TALLINNA ÜLIKOOL

Informaatika Instituut

# Optimeeritud infotehnoloogilise infrastruktuuri mudeli rakendamise analüüs Majandus- ja Kommunikatsiooniministeeriumi näitel

Magistritöö

Autor : Kristjan Kaiklem

Juhendaja : MSc Andro Kull

Autor: ……..……..... „ … “ …….. 2009.a.

Juhendaja: ……..…… „ … “ …….. 2009.a.

Instituudi direktor: ……..……..... „ … “ …….. 2009.a.

Tallinn 2009

## Autori deklaratsioon

Olen koostanud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud. Käesolevat tööd ei ole varem esitatud kaitsmisele kusagil mujal.

Kuupäev:

Autor: Allkiri:

# Sisukord

# Jooniste loetelu



# Tabelite loetelu

# Sissejuhatus

Infotehnoloogia tähtsus meie elus tõuseb pidevalt ja see poeb aina sügavamalt meie igapäeva ellu. Seega on väga raske juba ette kujutada organisatsiooni, mis suudaks infotehnoloogia võimalusi täielikult kasutamata jättes efektiivselt toimida.

Iga organisatsiooni üheks suuremaks strateegiliseks varaks on muutumas tema infotehnoloogiline infrastruktuur, mis vastaks organisatsiooni ärilistele ja põhitegevusest tingitud vajadustele ning mille peal on võimalik pakkuda erinevaid teenuseid ja rakendusi ettevõtte sisestele või välistele kasutajatele. Paljude suurte organisatsioonide jaoks on pidev uute tehnoloogiliste arengusuundade peale tulemine ja lahenduste kasutusele võtmine viinud sinna punkti, kus serveritega seotud andmeladude, arvutitöökohtade ja kogu sellega kaasnev infrastruktuur on muutunud suhteliselt keeruliseks ning kohati raskesti hallatavaks. Mida suuremaks kasvab infotehnoloogiline infrastruktuur, seda keerulisemaks ja kallimaks on muutunud äripoole vajadustele vastamine.

Teema aktuaalsus tänapäeva kontekstis on põhiliselt tingitud hetkel valitsevast majandusolukorrast, kus organisatsioonid peavad tõsiselt üle vaatama oma kulusid ja tulusid ning otsima võimalusi, kuidas praeguses olukorras kõige paremini ellu jääda. Kindlasti kergendaks seda tööd see, kui organisatsioon tegeleks aktiivselt oma IT infrastruktuuri auditeerimisega ja üritaks seeläbi leida sealt kohti parandamiseks, mida on võimalik teha kulude vähendamiseks ja tulude tõstmiseks. Kahjuks autori töökogemuse põhjal riigisektoris, sellega piisaval tasemel veel ei tegeleta.

Magistritöö uurimisprobleemiks on see, et kiiresti kasvava IT infrastruktuuri puhul pööratakse vähe tähelepanu hetkeolukorra hindamisele ja IT infrastruktuuri optimeerimisele.

Käesoleva magistritöö **eesmärgiks** on optimeeritud infotehnoloogilise infrastruktuuri mudeli koostamine, ühe olemasoleva IT infrastruktuuri kaardistamine vastavalt välja töötatud mudelile ning tulemuste analüüsi põhjal soovituste välja pakkumine optimeeritud IT infrastruktuuri saavutamiseks.

Käesoleva töö ülesannete püstitus:

- Optimeeritud IT infrastruktuuri mudeli välja töötamine toetudes parimatele praktikatele;
- IT infrastruktuuri auditi läbi viimine järgmises 6 asutuses hetkeolukorra hindamiseks : Majandus- ja Kommunikatsiooniministeeriumis (edaspidi MKM), Lennuametis (edaspidi ECAA), Tehnilise Järelevalve Ametis (edaspidi TJA), Konkurentsiametis (edaspidi KA), Autoregistrikeskus (edaspidi ARK) ja Maanteeametis (edaspidi MNT);
- Auditi tulemuste põhjal saadud info analüüsimine ja soovituste koostamine IT infrastruktuuri optimeerimiseks.

Konkreetselt IT infrastruktuuri auditeerimisest ja optimeerimisest pole veel autorile teada-olevalt ühtegi teadustööd Eestis kirjutatud. Samas võib leida teisi sarnase lähenemisega uurimusi Tallinna Ülikoolis, kus läbi IT auditeerimise üritatakse organisatsiooni parandada: Marily Visnapuu magistritöö „IT auditi metoodikatest tulenevad soovitused IT juhtidele“ ja Kadi Raidvere diplomitöö „Infosüsteemi auditi põhimõtete rakendamine Eesti Kaitseväes“. Väljaspool Eestit on aktiivselt tegelenud IT infrastruktuuri optimeerimise metoodikate välja töötamisega suuremad IT valdkonna tehnoloogiafirmad. Nt. Microsoft ja IBM.

Magistritöö koosneb neljast peatükist.

Esimene peatükk annab ülevaate IT infrastruktuuri mõistest ja põhjustest, milleks on seda vaja auditeerida. Samuti kirjeldatakse ühte olemasolevat organisatsiooni ja selle IT infrastruktuuri, mille põhjal plaanitakse konkreetne audit läbi viia.

Teine peatükk annab ülevaate enamlevinud IT infrastruktuuri auditeerimise metoodikatest ja üritab vastust anda selle küsimusele, miks neid praktikas on keeruline rakendada.

Kolmas peatükk annab ülevaate autori poolt loodud optimeeritud IT infrastruktuuri mudelist ja selle komponentidest. Iga infrastruktuuri komponendi juures keskendutakse sellele, millist lisaväärtust selle kasutamine organisatsiooni jaoks juurde annab.

Neljas peatükk annab ülevaate Majandus- ja Kommunikatsiooniministeeriumis ja selle haldusala asutustes läbiviidud auditi tulemusel optimeeritud infrastruktuuri mudeli rakendamise analüüsist – tuues iga asutuse kohta välja koondtulemused koos täpsema olukorra kirjelduste ja soovitustega.

# Auditi mudeli välja töötamine ja läbi viimine praktikas

Auditi mudeli leidmiseks on eelnevalt läbi viidud teoreetiline uurimus erinevate teabeallikate põhjal. Uurimuse käigus analüüsiti erinevate IT infrastruktuuri komponentidega seotud parimaid praktikaid. Analüüsi tulemusel koostati parimate praktikate põhjal optimeeritud IT infrastruktuuri mudel.

Auditi läbiviimiseks koostati mudeli põhjal struktureeritud ankeet 55 küsimusega. Iga ankeedi küsimus üritab tuvastada parima praktika kasutamist konkreetse mudeli IT infrastruktuuri komponendi juures. Andmete analüüsimine antud magistriöö raames toimub kodeerimise teel. Küsimustele vastamisel on olemas kaks võimaliku vastuse varianti: a) „Jah“. See tähendab, et kasutusel konkreetses infrastruktuuri komponendi juures parim praktika, mis tagab konkreetse osa optimeerituse. Vastus loetakse selle tõttu positiivseks ning antakse selle numbriline punkti-hinne 1. b) „Ei“. See tähendab, et kasutusel ei ole parim praktika ja seda infrastruktuuri osa ei saa lugeda optimeerituks. Vastus loetakse selle tõttu negatiivseks ja antakse tulemuse punktihinne 0. Nt. Kas kasutakse ründekaitse tarkvara (Nt. IPS) arvutitöökohtade, seadmete ja serverite kaitsmiseks? Jah Ei . Küsimuste tulemused ehk antud juhul konkreetsed punktihinded lisatakse koondtabelisse edaspidiseks analüüsimiseks. Vastavalt optimeeritud IT infrastruktuuri mudelile on defineeritud ära küsimustiku jaoks 2 erinevat valdkonda, mille läbi organisatsiooni infotehnoloogilist infrastruktuuri hinnatakse;

- tehnoloogia kasutamine. Küsimused katsuvad välja selgitada seda, kas on konkreetne tehnoloogia on kasutusel ja kui on siis, kas seda on tehtut vastavalt parimale praktikale. Audit sisaldab 32 antud valdkonna küsimust;
- protsesside juhtimine. Küsimused katsuvad välja selgitada IT alase põhidokumentatsiooni olemasolu, ISKE rakendamise seisu ja rakendatud haldusprotsessid. Audit sisaldab 23 antud valdkonna küsimust.

Auditi tegemise metoodikana kasutati vastavusauditit, mille aluseks võeti loodud optimeeritud IT infrastruktuuri mudel ja võrreldi sellega tegelikku olukorra vastavust. Auditi eesmärgiks oli välja

selgitada olemasoleva IT infrastruktuuri tugevused ja nõrkused ning leida võimalused selle optimeerimiseks.

Valimi koostamisel on piirdutud Majandus- ja Kommunikatsiooniministeeriumi ning selle osade haldusala asutustega, kuna põhjalik infotehnoloogilise infrastruktuuri hindamine nõuab suhteliselt põhjalikku ja suurt auditeerimisküsimustiku. Samuti sai otsustavaks see, et kuuest asutusest viis asutust (MKM, Lennuamet, Konkurentsiamet, Tehnilise Järelevalve Amet, Autoregistrikeskus) hetkel kasutavad ühist IT infrastruktuuri, mis võimaldab välja tuua selles erisused erinevate asutuste kaupa. Maanteeameti lisamine antud skoopi oli tingitud sellest, et planeeritakse selle asutuse liitmist eelpool mainitud ühise IT infrastruktuuriga – seega saab väga täpselt määratleda tegevused, mida tuleb teha liitmise protsessis IT infrastruktuurilise taseme ühtlustamiseks. Samas välja töötatud küsimustiku on võimalik vabalt kasutada ka teiste asutuse infotehnoloogilise infrastruktuuri hindamiseks, kuna ei sisalda konkreetsele organisatsioonile iseloomulikke näitajaid.

Andmeid koguti auditi käigus otse haldusala infotehnoloogia valdkonna töötajate käest. Samuti osales autor auditi läbiviijana auditeerimisprotsessis, kuna küsimused on suhteliselt spetsiifilised ning need võivad vajada mõnedel juhtudel täiendavaid selgitusi vastamiseks.

Kuigi magistriöö raames viidi audit läbi ühekordselt, siis on võimalik auditeerimismeetodit tulevikus kasutada edasi selleks, et tuvastada infotehnoloogilises infrastruktuuris toimunud arenguid ja selle põhjal tuua välja uusi soovitusi olukorra parandamiseks.

# 1. Taust

Käesolev peatükk on mõeldud sissejuhatava osana magistritöösse, et anda ülevaade IT infrastruktuuriga seotud mõistetest ja selle auditeerimise vajalikkusest. Samuti tutvustakse konkreetset organisatsiooni ja selle IT infrastruktuuri, tuues välja teema olulisuses konkreetse organisatsiooni tasemel.

## *1.1 Mis on IT infrastruktuur?*

Infotehnoloogiline infrastruktuuri koosneb ühe organisatsiooni puhul järgmistest komponentidest: riistvara, tarkvara, telekommunikatsioonivahendid, infotehnoloogilised protsessid ja infotehnoloogia alane dokumentatsioon.

Mida kujutab endast optimeeritud infotehnoloogiline infrastruktuur? Infotehnoloogiline infrastruktuur, mis suudab kõige paremini kohanduda organisatsiooni muutuvate vajadustega.

## *1.2 Mida annab organisatsiooni jaoks IT infrastruktuuri auditeerimine?*

Põhjused, miks on vaja ühe organisatsiooni jaoks IT infrastruktuuri auditeerida:

- tehnoloogiline sõltuvus - organisatsioonides kasvab pidevalt sõltuvus infotehnoloogiast;
- tehnoloogia lai levik - IT on muutunud märkimisväärseks organisatsiooni toodete ja teenuste edastamise kanaliks;
- keerukus - IT infrastruktuur muutub suuremaks, rohkem hajusamaks ja keerukamaks;

- paindlikkus – muutuvad ärivajadused toovad kaasa selle, et kasutajad nõuavad uusi teenuseid ja enamasti tuleb neid pakkuda olemasoleva infrastruktuuri peal;
- klientide rahulolu – kliendid muutuvad vähem tolerantsemaks tehnoloogilistele tõrgetele, mis mõjutavad peamiste ärifunktsioonide tööd;
- investeeringud – paljude organisatsioonide jaoks IT investeeringud moodustavad kaaluka osa eelarvest, sellest lähtuvalt nõutakse IT-lt rohkem pikemaajaliste väärtuste loomist investeeringutest sõltuvalt;
- ettevalmistusaeg toodete turuküpseks saamisel – üleüldine konkurents ja lühemad tehnoloogiate elutsüklid, mis loovad konkurentsieelise, tõstavad vajadust tuua uusi tooteid ja teenuseid turule lühema ajakuluga.

IT infrastruktuuri auditeerimise kasu organisatsiooni jaoks auditi tulemuste ellu rakendamisel väljendub selles, et IT infrastruktuuri teenused vastavad efektiivsemalt äripoole vajadustele, mille tõttu on organisatsioonil võimalik saavutada edu läbi produktiivsuse tõusu. Organisatsioonilised kasutegurid IT auditeerimisel: teenuste käideldavuse ja kvaliteedi tõstmine kastutajate jaoks, parem võimekus vastata kasutajate infotehnoloogilistele vajadustele, muudatuste läbiviimine IT infrastruktuuris avaldab vähem kahjulikku mõju, probleemide lahendamine muutub palju efektiivsemaks, IT infrastruktuuri haldamise kulud vähenevad, väheneb tõrgete esinemise oht ja nende tõrgete tekkimise mõju on võimalik paremini minimeerida.

IT infrastruktuuri auditeerimise kasu IT üksuse enda jaoks väljendub muutumises rohkem tõhusamaks ja efektiivsemaks. IT poolsed auditeerimise kasutegurid: a) muutub IT infrastruktuuri haldamine – väheneb ressurssi vajadus kahjulikke mõjudega toime tulekuks; b) probleemide haldamine – teenustasemete jälgimine võimaldab erinevaid trende ja probleeme süsteemis kiiresti avastada ja lahendada. See omakorda vähendab probleemide arvu ja nende lahendamiseks vajaminevat ressurssi; c) probleemide ettenägemine – võimalikke jõudluse, mahu ja käideldavuse probleemide ettenägemisel on võimalik koheselt algatada probleeme vältivaid tegevusi; d) aitab IT juhtidel paremini aru saada nende IT infrastruktuurist ja selle tõttu vastu

võtta paremini informeeritud otsuseid selle arendamiseks; e) väheneb IT töötajate töökoormus (tegeletakse vähem nö. tulekahjude kustutamisega); f) väheneb IT risk mitte vastata äri vajadustele; g) uute tehnoloogiate avastamine, mis omakorda aitab vähendada kulusid, parandada teenustasemeid või kergendab äriprotsesside parandamist ja nende innovaatilisust; h) IT laienemise ja teenuste uuenemise parem planeerimine – säilitatakse parem nõudluse ja olemasolevate mahtude tasakaal, et organisatsioon saab palju efektiivsemalt ära kasutada oma ressursse.

## *2.1 Majandus- ja Kommunikatsiooniministeeriumi tutvustus*

Majandus- ja Kommunikatsiooniministeerium Vabariigi valitsuse seaduse järgi valitsusasutus, mis on riigieelarvest finantseeritav ning mille seadusega või seaduse alusel antud põhiülesandeks on täidesaatva riigivõimu teostamine. (Majandus- ja Kommunikatsiooniministeerium 2009)

Ministeeriumi valitsemisalas on riigi majanduspoliitika ja majanduse arengukavade väljatöötamine ning elluviimine tööstuse, kaubanduse, energeetika, elamumajanduse, ehituse, transpordi (sealhulgas transpordi infrastruktuur, veondus, transiit, logistika ja ühistransport), liikluskorralduse (sealhulgas liiklus raudteel, maanteedel ja tänavatel, vee- ja õhuteedel), liiklusohutuse suurendamise ja liiklusvahendite keskkonnakahjulikkuse vähendamise, informaatika, telekommunikatsiooni, postside ja turismi valdkonnas; riigi infosüsteemide arendamise koordineerimine; tehnoloogiline arendustegevus ja innovatsioon; metroloogia, standardimise, sertifitseerimise, akrediteerimise, tegevuslubade, registrite, tööstusomandi kaitse, konkurentsijärelevalve, tarbijakaitse, ekspordiarengu ja kaubanduse kaitsemeetmete korraldamine; ettevõtluse regionaalse arengu ja investeeringute alased küsimused, vedelkütuse miinimumvaru haldamine ning vastavate õigusaktide eelnõude koostamine. (Majandus- ja Kommunikatsiooniministeerium 2009)

Ministeeriumi põhiülesanded ( § 12 ) :

1) valitsemisala valdkondades riigi arengukavade väljatöötamine ja nende kooskõla tagamine üleriigiliste arengukavadega, nende finantseerimise, elluviimise ja tulemuste hindamise korraldamine;

2) osalemine üleriigiliste majanduse arengut puudutavate arengukavade väljatöötamisel koostöös teiste asjaomaste ministeeriumidega;

3) valitsemisala valdkondade korraldamiseks õigusaktide eelnõude koostamise, nende põhiseadusele ja seadustele vastavuse tagamine ning õigusaktidega määratud ülesannete täitmine;

4) valitsemisalas rahvusvahelise koostöö korraldamine, sealhulgas Euroopa Liidu ja rahvusvaheliste organisatsioonide alane tegevus;

5) riigi infosüsteemide arendamise koordineerimine;

6) valitsemisala valdkondades võimalike hädaolukordade väljaselgitamiseks riskianalüüsi tegemine ja valitsemisala kriisireguleerimisplaani koostamine ning selle rakendamine hädaolukorras.
(Majandus- ja Kommunikatsiooniministeerium 2009)

Lisaks kuuluvad ministeeriumi haldusalasse järgmised valitsemisala asutused: a) ametid - Konkurentsiamet, Tehnilise Järelevalve Amet, Lennuamet, Maanteeamet, Tarbijakaitseamet, Veeteede amet; b) hallatavad riigiasutused – Eesti Riiklik Autoregistrikeskus, Patendiraamatukogu, Riigi Infosüsteemi Arenduskeskus; c) sihtasutused - Krediidi ja Ekspordi Garanteerimise Sihtasutus KredEx, Arengufond, Ettevõtluse Arendamise Sihtasutus, Eesti Akrediteerimiskeskus, Riigi Infokommunikatsiooni Sihtasutus, Tallinna Tehnoloogiapargi Arendamise SA; d) mittetulundusühingud – Eesti Standardikeskus, Maailma Energeetikanõukogu Eesti Rahvuskomitee. Samuti on ministeerium seotud osade riigi osalusega riigiettevõtetega juhtimisega: Eesti Energia, Eesti Post, Eesti Raudtee, Estonian Air, Tallinn Sadam jne.

Ministeeriumis struktuur koosneb juhtkonnast (minister, ministri nõunikud, kantsler, abid) ja osakondadest. Ministeeriumi põhilised struktuuriüksused osakonnad jagunevad veel omakorda: põhitegevuse osakonnad, põhitegevusi integreerivad osakonnad, tugiosakonnad ning spetsiifilisi ülesandeid täitvad osakonnad.

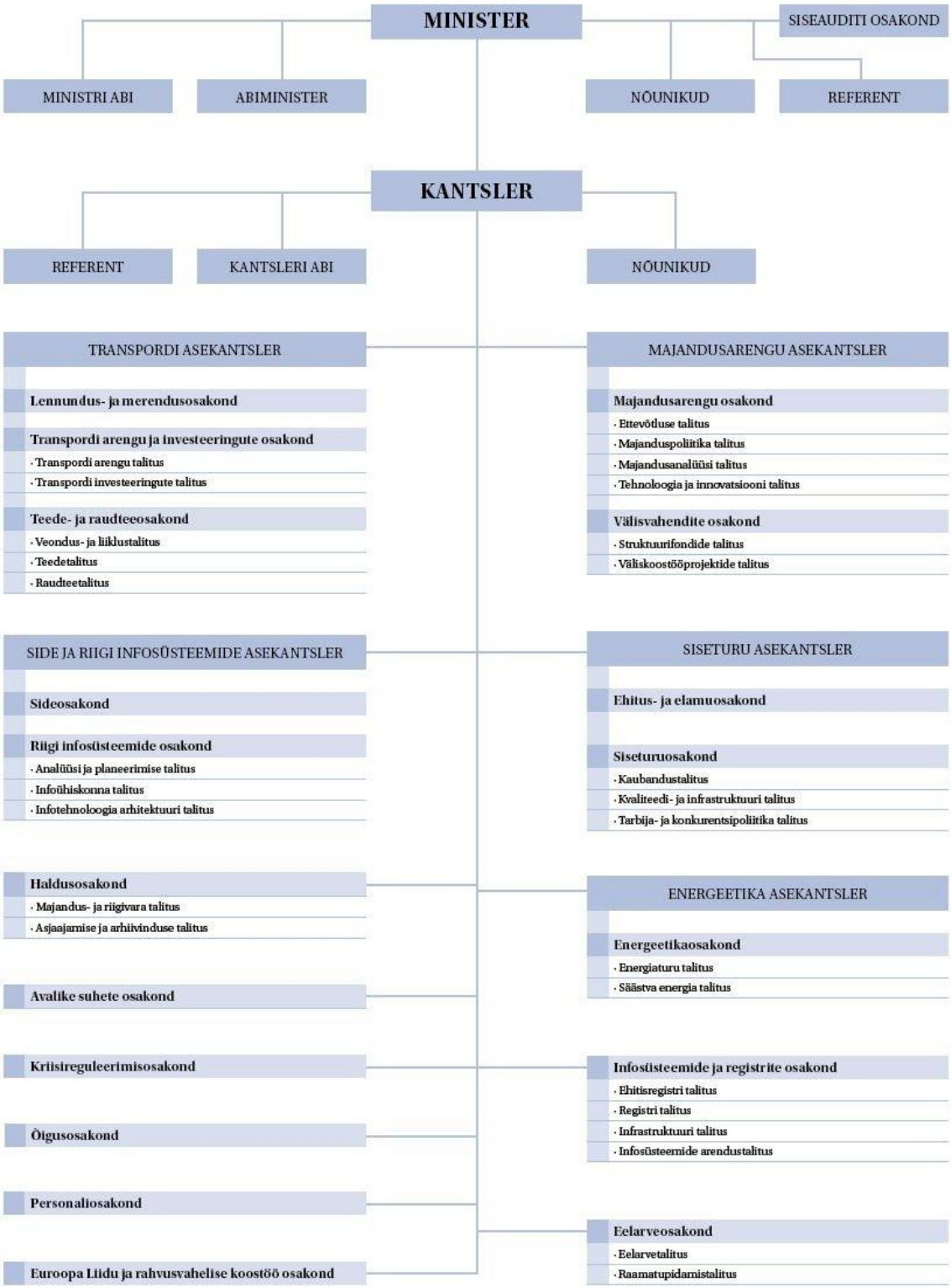
Põhitegevuse osakondades toimub ministeeriumi ülesannete täitmine valitsemisalaga määratud valdkonda. Põhitegevuse osakonnad jagunevad: energeetikaosakond, siseturuosakond, lennundus- ja merendusosakond, teede- ja raudteeosakond ning sideosakond.

Põhitegevusi integreerivates osakondades toimub ministeeriumi tegevuse eesmärgi täitmine valitsemisalasse kuuluvate erinevate valdkondade ühtse ning tasakaalustatud arendamise ja omavahelise seostamise kaudu. Põhitegevusi integreerivad osakonnad jagunevad: Euroopa Liidu ja rahvusvahelise koostöö osakond, majandusarengu osakond, välisvahenditeosakond, transpordiarengu ja investeeringute osakond ning õigusosakond. (Majandus- ja Kommunikatsiooniministeerium 2009)

Tugiosakondades toimub ministeeriumi igapäevast tööd toetav tegevus. Tugiosakonnad jagunevad: avalike suhete osakond, haldusosakond, eelarveosakond, personaliosakond, siseauditi osakond ning infosüsteemide ja registrite osakond. (Majandus- ja Kommunikatsiooniministeerium 2009)

Spetsiifilisi ülesandeid täitvateks osakondadeks on riigi infosüsteemide osakond ja kriisireguleerimise osakond.

Joonisel 1 leheküljel 16 on esitatud MKM-i struktuuri skeem, kus on välja toodud struktuuriüksused koos alluvussuhetega. Skeem on esitatud 2009 kevade seisuga.




**Joonis 1. MKM-i struktuuri skeem seisuga 2009 kevad**

### 2.1.1 Infosüsteemide ja registrite osakonna lühitutvustus

Osakonna põhiülesanneteks on ministeeriumi ja ministeeriumi valitsemisala riigiasutuste infosüsteemide arengutegevuse kavandamine, koordineerimine ja tagamine, ministeeriumi varustamine infotehnoloogilise riist- ja tarkvaraga, registrite pidamine, arendamine, haldamine ning nende üle järelevalve teostamine ning andmekogude haldamise ja arendamise korraldamine. (Majandus- ja Kommunikatsiooniministeerium 2009a)

Osakonnas koosseisus töötab 24 inimest, kellest suurem osa jaotub struktuuris 4 talituse vahel: a) registri talitus (5 töötajat), b) ehitisregistri talitus (4 töötajat), c) infrastruktuuri talitus (8 töötajat), d) infosüsteemide arendustalitus (4 töötajat).

Põhjusel, et magistritöö keskendub infotehnoloogilise infrastruktuuri optimeerimisele Majandus- ja Kommunikatsiooniministeeriumis ja selle haldusalas, siis seda tegevust korraldaks ministeeriumi struktuuri järgi infosüsteemide ja registrite osakonna infrastruktuuri talitus.

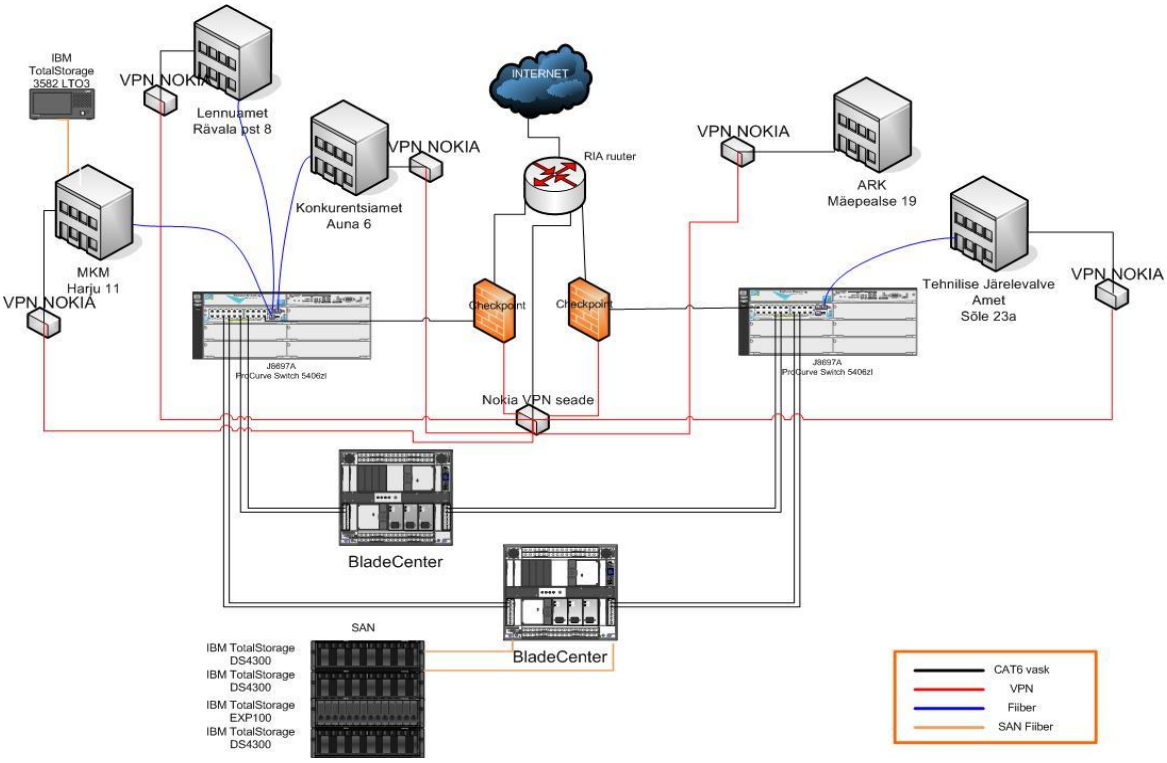
Infrastruktuuride talituse ülesanded:

1) korraldab ministeeriumi ja ministeeriumi valitsemisala infosüsteemide ja infotehnoloogia infrastruktuuri arendamist ja haldamist, tagades nende häireteta töö;
2) korraldab ministeeriumi ja Konkurentsiameti ning Tehnilise Järelevalve Ameti varustamist infotehnoloogiavahenditega ja nende eest tasumist;
3) korraldab rakenduste ja andmebaaside arendamist, juurutamist ja hooldust;
4) korraldab ja planeerib koostöös personaliosakonnaga infosüsteemide kasutajate koolitust;
5) abistab ja nõustab ministeeriumi teenistujaid IT alal ning korraldab kasutajatel tekkivate IT probleemide asjakohase ja viivitamatu lahendamise;
6) töötab välja infoturbe põhimõtted ning meetmed ja tagab volitatud kasutajatele juurdepääsu süsteemidele, andmetele ja programmidele ning arvutivõrgus andmete säilimise vastavalt kehtestatud korrale;

7) töötab välja arvutitöökoha riist-ja tarkvarastandardid ja tagab nende nõuetekohase täitmise.
(Majandus- ja Kommunikatsiooniministeerium 2009a)

### 2.1.2 MKM-i IT infrastruktuuri tutvustus

MKM-i infotehnoloogilist infrastruktuuri kasutab hetkel kuskil 850 kasutajat, kellele kõigile pakutakse ühtseid keskseid teenuseid. MKM IT infrastruktuuri kasutavad asutused ja allasutused: 1) Majandus- ja Kommunikatsiooniministeerium, 2) Lennuamet, 3) Tehnilise Järelevalve Amet, 4) Autoregistrikeskus, 5) Konkurentsiamet. Süsteemis on 930 arvutitöökohta ning lisaks on veel 56 serverit, mis pakkuvad erinevaid teenuseid. MKM-i sisevõrk paikneb 30 erinevas geograafilises punktis üle terve Eesti. Alljärgneval Joonisel 2 on välja toodud võrguline ülesehitus MKM-i IT infrastruktuurist.




**Joonis 2. MKM-i IT infrastruktuuri ülesehitus**

Põhilised kesksed IT teenused MKM-i IT infrastruktuuris:

- E-posti ja grupitöö teenus MS Exchange 2003 koos spämmitõrjega;
- Rakendusserverite majutusteenus (Apache ja IIS);
- Andmebaasiserverite majutusteenus (MSSQL, MySQL, Postgre, Progress);
- Varundusteenus koostöös IBM-iga (Tivoli Storage Manager);
- Veebipõhine grupitöö keskkond (MS Sharepoint ja MS Project Server);
- Võrguteenuste haldamine (VPN, Wifi, LAN, DHCP, DNS, DC, IAS, DFS, X-tee, tulemüürid);
- Dokumendihalduse teenused (GoPro, Postipoiss);
- Finantsinfosüsteemide teenused (Navision Axapta, Taavi, Eeva);
- Arvutitöökohtade haldusteenus (rühmapoliitikad, tarkvarahaldus, krüpteerimine, viirustõrje, tulemüür);
- Failijagamis- ja printimisteenuste haldus;
- Kasutajatoe teenus (Helpdesk) ja e-õppekeskkond Wiki;
- Terminalteenused (nt. Kodutöö ja Eksamisüsteem);
- Serverite monitooringu teenused (MS System Center Operations Manager).

### 2.1.3 Teema aktuaalsus Majandus- ja Kommunikatsiooniministeeriumi jaoks

Teema on aktuaalne järgmiste põhiliste IT infrastruktuuri probleemide tõttu:

- Geograafiliselt laiali paisatud võrk. Kui arvutivõrk katab suuremat osa Eesti linnasid ja lisaks mõned väiksemad kohad, siis on keeruline kõigile pakkuda samu teenuseid või üritada tagada ühtlast turvataset;
- IT inimressurssi ebaefektiivne ära kasutamine. Tänu IT süsteemide konsolideerimisele on suudetud liita omavahel põhilisemad IT teenused ning MKM on võtnud suure kohustuse neid hallata. Samas allasutuste spetsialistide koormus on tõsiselt vähenenud ja neid peaks kasutama ära kesksete süsteemide haldamises või arendamises;
- Rahaliste ressursside ebaefektiivne kasutamine. Igal asutusel on eraldi oma IT eelarve ja enamus tehnoloogiat hangitakse eraldi. Tihti juhtub seda, et hangitakse samu tooteid eraldi erinevates asutustes, kuigi kõiki asjade koos soetamine tuleks tunduvalt soodsam;
- IT haldusprotseduurid on erinevad allasutustes. Erinevate rakendusserverite süsteemide vohamine allasutustes. Haldamisprotsessid on suhteliselt vähe veel automatiseeritud. Arvutite tarkvaraline konfiguratsioon erineb igas asutuses.

**Auditeerimisest loodetav tulemus**

Auditi läbi viimine MKM-is ja haldusalas annaks ülevaatliku seisu infotehnoloogilise infrastruktuuri kohta, mille põhjal üritab autor välja tuua selle, et vaja on terviklikku lähenemist IT infrastruktuurile terves haldusalas. Selleks, et IT suudaks MKM-i haldusalas paremini kokku sobituda kogu organisatsiooni vajadustega - on vaja vaadata kaugemale, kui lihtsalt serverite ja teenuste konsolideerimine. Suund tuleb võtta suurema IT organisatsiooni loomiseks, millel oleks üks konkreetne eelarve ja optimeeritud inimressurss ning mis suudaks pakkuda omalt poolt kvaliteetseid teenuseid tervele haldusalale.

# 2. Enamlevinud IT infrastruktuuri auditeerimise metoodikad

Kõige enamlevinud on suurte tehnoloogiafirmade (nt. Microsoft, IBM) poolt välja töötatud infrastruktuuri auditeerimise metoodikad, kuna need on vabalt kõigile kättesaadavad ja nende levikule aidatakse kaasa läbi partnervõrgustiku. Lisaks tegelevad väga paljud audiitorid ise vastavate metoodikate välja töötamisega, kuna valdkond on väga perspektiivikas, kuigi kahjuks nende tegemiste kohta on autoril vähe informatsiooni.

## *2.1 Microsoft Core Infrastructure Optimization*

Microsofti poolt välja töötatud Microsoft Core Infrastructure Optimization (edaspidi CIO) raamistik, mis aitab organisatsioonil arendada välja turvalisemalt, paremini hallatavamat ja dünaamilisemat IT infrastruktuuri. Raamistiku rakendamisel praktikas on võimalik vähendada IT kulusid, kasutada paremini ära olemasolevat ressurssi ning muutuda IT infrastruktuuril paremini ärivajadustele vastavaks. (Microsoft 2009)

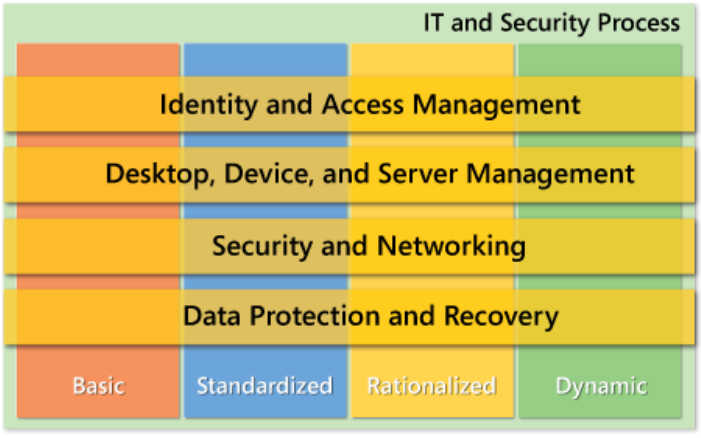
Vastava auditeerimismeetodi puhul eksisteerib 4 küpsustaset:

1. Baastase. Kasutakse manuaalseid ja lokaalseid haldusprotsesse, minimaalset keskset kontrolli, ühtsed standardid ja IT poliitikad puuduvad mitmetes valdkondades. Sellel tasemel puudub organisatsioonil teadmine enda infrastruktuuri osade kohta ja samuti taktika, kuidas kõige paremini kasu saada infrastruktuuri arendamisest. IT poolt pakutavate teenuste ja rakenduste kohta on vähene ülevaade;
2. Standardtase. Rakendatakse kontrolli infrastruktuuri üle läbi standardite ja poliitikate kasutamise. Need võimaldavad organisatsioonis hallata paremini arvuti töökohti ja servereid. Kasutatakse Active Directory teenust ressursside haldamiseks, turvapoliitikate rakendamiseks ja ligipääsude kontrollimiseks. Kuigi teadmine organisatsioonis on olemas infrastruktuuri parandamiseks, tehakse seda suhteliselt vähe;

3. Ratsionaliseeritud tase. Kulutused arvuti töökohtade ja serverite haldamisel on väga madalad. Kasutusel olevad IT haldamise protsessid ja poliitikad on arenenud sinnamaale, et nad mängivad tähtsat rolli äripoole toetamises. Turvalisuse rakendamises kasutatakse selgelt ennetavaid poliitikaid alates arvuti töökohast, serveritest kuni tulemüürini;
4. Dünaamiline tase. Organisatsiooni on täielikult teadlik, millist väärtust pakub infotehnoloogiline infrastruktuur, et nende äri oleks veel efektiivsem ning konkurentsi-võimelisem. Kõik IT kulud on täielikult kontrollitavad. Lisa investeeringud tehnoloogiasse on valdkonnapõhised ning võimaldava äri jaoks anda kiiresti mõõdetavaid tulemusi. Võimaldab kõige paremat integreeritust kasutajate, andmete, arvuti töökohtade ja serverite vahel. IT alane koostöö kasutajate ja struktuuriüksuste tasemel on laialt levinud. Mobiilsetele kasutajatele on sõltumata nende asukohast tagatud samad võimalused teenuste kasutamiseks. Kõik IT protsessid on täielikult ära automatiseeritud tehnoloogia abil. Kõik eelpool mainitu võimaldab IT-l paremini kohanduda muutuvate organisatsiooni vajadustega.
   (Microsoft 2009)

CIO audit hindab IT infrastruktuurist hindab viit erinevat valdkonda ja püüab nende läbi määrata arengutaset: a) identiteedi ja ligipääsude haldamine; b) arvuti töökohtade, serverite ja seadmete haldamine; c) turvalisus ja võrgu kasutamine; d) andmete kaitsmine ja taastamine: e) IT ja turvaprotsesside haldamine.

Alljärgnev Joonis 3 tutvustab CIO auditi raamistiku osasid.




**Joonis 3. Microsoft Core Infrastructure Optimization mudel**

## *2.2 IBM Dynamic Infrastructure*

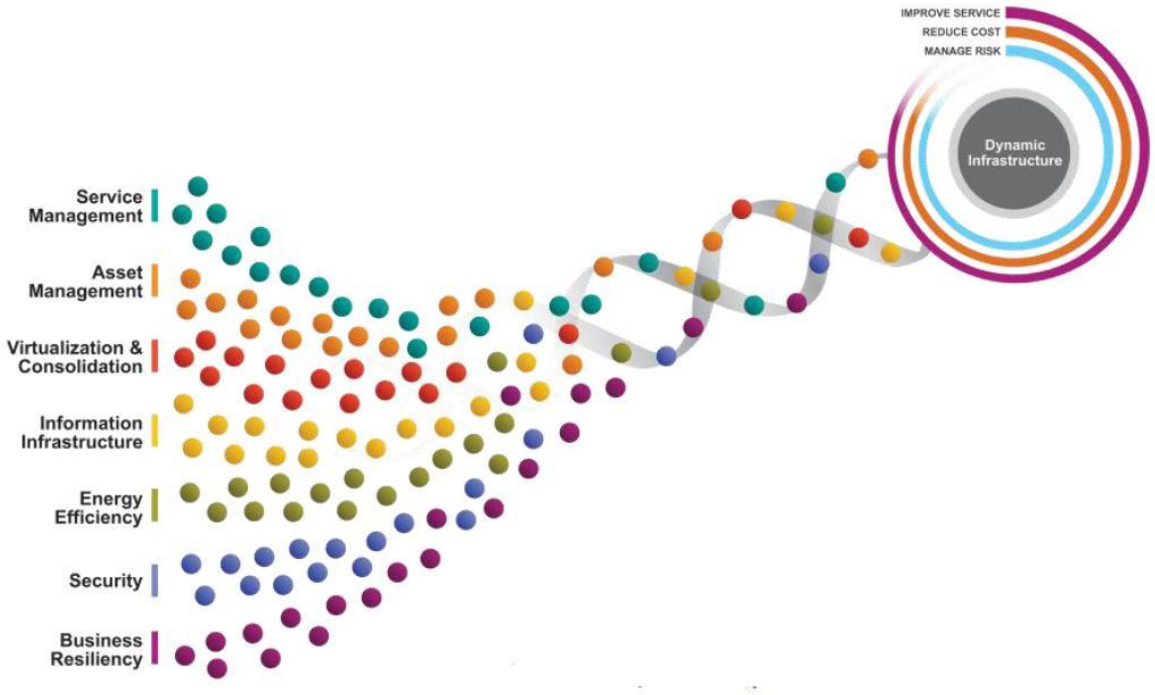
IBM-i poolt loodud dünaamilise infrastruktuuri raamistik, mis integreerib äri ja IT selliselt, et IT vastaks äri eesmärkidele. Pakutakse välja targem ja uuem lähenemine läbi kolme eesmärgi püstitamise: parandada IT teenuseid, vähendada kulusid ja hallata riske. (IBM 2009)

Auditi põhielemendid, millele organisatsiooni IT infrastruktuuri vastavust hinnatakse ja mille baasilt arendusettepanekuid tehakse:

- teenuste haldamine. Teenuste haldamise lahendused, mis aitavad luua ja hallata ärile orienteeritud ja dünaamilist infrastruktuuri selleks, et paremini reageerida muutustele ja tagada teenuste kõrgem kvaliteet madalama hinnaga;
- varade haldamine. Konkreetsete riistvara, tarkvara ja teenuste välja pakkumine selleks, et tõsta varade töövõimet ja väärtust;
- virtualiseerimine. Läbi virtualiseerimise ja konsolideerimise aidatakse vähendada IT keerukust, muutes serveriruumis kasutatava tehnoloogia rohkem elastsemaks ja turvalisemaks – samal ajal kulusid vähendades;
- energia kasutamise efektiivsus. Pakutakse välja lahendused, mis aitavad serveriruumis kasutatavat tehnoloogiat muuta energiasäästlikumaks läbi efektiivsema elektri ja jahutuse kasutamise;
- informatsiooni infrastruktuur. Hõlmab endas tarkvara, serverite, salvestusseadmete ja võrkude integreerimist selleks, et informatsioon oleks turvaliselt kogu aeg kättesaadav. Selleks kasutatakse erinevaid lahendusi, mis tagaksid info käideldavuse, säilivuse, turvalisuse ja vastavuse;
- äri jätkusuutlikus ja võime muutustega kohaneda. Pakutakse välja lahendused, mis hoiavad äri töös erinevate sisemiste ja väliste ohtude tekkimisel ning võimaldavad IT inimestel tegeleda vähem nn. tulekahjude kustutamisega;

- turvalisus. Turvalahendused, mis võimaldavad organisatsioonil luua terviklik ja ärile orienteeritud lähenemisviis turvalisusele, sidudes selleks riskihalduse ja IT valitsemise raamistiku. Põhieesmärk on tagada kiire ja turvaline teenuste kätte toimetamine. (IBM 2009)

Alljärgnev Joonis 4 annab ülevaate IBM Dynamic Infrastructure auditi raamistiku põhielementidest.




**Joonis 4. IBM Dynamic Infastructure mudel**

## *2.3 Erinevate audiitorite poolt välja töötatud metoodikad*

Suur osa IT infrastruktuuri hindamise metoodikatest on audiitorite või auditeerimisega tegelevate ettevõtete poolt välja töötatud. Nende metoodikate puhul tavaliselt kohandatakse auditi metoodikat kliendi vajadustele ja auditi läbiviimise skoobile. Samas leiab kõikide selliste uuemate auditi metoodikate puhul sarnaseid mõõtmise valdkondi: kasutatava riistvara ja tarkvara

hindamine, olemasoleva dokumentatsiooni vastavuse kontrollimine, riskide tuvastamine, üldisele IT toimivusele hinnangu andmine. Samuti kasutatakse suhteliselt standardseid eesmärke auditi läbi viimiseks: a) IT infrastruktuuri kulude vähendamine. Nt. töökoha arvutite ja serverite parem ära kasutamine. Uute IT konsolideerimise ja virtualiseerimise eesmärkide leidmine; b) olemasoleva keskkonna standardiseerimine ja lihtsustamine. Üritatakse tuvastada mitte standardsed ja vananenud tehnoloogiad, mille kasutamine muudab organisatsiooni ebaefektiivsemaks; c) rohelise mõtlemise juurutamine – mõõdetakse IT energiakulu ja CO2 emissioone selleks, et selgitada välja IT poolt tekitatav ökoloogiline jalajälg. Uute keskkonda säästvate tehnoloogiate kasutusele võtmise soovitamine; d) riskide maandamine ja turvalisuse tõstmine. Hinnatakse organisatsiooni poolset võimekust oma infovarasid kaitsta ja puudusi IT teenuste kättesaadavuses. Pakutakse välja ettepanekud kaardistatud puuduste likvideerimiseks ja riskide minimeerimiseks.

Täpsemat informatsiooni erinevate audiitorite ja auditeerimisfirmade konkreetsete kasutatavate metoodikate kohta on tihti keeruline saada, kuna väga paljudel juhtudel võidakse seda lugeda ärisaladuseks, mis võiks sama valdkonna konkurentidele anda eeliseid.

## *2.4 Probleem olemasolevate metoodikate kasutamisega*

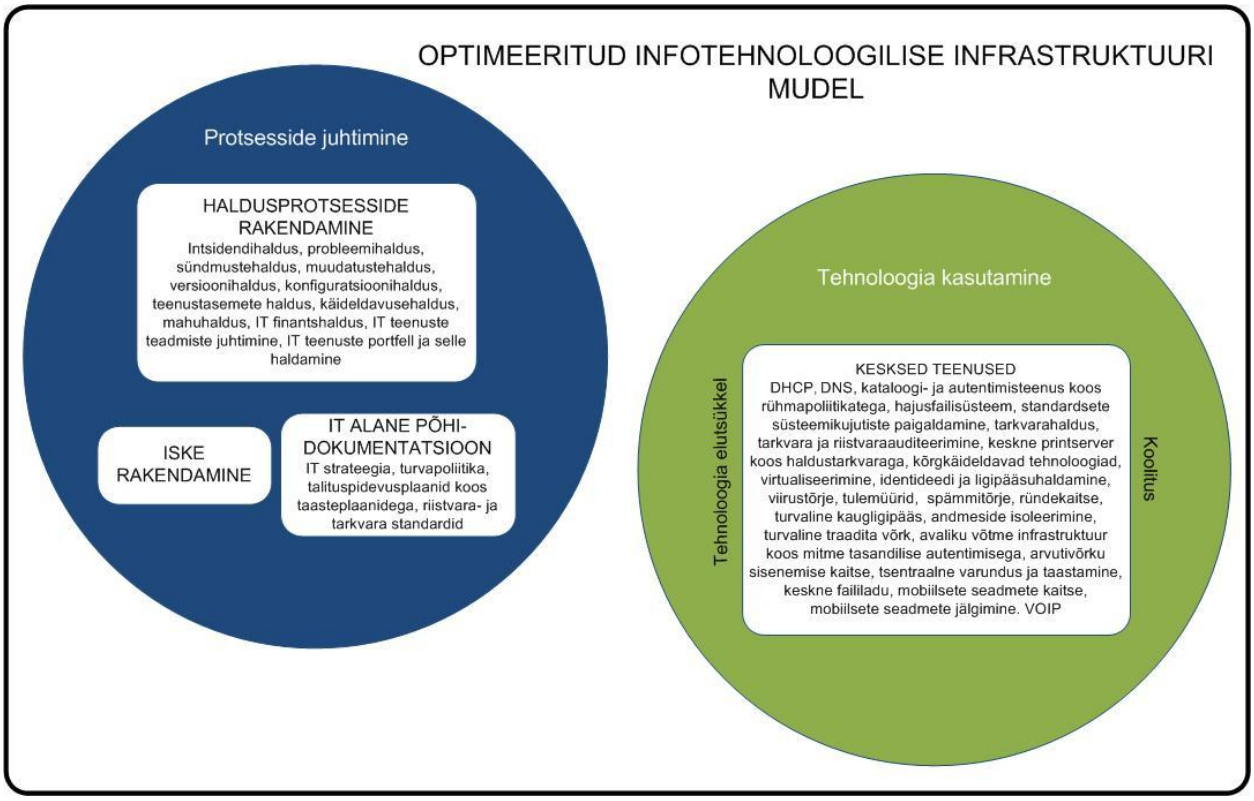
Põhiliselt saab siin keskenduda ainult 2 suurema tehnoloogiafirma (Microsoft ja IBM) auditeerimise metoodikale, sest teiste kohta puudub lihtsalt autoril piisavalt avaliku informatsiooni. Sisuliselt on Microsofti ja IBM-i metoodikad väga head, kuna mõlemad täidavad täielikult oma eesmärki, sest üritavad olemasoleva IT infrastruktuuri puhul leida probleemseid kohti ja pakkuda erinevaid võimalusi nende parandamiseks. Samas on nende juures üks tõsisem viga selles, et auditi tulemusel pakutakse konkreetseid tootjapoolseid tehnoloogilisi lahendusi, mida auditeeritav peaks hakkama hankima oma IT infrastruktuuri optimeerimiseks. Selle tõttu on mõneti auditi poolt kaardistatavad IT infrastruktuuri komponentide skoop piiratud, kui konkreetset tehnoloogiat tootja müügiportfellis ei ole, siis audit neid olemasolevaid komponente ei kaardista. Lähtuvalt sellest probleemist koostas autor endapoolse optimeeritud IT infrastruktuuri mudeli.

# 3. Optimeeritud IT infrastruktuuri mudel

Mudeli välja töötamisel on lähtutud ITIL-i poolsest IT infrastruktuuri määratlusest ning selle läbi jaotud mudel kahte põhivaldkonda: tehnoloogia kasutamine ja IT protsesside juhtimine (sisaldab endas alamvaldkondi: IT alane põhidokumentatsioon, IT infrastruktuuri haldusprotsesside rakendamine, infosüsteemide turvameetmete süsteemi ISKE rakendamine). Suurema osa valdkonnapõhiste komponentide paika panemisel on autor lähtunud enda kogemustest ja kogunud kokku info, milliseid keskseid tehnoloogiaid, regulatsioone või haldusprotsesse kasutatakse ning võrrelnud nende vastavust hetkel teadaolevatele parimatele praktikatele. Ülejäänud komponentide väljatöötamisel on üritatud välja selgitada olemasoleva IT infrastruktuuri puudusi, mida autor ise on avastanud või mis on selgunud erinevat tüüpi IT alaste auditite läbi viimisel, tehes seda samuti läbi parimate praktikate võrdluse. Seega lõplik mudel sisaldab autori endapoolset nägemust optimeeritud IT infrastruktuurist.

Joonisel 5 leheküljel 27 on tekitatud terviklik vaade optimeeritud infrastruktuuri mudelile tuues välja kõik selle põhivaldkonnad, alamvaldkonnad ja komponendid.

Järgnevalt on tekstis iga valdkond kirjutatud lahti infrastruktuuri komponentideks näidatates missugust lisaväärtust annab ühe või teise tehnoloogia, regulatsiooni või haldusprotsessi rakendamine organisatsioonile.




**Joonis 5. Optimeeritud infotehnoloogilise infrastruktuuri mudel**

## *3.1 Tehnoloogia kasutamine*

### DHCP ja DNS teenuse kasutamine

DHCP teenust pakkuv server aitab suuri arvutivõrke hallata palju efektiivsemalt. Tsentraalne võrguserver jagab automaatselt arvutitele edasi järgneva informatsiooni võrgu kohta: nimeserverid, alamvõrgumask, võrgu lüüs (gateway) ja personaalne IP aadress. DHCP teenuse eelised: a) automatiseerib alamvõrkude kohta arvestuse pidamist. Nt. millised IP aadressid on hetkel kasutusel ja kes neid kasutavad; b) dokumenteerib kohaliku võrgu külastused; c) tsentraliseerib võrgus olevate seadmete häälestamist; d) kergendab suurte muudatuse rakendamist IP protokolli konfiguratsioonis. Nt. Nimeserverite ja lüüside info saab vahetada ilma iga seadet eraldi üle häälestamata; e) võimaldab rakendada IP aadresside jagamisel piiranguid konkreetses alamvõrgus; f) kasutajad saavad lihtsamini liikuda võrgust võrku.

Nimeserveri teenust (DNS) on vaja selleks, et ära siduda omavahel domeeninimi ja selle vastav IP aadress võrgus ning jagada seda informatsiooni edasi nimeserveri klientidele. DNS-i teenuse kasutamise lisafunktsioonid: a) suhtlemine teiste nimeserveritega – juhul, kui nimeserver ise ei saa nimelahendusega hakkama, siis on võimalik saata päringud edasi teistele nimeserveritele lahendamiseks; b) nimeserveri tsoonide haldamine ja ülekanne – nimeserver saab edastada olemasolevate tsoonide infot teistele serveritele, et need suudaksid samaväärselt oma kliente teenindada; c) jõudluse suurendamine – nimeserveri poolt teenindavate klientide arvu kasvades saab kasutada erinevaid tehnikaid selleks, et vähendada nimepäringutele vastamise aega. Nt. koormuse jaotamine, päringute salvestamine (caching); d) administreerimisinfo lisamine domeeninimedele.

Tehnoloogia näited DHCP teenuse puhul: DHCPD, Microsoft DHCP.

Tehnoloogia näited DNS teenuse puhul: BIND, Microsoft DNS, Simple DNS Plus, PowerDNS.

**Kataloogi- ja autentimisteenuse kasutamine koos rühmapoliitikatega**

Kataloogi- ja autentimisteenuse puhul on tegemist kahe sümbioosis oleva teenusega ning sellepärast tasub neid vaadata koos. Kataloogiteenus (LDAP) osa kujutab endast tsentraalset andmebaasi, kuhu on võimalik koondada kokku infot IT infrastruktuuri kohta, alates selle kasutajatest (kasutajakontod) ja gruppidest ning lõpetades seadmete ( nt. arvuti töökohad, serverid, printerid jne.) ja kesksete teenustega (nt. e-postiteenus). Autentimisteenuse ( nt. Kerberos) osa loob turvalise kihi kataloogiteenuse peale ja võimaldab teostada kataloogiteenuse andmebaasis olevate kasutajate, gruppide, seadmete ja teenuste tuvastamist. Kataloogi- ja autentimisteenuse kasutamisest saadav kasu: a) informatsiooni turvalisus – kataloogiteenuse andmebaasi objektidele saab määrata erinevaid ligipääsu reegleid. Lisaks saab välja töötada turvapoliitikad, mis võimaldavad tõsta kataloogiteenusega seotud seadmete ning kasutajakontode turvalisust; b) rühmapoliitikate põhised haldamisprotsessid; c) laiendatavus – kataloogiteenuse andmebaasi on võimalik luua uusi objekt uute teenuste jaoks; d) skaleeritavus – võrgu tasemel on võimalik kokku siduda omavahel erinevaid domeene, et tagada parem suhtlus teiste sarnaste teenustega ja neid omavate asutustega; e) andmetest koopiate tegemine – kataloogiteenuse andmeid saab edastada teistesse sarnastesse serveritesse, tagades nii parema informatsiooni kättesaadavuse, koormusjaotuse ja parema jõudluse kogu teenusele; f) integratsioon nimiserveri

teenusega – nimeserverite infot hoitakse tihti kataloogiteenuse andmebaasis ja tänu sellele saavad kataloogiteenuse kliendid ühenduse kataloogiteenust pakkuvate serveritega; g) paindlik päringute süsteem andmete välja võtmiseks.

Koos kataloogi- ja autentimisteenusega on võimalik kasutada rühmapoliitikaid, mis aitavad suurenda kontrolli kasutajate ja arvutite üle domeenis. Rühmapoliitikate rakendamisel tõuseb produktiivsus läbi järgmiste komponentide: standardiseeritud tarkvaralise konfiguratsiooni häälestus ja automaatne õiguste jagamine. Seega näiteks väheneb märgatavalt vajadus teha eraldi arvuti töökohtadele spetsiifilisi häälestusi kasutusmugavuse ja turvalisuse parandamiseks.

Tehnoloogia näited : OpenLDAP+Kerberos, Active Directory, Tivoli Directory Server.

**Hajusfailisüsteemi kasutamine**

Tegemist on süsteemiga, mille kasutamine võimaldab organisatsioonil kokku koguda kõik erinevad failiserverite välja jagatud kaustad ja panna need ühte selgesse kaustastruktuuri ehk hajusfailisüsteemi. Selle kasutamise võlu peitub selles, et kasutaja näeb alati enda andmete asukohaks võrgus hajusfailisüsteemi linki ja juhul, kui midagi peaks juhtuma selle failiserveriga on suhteliselt lihtne kasutajad suunata teise asukohta, kuhu on need samad andmed juba kopeeritud. Lisaks võimaldab hajusfailisüsteem jagada koormust erinevate serverite vahel, kuna andmed paiknevad erinevates kohtades.

Tehnoloogia näited: Microsoft DFS, OpenAFS.

**Standardsete süsteemikujutiste (image) kasutamine ja nende tsentraalne haldamine**

Süsteemikujutiste tegemine võimaldab olemasoleva arvuti operatsioonisüsteemi, andmete ja programmide seisu kloonimist ühte faili või failidesse. Seda sama faili originaal arvuti süsteemist kasutades on võimalik pärast luua täpselt sarnaseid kloonsüsteeme teiste arvutitesse, kui oli originaalsüsteem. Süsteemikujutiste kasutamisega saavutatakse märkimisväärne kokkuhoid IT spetsialisti poolt töökoha paigaldamiseks kuluvast ajast ning samuti tagatakse täpselt sama tarkvaraline konfiguratsioon kõikides arvutites. Samas lihtsalt süsteemikujutiste kasutamine ei taga veel maksimaalset efektiivsust - selle saavutamisele aitab kaasa tsentraalne süsteemikujutiste paigaldamise tarkvara.

Tsentraalne süsteemikujutiste paigaldamise tarkvara võimaldab ühest kesksest asukohast paigaldada üle võrgu süsteemikujutisi serveritele, lauaarvutitele, sülearvutitele ja seadmetele vähendades nii tunduvalt paigaldusega seotud ajakulu. Lisaks saab migreerida kasutaja profiile koos seadistusega, häälestada süsteemikujutiste paigaldamise ajakava ning paigalduse lõppedes lisada automaatselt kõiki tarkvaralisi uuendusi.
Tehnoloogia näited: Altiris Deployment, Microsoft System Center Configuration Management, Landesk, Tivoli Provisioning Manager for OS Deployment, KBOX.

**Keskne tarkvarahaldus koos tarkvara ja riistvara auditeerimisega**

Protsess, mis sisaldab endas tarkvara paigaldamist, hooldust, kasutamist ja eemaldamist ning sellega seotud hangete optimeerimist. Tarkvarahalduse eesmärk on vähendada tarkvara soetuskulusid ning minimeerida õiguslikke ja ärilisi riske, mis seotud selle kasutamisega. Hea tarkvarahaldus tõstab IT operatiivsust ja lõppkasutaja produktiivsust. Tarkvarahalduse lisaväärtused: a) süsteemist kogutakse kokku alginfo riistvarast ja tarkvarast ning selle põhjal tekib ülevaatlik andmebaas; b) saab teostada järjepidevat inventuuri süsteemis – igal ajahetkel on teada, millist riistvara ja tarkvara kasutatakse; c) tarkvaralist seisu on võimalik võrrelda ostetud litsentside kogustega – tekib teadmine, kas kasutusel olev litsentside arv vastab ostetule; d) tarkvarahalduse poliitikate rakendamise kaudu on võimalik seadme tarkvaralisse konfiguratsiooni sisse viia muudatusi (installeerida, uuendada ja eemaldada tarkvara) sobival ajamomendil ning rakendada neid mitmele seadmele korraga; e) tekib tarkvarahalduse plaan – teame, kui tihti arvutite tarkvaralist konfiguratsiooni kontrollida ning millise tarkvara installeerimist lubada või mida mitte.
Tehnoloogia näited: Altiris Client Management Suite, Microsoft System Center Configuration Management, WinINSTALL, Novell ZENworks Patch Management, WMI+skriptid.

**Keskse printserveri ja selle haldustarkvara kasutamine**

Hästi väikese asutuse (kuni 10 töötajat) puhul on keeruline põhjendada keskse printserveri vajadust. Probleem tõuseb suurema kasutajate arvuga võrkudes, kus printerite lokaalne häälestamine võib muutuda tülikaks ning võrguprinterid ei pruugi hästi hakkama saada mitmete kasutajate paralleelse teenindamisega. Sellisel puhul aitab printserveri kasutusele võtmine

tunduvalt nende haldamisprotseduure lihtsustada: kõik printerid on ühest võrgu asukohast kätte saadavad, ei pea käsitsi riistvaralisi draivereid paigaldama ja uuendama, printimistööde koormust on võimalik jagada, saab kasutada automaatset printeri paigaldust läbi võrgu kasutajale kataloogi- ja autentimisteenuse abiga ja paraneb printimisteenuse kättesaadavus.

Kesksele printserverile lisaks haldustarkvara kasutamine võimaldab paremini kontrolli alla võtta printserveris toimuvat: a) koguda kasutajate ja seadmete statistikat (kes, mida ja kui palju prindib); b) monitoorida printereid (kättesaadavus võrgus, teavitatakse toonerite ja paberite otsa saamisest ning tehniliste rikete tekkimisest); c) võimaldab kasutada lahendusi, kus kasutaja ei ole enam seotud konkreetse printeriga, vaid saab vajaliku printimistöö sellisest printerist, kust ise soovib; d) võimaldab rakendada piiranguid printimisteenuse kasutamisele (nt . kasutaja- või grupipõhised limiidid).

Tehnoloogia näited: Uniflow, Print Audit, Callisto, PrintManager Plus.

**Kõrgkäideldavate tehnoloogiate kasutamine teenuste majutamisel**

Teenuste kõrgkäideldavuse nõuded määratakse IT-le tavaliselt organisatsiooni poolt ( nt. kasutades selleks teenustasemelepinguid ) selleks, et tagada võimalikult parim teenuste kättesaadavus minimaalse maasoleku ajaga. Saavutatakse see tavaliselt kasutades klasterdamise tehnoloogiat, mis võimaldab omavahel kokku siduda üle võrgu kaks või enam arvutit, pannes need üheskoos funktsioneerima kui üks arvuti. Juhul, kui midagi ühe arvutiga peaks juhtuma võtavad teised selle masina töö üle. Klasterdamise tehnoloogia jaguneb omakorda järgmistesse kategooriatesse: a) kõrgkäideldavad (High Availability) klastrid – eesmärk tagada maksimaalne käideldavus teenusele kasutades selleks lisa seadmeid; b) koormust jagavad (Load Balancing) klastrid – eesmärk tagada maksimaalne jõudlus teenuse jaoks kasutades selleks lisaseadmeid; c) võrkandmetöötlus (Grid computing) klastrid – eesmärk suure hulga seadmete ühendamine selleks, et saavutada maksimaalne arvutusvõimsus konkreetse ülesande lahendamiseks, d) pilvandmetöötlus (Cloud Computing) klastrid – eesmärk seadmete ühendamine vähendamaks kasutaja poolseid kulusid riistvarale ja tarkvarale, sest andemete töötlemine toimub pilve sees, kus kasutajale on eraldatud just temale vajalik minimaalne ressurss.

Tehnoloogia näited: Linux HA, Microsoft Cluster Server, Microsoft NLB, Citrix Cloud Center, IBM Grid & Grow, Linux Virtual Server.

**Riistvara virtualiseerimise rakendamine**

Tegemist sellise tehnoloogia rakendamisega, mis võimaldab ühele serverile installeerida palju üksteisest sõltumatuid nn. „virtuaalseid masinaid“, mis kõik kasutavad ühte ja sama füüsilist ressurssi, kuid paistavad kasutajatele eraldiseisvatena. Virtualiseerimistarkvaral on kaks põhilist lähenemist: serveriruumi kulude kokkuhoidmine ning tarkvara testimine kontrollitud olukorras. Kui ühe serveri peal jooksutada ühte rakendust, siis võib esineda suure tõenäosusega ressursi raiskamist. Mida rohkem on asutusel servereid, seda rohkem tuleb tähelepanu pöörata nende ülalpidamise kuludele: jahutus, elekter ja hooldus. Kõige suurem pluss virtualiseerimise juures ongi nende kulude kokkuhoid. Praktikas võib see säästlikkus alles ilmneda ligi 15 ja enama serveri asendamisel ühe mitmerakenduslikuga.

Tehnoloogia näited: VMWare, Windows 2008 Hyper-V, Citrix XenServer.

**IT seadmete optimaalne elutsükkel**

Arvuti töökohtade, serverite ja muude IT seadmete optimaalseks elutsükliks loetakse 3-4 aastat, mille möödudes tuleks kindlasti olemasolev seadmete park ära uuendada [Gartner]. Selline kiire elutsükkel on tingitud tavaliselt kiiresti toimuvast innovatsiooni tegevusest nii tehnika-, kui tarkvara tootjate hulgas. Seadmete kasutusaja üleminek eelpool mainitud 3-4 aastast toob omakorda kaasa järgmiste probleemide tekke: a) tõuseb seadmete omamiskulu; b) kasvab riistavara seadmete ja operatsioonisüsteemide erisus seadmete pargis; c) lõppkasutaja jaoks langeb seadmetega töötamise produktiivsus ning suureneb erinevate rikete oht.

Kõikide amortiseeruvate varade soetamise puhul on kõige mugavam kasutada rentimise mudelit, mis loob järgmised eelised: a) alati viimasel tasemel tehnoloogia ja organisatsioonile sobiv toodete elutsükkel; b) võimaldab kiiresti ja paindlikult tegutseda muutuvate vajaduste puhul; c) vähendab IT varade omamise seotud kogukulu.

**Kasutajate koolitamine vastavalt organisatsiooni vajadustele**

Hea kasutajate IT alane koolitus annab organisatsiooni jaoks väga palju juurde. Seda juhul, kui koolituse korraldamisel lähtutakse organisatsiooni vajadustest, koolitatava konkreetsetest tööülesannetest ning koolituse tulemusi mõõdetakse läbi konkreetsete organisatsiooniliste

näitajate paranemise. Vastavalt organisatsiooni vajadustele koolitamine toimub kahel juhul: a) uue töötaja tööle tulekul – tutvustakse uutele töötajale kõiki IT teenuseid ning infosüsteeme. Pakutakse võimalust koheselt täiendada teadmisi kasutusel olevast standardtarkvarast ja infosüsteemidest; b) uute tarkvarade või infosüsteemide juurutamisel – nt. uue versiooni tarkvara kasutusele võtmisel on kasutajal võimalik saada koheselt koolitust.

Koolituse positiivne mõju avaldub organisatsioonis järgmiselt: tõuseb kasutajate arvutikasutamise oskus ja rahuolu töökohaga, paraneb klientide rahuolu, kasvab produktiivsus ja teenuste kvaliteet, vähenevad kulud ja tõusevad tulud.

**Identiteedi ja ligipääsu haldamine**

Lihtsamalt öeldes on tegemist protsessiga, mis tagab, et õiged inimesed saaksid ligi õigetele asjadele (teenused, infosüsteemide jne.) IT infrastruktuuris õigel ajal. Ilma identiteedi ja ligipääsu haldamiseta tekivad kasutajaandmed ja kontod mitmesse süsteemi korraga ehk kasutajal on igas süsteemis erinev konto, mille tõttu nende andmetega ümber käimine on keerukas protsess ning toob kaasa lisa turvariske. Identiteedi ja ligipääsu haldamise tarkvara kasutamisest saadav kasu: a) paraneb kaitse andmete lekkimise vastu - tekib tsentraalne andmekogu infovarade ligipääsu kohta kasutaja põhiselt, mis on integreeritud kataloogi- ja autentimisteenusega; b) kasutajal on ainult üks identiteet, mida ta kasutab mitmes infosüsteemis korraga; c) kasutaja jaoks lihtsustub autentimisprotseduur – korra ennast süsteemi vastu autentides (kiipkaart või parool) saab teistesse süsteemidesse ilma uuesti autentimiseta ehk teostatakse automaatne sisselogimine, d) väheneb kasutajatoe koormus, kuna kasutajal tekivad vahendid enda paroolide või PIN koodide muutmiseks.

Tehnoloogia näited: RSA Identity Protection and Verification Suite, Microsoft Identity Lifecycle Manager 2007, Novell eDirectory, IBM Tivoli Access Manager, Sun Identity Management.

**Keskne viirustõrje arvutitöökohtadel ja serverites**

Keskne viirustõrje kaitseb tervet IT infrastruktuuri viiruste, pahavara ja muude nendega seotud ohtude vastu. Tsentraalne viirustõrje vähendab organisatsiooni jaoks riske, mis on seotud võrgukatkestuste, andmete või töö produktiivsuse kadumisega, identiteedi vargusega või teiste turvaintsidentidega. Miks peab kasutama keskset viirustõrje lahendust: a) tekib tervik pilt viirustõrje programmi kasutuse kohta. Nt. kasutatav viirustõrjetarkvara versioon, kasutatavad viirustõrje mustrid, tekkinud turvaintsidendid, tõrked viirustõrje tarkvara töös; b) turvaohu avastamisel on võimalik ohu allikas võrgust eemaldada; c) toimub keskne viirustõrjetarkvara kliendi tarkvara ja viirustõrje mustrite uuendamine.
Tehnoloogia näited: Trend Micro Officescan, F-Secure, Kaspersky, McAfee.

**Keskne spämmitõrje**

Seadme- või serveripõhine lahendus olemasolevas süsteemi kaitsmiseks spämmikirjade (ebasoovitavad e-kirjad) eest, kus spämmi kaitse ei toimu kasutaja postkasti sees – spämmikiri üritatakse tuvastada ja peatada enne selle jõudmist kasutaja postkasti. Keskse spämmitõrje lahenduse plussid: a) spämmikirjad peatatakse enne kasutaja postkasti hoidvat serverit. Väheneb meiliserverite jõudluse ja mahu vajadused. Kasutaja näeb vähem spämmikirju enda e-postkastis; b) tsentraalne haldamine. Tekib keskne ülevaade e-posti liiklusest ja lihtsam on leida kuhugi kinni jäänud e-kirjasid; c) spämmitõrje süsteemi komponentide (filtrid, antiviirus jne.) uuendamist on tunduvalt lihtsam läbi viia ühes kohas; d) spämmirünnakuid on tunduvalt kergem blokeerida; e) võimalik integreerida teiste teenustega. Nt. kataloogi- ja autentimisteenusega.
Tehnoloogia näited: Postix + Spamassassin+antiviirus, Cisco Ironport, Barracuda Spam Firewall.

**Keskne tulemüür integreeritud viirustõrjega ( teenuste ja sisevõrgu kaitse, serverite kaitse ja arvuti töökohtade kaitse)**

Tulemüür on tarkvara või riistvara, mis kontrollib Internetist ja sisevõrgus tulevat teavet ning seejärel, kas blokeerib selle või lubab vastavate reeglite põhjal arvutisse või võrku. IT infrastruktuuris kasutatakse tavaliselt kahte tüüpi keskseid tulemüüre:
a) keskne tulemüür, mis paigaldatakse sisevõrgu välisvõrgu vahele, eraldamaks kahte võrku füüsiliselt. Kaitse skoobiks on organisatsiooni sisevõrk ja teenused; b) keskne tulemüür, mis paigaldatakse sisevõrgus olevate kõikidele seadmetele selleks, et filtreerida sisevõrgu liiklust ja vajadusel vastavalt kaitsta sisevõrgu seadet välisvõrku sattudes. Kaitse skoop arvuti töökohad, serverid ja seadmed.
Kindlasti tuleb kasutada mõlemat tüüpi tulemüüre arvutivõrgu ja selle seadmete kaitsmisel. Kesksete tulemüüride kasutamisest saadav kasu on põhifunktsioonide tasemel mõlemal sarnane: võimaldab defineerida ja rakendada standardsed tulemüüri poliitikad nii serveritele kui arvuti töökohtadele, toimuvad turvaintsidendid kogutakse ühte kohta, võrgu liikluses viiruste tuvastamine, ründetuvastus, sissetuleva ja väljamineva liikluse filtreerimine.
Tehnoloogia näited teenuste ja sisevõrgu tulemüüril: CheckPoint, Juniper, Cisco.
Tehnoloogia näited arvuti töökohtade ja serverite tulemüüril: Symantec Endpoint Protection, Trend Micro Officescan.

**Ründekaitse tarkvara kasutamine**

Tegemist on tarkvaraga, mis monitoorib võrgu ja süsteemide tegevusi ning otsib nendest pahatahtlikku või ebasoovitavat käitumist, mida reaalajas takistada. Ründekaitse tarkvara pakub täpsemat informatsiooni üliaktiivsete seadmete, ebaõnnestunud autentimiste, ebasoovitavate pakettide sisu ja teiste võrgu- või rakendustaseme funktsioonide kohta. Tarkvara kasutamise plussid: a) puhastab võrguliiklust ebasoovitavatest tegevustest - andes nii rohkem võrguressurssi missioonikriitilistele rakendustele ja teenustele; b) blokeerib automaatselt rünnakud – jättes nii võimaluse testida turvapaikasid enne nende paigaldamist ning säilitades seejuures süsteemi ülevaloleku; c) kaitstakse süsteemi nullpäeva rünnakute (viiruserünnak süsteemile samal päeval,

kui viirustõrjetarkvara arendamisega seotud organisatsioonid tegelevad selle avastamisega) eest. Tehnoloogia näited: Snort, TippingPoint IPS, Cisco IPS, CheckPoint IPS-1.

**Turvaline kaugligipääs teenustele**

Suuremal osal tänapäeva organisatsioonidel on vajadus tagada oma töötajatele, partneritele ja klientidele vastav turvaline ligipääs organisatsiooni sisemistele teenustele ja arvuti töökohaga seotud keskkondadele (dokumendid, rakendused, e-post jne.) väljastpoolt asutuse võrku. Kaks enamlevinud turvalise kaugligipääsu lahendust on: a) VPN ehk virtuaalne privaatvõrgu tehnoloogia, mis loob kahe üksteisest eemal asetseva punktis vahel turvalise andmeside kanali; b) terminalserver tehnoloogia, mis tekitab välistele kasutajatele ühe konkreetse serveripõhise võrguühenduspunkti.

Kuigi funktsionaalsuse poole pealt on mõlemad lahendused turvalise kaugligipääsu rakendamisel erinevad, siis nende rakendamisest saadav kasu on suhteliselt sarnane: a) suureneb organisatsiooni geograafiline seotus – töötada saab asukohast sõltumata; b) tõuseb töö produktiivsus ja vähenevad kontorikulud – selleks, et tööd teha ei pea enam kontorisse minema.

Tehnoloogia näited VPN: Citrix Access Gateway, OpenVPN, Juniper SA Series, CheckPoint SSL Extender, Microsoft Intelligent Application Gateway 2007, F5 FirePass SSL.

Tehnoloogia näited terminalserver: LTSP, MS Windows Server 2008 Terminal Services.

**Serverite ja töökohtade vahelise andmeside isoleerimine sisevõrgus**

Mida suuremaks kasvab organisatsioon ning mida rohkem teenuseid pakutakse läbi selle sisevõrgu, seda keerulisemaks muutub arvutivõrgu füüsilise ligipääsu turve. Nt. klientide, külaliste ja partnerite eest, kes kasutavad asutuse sisevõrku. Samuti on traadita võrgu tehnoloogia laiem levik muutnud tunduvalt keerulisemaks võrgu füüsilist turvet. Selleks, et juba eelnevalt vältida võimalikke turvaprobleemide (infoliikumise pealtkuulamine, ebaterve huvi võrgus olevate teenuste kohta jms.) tekkimist sisevõrgus füüsilisest võrgu ligipääsust, tuleb isoleerida serverid ja arvutitöökohad kõigest ülejäänust.

See on võimalik läbi vastavate andmeside krüpteerimise ja autentimistehnoloogiate koostööna, mille tõttu tekib eraldi turvaline võrgu kiht sisevõrgu peale. Selline sisevõrgu isoleerimine annab järgmist lisaväärtust: a) tekib eraldi turvatud võrk asustuse sisevõrgu sisse; b) paraneb kontroll, kes ja kuhu peaks ligi pääsema ning sellest jääb alati jälg maha; c) vähenevad kulud. Vastav füüsiline võrgu isoleerimine on tunduvalt kallim; c) väheneb hallatavate seadmete hulk võrgus; d) pahavara rünnakute ja muude küberrünnakute mõju saab kergesti minimeerida võrgus; f) andmevahetust krüpteeritakse info kaitsmiseks.
Tehnoloogiate näited: IPSec ja teised VPN tehnoloogiad.

**Turvaline traadita võrk sisevõrku pääsemiseks**

Kõige viimane trend turvalise traadita võrgu (Wifi) loomiseks soovitab ära jätta uute investeeringute tegemist spetsiaalsetesse traadita võrku lahendustesse ning teha seda palju lihtsamalt. Kuidas võiks välja näha optimeeritud turvaline traadita võrk IT infrastruktuuris: a) traadita võrku käsitletakse, kui välisvõrku ning eraldatakse see vastavalt füüsiliselt sisevõrgust; b) turvalise ühenduse loomiseks sisevõrku kasutakse VPN ühendust. Nt. Sobib eriti hästi SSL protokolli kasutav VPN tehnoloogia.
Põhjused, miks kasutada ainult VPN ühendust spetsiaalsete traadita võrgu lahenduste asemel: a) tekib ainult üks keskne punkt võrguühenduste ja turvalisuse haldamiseks; b) kasutatav krüpteering ja andmete kaitsmise meetodid on tugevamad; c) erinevate traadita levialade vahel liikudes suudetakse hoida VPN ühendust katkemise eest.
Tehnoloogia näited on samad, mis turvalise kaugligipääsu VPN tehnoloogia puhul.

**Avaliku võtme infrastruktuuri kasutamine koos mitmetasemeliste autentimisskeemidega**

Autentimise protsess võiks koosneda 3 tasemest : a) midagi, mida sa tead (nt. parool); b) midagi, mis sul on olemas (nt. digitaalne võti, ID-kaart); c) midagi sellist, mida kellelgi teisel kunagi olla ei saa (nt. sõrmejälg, silma iiris ja allkiri). Suurem osa asutusi piirdub tavalisel ainult 1 taseme kasutamisega (kõige levinum on kasutajanime ja parooli põhine ligipääs) autentimisel ja sellest

tulenevad järgmised probleemid: kasutaja identiteeti on väga lihtne varastada või edasi anda ning krüpteerimata andmeid on väga lihtne lahti murda. (Rea 2007).

Avaliku võtme infrastruktuuri kasutusele võtmine koos erinevate autentimisskeemidega võimaldab neid riske päris kõvasti vähendada: a) kasutajaid autenditakse ilma paroole reaalselt edastamata; b) kasutajatel on võimalik teostada autentimist erinevate süsteemide vastu isegi siis, kui need asuvad erinevates võrkudes; c) keeruline on korraldada küberrünnakuid (nt. sõnaraamatu põhised ründed ei tööta, võtme lahti muukimine võtab mõttetult palju aega); d) integratsioon teiste tehnoloogiatega: turvaline traadita võrk, krüpteeritud failisüsteemid, turvaline e-post, automaatne sisselogimine jne.

Tehnoloogia näited: Cryptolog Unicity, IDControl USB Token, FingerTec

**Arvutivõrku sisenemise kaitse**

Tegemist on lahendusega, mis kontrollib sisevõrgus kasutaja arvuti ligipääsu võrguressurssidele, tehes ennem kindlaks selle vastavuse organisatsiooni poliitikale. Põhjused, miks on vaja võrgu ligipääsu kontrollida: a) võimaldab vähendada tarkvara uuendamata jätmisest tekkivaid probleeme. Põhiline väärtuse seisnebki selles, et on võimalik piirata arvuti töökoha ligipääsu võrgule, millel on puudu uuendatud viirustõrje, tarkvara uuendused või vajalik tulemüüri tarkvara. Eelpool mainitud elementides puuduste tuvastamisel saab võrgu ligipääsu kontrolliv süsteem käivitada vastavad uuenduse protsessid; b) ligipääsupoliitikate rakendamine. Võrguadministraatorid saavad luua erinevaid ligipääsupoliitikaid vastavalt arvuti töökoha tüübile või kasutaja rollile, ning rakendada neid juba võrguseadmete tasemel; c) identiteedi haldamine. Kui tavaliselt autentimist ja identiteedi haldamist tehakse rakenduste tasemel, siis arvutivõrgu sisenemise kaitset kasutades saab lisada juurde eraldi turvakihi, mis piirab teenustele ilma vastava õiguseta võrgu ligipääsu.

Tehnoloogia näited: Cisco NAC, FreeNAC, Juniper Unified Access Control, Netpass, Microsoft Network Access Protection.

**Tsentraalne varundus ja taastuslahendus**

Selle lahenduse puhul varundamisel arhiveeritakse kõik taastamiseks vajalikud andmed kesksesse salvestusseadmesse. Tsentraalse varunduse kasutamise korral on võimalik paremini tagada varundussüsteemi töötamise asukoha erinevus süsteemi käitamise asukohast. Keskse varundus ja taastelahenduse plussid: a) väheneb andmete deduplitseerimine ehk lihtsamalt öeldes ühte ja sama asja ei varundata mitu korda. Selle läbi omakorda vähenevad varundamise mahud ja aeg; b) varundusprotsess muutub läbipaistvamaks, sest tekib andmebaas, kus on sees kogu selle protsessi info: varundusplaanid ja detailne ülevaade varundus toimimise kohta koos vastavate raportitega; c) võimaldab lihtsamalt ja turvalisemalt teostada varundamist üle interneti. Nt. varundamine väiksematest kontoritest; d) saab integreerida teiste andmete salvestuslahendustega (SAN, NAS) tagamaks maksimaalselt kiire taasteaja.
Tehnoloogia näited: EMC Avamar, IBM Tivoli Storage Manager, Veritas Netbackup.

**Kasutajate profiilide hoidmine keskses failiserveris**

Tegemist on olukorraga, kus kasutaja arvuti profiilis olevad andmed (dokumendid, töölaud, brauseri lingid ja muu kasutajaga seotus seadistused) suunatakse kesksesse failiserverisse. Lauaarvuti puhul kasutatakse tavaliselt profiili otse suunamist serverisse ja sülearvuti puhul jäetakse profiilist koopia, mida sünkroniseeritakse serveriga. Profiliide serverisse suunamise kasulikkus : a) kasutaja seotud profiil ei ole seotud konkreetse arvutitöökohaga ning midagi ei juhtu arvuti katki minemisel; b) failiserveris tagatakse nende andmed kaitse – juhul, kui midagi peaks hävinema on võimalik andmed taastada varundusserverist või kasutaja enda poolt failiserveri vahekoopiast.

**Mobiilsete seadmete kaitse ja jälgimine**

Tänapäeva organisatsioonil kasvab pidevalt infosüsteeme kasutavate mobiilsete seadmete (nt. sülearvuti, PDA, mobiiltelefon) arv, sellega seoses suureneb ka risk nende seadmete ära

kadumiseks või varastamiseks. Kõige suurem kahju tavaliselt sellisel juhul ei ole seadme enda ära kaotamine vaid seadmes olevate andmete kadumine. Uuringute tulemusel on 49 % organisatsioonidest langenud sülearvuti varguse ohvriks 12 kuu jooksul (Ponemon Institute 2007). Organisatsiooni poolt on selle riski vähendamiseks mitmeid levinud viise: a) võtta kasutusele mobiilsete seadmete jälgimise tarkvara, mis võimaldab arvestust pidada väljaspool asutuse võrku olevate seadmete kohta (nt. tuvastada nende asukohta), kaitsta nendes olevaid andmeid (nt. käivitades üle võrgu andmete kustutamise või lukustamise) ja vajadusel uuendada nende tarkvaralist konfiguratsiooni; b) kasutaja autentimise protsessis kasutada biomeetrilisi andmeid (enamlevinud sõrmejälg) koos teiste riistvaraliste paroolidega (kõvaketta parool, BIOS-e parool) seadme käivitamiseks ja autentimise informatsiooni sisestamiseks. Autentimise protseduur arvuti käivitamisel ja autentimisinformatsioon sisestamisel muutub kahe tasemeliseks (parool + sõrmejälg) ning lihtsustub kasutaja jaoks paroolide meelespidamine; c) sülearvutis olevate andmete krüpteerimine kõvakettal. Seda soovitav kasutada seadmetes, kuhu on integreeritud riisvaraline turvakiip, mis suudab hallata krüptovõtmeid ning ei lase ennast ilma selleta kõvakettast lahti krüpteerida – juhul, kui seda pole on ikka võimalus kõvaketta andmete lahti murdmiseks väljaspool mobiilset seadet.
Tehnoloogia näited: Computrace, Backstopp, Adeon, The CyberAngel Wii-Trac, GadgetTrak.

**VOIP (Voice over IP)**

Tehnoloogia kõneside edastamiseks mööda andmeside võrku. VOIP telefonisüsteemi eelised võrreldes tavaliste telefonikeskjaamadega: a) vähenevad sidekulud ja seda eriti just läbi väliskõnede hinna alanemise; b) vähenevad elektrikulud, sest vana telefonijaamaga võrreldes säästavad VOIP telefonijaamad 50% kui mitte rohkem elektrit; c) vähenevad telefonivõrgu arendamise kulud – need, kes on seni arendanud eraldi telefoniside võrku, siis ei pea seda enam tegema, kuna selleks saab ära kasutada olemasolevat andmeside võrku; d) kaasnevad põnevad tehnoloogilised lisavõimalused: telefonikõnede salvestamine ja taasesitamine, telefoninumbrit on võimalik läbi arvuti või mobiilse seadme kasutada igal pool hea interneti ühendusega kohtades,

andmete edastamine jpm.
Tehnoloogia näited: IPCentrex, Innovaphone, Cisco Unified Communications.

## *3.2 Protsesside juhtimine*

### IT strateegia

Tegemist on detailse kogumiga organisatsiooni infotehnoloogilistest eesmärkidest, põhimõtetest ja taktikatest. Traditsiooniliselt pannakse see kirja dokumendina, mis seletab lahti, kuidas infotehnoloogia kasutamisega toetatakse organisatsiooni põhiprotsesside optimeerimist – seega IT strateegiat tuleb vaadelda organisatsiooni strateegia osana. Hea IT strateegia protsess organisatsioonis koosneks järgmistest etappidest: a) strateegia välja töötamine (vastuste leidmine küsimustele: kus me oleme? kuhu tahame minna? kuidas me sinna saame?); b) strateegia ellu rakendamine ja selle täitmise tulemuste mõõtmine.
IT strateegia eemärgid: a) tõsta organisatsiooni väärtust läbi infotehnoloogia. Nt. uute toodete või teenuste välja töötamine, aidata muutuda efektiivsemaks läbi kulude vähendamise; b) kasutajate / klientide rahulolu tõstmine. Nt. uute projektide lõpetamine õigeaegselt ja eelarve piires, tagada süsteemide töökindlus, kiirem probleemide lahendamine läbi kasutajatoe; c) organisatsiooni tööprotsesside kvaliteedi tõstmine; d) tulevikusuund potentsiaalsete võimaluste leidmiseks. Organisatsiooni tööprotsesside pidev parandamine vajab kogemustega ja hea motivatsiooniga töötajate poolt organisatsiooni strateegiaga ühtivate eesmärkide leidmist.

### IT turvapoliitika

Organisatsiooni infoturbe alusdokument, mis kehtestab reeglid, abinõud, protseduurid turvalisuse tagamiseks. Infoturbepoliitika on mõistlik koostada kasutades ISO 13335 ja 27002 standardi suuniseid (nt. http://www.ria.ee/public/ISKE/Infoturbe_poliitika_sisukorra_naidis.pdf). Turva-poliitika eesmärk on organisatsiooni infovarade majanduslikult optimaalselt kaitsmine

mitmesuguste ohtude eest – selleks, et tagada talitluse jätkuvus, minimeerida organisatsiooni riske ning suurendada investeeringute tasuvust.

**Riist- ja tarkvarastandardite rakendamine**

Tegemist on dokumendiga, mis kehtestab infrastruktuuris oleva riistvara, tarkvara ja infosüsteemide ühetaolisuse ning selle läbi tagab nende kergema hallatavuse. Riist- ja tarkvarastandard koosneb järgmistest komponentidest: a) riistvaralised minimaalsed nõuded (nt. riistava puhul tuleb nendele mitte vastavaid seadmeid hakata välja vahetama) ja maksimaalsed nõuded (spetsifikatsioon, millest lähtutakse hangete tegemisel); b) tarkvaraline konfiguratsioon arvutitöökohtadel, serveritel ja rakendusplatvormidel. Juhul, kui ei ole organisatsioonis ühtset standardit võivad tekkida järgmised probleemid: ostetud tooted ja lahendused ei sobi olemasolevate lahendustega kokku. Keeruline on põhjendada tehnoloogiliste uuenduste vajadust juhtkonnale.

Standardi rakendamise efekt: a) vähenevad hooldus-, haldus- ja koolituskulud; b) välditakse võimalikke probleeme süsteemide integreerimisel; c) kasutava riist- ja tarkvara ühtlustamine vähendab nende hankekulusid; d) vähenevad turvariskid; e) kasutaja jaoks luuakse mugav ja efektiivne töökeskkond.

**Organisatsiooni talituspidevuse ja taasteplaneerimine**

Talitluspidevuse planeerimine aitab ette valmistuda kriisideks, mis võivad mõjutada organisatsiooni normaalset toimimist. Ilma vajaliku ettevalmistuseta võib kriisi lahendamine ja sellest välja tulemine võtta päevi, nädalaid või isegi kuid ning samuti kaasneb põhitegevuse katkemisega kahju saamata jäänud tulu näol. Talitluspidevusplaani põhikomponendid: a) põhiprotsessi ja tugiprotsesside kirjeldus koos oluliste ressurssidega; b) kriiside määratlus, vastutava kriisijuhi määramine ja kriisiteavituse korraldus; c) alternatiivtegevuste kavad ja oluliste ressursside taasteplaanid; d) plaani kaasajastamise, koolituse ja testimise korraldus. Talituspidevusplaan tuleb tavaliselt integreerida taasteplaaniga, mis kirjeldab rolle, vastutusi

ning tegevusi äri- ja muude protsesside taastamiseks pärast ettenägematu põhitegevuse katkestust.

**ISKE rakendamine**

ISKE on infosüsteemide kolmeastmeline etalonturbe süsteem. ISKE rakendamine on kohustuslik riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavate infosüsteemide ning nendega seotud infovaradele turvalisuse tagamiseks. ISKE süsteem põhineb turvet vajavate infovarade kirjeldamisel tüüpmoodulite abil ning sisaldab vahendeid iga tüüpmooduli turvaklassi määramiseks ja mooduli nõutava turbeastme määramiseks selle turvaklassi järgi. Sõltuvalt tüüpmooduli nõutavast turbeastmest määratakse mooduli turvaspetsifikatsiooni kaudu etalonkataloogidest turvameetmed ja kontrollitakse mooduli turvalisust ohtude etalonkataloogi abil. (ISKE 2008, 9). Peale selle, et ISKE rakendamine on kohustuslik seadusega riiklike andmekogude pidajatele, annab selle rakendamine reaalset kasu: a) minimeeritakse andmekogude pidamisega seotud riske; b) tõstetakse üldist infoturbe teadlikust organisatsioonis; c) tagatakse andmete parem ja turvalisem kaitse.

**Teenustasemete haldamine**

Selleks sõlmitakse vastav leping teenuse osutaja ja kliendi vahel, mis kirjeldab ära teenuse osutamise parameetrid. Tüüpiline teenustaseme leping koosneb järgmistest punktidest: teenuse kirjeldus, teenuse osutamise parameetrid, tuleviku prognoosid teenuse osutamisel, osapoolte kohustuste kokkuvõte, intsidendi- ja probleemihaldus, osapoolte teavituse korraldamine, lepingut mõjutavad muudatused, kahju hüvitamine, järelevalve.

Probleemid teenustaseme lepingute puudumisel: 1) pole organisatsioonis täpselt aru saada, millisel tasemel IT teenust pakutakse; 2) äripool ei näe põhjust, millest on tingitud suured kulud teenuste ülahoiule; 3) IT-lt nõutakse kulutuste vähendamist - samas tõstetakse nõudeid teenuse pakkumisel; 4) määratud on ebarealistlikud ja ühepoolsed teenustasemed.

Teenustaseme lepingutest loodetav kasu: a) suurendada äripoole jaoks IT teenuste väärtust;

b) panna paika selged ootused IT teenuste kättesaadavuse koha pealt; c) luua mõõdikute süsteem IT teenuse osutamise mõõtmiseks, d) siduda teenuste osutamisel tekivad ülahoiu kulud reaalsete vajadustega.

**Intsidentide haldamine**

Tegevused, mille eesmärgiks on kindlustada lõppkasutaja IT teenuste võimalikult kiire taastamine läbi intsidentide määratlemise, registreerimise, diagnoosimise, lahendamise ja sulgemise. (ITSMF 2007).Võimalikult kiire taastamise aeg on tavaliselt reguleeritud teenustaseme lepinguga. Intsidendihaldus on kasutajatoe kõige tähtsam ja suurem ülesanne. Intsidendihaldus peaks olema üks osa kasutajatoe rakendusest või sellega tihedalt seotud. Intsidendihalduse mitte rakendamine toob kaasa järgmised probleemid: a) kui keegi ei halda intsidente, hakkavad nad mõjutama IT teenuse kvaliteeti; b) kasutajatoe spetsialistide töö on rohkem häiritud ja selle tõttu vähem efektiivsem; c) intsidendid võivad kaduma minna või neid lahendatakse puudulikult.
Intsidendihalduse rakendamise positiivne efekt : a) äritegevus on intsidentidest vähem mõjutatud; b) võimaldab koguda informatsiooni intsidentide kohta (intsidentide jälgimine, ajalugu, analüüs ); c) IT spetsialistide töö on produktiivsem; d) paraneb kasutajate rahulolu.

**Probleemide haldamine**

Probleemihaldus aitab vältida või ära hoida tulevasi intsidente. Korduvad või struktureeritud intsidendid viivad sageli suuremate probleemideni ja mitmete pöördumisteni kasutajatoe osutajate poole samade küsimustega. Probleemihaldus töötab eesmärgiga tagada IT infrastruktuuri stabiilsus ning välja selgitada ja kõrvaldada süstemaatiliselt esinevaid intsidente IT infrastruktuuris. Probleemihalduse mitte rakendamine toob kaasa selle, et: a) organisatsioon lahendab probleeme siis, kui teenustega töö on klientide jaoks katkestatud; b) kasutaja kaotab IT struktuuriüksuse vastu usalduse; c) ebaefektiivne tugi organisatsioonile, kõrged kulud ja töötajate madal motivatsioon, kuna samu intsidente lahendatakse pidevalt uuesti ilma keskse lahenduseta.

Probleemihalduse rakendamise kasu: väheneb korduma kippuvate intsidentide esinemissagedus, suureneb süsteemi stabiilsus ja toimivuse aeg, võimalus mõõta probleemi avastamise ja lahenduse vahelist aega parandamaks kasutajatuge.

**Sündmuste haldamine**

Protsess, mille eesmärk on tuvastada ja kategoriseerida kõik sündmused ning otsustada nende põhjal vajalikud tegevused. (ITIL Service Operation 2008, 35). Sündmuste haldamine on tihedalt seotud igapäevaste IT süsteemide haldustööde tegemisega. Sündmuste haldamine koosneb järgmistest komponentidest: monitoorimine, grupeerimine, lahendamine, uuesti läbivaatamine ja sulgemine. Sündmuste haldamise rakendamine aitab tagada stabiilset IT töökeskkonda ning vältida paremini intsidentide teket või tagab nende kiirema lahendamise.
Tehnoloogia näited : Tivoli Monitoring, BMC Patrol, HP Openview NNM, NetIQ AppManager jt.

**Muudatuse haldamine**

Infrastruktuuri või teenuste igasuguse aspekti muudatuste kontrollimise tegevus sellisel ohjatud viisil, mis võimaldab viia miinimumini muudatustest tingitud intsidentide mõju teenuste kvaliteedile. (ITSMF 2007). Uuringud näitavad, et 80% nn. IT kriiside tekkest on põhjustatud inimlikest vigadest, ning suurem osa tekkinud probleemidest IT-s on seotud inimeste väheste IT alaste teadmistega ja need süvenevad seoses süsteemi keerukuse tõusuga. ( Spafford 2005). Muudatustehalduse rakendamisest saadav kasu: a) paraneb muudatustest tingitud riskide juhtimine; b) muudatustest tingitud mõju teenuste kvaliteedile ja teenustasemetele on väiksem; c) kasutaja enda töö on vähem mõjutatud muudatustest; d) parem kulude hindamine, sest saab kindlaks teha muudatustest tingitud kulusid ennem, kui nad on juhtunud.

### Mahtude haldamine

Tegemist on protsessiga, mille eesmärk on tagada seda, et IT ressursid vastaksid organisatsiooni hetke ja tuleviku vajadustele maksimaalse kasumlikkusega. (ITIL Service Design 2007, 79). Mahuhalduse mitte kasutamine toob kaasa selle, et organisatsioon ei ole teadlik palju ühe või teenuse pakkumine ressursse nõuab ning ei osata efektiivselt planeerida nende kasutamist. Mahuhaldust on vaja järgmistel põhjustel: a) saada rohkem kätte olemasolevatest IT ressurssidest ja parandada kulusid IT teenuse kohta; b) teostada efektiivset järelvalvet IT ressursside kasutuse kohta; c) infosüsteeme ja teisi teenuseid saab paremini häälestada jõudluse parandamiseks ning ressursside kasutamise optimeerimiseks; d) organisatsioonile saab anda perioodiliselt infot mahtude kasvamise kohta ning sellega seoses planeerida järgnevaid infrastruktuuri arenguid.

### Versioonide haldamine

Tegevused, mis on kontrollivad versioonide arendamise ja haldamisega seotud tegevusi eesmärgiga kaitsta IT keskkonda ja selle teenuseid. Peamised tegevused on versioonide planeerimise, installeerimise ja testimise korraldamine ning koopiate haldamine. (ITSMF 2007). Juhul, kui asutus ei kasuta versioonihaldust, siis ei jää jälge kuskile maha süsteemis tehtud tarkvaraliste muudatuste kohta, mille tõttu võivad tekkida tõrked infosüsteemide kasutamisel ja nende töö kiirel taastamisel. Versioonihalduse plussid: a) loob struktureeritud lähenemise tarkvara uuenduste paigalduse protsessile; b) võimaldab muuta enne uue versiooni rakendamist selle kasutamismugavust ja funktsionaalsust läbi testimise protseduuride, c) tekib tsentraalne kontroll ja andmebaas selle kohta, missugust tarkvara versiooni kasutatakse, d) versiooniuuendusse on kogutud kokku erinevad muudatused, mis minimeerivad lõppkasutajale tekkivat mõju tarkvara uuendamisel.

### Käideldavuse haldamine

Protsess, mis on seotud IT-teenuste ja nende komponentide käideldavuse ärinõuete defineerimisega, mõõdikute määratlemise ning kokkuleppimisega, käideldavuse jälgimise ja analüüsimisega ning aruandluse korraldamisega. (ITSMF 2007). Seoses sellega, et tänapäeval on organisatsiooni tegevus tihedalt seotud IT-ga, siis tavaliselt IT teenuste peatumisel lõppeb organisatsiooni normaalne töö – sellepärast tulebki IT teenuste käideldavust pidevalt kontrollida. Käideldavuse haldamisest saadav kasu: a) teenused on kättesaadavad teenustaseme lepingutes paika pandud ajaraamide sees; b) teenuseid jälgitakse vastavalt nende käideldavuse nõuetele. See tähendab seda, et vähem kriitiliste süsteemide puhul tuleb kulutada nende käideldavuse mõõtmiseks vähem ressursse; c) teenuste käideldavust mõjutavad potentsiaalsed probleemid avastatakse ennem, kui need suudavad negatiivset mõju avaldada teenusele.

### IT finantshaldamine

IT finantshaldamine koosneb kolmest põhiprotsessist: a) eelarvestamine – protsess IT kulude planeerimiseks ja nende kontrollimiseks organisatsiooni sees, b) teenuste kulude üle arve-pidamine – protsess kulude arvestamiseks teenuste ja nende kasutajate raames, c) tasustamine – protsess osutatud teenuste eest arvete esitamiseks. (ITIL Service Strategy 2007, 148). Olukorras, kus ei tegeleta IT finantshaldamisega on väga keeruline ära põhjendada investeeringute ja tegevuskulude vajadust, kuna puudub ülevaade, mida konkreetselt saadud rahaga üritatakse saavutada. IT finantshaldamise plussid: a) saab planeerida ja ennustada IT kulusid, et hoida ja arendada teenuseid vajalikul tasemel; b) luuakse parem arusaamine kuludest, mis on seotud teenuse pakkumisega; c) tagab IT kulude jäämise kokkulepitud vahemikesse ning selle läbi raha õige kasutamise; d) parandab kontrolli selle üle, et IT teenuseid kasutatakse efektiivselt.

### Konfiguratsiooni haldamine

Tegevused, mis fikseerivad ja teavitavad konfiguratsioonielementide ning muudatussoovide seisundist ning kontrollivad konfiguratsioonielementide täielikkust ja õigsust. Konfiguratsioonielemendid määratletakse konfiguratsioonihalduse protseduuridega. (ITSMF 2007). Konfiguratsioonihalduse plussid: a) tekib keskne ja usaldusväärne konfiguratsioonihalduse andmebaas (CMDB) konfiguratsioonielementide kohta; b) tekivad seosed konfiguratsioonielementide ja erinevate komponentide vahel, mis mõjutavad teenuseid.

### IT teenuste teadmiste juhtimine

Selle protsessi eesmärk on võimaldada organisatsioonil tõsta juhtimisotsuste tegemise kvaliteeti, tagades selle, et usaldusväärne informatsiooni on kättesaadav terve IT teenuse elutsükli jooksul – kõikidele teenuse osutamisega seotud pooltele on täpselt teada, millist lisaväärtust teenus toob. (ITIL Service Transition 2007, 145). Teenuse teadmiste juhtimine koosneb järgmistest tegevustest: täpsete andmete kogumine (nt. konfiguratsiooni halduse andmebaasi põhjal) ühte andmebaasi, andmete analüüsimine ja nende muutmine informatsiooniks, vajalike andmete tuvastamine ja ressursside planeerimine nende salvestamiseks. IT teenuste teadmiste juhtimisest saadav kasu: a) otsuste tegemise perioodi saab vähendada teadmiste juhtimise andmebaasi kasutamisega; b) kulub vähem aega vajaliku dokumentatsiooni leidmiseks; c) teadmised ei ole seotud väga enam konkreetse indiviidiga.

### IT teenuste portfell ja selle haldamine

Teenuste portfell on täielik kogum teenusepakkuja poolt hallatavatest teenustest – see aitab kasutajal mõista, milliseid teenuseid IT pakub ja milliseid teenuseid ei pakuta. Selle haldamine on protsess, mis vastutab vastavate investeeringute juhtimise eest, et siis vastavalt tõsta või langetada teenuse väärtust organisatsiooni jaoks. (ITIL Service Strategy 2007, 186). Lihtsamalt öeldes tehakse läbi haldamise investeeringuid uute teenuste arendamiseks, olemasolevate

teenuste muutmiseks ja vanade teenuste sulgemiseks. Organisatsiooni jaoks peitub kasu IT teenuste portfelli haldamise puhul selles, et paraneb IT teenuste ja nendega seotud kulude läbipaistvus – kõigile on teada milliseid teenuseid täpselt pakutakse ja palju nendega on seotud kulusid.

# 4. Optimeeritud infrastruktuuri mudeli rakendamise analüüs MKM-is

Optimeeritud infrastruktuuri mudeli vastavusauditi jaoks koostatud küsimused koos vastustevariantidega leiab töö Lisa 1 Optimeeritud infrastruktuuri auditi küsimustikust. Selle põhjal täideti iga asutuse kohta vastav osa koondtabelis, mis on välja toodud Lisa 2 Optimeeritud infrastruktuuri vastavusauditi tulemused asutuste lõikes. Punktihinnete saamiseks koondtabelisse kasutati kodeerimist andes „Jah“ vastuse puhul punktihinde 1 ja „Ei“ vastuse puhul punktihinde 0. Lähtudes saadud punktihindest konkreetse IT infrastruktuuri komponendi juures üritatakse andmete analüüsimise teel tuua välja infrastruktuuri tugevused ja nõrkused ning nende põhjal anda konkreetseid soovitusi olemasoleva olukorra parandamiseks.

## *4.1 Auditi koondtulemused*

Selleks, et kindlaks teha, kas ja kui palju vastab saadud auditi kogutulemus optimeeritud infrastruktuuri mudelile, üritati leida kõikide vastavate infrastruktuuri komponentide punktihinnete kokku liitmise teel koontabelis. Vastavalt sellele kujunes välja iga asutuse kohta koondhinne, mis kõige paremini iseloomustab saadud tulemust. Maksimaalselt võib auditi puhul saavutada asutuse koondhindeks 55 punkti – seda juhul, kui tõesti on suudetud olemasolev infrastruktuur täielikult ära optimeerida. Kahjuks ükski auditis osalenud asutus sellist tulemust ei saanud ja koondhinde tulemused jäid kõvasti alla selle numbri.

Järgnevalt esitatud Tabel 1 asutuste saadud koondhinnetega vastavusauditi põhjal ning lisatud vahehinded mudeli valdkondade kaupa.

| Organisatsiooni nimetus | Tehnoloogia kasutuse vald-konna vahehinne | Protsesside juhtimise vald-konna vahehinne | Koondhinne |
|---|---|---|---|
| Majandus- ja Kommunikatsiooniministeerium | 20 | 12 | 32 |
| Tehnilise Järelevalve Amet | 19 | 12 | 31 |
| Konkurentsiamet | 19 | 12 | 31 |
| Autoregistrikeskus | 10 | 9 | 19 |
| Lennuamet | 15 | 12 | 27 |
| Maanteeamet | 2 | 9 | 11 |

**Tabel 1. Vastavusauditi koondtulemused**

## *4.2 Olemasoleva hetkeolukorra analüüs vastavalt mudelile*

Auditi tulemusel tehti ülevaade olemasolevast IT infrastruktuurist, kirjeldades ära selle optimeeritud osad ning lisati juurde vastavad soovitused IT infrastruktuuri optimeerituse taseme tõstmiseks.

### 4.2.1 MKM-i IT infrastruktuur

Hetkeolukorra analüüs on tehtud selle eeldusega, et kõik asutused kasutavad ühte ja sama IT infrastruktuuri. Praegusel momendil kasutavad ühte infrastruktuuri 5 asutust: Majandus- ja

Kommunikatsiooniministeerium, Tehnilise Järelevalve Amet, Konkurentsiamet, Autoregistrikeskus ja Lennuamet.

Tehnoloogia kasutamine. Võrgus olevate baasteenuste tasemel vaadates on kasutusel keskne võrguaadresside jagamise (DHCP) ja nimeserveri (DNS) lahendus neljas asutuses (MKM, ECAA, TJA, KA) ning ühes asutuses (ARK) on olemas kahest lahendusest ainult tsentraalne nimeserveri teenus. Töökohtade haldamiseks on kõigil olemas kataloogi- ja autentimisteenus, mille abil omakorda rakendatakse erinevaid rühmapoliitikaid arvutite ja kasutajate administreerimiseks. Kasutajate andmete hoidmisega seotud kasutajaprofiilid on suunatud arvuti töökohast välja failiserverisse selliselt, et kasutaja enda tähtsamaid faile enam arvutis ei hoiaks. Lisaks failiserveri teenusele kasutakse kolme asutuse (MKM, TJA, KA) puhul hajusfailisüsteemi, tagades nii teenusele parema töökindluse ja käideldavuse. Arvuti töökohtade paigaldamisel kasutatakse standardseid süsteemikujutisi (image) ja nende paigaldamist teostatakse läbi vastava tarkvara üle võrgu kolmes asutuses (MKM, TJA, KA) – seega läheb nende asutuste IT spetsialistidel tunduvalt vähem aega uute töökoha paigaldamisele. Tarkvarahalduse ja sellega seoses tarkvara ja riistvara auditeerimist teostakse keskselt neljas asutuses (MKM, TJA, KA, ECAA) ehk nende puhul tarkvara paigaldamiseks, uuendamiseks ja auditeerimiseks ei pea füüsiliselt arvuti töökoha juurde minema. Printimise puhul kasutatakse keskset printserverit terve printerite pargi haldamiseks samuti neljas asutuses (MKM, TJA, KA, ECAA). Kõik kriitilisemad teenused, mille puhul organisatsiooni töö jääb seisma on ära kindlustatud kolme asutuse (MKM, TJA, KA) puhul kõrgkäideldavate tehnoloogiate kasutamisega – see tähendab seda, et kui üks server oma töö lõpetab võtab teine server selle rolli sujuvalt ja automaatselt üle. Kasutajate koolitamine toimub koheselt uue süsteemi juurutamisel või uue töötaja tööle tulekul kahjuks ainult MKM-is. Viiruste ja muude pahavara eest kaitsmisel on kasutusel keskne viirustõrjetarkvara, mis võimaldab saada ülevaate viirustega seotud intsidentide kohta ja uuendada viirustõrje serveri kliente automaatselt. Keskset tulemüüri kasutatakse kahes kohas: a) teenuste ja sisevõrgu kaitsel; b) arvutitöökohtade kaitsel – seda kahjuks ainult neljas asutuses (MKM, TJA, KA, ECAA). Selline tulemüüride tsentraliseerimine on tekitanud olukorra, kus osades asutustes võimalik rakendada konkreetseid ligipääsu poliitikaid ühest kohast ning kergendanud ülevaadet võrgus toimuvast. Spämmitõrjet teostatakse

kekselt ja selle tõttu ei jõua suurem osa ebasoovitavaid kirju e-postisüsteemi. Kaugligipääsu korraldamiseks kasutatakse tehnoloogiat, mille puhul on tagatud kasutajate turvaline autentimine ja sideseansi krüpteerimine üle avaliku võrgu, samas andes ligipääsu vajalikele ressurssidele. Eelpool mainitud lahendust kasutatakse kasutajate pöördumisel üle traadita võrgu (Wifi) sisevõrku. Varundamist korraldatakse koos keskse varundus- ja taastelahendusega.

IT protsesside juhtimine. Kõikide asutuste tasemel on olemas ühtne põhidokumentatsioon: IT strateegia, turvapoliitika, riist- ja tarkvarastandard ning taasteplaanid. Samuti ollakse samas staadiumis ISKE rakendamise protsessiga: kõik infovarad on kaardistatud, määratud nende turvaklassid koos vastavate turbeastmetega, määratud lähtuvalt turvaastmest vastavad turvameetmed, koostatud turvameetmete rakenduskava ja on välja jõutud ISKE turvameetmete rakendamise faasi. IT haldusprotsesside rakendamise koha pealt neljas asutuses (MKM, TJA, KA, ECAA) on vastavalt ITIL-ile rakendatud intsidendihaldus, probleemihaldus, mahtude halduse ja IT finantshaldus. Ühes asutuses (ARK) on vastavalt ITIL-ile rakendatud ainult IT finantshaldus.

### 4.2.2 Lisanduva organisatsiooni IT infrastruktuur

Seoses ministeeriumi plaaniga omavahel liita Maanteeamet ja Autoregistrikeskus üheks asutuseks, on tehtud otsus olemasoleva Maanteeameti IT infrastruktuuri konsolideerimiseks MKM-i omaga. Hetkeolukorra analüüs on tehtud olemasoleva Maanteeameti IT infrastruktuuri põhjal, et saada selgem pilt selle optimeerituse tasemest. Samuti on see vajalik selleks, et hiljem soovituste all oleks võimalik välja tuua need tegevused, mis tõstaksid liitumise hetkel optimeerituse taset.

Üleüldine vastavus optimeeritud IT infrastruktuuri mudelile on väga väike. Selle põhjuseks on see, et MNT üle Eesti laiali ja nende IT infrastruktuuri pole suudetud ära tsentraliseerida ja luua keskseid teenuseid. Tava praktikas väljendub see olukorra, kus igas erinevas geograafilises kohas

on omad serverid, võrk, teenused ning iga konkreetse koha eest vastutab konkreetne eraldi inimene.

Tehnoloogia kasutamine. Spämmitõrjet teostatakse kesksel ja selleläbi ei jõua suurem osa ebasoovitavaid kirju e-postisüsteemi. Turvalise kaugligipääsu korraldamiseks kasutatakse tehnoloogiat, mille puhul on tagatud kasutajate turvaline autentimine ja sideseansi krüpteerimine üle avaliku võrgu, kuid kahjuks antakse kesksete teenuste puudumisel ligipääs erinevates asukohtades paiknevatele ressurssidele.

IT protsesside juhtimine. Olemas põhilised IT organisatsioonilised dokumendid : IT strateegia, turvapoliitika, riist- ja tarkvarastandardid ja taasteplaanid. ISKE rakendamise protsessi raames on tehtud järgmised tegevused: kõik infovarad on kaardistatud, määratud nende turvaklassid koos vastavate turbeastmetega, määratud lähtuvalt turvaastmest vastavad turvameetmed, koostatud turvameetmete rakenduskava ja on välja jõutud ISKE turvameetmete rakendamise faasi. ITIL-ile vastavalt on rakendatud IT finantsjuhtimise protsess.

## *4.3 Auditi tulemuste põhjal soovitused IT infrastruktuuri optimeerimiseks*

Vastavusauditi tulemuste põhjal tuuakse soovitused kõigepealt välja terve MKM-i infrastruktuuri ulatuses ja siis erinevate asutuste tasemel, et oleks selgelt välja toodud, mida peab tegema optimeeritud taseme ühtlustamiseks. Soovituste rakendamiseks praktikas on mõistlik need sisse viia MKM-i olemasolevasse strateegiasse ja tööplaani selleks, et nende põhjal alustada konkreetseid tegevusi.

### *4.3.1 MKM-i IT infrastruktuur*

Seosese sellega, et vastavusauditi käigus selgusid mitmed asjaolud, mis aitaksid IT infrastruktuuri optimeerimisele MKM-is ja selle haldusalas kaasa, siis siinkohal esitatakse järgmised soovitused:

- Kasutusele võtta printserveri haldustarkvara selleks, et paremini kontrolli alla võtta printserveris toimuv. Läbi selle on võimalik kasutajal printeriga seotud probleemidest varem teada saada (nt. tehnilised rikked, toonerite tühjenemine), tekib ülevaade palju konkreetselt keegi neid printimiseteenuseid kasutab ja saab kehtestada erinevaid piiranguid (printerite ligipääsule või printimiskogustele);

- Palju rohkem tähelepanu tuleks pöörata serverite ja rakenduste virtualiseerimisele ning luua selleks vastav virtuaalserveri keskkond teenuste majutamiseks. Mõistlik on alustada füüsiliste serverite jõudlusnäitajate kaardistamisega selleks, et teada saada palju ühe või teise teenuse pakkumine reaalselt ressursse nõuab – suure tõenäosusega ei suudeta neid maksimaalselt ära kasutada. Vastavalt kaardistuse tulemusele tasub alustada siis füüsiliste serverite migreerimist virtuaalkeskkonda. Selle projekti ettevõtmisel on võimalik päris korralikult kokku hoida energiakulusid läbi olemasoleva serveripargi vähendamise;

- Lähtuda IT seadmete optimaalsest elutsüklist 3 – 4 aastat ning arvestada uute hangete planeerimisel sellest. Vanemate seademete puhul tõuseb risk, millegi katki minemiseks väga kiiresti ning samuti tõuseb seademete omamiskulu. Kui suurem osa seadmeid renditakse, siis seoses riistvara hindade pideva langemisega, on mõistlik rendiperioodi lõppedes alati need vahetada uute vastu välja;

- Identiteedi ja ligipääsu haldamise lihtsustamiseks tasuks kaaluda vastava tarkvaralise lahenduse kasutusele võtmist selleks, et vähendada mitmesse infosüsteemi eraldi kasutaja andmete tekkimist. Lisaks tekib siis keskne ülevaade informatsiooni kasutamise kohta ning on võimalik kasutada igal poolt automaatset sisselogimist;

- Tulemüüride koha pealt tasuks kaaluda tsentraalse tulemüüri halduse loomist serveritele, sellisel juhul ei häälestata serverite jaoks enam tulemüüre individuaalselt. Läbi vastava tarkvara on kergem ligipääsu reegleid kehtestada, samuti tekiks võimalus tulemüüri logide informatsiooni kesksekstalletamiseks ja analüüsimiseks.

- Sisevõrgu kaitse parandamine. Sisevõrgus toimuvate rünnakute eest hoidumiseks tuleks kasutada ründekaitse tarkvara, mis suudaks need tuvastada ja vajadusel blokeerida. Serverite vaheline ja arvuti töökohtade vaheline andmeside oleks mõistlik eraldada vastavate krüpteerimise vahendite kasutamisega. Sellisel juhul tekib sisevõrgu sisse eraldi võrk, kuhu võõrad arvutid ligi ei pääse. Enne arvutite sisevõrku pääsemist tuleks need üle kontrollida viimaste tarkvara ja viirustõrje uuenduste koha pealt läbi vastava lahenduse. Sellisel juhul oleks tagatud see, et ebaturvaline arvuti võrku ei pääse;

- Täiustada avaliku võtme infrastruktuuri koos erinevate autentimisskeemidega, kas siis näiteks ID-kaardi või juba biomeetrilist logimist võimaldavate süsteemidega;

- Mobiilsete seadmete kaitsmisel tuleks tähelepanu pöörata järgmistele nõuannetele: kõik andmed peaksid olema krüpteeritud, sisselogimisel kasutada rohkem kui ühte autentimisprotsessi ning vajadusel peaks olema võimalik jälgida nende asukohta väljaspool asutuse võrku;

- Kasutusele võtta keskne VOIP telefonisüsteem energia- ja kõneside kulude kokku hoidmiseks hallatavas infrastruktuuris;

- Luua talituspidevuse plaan, mis oleks integreeritud taasteplaanidega selleks, et tõsta valmisolekut erinevate kriiside tekkel;

- ISKE turvameetmete rakendamisega peaks jõudma kindlasti sinna kohta, kus juba teostakse järjepidevat turvameetmete vastavuse kontrolli süsteemis;

- Parandada IT teenustega seotud haldamisprotsesse läbi puuduolevate ITIL-i moodulite rakendamise: konfiguratsioonihaldus, teenustasemetehaldus, käideldavuse haldus,

muudatuste haldus, versioonide haldus, IT teadmiste juhtimine teenustega seotud info säilimiseks, koostada IT teenuste portfell ja tegeleda selle haldusega.

### 4.3.2 Tehnilise Järelevalve Amet ja Konkurentsiamet

Kahte asustust vaadeldakse koos sellepärast, et IT organisatsioon on mõlemal ühine MKM-iga. See tähendab seda, et Konkurentsiameti ja Tehnilise Järelevalve Ameti all ei ole eraldi IT üksust, vaid nende eest vastutab MKM-i Infosüsteemide- ja registrite osakond. Soovitused optimeeritud taseme ühtlustamiseks:

- Parandada infosüsteemide kasutajate jaoks IT alaste koolituste kättesaadavust. Kindlasti alustada uute töötajate koolituste läbi viimist infosüsteemidega tutvumiseks.

### 4.3.3 Lennuamet

Kasutab MKM-i IT infrastruktuuri, kuid omab eraldi IT organisatsiooni. Asutuse kätte on jäetud oma arvuti töökohtade haldamine, mida hetkel ostetakse sisse, ning korraldab ise IT seotud tegevuste ja eelarve planeerimist. Soovitused optimeeritud taseme ühtlustamiseks:

- Kasutusele võtta hajusfailisüsteem tagamaks parem failiteenuse töökindlus;
- Arvuti töökohtade paigaldamisel oleks mõistlik luua standardsed süsteemikujutised ja hakata neid tsentraalselt paigaldama käsitsi tehtava töö vähendamiseks;
- Kasutusele võtta kriitiliste teenuste puhul kõrgkäideldavad tehnoloogiad, et teenused oleks paremini kaitstud katkestuste eest;
- Parandada infosüsteemide kasutajate jaoks IT alaste koolituste kättesaadavust. Kindlasti alustada uute töötajate koolituste läbi viimist infosüsteemidega tutvumiseks.

### 4.3.4 Autoregistrikeskus

Kasutab samuti MKM-i IT infrastruktuuri, kuid haldab ja juhib enda poolset osa täiesti eraldi. Soovitused optimeeritud taseme ühtlustamiseks:

- Loobuda käsitsi IP aadresside jagamisest ning selle asemel võtta kasutusele võrguaadresside jagamise teenus (DHCP);
- Kasutusele võtta hajusfailisüsteem tagamaks paremat failiteenuse töökindlus;
- Arvuti töökohtade paigaldamisel oleks mõistlik luua standardsed süsteemikujutised ja hakata neid tsentraalselt paigaldama käsitsi tehtava töö vähendamiseks;
- Hakata teostama tarkvarahaldust ning riistvara ja tarkvara auditeerimist kesksete vahenditega. Soovitavalt võttes kasutusele juba olemasolev süsteem ning kohendada seda vastavalt oma vajadustele;
- Printerite pargi haldamise lihtsustamiseks kasutusele võtta keskne printserver;
- Kasutusele võtta kriitiliste teenuste puhul kõrgkäideldavad tehnoloogiad, et teenused oleks paremini kaitstud katkestuste eest;
- Parandada infosüsteemide kasutajate jaoks IT alaste koolituste kättesaadavust. Kindlasti alustada uute töötajate koolituste läbi viimist infosüsteemidega tutvumiseks;
- Arvutitöökohtade kaitsmiseks juurutada kesksel hallatavad tulemüürid;
- IT protsesside parandamiseks käivitada intsidendi- ja probleemihaldus läbi vastava tarkvaralise lahenduse, et tekiks keskkond nende protsesside haldamiseks. Mahtude haldamiseks siduda need konkreetse organisatsiooni vajadustega.

### 4.3.5 Maanteeamet

Omab täiesti iseseisvat IT infrastruktuuri, mille haldamine ja juhtimine toimub eraldi. Auditi raames keskenduti sellel momendile, et seoses vajadusega liita MNT olemasoleva MKM-i infrastruktuuriga, mida annab teha üldise infrastruktuuri optimeeritud taseme tõstmiseks. Soovitused koostatud vastavalt selle MNT hakkab kasutama MKM-i IT infrastruktuuri:

- Juurutada võrgu põhiteenused keskne DHCP ja DNS server. Arvuti töökohad ja kasutajad liita ühtse kataloogi- ja autentimisteenusega ning rakendada vastavaid rühmapoliitikaid;
- Suunata kasutajate profiilid välja töökoha arvutitest failiserverisse ja rakendada hajusfailisüsteemi failiserverite töökindluse tõstmiseks;
- Parandada töökohtade haldamist läbi standardsete süsteemikujutiste kasutusele võtmise ja nende tsentraalse paigaldamise. Käivitada keskne tarkvarahaldus koos riistvara ja tarkvara auditeerimise vahenditega;
- Parandada IT teenuste osutamist läbi intsidendi-, probleemi- ja mahtude halduse juurutamise;
- Kasutusele võtta kriitiliste teenuste puhul kõrgkäideldavad tehnoloogiad, et teenused oleks paremini kaitstud katkestuste eest;
- Parandada infosüsteemide kasutajate jaoks IT alaste koolituste kättesaadavust. Kindlasti alustada uute töötajate koolituste läbi viimist infosüsteemidega tutvumiseks;
- Käivitada kesksed tehnoloogiad: varunduslahendus, printimisteenus, tulemüürindus, turvaline traadita võrk ja viirustõrje.

# Kokkuvõte

Käesoleva magistritöö eesmärgiks oli optimeeritud infotehnoloogilise infrastruktuuri mudeli koostamine, ühe olemasoleva IT infrastruktuuri kaardistamine vastavalt välja töötatud mudelile ning tulemuste analüüsi põhjal soovituste välja pakkumine optimeeritud IT infrastruktuuri saavutamiseks. Autor leiab, et püstitatud eesmärgid said töö raames saavutatud.

Magistritöö tulemusena loodi parimate praktikate põhjal optimeeritud IT infrastruktuuri mudel, ning lisaks sellel arendati välja metoodika, kuidas analüüsida organisatsiooni IT infrastruktuuri seisundit vastavale mudelile. Autor arvab, et loodud mudelit ja metoodikat saab vabalt kasutada teiste avaliku halduse asutuste IT infrastruktuuri peal. Need on kergendavaks abivahendiks IT valdkonnas tegutsevatele inimestele, kes soovivad hinnata, kas kõik olemasoleva IT infrastruktuuri arendamisel tehtu on olnud optimeeritud ning vastav organisatsiooni vajadustele.

Antud magistritöö raames üritati lisaks optimeeritud IT infrastruktuuri mudeli loomisele, ka seda rakendada Majandus- ja Kommunikatsiooniministeeriumis ja selle haldusala asutustes selleks, et näha kas see tegelikult töötab. Autor kinnitab magistritöö kirjutamise tulemusel omalt poolt, et tõesti on tegemist täiesti töötava mudeli ja metoodikaga, mida saab kasutada edukalt toimiva organisatsiooni peal. Vastavusaudit läbi viimine MKM-is ja selle haldusalas näitas, et optimeeritud taseme saavutamiseks on veel palju tööd vaja ära teha. Loodetavasti annavad auditi tulemuste analüüsi põhjal saadud soovitused paremini selgust selles, millega konkreetselt alustama peaks. Magistritöö tulemusena veenduti veelkord selles, et olemasolevat IT infrastruktuuri on vaja järjepidevalt ja süstemaatiliselt hinnata, muidu puudub selge visioon, kuidas kõige optimeeritumalt tegutseda.

Magistritöö käigus vastavustauditi tulemuste põhjal saadud soovitustele on mõistlik auditeeritud organisatsioonisatsioonis rohkem tähelepanu pöörata, sest see võimaldab IT infrastruktuuri efektiivsemalt ja turvalisemalt tulevikus kasutada. Autor püüab seoses oma töötamisega auditeeritavas organisatsioonis lähtuda saadud kogemustest ja leitud soovitustest olemasoleva IT infrastruktuuri arendamisel. Täpsemalt on plaanis soovitused sisse viia MKM-i strateegiasse ja tööplaani selleks, et neid erinevate tegevustena ellu rakendada.

Magistritööd on kindlasti võimalik edasi arendada lähtudes sellest aspektist, et loodud mudel ja auditeerimismetoodika vajaks täiendamist uute tehnoloogiate peale tulekuga. Kahjuks toimub see tehnoloogiline progress suhteliselt kiiresti, seega tulevikus on alati mõistlik mudeli infrastruktuuri komponentide ja nende parimate praktikate kasutamise koha pealt kriitiliselt läbi vaadata, kas mingeid muutusi on toimunud vahepeal.

# RESUME

Optimized Information Technology Infrastructure Model Implementation Analysis. The Case of Ministry of Economic Affairs and Communications

The importance of information technology is constantly increasing and it is making deeper inroads into our daily lives. Thus it is very hard to imagine an organization that would be able to function effectively if it failed to tap the full possibilities afforded by IT. As a result, an organization's IT infrastructure is becoming one of its greatest strategic assets, provided that it conforms to the organization's business needs or demands of its primary activity and which can be used to offer various services and applications for internal or external users. Unfortunately, in connection with the advent of new directions in technology, it is becoming more complicated and costly to administer IT infrastructure and it is also harder to meet the changing needs of business operations. In this master's thesis, the author attempts to find ways of optimizing the existing IT infrastructure through auditing in order to make it more effective and secure.

The problem for research in this master's thesis is that, in the case of rapidly growing IT infrastructure, too little attention is being paid to assessing the current situation and optimizing IT infrastructure.

The purpose of this master's thesis is to compile an optimized IT infrastructure model, auditing one existing IT infrastructure based on the model, and to offer suggestions, on the basis of the results of the analysis, for achieving optimized IT infrastructure. The aims were achieved in the framework of the work through the following activities:

- Theoretical research was conducted on the basis of various information sources to find a audit model. In the course of the study, the best practices related to IT infrastructure components were analyzed. As a result of the analysis, an optimized IT infrastructure model and methodology for implementing the model were compiled on the basis of the best practices.

- In order to implement the model developed, a compliance audit was conducted on the basis of the model in the following six agencies: the Ministry of Economic Affairs and Communications (MEAC), the Aviation Board, Technical Inspectorate, Competition Board, Motor Vehicle Register and the Road Administration. As a result of the audit, an overview was presented of existing IT infrastructure, describing its optimized components. Relevant recommendations for raising the level of optimization of IT infrastructure were also included.

In the course of implementing the optimized IT infrastructure model at the MEAC and its area of administration, weak spots became evident in the existing IT infrastructure – areas that must definitely be addressed. More attention must be paid in the organization to the recommendations received from analysis of the compliance audit and implementing these recommendations, as these allow expenses related to IT infrastructure to be reduced. In connection with the author's experience working for an auditing organization, the author has attempted to proceed from the experiences gained and recommendations identified in developing existing IT infrastructure. More precisely, it is planned to introduce the recommendations into the MEAC strategy and work plan in order to implement them as various activities.

# Kasutatud kirjandus


**(Gartner Group 2003)**. Gartner Group (2003). Gartner Says Extending the Life Cycle of Desktop PCs Won't Necessarily Save Money on Total Cost of Ownership. URL : http://www.gartner.com/press_releases/pr15sept2003b.html. [ 20.03.2009]

**(IBM 2009).** IBM Corporation (2009). IBM Infrastructure Management – Key Elements of Dynamic Infrastructure. URL: http://www-03.ibm.com/systems/dynamicinfrastructure/key_elements.html [18.04.2009]

**(ISKE 2008, 9).** Riigi Infosüsteemide Arenduskeskus (2008). ISKE rakendusjuhend versioon 4.01. URL: http://www.ria.ee/public/ISKE/ISKE_rakendusjuhend_4_01_16122008.pdf [18.04.2009]

**(ITIL Service Design 2007, 79).** Office of Goverment Commerce (2007). ITIL Version 3 – Service Design, TSO ( The Stationery Office) 2007, ISBN: 9780113310906.

**(ITIL Service Operation 2008, 35).** Office of Goverment Commerce (2008). ITIL Version 3 – Service Operation, TSO ( The Stationery Office) 2008, ISBN: 9780113310920.

**(ITIL Service Strategy 2007, 148).** Office of Goverment Commerce (2007). ITIL Version 3 – Service Strategy, TSO ( The Stationery Office) 2007, ISBN: 9780113310524.

**(ITIL Service Strategy 2007, 186).** Office of Goverment Commerce (2007). ITIL Version 3 – Service Strategy, TSO ( The Stationery Office) 2007, ISBN: 9780113310524.

**(ITIL Service Transition 2007, 145).** Office of Goverment Commerce (2007). ITIL Version 3 – Service Transition, TSO ( The Stationery Office) 2007, ISBN: 9780113310555.

**(ITSMF 2007).** itSMF Estonia (2007). Teenuste halduse eesti keelne sõnastik. URL: http://www.itsmf.ee/index.php?option=com_content&view=article&id=57&Itemid=29 [02.04.2009]

**(Majandus- ja Kommunikatsiooniministeerium 2009).** Majandus- ja Kommunikatsiooniministeeriumi kodulehekülg. URL: http://www.mkm.ee [16.03.2009]

**(Majandus- ja Kommunikatsiooniministeerium 2009a).** Majandus- ja Kommunikatsiooni-ministeeriumi Infosüsteemide ja registrite osakonna põhimäärus. URL: http://www.mkm.ee/failid/IROuus_p_him__rus_VE.doc [16.03.2009]

**(Microsoft 2009).** Microsoft Corporation (2009). Microsoft Core Infrastructure Optimization. URL: http://www.microsoft.com/infrastructure/about/overview.mspx [18.04.2009]

**(Ponemon Institute 2007)** Ponemont Institute (2007). Computer Theft & Recovery Statistics. URL: http://www.absolute.com/resources/computer-theft-statistics.asp

**(Rea 2007).** Scott Rea. Why PKI?

URL: http://www.checoweb.org/drupal/sites/default/files/whypki.ppt [18.04.2009]

**(Spafford 2005).** George Spafford (2005). The True Value of Change Management. URL: http://itmanagement.earthweb.com/service/article.php/3527471 [16.03.2009]

# Mõisted

Infotehnoloogiline infrastruktuur - infotehnoloogilise infrastruktuuri komponendid: riistvara, tarkvara, telekommunikatsioonivahendid, infotehnoloogilised protsessid, infotehnoloogia alane dokumentatsioon.

Optimeeritud infotehnoloogiline infrastruktuur - infotehnoloogilise infrastruktuur, mis suudab kõige paremini kohanduda organisatsiooni muutuvate vajadustega.

Andmehoidla – andmete hoidmise koht hilisema kasutamise eesmärgil.

Käideldavus - komponendi või teenuse võime täita nõutud funktsiooni kindlaksmääratud hetkel või kindlaksmääratud aja jooksul.

Teenusetase - määratakse tavaliselt lepinguga teenusepakkuja ja kasutaja vahel, kus on kirjas lepingu kehtivusaja kestel oodatav teenuse kvaliteet. Neid lepinguid kasutatakse nii müüjate ja ostjate vahel, kuid ka sisemiselt IT-osakondade ja nende lõppkasutajate vahel.

DHCP (Dynamic Host Configuration Protocol) - protokoll, mis võimaldab süsteemiadministraatoritel ühest kesksest kohast hallata ja automatiseerida dünaamiliste IP aadresside omistamist organisatsiooni võrku ühendatud seadmetele.

DNS (domain name system) - teenus, mis tõlgib domeeninimed IP aadressideks. Seoses sellega, et domeeninimed koosnevad tähtedest, siis on neid kergem meeles pidada, kui numbritest koosnevaid IP aadresse.

IP aadress - arvutite ja muude arvutivõrgus toimivate seadmete omavaheliseks suhtlemiseks arvutivõrgus vajalik unikaalne aadress.

Alamvõrgumask – määrab IP aadresside vahemiku suuruse.

Võrgu lüüs – kahte erineva arhitektuuriga võrku ühendav seade. Nt sisevõrgu ja interneti vahel.

Domeeninimi - unikaalne märgend, mis koosneb punktidega eraldatud tähtedest või numbritest, ning mis on määratud konkreetsele IP aadressile.

Nimeserveri tsoon – osa nimeserveris olevast nimeruumis, mille kasutamist on võimalik edasi delegeerida teiste nimeserveritele.

Domeen - kindlale kasutajate rühmale ette nähtud võrguressursside komplekt (rakendused, printerid jne).

Skaleeritavus - võime kasvada järk-järgult.

Rühmapoliitika – vahend keskse halduse ja konfiguratsiooni loomiseks arvutitele ja kasutajakontodele.

Jagatud kaust – võrgusoleva serveri ressurss, mida saavad kasutada mitu kasutajat korraga.

Printserver – printerite tööd juhtiv server arvutivõrgus.

Küberrünnak - kallaletung arvutisüsteemile või võrgule eesmärgiga andmeid varastada, rikkuda või ligipääsmatuks muuta.

Avaliku võtme infrastruktuur - sertifikaadihaldussüsteem, mis verifitseerib ja autendib erinevaid osapooli.

Krüpteerimine - andmete teisendamine sellisele kujule, mida teistel on võimalik lugeda ainult vastava võtme olemasolu korral.

Intsident - sündmus, mis ei ole teenuse kokkulepitud toimimise osa ning mis põhjustab või võib põhjustada selle teenuse katkemise või kvaliteedi halvenemise võrreldes Teenustaseme lepingus kokkulepituga.

Probleem - ühe või mitme Intsidendi tundmatu tekkepõhjus.

Sündmus – avastatav ja eristatav ilming, mis omab tähtsust IT infrastruktuuri haldamise, teenuste pakkumise või võimalikke kahjude tekkimise aspektist.

Muudatus - heakskiidetud, toetatud või jäädvustatud riistvara, võrgu, tarkvara, rakenduse, keskkonna, süsteemi, lõppkasutaja jaoks tehtud IT lahenduse või nendega seotud dokumentatsiooni lisamine, muutmine või eemaldamine.

Konfiguratsioonielement - infrastruktuuri komponent, mis on Konfiguratsioonihalduse kontrolli all. Infrastruktuuri komponendid võivad varieeruda keerukuse, suuruse ja tüübi osas. Ühe Konfiguratsioonielemendina võib kirjeldada nii terve süsteemi (riistvara, tarkvara, dokumentatsioon) kui ka üksikmooduli või väikese riistvarakomponendi.

Versioon - ajas fikseeritud Konfiguratsioonielemendi seisund.

# Lisa 1. Optimeeritud infrastruktuuri auditi küsimustik

Organisatsiooni nimi :

Töötajate arv :

Arvuti töökohtade arv :

Mobiilsete arvuti töökohtade arv:

**Tehnoloogia kasutamine**

1) Kas kasutatakse keskset võrguaadresside jagamise (DHCP) serveri teenust ? Jah Ei
2) Kas kasutatakse keskset nimelahenduse (DNS) serveri teenust ? Jah Ei
3) Kas kasutatakse keskset kataloogi- ja autentimisteenust kasutajate autentimiseks ? Jah Ei
4) Kas keskse kataloogi- ja autentimisteenuse juures kasutatakse kõikide töökohtade ja kasutajatekontode sarnase häälestuse tagamiseks rühmpoliitikaid ? Jah Ei
5) Kas organisatsiooni kasutab failiserverit parema töökindluse tagamiseks hajusfailisüsteemi (nt. DFS, AFS)? Jah Ei
6) Kas arvutitöökohtade paigaldamiseks kasutatakse standardseid süsteemikujutisi (image)? Jah Ei
7) Kas arvutitöökohtade paigaldamisel kasutatakse tsentraalset lahendust süsteemikujutiste (image) peale laadimiseks üle võrgu (nt. Altiris, Windows Deplyment Services)? Jah Ei
8) Kas arvutitöökohtade tarkvaralist konfiguratsiooni hoitakse standardsena läbi tsentraalsete tarkvarahalduse vahendite kasutamise (nt. skriptid, System Center Configuration Manager) ? Jah Ei
9) Kas organisatsiooni kasutab riistvaralise ja tarkvaralise konfiguratsiooni auditeerimiseks keskset lahendust (nt. WMI, IBM Tivoli Asset Manager, System Center Configuration Manager) ? Jah Ei
10) Kas printimisteenuse tagamiseks kasutakse keskset serveripõhist lahendust kõikides arvuti töökohtades (võrguprinterid ja keskne printserver)? Jah Ei

11) Kas keskse printimisteenuse haldamiseks kasutatakse haldustarkvara printerite monitoorimiseks, printimistööde kontrollimiseks ja vajadusel kasutaja turvaliseks autentimiseks ( Nt Uniflow, HP Easy Care)? Jah Ei
12) Kas kriitilised IT teenused ( teenused, mille maas olek häirib või katkestab organisatsiooni töö ) on kõrgkäideldavad? Jah Ei
13) Kas serverite majutamisel kasutakse virutaliseerimist suurema osa teenuseid pakkuvate serverite puhul? Jah Ei
14) Kas arvutitöökohtade, serverite ja muude seadmete haldamisel lähtutakse 3-4 aastasest elutsüklist? Jah Ei
15) Kas organisatsiooni IT teenuste kasutajaid koolitakse pidevalt vastavalt muutuvatele organisatsiooni vajadustele? Jah Ei
16) Kas organisatsiooni kasutab keskset identiteedi ja ligipääsu tarkvara lisaks kataloogi- ja autentimisteenusele? Jah Ei
17) Kas on olemas keskselt uuendatav ja hallatav viirustõrje tarkvara, mis katab olemasolevad töökohad ja serverid? Jah Ei
18) Kas organisatsioonil on keskne tulemüür koos integreeritud viirustõrjega , mis kaitseb kõiki organisatsiooni teenuseid ja sisevõrku (nt. Checkpoint, NetScreen)? Jah Ei
19) Kas organisatsioonis kasutakse keskset hallatavat tulemüüri koos integreeritud viirustõrjega kõikides serverites (nt. Trend Micro, Windows Firewall)? Jah Ei
20) Kas organisatsioonis kasutakse keskset hallatavat tulemüüri koos integreeritud viirustõrjega kõikides arvutitöökohtades (nt. Trend Micro, Windows Firewall)? Jah Ei
21) Kas organisatsiooni kasutakse keskset spämmitõrje lahendust? Jah Ei
22) Kas kasutakse ründekaitse tarkvara (Nt. IPS) arvutitöökohtade, seadmete ja serverite kaitsmiseks? Jah Ei
23) Kas töötajatel ja partneritel võimaldatakse turvalist ligipääsu sisemistele organisatsiooni teenustele ja rakendustele (nt VPN ja terminalteenuste kasutamine)? Jah Ei
24) Kas serverite ja arvutitöökohtade vahelised võrguühendused on isoleeritud sisevõrgus teiste võrgus ajutiselt viibivate seadmete eest (Nt. domeenikontrolleri ja e-posti serveri vaheline suhtlemine)? Jah EI

25) Kas on kasutusele võetud traadita võrgu lahendus, mis võimaldab turvalist ligipääsu sisevõrgule läbi kaugligipääsu tehnoloogiate? Jah Ei
26) Kas organisatsioonil on olemas avaliku võtme infrastruktuur koos mitmetasemeliste autentimisskeemidega ? Jah Ei
27) Kas on olemas võrgulahendus turvaparandusteta ja viirusega nakatunud arvutite ligipääsu piiramiseks võrku? Jah Ei
28) Kas organisatsioonil on olemas tsentraalne varundamise ja taastamise lahendus, mis katab kõiki servereid? Jah Ei
29) Kas on tagatud kasutajate profiilide hoidmine keskses failiserveris? Jah Ei
30) Kas mobiilsete seadmete puhul kasutatakse järgmisi tehnoloogiaid andmete kaitseks : kõvaketta ligipääsu paroolid, kõvaketta krüpteerimine, biomeetriline autentimine?
31) Kas mobiilsete seadmete puhul kasutatakse jälgimistarkvara (nt. Computrace)?
32) Kas kasutatakse VOIP tehnoloogiat kõneside edastamiseks üle andmeside võrgu? Jah Ei

**Protsesside juhtimine**

33) Kas organisatsioonis on olemas perioodiliselt uuenev IT strateegia? Jah Ei

34) Kas organisatsisoonis on olemas IT turvapoliitika, mis vastab ISO 13335 ja ISO 27002 nõuetele? Jah Ei

35) Kas organisatsioonis on olemas kokkulepitud riist- ja tarkvarastandardid? Jah Ei

36) Kas organisatsioonil on olemas talituspidevuse plaan? Jah Ei

37) Kas organisatsioonil on olemas kõiki teenuseid ja infosüsteeme kattev taasteplaan või taasteplaanid? Jah Ei

38) Millises etapis asub organisatsioon ISKE (infosüsteemide kolmeastmelise etalonturbesüsteemide) rakendamisega:
    a) kas infovarad on kaardistatud ? Jah Ei
    b) kas infovaradele on määratud turvaklassid koos vastavate turbeastmetega? Jah Ei
    c) kas infovaradele on määratud lähtuvalt turvaastmest vastavad turvameetmed? Jah Ei

d) kas on koostatud turvameetmete vastav rakenduskava? Jah Ei

e) kas ISKE turvameetmed on rakendatud? Jah Ei

f) kas teostatakse järjepidevat kontrolli selgitamaks rakendatud turvameetmete piisavust tegelikus olukorras? Jah Ei

39) Millised järgmised olulisemad on IT teenuste haldamisega seotud protsessid on rakendatud:

a) intsidentide haldamine? Jah Ei

b) probleemide haldamine? Jah Ei

c) konfiguratsiooni haldamine? Jah Ei

d) teenustasemete haldamine? Jah Ei

e) käideldavuse haldamine? Jah Ei

f) mahtude haldamine? Jah Ei

g) IT finantshaldamisega? Jah Ei

h) sündmuste haldamine? Jah Ei

i) muudatuste haldamine ? Jah Ei

j) versioonide haldamine? Jah Ei

k) IT teenuste seotud teadmiste juhtimine ? Jah Ei

l) IT teenuste portfell ja selle haldamine? Jah Ei

# Lisa 2. Optimeeritud infrastruktuuri vastavusauditi tulemused asutuste lõikes

| Tehnoloogia kasutamine ja protsesside juhtimine | MKM | TJA | KA | ARK | ECAA | MNT |
|---|---|---|---|---|---|---|
| Küsimus 1. DHCP teenus | 1 | 1 | 1 | 0 | 1 | 0 |
| Küsimus 2. DNS teenus | 1 | 1 | 1 | 1 | 1 | 0 |
| Küsimus 3. Kataloogi- ja autentimisteenus | 1 | 1 | 1 | 1 | 1 | 0 |
| Küsimus 4. Rühmapoliitikate kasutamine | 1 | 1 | 1 | 1 | 1 | 0 |
| Küsimus 5. Hajusfailisüsteemi kasutamine | 1 | 1 | 1 | 0 | 0 | 0 |
| Küsimus 6. Standardsete süsteemikujutiste kasutamine | 1 | 1 | 1 | 0 | 0 | 0 |
| Küsimus 7. Tsentraalne süsteemikujutiste paigaldamine | 1 | 1 | 1 | 0 | 0 | 0 |
| Küsimus 8. Keskne tarkvarahaldus | 1 | 1 | 1 | 0 | 1 | 0 |
| Küsimus 9. Keskne riistvara ja tarkvara auditeerimise tarkvara | 1 | 1 | 1 | 0 | 1 | 0 |
| Küsimus 10. Keskne printserver | 1 | 1 | 1 | 0 | 1 | 0 |
| Küsimus 11. Keskse printserveri haldustarkvara | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 12. Kõrgkäideldavate tehnoloogiate kasutus | 1 | 1 | 1 | 0 | 0 | 0 |
| Küsimus 13. Serverite ja rakenduste virtualiseerimine | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 14. Arvutite, serverite ja seadmete 3 kuni 4 aastane elutsükkel | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 15. Kasutajate koolitamine vastavalt organisatsiooni vajadustele | 1 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 16. Identiteedi ja ligipääsu haldamise tarkvara | 0 | 0 | 0 | 0 | 0 | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Küsimus 17. Keskne viirustõrje-tarkvara | 1 | 1 | 1 | 1 | 1 | 0 |
| Küsimus 18. Keskne tulemüür teenuste ja sisevõrgu jaoks | 1 | 1 | 1 | 1 | 1 | 0 |
| Küsimus 19. Keskne tulemüür serverite jaoks | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 20. Keskne tulemüür arvutitöökohtade jaoks | 1 | 1 | 1 | 0 | 1 | 0 |
| Küsimus 21. Keskne spämmikaitse | 1 | 1 | 1 | 1 | 1 | 1 |
| Küsimus 22. Ründekaitse tarkvara | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 23. Turvaline kaugligipääs | 1 | 1 | 1 | 1 | 1 | 1 |
| Küsimus 24. Serverite ja töökohtade vahelise andmeside isoleerimine | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 25. Turvaline traadita võrk | 1 | 1 | 1 | 1 | 0 | 0 |
| Küsimus 26. Avaliku võtme infra. koos mitmetasandilise autentimisega | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 27. Arvutivõrku sisenemise kaitse | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 28. Tsentraalne varundus ja taastelahendus | 1 | 1 | 1 | 1 | 1 | 0 |
| Küsimus 29. Profiili hoidmine keskses failiserveris | 1 | 1 | 1 | 1 | 1 | 0 |
| Küsimus 30. Mobiilsete seadmete kaitse | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 31. Mobiilsete seadmete jälgimine | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 32. VOIP tehnoloogia | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 33. IT strateegia | 1 | 1 | 1 | 1 | 1 | 1 |
| Küsimus 34. IT turvapoliitika | 1 | 1 | 1 | 1 | 1 | 1 |
| Küsimus 35. Riist- ja tarkvara standardid | 1 | 1 | 1 | 1 | 1 | 1 |
| Küsimus 36. Talituspidevusplaan | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 37. Taasteplaan | 1 | 1 | 1 | 1 | 1 | 1 |
| Küsimus 38.ISKE rakendamise staatus: | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Küsimus 38.a. Infovarad on kaardistatud | 1 | 1 | 1 | 1 | 1 | 1 |
| Küsimus 38.b. Määratud turvaklassid koos vastavate turbeastmetega | 1 | 1 | 1 | 1 | 1 | 1 |
| Küsimus 38.c. Määratud lähtuvalt turvaastmest vastavad turvameetmed | 1 | 1 | 1 | 1 | 1 | 1 |
| Küsimus 38.d. Koostatud turvameetmete vastav rakenduskava | 1 | 1 | 1 | 1 | 1 | 1 |
| Küsimus 38.e. ISKE turvameetmed on rakendatud | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 38.f. Teostatakse järje-pidevat kontrolli turvameetmete üle | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 39. Haldamis-protsesside rakendamine: | | | | | | |
| Küsimus 39.a. Intsidentide haldamine | 1 | 1 | 1 | 0 | 1 | 0 |
| Küsimus 39.b. Probleemide haldamine | 1 | 1 | 1 | 0 | 1 | 0 |
| Küsimus 39.c. Konfiguratsiooni haldamine | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 39.d. Teenustasemete haldamine | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 39.e. Käideldavuse haldamine | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 39.f. Mahtude haldamine | 1 | 1 | 1 | 0 | 1 | 0 |
| Küsimus 39.g. IT finantshaldamine | 1 | 1 | 1 | 1 | 1 | 1 |
| Küsimus 39.h. Sündmuste haldamine | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 39.i. Muudatuste haldamine | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimus 39.j. Versioonide haldamine | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimust 39.k. IT teenuste teadmiste juhtimine | 0 | 0 | 0 | 0 | 0 | 0 |
| Küsimust 39.l. IT teenuste portfell ja selle haldamine | 0 | 0 | 0 | 0 | 0 | 0 |
| Optimeeritud mudeli koguhinne : | 32 | 31 | 31 | 19 | 26 | 11 |