Avaliku pilvetehnoloogia riskide analüüs K1T1So turvaklassiga andmekogu näitel

Aruanne
Juuli 2016

12.07.2016

Building a better working world

Sisukord

1. Sissejuhatus

Ernst & Young Baltic AS (edaspidi EY) viis 2016. aasta mais ja juunis Majandus- ja Kommunikatsiooniministeeriumi (edaspidi Tellija) tellimusel läbi avaliku pilvetehnoloogia riskianalüüsi. Riskianalüüsi eesmärgiks oli hinnata K1T1S0 turvaklassiga andmekogu infosüsteemi ja selle opereerimise võimalikkust avalikus pilves ning tuua välja avaliku pilvetehnoloogia kasutamisega tekkivad riskid.

Riskianalüüsi metoodika, läbiviidud protseduurid ning tuvastatud riskid ja vastumeetmed on esitatud käesolevas aruandes vastavates peatükkides.

Käesoleva aruande eesmärk on kaardistada avaliku pilve kasutamisest tulenevad riskid K1T1S0 turvaklassiga andmekogule, tuua konkreetse praktilise näite põhjal avaliku pilvetehnoloogiaga kaasnevatest riskidest ja nende maandamise viisidest ning teha ettepanekuid ISKE infoturbe standardi täiendamiseks pilve-spetsifiiliste ohtude ja meetmetega. Juhul, kui Teil tekib küsimusi või kommentaare esitatud ettepanekute ja soovituste kohta, või vajaksite abi nimetatud soovituste rakendamisel, oleme meeleldi valmis Teid aitama.

Riskianalüüsi läbiviijad on lähtunud analüüsi teostamisel eeldusest, et esitatud materjalid, dokumendid ja informatsioon on õiged ja täielikud. Vastasel juhul ei saa EY partnereid ega ka töötajaid pidada vastutavateks ebatäpse või eksliku informatsiooni esitamise eest käesolevas aruandes. Samuti ei tohi eelnimetatud isikuid pidada vastutavaks ka kahjude eest, mis võivad tekkida aruandes oleva informatsiooni kasutamisel.

Töövõtt viidi läbi kooskõlas infosüsteemide audiitorite ühingu (Information Systems Audit and Control Association, ISACA) kutse-eetika koodeksist, standarditest ja suunistest, protseduurireeglitest ja headest tavadest

Täname Majandus- ja Kommunikatsiooniministeeriumi ja Riigi Infosüsteemi Ameti esindajaid meeldiva ja abivalmi koostöö eest!

Juuli 2016

Sander Saveli
Vanemkonsultant
Sertifitseeritud infosüsteemide audiitor

Siim Aben
Juhtivkonsultant
Sertifitseeritud infosüsteemide audiitor

Ernst & Young Baltic AS

2. Riskianalüüsi ülevaade

2.1 Riskianalüüsi eesmärk

Käesoleva riskianalüüsi eesmärgiks oli:

- Tuvastada K1T1S0 ISKE turvaklassiga infosüsteemi pilves paiknemisest tulenevad täiendavad riskid ja vastumeetmed **(peatükk nr. 3);**
- Koostada nimekiri K1T1S0 taseme ISKE meetmed, mille rakendamine ei ole avaliku pilvetehnoloogia kasutamisel andmete omaniku poolt enam vahetult võimalik **(Lisa 1)**;
- Teha ettepanekud ISKE täiendamiseks pilve spetsiifiliste ohtudega K1T1S0 turvaklassis **(peatükk nr. 4)**;
- Teha ettepanekud ISKE täiendamiseks pilve spetsiifiliste meetmetega K1T1S0 turvaklassis **(peatükk nr. 5)**;

2.2 Riskianalüüsi meeskond

Riskianalüüsi meeskond ja rollid on toodud järgnevalt:

- Siim Aben – Projektijuht, Ernst & Young Baltic AS juhtivkonsultant ja sertifitseeritud projektijuht;
- Sander Saveli – analüütik, Ernst & Young Baltic AS vanemkonsultant ja sertifitseeritud infosüsteemide audiitor;
- Jaak Tepandi – ekspert, OÜ Tepinfo infoturbe ekspert;

2.3 Riskianalüüsi metoodika ja protseduurid

K1T1S0 andmekogu pilveriskide ja vastumeetmete kaardistamine

Pilves paiknemisest tulenevate täiendavate riskide kirjeldamisel lähtuti ISKE/BSI pilvtöötlust puudutavate moodulite ohtudest ning riskianalüüsi käigus tuvastatud lisanduvatest pilveohtudest. Iga tuvastatud riski puhul kirjeldati:

- Riski number;
- Oht;
- Tagajärg;
- Tõenäosus;
- Mõju;
- Vastumeetmed;
- Tõenäosus vastumeetmete rakendamisel;
- Mõju Vastumeetmete rakendamisel.

Lisaks toodi iga riski puhul välja erisused, mis tekivad seoses üleminekuga suure välisriigi avaliku pilveteenuse pakkuja avalikule pilveteenusele.

Riskide mõju hindamise skaala puhul arvestati K1T1S0 andmekogu ISKE tagajärgede kaalukusega, mille põhjal töötati välja kolmeastmeline skaala:

- **Ebaoluline mõju**– turvaintsidendiga (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmisega) ei kaasne märkimisväärseid kahjusid;
- **Vähe oluline mõju** – kaasnevad vähe olulised kahjud;
- **Oluline mõju** - turvaintsident (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt märkimisväärseid takistusi asutuse funktsiooni täitmisele või märkimisväärseid rahalisi kaotusi.

Kuna analüüsi esimeses etapis infosüsteemi rakendusala ei olnud kitsendatud ning erinevatel infosüsteemidel võivad olla sama turvaintsidendiga kaasneda erinevad mõjud, toodi analüüsis välja riski maksimaalne võimalik mõju.

Riskide tõenäosuse hindamise skaala aluseks võeti hädaolukorra riskianalüüsi koostamise juhendi riski tõenäosuse skaala:[1]

Tõenäosus	Kriteerium
Väga suur	**>99% tõenäosusega;** **juhtub sageli;** **võib juhtuda päevade ja nädalate jooksul.**

[1] *https://www.riigiteataja.ee/aktilisa/0000/1332/6405/13327718.pdf#*

Suur	**>50% tõenäosusega; võib kergesti juhtuda; võib juhtuda nädalate ja kuude jooksul.**
Keskmine	**>10% tõenäosusega; on varem juhtunud; võib juhtuda aasta jooksul.**
Väike	**>1% tõenäosusega; ei ole juhtunud, kuid võib juhtuda; võib juhtuda aastate pärast.**
Väga väike	**>1% tõenäosusega; mõeldav, kuid ainult ekstreemsetes tingimustes; 100 aasta vältel**

Kõikide tuvastatud riskide puhul toodi välja võimalikud turvameetmed riski tõenäosuse ja mõju vähendamiseks. Lisaks anti hinnang riski tõenäosusele ja mõjule juhul kui riski maandavad turvameetmed on rakendatud.

Ettepanekute tegemine ISKE täiendamiseks pilve-spetsifiiliste ohtudega K1T1S0 turvaklassis

K1T1S0 turvaklassiga pilve-spetsiifiliste ohtude kirjeldamisel lähtuti erinevate ohtude uudsuse astmest:

- Täiesti uued ohud, mida ei saa tuletada ISKE ohtude nimekirjas juba olemas olevate ohtude baasil.
- Ohud, mis on olemas ISKE ohtude nimekirjas [2] või mida saab selle nimekirja ohtudest tuletada, kuid mida pole moodulis B1.17 „Pilvteenuse kasutamine".[3]
- Ohud, mis on ISKE mooduli B 1.17 ohtude nimekirjas või mida saab selle nimekirja ohtudest tuletada

Analüüsis toodi välja täiesti uued ohud ning ohud, mida pole moodulis B1.17 „Pilvteenuse kasutamine". Ohustusid, mis on mooduli B 1.17 ohtude nimekirjas või mida saab selle nimekirja ohtudest tuletada eraldi ei kirjeldatud.

[2] *https://iske.ria.ee/8_00/ISKE_ohtude_kataloog*

[3] *https://iske.ria.ee/8_00/ISKE_kataloogid/5_Kataloog_B/B1/B_1.17*

Ettepanekute tegemine ISKE täiendamiseks pilve-spetsiifiliste meetmetega K1T1S0 turvaklassis

K1T1S0 turvaklassiga pilve-spetsiifiliste meetmete kirjeldamisel lähtuti erinevate ohtude uudsuse astmest:

- Täiesti uued meetmed, mida ei saa tuletada ISKE meetmete nimekirjas juba olemas olevate meetmete baasil.
- Meetmed, mida saaks lisada kas iseseisva meetmena või täienduseks mõnele ISKE meetmete nimekirjas[4] olevale meetmele.
- Meetmed, mis on ISKE mooduli B 1.17 meetmete nimekirjas või mida saab selle nimekirja meetmetest tuletada.

Analüüsis toodi välja täiesti uued meetmed ning meetmed, mida saaks lisada nimekirjas või mida saab selle nimekirja ohtudest tuletada eraldi ei kirjeldatud iseseisva meetmena või täienduseks mõnele ISKE meetmete nimekirjas olevale meetmele. Meetmed, mis on ISKE mooduli B 1.17 meetmete nimekirjas või mida saab selle nimekirja meetmetest tuletada eraldi ei kirjeldatud.

Andmete omaniku poolt rakendamatute turvemeetmete kirjeldamine

K1T1S0 taseme ISKE andmekogu omaniku poolt rakendamatute turvemeetmete väljaselgitamisel, lähtuti põhimõttest, et kaardistati ainult turvameetmed, mida andmete omanik enam üldse vahetult mõjutada ei saa ning jäeti välja turvameetmed, mis jäävad osaliselt andmete omaniku kontrolli all.

[4] *https://iske.ria.ee/8_00/ISKE_kataloogid*

3. K1T1S0 andmekogu pilveriskid ja vastumeetmed

Lähtuvalt ISKE rakendusjuhendist vastab K1T1S0 turvaklassiga andmekogu järgmistele nõuetele:

- Käideldavus - suurem või võrdne 80% ja väiksem kui 99% aastas ning maksimaalne lubatud ühekordse katkestuse pikkus teenuse töö ajal kuni 24 tundi (st ühekordse katkestuse pikkus võib olla vahemikus väiksem või võrdne 24 tunniga ja suurem kui 4 tundi)*;
- Terviklus – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; info õigsuse, täielikkuse, ajakohasuse kontrollid erijuhtudel ja vastavalt vajadusele;
- Konfidentsiaalsus – avalik info: juurdepääsu teabele ei piirata (st lugemisõigus kõigil huvitatutel, muutmise õigus määratletud tervikluse nõuetega);
- Tagajärgede kaalukus - turvaintsidendiga (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmisega) ei kaasne märkimisväärseid kahjusid või turvaintsidendiga kaasnevad vähe olulised kahjud, turvaintsident (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt märkimisväärseid takistusi asutuse funktsiooni täitmisele või märkimisväärseid rahalisi kaotusi.

Riskianalüüs kajastab eraldi suure välisriigi avaliku pilveteenuse pakkuja avalikus pilves olevate infosüsteemide riskide erisus. Suurt välisriigi avaliku pilveteenuse pakkujat (edaspidi SVAPP) iseloomustavad järgmised tingimused:

- suur globaalne teenusepakkuja;
- andmete hoidmine välisriigis;
- andmete transiit läbi välisriigi;
- ressursi jagatud kasutus (*multitenancy*, simultaanteenindus);

SVAPP näide on Amazon Web Services (AWS).

Järgneva tabeli lahter pealkirjaga "SVAPP-i avalikule pilvele ülemineku erisused" sisaldab erisusi, mis tekivad seoses üleminekuga suure välisriigi avaliku pilveteenuse pakkuja avalikule pilveteenusele, võrreldes selliste pilveteenuste pakkujatega, mille puhul SVAPP-i erisused ei kehti.

K1T1S0 andmekogu pilves paiknemisest tulenevate täiendavate riskide loetelu

Nr	Oht	Tagajärg	Tõenäosus	Mõju	Vastumeetmed	Tõenäosus vastumeetmetega	Mõju vastumeetmetega	SVAPP-i avalikule pilvele ülemineku erisused
Üldised ohud, sh vääramatu jõud								
1.	Pilveteenusepakkuja IT-süsteemi avarii (tehnilise rikke, inimvea, vääramatu jõu vms tõttu) (oht käideldavusele)	Pilveteenuse pakkuja IT-süsteemi väljalangemise tõttu ei suuda pilveteenuse pakkuja tagada kokkulepitud käideldavusnõudeid ning andmekogu ei ole kättesaadav üle 24 tunni.	Väike	Oluline mõju	Pilveteenuse pakkuja valimisel teostatakse teenusepakkujate analüüs ning valitakse kõrgete käideldavusnäitajatega teenuse-pakkuja. Pilveteenuse pakkujaga sõlmitavas lepingus fikseeritakse teenuse käideldavuse nõuded. Andmekogu on majutatud mitme erineva pilveteenuse pakkuja juures, ühe teenuse-pakkuja väljalangemisel on võimalik teenus ümber lülitada teise teenusepakkuja juurde.	Väga väike	Oluline mõju	SVAPP-i puhul võib intsidendi tõenäosus olla väiksem (suur globaalne teenusepakkuja)
2.	Pilveteenusepakkuja IT-süsteemi avarii (tehnilise rikke, inimvea, vääramatu jõu vms tõttu) (oht terviklusele)	Pilveteenuse pakkuja IT-süsteemi väljalangemise korral pole võimalik taastada andmestikku kokkulepitud ulatuses ning esineb infokadu.	Väike	Oluline mõju	Pilveteenuse pakkuja valimisel teostatakse teenusepakkujate analüüs ning valitakse sertifitseeritud parimaid praktikaid ja standardeid järgiv teenusepakkuja Andmekogu omanik teostab andekogus olevast informatsioonist regulaarselt varukoopiaid, mida säilitatakse pilveteenuse-pakkujast sõltumatus keskkonnas	Väga väike	Vähe oluline mõju (infokadu võib olla väiksem)	Erisused puuduvad
3.	Pilveteenusepakkuja väljalangemine (oht käideldavusele)	Pilveteenuse pakkuja ühepoolse lepingu lõpetamise korral (nt pankrot, mainekahju, loodusjõududest või personali väljalangemisest tingitud probleemid) pole võimalik tagada andmekogu käideldavusnõudeid ning andmekogu ei ole enam kättesaadav.	Väike	Oluline mõju	Pilveteenuse pakkuja valimise teostatakse teenusepakkujate analüüs ning valitakse kõrgete käideldavusnäitajatega teenuse-pakkuja. Pilveteenuse pakkujaga sõlmitavas lepingus fikseeritakse teenuse käideldavuse nõuded. Andmekogu on majutatud mitme erineva pilveteenuse pakkuja juures, ühe teenuse-pakkuja väljalangemisel on võimalik teenus ümber lülitada teise teenusepakkuja juurde	Väga väike	Oluline mõju	SVAPP-i puhul võib intsidendi tõenäosus olla väiksem(suur globaalne teenusepakkuja)

Nr	Oht	Tagajärg	Tõenäosus	Mõju	Vastumeetmed	Tõenäosus vastu-meetmetega	Mõju vastumeetme-tega	SVAPP-i avalikule pilvele üle-mineku erisused
4.	Pilveteenusepakkuja väljalange-mine (oht terviklusele)	Pilveteenuse pakkuja ühepoolse lepingu lõpetamise korral (nt pank-rot, mainekahju, loodusjõududest või personali väljalangemisest tingitud probleemid) pole pilveteenuse pakkujalt võimalik kätte saada terviklikku andmestiku ning esineb infokadu.	Väike	Oluline mõju	Andmekogu omanik teostab andekogus olevast infor-matsioonist regulaarselt varukoopiaid, mida säilitatakse pilveteenuse-pakkujast sõltumatus keskkonnas.	Väga väike	Vähe oluline mõju (infokadu võib olla väiksem)	SVAPP-i puhul võib intsidendi tõenäosus olla väiksem(suur globaalne teenusepakkuja)
5.	Pilveteenusepakkuja väljalange-mine (oht konfidentsiaalsusele)	Pilveteenuse pakkuja ühepoolse lepingu lõpetamise (nt pankrot, loodusjõududest või personali väljalangemisest tingitud probleemid) tulemusena muutub avalikuks salajane andmekogu haldamise ja/või autentimise info.	Väike	Oluline mõju	Andmekogu salajane haldamise ja autentimise informat-sioon säilitatakse andmekogus krüpteeritud kujul. Pilveteenuse pakkuja valimisel teostatakse teenusepak-kujate analüüs ning valitakse sertifitseeritud üldtunnus-tatud infoturbe ja pilveteenuse standardeid (NT ISO 27001, 27017, 27018, CSA, IT Grundschutz jne) järgiv teenusepakkuja.	Väga väike	Oluline mõju	SVAPP-i puhul võib intsidendi tõenäosus olla suurem (andme-te transiit läbi välisriigi, andme-te hoidmine välisriigis, ressursi jagatud kasutus)
Organisatoorsed								
6.	Pilveteenusepakkuja sisemiste reeglite puudumine või puudulik-kus	Pilveteenuse pakkuja puudulike sisemiste reeglite tõttu pole andme-kogus oleva info muutmine ja hävitamise faktid alati tuvastatavad.	Keskmine	Oluline mõju	Pilveteenuse pakkuja valimisel teostatakse teenusepak-kujate analüüs ning valitakse serti-fitseeritud üldtunnus-tatud infoturbe ja pilve-teenuse standardeid (NT ISO 27001, 27017, 27018, CSA, IT Grundschutz jne.) järgiv tee-nusepakkuja. Tervikluse tagamiseks kasutatakse andmete töötlemise sündmuste logimist, logide krüptoaheldamist, räsifunkt-sioone, sõnumi autentimiskoode, digiallkirju jm vahen-deid. Vajadusel tuleb kasutada publitseerimise meedet (avali-kus pilves olev sisu kirjutatakse teatud aja tagant üle).	Väike	Vähe oluline mõju (intsidendi ulatus võib olla väiksem)	Erisused puuduvad
7.	Reeglite puudulik tundmine	Pilveteenuse pakkuja puudulike sisemiste reeglite tundmise tõttu pole andmekogus oleva info muutmine ja hävitamise faktid alati tuvastatavad.	Keskmine	Oluline mõju	Pilveteenuse pakkuja valimisel teostatakse teenusepak-kujate analüüs ning valitakse serti-fitseeritud üldtunnus-tatud infoturbe ja pilve-teenuse standardeid (NT ISO 27001, 27017, 27018, CSA, IT Grundschutz jne) järgiv tee-nusepakkuja Pilveteenuse pakkujalt nõutakse sisemiste reeglite jär-gimise sõltumatut auditeerimist. Tervikluse tagamiseks kasutatakse andmete töötlemise sündmuste logimist, logide krüptoaheldamist, räsifunkt-sioone, sõnumi autentimiskoode, digiallkirju jm vahen-deid. Vajadusel tuleb kasutada publitseerimise meedet (avali-kus pilves olev sisu kirjutatakse teatud aja tagant üle).	Väike	Vähe oluline mõju (intsidendi ulatus võib olla väiksem)	Erisused puuduvad
8.	Puudused pilveteenusepakkujaga sõlmitud lepingu tingimustes (oht käideldavusele)	Puuduste tõttu pilveteenusepakkujaga sõlmitud lepingu tingimustes ei taga teenusepakkuja käideldavusnõudeid ning andmekogu ei ole kättesaadav üle 24 tunni.	Keskmine	Oluline mõju	Viiakse läbi pilveteenusepakkuja tüüplepingu analüüs (SLA, teenusepakkuja tugi, teenuse muutmine, kliendi kohustused, teenuse ajutine peatamine, lepingu lõpeta-mine, teenusepakkuja kohutused, teenusepakkuja vastu-tus, lepingu muutmine, kolmandate osapoolte kasutami-ne jne) ning viiakse sisse parandused ja lisatingimused, mis aitavad tagada andmekogu käideldavusnõudeid.	Väike	Oluline mõju	Riski hinnang on sama (SVAPP-i puhul võib käideldavuse risk olla väiksem, samas aga ka tüüplepingu paranduste võim-alus võib olla väiksem)

Nr	Oht	Tagajärg	Tõenäosus	Mõju	Vastumeetmed	Tõenäosus vastumeetmetega	Mõju vastumeetmetega	SVAPP-i avalikule pilvele ülemineku erisused
9.	Puudused pilveteenusepakkujaga sõlmitud lepingu tingimustes (oht terviklusele)	Puuduste tõttu pilveteenusepakkujaga sõlmitud lepingu tingimustes ei taga teenusepakkuja andmete tervikluse nõudeid ning info allikas, selle muutmise ja hävitamise fakt pole alati tuvastatavad, mis võib kaasa tuua olulise andmekao.	Keskmine	Oluline mõju	Viiakse läbi pilveteenusepakkuja tüüplepingu analüüs (andmeprivaatsus, andmetele ligipääsu õigus, andmete omaniku õigused, teenusepakkuja tugi, varundamine, teenuse muutmine, kliendi kohustused, teenuse ajutine peatamine, lepingu lõpetamine, teenusepakkuja kohutused, teenusepakkuja vastutus, lepingu muutmine, kolmandate osapoolte kasutamine jne) ning viiakse sisse parandused ja lisatingimused, mis aitavad tagada andmekogu tervikluse nõudeid.	Väike	Vähe oluline mõju (intsidendi ulatus võib olla väiksem)	Riski hinnang on SVAPP-i puhul suurem, sest tüüplepingu paranduste võimalus võib olla väiksem
10.	Turvameetmete ebapiisav järelevalve (oht terviklusele)	Pilveteenuse pakkuja turvameetmete rakendamise ebapiisava järelevalve tulemusena pole andmekogus oleva info muutmise ja hävitamise faktid alati tuvastatavad, mis võib kaasa tuua olulise andmekao.	Keskmine	Oluline mõju	Pilveteenuse pakkujalt nõutakse sisemiste reeglite järgimise sõltumatut auditeerimist. Tervikluse tagamiseks kasutatakse andmete töötlemise sündmuste logimist, logide krüptoaheldamist, räsifunktsioone, sõnumi autentimiskoode, digiallkirju jm vahendeid. Vajadusel tuleb kasutada publitseerimise meedet (avalikus pilves olev sisu kirjutatakse teatud aja tagant üle).	Väike	Vähe oluline mõju (intsidendi ulatus võib olla väiksem)	Riski hinnang on SVAPP-i puhul suurem, sest võimalus pilveteenuse pakkujalt midagi nõuda võib olla väiksem
11.	Turvameetmete ebapiisav järelevalve (oht konfidentsiaalsusele)	Pilveteenuse pakkuja turvameetmete rakendamise ebapiisava järelevalve tulemusena muutub avalikuks salajane andmekogu haldamise ja/või autentimise info.	Keskmine	Oluline mõju	Andmekogu salajane haldamise ja autentimise informatsioon säilitatakse andmekogus krüpteeritud kujul, vajadusel toimub ka selle informatsiooni edastamine krüpteeritult. Pilveteenuse pakkuja valimisel teostatakse teenusepakkujate analüüs ning valitakse sertifitseeritud üldtunnustatud infoturbe ja pilve-teenuse standardeid (NT ISO 27001, 27017, 27018, CSA, IT Grundschutz jne) järgiv teenusepakkuja. Valida sobiv marsruutimise meetod (*traffic-routing method*), kasutada otseühendust (*dedicated connection*) vms.	Väike	Vähe oluline mõju (andmeleke võib olla väiksem)	SVAPP-i puhul võib intsidendi tõenäosus olla suurem (andmete transiit läbi välisriigi, andmete hoidmine välisriigis, ressursi jagatud kasutus)
12.	Õiguste volitamata kasutamine	Pilveteenuse pakkuja töötajate õiguste volitamata kasutamise tulemusena pole andmekogus oleva info muutmise ja hävitamise faktid alati tuvastatavad.	Keskmine	Oluline mõju	Tervikluse tagamiseks kasutatakse andmete töötlemise sündmuste logimist, logide krüptoaheldamist, räsifunktsioone, sõnumi autentimiskoode, digiallkirju jm vahendeid. Vajadusel tuleb kasutada publitseerimise meedet (avalikus pilves olev sisu kirjutatakse teatud aja tagant üle). Pilveteenuse pakkujalt nõutakse sisemiste reeglite järgimise sõltumatut auditeerimist.	Väike	Vähe oluline mõju (intsidendi ulatus võib olla väiksem)	Erisused puuduvad
13.	Halvad pilveteenuse projekti lõpetamise sätted (oht käideldavusele)	Puuduste tõttu pilveteenuse lõpetamise sätetes ei ole võimalik tagada käideldavusnõudeid ning andmekogu ei ole kättesaadav üle 24 tunni.	Keskmine	Oluline mõju	Viiakse läbi pilveteenusepakkuja tüüplepingu analüüs (SLA, teenusepakkuja tugi, teenuse muutmine, kliendi kohustused, teenuse ajutine peatamine, lepingu lõpetamine, teenusepakkuja kohutused, teenusepakkuja vastutus, lepingu muutmine, kolmandate osapoolte kasutamine jne) ning fikseeritakse lepingu lõpetamisel teostatavad protseduurid ning tähtajad. Andmekogu on majutatud mitme erineva pilveteenuse pakkuja juures, teenus on võimalik ümber lülitada teise teenusepakkuja juurde	Väike	Oluline mõju	Erisused puuduvad

Nr	Oht	Tagajärg	Tõenäosus	Mõju	Vastumeetmed	Tõenäosus vastu-meetmetega	Mõju vastumeetme-tega	SVAPP-i avalikule pilvele üle-mineku erisused
14.	Halvad pilveteenuse projekti lõpetamise sätted (oht terviklusele)	Puuduste tõttu pilveteenuse lõpetamise sätetes pole pilveteenuse pakkujalt võimalik kätte saada terviklikku andmestikku ning esineb infokadu.	Keskmine	Oluline mõju	Viiakse läbi pilveteenusepakkuja tüüplepingu analüüs (andmeprivaatsus, andmetele ligipääsu õigus, andmete omaniku õigused, teenusepakkuja tugi, varundamine, teenuse muutmine, kliendi kohustused, teenuse ajutine peatamine, lepingu lõpetamine, teenusepakkuja kohutused, teenusepakkuja vastutus, lepingu muutmine, kolmandate osapoolte kasutamine jne) ning fikseeritakse lepingu lõpetamise tingimused ning andmete tagastamise protseduur andmekogu omanikule. Andmekogu omanik teostab andekogus olevast informatsioonist regulaarselt varukoopiaid, mida säilitatakse pilveteenuse-pakkujast sõltumatus keskkonnas.	Väike	Vähe oluline mõju (intsidendi ulatus võib olla väiksem)	Erisused puuduvad
15.	Sõltuvus välisteenusepakkujast (oht käideldavusele)	Pilveteenusepakkuja vahetamine on keerukas ning ajamahukas, mille tulemusena ei ole andmekogu kättesaadav üle 24 tunni.	Keskmine	Oluline mõju	Viiakse läbi pilveteenusepakkuja tüüplepingu analüüs (SLA, teenusepakkuja tugi, teenuse muutmine, kliendi kohustused, teenuse ajutine peatamine, lepingu lõpetamine, teenusepakkuja kohutused, teenusepakkuja vastutus, lepingu muutmine, kolmandate osapoolte kasutamine jne) ning fikseeritakse lepingu lõpetamisel teostatavad protseduurid ning tähtajad. Andmekogu on majutatud mitme erineva pilveteenuse pakkuja juures, teenus on võimalik ümber lülitada teise teenusepakkuja juurde	Väike	Vähe oluline mõju (intsidendi ulatus võib olla väiksem)	Erisused puuduvad
16.	Sõltuvus välisteenusepakkujast (oht terviklusele)	Raamtingimuste muutumisele (nt välisteenusepakkuja omanikuvahetus, seaduste muutumine, kahtlus välis-teenusepakkuja usaldusväärsuses) võib teatud asjaoludel olla keeruline sobivalt reageerida ning käideldavus- ja terviklusnõuded ei ole täidetud.	Keskmine	Oluline mõju	Viiakse läbi pilveteenusepakkuja tüüplepingu analüüs (andmeprivaatsus, andmetele ligipääsu õigus, andmete omaniku õigused, teenusepakkuja tugi, varundamine, teenuse muutmine, kliendi kohustused, teenuse ajutine peatamine, lepingu lõpetamine, teenusepakkuja kohutused, teenusepakkuja vastutus, lepingu muutmine, kolmandate osapoolte kasutamine jne) ning fikseeritakse lepingutingimuste muutmise ning lõpetamisega seotud protseduurid ja tähtajad.	Väike	Oluline mõju	Erisused puuduvad
17.	Puudulik jätkusuutlikkuse planeerimine väljasttellimise korral	Tõrke esinemisel teenuse töös on raske määrate vea asukohta ning andmekogu ei ole kättesaadav üle 24 tunni.	Keskmine	Oluline mõju	Jätkusuutlikkuse planeerimisel ning taaste organiseerimisel arvestatakse pilve spetsiifiliste riskidega. Teenuse intsidendihalduse-, taaste- ja varundusplaanid peavad arvestama avalike teenuste eripärasid ja suurt avalikku huvi intsidentide vastu.	Väike	Oluline mõju	Erisused puuduvad
18.	Puudulik teenusepakkuja tugi	Pilveteenuse kasutamise tugi ei ole kättesaadav või asjakohane ning andmekogu ei ole kättesaadav üle 24 tunni.	Keskmine	Oluline mõju	Pilveteenuse lepingu sõlmimisel fikseeritakse teenustaseme lepe ning teenusepakkuja toe pakkumise kriteeriumid ja tähtajad. Pilveteenuse pakkuja valimisel teostatakse teenusepakkujate analüüs ning valitakse sertifitseeritud üldtunnustatud infoturbe ja pilve-teenuse standardeid (NT ISO 27001, 27017, 27018, CSA, IT Grundschutz jne) järgiv teenusepakkuja. Testitakse toe toimimist ebastandardsetes tingimustes (nt intsidendid).	Väike	Oluline mõju	Erisused puuduvad

Nr	Oht	Tagajärg	Tõenäosus	Mõju	Vastumeetmed	Tõenäosus vastu-meetmetega	Mõju vastumeetme-tega	SVAPP-i avalikule pilvele üle-mineku erisused
19.	Puudulikud nõuded litsentsihal-dusele pilveteenuse kasutamisel	Litsentsid võivad aeguda või litsentside arv ei ole piisav, mille tule-musena andmekogu ei ole kättesaadav üle 24 tunni.	Väike	Oluline mõju	Litsentsihaldust planeeritakse ja litsentside kasutamist ning arvu jälgitakse. Pilveteenuse pakkuja valimisel teostatakse teenusepak-kujate analüüs ning valitakse sertifitseeritud üldtunnus-tatud infoturbe ja pilve-teenuse standardeid (NT ISO 27001, 27017, 27018, CSA, IT Grundschutz jne) järgiv teenusepakkuja. Pilveteenuse pakkujalt nõutakse sisemiste reeglite jär-gimise sõltumatut auditeerimist.	Väga väike	Oluline mõju	SVAPP-i puhul võib risk olla väiksem tänu heale skaleeruvu-sele
20.	Puuduv või ebapiisav pilvtöötluse kasutamise strateegia	Pilveteenuse kasutamisel ei ole tähelepanu pööratud infoturbe nõuetele, mille tulemusena ei ole andmekogu terviklus ja käideld-avusnõuded täidetud.	Keskmine	Oluline mõju	Enne pilveteenuse kasutamist viiakse läbi pilveteenuse kasutamise riskianalüüs, kaardistatakse lisanduvad riskid ning kirjeldatakse vastumeetmed.	Väike	Oluline mõju	SVAPP-i puhul võib risk olla väiksem, intsidendi tõenäosus vastumeetmetega = väga väike (suur globaalne teenusepakku-ja)
21.	Ebapiisav pilvtöötluse kasutamise administratsioonimudel	Kui pilvtöötluse kasutamisel protsessid muutuvad, kuid uued rollid ei ole piisavalt määratletud või töötajatel pole vajalikku pädevust, võib see kaasa tuua katkestused teenuse osutamisel, mille tulemusena andmekogu ei ole kättesaadav üle 24 tunni.	Väike	Oluline mõju	Enne pilveteenuse kasutamist viiakse läbi pilveteenuse kasutamise riskianalüüs, kaardistatakse lisanduvad riskid ning kirjeldatakse vastumeetmed.	Väga väike	Oluline mõju	Erisused puuduvad
22.	Ebapiisav rollide ja pääsuõiguste kontseptsioon	Tänu ebapiisavale rollide ja pääsuõiguste kontseptsioonile on pilve-teenuse pakkuja töötajatel võimalik muuta andmeid nii, et andmete muutmine pole tuvastatav.	Väike	Oluline mõju	Enne pilveteenuse kasutamist viiakse läbi pilveteenuse kasutamise riskianalüüs, ning defineeritakse nõuded andmetele ligipääsemiseks ja muutmiseks.[5] Pilveteenuse pakkuja valimisel teostatakse teenusepak-kujate analüüs ning valitakse sertifitseeritud üldtunnus-tatud infoturbe ja pilve-teenuse standardeid (NT ISO 27001, 27017, 27018, CSA, IT Grundschutz jne.) järgiv teenusepakkuja Tervikluse tagamiseks kasutatakse andmete töötlemise sündmuste logimist, logide krüptoaheldamist, räsifunkt-sioone, sõnumi autentimiskoode, digiallkirju jm vahen-deid. Vajadusel tuleb kasutada publitseerimise meedet (avali-kus pilves olev sisu kirjutatakse teatud aja tagant üle).	Väga väike	Oluline mõju	Erisused puuduvad
23.	Asutuse ebapiisav kohandamine pilveteenuste kasutamiseks	Kui näiteks asutuses oodatakse, et pilveteenusele üleminek toob kaasa kiire tööjõukulude kokkuhoiu ja vähendatakse kvalifitseeritud töötajate arvu, ent samas vajalike pädevuste arv hoopis kasvab, sest osaliselt jäävad alles ka klassikalised infosüsteemid, siis see võib kaasa tuua antud turvaklassi puhul eeldatud käideldavuse või tervik-luse nõuete rikkumised.	Keskmine	Oluline mõju	Pilveteenusele üleminekule eelneb analüüs, mille põhjal koostatakse pilveteenusele ülemineku strateegia ning konkreetsed tegevused ja mõõdikud.	Väike	Oluline mõju	Erisused puuduvad

[5] *ISKES reguleerivad andmetele ligipääsemist ja muutmist peamiselt tervikluse ja konfidentsiaalsuse turvaosaklasside nõuded.*

Nr	Oht	Tagajärg	Tõenäosus	Mõju	Vastumeetmed	Tõenäosus vastu-meetmetega	Mõju vastumeetme-tega	SVAPP-i avalikule pilvele üle-mineku erisused
24.	G 2.196 Pilveteenuste tervikliku kasutustsükli puuduv tulude ja kulude analüüs	Kui pilveteenuste kasutuselevõtule ei eelne kulude ja tulude tervik-likku analüüsi, võib osutuda, et pilveteenusele üleminek on tegelikult majanduslikult mittetasuv või isegi kahjulik.	Keskmine	Oluline mõju	Pilveteenuse kasutamise strateegia analüüsi käigus tehakse tulude ja kulude analüüs selgitamaks, kas pilve-teenuste juurutamine annab majanduslikke eeliseid. Seejuures arvestatakse pilveteenusele üleviimisega seotud kuludega, käitamiskuludega, koolituskuludega ning võimaliku uue riistvara soetamise ja võrgu jõudlus-näitajate suurendamise kuludega.	Väike	Oluline mõju	Erisused puuduvad
25.	Puudulik nõuete haldus pilvtöötluse kasutamisel	Pilveteenuse kasutamisel ei ole tähelepanu pööratud andmekogu turvaklassist tulenevatele infoturbe nõuetele, mille tulemusena ei ole andmekogu terviklus ja käideldavusnõuded täidetud.	Keskmine	Oluline mõju	Enne pilveteenuse kasutamist viiakse läbi pilveteenuse kasutamise riskianalüüs, kaardistatakse lisanduvad riskid ning kirjeldatakse vastumeetmed. Seejuures tuleb arvestada, et kuna andmete pilves töötlemisega kaasnevad muutunud ja täiendavad ohud (andmed asuvad ja neid töödeldakse pilveteenuse pakkuja arvutites, kes seega pääseb andmetele ligi), tuleb teatud juhtudel rakendada andmete tervikluse ja käideldavuse kaitseks kõrgema turbeastme meetmeid.	Väike	Oluline mõju	Erisused puuduvad
26.	Puudulik nõuete haldus pilvtöötluse kasutamisel (oht konfidentsiaalsusele)	Pilveteenuse kasutamisel ei ole tähelepanu pööratud infoturbe nõuetele, mille tulemusena ei ole tagatud andmekogu haldamise ja autentimise salajase info konfidentsiaalsus.	Keskmine	Oluline mõju	Andmekogu salajane haldamise ja autentimise informat-sioon säilitatakse andmekogus krüpteeritud kujul. Enne pilveteenuse kasutamist viiakse läbi pilveteenuse kasutamise riskianalüüs, kaardistatakse lisanduvad riskid ning kirjeldatakse vastumeetmed. Kuna andmete pilves töötlemisega kaasnevad muutunud ja täiendavad ohud, tuleb teatud juhtudel rakendada haldamise ja autentimise info tervikluse ja käideldavuse kaitseks kõrgema turbeastme meetmeid. Valida sobiv marsruutimise meetod (traffic-routing method), kasutada otseühendust (dedicated connection) vms.	Väike	Oluline mõju	SVAPP-i puhul võib intsidendi tõenäosus olla suurem (andme-te transiit läbi välisriigi, andme-te hoidmine välisriigis, ressursi jagatud kasutus)
27.	Teenuse osutamise ebapiisav järelevalve	Pilveteenuse pakkuja poolt osutatav teenus ei vasta nõutud käidel-davus- ja terviklusnõuetele	Keskmine	Oluline mõju	Pilveteenuse pakkujalt nõutakse sisemiste reeglite jär-gimise sõltumatut auditeerimist. Kuna andmete pilves töötlemisega kaasnevad muutunud ja täiendavad ohud, tuleb vajadusel rakendada teenuse käideldavuse ja tervikluse kaitseks kõrgema turbeastme meetmeid. Vajadusel tuleb kasutada publitseerimise meedet (avali-kus pilves olev sisu kirjutatakse teatud aja tagant üle)	Väike	Oluline mõju	SVAPP-i puhul võib intsidendi tõenäosus olla suurem (järele-valve võib olla raskem)
28.	Ebapiisav pilvtöötluse integreeri-mine asutuse olemasoleva info-töötlusega	Kui osa infotöötlusest (näiteks andmete esmane kogumine) toimub klassikaliste IT vahenditega ning osa pilvtöötluse vahenditega, siis selliste komponentide integreerimine võib ebapiisava pädevuse korral kaasa tuua efektiivsuse vähenemist, tõrkeid süsteemides ning antud turvaklassi puhul eeldatud käideldavuse või tervikluse nõuete rikkumisi.	Keskmine	Oluline mõju	Pilveteenusele üleminekule eelneb analüüs, mille põhjal koostatakse pilveteenusele ülemineku strateegia ning konkreetsed tegevused ja mõõdikud.	Väike	Oluline mõju	Erisused puuduvad
29.	Puudulik pilveteenustele üleme-neku kavandamine (oht käideldavusele)	Pilveteenuse üleminek on puudulikult planeeritud, mille tulemusena ei ole andmekogu kättesaadav üle 24 tunni.	Keskmine	Oluline mõju	Pilveteenusele üleminekule eelneb analüüs, mille põhjal koostatakse pilveteenusele ülemineku strateegia ning konkreetsed tegevused ja mõõdikud.	Väike	Oluline mõju	Erisused puuduvad

Nr	Oht	Tagajärg	Tõenäosus	Mõju	Vastumeetmed	Tõenäosus vastumeetmetega	Mõju vastumeetmetega	SVAPP-i avalikule pilvele ülemineku erisused
30.	Puudulik pilveteenustele ülemineku kavandamine (oht konfidentsiaalsusele)	Pilveteenuse üleminek on puudulikult planeeritud, mille tulemusena muutub avalikuks salajane andmekogu haldamise ja/või autentimise info.	Keskmine	Oluline mõju	Pilveteenusele üleminekule eelneb analüüs, mille põhjal koostatakse pilveteenusele ülemineku strateegia ning konkreetsed tegevused ja mõõdikud. Andmekogu salajane haldamise ja autentimise informatsioon säilitatakse andmekogus krüpteeritud kujul. Valida sobiv marsruutimise meetod (traffic-routing method), kasutada otseühendust (dedicated connection) vms.	Väike	Oluline mõju	SVAPP-i puhul võib intsidendi tõenäosus olla suurem (andmete transiit läbi välisriigi, andmete hoidmine välisriigis, ressursi jagatud kasutus)
31.	Pilveteenuse pakkuja puudulik valik	Valitud pilveteenuse pakkuja ei suuda täita kokkulepitud terviklus- ja käideldavusnõudeid.	Keskmine	Oluline mõju	Pilveteenuse pakkuja valimisel teostatakse teenusepakkujate analüüs ning valitakse sertifitseeritud üldtunnustatud infoturbe ja pilve-teenuse standardeid (NT ISO 27001, 27017, 27018, CSA, IT Grundschutz jne) järgiv teenusepakkuja. Teenusepakkujalt nõutakse regulaarseid SLA täitmise raporteid.	Väike	Oluline mõju	SVAPP-i puhul võib risk olla väiksem, intsidendi tõenäosus vastumeetmetega = väga väike (suur globaalne teenusepakkuja)
32.	Väliste teenuste volitamata kasutamine	Pilveteenuse pakkuja kasutab väliseid teenusepakkujaid, kellele esitatud infoturbe nõuded ei vasta andmekogu terviklus ja käideldavusnõuetele.	Keskmine	Oluline mõju	Viiakse läbi pilveteenusepakkuja tüüplepingu analüüs ning fikseeritakse kolmandate teenusepakkujate kasutamise tingimused.	Väike	Oluline mõju	Erisused puuduvad
33.	Väliste teenuste volitamata kasutamine (oht konfidentsiaalsusele)	Pilveteenuse pakkuja kasutab väliseid teenusepakkujaid, kellele lubatakse ligipääs salajasele andmekogu haldamise ja/või autentimise infole.	Keskmine	Oluline mõju	Viiakse läbi pilveteenusepakkuja tüüplepingu analüüs ning fikseeritakse kolmandate teenusepakkujate kasutamise tingimused. Andmekogu salajane haldamise ja autentimise informatsioon säilitatakse andmekogus krüpteeritud kujul. Valida sobiv marsruutimise meetod (traffic-routing method), kasutada otseühendust (dedicated connection) vms.	Väike	Oluline mõju	Erisused puuduvad
34.	Virtuaalsetel IT-süsteemidel kasutatavate rakenduste ebapiisav tootjatugi	Kui virtuaalsetel IT-süsteemidel kasutatavate rakenduste tootjatugi on puudulik või informatsioon uuenduste ja paikade kohta ei ole kättesaadav, võib see kaasa tuua ohud andmete ja süsteemide käideldavusele, terviklusele või konfidentsiaalsusele.	Keskmine	Oluline mõju	Pilveteenusele üleminekule eelneva analüüsi käigus selgitatakse, kas pilves kasutatava rakenduse tarkvara tootja annab aegsasti vastavad paigad kõikide vajalike komponentide jaoks. Komponendid, mille kasutamine vastava tootja poolt katkestatakse, tuleb kiiresti välja vahetada. Samuti tuleb selgitada, milliste kanalite kaudu saab andmeid turvaaukude, uuenduste ja paikade kohta ja kuidas neid oma paikade ja muudatuste protsessis tuleb töödelda.	Väike	Oluline mõju	Erisused puuduvad

Nr	Oht	Tagajärg	Tõenäosus	Mõju	Vastumeetmed	Tõenäosus vastumeetmetega	Mõju vastumeetmetega	SVAPP-i avalikule pilvele ülemineku erisused
Tehnilised rikked								
35.	Usaldusteenuste puudulik toimimine pilveteenuse puhul (oht terviklusele või konfidentsiaalsusele)	Digitaalallkirjastamine, sertifikaadi kehtivuse kontroll või muud usaldusteenused ei toimi pilve puhul, sest nad sõltuvad Eesti ID-kaardi või usaldusteenuse pakkuja eripärast.	Keskmine	Oluline mõju	Enne pilveteenuse kasutamist viiakse läbi pilveteenuse kasutamise riskianalüüs, kaardistatakse lisanduvad riskid ning kirjeldatakse vastumeetmed. Püütakse saavutada pilveteenuse pakkujaga kokkuleppeid usaldusteenuste toimimise kohta. Kuna andmete pilves töötlemisega kaasnevad muutunud ja täiendavad ohud, tuleb vajadusel rakendada andmete tervikluse ja konfidentsiaalsuse kaitseks kõrgema turbeastme meetmeid. Tervikluse tagamiseks kasutatakse andmete töötlemise sündmuste logimist, logide krüptoaheldamist, räsifunktsioone, sõnumi autentimiskoode, digiallkirju jm vahendeid.	Väike	Oluline mõju	SVAPP-i puhul võib intsidendi tõenäosus olla suurem (globaalne teenusepakkuja, andmete transiit läbi välisriigi, andmete hoidmine välisriigis, ressursi jagatud kasutus)
36.	Ebaturvalised protokollid avalikes võrkudes	Ebaturvaliste protokollide puhul kantakse kasutajanimed, paroolid ja kasulikud andmed võrgus üle avatekstina (oht konfidentsiaalsusele ja terviklusele)	Keskmine	Oluline mõju	Halduseks tuleb kasutada kas eraldi haldusvõrku või protokolle, mis toetavad turvatud autentimist ja krüpteeritud andmeedastust (näiteks SSH-2).	Väga väike	Oluline mõju	Erisused puuduvad
37.	Ebaturvalised krüptoalgoritmid või vananenud krüptomeetodid	Ebaturvaliste krüptoalgoritmide või vananenud krüptomeetodite kasutamise tõttu tekib oht terviklusele või muutub avalikuks salajane andmekogu haldamise ja/või autentimise info.	Väike	Oluline mõju	Rakendatakse krüpteerimisega seotud meetmeid, sh krüptoalgoritmide ja krüptomeetodite elutsüklite jälgimine, krüptokontseptsiooni väljatöötamine, krüptoprotseduuride ja –toodete vajaduse määramine, sobiva krüptotoote valimine, krüpteerimise õige korraldus jne.	Väga väike	Oluline mõju	Erisused puuduvad
38.	Pilveteenuse haldamise vahendite häired pilvtöötluse kasutamisel	Pilveteenuse haldamise vahendite häirete tulemusena pole andmekogus oleva info muutmise ja hävitamise faktid alati tuvastatavad.	Väike	Oluline mõju	Pilveteenuse pakkuja valimisel teostatakse teenusepakkujate analüüs ning valitakse sertifitseeritud parimaid praktikaid ja standardeid järgiv teenusepakkuja. Pilveteenuse pakkuja valimisel teostatakse teenusepakkuja teenuste ja haldusvahendite analüüs Andmekogus oleva info muutmise ja hävitamise faktide tuvastamiseks kasutatakse andmete töötlemise sündmuste logimist, logide krüptoaheldamist, räsifunktsioone, sõnumi autentimiskoode, digiallkirju jm vahendeid. Vajadusel tuleb kasutada publitseerimise meedet (avalikus pilves olev sisu kirjutatakse teatud aja tagant üle).	Väga väike	Oluline mõju	SVAPP-i puhul võib risk olla väiksem (suur globaalne teenusepakkuja)
39.	Pilveteenuse pakkuja puudulik varukoopiate tegemise protsess	Pilveteenuse pakkuja puuduliku varukoopiate tegemise protsessi tõttu pole võimalik taastada andmestikku kokkulepitud ulatuses ning esineb infokadu.	Keskmine	Oluline mõju	Pilveteenuse pakkuja valimisel teostatakse teenusepakkujate analüüs ning valitakse sertifitseeritud parimaid praktikaid ja standardeid järgiv teenusepakkuja Andmekogu omanik teostab andekogus olevast informatsioonist regulaarselt varukoopiaid, mida säilitatakse pilveteenuse-pakkujast sõltumatus keskkonnas	Väike	Oluline mõju	SVAPP-i puhul võib risk olla väiksem, intsidendi tõenäosus vastumeetmetega = väga väike (suur globaalne teenusepakkuja)

Nr	Oht	Tagajärg	Tõenäosus	Mõju	Vastumeetmed	Tõenäosus vastumeetmetega	Mõju vastumeetmetega	SVAPP-i avalikule pilvele ülemineku erisused
40.	Pilveteenuse kasutajate üheaegne koormuse tõus	Pilveteenuse klientide üheaegse koormuse tõusu tõttu, ei suuda pilveteenuse pakkuja tagada kokkulepitud käideldavusnõudeid, mille tulemusena ei ole andmekogu kättesaadav üle 24 tunni.	Väike	Oluline mõju	Pilveteenuse pakkuja valimisel teostatakse teenusepakkujate analüüs (arvestatakse ka teenusepakkuja poolt läbiviidud koormus-testidega) ning valitakse teenusepakkuja, kellel on võimekus koormuse tõusuga toimetulekuks. Andmekogu on majutatud mitme erineva pilveteenuse pakkuja juures, ühe teenuse-pakkuja väljalangemisel on võimalik teenus ümber lülitada teise teenusepakkuja juurde.	Väga väike	Oluline mõju	SVAPP-i puhul võib risk olla väiksem (suur globaalne teenusepakkuja)
41.	Puudulikud ühendused välisteenuse või pilveteenuse osutajaga	Puudulike ühenduste tõttu välisteenuse või pilveteenuse osutajaga tekib oht käideldavusele või terviklusele.	Keskmine	Oluline mõju	Pilveteenusele üleminekule eelneb analüüs, mille käigus selgitatakse välja ühenduse vajadused, sealhulgas teenustasemed. Vajadusel planeeritakse varusidekanalid. Pilveteenuse osutajaga lepitakse kokku ühenduste tehnilised parameetrid ja teenustasemed.	Väike	Oluline mõju	Erisused puuduvad
42.	Pilveteenuse konservatiivne konfigureerimine	Pilveteenuse konservatiivse konfigureerimise tõttu ei ole täidetud andmetöötluse jõudlusnõuded, mistõttu tekib oht käideldavusele või terviklusele.	Keskmine	Oluline mõju	Võtta pilveteenuse kavandamise ja konfigureerimise aluseks reaalses kasutuses oleva süsteemi nõuded, eriti arvestades andmebaasiserverite jõudlusnõudeid.	Väike	Oluline mõju	Erisused puuduvad
43.	Avaliku pilve konfiguratsiooni probleemid	Kui pilve virtuaalsed masinad on konfigureeritud teisiti kui rakendus eeldab (näiteks, virtuaalmasina TCP/IP aadressid muutuvad, kui süsteem vabastatakse, kuid ligipääs süsteemile eeldab kindlat TCP/IP aadressi), siis see võib põhjustada viivitusi ja käideldavuse probleeme pilve kasutamisel.	Keskmine	Vähe oluline mõju	Planeerida ja testida avaliku pilve virtuaalsete masinate konfiguratsioon pilveteenuse rakendamisel (näiteks, reserveerida rakendamise käigus vajalikud staatilised TCP/IP aadressid).	Väike	Vähe oluline mõju	Erisused puuduvad
44.	Ümberlülitumisel andmebaasi peegelserverile ei ole tagatud andmete terviklus	Kui esmane andmebaasi server muutub ligipääsmatuks ja on vaja ümber lülituda peegelserverile, võivad tekkida häired andmete tervikluse ja käideldavuse tagamisel.	Keskmine	Oluline mõju	Dokumenteerida ja testida olukorrad, kus esmane andmebaasi server muutub ligipääsmatuks ja on vaja ümber lülituda peegelserverile. Planeerida ette, kas olulisem on tervikluse säilitamine või rakenduse funktsionaalsuse säilitamine, kui selline valik osutub vajalikuks.	Väike	Oluline mõju	Erisused puuduvad
45.	Avaliku pilve kasutamine avarii järgse taastusressursina pole kindlustatud ilma andmete omaniku eritegevusteta	Avaliku pilve taaste sihtajad (*Recovery Time Objective, RTO*) võivad olla põhimõtteliselt saavutatavad, kuid see nõuab vastavate tegevuste planeerimist ning pole võimalik ilma eritegevusteta.	Keskmine	Oluline mõju	Planeerida ja rakendada meetmed avaliku pilve taaste sihtaegade saavutamiseks, muuhulgas kindlustades kõigi vajalike süsteemide ja sõltuvuste olemasolu pilves enne avarii-ümberlülituse (*failover*) sündmust.	Väike	Oluline mõju	Erisused puuduvad
Ründed								
46.	Küberrünne pilveteenuse pakkuja vastu	Pilveteenuse pakkuja vastu suunatud küberrünnaku tõttu ei suuda pilveteenuse pakkuja tagada kokkulepitud käideldavusnõudeid ning andmekogu ei ole kättesaadav üle 24 tunni.	Keskmine	Oluline mõju	Andmekogu on majutatud mitme erineva pilveteenuse pakkuja juures, ühe teenuse-pakkuja väljalangemisel on võimalik teenus ümber lülitada teise teenusepakkuja juurde.	Väike	Oluline mõju	SVAPP-i puhul võib risk olla väiksem, intsidendi tõenäosus vastumeetmetega = väga väike (suur globaalne teenusepakkuja)

Nr	Oht	Tagajärg	Tõenäosus	Mõju	Vastumeetmed	Tõenäosus vastumeetmetega	Mõju vastumeetmetega	SVAPP-i avalikule pilvele ülemineku erisused
47.	Administraatori õiguste väärkasutus	Pilveteenuse pakkuja IT administraatorite õiguste volitamata kasutamise tulemusena pole andmekogus oleva info muutmise ja hävitamise faktid alati tuvastatavad ning esineb tervikluse kadu	Väike	Oluline mõju	Pilveteenuse pakkuja valimisel teostatakse teenusepakkujate analüüs ning valitakse sertifitseeritud parimaid praktikaid ja standardeid järgiv teenusepakkuja. Pilveteenuse pakkujalt nõutakse sisemiste reeglite järgimise sõltumatut auditeerimist. Andmekogus oleva info tervikluse tagamiseks kasutatakse andmete töötlemise sündmuste logimist, logide krüptoaheldamist, räsifunktsioone, sõnumi autentimiskoode, digiallkirju jm vahendeid. Vajadusel tuleb kasutada publitseerimise meedet (avalikus pilves olev sisu kirjutatakse teatud aja tagant üle).	Väga väike	Oluline mõju	Erisused puuduvad
48.	Välise teenusepakkuja poolne käideldavuse häirimine	Välise teenusepakkuja sihiliku käideldavuse häirimise tõttu ei ole andmekogu kättesaadav üle 24 tunni.	Väike	Oluline mõju	Andmekogu on majutatud mitme erineva pilveteenuse pakkuja juures, ühe teenuse-pakkuja väljalangemisel on võimalik teenus ümber lülitada teise teenusepakkuja juurde	Väga väike	Oluline mõju	SVAPP-i puhul võib risk olla väiksem (suur globaalne teenusepakkuja)
49.	Välise teenusepakkuja poolne andmete paljastamine kolmandatele isikutele	Välise teenusepakkuja sihiliku tegevuse tulemusena muutub avalikuks salajane andmekogu haldamise ja/või autentimise info.	Väike	Oluline mõju	Andmekogu salajane haldamise ja autentimise informatsioon säilitatakse andmekogus krüpteeritud kujul, vajadusel toimub ka selle informatsiooni edastamine krüpteeritult. Pilveteenuse pakkuja valimisel teostatakse teenusepakkujate analüüs ning valitakse sertifitseeritud parimaid praktikaid ja standardeid järgiv teenusepakkuja. Pilveteenuse pakkujalt nõutakse sisemiste reeglite järgimise sõltumatut auditeerimist	Väga väike	Oluline mõju	SVAPP-i puhul võib intsidendi tõenäosus olla suurem (andmete transiit läbi välisriigi, andmete hoidmine välisriigis, ressursi jagatud kasutus)
50.	Transporditavate andmete (*data in motion*) salvestamine ja hilisem dekrüpteerimine	Kui salajast andmekogu haldamise ja/või autentimise infot saadetakse krüpteeritult üle avaliku interneti, kontrollimata seejuures osapooli ning nende turvameetmeid, võib ründajal olla võimalik andmed vahepeal salvestada. Salvestatud andmed saab dekrüpteerida hiljem, kui kasutatud krüptomeetodid on vananenud ning dekrüpteerimise meetodid edasi arenenud, kusjuures see võimalus võib realiseeruda enne salastamistähtaja möödumist.	Väike	Oluline mõju	Valida sobiv marsruutimise meetod (traffic-routing method), kasutada otseühendust (dedicated connection) vms	Väga väike	Vähe oluline mõju	SVAPP-i puhul võib intsidendi tõenäosus olla suurem (andmete transiit läbi välisriigi, andmete hoidmine välisriigis, ressursi jagatud kasutus)

Nr	Oht	Tagajärg	Tõenäosus	Mõju	Vastumeetmed	Tõenäosus vastumeetmetega	Mõju vastumeetmetega	SVAPP-i avalikule pilvele ülemineku erisused
51.	Paremad ründevõimalused seoses simultaanteeninduse (*multi-tenancy*) rakendamisega	Simultaanteeninduse rakendamisel töötab serveril tarkvara üksainus eksemplar ja virtuaalselt tükeldatuna teenindab ta paljusid klientorganisatsioone; kui selline klientorganisatsioon on ründaja, võib ta omada eeliseid ligipääsuks teistele sama tarkvara poolt teenindavatele süsteemidele (sh virtuaalsete IT-süsteemide hüperviisori kompromiteerimine). See võib kaasa tuua ohte andmete terviklusele, konfidentsiaalsusele või käideldavusele.	Väike	Oluline mõju	Pilveteenuse pakkujalt nõutakse infot selle kohta, kas virtuaalsete IT-süsteemide ja nendel käitatavate rakenduste isolatsioon ja eraldatus on piisaval määral tagatud. Kogutakse kättesaadavat infot pilveteenuse pakkuja teiste klientorganisatsioonide kohta. Andmekogu salajane haldamise ja autentimise informatsioon säilitatakse andmekogus krüpteeritud kujul, vajadusel toimub ka selle informatsiooni edastamine krüpteeritult. Andmekogus oleva info tervikluse tagamiseks kasutatakse andmete töötlemise sündmuste logimist, logide krüptoaheldamist, räsifunktsioone, sõnumi autentimiskoode, digiallkirju jm vahendeid. Vajadusel tuleb kasutada publitseerimise meedet (avalikus pilves olev sisu kirjutatakse teatud aja tagant üle).	Väga väike	Vähe oluline mõju	SVAPP-i puhul võib intsidendi tõenäosus olla suurem (andmete transiit läbi välisriigi, andmete hoidmine välisriigis, ressursi jagatud kasutus)

4. Ettepanekud ISKE täiendamiseks pilve-spetsifiiliste ohtudega K1T1S0 turvaklassis

Riskide tabelis on esitatud erineva uudsuse astmega ohud. Ohtude uudsuse astmed ja sellest tulenevad ohtude lülitamise tegevused ISKE täiendamise nimekirja on järgmised.

- Täiesti uued ohud, mida ei saa tuletada ISKE ohtude nimekirjas juba olemas olevate ohtude baasil. Need on lülitatud alltoodud ettepanekutesse (1) lisamiseks ISKE ohtude nimekirja ja (2) lisamiseks moodulisse B 1.17 "Pilvteenuse kasutamine".
- Ohud, mis on olemas ISKE ohtude kataloogis või mida saab selle nimekirja ohtudest tuletada, kuid mida pole moodulis B1.17. Need on lülitatud alltoodud ettepanekutesse lisamiseks moodulisse B 1.17 "Pilvteenuse kasutamine". Näide: riskide tabeli riski Nr 1 oht "Pilveteenusepakkuja IT-süsteemi avarii (tehnilise rikke, inimvea, vääramatu jõu vms tõttu) (oht käideldavusele)" on tuletatav ISKE olemasolevast ohust "G 1.2 IT-süsteemi avarii", kuid seda pole toodud moodulis B 1.17. Seetõttu on see pakutud lisamiseks moodulisse B 1.17, kuid mitte üldisesse ISKE riskide nimistusse.
- Ohud, mis on ISKE mooduli B 1.17 "Pilvteenuse kasutamine" ohtude nimekirjas või mida saab selle nimekirja ohtudest tuletada. Neid ei ole ettepanekutena esitatud. Näide: riskide tabeli riski Nr 3 oht "Pilveteenusepakkuja väljalangemine" on tuletatav mooduli B 1.17 "Pilvteenuse kasutamine" ohtude nimekirjas olevast ohust "G 1.19 Teenusepakkuja või tarnija väljalangemine", seepärast pole seda uue ohuna lisatud. Vajadusel võib sellised tuletatud ohud lisada.

Viitamisel tabelile "Pilves paiknemisest tulenevate täiendavate riskide loetelu koos põhjendustega infosüsteemi kohta, mille ISKE turvaklass on K1T1S0" (edaspidi "riskide tabel") kasutatakse peatükk nr. 3 K1T1S0 andmekogu pilveriskid ja vastumeetmed Tabelit.

Ohu nr	Oht	Nr riskide tabelist	Kas lisada ISKE ohtude nimekirja?	Kas lisada moodulisse B 1.17?
Vääramatu jõud				
1.	G 1.2 IT-süsteemi avarii	1, 2	Ei	Jah
Organisatsioonilised puudused				
2.	Puudulik teenusepakkuja tugi	18	Jah	Jah
3.	Väliste teenuste volitamata kasutamine	32, 33	Jah	Jah
Tehnilised rikked				
4.	Usaldusteenuste puudulik toimimine pilveteenuse puhul	35	Jah	Jah
5.	Pilveteenuse pakkuja puudulik varukoopiate tegemise protsess	39	Jah	Jah
6.	Pilveteenuse kasutajate üheaegne koormuse tõus	40	Jah	Jah
7.	Puudulikud ühendused välisteenuse või pilveteenuse osutajaga	41	Jah	Jah
8.	Pilveteenuse konservatiivne (aladimensioneerimine) konfigureerimine	42	Jah	Jah

Ohu nr	Oht	Nr riskide tabelist	Kas lisada ISKE ohtude nimekirja?	Kas lisada moodulisse B 1.17?
9.	Avaliku pilve konfiguratsiooni probleemid	43	Jah	Jah
10.	Ümberlülitumisel andmebaasi peegelserverile ei ole tagatud andmete terviklus	44	Jah	Jah
11.	Avaliku pilve kasutamine avarii järgse taaste ressursina pole kindlustatud ilma andmeomaniku eritegevusteta.	45	Jah	Jah
Ründed				
12.	Küberrünne pilveteenuse pakkuja vastu	46	Jah	Jah
13.	Transporditavate andmete (*data in motion*) salvestamine ja hilisem dekrüpteerimine	50	Jah	Jah
14.	Paremad ründevõimalused seoses simultaanteeninduse (*multitenancy*) rakendamisega	51	Jah	Jah

5. Ettepanekud ISKE täiendamiseks pilve-spetsifiiliste meetmetega K1T1S0 turvaklassis

Riskide tabelis on esitatud erineva uudsuse astmega meetmed. Meetmete uudsuse astmed ja sellest tulenevad meetmete lülitamise tegevused ISKE täiendamise nimekirja on järgmised.

- Täiesti uued meetmed, mida ei saa tuletada ISKE meetmete nimekirjas juba olemas olevate meetmete baasil. Need on lülitatud alltoodud ettepanekutesse (1) lisamiseks ISKE meetmete nimekirja ja (2) lisamiseks moodulisse B 1.17 "Pilvteenuse kasutamine".
- Meetmed, mida saaks lisada kas iseseisva meetmena või täienduseks mõnele ISKE meetmete nimekirjas olevale meetmele. Nende puhul on lisatud märkus selle kohta, millist olemasolevat meedet saaks täiendada.
- Meetmed, mis on ISKE mooduli B 1.17 "Pilvteenuse kasutamine" meetmete nimekirjas või mida saab selle nimekirja meetmetest tuletada. Neid ei ole ettepanekutena esitatud. Näide: riskide tabeli riski Nr 1 meede "Pilveteenuse pakkuja valimisel teostatakse teenusepakkujate analüüs ning valitakse kõrgete käideldavusnäitajatega teenuse-pakkuja" on tuletatav mooduli B 1.17 "Pilvteenuse kasutamine" meetmete nimekirjas olevast meetmest "M 2.540 Pilvteenuste osutaja hoolikas valimine", seepärast pole seda uue meetmena lisatud. Vajadusel võib sellised tuletatud meetmed lisada.

Viitamisel tabelile "Pilves paiknemisest tulenevate täiendavate riskide loetelu koos põhjendustega infosüsteemi kohta, mille ISKE turvaklass on K1T1S0" (edaspidi "riskide tabel") kasutatakse peatükk nr. 3 K1T1S0 andmekogu pilveriskid ja vastumeetmed Tabelit.

Meetme nr	Meede	Nr riskide tabelist	Kas lisada ISKE meetmete nimekirja?	Kas lisada moodulisse B 1.17?	Meetme täpsustus riskide tabelist
Planeerimine ja kontseptsioon					
1.	Andmekogu majutamine mitme erineva pilveteenuse pakkuja juures	1	Jah	Jah	Andmekogu on majutatud mitme erineva pilveteenuse pakkuja juures, ühe teenuse-pakkuja väljalangemisel on võimalik teenus ümber lülitada teise teenusepakkuja juurde.
2.	Lisavahendid tervikluse tagamiseks pilves	6	Jah	Jah	Tervikluse tagamiseks kasutatakse andmete töötlemise sündmuste logimist, logide krüptoaheldamist, räsifunktsioone, sõnumi autentimiskoode, digiallkirju jm vahendeid.
3.	Pilveteenuse litsentsihalduse planeerimine ja jälgimine	19	Jah	Jah	Pilveteenuse litsentsihaldust planeeritakse ja litsentside kasutamist ning arvu jälgitakse.
4.	Kõrgema turbeastme meetmete kasutamine pilveteenustele üleminekul	25	Jah	Jah	Tuleb arvestada, et kuna andmete pilves töötlemisega kaasnevad muutunud ja täiendavad ohud (andmed asuvad ja neid töödeldakse pilveteenuse pakkuja arvutites, kes seega pääseb andmetele ligi), tuleb teatud juhtudel rakendada andmete tervikluse ja käideldavuse kaitseks kõrgema turbeastme meetmeid. Märkus: võimalik on meetme M 2.537 täiendamine.
5.	Pilves kasutatava rakenduse tarkvara tootjatoe tagamine	34	Jah	Jah	Pilveteenusele üleminekule eelneva analüüsi käigus selgitatakse, kas pilves kasutatava rakenduse tarkvara tootja annab aegsasti vastavad paigad kõikide vajalike komponentide jaoks. Komponendid, mille kasutamine vastava tootja poolt katkestatakse, tuleb kiiresti välja vahetada. Samuti tuleb selgitada, milliste kanalite kaudu saab andmeid turvaaukude, uuenduste ja paikade kohta ja kuidas neid oma paikade ja muudatuste protsessis tuleb töödelda.
6.	Pilveteenuste reaalne konfigureerimine ja testimine	42, 43	Jah	Jah	Võtta pilveteenuse kavandamise ja konfigureerimise aluseks reaalses kasutuses oleva süsteemi nõuded, eriti arvestades andmebaasiserverite jõudlusnõudeid. Planeerida ja testida avaliku pilve virtuaalsete masinate konfiguratsioon pilveteenuse rakendamisel (näiteks, reserveerida rakendamise käigus vajalikud staatilised TCP/IP aadressid).

Meetme nr	Meede	Nr riskide tabelist	Kas lisada ISKE meetmete nimekirja?	Kas lisada moodulisse B 1.17?	Meetme täpsustus riskide tabelist
7.	Sobiva marsruutimise meetodi valimine	11	Jah	Jah	Valida sobiv marsruutimise meetod (traffic-routing method), kasutada otseühendust (dedicated connection) vms.
Soetamine					
8.	Teenusepakkuja toe täiendav testimine	18	Jah	Jah	Testitakse toe toimimist ebastandardsetes tingimustes (nt intsidendid).
9.	Usaldusteenuste toimimise kokkulepped pilveteenuse pakkujaga	35	Jah	Jah	Püütakse saavutada pilveteenuse pakkujaga kokkuleppeid usaldusteenuste toimimise kohta.
Rakendamine					
10.	Turvalised protokollid pilveteenuste halduseks	36	Jah	Jah	Halduseks tuleb kasutada kas eraldi haldusvõrku või protokolle, mis toetavad turvatud autentimist ja krüpteeritud andmeedastust (näiteks SSH-2).
Kasutamine					
11.	Avalikus pilves oleva sisu ülekirjutamine	6	Jah	Jah	Vajadusel tuleb kasutada publitseerimise meedet (avalikus pilves olev sisu kirjutatakse teatud aja tagant üle).
Valmisolek hädaolukorraks					
12.	Pilve spetsiifiliste riskide ning kõrgendatud avaliku huvi arvestamine	17	Jah	Jah	Jätkusuutlikkuse planeerimisel ning taaste organiseerimisel arvestatakse pilve spetsiifiliste riskidega. Teenuse intsidendihalduse-, taaste- ja varundusplaanid peavad arvestama avalike teenuste eripärasid ja suurt avalikku huvi intsidentide vastu. Märkus: võimalik on meetme M 6.155 täiendamine.
13.	Peegelserverile ülemineku planeerimine ja testimine	44	Jah	Jah	Plaanida ette ja testida olukorrad, kus esmane andmebaasi server muutub ligipääsmatuks ja on vaja ümber lülituda peegelserverile. Planeerida ette, kas olulisem on tervikluse säilitamine või rakenduse funktsionaalsuse säilitamine, kui selline valik osutub vajalikuks. Märkus: võimalik on meetme M 6.155 täiendamine.
14.	Avaliku pilve kasutamine avarii järgse taaste ressursina pole kindlustatud ilma andmeomaniku eritegevusteta.	45	Jah	Jah	Planeerida ja rakendada meetmed avaliku pilve taaste sihtaegade (Recovery Time Objective, RTO) saavutamiseks, muuhulgas kindlustades kõigi vajalike süsteemide ja sõltuvuste olemasolu pilves enne avarii-ümberlülituse (failover) sündmust. Märkus: võimalik on meetme M 6.155 täiendamine.

Meetme nr	Meede	Nr riskide tabelist	Kas lisada ISKE meetmete nimekirja?	Kas lisada moodulisse B 1.17?	Meetme täpsustus riskide tabelist
15.	Simultaanteeninduse (multitenancy) rakendamisega seotud ründevõimaluste arvestamine	51	Jah	Jah	Pilveteenuse pakkujalt nõutakse infot selle kohta, kas virtuaalsete IT-süsteemide ja nendel käitatavate rakenduste isolatsioon ja eraldatus on piisaval määral tagatud. Kogutakse kättesaadavat infot pilveteenuse pakkuja teiste klientorganisatsioonide kohta. Märkus: võimalik on meetme M2.540 täiendamine

6. Lisad

Lisa 1 - K1T1S0 rakendamatud_ISKE_meetmed_7_00.xlsx