E-ITS PROFIIL

KOHALIKELE OMAVALITSUSTELE

v.2023_1.2

Tallinn 2023

E-ITS profiil kohalikele omavalitsustele

Andres Anier, FocusIT OÜ
Jaan Oruaas, FocusIT OÜ
Valdo Praust, FocusIT OÜ
Jaanus Altoja, Alutaguse vald
Allan Liblik, Võru linn
Ragnar Luup, Tori vald
Katrin Rajamäe, ELVL

Tartu mnt 82 Workland Fahle Tallinn
www.focusit.ee
focusit@focusit.ee

Sisukord

1 Profiili koostamise alused

Käesolev Eesti infoturbe standardi (E-ITS) kasutusprofiil on loodud eesmärgiga abistada kohalikke omavalitsusi Eesti infoturbestandardiga kooskõlas oleva infoturbe halduse süsteemi (ISMS) kavandamisel, rakendamisel ja haldamisel.

Profiili loomisel on arvestatud tüüpsete KOV-ide infotehnoloogia kasutust, IT ressursse ja infoturbe küpsustaset, mis vastab E-ITS-s toodud **põhiturbe** eeldustele. **Profiil ei kehtesta turbeviisi**, see tuleb igal rakendajal ise määrata.

Profiili rakendaja peab tutvuma Eesti infoturbestandardiga E-ITS ja E-ITS rakendusjuhendiga ning järgima neid dokumente sh riskihaldusjuhendit. Profiili peatükid **ei loo** uusi, rakendusjuhendist erinevaid tegevuspõhimõtteid ning **ei asenda** rakendusjuhendi peatükke ei osadena ega tervikuna, vaid on mõeldud **abivahendina** etalonturbe protsessi käivitamisel kohalikus omavalituses.

Profiili koostamisel on eeldatud, et profiili tuleb vähemalt korra aastas täiendada mh standard- ja kõrgmeetmete rakendamise suunistega, arvestades E-ITS uuendusi ning profiili rakendajate kogemusi, konkreetse rakendaja küpsustaset ja riskianalüüse.

Profiil on mõeldud abistama E-ITS 2022 rakendusjuhendi sammude läbimist eelkõige etalonturbe käivitamise osas vastavalt järgnevale tabelile:

Tabel 1 Profiili käsitlusala

Profiili peatükk	E-ITS 2022 rakendusjuhendi peatükk
3 Kaitseala piiritlemine	10.2 Samm 1 – kaitseala piiritlemine 10.3 Samm 2 – kaitseala struktuurianalüüs
3.1 Äriprotsesside määratlemine	9.3.1 Äriprotsesside arvelevõtt
3.2 Äriprotsesside alusteave ja rakendused	9.3.2.1 Äriprotsesside alusteave 9.3.2.2 IT süsteemid ja rakendused
3.3 Võrguarhitektuur	9.3.2.3 Sideühendused
3.4 IT-süsteemid	9.3.2.2 IT süsteemid ja rakendused
3.5 Ruumid	9.3.2.5 Muud sõltuvused
4.1 Kaitsetarbe kategooriate määramine	4.3.1.1 Potentsiaalne kahju
Lisa 1. Kahjustsenaariumid	10.4 Samm 3 – kaitsetarbe määramine Lisa B Kahjustsenaariumid
Lisa2. Kaitseala modelleerimine	10.5 Samm 4 – kaitseala modelleerimine ja meetmete tuvastamine

6 Rakenduskava koostamine	10.7 Samm 5 – turvameetmete kinnitamine

Tabel 1 Profiili käsitlusala

Omavalitsuste tegevuseesmärgid on kehtestatud kohaliku omavalitsuse korralduse seadusega. Erinevad omavalitsused on eesmärkide saavutamiseks loonud erineva struktuuri ja kasutavad erinevaid tehnilisi vahendeid.

Infoturbe halduse süsteemi kavandamisel ja praktilisel rakendamisel peab lähtuma KOV-i eesmärkide saavutamiseks loodud protsessidest, oma inimestest, kasutatavatest rakendustest, IT-süsteemidest ja IT-komponentidest, arvutivõrkudest ja taristust .

E-ITS rakendamise eelduseks on kaitsetarbe hindamine. Kaitsetarvet peab hindama standardi mõistes tippjuhtkonna liige, kes vastutab konkreetse valdkonna eest. Kuna tippjuhtkonna liikmete vastutuse jaotus on omavalitsustes erinev, ei saa profiil kaitsetarbe hindamist ühtsel viisil lahendada. Küll aga on profiilis esitatud omavalitsustele kohandatud meetodid ja vahendid, mis peaksid seda tööd oluliselt lihtsustama.

Profiili üks eesmärkidest on aidata läbi viia täiendav analüüs ja kohandada profiilis esitatud meetmeid vastavalt konkreetse organisatsiooni vajadusele. Sellise analüüsi läbiviimise lihtsustamiseks rakendatakse profiilis esitatud meetmed kategooriate kaupa. Lähenemine võimaldab konkreetses omavalitsuses kasutusel olevad lahendused kategoriseerida ning seejärel rakendada sihtobjektidele[1] meetmed nende kategooriast tulenevalt.

Profiili põhjal rakendatud infoturbemeetmed ei pruugi olla piisavad[2] infoturbe riskide aktsepteeritavale tasemele viimiseks, neid tuleks kohandada vastavalt analüüsi käigus selgunud tegelikele vajadustele. Profiili põhjal infoturbesüsteemi käivitamisele peab järgnema selle käigushoidmine ja infoturbeprotsessi pidev täiustamine eesmärgiga saavutada organisatsioonis vähemalt standardturbe tase.

[1] Vt E-ITS sõnastik (link)

[2] Vt E-ITS. Riskihaldusjuhend. 4.4 Meetmete sobivus (link)

2 Terminoloogia ja lühendid

E-ITS profiilis omavalitsustele kasutatakse E-ITS terminoloogiat ja lühendeid. Selguse huvides on profiilis täiendavalt kasutusel järgmised mõisted ja lühendid:

Tippjuhtkond – linnavalitsus või vallavalitsus

Valdkond – äriprotsess E-ITS mõistes ühe või mitme KOV eesmärgi saavutamiseks

Omanik – tippjuhtkonna liige, kes vastutab konkreetse valdkonna eest

Vastutus – tulemusvastutus ehk aruandekohustus, mida ei saa delegeerida, *ing.k. accountability*

E-ITS – Eesti infoturbestandard

IKT – info- ja kommunikatsiooni tehnoloogia

IMR – infoturbe meetmete rakendusplaan

ISMS – infoturbe halduse süsteem (ingl Information Security Management System)

KOKS – kohaliku omavalitsuse korralduse seadus

KOV – kohalik omavalitsus

KS – kahjustsenaarium

3 Kaitseala piiritlemine

Kaitsealaks nimetatakse turvapoliitika käsitlusala, mille ulatuses koostatakse turbekontseptsioon ja rakendatakse infoturbemeetmed. Etalonturbes nimetatakse kaitsealasse kuuluvaid varasid sihtobjektideks.

Käesolevas profiilis piiritletakse kaitseala loeteludena:

1. valdkonnad;
2. rakendused ja alusteave;
3. sidevõrgud;
4. IT-süsteemid;
5. hooned ja ruumid.

Protsessi järgmistes sammudes käsitletakse vaid neid sihtobjekte, mis on määratud kaitseala koosseisu.

3.1 Valdkondade määratlemine

Üldiselt puuduvad selged ja üldiselt kohaldatavad käsitlused selle kohta, mida äriprotsessina mõistetakse. E-ITS käsitleb äriprotsessina mingi eesmärgi saavutamisele suunatud tegevuste, toimingute või protseduuride kogumit.

Edaspidi kasutatakse mõiste äriprotsess asemel mõistet valdkond, mis on äriprotsess E-ITS mõistes ühe või mitme KOV eesmärgi saavutamiseks

Valdkonnad liigitatakse tüübi järgi operatiivvaldkondadeks ja toetavateks valdkondadeks. Operatiivvaldkonnad aitavad otseselt kaasa ühe või mitme KOV operatiiveesmärgi saavutamisele. KOV-i operatiivvaldkond võib olla näiteks KOV-ile pandud riiklike ülesannete täitmine ja teenuste osutamine.

KOV operatiiveesmärgid tulenevad eelkõige KOKS § 6 lõigetest 1 ja 2 so korraldada:

1. sotsiaalteenuste osutamist,
2. sotsiaaltoetuste ja muu sotsiaalabi andmist,
3. eakate hoolekannet,
4. koolieelsete lasteasutuste, põhikoolide, gümnaasiumide ja huvikoolide, raamatukogude, rahvamajade, muuseumide, spordibaaside, turva- ja hooldekodude, tervishoiuasutuste ning teiste kohalike asutuste ülalpidamist,
5. kultuuri-, spordi- ja noorsootööd,

6. elamu- ja kommunaalmajandust,
7. veevarustust ja kanalisatsiooni,
8. heakorda,
9. jäätmehooldust,
10. ruumilist planeerimist,
11. valla- või linnasisest ühistransporti,
12. valla või linna teede ehitamist ja korrashoidu.

Lisaks käsitletakse profiilis eraldi strateegia valdkonda, mida organisatsioon kasutab strateegiliste otsuste tegemiseks.

Toetavad valdkonnad ei aita otseselt kaasa operatiiveesmärkide saavutamisele, kuid võivad olla kaudselt väga olulised ja seetõttu siiski olulisel kohal, kuna neid on vaja operatiivvaldkondade käigushoiuks ja tulemite säilitamiseks. Klassikalised näited toetavatest valdkondadest on teabehaldus, finantsjuhtimine, personalijuhtimine ja IT-haldus.

Kaitsetarbe hindamise hõlbustamiseks on mõistlik valdkondi kirjeldada nii, et need paikneksid (võimaluse korral) täielikult ühes organisatsiooniüksuses ja seega ühes vastutusvaldkonnas. Igal valdkonnal on täpselt üks omanik. Üks omanik võib vastutada mitme valdkonna eest. Omanik on E-ITS mõistest tippjuhtkonna liige, kes vastutab operatiiveesmärgi saavutamise eest. Iga valdkonna omanik vastutab ka selle valdkonna infoturbe eesmärkide seadmise ja saavutamise eest.

Väga oluline on esimese sammuna selgitada välja **kõik** käsitlusalasse kuuluvad valdkonnad, kuna valdkondade kaitsetarve "pärandatakse" kõikidele valdkonna toimimiseks vajalikele sihtobjektidele. Mitut valdkonda teenindavale sihtobjektile määratakse neist kõrgeima kaitsetarbega valdkonna kaitsetarve. Selleks aga on vaja teada kõiki valdkondi ja nende kaitsetarvet.

Täiendavalt soovitame profiili rakendamisel IT-haldus kui toetav valdkond jätta kõige viimaseks. Nii peaks olema võimalik jõuda käsitluseni, kus IT hallavad süsteemid on valdkondade kahjuanalüüsi käigus juba omaniku leidnud ning IT-halduse kui sellise toimimiseks vajalike süsteemide hulk on minimaalne.

Profiilis on KOV valdkonnad[3] grupeeritud nagu näidatud järgnevas tabelis. Kuigi valdkonnad on erinevates KOV-ides erinevad, saab kõik need valdkonnad liigitada ühte alltoodud gruppidest. Edasises analüüsis saab sarnastele valdkondadele viidata grupi nime või identifikaatoriga tuues vajadusel konkreetse valdkonna erisused eraldi välja.

[3] Siin toodud valdkondade loetelu tuleb käsitleda näidisena, mille peab iga rakendaja täitma oma andmetega.

Tabel 2 Valdkonnad (näidis)

ID	**Valdkond** *(näited)*	**Omanik** *(näited)*
V1	**Strateegilised valdkonnad**	
V1.1	Volikogu, valitsuse töö	Volikogu esimees, linnapea, vallavanem
V1.2	KOV asutuste haldamine ja ülalpidamine	Linnapea, vallavanem
V2	**Operatiivprotsessid**	
V2.1	Sotsiaaltöö	Sotsiaaltööosakonna juhataja
V2.2	Haridus, kultuur ja sport	Haridus- ja kultuuriosakonna juhataja
V2.3	Ehitus, planeerimine	Arhitektuuriameti juhataja
V2.4	Haldus	Linnamajanduse osakonna juhataja
V3	**Toetavad valdkonnad**	
V3.1	Kantselei	Linnasekretär, vallasekretär
V3.1.1	Finants	Rahandusosakonna juhataja
V3.1.2	Õigus	Juriidilise osakonna juhataja
V3.1.3	IT-haldus	IT-osakonna juhataja

Tabel 2 Valdkonnad (näidis)

Kuna erinevates KOV-ides on valdkonnad ja vastutused jagunenud väga erinevalt, soovitame kasutada järgnevat kontrolltabelit veendumaks, et iga KOV operatiiveesmärgi saavutamiseks on arvele võetud operatiivprotsess:

Tabel 3 Operatiiveesmärkide ja valdkondade kontrolltabel (näidis)

	KOV valdkond				
Operatiiveesmärgid (KOKS § 6 lg 1)	V1.2	V2.1	V2.2	V2.3	V2.4
Sotsiaalteenused		X			
Sotsiaaltoetused ja -abi		X			
Hoolekanne		X			
Kultuur			X		
Sport			X		
Noored			X		
Elamu- ja kommunaalmajandus					X
Veevarustust ja kanalisatsioon					X
Heakord					X
Jäätmehooldus					X
Ruumiline planeerimine				X	

Ühistransport	X[4]				
Teedeehitus ja korrashoid	X[5]				
Koolieelsete lasteasutuste, põhikoolide, gümnaasiumide ja huvikoolide, raamatukogude, rahvamajade, muuseumide, spordibaaside, turva- ja hooldekodude, tervishoiuasutuste ning teiste kohalike asutuste ülalpidamine	X				

Tabel 3 Eesmärkide ja valdkondade kontrolltabel (näidis)

3.2 Valdkondade alusteave ja rakendused

Selles etapis tuleb igas valdkonnas tuvastada valdkonna toimimiseks vajalikud rakendused ning nendega töödeldav alusteave.

Rakenduste ja alusteabe esmaseks kaardistuseks tuleb valida sobiv detailsusaste arvestades, et alusteabe ja sihtobjektide detailne arvelevõtt toimub hiljem.

Käesolevas etapis on eesmärgiks struktuurianalüüs ning optimaalse läbipaistvuse ja efektiivsuse saavutamine tippjuhtkonnale esitamiseks kaitsetarbe määratlemiseks sobival kujul.

Rakenduste kaardistamisel tuleb piirduda rakenduste ja alusteabega, mis on vajalikud eelmises analüüsi etapis defineeritud valdkondade jaoks. Oluline on mõista, et antud juhul ei ole tegemist ühekordse tegevusega, vaid sellesse etappi tullakse nii E-ITS esmase rakendamise kui ka hilisema parendamise protsessi käigus iteratiivselt tagasi. Esmasel läbimisel tuleb valida detailsusaste ja spetsiifilisus, mis on tippjuhtkonna jaoks piisav riskide mõistmiseks ja tulenevate otsuste tegemiseks sh kahjustsenaariumite analüüsimisel.

Küll aga on oluline selgitada välja **kõik** käsitlusalasse kuuluvate valdkondade toimimiseks vajalikud rakendused ja alusteave, kuna nende kaitsetarve "pärandatakse" kõikidele nende toimimiseks vajalikele sihtobjektidele – IT-süsteemidele, sidevõrkudele, hoonetele ja ruumidele. Oluline on kindlaks määrata **kõik** seosed valdkondade ja rakenduste vahel, sest mitme rakenduse toimimiseks vajalikele sihtobjektile määratakse neist kõrgeima kaitsetarbega rakenduse kaitsetarve.

Selle saavutamiseks tuleb tagada, et vähemalt need rakendused ja alusteave, mis lähtuvalt käsitlusala valdkondade nõuetest vajavad vähemalt minimaalsel tasemel konfidentsiaalsust, terviklust ja/või käideldavust, võetakse kaardistuses arvesse.

[4] Maakondlik ühistranspordikeskus

[5] KOV omandis ettevõte

Sageli ei ole sõltuvused valdkondade ning rakenduste ja alusteabe vahel lihtsad. Seega tuleks iga konkreetse valdkonna jaoks vajalikud rakendused ja vastavad alusandmed kaardistada ühiselt vastutava osakonnaga, üksikute rakenduste eest vastutavate isikutega, toetava IT-osakonnaga vms.

Valdkondade kaardistuste põhjal on võimalik moodustada koondtabel, mida kasutatakse edaspidi rakenduste ja andmete kaitsetarbe määramisel. Sarnased sihtobjektid rühmitatakse (näiteks kontoritarkvarad). See võimaldab lihtsustada sarnaste sihtobjektidega tehtavaid tegevusi järgnevates sammudes.

Tabel 4 Rakendused ja alusteave (näidis[6]):

ID	Rakendus	Alusteave	Valdkonnad
001	Amphora	Dokumendihaldus	V1-V3
002	Spoku	Taotluste esitamine ja menetlemine	V1-V3
003	Evald	Jäätmevaldajate register	V2.4
004	Arno	Haridusteenused	V2,2
005	Word, Excel, Powerpoint (58tk)	-	V1-V3
006	Koduleht	Avalik info	V3.1
007	Facebook	Avalik info	V3.1
008	Veera	Eelarve	V3.1.1
009	Persona	Personaliinfo	V3.1
010	Outlook (58tk)	Kirjavahetus ja kalendrid	V1-V3
011	Exchange	Kirjavahetus ja kalendrid	V1-V3
012	OneDrive	Valdkonnakohased failid (privaatsed ja jagatud sh väliste osapooltega)	V1-V3
013	Synology (5tk)	Valdkonnakohased (privaatsed ja jagatud)	V1-V3
014	Autocad (4tk)	Kasutajate profiilid	V2.3
015	Brave (2tk)	Kasutajate profiilid	V3.1.3
016	Chrome (100tk)	Kasutajate profiilid	V1-V3
017	Rahvastikuregister	Elukoha info	V2.1, V2.2

Tabel 4 Rakendused ja alusteave (näidis)

Tuleb veelkord tähele panna, et **rakenduste ja alusteabe kaardistus ei ole detailne arvelevõtu register** ega dubleeri seda, vaid ülevaatetabel infoturbesüsteemi ja selle rakendamise juhtimiseks ja planeerimiseks.

[6] Siin toodud alusteabe ja rakenduste loetelu tuleb käsitleda näidisena, mille peab iga rakendaja täitma oma andmetega.

Kaardistuse sihtrühm on tippjuhtkond, detailset registrit tuleb pidada eraldi kasutades selleks sobivat tehnilist vahendit ja selle sihtrühmaks on mh infoturbejuht ja infoturbemeetmete rakendamise eest vastutajad. Edaspidi tuleb (olemasolevat) detailset registrit ja/või selle funktsionaalsust täiendada selliselt, et juhtimisotsuste tegemiseks vajalikku teavet on võimalik esitada selleks sobiva detailsusega.

3.3 Võrguarhitektuur

Tehnilise analüüsi lähtepunktis on võrguplaan näiteks võrgu topoloogiaplaani kujul, so info- ja sidetehnoloogias kasutatavate komponentide ja nendevaheliste ühenduste graafiline esitus. Plaanil peaksid infoturbe seisukohast olema näidatud vähemalt järgmised komponendid:

- IT-süsteemid, st klient- ja serverarvutid, aktiivsed võrgukomponendid nt kommutaatorid, ruuterid, WLAN-i pääsupunktid), võrguprinterid jne.
- võrguühendusega IKT ja IoT komponendid, nt printerid, skannerid, ajamid jne.
- võrguühendused nende süsteemide vahel, st LAN-ühendused, WLAN-id, magistraaltehnoloogiad jne.
- ühendused kaitseala ja välismaailma vahel, nt ruutereid kasutavad Interneti-ühendused, raadiolingid või püsiliinid kaugematesse hoonetesse või objektidesse jne.

Erineva kaitsetarbega alad tuleks tähistada.

Iga IT-süsteemi ja seadme kohta tuleks üles märkida vähemalt järgmine teave:

- kordumatu nimi (nt täielik hostinimi või identifitseerimisnumber),
- tüüp ja funktsioon (nt andmebaasiserver rakenduse X jaoks),
- aluseks olev platvorm (st riistvaraplatvorm ja operatsioonisüsteem),
- omanik ja vastutav administraator,
- asukoht (nt hoone ja ruumi number),
- sideliidesed (nt Interneti-ühendus, Bluetooth, WLAN-adapter),
- võrguühenduse tüüp ja võrguaadress.

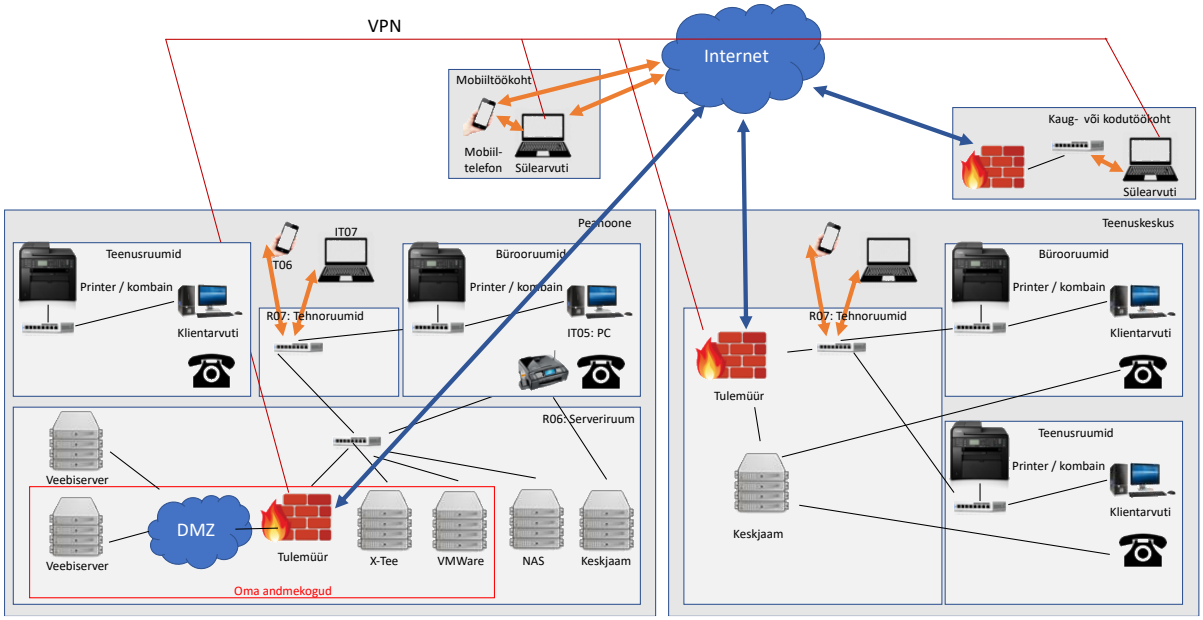
Väliste ühenduste või traadita sideühenduste (WLAN, UMTS, LTE jne) korral täiendavad andmed välisvõrgu kohta, nt Internet, äripartner, andmeedastuse pakkuja nimi ja liini tüüp, nt MPLS, püsiliin , VPN jms.

Võrguplaanis tuleks esitada ka virtuaalsed IT-süsteemid (virtuaalsed kommutaatorid, virtuaalserverid jne) ja virtuaalsed võrguühendused, nagu virtuaalsed kohtvõrgud (VLAN) või virtuaalsed privaatvõrgud (VPN). Virtuaalseid IT-süsteeme käsitleda vastavalt nende tüübile ja otstarbele, nagu ka füüsilisi IT-süsteeme. Lisaks peab virtuaalsete IT-süsteemide seostamine füüsiliste (host)süsteemidega olema arusaadav. Selguse suurendamiseks on võrgu suuruse kasvades mõttekas jagada võrguplaan mitmeks osaliseks võrguplaaniks.

Võrguplaanil on lihtsuse ja ülevaatlikkuse huvides otstarbekas komponendid rühmitada.

Samuti on otstarbekas võrguplaanil eraldi välja tuua komponendid, mis on vajalikud oma andmekogude toimimiseks, sest nende kaitsetarve ja neile rakenduvad meetmed võivad olla väga erinevad.

Joonisel 1 on kujutatud tüüpne võrguplaan, mida tuleks vastavalt kaardistusele täiendada[7]. Joonisel 1 on näidatud valik tehnoloogilisi ja infrastruktuuri osi.



Joonis 1 Tüüpne võrguplaan (näidis)

3.4 IT-süsteemid

Kaitseala edasiseks modelleerimiseks tuleks koostada olemasolevate ja kavandatavate IT-süsteemide loetelu, mis on vajalikud eelmises sammuga määratud rakenduste toimimiseks. Mõiste IT-süsteem ei tähenda ainult arvuteid, vaid ka aktiivseid võrgukomponente, võrguprintereid, telekommunikatsioonisüsteeme, nutitelefone, virtuaalseid IT-süsteeme, tööjaamasid, servereid, jne.

Kuigi IT-süsteemide nõuetekohane toimimine eeldab olemasolevate ja planeeritavate IT süsteemide täielikku ja korrektset arvelevõttu, nt. IT-süsteemide kontrollimiseks, hooldamiseks, tõrkeotsinguks ja hoolduseks, siis käesolevas etapis piisab

[7] Siin toodud võrguplaani tuleb käsitleda näidisena, iga rakendaja peab võrguplaani ise dokumenteerima.

tippjuhtkonnale riskide hindamiseks ja esmaste otsuste tegemiseks rühmitatud IT-süsteemidest. **Kõikide IT-süsteemide detailne arvelevõtt ja täiendavate otsuste tegemine toimub järgmistes iteratsioonides.** Seega on IT-süsteemide kaardistamise põhimõte väga sarnane eelnevalt kirjeldatud alusteabe ja rakenduste kaardistamisele.

Kaardistamise käigus vaadeldakse süsteeme tervikuna (nt Linuxi server, tööjaam), mitte aga üksikuid komponente, millest IT-süsteemid koosnevad (st mitte arvuti, klaviatuur, monitor jne).

Kaardistada tuleb nii võrguga ühendatud kui ka võrguta IT-süsteemid, st ka need, mis ei ole võrguplaanil näidatud. Võrguplaanil rühmitatud IT-süsteeme tuleks võimalusel ka edaspidi vaadelda ühe objektina. Ka neid IT-süsteeme, mida võrguplaanis kirjas ei ole, tuleks sobivalt rühmitada. See võib olla võimalik näiteks suure hulga üksikute võrguühenduseta printerite puhul.

Seejärel määratakse igale varasemalt kaardistatud rakendusele IT-süsteemid, mis on nende käitamiseks vajalikud. See võib olla IT-süsteem, milles töödeldakse taotlusi, kuid see võib hõlmata ka IT-süsteeme, mis edastavad nendes rakendustes loodud andmeid. Tulemuseks on kokkuvõte, mis näitab seoseid kõikide valdkondade toimimiseks vajalike rakenduste ja asjakohaste IT-süsteemide vahel.

Kaardistada tuleks järgmine teave, mida läheb vaja järgmistes etappides:

- IT-süsteemide grupi identifikaator;
- kirjeldus (nt funktsioon, tüüp) ja arv;
- platvorm (nt riistvaraarhitektuur/operatsioonisüsteem);
- asukoht (nt hoone, ruum).

Tabel 5 IT-süsteemid (näidis[8]):

ID	IT-süsteem	Platvorm	Rakendused	Asukoht
101	Active Directory	Win2019	005, 010-013	Serveriruum
102	Viirusetõrje haldus	Linux	010, 011	Serveriruum
103	NAS (5tk)	Synology	013	Serveriruum
104	Tulemüür (4tk)	Fortigate	001-004, 008-013, 017	Serveriruum
105	Tulemüür	Fortigate	001-004, 008-013, 017	Serveriruum
106	Switch (8tk)	Fortiswitch	001-004, 008-013, 017	Raekoda, teenuskeskused, seadmekapid

[8] Siin toodud IT-süsteemide loetelu tuleb käsitleda näidisena, mille peab iga rakendaja täitma oma andmetega.

107	Switch	Fortiswitch	001-004, 008-013, 017	Serveriruum
108	Printerid (5tk)	HP LaserJet	001-005	Teenuskeskused
109	Printerid (6tk)	Canon MF	001-005	Raekoda
110	Kombain (3tk)	HP MFP	001-005	Raekoda
111	Plotter	HP	014	Raekoda
112	Nutitelefon (15tk)	Redmi	010	Mobiiltöökoht
113	Nutitelefon (10tk)	Samsung	010	Mobiiltöökoht
114	Tahvel (5tk)	GalaxyTab	002, 010	Mobiiltöökoht
115	Sülearvuti (25tk)	HP	001-017	Mobiiltöökoht
116	Sülearvuti (35tk)	Lenovo	001-017	Mobiiltöökoht
117	Tööjaam (15tk)	Thinkstation	001-017	Raekoda
118	Tööjaama OS (75tk)	Win11	001-017	Raekoda, teenuskeskused, mobiiltöökoht
119	X-Tee turvaserver	Riigipilv	001-004	
120	X-Tee HSM	Riigipilv	001-004	

Tabel 5 IT-süsteemid (näidis)

3.5 Hooned ja ruumid

Olenevalt KOV suurusest ja paljudest muudest teguritest võib organisatsioon asuda ühes majas või paljudes asukohtades, mis on üksteisest kaugel ja/või mida tuleb teiste kasutajatega jagada. Tihti on valdkondade funktsioneerimiseks vaja ka teiste isikute ruume, nt. teenuslepingute raames.

Turbekontseptsioonis peavad sisalduma kõik asukohad, mis on valdkondade toimimiseks vajalikud: kinnistud, hooned, korrused, ruumid ja nendevahelised ühendused. Kõiki sidekanaleid, mis läbivad teistele isikutele ligipääsetavaid asukohti, tuleb pidada välisteks. See kehtib ka traadita side linkide kohta, kui ei saa välistada, et kolmandad osapooled võivad neile juurde pääseda. Unustada ei tohi ruume, mis on väljaspool tavapäraselt omavalitsuse kasutatavaid asukohti, kuid mida on valdkondade toimimiseks aeg-ajalt või regulaarselt vaja. Siia alla kuuluvad ka näiteks kaugtöökohad või ajutiselt renditud töökohad ja laopinnad.

Ruumide kaardistus hõlmab ka ruume, mida kasutatakse eranditult IT-toiminguteks (nagu serveriruumid, andmekandjate arhiivid), ruume, kus käitatakse muid IT-, IKT- või IoT-süsteeme (nt kontorid või teenindussaalid), ja ka sideühenduste marsruute. Kui IT-süsteeme hoitakse spetsiaalse tehnoruumi asemel kaitsekapis, tuleb kapp ruumina arvele võtta.

Lisaks tuleb kontrollida, kas kaitset vajavat teavet hoitakse teistes ruumides. Siis tuleb need ruumid ka kirja panna. Siin on ka ruumid, kus hoitakse kaitset vajavat mitteelektroonilist infot, nt. dokumendikaustad või joonistemapid. Töödeldava teabe liik peab olema kaardistusel näidatud.

Hooned ja ruumid võib kaardistada **näiteks**[9] järgmise tabeli kujul:

Tabel 6 Hooned ja ruumid (näidis)

ID	Nimetus	Asukoht	Valdkonnad
201	Raekoda	Raekoja 1	V1-V3
202	Teenuskeskus (2tk)	Teenuse tn 15 Keskuse tn 18	V2
203	Klienditeenindus (12tk)	201, 202	V2
204	Mobiiltöökoht (5tk)	-	V2.1, V2.4
205	Serveriruum	201	V1-V3
206	Seadmekapp (2tk)	202	V2

Tabel 6 Hooned ja ruumid (näidis)

[9] Siin toodud kaardistust tuleb käsitleda näidisena, mille peab iga rakendaja täitma oma andmetega.

4 Kaitsetarbe määramine

Kaitsetarbe määramise eesmärk on hinnata kaitseala sihtobjektide kaitsetarvet konfidentsiaalsuse, tervikluse ja käideldavuse osas. Kaitsetarve tuleneb võimalikust kahjust ühele või mitmele KOV valdkonnale, mis on seotud võimaliku kahjuliku mõjuga ühele või mitmele sihtobjektile.

Kaitsetarbe määramise etapid on:

- kaitsetarbe- ja kahjukategooriate määratlemine;
- kahjuanalüüs sh valdkondade kaitsetarbe määratlemine
- alusteabe ja rakenduste kaitsetarbe määratlemine;
- IT-süsteemide kaitsetarbe määratlemine;
- hoonete ja ruumide kaitsetarbe määratlemine.

Pärast kaitsetarbe kategooriate määratlemist defineeritakse esmalt valdkondade ning alusteabe ja rakenduste kaitsetarve kasutades tüüpilisi kahjustsenaariume. Seejärel tuletatakse sellest üksikute IT-süsteemide, ruumide ja sideühenduste kaitsetarve.

4.1 Kaitsetarbe kategooriate määramine

Kaitsetarve väljendab valdkonna infoturbe vajadust. Hinnang valdkonna kaitsetarbele tuleneb eelkõige valdkonnas töödeldava alusteabe kaitsetarbest. Kaitsetarbe määramine võib toimuda näiteks äritoime analüüsi (BIA - *Business Impact Analysis* - äritoime analüüs) tulemuste põhjal, kui see on eelnevalt tehtud või koos sellega.

Kaitsetarbe määramisel on keskne ülesanne hinnata infoturbe põhieesmärkide, so **konfidentsiaalsuse, tervikluse** või **käideldavuse**, rikkumise tagajärjel tekkivad võimalikud kahjud. Kahju võib koosneda rahalistest kaotustest, seaduste või lepingute rikkumisest, maine kahjustamisest või muudest kahjustsenaariumidest.

Selliste kahjude hindamise eelduseks on igakülgsed teadmised nii organisatsiooni toimimisest ja ülesannetest kui ka organisatsiooni struktuurist ja põhiandmetest. See hõlmab teadmisi nii valdkondade ja operatiiveesmärkide kohta kui ka organisatsioonilise struktuuri, asukohtade ja tarnijate kohta. Kaitsetarbe määramiseks vajalikud materjalid valmistavad ette valdkonna spetsialistid infoturbejuhi juhtimisel. Iga valdkonna kaitsetarbe määramiseks vajalikud otsused teeb valdkonna omanik, so tippjuhtkonna liige, kas vastutab konkreetse valdkonna vastutuses olevate KOV eesmärkide täitmise eest. Sisendi selle otsuse tegemiseks annavad valdkonna juht ja -spetsialistid.

Kaitsetarbe hinnang on kvalitatiivne, see antakse järgmisel skaalal:

Tabel 7 Kaitsetarbe kategooriad

Arvuline tähistus	Lühend	Nimetus	Kaitsetarbe kategooria selgitus
1	N	Normaalne	Etalonturbe meetmed osutuvad asjakohasteks ja mõistlikeks ning üldiselt nende rakendamisest piisab.
2	S	Suur	Etalonturbe meetmetest ei pruugi alati piisata. Tuleb läbida etalonturbe täiendav riskianalüüs ning vajadusel määrata lisaturbemeetmed.
3	VS	Väga suur	Etalonturbe meetmetest ei piisa kindlasti. Riskianalüüs on kohustuslik, konkreetsele ohule tuleb määrata individuaalsed turvameetmed.

Tabel 7 Kaitsetarbe kategooriad

4.2 Lisa 1. Kahjustsenaariumid

Kahjuanalüüsi abil uuritakse iga valdkonna infoturbe põhieesmärkide, so konfidentsiaalsuse, tervikluse või käideldavuse, rikkumise tagajärjel tekkivat võimalikku kahju. Kahju koosneb otsesest kahjust (nt saamata jäänud toetusrahastus või sunniraha õiguslike tagajärgede tõttu) ja kaudsetest kahjudest (nt maine kaotus).

Kuna mainitud kahjuklasside kohta on vähe põhjendatud arve, siis ei ole mõtet kahjusid arvutada kvantitatiivselt, vaid liigitada kahjud kvalitatiivselt kahjukategooriatesse. Iga organisatsioon peab ise täpsustama, mida iga kahjukategooria tähendab.

Enamasti kasutatakse kolme kuni viit kategooriat. Käesolevas profiilis kasutame jaotust nelja kategooriasse. Kahjukategooriad on vastavuses E-ITS kaitsetarbe määramisel kasutatavate kategooriatega. Järgnevas tabelis on toodud kahjukategooriate ja kaitsetarbe kategooriate võrdlus.

Tabel 8 Kahjukategooriad:

Kahjukategooria	Kirjeldus	Kaitsetarve

Tühine	Kahju mõju KOV-ile on väike või raskesti märgatav. Kahjustuste mõjud ei suuda KOV tööd märgatavalt piirata.	-
Piiratud	Kahju mõju KOV-ile on piiratud ja ohjatav. Kahjustuste mõjud võivad KOV tööd märgatavalt piirata kuid ei kahjusta märkimisväärselt sihtrühma.	Normaalne
Tõsine	Kahjustuse mõjud võivad KOV tööd märkimisväärselt piirata. Tagajärjed KOV sihtrühmale võivad olla märkimisväärsed.	Suur
Katastroofiline	Kahjustuste mõjul võib KOV töö katkeda. Tagajärjed KOV sihtrühmale võivad olla eksistentsiaalsed või eluohtlikud.	Väga suur

Tabel 8 Kahjukategooriad

Iga kahjukategooria piirmäärade määratlemisel ja täpsustamisel saab põhimõtteliselt lähtuda otsesest rahalisest kahjust, kuid mõttekam on arvestada ka teiste kahjustsenaariumidega. Mittemateriaalne või kaudne rahaline kahju võib olenevalt organisatsioonist tegelikult olla suurem kui otsene rahaline kahju.

Organisatsioon peab määratlema, milliseid kahjustsenaariume tuleks kasutada, võimaluse korral koos nende prioriteetidega. Enamiku ettevõtete jaoks on finantsmõju kõige olulisem kriteerium, kuid mõnes valdkonnas nagu pangandus või kindlustus mängib väga olulist rolli ka nende maine võimalik kahjustumine. Valitsusasutuste jaoks on esmatähtis avalike ülesannete täitmise võime, millele järgneb maine säilitamine.

„Normaalse" ja „suure" kaitsetarbe vahelise piiri määramisel tuleks arvesse võtta asjaolu, et E-ITS põhi- ja standardsed infoturbemeetmed peaksid olema normaalse kaitsenõude jaoks piisavad.

Kahjuanalüüsi läbiviimisel valib organisatsioon asjakohase arvu kahjustsenaariume.

Käesolevas profiilis eeldatakse, et KOV valdkonnad ei suuda otseselt kahjustada inimese füüsilist puutumatust (E-ITS rakendusjuhend lisa B, kahjustsenaarium 3, isiku füüsilise puutumatuse rikkumine) ning EITS.CON.2 ja eelkõige GDPR-st tulenevad inimese teabelise enesemääramisõiguse meetmete rakendamise tõttu ei ole teabelise enesemääramise õiguse rikkumine tõenäoline (E-ITS rakendusjuhend lisa B, kahjustsenaarium 2, teabelise enesemääramisõiguse rikkumine).

Seega, kaitsetarbe määramisel kasutatakse käesolevas profiilis järgenvat E-ITS rakendusjuhend lisa B kahjustsenaariumide (KS), alamhulka

- KS4: Ülesannete täitmise võime kahjustamine
- KS5: Negatiivsed sisemised või välised toimed
- KS1: Õigusaktide, eeskirjade või lepingute rikkumine
- KS6: Rahalised tagajärjed

See ei tähenda, kahjustsenaariume KS2 ja KS3 ei või kasutada. Pigem soovitame need kahjustsenaariumid läbi käia hiljemalt E-ITS rakendamisele järgneva(te) ülevaatus(te) käigus ning vajadusel lisada täiendavaid kahjustsenaariume vastavalt vajadustele.

Infoturbe halduse süsteemi läbivaks põhimõtteks on tegutseda prioriteetide järjekorras arvestades meetmete ja sihtobjektide omavahelisi sõltuvusi ja võimalikult kiiret turvakasu. Seetõttu vaadeldakse ka edaspidises kahjuanalüüsis kahjustsenaariume ülaltoodud järjekorras seades esmatähtsaks ülesannete täitmise võime. Sihtrühmade ja osapoolte jaoks on väga oluline usaldus KOV vastu. Negatiivse välise mõju (KS5) tõttu võib see usaldus kaduda, negatiivse sisemine mõju toimel kaduda usaldus KOV enda või allasutuste töötajate silmis.

Kahjustsenaariume tuleks käsitleda kui sama sündmuse erinevaid dimensioone. Näiteks, kui KOV ei saa oma ülesandeid täita (KS4) võib sellega kaasneda nii välisest mõjust tulenev mainekahju (KS5) kui ka õigusaktide, eeskirjade või lepingute rikkumine (KS1). Ka isikuandmete kaitse seaduste rikkumised kuuluvad kahjustsenaariumi KS1 alla. Kõigil neil juhtumitel võivad lisanduda kahjunõuetest tulenevad rahalised tagajärjed (KS6).

Kahjukategooriate piiride määratlemiseks peab organisatsioon ise kahjustsenaariumite põhjal piirid eraldi täpsustama. Riskihalduse üldisemas käsitluses on see riskitaluvuse ja riski kriteeriumite määramine. Järgnevas tabelis on näidatud üks võimalus soovitatud stsenaariumide ja kategooriate jaoks. Iga KOV-i tippjuhtkond peab veenduma, et need vastavad konkreetse KOV-i vajadustele ning vajadusel kohendama.

Tabel 9 Kahjustsenaariumite piirid (üks võimalus):

Kahjustsenaarium	Mõju
Tühine	
KS4: Ülesannete täitmise võime kahjustamine	Ülesannete täitmise võime langemine on väike või raskesti märgatav.
KS5: Negatiivsed sisemised või välised toimed	KOV usaldusväärsus (potentsiaalse) sihtrühma, töötajate, partnerite, huvipoolte silmis ei lange.

KS1: Õigusaktide, eeskirjade või lepingute rikkumine	Õiguslikud tagajärjed või leppetrahvid puuduvad. Sellised lepingud puuduvad.
KS6: Rahalised tagajärjed	Rahalised kahjud alla 0.01% eelarvest.
Piiratud	
KS4: Ülesannete täitmise võime kahjustamine	KOV protsessid on vähesel määral häiritud kuni 3 päeva. Valdkonna toimimiseks on alternatiivsed võimalused, kusjuures täiendavad kulud on aktsepteeritavad.
KS5: Negatiivsed sisemised või välised toimed	KOV usaldusväärsus langeb hinnanguliselt kuni 10% (potentsiaalse) sihtrühma, töötajate, partnerite, huvipoolte silmis.
KS1: Õigusaktide, eeskirjade või lepingute rikkumine	Vähesed õiguslikud tagajärjed (järelevalve menetlus, ettekirjutus, korduvrikkumisel trahvid) või leppetrahvid 0.01% - 0.5% eelarvest
KS6: Rahalised tagajärjed	Rahalised kahjud 0.01% - 0.5% eelarvest
Tõsine	
KS4: Ülesannete täitmise võime kahjustamine	KOV protsessid on olulisel määral häiritud rohkem kui 24h. Valdkonna toimimiseks on alternatiivsed võimalused, kuid täiendavad kulud on märkimisväärsed.
KS5: Negatiivsed sisemised või välised toimed	Organisatsiooni usaldusväärsus langeb oluliselt või üle 10% (potentsiaalse) sihtrühma, töötajate, partnerite, huvipoolte silmis.
KS1: Õigusaktide, eeskirjade või lepingute rikkumine	Märkimisväärsed õiguslikud tagajärjed (korduvrikkumisel trahvid) või leppetrahvid 0.5% - 1.5% eelarvest
KS6: Rahalised tagajärjed	Rahalised kahjud 0.5% - 1.5% eelarvest

Katastroofiline	
KS4: Ülesannete täitmise võime kahjustamine	Enamik KOV protsessidest on väga olulisel määral häiritud rohkem kui 24h. Valdkonna toimimiseks ei ole alternatiivseid võimalusi.
KS5: Negatiivsed sisemised või välised toimed	Organisatsiooni usaldusväärsus enamiku elanike, töötajate, partnerite, huvipoolte silmis muutub olematuks
KS1: Õigusaktide, eeskirjade või lepingute rikkumine	Õiguslikud tagajärjed või leppetrahvid (üle 1.5% eelarvest) seavad ohutu organisatsiooni eksistentsi.
KS6: Rahalised tagajärjed	Rahalised kahjud üle 1.5% eelarvest

Tabel 9 Kahjustsenaariumite piirid (üks võimalus)

Protsesside kaitsetarbe määramiseks tuleb kindlaks määrata vastava protsessi potentsiaalse kahjustuse võimalik ulatus iga kahjustsenaariumi puhul. Tulenevalt KOV prioriteetidest määratakse kõigepealt iga protsessi kättesaadavuse nõue. Sellele järgneb konfidentsiaalsuse nõuete määramine. Lõpuks määratakse kindlaks nõuded terviklusele.

Kaitsetarbe hindamiseks vajaliku teabe saab nõuete analüüsi, küsimustike, töötubade või individuaalsete intervjuude abil. Mõistlik on valida nende meetodite kombinatsioon, kuna igal neist on oma eelised ja puudused ning need täiendavad üksteist.

Dokumenteeritud nõuete (seadused, määrused, standardid jne) alusel saab määrata suuna teiste meetoditega jätkamiseks. Näiteks küsimustikke, olgu need siis paberkujul või tarkvarapõhised, saab koostada ainult üldiselt ja need peavad kehtima kõigis valdkondades. Töötoad, mis võivad jõuda suure hulga inimesteni, sobivad infoturbe juhtimise teema tutvustamiseks ja töötajate teavitamiseks, miks on vaja teatud samme teha ning millised on iga sammu eesmärgid. Individuaalsed intervjuud valdkondade juhtide, protsessi eest vastutavate isikute või muude vajalikku infot andvate töötajatega võivad võtta aega, kuid võivad anda spetsiifilist teavet, vältida arusaamatusi esitades küsimused õigesti ja kasutades sobivaid küsitlustehnikaid ning esitada olulist teavet sobival kujul.

Protsesside kaitsetarbe määramisel soovitame kasutada E-ITS kahjustsenaariumite küsimustike põhjal loodud KOV konteksti sobitatud ja täiendatud küsimustikke. Neid küsimusi võib konkreetse KOV-i iseärasuste põhjal sobitada ja täiendada.

Kaitsetarbe määramisel tuleb aluseks võtta

- uuritava valdkonna kõige kriitilisemad rakendused ja alusteave;
- varasemalt defineeritud kaitsetarbe piirtingimused vt *Tabel 9 Kahjustsenaariumite piirid;*
- tabelis toodud abistavad küsimused.

4.2.1 Käideldavus

KS	Küsimused
KS4	**Ülesannete täitmise võime kahjustamine**
	- **Millisel määral on KOV ülesannete täitmine IKT-süsteemide tõrgete korral takistatud?** - **Kui kiiresti õnnestub IKT-süsteemide töö aktsepteeritaval tasemel taastada?** Abistavad küsimused: - Kas on teavet, mille käideldavuse vähenemisel oleksid tõsised tagajärjed organisatsioonile või selle valdkonnale? - Kas rakenduste tõrge võib nii tõsiselt mõjutada organisatsiooni tegevust, et asjaomastele ei ole ooteajad enam vastuvõetavad? - Kas selle rakenduse tõrge võib mõjutada teisi rakendusi? - Kui oluline on organisatsioonile, et rakendused ja programmid töötaksid alati ning et andmed oleksid alati kättesaadavad?
KS5	**Negatiivsed sisemised või välised toimed**
	- **Kui kiiresti saab teabe käideldamatus või sellest tulenev valdkonna protsesside tõrge märgatavaks väljaspool?** - **Kui kaua peavad töötajad pärast katkestust tagantjärele andmeid sisestama?** Abistavad küsimused: - Kas rakenduste tõrge piiraks kolmandatele pakutavaid infoteenuseid? - Kas teabe käideldamatus või valdkonna protsesside tõrge võib takistada organisatsiooni eesmärkide saavutamist?
KS1	**Õigusaktide, eeskirjade või lepingute rikkumine**
	- **Millised õigusaktidest tulenevad sanktsioonid rakenduvad IKT-süsteemide käideldamatusest tulenevate valdkonna protsesside tõrgete puhul?** - **Kui suure õigusaktidest tuleneva rahalise nõude võivad kaasa tuua IKT-süsteemide käideldamatusest tulenevad valdkonna protsesside tõrked?**

	- **Millised sanktsioonid on alusteabe käideldavuse kao puhul ette nähtud kehtivate lepingutega?** Abistavad küsimused: - Kas selle rakenduse tõrge võib põhjustada eeskirjade või isegi õigusaktide rikkumist? - Kas õigusaktid nõuavad mingi teabe pidevat kättesaadavust (24/7)? - Kas on seatud mingeid tähtaegu, mida tuleb selle rakenduse kasutamisel järgida? - Kas mõne lepingu tingimused käsitlevad tähtaegu?
KS6	**Rahalised tagajärjed**
	- **Kui palju maksaks IT-süsteemide remont või taaste nende tõrke, defekti, hävimise või varguse korral?** - **Kui suuri kahjutasunõudeid põhjustaks käideldavuse kadu?** - **Kui suuri täiendavaid kulusid põhjustaks käideldavuse kadu?** Abistavad küsimused näiteks hankeprotsessi või toetuste kontekstis: - Kas rakenduste või valdkonna protsesside tõrke puhul tekiks rahaline kahju hilinenud maksete või intressikao tõttu? - Kas rakenduste või valdkonna protsesside tõrge võib põhjustada leppetrahvi, finantseeringust ilma jäämist, enampakkumise ebaõnnestumist vms? - Kui paljusid olulisi huvigruppe mõjutaks rakenduste või valdkonna protsesside tõrge?

4.2.2 Konfidentsiaalsus

KS	Küsimused
KS4	**Ülesannete täitmise võime kahjustamine**
	- **Millisel määral takistab alusandmete konfidentsiaalsuse kadu valdkonna protsesside toimimist?** Abistavad küsimused:

	- Kas on mingit teavet, mille konfidentsiaalsus on ülesande täitmiseks oluline (õiguskaitseteave, uurimistulemused)?
KS5	**Negatiivsed sisemised või välised toimed**
	- **Millised on tundliku teabe lubamatu avaldamise tagajärjed organisatsiooni usaldusväärsusele so nt mainekahju (potentsiaalse) sihtrühma või (potentsiaalsete) töötajate silmis?** Abistavad küsimused: - Kas konfidentsiaalse teabe paljastumine võib panna kahtlema organisatsiooni usaldatavuses? - Kas teabe avaldamine võib tekitada poliitilist või sotsiaalset ebaturvalisust? - Kas teabe lubamatu avaldamine võib kaotada töötajate usalduse organisatsiooni vastu?
KS1	**Õigusaktide, eeskirjade või lepingute rikkumine**
	- **Millised on teabe konfidentsiaalsuse kao puhul õigusaktidest tulenevad sanktsioonid?** - **Kui suure kahjutasunõude võib kaasa tuua teabe paljastumine?** - **Millised sanktsioonid on protsessikohase teabe konfidentsiaalsuse kao puhul ette nähtud kehtivate lepingutega?** Abistavad küsimused: - Kas õigusaktid nõuavad selle teabe konfidentsiaalsust? - Kas teabe paljastumine võib tuua kaasa kriminaalmenetluse või suure kahjutasunõude? - Kas on lepinguid, mis nõuavad teatava teabe konfidentsiaalsuse säilitamist?
KS6	**Rahalised tagajärjed**
	- **Kui suuri kahjutasunõudeid põhjustaks konfidentsiaalse teabe edastamine või teatavaks saamine kolmandatele isikutele?** - **Kui suuri täiendavaid kulusid põhjustaks konfidentsiaalse teabe edastamine või teatavaks saamine kolmandatele isikutele?**

	Abistavad küsimused näiteks hankeprotsessi või toetuste kontekstis: - Kas konfidentsiaalse teabe avaldamine põhjustaks kahjutasunõudeid? - Kas on mingit valdkonn protsessi- või rakenduseteavet, mis annaks kolmandate isikute kätte sattumisel neile rahalist kasu? - Kas rakendustega salvestatakse väärtuslikke uurimisandmeid? Mis juhtuks nende loata kopeerimisel ja edasiandmisel? - Kas tundliku teabe enneaegne avaldamine võib tekitada kahju?

4.2.3 Terviklus

ID	Küsimused
KS4	**Ülesannete täitmise võime kahjustamine**
	- **Millisel määral on ülesannete täitmine rikutud teabega takistatud?** - **Kui kiiresti õnnestub lubamatud muudatused andmetes avastada ja kõrvaldada?** Abistavad küsimused: - Kas teabe muutumine takistaks ülesannete täitmist määral, et protsessid ei saaks enam toimida? - Kas ülesannete täitmine rikutud teabega tekitaks olulist kahju? - Kas rikutud teave vaadeldavas rakenduses võib tekitada vigu teisteski rakendustes? - Millised on tagajärjed kui andmete loomine omistatakse valele isikule?
KS5	**Negatiivsed sisemised või välised toimed**
	- **Millist kahju võib tekitada väära või puuduliku teabe töötlus, levi või edastus usaldusväärsusele so mainekahju (potentsiaalse) sihtrühma või (potentsiaalsete) töötajate silmis?** Abistavad küsimused: - Kas teabe rikkumine saab avalikult teatavaks? - Kas rikutud teabe avaldamine võib tekitada prestiiži langust?

	- Kas rikutud teabe avaldamine võib tekitada poliitilist või sotsiaalset ebaturvalisust? - Kas rikutud teabe avaldamine võib halvendada toote kvaliteeti ja seeläbi prestiiži langust?
KS1	**Õigusaktide, eeskirjade või lepingute rikkumine**
	- **Millised on teabe tervikluse kao puhul õigusaktidest tulenevad sanktsioonid?** - **Millised sanktsioonid on teabe tervikluse kao puhul ette nähtud kehtivate lepingutega?** Abistavad küsimused: - Kas õigusaktid nõuavad selle teabe terviklust? - Kas terviklusrike oleks vastuolus seaduste, eeskirjadega või lepingutega?
KS6	**Rahalised tagajärjed**
	- **Kui suurt rahalist kahju saab protsesside alusandmeid manipuleerides tekitada sh rikutud teabe põhjal tehtud väärade otsuste tulemusel?** - **Kui suuri kahjutasunõudeid võib põhjustada väära teabe avaldamine, edastamine või teatavaks saamine kolmandatele isikutele?** Abistavad küsimused näiteks hankeprotsessi või toetuste kontekstis: - Kas andmeid manipuleerides saab tekitada rahalist kahju, *näiteks maamaksu andmete valesti sisestamisel või isikuandmete ekslikul töötlemisel?* - Kas väära teabe avaldamine võib põhjustada kahjutasunõudeid? - Kas rikutud tellimisandmed võivad tekitada rahalist kahju, *näiteks täppisajastusega tootmisel, eksimus tellitava koguse sisestamisel*)? - Kas rikutud teave võib viia väärade otsusteni?

4.3 Valdkondade kaitsetarbe määramine

Kuna erinevad KOV-id on KOKS-iga pandud ülesannete täitmise jaganud valdkondadeks erinevalt, ei saa käesoleva profiiliga KOV-idele ette anda konkreetset valdkondade nimekirja koos eeldefineeritud kaitsetarbega ja sellest tulenevate infoturbemeetmetega.

Alltoodud näide ühe konkreetse valdkonna kahjuanalüüsist on **näidis**, mida võib kasutada KOV konkreetsete valdkondade kahjuanalüüsi läbi viimisel. Kahjuanalüüsi käigus on oluline arvestada muudatustega, mida KOV on sisse viinud eelmistes peatükkides käsitletud kahjustsenaariumitesse, -kategooriatesse ja -kriteeriumitesse. Samuti ei ole oluline jäigalt kinni pidada näites kasutatud formaadist.

Kõige olulisem on, et iga valdkonna kahjuanalüüsi käigus teeb otsused valdkonna eest vastutav tippjuhtkonna liige.

Kahjukategooriate määramine

Kahjukategooriate määramisel peab iga valdkonna omanik infoturbejuhi ettevalmistatud materjalide põhjal vastama küsimustele, mis on toodud peatükkides 4.2.1-4.2.3 selliselt, et *Tabel 9 Kahjustsenaariumite piirid* vastava rea valik oleks selgesti ja üheselt mõistetav ning korratav. Kuna valdkonna omanik on tippjuht, kes ei pruugi kõikide aspektidega detailselt kursis olla, on vajalik kahjukategooriate määramisel kaasata valdkonna juhid ja spetsialistid.

Tabel 10 Valdkonna alusteabe käideldavuse võimalikest probleemidest tulenevad kahjud (Näidis[10])

Alusteabe käideldavuse võimalikest probleemidest tulenevad kahjud		
KS	**Kahjukategooria**	**Põhjendus**
KS4	Piiratud	Ootamatu IKT katkestuse korral on protsessid vähesel määral häiritud juhul, kui katkestus kestab kuni 3 päeva. Valdkonna toimimiseks on alternatiivsed võimalused kusjuures täiendavad kulud on aktsepteeritavad. Andmed on vaja tagantjärele sisestada. Planeeritud katkestused protsesse ei häiri.
KS5	Tühine	KOV usaldusväärsus (potentsiaalse) sihtrühma, töötajate, partnerite, huvipoolte silmis ei lange, kuna KOV valdkond suudab oma avalikud ülesanded täita.
KS1	Piiratud	Maksed tarnijatele võivad viibida tuues kaasa viivised, kui valdkond ei edasta makseinfot õigeaegselt rahandusosakonnale ja siis on

[10] Siin toodud määratlust tuleb käsitleda näidisena, mille peab iga rakendaja täitma oma andmetega.

		süsteemid täpselt maksetähtajani maas. Lepingutes sisalduvad viivised mitte rohkem kui 0.5% eelarvest.
KS6	Piiratud	Otsene rahaline kahju: viivised kuni 0.5% eelarvest

Tabel 10 Valdkonna alusteabe käideldavuse võimalikest probleemidest tulenevad kahjud (näidis)

Tabel 11 Valdkonna alusteabe konfidentsiaalsuse võimalikest probleemidest tulenevad kahjud (näidis)

Alusteabe konfidentsiaaluse võimalikest probleemidest tulenevad kahjud		
Stsenaarium	**Kahjukategooria**	**Põhjendus**
KS4	Tühine	Alusandmete konfidentsiaalsuse kadu ei põhjusta häireid valdkonna protsessides.
KS5	Piiratud	KOV usaldusväärsus langeb hinnanguliselt kuni 10% (potentsiaalse) sihtrühma, töötajate, partnerite, huvipoolte silmis. Tagajärgedega tuleb täiendavalt tegeleda
KS1	Piiratud	Vähesed õiguslikud tagajärjed (järelevalve menetlus, ettekirjutus, korduvrikkumisel trahvid ja/või sunnirahad 0.01% - 0.5% eelarvest) Kriitilised alusandmed: Isiku kontaktandmed; väärteo- ja järelevalve menetlus; eluruumide kohandamise leping puuetega inimestele; küttekolded; mis inimesel üldse kodus on sh ehitusprojekt; registrid: muinsuskaitse toetused; koerad, kassid, ussid; riigihangete seadus, VÕS; lepingud, nendes ärisaladused; planeeringute juures kaitsealused liigid; piiriäärsed riigikaitselised objektid
KS6	Piiratud	Otsene rahaline kahju: trahvid, sunnirahad, viivised 0.01% - 0.5% eelarvest

Tabel 11 Valdkonna alusteabe konfidentsiaalsuse võimalikest probleemidest tulenevad kahjud (näidis)

Tabel 12 Valdkonna alusteabe tervikluse võimalikest probleemidest tulenevad kahjud (näidis)

Alusteabe tervikluse võimalikest probleemidest tulenevad kahjud		
Stsenaarium	**Kahjukategooria**	**Põhjendus**
KS4	Piiratud	Protsesside toimimiseks on alternatiivsed võimalused kusjuures täiendavad kulud on aktsepteeritavad. Kriitilised andmed: kaevude asukohad on valed – keskkonnaamet, kaevu kaitsetsooni ei tohi ehitada; lume lükkamine – aadressid puudulikud, piiride teema; trassid, eelkõige vanad veetrassid, mille andmed ei ole usaldusväärsed; maaküttekontuurid.
KS5	Tühine	KOV usaldusväärsus (potentsiaalse) sihtrühma, töötajate, partnerite, huvipoolte silmis ei lange. Andmekvaliteedi probleemide lahendamine on tavapärane töö osa.
KS1	Tühine	Õiguslikud tagajärjed või leppetrahvid puuduvad. Lepingulised sanktsioonid puuduvad.
KS6	Piiratud	Otsene rahaline kahju 0.01% - 0.5% eelarvest, näiteks trassi lõhkumise tagajärgede likvideerimine

Tabel 12 Valdkonna alusteabe tervikluse võimalikest probleemidest tulenevad kahjud (näidis)

Näide: ühe valdkonna kahjukategooriate koondtabel[11]

Kahjustsenaariumist tulenevad valdkonna kahjukategooria väärtuseks on kõige kõrgem kahjukategooria väärtus käideldavuse, konfidentsiaalsuse ja tervikluse vaatest.

Tabel 13 Valdkonna kahjukategooriate koondtabel (näidis)

KS	Kahjukategooria	Käideldavus	Konfidentsiaalsus	Terviklus
KS4	**1 - Piiratud**	1 – Piiratud	0 - Tühine	1 – Piiratud
KS5	**1 - Piiratud**	0 - Tühine	1 – Piiratud	0 - Tühine
KS1	**1 - Piiratud**	1 – Piiratud	1 – Piiratud	0 - Tühine
KS6	**1 - Piiratud**	1 – Piiratud	1 – Piiratud	1 – Piiratud

Tabel 13 Valdkonna kahjukategooriate koondtabel (näidis)

Näide: kõikide valdkondade kaitsetarbe koondtabel

Valdkondade kaitsetarbe koondtabel täidetakse läbiviidud kahjuanalüüside tulemuste põhjal kombineerides Tabel 2 Valdkonnad (näidis) ja iga valdkonna kohased Tabel 13 Valdkonna kahjukategooriate koondtabel (näidis).

Põhjenduse veergudes on kasutatud kaitsetarbe kategooria arvulist tähistust, *vt Tabel 7 Kaitsetarbe kategooriad*.

Iga valdkonna kaitsetarbe defineerib kõige kõrgem kahjustsenaariumitest tulenev kahjukategooria vastavalt *Tabel 8 Kahjukategooriad*.

Kahjuanalüüsi põhjal saadud nõuded kaitsetarbele tuleb dokumenteerida näiteks järgmise tabeli[12] kujul:

Tabel 14 Kaitsetarbe koondtabel (näidis)

ID	Valdkond	Kaitsetarve	Põhjendus			
			KS4	KS5	KS1	KS6
V1	**Strateegilised protsessid**					
V1.1	Volikogu, valitsuse töö	**Normaalne**	1	1	1	1

[11] Siin toodud määratlust tuleb käsitleda näidisena, mille peab iga rakendaja täitma oma andmetega.

[12] Siin toodud määratlust tuleb käsitleda näidisena, mille peab iga rakendaja täitma oma andmetega.

V1.2	KOV asutuste haldamine ja ülalpidamine	**Normaalne**	1	1	1	1
V2	**Operatiivprotsessid**					
V2.1	Sotsiaaltöö	**Suur**	1	**2**	1	1
V2.2	Haridus, kultuur ja sport	**Normaalne**	1	1	1	1
V2.3	Ehitus, planeerimine	**Normaalne**	1	1	1	1
V2.4	Haldus	**Normaalne**	1	1	1	1
V3	**Toetavad valdkonnad**					
V3.1	Kantselei	**Normaalne**	1	1	1	1
V3.1.1	Finants	**Normaalne**	1	1	1	1
V3.1.2	Õigus	**Normaalne**	1	1	1	1
V3.1.3	IT-haldus	**Normaalne**	1	1	1	1
V4.2	Finants	**Normaalne**	1	1	1	1

Tabel 14 Kaitsetarbe koondtabel (näidis)

NB! Valdkonnale V2.1 Sotsiaaltöö on suur kaitsetarve määratud **näitena**, et **illustreerida** edasises analüüsis rakenduvat kaitsetarbe „pärandamise“ ja maksimaalse kaitsetarbega põhjendamise põhimõtet. Profiili käesolevas versioonis käsitletakse ainult **põhiturbe** meetmeid.

4.4 Alusteabe ja rakenduste kaitsetarbe määramine

Alusteabe ja rakenduste kaitsetarbe määramiseks täiendatakse peatükis *3.2 Valdkondade alusteave ja rakendused* koostatud kaardistust *Tabel 4 Rakendused ja alusteave* kahjuanalüüsi käigus saadud kaitsetarbe määratlustega *Tabel 14 Kaitsetarbe koondtabel (näidis)*,

Valdkondade kaitsetarve "pärandatakse" sihtobjektidele, milleks antud juhul on rakendused ja alusteave. Mitut valdkonda teenindavale sihtobjektile määratakse nendest valdkondadest kõrgeima kaitsetarbega valdkondade kaitsetarve, ja see seos dokumenteeritakse veerus „Põhjendus“. Siinjuures arvestatakse sihtobjektide omavahelisi sõltuvusahelaid ja koostoimeid.

Näiteks, kui rakendus on andmekogu AvTS §43 mõistes, tuleb selle kaitsetarbe määramisel lisaks sõltuvate valdkondade kaitsetarbele arvestada ka andmekogu põhimäärusega. Andmekogu põhimäärusest tulenev kaitsetarve tuletatakse andmekogu turbeastmest vastavalt valitsuse määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 11, milles sätestatakse turvameetmete rakendamine andmekogu turbeastmest

lähtuvalt. Võttes arvesse, et E-ITS ISMS (infoturbe halduse süsteem) nõuab reageerimist muutustele regulatsioonide nõuetes, lepingulistes kohustustes ning ümbritsevas infoturbeolukorras, tuleb veenduda, et määratud turvaklass on jätkuvalt asjakohane. Vajadusel tuleb andmekogu kaitsetarve uuesti hinnata vastavalt nimetatud määruse 2. jao turvameetmete erinõuded 1. jaotisele andmekogu.

Järgnevalt on esitatud alusteabe ja rakenduste kaitsetarbe määratlemise näidis[13]: *(*) alusteabe hulka ei kuulu V2.1 konfidentsiaalsed andmed.*

Tabel 15 Alusteabe ja rakenduste kaitsetarbe määramine (näidis)

ID	Rakendus	Alusteave	Valdkonnad	Kaitsetarve	Põhjendus
001	Amphora	Dokumendihaldus	V1-V3	suur	V2
002	Spoku	Taotluste esitamine ja menetlemine	V1-V3	suur	V2
003	Evald	Jäätmevaldajate register	V2.4	normaalne	V2.4
004	Arno	Haridusteenused	V2.2	normaalne	V2.2
005	Word, Excel, Powerpoint (58tk)	-	V1-V3	normaalne	(*)
006	Koduleht	Avalik info	V3.1	normaalne	V3.1
007	Facebook	Avalik info	V3.1	normaalne	V3.1
008	Veera	Eelarve	V3.1.1	normaalne	V3.1.1
009	Persona	Personaliinfo	V3.1	normaalne	V3.1
010	Outlook (58tk)	Kirjavahetus ja kalendrid	V1-V3	normaalne	V2(*)
011	Exchange	Kirjavahetus ja kalendrid	V1-V3	normaalne	V2(*)
012	OneDrive	Valdkonnakohased failid (privaatsed ja jagatud sh väliste osapooltega)	V1-V3	normaalne	V2(*)
013	Synology (5tk)	Valdkonnakohased (privaatsed ja jagatud)	V1-V3	normaalne	V2(*)
014	Autocad (4tk)	Kasutajate profiilid	V2.3	normaalne	V2.3
015	Brave (2tk)	Kasutajate profiilid	V3.1.3	normaalne	V3.1.3

[13] Siin toodud määratlust tuleb käsitleda näidisena, mille peab iga rakendaja täitma oma andmetega.

016	Chrome (100tk)	Kasutajate profiilid	V1-V3	normaalne	V2
017	Rahvastikuregister	Elukoha info	V2.1, V2.2	suur	V2.1

Tabel 15 Alusteabe ja rakenduste kaitsetarbe määramine (näidis)

4.5 IT-süsteemide kaitsetarbe määramine

IT-süsteemid kaitsetarbe määramiseks täiendatakse peatükis *3.4 IT-süsteemid* koostatud kaardistust *Tabel 5 IT-süsteemid* alusteabe ja rakenduste analüüsi käigus saadud kaitsetarbe määratlustega *Tabel 15 Alusteabe ja rakenduste kaitsetarbe määramine (näidis).*

Alusteabe ja rakenduste kaitsetarve "pärandatakse" sihtobjektidele, milleks antud juhul on IT-süsteemid. Mitut rakendust teenindavale IT-süsteemidele määratakse nendest kõrgeima kaitsetarbega rakendus(t)e kaitsetarve ja see seos dokumenteeritakse veerus „Põhjendus“. Siinjuures arvestatakse sihtobjektide omavahelisi sõltuvusahelaid ja koostoimeid.

Tabel 17 IT-süsteemide kaitsetarbe määratlemine (näidis[14])

ID	IT-süsteem	Platvorm	Rakendused	Kaitsetarve	Põhjendus
101	Active Directory	Win2019	005, 010-013	normaalne	005, 010-013
102	Viirusetõrje haldus	Linux	010, 011	normaalne	010, 011
103	NAS (5tk)	Synology	013	normaalne	013
104	Tulemüür (4tk)	Fortigate	001-004, 008-013, 017	suur	001, 002, 017
105	Tulemüür	Fortigate	001-004, 008-013, 017	suur	001, 002, 017
106	Switch (8tk)	Fortiswitch	001-004, 008-013, 017	suur	001, 002, 017
107	Switch	Fortiswitch	001-004, 008-013, 017	suur	001, 002, 017
108	Printerid (5tk)	HP LaserJet	001-005	suur	001, 002
109	Printerid (6tk)	Canon MF	001-005	suur	001, 002
110	Kombain (3tk)	HP MFP	001-005	suur	001, 002

[14] Siin toodud määratlust tuleb käsitleda näidisena, mille peab iga rakendaja täitma oma andmetega.

111	Plotter	HP	014	normaalne	014
112	Nutitelefon (15tk)	Redmi	010	normaalne	010
113	Nutitelefon (10tk)	Samsung	010	normaalne	010
114	Tahvel (5tk)	GalaxyTab	002, 010	suur	002
115	Sülearvuti (25tk)	HP	001-017	suur	001, 002, 017
116	Sülearvuti (35tk)	Lenovo	001-017	suur	001, 002, 017
117	Tööjaam (15tk)	Thinkstation	001-017	suur	001, 002, 017
118	Tööjaama OS (75tk)	Win11	001-017	suur	001, 002, 017
119	X-Tee turvaserver	Riigipilv	001-004	suur	001, 002
120	X-Tee HSM	Riigipilv	001-004	suur	001, 002

Tabel 16 IT-süsteemide kaitsetarbe määratlemine (näidis)

4.6 Hoonete ja ruumide kaitsetarbe määramine

Hoonete ja ruumide kaitsetarbe määramiseks täiendatakse peatükis *3.5 Hooned* ja ruumid koostatud kaardistust *Tabel 6 Hooned ja ruumid (näidis)* kahjuanalüüsi käigus saadud kaitsetarbe määratlustega *Tabel 14 Kaitsetarbe koondtabel (näidis).*

Valdkondade kaitsetarve "pärandatakse" sihtobjektidele, milleks antud juhul on hooned ja ruumid. Mitut valdkonda teenindavale sihtobjektile määratakse nendest valdkondadest kõrgeima kaitsetarbega valdkondade kaitsetarve, ja see seos dokumenteeritakse veerus „Põhjendus“. Siinjuures arvestatakse sihtobjektide omavahelisi sõltuvusahelaid ja koostoimeid.

Näiteks võivad mõned hooned ja ruumid mõjutada valdkondade toimimist kaudselt, kuna neis on olulised IT- ja/või tehnosüsteemid. Sellisel juhul dokumenteeritakse põhjenduse veerus ka vastava sihtobjekti tunnus.

Tabel 17 Hoonete ja ruumide kaitsetarbe määratlemine (näidis[15])

ID	Nimetus	Asukoht	Valdkonnad	Kaitsetarve	Põhjendus

[15] Siin toodud määratlust tuleb käsitleda näidisena, mille peab iga rakendaja täitma oma andmetega.

201	Raekoda	Raekoja 1	V1-V3	suur	V2.1, 205
202	Teenuskeskus (2tk)	Teenuse tn 15 Keskuse tn 18	V2	normaalne	ei ole V2.1
203	Klienditeenindus (12tk)	201, 202	V2	suur	V2.1 (2tk)
204	Mobiiltöökoht (5tk)	-	V2.1, V2.4	suur	V2.1 (1tk)
205	Serveriruum	201	V1-V3	suur	V2.1, 105,107
206	Seadmekapp (2tk)	202	V2	normaalne	ei ole V2.1

Tabel 17 Hoonete ja ruumide kaitsetarbe määratlemine (näidis)

5 Kaitseala modelleerimine

Pärast valdkondade, rakenduste, IT-süsteemide ja sidevõrkude kaitsetarbe määramist on järgmiseks sammuks tuvastada vastavad moodulid ja kohaldada moodulites esitatud meetmed vastavale sihtobjektidele. Meetmete kohaldamise tulemus võib tähendada, et kõik või ainult teatud mooduli meetmed on KOV-i infoturbe seisukohalt olulised. Samuti tuleks tuvastada E ITS nõuetest tulenevate meetmete asjakohasus konkreetses KOV-is.

5.1 Rakendused

Käesoleva profiili ülesehitus eeldab, et erinevad KOV-id võivad sama eesmärgi saavutamiseks kasutada erinevaid rakendusi, milliste funktsionaalsus on sarnane. Lisaks võimaldab profiil paindlikkust ka selles osas, kas konkreetset eesmärgi saavutamiseks vajalikku rakendust haldab KOV ise, on see väljasttellitud või pilvrakendus.

Profiili efektiivseks rakendamiseks tuleks esmase kaardistuse järel rakendused sobivalt rühmitada so jagada kategooriatesse ja liikidesse. E-ITS soovitab rühmitamisel juhinduda etalonturbe kataloogi moodulite loendist.

Käesolevas profiilis on rakendused rühmitatud kategooriatesse ja liikidesse, mis on moodustatud vastavalt E-ITS moodulitele APP ja OPS. Iga rakendaja võib rühmitamisel kasutada oma harjumuspäraseid termineid, kuid peab olema suuteline need seadma vastavusse E-ITS moodulitega.

Rakenduste rühmitamise **näide** E-ITS APP mooduli põhjal:

Tabel 18 Rakenduste kategooriad (näidis)

Rakenduse kategooria
Kataloogiteenus (autentimine ja autoriseerimine)
Samba
Kubernetes
DNS
Failiserver
Kontoritarkvara
Andmebaasisüsteem
Rühmatarkvara (Exchange ja Outlook)
Veebiserver
Veebibrauser
Veebirakendus
X-tee andmeteenus

Tabel 18 Rakenduste kategooriad (näidis)

Rakenduse liigi määramine annab võimaluse tunnetuslikult hinnata enda ja teenusepakkuja vastutuse piire turvameetmete määramisel, aktsepteerimisel ja rakendamisel. Seda läbivalt kogu rakenduse elutsükli jooksul.

Rakenduste rühmitamise **näide** E-ITS OPS põhjal:

Tabel 19 Rakenduste liigid (näidis)

Lühend	Rakenduse liik
Oma	Oma rakendused
Välj	Väljasttellitud rakendused
Pilv	Pilverakendused

Tabel 19 Rakenduste liigid (näidis)

Alternatiivina rakenduste ja alusteabe kaardistamisele valdkondade kaupa võib olemasoleva info põhjal kaardistada rakendused kategooriate kaupa koostades alltoodud näidiste põhjal nimekirja kõikidest antud kategooria rakendustest, mida KOV-is kasutatakse ning seejärel mõelda läbi, millised valdkonnad neid rakendusi kasutavad ja millist teavet töötlevad ning lõpuks määrata rakenduse tehniline lahendus ja liik vastavalt tabelitele 18 ja 19. Saadud kaardistus tuleb koos valdkonna juhi ja -spetsialistidega üle vaadata ning veenduda kaardistuse täielikkuses.

Tabel 20 Alusteabe ja rakenduste kaitsetarbe määramine (näidis[16])

ID	Rakendus	Kaitsetarve	Põhjendus	Kategooria	Liik
001	Amphora	suur	V2	Veebirakendus	Pilv
002	Spoku	suur	V2	Veebirakendus	Pilv
003	Evald	normaalne	V2.4	Veebirakendus	Pilv
004	Arno	normaalne	V2.2	Veebirakendus	Pilv
005	Word, Excel, Powerpoint (58tk)	normaalne	(*)	Kontoritarkvara	Oma
006	Koduleht	normaalne	V3.1	Veebiserver	Välj
007	Facebook	normaalne	V3.1	Veebirakendus	Pilv
008	Veera	normaalne	V3.1.1	Veebirakendus	Pilv
009	Persona	normaalne	V3.1	Veebirakendus	Pilv
010	Outlook (58tk)	normaalne	V2(*)	Rühmatarkvara	Oma
011	Exchange	normaalne	V2(*)	Rühmatarkvara	Pilv
012	OneDrive	normaalne	V2(*)	Veebirakendus	Pilv
013	Synology (5tk)	normaalne	V2(*)	Failiserver	Oma

[16] Siin toodud määratlust tuleb käsitleda näidisena, mille peab iga rakendaja täitma oma andmetega.

014	Autocad (4tk)	normaalne	V2.3	Kontoritarkvara	Oma
015	Brave (2tk)	normaalne	V3.1.3	Veebibrauser	Oma
016	Chrome (100tk)	normaalne	V2	Veebibrauser	Oma
017	Rahvastikuregister	suur	V2.1	Veebirakendus	Pilv

Tabel 20 Alusteabe ja rakenduste kaitsetarbe määramine (näidis)

Tuleb tähele panna, et kui sama rakendust kasutatakse infoturbe mõistes erineval otstarbel, tuleb nad kaardistuses näidata erinevatel ridadel.

Näiteks kui konkreetset veebibrauserit kasutatakse andmekogude administreerimiseks (Näiteks rakendus 015 Brave), võivad sellele rakenduda tavapärasest erinevad nõuded ja sellisel juhul tuleks need näidata kaardistuses eraldi real ning näidata nende seotust valdkonnaga, mille osaks on andmekogude administreerimine.

Samas, kui KOV-is on 100 töötajat, kes kõik kasutavad tavapärase töö tegemiseks sarnasel viisil veebibrauserit, võetakse kõik need veebibrauserid kaardistuse tabelis arvele ühel real (Näiteks rakendus 016 Chrome).

Et rakenduste rühmitamise mõttest veel paremini aru saada, on soovitatav tutvuda käesoleva profiili süsteemimooduli peatüki *APP. Rakendused* ja protsessimooduli peatüki *OPS. Käidutööd* ülesehitusega: iga konkreetne meede rakendatakse selgitatud viisil kõikidele vastavasse rühma kuuluvatele rakendustele.

Näiteks tuleb kategooriasse veebibrauser kuuluvate rakenduste, so 015 Brave (2tk) ja 016 Chrome (100tk) puhul veenduda ja dokumenteerida, et igas konkreetses Chrome ja Brave brauseris on rakendatud APP.1.2.M6 alapunkt e) Paroolihalduri paroolide sünkroniseerimine pilvteenuse vahendusel on keelatud.

Sageli on raske vahet teha, kas tegemist on väljasttellitud rakendusega või pilveteenusega. E-ITS kontekstis on sellise vahe tegemine väga oluline, kuna rakendatavad turvameetmed on sisult ja mahult erinevad. Tulenevalt E-ITS turvameetmete ülesehitusest soovitame lähtuda eelkõige sellest, kas KOV saab sõlmida teenuslepingu enda tingimustel (väljasttellimine) või peab aktsepteerima teenusepakkuja tingimused (pilveteenus). Sellest loogikast lähtudes on näiteks rahvastikuregister pilveteenus, sest selle kasutamiseks peab KOV aktsepteerima rahvastikuregistri kasutustingimused sh turvameetmed ja protseduurid, mis on kõigi KOV-ide jaoks samad.

Samas, kui rakendus on kasutusele võetud hanke tulemusena ning hankedokumentidega on määratud nõuded ja tingimused pakkujale ja pakutavale, on tegemist väljasttellitud rakendusega.

5.2 IT-süsteemid

Profiili efektiivseks rakendamiseks tuleks esmase kaardistuse järel IT-süsteemid sobivalt rühmitada so jagada kategooriatesse. E-ITS soovitab rühmitamisel juhinduda etalonturbe kataloogi moodulite loendist.

Käesolevas profiilis on IT-süsteemid rühmitatud kategooriatesse, mis on moodustatud vastavalt E-ITS moodulile SYS. Iga rakendaja võib rühmitamisel kasutada oma harjumuspäraseid termineid, kuid peab olema suuteline need seadma vastavusse E-ITS moodulitega.

Rakenduste rühmitamise **näide** E-ITS SYS mooduli põhjal:

Tabel 21 IT-süsteemide kategooriad (näidis)

Lühend	Kategooria
Arvuti	Klientarvuti
VoiP	VoiP-telefon
Keskj	Telefonikeskjaam
Linux	Linux või Unix server
Mob	Mobiilseade
Print	Printer, kombain jms
Võrk	Ruuter, switch, WLAN AP
Tmüür	Tulemüür
USB	Irdandmekandja
VPN	VPN
Wserv	Windows server
Xtee	X-Tee turvaserver

Tabel 21 IT-süsteemide kategooriad (näidis)

Tabel 22 IT-süsteemide rühmitamine (näidis[17])

ID	IT-süsteem	Platvorm	Kaitsetarve	Kategooria	Liik
101	Active Directory	Win2019	normaalne	Wserv	Oma
102	Viirusetõrje haldus	Linux	normaalne	Linux	Oma
103	NAS (5tk)	Synology	normaalne	Linux	Oma
104	Tulemüür (4tk)	Fortigate	Suur	Tmüür	Oma
105	Tulemüür	Fortigate	Suur	Tmüür	Oma
106	Switch (8tk)	Fortiswitch	Suur	Võrk	Oma

[17] Siin toodud määratlust tuleb käsitleda näidisena, mille peab iga rakendaja täitma oma andmetega.

107	Switch	Fortiswitch	Suur	Võrk	Oma
108	Printerid (5tk)	HP LaserJet	Suur	Print	Välj
109	Printerid (6tk)	Canon MF	Suur	Print	Oma
110	Kombain (3tk)	HP MFP	Suur	Print	Oma
111	Plotter	HP	normaalne	Print	Oma
112	Nutitelefon (15tk)	Redmi	normaalne	Mob	Oma
113	Nutitelefon (10tk)	Samsung	normaalne	Mob	Oma
114	Tahvel (5tk)	GalaxyTab	Suur	Mob	Oma
115	Sülearvuti (25tk)	HP	Suur	Mob, Arvuti	Välj
116	Sülearvuti (35tk)	Lenovo	Suur	Mob, Arvuti	Oma
117	Tööjaam (15tk)	Thinkstation	Suur	Arvuti	Oma
118	Tööjaama OS (75tk)	Win11	Suur	Arvuti	Oma
119	X-Tee turvaserver	Riigipilv	Suur	Xtee	Pilv
120	X-Tee HSM	Riigipilv	Suur	Xtee	Pilv

Tabel 22 IT-süsteemide rühmitamine (näidis)

5.3 Hooned ja ruumid

Profiili efektiivseks rakendamiseks tuleks esmase kaardistuse järel hooned ja ruumid sobivalt rühmitada so jagada kategooriatesse. E-ITS soovitab rühmitamisel juhinduda etalonturbe kataloogi moodulite loendist.

Käesolevas profiilis on hooned ja ruumid rühmitatud kategooriatesse, mis on moodustatud vastavalt E-ITS moodulile INF. Iga rakendaja võib rühmitamisel kasutada oma harjumuspäraseid termineid, kuid peab olema suuteline need seadma vastavusse E-ITS moodulitega.

Rakenduste rühmitamise **näide** E-ITS INF mooduli põhjal:

Tabel 23 Ruumide kategooriad (näidis)

Lühend	Kategooria
Hoone	hoone üldiselt
Serv	serveriruum või andmekeskus
Tehn	tehnilise taristu ruum või kapp
Andm	andmekandjate arhiiv
Büroo	bürootöökoht
Nõup	Koosoleku-, ürituse- ja koolitusruum
Mob	Mobiiltöökoht

Tabel 23Ruumide kategooriad (näidis)

Tabel 24 Hoonete ja ruumide rühmitamine (näidis[18])

ID	Nimetus	Asukoht	Valdkonnad	Kaitsetarve	Kategooria
201	Raekoda	Raekoja 1	V1-V3	suur	Hoone
202	Teenuskeskus (2tk)	Teenuse tn 15 Keskuse tn 18	V2	normaalne	Hoone
203	Klienditeenindus (12tk)	201, 202	V2	suur	Büroo
204	Mobiiltöökoht (5tk)	-	V2.1, V2.4	suur	Mob
205	Serveriruum	201	V1-V3	suur	Serv
206	Seadmekapp (2tk)	202	V2	normaalne	Tehn

Tabel 24 Hoonete ja ruumide rühmitamine (näidis)

[18] Siin toodud määratlust tuleb käsitleda näidisena, mille peab iga rakendaja täitma oma andmetega.

6 Infoturbe meetmete rakendusplaani (IMR) koostamine

Kõiki infoturbenõudeid ei ole võimalik rakendada korraga. IMR-i koostamisel tuleb veenduda, et olulised turvanõuded saaks täidetud varakult ning vastavad turvameetmed põhiriskide katmiseks ja tervikliku infoturbe loomiseks oleks rakendatud esmajärjekorras.

Käesolevas profiilis esitatud kaitseala mudelis on iga mooduli juures näidatud selle asjakohasus ning sihtobjektide grupid, millele seda rakendada. Lisaks on antud soovitusi, kuidas moodulit rakendada ning näidatud, millise prioriteediga peaks moodulit rakendama.

Prioriteet näitab ainult vastava mooduli nõuete rakendamise soovitatavat ajalist järjekorda ja seda ei tohi tõlgendada kui moodulite olulisust üksteise suhtes. Nõutava infoturbetaseme saavutamiseks tuleb rakendada kõik asjakohased moodulid.

P1 prioriteediga moodulid on tõhusa turbeprotsessi aluseks ja tuleks seetõttu rakendada esmajärjekorras. Siia alla kuuluvad eelkõige moodulid ISMS turbehaldus, OPR organisatsioon ja personal, OPS.1 oma IT-süsteemide turvalisuse tagamise põhiülesanded.

P2 prioriteediga moodulid on vajalikud kaitseala oluliste osade infoturbe jätkusuutlikuks tagamiseks ning need tuleks reaaliseerida järgmisena.

P3 moodulite rakendamine on vajalik soovitud turbetaseme saavutamiseks ja ka need tuleb rakendada, siiski on soovitatav käsitleda neid alles pärast prioriteetsemate moodulite rakendamist.

Samuti võib olla otstarbekas järjestada tegevused valdkondade kaupa. Näiteks võib alustada esmase turbetaseme saavutamise sotsiaalvaldkonnas, kuna osapoolte sotsiaalteenuste kättesaadavusele ja alusandmete turvalisusele on kõrgendatud ootused.

Teise sammuna võib kaaluda meetmete rakendamist kantseleis ja seejärel halduse valdkonnas.

Suure tõenäosusega on nende kolme valdkonna katmisega kaetud suurem osa KOV kaitseala sihtobjektidest ning need mis ei ole, saab ära lahendada neljandas etapis.

IMR tuleks kohe alguses koostada iteratiivne, mitte tegutseda rangelt prioriteetide järjekorras. Iteratiivne lähenemine võimaldab tegevuskava kohendada vastavalt muutustele regulatsioonide nõuetes, lepingulistes kohustustes ning ümbritsevas infoturbeolukorras luues eeldused ISMS nõuetest tulenevaks infoturbeprotsessi ning turvameetmete pidevaks ja jätkusuutlikuks toimimiseks.

Infoturbe meetmete rakendusplaan (IMR) peab sisaldab kõiki modelleerimise käigus tuvastatud E-ITS turvameetmeid. IMR-i haldamiseks tuleb valida sobilik tehniline vahend, mille abil on võimalik esitada meetmete rakendamise hetkeseisu.

Infoturbe meetmete rakendusplaanis on iga meetme kohta sisestatud vähemalt:

- meetme identifikaator;
  Näiteks: APP.1.2.M6.e

- meetme nimetus;
  Näiteks: Paroolihalduri paroolide sünkroniseerimine pilvteenuse vahendusel on keelatud

- valdkond;
  Näiteks: Kantselei

- meetme teostatuse määr;
  Näiteks: Meede on rakendatud kõikides tööjaamades ja sülearvutites

- meetme rakendamise puhul selgitus, kuidas meede on organisatsioonis rakendatud;
  Näiteks: Meede rakendatakse kasutades tööjaamade keskhalduse tarkvara

- meetme mitterakendamise puhul juhtkonna aktsept meetme mitterakendamisest tulenevatele jääkriskidele või meetme mittekohaldamise põhjendus;
  Näiteks: linnavalitusus on aktsepteerinud meetme mitterakendamise mobiiltelefonides ja tahvalarvutites kuni sobiva keskhalduse tarkvara hankeprotsessi lõpuni.

- meetme osalise rakendamise puhul täpsustav selgitus, milliste valdkondade, varade või alammeetme osas on meede täitmata;
  Näiteks: Meetmed ei ole rakendatud mobiiltelefonide ja tahvelarvutite puhul kuni vastava keskhalduse tarkvara hankimiseni

- meetme rakendamise eest vastutaja;
  Näiteks: aruandev isik: linnasekretär, vastutav isik: IT-juht

- meetme rakendamise või meetme järgmise sisulise ülevaatuse tähtaeg.
  Näiteks: 31.12.2023

7 Kasutatud materjalid

1. Eesti infoturbestandard E-ITS 2022, RIA
2. E-ITS profiil perearstidele v.2023_1, RIA
3. Information Security Management Systems (ISMS), BSI Standard 200-1, Version 1.0, October 2017
4. IT-Grundschutz Methodology, BSI-Standard 200-2, Version 1.0, October 2017
5. IT-Grundschutz- Kompendium, Reguvis Fachmedien GmbH 2023
6. Risk Analysis based on IT Grundschutz, BSI Standard 200-3, Version 1.0, October 2017
7. Business Continuity Management, BSI Standard 100-4, Version 2009
8. Business Continuity Management, BSI Standard 200-4, Community Draft 2.0 2022
9. Information security management systems requirements, ISO/IEC 27001:2022
10. Information security, cybersecurity and privacy protection — guidance on managing information security risks, ISO/IEC 27005:2022
11. IT-Grundschutz, Online-Kurs, Bundesamt für Sicherheit in der Informationstechnik 2018
12. Erstellung eines IT-Grundschutz- Profils für Rettungsleitstellen, Masterarbeit zur Erlangung des Grades eines Master of Science, Henning Schmidtpott 02.01.2020
13. Basis-Absicherung Kommunalverwaltung, IY-Grundschutz-profil ARBEITSGRUPPE KOMMUNALE BASIS-ABSICHERUNG (AG KOBA) mit Unterstützung durch Deutscher Städtetag, Deutscher Landkreistag, Deutscher Städte- und Gemeindebund 31.03.2022

Lisa 1. Kaitseala modelleerimine

Moodulite üldine rakendamine

Profiil käsitleb ainult **põhimeetmete** valikut ja kohandamist KOV oludega. Kui konkreetne KOV on kahjuanalüüsi tulemusel leidnud, et E-ITS rakendamise esimeses etapis tuleb suurest või väga suurest kaitsetarbest tulenevalt rakendada mõne(de)le sihtobjektidele standard- või kõrgmeetmed, tuleb täiendavalt teostada vastav riskianalüüs ja modelleerimine.

Veegu „J/E/?“ tuleb tõlgendada järgmiselt:

- „Jah“ – Moodul tuleb rakendada;
- „Ei?“ – Enamasti ei kuulu moodul rakendamisele tulenevalt viimases veerus toodud põhjendusele (NB! Iga rakendaja peab siinkohal kaaluma põhjenduse paikapidavust oma organisatsioonis!);
- „?“ – Kui konkreetses KOV-is kehtib viimases veerus toodud põhjendus, tuleb veergu kanda „Ei“ ning moodul ei kuulu rakendamisele. Vastasel juhul tuleb veergu kanda „Jah“ ning moodul kuulub rakendamisele. Enamasti tähendab „?“ seda, et KOV-is on kindlasti olemas sihtobjekt, näiteks välisveeb, kuid rakendatavad meetmed sõltuvad näiteks sellest, kas antud juhul välisveeb on pilveteenus, väljasttellitud teenus või KOV enda IT teenus.

Profiili koostamisel ei ole arvestatud kõikide KOV-ide eripäradega. Seetõttu tuleb ka iga „Ei“ ehk mitterakendamisele kuuluva mooduli juures veenduda, et toodud põhjendus konkreetses KOV-is kehtib.

Profiili loomisel on arvestatud tüüpsete KOV-ide infotehnoloogia kasutust, IT ressursse ja infoturbe küpsustaset, mis vastab E-ITS-s toodud **põhiturbe** eeldustele. **Profiil ei kehtesta turbeviisi**, see tuleb igal rakendajal ise määrata. Sellegipoolest võimaldab profiilis esitatud metoodika täiendada infoturbe meetmete rakendusplaani standard- ja kõrgmeetmetega.

ISMS. Turbehaldus

Moodul		J/E/?	Prioriteet	Põhjus, kui ei rakenda
ISMS.1	**Turbehaldus**	**Jah**	**P1**	
	M1-M4, M6-M15	Jah		
	M5	Ei?		Välist infoturbejuhti ei ole

ORP. Organisatsioon ja personal

Moodul		J/E/?	Prioriteet	Põhjus, kui ei rakenda
ORP.1	**Infoturbe korraldus**	**Jah**	**P1**	
	M1, M2	Jah		
	M3, M4, M15	Jah		Vajadusel täiendada olemasolevaid asjakohaseid dokumente.
ORP.2	**Personal**	**Jah**	**P1**	
	M1-M5, M14, M15	Jah		Vajadusel täiendada olemasolevaid asjakohaseid dokumente.
ORP.3	**Infoturbe teadlikkuse tõstmine ja koolitus**	**Jah**	**P1**	
	M1, M3	Jah		
ORP.4	**Identiteedi- ja õiguste haldus**	**Jah**	**P1**	
	M1-M7	Jah		Vajadusel täiendada olemasolevaid asjakohaseid dokumente.

	M8, M9, M22, M23	Jah		
ORP.5	**Vastavusehaldus (nõuete haldus)**	**Jah**	**P3**	
	M1, M2			Võimalusel teha koostööd vastavate katusorganisatsioonidega

CON. Kontseptsioonid ja metoodikad

Moodul		J/E/?	Prioriteet	Põhjus, kui ei rakenda
CON.1	Krüptokontseptsioon	Jah	P3	
CON.2	Isikuandmete kaitse	Jah	P2	
CON.3	Andmevarunduse kontseptsioon	Jah	P1	
CON.6	Andmete kustutus ja hävitamine	Jah	P1	
CON.7	Välislähetuste infoturve	Jah	P3	
CON.8	Tarkvaraarendus	Ei?		KOV eesmärkide saavutamiseks vajalike protsesside hulka ei kuulu tarkvaraarendus
CON.9	Teabevahetus	Jah	P2	Teabevahetust reguleerivad näiteks Teenuste korraldamise ja teabehalduse alused; AvTS; jms
CON.10	Veebirakenduste arendus	Ei?		KOV eesmärkide saavutamiseks vajalike protsesside hulka ei kuulu veebirakenduste arendus

OPS. Käidutööd

Moodul		J/E/?	Prioriteet	Põhjus, kui ei rakenda
OPS.1.1.2	IT-haldus	Jah	P1	
OPS.1.1.3	Paiga- ja muudatusehaldus	Jah	P1	
OPS.1.1.4	Kaitse kahjurprogrammide eest	Jah	P1	
OPS.1.1.5	Logimine	Jah	P1	
OPS.1.1.6	Tarkvara testimine ja kasutuselevõtt	Ei?		KOV eesmärkide saavutamiseks vajalike protsesside hulka ei kuulu tarkvara testimine
OPS.1.1.7	Süsteemihaldus	Jah	P1	
OPS.1.2.2	Arhiveerimine	Jah	P3	
OPS.1.2.4	Kaugtöö	Jah	P2	
OPS.1.2.5	Kaughooldus	Jah	P3	
OPS.1.2.6	Kellade sünkroniseerimine	Jah	P2	
OPS.2.1	Väljasttellimine	Jah	P2	
OPS.2.2	Pilvteenuste kasutamine	Jah	P2	
OPS.3.1	Teenuseandja infoturve	Ei?		KOV eesmärkide saavutamiseks vajalike protsesside hulka ei kuulu IT-teenuste osutamine. Kui KOV siiski tegutseb teenuseandjana, tuleks seda käsitleda eraldi valdkonnana ja rakendada sellele valdkonnale asjakohane infoturbesüsteem.

DER. Avastamine ja reageerimine

Moodul		J/E/?	Prioriteet	Põhjus, kui ei rakenda
DER.1	Turvaintsidentide avastamine	Jah	P1	
DER.2.1	Turvaintsidentide käsitlus	Jah	P1	
DER.2.2	IT-kriminalistika võimaldamine	Jah	P3	
DER.2.3	Ulatuslike turvaintsidentide lahendamine	Jah	P3	
DER.3.1	Auditid ja läbivaatused	Jah	P3	
DER.3.2	Infoturbe vastavusauditid	Jah	P3	
DER.4	Avariihaldus	Jah	P3	

INF. Taristu

Moodul		J/E/?	Prioriteet	Põhjus, kui ei rakenda
INF.1	Hoone üldiselt	Jah	P2	
INF.2	Serveriruum ja andmekeskus	Jah	P2	
INF.5	Tehnilise taristu ruum või kapp	Jah	P2	

INF.6	Andmekandjate arhiiv	Jah	P2	
INF.7	Bürootöökoht	Jah	P2	
INF.8	Kodutöökoht	Jah	P2	
INF.9	Mobiiltöökoht	Jah	P2	
INF.10	Koosoleku-, ürituse- ja koolitusruum	Jah	P2	
INF.11	Sõidukite IT-komponendid	Ei?		KOV eesmärkide saavutamiseks vajalike protsessid ei sõltu sõidukite IT-komponentidest.
INF.12	Kaabeldus	Jah	P2	
INF.13	Hoonete tehniline haldus	Jah	P2	
INF.14	Hooneautomaatikasüsteemid	?	P2	Hooneautomaatikasüsteemid ei ole kasutusel või ei ole liidestatud IT-süsteemidega

NET. Võrgud ja side

Moodul		J/E/?	Prioriteet	Põhjus, kui ei rakenda
NET.1.1	Võrgu arhitektuur ja lahendus	Jah	P2	
NET.1.2	Võrguhaldus	Jah	P2	
NET.2.1	Raadiokohtvõrgu käitamine	Jah	P2	
NET.2.2	Raadiokohtvõrgu kasutamine	Jah	P2	
NET.3.1	Ruuter ja kommutaator	Jah	P2	
NET.3.2	Tulemüür	Jah	P2	
NET.3.3	Virtuaalne privaatvõrk (VPN)	Jah	P2	
NET.4.1	Telefonikeskjaam	?	P2	Telefonikeskjaam puudub
NET.4.2	IP-telefon (VoIP)	?	P2	IP-telefonid puuduvad

SYS. IT-süsteemid

Moodul		J/E/?	Prioriteet	Põhjus, kui ei rakenda
SYS.1.1	Server üldiselt	?	P2	Serverid puuduvad so kõik rakendused on väljasttellitud või pilverakendused

SYS.1.2.2	Windows Server 2012	?	P2	Windows serverid puuduvad
SYS.1.3	Linuxi ja Unixi server	?	P2	Linuxi ja Unixi serverid puuduvad
SYS.1.5	Virtualiseerimissüsteem	?	P2	Virtualiseerimissüsteemid puuduvad
SYS.1.6	Konteinerdus	?	P2	Konteinerdus puudub
SYS.1.8	Salvestilahendused	?	P2	Salvestilahendused puuduvad
SYS.2.1	Klientarvuti üldiselt	Jah	P2	
SYS.2.2.3	Windows 10 klient	?	P2	Ei ole kasutusel
SYS.2.3	Linuxi ja Unixi klient	?	P2	Ei ole kasutusel
SYS.2.4	macOS-i klient	?	P2	Ei ole kasutusel
SYS.3.1	Sülearvutid	?	P2	Ei ole kasutusel
SYS.3.2.1	Nutitelefon ja tahvelarvuti üldiselt	?	P2	Ei ole kasutusel
SYS.3.2.2	Mobiilseadmete haldus (MDM)	?	P2	Ei ole kasutusel või mobiilseadmed ei ole integreeritud organisatsiooni IT-taristuga
SYS.3.2.3	Organisatsiooni iOS	?	P2	Ei ole kasutusel
SYS.3.2.4	Android	?	P2	Ei ole kasutusel
SYS.3.3	Mobiiltelefon	?	P2	Ei ole kasutusel
SYS.4.1	Printer ja kontorikombain	Jah	P2	

SYS.4.3	Sardsüsteemid (embedded systems)	Ei?		KOV eesmärkide saavutamiseks vajalike protsessid ei sõltu sardsüsteemidest
SYS.4.4	Esemevõrgu (IoT) seade üldiselt	Ei?		KOV eesmärkide saavutamiseks vajalike protsessid ei sõltu esemevõrgu seadmetest
SYS.4.5	Irdandmekandjad	?	P2	Ei ole kasutusel
SYS.EE	X-tee turvaserver	?	P2	Väljasttellitud

APP. Rakendused

Moodul		J/E/?	Prioriteet	Põhjus, kui ei rakenda
APP.1.1	Kontoritarkvara	Jah	P2	
APP.1.2	Veebibrauser	Jah	P2	
APP.1.4	Mobiilirakendused (äpid)	Ei?		Ei ole kasutusel
APP.2.1	Kataloogiteenus üldiselt	Jah	P2	
APP.2.2	Active Directory	?	P2	Ei ole kasutusel või on väljasttellitud või pilveteenus
APP.2.3	OpenLDAP	?	P2	Ei ole kasutusel või on väljasttellitud või pilveteenus
APP.3.1	Veebirakendused	?	P2	Ei ole kasutusel või on väljasttellitud või pilveteenus

APP.3.2	Veebiserver	?	P2	Ei ole kasutusel või on väljasttellitud või pilveteenus
APP.3.3	Failiserver	?	P2	Ei ole kasutusel või on väljasttellitud või pilveteenus
APP.3.4	Samba	?	P2	Ei ole kasutusel või on väljasttellitud või pilveteenus
APP.3.6	DNS-server	?	P2	Ei ole kasutusel või on väljasttellitud või pilveteenus
APP.4.3	Andmebaasisüsteemid	?	P2	Ei ole kasutusel või on väljasttellitud või pilveteenus
APP.4.4	Kubernetes	?	P2	Ei ole kasutusel või on väljasttellitud või pilveteenus
APP.5.2	Microsoft Exchange ja Outlook	?	P2	Ei ole kasutusel või on väljasttellitud või pilveteenus
APP.5.3	E-posti server ja klient üldiselt	?	P2	Ei ole kasutusel või on väljasttellitud või pilveteenus
APP.6	Tarkvara üldiselt	Jah	P2	
APP.7	Tellimustarkvara arendus	Ei?		KOV eesmärkide saavutamiseks vajalike protsesside hulka ei kuulu tellimustarkvara arendus

APP.EE.1	X-tee andmeteenus	Jah	P2	

IND. Tööstuse IT

Moodul		J/E/?	Prioriteet	Põhjus, kui ei rakenda
IND.1	Käidu- ja protsessijuhtimissüsteemid	Ei?		KOV eesmärkide saavutamiseks vajalike protsessid ei sõltu tööstuse IT lahendustest
IND.2	Tööstusautomaatika	Ei?		KOV eesmärkide saavutamiseks vajalike protsessid ei sõltu tööstuse IT lahendustest
IND.3.2	Käidutehnoloogia komponentide kaughooldus	Ei?		KOV eesmärkide saavutamiseks vajalike protsessid ei sõltu tööstuse IT lahendustest

Süsteemimoodulite rakendamine sihtobjektidele

Tabelites olev rida „Sihtobjektid“ sisaldab nimekirja sihtobjektide rühmadest so ülal defineeritud liikidest ja kategooriatest. Tabelis näidatud meetmed tuleb rakendada kõikidele sihtobjektidele, mis kuuluvad vastavalt märgistatud sihtobjektide rühma.

Näiteks tuleb mooduli APP.1.2: Veebibrauser meetmed rakendada kõikidele rakendustele, mis kuuluvad kategooriasse „Veebibrauser“ ja liiki „Oma“. Seega tuleb 015 Brave (2tk) ja 016 Chrome (100tk) puhul veenduda ja dokumenteerida, et igas konkreetses Chrome ja Brave brauseris on mh rakendatud APP.1.2.M6 alapunkt e) Paroolihalduri paroolide sünkroniseerimine pilvteenuse vahendusel on keelatud.

APP. Rakendused

Moodul	APP.1.1: Kontoritarkvara
Meetmed	M2, M3, M17
Sihtobjektid	Kontoritarkvara; Oma, Pilv. *Näide: 005, 014.*
Juhised ja kommentaarid	

Moodul	APP.1.2: Veebibrauser
Meetmed	M1-M3, M6, M7, M11, M13
Sihtobjektid	Veebibrauser; Oma. *Näide: 015, 016*
Juhised ja kommentaarid	

Moodul	APP.2.1: Kataloogiteenus üldiselt
Meetmed	M1-M6
Sihtobjektid	Kataloogiteenus; Oma, Pilv. *Näide: 011*

Juhised ja kommentaarid	M5, M6 – rakendatakse juhul, kui kataloogiteenus on kohalik rakendus

Moodul	**APP.2.2: Active Directory**
Meetmed	M1-M7
Sihtobjektid	Kataloogiteenus; Oma, Pilv. *Näide: 011*
Juhised ja kommentaarid	Moodul rakendatakse juhul kui AD on kasutusel

Moodul	**APP.2.3: OpenLDAP**
Meetmed	M1-M6
Sihtobjektid	Kataloogiteenus; Oma, Pilv. *Näide: ei ole kasutusel*
Juhised ja kommentaarid	Moodul rakendatakse juhul kui AD on kasutusel M1 - rakendada vajaduspõhiselt M3, M4 - rakendatakse juhul, kui kataloogiteenus on kohalik rakendus

Moodul	**APP.3.1: Veebirakendused**
Meetmed	M1, M4, M7, M14
Sihtobjektid	Oma, Välj, Pilv. *Näide: 001-004, 007-009, 012, 017*
Juhised ja kommentaarid	Väljasttellitavate ja pilverakenduste puhul rakendatakse meetmed läbi protsessimooduli OPS.2: Käidutööd teenusena

Moodul	**APP.3.2: Veebiserver**
Meetmed	M1-M5, M7, M11
Sihtobjektid	Veebiserver; Oma, Välj, Pilv. *Näide: ei ole kasutusel*

Juhised ja kommentaarid	Väljasttellitavate ja pilverakenduste puhul rakendatakse meetmed läbi protsessimooduli OPS.2: Käidutööd teenusena. Veebiserveritena tuleb käsitleda ka IT-süsteemides (nt meiliserveri veebiliides, failiserveri veebiliides, 4G router, jms) sisalduvaid veebiservereid ja rakendada meetmed vastavalt võimalustele.

Moodul	**APP.3.3: Failiserver**
Meetmed	M2, M3, M15
Sihtobjektid	Failiserver; Oma, Välj, Pilv. *Näide: 013*
Juhised ja kommentaarid	Väljasttellitavate ja pilverakenduste puhul rakendatakse meetmed läbi protsessimooduli OPS.2: Käidutööd teenusena. Failiserveritena tuleb käsitleda ka IT-süsteemides sisalduvaid failiservereid ja rakendada meetmed vastavalt võimalustele.

Moodul	**APP.3.4: Samba**
Meetmed	M1, M2
Sihtobjektid	Samba; Oma. *Näide: ei ole kasutusel*
Juhised ja kommentaarid	M1 - rakendada vajaduspõhiselt

Moodul	**APP.3.6: DNS-server**
Meetmed	M1-M9
Sihtobjektid	DNS; Oma, Välj, Pilv. *Näide: ei ole kasutusel*
Juhised ja kommentaarid	M1 - rakendada vajaduspõhiselt Väljasttellitavate ja pilverakenduste puhul rakendatakse meetmed läbi protsessimooduli OPS.2: Käidutööd teenusena.

Moodul	APP.4.3: Andmebaasisüsteemid
Meetmed	M1, M3, M4, M9
Sihtobjektid	Andmebaasisüsteem; Oma, Välj, Pilv. *Näide: ei ole kasutusel*
Juhised ja kommentaarid	M4 - rakendada vajaduspõhiselt Väljasttellitavate ja pilverakenduste puhul rakendatakse meetmed läbi protsessimooduli OPS.2: Käidutööd teenusena.

Moodul	APP.4.4: Kubernetes
Meetmed	M1-M5
Sihtobjektid	Kubernetes; Oma, Välj, Pilv. *Näide: ei ole kasutusel*
Juhised ja kommentaarid	Väljasttellitavate ja pilverakenduste puhul rakendatakse meetmed läbi protsessimooduli OPS.2: Käidutööd teenusena.

Moodul	APP.5.2: Microsoft Exchange ja Outlook
Meetmed	M1-M3, M5
Sihtobjektid	Rühmatarkvara; Oma, Välj, Pilv. *Näide: 010, 011*
Juhised ja kommentaarid	M1 - rakendada vajaduspõhiselt Väljasttellitavate ja pilverakenduste puhul rakendatakse meetmed läbi protsessimooduli OPS.2: Käidutööd teenusena.

Moodul	APP.5.3: E-posti server ja klient üldiselt
Meetmed	M1-M4
Sihtobjektid	Rühmatarkvara, Kontoritarkvara; Oma, Välj, Pilv. *Näide: 010, 011*
Juhised ja kommentaarid	Moodul rakendatakse rühma- ja kontoritarkvaradele, mis evivad vastavat funktsionaalsust.

	Väljasttellitavate ja pilverakenduste puhul (nt Office365) rakendatakse meetmed läbi protsessimooduli OPS.2: Käidutööd teenusena.

Moodul	APP.6: Tarkvara üldiselt
Meetmed	M1-M5
Sihtobjektid	Kõik tarkvara kategooriad ja liigid. *Näite: 001-017*
Juhised ja kommentaarid	M1 - rakendada vajaduspõhiselt Väljasttellitavate ja pilverakenduste puhul rakendatakse meetmed läbi protsessimooduli OPS.2: Käidutööd teenusena.

Moodul	APP.EE: X-tee andmeteenus
Meetmed	M1-M17
Sihtobjektid	Xtee; Oma, Välj, Pilv. *Näide: 017*
Juhised ja kommentaarid	Väljasttellitavate ja pilverakenduste puhul rakendatakse meetmed läbi protsessimooduli OPS.2: Käidutööd teenusena.

SYS. IT-süsteemid

Moodul	SYS.1.1: Server üldiselt
Meetmed	M1, M2, M5, M6, M9, M10
Sihtobjektid	Linux, Wserv; Oma, Välj.
Juhised ja kommentaarid	Väljasttellitavate serveriteenuste puhul rakendatakse meetmed läbi protsessimooduli OPS.2.1: Väljasttellimine

Moodul	SYS.1.2.2: Windows Server 2012

Meetmed	M1-M3
Sihtobjektid	Wserv; Oma, Välj.
Juhised ja kommentaarid	M1, M2 - rakendada vajaduspõhiselt Väljasttellitavate serveriteenuste puhul rakendatakse meetmed läbi protsessimooduli OPS.2.1: Väljasttellimine

Moodul	**SYS.1.3: Linuxi ja Unixi server**
Meetmed	M2-M5
Sihtobjektid	Linux; Oma, Välj.
Juhised ja kommentaarid	Väljasttellitavate serveriteenuste puhul rakendatakse meetmed läbi protsessimooduli OPS.2.1: Väljasttellimine

Moodul	**SYS.1.5: Virtualiseerimissüsteem**
Meetmed	M2-M7
Sihtobjektid	Linux, Wserv; Oma, Välj.
Juhised ja kommentaarid	Rakendatakse sihtobjektidele, milles on kasutusel virtualiseerimisüsteem. Väljasttellitavate virtualiseerimisteenuste puhul rakendatakse meetmed läbi protsessimooduli OPS.2.1: Väljasttellimine

Moodul	**SYS.1.6: Konteinerdus**
Meetmed	M1-M8
Sihtobjektid	Linux, Wserv; Oma, Välj.
Juhised ja kommentaarid	Rakendatakse sihtobjektidele, milles on kasutusel konteinerdus. Väljasttellitavate konteinerdusteenuste puhul rakendatakse meetmed läbi protsessimooduli OPS.2.1: Väljasttellimine

Moodul	SYS.1.8: Salvestilahendused
Meetmed	M1, M2, M4
Sihtobjektid	Linux, Wserv; Oma, Välj.
Juhised ja kommentaarid	Rakendatakse sihtobjektidele, milles on kasutusel salvestilahendused. Väljasttellitavate salvestilahenduste puhul rakendatakse meetmed läbi protsessimooduli OPS.2.1: Väljasttellimine

Moodul	SYS.2.1: Klientarvuti üldiselt
Meetmed	M1, M3, M6, M8, M9, M42
Sihtobjektid	Klient; Oma, Välj.
Juhised ja kommentaarid	Väljasttellitavate lahenduste puhul rakendatakse meetmed läbi protsessimooduli OPS.2.1: Väljasttellimine

Moodul	SYS.2.2.3: Windows 10 klient
Meetmed	M1, M2, M4, M5, M12
Sihtobjektid	Klient; Oma, Välj.
Juhised ja kommentaarid	Rakendatakse Windows klientarvutitele

Moodul	SYS.2.3: Linuxi ja Unixi klient
Meetmed	M1, M2, M4, M5
Sihtobjektid	Klient; Oma, Välj.
Juhised ja kommentaarid	Rakendatakse Linux ja Unix klientarvutitele M2 - rakendada vajaduspõhiselt

Moodul	SYS.2.4: macOS-i klient
Meetmed	M1-M3
Sihtobjektid	Klient; Oma, Välj.
Juhised ja kommentaarid	Rakendatakse macOS klientarvutitele

Moodul	SYS.3.1: Sülearvutid
Meetmed	M1, M3, M5, M9
Sihtobjektid	Mob; Oma, Välj.
Juhised ja kommentaarid	Rakendatakse sülearvutitele

Moodul	SYS.3.2.1: Nutitelefon ja tahvelarvuti üldiselt
Meetmed	M1-M8
Sihtobjektid	Mob; Oma.
Juhised ja kommentaarid	

Moodul	SYS.3.2.2: Mobiilseadmete haldus (MDM)
Meetmed	M1-M5, M20
Sihtobjektid	Mob; Oma.
Juhised ja kommentaarid	

Moodul	SYS.3.2.3: Organisatsiooni iOS
Meetmed	M1, M2, M7
Sihtobjektid	Mob; Oma.
Juhised ja kommentaarid	Rakendatakse iOS seadmetele

Moodul	SYS.3.2.4: Android
Meetmed	M1
Sihtobjektid	Mob; Oma.
Juhised ja kommentaarid	Rakendatakse Android seadmetele

Moodul	SYS.3.3: Mobiiltelefon
Meetmed	M1-M6
Sihtobjektid	Mob; Oma.
Juhised ja kommentaarid	Rakendatakse mobiiltelefonidele

Moodul	SYS.4.1: Printer ja kontorikombain
Meetmed	M1, M2, M5, M22
Sihtobjektid	Print; Oma, Välj
Juhised ja kommentaarid	Väljasttellitavate lahenduste puhul rakendatakse meetmed läbi protsessimooduli OPS.2.1: Väljasttellimine

Moodul	SYS.4.5: Irdandmekandjad
Meetmed	M1, M2, M12

Sihtobjektid	USB; Oma.
Juhised ja kommentaarid	

NET. Võrgud ja side

Moodul	**NET.1.1: Võrgu arhitektuur ja lahendus**
Meetmed	M1-M9, M11-M15
Sihtobjektid	Tmüür, Võrk, VPN; Oma.
Juhised ja kommentaarid	

Moodul	**NET.1.2: Võrguhaldus**
Meetmed	M1, M2, M6-M11
Sihtobjektid	Tmüür, Võrk, VPN; Oma.
Juhised ja kommentaarid	

Moodul	**NET.2.1: Raadiokohtvõrgu käitamine**
Meetmed	M1-M8
Sihtobjektid	Tmüür, Võrk; Oma.
Juhised ja kommentaarid	

Moodul	**NET.2.2: Raadiokohtvõrgu kasutamine**

Meetmed	M1-M3
Sihtobjektid	Arvuti, Mob, Print; Oma, Välj.
Juhised ja kommentaarid	Raadiovõrgu võimalusega seadmed

Moodul	**NET.3.1: Ruuter ja kommutaator**
Meetmed	M1, M4-M9
Sihtobjektid	Võrk; Oma.
Juhised ja kommentaarid	

Moodul	**NET.3.2: Tulemüür**
Meetmed	M1-M4, M6-M10, M14, M15, M22
Sihtobjektid	Tmüür; Oma.
Juhised ja kommentaarid	

Moodul	**NET.3.3: Virtuaalne privaatvõrk (VPN)**
Meetmed	M1-M5
Sihtobjektid	VPN; Oma.
Juhised ja kommentaarid	M1-M3 rakendatakse vastavalt vajadusele

Moodul	**NET.4.1: Telefonikeskjaam**

Meetmed	M1, M2, M5, M15
Sihtobjektid	Keskj; Oma.
Juhised ja kommentaarid	M1-M2 rakendatakse vastavalt vajadusele

Moodul	**NET.4.2: IP-telefon (VoIP)**
Meetmed	M1, M3-M5
Sihtobjektid	VoiP; Oma.
Juhised ja kommentaarid	M1 rakendatakse vastavalt vajadusele

INF. Taristu

Moodul	**INF.1: Hoone üldiselt**
Meetmed	M1-M8, M10, M27
Sihtobjektid	Hoone
Juhised ja kommentaarid	Lõimitud haldussüsteemi põhimõttest lähtuvalt tuleb veenduda, et oluliste haldussüsteemide asjakohased dokumendid vastavad meetmetes esitatud nõuetele. Näiteks tuletõrje eeskirjad.

Moodul	**INF.2: Serveriruum ja andmekeskus**
Meetmed	M1-M11, M17, M19
Sihtobjektid	Serv
Juhised ja kommentaarid	Lõimitud haldussüsteemi põhimõttest lähtuvalt tuleb veenduda, et oluliste haldussüsteemide asjakohased dokumendid vastavad meetmetes esitatud nõuetele. Näiteks tulekahjusignalisatsioon.

	M1, M2 vastavalt vajadustele ja võimalustele

Moodul	INF.5: Tehnilise taristu ruum või kapp
Meetmed	M1-M7, M9, M16
Sihtobjektid	Tehn
Juhised ja kommentaarid	M1, M2, M5 vastavalt vajadustele ja võimalustele. M3, M4, M6, M7, M9, M16 - Lõimitud haldussüsteemi põhimõttest lähtuvalt tuleb veenduda, et asjakohased dokumendid vastavad meetmetes esitatud nõuetele.

Moodul	INF.6: Andmekandjate arhiiv
Meetmed	M1-M4
Sihtobjektid	Andm
Juhised ja kommentaarid	Lõimitud haldussüsteemi põhimõttest lähtuvalt tuleb veenduda, et oluliste haldussüsteemide asjakohased dokumendid vastavad meetmetes esitatud nõuetele. Näiteks tuletõrje eeskirjad.

Moodul	INF.7: Bürootöökoht
Meetmed	M1, M2, M6
Sihtobjektid	Büroo
Juhised ja kommentaarid	Lõimitud haldussüsteemi põhimõttest lähtuvalt tuleb veenduda, et oluliste haldussüsteemide asjakohased dokumendid vastavad meetmetes esitatud nõuetele. M1 - vastavalt vajadustele ja võimalustele

Moodul	INF.8: Kodutöökoht
Meetmed	M1-M3

Sihtobjektid	Kodutöökohtade kaardistamine ei ole põhjendatud
Juhised ja kommentaarid	Töötajatele, kes soovivad teha kodutööd, kehtestatud eeskirjad vastavad M1-M3 nõuetele

Moodul	**INF.9: Mobiiltöökoht**
Meetmed	M1-M4
Sihtobjektid	Mobiiltöökohtade kaardistamine ei ole põhjendatud
Juhised ja kommentaarid	Töötajatele, kes soovivad kasutada mobiiltöökohta, kehtestatud eeskirjad vastavad M1-M4 nõuetele

Moodul	**INF.10: Koosoleku-, ürituse- ja koolitusruum**
Meetmed	M1, M3
Sihtobjektid	Nõup
Juhised ja kommentaarid	Lõimitud haldussüsteemi põhimõttest lähtuvalt tuleb veenduda, et oluliste haldussüsteemide asjakohased dokumendid vastavad meetmetes esitatud nõuetele.

Moodul	**INF.12: Kaabeldus**
Meetmed	M1-M3, M10, M11, M13
Sihtobjektid	Hoone
Juhised ja kommentaarid	M1-M3 rakendada vajaduspõhiselt M11, M13 - Lõimitud haldussüsteemi põhimõttest lähtuvalt tuleb veenduda, et oluliste haldussüsteemide asjakohased dokumendid vastavad meetmetes esitatud nõuetele.

Moodul	**INF.13: Hoonete tehniline haldus**
Meetmed	M1-M3

Sihtobjektid	Hoone
Juhised ja kommentaarid	M1 rakendada vajaduspõhiselt M2, M3 - Lõimitud haldussüsteemi põhimõttest lähtuvalt tuleb veenduda, et oluliste haldussüsteemide asjakohased dokumendid vastavad meetmetes esitatud nõuetele.

Moodul	**INF.14: Hooneautomaatikasüsteemid**
Meetmed	M1-M6
Sihtobjektid	Hoone
Juhised ja kommentaarid	M1, M2 rakendada vajaduspõhiselt M5 - Lõimitud haldussüsteemi põhimõttest lähtuvalt tuleb veenduda, et oluliste haldussüsteemide asjakohased dokumendid vastavad meetmetes esitatud nõuetele.