalt RIK ja SMIT. RIK oli ka antud magistritöö valimis ning nemad ostavad osaliselt arenduse teenust sisse, kuid halduse teenust pakuvad ise kogu Justiitsministeeriumi valitsemisalale.

Maksu- ja Tolliamet, G4S ja telekommunikatsiooni ettevõte pakuvad esmast IT abi *helpdeski* kujul ise ning sisse ostetakse suuremahulisemad arendustööd. Ärikriitilised infosüsteemid on jäetud ettevõttesse ning kui kriitilise vea parandusega ise hakkama ei saada, alles seejärel kaasatakse välispartner (reeglina on sõlmitud selleks raamlepingud).

Intervjuu käigus kaardistas magistritöö autor ka asutuste infosüsteemide arvu ning nende jagunemise tugiprotsesside ja põhiprotsesside toetamise alusel. Paraku saadud tulemuse alusel järeldusi teha ei saa, kuna intervjueeritavad märkisid, et jaotus põhiprotsesse ja tugiprotsesse toetavate infosüsteemide vahel on valdavalt tunnetuslik ning konkreetset eristust raske teha. Hinnanguliselt oli valimi asutustes 1/3 tugiprotsesse ja 2/3 põhiprotsesse toetavad infosüsteemid. Erandiks oli G4S, kellel jagunesid infosüsteemid võrdselt põhiprotsesside ja tugiprotsesside vahel, mõlemaid oli kaheksa.

Kas protsessid on kaardistatud ning neile omanikud määratud? Kas on sõlmitud teenustaseme kokkulepped (SLA)?

Ainukestena valimi ettevõtetest tõdesid Maksu-ja Tolliamet, Häirekeskus ja G4S, et neil on põhiprotsessid kaardistatud. Häirekeskus lõpetas selle tööga 2010. aastal ning kõik põhiprotsessid said kirja ja teenustena kirjeldatud ja igale protsessile on omanik määratud (Rinne 2011). G4S rakendab ISO 9001:2008 standardit ning sellega seoses on nii IT valdkond kui ka klienditeeninduse protsessid kaardistatud. Protsessidena on välja

joonistatud samm-sammult, kuidas käib häire vastuvõtmine või kliendiga lepingu sõlmimine. Omanik on määratud äripoolelt ning temaga IT küsimustes suhtleb rakenduse haldur. (Jauk 2011)

Maksu-ja Tolliametil on põhiprotsessid kaardistatud, kuid kõik protsessid ei ole veel kirjeldatud teenustena. Omanikud on protsessidele siiski üldjuhul määratud. (Holm 2011)

Telekommunikatsiooni ettevõte tõdes, et neil on valdavalt klienditeeninduse protsessid kaardistatud ja suund on see, et kaardistada kõik äriprotsessid ning määrata neile omanikud (praegu on veel olukordi, kus kõigil protsessidel ei olegi üheselt määratud omanikku). Justiitsministeerium ja RIK märkisid, et tööprotsessid ei ole kaardistatud, kuid üldine teadmine on olemas ning IKT teenuse toimimiseks vajalik info on kirjeldatud teenustaseme kokkulepetes.

Teenustaseme kokkulepete olemasolu kinnitasid Häirekeskus ja Justiitsministeerium, mis on põhjendatav sellega, et mõlemad asutused tellivad IKT teenust väljast sisse ning see eeldab kokkulepete olemasolu (juba asutuste sisemistest regulatsioonidest lähtuvalt). Häirekeskus märkis, et nemad teenusaseme kokkuleppe sõlmimisel siiski mõtet ja lisandväärtust ei näe, kuna vastav kokkulepe ei taga neile teenust nõutaval tasemel. SMIT pakub teenust madalamal tasemel, kui on Häirekeskusele tulenevad nõuded, seega on dokument eriarvamustega allkirjastatud ning sisupool ei ole rahul saadava teenusega (Rinne 2011).

Magistritöö autor antud juhul Rinne märkusega nõustuda ei saa, kuna teenustaseme kokkulepe määrab ära üldised teenuse pakkumise alused ning pakutava teenuse parameetrites tuleks siiski kokku leppida, kasvõi lisada märkus, mis ajal klient saab tema oodatud tasemel teenust. Eelmises peatükis tutvustatud teenustaseme kokkuleppe sõlmimise põhimõtete kohaselt tuleks siiski mõlemaid osapooli rahuldav kokkulepe saavutada, kuna dokumendi põhirõhk on kokkuleppel ning mõlema osapoole jaoks selgelt defineeritud mõõdetavates tulemites.

Justiitsministeeriumist Varik (2011) kinnitab SLA sõlmimise vajalikkust, kuna omanik osaleb selle kokkuleppimisel ning näeb, mis on tema teenuse jaoks nõutav kriitiline piir ning seega peab arvestama kaasnevate rahaliste kohustustega, kuna mida kõrgem käideldavus, seda kallim on reeglina süsteemi üleval pidada.

Maksu- ja Tolliametist Holm (2011) rõhutab samuti SLAde sõlmimise vajadust, kuid praegu on neil sõlmitud alles üksikud kokkulepped. Positiivsena peab autor vajalikuks rõhutada, et Maksu-ja Tolliametil on sõlmitud ka maja-sisesed SLAd, kuigi need on alles üksikud ja mitte väga oluliste põhiteenuste kohta. Kuid Holm (2011) märkis, et neil kehtivad Euroopa Liidu poolt kehtestatud SLAd konkreetsetele rakendustele, kus on Euroopa Liiduga sõnumivahetus ööpäevaringselt.

G4S-il on sõlmitud teenustaseme kokkulepped nelja infosüsteemi osas, need määravad ära, mis teenust nad ootavad väliselt partnerilt. Sisemiselt nad SLA-de sõlmimise vajadust ei näe, sest IT osakonna tagatavate süsteemide töö on sätestatud osakonna põhimääruses, mis on juhatuse otsusega kinnitatud, seega eraldi kokkuleppe sõlmimine sisupoolega enam midagi juurde ei anna. Jauk (2011) märkis, et kriitilisematele olukordadele lähenetakse juhtumi põhiselt (*case by case*) ning juhtkond langetab otsuse edasise käitumise osas. Mingeid eraldi reeglistikke selleks pole ning nad ei näe ka selle järele vajadust.

Telekommunikatsiooni ettevõtte esindaja rõhutas samuti, et väliste partneritega on SLA-d kokku lepitud, kuid ärikriitilisemad infosüsteemid on asutusse jäetud. Seal toimub töö sisemiste kokkulepet alusel ning seda tehakse läbi intsidendi haldamise protsessi. Vajadusel kaasatakse juhtumi lahendusse juhtkond, kuid see sõltub eelkõige mõjutatud klientide arvust.

Kas asutuses on võimalik tööd ümber korraldada, kui infosüsteem ei tööta?

Kõik valimisse kuuluvad asutused kinnitasid, et neil on vajadusel võimalik tööd ümber korraldada, kui infosüsteem ei tööta, kuid seda ei peeta alati ratsionaalseks ja mõistlikuks. Pigem tuleb hinnata reaalselt, millal infosüsteem tööle hakkab ja kui äärmisel juhul on vaja, siis kriisikomisjoni otsuse alusel minnakse üle paberitööle (IT juht 2011). Töö

korraldatakse kindlasti koheselt ümber teenuste puhul, kus ei saa katkestusi lubada, näiteks kriitiliste objektide valves, kus saadetakse kohale mehitatud valve (Jauk 2011) või inimestelt hädaabi kõnede vastu võtmine ja vajaliku info üleskirjutamine ettevalmistatud vormidele (Rinne 2011).

Klienditeeninduses (Jauk 2011; IT juht 2011) võetakse pigem kliendi number ja helistatakse talle tagasi või vabandatakse ja palutakse paari tunni pärast uuesti teenindusse pöörduda, va juhtumid, mis nõuavad koheselt tegutsemist (näiteks mobiiltelefoni numbri sulgemine).

Kõik asutused tõid välja, et erinevalt vaadatakse sise- ja väliskliente ning põhi- ja tugiprotsesse toetavaid infosüsteeme. Kriitilisemalt jälgitakse ja monitooritakse väliskliente mõjutavaid protsesse, negatiivne info väljapoole mõjutab ettevõtte usaldusväärsust ning sellel on otsene seos müügitulemustega. Tugiprotsesse toetavad infosüsteemid on asutuse sisemiseks toimimiseks vajalikud ning seega ei ole vajalik niivõrd kõrgeid käideldavuse nõudeid sätestada. Asutuse enda puhul saab IT osakond selgitustööd teha ja rahustada inimesi ning öelda, mis ajaks olukord paraneb.

Kuuest küsitletud asutusest viis vastasid, et rakendatakse ITILi põhimõtteid, mida kohandatakse vastavalt asutuse spetsiifikale. G4S tõdes, et nemad rakendavad ISO 9001:2008 standardile vastavat emaettevõtte poolt väljatöötatud infoturbepoliitikat.

Kõik asutused tõdesid, et neil on ärikriitilisemate infosüsteemide taasteplaanid, kust selgub, mida tuleb teha probleemi ilmnemisel ja kuhu on vajalik pöörduda. Maksu- ja Tolliameti, RIKi, G4Si ja telekommunikatsiooni ettevõtte esindajad kinnitasid, et neil on olemas monitooringusüsteemid, mille alusel saab jälgida infosüsteemi tööd ja tekkivate katkestuste hulka. Justiitsministeeriumil ja Häirekeskusel eelpool mainitud tehnilist lahendust ei ole, kuna nemad ostavad IKT teenust sisse ning vastavad monitooringusüsteemid on olemas RIK-is ja SMIT-is.

Infosüsteemide põhiparameetrid ja kriitilisuse aste on igas asutuses küll määratud, kuid rakendatud asutustes erinevalt, nt Justiitsministeeriumis, Häirekeskuses, RIK-is on see

määratud SLA-s ning Maksu- ja Tolliametis, G4S-is, telekommunikatsiooni ettevõttes sisemises dokumendis.

Telekommunikatsiooni ettevõte juurutab ITIL-it ning neid põhimõtteid kasutades oli välja töötatud intsidendi haldamise protsess, mis jagab tekkinud intsidendi viieks kategooriaks, kus esimene kategooria on ülikriitiline ning viies kategooria kõige madalam. Eelpool nimetatud kategooria määramiseks teeb juhtimiskeskus mõjuanalüüsi ning määrab intsidendile vastava kategooria. Vastavalt saadud kriitilisuse astmele tegutsetakse, kas tullakse öösel kodust välja või kannatab järgmise päevani oodata (IT juht 2011). Mõjuanalüüs baseerub eelkõige mõjutatud klientide arvule. Sama põhimõtet kriitilisuse määramiseks soovitab kasutada ka eelmises peatüki kajastatud ITILi intsidendi halduse protsess.

Kas ja kuidas ettevõte mõõdab IKT katkestuse mõju põhitegevusele? Kuidas ettevõte saadud tulemusi kasutab?

Kõik vastajad tõdesid, et IKT katkestuse ametlikku definitsiooni kellelgi sätestatud ei ole, kuid siiski olid arvamused katkestuse mõiste kohta valdavalt ühesugused. IKT katkestus on olukord, kus infosüsteem ei tööta, kliendid ei saa seda eesmärgipäraselt kasutada ning teenus pole kättesaadav (Rinne 2011; Varik 2011; Allingu 2011). Ainukesena lisas mõiste selgitusse juurde ajavahemiku Jauk (2011), kes märkis, et katkestus on see, kui töö on häiritud 60 minutit. Põhjendades selgitust asjaoluga, et sellisel juhul annab nende sisemine katkestuste halduse süsteem häire kokkulepitud isikute ringile, kellele tuleb teade meilile ja mobiiltelefonile. Üldiselt on 60 minutit katkestust selline aeg, kus tema IT-juhina sekkub, et probleem saaks kiirema lahenduse. Kõik lühemad intsidendid lahendatakse jooksvalt ning katkestuse nimetuse alla ei lähe, kuigi ka intsidentide osas käib jälgimine ja monitooring. Teised intervjueeritavad sellist eristust välja ei toonud.

Kokkuvõtvalt saab väita, et IKT katkestus on olukord, kus kliendid (sh sisekliendid) ei saa infosüsteemi kasutada ning pakutav teenus ei toimi. Katkestused jagunevad omakorda plaanilisteks ja planeerimata katkestustest ning antud magistritöö raames huvitab autorit planeerimata katkestused ning nende mõju teenuse kasutajate põhitegevusele. Planeeritud

katkestusi üritatakse üldjuhul teha ajal, millal see mõjutab põhitegevust võimalikult vähe ja see toimub kokkuleppel IT osakonna/teenuse pakkujaga ning sellisel juhul ei ole vaja reeglina hinnata mõju põhitegevusele.

IKT katkestuste üle peavad arvestust kõik valimis olevad asutused, seda tehakse kas IKT teenuse pakkujalt küsitud väljavõtte alusel või infotehnoloogiliste monitooringusüsteemide abil ning täiendavalt vaadatakse juurde intsidentide arvusid (G4S ja telekommunikatsiooni ettevõte).

Maksu- ja Tolliamet, Justiitsministeerium ja Häirekeskus tõdesid, et nemad IKT katkestuse mõju põhitegevusele ei hinda ning rahalisse vääringusse ümber ei arvuta. Varik (2011) märkis täiendavalt juurde, et RIK esitab neile teenuse katkestuse korral juhtumianalüüse olnud intsidentidest, kuid sisus on see pigem toimunud sündmuse faktide väljatoomine ning kaitsemehhanismi loomine sarnase olukorra teistkordseks ärahoidmiseks, sest tekkinud kahju rahasse ümber ei arvutata.

Jauk (2011) märkis, et G4S mõõdab IKT katkestuste mõju. Nad teevad juhtumianalüüse suurematest katkestusest, mis on olnud. Kaardistavad tekkinud probleemid, põhjused ja töötavad välja lahendused, kuidas neid probleeme edaspidi vältida. Suuremad probleemid olid vahepeal pikaajalisem elektri- ning andmesidekatkestus, kuid probleemidest räägiti juhtkondade tasemel ning G4S tegi ka oma maja siseselt teatavad järeldused ning töötas välja täiustatud varuplaanid, kuidas neid asju edaspidi vältida. Konkreetselt iga katkestust rahalisse väärtusesse ei arvestata. Vajadusel arvutatakse välja konkreetsed kulud (otsesed kulud), mis olid seotud katkestusega ning seejärel oleneb kulu iseloomust, kas see kantakse kulusse või tehakse partneriga tasaarvelduse, kui katkestus oli tingitud partneri süül.

Telekommunikatsiooni ettevõte iga katkestuse puhul ei pea vajalikuks mõõta IKT katkestuse mõju põhitegevusele, kuid vajadusel saavad nad hinnata seda läbi mõjutatud klientide arvu ning kui kaua katkestus kestis. Rahalisse vääringusse nad seda reeglina ei pane, kuigi oleks võimalik arvutada välja katkestuse rahaline maksumus keskmiste teenuste hindade baasil. Juhtimisotsused langetatakse reeglina mõjutatud klientide arvu alusel.

Allingu (2011) märkis, et nemad ei mõõda põhjalikult IKT katkestuse mõju põhitegevusele, pigem antakse hinnang katkestusele SLA-s kokkulepitud tingimuste põhjal (kui kriitiline ja kui palju aastas lubatud planeeritud ja planeerimata katkestusi). Ta nentis, et saamata jäänud tulu on võimalik hinnata infosüsteemide osas, mida nad müüvad väljapoole. Kuna RIK ei saa raha ainult riigieelarvest, vaid teenib tulu ka oma teenuste müügilt, mistõttu on teatud teenuste katkemise korral võimalik saamata jäänud tulu selgelt välja arvutada. Asutuse siseselt tehakse iga kuu ülevaateid müükidest ning kui on toimunud ulatuslikumad katkestused, siis on neist võimalik märgata rahaliste vahendite langust ning selle kaudu tuletada katkestuse rahaline mõju RIK-ile.

Kõik valimis olevad asutused teadsid elutähtsa teenuse toimepidevuse riskianalüüsist, kuid selle metoodika rakendamist IKT katkestuste ja mõju mõõtmiseks põhitegevusele ei pidanud ükski intervjueeritav mõistlikuks ja otstarbekaks. Põhjus oli kindlasti ka asjaolus, et tegemist on veel niivõrd uue nõudega ning asutused ei oska sellest endale kasu näha, vaid tajuvad pigem uut bürokraatlikku kohustust.

Eeltoodust magistritöö autor järeldab, et kõik asutused küll jälgivad katkestuste arvu ning eraettevõtted hindavad ka katkestusega seotud reaalselt tekkinud kulutusi ning kasutavad saadud järeldusi juhtimisotsuste tegemiseks. Antud magistritöö raames uuritavalt IKT katkestuse mõju põhitegevusele koos otseste ja kaudsete kuludega ükski valimis olev ettevõte ei mõõtnud.

Kas asutused peavad IKT katkestuse hindamise metoodikat vajalikuks? Mis on/oleksid olulised mõõdikud IKT katkestuse mõju hindamiseks?

Jauk (2011) peab G4S-is tehtavat katkestuste hindamist vajalikuks. Esmalt analüüsivad tekkinud intsidente ning püüavad parandada tekkinud vigu (kas siis riistvarast või süsteemist tingituna). Kui on suurem probleeme, mis vajab investeeringuid, siis läheb tema seda nõukogu ette kaitsma, et rahalisi vahendeid saada. Juhtkonnale tuleb ära näidata, mis sellest muutub, mis läheb klientide jaoks paremaks ja kuidas firma sellest tervikuna kasu saab. Samas ta möönab, et konkreetset metoodika neil selleks välja töötatud ei ole, kuid

olemasolev otseste kulude analüüs on parandanud IKT valdkonna tulemuslikkust ning aidanud prioritiseerida investeeringu vajadusi.

Kõik vastanud tõdesid, et ühest metoodikat IKT katkestuste mõju hindamiseks välja töötatud ei ole. Rinne (2011) ja Allingu (2011) pidasid metoodika välja töötamist vajalikuks, kuna see võimaldaks paremini kulutusi hinnata (sh ka personali) ja tulemused oleksid aluseks SLA-de sõlmimisele. Holm (2011) pidas samuti katkestuse mõõtmist põhitegevusele vajalikuks ning lisas juurde, et see aitaks parandada IT teenuste taset. Varik (2011) möönis, et katkestusest tulenevat mõju on väga raske rahasse ümber arvestada, kuna teenuse mittetoimimisega võib tihtipeale kaasneda ka mittevaraline kahju (nt kahju teenuse või teenust pakkuva asutuse mainele), mis ei pruugi olla rahas mõõdetav või tööde kuhjumisest tekkinud ülekoormus peale IKT teenuse normaliseerumist, ning jäi kahtlevale seisukohale, kas taoline arvutustulemus võiks omada teenuse toimimises olulist lisandväärtust. IT juht (2011) ei välistanud metoodika vajalikkust, kuid arvas, et nemad saavad praegu hakkama, kui hindavad ainult mõjutatud klientide arvu ja katkestuse ajalist kestust.

Rinne (2011) märkis, et metoodika loomisel on oluline, et see oleks lihtne ja arusaadav. Kui on vaja täita lehekülgede viisi pabereid ja see tekitab bürokraatiat juurde, siis väljapakutav metoodika rakendust ei leia.

Metoodika loomisel tõid intervjueeritavad välja järgmised mõjurid, mida tuleks arvestada:

- inimeste tööaeg (sh aeg, kui nad ei saa oma tööd teha);
- inimeste töötasu (kui tuleb täiendavalt inimesi tööle kutsuda);
- kahju riigile/erasektorile (saamata jäänud tulu);
- maine kahju;
- kommunikatsioonikulud katkestustest teavitamiseks;
- otsekulud, mis tekivad seoses katkestusega;
- ärikriitilisus.

Intervjuude põhjal saab välja tuua, et üldjuhul erasektor ei pea vajalikuks reglementeerida IKT valdkonna teenuse osutamist, kuna on olemas raamdokumendid ja taasteplaanid, mis

panevad paika süsteemide ärikriitilisuse. Esmased tegevussuunad katkestuste korral on kirja pandud ja määratud teavitatavate inimeste ring, kuid keerukamad või suuremaid kliente puudutavad juhtumid lahendatakse *case by case*. Siit tuleb ilmekalt välja, et erasektor on infosüsteemide katkestuste hindamisel ja nendest tulenevate probleemide lahendamisel palju paindlikum, kui riigiasutus.

Katkestuste hindamisel erasektor määratleb tekkinud otsekulud, kaudseid kulusid valimis olevad ettevõtted üldjuhul ei hinda. Tekkinud kuludest olulisem on katkestusest mõjutatud kliendibaas ning infosüsteemi ärikriitilisus, sellisel juhul tegutsetakse viivitamatult. Edaspidiste vigade vältimiseks püütakse tuvastada vea põhjus (kui see on korduv) ning vajadusel minnakse nõukogu/juhatuse ette kaitsma vajaliku investeeringu jaoks saadavat summat.

Riigiasutuste puhul IKT katkestuse mõju üldjuhul ei mõõdeta (sh ka tekkinud otsekulusid), pigem keskendutakse seirele ning monitooritakse katkestuste arvu. Justiitsministeerium ja RIK tõid välja infotehnoloogilise monitooringu süsteemi ning Justiitsministeeriumi juures tegutseva infoturbe juhtrühma, kus vaadatakse kvartaalselt läbi suuremad katkestused RIK-i ettevalmistatud materjalide põhjal, kuid katkestusest tekkinud kahju need materjalid üldjuhul ei sisalda, vaid kätkevad endas põhjuste analüüsi ja ettepanekut, kuidas tulevikus sarnastel eelustel samast olukorda ära hoida ja/või riskitegureid vähendada/maandada. RIK-i ettekande alusel seab ministeerium prioriteetsed arengusuunad, mille edendamisse raha suunata.

Siseministeeriumi valitsemisalas (Häirekeskus) on intsidentide/katkestuste monitoorimine tehniliselt SMITi ülesanne, sisupool saab anda tagasisidet katkestustest ainult kasutajatelt saadud info põhjal. Eraldi juhtrühma või nõukogu selleks Siseministeeriumi valitsemisalas ei ole, et hinnata katkestuste mõju põhitegevusele ning selle alusel teha otsuseid infosüsteemide arendusteks.

2.3 IKT katkestuse mõju hindamise metoodika Politsei- ja Piirivalveametis

PPA loodi 01. jaanuaril 2010 Politseiameti, Keskkriminaalpolitsei, Julgestuspolitsei, Piirivalveameti ning Kodakondsus- ja Migratsiooniameti ühendamisel. Politseiprefektuuride, piirivalvepiirkondade ja KMA regionaalsete büroode baasil moodustus neli territoriaalselt prefektuuri. PPA põhiülesanne on Euroopa välispiiri tagamine; kodakondsuse määratlemine, dokumentide väljastamine; turvalisus ja avalik kord riigi sees; kuritegude menetlemine ja ennetamine. PPA-s on umbes 7000 ametikohta, millest 6000 on põhitöö valdkondades ja 1000 administratsiooni valdkonnas ning ühendasutuse loomisega on PPA muutunud Eesti suurimaks riigiasutuseks. IKT võimekust alates 01. jaanuarist 2010 PPA-s enam ei ole ning IKT teenust pakub tervikuna SMIT.

Magistritöö autor töötab käesoleval ajal peadirektorile alluvas koordinatsioonibüroo arendustalituses, mis koordineerib PPA tervikvaates IKT rakendamist, IKT sisulist arendust, haldust ja teenuste tellimist ning on põhipartneriks SMIT-iga suhtluses. Seega on autoril olemas ülevaade IKT valdkonna korraldamisest PPA-s ning eraldi intervjuud PPA IKT valdkonna töökorralduse uurimiseks läbi ei viidud.

PPA-s on 29 põhiprotsessi ning 20 tugiprotsessi toetavat infosüsteemi (väiksemaid rakendusi siin eraldi välja toodud ei ole). PPA-le pakub nii halduse kui ka arenduse IKT teenust SMIT, seega on vajalik vastavalt kehtestatud põhimõtetele (Info- ja kommunikatsioonitehnoloogia valdkonna teenuse osutamise üldtingimused, siseministri 21.12.2009 käskkiri nr 236L) (edaspidi Teenuse osutamise üldtingimused) teenustaseme kokkulepete olemasolu. Teenustaseme kokkulepete sõlmimine PPA ja SMIT-i vahel magistritöö kirjutamise ajal käib, kuid valdavalt põhiprotsesse toetavate infosüsteemide osas on teenustaseme kokkulepped juba sõlmitud. Vältimaks võimalust, et mõnede teenustaseme kokkulepete kavandid võivad seisma jääda koostamise faasi või ära ununeda, on peadirektor sätestanud (Teenuste tehnilise kirjelduse koostamine, peadirektori 23.02.2011 korraldus nr 31), et kõik asutuse teenustaseme kokkulepped peavad sõlmitud olema hiljemalt 30.06.2011.

Põhiprotsessid ei ole PPA-s täielikult ja ühetaoliselt kaardistatud, kuid teadmine on põhivaldkondades olemas ning hetkel ei ole lihtsalt jõutud kõike dokumentaalselt vormistada. Põhiprotsesside toetamiseks vajalikud infovarad (magistritöös on mõisted infovara ja infosüsteem kasutusel sünonüümidena) on kaardistatud ning nendele omanikud ja tootejuhid määratud. Vastav loetelu on kinnitatud ning seda uuendatakse regulaarselt mõne tootejuhi nime või infovara tehniliste näitajate muutumisel (Infovarade loetelu ja infosüsteemi pidamise korra vormi kinnitamine, peadirektori 24.05.2010 käskkiri nr 241).

Igale infovarale tuleb vastavalt Teenuse osutamise üldtingimustele määrata teenuse kvaliteedi parameetrid: ISKE turvaklass, teenuse ärikriitilisuse ning teenuse tööaja klass, andmete taastamise aeg ning maksimaalne aktsepteeritav andmekadu. Ärikriitilisuse määrab sisupool ning see on vahemik ühest kuni neljani, kus üks on kõike ärikriitilisem (teenuse mittetöötamine peatab organisatsiooni poolt osutatava avaliku teenuste osutamise suurel märal või osaliselt) ning neli on kõige vähem ärikriitiline (teenuse osutamine ei mõjuta oluliselt teiste teenuste toimimist) teenus. Tööaeg on ajavahemik, millal peab teenus kättesaadav olema. Tööaeg on jaotatud klassideks järgnevalt A: E-P:00-24.00 (24/7), B: E-R 7.00-22.00, C: E-R 8.00-18.00. Nimetatud mõisted on defineeritud Teenuse osutamise üldtingimuste käskkirjas.

Eelpool märgitud parameetrid tuleb SMIT-iga kokku leppida ning kajastada teenustaseme kokkuleppes. Paraku on nende tingimuste kokkuleppimine komplitseeritud, sest infrastruktuur ja tarkvara on vananenud ning SMIT ei suuda sisupoolele vajalikku ja nõutavat töökindlust tagada. Seega lisatakse teenustaseme kokkuleppesse alati märkus, mis ajaks SMIT esitab tegevuskava, kuidas ja mis ajaks sisupoolele vajalikud nõuded tagatakse.

PPA infoturbepoliitika põhimõtetes on sätestatud, et kriitilisemate süsteemide jaoks peavad olema välja töötatud talituspidevuse plaanid, mida tuleb pidevalt testida ning jälgida ja muudatused infosüsteemides tuleb seal kajastada (Infoturbepoliitika põhimõtted asutuses, peadirektori 01.01.2010 käskkiri nr 46).

Seega töö ümberkorraldamise võimalus IKT katkestuse korral sõltub suuresti pakutava teenuse iseloomust ja iseärasustest ning valdkonniti on see PPA-s erinev.

Piirivalve valdkonnas on põhiliseks tegevuseks piirikontroll ning seal ei ole üldjuhul võimalust tööd ümber korraldada. Kolmandatest riikidest pärit kodanike andmeid on vaja andmebaasidest kontrollida ning isikusamasus tuvastada. Ilma vastavaid päringuid tegemata (näiteks Schengeni Infosüsteemist) ei ole võimalik inimest riiki lubada. Seega on piirivalve valdkonnas väga oluline läbi mõelda IT tehniline lahendus piirikontrolli infosüsteemi töötamisel, kuna sobiva tehnilise lahenduse kaudu on võimalik probleemi ennetada. Tagajärgedega tegelemine on antud valdkonnas palju raskem ning sisupoole töö ümberkorraldamise võimalus praktiliselt puudub. Piirikontrolli infosüsteemi tõrgeteta töö tagamiseks on loodud lokaalserverite süsteem ning sel viisil püütakse minimaliseerida katkestustest tekkivat mõju piirikontrollile ja vältida võimalikke järjekordi piiril.

Kriminaal- ja korrakaitsepolitsei valdkonnas oleneb ametniku tehtava töö spetsiifikast töö ümber suunamise võimalus. Kui patrullpolitseiniku päringusüsteem ei tööta, siis vajadusel on võimalik raadiosidet või mobiiltelefoni sidet kasutades helistada juhtimiskeskusesse, et kontrollida isiku andmeid. Üldjuhul saab see olla ajutine lahendus ning hädapäraste kontrollide puhul, reeglina infosüsteemi töö katkestuse korral lauskontrolli ei tehta. Menetlejad saavad üldjuhul infosüsteemi katkestuse korral oma tööd ümber korraldada ning sisestada nõutud andmed hiljem, kuigi see on ebamugav ja tülikas, eriti kui kodanik on mingi põhjusel kohale kutsutud. Kõige kriitilisemad infosüsteemid korrakaitsepolitsei valdkonnas on OPIS (operatiivjuhtimise infosüsteem, mida kasutatakse politsei hädaabinumbrile laekuvate kõnede registreerimiseks ja haldamiseks ning operatiivsete ressursside juhtimiseks), seejärel ORANGE (kõnehaldussüsteem politsei hädaabinumbrile laekuvaste kõnede vastuvõtmiseks) ning m-KAIRI (politseisõidukites kasutatav mobiilne päringute tegemise ja maakaardiga seotud funktsionaalsusi sisaldav rakendus). Kõigi nende kolme üheskoos või üksikult maha kukkumise tõttu on politseiline tegevus ja operatiivsus tugevasti häiritud. Näiteks politsei juhtimiskeskuses on võimalik väljakutseid vastu võtta ja reageerida ka infosüsteemi kasutamata nö paberil, ent see on oluliselt aeglasem, ressurssidest puudub ülevaade ning nõuab täiendavat tööjõudu.

Kodakondsus- ja migratsiooni valdkonnas on kriitilisemaiks teenused, mis on seotud inimeste teenindamise ja dokumentide väljastamisega. Juhul, kui UUSIS (kodakondsus- ja migratsiooni valdkonna menetluse infosüsteem) ei tööta (ei saa sisse logida, on aeglane, jookseb kinni), tuleb klientidel taotlused täita käsitsi (praegu täidab ametnik esiteks arvutis kliendilt küsides ning pärast prindib välja ja laseb kontrollida andmete õigsust ning allkirjastada) ning ametnikul tuleb sisestada ankeedid hiljem infosüsteemi. Kui infosüsteem ei tööta, ei ole võimalik kontrollida ka riigilõivu laekumisi, siduda taotlusega fotoboksis tehtud fotot (vajalik ka kontrollida, kas foto on nõuetekohane) ega reisidokumendi taotlemisel hõivata sõrmejälgi. Erinevad puudused ilmnevad hiljem taotluse sisestamisel, mistõttu võib juhtuda, et taotleja tuleb tagasi kutsuda puuduste kõrvaldamiseks. See põhjustab inimestes rahulolematust ning võib tekitada negatiivset meediatähelepanu. Samuti ei ole võimalik infosüsteemi tõrgete korral taotletud dokumente kliendile väljastada, st süsteemis märkida kehtivaks, ning tuvastada, kas dokument kuulub kliendile.

Tugivaldkonda toetavad infosüsteemid on koondatud administratsiooni alla ning need puudutavad eelkõige ameti toimimiseks vajalike tegevuste tagamist. Siia kuuluvad näiteks töövahendite tellimine, palga maksmine, tööaja arvestus ning e-maili teenus. Kui mõni infosüsteem on maas tugiprotsesside osas, siis see tekitab ärritust sisekliendis, kuid reeglina ei takista see PPA-l avalikku teenust pakkumast. Lisaks on võimalik osades infosüsteemides tööd ümber korraldada ja vajadusel spetsiaalsetel vormidel (paberil) arvestust pidada ning kui infosüsteemi töö taastub, saab sisestada vajalikud andmed infosüsteemi (näiteks laoarvestus). Selline olukord ei saa kesta pikalt (olenevalt süsteemist tunde või mõned päevad), kuid ajutiselt on see lahendus aktsepteeritav.

Peatükist 2.2 järeldus, et intervjueeritavad tõid välja järgmised mõjurid katkestuse hindamiseks:

- inimeste tööaeg (sh aeg, kui nad ei saa oma tööd teha);
- inimeste töötasu (kui tuleb täiendavalt inimesi tööle kutsuda);
- kahju riigile/erasektorile (sh saamata jäänud tulu);
- maine kahju;
- kommunikatsioonikulud katkestustest teavitamiseks;

- otsekulud, mis tekivad seoses katkestusega;
- ärikriitilisus.

Magistritöö autor uuris täiendavalt kolmelt PPA-s infovaradega tegelevalt ametnikult, mida tuleks lisada või eemaldada PPA näitel eelpool toodud nimekirjast. Küsimustele vastasid korrakaitsepolitseiosakonna arendusbüroo infovarade talituse juht Imre Kollo, kriminaalpolitseiosakonna arendusbüroo juhtivkriminaalametnik Sergo Eelmäe ja piirivalveosakonna arendusbüroo infovaradetalituse vanemspetsialist Illo Talur. Kõik vastasid küsimustele e-maili teel märtsikuu jooksul.

Kollo (2011) leidis, et kulude mõistes tuleks vaadelda ainult kahte aspekti:

- inimeste tööaeg, kui katkestuse tõttu on tööseisak ja see pikendab töösoorituse tähtaega;
- inimeste töötasu, kui katkestuse tõttu on vaja täiendavalt inimesi tööle kutsuda (ehk automatiseeritud protsessid manuaalselt teha).

Kollo (2011) rohkem mõjurite sissetoomist põhjendatuks ei pidanud, kuna leidis, et paljuski on tekkiv kahju mittemateriaalne ning seega on äärmiselt raske hinnata tegelikku ja reaalselt tekkinud kahju. Samas ta ei välistanud teiste mõjurite olemasolu, kuid rõhutas, et nende mõju on äärmiselt raske hinnata ning seega võib saadud tulemus pigem ebaõige või äärmiselt hinnanguline olla. Kuna PPA on avalikku võimu teostav asutus ja teenuse tellimise aluseks ei ole eraõiguslikud suhted, vaid avalikkuse ootus, ning leppetrahvide kohandamist ei toimu, seega on äärmiselt raske mudelisse muude mõjurite tekitatud kahju lisada.

Sergo Eelmäe (2011) pidas oluliseks rõhutada järgmisi väljapakutud mõjureid

- inimeste tööaeg (sh aeg, kui nad ei saa oma tööd teha);
- inimeste töötasu (kui tuleb täiendavalt inimesi tööle kutsuda);
- maine kahju.

Täiendavalt tõi Eelmäe (2011) välja kohalike ja globaalsete julgeolekuriskide suurenemisest tuleneva kahju ja väitis, et tegelikult me ei tea, kui palju isikuid jääb seetõttu

piiril tabamata, seega saavad nad liikuda riigist riiki ning jätkata oma kuritegelikku elu. Magistritöö autori hinnangul on julgeoleku riskist tulenevat kahju äärmiselt raske määrata, seda võib hinnata kaudselt kuritegude statistika kaudu või läbi viia vastav uuring. Mõlemal juhul on tulemus äärmiselt abstraktne.

Talur (2011) tõi Eelmäega välja samad mõjurid ning märkusena lisas juurde ametnikes tekkiva frustratsioon ja motivatsiooni languse mõne töörutiini pidevast kordamisest, kuna esimese sisestusega ei pruugi päring vastust saada. Talur (2011) lisas täiendavalt juurde, et metoodikast on kasu eelkõige eelarve planeerimisel ja investeeringute taotlemise põhjendamisel.

Magistritöö autor annab ülevaate intervjueeritavate ning PPA ekspertide hinnangute alusel moodustunud IKT katkestuse mõjuritest ning toob välja asjaolu, kas neid näitajaid on võimalik magistritöö raames välja pakutavas metoodikas kasutada.

Teenus katkestuse aeg on kõige olulisem näitaja, kuna fikseerib katkestuse ajalise mõõtme. Aeg hakkab lugema hetkest, kui probleemist on IT abi teavitatud ning lõppeb intsidendi sulgemisega. Põhimõte tuleneb Teenuse osutamise üldtingimustest, kus on nimetatud katkestuse alguse fikseerimise aeg. Intsidendi sulgemine eeldab kasutaja teavitamist, et teenus jälle toimib. Sama põhimõtet rakendatakse ka ITIL-i intsidentide haldamise protsessis, mida käsitleti magistritöö alapeatükis 1.2. Katkestuse aeg tuleb fikseerida tunni täpsusega ning ümardused teha vastavalt sellele, et kui tegelik kestus on x tundi ja alla 30 minuti, ümardatakse katkestuse aeg alla ning kui on üle 30 minuti, siis ümardatakse üles. Kuna mudel ei tohi keeruline olla (Kollo 2011; Rinne 2011) ning peaks näitama mõõdetavaid tulemusi võimalikult täpselt ning moonutamata, seega ei ole mõistlik alla 30-minutise katkestuse puhul kulu hinnangut teha. See ei kehti juhtudel, kui sellel ajal tekivad konkreetsed ja hinnatavad otsesed kulud sisupoolele või kui erinevate katkestuste üldsumma on 24 tunni jooksul rohkem kui üks tund. Üksikute katkestuste jada mõjutab kasutajate hinnangut infosüsteemist, mõjub nende töö motivatsioonile ja töökorraldusele ning seega on sellisel juhul mõistlik kulu kajastada.

Inimeste tööaja kaudset kulu (arvestatuna eurodes) tuleb hinnata, kui katkestuse tõttu on tööseisak ja see pikendab töösoorituse tähtaega. Katkestusest mõjutatud kasutajate keskmine tunnitasu tuleb korrutada mõjutatud kasutajate arvuga. Kasutajate arvuks tuleb arvestada teenuse tehnilises kirjelduses kokkulepitud samaaegselt süsteemi kasutajate arv, kui ei ole teada täpset arvu. Täiendavate inimeste väljakutsumisest tekkinud palgakulu selle nimetuse all ei vaadelda, kuna seda on võimalik täpselt määrata ning kajastatakse otseste kulude all. Tööaja kulu on ametnike hinnanguline palgakulu, kuna nad ei saanud oma tööd mingil ajahetkel teha või pidid ühte töösooritust mitmeid kordi tegema ning seega tekkis töö seisak mõnes teiseks sektoris (nt tekkisid piirijärjekorrad). See on tööandja kulu, mida küll reeglina täiendava lisarahana välja ei maksta, kuid seda on vajalik arvestada, kuna see on kaotatud produktiivsusega seotud kulutus ning mingil hetkel võib tööandja olla sunnitud täiendavat tööjõudu palkama, kuna olemasoleva isikkoosseisuga ei ole võimalik kõiki töid ära teha. Samuti võib see näiteks tähendada vajadust täiendava vaba aja andmist töötajale, kes oli mingil päeval kauem tööl. Nimetatud põhimõte oli kajastatud magistritöö alapeatükis 1.1, kus TCO kulude jaotuse puhul toodi välja, et seisva süsteemi kulusid on keeruline arvutada ning need on hinnangulised. Autor peab vajalikuks saadud tulemuse subjektiivsuse vähendamiseks arvestada väljatöötatavas mudelis ärikriitilisusest tulenevat mõju. Seda seletatakse lahti ärikriitilisuse all.

Otsene kulu (sh inimeste töötasu). Kajastatakse juhul, kui on võimalik välja tuua sisupoole kantavad katkestusega otseselt seotud kulutused. Otsene kulu ei pea olema katkestuse lõppemise ajaks tehtud, kuid see peab olema tekkinud katkestusest tingituna või selle juurpõhjus peab olema katkestus, kuigi see võis ilmneda alles peale katkestuse likvideerimist. Otseste kulude mõõdetavuse põhimõte on toodud magistritöö alapeatükis 1.1. Näiteks täiendavalt tööle kutsutud inimesed (nende brutopalk), vajadusel tehtavate ametlike teadaannete maksumus või logistika ümberkorralduse maksumus. Arvestada tuleb kõiki katkestusega otseselt seotud kulutusi, moonutuste vältimiseks ei tule siia hulka arvestada inimeste tööjõu kulu, kelle põhiülesannete hulka kuulub mõni eelpool nimetatud töö või kaudsete kulude all kirjeldatud tegevuste tegemine (näiteks pressiteate puhul kommunikatsiooni valdkonna inimese töötasu).

Kahju riigile/erasektorile (saamata jäänud tulu). PPA on avalikku võimu teostav asutus ning tulu ei taotle, seega ei ole PPA-l ka saamata jäänud tulu. Autor ei pea mõistlikuks kajastada katkestusest tingituna riigile saamata jäävat potentsiaalset trahvide tulu, kuna seda on äärmiselt raske hinnata. Lisaks ei ole PPA ainult karistav asutus, vaid ka suunav ja abistav ning seega ei ole mõistlik tekitada organisatsiooni siseselt vale rõhuasetust ning kajastada kulu, mida ei ole tekkinud või mis peaks tekkima seoses inimeste karistamisega. Antud mõjurit eelpool toodud põhjendustel metoodika loomisel ei kasutata. Muud tekkinud materiaalset kahju siin ei arvestata, kuna need kulud kajastatakse tekkinud otseste kulutuste all (näiteks vajaliku seadme välja vahetamine, juhul kui see on sisupoole ülesanne).

Maine kahju tingituna IKT katkestusest on väga raske mõõta ning hinnata. Võimalus oleks seda hinnata PPA kohta läbiviidavas kliendirahulolu-uuringus. PPA hõlmab nii politseilise, piirivalve kui ka kodakondsus- ja migratsiooni valdkonna tegevust, seega on äärmiselt raske välja tuua konkreetset hinnangut või koefitsiente, kus inimeste usaldamatus oli tingitud sellest, et infosüsteemid ei töötanud. Paljudel juhtudel ei pruugi inimesed sellest ka teadlikud olla, mis neile ebameeldiva viivituse, tekkivate piirijärjekordade või teistkordse ametniku juurde tagasikutsumise aluseks võis olla. Maine kahjuga mudelis arvestada ei saa, kuna seda pole võimalik adekvaatselt mõõta. Samas kui oli teada, et toimusid ulatuslikud katkestused, mis võisid eesti elanikele välja paista ning samal ajal inimeste usaldus asutuse vastu langes, selle saab katkestuse metoodikas välja tuua, kuid mudelis seda kajastada ei saa.

Kommunikatsioonikulusid katkestustest teavitamiseks eraldi mudelis välja ei tooda. Katkestusega otseselt seotud kulud (nt pressiteadete maksumused, ostetud ajalehe artikli pind) tuleb kajastada otseste kulude all. Ametnike töötasu, kes olid hõivatud teate kommunikeerimisega, tuleks arvestada otseste kulutuste alla, kui selleks tuli inimesi täiendavalt tööle kutsuda ning palka juurde maksta. Kui oli tegemist inimese põhitööga ning sellega tema töödes olulist seisakut ei tekkinud, sellisel juhul palgakulu arvestada ei tule. Juhul kui sellest tekkis oluline tööseisak, siis seda tuleks samuti hinnata inimeste tööaja kaudse kulu näitaja juures.

Kohalike ja globaalsete julgeolekuriskide suurenemisest tulenev kahju on hinnanguline ning seda on raske mõõta. Autor märkis ka eelpool, et seda oleks võimalik teha elanikkonna turvatunde indeksi alusel, millist turvariski inimesed Eestis elades tajuvad. Reeglina näitab see pigem seda, kui palju inimesed Eesti elu kajastavaid kriminaalsarju vaatavad, kus näidatakse toimunud kuritegusid, või milline on inimesel olnud isiklik kokkupuude politseiga ja kui operatiivselt on tema probleemiga tegeletud. Seega ei ole võimalik selle alusel hinnata IKT katkestusest tekkinud suurenenud julgeoleku riski mõju. Teine võimalus on seda hinnata teiste riikide tehtud turvalisuse näitajast Eesti kohta, kus hinnatakse Eesti võimekust enda riigis ja välispiiril korra hoidmisega toime tulemist. Samas see ei anna jälle tulemust konkreetse katkestuse mõju hindamisel. Eelpool kirjeldatud näitajaid võib kasutada ilmestamisel aasta kokkuvõtete tegemisel, kus vaadeldakse eelmisel aastal olnud katkestuste koguarvu ja maksumust ning tuua taustaks juurde Euroopa Liidu institutsioonide/töörühmade antud hinnangud, et näha, kas on võimalik tuletada seaduspärasusi IKT katkestuse toimumisega. Seega kohalike ja globaalsete julgeoleku riskide suurenemisest tulenevat kahju mudelis ei kajastata, kuna seda ei ole võimalik hinnata adekvaatselt konkreetse katkestuse kohta.

Ametnike motivatsiooni langust konkreetse IKT katkestuse mõistes on raske hinnata ja mõõta. Seda saab teha kasutajate rahulolu küsitlusega infosüsteemide töökindluse kohta ning sealt tuleb välja, mis on probleemid või missuguste infosüsteemide osas on mured suurimad. Konkreetse katkestuse kohta motivatsiooni langust arvestada ei ole võimalik ning seega ei saa seda arvestada ka mudeli loomisel. Ametnike rahulolu küsitlus infosüsteemide töökindlusega on vajalik ja seda tuleks teha kokkulepitud intervalli tagant ning seejärel saadud tulemust kasutada aasta kokkuvõtete tegemisel taustainformatsioonina, mis aitab mõista infosüsteemide üldist töökindlust ja inimeste rahulolu nendega.

Ärikriitilisust tuleb hinnata ning metoodikas kajastada, kuna see annab indikatsiooni süsteemi olulisusest asutuse jaoks. Ärikriitilisus on PPA-s määratud kõikide infosüsteemide ja rakenduste kaupa. Kuna mudel peab olema lihtne (Rinne 2011), siis ei pea magistritöö autor mõistlikuks hakata uuesti infosüsteemidele määratud ärikriitilisust üle vaatama või teise metoodika alusel seda määrama ning mudelis tuleb kasutada juba

määratud ärikriitilisuse näitajat. Nimetatud näitaja on määratud vahemikus üks kuni neli, kus üks on kõige ärikriitilisem ning neli on vähem ärikriitiline teenus. Seega tuleb katkestusest tekkinud kõigi inimeste tööaja kaudne kulu (kajastatud eurodes) korrutada ärikriitilisuse koefitsiendiga. Ärikriitilisemate tegevuste tõttu ei ole võimalik inimeste tööd ümber korraldada selliselt, et sellest suurt töö seisakut ei tekiks ja/või töö ümberkorraldusest ei tekiks inimestele töö kuhjumist. Vähem ärikriitiliste tegevuste puhul on inimestel võimalik täita muid tööülesandeid kuni infosüsteemi töö taastub või muudetakse töökorraldust selliselt, et see mõjutab tööde kuhjumist vähesel määral. Seega saab ärikriitilisuse koefitsiendi arvestamisega vähendada mudelist tööjõu kulude kaudsest arvutusest tulenevat subjektiivsust ning saadud rahaline hinnang on reaalsem. Näiteks ei pruugi teenuse kirjelduses märgitud arv kasutajaid infosüsteemi tegelikkuses korraga kasutada, töötajad teevad tööaja jooksul lühiajalisi puhkepause jne. Koefitsient on tuletatud sellest, et mida ärikriitilisem on tegevus, seda rohkem tuleb inimeste tööd ümber korraldada ja seda suurem on katkestuse mõju asutusele ning seda vähem tuleb korrigeerida juba hinnatud kaudset tööaja kulu. Tabelis 5 toodud jaotus on magistritöö autori välja pakutud kohandus, mille aluseks on võetud ITIL-is toodud intsidentide prioritiseerimise ning elutähtsa teenuse toimepidevuse riskianalüüsi teenuste kriitilisuse määramine põhimõtted.

Tabel.5. Ärikriitilisuse koefitsiendi määramise alus (allikas: autor)

Ärikriitilisus	Koefitsent
1	0,75
2	0,5
3	0,25
4	0,1

Eelpool toodud mõjurite analüüsi alusel pakub autor välja PPA IKT katkestuse mõju hindamise metoodika, mis koosneb kahest osast: mitterahalised mõjurid ning mudel katkestusest tekkinud kulutuste arvutuseks. Mudelit saab kasutada igapäevaselt tekkinud katkestuse hindamiseks ning selle loomisel on arvestatud rahaliselt hinnatavate mõjuritega. Mitterahalised mõjurid tuleks välja tuua siis, kui tehakse aasta kokkuvõtteid ning kasutada

neid taustainfona trendi väljaselgitamiseks. Mitterahaliste mõjuritena tuleks kindlasti kasutada PPA kohta tehtud kliendi rahulolu-uuringu ning töötajate rahulolu infosüsteemide töökindlusega tulemusi, võimalusel ka julgeolekuriske iseloomustavaid näitajaid.

IKT katkestuse kulu hindamise aluseks on autori poolt esitatud alljärgnev mudel, mis kombineerib IKT teenuse katkestuse aja, tööaja kaudse kulu, ärikriitilisuse koefitsendi ja katkestusest tekkinud otsesed kulud. IKT katkestuse kulu arvutatakse järgmise valemi alusel

IKT katkestuse kulu = katkestuse aeg (tundides) x (tööaja kaudne kulu (eurodes) x ärikriitilisuse koefitsient)+ otsesed kulud (eurodes)

Eelpool toodud mudelit saab kasutada IKT katkestuse mõju hindamiseks põhitegevusele ning arvutada välja sellest tingitud rahalise kahju. Mudelis on arvestatud otseselt tekkinud kulutusi, kaudsetelt arvutatud inimeste töötasu kulutuste ebatäpsust on parandatud ärikriitilisuse koefitsiendiga. Mudel arvestab nii avaliku teenuse kui ka siseteenuse pakkumisel IKT katkestusest tingitud kahju asutusele. Magistritöö raames ei ole uuritud kodanikule tekitatud kahju, kuna riigiasutus pakub avalikku hüve ning seega saab üldistades väita, et asutusele tekkinud kahju on nii riigile kui ka kodanikule tekkinud kahju, kuna viimane ei saa avalikku hüve tarbida. Konkreetsele üksikindiviidile tekitatud kulu (nt käib inimene kaks korda dokumendi järel) ei pea autor võimalikuks hinnata, kuna kodanikuga ei olda lepingulistes suhetes ning seega on keeruline määrata kahju tekkimise algust/ulatust. Autor peab siiski vajalikuks rõhutada, et avaliku teenuse mittetoimimine ongi tegelikult kõigile eesti kodanikele tekitatud kahju ning kaudselt saab väljatöötatavas mudelis hinnatavat kahju tõlgendada kõigile avaliku teenuse tarbijatele tekitatud kahjuks, kuigi reaalseks kulu kandja on riigiasutus.

Mudel on sobilik toimunud katkestuse mõju hindamiseks ning arvestada tuleks katkestusi, mis on pikemad kui 30 minutit. Rahaliselt mittehinnatavaid mõjusid mudelis arvestatud ei ole ning need tuleksid välja tuua vastavalt metoodikale aastakokkuvõtete tegemisel. Autor ei näinud antud magistritöö raames võimalust kajastada mudelis hinnangulisi näitajaid,

kust ei selgunud täpselt, kui suur osa antud hinnangust oli seotud konkreetse IKT katkestusega. Seda tuleb uurida edasi juba teiste tööde raames.

Väljatöötatud metoodika on kooskõlas magistritöö esimeses peatükis vaadeldud teoreetiliste alustega. Mõjurid ja mudel lähtuvad põhitegevuse ja IT teenuse järjepidevusest (vastavalt toimepidevuse kriteeriumitele ja IT halduse parimates praktikates käsitletule). Valitud mõjurid on oma valdkonnas konkreetsed ning võimaldavad nende esinemise mõõtmist (nagu soovitas COBIT). Mõned nendest mõjuritest (otsesed ja kaudsed kulud) on magistritöö autori poolt väljatöötatud mudelis vahetult arvestatud, teiste (motivatsiooni langus, maine kahju jne) vajavad autori hinnangul eraldi perioodiliste uuringute läbiviimist ning nende tulemuste sidumine IKT katkestuste mudeliga oleks täiendava rahuolu-uuringu teema. Valitud mõjurid ning väljatöötatud valem arvestab IKT katkestuste mõju terviklikult (nagu käsitleb ISO 27002).

Mudeli igapäevaseks rakendamise lihtsustamiseks tuleb luua eeltäidetud Exceli tabel, kuhu on vajalikud valemid sisse kirjutatud ning konkreetse katkestuse puhul peab ametnik sisestama katkestuse kestuse, katkestusest mõjutatud töötajate arvu, nende keskmise tunnitasu, ärikriitilisuse koefitsendi ning katkestusega seotud otsesed kulutused. Tabeli näidis on toodud Lisas 4. Sellisel kujul oleks võimalik teha infosüsteemide kaupa eelmise perioodi kohta katkestuste arvust ja maksumusest statistikat ja kokkuvõtteid ning juhtkond saaks kasutada nimetatud infot abimaterjalina otsuste tegemisel investeeringute suunamiseks infosüsteemide töökindluse tõstmiseks või kasutada eelarve läbirääkimistel SMITiga.

Autori hinnangul on IKT katkestuste mõju hindamise metoodika PPA-s rakendatav nii tervikuna kui ka osaliselt. Metoodikat tervikuna rakendades tuuakse välja mitterahalised mõjurid ning kajastatakse vaadeldava perioodi katkestuste üldarv ning nende kogukulu. Ainult mudelit kasutades saab arvutada konkreetse katkestuse kulu põhitegevusele.

Metoodika on rakendatav ka teistes Siseministeeriumi valitsemisala asutustes ning vajadusel võimalik kasutada kõigis avaliku sektori asutustes. Metoodika edasiarenduseks tuleks uurida mitterahaliste mõjurite trende ja nende seost IKT katkestustega ning võimalusel kajastada ka neid näitajaid mudelis kahju arvutamisel.

KOKKUVÕTE

Kaasaegsed IKT lahendused mõjutavad avaliku sektori asutuse tööprotsesse ja nende toimimist ning ilma automatiseeritud tööprotsessideta ei kujuta ametnik enam oma igapäevast tööd ettegi. Selle mugavusega on lihtne ära harjuda, kuid mida teha siis, kui infosüsteem lakkab töötamast, mis on selle katkestuse mõju põhitegevusele ja kuidas seda hinnata.

Magistritöö eesmärgiks oli luua metoodika IKT katkestusest tekkiva mõju hindamiseks asutuse põhitegevusele Politsei-ja Piirivalveameti näitel.

IKT katkestuse mõju põhitegevusele avalikus sektoris uuritud ei ole ning seega oli teoreetilist baasi selle kohta väga raske leida. Esimese uurimisülesande saavutamiseks kajastas autor oma töös valdkonnad, mis on seotud IKT katkestuse mõõtmisega: IT valdkonna tulemuslikkuse mõõtmine (sh seotud finantsnäitajad), ITIL-i raamistik ning elutähtsa teenuse toimepidevuse tagamiseks vajaliku riskianalüüsi koostamise metoodika põhimõtted. Ükski eelpool nimetatud teoreetiline käsitlus ei kata iseseisvalt IKT katkestuse mõju hindamist põhitegevusele antud magistritöö raames, kuid koos moodustus tervik, mille alusel sai autor välja töötada metoodika.

Valdavalt mõõdetakse IKT tasuvust tööprotsesside konsolideerimisel ja automatiseerimisel ning katkestusi hinnatakse IKT teenuse pakkuja seisukohast lähtuvalt, et oleks määratletud teenuse ärikriitilisus ning kokkulepitud sisupoolega erinevate intsidentide korral käitumisjuhised. Selle juures vajalikud taasteplaanid on pigem tehnilist laadi ning kajastavad, kuidas peaks IKT teenuse pakkuja tagama teenuse jätkusuutlikkuse. Riskianalüüsi metoodika hindab riski võimalikku toimumise tõenäosust ning seejärel rakendatakse suurima riski maandamiseks vajalikke meetmeid. Antud töös vaadeldi juba toimunud katkestust ning määrati sellega seotud kulud, et edaspidi saaks selle teadmise alusel paremaid juhtimisotsuseid teha.

Magistritöö autor ei leidnud ühtset teoreetilist baasi IKT katkestuse mõju hindamiseks põhitegevusele, seega tuli sobivad teoreetilised alused uudse lähenemisena kombineerida ning juhtumianalüüsi käigus keskenduda ka tavapärasest rohkem valimis olnud asutuste üldise IKT toimimise regulatsioonidele ja põhimõtetele. Eelkõige tuli asutusi täpsemalt vaadelda, et mõista, millises keskkonnas asutus tegutseb, kas tellitakse IKT teenust tervikuna sisse või ainult osaliselt. Välise teenuse pakkuja olemasolul tuleb paratamatult tellitava teenuse tingimusi rohkem reglementeerida, kui oleks seda vaja teha asutuse sees. Juhtumianalüüsist järeldus, et enamus intervjueeritavaid tõdesid vajadust IKT katkestuse mõju hindamiseks põhitegevusele, kuigi konkreetset mudelit kellelgi välja töötatud ei olnud. Katkestusi ja nende mõju (sh just tekkinud kahju) monitoorisid eraettevõtted ning vajadusel rakendati ka leppetrahve või tasaarveldusi lepingupartneritega. Riigiasutused tõdesid katkestuse olemasolu fakti, kuid rahalist hinnangut sinna juurde ei osatud anda, kuna seda ei mõõdeta.

Magistritöö teine uurimisülesanne oli välja selgitada mõjurid, mida peab arvestama katkestuse hindamise metoodika välja töötamisel. Intervjueeritavate ja PPA ekspertide hinnangul sai selliseid mõjureid kokku üheksa, mis mõjutavad põhitegevust. Autor jagas need kaheks: rahalised ja mitterahalised mõjurid ning viimaseid kasutatakse taustainformatsioonina kokkuvõtete tegemisel. Kolmanda uurimisülesande saavutamiseks kasutas autor eelpool nimetatud mõjureid ning pakkus välja IKT katkestuse mõju hindamise metoodika põhitegevusele PPA näitel. Metoodika koosneb kahest osast, mitterahalised mõjurid IKT katkestuse hindamiseks ning mudel katkestusest tekkinud kulutuste arvutuseks. Mitterahalisi mõjureid oli keeruline mudelis kajastada, kuna nende puhul ei olnud võimalik hinnata, kas näitajate muutus oli mõjutatud IKT katkestusest tingitud teenuse häirest või mõnest muust vastajale olulisest isiklikust kogemusest.

Töös välja pakutud mudelis on kajastatud IKT katkestusest tingitud otsesed kulud ning kaudsed kulud, mis on tingitud tööde kuhjumisest, kuna infosüsteemi kasutaja(te)l ei ole võimalik selleks ettenähtud ajal tööd teha. See on produktiivsuse kaotusega seotud kulu ning seda tuleb mudelis arvestada, kuid kulu ülehindamise riski maandamiseks korrigeeritakse seda ärikriitilisuse koefitsiendiga. Üldjuhul ei ole antud mudelit mõistlik

rakendada katkestuste korral, mis kestavad alla 30 minuti, va juhul kui katkestusest tekkisid otsesed kulud.

Magistritöö teises peatükis näidati ka lühidalt, et väljatöötatud mudel arvestab töö esimese peatükis kirjeldatud teoreetilise baasi komponentide poolt pakutud soovitustega. Kokkuvõttes on väljapakutud metoodika uudne ning arvestab toimepidevate organisatsioonide vajadustega.

Autori hinnangul on mudel PPA-s lihtsalt rakendatav eeltäidetud Exceli tabelit kasutades. Metoodikat tervikuna rakendades (koos mitterahaliste mõjuritega) saab kasutada ülevaadete või kokkuvõtete tegemisel ning see oleks abimaterjalina kasutatav eelarve planeerimisel ja läbirääkimistel SMITiga ning juhtkonnale ülevaadete tegemisel.

Väljatöötatud metoodika on rakendatav ka teistes Siseministeeriumi valitsemisala asutustes ning vajadusel oleks võimalik kasutada kõigis avaliku sektori asutustes.

Metoodika edasi arendamiseks tuleks kindlasti jälgida mitterahaliste näitajate trende (PPA mainet/usaldust, töötajate rahulolu infosüsteemide töökindlusega) ning uurida, kas on võimalik hinnata seoseid eelpool nimetatud näitajate ja IKT katkestuste vahel. Saadud tulemuste alusel tuleks vajadusel täiendada antud töös välja pakutud mudelit.

SUMMARY

Measuring the loss from interruptions related to Information and Communications Technology (ICT) has become a hot topic in the area of governance of the Ministry of Interior in Estonia because ICT related activities have been consolidated and offered as services by the IT and Development Centre (ITDC, or SMIT by its Estonian acronym). The effectiveness and performance wasn't measured previously when IT systems were managed by the organisations' own IT departments.

The goal of this thesis is to develop a methodology to measure the impact of ICT interruptions on the main business activities on the example of the Police and Border Guard Board (PBGB) of Estonia.

The following research tasks have been posed to achieve this goal:

- To analyse the principles of measuring the impact of ICT related interruptions;
- To define the key factors that should be taken into account when measuring the impact of ICT interruptions;
- To work out a methodology for the PGBG to measure ICT related interruptions.

The thesis has two chapters. The first chapter consists of the theoretical part concerned with the first of the research tasks. The second chapter if the empirical part where the results of the case study and the relevant factors are being discussed in order to develop a model to measure the impact of ICT related interruptions.

As a result of the interviewees and experts in the PBGB there are 9 such factors through which interruptions in the work and functioning of ICT has an impact on the main business activities of an organisation. The author of the thesis has separated these factors into 2 groups: monetary and non-monetary factors and the latter group is used as background

information when making conclusions. The methodology consists of 2 parts, of the non-monetary factors to measure ICT related interruptions and a model to measure the costs of the interruptions.

In the model proposed in this thesis there have been included both the direct costs and indirect costs that are caused by cumulative effects from work that is not being done because the users of ICT systems are not able to work effectively during the interruptions of these systems. These are costs from the loss of productivity and they need to be taken into account in the model but to manage the risk of over evaluating the costs they are being corrected with a business criticality coefficient.

In the author's opinion this model is easily applicable in the PBGB using prefilled Excel files. The whole methodology (together with the non-monetary factors) can be used when giving a review or the big picture and it can be helpful when planning the budget, when conducting negotiations with SMIT or when giving an overview to the management.

The proposed methodology is also applicable in other institutions subordinate to the Ministry of Interior and in other public sector organisations in Estonia.

VIIDATUD ALLIKATE LOETELU

Allingu, M. 2011. IKT katkestuse mõju hindamine põhitegevusele RIKis. Autori intervjuu. Helisalvestis. Tallinn, 25.veebruar. Autori valduses

Brooks, P., van Bon, J., Verheijen, T. 2010. Metrics for IT Service Management. Van Haren Publishing

Buytendijk, F. and Geishecker, L. 2004. Corporate Performance Management: Connecting the Dots. Gartner Groupi koduleheküljelt www.gartner.com välja otsitud 02.02.2011

Chan, K-C., Chandrashekhar, U., Richman, S.-H. and Vasireddy, S.-R.2004. The Role of SLAs in Reducing Vulnerabilities and Recovering from Disasters. Bell Labs Technical Journal, 9(2), 189-203. Välja otsitud EBSCOhost andmebaasist 05.03.2011

Chitakornkijsil, P. 2010. Enterprise Risk Management. International Journal of Organizational Innovation, 3 (2), 309-337. Välja otsitud EBSCOhost andmebaasist 15.04.2011

Ciuhureanu, A.-T. 2009. Cost of Ownership (TCO analysis) during economic and financial crisis? Review of Management & Economic Engineering, 8(2), 87-97. Välja otsitud EBSCOhost andmebaasist 15.04.2011

Drysdale, D., Bonanni, C. & Shuttlewood, P. 2010. Return On Investment For Backgound Screening. International Business & Economics Research Journal, 11 (9), 65-70. Välja otsitud EBSCOhost andmebaasist 15.04.2011

Eesti julgeolekupoliitika alused. Vastu võetud Riigikogu 12.05.2010 otsusega, jõustunud 17.05.2010 – RT I 2010, 22, 110

ISO 31000:2009 tutvustus. Eesti Standardikeskuse koduleheküljelt http://www.evs.ee/Checkout/tabid/36/screen/freedownload/productid/195874/doclang/et/preview/1/EVS_ISO_31000;2010_et_preview.aspx välja otsitud 15.04.2011

Epstein, M. and Rejc, A. 2004. Measuring the payoffs of IT investments. CMA Management, 78(8), 20-25. Välja otsitud EBSCOhost andmebaasist 19.11.2010

Epstein, M. and Rejc, A. 2005. How to measure and improve the value of IT. Strategic Finance, 87 (4), 34-41. Välja otsitud EBSCOhost andmebaasist 19.11.2010

Elutähtsad valdkonnad ja teenused. Siseministeeriumi koduleheküljelt www.siseministeerium.ee/elutahtsad-valdkonnad-ja-teenused-2/ välja otsitud 03.03.2011

Galup, S., Dattero R., Quan, J., Conger, S. 2009. An Overview of IT Service Management. Communications of the ACM, 52(5), 124-127. Välja otsitud EBSCOhost andmebaasist 19.11.2010

Grasseova, M. 2010. Utilization of balanced scorecard in public administration. Revista Academiei Fortelor Terestre, 57 (1), 49-57. Välja otsitud EBSCOhost andmebaasist 19.11.2010

G4S üldinfo ja väärtused. G4Si koduleheküljelt www.g4s.ee/ettevottest/uldinfo välja otsitud 15.03.2011.

Hartley, K.-L. 2005. Defining Effective Service Level Agreements for Network Operation and Maintenance. Bell Labs Technical Journal, 9(4), 139-143. Välja otsitud EBSCOhost andmebaasist 05.03.2011

Hirsjärvi, S., Remes, P. ja Sajavaara, P. 2005. Uuri ja kirjuta (Tutki ja kirjoita). Tõlge eesti keelde: I. Kraav, T. Kuurme, U. Kala, M.-L. Laherand, V. Maansoo ja J. Orn. Tallinn, Kirjastus Medicina. (Originaal on publitseeritud Kustannusosakeyhtiö Tammi, Helsinki, 2004)

Holm, K. 2011. IKT katkestuse mõju hindamine põhitegevusele Maksu- ja Tolliametis. Email autorile. 22.märts. Autori valduses

Hädaolukorra seadus 15.06.2009, jõustunud 24.07.2009 - RT I 2009, 39, 262- RT I, 17.02.2011, 9

Häirekeskus. Päästeameti koduleheküljelt www.rescue.ee/390 välja otsitud 15.03.2011.

Info- ja kommunikatsioonitehnoloogia valdkonna teenuse osutamise üldtingimused. Siseministri 21.12.2009 käskkiri nr 236L. Asutusesiseseks kasutamiseks. Dokumendiga tutvuti 01.03.2011

Infoturbepoliitika politseiasutuses. Politsei-ja Piirivalveameti peadirektori 01.01.2010 käskkiri nr 46. Asutusesiseseks kasutamiseks. Dokumendiga tutvuti 01.03.2011

Infovarade loetelu ja infosüsteemi pidamise korra vormi kinnitamine. Politsei-ja Piirivalveameti peadirektori 24.05.2010 käskkiri nr 241. Asutusesiseseks kasutamiseks. Dokumendiga tutvuti 01.03.2011

IT juht. 2011. IKT katkestuse mõju hindamine põhitegevusele telekommunikatsiooni ettevõttes. Autori intervjuu. Helisalvestis. Tallinn, 18.veebruar. Autori valduses

IT Strategy. A CIO Success Kit. 2009. Gartner Group koduleheküljelt www.gartner.com/technology/research.jsp välja otsitud 12.03.2011

Jauk, A. 2011. IKT katkestuse mõju hindamine põhitegevusele G4Sis. Autori intervjuu. Helisalvestis. Tallinn, 9.veebruar. Autori valduses

Justiitsministeerium. Justiitsministeeriumi koduleheküljelt www.just.ee/5327 välja otsitud 15.03.2011.

Kaplan, R.-S. ja Norton, D.-P. 2003. Tasakaalus tulemuskaart: strateegialt tegudele (The Balanced Scorecard: From Strategy to Action). Tõlge eesti keelde Kährik, K. Kirjastus Pegasus. (Originaal on publitseeritud Harvard Business School Press, 1996)

Kasenõmm, E. 2010. IT teenuste haldamise parimad praktikad (ITIL): raamistik avaliku halduse reformide kontekstis ja rakendamine Siseministeeriumi haldusalas. Publitseerimata magistritöö. Tallinna Tehnikaülikool

Knahl, M.-H. 2009. A Conceptual Framework for the Integration of IT Infrastructure Management, IT Service Management and IT Govenance. Proceedings of World Academy of Science, Engineering and Technology, 40, 447-451. Välja otsitud EBSCOhost andmebaasist 03.01.2011

Knight, K.-W. 2010. AS/SZS ISO 31000:2009- the new standard for managing risks. Keeping Good Companies, 2, 68-69. Välja otsitud EBSCOhost andmebaasist 10.04.2011

Kramer, L. 2005. CIO challenge. Wall Street &Technology, 23 (11), 44-46. Välja otsitud ProQuest andmebaasist 02.03.2011

Kollo, I., Eelmäe, S. ja Talur, I. 2011. Mõjurid IKT katkestuse hindamise metoodika väljatöötamisel PPA näitel. Email autorile. 22.märts. Autori valduses

Kuusk, K. 2006. Juhtumiuuring. EMSLi koduleheküljelt www.ngo.ee/orb.aw/class=file/action=preview/id=11594/Juhtumiuuring.ppt välja otsitud 20.11.2010

Laherand, M.-L. 2008. Kvalitatiivne uurimisviis. Tallinn OÜ Infotrükk

Leimann, J., Skärvad P.-H., Teder, J. 2003. Strateegiline juhtimine. Kirjastus Külim

Maksu-ja Tolliamet. Maksu- ja Tolliameti koduleheküljelt www.emta.ee/index.php?id=618 välja otsitud 15.03.2011

McAdam, R. & Maguire, M. 2004. Strategic Improvement or Service Measures? Best Value in UK Local Government. Public Policy and Administration, 19 (4), 57-81. Välja otsitud SAGE andmebaasist 15.04.2011

Nastase, P., Nastase, F. and Ionescu, C. 2009. Challenges Generated by The Implementation of The IT Standards COBIT 4.1, ITIL v3 and ISO/IEC 27002 in Enterprises. Economic Computation &Economic Cybernetics Studies & Research, 43 (3), 1-16. Välja otsitud EBSCOhost andmebaasist 14.03.2011

Office of Government Commerce (OGC). 2007a. ITIL: Service Design. London: The Stationery Office

Office of Government Commerce (OGC). 2007b. ITIL: Service Operation. London: The Stationery Office

Office of Government Commerce (OGC). 2007c. ITIL: Service Strategy. London: The Stationery Office

Pollard, C. & Cater-Steel, A. 2009. Justifications, Strategies, and Critical Success Factors in Successful ITIL Implementations in U.S. and Australian Companies: An Exploratory Study. Information Systems Management, 26 (2), 164-175. Välja otsitud EBSCOhost andmebaasist 15.04.2011

Priandoyo, A. 2008. Comparison between COBIT, ITIL and ISO 27001. Security Procedure koduleheküljelt http://www.securityprocedure.com/comparison-between-COBITitil-and-iso-27001 välja otsitud15.04.2011

Praust, V., Kumar, K., Leis, P. ja Kivimaa, J. 1999. IT juhtimise käsiraamat. Äripäeva Kirjastus

Rinne, E. 2011. IKT katkestuse mõju hindamine põhitegevusele Häirekeskuses. Autori intervjuu. Helisalvestis. Tallinn, 17.märts. Autori valduses

Smith, D.-A. 2008. Implementing Metrics for IT Service Management. Van Haren Publishing

Stulz, R.-M. 2009. 6 Ways Companies Mismanage Risk. Harvard Business Review, 87 (3), 86-94. Välja otsitud EBSCOhost andmebaasist 15.04.2011

Tamm, M. 2006. Infotehnoloogia valdkonna tulemuslikkuse mõõtmine. Publitseerimata magistritöö. Estonian Business School

Tammineedi, R.-L. 2010. Business Continuity Management: A Standards-Based Approach. Information Security Journal: A Global Perspective, 19, 36-50. Välja otsitud EBSCOhost andmebaasist 01.04.2011

Tan, W.-G., Cater-Steel, A. & Toleman, M. 2009. Implementing IT service management: a case study focussing on critical success. Journal of Computer Information Systems, 20 (2), 1-12. Välja otsitud EBSCOhost andmebaasist 15.04.2011

Teenuste tehnilise kirjelduse koostamine. Politsei- ja Piirivalveameti peadirektori 23.02.2011 korraldus nr 31. Asutusesiseseks kasutamiseks. Dokumendiga tutvuti 22.03.2011

Toimepidevuse riskianalüüsi koostamise juhend. Vastu võetud siseministri 08.06.2010 määrusega nr 16, jõustunud 21.06.2010- RT I 2010, 33, 179

Tomik, T. ja Aben, S. 2010. IT riskianalüüsi koolitusmaterjal. Riigi Infosüsteemide Arenduskeskuse koduleheküljelt http://www.ria.ee/it-riskianaluus-asutuses välja otsitud 22.03.2011

Trček, D. 2010. Security Metrics Foundations for Computer Security. Computer Journal, 53(7), 1106-1112. Välja otsitud EBSCOhost andmebaasist 19.11.2010

Valk, A. 2003. Organisatsoon ja juhtimine avalikus sektoris. Sisekaitseakadeemia kirjastus

Varik, H. 2011. IKT katkestuse mõju hindamine põhitegevusele Justiitsministeeriumis. Autori intervjuu. Üleskirjutus. Tallinn, 1.märts Autori valduses

Vintar, M. 2003. Infojuhtimise meetodite ja tehnoloogiate rakendamine Kesk- ja Ida-Euroopa riikides. Raamatus Haldusjuhtimine Kesk- ja Ida-Euroopa siirderiikides: teooria ja juhtumianalüüsid. (Toimetajad Writh, G. & Nemec, J). (lk 339-390). OÜ Greif

Waheed, A., Mansor, N.& Ismail, N.-A. 2010. Assessing Performance of Public Sector Organizations: A Theoretical Framework. Interdisciplinary Journal of Conteporary Research in Business, 8 (2), 329-349. Välja otsitud EBSCOhost andmebaasist 14.04.2011

TABELITE JA JOONISTE LOETELU

LISA 1. Elutähtsa teenuse kriitilisuse hindamine

Tabel 1 Katkestuse ajaline mõõde

Kriitilisuse aste	Aeg, mis kulub elutähtsa teenuse katkestuseni
1	Väga pikk ajavahemik (kuud, aastad)
2	Pikk ajavahemik (nädalad)
3	Keskmine ajavahemik (päevad)
4	Väike ajavahemik (tunnid)
5	Väga väike ajavahemik (sekundid, minutid)

Tabel 2 Teenuse katkemise ulatuse mõõde[3]

Kriitilisuse aste	Elutähtsa teenuse katkemise ulatus
1	Väga madal (0…10 %)
2	Madal (10…30 %)
3	Keskmine (30…50 %)
4	Suur (50…80 %)
5	Väga suur (80…100 %)

Elutähtsa teenuse tegevuse kriitilisuse määramiseks kasutatakse järgmist valemit:

Elutähtsa teenuse tegevuse kriitilisus = (võrdub) katkestuse ajaline mõõde x (korrutatud) katkestuse ulatuse mõõde

Saadud punktide alusel hinnatakse teenuse tegevuse kriitilisust kasutades tabelit 3.

Tabel 3. Elutähtsa teenuse tegevuse kriitilisus[4]

Kriitilisuse punktid	Kriitilisuse aste
1-5	tegevus ei ole kriitiline
6-10	tegevus on vähesel määral kriitiline
11-15	tegevus on tähtis, keskmiselt kriitiline
16-20	tegevus on kriitiline
21-25	tegevus on väga kriitiline

[3] Teenuse osutaja hindab ise, millisest teenust iseloomustavast näitajast suhtarv arvutatakse

[4] Saadud tulemuse alusel määratakse need kriitilised tegevused, mille kriitilisuse punktid jäävad vahemikku 6-25. Viimaste suhtes jätkatakse riskianalüüsi

LISA 2. Infosüsteemide mõjude hindamine

Kriitilise tegevuse toimepidevust mõjutavad infotehnoloogilised süsteemid

Infosüsteem või IT teenuse nimetus	Infosüsteemiga seotud kriitilise tegevuse number või numbrid (numbrid tulenevad eelmisest tabelist lisas 4)	Infosüsteemi või IT teenuse kirjeldus	Teenuse pakkuja ja asukoht (asutuse/ettevõtte sisene ja väline)	Katkestuse maksimaalne lubatud kestus	Nõutav taasteaeg	Kriitilise tegevuse sõltuvus infosüsteemist või IT teenusest skaalal: 1 – sõltuvus ei ole eriti oluline; 2 – sõltuvus on oluline, aga on olemas alternatiivne lahendus 3 – kriitiline sõltuvus

LISA 3. Intervjueeritavatele esitatud küsimused

1. Ettevõtte nimetus ning tegevusvaldkond.
2. Kas Te ostate IKT[5] teenust sisse (outsourcing)? Kui ostate, siis mis mahus ja mis teenuseid? Kui ei osta, siis kui suur on ettevõtte IT töötajate arv/IT osakonna suurus?
3. IT investeeringute suurusjärk aastas. IT halduskulu aastas (suurusjärk).
4. Infosüsteemide arv, mis toetab tugiprotsesse. Infosüsteemide arv, mis toetab põhiprotsesse.
5. Kuidas on seotud infosüsteemid põhitegevuse protsessidega? Kas Teil on oma põhitööks infosüsteeme kasutavate inimeste tööprotsessid/töörutiinid kaardistatud? Kui vastasite JAH, siis kas tööprotsessid on kirjeldatud teenustena? Kas teil on määratud vastava tööprotsessi omanik (protsessijuht) või esindab omanikku tootejuht?
6. Mida teete, kui infosüsteem ei tööta st kas Teil on võimalik tööd ümber korraldada?
7. Kas Te rakendate mõnda IT haldamise parimat praktikat (nt ITIL, CobiT, ISO 27001)?
8. Kas Teil on sõlmitud teenustaseme kokkulepped (SLAd) infosüsteemide töö tagamiseks? Kas Te näete infosüsteemi töö tagamisel lisandväärtust SLAde sõlmimisel?
9. Kuidas Te tagate, et Teie asutuse jaoks olulised infosüsteemid töötaksid vastavalt nõuetele?
10. Kuidas Te defineerite IKT katkestust?
11. Kas Te mõõdate IKT katkestuse mõju põhitegevusele?

[5] Antud küsimustikus on IT ja IKT sünonüümidena kasutusel

Kui vastasite küsimusele 11 „JAH“

12. Kuidas Te mõõdate IKT katkestuse mõju põhitegevusele (mis näitajaid ja kriteeriume selleks kasutate)?
13. Kas Teil on selleks metoodika välja töötatud?
14. Kuidas Te saadud tulemusi kasutate? Kas mõõtmine on parandanud IKT valdkonna tulemuslikkust?
15. Kuidas Te saadud tulemustest tagasisidet annate juhtkonnale/töötajatele?
16. Kuidas Te mõõdate töötajate rahulolu infosüsteemide töökindlusega (küsitlus, monitooring, muu)?

Kui vastasite küsimusele 11 „EI“

17. Kas peate vajalikuks mõõta IKT katkestuse mõju põhitegevusele? Kui ei pea vajalikuks, siis miks ei pea?
18. Kui peate vajalikuks, siis mis oleksid olulised kriteeriumid (mõõdikud) mõju hindamiseks ning kuidas Te saadud tulemusi kasutaksite?
19. Kuidas Te mõõdate töötajate rahulolu infosüsteemide töökindlusega (küsitlus, monitooring, muu)? Kuidas Te saadud tulemustest tagasisidet annate?
20. Kuidas Te IT eelarvet planeerite? Kas näeksite planeerimisel abi, kui Te mõõdaksite IKT katkestuse mõju põhitegevusele?

LISA 4. IKT katkestuse kulu hindamise mudel

katkestuse kuupäev							
katkestuse algus							
katkestuse lõpp							
Näide							
Mõjutatud infosüsteem	**Katkestuse aeg**	**Mõjutatud kasutajate arv**	**Keskmine tunnitasu**	**Ärikriitilisuse koefitsient**	**Kaudsed kulud kokku**	**Otsesed kulud**	**Katkestuse kulu kokku**
nimetus	*tund*	*inimeste arv*	*eurot/tunnis*	*koefitsient*	*euro*	*euro*	*euro*
					veerg 2 veerg 3* veerg 4* veerg 5*		*veerg 6 + veerg 7*
1	2	3	4	5	6	7	8
UUSIS	1	78	4,5	0,5	175,5	300	475,5
							0
							0

1. Ametnikul tuleb täita valgeks jäetud lahtrid ning selle alusel eeltäidetud tabelis automaatselt arvutakse kaudne kulu ja kulu kokku.

2. Kui infosüsteemide lõikes on vajadus eristada kulu arvutusel erinevat keskmist tunnitasu, siis tuleb arvutada see erinevate ridade kaupa ning saadud tulemus summeerida.

3. Ärikriitilisuse koefitsendi peab ametnik kirjutama vastavalt etteantud tabelile (vt lk 58) vahemikus 0,75 kuni 0,1.