

Küberturvalisuse kulude arvestamise mudeli loomine Majandus- ja Kommunikatsiooni- ministeeriumile



Rahastanud Euroopa Liit
NextGenerationEU



Eesti
tuleviku heaks

Sisukord

Kokkuvõte	3
1. Sissejuhatus	5
2. Küberturvalisuse kulude hetkeolukorra kirjeldus	7
2.1 Küberturvalisuse mõiste määratlus	7
2.2 Küberturvalisuse kulude arvestamise lahendused	9
2.3 Ülevaade analüüsitud IT-asutuste kulumudelitest	10
2.3.1 Eesti IT-asutuste finantsarvestuse, eelarvestamise ja kuluarvestuse praktikatest	11
2.3.1.1 Rahandusministeeriumi info- ja tehnoloogiakeskus (RMIT)	14
2.3.1.2 Siseministeeriumi infotehnoloogia- ja arenduskeskus (SMIT)	17
2.3.1.3 Riigi Infosüsteemi Amet (RIA)	19
2.3.1.4 Riigi Info- ja Kommunikatsioonitehnoloogia Keskus (RIT)	22
2.3.1.5 Keskkonnaministeeriumi infotehnoloogiakeskus (KEMIT)	24
2.3.1.6 Registrate ja Infosüsteemide Keskus (RIK)	26
2.3.2 Asutuste kulumodelite kokkuvõte	28
3. Väljapakutav kulumudel	30
3.1 Kulumodeli tehnoloogiline vaade	30
3.1.1 Küberturvalisuse kulude paiknemine arvestussüsteemis	30
3.1.2 IT ja küberturvalisuse kulude üldine liigitus	31
3.1.2.1 Kulude eesmärgi põhine liigitus	32
3.1.2.2 Kululiigi põhine liigitus	33
3.1.3 Selgitused küberturvalisuse kulude eesmärgi põhiseks jaotamiseks	34
3.1.3.1 Riistvara kulud	34
3.1.3.2 Tarkvara kulud	34
3.1.3.3 Teenuste kulud	34
3.1.3.4 Personalikulud	34
3.1.3.5 Füüsilise turvalisusega seotud kulud	35
3.2 Kulumodeli finantsvaade	35
3.2.1 Asutuse tasemel kulude koondamine/arvutamine	36
3.2.1.1 Ressursitunnuseid kasutavad infoturbe kulude jaotusalused	36
3.2.1.2 Kontosid kasutavad infoturbe kulude jaotusalused	38
3.2.1.3 Muid jaotusaluseid kasutavad infoturbe kulude jaotusalused	38
3.2.1.4 Variantide kokkuvõte	40
4. Lisa 1. Toodete ja teenuste nimekiri	42

Kokkuvõte

Tänases riigiasutuste IKT kulude arvestamise süsteemis ei peeta eraldi arvestust küberturvalisuse kulude üle. Küberturvalisuse kulud moodustavad teatud osa IKT või sellega seotud kuludest, kuid raamatupidamislikult ja kuluarvestuslikult nende kulude üle ühtsetel põhimõtetel arvestust ei peeta. Asutustes on kasutusel enda asutuse põhised spetsiifilised kulumudelid, mis paljudel juhtudel ka arvestavad küberturvalisuse kulusid, kuid kuna asutuste kuluarvestuse põhimõtted on erinevad, siis seetõttu ei ole ka tulemused asutuste vahel võrreldavad.

Käesolev aruanne esitab analüüsi, kuidas täna asutustes küberturvalisuse kulude üle arvestust peetakse ning pakub välja tehnoloogilise ning finantsarvestusliku vaate kulude arvestamise põhimõtetest ja alternatiividest.

Küberturvalisuse mõiste

Küberturvalisus on mõiste, millel ei ole erialaringkondades ühtset kokkuleppelist definitsiooni või on need definitsioonid omavahel vastuolus. Küberturvalisus on olemuselt sarnane inforturbega ja selle all mõeldakse riskihalduslikku tegevust teabe turvalisuse säilitamiseks ja andmekaitse tagamiseks. Küberturvalisuse teatav erisus infoturbest on seotud fookusega digitaalsetele infovaradele (kui info turve vaatleb kõiki infovarasid). Kuna mittedigitaalsete infovaradega tegelemise osakaal langeb, siis käesoleva töö kontekstis käsitleme küberturvalisust ja infoturvet samatähenduslikena, seda ka põhjusel et sisuliselt ollakse Eesti riigiasutustest rohkem harjutud viimase mõistega ja infoturbe mõiste esineb ka nii organisatsiooniliste üksuste (infoturbe osakond, infoturbe talitus) kui ka ametkohtade (infoturbejuht, infoturbe-ekspert) nimetustes.

Küberturvalisuse mõistet on põhjalikumalt käsitletud analüüsi peatükis 2.1.

Küberturvalisuse kulude hetkeolukord

Küberturvalisuse kulude tänast käsitlust tuleb vaadelda laiemalt IKT kulude kontekstis. IKT kulude üle arvepidamiseks on riigiraamatupidamise kontoplaanis eraldatud kontod IKT kulude haldamiseks. Need kontod võimaldavad pidada arvestust olulisemate IKT kululiikide või infovara liikide lõikes (nt riistvara, tarkvara, teenused).

Küberturvalisuse kulud võivad aga sisalduda erinevate kululiikide sees, lisaks ka investeeringutes ja personalikuludes. Seetõttu peetakse asutustes arvestust küberturvalisuse üle eraldi finantsdimensioonide¹ ehk tunnuste abil. Selliseks tunnuseks on reeglina nii raamatupidamises kui kuluarvestuses kasutatav tunnus „ressurss/kulukoht“. Kuigi küberturvalisuse kulude üle arvestust peetakse, siis on riigi seisukohast ühtse ja võrreldava ülevaate saamise vaates siiski mitmeid puudusi. Näiteks ei ole riigis ühtseid põhimõtteid, kuidas kulusid IKT ja küberturvalisuse vahel jagada.

Küberturvalisuse kuluarvestuse hetkeolukorda on asutuste lõikes vaadeldud peatükis 2.3.1.

Küberturvalisuse kulude arvestamise mudeli ettepanek

Analüüs pakub välja küberturvalisuse kulude arvestamise loogika nii infotehnoloogilises kui finantsarvestuslikus vaates. Tehnoloogilises vaates pakutakse nimekiri enamlevinud IKT kuluartiklitest, mida IKT või infoturbe funktsioon hangib või millele vahendid kuluvad. Need kuluartiklid on liigitatud kolme gruppi – kas täielikult IKT kulude alla, täielikult küberturvalisuse kulude alla või segakulude alla, mille puhul on antud üldised juhised ja põhimõtted nende kulude kajastamiseks. Üldine põhimõte kulude

¹ Finantsdimensiooni all on mõeldud finantskannet või -tehingut kirjeldavat andmedimensiooni, mis iseloomustab kande majanduslikku sisu selles osas, mida ei ole võimalik kirjeldada raamatupidamiskontoga (sh küberturvalisus).

liigitamisel on lähtumine kulu tegemise eesmärgist ja tehtava kulutuse seosest äritegevust toetava IT funktsiooniga. Kui vastava IKT komponendi hankimata jätmine ei mõjuta vahetult äritegevust toetavat IT funktsioneerimist, siis võib selle kulu liigitada küberturvalisuse alla.

Detailne IKT ja küberturvalisuse kuluartiklite nimekiri on esitatud aruande lisas 1.

1. Sissejuhatus

Ernst ja Young Baltic AS (edaspidi EY) viis Majandus- ja Kommunikatsiooniministeeriumi tellimusel läbi projekti „Küberturvalisuse kulude arvestamise mudeli loomine Majandus- ja Kommunikatsiooniministeeriumile“. Projekti eesmärgiks oli luua põhimõtted ja juhised, millest lähtuda küberturvalisuse kulude käsitlemisel asutustes nii tehnoloogiliselt kui finantsilisest vaatenurgast.

Tänased riigiasutustes rakendatud finantsarvestuse praktikad nii infotehnoloogia kulude üldisemaks, kui küberturvalisuse kulude spetsiifiliseks käsitlemiseks on erinevad. Kuigi küberturvalisuse kulude üle paljudel juhtudel arvestust mingil kujul peetakse, siis ei ole head ülevaadet kui palju riigis kokku küberturvalisusele kulub.

Käesolev analüüsiprojekt koosnes kolmest etapist. Esimeses etapis täpsustati projekti jaoks sisendit andvad osapooled ja selgitati nende vajadused. Peamisteks partneriteks said IT asutuste IT-, infoturbe- ja finantsjuhid, kelle abil täpsustati tänaseid kuluarvestuse praktikaid ning arutati võimalike tuleviku-lahenduste üle.

Projekti teises etapis analüüsiti süvitsi IT asutuste poolt kasutatavaid kulumudeleid ning kaardistati tänased IT ja küberturvalisuse kulude arvestamise praktikad. Infoturbekulude käsitlemise ja asutuses kasutatavate kulumudelite kohta andsid sisendit KEMIT, RIA, RIT, RMIT, SMIT ning RIKS.

Kolmandas etapis pakuti välja küberturvalisuse arvestamise mudel nii finantsarvestuslikus kui infotehnoloogilises vaates.

Tabel 1. Aruandes kasutatud lühendid

Mõiste	Selgitus
ATK	arvutitöökohta teenus
CERT	RIA koosseisu kuuluv intsidentide käsitlemise osakond (<i>CERT - Computer Emergency Response Team</i>)
CIA triaad	Inglise keelest tulenev infoturbe mudel (Confidentiality, Integrity, Availability)
E-ITS	Eesti Infoturbestandard
EK	Eelarveklassifikaator
EL	Euroopa Liit
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
IKT	Info- ja kommunikatsioonitehnoloogia
Infoturve	Info- ja küberturbe valdkond (edaspidi kokkuvõtlikult infoturve)
ISO/IEC	Ülemaailmselt tunnustatud infoturbestandardi väljastaja
IT	Infotehnoloogia
KAIS	Kuluarvestuse Infosüsteem
KEMIT	Keskkonnaministeeriumi info- ja tehnoloogiakeskus

Mõiste	Selgitus
KTU	Küberturvalisus
MKM	Majandus- ja Kommunikatsiooniministeerium
NIS direktiiv	Küberturvalisuse direktiiv (EL 2016/1148)
NIST	<i>National Institute of Standards and Technology</i> - USA riiklik standardite ja tehnoloogia instituut
RaM	Rahandusministeerium
RIA	Riigi Infosüsteemi Amet
RIKS	Riigi Infokommunikatsiooni Sihtasutus
RIT	Riigi IKT Keskus
RKAS	Riigi Kinnisvara Aktsiaselts
RMIT	Rahandusministeeriumi infotehnoloogia ja arenduskeskus
SAP	Finantsarvestustarkvara
SAT	serveri alustaristu teenus
SLA	Teenustaseme lepe (ingl. k. <i>Service Level Agreement</i>)
SMIT	Siseministeeriumi infotehnoloogia ja arenduskeskus
TERE	Tegevuspõhine Riigieelarve
VPN	inglise keelest tulenev termin „virtual private network“, ehk virtuaalne privaatvõrk
VV	Vabariigi Valitsus

2. Küberturvalisuse kulude hetkeolukorra kirjeldus

2.1 Küberturvalisuse mõiste määratlus

Küberturvalisuse mõistel ei ole erialaringkondades kujunenud ühtset definitsiooni. EL-i küberturvalisuse määrus ja teised seonduvad dokumendid defineerivad küberturvalisuse kui "tegevused, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid küberohtude eest", aga see määratlus on üldine ja jätab palju olulisi aspekte määratlemata. Juriidilises kontekstis lähtub definitsioon tihtipeale varasemast õiguskirjandusest, seevastu tehnilise valdkonna praktik võib aga määratlemisel eelistada lähtumist tehnilisest spetsiifikast. Selle tulemusena võib üsna lihtsalt juhtuda see, et sama nähtust on defineeritud erinevate praktikute poolt erinevalt ning tulenevalt vajaduste või konteksti erinevusest on võõrast määratlust raske aktsepteerida.

Jättes kõrvale definitsiooni korrektse defineerimise didaktika, siis ka käesoleva aruande uurimisteema käsitluses puudub siiani kõikehõlmav määratlus, mis sobiks kõigi küberturbe erivaldkondade katmiseks. Seda kinnitab ka Euroopa Komisjoni *Scientific Advice Mechanism* Märtsi 2017 väljaande tõdemus et „küberturvalisus ei ole selgelt piiritletud akadeemilise uurimistöö valdkond, mis sobib kergesti teaduslikuks uurimiseks. Pigem ühendab küberturvalisus paljusid distsipliine alates tehnilisest kuni käitumise ja kultuurini. Teadusuuringud muudavad veelgi keerulisemaks ohtude kiiresti arenev iseloom, kontrollitud katsete läbiviimise raskus ning tehniliste muutuste ja uuenduste tempo. Lühidalt öeldes on küberturvalisus palju enam kui teadus”².

Püüdes küberturbe tähendust määratleda sellele lähedal seisva definitsiooni „infoturvalisus“ kaudu, siis laialt on levinud arusaam (nt Forbes 2022³), et küberturvalisus on olemuslikult suuresti infoturvalisuse alamosa. Ehk kui infoturbe seondub andmete kaitsega igasuguste ohtude eest, siis küberturvalisus seondub andmete kaitsega nende digitaalsel kujul ja reeglina küberruumis⁴.

Analüüsides regulatiivsel tasandil kasutatud definitsioone, siis Eestis ja Euroopa Liidus (edaspidi EL) on olemas mitmeid regulatsioone valdkonna reguleerimiseks. Nii on olemas Küberturvalisuse direktiiv (EL 2016/1148, nn „NIS direktiiv“, mis nõuab liikmesriikidelt küberturbe strateegiat ja kehtestab koostöömehhanismid), Küberturvalisuse määrus (EL 2019/881, IKT toodete ja teenuste küberturbealane sertifitseerimine), eIDAS määrus elektrooniliste tehingute reguleerimiseks (910/2014), direktiiv 2013/40/EL (infosüsteemide vastu suunatud ründed), direktiiv EL 2019/713 (mittesularahaliste maksevahendite vastased pettused) aga lisaks ka isikuandmete kaitse üldmäärus (edaspidi GDPR).

² [Introduction \(esaforum.eu\)](https://esaforum.eu/)

³ <https://www.forbes.com/advisor/education/information-security-vs-cyber-security/>

⁴ EKI: "hiiglasuur ja peaaegu hõlmamatu võrgustikusüsteem, kuhu kuulub ka Internet". <https://eki.ee/dict/ekss/index.cgi?Q=k%C3%BCberruum>, viimati vaadatud 30.12.2022

Küberturbe definitsioone

- ▶ Info konfidentsiaalsuse, terviklikkuse ja kättesaadavuse säilitamine küberruumis (ISO/IEC 27032:2012).
- ▶ Võrgu- ja infosüsteemide turvalisuse tagamine (Küberturvalisuse strateegia 2019-2022).
- ▶ Tegevused, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid küberohtude eest (EL 2019/881 ENISA).
- ▶ Ühiskonna seisund, mida iseloomustab võrgu- ja infosüsteemi kaudu avalikku korda, isikute tervist, vara ja keskkonda mõjutavate ohtude realiseerumise madal tõenäosus, võimekus ohtudele reageerida ja leevendada ohtude realiseerumisel tekitatud kahjulikku mõju (Eesti küberturvalisuse seaduse seletuskiri).
- ▶ Tegevused, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid küberohtude eest (EL küberturvalisuse määrus).

Infoturbe definitsioone

- ▶ Teabe konfidentsiaalsuse, terviklikkuse ja kättesaadavuse säilitamine (ISO/IEC 27000:2018).
- ▶ Asutuse turvameetmete loomise, valimise ja rakendamise protsesside kogum (Vabariigi Valitsuse määrus Infoturbe juhtimise süsteem, RT I, 19.03.2012, 4).
- ▶ Süsteemile turvameetmete loomise, valimise ja rakendamise protsesside kogum. (Võrgu- ja infosüsteemide küberturvalisuse nõuded 09.12.2022 nr 121).

Lisaks on „NIS direktiivi“ alusel loodud ELi Küberturvalisuse Amet (ENISA), mille definitsiooni puhul tasub märkida, et see võtab omaks „võrgu- ja infosüsteemide kaitse“ lähenemisviisi ja seega ka CIA triadi, lisaks rõhutab ka seda, et küberjulgeolek ei kaitse mitte ainult infosüsteeme vaid ka kõiki isikuid (s.t. nii süsteemi kasutajaid kui ka kolmandaid isikuid), keda küberohud mingil viisil mõjutavad. Sarnaselt määratleb küberturvalisusena Euroopa Komisoni vastav raport kõik kaitsemeetmed ja samud, mida võetakse selleks, et kaitsta infosüsteeme ja nende kasutajaid volitamata juurdepääsu, rünnete ja kahju eest, et tagada andmete konfidentsiaalsus, terviklus ja käideldavus.⁵

Eestis on vastu võetud Küberturvalisuse seadus (2018), mille alusel on antud välja määrus võrgu- ja infosüsteemide riskianalüüsi nõuetele ning kehtestatud infoturbe standard E-ITS. Samuti on koostatud Küberturvalisuse strateegia 2019-2022, Riigi küberturvalisuse käsiraamat (2020), lisaks erinevaid juhendmaterjale RIA eestvedamisel. Täiendavalt on defineeritud küber- ja infoturvet ka rahvusvahelistes standardites, kuid ühist valdavat definitsiooni ei eksisteeri.

Ka käesoleva analüüsi raames selgus ekspertidega läbiviidud intervjuudest, et Eesti IT asutused defineerivad küberturvet/infoturvet erinevalt. Sealhulgas tõi RIA CERT välja, et nende jaoks on infoturvet ja küberturvet samatähenduslik, MKM esindajate hinnangul võiks infoturvet seonduda üksikute asutuste ning küberturvet riikliku tasandi otsustega.

⁵ „ELi küberturvalisuse poliitika tõhusust mõjutavad probleemid“, 2019. https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_ET.pdf

2.2 Küberturvalisuse kulude arvestamise lahendused

Info- ja küberturbe valdkond on ristfunktsionaalne, puudutades kogu organisatsiooni tegevusi. See on peamine väljakutse sinna kuuluvate kulude tuvastamisel ja juhtimisel, sest kulud esinevad nii organisatsiooniliste kulude juures (töötajate palgad, koolituskulud jms) kui ka tehnoloogiliste komponentide all (riistvara, tarkvara, teenused). Lisaks võivad otseselt või kaudselt infoturbega seotud kulud esineda ka IT-ga mitteseotud valdkondades (näiteks hoonete ligipääsusüsteemid, valveteenused jms).

Ka maailmas laiemalt on küberturbekulude klassifitseerimise osas tehtud vaid piiratud arvul uurin-
guid. Nii nenditakse „Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Mana-
gement”⁶ artiklis, et hetkel veel puudub standard küberturbe programmide kulude mõõtmiseks ja
kontrollimiseks, pakkudes välja NIST -i põhise kaardistuse. Brecht⁷ toob välja, et täiendavat keerukust
lisab infoturbe lai mõõde ning peidetud kulud. Lisaks on EL tasemel nenditud, et avaliku sektori kulu-
tusi küberturvalisusele on raske hinnata, kuna küberturvalisus puudutab erinevaid valdkondi ja IT-üld-
kulud ei ole sageli eristatavad⁸. Samuti on ebapiisavat ettevalmistust küberründe vastu raske kvanti-
fitseerida, sest puuduvad usaldusväärsed andmed⁹. Lisaks on oluline teadvustada, et küberturvalisus-
sega seotud kulud tekivad ka IKT valdkonnast väljaspool, ühe uuringu järgi 22% ulatuses (ENISA, NIS
Investments 2021). Näiteks ei hõlma IKT kulukontod personalikulusid, kus võivad olla küberturbe ku-
lud, sh infoturbe juht ja teised infoturbega seotud rollid.

Käesoleva analüüsi mõistes on kõige olulisem välja tuua NIS direktiivi alusel koostatava NIS investee-
ringute raport¹⁰, mis kategoriseerib kulutusi järgnevasse klassidesse:

1. Identiteedi- ja juurdepääsuhooldus (i.k. Identity and Access management / IAM);
2. Võrgu turvalisus (i.k. Network security);
3. Lõpp-punkti turvalisus (i.k. Endpoint security);
4. Andmete turvalisus (i.k. Data security);
5. Haavatavuse juhtimine (i.k. Vulnerability management);
6. Turvaanalüütika (i.k. Security Analytics);
7. Rakenduse turvalisus (i.k. Application Security);
8. Juhtimine, riski- ja vastavusjuhtimine (i.k. Governance Risk and Compliance).

Käesoleva analüüsi mõistes on kirjeldatud mudeli kitsaskohaks ülaltoodud kategooriatesse määratle-
mise alus, sest iga vastaja saab ise otsustada raporteeritavate kulude jaotuse. Arvestades, et paljud
seadmed (nt tulemüür, *switch*) ja teenused (nt pilveteenused, programmeerimisteenused) katavad
toodud kategooriatest mitmeid nimetusi, on aga kulude objektiivne jaotus keeruline ülesanne. See-
tõttu on viidatud raporti lugejal ka suur risk ekslikeks järeldusteks.

⁶ Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management, 2017. <https://arxiv.org/ftp/arxiv/papers/1707/1707.02653.pdf>

⁷ A Closer Look at Information Security Costs, 2013. https://econinfosec.org/archive/weis2012/papers/Brecht_WEIS2012.pdf

⁸ Euroopa Komisjon, COM(2018) 630 final, 2018. [https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2018/0630/COM_COM\(2018\)0630_EN.pdf](https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2018/0630/COM_COM(2018)0630_EN.pdf)

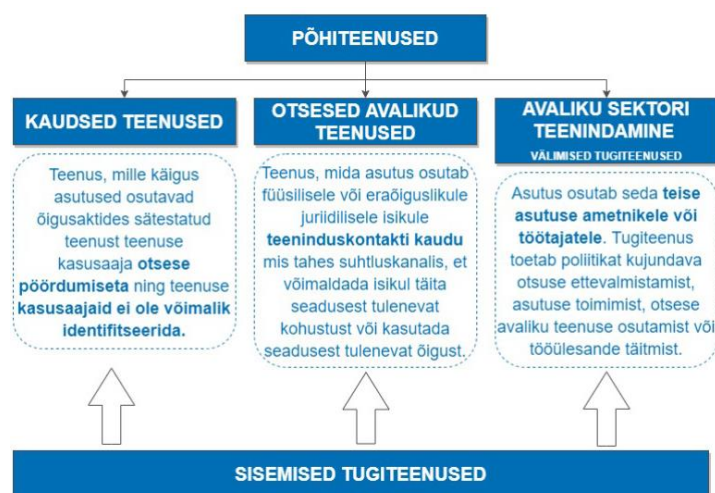
⁹ „ELi küberturvalisuse poliitika tõhusust mõjutavad probleemid”, 2019. https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_ET.pdf

¹⁰ NIS direktiiv on 2016 aastal vastu võetud esimene ELi tervikuna hõlmav küberjulgeolekualane õigusakt, mille eesmärk on suurendada küberjulgeolekut kogu ELis. NIS raporti koostamise eest vastutab ELi küberjulgeoleku asutus ENISA (European Union Agency for Cybersecurity). 2022 raport vt <https://www.enisa.europa.eu/publications/nis-investments-2022>

Hoolimata kirjeldatud puudusest, kasutab viidatud NIS raporti klassifikatsiooni ülesehitus tehnoloogiliste uuringute ja konsultatsioonide firma Gartner aruande "IT Key Metrics Data 2021: *Security Measures, Worldwide*" jaotust¹¹. Seal on infoturbe kulutused jaotatud nelja klassi - personal (2021 a, 37%), tarkvara (28%), riistvara (13%) ning välised teenused (22%). Taksonoomiliselt võiks selline kulude jaotus olla esimeses lahenduses ka lähtekohaks käesoleva analüüsi tulemusel väljapakutud kulumudelile.

2.3 Ülevaade analüüsitud IT-asutuste kulumudelitest

Eesti riigiasutused, sh IT asutused, kasutavad eelarvestamiseks ja kuluarvestuseks tegevuspõhise kuluarvestuse meetodil põhinevat Tegevuspõhise Riigieelarve (edaspidi *TERE*) mudelit. Mudelis kasutatakse eelarve planeerimiseks tulemusvaldkondi, mille arendamiseks kulutusi kavandatakse. Viimased on seotud tulemusvaldkonnaga läbi sellele suunatud teenuste, mis jagunevad põhiteenusteks ning sisemisteks tugiteenusteks (vt Joonis 1).



Joonis 1. Teenuste liigid TERE kulumodelis (<https://www.fin.ee/media/4669/download> lk 26)

TERE mudeli kohaselt arvutatakse teenuste maksumus nende osutamiseks vajalike tegevuste maksumuse kaudu, need omakorda arvutatakse vajalike ressursside kasutuse kaudu. Ressurssideks on kõik rahalise kuluga seotud hangitavad ressursid, nagu töötajate palgakulud, asutuse majanduskulud (osute teel soetatud asjad ja teenused), samuti investeeringud (jaotatakse tegevustele amortisatsiooni kaudu).

Mudeli alusel kuuluvad IKT-teenused väliste tugiteenuste gruppi, mis avalikus sektoris seonduvad eelkõige tugiteenuseid pakkuvate asutuste panusega avaliku teenuse osutamisse, mida saab käsitleda avaliku sektori teenindamisena. IKT-teenuste kohta on TERE käsiraamatus mainitud¹², et keskmise IT asutuste teenuste käsitlemine võib erineda teiste asutuste teenustest ning et seda tehakse „IKT teenuste kirjeldamise ja hinnastamise mudeli“ alusel (vt Tabel 2).

¹¹ <https://www.gartner.com/en/documents/4008848>

¹² <https://www.fin.ee/media/4669/download> lk 30

Tabel 2. Teenuste grupid IKT teenuste kirjeldamise mudelist (kinnitatud VV poolt 21.12.2017)

IKT teenuste grupp	Teenuste grupeerimise alused
1. IT Äriteenused	Spetsiifilise sisulise IT teenuse (äriteenuse) osutamiseks või ülesande lahendamiseks loodud või kohandatud infosüsteemide pakutavad teenused - sisulised tarbijale suunatud teenused ja sisemised spetsiifilised teenused ning sisemised tava-teenused
2. Tehnilised teenused	Kasutajatele tajutavate infosüsteemide toimimiseks ja selle turvalisuse tagamiseks vajalikud IT-tehnilised teenused, mida osutab IT organisatsioon ja mis tavakasutajate eest praktiliselt peidetuks jäävad. Näiteks IT taristu haldamise ja -juhtimise süsteemid, varundus, monitooring, logimine, lähtekoodide ja versioonihaldus, turvatarkvarad jne. Siia kuulub olemuselt ka spetsiifiliste ligipääsuõiguste haldus.
3. Töökoha teenused	Teenused, mis on seotud kasutaja konkreetse lokaalse töökohaga (so vahetult tema kasutuses olevad seadmed (arvuti, monitor, lisaseadmed jms) ja tarkvara), samuti töökohaarvuti ühendamine vajalike võrkudega, ühendatuse tagamine jms.
4. Välised teenused	Teenused, mida organisatsiooni liikmed enda kasutuses olevate vahenditega tarbivad teistest organisatsioonidest. Eelkõige on siin sideteenused, mida pakuvad välised organisatsioonid ja sisuteenused, nt Äriregister või autentimis- ja digitaalallkirjastamise teenused.
5. Sisemine tugiteenus	Teenused, mis peavad olema korraldatud, et IT teenuseid vajalikul viisil osutada saaks. Nt IT organisatsiooni juhtimine, mitmesuguste sertifikaatide hankimine ja auditeerimine (nt ISKE) jne.

Hoolimata TERE metoodikal põhinevate kulumudelite põhjalikkusest, puudub IT kulude tegevuspõhise eel- ja kuluarvestamise osas täna IT-asutustes ühtne praktika. Teisisõnu kasutatakse küll ühte ja sama metoodikat, kuid mudeli aluseks olevaid arvestusobjekte kasutatakse erinevalt ja erinevas tähenduses. Seega võivad sama või sarnase nimetusega teenuse maksumused klientasutustele sõltuda teenust osutavate IT-asutuste teenuste sisulisest tõlgendusest.

2.3.1 Eesti IT-asutuste finantsarvestuse, eelarvestamise ja kuluarvestuse praktika-test

IT-asutused nagu ka kõik teised riigieelarvelised asutused lähtuvad eelarvestamisel, eelarve kasutamisel, finantsarvestuse pidamisel ja kulude jaotamisel teenustele rahandusministri määrusest „Eelarveklassifikaator“¹³ (EK) ja TERE põhimõttest:

- ▶ EK-de kasutamise abil on võimalik läbi viia asutuste eelarvestamist, eelarve kasutamise jälgimist ja finantsarvestuse pidamist. Eelarvestamise käigus seostatakse EK-d tunnusena asutuse iga eelarvestatud ja jooksva tuluga ja kuluga.
- ▶ Asutuste eelarve koostamisel järgitakse TERE põhimõtteid. Selle käigus planeerivad asutused oma tegevuseks vajalikud ressursid ja nende kogused, ning asutuse kõikide ressursside maksumuste kogusumma võrdub asutuse eelarve suurusega. Detailsemalt on IT-asutustel näiteks sagedaseks

¹³ <https://www.riigiteataja.ee/akt/131122021030>. EK-d kasutatakse järgmiste arvestusobjektide juures: 1) administratiivne tunnus; 2) eelarve liik; 3) eelarve konto; 4) eelarve objekt; 5) toetus; 6) tegevusala; 7) planeerimistasand (kui asutus on üle läinud tegevuspõhisele eelarvele); 8) tehingupartner; 9) tugiteenus; 10) teenuse tegevus; 11) klient; 12) tulu-/kuluüksus; 13) projekt; 14) ressurss/kulukoht.

ressursiks serverid, mille planeeritud aastane summaarne maksumus moodustub ressursiga seostatatud kontode (nt kulum, hoolduskulud, tarkvara) maksumustest.

Nimetatud tegevuste läbiviimiseks kasutatavate lahenduste osas on käesoleva aruande kontekstis oluline välja tuua järgnevad infosüsteemid:

- ▶ Finantsarvestustarkvara SAP - raamatupidamislik kuluarvestus, eelarve täitmise aruandlus
- ▶ Kuluarvestuse Infosüsteem KAIS - koosneb kolmest tarkvarast, mida kasutatakse kulumodelite koostamisel ja haldamisel (SAS Enterprise Guide), arvutuste tegemisel (SAS Cost and Profitability Management) ning aruannete loomisel (SAS Visual Analytics).

Kulude eelarvestamine ja kuluarvestus

Kulud eelarvestatakse ja kajastatakse KAIS-is 4-kohalise kontogrupi tasandil, nt IT kulud kontogrupi 5514 tasandi detailsusega (vt ka Tabel 4), võttes selle konto koosseisu konkreetse ressursi maksumuse moodustavad kulud majandusliku sisu alusel (nt riistvara, tarvikud, tarkvara, remondi- ja hooldusteenused). Asutuse kulude jaotamiseks teenustele kasutatakse järgmisi eelarveklassifikaatoreid:

- ▶ tegevusala;
- ▶ planeerimistasand;
- ▶ tulu-/kulukeskus;
- ▶ projekt;
- ▶ ressurss/kulukoh;
- ▶ tugiteenus;
- ▶ teenuse tegevus;
- ▶ klient.

Eelarvestamisprotsessi kooskõla korral TERE metoodikaga on võimalik eelarvestatud kulude põhjal välja arvutada ka asutuse põhiteenuste maksumus¹⁴, samamoodi planeerida investeeringuid.

Kuluarvestuse tarbeks on iga asutus koostanud kulumodeli juhendi, kus on asutuse kuluarvestus detailselt kajastatud kooskõlas TERE põhimõtetega. See sisaldab (vt Tabel 3) kulude jaotuspõhimõtete/käituri kirjeldusi, sisendeid teistelt asutustelt (s.o moodul 1), otse- ja kaudkulude loetelusid, kaudkulude kogumeid, neid moodustavate ressursside jaotuspõhimõtteid ja käituri teenustele jaotamiseks, sisemiste tugiteenuste (s.o moodulist 7) maksumuste jaotamist põhiteenustele (s.o moodulisse 9).

Tabel 3. TERE moodulid

		MOODUL	MÄRKUS
SISENDID	SISESTATAVAD SUMMAD	Moodul 1	Asutuse välised kulud
		Moodul 2	Asutuse sisemised kulud
RESSURSID		Moodul 3	
		Moodul 4	
		Moodul 5	

¹⁴ See eeldab 1) asutuse poolt kasutatavate ressursside maksumuste teadmist; 2) nende ressursside jagamise kas otse või läbi mitmekordse jagamise (asutuse poolt eelnevalt määratletud jagamisreeglite/käituri alusel) kuluarvestuse moodulite põhiteenustele (moodul 9) ja klientidele (moodul 10).

TEGEVU- SED	ARVUTATAVAD SUMMAD	Moodul 6	Tugiteenuse tege- vus
		Moodul 7	Tugiteenus
		Moodul 8	Põhiteenuse tege- vus
VÄLJUN- DID		Moodul 9	Põhiteenus
		Moodul 10	Klient

Iga asutus valib ise kasutatavad ressursid, moodulid, jaotamispõhimõtted ja käituriid. Seetõttu need erinevad IT-asutuste vahel, mis omakorda mõjutab ka teenuste maksumuse arvutamist.

Finantsarvestus

Asutuste raamatupidamist reguleerib „Avaliku sektori finantsarvestuse ja -aruandluse juhend“¹⁵, kus tehingute kajastamiseks kasutatakse kuuekohalisi kontosid¹⁶. Selle järgi kajastatakse tööjõukulud kontoklassis 50, majandamiskulud kontoklassis 55, (muud) tegevuskulud kontoklassis 60, amortisatsioon kontoklassis 61. Materiaalset põhivara kajastatakse kontorühmas 155 ja immateriaalset kontorühmas 156.

Asutuse jooksvad kulud kajastatakse finantsarvestuses SAPi tarkvaras kas 6 või 8-kohalistel (alam)kontodel. SAPist liiguvad andmed jooksvalt KAISI. Kuna finantsarvestuses kasutatavad kontod on seotud eelnevalt määratletud eelarvestamisel kasutatavate ressurssidega, siis moodustuvad samade tegelike kulude pealt jooksvalt (varem eelarvestatud) ressursside tegelikud maksumused. Kasutades eelnevaid ressursside otse (otsekulude puhul) või mitmekordseid jagamisi (kaudkulude puhul) mitmetes moodulites, kanduvad need kulud lõpuks põhiteenuste maksumustesse (s.o moodul 9). Nii on võimalik jälgida põhiteenuste tegeliku maksumust, mis majandusliku sisu järgi moodustub tööjõu-, majanduskuludest ja amortisatsioonist.

IKT-ga seotud põhivarasid kajastatakse allolevas tabelis (Tabel 4) olevatel kontodel.

Tabel 4. Riigi raamatupidamise kontoplaani kontoklassi 15 ja kontode väljavõte

Konto nr	Nimetus
155500	Info- ja kommunikatsioonitehnoloogia seadmed soetusmaksumuses
155510	Info- ja kommunikatsioonitehnoloogia seadmete kogunenud kulum
156000	Tarkvara soetusmaksumuses
156010	Tarkvara kogunenud kulum

IKT kuludid kajastatakse täna riigi raamatupidamise kontoplaani kohaselt majandamiskulude (konto-klass 55) IKT kontogrupis (5514). Nendel kontodel on IKT kulud eristatud järgmiselt (vt **Error! Reference source not found.** 5):

Tabel 5. Riigi raamatupidamise kontoplaani kontogrupi 5514 ja kontode väljavõte

¹⁵ <https://www.riigiteataja.ee/akt/12874684?leiaKehtiv>

¹⁶ Kontode koodid koosnevad järgmistest osadest: 1 - konto liik, 2 - kontoklass, 3 - kontorühm, 4 - kontogrupp, 5 - kontogrupi alamgrupp, 6 - konto. 7 - alamkonto grupp. 8 - alamkonto.

Konto nr	Nimetus
551400	Infotehnoloogiline riistvara ja tarvikud
551401	Kommunikatsioonitehnoloogiline riistvara ja tarvikud
551410	Info- ja kommunikatsioonitehnoloogiline tarkvara
551460	Remondi- ja hooldusteenused
551480	Info- ja kommunikatsioonitehnoloogilise riist-ja tarkvara rent ja majutusteenus
551485	Info- ja kommunikatsioonitehnoloogiline arendustöö
551490	Muud info- ja kommunikatsioonitehnoloogilised kulud

ITK-ga seotud riistvarade ja tarkvarade amortisatsiooni kajastatakse tabelis olevatel kontodel (vt Tabel 6).

Tabel 6. Riigi raamatupidamise kontoplaani kontoklassi 61 ja kontode väljavõte

Konto nr	Nimetus
611500	Info- ja kommunikatsioonitehnoloogia seadmete amortisatsioon
613000	Tarkvara amortisatsioon

Iga asutus otsustab ise oma IKT-kulude jaotuse antud kontogrupi sees. Seetõttu võivad sisuliselt sarnased kulutused olla erinevates IT-asutustes klassifitseeritud erinevalt, mõjutades omakorda detailsete kulugruppide, sh infoturbekulude, aruandluste omavahelist võrreldavust.

2.3.1.1 Rahandusministeeriumi info- ja tehnoloogiakeskus (RMIT)

Asutuse taust ja teenused

RMIT pakub IT teenuseid Rahandusministeeriumile, Rahapesu Andmehüroole, Maksu- ja Tolliametile, Statistikametile, Riigi Tugiteenuste Keskusele ja Riigi Info- ja kommunikatsioonitehnoloogia Keskusele. Lisaks on portfellis erinevate valitussasutuste välisveebid, millele pakutakse pilvetehnoloogial valitusportaali platvormi majutus- ja haldusteenuseid.

RMITi põhiteenused panustavad riigi tasandil Halduspoliitika programmi. Põhiteenuse kulud tekivad moodulis 9 ja eelneva programmi (mis jaguneb neljaks programmegevuseks) maksumus on RMITi põhiteenuste summa.

RMITil on ca 200 põhiteenust, millest üks põhiteenus on infoturbeteenus (joonisel 2 KT) Infoturbeteenus jaguneb tinglikult RMITis alamteenusteks:

- ▶ arvutitöökohta infoturbe (viirusetõrje tarkvara, lõppkasutaja koolitused. See teenus läheb lähiajal RITI);
- ▶ perimeetri kaitse (tulemüürid, logimislahendused);
- ▶ õiguste haldus (andmekogude registreerimine).

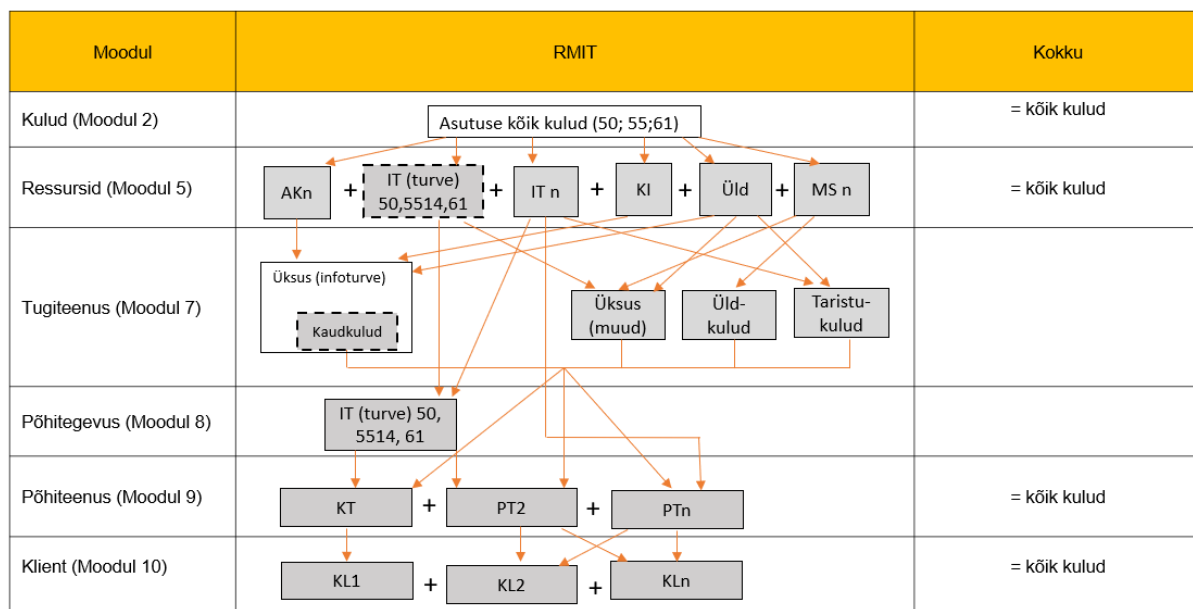
Käesoleval hetkel on RMITi infoturbe põhiteenus eraldi põhiteenus, lähituleviks on plaanis infoturbe kulud jaotada kõigile põhiteenustele ja seda eraldi põhiteenusena mitte käsitleda.

Kulumudeli kirjeldus

Jooksvalt, kulude tekkides konteeritakse kõik kulud mis panustavad infoturbesse vastavatele infoturbe ressursikoodidele ja saavad külge vastavad ressursikoodid. Ressursikood on seotud struktuuriüksuse koodiga. Samuti kõigi töötajate, kes panustavad infoturbesse, tööjõukulud konteeritakse infoturbeosakonna ressursikoodidele (moodulis 5). Kui töötaja ei tegele 100% infoturbega, siis töötaja tööjõukuludest konkreetne osa (panus vastavasse teenusesse osakonna juhi hinnangul, %) kantakse kuluks vastavalt infoturbe ressursikoodile.

RMIT lahenduses toimub kulude allokeerimine KAIS-infosüsteemis järgnevalt (vt ka Joonis 2 all):

- ▶ Moodulis 2 kajastatakse sisendandmetena asutuse eelarvestatud ja tegelikke kulusid ning planeeritud investeeringuid (soetusmaksumused). Moodulist 2 suunatakse summad moodulisse 5.
- ▶ Moodulis 5 (võib nimetada ka detailiseeritud eelarveks) koondatakse kõik moodulis 2 olevad asutuse (eelarvestatud või jooksvad) kulud erinevatesse ressursidesse: tööjõukulud (AK); IT kulud (IT); inventarikulud (MM); muud kulud (YY); põhivahendite amortisatsioon; investeeringud (IV); otsekulud (OK) ja käibemaks (ei jagata teenustele).
- ▶ Kulumudeli alusel kantakse moodulitest 7 ja 9 vastavalt asutuse enda kehtestatud kuluarvestuse metoodikale kulutused põhiteenustele ja tugiteenustele. RMIT-is suunatakse moodulist 5 põhiteenuste kaudkulud (ressurssidena) jaotusreeglite alusel moodulisse 7 tugiteenustele ja üldkuludele (nt asutuse juhtimine ja taristukulud) ning (põhi)teenuste otsekulud (sh infoturbeteenuse otsekulud) moodulisse 8 ja sealt edasi põhiteenustele moodulisse 9.
- ▶ Moodulis 7 kajastatakse asutuse tugiteenustega seotud summad vastavalt kaardistatud ja kinnitatud tugiteenuste nimekirjale, millest üks on infoturve.
- ▶ Moodulist 9 saadakse asutuse põhiteenuste maksumused. RMITi põhiteenuste maksumused kujunevad moodulis 5 olevatest põhiteenuse osutamiseks vajalikest otsestest ressursidest (otsekulud (OK), nt (IT) tarkvarad) ja moodulis 7 kajastatud tugiteenuste jaotatud maksumustest (kaudkulud) ja moodulis 7 kajastatud asutuse üldkuludest (nt asutuse juhtimine). Põhiteenuste hind (täiskuluna) koosneb moodulis 2 kulumudeli sisendina kasutatud kuludest majandusliku sisu järgi = tööjõukulud (kontoklass 50) + majandamiskulud (kontoklass 55) + amortisatsioon (kontoklass 61).
- ▶ Moodulis 10 leitakse asutuse põhiteenuste maksumused asutuse klientidele. Enamus teenustel on vaid üks klient. Teenuseid mida kasutab mitu klienti nagu arvutitöökoht, dokumendihaldus, e-post, telefoniraamat jne., jaotatakse klientide vahel jaotusreeglite alusel. Samal alusel jagatakse ka infoturbe teenus klientidele - domeeni kasutajate arvu järgi.



Joonis 2. Kulude allokeerimine RMIT-i kulumudelil

RMITi infoturbekulud moodustuvad punktiiriga näidatud dimensioonide summadest.

Küberturvalisuse kulude käsitlemine

RMITi struktuuris on ühe üksusena infoturbeosakond/valdkond, kes tegeleb:

1. RMITi infoturbe põhiteenuse ja teiste põhiteenuste infoturbe tagamisega (need kulud kajastatakse moodulis 5 nende põhiteenuste otsekuludena (kontoklassidest ja -gruppidest 50, 5514, 61, 15) ja
2. RMITi enda infoturvalisusega (TERE mõistes tugiteenusena osutab infoturbeteenust RMITi siseselt RMITi tugiteenustele (finants, õigus, üldjuhtimine, kommunikatsioon, personal, hanked).

RMITi infoturbeosakonna kulud on tööjõukulud (50), töötajatega seotud kulud (ruumid, koolitused), majandamiskulud, IKT kulud kontogrupist 5514 ja kulumid (61, kui põhivara soetamisel on tegemist infoturbeosakonna vastutusel oleva põhivaraga). Infoturbega seotud administreerimise, sõidukite jm kulud on üldosakonna kulud ja need jaotatakse infoturbeteenusele (moodulis 9).

RMITi info-/küberturvalisuse kulude moodustumist KAISis kirjeldab skeem (vt Joonis 2 ülal), kus RMITi infoturbe kulud moodustuvad punktiiriga näidatud dimensioonide summadest. RMITis tehtavad kulud saab KAISist kokku summeerides:

1. moodulis 5 olevad infoturbe ressursside kulud, (mis tehakse: 1) arvutitöökoha infoturbe, 2) perimeetri kaitse, 3) õiguste haldamiseks (otseste ressursside, nt infoturbe tarkvara, 5514, infoturbevarade kulumist (61), infoturbe tööjõukulud (50)) mis on infoturbe põhiteenuse otsekulud (punktiirina joonisel);
2. moodulis 7 olevad infoturbeosakonna tugiteenuse kulud (kui infoturbeosakonna kaudkulud, sisaldades kõigi infoturbega seotud töötajate, töökoha ja majandamiskulusid (55), punktiirina joonisel).

2.3.1.2 Siseministeeriumi infotehnoloogia- ja arenduskeskus (SMIT)

SMIT on suurim riigi IT-asutus, kes loob ja haldab siseturvalisuse tagamiseks vajalikke infosüsteeme Politsei- ja Piirivalveametile, Päästeametile, Häirekeskusele, Sisekaitseakadeemiale ja Siseministeeriumile. SMIT pakub teenuseid ka Siseministeeriumist väljapoole. Näiteks: Rahandusministeeriumile, Kaitseministeeriumile, Justiitsministeeriumile, Maanteeametile jne

SMIT-i teenuseportfellis on 134 IKT teenust, millest 104 põhiteenust on ainult ühele kliendile ja 30 põhiteenust jaotub rohkem kui ühe kliendi vahel. 134st põhiteenusest on 12 osutatavad Siseministeeriumi välistele klientidele.

Teenuseid osutatakse ühise standardiseeritud SLA alusel. Teenuse tingimused lepatakse iga teenuse puhul kliendiga eraldi kokku. SLA-s on toodud nii tingimused kui maksumus. Teenuse maksumus on tänu kulumudelile kliendile läbipaistev. Teenuste hinnad on kättesaadavad SMIT-i siseportaaalis.

SMIT kasutab TERE metoodikat oma põhiteenuste eelarvestatud ja tegelike maksumuste leidmiseks.

SMIT-i põhiteenused panustavad riigi tasandil Siseturvalisuse ja Sidusa ühiskonna tulemusvaldkonna programmidesse. Küberturbe on kõigi eelnevate programmide programmeerimise osa.

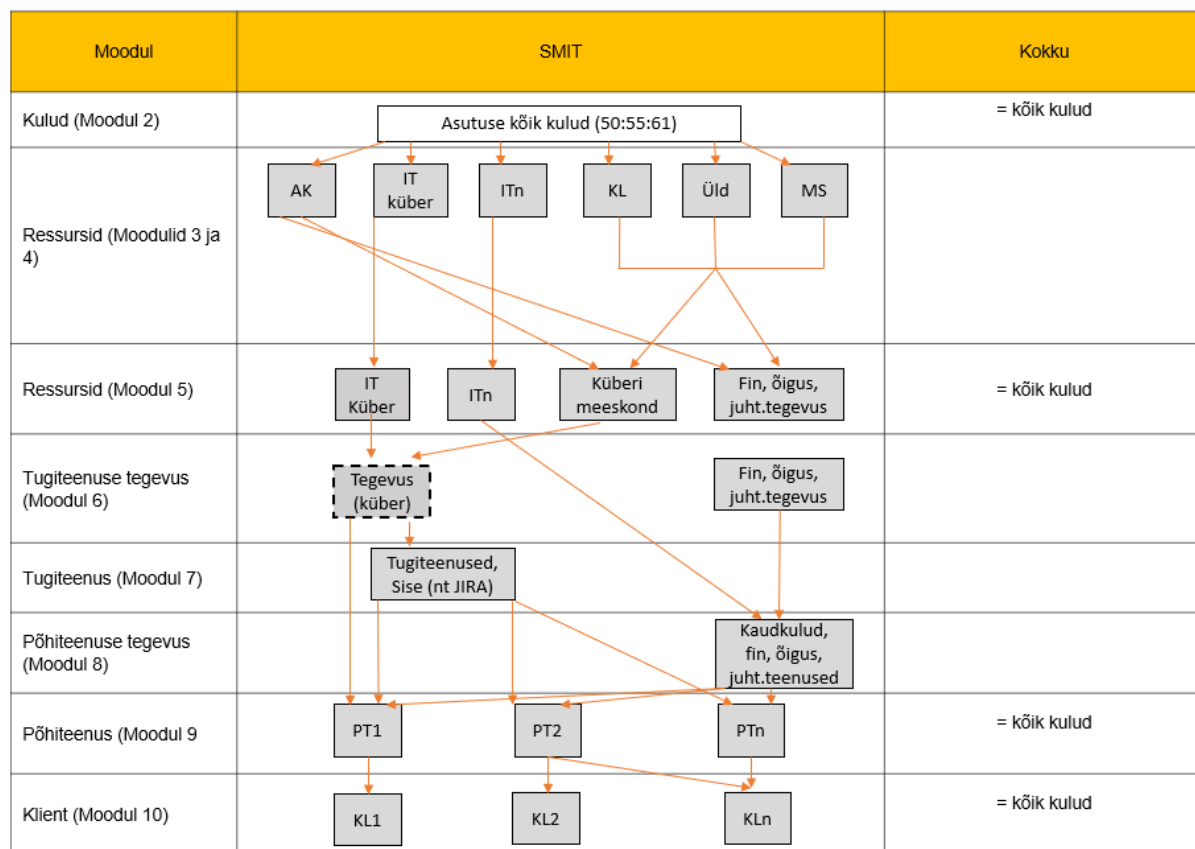
SMITil ei ole info- ja küberturbeteenus asutuse põhiteenus vaid seda käsitletakse tugiteenusena, olles üks mitmetest, põhiteenuste osutamiseks vajalikest teenuse alamteenustest.

Kulumudeli kirjeldus

Jooksvalt, kulude tekkides konteeritakse kõik kulud mis panustavad küberturbesse vastavate küberturbe ressursikoodidele. Samuti kõigi töötajate, kes panustavad küberturbesse, tööjõukulud konteeritakse küberturbeosakonna ressursikoodile. Nii SMIT-i põhiteenused kui ka põhiteenuse alamteenused/komponendid omavad üksteisest eristamiseks ja arvestuse pidamiseks oma ressursikoode/tunnuseid.

SMIT lahenduses toimub kulude allokeerimine KAIS-infosüsteemis järgnevalt (vt ka Joonis 3 all):

- ▶ Moodulis 2 kajastatakse sisendandmetena asutuse eelarvestatud ja tegelikke kulusid ning planeeritud investeeringuid (soetusmaksumuses). Moodulist 2 suunatakse summad moodulitesse 3-5.
- ▶ Moodulis 3 ja 4 jagatakse ainult töötajatega kaasnevaid kulusid (kinnisvara, koolitus, erisoodustus jne). Infoturbe kulud (meeskond, IT) liiguvad moodulist 2 moodulisse 5.
- ▶ Moodulis 5 on ressursidena (põhi- ja tugi)teenuste otsekulud ja SMIT-i tugiüksused (nt küberturbe, finants-, õigusosakond, edasi liiguvad ressursid tugiteenuse tegevuse moodulisse 6.
- ▶ Moodulis 6 on lisaks eelnevalt ka põhiteenuste ressursside kulud.
- ▶ Küberturbeosakonna kulud liiguvad moodulist 6: a) moodulisse 7 sise/tugiteenustele ja b) põhiteenustele põhiteenuste moodulisse 9 hinnaindeksi (SMIT-i loodud näitaja, mis arvestab kliendi serveriressursi kasutust (protssori võimsus, mälu, kettamaht)) alusel.
- ▶ SMIT-i teiste tugiteenuste (kaudsed) kulud (asjaajamine, finants, haldus, kommunikatsioon, personal, strateegia, õigus- ja hanked, üldjuhtimine) koondatakse tugiteenuste tegevustena moodulisse 6 ja need jagatakse moodulist 8 edasi ainult põhiteenustele (moodul 9), põhiteenuste maksumuste alusel.
- ▶ Moodulis 9 tekivad põhiteenuste täiskulud (põhiteenuste otsekulud ja asutuse kaudkulud), mis jõuavad edasi moodulisse 10, kus selguvad kulud kliendi kohta üldjuhul klientide kasutajate arvu alusel.



Joonis 3. Kulude allokeerimine SMIT-i kulumudelil

SMITi küberturbe kulud moodustuvad punktiiriga näidatud dimensiooni summast.

Küberturvalisuse kulude käsitlemine

SMITi struktuuris on ühe üksusena küberturbeosakond (kajastatakse moodulis 6, küberturbe tugiteenuse tegevusena), kes tegeleb:

1. SMITi põhiteenuste küberturbe tagamisega, kasutades selleks kulusid mis moodustuvad kontogrupidest: 50, 55, 61 (näiteks põhiteenuste küberturvalisuse tagamiseks kasutatavad serverid ja tarkvarad, töötajatega kaasnevad kulud). Need kulud liiguvad moodulitest 3, 4 ja 5 moodulisse 6 (küberturbe tugiteenuse tegevusele) ning
2. SMITi enda küberturvalisusega (TERE mõistes tugiteenusena osutab küberturbe teenust SMITi siseselt SMITi tugiteenustele - (nt JIRA, ametnike register jne)).

Küberturbeosakonna kulud (moodulis 6) tekivad eelnevast kahest kulugrupist (põhiteenuste otsestest küberkuludest (riist - ja tarkvara) ning küberturbeosakonna kuludest. Kokku on moodulis 6 küberturbe tööjõukulud, tööjõuga seotud ruumikulud, tervishoid, erisoodustusega seotud kulud, administreerimiskulud, sõidukite majandamiskulud, koolituskulud, IKT kulud kulugrupist 5514 ja kulumid (61, kui põhivara soetamisel on tegemist küberturbeosakonna vastutusel oleva põhivaraga) ja mida kasutatakse ka põhiteenuste osutamisel.

SMITi küberturbe kulud tekivad summeerides kõik küberturbeosakonna kulud moodulis 6 (punktiirina joonisel 3 ülal). **Error! Reference source not found.**

2.3.1.3 Riigi Infosüsteemi Amet (RIA)

Asutuse taust ja teenused

RIA on MKM-i valitsemisalaselle kuuluv riiklik kompetentsikeskus, kes arendab ja haldab digiriigi keskeid tehnoloogilisi platvorme ja tagab riigi küberturvalisust.

RIA-l on põhiteenuseid 76, sh TERE teenuseid 14, mille hulgas on kolm küberturvalisuse põhiteenust (vt Joonis 4 KÜ1-KÜ3, suunatud kõik avalikule sektorile):

- ▶ infoturbe meetmete arendamine,
- ▶ intsidentide ja kriiside ennetamine, valmisolek ja haldamine ning
- ▶ küberturbe analüüside ja uuringute teostamise korraldamine.

Nii RIA põhiteenused kui ka põhiteenuse alamteenused/komponendid omavad üksteisest eristamiseks ja arvestuse pidamiseks oma ressursikoode/tunnuseid. RIA põhiteenused panustavad riigi tasandil Digiühiskonna ja Teadmussiirde programmidesse ja nende programme programmegevustesse.

Kulumudeli kirjeldus

Jooksvalt, kulude tekkides, kõik kulud mis panustavad programmegevustesse, kaasa arvatud eelpool mainitud kolme küberturvalisuse põhiteenusesse, identifitseeritakse ja konteeritakse vastavate dimensiooni tunnustega nagu:

1. kuluüksuse tunnus (KN algusega);
2. ressursikood (sõltub kulu omadustest, sisust, eesmärgist);
3. GRANT (Tunnus välisvahenditele, et siduda kulu konkreetse tegevusega, milleks raha on eraldatud);
4. vajadusel WBS (*Work Breakdown Structure*) tunnus (identifitseerides üksuste üleselt ühesuse sisu ja ressursi tunnusega kulusid, mille tarvis puudub eristav konto või muu dimensioon. Näiteks litsentsid, tugi, optika, Ddos jne).

Kande juures olevad tunnused määravad ära, millistesse moodulitesse ja millistele ressursitunnustele kulud suunduvad. Sarnaselt majandamiskuludele (kontoklass 55) lisatakse töötajate tööjõukuludele (Konto 50) täiendavad tunnused nagu kuluüksuse tunnus, Grant tunnus, kui töötaja panustab konkreetse välisprojekti ja ressursi tunnus, kui tegu on sisemise üksusega, millel on all *teamid*, mis on seotud konkreetse tegevusega nagu näiteks hanke *team* adminosakonnas või arvutitöökoha *team* tehnoloogia osakonnas. Kui töötaja ei tegele 100% küberturbe tegevustega, siis töötaja tööjõukuludest konkreetne osa (panus vastavasse teenusesse osakonna juhi hinnangul, %) kantakse kuluks kas vastava küberturbe ressursikoodile või siis teisele tegevusele, mis ei ole küberturbe tegevus.

Küberintsidentidega seotud üksuse töötajate tööaeg jaguneb osakonna poolt pakutavate teenuste tegevuste vahel nagu küberruumi seire, *red teaming*, küberintsidentide ennetamine, lahendamine, SOC.

RIA puhul toimub kulude allokeerimine kulumudelis järgnevalt (vt ka Joonis 4 all):

Moodulis 2 kajastatakse sisendandmetena asutuse eelarvestatud ja tegelikke kulusid ning planeeritud investeeringuid (soetusmaksumuses). Moodulist 2 suunatakse summad järgnevatesse moodulitesse.

RIA struktuuris on ühe üksusena küberturvalisuse teenistus (KTT ja mis pakub põhiteenuseid ja mille kulud on moodulites 3 ja 5) ja mille alla kuuluvad struktuuriliselt:

1.Intsidentide käsitlemise osakond (CERT üksus), kes tegeleb küberturvalisuse tagamisega programmi tegevuse tasandil.

2.Riigi Infoturbe meetmete osakond (RIMO üksus), kes panustab küberturvalisuse tagamisse.

3.Analüüsi ja ennetus osakond (AEO üksus), kes panustab küberturvalisuse tagamisse ja suundumuste, riskide ja mõjude analüüsivõime arendamise.

4.Kriitilise info infrastruktuurikaitse osakond (KIK üksus), kes panustab küberturvalisuse tagamisse.

5.Järelvalve osakond (JVO üksus), kes panustab küberturvalisuse tagamisse.

Lisaks küberturbeteenistusele on küberturvalisusega seotud ka alustaristu tegevust pakkuv infoturbe osakond, kes tegeleb küberturvalisuse kaitsmisega ja tema tegevusteks on infoturbe (kontoklassid 50, 55, 61), füüsiline turve (50, 55, 61. Keskendub füüsilise vara turvamisele) ja riskihaldus (55).

IT üksuse kulud jaotatakse enne põhiteenustele jaotamist ühes osas alustaristu tegevustele (moodulisse 4) ja teises osas suunatakse moodulisse 5 vastavas üksuse tunnusega kulugruppi sisuteenustele kasutuse osakaalu (%) alusel. Riskihaldus käitub nagu tugiteenus ja liigub (moodulist 3) moodulisse 7, teiste tugiteenuste koosseisu.

Moodulis 3 koondatakse kokku kõik IT üksuse enda tegevuse kulud (kontoklassid 50,55,61) kulud. Moodulis 4 lisanduvad neile adminüksuse halduskulud, üldkulud (tegemist on RIA tasandi kuludega, mis jaotatakse neile tegevustele/osakondale, kes kasutavad oma tegevuse tarbeks ruume, elektrit jne, vastavalt sellele mida nad kasutavad) ja alustaristu kulud (alustaristut pakkuvate kulude kogumist jagatakse IT üksusele vaid see osa, mida nemad kasutavad).

Moodulist 3 suunduvad IT kulud Moodulisse 4, 52% ulatuses Infoturbele (millele lisandub moodulis 4 veel alustaristu kulude osa ja liiguvad koos moodulisse 5, AKN50 ressursigrupile) ja 48% ulatuses alustaristu tegevustele(, mis liigub edasi IAAS ressursidele moodulisse 5).

Moodulis 3 olevaid infoturbe ja füüsilise turbe kogutud kulusid võib lugeda 52% ulatuses põhiteenuste otsesteks kuludeks ja määrata selle tegevuse kogumaksumuse. Moodulis 4 on neile lisandunud kaudsed kulud ümberjagamise käigus ja tegevus saab tervik maksumuse (sisaldades ka IT üksusele jaotatud adminüksuse halduskulusid jm).

Seega moodulis 5 sisuteenustele jagunev kogukulu sisaldab nii üksuse enda kõiki kulusid kui alustaristult saadud kulusid.

Moodulis 5 olevatest muudest otsekuludest (skeemil OK, muu) läheb küberi vastavale teenusele ressursikoodiga OKN-50-TP tähistatu. Muu tähistusega otsekulud lähevad teistele põhiteenustele.

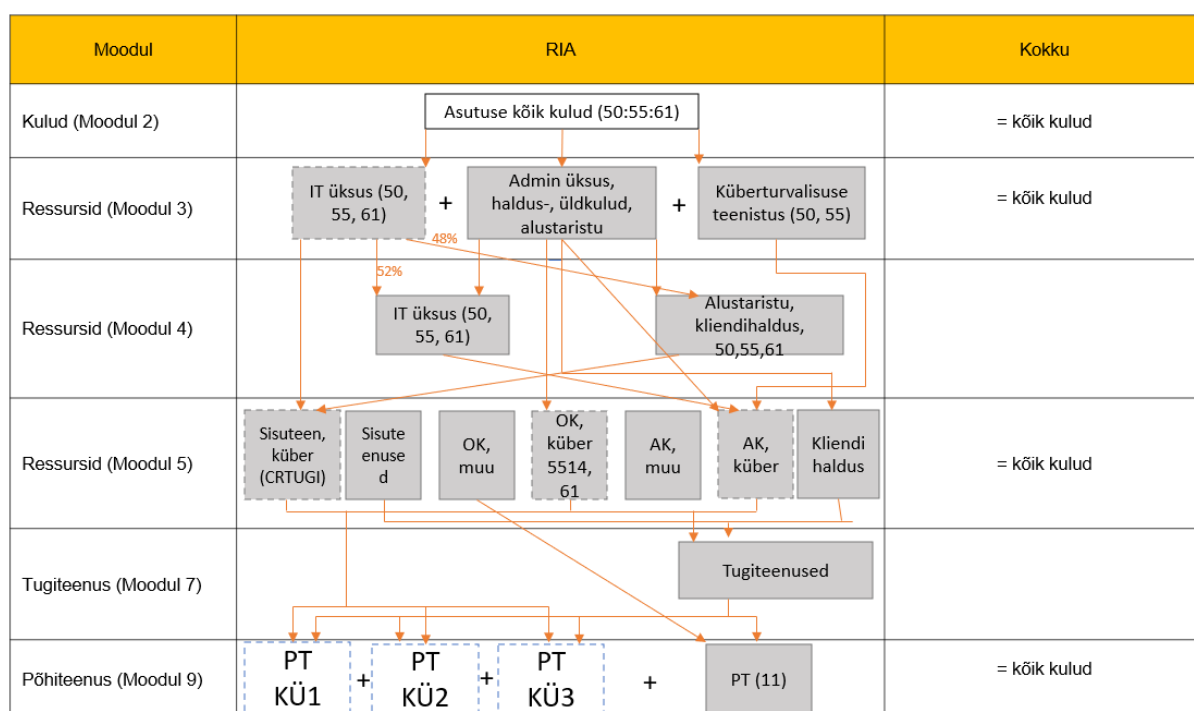
Moodulis 5 kasutusel olevad ressursikogumid on järgmised:

1. Otsekulud tunnuse algusega OKN on teenuse koodiga seotud ja ainult ühte teenusesse suunduvad kulud.
2. IAAS tunnuse algusega (erinevad grupid) on alustaristu tehnoloogiakulude kogumid, mis on suunatud konkreetsele teenusegrupile ning jaguneb selle alla kuuluvate teenuste vahel kasutuse osakaalu alusel.
3. CRT tugi(BT-CRTUGI), Bürokrati tugi (BT-JUT) ja RP tugi (BT-KKJUHT) tegevuste kulud suunduvad vastavalt CERT osakonna, Bürokrati osakonna ja Riigiportaali osakonna teenustele vastavalt juhataja hinnangule.
4. Klienditoe tegevused I_tugi, II_tugi ja III_tugi, kogutud kulude suunamise aluseks põhiteenustele on pöördumiste arv igas grupis.
5. Ametikoha koondatud kulud tunnusega AKN, mille oluliseks dimensiooniks on kuluüksuse tunnus, mis võimaldab koondatud kulud edasi jagada teenusele tööajamahu alusel.
6. Tugiteenuste tegevused nagu Juhtimine, Rahvusvahelised suhted, personali tegevus, riskihaldus, protsesside juhtimine suunduvad moodulisse 7 tugitegevustele.

7. Infoturbe, füüsilise turbe, kliendihalduse ja MSN kulud liiguvad vastavalt üksuse tunnusele edasi üksuse poolt pakutavatele põhiteenustele moodulisse 9.

TERE metoodika järgi kajastatakse moodulis 7 asutuse tugiteenustega seotud summad vastavalt kaardistatud ja kinnitatud tugiteenuste nimekirjale. RIA kulumudelil on kasutusel 15 tugiteenust, millest üks on IT üksuse koosseisus olev riskihaldus. Moodulist 7 suunatakse tugiteenuste summad RIA loodud jaotusreeglite alusel põhiteenustele, moodulisse 9. Jaotuse aluseks on põhiteenuste kulude suurus enne tugiteenuste kulude jaotust.

TERE metoodika järgi leitakse moodulis 9 asutuse põhiteenuste maksumused (täiskuluna). RIA põhiteenuste (sh kolme küberturvalisusega seotud põhiteenuse) maksumused kujunevad moodulis 5 olevatest põhiteenuse osutamiseks vajalikest ressursi gruppidest ja mooduli 7 tugiteenuste kuludest. TERE metoodika järgi leitakse moodulis 10 asutuse põhiteenuste maksumused asutuse klientidele. RIA ei kasuta moodulit 10 ega ei jaga oma kulusid klientidele põhjusel, et RIA klientideks on avalikõiguslikud asutused, kellega RIA ei arvelda.



Joonis 4. Kulude allokeerimine RIA kulumudelil

RIA küberturbe kulud moodustuvad musta värvi punktiiriga (vt Joonis 4) näidatud dimensioonide summadest. Alternatiiviks oleks ka küberturbe kättesaamine kolme küberpõhiteenuste maksumuse (sinise punktiiriga) summana, kuid see ei sisalda ühte osa nendest küberturbe kuludest, mis on seotud RIA enda küberturvalisusega (CRTUGI, sest see jaguneb ka ülejäänud 11-le TERE põhiteenusele). RIA küberturvalisuse kulud on RIA kõigi IKT põhiteenuste oluliseks komponendiks (näiteks pakub RIA riigi kesksete IT platvormidena autentimisteenuste platvormi, X-tee, riigiportaali platvormi jne). Sellest lähtuvalt on RIA infoturbe üksuse kulud seotud ka kõigi RIA IKT põhiteenustega (näiteks turvatestimised vms).

Info- ja küberturvalisuse kulude käsitlemine

RIAs tehtavad küberturbe tegevusega seotud kulud saab KAISist, kui summeerida kõik küberturbega seotud teenuste kulud, mis on:

1. IT-üksuse kulud mis on moodulis 3 (sisaldavad kontosid klassidest 55, 50, 61);
2. otsekulud (OK algusega tunnused kontogruppidest 5514 ja 61, nt infotehnoloogilised arendustegevused ja varad (ei lähe OK-ile)) moodulis 5 (musta punktiirina joonisel 4);
3. küberturbega seotud ametikohtade kulud st kõik töötajatega seotud kulud sh tööjõukulud, ruumide kulud, arvutitöökohta kulud (kontoklassidest 50 ja 55) moodulis 5 (musta punktiirina joonisel 4). Need kulud kantakse põhiteenustele vastavate töötajate panuse osakaalu alusel küberi põhiteenustesse.
4. RIA enda küberturvalisuse kulud moodulis 5 (CRTUGI).

2.3.1.4 Riigi Info- ja Kommunikatsioonitehnoloogia Keskus (RIT)

Asutuse taust ja teenused

Majandus- ja Kommunikatsiooniministeeriumi hallatava asutusena loodud Riigi IKT Keskus (RIT) osutab arvutitöökohta- ja serveri baastaristu teenuseid riigis. RIT on keskne asutus, mis osutab teenuseid ligikaudu kahekümne viie tuhandele avaliku sektori töökohale.

RIT kasutab TERE metoodikal põhinevat kulumudelit oma põhiteenuste eelarvestatud ja tegelike maksumuste leidmiseks. RIT-il on kulumudelis põhiteenuseid defineeritud 3 - arvutitöökohta (ATK) teenus, serveri alustaristu teenus (SAT) ja kesksed tugiteenused.

ATK ja SATi põhiteenustele on alamteenusteks/sisendkomponentideks infoturbe osas vastavalt ATK infoturbe ja SAT infoturbe. RITi kaks põhiteenust (ATK ja SAT) panustavad riigi tasandi programmi: IKT alusteenuste keskne osutamine. See kuulub tegevuse: digiriigi alusbaasi kindlustamine alla. Kahe põhiteenuse kulud tekivad moodulis 9 ja programmi: IKT teenuste keskne osutamise maksumus, on kahe põhiteenuse (ATK) ja (SAT) summa.

RITi infoturbe ei ole asutuse põhiteenus ja on üks mitmetest, eelneva kahe esimese põhiteenuse osutamiseks vajalikest teenuse alamteenustest. Näiteks lisaks infoturbele on ATK põhiteenuse alamteenuseks töökohaarvutid ise.

Kulumudeli kirjeldus

Nii RITi põhiteenused kui ka alamteenused/komponendid omavad üksteisest eristamiseks ja arvestuse pidamiseks oma ressursikoodide/tunnuseid.

Jooksvalt, kulude tekkides konteeritakse kõik kulud mis panustavad SAT või ATK infoturbesse SAT või ATK infoturbe ressursikoodidele. Samuti kõigi töötajate, kes panustavad SAT või ATK infoturbesse, tööjõukulud konteeritakse samuti SAT või ATK infoturbe ressursikoodidele. Kui töötaja ei tegele 100% infoturbega, siis töötaja tööjõukuludest konkreetne osa (panus vastavasse teenusesse osakonna juhi hinnangul, %) kantakse kuluks vasta infoturbe ressursikoodile.

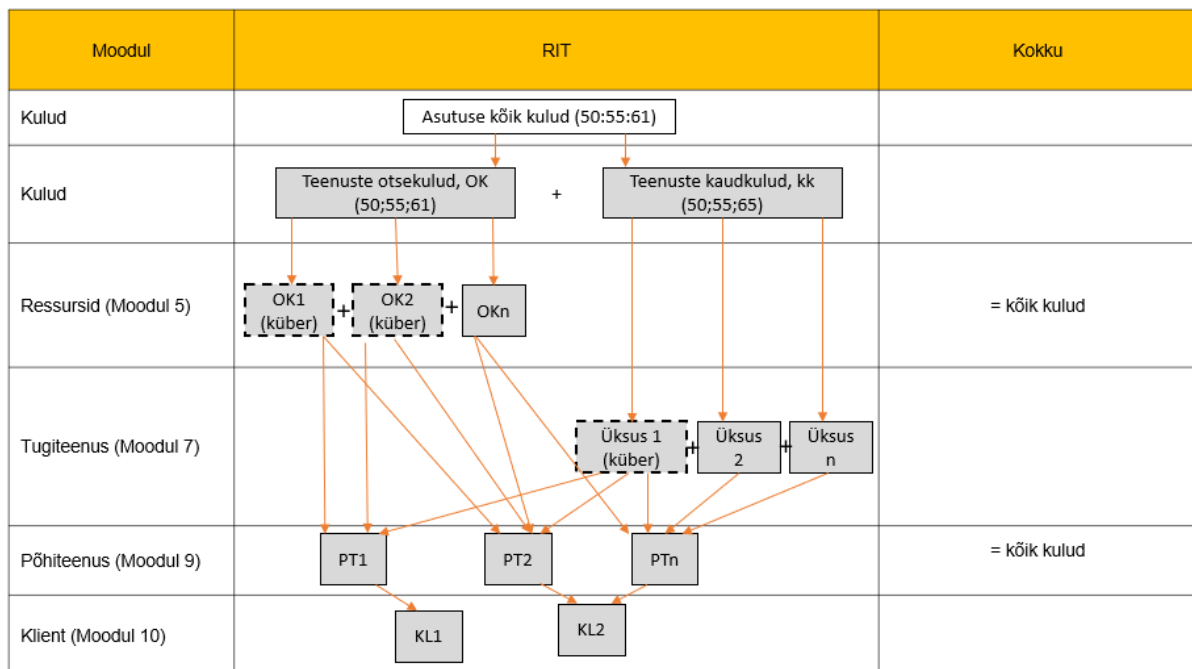
RITi igal kliendil on oma kuluüksuse kood, kuhu konteeritakse selle kliendiga seotud otsekulud (olenevatest ressursitunnusest, st sama kulu võib kanda lisaks kliendile ka SAT põhiteenuse või ATK infoturbe ressursitunnust.

RIT lahenduses toimub kulude allokeerimine KAIS-infosüsteemis järgnevalt (vt ka Joonis 5 all):

- ▶ Moodulis 2 kajastatakse sisendandmetena asutuse eelarvestatud ja tegelikke kulusid ning planeeritud investeeringuid (soetusmaksumuses). Moodulist 2 suunatakse summad moodulisse 5.

- ▶ Moodulis 5 (võib nimetada ka detailiseeritud eelarveks) koondatakse kõik moodulis 2 olevad asutuse (eelarvestatud ja jooksvad) kulud erinevatesse ressursidesse: tööjõukulud (AK); IT kulud (IT); inventarikulud (MM); muud kulud (YY); põhivahendite amortisatsioon; investee-ringud (IV); otsekulud (OK) ja käibemaks.
- ▶ Kulumudeli alusel kantakse moodulitest 7 ja 9 vastavalt asutuse enda kehtestatud kuluarvestuse metoodikale kulutused põhiteenustele ja tugiteenustele.
- ▶ Moodulis 7 kajastatakse asutuse tugiteenustega seotud summad vastavalt kaardistatud ja kinnitatud tugiteenuste nimekirjale, millest üks on infoturbe.
- ▶ Moodulist 9 leitakse TERE metoodika järgi asutuse põhiteenuste täiskulud (sh põhiteenuste otsekulud ja asutuse kaudkulud).
- ▶ Moodulis 10 leitakse TERE metoodika järgi asutuse põhiteenuste maksumused asutuse klientidele vastavalt konkreetse kliendi lõppkasutajate arvu alusel.

RITi igal kliendil on oma kuluüksuse kood, kuhu konteeritakse selle kliendiga seotud otsekulud (olenevatest ressursitunnusest, st sama kulu võib kanda lisaks kliendile ka SAT põhiteenuse või ATK infoturbe ressursitunnust. Kui kliendiga X seoses on tehtud mingi infoturbe kulu (kandele lisatud nii kliendi kui infoturbe tunnus), siis saab selle kliendi infoturbe kulu kätte infoturbe ressursitunnuse abil.



Joonis 5. Kulude allokeerimine kuluarvestuse infosüsteemis KAIS: RIT

RITi infoturbe kulud moodustuvad punktiiriganäidatud dimensioonide summadest.

Info- ja küberturvalisuse kulude käsitlemine

RITi struktuuris on ühe üksusena infoturbeosakond, mis tegeleb:

1. ATK ja SATi infoturbe tagamisega (need kulud kajastatakse nende teenuste otsekuludena (kontoklassid 50, 55, 61) ning

2. RITi enda küberturvalisusega (osutab infoturbe teenust RITi siseselt RITi tugiteenustele (finants, õigus, üldjuhtimine, kommunikatsioon, personal, hanked) ja sisu põhiosakondadele (arvutitöökoha osakond, tehnoloogia osakond jne)).

Infoturbeosakonna kulud on tööjõukulud, administreerimiskulud, sõidukite majandamiskulud, koolituskulud, IKT kulud kontogrupist 5514 ja kulumid (kui põhivara soetamisel on tegemist infoturbe osakonna vastutusel oleva põhivaraga). Infoturbeosakonna kulud teiste RITi tugiteenuste toetamiseks ei ole SAT ja ATK infoturbe otsekulud.

RITi küberturvalisuse kulude moodustumist KAISis kirjeldab skeem (vt Joonis 5 ülal), kus RITi infoturbe kulud moodustuvad punktiiriga näidatud dimensioonide summadest. RITi infoturbe kulud saab kokku summerides:

1. kõik kulud mis kannavad (eelnevalt kirjeldatud) infoturbeosakonna kuluüksuse tunnust (moodulis 7 – tugiteenus, punktiirina joonisel 5) ja
2. kõik kulud mis on SAT ja ATK infoturbe otsekulud (OK ressursitunnusega, punktiirina joonisel 5) sh SAT ja ATK infoturbega tegelevate töötajate (kes RITi struktuuri järgi kuuluvad Infoturbeosakonda) tööjõukulud, kulumid (kannavad SAT või ATK infoturbe ressursikoode) ja neil ei ole infoturbeosakonna kuluüksuse tunnust (liiguvad välja moodulisse 10 ja lähevad jagamisele klientidele vastavalt kasutajate arvu alusel).

2.3.1.5 Keskkonnaministeeriumi infotehnoloogiakeskus (KEMIT)

Asutuse taust ja teenused

KEMIT on Keskkonnaministeeriumi haldusala asutuste IT partner, mille ülesandeks on tagada IT töövahendid ja teenused haldusala töötajatele ning e-teenused avalikkusele. Ameti alla kuuluvad infoturbe-, taristu-, teenindus-, teenuste, tehnoloogia- ja õigusvaldkonnad.

KEMIT kasutab TERE metoodikal põhinevad tegevuspõhist kulumodelit oma põhiteenuste eelarvestatud ja tegelike maksumuste leidmiseks. KEMIT-i kuluarvestuse aluseks on ressursikoodid, millega on konteeritud kõik kulud, kaasa arvatud põhivarade soetus. Põhivarade amortisatsiooni arvestus on ressursikoodi põhine.

KEMIT-il on põhiteenuseid ca 150, mille moodustavad peamiselt infosüsteemid. KEMIT-i põhiteenused panustavad läbi Keskkonnaministeeriumi hallatavate asutuste põhiteenuste riigi tasandil keskkonnakaitse ja kasutuse ning kalanduse programmi. Põhiteenuse kulud tekivad moodulis 9 ja eelnevate programmide maksumus on asutuse põhiteenuste summa.

KEMITi infoturbeteenust ei ole asutuses otseselt kirjeldatud põhiteenuse ega tugiteenusena, kuid infoturbe on kõikidesse äriprotsessidesse ja põhiteenustesse sissekirjutatud, seega saab väita, et infoturbeteenus esineb tugiteenusena *de facto*.

Kulumodeli kirjeldus

Jooksvalt, kulude tekkides, kõik kulud mis panustavad infoturbesse konteeritakse: 1) infoturbeosakonna ressursikoodile: kõigi infoturbesse panustavate töötajate tööjõukulud ja muud töötajatega seotud kulud (vt all) ja 2) põhiteenuste infoturvet tagavate ressursside (nt ITL90-TURVA) ressursikoodidele.

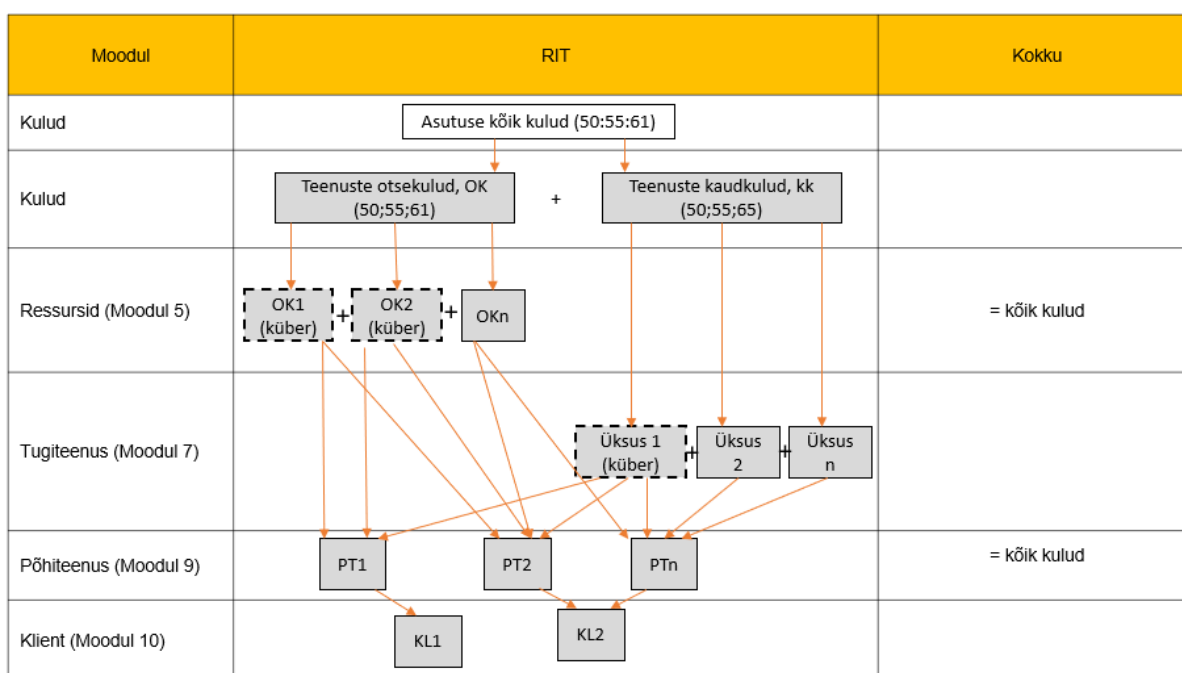
KEMIT lahenduses toimub kulude allokeerimine KAIS-infosüsteemis järgnevalt (vt ka Joonis 6):

- Moodulis 2 kajastatakse sisendandmetena asutuse eelarvestatud ja tegelikke kulusid ning planeeritud investeeringuid (soetusmaksumuses). Moodulist 2 suunatakse summad järgnevatess moodulitesse.

- ▶ Moodulis 3 jaotatakse KEMIT tugi- ja põhiteenuste osutamiseks vajalikud ressursid, mis omavad kõik konkreetset ressursitunnust. Kasutatavad ressursid jagunevad tööjooks (AK), kinnistuteks (KI), IT sh riist- ja tarkvaraks (IT) ja sõidukiteks (MS). Arvuliselt on kõige enam IT ressursse (ca 180/200). Suurem osa ressursidest (sh enamus IT ressursitunnusega ressursse, riist- ja tarkvarad) kantakse läbi moodulite 4 ja 5 otse asutuse põhiteenustele (moodul 9).
- ▶ Moodulist 4 omakorda jagunevad (kuue) infoturbe ressursid moodulisse 5, vastavalt äriteenuste ja IT- siseteenuse (siseteenus on IT-üldine teenus, mis suunatakse asutustele vastavalt asutuse töökohtade arvule) ressursidele.
- ▶ Moodulis 5 on IT ressursside jaotamise aluseks kaardistatud asutustes kasutatavad IT-äri/põhiteenused. Moodulist 5 liiguvad kliendi põhised IT ressursid moodulisse 9.

Moodulis 9 tekivad põhiteenuste maksumused (mooduli 5 ressursid), mis jõuavad moodulisse 10.

Moodulis 10 leitakse TERE metoodika järgi asutuse põhiteenuste maksumused asutuse klientidele. Igal KEMITi kliendil on oma asutuse (kuluüksuse) tunnus ja kliendile jaotatakse põhiteenuste kulud vastavalt töökohtade arvule.



Joonis 6. Kulude allokeerimine kuluarvestuse infosüsteemis KAIS: KEMIT

KEMITi infoturbe kulud moodustuvad punktiiriga näidatud dimensioonide summadest.

Info- ja küberturvalisuse kulude käsitlemine

KEMIT-i finantsarvestuses on infoturbe kulude eristamiseks klassifikaatorina kasutusel ressursitunnus „ITL90-TURVE“, mille sisuks on turvatarkvara. Seda klassifikaatorit on kasutanud peamiselt infoturbeüksus, aga ka tugi-/teenindusvaldkond. Kokku on kulu 2022. aastal olnud 70 tuhat eurot.

KEMITi struktuuris on ühe üksusena infoturbeosakond/valdkond, kes tegeleb:

- 1) KEMITi põhiteenuste infoturbe tagamisega (need kulud kajastatakse nende põhiteenuste otsekuludena moodulis 5 (55, 61), punktiirina joonisel 6) ning

- 2) KEMITi enda küberturvalisusega (TERE mõistes tugiteenusena osutab infoturbe teenust KEMITi siseselt KEMITi tugiteenustele), mis konteeritakse IT- üldkulude ressursile.

KEMITi infoturbeosakonna kulud moodustuvad tööjõukuludest (kontoklass 50), lähetuskuludest (kontogrupp 5503), sõidukite majandamiskuludest (kontogrupp 5513), koolituskuludest (kontogrupp 5504), mis kõik seostatakse moodulis 3 ühe ja sama infoturbeosakonna ressursitunnusega (AKL90TURBE). Infoturbega tegeleb seisuga 01.12.2022 5 inimest, kelle kulud pannakse IT üldkulu- desse.

Infoturbeosakonna töötajate tööaja jaotuse alusel jaotatakse KEMITi infoturbeosakonna töötajatega seotud kulud kuue erineva infoturbega seotud (IT ressursi) ressursikoodi (nt ITL90-CESA) vahel moodulis 4 (punktiirina joonisel). Moodulist 4 omakorda jagunevad (kuue) infoturbe ressursid moodulisse 5, vastavalt põhiteenuste ja IT- siseteeenuse (siseteenus on IT-üldine teenus) ressursile. See suunatakse klientidele (moodulis 10) vastavalt asutuse töökohtade arvule.

Moodulis 5 on IT ressursside jaotamise aluseks kaardistatud klientide põhiteenuste kasutatavad IT- äri/põhiteenused. Moodulis 5 on eraldi konkreetse ressursitunnusega ka põhiteenuste infoturbe taga- misega seotud infoturbe ressursid (nt ITL90-TURVA - arvutite turvatarkvara, joonisel punktiiriga).

Moodulist 5 liiguvad põhiteenuse põhised IT ressursside kulud moodulisse 9.

Tugiteenused ei ole KEMIT-i kulumudelil eraldi arvestatud. Tugiteenusena klassifitseeruvad kulud on arvestatud otse IT-üldkuludena moodulites 5 ja 9.

KEMITis tehtavad jooksvad infoturbe kulud saab KAISist kokku summeerides:

1. moodulis 4 oleva kuue infoturbe ressursi kulud (punktiiriga joonisel 6).
2. Moodulis 5 olevate põhiteenuste infoturbe tagamisega seotud infoturbe ressursid (punktiiriga joonisel 6).

Moodulis 9 tekivad põhiteenuste täiskulud (sh põhiteenuste otsekulud (mooduli 5 ressursid) ja KEMITi kaudkulud IT-üldkulude näol), mis jõuavad moodulisse 10.

2.3.1.6 Registrite ja Infosüsteemide Keskus (RIK)

Asutuse taust ja teenused

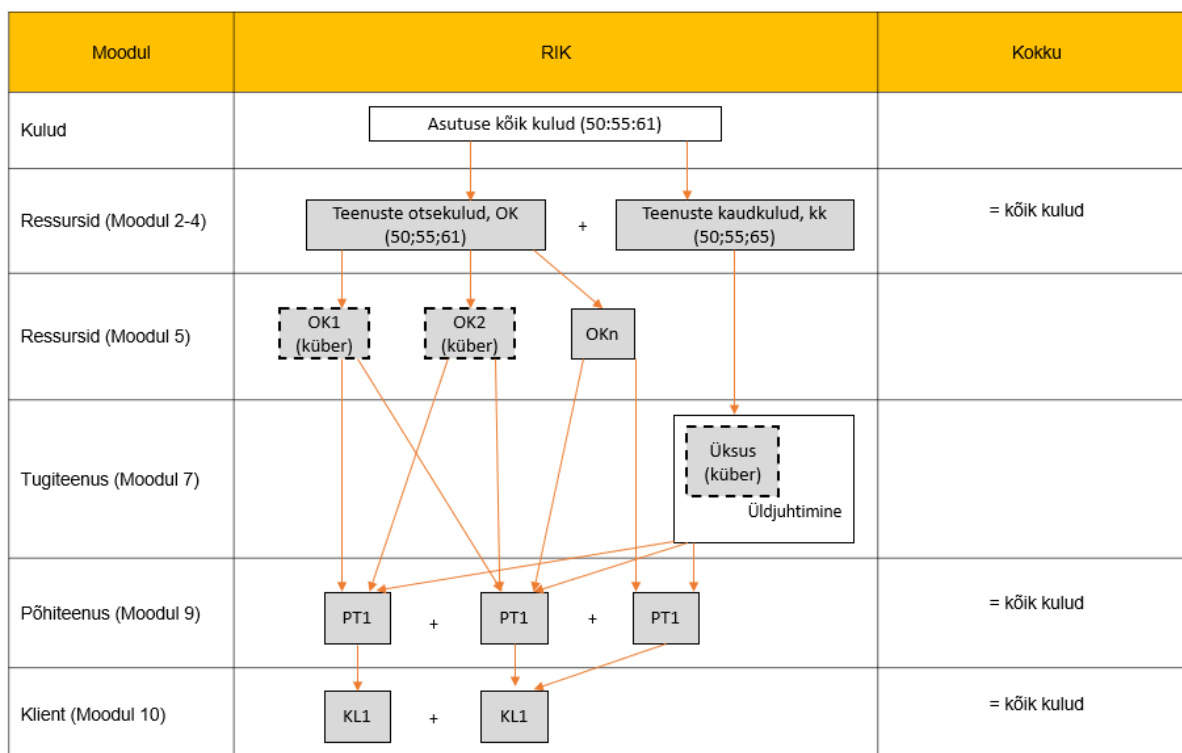
RIK on Justiitsministeeriumi haldusala asutus, mis arendab ja haldab olulisi registreid ja infosüsteeme nagu näiteks e-äriregister, e-notar, e-kinnistusraamat, kohtuinfosüsteem, kriminaalhooldusregister, kinnipeetavate register, karistusregister, e-toimik, elektrooniline Riigi Teataja.

RIKi põhiteenused panustavad riigi tasandil Justiitsministeeriumi programmi „Usaldusväärne ja tule- muslik õigusruum“ kuude programmitegevusse.

RIKil on TERE moodulis 9 ca 60 põhiteenust. Infoturbe ei ole asutuse põhiteenus, see on on RIKi tugiteenus.

Kulumudeli kirjeldus

Jooksvalt, kulude tekkides konteeritakse kõik kulud mis panustavad infoturbesse vastavate infoturbe ressursikoodidele (saavad külge vastavad ressursikoodid). Samuti kõigi töötajate, kes panustavad infoturbesse, tööjõukulud konteeritakse infoturbeosakonna ressursikoodile. Kui töötaja ei tegele 100% infoturbega, siis töötaja tööjõukuludest konkreetne osa (panus infoturbesse osakonna juhi hinnangul, %) kantakse kuluks infoturbeosakonna ressursikoodile.



Joonis 7. Kulude allokeerimine kuluarvestuse infosüsteemis KAIS: RIK

RIKi infoturbe kulud moodustuvad punktiiriganäidatud dimensioonide summadest.

Info- ja küberturvalisuse kulude käsitlemine

RIKi struktuuris on sisuliselt ühe üksusena infoturbeosakond, kes tegeleb:

1. põhiteenuste infoturbe tagamisega (need kulud kajastatakse võimalusel nende teenuste otsekuludena (kontoklassidest 50, 55, 61)) moodulis 5 ning
2. RIKi enda infoturvalisusega ja osutab infoturbe teenust RIKi siseselt RIKi tugiteenustele mis on sisuliselt RIKi üldjuhtimise koosseisus.
3. kogu Justiitsministeeriumi valitsemisala infoturbega seotud teemadega.

Infoturbeosakonna kulusid eristatakse konkreetse kuluüksuse koodiga aga ei eristata konkreetse ressursi tunnusega (ressursse (kulukohti) võib olla mitu, sõltuvalt sellest, kuidas on soovitud infoturbega seotud kulusid jagada (nt. võrguturbe ja monotooring, infoturbe juhtimine)).

Infoturbeosakonna kulud on RIKi üldjuhtimise koosseisus, mis TERE mõttes on tugiteenus. Üldjuhtimise ja sh Infoturbeosakonna kulud on tööjõukulud (50), administreerimiskulud (55), koolituskulud, IKT kulud kulugrupist 5514 ja kulumid (kui põhivara soetamisel on tegemist infoturbe osakonna vastutusel oleva põhivaraga). Hetkel veel IT infoturbeosakonnale ruumide jm ei lisata, aga seda on plaanis lähiajal muuta. Arvutitöökohta kulusid üldjuhtimisse ja sh infoturbeosakonnale ei lisata (need kulud tehakse RIT-is ja RIKini need summad ei jõua).

RIKi infoturbe kulud saab kokku summerides:

1. kui eristada RIKi üldjuhtimise kulude koosseisust RIKi infoturbeosakonna kulud (moodulis 7 - tugiteenus, joonisel 7 näidatud üldjuhtimise koosseisust eraldi, punktiirina) ja
2. kõik kulud mis on põhiteenuste infoturbe tagamiseks otsekulud (Moodulist 5, OK ressursitunnusega, nt mingi konkreetse süsteemi ründetestimine, punktiirina joonisel 7).

Moodulis 9 tekivad põhiteenuste täiskulud (sh põhiteenuste otsekulud ja asutuse kaudkulud üldjuhtimise näol sh infoturbeosakond). Infoturbeosakond kulud jõuavad põhiteenustesse üldkulude koosseisus kliendi arvutitöökohtade arvu alusel ja edasi moodulisse 10 kliendi kohta vastavalt konkreetse kliendi arvutitöökohtade arvu alusel.

2.3.2 Asutuste kulumudelite kokkuvõte

Kokkuvõtlikult on eelpool analüüsitud asutuste kulumodeli kirjeldatud järgmises tabelis (Tabel 7).

Tabel 7. Asutuste kulumudelite ülevaade

	KEMIT	RIA	RIT	RMIT	SMIT	RIK
Teenuste arv kulumodelis	150	76 (14)	3	200	134	60
Ressurss/kulukoht (Moodul 3)		√				
Ressurss/kulukoht (Moodul 4)	√					
Ressurss/kulukoht (Moodul 5)	√	√	√	√		√
Tugiteenuse tegevus (Moodul 6)					√	
Tugiteenus (Moodul 7)			√	√		√
Põhiteenuse tegevus (Moodul 8)						
Põhiteenus (Moodul 9)		√		√		

IT-asutuste tegevuste analüüsi tulemusena on võimalik teha alljärgnevad järeldused:

1. Tulenevalt erinevatest IT-asutuste praktikatest on isegi pealtnäha samad IT- teenused erinevad nii funktsionaalsuse kui teenuse tagamise viisi ja vahendite osas:
 - ▶ Enamikel IT-asutustel on eraldi struktuuriüksus, mis tegeleb küberturvalisusega. Kuna kulüksuse ja ressursitunnuse kasutamine on kohustuslik iga kulukande puhul, siis need võimaldavad küberturvalisuse üksusega seostada tema põhjustatud tegelikke kulusid kontodelt 50 (tööjõukulud), 55 (majandamiskulud), 60 (muud tegevuskulud) ja 61 (amortisatsioon). Asutuste puhul võivad siin esineda erisused, milliseid kulusid küberturvalisuse üksusega seostatakse otse.
 - ▶ Samamoodi võib struktuuriüksuse kaudkulude seostamine küberturvalisuse üksusega käia asutuste vahel erinevalt. On asutusi, kes lisavad kaudkulud teistele tugiteenustele ja on asutusi kes ei lisa. Teisel juhul liiguvad need otse põhiteenusele. Selline erisus kaudkulude kajastamise ja mittekajastamise osas toob kaasa selle, et ühtedel (esimesel juhul) on asutustel küberturvalisuse üksusega seostatud kaudkulud ja teistel (teise juhul) mitte. See vajab määratlust: 1) mida pidada üksuse otsekuludeks, 2) mis oleks sama põhivahendi amortisatsiooni periood (nt tule müüri eluiga võib olla ühel asutusel 5 aastat, teisel 7 aastat) ja 3) mida pidada kaudkuludeks ja kas viimaseid lugeda ka küberturvalisuse kulude hulka.

2. Riigi raamatupidamise kontoplaani kontodel toimub küll IT kulude eristamine, kuid infoturvalisusega seotud kulud eristatud ei ole. Lisaks on info- ja kommunikatsioonitehnoloogiaga (sh. infotur-bega) tegelevate töötajate tööjõukulud personalikulude hulgas, mis on eraldi kontogrupi all. See tähendab, et tänase arvepidamise praktika juures ei ole võimalik infoturbe kulusid eristada, sest oma iseloomu tõttu võivad need esineda erinevate IKT kulude koosseisus (ja ka väljaspool IKT kulusid). Näiteks võib serveri riistvara puhul selles sisalduda tarkvaraline tulemüüri komponent, mis on oma iseloomult küberturbe kulu, kuid moodustab serveri maksumusest ainult teatud väi-kese osa.

Need erisused raskendavad oluliselt üleriigilist küberturvalisuse kulude standardiseeritud lahenduse loomist. See võib kõne alla tulla kogu kuluarvestuse metoodika muutmise juures. Selles kontekstis on lähiajal võimalik küberturvalisuse kulusid kokku koondada lähtuvalt asutuste väljakujunenud ar-vestusspetsiifikast.

3. Väljapakutav kulumudel

Käesolev peatükk annab ülevaate küberturvalisuse kulumudelist kahes vaates – tehnoloogilises ja finantsvaates. Tehnoloogiline vaade käsitleb seda, kuidas infotehnoloogiliste komponentide kulude tegemisel sisuliselt liigitada ja eristada küberturvalisuse kulusid. Finantsvaade käsitleb raamatupidamislikku ja kuluarvestuslikku kulude liigitamise võimalusi.

3.1 Kulumudeli tehnoloogiline vaade

Kulumudeli tehnoloogiline vaade esitab põhimõtted, kuidas erinevaid infotehnoloogilisi kulusid ja investeeringuid sisuliselt liigitada küberturvalisuse vaates. Kui kulumudeli finantsvaade pakub lahenduse raamatupidamislikuks ja kuluarvestuslikeks käsitluseks, siis tehnoloogiline vaade on mõeldud IT kulujuhtidele sisuliseks ja eesmärgist lähtuvaks käsitluseks.

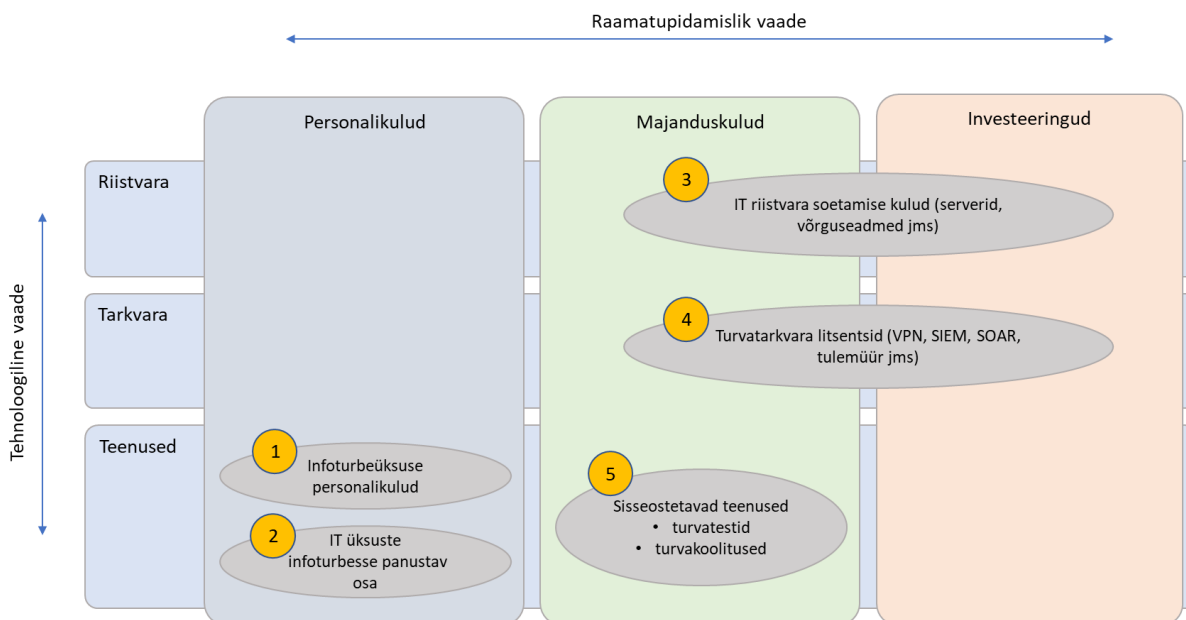
Küberturvalisuse kulude arvestamise mudeli puhul tuleb silmas pidada, et ei ole olemas ühte ja õiget kulude jaotamise loogikat, mistõttu iga kulude jaotamise põhimõtte või reegel saab olla üksnes kokkuleppeline. Selle põhjuseks on asjaolu, et küberturvalisust tagavad tehnoloogilised lahendused ja meetmed sisalduvad mingil määral praktiliselt kõigis tänapäevastes IT süsteemides ning komponentides ja nende rahaline või mahuline eristamine saab olla üksnes tinglik ja kokkuleppeline.

Sellist lähenemist toetab ka sisseprojekteeritud turbe (*security by design*) kontseptsioon, mille kohaselt on turvalisus IT süsteemide ja komponentide loomulik ning lahutamatu osa ning ei ole füüsiliselt ega finantsiliselt selgelt eraldatav. Seetõttu pakub käesolev mudel välja ühe võimaliku kokkuleppelise kulude jaotamise loogika ja selle eesmärk on, et nende põhimõtete ühtsel kasutamisel eri asutuste poolt on küberturvalisuse kulud asutuste vahe paremini võrreldavad (erinevalt olukorrast, kui iga asutus tõlgendaks kulusid oma moodi).

3.1.1 Küberturvalisuse kulude paiknemine arvestussüsteemis

Küberturvalisuse kulud tekivad asutustes tehnoloogilises ja finantsarvestuslikus vaates eri kohtades ja kujul. Näiteks tekivad kulud erinevates organisatsioonilistes üksustes – lisaks infoturbe osakonnale ka IT osakonnas. Küberturvalisuse kulude arvestamise mudeli eesmärk on koondada sellised kulud kokku olenemata sellest millises üksuses need tekivad ja millise IT varaliigi raames teda hangitakse.

Enamasti tekivad küberturvalisuse kulud järgmistes kulukohtades (vt Joonis 8):



Joonis 8. Küberturvalisuse kulude paiknemine arvestussüsteemis

1. Küberturvalisusesse panustavad personalikulud

- a. Infoturbeüksuse personalikulud (1) - infoturbe üksus on üldjuhul peamiselt infoturbesse panustav üksus, mistõttu on põhjendatud sellesse kuuluvate ametikohtadega seotud kulud (tööjõukulud, koolituskulud jms) arvestada küberturvalisuse kuludeks.
- b. IT üksuste personalikulude infoturbesse panustav osa (2) - IT üksustes töötavad spetsialistid võivad osa oma tööajast panustada infoturbesse; näiteks kuulub siia alla infoturbe tegelevate süsteemiadministraatorite tööaeg (kas osaliselt või täielikult).

2. Majanduskulud ja Investeeringud, mis panustavad infoturbesse.

- a. IT ja infoturbeüksuste poolt hangitav infoturbe seotud riistvara ja tarkvara (3, 4) - siia kuuluvad kas otseselt infoturbe jaoks mõeldud tarkvaralahendused (IDS, VPN jms) või mingiks muuks äriliseks otstarbeks loodud tarkvaras sisalduv osa, mis panustab infoturbesse.
- b. Sisseostetavad infoturbe tagamiseks vajalikud teenused (5) - siia kuuluva nt turvatestid, konsultatsioonid, turvaauditi jms)

3.1.2 IT ja küberturvalisuse kulude üldine liigitus

Vaatleme kulude liigitust kahes lõikes - eesmärgipõhises osas vaatame, kuidas eristada kulusid IT ja küberturvalisuse eesmärkidest tulenevalt. Kululiigi põhine liigitus põhineb üldistel IT valdkonna nn „IT varade“ põhisel jaotusel.

3.1.2.1 Kulude eesmärgi põhine liigitus

Kui IT kulud teenivad üldjuhul erinevaid ärieesmärke, siis küberturvalisuse kulude puhul tuleb vaadelda nende seotust turvaeesmärkide saavutamisega. Kuigi turvaeesmärke võib olla mitmesuguseid¹⁷, siis käesoleva töö puhul oli eesmärgiks eristada küberturvalisuse kulud tervikuna.

Mudel jaotab küberturvalisuse kulud esmalt kaheks – täielikult infoturbesse panustavad kulud ja osaliselt infoturbesse panustavad kulud.

1. Täielikult infoturbe tagamisse panustavad kulud

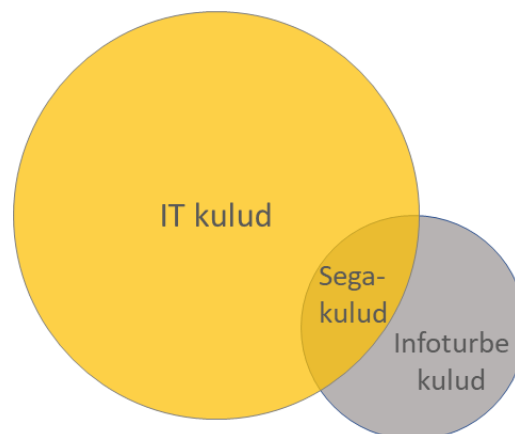
Need on sellised kulud, mille peamine funktsioon on küberturvalisuse tagamine ja mille eest enamasti vastutab küberturbe (infoturbe) funktsioon (infoturbe osakond, infoturbejuht). Sellised kulud tuleks ühtse reegli alusel liigitada täielikult küberturvalisuse alla. Nii näiteks on HSM (*Hardware Security Module*) seadme või infoturbe auditi maksumus täielikult küberturvalisuse kulu.

2. Osaliselt infoturbesse panustavad kulud (segakulud)

Osaliselt infoturbesse panustavad kulud on sellised IT kulud, millele on kahetine eesmärk ja mis mingis osas panustavad ärieesmärke teenindavasse IT funktsiooni ning mingis osas küberturvalisusesse. Nii võib näiteks olulise turvaalase funktsionaalsusega tulemüüri puhul jaotada 50% soetushinnast IT kulude alla, sest ühest küljest tagab tulemüür ligipääsu võrguressursile, kuid 50% küberturvalisuse alla, kuna ta panustab olulisel määral arvutivõrgu turvalisusesse.

Kuigi sellise jaotuse kasutamine on mingis mõttes meelevaldne, siis ühtse praktika loomiseks asutuste vahel, on mingi jaotuse kokku leppimine vajalik.

Kulu **eesmärgiga** eristame kulu panustamist kas IT-sse üldiselt või küberturvalisusesse.



Joonis 9. Küberturvalisuse kulude jaotus eesmärgi järgi

Küberturvalisusele jaotatava kulu määramisel tuleks lähtuda küsimusest, kas tehtav kulutus on kõrgema turvalisuse tõttu suurem kui oleks ilma turvalisuse vajaduseta. Näiteks, juhul kui IT komponendi (näiteks võrguseadet) hankides ei ole turvalisus eraldi kaalutlus, mille eest ollakse valmis täiendavalt kõrgemat hinda maksma, siis on tegemist 100% tavalise IT kuluga ja turvalisuse kulu on 0%. Kui aga vajatakse kõrgendatud turvalisust ning seetõttu osutub hangitav seade 20% kallimaks on põhjendatud

¹⁷ Klassikaline turvaeesmärkide jaotus vaatlleb kolme alaeesmärgi – käideldavus, terviklus, konfidentsiaalsus.

selle kulu arvestamine KTU (küberturvalisuse) kuluna. Samuti võib kaalutlemisel vaadelda aspekti, et kas ilma vaadeldava IT vara hankimiseta äriine funktsionaalsus säilib. Kui jah, siis võib öelda, et tegemist ei ole tavapärase IT kuluga ja selline turvakaalutlustel hangitav vara tuleks konteerida küberturvalisuse alla.

3.1.2.2 Kululiigi põhine liigitus

Kululiigi (kulud majandusliku sisu järgi) all mõtleme infotehnoloogilist kategooriat, millist liiki IT varadeid hangitakse. Klassikalises IT varade jaotuses, mida järgib ka riigi raamatupidamise kontoplaan, jaotuvad IT kulud riistvaraks, tarkvaraks, teenusteks ja muudeks kuludeks.

Tabel 8. IT kululiigid ja neile vastavad raamatupidamiskontod

Kululiik	Konto nr	Nimetus
Riistvara	551400	Infotehnoloogiline riistvara ja tarvikud
	551401	Kommunikatsioonitehnoloogiline riistvara ja tarvikud
Tarkvara	551410	Info- ja kommunikatsioonitehnoloogiline tarkvara
Teenused	551460	Remondi- ja hooldusteenused
	551480	Info- ja kommunikatsioonitehnoloogilise riist- ja tarkvara rent ja majutusteenus
	551485	Info- ja kommunikatsioonitehnoloogiline arendustöö
Muud kulud	551490	Muud info- ja kommunikatsioonitehnoloogilised kulud

Lisaks võivad küberturvalisuse kulud tekkida ka personalikulude ja investeeringute all (vastavalt kontoklass 50 ja 61).

Küberturvalisuse kulude käsitlusel järgitakse kululiigi põhist jaotust sarnaselt IT kuludega ja mingeid erisusi ei rakendata.

Kulu liigiga eristame kulu infotehnoloogilist kategooriat (riistvara, tarkvara, teenused, personalikulud)

Küberturvalisuse kulude arvestamise mudeli loomise üks väljakutse seisneb selles, et kuivõrd konkreetselt anda ette segakulude puhul KTU kulu osakaal mingi konkreetse IT seadme või tarkvara puhul või kui suur peaks olema vabadus seda kulujuhi poolt ise määrata. Näiteks kui monitooringu tarkvaral on nii ärirakenduse kui turvamonitoringu funktsioon, siis kas fikseerida KTU osakaal mudelis näiteks 50% või jätta IT kulujuhile diskretsioon hinnata ise professionaalselt konkreetse lahenduse panust küberturvalisusesse ning määrata sellest lähtuvalt mõni muu KTU kulu osakaal (näiteks 30% või 70%). Kohtumistel IT asutuste esindajatega leiti, et liigse variatiivsuse lubamine kulude tõlgendamisel toob kaasa erineva praktika, mis vähendab hiljem eri asutuste kulude võrdlustulemuste usaldusväärsust. Eriti problemaatiliseks osutub selline otsustusvabadus suure maksumusega kulude puhul (näiteks mahukad tarkvaraarendused, kus ka väike erinevus osakaalu määramisel toob kaasa suure rahalise mõju).

Neist argumentidest lähtudes püüab mudel järgida kahte eesmärki:

1. esiteks peab mudel olema lihtsalt rakendatav; see tähendab, et kulujuhid peavad lihtsalt leidma IT toodete ja teenuste nimekirjast hangitava kuluartikli, et rakendada pakutavat kulu reeglilt.
2. teiseks peab mudel jätma võimalikult vähe tõlgendamisruumi, mistõttu on mudelis püütud minimeerida segakulude (hangitava objekti kulu jagatakse kahe eesmärgi - IT ja KTU vahel) osakaalu ja eelistatud on lahendus, kus kulu liigitatakse täielikult kas ainult IT või ainult KTU alla.

3.1.3 Selgitused küberturvalisuse kulude eesmärgi põhiseks jaotamiseks

Allpool on toodud selgitused, kuidas eri kululiikide puhul käituda. Detailsed jaotusreeglid on esitatud dokumendi lõpus olevas toodete ja teenuste nimekirjas.

Küberturvalisuse kulude alla kuuluvad need kulud, mille puhul saab öelda, et ilma neid kulusid tegemata saavad ärifunktsioone toetavad IT teenused toimida. Ja vastupidi – IT kulude alla kuuluvad need kulud, mida tegemata ei saaks IT äriteenused toimida.

Täielikult küberturvalisuse kulude alla on koondatud need kulud, mis tuleks finantsarvestuses täielikult liigitada küberturvalisuse alla ilma kulu jaotamata. Allpool on neid kulusid käsitletud liikide lõikes. Dokumendi lõpus olevas tabelis on täielikult küberturvalisuse kulud need, mille puhul on KTU osakaal 100%.

3.1.3.1 Riistvara kulud

Riistvara grupis tuleks analüüsi hinnangul küberturvalisuse kuludena käsitleda näiteks HSM-e (*Hardware Security Module*), andmediodide ja varundusseadmeid eeldusel, et need täidavad käideldavuse eesmärki. Juhul kui salvestusseadet kasutatakse arhiveerimiseks, mis on äriline eesmärk, tuleks seda käsitleda IT kuluna.

Andmekeskusega seotud infrastruktuuri kulusid (varugeneraator, tulekustutussüsteemid jms) tuleks käsitleda osana kinnisvarast ja kuna seda pakub sageli ka kinnisvara pakkuja, siis mitte liigitada KTU alla.

Osaliselt küberturvalisuse kuludena tuleks käsitleda näiteks tulemüüri, millel on nii IT-st kui infoturbest lähtuv eesmärk.

3.1.3.2 Tarkvara kulud

Täielikult küberturvalisuse alla tuleks liigitada turvatarkvarad, kuhu kuuluvad viirusetõrje, ligipääsu reguleerivad, turvaintsidente ja nõrkusi tuvastavad jt tarkvarad, mida ei hangita ärilistel eesmärkidel, vaid mille peamine või ainuke eesmärk on arvutivõrgu ja infosüsteemide turvalisus. Siia kuuluvad ka IT riskihalduse, logianalüütika jms lahendused.

Osaliselt KTU alla tuleks liigitada rakenduste monitooringu tarkvara, mille puhul on üldjuhul tegemist nii ärirakenduse toimivuse kui turvalisuse funktsiooniga. Seetõttu pakub mudel selle kulu jagamist proportsioonis 50/50.

3.1.3.3 Teenuste kulud

Täielikult küberturvalisusesse panustavateks teenusteks on infoturbe alased konsultatsioonid, auditid, sisse ostetav infoturbe juhtimise teenus, riskide hindamine jms. Samuti kuuluvad siia turvatestimised (lõbistustestimised) nii tarkvarale kui arvutivõrgule. Siia kuuluvad ka infoturbe alased koolitused nii IT ja infoturbe personalile, aga ka tavatöötajatele.

Kõik ülejäänud tavapärase IT alased teenused, millel ka olla teatav infoturbe alane alamkomponent, tuleks selguse huvides liigitada IT teenuste alla.

3.1.3.4 Personalikulud

Täielikult kuuluvad küberturvalisuse kulude hulka infoturbe osakonna või muu küberturvalisusega tegeleva üksuse töötajate tööjõukulud. Siia kuuluvad infoturbejuht, infoturbespetsialistid jt infoturbega tegelevad töötajad. Samuti kuuluvad siia asutuse sisesed (juhul kui on) IT audiitorid.

Juhul kui infoturbefunktsiooni täitvad töötajad töötavad organisatsioonis väljaspool infoturbeüksust, oleks korrektne nende inimeste kulud osaliselt allokeerida kulumudelis infoturbele. Personalikulude puhul on kulu jaotamine erinevate tegevuste (ressursside) vahel ka täna tavapärane praktika, kuna töötajad panustavad sageli erinevatesse tegevusvaldkondadesse. Selliseks jaotamiseks kasutatakse asutustes tegevuspõhiseid kulumudeleid ning eelarvestamise ja kuluarvestuse infosüsteemi KAIS, kus on valmidus selliseks jaotuseks olemas (vt ka 0).

3.1.3.5 Füüsilise turvalisusega seotud kulud

Kuigi füüsilist turvalisust vaadeldakse infoturbe osana, siis välja pakutavas mudelis on ettepanek jätta füüsiline turvalisus küberturvalisuse kulude arvestusest välja. Füüsilise turvalisuse tagamise peamised komponendid, mis puutuvad hoonesse, serveriruumi ja tehnilisse taristusse on sageli ka teise organisatsiooni (n. RKAS) vastutada, mistõttu on keeruline küberturbe kulude eristamine ja ühtlane määramine.

Analüüsi käigus olid mitmed IT asutused seisukohal, et füüsilise turvalisuse kulud tuleks siiski küberturvalisuse alla liigitada. Sisuliselt saab selle seisukohaga nõustuda, sest enamasti nad küberturbe eesmärki täidavad. Käesolevas mudeli on aga nende kulude välja jätmise kaalutluseks eelkõige asutuste vaheline parem võrreldavus, sest eri asutustel on füüsiline turvalisus korraldatud erinevalt - mõnedel asutustel enda poolt, mõnedel aga pakutud kinnisvara haldusteenuse raames teise asutuse poolt.

3.2 Kulumudeli finantsvaade

Mudeli finantsvaade käsitleb kulude raamatupidamislikku ja kuluarvestuslikku käsitlemist.

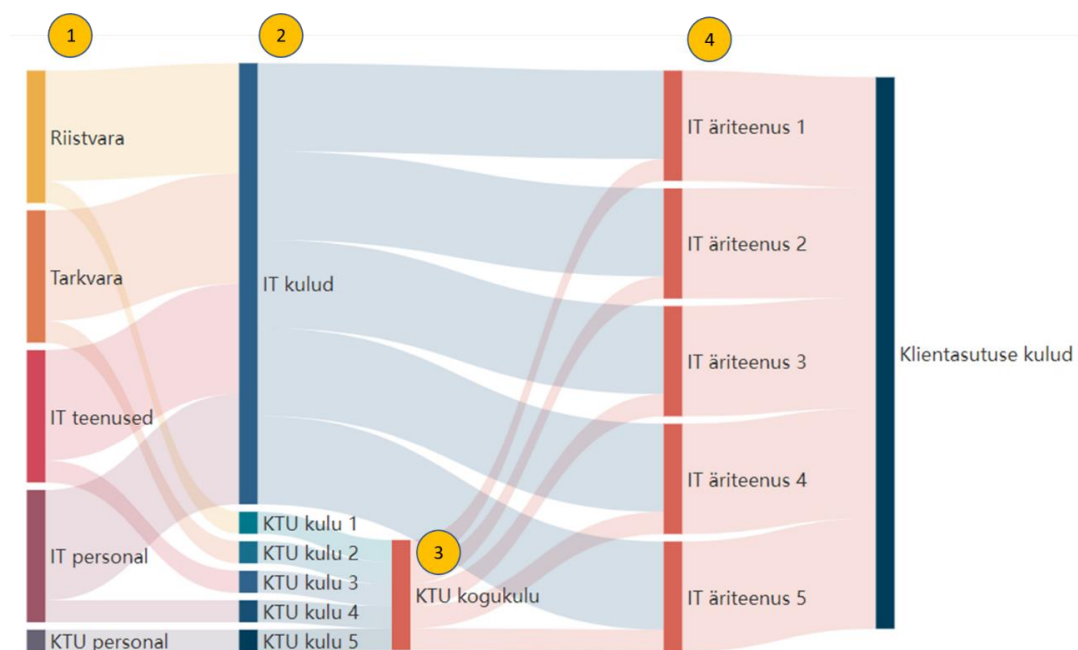
Küberturvalisuse kulud tekkivad finantsarvestuslikult peamiselt kahest allikast:

1. IT varade (riistvara, tarkvara) ja teenuste hankimisel, kus kulud jagunevad lähtuvalt olemusest:
 - a. Majandamiskulud, kontoklass 55
 - b. Investeeringud (kontoklass 15) ja kulumid (kontoklass 61)
2. Personalikulud, kontoklass 50 - IT ja infoturbe valdkonna töötajatega seotud kulud (peamiselt tööjõukulud), mis tagavad protsesside toimimise.

Nagu küberturvalisuse kulude tehnoloogilise vaate juures on eelpool kirjeldatud (vt 3.1), siis mõlemat tüüpi kulude, nii IT varade ja teenuste kui personalikulude puhul, on vaja kulusid liigitada IT ja küberturvalisuse vahel. Neil kahel kulude grupil on aga see erinevus, et kui personalikulude puhul on üldiselt püsivalt teada, millised töötajad (või ametikohad) milliste tegevustega tegelevad (kas IT või küberturvalisusega), siis IT varade hankimisel on vajalik teha kulu liigitus igal üksikjuhtumil juhul juhul põhiselt. Seetõttu pakub mudel välja kaks paralleelselt toimivat lahendust kulude käsitlemisel, mis lähtuvad riigiasutustes kasutatavatest arvepidamise infosüsteemidest

1. Üksikute IT kulude korral, kus standardse kulujaotusreegli defineerimine ei ole võimalik, määrab kulujuht ostuarve konteerimisel ja kinnitamisel SAP-is kulule õige ressursitunnuse. Vajadusel jagatakse kulu IT ja küberturvalisuse ressursikoodide vahel (juhul kui on tegemist segakuluga).
2. Personalikulude puhul defineeritakse kulumudelis (KAIS-is) küberturvalisusesse panustava ametikoha panus jaotusreegliga ning igakuise kuluarvestuse käigus allokeeritakse vastav kulu küberturvalisusele.

Küberturvalisuse kulude käitumist tegevuspõhises kulumudelil kirjeldab allolev joonis (vt joonis 10).



Joonis 10. Küberturvalisuse kulude moodustumine ja jaotumine tegevuspõhises kulumudelil

Küberturvalisuse kulude puhul on oluline asjaolu, et nad paigutuvad tüüpiliselt hangitavate IT varade kategooriate all (riistvara, tarkvara jne; joonisel etapp 1), kuid moodustavad oma eesmärgi poolest (küberturvalisus) eraldi kulude kogumi (joonisel etapp 3 – KTU kogukulu). Soovi korral on võimalik küberturvalisuse kulud jaotada ka asutuse poolt pakutavatele IT äriteenustele (joonisel etapp 4).

3.2.1 Asutuse tasemel kulude koondamine/arvutamine

Variandid asutuste infoturbekulude jälgimiseks saab jaotada standardiseerituteks (asutuste üleselt ühtmoodi kasutatavateks) ja lokaalseteks (asutuste põhisteks). Infoturbe kulude eristamiseks kasutatavate tunnuste alusel saab variandid jaotada: ressursitunnuseid kasutavad, kontosid kasutavad ja muid jaotusaluseid kasutavateks (Tabel 9).

Tabel 9. Infoturbekulude jälgimise variantide liigitus

Eristamistunnused/ ulatus	Standardiseeritud	Asutuse põhine
Ressursitunnused	Variant 2, Variant 3	Variant 1
Kontod	Variant 4	
Muud	Variant 6, Variant 7	Variant 5, Variant 6

3.2.1.1 Ressursitunnuseid kasutavad infoturbekulude jaotusalused

Variant 1 - asutuse põhiste ressursitunnuste kasutamine

SAPis ja KAISis tähistab iga asutus oma infoturbekulusid erinevate, oma asutuse kesksete ressursitunnustega (*Internal Order*). Jooksvatele infoturbekuludele (50, 5514, 61) lisatakse asutuses külge

vastav seni kasutusel olnud ressursitunnus. Kui mingi ostuarve panustab nii IT-sse kui ka infoturbe- ludesse, siis on võimalik see jaotada FITEKis vastava proportsiooniga, nt 25 küber ja 75% IT. See tugi- neb sellele, et iga sellise ostuarve puhul tuleb teha nii mitu kanderida kui mitme ressursitunnuse vahel arve jaotatakse. Teoreetiliselt võib ostuarve sellise ositamisega tekkida oht, et IT eest tervikuna vas- tutajal kaob ära tervikvaade asutuse IT kuludest, kuid asutused sellise ohu olulisust ja realiseerumist esile ei toonud. Infoturbe- kulud saaks aruande jaoks kätte vastavate ressursitunnuste alt SAPist. Uute infoturbe- kulude puhul loob asutus uue ressursitunnuse ja kasutab konteerimisel seda.

Vastavalt tegevuspõhise eelarvestamise käsiraamatule on ressurs/kulukoht arvestusobjekt, mis kir- jeldab asutuse otsekulusid teenuste osutamisel või tegevuste tegemisel või asutuse kasutuses olevaid vahendeid (näiteks inimvara, raha, põhivara, kapital) ning seda kasutatakse asutuse kuluarvestuses. Ressurs on 12-kohalise koodiga kolmetasemeline arvestusobjekt, mida kodeeritakse ning hallatakse asutuse poolt (ressursi liik määratakse tsentraalselt). Ressurs/kulukoht on kasutusel ka tegevuste maksumuste arvestuseks asutuse vajadustest lähtuvalt. Tsentraalselt on määratud järgmised ressur- siliigid:

KI - Kinnistud või hooned SE - Masinad ja seadmed MS - maismaasõidukid VS - veesõidukid PN - Püsi- navigatsioonimärgid (Veeteede Amet) OS - õhusõidukid IT - IT varad UR - üritused ja uuringud OK - tegevuste otsekulud AT - antud toetused (tegevuste otsekulu) TH - teehoiukulud (Maanteeamet) LH - loodushoiukulud (KEM) MK - muud kulukogumid

Igal asutusel on võimalus luua koodid oma äranägemise alates kuuendast tähemärgist.

Seoses infoturvalisusega võiks asutus kasutada minimaalselt kuut erinevat kululiiki mida eraldi kon- teerida:

- ▶ Tööjõukulud kontoklassist 50, kasutades selleks infoturvalisuse ametikohtade ressursi- koodi KAISt
- ▶ Riistvarakulud kontogrupist 5514, kasutades selleks infoturvalisuse ressursitunnust SA- Pis/KAISt
- ▶ Tarkvarakulud kontogrupist 5514, kasutades selleks infoturvalisuse ressursitunnust SA- Pis/KAISt
- ▶ IT teenused kontogrupist 5514, kasutades selleks infoturvalisuse ressursitunnust SA- Pis/KAISt
- ▶ Riist ja tarkvara kulumid kontoklassist 61, kasutades selleks infoturvalisuse ressursitunnust SAPis (Varale tehakse alamvara kaart ja sinna pannakse eraldi kulukoht/ressurs ning sel- lega saab amortisatsiooni kulusid jaotada mitme ressursi (nt IT ja infoturbe vahel).
- ▶ Riist ja tarkvara põhivarad kontoklassist 15 (soetusmaksumuse saab vajadusel kaheks (IT vara ja kübervara) jaotada ja teha alamvara kaardi ja sinna saab lisada eraldi kulukoht/res- surss).

Intervjuudest IT asutustega selgus, et see variant on asutuste poolt kõige eelistatum. Selle peamise eelisena toodi välja, et praegune kasutusel olev kuluarvestuse ja KAISt moodulite kasutamise süsteem on juba väljakujundatud ja nende muutmine infoturbe- kulude kättesaamise eesmärgil ei oleks kasu- kulu põhimõttest kasusid ülesse kaaluv. Selle variandi puuduseks on, et selle alusel ei ole võimalik teha jooksvalt üleriigilist tsentraalselt infoturbe- kulude päringut.

Variant 2 - üleriigiliste ressursitunnuste kasutamine

KAISt infoturbe ressursiliikide/kulukohtade standardsete tunnuste loomine (moodulis 5). Erineb eel- misest selle poolest, et ressursitunnused oleksid standardiseeritud (üle riigi kasutaksid kõik asutused

sama vara/kulu puhul sama ressursitunnust). Selle variandi järgi konteeriks asutus infoturvalisuse kulud uutele, vastavatele üleriigilistele infoturvalisuse ressursiliikidele. Asutused teevad juba praegu kulusid infoturvalisusele, kasutades selleks oma loodud ressursitunnuseid, selle variandi järgi tuleks neid muuta nendeks, mis kehtiks üle riigi. Ressursitunnuse kasutamine võimaldab kulusid jaotada mitme ressursi vahel (eraldi IT kulud ja infoturvalisuse kulud).

Selle variandi eeliseks on, et selle alusel oleks võimalik teha jooksvalt üleriigilist tsentraalselt infoturbekulude päringut. Standardsena oleks selle lahenduse puudus, igal asutusel on juba oma ressursitunnused loodud ja nende ümbermuutmine kaotab võimaluse vaadata nende varasemaid kulusid. Lisaks on asutustel KAISI moodulid erinevalt sisustatud ja see variant tooks kaasa asutuse kogu KAISI ümberkujundamise. Lisaks ei ole üle riigi IT-teenused standardiseeritud.

Variant 3 - üldeskirjas üleriigiline infoturbe kuludele oma ressurs/kulukoha kasutamine

Standardse ressurs/kulukoht kasutamine (moodulis 2) - nagu maismaasõidukitel. Selle rakendamiseks on vaja muuta üldeskirja. See tähendaks ressursiliikide pikendamist ehk juurde tuleks üks liik.

Selle variandi eeliseks on, et selle alusel oleks võimalik teha jooksvalt üleriigilist tsentraalselt infoturbekulude päringut. Selle lahenduse puudus oleks, et see lahendus ei hõlma tööjõukulusid ega kulumit, mistõttu jääksid need kululiigid infoturbekulude hulgast välja. Lisaks selgus intervjuudest, et selle tegemine infoturvalisusele võib mõjutada ka teiste valdkondlike kulude jaoks oma kulude kokkuvõtmiseks ressurs/kulukohtade kasutamist, kuid millest saadav kasu ei pruugi olla suurem tekkivast halduskoormusest. Seetõttu on praegune praktika olnud see, et pigem hoida erisused (analoogsed kululiikide grupid) minimaalsed ja tekkivaid eristamisvajadusi lahendada kompromissidega. Puuduseks on ka see, et igal asutusel on juba oma ressursitunnused loodud ja nende ümbermuutmine kaotab võimaluse vaadata nende varasemaid kulusid. Lisaks ei ole üle riigi IT-teenused standardiseeritud

3.2.1.2 Kontosid kasutavad infoturbekulude jaotusalused

Variant 4 - üleriigiliselt SAPis ainult kontogrupi 5514 kontode kasutamine

Selle variandi puhul loodaks standardsed alamkontod (8-kohalised) IKT kulu- ja investeeringu kontode (551400, 551401, 551410, 551460, 551480, 551481, 551490, 611500, 613000) alla. See lahendus võimaldab kulu jaotamist nt IT kulu ja infoturvalisuse kulu vahel (nt ostuarve summaga 1000€, millest 800€ oleks IT-kulu, mis konteeritaks IT alamkontole nt 55140001 ja 200€ oleks infoturbekulu, mis konteeritaks infoturbekulu alamkontole nt 55140002, siis konto tasandil - 551400 oleks kulu 1000€).

Selle lahenduse puudus oleks, et see lahendus ei hõlma tööjõukulusid (nende kontode rohkuse tõttu). Lisaks ei saa konkreetse vara kulumit (61) jaotada mitme alamkonto vahel. Lisaks ei ole üle riigi IT-teenused standardiseeritud. See variant eeldab üleriigiliste alamkontode loomist RTK poolt kontogrupp 5514.

3.2.1.3 Muid jaotusaluseid kasutavad infoturbekulude jaotusalused

Variant 5 - asutuse põhise WBS tunnuse kasutamine

WBSi (*Work Breakdown Structure*) dimensiooni kasutamine. Igale kulule mis on seotud infoturvalisusega lisatakse asutuse poolt projekti/WBS tunnus SAPis/KAISis.

Tegevuspõhise eelarvestamise käsiraamatust:

„Projekt on arvestusobjekt, mida kasutatakse eelarvestamisel ja raamatupidamises tekkepõhise projektiarvestuse pidamiseks. Projekt on omavahel seotud ülesannete hulk, mida teostatakse kindlate

piirangute raames, nagu ajakava ja eelarve. Projekt on maksimaalselt 20-kohalise koodiga kahetase-meline arvestusobjekt, mida kodeeritakse ning hallatakse asutuse poolt. Koodi esimesed neli kohta on määratud tsentraalselt. Projekt koosneb kahest tasemest: projekti grupp ja projekt. Projektide arves-tust peetakse üldjuhul asutuse vajadustest lähtuvalt, kohustuslik on see aga materiaalse ja immate-riaalse põhivara soetamisel Projekti eest vastutab projektijuht. Projekte on sobiv kasutada ka kindla ajapiiranguga kodumaiste toetuste kajastamisel.

Näiteks kood G10-IKT-TV1, kus G10=asutus, IKT=projektide tüüp ja TV1=konkreetne arendatav tark-vara."

Kuigi projekti tunnust peetakse sobivaks kasutada ajapiiranguga projektidel, siis puudub otsene välis-tus neid kasutada ka kehtvatel projektidel. See lahendus võimaldab kulu jaotamist WBS tunnuse abil nt IT kulu ja infoturvalisuse kulu vahel (v.a. kulum).

Seoses infoturvalisusega võiks asutusel olla minimaalselt kuus erinevat projekti mida eraldi kontee-rida:

- ▶ Tööjõukulud kontoklassist 50
- ▶ Riistvarakulud kontogrupist 5514
- ▶ Tarkvarakulud kontogrupist 5514
- ▶ IT teenused kontogrupist 5514
- ▶ Riist ja tarkvara kulumid kontoklassist 61
- ▶ Riist ja tarkvara põhivarad kontoklassist 15

Selle lahenduse puudus oleks, et see lahendus ei võimalda infoturvalisuse riistvara ja tarkvara kulumit (61) jaotada mitme WBSi vahel. Lisaks tuleks selle lahenduse järgi igale infoturvalisusega seotud töö-taja tööjõukuludele (mida kajastatakse mitmetes 50 kontoklassis olevatel kontodel) lisada kõigile WBS tunnuse.

Variant 6 - Hübriidne, mitme erineva tunnuse kasutamine

Osadel infoturvalisusega seotud kuludel kasutatakse asutuse poolt ressursitunnust SAPis ja osadid ka-jastatakse SAPis infoturbe alamkontodel. Iga asutus kasutaks oma kasutusele võetud tunnuseid. See lahendus võimaldab kulu jaotamist nt IT kulu ja infoturvalisuse kulu vahel.

Seoses infoturvalisusega võiks asutus kasutada minimaalselt kuut erinevat kululiiki mida eraldi kon-teerida:

- ▶ Tööjõukulud kontoklassist 50, kasutades selleks infoturvalisuse asutuse põhiste ametikoh-tade ressursikoode KAISis
- ▶ Riistvarakulud kontogrupist 5514, kasutades selleks infoturvalisuse standardiseeritud alamkontot SAPis (nt ostuarve summaga 1000€, millest 800€ oleks IT-kulu, mis kontee-ritaks IT alamkontole nt 55140001 ja 200€ oleks infoturbekulu, mis konteeritaks infoturbe-kulu alamkontole nt 55140002, siis konto tasandil - 551400 oleks kulu 1000€)
- ▶ Tarkvarakulud kontogrupist 5514, kasutades selleks infoturvalisuse standardiseeritud alamkontot SAPis
- ▶ IT teenused kontogrupist 5514, kasutades selleks infoturvalisuse standardiseeritud alam-kontot SAPis

- ▶ Riist ja tarkvara kulumid kontoklassist 61, kasutades selleks infoturvalisuse asutuse põhiste ressursikode KAISis. Varale tehakse alamvara kaart ja sinna pannakse eraldi kulu-koht/ressurss ning sellega saab amortisatsiooni kulusid jaotada mitme ressursi (nt IT ja infoturbe) vahel.
- ▶ Riist ja tarkvara põhivarad kontoklassist 15, kasutades selleks infoturvalisuse asutuse põhi-seid ressursikode KAISis.

Selle peamise eelisena toodi välja, et praegune kasutusel olev kuluarvestuse ja KAISi moodulite (sh ressursitunnuste) kasutamise süsteem on juba väljakujundatud. Sama eelis saab selle variandi puuduseks, et selle alusel ei ole võimalik teha jooksvalt üleriigilist tsentraalselt infoturbekulude päringut.

See variant eeldab üleriigiliste alamkontode loomist kontogrupis 5514, RTK poolt.

Variant 7 - ühtne kajastamine KAISi moodulites

Kõik asutused kajastaksid standardselt infoturvalise kulusid ühtemoodi KAISis: otsekulusid (moodul 5) ja küberosakonna kulusid (moodulis 6 või 7). Intervjuust: *tugiteenuse kasutamine (moodulis 7) oleks kõige lihtsam. Või moodul 6 - kuid natuke lisatööd juures, sest vaja teha lisasuunamisi. Mõlemad tähendaks standardiseerimist ja kehtestamist.*

Selle variandi alusel oleks võimalik teha jooksvalt üleriigilist tsentraalselt infoturbekulude päringut. Selle lahenduse puudus oleks, igal asutusel on moodulid erinevalt kasutuses ja sisustatud, seetõttu tooks standardiseerimine kaasa kõikide asutuste senise KAISi kasutamise muutmise, mis on väga aja- ja ressursimahukas, seniseid praktikaid muutev jne, mis muudavad selle lahenduse kasutamise lähiajal väga ebatõenäoliseks. Lisaks ei ole üle riigi IT-teenused standardiseeritud.

3.2.1.4 Variantide kokkuvõte

Eelnevate asutuste infoturbekulude jälgimise variantide eelised ja puudused on kokku võetud järgnevas tabelis (Tabel 10).

Tabel 10. Variantide eelised ja puudused

Variandid	Eelised	Puudused
Variant 1 - asutuse põhiste ressursitunnuste kasutamine	Praegune kasutusel olev kuluarvestuse ja KAISi moodulite kasutamise süsteem on juba väljakujundatud	Selle alusel ei ole võimalik teha jooksvalt üleriigilist tsentraalselt infoturbe kulude päringut
Variant 2 - üleriigiliste ressursitunnuste kasutamine	Selle alusel oleks võimalik teha jooksvalt üleriigilist tsentraalselt infoturbekulude päringut	Igal asutusel on juba oma ressursitunnused loodud ja nende ümbermuutmine kaotab võimaluse vaadata nende varasemaid kulusid
Variant 3 - üldeskirjas infoturbe kuludele oma ressursi/kulukohta kasutamine	Selle alusel oleks võimalik teha jooksvalt üleriigilist tsentraalselt infoturbekulude päringut	See lahendus ei hõlma tööjõukulusid ega kulumit, mistõttu jääksid need kululiigid infoturbekulude hulgast välja. Igal asutusel on juba oma ressursitunnused loodud ja nende ümbermuutmine kaotab võimaluse vaadata nende varasemaid kulusid
Variant 4 - üleriigiliselt SAPis ainult kontogrupi 5514 kontode kasutamine	Selle alusel oleks võimalik teha jooksvalt üleriigilist tsentraalselt infoturbekulude päringut	See lahendus ei hõlma tööjõukulusid (nende kontode rohkuse tõttu). Lisaks ei saa konkreetse vara kulumit (61) jaotada mitme alamkonto vahel

Variant 5 - asutuse põhise WBS tunnuse kasutamine		See lahendus ei võimalda infoturvalisuse riistvara ja tarkvara kulumit (61) jaotada mitme WBSi vahel
Variant 6 - hübriidne, mitme erineva tunnuse kasutamine	Praegune kasutusel olev kuluarvestuse ja KAISI moodulite kasutamise süsteem on juba väljakujundatud	Selle alusel ei ole võimalik teha jooksvalt üleriigilist tsentraalselt infoturbe kulude päringut
Variant 7 - ühtne kajastamine KAISI moodulites	Selle alusel oleks võimalik teha jooksvalt üleriigilist tsentraalselt infoturbe kulude päringut	Igal asutusel on moodulid erinevalt kasutuses ja sisustatud

IT- Asutuste eelistatavim variant oli variant 1, mille järgi asutused kasutavad oma väljakujunenud infoturbe kulude ja -varade ressursitunnuseid. Kui asutus peaks tegema kulutusi nendele infoturbe kuludele ja -varadele mis on käesoleva projekti käigus väljatöötatud tehnoloogilises kulumudelil, kuid mida asutus ei ole varem teinud, siis saab ta nende jaoks luua uue infoturbe kulude ressursitunnuse või konteerida need juba kasutusel oleva infoturbe kulude ressursitunnuse alla.

Variant 1 - asutuse põhiste ressursitunnuste kasutamine võimaldab asutusel eelarvestatud ja tegelikud infoturbe kulud kokku võtta ja esitada ühe koondnumbrina, aga ka liigendustega. Näiteks kuidas moodustuks koondnumber kontoklasside 50- tööjõukulude, 55- majandamiskulud ja 61-amortisatsioonikulude või ressursiliikide: tööjõuga seotud, otsekulud, IT, kinnistu, koolitus, lähetus, sõidukite, ürituste ja muude kulude pealt kokku.

4. Lisa 1. Toodete ja teenuste nimekiri

IT vara liik	IT vara grupp	Artikkel	KTU osakaal				
			0%	25%	50%	75%	100%
Personal	Infoturbe töötajad	Infoturbejuht					100%
Personal	Infoturbe töötajad	Infoturbespetsialistid					100%
Personal	Infoturbe töötajad	Muud infoturbega seotud rollid (infoturbe projektijuht, IT audiitor)					100%
Personal	Infoturbe töötajad	Intsidendihalduse spetsialist					100%
Personal	IT osakonna töötajad	Süsteemiadministraatorid	Vastavalt asutuse kulumudelile				
Personal	IT osakonna töötajad	Tarkvara arendajad	Vastavalt asutuse kulumudelile				
Personal	IT osakonna töötajad	Muud IKT töötajad (nt. projektijuhid, toote omanikud)	Vastavalt asutuse kulumudelile				
Infrastruktuur	Andmekeskused	UPS	0%				
Infrastruktuur	Andmekeskused	Andmekeskuse varugeneraator	0%				
Infrastruktuur	Andmekeskused	Tehniline infrastruktuur (kliimaseadmed, tulekustutussüsteem jms)	0%				
Infrastruktuur	Andmekeskused	Muu andmekeskuse sisustus	0%				
Riistvara	Arvutitarvikud	Tarvikud	0%				
Riistvara	Printerid, skännerid	Printerid, skännerid ja multifunktsionaalsed seadmed	0%				
Riistvara	Serverid	Serverid	0%				
Riistvara	Tahvel ja mobiilseadmed	Tahvel ja mobiilseadmed	0%				
Riistvara	Töökohaarvutid	Töökohaarvutid	0%				
Riistvara	Turvalisuse seadmed	HSM					100%
Riistvara	Turvalisuse seadmed	Andmediodid					100%
Riistvara	Turvalisuse seadmed	Valve ja häiresüsteemid			50%		
Riistvara	Salvestusseadmed seadmed	SAN, NAS seadmed	0%				
Riistvara	Varundusseadmed	Varundusseadmed					100%
Riistvara	Võrguseadmed	VPN seadmed			50%		
Riistvara	Võrguseadmed	Tulemüürid					100%

Riistvara	Võrguseadmed	Võrguseadmete (kommutaatorid, wifi) turvalisuse lisafunktsionaalsus (EDR, Threat intelligence etc)					100%
Riistvara	Võrguseadmed	Marsruuterid	0%				
Riistvara	Võrguseadmed	Traadita võrgu komponendid	0%				
Riistvara	Võrguseadmed	Kommutaatorid	0%				
Riistvara	Võrguseadmed	Muud võrguseadmed ja tarvikud (nt. Kaablid)	0%				
Sisseostetavad teenused	Auditorteenused	Infoturbe auditid					100%
Sisseostetavad teenused	Infoturbe teenused	Infoturbe juhtimise teenus					100%
Sisseostetavad teenused	Infoturbe teenused	Infoturbe spetsiifilised teenused (nt. SoC, monitooring)					100%
Sisseostetavad teenused	Infoturbe teenused	Infoturbe riskide hindamine					100%
Sisseostetavad teenused	IT halduse teenused	Kommunikatsiooniteenused	0%				
Sisseostetavad teenused	IT halduse teenused	Majutusteenused	0%				
Sisseostetavad teenused	IT halduse teenused	IT Infrastruktuuriteenused	0%				
Sisseostetavad teenused	IT halduse teenused	Tehniline tugi ja teenustugi	0%				
Sisseostetavad teenused	IT halduse teenused	Võrguteenused	0%				
Sisseostetavad teenused	IT hoolduse teenused	IT hoolduse teenused	0%				
Sisseostetavad teenused	IT juurdluse teenus (ingl. k Forensics)	IT juurdluse teenus (ingl. k Forensics)					100%
Sisseostetavad teenused	Koolitused	Infoturbe koolitused					100%
Sisseostetavad teenused	Koolitused	Muud koolitused (va. Infoturbe koolitused)	0%				
Sisseostetavad teenused	Nõustamisteenused ja uuringud	Nõustamisteenused ja uuringud	0%				
Sisseostetavad teenused	Infoturbe teenused	Koodivigade otsimise teenused (buyg bounty)					100%
Sisseostetavad teenused	Pilveteenused	Pilveteenused	0%				
Sisseostetavad teenused	Rakenduste hooldus (ingl. K Application maintenance)	Rakenduste hooldus (ingl. k Application maintenance)	0%				
Sisseostetavad teenused	Sertifitseerimise teenused	Eriotstarbelised PKI teenused, sertifikaadid					100%
Sisseostetavad teenused	Sertifitseerimise teenused	Standardised PKI teenused, sertifikaadid (SK)	0%				

Sisseostetavad teenused	Tarkvara arenduse teenused	Tarkvara arenduse ja programmeerimise teenused	0%				
Sisseostetavad teenused	Turvatestimised	Läbistuvustestide teenused					100%
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	Paroolidehalduse tarkvara					100%
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	Varundustarkvara					100%
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	Varade halduse ja arvestuse tarkvara	0%				
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	Äriarvestuse, statistika ja analüütika tarkvara	0%				
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	Serveri kommunikatsiooni tarkvara	0%				
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	Andmebaasitarkvara	0%				
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	Sisulevivõrgu (ingl k CDN) teenused	0%				
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	Salvestustarkvara	0%				
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	E-maili ja rühmatöö tarkvara	0%				
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	Virtualiseerimise tarkvara	0%				
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	Lõppseadmete halduse tarkvara (mh. MDM)			50%		
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	Töökoha operatsioonisüsteem	0%				
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	Operatsioonisüsteemid	0%				
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	Infratraktuuritarkvara turvalisuse lisafunktsionaalsus (e.g. Andmebaasi krüpteerimine)					100%
Tarkvara (mh. SaaS)	Infrastruktuuri tarkvara	Tarkvara arenduse ja programmeerimise tarkvara	0%				
Tarkvara (mh. SaaS)	Rakendused ja äritarkvara	Töökoha kontoritarkvara	0%				
Tarkvara (mh. SaaS)	Rakendused ja äritarkvara	Graafika- ja multimeedia tarkvara	0%				
Tarkvara (mh. SaaS)	Rakendused ja äritarkvara	Võrgu- ja süsteemihalduse tarkvara	0%				
Tarkvara (mh. SaaS)	Rakendused ja äritarkvara	IT-juhtimise tarkvara (CMDB)	0%				
Tarkvara (mh. SaaS)	Rakendused ja äritarkvara	Dokumendihalduse tarkvara	0%				
Tarkvara (mh. SaaS)	Rakendused ja äritarkvara	Müügi ja turundustarkvara	0%				
Tarkvara (mh. SaaS)	Rakendused ja äritarkvara	Majandustarkvara	0%				
Tarkvara (mh. SaaS)	Rakendused ja äritarkvara	Koodianalüütika tarkvara			50%		
Tarkvara (mh. SaaS)	Rakendused ja äritarkvara	IT arhitektuur tarkvara (ingl. k enterprise architecture)	0%				
Tarkvara (mh. SaaS)	Rakendused ja äritarkvara	Personali ja palgaarvestuse tarkvara	0%				
Tarkvara (mh. SaaS)	Rakendused ja äritarkvara	Geo- ja kaarditarkvara	0%				

Tarkvara (mh. SaaS)	Rakendused ja äritarkvara	Töökoha rakendused	0%				
Tarkvara (mh. SaaS)	Turvatarkvara	Rakenduste monitooringu tarkvara			50%		
Tarkvara (mh. SaaS)	Turvatarkvara	Pilvturbeagent tarkvara (Ingl k. CASB)					100%
Tarkvara (mh. SaaS)	Turvatarkvara	Emaili turvatarkvara					100%
Tarkvara (mh. SaaS)	Turvatarkvara	Turvalise juurdepääsu teenuseserv (SASE)					100%
Tarkvara (mh. SaaS)	Turvatarkvara	Serveri lõppseadme turvatarkvara (viiruse- tõrje, antispam, EDR)					100%
Tarkvara (mh. SaaS)	Turvatarkvara	Veebi rakendustulemüür (ingl. k web appli- cation firewall)					100%
Tarkvara (mh. SaaS)	Turvatarkvara	Identiteedi ja ligipääsutarkvara (mh IDM, MFA, EUBA)					100%
Tarkvara (mh. SaaS)	Turvatarkvara	Turvateabe ja sündmuste halduse tarkvara (SIEM, SOAR)					100%
Tarkvara (mh. SaaS)	Turvatarkvara	Rakenduste turvatestimise tarkvara (ingl. k application security testing)					100%
Tarkvara (mh. SaaS)	Turvatarkvara	Nõrkuste halduse tarkvara					100%
Tarkvara (mh. SaaS)	Turvatarkvara	Võrgu turvatarkvara IPS, IDS					100%
Tarkvara (mh. SaaS)	Turvatarkvara	Muu turvatarkvara (nt krüpteerimine)					100%
Tarkvara (mh. SaaS)	Turvatarkvara	Töökoha turvatarkvara (antiviirus, EDR, antispam)					100%
Tarkvara (mh. SaaS)	Turvatarkvara	DoS ja DDoS vastane tarkvara					100%
Tarkvara (mh. SaaS)	Turvatarkvara	Privilegeeritud ligipääsu haldamise tarkvara					100%
Tarkvara (mh. SaaS)	Turvatarkvara	GRC tarkvara					100%
Tarkvara (mh. SaaS)	Turvatarkvara	Infovarade klassifitseerimise tarkvara, DLP					100%
Tarkvara (mh. SaaS)	Turvatarkvara	Logimise ja logianalüütika tarkvara					100%