Tallinna Ülikool

Digitehnoloogiate Instituut

# "IT riskijuhtimise standardite ja parimate praktikate rakendamisest Eesti avaliku sektori asutustes"

Magistritöö

Autor: Oliver Närep

Juhendaja: Andro Kull

Autor: …… „ …….. „ 2016

Juhendaja: …… „ ……..….. „ 2016

Instituudi direktor: ……... „ ……..….. „ 2016

Tallinn 2016

**Autorideklaratsioon**

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

..... .....

*(kuupäev)* *(allkiri)*

**Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks**

Mina _____ (sünnikuupäev: _____)

(*autori nimi*)

annan Tallinna Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose:

"IT riskijuhtimise standardite ja parimate praktikate rakendamisest Eesti avaliku sektori asutustes"

mille juhendaja on Andro Kull,

säilitamiseks ja üldsusele kättesaadavaks tegemiseks Tallinna Ülikooli Akadeemilise Raamatukogu repositooriumis.

olen teadlik, et nimetatud õigused jäävad alles ka autorile.

kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas, _____

*allkiri ja kuupäev*

# SISUKORD

# 1. SISSEJUHATUS

IT süsteemide kasutamine oma igapäeva töö korraldamises on muutunud tavapäraseks igas ettevõttes. Infotehnoloogia arenguga on muutunud IT lahenduste kasutamine meie elu loomulikuks osaks olgu siis parkimise eest tasumisel või oma pangaasju korraldades. Keerulisemad infosüsteemid haldavad energiataristuid ja aitavad juhtida süsteeme väga erinevates eluvaldkondades. Nii suures ulatuses IT lahenduste kasutamine kujutab endast ka riski ja eeldab süsteemide teadlikku kasutamist. Ei ole ju raske ette kujutada kaost või kahju tekkimist vangla turvasüsteemi rikkest või haiguslugude andmete lekkimisel. Sageli riske ei teadvustata või ei osata neid riske piisavalt hinnata. Paljud Eesti avaliku sektori asutused ja ka eraettevõtted peavad igapäevaselt langetama otsuseid, kuidas korraldada oma asutuse IT riskide juhtimist. Väga sageli puudub asutusel terviklik IT riskijuhtimise poliitika ning riskide haldusega ei tegeleta süsteemselt ja regulaarselt. Vastavaid tööülesandeid täidab harilikult oma põhitöö kõrvalt mõni IT spetsialist, tuginedes omandatud haridusele, töökogemusele ning isiklikule eelistusele. Selline töökorraldus ei taga piisavalt IT riskide maandamist asutuses. Mõned asutused ei pööra IT riskidele ning nende juhtimisele üldse tähelepanu, teistel juhtudel on aga näiteks IT riskide piirangutele viidates takistatud kiire ning mugav asutuse igapäevaste ülesannete täitmine. Eespool kirjeldatut kinnitab ka RIA (Riigi Infosüsteemi Amet) 2014. aasta küberturbe aruanne, kus märgitakse, et kahjuks iseloomustab Eesti IT turvalisuse maastikku asjaolu, et toimub IT-ressursside hoolduskohustuse ignoreerimine, mida võimendab asjaolu, et mitmed organisatsioonid ei reageeri turvavigadele mõistliku aja jooksul. Selline reageerimislünk on oht nii infosüsteemidele kui ka internetti ühendatud automaatjuhtimissüsteemidele, mis reguleerivad näiteks vee, elektri ja kütte toimimist (RIA, 2015). IT riskide haldamiseks vajavad organisatsioonid IT riskijuhtimissüsteemi, mis tugineks asjakohastele standarditele, metoodikale ning parimale praktikale.

Käesoleva magistritöö teemaks on valitud "IT riskijuhtimise standardite ja parimate praktikate rakendamisest Eesti avaliku sektori asutustes". Magistritöö teema on valitud lähtudes autori huvist IT-riskijuhtimise valdkonna vastu, kuna ta täidab ka ise IT-riskijuhi rolli oma igapäevases töös avaliku sektori asutuses. Uurinud vastavat erialast kirjandust, selgus, et erinevate standardite, metoodikate ja parimate praktikate omavahelisest võrdlemisest ei ole

väga palju kirjutatud. Seetõttu süvenes autori soov uurida, kuidas analoogsed organisatsioonid on korraldanud IT-riskijuhtimist Eestis ning millised võiksid olla valikukriteeriumid, millele toetudes saaks kasutusele võtta asjakohaseid standardeid, metoodikaid ning töövahendeid.

Viimastel aastatel on oluliselt kasvanud organisatsioonides mure, et IT süsteemide või lahenduste kasutamisel võib lekkida konfidentsiaalne info või ärisaladused. Igapäevaseks on muutunud meedia teated selle kohta, et lekkinud on teave ettevõtte personali, toodete või muu tundliku info kohta. Poliitiline ebastabiilsus mitmetes riikides ja piirkondades mõjutab tuntavalt antud olukorda ning kasvatab vastavaid IT riske. Ka küberrünnakud on jätkuvalt oluline ohuallikas, millega puutuvad kokku igat tüüpi organisatsioonid. Selle tagajärjel kannavad nad kahju oma varade võimaliku väärtuse langusest või potentsiaalsest ohust muutuda ajutiselt tegutsemisvõimetuks. IT varad ning nende kaitsmine on muutunud väga oluliseks, kuna nende abil on võimalik tagada organisatsiooni elujõulisuse ning järjepidevus (Kouns, Minoli, 2010). IT riskide mõistmise olulisusest saadakse üha paremini aru. Ernst & Young'i poolt 2013. aastal läbi viidud uuringu kohaselt on rohkem kui 50% ettevõtetest suurendanud oma investeeringuid IT riskide juhtimisse ning IT riskide olemust mõistetakse üha paremini, mistõttu on kokkuvõttes suurenenud teadlikkus IT riskide olemusest (Ernst & Young Managing IT risk, 2013). RIA poolt 2014. aasta sügisel Eesti riigiasutuste ja elutähtsat teenust osutavate asutuste IT juhtide seas läbi viidud küsitluse põhjal tegi RIA muuhulgas järelduse, et parandada tuleb juhtkonna riskiteadlikust ning targaks riskide hindamiseks on oluline panustada riskide tuvastamisse ja analüüsi, eriti sõltumatute auditite ja testide kaudu (RIA, 2015). Seega, eelkõige vajab organisatsioon IT riskijuhtimist selleks, et riskide juhtimise abil maandada võimalikke riske ja ohte ning selleks, et tagada endale võetud eesmärkide täitmine.

Eelpool kirjeldatud probleemide uurimiseks seadis autor neli eesmärki:

1) Anda ülevaate IT riskijuhtimise olemusest ning erinevatest standarditest, metoodikatest ja töövahenditest.
2) Selgitada välja sobivad hindamiskriteeriumid ja metoodika Eesti avaliku sektori asutuste ning elutähtsa teenuse osutajate[1] jaoks ning viia läbi standardite, metoodikate ja töövahendite hindamine.

[1] Elutähtsa teenuse osutaja Hädaolukorra seaduse mõistes.

3) Saada ülevaade sellest, kuidas on IT riskijuhtimine korraldatud Eesti avaliku sektori asutustes ning elutähtsa teenuse osutajate juures. Ülevaate saamiseks korraldab töö autor veebipõhise uuringu vastava valimi hulgas.
4) Teha magistritöö uuringu tulemustest kokkuvõte ja järeldused ning esitada omapoolsed soovitused, millega võiks arvestada erinevate standardite, metoodikate ja töövahendite valimisel.

## 1.1 Eesmärk ja metoodika

Magistritöö eesmärk oli läbi töötada asjakohane erialane kirjandus ja interneti allikad, et saada ülevaade kasutatavatest IT riskijuhtimise standarditest, metoodikatest ja töövahenditest. Samuti oli uurimistöö üks eesmärke selgitada välja, millised võiksid olla need hindamiskriteeriumid ja metoodika, mille abil oleks võimalik hinnata teoreetilisest vaatenurgast lähtuvalt erinevaid IT riskijuhtimise standardeid, metoodikaid ja töövahendeid ning viia läbi ka esialgne hindamine. Autor soovis välja selgitada kas Eesti avaliku sektori asutuses valdavalt rakendatav ISKE (Infosüsteemide Kolmeastmeline Etalonturbe Süsteem) meetod on parim valik IT riskide maandamiseks või sobivad ka teised standardid ja metoodikad mida võiks kasutada. Kas eksisteerib laiem praktika standarditest ja metoodikatest ning kas nende omavahelised võrdlemistulemused ja Eesti rakendatav praktika annavad samu tulemusi.

Tuginedes väljavalitud hindamiskriteeriumitele hindas autor *Saaty* analüütiliste hierarhiate meetodi abil (vt. p. 4.2.2) erinevaid standardeid ja metoodikaid, mida võiks Eestis avaliku sektori organisatsioonid ja elutähtsa teenuse osutaja kasutada oma organisatsioonide IT riskide juhtimiseks.

Võrdlemaks magistritöö teoreetilise osa tulemusi tegeliku praktikaga Eesti avaliku sektori asutuste ja elutähtsa teenuse osutajate hulgas, viis autor läbi vastava küsitluse. Uuring võimaldas saada ülevaate, millised erinevaid IT-riskijuhtimisega seotud standardeid ja metoodikaid juba kasutatakse IT-riskide juhtimisel. Küsitluse tulemustele tuginedes oli järgnevalt võimalik võrrelda uurimistöö teoreetilise osa tulemusi praktilise osa tulemustega.

Kasutades uurimistöö teoreetilise osa ülevaadet ning IT riskijuhtimise standardite, metoodikate ja võrdlemise tulemusi, koostas autor magistritöö praktilises osas uuringu küsimused. Läbi

viidud küsitlus andis ülevaate sellest, milliseid standardeid ja metoodikaid tegelikult juba kasutatakse avaliku sektori asutustes ja elutähtsa teenuse osutajate poolt. Küsitluses kasutatud uurimismeetodiks oli kvalitatiivne uuring, mis viidi läbi sihtrühma hulgas.

Ettevalmistatud küsimustiku (vt. Lisa 1) koostamisel lähtuti eelkõige magistritöös püsitatud eesmärkidest, et oleks võimalik võrrelda ja analüüsida teoreetilise osa hindamise tulemusi. Informatsiooni kogumisel tagati küsitluses osalejatele anonüümsus. Koostatud küsimustik koosnes kaheteistkümnest küsimusest (vt. Lisa 1) ning elektroonilises uuringus osalemise kutse saadeti kokku 379 organisatsioonile Eestis. Valimi koostamisel võeti aluseks eelkõige Riigi Infosüsteemi haldussüsteemi andmebaas (RIHA, 2015) ning valimit täiendati selliselt, et küsitlusse oleks haaratud ka Hädaolukorra seadusest tulenevad elutähtsa teenuse osutajate tegevusvaldkonnad.

Peamised põhjused, miks autor kasutas andmete kogumiseks küsimustikku:

1) Küsimustik andis võimaluse saada ülevaate kuidas avaliku sektori asutused ja elutähtsa teenuse osutajad on korraldanud oma organisatsioonides IT riskijuhtimist.
2) Saada ülevaade milliseid IT riskijuhtimise standardeid ja metoodikaid on kasutusele võetud.
3) Saada ülevaade, milliseks hinnatakse vajadust IT riskijuhtimise järele.
4) Saada ülevaade, kas IT riskijuhtimises planeeritakse teha muudatusi.

Autor koostas uuringu tulemustest kokkuvõtte (vt. pt.6). Valikvastustega küsimuste vastuseid analüüsiti lähtudes nii vastuste numbrilistest väärtustest kui ka protsentuaalsest osakaalust. Uuringu avatud küsimustes oli vastajatel võimalik oma sõnadega kirjeldada IT riskijuhtimise korraldust ning anda täiendavaid selgitusi, arvamusi ja kommentaare, millele tuginedes oli autoril võimalik teha täiendavaid omapoolseid järeldusi (vt. pt.7 ). Nii küsitluse suletud kui ka avatud küsimused aitasid kaasa magistritööle seatud eesmärkide täitmisele.

Magistritöö teoreetilise osa tulemuste ja praktilise osa uuringu põhjal tegi autor omapoolseid soovitusi ja ettepanekuid millega võiksid Eesti avaliku sektori asutused ning elutähtsa teenuse osutajad arvestada, kui nad plaanivad võtta kasutusele mõnda IT-riskijuhtimise standardit, metoodikat või töövahendit. Lisaks pakutakse magistritöös välja ka mõningaid ideid ja

soovitusi kuidas oleks üldiselt võimalik antud valdkonnas tööd korraldada selliselt, et kõik osapooled saaksid sellest maksimaalselt kasu.

Magistritöö tulemusel on teistel sarnastel organisatsioonidel võimalik hoida kokku oma raha- ja inimressurssi selleks, et teha paremini põhjendatud ning läbimõeldud valikuid IT riskijuhtimissüsteemi standardite, metoodikate ja töövahendite juurutamiseks või muudatuste ellu kutsumiseks IT riskijuhtimissüsteemi ümberkorraldamisel.

## 1.2 Magistritöö struktuur

Magistritöö koosneb seitsmest peatükist. Eraldiseisvateks osadeks on lühendite seletused ning lisad.

Esimene peatükk on sissejuhatus, mis annab ülevaate teema valiku põhjendustest, ja töö eesmärgist ning ülesannete püstitusest. Lisaks kirjeldab autor põhjalikumalt magistritöö kasutatavat uurimis- ja arendusmetoodikat. Teises peatükis tutvustatakse IT riskijuhtimise olemust ning antakse ülevaade IT riskidest juhtimisest ja hindamisest. Kolmandas peatükis tutvustab autor rahvusvahelisi standardeid, millele paljuski tuginevad kasutusele võetud erinevad metoodikad ning töövahendid. Järgnevalt tutvustatakse lähemalt IT riskijuhtimise meetodeid ning erinevaid töövahendeid. Neljandas peatükis annab autor ülevaate IT riskijuhtimise standardite ja metoodikate hindamise erinevatest võimalusest. Viiendas peatükis võrdleb autor erinevaid IT riskijuhtimise standardeid ja metoodikaid, kasutades selleks analüütilise hierarhia meetodit. Tuginedes loodud mudelile saadakse tulemused. Kuues peatükk annab ülevaate läbi viidud praktilisest küsitlusest, mis viidi läbi avaliku sektori asutuste ning elutähtsa teenuse pakkujate hulgas selleks, et saada tagasisidet hetkel igapäevases töös kasutavatest parimatest IT riskijuhtimise standarditest ja praktikast. Seitsmendas peatükis analüüsib autor analüütilise hierarhia metoodikat kasutades saadud tulemusi ning võrdleb neid praktilise küsitluse tulemustega. Tuginedes eelnevale teeb autor uuringust järeldusi ning annab mõningaid soovitusi, kuidas võiks IT-riskijuhtimist korraldada avalikus sektori asutustes ning elutähtsa teenuse osutajate juures. Magistritöö võtab kokku viimane peatükk, milles antakse lühiülevaade magistritöö tulemusest.

# 2. RISKIJUHTIMISE KONTSEPTSIOON

## 2.1 Riskjuhtimise mõiste

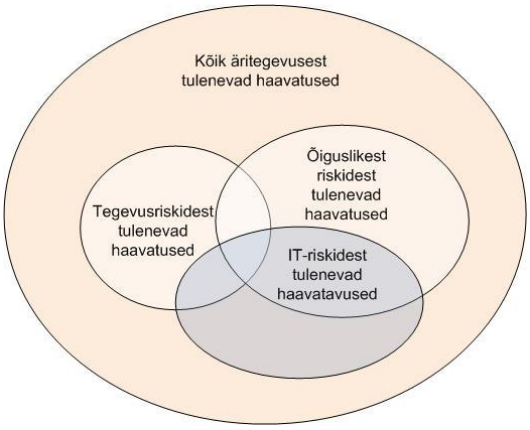
Käesolev peatükk annab ülevaate riski olemusest üldisemalt ning kirjeldab täpsemalt IT riskiga seonduvat. Defineeritakse IT riski mõiste, antakse ülevaade riskijuhtimisest ning selle juhtimise süsteemist.

Avaliku sektori asutused jaoks Eestis võivad riski mõiste defineerimisel lähtuda Rahandusministeeriumi juhendmaterjalist, mis ütleb, et *risk on võimalik oht, kui mingi sündmus (sündmuste kompleks), tegevus (tegevuste kompleks) või tegevusetus võib põhjustada vara või maine kaotuse ning mõjutab asutuse eesmärkide tulemuslikku täitmist*. Risk ei ole igasugune ebakindlus, vaid selline oht, mis omab potentsiaalset mõju ühele või mitmele eesmärgile. Selleks, et riskide esinemine ja nende esinemisega kaasnev võimalik mõju miinimumini viia nii, et nende ilmnemine ei tooks kaasa asutusele saatuslikke tagajärgi (s.t eesmärkide mittesaavutamine, ülesannete tulemuslik täitmine, vara või maine kaotus), on vajalik riskide pidev juhtimine (Riskijuhtimine. Rahandusministeerium, 2015).

Riskijuhtimise peamine ülesanne organisatsioonis on tagada, et läbi riskide juhtimise on võimalik kaitsta organisatsiooni vara. Järelikult tuleb riskijuhtimist käsitleda eelkõige kui haldamise funktsiooni, mitte pelgalt kui tehnilist ülesannet. Mõistmaks riske ning eriti aru saamaks riskide spetsiifilisusest, võimaldab riskijuhtimine omanikul oma vara kaitsta vastavuses selle tegeliku väärtusega organisatsioonile. Kuivõrd kõikide organisatsioonide ressursid on piiratud siis ei ole võimalik mitte kunagi kõiki riske vähendada nullini. Niisiis, riskide mõistmine, eriti selle ohu suurusest aru saamine, võimaldab organisatsioonidel prioritiseerida ressursse, et vähendada riske (Elky, 2006).

IT riskijuhtimine on osa üldisest äririskide juhtimisest (vt. Joonis 1). Pole kahtlust, et IT riskijuhtimine on osa organisatsiooni terviklikust riskijuhtimise protsessist. Riskid muutuvad ajas pidevalt ning seetõttu ei ole ammendavat lahendust riskijuhtimisega seotud väljakutsetele. Viimase veerandsajandi jooksul on avaldatud palju raamatuid ning erialakirjandust infoturbe juhtimise kohta ning selle üldistest toimemehhanismidest, kuid kahjuks pööratakse nendest

teostes pigem tähelepanu andmevõrkude turvalisuse probleemidele ning vähem on leidnud käsitlust terviklik riskijuhtimine ning IT riskijuhtimine kui osa sellest protsessist (Kouns, Minoli, 2010).




Joonis 1. Riskijuhtimine *(Kouns, Minoli, 2010)*

IT riskidega ei tegeleta organisatsioonis piisavalt eelkõige seetõttu, et sellele ei pöörata piisavalt tähelepanu, puuduvad vastavad teadmised või on need puudulikud. Selle põhjuseks on sageli töötajate lahkumine või koondamine aga ka liigne toetumine välistele konsultantidele või ekspertidele. Teiseks on suur probleemide rühm seotud halvasti juhitud infrastruktuuri korraldusega, mis on seotud sageli vananenud tehnoloogiate kasutamisega. Väga oluline on ka inimfaktor. Töötajate ignorants, hoolimatus ja ükskõiksus põhjustab väga märkimisväärsel määral IT riske. Lisaks puuduvad automaatsed kontroll- ning monitooringusüsteemid, mis suudavad jälgida erinevate süsteemide ning rakenduste tööd (Georg Westerman, Richard Hunter, 2007).

## 2.2 IT risk ja riskijuhtimine

Mõistet „IT risk“ on võimalik defineerida mitut moodi. Järgnevalt kirjeldan, kuidas selgitavad IT riski mõistet tähtsamad rahvusvahelised institutsioonid maailmas:

**ISO** (The International Organization for Standardization) defineerib IT riski kui ohu, mis potentsiaalselt võimaldab ära kasutada varade või nende grupi nõrkusi ja põhjustab seetõttu

erinevat haavatavust. Seda mõõdetakse korrutades sündmuse ja selle tagajärgede toimumise tõenäosust (EVS-ISO/IEC 27005:2014, 2014).

**NIST** (National Institute of Standards and Technology) defineerib IT riske läbi mitme erineva dokumendi. IT risk on mõõdik, mille abil hinnatakse võimalikku sündmust või olukorda ning on tüüpiliselt jaotatud:

- kahjuks, mis võib tekkida, kui sündmus või olukord leiab tõenäoliselt aset;
- juhtumi toimumise tõenäosuseks.

Infosüsteemiga seonduvad turvariskid on need, mis tekivad konfidentsiaalsuse puudulikkusest, rikutusest või info kättesaadavusest ja nad omavad võimalikku kahjustavat mõju tegevusele (kaasa arvatud ülesanded, funktsioonid, kuvandid ja maine), ligipääsule, isiklikele ja teistele organisatoorsetele ja riiklikele funktsioonidele (NIST Special Publication 800-37. Revision 1, 2015).

**ISACA** (Information Systems Audit and Control Association) poolt avaldatud *Risk IT Framework´is* on selgitatud IT riski selliselt: „Äririsk seondub kasutamise, omandi, äritegevuse, selles osaluse, mõju ja IT rakendamisega ettevõtte siseselt“. *Risk IT Framework* kohaselt on IT riskil laiem tähendus. See ei hõlma mitte ainult negatiivset mõju tegevustele ja teenuste osutamisele, mis võib tuua kahju organisatsioonile, vaid pakub ka kasu ning väärtust. IT riskide juhtimine võimaldab lõigata riskidest kasu läbi tehnoloogiate kasutamise selleks, et vähendada äritegevusele ebasoodsaid mõjusid (The Risk IT Framework, 2015).

Riskide juhtimine on eelkõige protsess, mis võimaldab IT-juhil leida vajalik tasakaal kaitsemeetmete ja majanduslike kulude vahel selleks, et tagada IT süsteemide ja andmete kaitse. See protsess ei ole unikaalne IT keskkond. See on läbiv protsess kõigis meie igapäeva otsuste tegemisel. IT juhi valikuid võib näiteks võrrelda kodumajapidamise turvalisuse tagamisega. Paljud inimesed otsustavad kodudesse paigaldada kalleid turvasüsteeme, millele lisanduvad igakuised teenustasud selleks, et paremini jälgida ning kaitsta oma vara. Võib oletada, et koduomanikud on põhjalikult kaalunud kulutuste suurust ning hinnanud neid kulutusi piisavalt väikesteks võrreldes oma kodus paiknevate esemete väärtusega.

Sarnaselt eelnevale alapunktile defineerime IT riskijuhtimise mõistet läbi kolme rahvusvahelise organisatsiooni (ISO, NIST ja ISACA) poolt pakutule.

Riskijuhtimine on kooskõlastatud tegevus organisatsiooni suunamiseks ja ohjamiseks riski suhtes. Riskijuhtimise protsess on juhtimispoliitika, protseduuride ja tavade süstemaatiline rakendamine riskialase teavituse ja nõupidamiste, selle konteksti määramise, tuvastamise, analüüsimise, hindamise, käsitlemise, seire ja ülevaatuse eesmärgil (EVS-ISO/IEC 31000:2010, 2010).

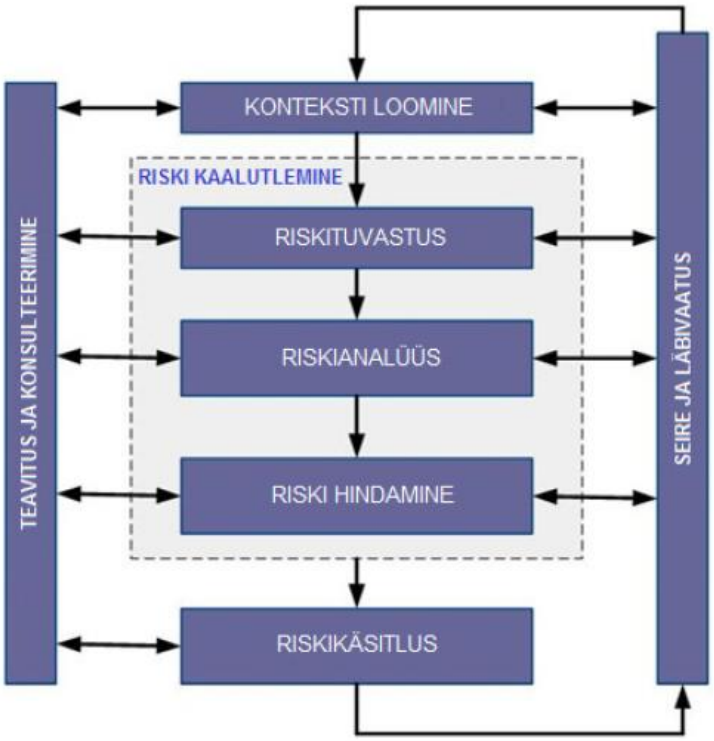
Riskide juhtimise protsess koosneb järgmistest osadest (EVS-ISO/IEC 31000:2010, 2010):

- Riskide konteksti määramine;
- riskihindamine, mis omakorda koosneb järgmistest osadest:
    - riskituvastus;
    - riskianalüüs;
    - riski taseme hindamine;
    - riskikäsitlus;
    - seire ja ülevaatus.

Selleks, et riskijuhtimine oleks mõjus, peaks organisatsioon oma kõigil tasanditel järgima järgnevaid riskijuhtimise põhimõtteid (EVS-ISO/IEC 31000:2010, 2010):

- ta loob ja kaitseb väärtusi;
- on lahutamatu osa kõigist organisatsioonilistest protsessidest;
- on osa otsustamisprotsessist;
- suunab üksikasjalikult määramatust;
- on süstemaatiline, struktureeritud ja õigeaegne;
- põhineb parimal teadaoleval teabel;
- on kohaldatud olemasolevate tingimustega;

- võtab arvesse inimlikke ja kultuurilisi tegureid;
- on läbipaistev ja kaasahaarav.




Joonis 2. Riskihalduse protsess *(EVS-ISO/IEC 31000:2010, 2010)*

Head riskijuhtimist iseloomustab (EVS-ISO/IEC 31000:2010, 2010):

- organisatsioonil on kehtiv, tõene ja ülevaatlik arusaam oma riskidest;
- organisatsiooni riskid on tema riski normide piires;
- toimub organisatsiooni tegevuste pidev parendamine;
- eksisteerib täielik riskide aruandekohustus ning osapoolte teavitamine;
- riskijuhtimine on ühildatud organisatsiooni struktuuriga.

## 2.3 IT riskide hindamine

Riskihindamine on kogu riskituvastuse, riskianalüüsi ja riski taseme hindamise protsess tervikuna. Riskide hindamisel on kolm olulist etappi. Nendeks on *riskituvastus, riskianalüüs ja riski tasemehindamine.* Seega tuleb kindaks teha riskide allikad, mõjualad sündmused ja nende põhjused ning võimalikud tagajärjed. Riskianalüüsi etapis on väga oluline, et see peab endaga kaasa tooma parema arusaamise riski olemusest. Ta annab vajaliku sisendi riski taseme hindamisele ja otsustele, kas riskid peavad olema käsitletud, samuti enamikule riskikäsitlemise strateegiatest ning meetoditest. Riski tasemehindamise eesmärk aga on aidata kaasa otsuste langetamisele, mis tulenevad riskianalüüsi väljunditest ning sellest, missugused riskid vajavad käsitlemist sh. prioriteetide rakendamisest. Vastav etapp sisaldab endas ka analüüsi ning leitud riski taseme võrdlemist riski kriteeriumitega. Eelnevale tuginedes on võimalik kaaluda ka riski käsitlemise vajadust. Kindlasti peab otsuste tegemisel arvestama ka riski laiemat konteksti nende riskide talutavuse kaalutlemisel, mida kannavad teised osapooled (EVS-ISO/IEC 31000:2010, 2010).

## 2.4 Infoturvariski haldus

Teabe turvalisuse nõudeid puudutavate organisatsiooni vajaduste väljaselgitamiseks ja toimiva infoturbe halduse süsteemi (ISMS-i) loomiseks on vajalik mingi süstemaatiline lähenemine infoturvalisuse haldusele. See lähenemisviis peaks sobima organisatsiooni keskkonnaga ja sealhulgas olema kooskõlas ettevõtte üldise riskihaldusega. Turbeüritused peaksid tegelema riskidega toimivalt ja õigeaegselt just seal, kus neid vajatakse ja just siis, kui neid vajatakse. Infoturberiski haldus peaks olema kõigi infoturbehalduse tegevuste lahutamatu osa ja seda tuleks rakendada nii ISMS-i käiku andmisel kui ka käigus hoidmisel (EVS-ISO/IEC 27005:2014, 2014).

Infoturvariski haldus peab andma panuse (EVS-ISO/IEC 27005:2014, 2014):

- riskide tuvastamisse;
- riskide kaalutlemisse, väljendatuna tagajärgedena äritegevusele ja realiseerumise tõenäosusena;

- nende riskide tõenäosuse ja tagajärgede teatavakstegemisele ja tundmisele;
- riskikäsitluse prioriteetide järjestamisele;
- riskide realiseerumist vähendavate meetmete prioriteetsusesse;
- riskiosaliste kaasamisele riskihalduse otsuste tegemisse ja informeerimisele riskihalduse seisust;
- riskikäsitluse seire toimivusele;
- riskide ja riskihaldusprotsessi regulaarsele seirele ja läbivaatusele;
- teabe kogumisele riskihalduse metoodika täiustamiseks;
- juhtide ja personali koolitusele riskide ja nende leevendamise meetmete alal.

# 3. IT RISKIJUHTIMISE JUHENDID

IT riskijuhtimise vahenditest ülevaate saamiseks peab lähemalt uurima kolme olulist osa: standardid, metoodikad ja töövahendid ehk tarkvara, mida kas üksinda kasutades või erinevaid standardeid ja metoodikaid või tarkvara omavahel kombineeritult kasutades on võimalik IT riskijuhtimist asutuses korraldada. Selle tulemusel tekib organisatsioonides igapäevase töö käigus IT riskijuhtimise praktika kogum. Aegamööda leiab parim praktika ja kogemused rakendamist ka teistes asutustes.

## 3.1 IT riskijuhtimise standardid

Olulisemad rahvusvahelised organisatsioonid, kes töötavad välja vastavaid standardeid on ISO, ISACA, NIST ja ENISA (European Union Agency for Network and Information Security). IT riskijuhtimises kasutatakse standardeid kui normdokumente, mis on koostatud valdkonna ekspertide konsensuse alusel ja mille on vastu võtnud tunnustatud asutus. Eesmärgiks on luua reeglite ja juhtnööride kogum IT riskide juhtimiseks, et saavutada protsesside ja teenuste parenemine (EVS, 2015). Järgnevalt käsitletakse põhjalikumalt nendest olulisemaid.

**ISO/IEC 27000.** Standard annab ülevaate infoturbe halduse süsteemidest ning ISMS-i standardiperes kasutatavatest ühistest terminitest ja määratlustest. Vastav standard on rakendatav igat liiki ja iga suurusega organisatsioonides, näiteks äriettevõtetes, riigiasutustes ning ka mittetulunduslikes organisatsioonides (EVS-ISO/IEC 27000:2015, 2015).

**ISO/IEC 27001.** Standard keskendub sertifitseerimise protsessile. Võimaldab võrrelda ja hinnata infoturbe juhtimise süsteemi kontrollküsimustiku abil. Standard ei hõlma riskianalüüsi või riskijuhtimise sertifitseerimist. Kuigi standard on algselt välja töötatud Ühendkuningriikides, on ta kohaldatud vastavaks ISO standardiga koos mõningate muudatustega. Standardi sertifikaat kinnitab organisatsiooni vastavust kindlaksmääratud nõuetele vastava infoturbe juhtimise osas (ISO/IEC 27001, 2015).

**ISO/IEC 27002.** Standard annab suunised organisatsiooni infoturbestandardite ja infoturbehalduse praktikate kohta, sealhulgas kuidas valida, rakendada ja hallata meetmeid, võttes arvesse organisatsiooni infoturberiski keskkonda või keskkondi. Sobib kasutamiseks

organisatsioonides, kes kavatsevad valida meetmeid protsessi käigus, millega teostatakse ISO/IEC 27001 põhinevat infoturbehalduse süsteemi. Võimaldab välja arendada omaenda infoturbehalduse suunised ning teostada üldtunnustatud infoturbemeetmeid (EVS-ISO/IEC 27002:2014, 2014).

**ISO/IEC 27003.** Standard keskendub olulisematele aspektidele, mida tuleb arvestada infoturbe halduse süsteemi (ISMS) edukaks kavandamiseks ja teostamiseks kooskõlas standardiga ISO/IEC 27005. Selles kirjeldatakse ISMS´i spetsifitseerimise ja kavandamise protsessi algatamisest kuni rakendusplaanide koostamiseni. Samuti kirjeldatakse protsessi, millega saadetakse ISMS'i teostamiseks juhtkonna heakskiit, määratakse ISMS'i rakendamise projekt ning antakse juhised selle kohta, kuidas planeerida ISMS projekti, mis tuleb lõplikult ISMS projekti rakendusplaanist.

**ISO/IEC 27004.** Vastav standard annab juhiseid kuidas läbi viia IT arendustöid ja pakub välja meetmed ning metoodika, kuidas hinnata ning kontrollida ISMS infoturbe halduse süsteemi efektiivsust nagu on kirjeldatud ISO/IEC 27001 standardis (EVS-ISO/IEC 27004:2009, 2009).

**ISO/IEC 27005.** Standard annab suuniseid infoturvariski halduseks organisatsioonis ning toetab muuhulgas ISO/IEC 27001 nõudeid infoturbe halduse süsteemidele (ISMS). See standard ei anna aga infoturvariski halduseks mingit konkreetset meetodit. Organisatsiooni ülesandeks jääb määratleda oma lähenemine riskihaldusele sõltuvalt näiteks ISMS´i käsitlusalast, riskihalduse kontekstist või majandussektorist. ISMS´i nõuete täitmiseks selles standardis kirjeldatud raamstruktuuris saab kasutada mitmeid olemasolevaid metoodikaid. Standardit saab rakendada igat tüüpi organisatsioonile, kes kavatsevad hallata riske, mis võivad rikkuda organisatsiooni teabe turvalisust (EVS-ISO/IEC 27005:2014, 2014).

**ISO/IEC 27032.** Standard annab juhiseid, kuidas arendada küberjulgeolekut, keskenduses seejuures info turvalisusele, võrkudele, internetile ja kriitilisele infrastruktuurile. Dokument tutvustab parimaid praktikaid, mida küberturvalisuse eest vastutavad isikud peaksid kasutama andes seejuures ülevaate küberturvalisusest. Standard selgitab küberturvalisuse vahekorda teist liiki turvavaldkondadega, määratleb vastutavad isikud ning nende rollid ning pakub raamistiku, et hallata ja teha koostööd küberturvalisuse valdkonnas (EVS-ISO/IEC 27032:2012, 2012).

**ISO/IEC 31000.** Standard on ette nähtud täitma laia huvipoolte ringi vajadusi. Standard on mõeldud neile, kelle kohustus on arendada riskijuhtimise poliitikat oma organisatsioonis. Samuti on ta suunatud vastutajatele, kes tagavad, et risk on mõjusalt hallatud organisatsioonis tervikuna, spetsiifilises valdkonnas, projektis või tegevuses. Lisaks aitab ta hinnata organisatsiooni riskijuhtimise mõjusust ning on abiks standardite, juhiste, protseduuride ja tavakoodeksite arendajatele, kes kehtestavad tervikuna või osaliselt riskijuhtimise viisid tulenevalt nende dokumentide spetsiifikast (EVS-ISO/IEC 31000:2010, 2010).

**ISO/IEC 31010.** Standard on ISO 31000 toetav ning annab juhised riskihindamise süstemaatiliste meetodite valimiseks ja rakendamiseks. Standardikohane riskide hindamine aitab kaasa muudele riskijuhtimistegevustele. Tutvustatakse mitmesuguste meetodite rakendamist, tehes asjakohaseid viiteid muudele rahvusvahelistele standarditele, kus kirjeldatakse üksikasjalikumalt meetodite kontseptsiooni ja rakendamist (EVS-ISO/IEC 31000:2010, 2010).

**NIST SP800-16.** Standardi eesmärgiks on soodustada ning aidata kaasa tervikliku, mõõdetava, kuluefektiivse IT turvakoolituse programmi väljatöötamisele, et toetada organisatsiooni IT juhtimist üldisemalt sh. IT riskijuhtimist. Standard aitab aru saada, kuidas ning millisel määral IT´ga seotud ametikoha tööülesannete hulka kuulub IT turvalisuse eest vastutamine (NIST, 2015).

**NIST SP800-30.** Metoodika annab väga üksikasjalikud juhised ja aitab riske identifitseerida. Õpetab, kuidas tuleb käsitleda riskijuhtimist ja riskide hindamist. Metoodikas leidub üksikasjalikke küsimustikke, graafika (sh voogskeeme) ja matemaatilisi valemeid, samuti viiteid, mis selgitavad peamiselt USA seadusandlusest tulenevaid regulatiivseid küsimusi (SP800-30, 2015).

**NIST SP800-39.** Standardi eesmärk on anda juhiseid, kuidas korraldada kogu organisatsiooni IT riskide juhtimist. Vastavad juhised on struktureeritud, kuid pakuvad paindlikku lähenemist IT turvariskide juhtimisele, võimaldades üksikasjalikult hinnata erinevaid riske. Suunised pakuvad juhtimismudelit, mis aitavad organisatsioonidel teha paremaid riskipõhiseid otsuseid (NIST, 2015).

## 3.2 Riskide juhtimise ja hindamise meetodid

IT riskide juhtimise meetodeid ning töövahendeid on mitmed. Enamus suuri arenenud tööstusriike omab vastavat metoodikat ning sageli ka vajalikku töövahendit metoodika kasutamiseks. Järgnevalt käsitletud metoodikate valik ei ole kindlasti ammendav, kuid annab piisavalt põhjaliku ülevaate meetoditest, mida erinevad riigid ning organisatsiooni kasutavad. Sobiliku metoodika valimine võib olla seotud ka organisatsiooni päritolumaa või seotusega näiteks ettevõtte peakontoriga. Seetõttu võib osutuda vajalikuks võtta kasutusele metoodika, mis ei ole Eestis laialt tuntud. Samas on Euroopa Liidus valdkonna arengut suunav ENISA tunnistanud, et ei ole avaldatud piisavalt vastavaid uuringud, mis annaksid ülevaate olemasolevatest meetoditest, vahenditest ja headest tavadest (ENISA, 2015).

Järgnevalt esitan loetelu erinevatest meetoditest ja töövahenditest koos lühiülevaatega.

**Riskianalüüsi metoodika Eestis.** 2010. aastal kinnitas siseminister tuginedes Hädaolukorra seadusele määruse „Toimepidevuse riskianalüüsi koostamise juhend“[2], mis reguleerib elutähtsa teenuse osutaja poolt osutatava elutähtsa teenuse toimepidevuse riskianalüüsi koostamise korraldust. Tegemist on juhendiga, mida järgivad elutähtsa teenuse osutajad, kuid mida kasutavad kas rohkemal või vähemal määral ka teised riigiasutused oma igapäevases töös.

2014. aastal alustas RIA elutähtsate teenuse osutajatele suunatud IT-riskianalüüsi metoodika täiendamist ja uuendamist. Nad töötasid läbi üle saja riskianalüüsi ja toimepidevuse plaani ning pidid tõdema, et IKT (info- ja kommunikatsioonitehnoloogia riskide) kohta on infot pigem napilt ja seda on käsitletud pealiskaudselt. Seega otsustati riigi ootusi IKT-riskianalüüsile täpsemalt ja ühtsemalt kirjeldada. Juhendi koostamise lõpetab RIA 2015. aastal, kaasates Siseministeeriumi ja elutähtsa teenuse osutajaid ja korraldajaid. Juhendiga täiendatakse kehtivat regulatsiooni (RIA, 2015).

**Austria IT turvalisuse käsiraamat** koosneb kahest osast. Esimene osa annab üksikasjaliku kirjelduse IT turvalisuse haldamise protsessist, sealhulgas kirjeldab kuidas arendada turvapoliitikaid, riskianalüüse, kujundada julgeolekukontseptsioone ning rakendada turvaplaane ja järeltegevusi. Teine osa on kogumik 230 etalonturbe meetmest. Rakendamiseks

[2] RT 2010, 33, 179 Siseministri määrus nr 16 „Toimepidevuse riskianalüüsi koostamise juhend“ 08.06.2010

on saadaval prototüüp. Austria IT turvalisuse käsiraamat oli algselt välja töötatud valitsusasutustele, kuid on nüüd kättesaadav kõikidele organisatsioonidele. Käsiraamat vastab standardile ISO/IEC IS 13335, Saksa IT-*Grundschutzhandbuch* ja osaliselt ISO/ IEC17799 standardile (Austrian IT Security Handbook, 2015).

**CRAMM** (CCTA Risk Analysis and Management Method) on riskianalüüsi meetod, mille on välja töötanud CCTA (Central Computer and Telecommunications Agency), mis on hiljem liidetud OGC'ga (Office of the General Counsel). Vastav tööriist kannab sarnast nime. Metoodikat on üsna raske kasutada ilma CRAMM tööriistata. Esimene versioon oli mõeldud Briti valitsusasutustele. See on tegemist eelistatuim riskianalüüsi meetodi Ühendkuningriigis, mis on kasutust leidnud ka teistes riikides. CRAMM on eriti sobiv kasutamiseks suurtes organisatsioonides nagu valitsusasutused ja tööstusettevõtted (CRAMM, 2015).

**A&K analüüs.** Meetod *Afhankelijkheids- en Kwetsbaarheidsanalyse* töötati välja Hollandi ettevõte RCC poolt. Hollandi siseministeerium täiendas ning lõpetas metoodika arendustööd 1996. aastal ja avaldas selle käsiraamatuna. Meetodit ei ole sellest ajast uuendatud. Meetodi analüüs on unikaalne ja enim eelistatud meetod riskianalüüside läbiviimisel Hollandi valitsusasutustes alates 1994. aastast. Lisaks Hollandi valitsusasutustele, kasutavad metoodikat sageli ka kohalikud ettevõtted (Dutch A&K analysis, 2015).

**Ebios (**Expression des Besoins et Identification des Objectifs de Sécurité) on terviklik kogum juhendeid, mis sisaldab ka tasuta avatud lähtekoodiga tarkvara. Algselt välja töötatud Prantsuse valitsuse poolt, mida tänasel päeval toetavad erinevad eksperdid. Ekspertidest moodustunud riskijuhtimise foorum on aktiivne, mis uuendab Ebios metoodikat järjepidevalt. Nad töötavad välja parimaid tavasid ning dokumentatsiooni, mis on suunatud lõppkasutajate erinevates kontekstides. Ebios'i kasutatakse laialdaselt nii avalikus kui ka erasektoris, nii Prantsusmaal kui ka välismaal. Ta vastab tähtsamatele IT turvastandarditele.

Ebios on jaotatud viieks osaks ning on paindlik, pakkudes mitmesuguseid erinevaid väljundeid (turvalisuse eesmärgid, profiilid, tegevuskava jne). Erinevad standardid on lihtsasti lisatavad (nt: Saksa IT Grundschutz) sisemiste andmebaasidega (rünnaku meetodid, nõrkused jne) ja heade tavade kataloogidega (Ebios parimaid tavasid, ISO / IEC 17799;). (EBIOS, 2015).

**ISAMM (Information Security Assessment & Monitoring Method)** on ISMS toetav riskijuhtimise meetod koos seda toetavate töövahenditega. Metoodika on pidevalt arenev ning sisaldab rohkem kui 20-ne aastast kogemust, mis on seotud tuhandete infoturbe ja riskijuhtimise projektidega ning sisaldab kümneid teisi riskijuhtimise meetodeid ja vahendeid. Tegemist on kvantitatiivset tüüpi riskijuhtimise metoodikaga. Metoodika sisaldab ka otselinke ISO/IEC 27002 standardile. Metoodika pakub ka maksimaalset ISO/IEC 27001 tuge (ISAMM, 2015).

**ISF** (Information Security Forum) metoodika näeb ette rea kõrgetasemelisi põhimõtteid ja eesmärke infoturbele, millega kaasnevaid aruanded headest tavadest. Neid saab kasutada, et parandada turvalisuse taset organisatsioonis mitmel viisil. Metoodika koosneb järgmistest osadest:

- Riskihindamine (ettevõtte *Scorecard, Sara, SPRINT*);
- riski muutmise protsess (*The Standard of Good Practice*). Näeb ette rea kõrgetasemelisi põhimõtteid ja eesmärke infoturbeks koos nendega kaasneva aruandlusega;
- riski kaalutlemine (*The Standard of Good Practice*);
- riski kommunikatsioon (*FIRM*) (ISF, 2015)**.**

**IT Grundschutz (**IT Baseline Protection Manual) metoodika pakub meetodi kuidas organisatsioonis luua infoturbe halduse süsteemi. Metoodika hõlmab nii üldisi IT-turvalisuse soovitusi, millele kohaldub IT turvalisuse protsess kui ka üksikasjalike tehnilisi soovitusi, et saavutada vajalik IT turvalisuse tase konkreetses valdkonnas. *IT-Grundschutz* koosneb kolmest suurest osast: protsessi algatamine, IT turvakonseptsiooni loomine ja rakendamise planeerimine ning elluviimine. *IT-Grundschutz* pakub võimaluse kuidas luua raamistik IT turvalisuse juhtimiseks, pakkudes teavet kuidas kasutada üldlevinud IT komponente (mooduleid). *IT-Grundschutz* moodulid hõlmavad nimekirju olulistest ohtudest ning vastumeetmetest ka suhteliselt tehnilisel tasemel. Neid elemente on võimalik laiendada, täiendada või kohandada vastavalt organisatsioon vajadustele (IT-Grundschutz, 2015). Autorile on teada, et metoodikas pööratakse tulevikus rohkem tähelepanu riskihalduse protsessile ning soovitakse, et *IT-Grundschutz* oleks alalises vastavuses ISO 27001 standardiga.

**ISKE** (Infosüsteemide Kolmeastmeline Etalonturbe Süsteem) on infosüsteemide kolmeastmeline etalonturbe süsteem. ISKE väljatöötamisel ja arendamisel on aluseks võetud

Saksamaa avaldatav infoturbe standard – IT Baseline Protection Manual (saksa k. *IT-Grundschutz*).

ISKE rakendamise eesmärk on tagada infosüsteemides töödeldavatele andmetele piisava tasemega turvalisus. Süsteem on loodud eelkõige riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavatele infosüsteemidele ning nendega seotud infovaradele turvalisuse tagamiseks. ISKE't saavad kasutada ka äriettevõtted oma IT varadele turvalisuse tagamiseks. ISKE rakendusjuhendi esimene versioon valmis 2003, hetkel kehtib ISKE versioon 7. Autorile on teada, et hetkel toimub *IT-Grundschutz* viimase versiooni tõlge eesti keelde, et ette valmistada ISKE versioon 8.

ISKE's on kirjeldatud kolme turbe taset – madal (L), keskmine (M) ja kõrge (H). Vastav turbetase määratakse andmetele turvaklasside (turvaosaklasside) määramise kaudu. Turvaklasside määramisel lähtutakse teabe konfidentsiaalsusest, teabe terviklikkusest, aegkriitilise teabe käideldavusest, teabe hilinemise tagajärgede lubatavast kaalukusest. ISKE rakendamine asutuses on pidev protsess, sest muutuvad nii IT keskkond, turvaohud ja -meetmed kui ka rakendusjuhend. ISKE rakendusjuhend ilmub täiendatud kujul uue versioonina kord aastas, sõltuvalt allikmaterjali uute versioonide avaldamisest (RIA, 2015).

**Magerit** on avatud metoodika riskide analüüsimiseks ja riskide juhtimiseks, mis on töötatud välja Hispaania valitsuse poolt. Arendatud raamistik ja juhendid on mõeldud eelkõige avalikule sektorile, kuid arvestades avatud olemust, saab seda kasutada ka mujal. Metoodika algne versioon avaldati 1997 aastal ning järgmine versioon ilmus 2005. aastal. Tekst on tõlgitud ka inglise keelde. Metoodika eesmärk on pakkuda juhiseid selleks, et vastutavad isikud saaksid teadlikuks infosüsteemide olemasolust ning oleksid teadlikud riskidest ja vajadusest hallata neid õigeaegselt. Magerit pakub metoodikat kuidas riske hinnata, kirjeldada ja planeerida asjakohaseid meetmeid, et riske hallata. Kaudselt annab metoodika juhiseid, kuidas valmistada organisatsiooni ette hindamisteks, auditeerimiseks, sertifitseerimiseks või akrediteerimise protsessiks (Magerit, 2015).

**Marion** (Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau) on Prantsusmaal välja töötatud meetodika, mida uuendati viimati 1998. aastal. Marion põhineb auditeerimise metoodikal ja võimaldab hinnata IT turvariskide taset ettevõttes. Selleks kasutatakse erinevaid küsimustike. Turvalisuse taset hinnatakse 27 näitaja abil, mis on jaotatud

kuueks suureks teemaks. Igaühele neist antakse hinne vahemikus 0 kuni 4. Turvalisuse tagamiseks tuleb saavutada vähemalt hinne 3. Metoodika on endiselt kasutusel, kuid seda ei arendata enam edasi. Marion metoodikat hakkab tulevikus asendama Mehari metoodikaga (Marion, 2015).

**Mehari 2010 (Method for Harmonized Analysis of Risk)** metoodika annab täieliku juhtimismudeli vastavalt ISO 27005 standardi nõuetele, kirjeldades modulaarseid komponente ja protsesse. Metoodika hõlmab auditi abil varade liigitamist, ohtude võimalikkuse analüüsi ja haavatavusi. Samuti aitab metoodika analüüsida üldisi riskiolukordi ning pakub välja riskistsenaariume. Metoodika tugineb erinevatele parameetritele ja valemitele ning pakub optimaalset valikut kuidas olukorda parandada (Mehari 2010, 2015).

**MIGRA (**Metodologia Integrata per la Gestione del Rischio Aziendale) metoodika on kvalitatiivne riski hindamise ja juhtimise metoodika, pakkudes analüüsi raamistiku, mis põhineb klassikalisel nägemusel riskist kui mitmemõõtmelisest suurusest. MIGRA on välja töötatud Itaalias. Metoodika annab vastuse kolmele küsimusele:

- mis võiks valesti minna?
- kui tõenäoline on, et midagi võib valesti minna?
- kui risk peaks realiseeruma, siis millised on võimalikud tagajärjed?

Erinevalt teistest metoodikatest sunnib ja aitab Migra analüütikut täpselt määratleda vahekorda ohu, ründe, turvameetmete ja turvakomponentide vahel. Sel moel metoodika kasutamine võimaldab selgelt mõista tagajärgi, et otsustada kuidas rakendada või mitte rakendada igat turvameedet (Migra, 2015).

**Octave (**Operationally Critical Threat, Asset, and Vulnerability EvaluationSM) metoodika kirjeldab riskipõhist strateegilise hindamise ja planeerimise tehnikat. Metoodika pakub lähenemisviisi kuidas vastutavaid isikuid suunata võtma vastutust, et tagada turvalisus organisatsioonis. Metoodikast on olemas Octave-S versioon, mis on kohandatud kasutamiseks piiratud võimaluste korral väikestes organisatsioonides (vähem kui 100 inimest) (Octave, 2015).

**RiskSafe Assessment.** Metoodika pakub "pilvepõhist“ riskide hindamise tarkvara, mis sisaldab laia valikut riskianalüüsi vahendeid, olles täielikult kooskõlas ISO 27001 ja ISO 27005

standardiga. Metoodika abil on võimalik korraldada ärimõju analüüsi, määratleda ohte ja haavatavusi ning hinnata riske. RiskSafe Assessment abil on võimalik selgitada välja vajalikud kontrollimeetmed, mis tuginevad riskide hindamisele (RiskSafe Assessment , 2015).

**NIST.** IT riskijuhtimise kontekstist on oluline ära märkida NIST 800-16, NIST 800-30 ja NIST 800-39 standardid, mis keskenduvad IT riskide juhtimisele. Standardid on koostanud USA valitsusasutus NIST ning valdavalt leiavad need laialdast kasutamist nii avalikus sektoris kui ka eraettevõtetes. Dokumentides seotakse IT riskijuhtimine organisatsiooni terviklike eesmärkidega ning kirjeldatakse riskihaldusega seotud rolle. Lisaks kirjeldatakse riskianalüüsi ''üheksat sammu'' ja riskide vähendamise strateegiat, erinevaid turvameetmeid, kontrollmeetmeid, jääkriskide käsitlust ning tasuvusanalüüsi. Käsitletud on ka riskihalduse integreerimist organisatsiooni teiste protsessidega ning selle paindliku muutmise võimalusi (NIST Special Publication 800-37. Revision 1, 2015).

**COBIT 5** (Control Objectives for Information and Related Technology) on äriprotsessile suunatud raamistik IT juhtimiseks ja haldamiseks, pakkudes põhjalikku ülevaadet IT juhtimise printsiipidest ja parimast praktikast. Raamistik baseerub analüütilistel tööriistadel ja mudelitel, mille abil on võimalik COBIT 5 juurutada. Sinna on integreeritud ka Val IT (IT Value Delivery) raamistik, Risk IT raamistik, ITIL (Information Technology Infrastructure Library) ning valdkonna ISO standardid. Raamistiku on välja töötanud ISACA ning ta on leidnud kasutust rohkem kui 160 riigis (Why use COBIT 5, 2015).

**Parimad praktikad** on eelkõige kogum IT riskijuhtimise parimatest kogemustest ja teadmistest, edukatest rakendamise näidetest, mida järgides on võimalik organisatsioonis riskijuhtimist korraldada. Tugineb sageli töötajate isiklikul kogemusel, teistelt õpitud teadmistelt ning võib hõlmata elemente erinevatest standarditest, metoodikates või töövahenditest. Sageli tekivad need omavahelise kombineerimise tulemusel. Suurimaks probleemiks on vastava dokumentatsiooni puudumine, millest tingituna võivad need aja möödudes kaduma minna.

## 3.3 Tuntumate Euroopas kasutatavate metoodikate võrdlus

Järgnev tabel annab ülevaate tuntumatest Euroopas kasutatavatest metoodikatest, nende arendaja ja päritolumaa andmetega.

| | **CRAMM** | **MEHARI** | **Ebios** | **IT Grundschutz** |
|---|---|---|---|---|
| **Päritoluriik** | Ühendkuningriigid | Prantsusmaa | Prantsusmaa | Saksamaa |
| **Arendaja** | CTTA | CLUSIF | DCSSI | BSI |
| **Koduleht** | http://www.cramm.com | http://www.clusif.asso.fr/en/clusif/present/ | http://www.ssi.gouv.fr | http://www.bsi.de/ |
| **Ajalugu (loodud/viimane versioon)** | 1985 /2003 | 1998 / 2010 | 1995 / 2005 | 1994 / 2005 |
| **Keeled** | saksa, inglise, tsehhi | prantsuse, inglise | prantsuse, inglise, saksa, hispaania | inglise, saksa, |
| **Tasu** | vajalik registreerida kasutajaks | tasuta | tasuta | tasuta |
| **Sihtrühm** | Valitsusasutused, suurkorporatsioonid | Valitsusasutused, väikesed- ja keskmised ettevõtted, mittetulundusühingud | Valitsusasutused, suurkorporatsioon-id, väikesed- ja keskmised ettevõtted, tehnoloogiaettevõtted | Valitsusasutused, suurkorporatsioon-id, väikesed- ja keskmised ettevõtted |
| **Standardid** | ISO/IEC 17799 | ISO/IEC IS 13335-1, SO/IEC 27005:2008, ISO/IEC 27001 ISMS | ISO/IEC 27001, ISO/IEC 15408, ISO/IEC 17799, ISO/IEC 13335, ISO/IEC 21827 | ISO/IEC 17799, ISO/IEC 27001 |
| **Kasutajarühm** | Juhtkond, operatiivtasand, tehniline personal | Juhtkond, operatiivtasand, tehniline personal | Juhtkond, operatiivtasand | Juhtkond, operatiivtasand, tehniline personal |

| | | | | |
|---|---|---|---|---|
| **Peamine töövahend** | CRAMM expert (tasuline) | MEHARI 2010 | Ebios tool | GSTOOL (tasuta avalikule sektorile) |

Tabel 1. Tähtsamate Euroopas kasutatavate metoodikate võrdlus

## 3.4 Riskide juhtimise ja hindamise tarkvara

Riskijuhtimiseks ja hindamiseks on arendatud mitmeid tarkvaralahendusi. Üldisemas mõttes võib neid nimetada töövahenditeks. See on tinglik nimetus, kuna ükski tarkvara ei sisalda vaid riski juhtimise ja hindamise võimalusi, vaid koosneb erinevatest funktsionaalsetest võimalustest. Sellisteks tööriistadeks on näiteks Callio, Casis, CCS Risk Manager, CloudeAssurance, Cobra, Countermeasures, Cramm, EAR / PILAR, Ebios, GSTool, GxSGSI, ISAMM, Mehari 2010 basic tool, MIGRA Tool, Modulo Risk Manager, Octave, Proteus, Ra2, REAL ISMS, Resolver Ballot, Resolver Risk, Risicare, Riskwatch, RM Studio, SISMS, TRICK light, TRICK Service, Acuity Stream, WCK (Risk Assessment Tools, 2015) ning ka Eesti päritolu ISKE rakendustööriist. Erinevaid tööriistu on oluliselt rohkem kui teadaolevaid metoodikaid. Lisaks tasuta töövahenditele on saadaval arvestatav valik tasulisi töövahendeid. Selliseid töövahendeid pakuvad alljärgnevad tootjad: EMC (RSA), IBM, MetricStream, Nasqad, Modulo, Rsam, Aqiliance, LockPath, Brinqa, Allgress ja ControllCase (Paul & Wheeler, 2015). Tööriista valikul tuleks eelkõige lähtuda rakendatavast metoodikast, kuigi mitmed tööriistad sobivad kasutamiseks ka teiste metoodikatega. Loomulikult ei saa unustada ka teisi olulisi aspekte nagu tootja tuge, versiooniuuenduste olemasolu, kasutusmugavust, maksumust, hooldus ja haldustasusid jne.

### 3.4.1 Tasuta töövahendid

**CRAMM töövahend** on riskianalüüsi tööriist, mis on välja arendatud Ühendkuningriigis. Tööriist kannab sama nime kui selle aluseks olev metoodika millele CRAMM toetub. Tegemist on Ühendkuningriigi valitsusasutuste eelistatuima riskianalüüsi vahendiga, kuid seda metoodikat ning tööriista kasutatakse ka paljudes riikides väljaspool Ühendkuningriiki. Metoodika ja tööriist on eriti sobiv suurtele organisatsioonidele, nagu valitsusasutused ja tööstusettevõtted (Inventory of Risk Management - Risk Assessment methods and tools, 2015).

**Risk Scenarios Using COBIT 5 for Risk töövahend** on võimas tööriist, mis aitab IT spetsialistil, kes hindab riske, küsida õigeid küsimusi ja valmistuda ootamatusteks. Erinevate stsenaariumite analüüs on saanud oluliseks osaks ettevõtte riskijuhtimisel. Tööriist nimega *Risk Scenarios Using COBIT 5 for Risk* annab juhiseid, kuidas välja arendada IT'ga seotud riski stsenaariume, samuti annab tööriist juhiseid, kuidas kasutada tööriista abi organisatsiooni probleemida lahendamisel. Tööriist annab ülevaate riskide kontseptsioonidest ning mõistetest koos 50 täieliku riskistsenaariumiga, mis hõlmab kõiki 20-et kirjeldatud kategooriat. Täpsed juhised on antud ka selle kohta, kuidas hallata riskijuhtimise tegevusi. Tööriist sisaldab interaktiivseid riskistsenaariumi malle iga 20-ne kategooria jaoks (Risk Scenarios Using COBIT 5 for Risk, 2015).

**Mehari 2010 töövahend** sisaldab mitmeid valemeid, mis võimaldavad esitada samm-sammult riskianalüüsi ja riskijuhtimise tulemusi ning pakkuda täiendavaid kontrolle riskide vähendamiseks. Lisaks on olemas ka teine töövahend RISICARE, mis on mõeldud kasutamiseks keerulisemates keskkondades (Mehari 2010 basic tool, 2015).

**Ebios töövahend.** Ebios tarkvara on välja töötatud Prantsusmaal, et toetada Ebios metoodika kasutamist. Tööriist aitab kasutajal viia läbi riskianalüüsi ja riskide juhtimise metoodika rakendamise igas etapis. Tarkvara võimaldab kõigi uuringute tulemused salvestada, et dokumenteerida vastav protsess. Ebios metoodika kasutamiseks mõeldud tarkvara on avatud lähtekoodiga ja mõeldud tasuta kasutamiseks (EBIOS tool, 2015).

**GSTOOL töövahend.** GSTool on välja töötatud Saksamaal BSI (Federal Office for Information Security) poolt, et toetada kasutajate *IT Grundschutz metoodika* kasutamist. Tarkvara aitab ettevalmistada, hallata ja ajakohastada IT turvalisuse kontseptsiooni, mis vastavad metoodikale. Pärast vajaliku teabe kogumist saavad kasutajad tervikliku aruandluse abil läbi viia analüüse. Kõik kogutud andmeid saab hallata elektrooniliselt või kasutada ka elektroonilisel kujul. GSTOOL-il on omaette andmebaas. Prooviversioon tarkvarast on saadaval tasuta kasutamiseks (GSTool, 2015).

**ISKE rakendustööriist.** ISKE rakendustööriist on 2009-2010. aastal Eestis välja töötatud ISKE rakendamist abistav ja toetav vahend (arendaja Smartlink OÜ), mis võimaldab organisatsioonis kasutusel olevaid infovarasid kaardistada, määrata turvaklasse ja turbeastmeid, siduda infovarasid tüüpmoodulitega, grupeerida ja tsoneerida infovarasid ja koostada ja hallata

rakendusplaani, mis aitab asutuses ISKE rakendamist protsessis hoida. Tööriist võimaldab kasutada ka Postgre SQL andmebaasi. Viimane valminud ISKE rakendustööriista tarkvara versioon on 2.0.9, kuid probleemiks on asjaolu, et hetkel toetab töövahend ISKE kataloogi versiooni 6, kuid avaldatud on ka juba versioon 7, mistõttu on hetkel selle kasutamine piiratud (RIA, 2015).

### 3.4.2 Tasulised töövahendid

IT riskijuhtimise turg on kasvav ning valdkonnas on välja arendatud mitmeid erinevad töövahendeid, mis võimaldavad automatiseerida erinevaid tööprotsesse toetamaks IT riskijuhtimise korraldamist. Tavaliselt sisaldavad selliseid tooted funktsioone nagu varade kaardistamine, tööülesannete planeerimine ja juhtimine, erinevate andmete impordi funktsionaalsust jne (Paul & Wheeler, 2015).

Gartner on 2014. aastal koostanud ülevaate erinevatest valdkonnas tegutsevatest tarkvara arendajatest (vt. Joonis 3) ning paigutanud tootjad nelja erinevasse rühma.


Joonis 3. Gartner ülevaade 2014 *(Paul & Wheeler, 2015)*

Järgnevalt annab autor lühikese ülevaate kolme juhtivama tootja pakutavatest lahendustest, mida Gartner on hinnanud kui paremaid võimalike valikuid.

**EMC (RSA).** Pakutakse *Archer GRC* tarkvara, mida saab kasutada kas asutusesiseses keskkonnas või pilvekeskkonnas. Peakontor paikneb USA-s, lisaks tugikeskused Ühendkuningriikides, Indias ja Austraalias. Tarkavara on eskaleeruv, dünaamiline ja mõeldud keerukatele organisatsioonidele. Peamised tugevused on eelkõige suurim kasutajate arv ning pikaealine arendus. Klienditeenidus ja tugi on kõrge kvaliteediga. Miinuseks keeruline hinnastamismudel (Paul & Wheeler, 2015).

**IBM**. *OpenPages GRC* tarkvaras on väga hea IT riskijuhtimise võimekus, mida tavaliselt rakendatakse koos operatsiooniriski juhtimisega. Peamiselt kasutatakse seda riskijuhtimises ja siseauditi töös. Võimalik kasutada nii asutusesisest lahendust kui ka *SaaS* mudelit. Peamiseks eeliseks on tehnilise toe olemasolu USA-s, Kanadas ning veel kuues riigis. Toetab 13 erinevat keelt. Suurima puudusena on esile toodud toote kõrget maksumust (Paul & Wheeler, 2015).

**MetricSteam**. Müüja on peamiselt keskendunud suurklientidele, kuid tahab tungida väikese ja keskmise suurusega klientide turule, kasutades oma platvormi ja *Zaplet* arhitektuuri. Tugevuseks on asjaolu, et pakutakse ka individuaalseid lahendusi ja püütakse rahuldada ainulaadseid ärivajadusi. Palju on panustatud tootearendusse. Müüja omab suuri kogemusi finantssektoris, jaekaubanduses, energeetika ja tootmise valdkonnas. Hinnastamisel eelistatakse pigem teenustasul põhinevat ärimudelit. Miinusena võib esile tuua asjaolu, et toode sisaldab palju individuaalsed erilahendusi (Paul & Wheeler, 2015).

# 4. STANDARDITE JA MEETODIKATE HINDAMINE

Olles läbi töötanud erialase kirjanduse ja tutvudes mitmete IT-riskijuhtimist käsitlevate rahvusvaheliste organisatsioonide internetiallikatega selgus, et IT riskijuhtimise korraldamiseks on võimalik rakendada väga erinevaid standardeid, metoodikaid ning töövahendeid. Peamine probleem seisneb autori hinnangul selles, millele tuginedes ning kuidas teha valik erinevate võimaluste vahel. Milliseid hindamiskriteeriume kasutada ning millist metoodikat kasutades viia läbi vastav praktiline hindamine.

## 4.1 Standardite ja metoodika hindamiskriteeriumid

IT riskijuhtimise standardite ja metoodikate hindamise probleemi on uurinud USA autorid Daniel Minoli ja Jake Kouns, kes väidavad, et kuigi IT-riskijuhtimise standardite ja metoodikate hindamiskriteeriumite valikuvõimalused on väga suured, võiks siiski tugineda valiku tegemisel järgnevatele kriteeriumitele (Minoli & Kouns, 2010):

- **Standardid.** Kui organisatsioon soovib järgida standardeid ning soovib saada ka vastavalt sertifitseeritud, siis tuleks loomulikult valida metoodika, mis seda võimaldab. Eelkõige tuleks järgida ISO 27000 ja ISO 31000 seeria standardeid.
- **Kvantitatiivne vs kvalitatiivne lähenemine.** Endiselt on pooleli valdkonna ekspertide debatt, kumba lähenemist pooldada. Probleemi kese on sellel, kuidas saada tegelikud usaldusväärsed numbrilised väärtused. Suure tõenäosusega ei ole siiski võimalik kasutada ainult kvantitatiivset lähenemist, kuna puudub vajalik usaldusväärne andmestik (tõenäosuse ja mõju kohta), kuigi mõnes piiratud situatsioonis on see kindlasti võimalik. Üheks võimaluseks on kasutada lihtsat ja kiiret kvalitatiivset riski hindamist, millele järgneb riskide analüüs, milleks kasutatakse detailseimaid kvantitatiivseid või kvalitatiivseid metoodikaid.
- **Hind ja väärtus.** Iga organisatsioon peab hindama võimaliku kasu, mida annab metoodika ja töövahendite kasutamine ning võrdlema seda tehtavate kulutustega.

- **Haldus ja tugi.** Mõned töövahendid pakuvad head tuge metoodika juurutamiseks samas kui teised abi ja tuge ei võimalda. Mida üldisem on töövahend, seda lihtsam on teda ka üldjuhul muuta ja kohendada oma vajadusele vastavaks. Enamus töövahendeid on algsel kujul kättesaadavad tasuta.
- **Kasutusmugavus.** Mõned metoodikad võimaldavad kasutada töövahendeid selliselt, et nende abil on võimalik läbida protsess samm-sammult, samas kui teised vahendid jätavad vabad käed, eeldades, et kasutaja omab ise vajalikke eelteadmisi ning kogemust.
- **Laiendatavus.** Organisatsioon peaks valiku tegemisel mõtlema ka sellele, kas lahendatakse IT riskiga seotud probleeme kitsalt IT süsteemi või rakenduse lõikes või viiakse läbi kogu organisatsiooni läbiv analüüs. Arvestama peaks ka sellega kui regulaarselt seda tehakse.

Ühendkuningriikide valitsusasutus CESG (Information Security arm of GCHQ, and the National Technical Authority for Information Assurance within the UK), kes annab organisatsioonidele nõu, kuidas kaitsta oma andmeid ja infosüsteemide erinevate ohtude vastu, avaldas oma kodulehel 2015. aastal soovitused, mida võiks käsitleda ka hindamiskriteeriumitena. Nendeks soovitusteks on (CESG, 2015):

- **Maksumus;**
- **projekti skoop ehk ulatus;**
- **erinevate ressursside kasutamine.** Kas on võimalik tagada vajalikud vahendid selleks, et planeeritava lahenduse jaoks nõutavate ressursside kasutamine oleks proportsionaalne ja säästlik?
- **piirangud.** Kas eksisteerib mistahes ärilisi aspekte, mis võivad piirata metoodika või töövahendi kasutamist?

Lisaks soovitatakse vajadusel kombineerida mitmeid erinevaid metoodikaid, kohaldada või töötada välja oma organisatsiooni jaoks unikaalselt sobiv lahendus soovitud lõppeesmärgi saavutamiseks (CESG, 2015).

Hindamiskriteeriumite ettevalmistamisel ning väljavalimisel otsustas autor osaliselt kriteeriume ümber sõnastada, et selle sisu oleks paremini arusaadav. Arvestades varasemalt kirjeldatud soovitusi otsustas autor lisada hindamiskriteeriumite juurde ka kolm omapoolset täiendust:

- **Juurutamise või rakendamise keerukus.** Organisatsioonide olemusest ning suurusest tulenevalt on organisatsioonidel erinevad ressursid ja võimekus.
- **Eesti keelne tugi.** Kas standardit, metoodikat ja tööriista saab kasutada eesti keeles?
- **Tuleviku perspektiiv.** Kas standardid, metoodikad ja töövahendid leiavad aktiivset kasutamist ning kas nende edasiarendamist korraldab mõni organisatsioon või vabatahtlike aktivistide grupp**.**

## 4.2 Hindamise metoodikad

### 4.2.1 ENISA IT riskijuhtimise hindamise metoodika

ENISA poolt IT riskijuhtimise metoodikate kasutamise hindamise ja võrdlemise metoodika väljatöötamiseks moodustatud töörühm pakkus välja omapoolse lahenduse kuidas otseselt omavahel võrrelda erinevaid standardeid ja metoodikaid, mis võimaldavad organisatsioonidel viia läbi IT riskide juhtimist. Välja töötatud metoodika käsitleb nii IT riskide hindamist kui ka juhtimist terviklikult koos nendest tulenevate sisendite ja väljunditega ning võrdleb neid töörühma poolt väljaarendatud võrdlusalustega.

Metoodika eesmärk on saavutada üks või mitu järgnevalt kirjeldatud eesmärkidest:

• Teha kindlaks milline on kõige sobivam IT riski hindamise ja juhtimise meetod, kasutades etteantud sisendeid. Nendeks sisendiseks on näiteks organisatsiooni tegutsemisvaldkond, tema suurus, seadusest tulenevad nõuded ja organisatsioonijuhtimisele esitatud nõuded. Lisaks eelnevale aitab metoodika täpsemalt kindlaks teha milline võiks olla lähenemine IT riskijuhtimisele ja millised peaksid olema võimalikud ressursid seatud eesmärgi saavutamiseks.

• Võimaldab teha otsest võrdlust kahe või enama IT riskianalüüsi või juhtimise metoodika osas selleks, et anda asjatundlikku nõu nende sobivuse kohta konkreetsetes oludes (ENISA, 2015).

Autori arvates eeldab metoodika kasutamine seda, et omatakse väga põhjalikku ja detailset ülevaadet hinnatavate standardite, metoodikate ja töövahendite kohta. Vastavat järeldust kinnitab kaudselt ka asjaolu, et ENISA töörühm, kuhu kuulusid valdkonna tunnustatud eksperdid, suutsid mitme aastase töö tulemusel kasutades iseenda poolt välja töötatud metoodikat hinnata ainult kolme võimalikku valikut. Seega on metoodika rakendamisel autori

seisukohast hinnates kaks suurt puudust. Metoodika kasutamine eeldab väga sügavuti minemist iga üksiku standardi, metoodika ja töövahendi lõikes, milleks aga puuduvad autoril nii vajalikud teadmised kui ka ajaline ressurss. Siiski saab ENISA töörühma poolt välja arendatud metoodika alusel tehtud üldist ülevaadet kasutada selleks, et nende võrdlemiskriteeriumite ja p 4.1 kirjeldatud teoreetiliste lähtekohtade alusel töötada välja vajalik sisend analüütilise hierarhiate meetodi AHM rakendamiseks, mida autor kasutab magistritöös hindamise läbiviimisel.

### 4.2.2 Analüütiliste hierarhiate meetod AHM

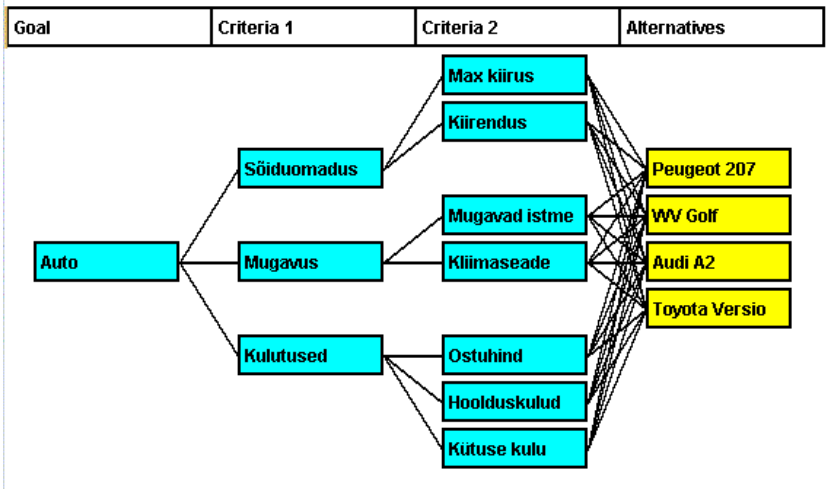
Analüütiliste hierarhiate meetod AHM, mida selle autori Thomas L. Saaty järgi tuntakse ka kui *Saaty* meetodit, on eeskätt mõeldud subjektiivsete hinnangute alusel tegutsevate süsteemide korrastamiseks. *Saaty* meetod võimaldab keerukat otsustusprobleemi modelleerida hierarhilise struktuuri kaudu, mille moodustavad *eesmärk, kriteeriumid, alamkriteeriumid, ja alternatiivid*. Selle eelis seisneb võimaluses käsitleda nii kvalitatiivseid, kui ka kvantitatiivseid objekte. Meetodi väljundiks on matemaatiliselt korrektne, kvantitatiivne hinnang analüüsitavatele alternatiividele. *Saaty* meetodi peamine idee seisneb selles, et otsustajad vabastatakse vajadusest vaadeldavatele objektidele absoluutsete hinnangute (kaalude skaala) andmisest. Selle asemel piirdutakse objektide võrdlemisega paarikaupa, mis on inimlikke hindamisvõimeid arvestades vastuvõetavam. Olgu meil näiteks kolm erineva kaaluga füüsilist eset A, B ja C. Neid paarikaupa käes hoides saame kergesti hinnata, et A on ”veidi raskem” kui B; C on ”tunduvalt raskem” kui A ning et C on ”mitu korda” raskem B-st. Samas, käsitledes esemeid ühekaupa (eriti kui neid on rohkem kui kolm), tekib meil arvatavasti raskusi kõikide kaalude hindamisel ehk korrektse kaalude absoluutskaala moodustamisel (Netekspert.com, 2015).

*Saaty* meetod põhineb eelkõige objektide paarikaupa võrdlemisel. Meetodi kasutamise võib jagada järgmisteks etappideks (Võhandu, 1998):

- probleemi defineerimine;
- eesmärgi defineerimine;
- modelleerimine ehk süsteemi analüüs (tükeldamine ehk dekomponeerimine) ja süntees (hierarhia koostamine);

- mõjurite (kriteeriumite) leidmine ja valikute (alternatiivide) leidmine;
- valikute paarikaupa võrdlemine iga mõjuri suhtes;
- mõjurite paarikaupa võrdlemine;
- valikute osakaalude leidmine;
- tulemuste analüüs, sealhulgas kindlasti ka hinnangute kooskõla ja tulemuste tundlikuse analüüs;
- vajaduse korral eelnevate sammude täpsustamine ehk järgmine iteratsioon;
- kui mõjurid ja valikud on leitud, siis korrastatakse need mitmetasemelisse hierarhilisse struktuuri. Kõigepealt tuleb eesmärk, siis mõjurid, teatud mõjuritel võivad olla alammõjurid ja viimasel tasemel on valikud.

Joonis 4 kirjeldab kõige lihtsamat 3-tasemelise hierarhiaga *Saaty* mudelit. Esimeses kihis on eesmärk (*Goal*), milleks antud näites on sobivaima auto valik. Teises kihis on mõjurid (*Criteria 1*), mis otsustust mõjutavad: sõiduomadused, mugavus, kulutused. Järgnev kiht (*Criteria 2*) on omakorda jaotatud kolme rühma. Sõiduomaduste osas on selleks maksimaalne kiirus ja kiirendus. Mugavus jaguneb mugavateks istmeteks ja kliimaseadmeks ning kulutused omakorda ostuhinnaks, hoolduskuludeks ning kütuse kuluks. Viimases kihis on valikud (*Alternatives*). Jooned elementide vahel on kaalud, mis arvutatakse paarikaupa võrdluste alusel. Paarikaupa võrdluse tulemus esitatakse nn. *Saaty* skaalal.




Joonis 4. *Saaty* mudeli näidiskirjeldus

Kokkuvõtteks võib öelda, et analüütiliste hierarhiate meetod AHM ehk *Saaty* meetod on väga universaalne. Metoodika on aastakümnete jooksul leidnud laialdast kasutamist väga erinevatel tegevusaladel, näiteks personali hindamisel, investeeringute tasuvuse hindamisel, tarkvara arendamisel, logistika valdkonnas, looduskaitses jne. Näiteks soovitab RIA kasutada *Saaty* metoodikat IT-projektide tasuvusanalüüsi teostamisel (RIA koduleht, 2015). Arvestades magistritöö eesmärki arvab autor, et *Saaty* metoodika kasutamisega on võimalik jõuda vajaliku tulemuseni.

# 5. STANDARDITE JA METOODIKATE VÕRDLEMINE

Läbi töötanud erialase kirjanduse ja erinevad interneti allikad, otsustas autor kasutada oma magistritöös erinevate IT riskijuhtimise standardite, metoodikate ja töövahendite hindamisel *Saaty* analüütilise hierarhia meetodit (vt. p 4.2.2), kasutades selleks Soome Aalto Ülikooli veebipõhist tasuta WEB-HIPRE tarkvara (Web-HIPRE, 2015).

Kuna üheaegselt on väga keeruline võrrelda erinevaid standardeid ja nendele tuginevaid metoodikaid ja töövahendeid, otsustas autor *Saaty* mudeli erinevad kihid üles ehitada selliselt, et lähtutakse eelkõige eesmärgist leida võimalikult sobivaim IT riskijuhtimise standard või metoodika, mis sobiks Eesti avaliku sektori asutusele. Nendele omakorda tuginevad erinevad tööriistad, kuigi ka tarkvara omakorda võib katta ainult osaliselt mõne standardi või metoodika poolt nõutud või pakutud tingimused.

## 5.1 Võrdlemiskriteeriumid

Võrdlemisel on omadused jaotatud kaheks suuremaks kategooriaks: funktsionaalsed ja mittefunktsionaalsed omadused. Funktsionaalsete omaduste valimisel on aluseks võetud ISO 31000 standardi funktsionaalsed omadused. Kriteeriumite visuaalse mudeliga saab tutvuda käesoleva töö lõpus ( LISA 2).

Järgnevalt on kirjeldatud tabelandmete kujul kriteeriume koos kirjelduste, osakaalude ja põhjendustega, mis on sellised osakaalud tinginud.

Esimese taseme omadused jagunevad kaheks kategooriaks:

| **Peakriteeriumi omadus** | **Kirjeldus** |
|---|---|
| Funktsionaalne | Omadused, mis võimaldavad täita põhifunktsioone (näiteks konteksti loomine, riski kaalutlemine, riskikäsitlus jt.). |

| | |
|---|---|
| Mittefunktsionaalne | Omadused, mis ei ole seotud funktsionaalsusega (näiteks maksumus, kasutajatugi, keelte valik, jt). |

Tabel 2. Esimese taseme kriteeriumid

Teise funktsionaalse taseme omadused jagunevad viieks kategooriaks:

| **Funktsionaalne omadus** | **Kirjeldus** |
|---|---|
| Konteksti loomine | Riskiallikate ja tema põhjuste nimekiri. |
| Riski kaalutlemine | Millised võimalused on riski kaalutlemise rakendamiseks. |
| Riskikäsitlus | Millised võimalused on riskikäsitlusstrateegia rakendamiseks. |
| Riskiteavitus ja konsulteerimine | Kui tõhus on teavitamine ning seotud tegevused teiste riskijuhtimise osadega. |
| Riski seire ja läbivaatus | Millised võimalused on regulaarselt seirata ja läbi vaadata riske. |

Tabel 3. Teise taseme kriteeriumid - funktsionaalsed omadused

Kolmanda taseme riski kaalutlemise omadused jagunevad kolmeks kategooriaks:

| **Riski kaalutlemise omadus** | **Kirjeldus** |
|---|---|
| Riskituvastus | Riskide hindamine on tervik, hõlmab riskituvastust, riskianalüüsi ja riskide kaalumust. Millised on võimalused nende funktsioonide rakendamiseks. |
| Riskianalüüs | |
| Riski hindamine | |

Tabel 4. Kolmanda taseme kriteeriumid - riski kaalutlemise omadused

Teise mittefunktsionaalse taseme omadused jagunevad seitsmeks kategooriaks:

| **Mittefunktsionaalne omadus** | **Kirjeldus** |
|---|---|
| Maksumus | Lahenduse hind ja kulud. |
| Versiooniuuendused | Kas standardeid uuendatakse. |
| Tööriista olemasolu | Võimalus automatiseerida tööd. |
| Keelte valik | Laiem keelte tugi sh. eesti keele olemasolu. |
| Juurutamise keerukus | Kuivõrd keeruline on standardi või metoodika juurutamine. |
| Piirkond | Kasutuse leviala. |
| Organisatsiooni suurus | Mida väiksem organisatsioon, seda keerulisem on standardi või metoodika kasutamine. |

Tabel 5. Teise taseme kriteeriumid - funktsionaalsed omadused

Kolmanda taseme maksumuse kaalutlemise omadused jagunevad kaheks kategooriaks:

| **Maksumuse kaalutlemise omadus** | **Kirjeldus** |
|---|---|
| Tasuline | Avaliku sektori asutuste jaoks on maksumus oluline. |
| Tasuta | |

Tabel 6. Kolmanda taseme kriteeriumid - maksumuse kaalutlemise omadused

Kolmanda taseme versiooniuuenduse omadused jagunevad kaheks kategooriaks:

| **Versiooniuuenduse omadus** | **Kirjeldus** |
|---|---|
| Uuendatakse regulaarselt | Uuenduste olemasolu ja regulaarsus. |
| Ei uuendata regulaarselt | |

Tabel 7. Kolmanda taseme kriteeriumid - versiooniuuenduse omadused

Kolmanda taseme tööriista kaalutlemise omadused jagunevad kolmeks kategooriaks:

| **Tööriista omadus** | **Kirjeldus** |
|---|---|
| Tasuline | Kas on võimalik kasutada tasuta tarkvara või peab kasutama tasulist lahendust. |
| Tasuta | |
| Liidestatavus | Millised on andmete andmevahetuse võimalused teiste süsteemidega. |

Tabel 8. Kolmanda taseme kriteeriumid - tööriista kaalutlemise omadused

Kolmanda taseme keele valiku kaalutlemise omadused jagunevad kolmeks kategooriaks:

| **Keelte valiku omadus** | **Kirjeldus** |
|---|---|
| Eesti keel | Kas on olemas hädavajalik keelte tugi sh. eesti keele tugi. |
| Inglise keel | |
| Saksa keel | |

Tabel 9. Kolmanda taseme kriteeriumid - keele valiku kaalutlemise omadused

Kolmanda taseme keele valiku kaalutlemise omadused jagunevad kolmeks kategooriaks:

| **Juurutamise keerukuse valiku omadus** | **Kirjeldus** |
|---|---|
| Lihtne | Kui keeruline on standardi või metoodika juurutamine. |
| Keskmine | |
| Keerukas | |

Tabel 10. Kolmanda taseme kriteeriumid - juurutamise keerukuse kaalutlemise omadused

Kolmanda taseme hinna kaalutlemise omadused jagunevad kolmeks kategooriaks:

| **Piirkonna valiku omadus** | **Kirjeldus** |
|---|---|
| Eesti | Millistes piirkondades standardeid ja metoodikaid kasutatakse. |
| Euroopa Liit | |
| Ameerika Ühendriigid | |

Tabel 11. Kolmanda taseme kriteeriumid - piirkonna valiku kaalutlemise omadused

Kolmanda taseme hinna organisatsiooni suuruse omadused jagunevad kolmeks kategooriaks:

| **Organisatsiooni suuruse valiku omadus** | **Kirjeldus** |
|---|---|
| Väike | Mida väiksem organisatsioon, seda keerukam võib olla juurutamine ja rakendamine. |
| Keskmine | |
| Suur | |

Tabel 12. Kolmanda taseme kriteeriumid - organisatsiooni suuruse valiku kaalutlemise omadused

## 5.2 Võrdlemise kriteeriumite osakaalud

Võrdlemiskriteeriumide koostamisel ja osakaalude määramisel võttis autor omale eesmärgiks koostada need selliselt, et neid kasutades võiks Eesti avaliku sektori asutus välja selgitada, milline standard või metoodika võiks sobida kõige paremini. Autor soovis teha võimalikult universaalse kriteeriumite valiku ning osakaalude määratlemise. Siiski võib vajaduse selgudes iga asutus muuta osakaale vastavalt oma organisatsiooni vajadustele.

Järgnevalt annab autor ülevaate enda poolt koostatud kriteeriumitest, osakaaludest koos põhjendustega, miks on just selline osakaal määratud.

Esimese taseme peakriteeriumite osakaalude ülevaade:

| **Peakriteeriumite omadus** | **Osakaal** | **Märkused** |
|---|---|---|
| Funktsionaalsed | 0,60 | Funktsionaalsete nõuete täitmine on olulisem, seetõttu on ka tema osakaal suurem. |
| Mittefunktsionaalsed | 0,40 | |

Tabel 13. Peakriteeriumite osakaalud

Teise taseme funktsionaalsete osakaalude ülevaade:

| **Funktsionaalne omadus** | **Osakaal** | **Märkused** |
|---|---|---|
| Konteksti loomine | 0,15 | Kõige rohkem tuleb tähelepanu pöörata riski kaalutlemisele, seetõttu on tema osakaal kõige suurem. |
| Riski kaalutlemine | 0,40 | |
| Riskikäsitlus | 0,15 | |
| Riskiteavitus ja konsulteerimine | 0,15 | |
| Riski seire ja läbivaatus | 0,15 | |

Tabel 14. Teise taseme osakaalud - funktsionaalsed osakaalud

Kolmanda taseme riskide kaalutlemise osakaalude ülevaade:

| **Riski kaalutlemise omadus** | **Osakaal** | **Märkused** |
|---|---|---|
| Riskituvastus | 0,30 | Mõnevõrra on suurendatud riskianalüüsi osakaalu. |
| Riskianalüüs | 0,40 | |
| Riski hindamine | 0,30 | |

Tabel 15. Kolmanda taseme osakaalud - riski kaalutlemise osakaalud

Teise taseme mittefunktsionaalsete osakaalude ülevaade:

| **Mittefunktsionaalne omadus** | **Osakaal** | **Märkused** |
|---|---|---|
| Maksumus | 0,20 | Kõik nõuded on olulised, kuid mõnevõrra olulisem on maksumus ja juurutamise keerukus. |
| Versiooniuuendused | 0,15 | |
| Tööriista olemasolu | 0,15 | |
| Keelte valik | 0,10 | |
| Juurutamise keerukus | 0,20 | |
| Piirkond | 0,10 | |
| Organisatsiooni suurus | 0,15 | |

Tabel 16. Teise taseme osakaalud - mittefunktsionaalsed osakaalud

Kolmanda taseme maksumuse kaalutlemise osakaalude ülevaade:

| **Maksumuse kaalutlemise omadus** | **Osakaal** | **Märkused** |
|---|---|---|
| Tasuline | 0,30 | |

| | | |
|---|---|---|
| Tasuta | 0,70 | Avaliku sektori asutuse selge eelistus on tasuta lahendusel. |

Tabel 17. Kolmanda taseme osakaalud - maksumuse kaalutlemise osakaalud

Kolmanda taseme versiooniuuenduse osakaalude ülevaade:

| **Versiooniuuenduse omadus** | **Osakaal** | **Märkused** |
|---|---|---|
| Uuendatakse regulaarselt | 0,80 | Uuendamine on väga oluline. |
| Ei uuendata regulaarselt | 0,20 | |

Tabel 18. Kolmanda taseme osakaalud - versiooniuuenduse osakaalud

Kolmanda taseme tööriista kaalutlemise osakaalude ülevaade:

| **Tööriista omadus** | **Osakaal** | **Märkused** |
|---|---|---|
| Tasuline | 0,20 | Igapäevase tasuta töövahendi olemasolu on oluline. Lisaks tuleb tagada ka liidestatavus teiste süsteemidega. |
| Tasuta | 0,60 | |
| Liidestatavus | 0,20 | |

Tabel 19. Kolmanda taseme osakaalud - tööriista kaalutlemise osakaalud

Kolmanda taseme keele valiku kaalutlemise osakaalude ülevaade:

| **Keelte valiku omadus** | **Osakaal** | **Märkused** |
|---|---|---|
| Eesti keel | 0,40 | Eesti ja inglise keel on eelistatud kuna üks on riigikeel ning inglise keel on kõige olulisem IT valdkonna suhtluskeel. |
| Inglise keel | 0,40 | |
| Saksa keel | 0,20 | |

Tabel 20. Kolmanda taseme osakaalud keele valiku kaalutlemise osakaalud

Kolmanda taseme keele valiku kaalutlemise osakaalude ülevaade:

| **Juurutamise keerukuse valiku omadus** | **Osakaal** | **Märkused** |
|---|---|---|
| Lihtne | 0,40 | Lihtsam juurutusviis on eelistatud. |
| Keskmine | 0,35 | |
| Keerukas | 0,25 | |

Tabel 21. Kolmanda taseme osakaalud - juurutamise valiku osakaalud

Kolmanda taseme hinna kaalutlemise osakaalude ülevaade:

| **Piirkonna valiku omadus** | **Osakaal** | **Märkused** |
|---|---|---|
| Eesti | 0,50 | Rakendamiskogemused Eestis on eelistaud ja seetõttu suurema osakaaluga. |
| Euroopa Liit | 0,30 | |
| Ameerika Ühendriigid | 0,20 | |

Tabel 22. Kolmanda taseme osakaalud - piirkonna valiku osakaalud

Kolmanda taseme organisatsiooni suuruse osakaalude ülevaade:

| **Organisatsiooni omadus** | **Osakaal** | **Märkused** |
|---|---|---|
| Väike | 0,50 | Arvestades Eesti organisatsioonide suurust, tuleb eelistada väikestele organisatsioonidele sobivaid lahendusi. |
| Keskmine | 0,30 | |
| Suur | 0,20 | |

Tabel 23. Kolmanda taseme osakaalud - organisatsiooni suuruse osakaalud

## 5.3 Metoodikate ja standardite valik

Metoodikate ja standardite valimisel arvestas autor erinevate asjaoludega. Näiteks peavad paljud Eesti avaliku sektori asutused täitma Hädaolukorra seadust ning Toimepidevuse riskianalüüsi koostamise juhendi nõudeid. ISKE rakendamine on aga eelduseks infosüsteemide andmevahetuskihi (edaspidi X-tee) kasutamiseks, mistõttu on selle rakendamine kohustuslik, kuna ilma andmete vahetamiseta ei ole võimalik oma igapäevast tööd korraldada. Seetõttu ei olnud neid võimalik valikust välja jätta. Lisaks sellel lisas autor valikusse ka segametoodika ning mitteformaalse lähenemise, kuna nende kasutamine on laialt levinud. Täiendavalt koondati üheks valikuvõimaluseks ka Euroopas tuntud metoodikad, ISO 27000 ja ISO 31000 seeria standardid ning USA NIST SP800 seeria standardi kui kõige olulisemad vastavad juhised selles valdkonnas.

| **Metoodika või standardi nimi** | **Selgitused** |
|---|---|
| Toimepidevuse riskianalüüsi koostamise juhend | Siseministri määrus nr 16, vastu võetud 08.06.2010 „Toimepidevuse riskianalüüsi koostamise juhend“ |
| ISKE | Infosüsteemide Kolmeastmelise Etalonturbe Süsteemi (ISKE) saksa analoog IT Grundschutz. |
| Segametoodika | Samaaegne erinevate metoodikate kasutamine kas osaliselt või täielikult. |
| Mitteformaalne lähenemine | Parimad praktikad ning kogemused. |
| EU metoodikad | CRAMM, Ebios, Mehari 2010, Octave, COBIT 5. |
| ISO 27000 seeria | ISO 27000 – 27005, ISO 27032 standardid. |
| ISO 31000 seeria | ISO 31000, ISO 31010. |
| NIST SP800 seeria | NIST SP800-16, NIST SP800-30, NIST SP800-39. |

Tabel 24. Kolmanda taseme osakaalud - piirkonna valiku osakaalud

## 5.4 Võrdlemise tulemused

Erinevate IT riskijuhtimise standardite ja metoodikate võrdluse tulemusel selgus, et kõige eelistatum oleks Eesti avaliku sektori asutuses kasutada ISKE-t, millele järgneb mitteformaalne lähenemine ja kolmandal kohal segametoodika (vt. Tabel 25).

Standardite, metoodikate hindamise tulemused:

| **Metoodika või standardi nimi** | **Tulemused** |
|---|---|
| ISKE | 0,302 |
| Mitteformaalne lähenemine | 0,160 |
| Segametoodika | 0,149 |
| Toimepidevuse riskianalüüsi koostamise juhend | 0,110 |
| EU metoodikad | 0,099 |
| ISO 27000 seeria | 0,095 |
| NIST SP800 seeria | 0,051 |
| ISO 31000 seeria | 0,050 |

Tabel 25. Standardite, metoodikate hindamise tulemused

Saadud võrdlemise tulemuste analüüsimisel tuleb siiski arvestada asjaoluga, et piisavalt universaalset kriteeriumite ja osakaalude määratlemist ei ole võimalik teha, kuna esineb piisavalt palju erinevaid asjaolusid (organisatsiooni suurus, eelarvelised võimalused, tegevusala jne.), mida autori poolt pakutu ei suuda arvestada. Isegi kui hindamise tulemusel soovitatakse kasutada mõnda standardit või metoodikat, tuleb selle sobivus täiendavat üle analüüsida. Näiteks ei sobi autori arvates suurtele organisatsioonidele mitteformaalne lähenemine, kuna sellisel juhul ei oleks võimalik tulemuslikult IT riskijuhtimist organisatsoonis korraldada. Mitteformaalne lähenemine on tavaliselt kogum erinevatest praktikatest, mis ei ole sageli piisavalt süstematiseeritud, dokumenteeritud ning ei kata kogu valdkonna nõudeid. Formaalsem ning standardiseeritud lähenemine sobib suurtele organisatsioonidele oluliselt paremini.

Seejuures võib ka Eestis kohustuslik ISKE rakendamine olla liiga suur väljakutse väikestele Eesti avaliku sektori asutustele ning lahendus võib peituda mitteformaalse lähenemise ja segametoodika baasil loodud parima praktika kogus, mille koostamisel võiks tulevikus abiks olla ka RIA.

Loodud hierarhilisel mudelil on mõningad puudused, mida on keeruline muuta ainult osakaalude abil. Lisaks on vaja kasutada ka inimese analüütilist mõtlemisvõimet. Koostatud mudel on avatud võimalikule laiendamisele ning vajadusel saab seda täiendada.

Vaatamata mõningatele puudustele võib järeldada, et väljatöötatud standardite ja metoodikate võrdlemise kriteeriumid ja nende põhjal saadud tulemused on mõistlikud. Loodud mudelit võib kasutada ja vajadusel täiendada ka teiste standardite ja metoodikate võrdlemisel.

# 6. PRAKTILINE UURING

Magistritöö praktilise uuringu eesmärk oli välja selgitada, milliseid IT riskijuhtimise standardeid, metoodikaid ja parimaid praktikaid kasutavad igapäevaselt Eesti avaliku sektori asutused ja elutähtsa teenuse osutajad. Uuring ei hõlmanud töövahendite ehk tarkvara kasutamist, kuna nende valik on väga suur ning autori arvates oleks eelnevalt oluline kaardistada standardite ja metoodikate kasutust, mis oleks võimaldanud hiljem piirata tarkvara nimekirja, mille kasutamist lähemalt uurida.

## 6.1 Küsitluse ülesehitus ja sihtrühm

Küsimustiku valimisse võeti kõik riigi infosüsteemi haldussüsteemi andmebaasis (RIHA) registreeritud asutused (RIHA, 2015) ning lisaks täiendati valimit ka Hädaolukorra seaduses kirjeldatud elutähtsa teenuse osutajatega, kes ei olnud ennast registreerinud RIHA-s. Kokku oli valmisse lisatud 373 organisatsiooni. Seega olid valmisse kaasatud Majandus- ja Kommunikatsiooniministeeriumi korraldatavast valdkonnast elektri, gaasi ja vedelkütustega varustajad aga ka erinevad sideoperaatorid, ringhääling, Tallinna Sadam ja raudteeveo ettevõtted jne. Sotsiaalministeeriumi valdkonnast olid kaasatud haiglad, kiirabi, suuremad vee ettevõtted, Keskkonnaministeeriumi valitsemisalast õhuseire, kiirgusohu, hüdroloogilise ja meteoroloogilise seire eest vastutavad organisatsioonid. Loomulikult olid esindatud ka Siseministeeriumi valdkonna organisatsioonid, kes tagavad avaliku korra kaitse, päästetöö, operatiivraadiosidet jne. Lisaks saadeti küsitlus ka Eesti Pangale ja kommertspankadele ning kohalikele omavalitsustele, kellele on seatud ka rida erinevad ülesandeid hädaolukorras tegutsemiseks. Mõlemad valimi allikad kattusid suures osas üksteisega, kuid samaaegselt võimaldas ka valimit täiendada.

*Saaty* analüütilise hierarhia meetodi abil tehtud hindamise tulemusel (vt. Tabel 25) selgus, et eelistatumad metoodikad on mitteformaalne lähenemine ja segametoodika. Samas arvab autor, et maailmas sh. Euroopas on laiemalt kasutamist ja tunnustamist leidnud ka teised standardid ja metoodikad, mille kasutamist peab Eesti kontekstis põhjalikumalt uurima, kuna lisaks RIHA

andmebaasile hõlmas küsitlus ka ettevõtted, kellele kohaldub Hädaolukorra seadus. Need ettevõtted on aga üldjuhul suured organisatsioonid ning lisaks on paljud neist seotud ka oma kontserniga Euroopas, kes tõenäoliselt pigem kasutavad IT riskijuhtimise valdkonnas tuntud ja tunnustatud standardeid ja metoodikaid (ISO, NIST, COBIT jne). Samuti oli juba enne küsimustiku väljasaatmist selge, et väike kohalik omavalitus ei kasuta tõenäoliselt suuri ja keerukaid IT riskijuhtimise lahendusi, kuna need oleksid talle rahaliselt liiga koormavad. Andmete kogumiseks kasutas autor struktureeritud elektroonilist ankeetküsitlust Google Docs küsitluskeskkonnas. Ankeetküsitlus saadeti valimile e-kirja teel ning vastamiseks oli aega 2 nädalat. Küsitlus viidi läbi aprillis 2015. aastal. E-kirjas tutvustati korraldatava uuringu eesmärki, lisaks olid märgitud vastamiseks kuluv orienteeruv aeg ning autori kontaktandmed. Ankeedi analüüsimiseks kasutati kvantitatiivset meetodit. Küsimustik saadeti kokku 373 organisatsioonile ning vastuseid laekus 69. Seega vastas küsitlusele 18,5% uuringukutse saanutest. (vt. Diagramm 1). Autor hindab laekunud vastuste arvu piisavaks, et saada ülevaade valitsevast hetkeolukorrast. Siiski ei saa mõningal juhul teha piisavalt põhjalike järeldusi, kuna mõningate organisatsiooni tüüpide lõikes oli vastajate arv liiga väike.

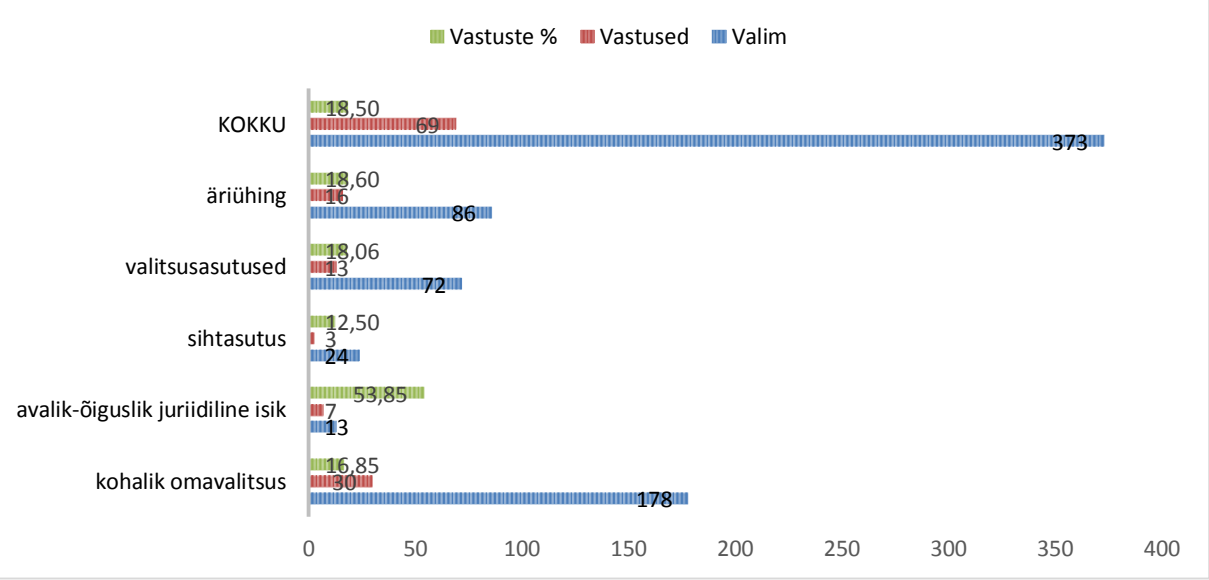



Diagramm 1. Küsitlusele vastanute ülevaade

## 6.2 Vastuste analüüs

Laekunud vastuste töötlemiseks ja analüüsiks on kasutatud andmetöötlusprogrammi *Microsoft Office 2013* ning lisaks tarkvaras sisalduvat *Power Pivot* funktsionaalsust.

- **Küsimus nr. 1**

Esimesele küsimusele **„Milline on organisatsiooni tüüp?“** olid kõik vastusevariandid ära kodeeritud lähtuvalt RIHA klassifikatsioonist, kuid oli tehtud mõningaid muudatusi, et lihtsustada vastuste andmist. Näiteks olid kokku liidetud üheks vastusevariandiks linna- ja vallavalituses ning nende ühiseks nimetajaks sai kohalik omavalitsus või tema hallatav asutus. Vastajad jagunesid selliselt, et 43,5% (30 vastajat) esindas kohaliku omavalitsust või tema hallatavat asutust, 10,1 % (7 vastajat) avalik-õigusliku juriidilist isikut või asutust, 4,3% (3 vastajat) olid sihtasutusest, 18,8% (13 vastajat) vastustest pärines valitsusasutusest ning valitsusasutuse hallatavatest riigiasutustest või nende kohalikust asutusest ning 23,2% esindas (16 vastajat) äriühingut või eraõigusliku asutust (vt. Diagramm 2). Võrreldes tulemusi valimiga võib väita, et üldjuhul laekus vastuseid organisatsioonide tüüpide lõikes sarnaselt küsitluse vastuste üldise protsendiga (vt. Diagramm 1), erandiks olid avalik-õiguslikud juriidilised isikud või asutused, kelle vastuste protsent 53,85% oli keskmisest oluliselt kõrgem ning negatiivse poole pealt kerkis esile sihtasutuste vastuste protsent, milleks oli 12,5%. Seega on uuringuga kaetud kõik organisatsioonide tüübid, mis võimaldab teha järgnevaid järeldusi ning üldistusi.

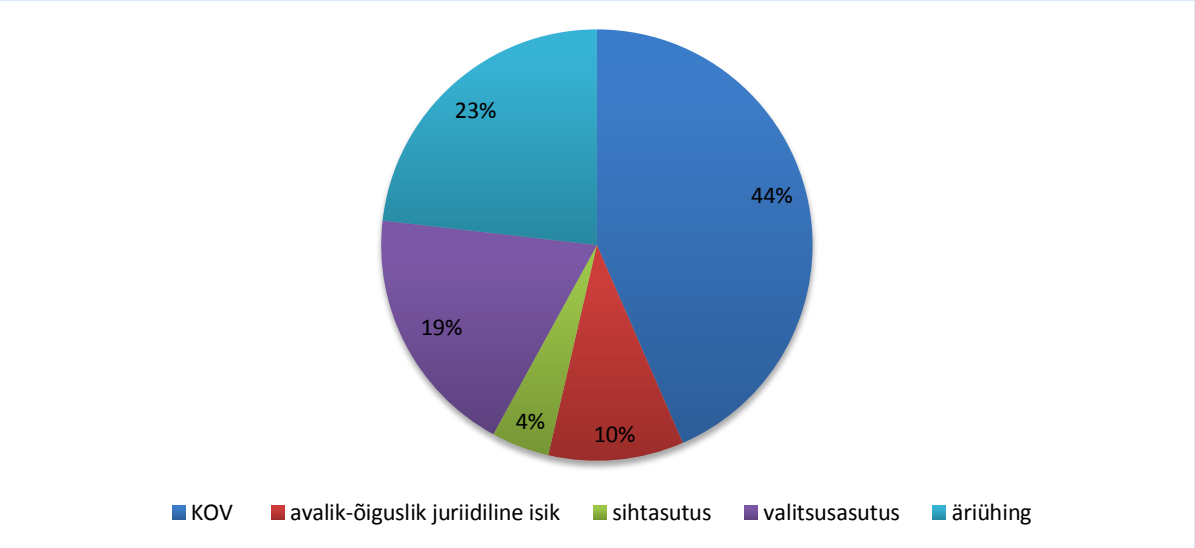



Diagramm 2. Organisatsiooni tüüp

- **Küsimus nr. 2**

Teine küsimus **„Milline on Teie positsioon organisatsioonis?“** võimaldas välja selgitada vastaja positsiooni organisatsioonis. Sellise informatsiooni hankimine oli vajalik selleks, et oleks võimalik paremini mõista vabateksti vastuste konteksti ja võimaldas ka paremini mõista teisi vastuseid. Vastajad jagunesid ametipositsiooni järgi järgmiselt: IT juht või (IT) riskijuht 40,6% (28 vastajat), IT spetsialist 26,1% (18 vastajat), tippjuht 8,7% (6 vastajat), muu loetlemata ametikoht 24,6% (17 vastajat) (vt. Diagramm 3). Kuna mõnevõrra suurem vastajate rühm olid IT juhid või (IT) riskijuhid, võib eeldada, et nende antud vastused olid täpsemad ning selgitused põhjalikumad. Sellegipoolest võib oletada, et IT riskide juhtimisega tegelevad organisatsioonides erinevate tööalaste rollide esindajad: IT juht, riskijuht, infoturbejuht, audiitor, IT spetsialist jne, mistõttu nende arusaamine ja teadmiste tase valdkonnast ning arusaamine IT riskijuhtimise vajalikkusest võib olla erinev. See omakorda viitab ka võimalikele probleemidele asutustes (vt. ka Küsimus nr 12 vastused).

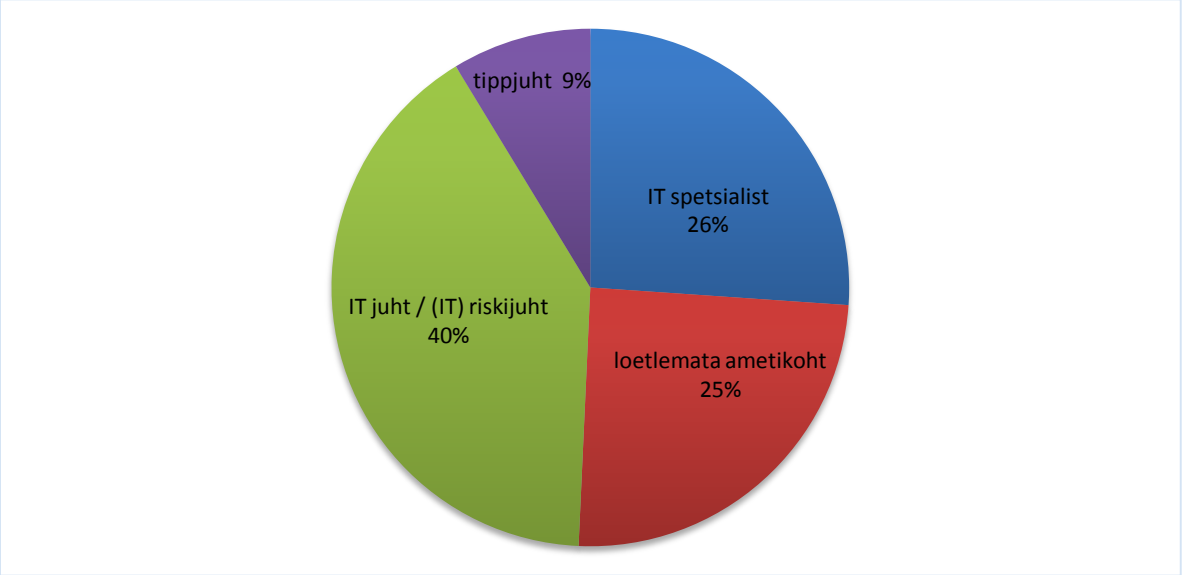



Diagramm 3. Vastajate positsioon organisatsioonis

- **Küsimus nr. 3**

Kolmanda küsimuse **„Milline on töötjate arv organisatsioonis?“** vastuse variandid olid ette kodeeritud selliselt, et hiljem oleks võimalik andmeid analüüsida. Vastajad jagunesid

ametikoha järgi järgmiselt: 1-10 töötajat 17,4% (12 vastajat), 11-30 töötajat 14,5% (10 vastajat), 31-50 töötajat 10,1% (7 vastajat), 51-100 18,8% (13 vastajat), 101-300 17,4% (12 vastajat), 301 ja rohkem töötajat 21,7% (15 vastajat). Vastajate hulgas oli esindajaid kõikidest kodeeritud vastuste valikutest (vt. Diagramm 4).

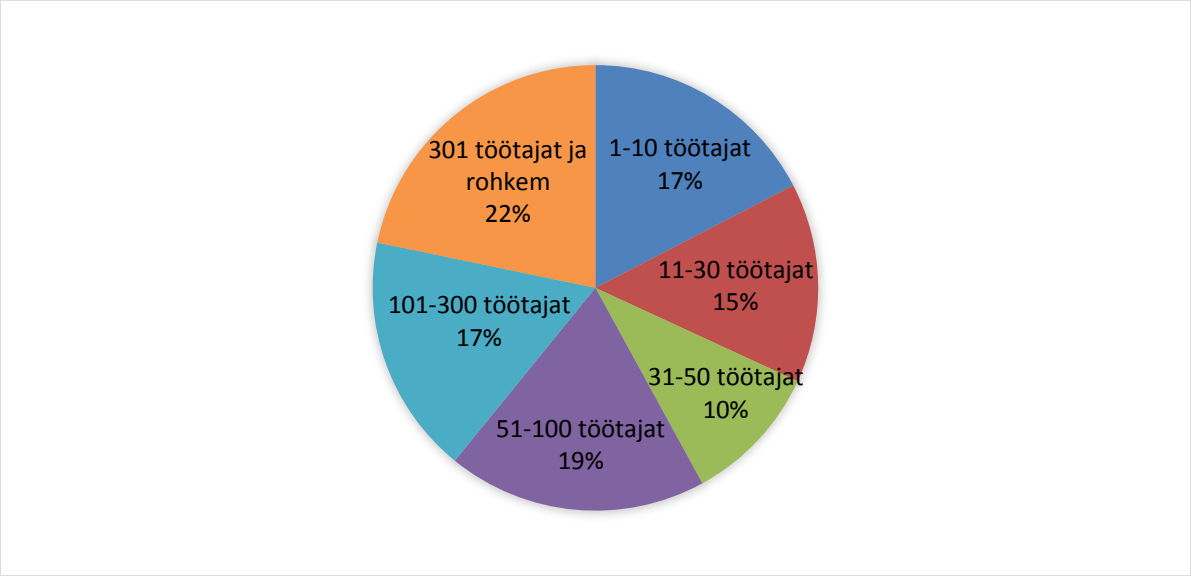



Diagramm 4. Töötajate arv organisatsioonis

- **Küsimus nr. 4**

Neljas küsimuse käsitles konkreetse IT-meeskonna suurust organisatsioonis ning oli sõnastatud järgmiselt**: „Milline on IT-ga seotud töötajate arv organisatsioonis?**“. Kõik vastuse variandid olid ette kodeeritud. Laekunud vastused jagunesid: 1 IT töötaja 39,1% (27 vastust), 2-4 IT töötajat 27,5% (19 vastust), 5-10 IT töötajat 8,7% (6 vastust), 11-30, 31-50, 51-100, 101 – 2,9% (2 vastajat) (vt. Diagramm 5 ja Tabel 26 ning Tabel 27).

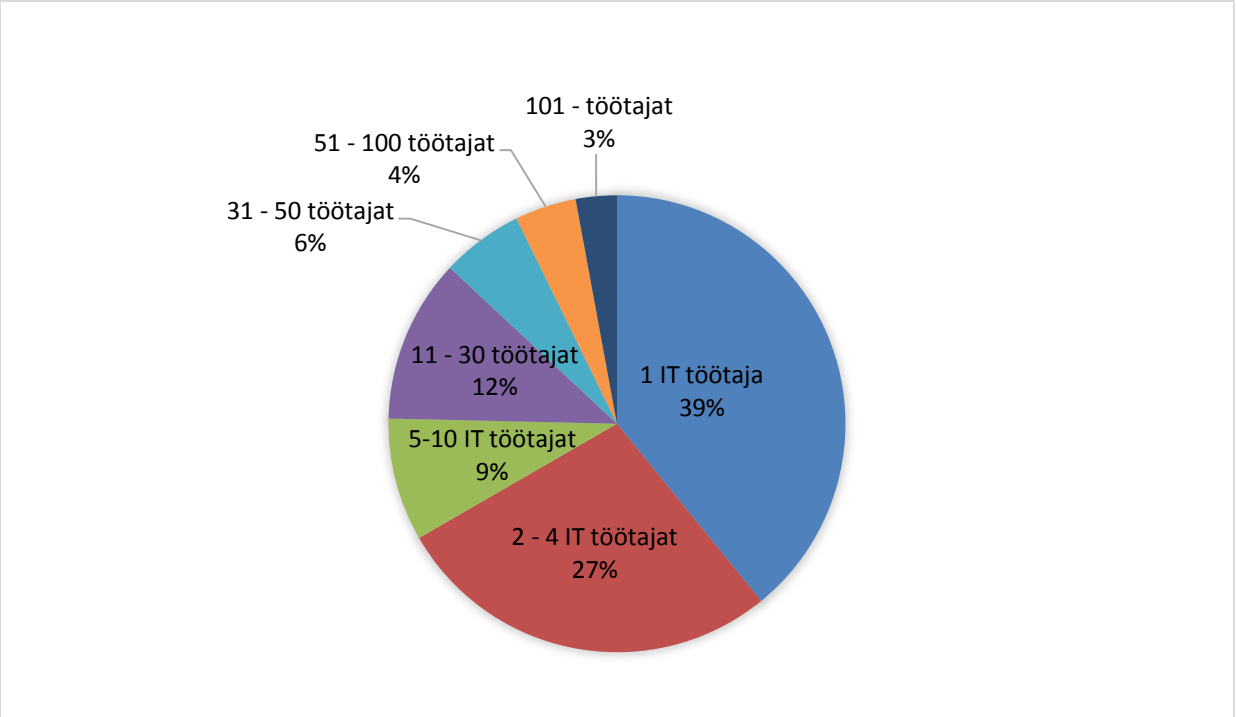



Diagramm 5. IT-ga seotud töötajate arv

Järgnevad tabelid annavad detailsema ülevaate, kuidas jagunesid vastused organisatsiooni tüübi ja vastanute ametikohtade vahel ning kui suur on nende IT meeskond, mis aitab paremini analüüsida vabateksti vastuseid.

| **Organisatsiooni tüüp** | **IT juht / riskijuht** | **IT spetsialist** | **loetlemata ametikoht** | **tippjuht** | **KOKKU** |
|---|---|---|---|---|---|
| avalik-õiguslik | 4 | 2 | 1 | | 7 |
| kohalik omavalitsus | 4 | 12 | 10 | 4 | 30 |
| sihtasutus | 3 | | | | 3 |
| valitsusasutus | 4 | 2 | 5 | 2 | 13 |
| äriühing | 13 | 2 | 1 | | 16 |
| **KOKKU** | **28** | **18** | **17** | **6** | **69** |

Tabel 26. Organisatsioonide tüübid ja küsitluses osalejate ametikohad

| Organisatsiooni tüüp | IT töötajate arv | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **1** | **2-4** | **5-10** | **11-30** | **31-50** | **51-100** | **101-** | **KOKKU** |
| avalik-õiguslik | 1 | 2 | 2 | 2 | | | | 7 |
| kohalik omavalitsus | 23 | 4 | 1 | 1 | 1 | | | 30 |
| sihtasutus | | 2 | | | 1 | | | 3 |
| valitsusasutus | 1 | 3 | | 4 | 2 | 2 | 1 | 13 |
| äriühing | 2 | 8 | 3 | 1 | | 1 | 1 | 16 |
| **KOKKU** | **27** | **19** | **6** | **8** | **4** | **3** | **2** | **69** |

Tabel 27. IT töötajate arv erinevat liiki organisatsioonides

Küsimuse tulemusi analüüsides võime näha, et väga paljudes kohalikes omavalitsustes töötab ainult üks IT valdkonna spetsialist, samas kui teised organisatsiooni tüübid on leidnud võimaluse palgata suurema IT meeskonna, mis loob ka paremad eeldused selleks, et oleks ressurssi ja teadmisi tegeleda süsteemselt IT-riskide juhtimisega.

- **Küsimus nr. 5**

Viiendale küsimusele **„Kuidas on IT riskijuhtimine Teie organisatsioonis korraldatud?** oli võimalik vastata vabateksti vormis oma sõnadega. Antud küsimusele esitatud vastuseid oli kõige otstarbekam analüüsida organisatsiooni tüüpide lõikes, kuna aitab paremini analüüsida küsimusi nr 7. ja nr. 8. Äriühingud ja eraõiguslikud asutused, keda oli vastajate koguarvust 23,2%, selgitasid, et nende organisatsioonides on üldjuhul tööl IT riskijuht (vt. Tabel 27) ehk 81% äriühingutest on ametis töötaja, kes vastutab valdkonna eest. Teine üldisem tähelepanek oli, et riskijuhtimine on eraldi funktsioon, mis hõlmab ka IT riskijuhtimist, et tagada koostöö äri ja IT otsustajate ning IT riskihalduri ja infoturbe juhi vahel. Kirjeldustest selgus, et sageli kasutatakse ka mitteformaalset IT-riskijuhtimise lähenemist, mida kinnitavad ka küsimustiku vastused (vt. Tabel 32). Selliselt toimib 69% äriorganisatsioonidest. Siiski on ka äriühinguid,

kes tegelevad IT riskijuhtimisega süsteemselt ning selgitasid oma töökorraldust selliselt: „S*üsteemid ja protsessid on viidud vastavusse ISO 27001 nõuetega. Tehtud on toimepidevuse riskianalüüs. Inimesed on läbinud koolituse ning testi kinnitamaks, et nad saavad aru, mida neilt nõutakse" või „Süsteemide toimepidavust tagavad nii firmasisesed protseduurid ning vahendid: ühtsed paigaldus- ja haldusprotsessid ning vahendid, monitooring, intsidentide haldus, eskalatsioonireeglid".* Erandlikult paistis silma üks vastaja, kes kirjutas, et nad on rakendanud Mehari 2010, millest võib järeldada, et tegemist on arvatavasti organisatsiooniga, kellel on tihedad rahvusvahelised sidemed.

Kohalikud omavalitsused vastasid, et nende IT-riskijuhtimise valdkonnas on rakendatud ISKE't. Mitmed vastasid, et on IT-riskide juhtimise teenuse ostnud sisse näiteks mõnelt äriühingult (näiteks Elion Ettevõtetelt) või teistelt teenusepakkujatelt ning vastavat tööd koordineerib kohaliku omavalituse ainuke IT-spetsialist. Lisaks tunnistasid mitmed, et tegelikult puudub neil vastav kompetents ning ressurss, kuna kohalik omavalitsus on väike ning napib eelarvelisi vahendeid. Kõik vastanud sihtasutused kirjeldasid, et IT riskijuhtimine piirdub kohustusliku ISKE rakendamisega ning täiendavalt midagi lisaks ei tehta. Seda kinnitavad ka küsitluse tulemused (vt. Tabel 31).

Valitsusasutuste lõikes olid vastused mitmekesisemad. Mitmel juhul selgitati, et detailsem IT-riskijuhtimise kirjeldus on salastatud ning piirdutakse kasutatavate standardite ja metoodikate äramärkimisega. Lisaks kirjeldati, et IT riskijuhtimine on kogu valitsemisalas tsentraliseeritud kokku, kuid lisaks konkreetsetele metoodikale kasutakse ka segametoodikat ning mitteformaalset lähenemist, mida kirjeldati järgmiselt: *„IT juhi enda arusaam riskidest"*. Mainiti ka ISKE kasutamist.

- **Küsimus nr. 6**

Ka kuues küsimus **„Kas organisatsioonis on juurutatud erinevad standardid (näiteks kvaliteedijuhtimine, riskijuhtimine jne)?"** võimaldas vastata vaba teksti vormis. Küsimuse eesmärk oli välja selgitada, kas lisaks IT-riskijuhtimisele on juurutatud ka teisi standardeid ja metoodikaid. Küsimus aitab paremini analüüsida organisatsiooni valmisolekut oma tegevust juhtida läbi erinevate raamistike. Vastustega tutvudes selgus, et viiel juhul tugineb

kvaliteedijuhtimissüsteem ISO 9001 standardile, seejuures neljal juhul oli tegemist äriühinguga ning ühel juhul valitsusasutusega. ITIL mainiti kahel korral ning mõlemal juhul töötas organisatsioonis rohkem kui 300 töötajat ning IT'-ga seotud töötajate arv jäi vahemikku 51-100 ning rohkem kui 101 töötajat, samad organisatsioonid kasutasid lisaks ka CAF (The Common Assessment Framework) ning üks nendest veel lisaks raamisiku EFQM (Excellence Model). Valdav enamus vastajatest teatas, et ei ole juurutanud mitte ühtegi süsteemi või metoodikat oma tegevuse korraldamiseks.

- **Küsimus nr. 7**

Seitsmes küsimus **„Milliseid IT riskijuhtimist käsitlevaid standardeid olete kasutanud IT riskijuhtimise korraldamiseks?"** andis konkreetse ülevaate sellest milliseid IT riskijuhtimise standardeid oma tegevuses kasutatakse. Vastused jagunesid: **ISO/IEC 27000** Infoturbe halduse süsteemid. (16 vastajat), **ISO/IEC 27001 -** Infoturbe halduse süsteemid. (13 vastajat), **ISO/IEC 27002 -** Infoturbemeetodite tavakoodeks (7 vastajat), **ISO/IEC 27003 -** Infoturbe halduse süsteemi teostusjuhis (5 vastajat), **ISO/IEC 27004 -** Infoturbe halduse süsteemid. (5 vastajat), **ISO/IEC 27005 -** Infoturvariski haldus (21 vastajat), **ISO/IEC 27032 -** Turbemeetodid. Suunised küberjulgeoleku valdkonnas (2 vastajat), **ISO/IEC 31000 -** Riskijuhtimine. (7 vastajat), **ISO/IEC 31010 -** Riskijuhtimine. Riskihindamise meetodid (6 vastajat), **NIST SP800-16 -** Infoturvariski koolituse nõuded (2 vastajat), **NIST SP800-30 - Riskijuhtimise juhised infosüsteemidele** (7 vastajat), **NIST SP800-39 -** Infosüsteemide riskijuhtimine (6 vastajat), **Muud standardid** (23 vastajat), **Ei ole kasutanud ühtegi standardit -** vastas jaatavalt 29 vastajat.

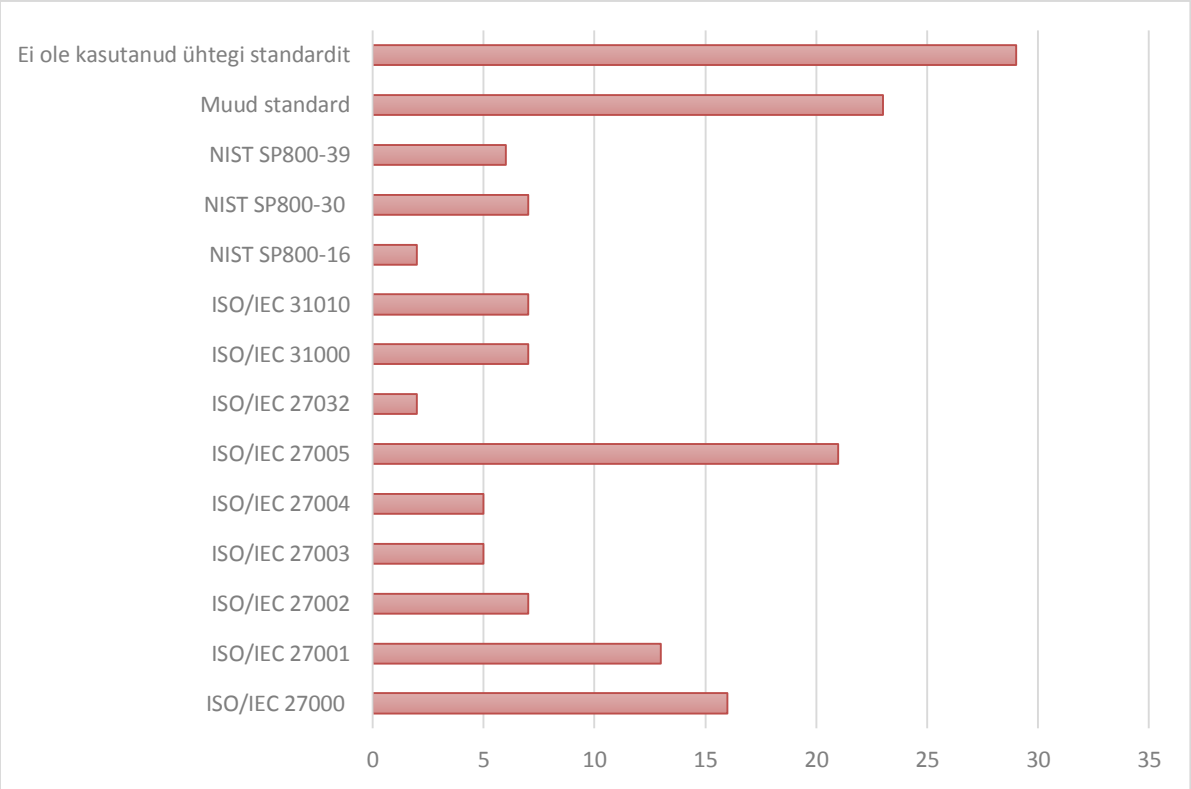



Diagramm 6. Ülevaade IT riskijuhtimise standarditest, mida organisatsioonid kasutavad

Järgnevad tabelid annavad ülevaate kuidas on standardid leidnud kasutust organisatsiooni tüüpide lõikes. Küsitluse tulemusel selgus, et kõige rohkem on leidnud rakendamist ISO/IEC 27005 standard, kokku 30,4% vastajatest, kuid veelgi tähelepanuväärsem on asjaolu, et tervelt 42% vastanutest ei kasuta ühtegi standardit IT-riskide juhtimisel. Küsitluse tulemusi analüüsides torkab silma, et kõige kõrgem protsent (66,7%) on kohalikel omavalitsustel, mida võib ka seletada asjaoluga, et nende IT-meeskond on üldjuhul väike ning tõenäoliselt jääb IT-riskijuhtimise standardite kasutamiseks puudu nii tööjõust kui ka teadmistest. Lisaks tõi küsitlus välja asjaolu, et äriühingutest tervelt 50% kasutab IT-riskijuhtimiseks standardeid, mida küsitluses ei nimetatud. Samuti on nad aktiivsemalt kasutanud ka USA päritolu NIST standardeid.

| Standard | avalik-õiguslik | KOV | sihtasutus | valitsusasutus | äriühing | KOKKU |
|---|---|---|---|---|---|---|
| ISO/IEC 27000 | 3 | 1 | 1 | 4 | 7 | **16** |
| ISO/IEC 27001 | 3 | 0 | 0 | 5 | 5 | **13** |
| ISO/IEC 27002 | 2 | 0 | 0 | 4 | 1 | **7** |
| ISO/IEC 27003 | 1 | 0 | 0 | 2 | 2 | **5** |
| ISO/IEC 27004 | 1 | 0 | 0 | 3 | 1 | **5** |
| ISO/IEC 27005 | 3 | 1 | 2 | 5 | 10 | **21** |
| ISO/IEC 27032 | 0 | 0 | 0 | 1 | 1 | **2** |
| ISO/IEC 31000 | 0 | 0 | 1 | 3 | 3 | **7** |
| ISO/IEC 31010 | 1 | 0 | 1 | 2 | 2 | **6** |
| NIST SP800-16 | 0 | 0 | 0 | 0 | 1 | **1** |
| NIST SP800-30 | 1 | 0 | 0 | 1 | 5 | **7** |
| NIST SP800-39 | 1 | 1 | 1 | 0 | 3 | **6** |
| Muud standardid | 0 | 8 | 1 | 6 | 8 | **23** |
| Ei kasuta standardeid | 2 | 20 | 0 | 4 | 3 | **29** |

Tabel 28. Standardite kasutamine organisatsioonides tüüpide lõikes

| Standard | avalik-õiguslik (%) | KOV (%) | sihtasutus (%) | valitsusasutus (%) | äriühing (%) | KOKKU (%) |
|---|---|---|---|---|---|---|
| ISO/IEC 27000 | 42,9 | 3,3 | 33,3 | 30,8 | 43,8 | **23,2** |
| ISO/IEC 27001 | 42,9 | 0,0 | 0,0 | 38,5 | 31,3 | **18,8** |

| | | | | | | |
|---|---|---|---|---|---|---|
| ISO/IEC 27002 | 28,6 | 0,0 | 0,0 | 30,8 | 6,3 | **10,1** |
| ISO/IEC 27003 | 14,3 | 0,0 | 0,0 | 15,4 | 12,5 | **7,2** |
| ISO/IEC 27004 | 14,3 | 0,0 | 0,0 | 23,1 | 6,3 | **7,2** |
| ISO/IEC 27005 | 42,9 | 3,3 | 66,7 | 38,5 | 62,5 | **30,4** |
| ISO/IEC 27032 | 0,0 | 0,0 | 0,0 | 7,7 | 6,3 | **2,9** |
| ISO/IEC 31000 | 0,0 | 0,0 | 33,3 | 23,1 | 18,8 | **10,1** |
| ISO/IEC 31010 | 14,3 | 0,0 | 33,3 | 15,4 | 12,5 | **8,7** |
| NIST SP800-16 | 0,0 | 0,0 | 0,0 | 0,0 | 6,3 | **1,4** |
| NIST SP800-30 | 14,3 | 0,0 | 0,0 | 7,7 | 31,3 | **10,1** |
| NIST SP800-39 | 14,3 | 3,3 | 33,3 | 0,0 | 18,8 | **8,7** |
| Muud standardid | 0,0 | 26,7 | 33,3 | 46,2 | 50,0 | **33,3** |
| Ei kasuta standardeid | 28,6 | 66,7 | 0,0 | 30,8 | 18,8 | **42,0** |

Tabel 29. Standardite kasutamine organisatsioonides tüüpide lõikes

Uurides lähemalt, kas suurema töötajaskonnaga organisatsioonid kasutavad ka aktiivsemalt erinevaid IT-riskijuhtimise standardeid oma töös, selgus, et äriühingute ja valitsusasutuste osas võib väita, et suuremad organisatsioonid on rohkem oma töös kasutanud IT-riskijuhtimise standardeid ning kohalike omavalitsuste vastustest selgub, et väiksemad organisatsioonid ei kasuta riskijuhtimiseks vastavaid IT-riskijuhtimise standardeid. Rohkem järeldusi aga ei ole võimalik teha, kuna vastuste arv erinevat tüüpi organisatsioonide kohta, olenevalt nende töötajate arvust, oli selleks liiga väike.

| Organisatsiooni tüüp | Töötajate arv | Vastanute arv | ISO/IEC 27000 | ISO/IEC 27001 | ISO/IEC 27002 | ISO/IEC 27003 | ISO/IEC 27004 | ISO/IEC 27005 | ISO/IEC 27032 | ISO/IEC 31000 | ISO/IEC 31010 | NIST SP800-16 | NIST SP800-30 | NIST SP800-39 | Muud standard | Ei ole ühtegi eelnevat kasutanud |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| avalik-õiguslik juriidiline isik | 1-10 | 1 | 1 | | | | | | | | | | | | | |
| | 50-100 | 3 | 1 | 1 | 1 | 1 | 1 | 2 | | | | | 1 | 1 | | 1 |
| | 101-300 | 1 | 1 | 1 | 1 | | | 1 | | | | | | | | |
| | 301 - | 2 | | 1 | | | | | | | | | | | | 1 |
| kohalik omavalitsus või tema hallatav asutus | 1-10 | 10 | | | | | | | | | | | | | 3 | 7 |
| | 11-30 | 9 | | | | | | | | | | | | | 1 | 8 |
| | 31-50 | 6 | 1 | | | | | 1 | | | | | | 1 | 1 | 3 |
| | 51-100 | 4 | | | | | | | | | | | | | 3 | 1 |
| | 301 - | 1 | | | | | | | | | | | | | | 1 |
| sihtasutus | 51-100 | 1 | 1 | | | | | 1 | | 1 | 1 | | | | | |
| | 101-300 | 1 | | | | | | 1 | | | | | | | | |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 301 - | 1 | | | | | | | | | | | | | 1 | |
| valitsusasutus, valitsusasutuse hallatav riigiasutusvõi kohalik asutus | 11-30 | 1 | 1 | 1 | 1 | | 1 | 1 | | 1 | 1 | | 1 | | | |
| | 31-50 | 1 | | | | | | 1 | | | | | | | | |
| | 101-300 | 5 | 1 | 1 | | | | 1 | | 1 | | | 1 | | 2 | 3 |
| | 301 - | 6 | 2 | 3 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 1 | 1 | 5 | 1 |
| äriühing/eraõiguslik asutus | 1-10 | 1 | | | | | | 1 | | | | | | | | |
| | 51-100 | 5 | 2 | 1 | | | | 3 | | 1 | 1 | 1 | 1 | 1 | 3 | 1 |
| | 101-300 | 5 | 2 | 1 | | 1 | | 2 | | | | | 1 | 1 | 1 | 1 |
| | 301 - | 5 | 3 | 2 | 1 | 1 | 1 | 4 | | 1 | 1 | | | 1 | 2 | 1 |

Tabel 30. Standardite kasutamine olenevalt organisatsiooni tüübist ja suurusest

- **Küsimus nr. 8**

Kaheksas küsimus **„Milliseid IT riskijuhtimist käsitlevaid metoodikaid olete kasutanud IT riskijuhtimise korraldamiseks?“** andis täpsema ülevaate kasutusel olevatest metoodikatest.

IT riskijuhtimise süsteemide kasutamist analüüsides selgub, et kõige laialdasemalt leiab kasutamist mitteformaalne lähenemine, kus kohalikest omavalitsustest kasutab sellist lähenemist 66,7% ja äriühingutest 68%. Avalik õiguslike asutuste seas oli kõige populaarsem segametoodika kasutamine (85,7%), sihtasutused kasutasid kõik (100%) IT Grundschutz (Eesti analoog ISKE'le) ja valitsusasutused eelistasid samuti segametoodikat (69,2%) (vt. Tabel 32 ja Diagramm 7).

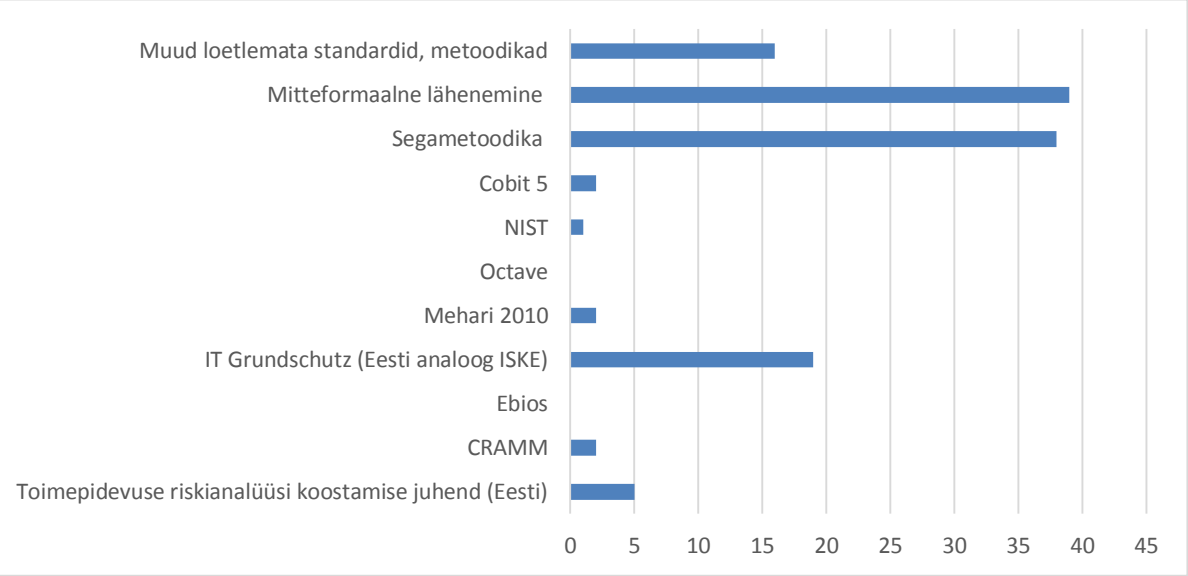



Diagramm 7. IT riskide juhtimise metoodikate kasutamine organisatsioonide lõikes

| **Riskijuhtimise süsteem** | **avalik-õiguslik** | **kohalik omavalitsus** | **sihtasutus** | **valitsusasutus** | **Äriühing** | **KOKKU** |
|---|---|---|---|---|---|---|
| Toimepidevuse riskianalüüsi | 0 | 0 | 1 | 2 | 2 | 5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| koostamise juhend (Eesti) | | | | | | |
| CRAMM | 0 | 1 | 0 | 0 | 1 | 2 |
| Ebios | 0 | 0 | 0 | 0 | 0 | 0 |
| IT Grundschutz (Eesti analoog ISKE) | 3 | 6 | 3 | 6 | 1 | 19 |
| Mehari 2010 | 0 | 0 | 0 | 1 | 1 | 2 |
| Octave | 0 | 0 | 0 | 0 | 0 | 0 |
| NIST | 1 | 0 | 0 | 0 | 0 | 1 |
| COBIT 5 | 0 | 0 | 0 | 0 | 2 | 2 |
| Segametoodika | 6 | 13 | 2 | 9 | 8 | 38 |
| Mitteformaalne lähenemine | 3 | 20 | 0 | 5 | 11 | 39 |
| Muud loetlemata standardid, metoodikad või töövahendid | 2 | 5 | 0 | 4 | 5 | 16 |

Tabel 31. IT riskide juhtimise metoodikad organisatsioonides tüüpide lõikes

IT-riskijuhtimise süsteemide kasutamist analüüsides võime märgata, et väga levinud on mitmete metoodikate samaaegne kasutamine. Eriti laialdast rakendamist on leidnud kombinatsioon segametoodikast ja mitteformaalset lähenemisest, mida kasutavad paralleelselt kõiki tüüpi organisatsioonid v.a sihtasutused, kus küsitluse tulemuste tõlgendamisel tuleb arvestada asjaoluga, et sihtasutuste hulgas oli ka vastajaid minimaalselt, seega selle põhjal järeldusi ei saa teha.

Tulemuste hindamisel peab kindlasti arvestama asjaoluga, et Eestis on ISKE rakendamine avaliku sektori asutustele kohustuslik, mistõttu võiks eeldada, et ISKE kasutamine on leidnud

laialt kasutust. Siiski selgub, et ainult 42,9% avalik-õiguslikest asutustest, 20% kohalikest omavalitsusest ja 46,2% valitsusasutustest kasutavad ISKE metoodikat (vt. Tabel 32). Esimene ISKE rakendusjuhend avaldati 2003. aastal, mistõttu võiks eeldada, et rohkem kui kümne aasta möödumisel võiks vastavad näitajad olla suuremad. Tõenäoliselt selgitab mõningal määral olukorda ka Andmekaitse Inspektsiooni poolt avaldatud ülevaade „Avaliku teabe seaduse ja Isikuandmete kaitse seaduse täitmisest aastal 2014. Soovitused aastaks 2015“ (Andmekaiste Inspetsioon, 2015), millest öeldakse, et „*Inspektsiooni hinnangul ei vasta tegelikkus päriselt välisele fassaadile. Lihtne näide: suur osa asutusi on andmekogude pidamisel eiranud korrapärase andmeturbeauditi tellimise kohustust. Riigi infosüsteemi haldussüsteemi ei tehta auditeerimise kohta ettenähtud märkeid, mis raskendab ülevaate saamist*“. Andmekaitse Inspektsioon ootab edaspidi RIA poolt tõhusat panust ja koostööd ISKE ning valitsusasutustes infoturbe juhtimise süsteemi rakendamise järelevalve alal, sealhulgas andmekogude auditeerimiskohustuse täitmise üle.

IT-riskijuhtimise süsteemi kasutus organisatsioonides:

| **Riskijuhtimise süsteem** | **avalik-õiguslik (%)** | **kohalik omavalitsus (%)** | **sihtasutus (%)** | **valitsus välist (%)** | **Äriühing (%)** |
|---|---|---|---|---|---|
| Toimepidevuse riskianalüüsi koostamise juhend (Eesti) | 0,0 | 0,0 | 33,3 | 15,4 | 12,5 |
| CRAMM | 0,0 | 3,3 | 0,0 | 0,0 | 6,3 |
| Ebios | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 |
| IT Grundschutz (Eesti analoog ISKE) | 42,9 | 20,0 | **100,0** | 46,2 | 6,3 |
| Mehari 2010 | 0,0 | 0,0 | 0,0 | 7,7 | 6,3 |
| Octave | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 |
| NIST | 14,3 | 0,0 | 0,0 | 0,0 | 0,0 |
| COBIT 5 | 0,0 | 0,0 | 0,0 | 0,0 | 12,5 |

| | | | | | |
|---|---|---|---|---|---|
| Segametoodika | **85,7** | 43,3 | 66,7 | **69,2** | 50,0 |
| Mitteformaalne lähenemine | 42,9 | **66,7** | 0,0 | 38,5 | **68,8** |
| Muud loetlemata standardid, metoodikad või töövahendid | 28,6 | 16,7 | 0,0 | 30,8 | 31,3 |

Tabel 32. IT riskide juhtimise metoodikate kasutus organisatsioonides

| **Organisatsiooni tüüp** | **Töötajate arv** | **Vastanute arv** | **Toimepidevuse riskianalüüs** | **CRAMM** | **Ebios** | **IT Grundschutz** | **Mehari 2010** | **Octave** | **NIST** | **Cobit 5** | **Segametoodika** | **Mitteformaalne lähenemine** | **Muud loetlemata metoodikad** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| avalik-õiguslik juriidiline isik | 1-10 | 1 | | | | | | | | | 1 | | |
| | 50-100 | 3 | | | | 2 | | | 1 | | 2 | 2 | 2 |
| | 101-300 | 1 | | | | 1 | | | | | 1 | | |
| | 301 - | 2 | | | | | | | | | 2 | 1 | |
| kohalik omavalitsus või tema hallatav asutus | 1-10 | 10 | | 1 | | 1 | | | | | 3 | 7 | 2 |
| | 11-30 | 9 | | | | | | | | | 4 | 7 | 2 |
| | 31-50 | 6 | | | | 1 | | | | | 4 | 4 | |
| | 51-100 | 4 | | | | 4 | | | | | 1 | 1 | 1 |
| | 301 - | 1 | | | | | | | | | 1 | 1 | |
| sihtasutus | 51-100 | 1 | | | | 1 | | | | | 1 | | |
| | 101-300 | 1 | | | | 1 | | | | | | | |
| | 301 - | 1 | 1 | | | 1 | | | | | 1 | | |
| valitsusasutus, valitsusasutuse hallatav | 11-30 | 1 | 1 | | | 1 | | | | | 1 | | |
| | 31-50 | 1 | | | | 1 | | | | | | | |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| riigiasutus või kohalik asutus | 101-300 | 5 | 1 | | | 1 | 1 | | | | 4 | 5 | 2 |
| | 301 - | 6 | | | | 3 | | | | | 4 | | 2 |
| äriühing/eraõiguslik asutus | 1-10 | 1 | | | | 1 | | | | | 1 | | |
| | 51-100 | 5 | | 1 | | | | | | 1 | 2 | 4 | 1 |
| | 101-300 | 5 | 1 | | | | | | | 1 | 2 | 3 | 2 |
| | 301 - | 5 | 1 | | | | 1 | | | | 3 | 4 | 2 |

Tabel 33. IT-riskide juhtimise metoodikate kasutus töötajate arvu järgi

- **Küsimus nr. 9**

Üheksanda küsimuse **„Milliseks hindate organisatsiooni vajadust IT riskijuhtimise järgi?“** hindasid vastajad organisatsiooni vajadusi riskijuhtimise järele. Laekunud vastused jagunesid selliselt, et väga oluliseks pidas vajadust IT riskijuhtimise järgi 50,72% küsitletavatest (35 vastajat), mõningal määral vajalikus pidas seda 42,02% vastajatest (29 vastajat) ja IT-riskijuhtimise järele puudus vajadus 7,24% (5 vastajat) (vt. Diagramm 8).

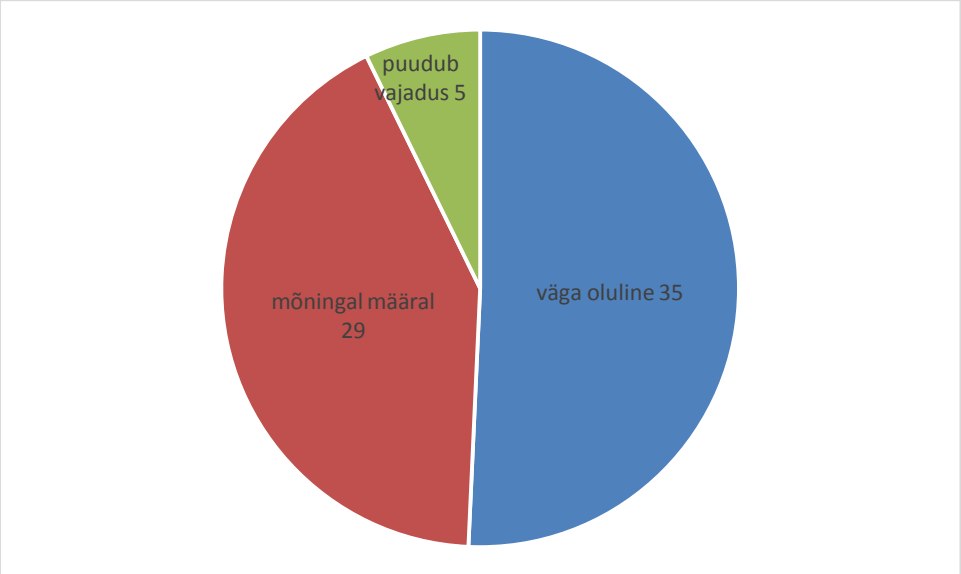



Diagramm 8. IT riskijuhtimise olulisus organisatsioonide jaoks

Uurides lähemalt kuidas hindavad erinevat tüüpi organisatsioonid vajadust IT-riskijuhtimise järele selgusid järgmised tulemused:

| Organisatsiooni tüüp | mõningal määral vajalik | vajadus puudub | väga oluline | KOKKU |
|---|---|---|---|---|
| avalik-õiguslik | 1 | | 6 | 7 |
| kohalik omavalitsus | 21 | 4 | 5 | 30 |
| Sihtasutus | | | 3 | 3 |
| Valitsusasutus | 5 | | 8 | 13 |
| Äriühing | 2 | 1 | 13 | 16 |
| **KOKKU** | **29** | **5** | **35** | **69** |

Tabel 34. Vajadus IT riskijuhtimise järele organisatsioonides

- **Küsimus nr. 10**

Kümnes küsimus: **„Kas Teie või Teie organisatsioon planeerib muudatusi organisatsiooni IT riskijuhtimises?** abil sai teada, kas organisatsioonid planeerivad muudatusi. Laekunud vastused jagunesid selliselt, et 52,2% vastanutest (36 vastajat) ei planeeri mitte mingisuguseid muutusi teha, 33,3% vastajatest (23 vastajat) on soov muutusi ellu viia, kuid puudub täpne plaan ning 15% vastajatest (10 vastajat) planeerivad muuta IT-riskijuhtimise korraldust ning neil on olemas plaan, kuidas seda teha (vt. Diagramm 9). Tuginedes eelnevale, võib järeldada, et ainult vähestel vastajatel on selge nägemus ja konkreetsem plaan, mida oleks vaja teha. Küsimustiku põhjal oletab autor, et üheks põhjuseks, mis moodustab tervelt 33,3%, on vajaliku info, teadmiste ja ressursi puudumine. Väidet kinnitavad ka küsimuse nr 4 tulemused, millest selgub, et paljudes organisatsioonides töötab ainult 1 IT spetsialist.

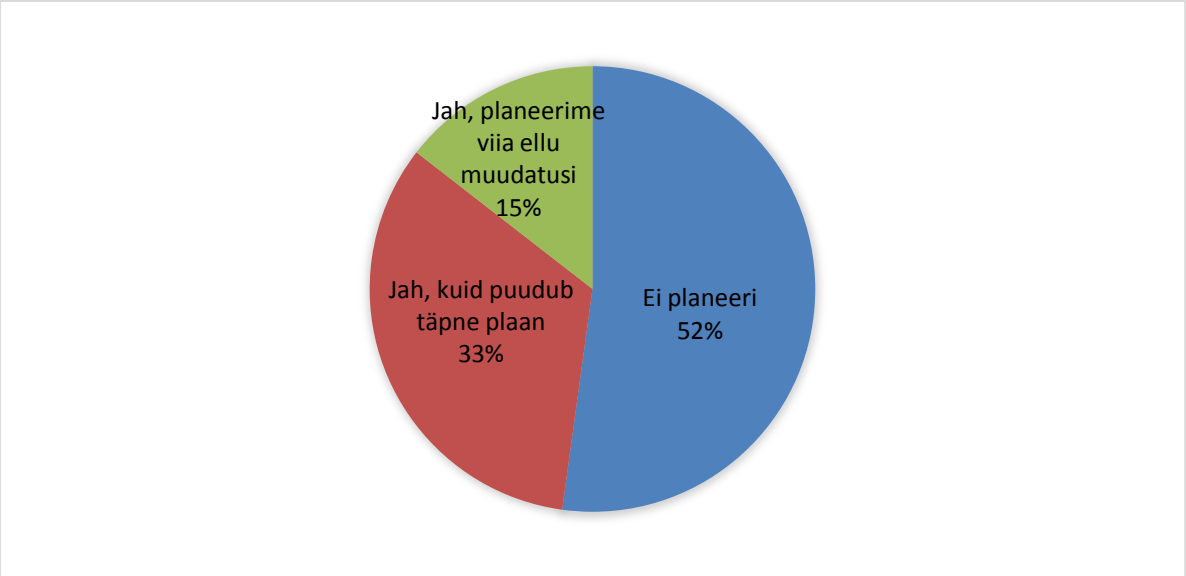



Diagramm 9. IT riskijuhtimise muudatuste planeerimine

Analüüsides täpsemalt, kes planeerivad muudatusi IT riskijuhtimises, selgusid järgmised tulemused:

| **Organisatsiooni tüüp** | **ei planeeri** | **jah, kuid puudub täpne plaan** | **jah, planeerime viia ellu muutusi** | **KOKKU** |
|---|---|---|---|---|
| avalik-õiguslik | 3 | 3 | 1 | 7 |
| kohalik omavalitsus | 14 | 14 | 2 | 30 |
| Sihtasutus | 1 | 1 | 1 | 3 |
| valitsusasutus | 8 | 3 | 2 | 13 |
| Äriühing | 10 | 2 | 4 | 16 |
| **KOKKU** | **36** | **23** | **10** | **69** |

Tabel 35. IT riskijuhtimise muutmise planeerimine

- **Küsimus nr. 11**

Eelviimase küsimuse eesmärk oli välja selgitada, milline on **IT riskijuhtimisega seotud lisatööjõu vajadus?** Laekunud vastused jagunesid selliselt, et 64% (44 vastajat) olid arvamusel, et pidev IT-riskijuhtimine toob endaga kaasa ka lisatööjõu vajaduse, 23% arvas, et lisatööjõudu ei ole vaja (16 vastajat) ning 13% vastajad ei oskanud vajadust hinnata (9 vastajat) (vt. Diagramm 10).

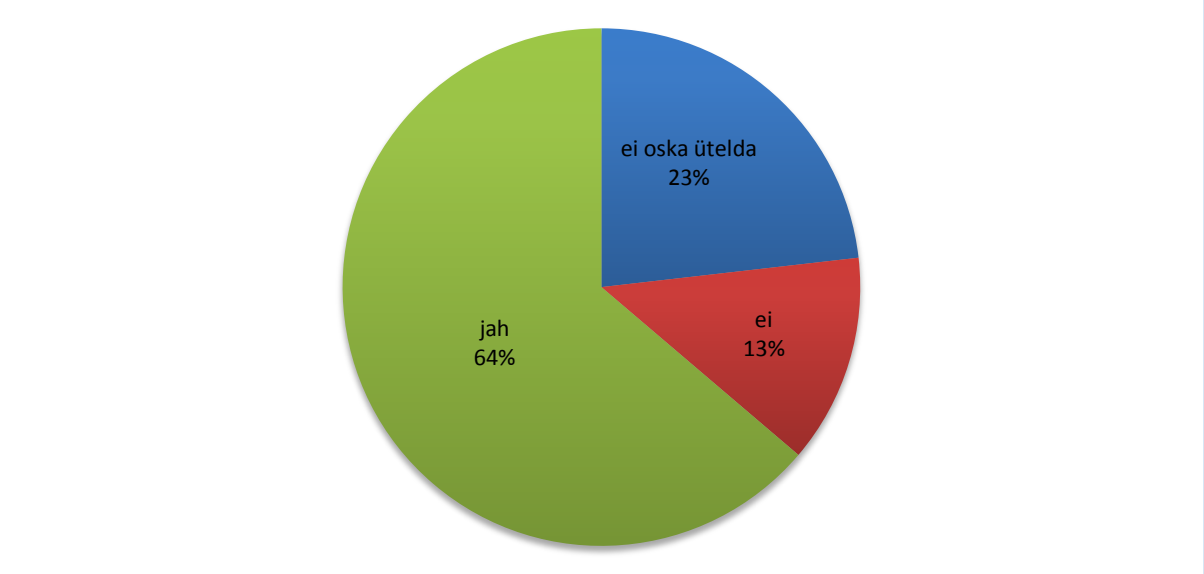



Diagramm 10. Lisatööjõu vajadus riskijuhtimise korraldamiseks

Laekunud vastustest näeme, et 64% vastajatest arvab, et IT riskijuhtimise korraldamine nõuab rohkem ressurssi, mistõttu võib see ka olla üheks põhjuseks, miks paljud organisatsioonid ei ole rakendanud mõnda konkreetset standardit või metoodikat (vt. ka küsimus nr 7 ja 8 vastuseid).

Millised organisatsioonid vajavad lisatööjõudu IT-riskijuhtimise korraldamiseks on toodud alljärgnevas tabelis.

| **Organisatsiooni tüüp** | **Ei suurenda tööjõu vajadust** | **ei oska öelda** | **Tööjõu vajadus suureneb** | **KOKKU** |
|---|---|---|---|---|
| avalik-õiguslik | 1 | | 6 | 7 |
| kohalik omavalitsus | 3 | 7 | 20 | 30 |

| | | | | |
|---|---|---|---|---|
| Sihtasutus | | | 3 | 3 |
| Valitsusasutus | 6 | 2 | 5 | 13 |
| Äriühing | 6 | | 10 | 16 |
| **KOKKU** | **16** | **9** | **44** | **69** |

Tabel 36. Lisa tööjõu vajadus IT riskijuhtimise korraldamiseks

- **Küsimus nr. 12**

Viimane küsimus **„Kas Teil on lisada veel kommentaare seoses IT riskijuhtimisega enda organisatsioonis?''** oli mõeldud täiendavate kommentaaride ja märkuste kogumiseks. Tegemist oli küsimusega, kus vastajatel oli täiendavalt võimalik anda omapoolseid selgitusi IT-riskijuhtimise kohta oma organisatsioonis. Täiendavalt selgitas olukorda 17 vastajat. Kokkuvõtvalt võib vastused jagada kahte suurde rühma. Esiteks organisatsioonid, kellel on IT-riskijuhtimise korraldamisega probleeme, kommenteerisid olukorda järgmiste selgitustega:

- *„puudub tegelikult vastav kompetents", „kogu valdkond on teadvustamata", „asutuses puudub kompetents", „tegelikult ei ole meil kompetentsi, arusaamaks mis on IT riskijuhtimine";*
- *„äri poolele on raske maha müüa ideed riskijuhtimise vajalikkusest ning sellesse investeerimisest (ressursid, aeg)";*
- *„Personali põud, ettevõte ei jaksa vajalike teadmistega spetsialiste palgata";*
- *„Kunagi sai arendatud ISKE-t, kuid jäänud soiku";*
- *„IT riskide juhtimine on väga oluline ja vajalik, aga kulude kokkuhoiu vajadusest lähtuvalt ei ole võimalik kaasata töökollektiivi IT-spetsialisti. Olulisem on igal töötajal jälgida, milliseid faile avab ja kus liigub internetis (st töötajate teadlikust erinevatest riskiallikatest)";*

Teise rühma moodustasid vastajad, kelle vastustest oli aru saada, et IT-riskijuhtimine on läbi mõeldud ning teadvustatud tegevus. Mõned olulisemad mõtted vastajatelt:

- *„Riskijuhtimine on võimalik tagada olemasoleva personaliga. Riski maandamistegevusteks ei näe alaliselt personali vajadust“ , „Oleme välja töötanud oma IT riskijuhtimise kontseptsiooni“;*
- *„Tegemist on asutusega, kus IT on konsolideeritud ministeeriumi tasemele. Oleme riikliku andmekogu vastutav töötleja, mistõttu on nõutav ISKE rakendamine“;*
- *„IT riskide hindamist oleme alati üritanud hoida vähemalt mingis vastavuses üle organisatsiooniliste riskide hindamisega. Kui hindasime riske lähtudes IT Grundschutz metoodikast, siis kasutasime ohtude hindamiseks tõenäosuse ja mõju maatriksit (5x5), mis oli üleüldiste riskide jaoks kasutatud. Kogemuse põhisele hindamisele läksime üle koos terve organisatsiooniga ka“;*
- *„IT ja organisatsiooni juhatuse koostöö on eduka IT riskijuhtimise üheks aluseks ja eelduseks. On vajalik, et juhatus (1) mõistaks vajadust, (2) toetaks ressurssidega, sealhulgas asjakohaste ametikohtade loomisega ning (3) annaks selgepiirilised volitused poliitika ja tegevuskava elluviimiseks“.*

# 7. MAGISTRITÖÖ JÄRELDUSED JA SOOVITUSED

Võrreldes *Saaty* analüütilise hierarhilise mudeli abil saadud tulemusi küsimustiku vastuste kokkuvõttega näeme, et mõlema uuringu kolm esimest tulemust on ühesugused (ISKE, segametoodika ja mitteformaalne lähenemine), kuid pingerida on neil erinev. Teoreetilises uuringus esikohale tulnud ISKE oli teostatud küsitluse tulemuste põhjal kolmandal kohal (vt. Tabel 31). Küsimustiku vastustest selgus, et mitteformaalset lähenemist kasutatakse kõige sagedamini (vt. Diagramm 7). Seetõttu võib teha järelduse, et Eesti avaliku sektori asutused kasutavad oma igapäevases töös autori poolt koostatud *Saaty* hierarhilise mudeli pingereas esile kerkinud metoodikaid IT riskijuhtimise korraldamiseks. Teiseks võime järeldada, et teoreetilise uuringu tulemus ning praktilise küsimustiku vastused toetavad teineteist. Kui võrrelda teoreetilisele võrdlusele baseerunud uuringut praktilise küsimustikuga, siis võib järeldada, et autori poolt määratud hindamiskriteeriumite osakaalud on üldjoontes piisavad, kuigi täiendavalt võiks kaaluda eraldi osakaalude määramist ka väikestele, keskmistele ja suurtele organisatsioonidele. Sellisel juhul võivad teoreetilise osa uurimistulemused olla veelgi täpsemad või kinnitada laiema valiku baasil tehtud otsuseid.

Küsimustiku vastustest selgub, et kõige enam on leidnud rakendamist ISO 27005 standard (21 korral) ning ISO 27000 standard (16 korral) ning valdavalt on neid rakendanud organisatsioonid kus töötab 100 või rohkem töötajat (vt. Tabel 30). Sellest võib järeldada, et vastavad ISO standardid on pigem leidnud rakendamist organisatsioonides, kus on rohkem töötajaid. Arvatavasti tagab suurem töötajaskond ka parema võimekuse ühelt poolt rakendada vastavaid standardeid ning samas ka põhjustab suurema vajaduse neid rakendada.

Autori arvates on murettekitav aga asjaolu, et tervelt 66,7% (vt. Tabel 29) kohalikest omavalitustest ei rakenda mingeid IT riskijuhtimise standardeid või metoodikaid. See on kindlasti üks võimalik riskiallikaks Eestis. Seejuures selgus, et 30-st vastanud kohalikust omavalitsusest pidas ainult 5 IT riskijuhtimist väga oluliseks (vt. Tabel 34). Oletatavasti on peamiseks põhjuseks omavalitsuste madal võimekus IT valdkonna juhtimiseks. Tõenäoliselt paraneb ka vastav võimekus peale riigireformi teostumist, kui alles jääb hinnanguliselt 60-70 omavalitsust, kus elab üldjuhul vähemalt 5000 inimest.

Autorile tuli üllatusena, et ainult 42,9% avalik õiguslikest asutustest ning 46,9% valitusasutusest on rakendanud ISKE metoodikat (vt. Tabel 32). Arvestades asjaolu, et ISKE rakendamine on neile üldjuhul kohustuslik, oleks eeldatav, et vastav protsent on oluliselt kõrgem. Üheks sellise tulemuse saavutamise põhjuseks võis olla ka asjaolu, et vastanute arv ei olnud piisavalt suur täpsema tulemuse saamiseks. Lisaks vajaks täiendavalt uurimist küsimus, kas vastajate poolt märgitud segametoodika kasutamine hõlmab juba ISKE metoodika rakendamist või mitte (vt. Tabel 32), kuna 85,7% avalik-õiguslikest asutustest ning 69,2% valitsusasutusest kasutavad uuringu kohaselt segametoodikat.

Täiendavalt oleks olnud huvitav teada saada, millised võiksid olla need „muud standardid", mida küsimustikule vastajad kasutavad. Selliseid vastuseid oli 33,3% vastanutest (vt. Tabel 29).

Töötanud läbi vastava erialase kirjanduse arvab autor, et tal ei jäänud märakamata ning kaardistama laialdaselt kasutuses olev IT riskijuhtimise standard või metoodika. Põhjalikumalt vajaks uurimist ka küsimus, millistel põhjustel planeerivad organisatsioonid muudatusi IT riskijuhtimises. Käesoleva magistritöö käigus koostatud küsimustik ei võimaldanud antud vastuseid detailsemalt kajastada.

Eesti avaliku sektori asutusele soovitab autor ennekõike kaaluda ISKE rakendamist, mille aluseks on võetud Saksamaal BSI poolt koostatud infoturbe standard - IT Baseline Protection Manual (saksa k. *IT-Grundschutz*). Turvameetmete süsteemi on Eestis pikaajaliselt rakendantud ja Riigi Informatsiooni Amet uuendab regulaarselt ka ISKE dokumentatsiooni. Siiski on üheks oluliseks puuduseks sobiva töövahendi ehk tarkvara puudumine, mis võimaldaks tööprotsessi automatiseerida ning versiooniuuenduste ja muudatuste korral infovarades andmestikku mugavalt ja kiirelt uuendada. Autorile on teada, et Riigi Infosüsteemi Amet korraldas 2015. aasta lõpus riigihanke uue tööriista loomiseks. Töö valmimise hetkeks aga ei ole arendustööde tulemusi veel laiemale avalikusele kättesaadavaks tehtud. Tööde eeldatav valmimise aeg on 2016. aasta lõpp või 2017. aasta algus. Lisaks pööratakse järgmistes ISKE versioonides suuremat tähelepanu riskihalduse protsessile, et tagada vastavus ISO 27001 standardile.

Täiendavalt soovitab autor kasutada ka ISO 27005 standardit, et organisatsioonis üles ehitada infoturbe halduse süsteem, et tagada süsteemne lähenemine. EMC (RCA) tasuline Archer GRC on küll väga hea ning ka Gartner poolt koostatud ülevaade soovitab kasutada eelpoolnimetatud

tarkvara, kuid tulenevalt tarkvara hinnast ning keerukusest, võiks vastava lahenduse soetamist kaaluda ainult mõne üksiku Eesti avaliku sektori asutuse vajadustest lähtuvalt.

Autor nõustub ENISA poolt 2015. aasta alguses avaldatud raporti soovitusega (ENISA Threat Landscape, 2015), milles korduvalt juhitakse tähelepanu asjaolule, et asjaomased standardite ja metoodikate arendajad peavad suutma ajaga kaasas käia. Erinevad ohud ja riskid on pidevas muutumises ning seetõttu peavad need olema ajakohaselt kaasajastatud. Seetõttu on väga oluline, et Eesti avaliku sektori asutused ja organisatsioonid kasutaksid ainult selliseid metoodikaid ja standardeid, mida uuendatakse süsteemselt ning regulaarselt.

Tuginedes magistritöö käigus kogutud informatsioonile leiab autor, et IT riskijuhtimise standardite ja metoodikate rakendamisel Eesti avaliku sektori asutustes peaks oluliselt suurenema RIA roll ning osakaal. RIA olles kompetentsikeskus, omab oluliselt suuremat teadmiste ja kogemuste pagasit valdkonnast võrreldes enamiku organisatsioonidega. Üheks lahenduseks võiks olla nõustamisteenuse pakkumine IT riskijuhtimise planeerimisel, juurutamisel, rakendamisel aga ka igapäevases töös. Teiseks võiks RIA koostada iga-aastaseid ülevaateid IT riskijuhtimise valdkonna muutustest, mis võimaldaks väiksematel organisatsioonidel hoida kokku ressursse. Kindlasti peaks oluliselt suurenema ka pakutavate koolituste maht sh. nii strateegilisel IT riskijuhtimise tasandil asutuste tippjuhtkonnale kui ka riskijuhtide ja spetsialistide hulgas. Lisaks vajab ühtlustamist lähenemine IT riskijuhtimise standarditel ja metoodikate kasutamine, kuna praktikas kasutatakse üheaegselt mitut erinevat varianti.

Küsitlusest selgus, et laialdast kasutamist on leidnud mitteformaalne lähenemine (vt. Tabel 32), mistõttu võib oletada, et ka IT riskijuhtimise praktika ning kvaliteet on väga erinev. Vastavate praktikate ühtlustamine saab toimuda aga ainult läbi koolituste ning ka ühtlustatud metoodikate kasutamise. Kindlasti on siin väga oluline ISKE rakendamine. Samas võib ISKE juurutamine väikestele organisatsioonidele olla liialt keeruline ja koormav või vajab asutus lisaks ISKE-le veel elemente ka teistest standarditest või metoodikatest.

Magistritöö tulemusel võib väita, et nii võrdluse kui küsitluse tulemuste põhjal selgus, et ISKE on sobivaim ning enim kasutatav meetod Eesti avaliku sektori asutuste poolt, kuid seda metoodikat võiks täiendada ISO 27001 ja ISO 27005 standardite rakendamisega. Hinnates tervikuna küsitluse tulemusi võib üldiselt järeldada, et Eesti avaliku sektori asutused

teadvustavad IT riskijuhtimise vajalikust, välja arvatud kohalikud omavalitused, kes ei tunneta hetkel veel valdkonna olulisust. Mida suurem on organisatsioon töötajate arvult, seda rohkem pööratakse ka tähelepanu IT riskijuhtimise süsteemsele korraldamisele, mis tugineks ka asjakohasel standardil või metoodikal.

# KOKKUVÕTE

Riskijuhtimise standardite ja metoodikate uuring koosnes kolmest osast. Viimases neljandas osas on autor käsitlenud kokkuvõtvalt kogu töö tulemusi. Esimeses osas on koostatud ülevaade teoreetilisest kirjandusest, mis võimaldas saada ülevaate asjakohastest standarditest, metoodikatest ning võimalikest tasuta ning tasulistest töövahenditest. Esimese osa tulemuste põhjal sai autor ülevaate, milliseid erinevaid metoodikaid ja standardeid maailmas kasutatakse, millest nad lähtuvad ja millised on nende erinevused. Samuti milliseid vahendeid kasutatakse IT riskijuhtimise haldamisel. Töö teises osas analüüsis autor esimeses osas läbitöötatud materjali. Autori eesmärgiks oli võrrelda erinevaid standardeid ja metoodikaid omavahel ning teha üldistavaid järeldusi ning soovitusi Eesti avaliku sektori asutustele. Standardite ja metoodikate võrdlemisel otsustas autor kasutada *Saaty hierarhilise analüüsi meetodit*, mis seisneb erinevate standardite ja metoodikate paarikaupa võrdlemises. *Saaty* meetodit kasutades sai töö teise ossa koondatud võrdlustulemused. Kolmandas osas käsitles autor praktilise uuringu läbiviimist ja analüüsis vastuseid ja vastajate struktuuri ning uuris kuidas on tegelikkuses IT organisatsioonid IT riskijuhtimist korraldanud. Selleks koostas autor küsimustiku, mis edastati 373 adressaadile vastamiseks. Töö kahele uuringuosale tuginedes oli võimalik analüüsida saadud tulemust, teha erinevad järeldusi ja pakkuda välja autoripoolseid ettepanekuid või soovitusi valikute tegemisel aga ka pakkuda välja täiendavaid ideid.

Riskide juhtimine aitab organisatsiooni lisandväärtuse loomisele kaasa, toetades organisatsioone nende eesmärkide realiseerimisel selliselt, et ta tagab organisatsiooni tegevusele järjepidevuse ja kontrolli raamistiku. See aitab kaasa otsuste tegemisele, planeerimisele ja prioriteetide seadmisele, luues organisatsiooni tegevusest, ohtudest ja võimalustest struktureeritud arusaama. Riskijuhtimine võimaldab hoida kokku ressursse ning neid efektiivselt kasutada, tagades samas töötajate arengu ja kogu teadmuste baasi laienemist (Liigand, 2005).

IT riskijuhtimist aitab korraldada ja reguleerida mitmed erinevad rahvusvahelised standardid. Tuntuimad on kindlasti ISO standardid (ISO 13335, ISO 17999, ISO 27000 seeria, ISO 31000 seeria) ja USA päritolu NIST standardid (NIST SP800-16, NIST SP 800-30, NIST SP800-39). Nendele standarditele tugineb ka valdav enamik välja töötatud IT riskijuhtimise metoodikaid (näiteks CRAMM, MEHARI, Ebios, GSTOOL, COBIT jne.). Kokkuvõttes eksisteerib täna

maailmas rohkem kui mitukümmend erinevat IT riskijuhtimise metoodikat. Nende kasutamiseks eksisteerib turul täna väga erinevaid töövahendeid. Üldjuhul on võimalik metoodikat ning vastavaid töövahendeid kasutada tasuta, kuid on olemas ka erinevad tasulisi lahendusi. Enamus juhtivaid tööstusriike on välja töötanud oma rahvusliku metoodika, mis arvestab eelkõige vastava riigi organisatsioonide vajadusi ning võimalusi, kuid on siiski üldjuhul rakendatavad ka teistes riikides. Suuremad riigid on tõlkinud ka oma metoodika suurematesse keeltesse (inglise, saksa, hispaania, prantsuse). See võimaldab nendega hõlpsamini tutvuda ning rakendada teist keelt kõnelevatel riikidel. Kindlasti tasub metoodika valikul arvestada ka oma organisatsiooni päritolumaa või peamiste koostööpartneritega, kellega tehakse koostööd. Tõenäoliselt on sellisel juhul ka hõlpsam mõista ühiselt IT riskide juhtimise korraldust ning sellega on võimalik tagada parem koostöö partneritega välismaal.

Autor leiab, et magistritöö on täinud püsitatud eesmärgi, kuna töö annab ülevaate IT riskijuhtimise olemusest ning erinevatest standarditest, metoodikatest ja töövahenditest. Töös pakutakse välja hindamiskriteeriumid ja metoodika ning viiakse läbi standardite, metoodikate ja töövahendite proovivõrdlemine. Lisaks sellele kaardistati küsitluse abil IT riskijuhtimise korraldust Eesti avaliku sektori asutustes ning elutähtsa teenuse osutajate juures. Autor kirjeldas ka omapoolseid soovitusi, millega peaks arvestama erinevate standardite, metoodikate ja töövahendite valimisel. Lõpetuseks tegi autor uuringu tulemuste põhjal kokkuvõtvad järeldused.

# SUMMARY

The author of the Master`s thesis was working for compile the review of proper literature and the sources of the internet to get his overview of different IT risk management standards, methodology, implements and these preliminary evaluation. So the one purpose of research work was to clear up, what would be the criteria's of estimations and these methodic possible help, possible from point of theoretical view, to estimate these. Resting upon these selected estimate criteria's, the author estimated by help of *Saaty* analytical hierarchies method, the different standards and methods, what can be used in Estonian public sector organizations and renders of vital services for management IT of risk leading.

In comparison the theoretical part of master´s thesis, the author carried through the questioning among Estonian public sector organizations and renders of vital services. The investigation permits get the review of standards and methods what already used in management of IT risk leading.

Supporting on the questionaries theoretical parts, the author comprised these with practical parts of investigation.

Using of theoretical part overview and IT risk managements standards, methods and the results of comparing, the author of the master´s thesis in this practical part compiles the questions of the research. The carried through questioning gives overlook of standards and methods already used in public sector and vital services. Used in questionaries research work was the qualitative research what was carried through the aim of the group.

The author compiles summary of results of carried through his thesis. The answers to the alternative questions were analyzed, started from answers numeral value and the part weight, calculated in percentage. In the open questions, there was possibility for the replies to answer with their own words to give descriptions to arrangement of IT risk management and give supplement explanations, their opinions and comments, to rest upon what the author has possibility to do his own conclusions.

On the ground of theoretical part of the master´s thesis and practical investigation, the author gives his recommendations and suggestions, which ones Estonian public sector institutions and

renders of vital services can take into consideration, when it´s planning to use some IT risk management standard, methods or implements. In addition in the master´s these offered some ideas and suggestions, how it is possible to reorganize work in this region so, that the all partners get the maximal profit.

In result of the this master´s thesis similar organizations can save their money and human resources and do better argumented and considered selections on management IT risk systems standards, methods and implements these plants or reforms on calling into being different IT risk management standards, methodology and implements and preliminary evaluation. IT risk management system rearrangement.

The Master`s thesis stand together seven chapters. Additional parts are explaining the abbreviations and other additions.

# LÜHENDITE SELETUSED

| Lühend | Tähendus | Selgitus |
|---|---|---|
| A&K | *Afhankelijkheids- en Kwetsbaarheidsanalyse* | Riskide juhtimise ja hindamise metoodika Hollandis. |
| AHM | Analüütiliste hierarhiate meetod | |
| BSI | Federal Office for Information Security | Saksamaa valitsusasutus, kes uurib turvariske, mis on seotud IT-ga ning töötab välja ennetavaid turvameetmeid. |
| CAF | The Common Assessment Framework | Total Quality Management (TQM) tööriist |
| CESG | Information Security arm of GCHQ, and the National Technical Authority for Information Assurance within the UK | Suurbritannia valitsusasutus, kes annab organisatsioonidele nõu, kuidas kaitsta oma andmeid ja infosüsteeme erinevate ohtude vastu. |
| CLUSIF | CLub for the Security of Information in France or CLub de la Sécurité de l'Information Français) | Prantsusmaal tegutsev mittetulundusühistu, mis tegeleb informatsioon ja IT turvalisusega. |
| CNSS | Committee on National Security Systems | Valitsusasutuste vaheline organisatsioon, mis kehtestab turvalisuse poliitikaid turvalisuse USA turvasüsteemides. |
| COBIT | Control Objectives for Information and Related Technology | Äriprotsessile suunatud raamistik IT juhtimiseks ja haldamiseks. |

| | | |
|---|---|---|
| CRAMM | CCTA Risk Analysis and Management Method | Suurbritannias välja töötatud riskianalüüsi meetod. |
| CTTA | Central Communication and Telecommunication Agency / Office of Government Commerce | Suurbritannia valitsusasutus |
| DCSSI | Direction Centrale de la Sécurité des Systémes d'Information, Premier Ministre | Prantsusmaa valitsusasutus, mis tegeleb IT turvalisusega. |
| EBIOS | Expression des Besoins et Identification des Objectifs de Sécurité | Terviklik kogum juhendeid, mis sisaldab ka tasuta avatud lähtekoodiga tarkvara, mis on algselt välja töötatud Prantsuse valitsuse poolt. |
| EFQM | EFQM (Excellence Model) | Juhtimismudel |
| ENISA | European Union Agency for Network and Information Security | EU agentuur, mis keskendub IT turvalisusele Euroopas. |
| ISACA | Information Systems Audit and Control Association | Rahvusvaheline kutseühing |
| ISAMM | Information Security Assessment & Monitoring Method | ISMS toetav riskijuhtimise meetod koos seda toetavate töövahenditega. |
| ISF | Information Security Forum | Riskianalüüsi meetod |
| ISKE | Infosüsteemide Kolmeastmeline Etalonturbe Süsteem | |
| ISMIS | Information Security Management Systems | Infoturbe halduse süsteem |
| ISO | International Organization for Standardization | Rahvusvahelise Standardiorganisatsioon |

| | | |
|---|---|---|
| IT Grundschutz | IT Baseline Protection Manual (saksa k. *IT-Grundschutz*). | Infoturbe standard |
| ITIL | Information Technology Infrastructure Library | Infotehnoloogia haldamise tavade ja protsesside standardite kogu |
| Magerit | Magerit metoodika | Hispaanias välja töötatud metoodika riskide analüüsimiseks ja riskide juhtimiseks. |
| Marion | Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau | Prantsusmaal välja töötatud riskianalüüsi metoodika |
| MIGRA | Metodologia Integrata per la Gestione del Rischio Aziendale | Itaalias välja töötatud riskianalüüsi meetod |
| NIST | National Institute of Standards and Technology | USA valitsusasutus |
| Octave | Operationally Critical Threat, Asset, and Vulnerability EvaluationSM | Metoodika, mis kirjeldab riskipõhist strateegilise hindamise ja planeerimise tehnikat. |
| OGC | Office of Government Commerce (also known as CTTA) | Suurbritannia valitsusasutus |
| RIA | Riigi Infosüsteemi Amet | Koordineerib riigi infosüsteemi arendamist ja haldamist Eestis. |
| Risk IT | Risk IT Framework | IT raamistik, mis sisaldub juba COBIT 5. |
| RiskSafe Assessmant | RiskSafe Assessmant | Riskianalüüsi meetod |
| Val IT | IT Value Delivery | IT raamistik, mis sisaldub juba COBIT 5 |

# LISA 1. Praktilise uuringu küsimustik

**1. Milline on organisatsiooni tüüp?**

Vastuse variandid:

- kohalik omavalitsus või tema hallatav asutus
- avalik-õiguslik juriidiline isik või asutus
- sihtasutus
- valitsusasutus, valitsusasutuse hallatav riigiasutusvõi kohalik asutus
- äriühing/eraõiguslik asutus

**2. Milline on Teie positsioon organisatsioonis?**

Vastuse variandid:

- Tippjuht
- IT juht / (IT) riskijuht
- IT spetsialist
- Loetlemata ametikoht

**3. Milline on Teie töötjate arv organisatsioonis?**

Vastuse variandid:

- 1 - 10 töötajat
- 11- 30 töötajat
- 31 - 50 töötajat
- 51 - 100 töötajat
- 101 - 300 töötajat
- 301 - ja rohkem töötajat

**4. Milline on IT-ga seotud töötajate arv organisatsioonis?**

Vastuse variandid:

- 1 - töötaja
- 2 - 4 töötajat
- 5 - 10 töötajat
- 11 - 30 töötajat
- 31 - 50 töötajat
- 51 - 100 töötajat
- 101 - ja rohkem töötajat

**5. Kuidas on IT riskijuhtimine Teie organisatsioonis korraldatud?**

Vastused: vaba tekst

**6. Kas organisatsioonis on juurutatud erinevad standardid (näiteks kvaliteedijuhtimine, riskijuhtimine jne)?**

Vastused: vaba tekst

**7. Milliseid IT riskijuhtimist käsitlevaid standardeid olete kasutanud IT riskijuhtimise korraldamiseks?**

Vastuse variandid:

- ISO/IEC 27000 - Infoturbe halduse süsteemid. Ülevaade ja sõnavara
- ISO/IEC 27001 - Infoturbe halduse süsteemid. Nõuded
- ISO/IEC 27002 - Infoturbemeetodite tavakoodeks
- ISO/IEC 27003 - Infoturbe halduse süsteemi teostusjuhis
- ISO/IEC 27004 - Infoturbe halduse süsteemid. Mõõtmine
- ISO/IEC 27005 - Infoturvariski haldus
- ISO/IEC 27032 - Turbemeetodid. Suunised küberjulgeoleku valdkonnas
- ISO/IEC 31000 - Riskijuhtimine – Põhimõtted ja juhised

- ISO/IEC 31010 - Riskijuhtimine. Riskihindamise meetodid
- NIST SP800-16 - Infoturvariski koolituse nõuded
- NIST SP800-30 - Riskijuhtimise juhised infosüsteemidele
- NIST SP800-39 - Infosüsteemide riskijuhtimine
- Muud standard
- Ei ole kasutatud ühtegi standardit

**8. Milliseid IT riskijuhtimist käsitlevaid metoodikaid olete kasutanud IT riskijuhtimise korraldamiseks?**

Vastuse variandid:

- Toimepidevuse riskianalüüsi koostamise juhend (Eesti)
- CRAMM
- Ebios
- IT Grundschutz (Eesti analoog ISKE)
- Mehari 2010
- Octave
- NIST
- Cobit 5
- Muud loetlemata standardid, metoodikad või töövahendid
- Segametoodika (riskide hindamine toimub standardi/metoodika abil ja meetmete valimine toimub kataloogidest, nt. ISKE)
- Mitteformaalne lähenemine (riskijuhtimine põhineb kogemusele ja tunnetusele)
- Muud loetlemata standardid, metoodikad või töövahendid

**8. Milliseks hindate organisatsiooni vajadust IT riskijuhtimise järgi?**

Vastuse variandid:

- Puudub vajadus
- Mõningal määral vajalik
- Väga oluline

**9. Kas Teie või Teie organisatsioon planeerib muudatusi organisatsiooni IT riskijuhtimises?**

Vastuse variandid:

- Ei planeeri
- Jah, kuid puudub täpne plaan
- Jah, planeerime viia ellu muudatusi

**10. Kas Teie hinnangul toob alaline IT riskijuhtimine kaasa lisatööjõu vajaduse organisatsioonis?**

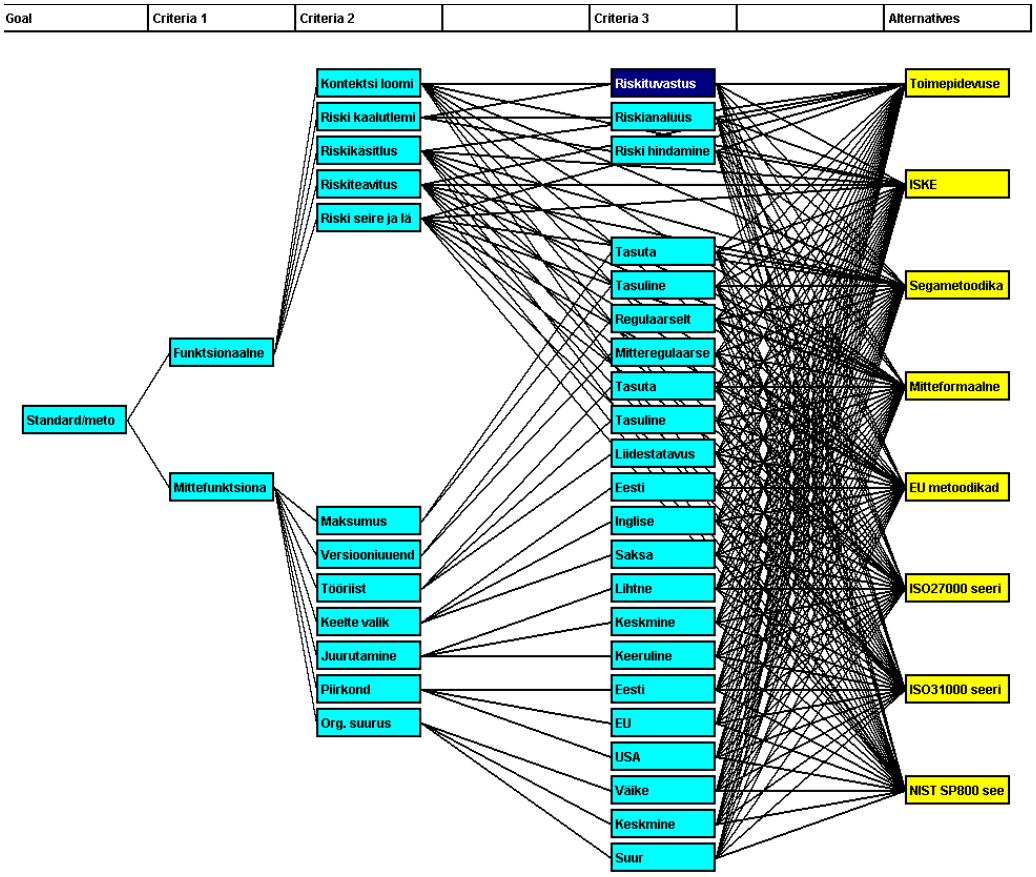
Vastuse variandid:

- Jah
- Ei
- Ei oska öelda

**12. Kas Teil on lisada veel kommentaare seoses IT riskijuhtimisega enda organisatsioonis?**

Vastused: vaba tekst

# LISA 2. Hindamiskriteeriumite visuaalne mudel



# JOONISED



# DIAGRAMMID



# TABELID

# KASUTATUD KIRJANDUS


Andmekaiste Inspetsioon. (15. 11 2015. a.). *Avaliku teabe seaduse ja Isikuandmete kaitse seaduse täitmisest aastal 2014. Soovitused aastaks 2015.* 2015: Andmekaitse Inspetsioon. Allikas: Andmekaitse Inspetsiooni koduleht: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/aastaraamat%202014.pdf

*Austrian IT Security Handbook*. (11. 31 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_au_it_security_handbook.html

*CESG*. (13. 03 2015. a.). Allikas: Analysis of information risk management methodologies: https://www.gov.uk/analysis-of-information-risk-management-methodologies#isoiec-270052011-information-technology---security-techniques---information-security-risk-management

*CRAMM*. (11. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_cramm.html

*Dutch A&K analysis*. (11. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_dutch_ak_analysis.html

*EBIOS*. (11. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_ebios.html

*EBIOS tool*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/tools/t_ebios.html

Elky, S. (31. 05 2006. a.). *An Introduction to information systems risk management.* Allikas: SANS Institute: http://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204

*ENISA*. (27. 03 2015. a.). Allikas: Inventory of Risk Management / Risk Assessment Methods and Tools : https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory

*ENISA Threat Landscape*. (15. 11 2015. a.). Allikas: ENISA Threat Landscape 2014: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

*Ernst & Young Managing IT risk.* (6 2013. a.). Allikas: Ernst & Young: http://www.ey.com/Publication/vwLUAssets/Managing_IT_risk_in_a_fast_changing_environment/$FILE/IT_Risk_Management_Survey.pdf

EVS. (14. 04 2015. a.). *Standardimine*. Allikas: Eesti Standarditkeskus: https://www.evs.ee/Standardimine/Standardimine/tabid/79/Default.aspx

EVS-ISO/IEC 27000:2015. (2015). *Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Ülevaade ja sõnavara (EVS-ISO/IEC 27000:2015).* Tallinn: Eesti Standardikeskus.

EVS-ISO/IEC 27002:2014. (2014). *Infotehnoloogia. Turbemeetodid. Infoturbemeetodite tavakoodeks (EVS-ISO/IEC 27002:2014).* Tallinn: Eesti Standardikeskus.

EVS-ISO/IEC 27004:2009. (2009). *Information technology. Security techniques. Information security management. Measurement.* Tallinn: Eesti Standardikeksu.

EVS-ISO/IEC 27005:2014. (2014). *Infotehnoloogia. Turbemeetodid. Infoturvariski haldus (EVS-ISO/IEC 27005:2014).* Tallinn: Eesti Standardikeskus.

EVS-ISO/IEC 27032:2012. (2012). *Information technology.Security techniques.Guidelines for cybersecurity.* Tallinn: Eesti Standardikeskus. Allikas: Information technology -- Security techniques -- Guidelines for cybersecurity.

*EVS-ISO/IEC 31000:2010.* (2010). Tallinn: Eesti Standardikeskus.

EVS-ISO/IEC 31000:2010. (2010). *Riskijuhtimine.Põhimõtted ja juhised.* Tallinn: Eesti Standardikeskus.

Georg Westerman, Richard Hunter. (2007). *IT Risk. Turning Business Threats into Competitive Advantage.* Boston: Harvard Business Review Press.

*GSTool*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/tools/t_gstool.html

*Inventory of Risk Management - Risk Assessment methods and tools*. (4. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_cramm.html

*ISAMM*. (11. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_isamm.html

*ISF*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_isf_methods.html

*ISO/IEC 13335-2*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_iso133352.html

*ISO/IEC 17799*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_iso17799.html

*ISO/IEC 27001*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_iso27001.html

*IT-Grundschutz*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_it_grundschutz.html

*KIK arengukava.* (02. 04 2015. a.). Allikas: KIK arengukava 2014-2020: http://kik.ee/sites/default/files/KIK_yld_failid/kik_arengukava_2014-2020.pdf

*KIK tutvustus*. (4. 3 2015. a.). Allikas: Kes me oleme: http://www.kik.ee/et/kes-me-oleme

Kouns, Minoli. (2010). *Information Technology Risk Management in Enterprise Environments.* Hoboken.New Jersy: John Wiley & Sons, Inc.

Liigand, J. (2005). *Ettevõtte riskid - äratundmine ja maandamine.* Tallinn: Äripäeva Kirjastus.

*Magerit*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_magerit.html

*Marion*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_marion.html

*Mehari 2010*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_mehari.html

*Mehari 2010 basic tool*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/tools/t_mehari.html

*Migra*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_migra.html

Minoli, D., & Kouns, J. (2010). *Information Technology Risk Management in Enterprise Environments.* Hoboken.New Jersy: John Wiley & Sons, Inc.

*Netekspert.com*. (20. 03 2015. a.). Allikas: Saaty meetod: http://www.netekspert.com/download/confpaper2.pdf

*NIST*. (25. 3 2015. a.). Allikas: http://csrc.nist.gov/publications: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf

*NIST*. (25. 3 2015. a.). Allikas: http://csrc.nist.gov/publications: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

NIST Special Publication 800-37. Revision 1. (10. 03 2015. a.). *Special Publication 800-37 rev 1. Guide for Applying the Risk Management Framework to Federal Information Systems.* Allikas: National Institute of Standards and Technology : http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

*Octave*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_octave.html

Paul, P., & Wheeler, J. (25. 05 2015. a.). *Gartner*. Allikas: Magic Quadrant for IT Risk Management: http://www.gartner.com/technology

*RIA*. (28. 03 2015. a.). Allikas: Infosüsteemide turvameetmete süsteem ISKE: https://www.ria.ee/iske/

*RIA*. (30. 3 2015. a.). Allikas: Riigi Infosüsteemi Amet: https://www.ria.ee/ohtlike-kuberjuhtumite-osakaal-on-aastaga-kasvanud/

*RIA*. (12. 3 2015. a.). Allikas: ISKE tööriist: https://www.ria.ee/isketooriist/

*RIA koduleht*. (16. 11 2015. a.). Allikas: www.ria.ee: https://www.ria.ee/public/ISKE/naidisdokumendid/LISA1.21.IT-projektide_tasuvusanaluus.doc

*RIHA*. (20. 03 2015. a.). Allikas: Riigi Infosüsteemi Haldussüsteem: https://riha.eesti.ee

*Riigiteataja*. (20. 03 2015. a.). Allikas: Hädaolukorra seadus: https://www.riigiteataja.ee/akt/116122014014

*Risk Assessment Tools*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/tools

*Risk Scenarios Using COBIT 5 for Risk*. (4. 3 2015. a.). Allikas: ISACA: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/risk-scenarios-using-cobit-5-for-risk.aspx

*Riskijuhtimine - kellele ja milleks?* (4. Märts 2015. a.). Allikas: Siseaudit avalikule- ja erasektorile: http://www.siseaudiitor.ee/riskijuhtimine-kellele-ja-milleks/

Riskijuhtimine. Rahandusministeerium. (10. 03 2015. a.). *Kasulik info.* Allikas: Eesti Siseaudiitorite Ühing (ESAÜ): http://www.siseaudit.ee/files/RISKIJUHTIMINE.pdf

*RiskSafe Assessment* . (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_risksafe-assessment

*SP800-30*. (12. 3 2015. a.). Allikas: European Union Agency for Network and Information Security: http://rm-inv.enisa.europa.eu/methods/m_sp800_30.html

The Risk IT Framework. (10. 03 2015. a.). *Knowledge-Center.* Allikas: www.isaca.org: http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework_fmk_Eng_0610.pdf?regnum=246314

*Web-HIPRE*. (30. 03 2015. a.). Allikas: http://www.hipre.hut.fi

*Why use COBIT 5*. (24. 3 2015. a.). Allikas: ISACA: https://cobitonline.isaca.org/about

Võhandu, L. (1998). *Subjektiivsetest hinnangutest objektiivsete tulemusteni : loengukonspekt.* Tallinn: Tallinna Tehnikaülikooli Kirjastus.