



Kaasrahanud
Euroopa Liit



Eesti
tuleviku heaks

RAPLAMAA OMAVALITSUSTE LIIT

**Raplamaa omavalitsuste küberturvalisuse
uuring ning Eesti infoturbestandardi E-ITS
rakendamise mudeli väljatöötamise ja
rakendamise nõustamine**

LÕPPARUANNE

Jaan Oruaas CISA

Andres Anier ISO27001 juhtiv rakendaja

Risto Bristol, ekspert

juuni 2025

Sissejuhatus

Vastavalt Raplamaa Omavalitsuste Liidu ja FocusIT OÜ vahel 10. mail 2024 sõlmitud hankelepingule Raplamaa omavalitsustele E-ITS rakendamise nõustamisteenuse osutamiseks nõustas FocusIT OÜ ajavahemikus 1. maist 2024 kuni 9. maini 2025 Raplamaa omavalitsusi E-ITS rakendamisel.

Projektiplaan

Projektiplaan koostati vastavuses hankelepinguga. Kuna lepingu allkirjastamine ja sellega seoses ka töödega alustamine venis, nihkusid suvesse planeeritud puhverajad sügisesse. Seega ei ole puhkustest tulenev suviste tähtaegade ületamine projekti üldises ajagraafikus püsimise seisukohalt probleem. Samuti eeldab E-ITS rakendamise metoodika lepingus ja sellest tulenevalt projektiplaanis toodust mõnevõrra erinevat tööde järjekorda, millest tulenevalt on mõistlik vaadata 1. ja 2. etappi tervikuna.

1. ja 2. etapi tööd pidid projektiplaan järgi lõppema 23. augustil, kuid valmisid tegelikult oktoobri lõpuks. Sellest hoolimata võis öelda, et projekt oli endiselt graafikus, sest kaitseala modelleerimise tööd olid suures osas tehtud 2. etapi raames ning veel teostamata tööd mahus 100h oli võimalik mahutada novembris.

Vahekoosolekul juhiti osapoolte tähelepanu asjaolult, et on projekti ajagraafik on pingeline ning vajab graafikus püsimiseks kõigi osapoolte tähelepanu ja pingutust.

3. ja 4. etapi tööd pidid projektiplaan järgi lõppema 17. jaanuaril, kuid valmisid tegelikult projekti lõpptähtajaks 9.mai 2025. Põhjused selleks on mitmeid, olulisemad neist on järgnevad:

- RIA väljakuulutatud hange EITS näidisdokumentatsiooni koostamiseks ebaõnnestus. Seega kulus dokumentatsiooni koostamiseks eeldatust rohkem aega

- RIA riigi infoturbe meetmete osakonna kui standardi looja ja haldaja lähenemine EITS-le muutus. Muutuse võtab kõige paremini kokku osakonnalt saadud info: on oluline jälle rõhutada – meedet ja eriti selle igat alammeetet ei tohiks käsitleda kohustuslik nõudena, neid peaks käsitlema riskipõhiselt ja proportsionaalselt.

Selline muutus on igati tervitatav ning aitas täiendavalt mõista asjaolu, et EITS 2023 standardist (uuendatud 26.02.24) arvati varasemalt 2022 standardi osaks olnud rakendusjuhend. Muudatuse tulemusena tuli koostada uus riskihalduse metoodika ning viia selle põhjal läbi mahukas riskihaldus, mille tulemusena hinnati kõikide EITS moodulite poolt leevendatavad riskid, kokku ligi 700 erinevat riski.

- Vähendamaks täiendavat tööd, mis oleks tulenenud EITS 2024 uuenduste haldusest otsustati kohese EITS 2024 versiooni rakendamise kasuks. Paraku selle versiooni publitseerimine venis ning ametlikult ei ole meetmete kataloog tänaseni allalaetav. Digitaalne kataloog õnnestus saada alles jaanuari lõpus.

Kõiki nimetatud asjaolusid kaaluti projekti juhtrühma koosolekul 23. jaanuaril 2025 ning tehti otsused, mis olid vajalikud projekti tähtaegseks lõpetamiseks.

Tabel 1 Projektiplaan

Ptk	Nimetus	Dokument	Algus (ndt)	Löpp (ndt)	Algus	Löpp	Kestus (ndt)	Maht (h)
2.1.2.1	Infoturbe organisatsiooni loomine	Infoturvapoliitika	20	20	13.05.2024	17.05.2024	1	16
2.1.2.2	Turvapoliitika ja -eesmärkide koostamine	Infoturvapoliitika	21	22	20.05.2024	31.05.2024	2	32
2.1.2.3	Äriprotsesside arvelevõtt	Kahjuanalüüs	23	23	03.06.2024	07.06.2024	1	16
	Puhver		24	24	10.06.2024	14.06.2024	1	
2.1.4.1	Kaitseala sihtobjektide loetelu dokumenteerimine	EITS sihtobjektid	25	27	17.06.2024	05.07.2024	3	32
2.1.4.2	Kaitseala struktuurianalüüs	EITS sihtobjektid	28	31	08.07.2024	02.08.2024	4	48
2.1.4.3	Kaitsetarbe määramine	Kahjuanalüüs, EITS sihtobjektid	32	34	05.08.2024	23.08.2024	3	40
	Puhver		35	35	26.08.2024	30.08.2024	1	
2.1.6.1	Etalonturbe väline riskihaldus	Riskianalüüs	36	39	02.09.2024	27.09.2024	4	48
2.1.6.2	Kaitseala modelleerimine	EITS sihtobjektid	40	46	29.09.2024	14.11.2024	7	40
2.1.6.3	Rakendatud infoturbe meetmete kaardistamine	IMR	40	46	29.09.2024	14.11.2024	7	56
	Puhver		47	48	18.11.2024	29.11.2024	2	
2.1.8.1	Teostusjärjekorra määramine	IMR, Turbekontseptsioon	49	50	02.12.2024	13.12.2024	2	16
2.1.8.2	Eelarvestamine	IMR	51	52	16.12.2024	27.12.2024	2	24
2.1.8.3	IMR kinnitamine	IMR	1	3	30.12.2024	17.01.2025	3	16
	Puhver		4	7	23.01.2025	14.02.2025	3	
2.1.8.4	Vahearuande koostamine	Esitatud	20	7	13.05.2024	14.02.2024	36	16
2.1.8.5	Lõpparuande koostamine		20	19	13.05.2024	09.05.2025	52	16

Võtmetegevused

2. mail 2024 toimus lühike **avakoosolek**, mille raames lepiti kokku osapoolte vaheline suhtlus sh kontaktisikud ning täpsustati lepinguga seonduvat.

9.mail 2024 toimus töötuba, milles osalesid kõikide Raplamaa omavalitsuste esindajad. Focus IT andis ülevaate Eesti infoturbestandardist. Määrati omavalitsuste **äriprotsessid** ja äriprotsesside eest vastutajad.

Ajavahemikul **17. mai 2024 – 12. juuni 2024** viidi määratud äriprotsesside kaupa läbi **kahjuanalüüs** vastavalt E-ITS 2023 rakendusjuhendi lisale B ning E-ITS profiilile kohalikele omavalitsustele. Kahjuanalüüsi tulemusena valmisid kaitsetarbe määramise protokollid, mis on omavalitsustele üle antud.

12. juunil 2024 toimus projekti juhtrühma koosolek, FocusIT andis ülevaate projekti käigust, seejärel lepiti kokku suvised tegevused so kuni 31.augustini. Suve jooksul planeeriti ISMS **kaitseala kaardistamine ja modelleerimine** sh sihtobjektide tuvastamine ja nende kaitsetarbe määramine. Selleks toimus **kokku 9 kohapealset töötuba**. Täiendavalt loodi iga omavalituse poolt jagatud kaust, mille abil sai omavalitsusi jooksvalt virtuaalselt nõustada.

5. septembril 2024 toimus järjekordne **juhtrühm** ning töökoosolek kõikide omavalitsuste võtmeisikutega. Nenditi, et **suveks seatud eesmärgid ei ole täidetud** kuid sellest hoolimata on võimalik projekti 3. etapp tähtajaks lõpetada. Selleks arutati kohapeal suvel üles kerkinud probleeme ja väljakutseid ning lepiti kokku täiendavad töötoad iga omavalitsusega eraldi.

11. oktoobril 2024 saatis FocusIT nii Raplamaa Omavalitsuste Liidule kui ka kõikidele E-ITS kontaktisikutele **märgukirja**, milles nentis, et kahjuks ei ole kõik kaardistamise tööd veel lõppenud ning vajalik on kiiresti kokku leppida täiendavad töötoad igas omavalitsuses ning ka juhtrühm tekkinud olukorra arutamiseks.

Ajavahemikul **17.oktoober 2024 – 31. oktoober 2024** lepiti kokku ning toimusid täiendavad ISMS **kaitseala kaardistamine ja modelleerimine** töötoad. Valminud kaardistuse põhjal vormistati

esialgsed versioonid **turvapoliitikast ja -eesmärkidest**, mis täpsustatati 3. etapi käigus vastavalt riskianalüüsi tulemustele.

24. oktoober 2024 toimus juhtrühma koosolek, mille käigus anti ülevaade projektist ja tutvustati käesolevat vahearuannet. Juhtrühm otsustas kooskõlas raamlepingu punktiga 3.2.2:

- võttes arvesse, et projekti kolmanda etapi tööde mahuks on planeeritud 144h (so ca 4 nädala jagu töötunde) ja kestvuseks 20 nädalat, määrata projekti teise etapi tähtajaks **31.10.2024**

- võtta kasutusel 1 nädal projekti puhvrist (20.01.2025-14.02.2025) ning pikendada 3. ja 4. etapi tähtaegu 1 nädala võrra.

28. oktoober 2024 toimus Kohila vallas töökoosolek, mille käigus loodi eeldused 2. etapi tööde lõpetamiseks oktoobri lõpuks.

1. november – 30. november esialgne versioon infoturbe meetmete rakendusplaanist EITS 2023 standardi põhjal.

1. detsember – 21. jaanuar meetmete rakendatuse kirjeldamine vastavalt koostatud rakendusplaanile.

23. jaanuaril toimus projekti juhtrühma koosolek, mille käigus võeti teatavaks ilmnenu asjaolud ning otsustati rakendada EITS 2024 versioon koos asjakohase riskianalüüsiga. Loodi eeldused projekti tähtaegseks lõpuleviimiseks.

29. jaanuaril alustati riskianalüüsiga. Riskianalüüsi põhjal koostati uus EITS 2024 vastav infoturvameetmete rakendusplaan, määrati teostusjärjekord vastavalt eeldatavatele töömahtudele, koostati alusdokumentide esialgsed versioonid.

26. märtsil esitleti ROL koosolekul riskianalüüsi tulemusi ja infoturbemeetmete rakendusplaani.

14. aprill alustati EITS audititsükli hankedokumentide ettevalmistamisega, mis koostati vastavalt EITS auditeerimiseeskirjale ja toetudes senisele auditite hankimise praktikale.

25. mail toimus projekti lõppkoosolek. Anti ülevaade projekti käigust, tutvustati tulemeid, toimus võimalike edasiste tegevusplaanide arutelu.

Kokkuvõte

Hoolimata pingelisest ajakavast, mis nõudis kõigi osapoolte tähelepanu ja pingutust, teostati projekti lõpptähtjaks kõik planeeritud tööd:

1. Äriprotsesside määratlemine, kahjuanalüüs ja kaitsetarvete määramine
2. Infoturvapoliitika omavalitsustele kohandamiseks ja kinnitamiseks sh turbeviisi valimine
3. Kaitseala kaardistus sh äriprotsessid, alusteave, rakendused, IT-süsteemid, hooned ja ruumid
4. Esmane kaitseala modelleerimine so kaardistatud sihtobjektide vastendamine etalonturbe kataloogi moodulitega
5. Riskihalduse meetoodika loomine ja kinnitamine
6. Riskihalduse läbiviimine vastavalt meetoodikale
7. Kaitseala modelleerimine so kaardistatud sihtobjektide vastendamine etalonturbe kataloogi moodulitega
8. Infoturbe hetkeolukorra kaardistamine so rakendatud infoturbemeetmete võrdlemine E-ITS etalonturbe kataloogiga
9. Rakendamata või osaliselt rakendatud infoturbemeetmete teostusjärjekorra määramine
10. Infoturbemeetmete rakendamise eelarvestamine
11. Infoturbe meetmete rakendusplaani (IMR) koostamine ja kinnitamine
12. Lõpparuande koostamine

Koostatud dokumentatsioon on tundliku iseloomuga ja seda ei ole seetõttu võimalik lisada käesolevale aruandele. Projekti käigus koostatud dokumendid on turvaliselt üle antud kohalikele omavalitsustele. Üleantud dokumentatsiooni hulka kuulusid järgnevad olulisemad dokumendid, mille osad vastavad lepinguga nõutud tulemitele:

1. Infoturvapoliitika (lisatud aruandele)
2. Kaitsetarbe määramise protokollid (konfidentsiaalne)
3. Kaitseala kaardistus (konfidentsiaalne)
4. Riskihalduse kord (lisatud aruandele)
5. Riskianalüüs (konfidentsiaalne)
6. Infoturbe kontseptsioon (konfidentsiaalne)
7. Infoturbe meetmete rakendusplaan (IMR) (konfidentsiaalne)
8. EITS audititsükli hankedokumendid (lisatud aruandele)

Jaana Oruaas
FocusIT OÜ juhatuse liige, CISA
/Allkirjastatud digitaalselt/

Aruande koostas Andres Anier, ISO27001 juhtiv audiitor ja rakendaja