



Valimiste infosüsteemide ja nendega seotud protsesside turvalisuse terviklik auditeerimine ja hindamine Majandus- ja Kommunikatsiooniministeeriumile

Viitenumber 241800

Majandus- ja Kommunikatsiooniministeerium

11.05.2022



KPMG Baltics OÜ
Narva mnt 5
Tallinn 10117
Estonia

Telephone +372 626 8700
Fax +372 626 8777
Internet www.kpmg.ee

Martin Sepp
Majandus- ja Kommunikatsiooniministeerium
Suur-Ameerika 1
10122, Tallinn

11.05.2022

Lugupeetud Martin Sepp

Vastavalt 22.10.2021 sõlmitud KPMG Baltics OÜ (edaspidi KPMG) ja Majandus- ja Kommunikatsiooniministeerium (edaspidi MKM) vahelisele töövõtulepingule (nr 1.9-8/21-406-1) viis KPMG ajavahemikus 27.10.2021–22.04.2022 läbi valimiste infosüsteemide ja nendega seotud protsesside turvalisuse tervikliku auditeerimise ja hindamise.

Valimiste infosüsteemide ja nendega seotud protsesside turvalisuse auditeerimise käigus tehtud tähelepanekute ja soovitude kohta on esitatud käesolev aruanne, mis on kooskõlastatud MKM-ga.

Materjalide avalikustamine kolmandatele pooltele on reguleeritud vastavalt MKM-i (Klient) ja KPMG vahel sõlmitud lepingu üldtingimustele. KPMG poolt Kliendile käesoleva lepingulise suhtega seoses edastatud mistahes teave, arvamused või muu Teenuste osutamise tulem on mõeldud Kliendi poolt kasutamiseks. Lepingu täitmise käigus loodud autoriõigusega kaitstavad teosed lähevad üle tellijale (MKM-le) peale üleandmise-vastuvõtmise akti allkirjastamist tellija ja töövõtja poolt. Autori isiklike õiguste osas, mis on oma olemuselt üleantavad, annab töövõtja tellijale tagasivõtmatu ainulitsentsi, mis kehtib kogu autoriõiguste kehtivuse aja.

Vastavalt töövõtulepingu (nr 1.9-8/21-406-1) punktile nr 7.3 on tellijal pärast lepingu täitmise käigus loodud teose üleandmist õigus kasutada teost oma äranägemisel. Teose kasutamise viis ega territoorium ei ole piiratud. Teose muudatuste puhul peab olema selgelt aru saada, et nende autoriks ei ole töövõtja. Kui see ei ole selge, peab tellija töövõtjat eelnevalt teavitama ning andma töövõtjale võimaluse nõuda oma nime eemaldamist töö tulemitelt.

Lugupidamisega

Tarmo Toiger
Partner
KPMG Baltics OÜ



Põhimõisted ja lühendid

Käesolevas raportis kasutatavad põhimõisted ja lühendid:

Lühend	Selgitus
EHS	Elektroonilise hääletamise süsteem
E-hääletamine	Elektrooniline hääletamine elektroonilise seadme vahendusel
Hääletaja	Isik, kes kasutab elektroonilise hääletamise süsteemi hääletamisetapil
i-hääletamine	Terminit „i-hääletus“ kasutatakse antud dokumendis elektroonilise hääletuse (e-hääletus) sünonüümina, termin tuleneb ingliskeelsest väljendist internet voting
Koguja	Isik, kes haldab Kogumisteenust, Valijarakendust ja Kontrollrakendust.
Kogumisteenus	Serverisüsteem, mis tuvastab hääleõiguslikkust Tuvastusteenuse abil, väljastab kandidaatide nimekirja, aitab Valijarakendusel Allkirjastamisteenuse abil e-häält moodustada, talletab hääli e-valimiskasti ning registreerib neid Registreerimisteenuses. Kogumisteenus vastab Kontrollrakenduse poolt tehtud hääle tervikluse kontrollpäringutele.
Kontrollrakendus	Võimaldab valijal kontrollida oma häält Eesti Vabariigi valimistel. Hääle kontrollimine võimaldab saada senisest enam teavet hääletamiseks kasutatava arvuti turvalisuse kohta. Kui arvuti on nakatunud pahavaraga, mis e-hääletaja e-häält muudab või blokeerib, siis kontrollimine võimaldab sellise olukorra tuvastada.
Lugeja	Genereerib võtmepaari e-hääle salastamiseks ja avamiseks.
Lugemistõend	Näitab, et avakujul olev hääli ja krüptogramm on omavahel seoses, lähtudes seejuures avalikust võtmest
MKM	Majandus- ja Kommunikatsiooniministeerium
MVP	Minimaalne töötav toode (Minimum Viable Product)
POC	Kontseptsiooni tõendus (Proof of Concept)
Registreerimisteenus	Teenus, mille abil Kogumisteenus peab registreerima kõik Valijarakendustelt saadud hääled. Pärast hääletamisperioodi lõppu edastab teenuseosutaja info registreeritud hääle kohta Töötlejale.
RIA	Riigi Infosüsteemi Amet
RVT	Riigi valimisteenistus
SMIT	Siseministeeriumi infotehnoloogia- ja arenduskeskus
Töötlemisrakendus	Töötlemisrakendus kontrollib iga üksikut häält eraldi, veendudes muuhulgas, et iga kogumisteenuse ning registreerimisteenuse poolt esitatud vaated e-valimiskasti sisu
Töötleja	Isik, kes kasutades Töötlemisrakendust töötleb töötlustapil hääletamisperioodil kogutud e-hääli.
Valijarakendus	Rakendus, mida Hääletaja kasutab e-hääle andmiseks valimistel. Valijarakendus suhtleb Kogumisteenusega ning võimaldab Hääletajal teha valikut, seda krüpteerida ja digitaalselt allkirjastada. Valijarakendus kuvab QR-koodi, mille alusel saab Hääletaja Kontrollrakendusega kontrollida e-hääle korrektset jõudmist Kogumisteenusesse.
VIS3	Valimiste infosüsteem võimaldab registreerida kandidaate, teha kindlaks valimistulemused ja hääletamisest osavõtu ning jagada seda infot avalikkusega
VVK	Vabariigi Valimiskomisjon
Võtmerakendus	On Korraldaja põhitööriist, millega genereeritakse iga hääletamise jaoks hääle salastamise ja hääle avamise võti. Võtmerakenduse abil toimub ka hääle (krüptogrammide) avamine.

Sisukord

1	Koondarvamus	5
2	E-valimiste protsessi kirjeldus	6
2.1	Põhiprotsessid	6
2.2	Võtmehaldus	6
2.3	Hääletaja tuvastamine	6
2.4	Hääle allkirjastamine	6
2.5	Hääle registreerimine	6
2.6	Hääletamine ja hääle kontrollimine	7
2.7	Häälte töötlemine	7
2.8	Häälte kokkulugemine	7
3	Eesmärk ja protseduurid	8
3.1	Metoodika	9
3.1.1	Standardid ja õigusaktid	9
3.1.2	Riskide hindamise metoodika	11
4	Eelnevate auditaruannete analüüs	13
4.1	E-valimiste turvalisuse tööühma koondaruande hetkehinnang	13
4.2	Recommendation CM/Rec(2017)5[1] of the Committee of Ministers to member States on standards for e-voting	16
4.3	OSCE/ODIHR-i valimiste hindamise missiooni aruanne 2011	16
5	Tähelepanekud	17
	Tähelepanek 1 – Puudulik turvatestimise protsessi kirjeldus arendustsüklis	17
	Tähelepanek 2 – VIS3 infosüsteemi seansihalduse sessiooni pikkus ei ole kooskõlas parimate praktikatega	18
	Tähelepanek 3 – Puudused riskianalüüside läbiviimisel	18
	Tähelepanek 4 – RVT ja RIA vastutusalad ei ole selgelt piiritletud	19
	Tähelepanek 5 – Jätkusuutliku arendamise puudumine	20
	Tähelepanek 6 – Mittetäielik testimine enne valimisi	21
	Tähelepanek 7 – Vaatlemise protsessi ebatäpsused	22
	Tähelepanek 8 – Ebapiisav kommunikatsioon enne valimisi	22
	Tähelepanek 9 – Valimiste veebilehe informatsioon on aegunud	23
	Tähelepanek 10 – Dokumentatsiooni puudused	24
	Tähelepanek 11 – Volitusnormi puudumine õigusaktides	24
	Tähelepanek 12 – Õigusaktide ebatäpsused	25
	Tähelepanek 13 – Valijarakenduse veateade ei viita õigele lehele	26
	Tähelepanek 14 – Kasutajat ei verifitseerita kontrollrakenduses	26
6	Kokkuvõte	28
	Lisa 1 - Edastatud dokumentatsioon	29

1 Koondarvamus

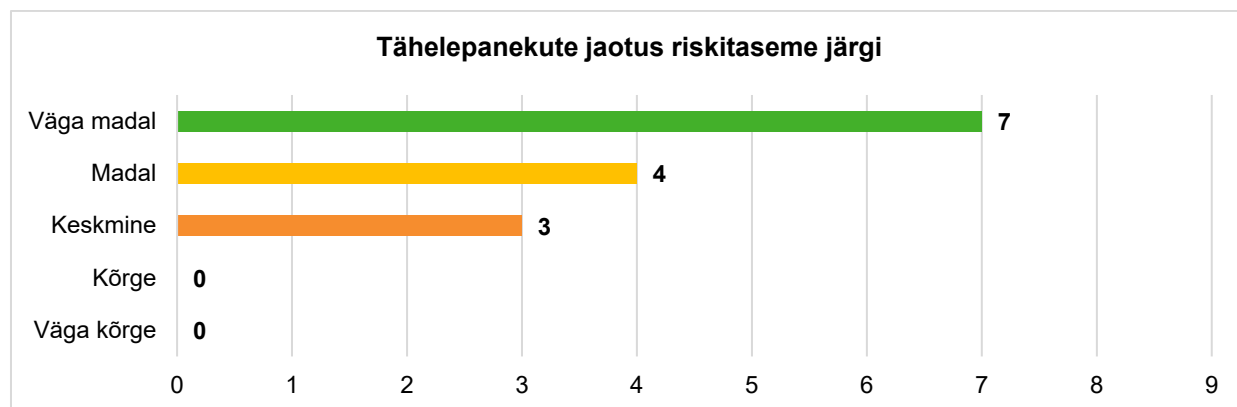
Valimiste infosüsteemide ja nendega seotud protsesside turvalisuse tervikliku auditeerimise käigus oleme hinnanud valimiste infosüsteemide ja nendega seotud protsesside turvalisust.

Valimiste infosüsteemide ja nendega seotud protsesside turvalisuse auditeerimise käigus viisime läbi intervjuud Majandus- ja Kommunikatsiooniministeeriumi (MKM), Riigi Valimisteenistuse (RVT), Riigi Infosüsteemi Ameti (RIA) ja Siseministeeriumi infotehnoloogia- ja arenduskeskuse (SMIT) esindajatega.

Auditi käigus tutvusime RVT, RIA, SMIT-i ja MKM-i poolt edastatud dokumentatsiooniga sh elektroonilise hääletamise infosüsteemi (EHS) valijarakenduse, valimiste infosüsteemi (VIS3), Rahvastikuregistri ja selle kasutajatoe protsessi ning loetletud osapoolte vahel sõlmitud omavaheliste kokkulepete dokumentatsiooniga.

Auditi käigus on audiitorid tuvastanud kokku 14 puudust ja mittevastavust, millest:

- **3 puudust on keskmise riskitasemega:** 1) puudulik turvatestimise protsessi kirjeldus arendustsükklis; 2) valimiste infosüsteemi seansihalduse sessiooni pikkus ei ole kooskõlas parimate praktikatega; 3) aegunud valijarakenduse riskianalüüs.
- **4 puudust on madala riskitasemega:** 4) RVT ja RIA vastutusalad ei ole selgelt piiritletud; 5) jätkusuutliku arendamise puudumine; 6) mittetäielik testimine enne valimisi; 7) vaatlemise protsessi ebatäpsused.
- **7 puudust on väga madala riskitasemega:** 8) ebapiisav kommunikatsioon valimistega seotud osapoolte vahel ning hiline tegevuste planeerimine; 9) valimiste veebilehe informatsioon on aegunud; 10) puudused protsesside dokumentatsioonis; 11) volitusnormi puudumine õigusaktides; 12) ebatäpsused õigusaktides; 13) valijarakenduse veateade ei viita õigele lehele; 14) kasutajat ei verifitseerita kontrollrakenduses.



Aruande 5. peatükis on välja toodud tähelepanekud koos soovistustega ning soovituslikud tähtajad puuduste kõrvaldamiseks.

Vastavalt audiitoritele edastatud informatsioonile ja meie poolt läbi viidud tööle, ei ole me tuvastanud kriitilise tähtsusega puuduseid või turvanõrkuseid valimiste infosüsteemides ega tööprotsessides. Oleksime saanud teistsugust või täiendavat teavet, oleksime võinud tõstatada teistsuguseid tähelepanekuid.

2 E-valimiste protsessi kirjeldus

2.1 Põhiprotsessid

Käesolevas peatükis kirjeldatakse süsteemi osapoolte tegevust, mille käigus selguvad süsteemi komponentide üldine funktsionaalsus ja välistele osapooltele esitatavad üldnõuded.

2.2 Võtmehaldus

Võtmehalduse protseduurid ja kasutatav turvaskeem on e-hääletamise süsteemi üks kriitilisemaid kohti, millest sõltub valimiste põhinõuete – hääletamise salajasus ja korrektsus, hääletaja sõltumatus – täitmine. Salajasus tagatakse asümmeetrilise krüptograafia vahendite abil häälte krüpteerimisega. Igaks hääletamiseks luuakse Võtmerakenduse abil süsteemi võtmepaar – häälte salastamise võti (avalik võti) ja häälte avamise võti (privaatvõti).

Võtmepaari genereerimist ja avamisvõtme kasutamist korraldavad mitu võtmehaldurit koos. Häälte avamise võtme aktiveerimine on võimalik ainult siis, kui kohal on eelnevalt kokkulepitud hulk võtmehaldureid. Võtmehalduritele antakse häälte avamise võtme aktiveerimiseks füüsilised ja teadmuslikud võtmeosakud.

2.3 Hääletaja tuvastamine

Hääletaja tuvastamine Koguja poolt on vajalik hääleõiguse esmaseks kontrolliks ning ringkonna kandidaatide nimekirja saamiseks. Hääletaja tuvastamine toimub ID-kaardi või Mobiil-ID abil.

2.4 Hääle allkirjastamine

Hääletaja allkirjastab krüpteeritud hääle, et tagada selle autentsus ja terviklus. Digitaalallkirjast tulenev isikudentiteet on aluseks e-hääle arvesse võtmisel. See tähendab, et Hääletaja tuvastamisel on elektrooniline autentimisvahend tavaliselt ühitatud allkirjastamisvahendiga samal kandjal (näiteks: ID-kaart). Otstarbekus avaldub sellisel juhul sama kandja kasutamises mõlemaks otstarbeks. Saadud identiteeti ei arvestata digiallkirjastatud hääle edasisel käitlemisel. Hääletaja kasutab digiallkirja andmiseks allkirja andmise vahendit, mis on kombinatsioon füüsilisest (näiteks kiipkaart, SIM-kaart) ja teadmuslikust (PIN) osast.

2.5 Hääle registreerimine

Registreerimisteenus on sõltumatu osapool, mis registreerib ning kinnitab iga Kogumisteenuse poolt edastatud krüpteeritud ja allkirjastatud hääle (selle sõnumilühendi) – toodab ajamärgendi koos omalt poolt lisatud ajaga. Registreerimisteenus identifitseerib turvaliselt kõik Koguja päringud. Hääletamise lõppedes annab Registreerimisteenus kõik ajamärgendid üle Töötlejale.

2.6 Hääletamine ja hääle kontrollimine

Valija kasutab hääletamiseks arvutisse paigaldatud Valijarakendust, mis suhtleb Kogumisteenusega. Kogumisteenus kasutab oma töös valijate nimekirja, kandidaatide nimekirja ning jaoskondade ja ringkondade nimekirja. Kogumisteenus registreerib digitaalselt allkirjastatud hääle Registreerimisteenuses. Valijarakendus teavitab Valijat hääle õnnestunud talletamisest, väljastades asjakohase QR-koodi.

Hääle kontrollimiseks kasutab Valija nutiseadmesse laetud Kontrollrakendust, mis suhtleb samuti Kogumisteenusega. Kontrollrakendus saab oma tööks vajalikud andmed Valijarakendusest, lugedes QR-koodi nutiseadme kaamera abil. Seejärel Kontrollrakendus kuvab Valijale tema valitud hääle tulemuse.

Hääletamine toimub kahes faasis – tuvastamis- ja hääletamisfaasis.

2.7 Häälte töötlemine

Häälte töötlemine toimub pärast hääletamisperioodi lõppu ja enne kokkulugemist. Töötlemise etappe viib läbi Töötleja. Töötleja allkirjastab kõikide etappide tulemid. Häälte töötlemine toimub andmesidevõrgust lahti ühendatud keskkonnas.

Häälte töötlemine toimub 5 etapis:

- 1) e-urni tervikluse kontroll;
- 2) korduvate e-häälte tühistamine;
- 3) topelthääletanute häälte tühistamine (ainult paralleelhääletamise korral);
- 4) e-häälte anonüümistamine;
- 5) miksimine (krüptograafiline segamine).

2.8 Häälte kokkulugemine

Häälte avamine ja kokkulugemine toimub andmesidevõrgust lahti ühendatud keskkonnas, kasutades Võtmerakendust. Kokkulugemist korraldab Lugeja koos võtmehalduritega, kelle vahel on jagatud häälte avamise võti.

Lugemistööend võimaldab Auditirakenduse abil kontrollida protsessi matemaatilist korrektsust. Juhul, kui lugemisele läinud hääled olid miksitud (krüptograafiliselt segatud), saab kokkulugemise korrektsust kontrollida ka avalikult. Lugeja allkirjastab kokkulugemise tulemused digitaalselt.

3 Eesmärk ja protseduurid

Töö eesmärk:	Auditi eesmärk on Eesti valimiste protsesside ning valimiste komponentide turvalisuse hindamine. Auditi eesmärgiks on saada rahvusvaheliselt tunnustatud audiitorite ja spetsialistide: ▪ põhjendatud hinnang valimiste protsesside ja nendega seotud infosüsteemide turvalisusele; ▪ parandusettepanekud turvalisuse tõstmiseks.
Töö teostamise periood:	Oktoober 2021 - Aprill 2022
Töö läbiviija(d):	▪ KPMG Baltics OÜ: Ivar Anton (CISA); Andris Männik; Jaan Vahtre (CISSP, CISM, MTCNA, Sophos Certified Engineer); Jaan Sõmer (FortinetNSE4: Network Security Professional, Microsoft Certified Professional, Microsoft Certified: Azure Fundamentals). ▪ KPMG Law Estonia: Urmas Kukk (CIPP/E). ▪ KPMG Finland OY: Olli Knuuti; Pasi Vänttinen.
Töö ulatus:	Valimiste infosüsteemide ja nendega seotud protsesside turvalisuse terviklik auditeerimine. Auditi ulatuses on Eestis kasutatavad valimiste komponendid: a) kehtivad valimiste infosüsteeme käsitlevad seadusandlikud aktid; b) valimiste infosüsteemid, sh Sertifitseerimiskeskus ja rahvastikuregister; c) valimiste infosüsteemidega seotud protsessid. Hindamisel võetakse aluseks olemasoleva dokumentatsiooni asjakohasus ja piisavus ning 2021. aasta kohaliku omavalituse volikogude valimistel reaalselt rakendatud infoturbe meetmed.

Viisime oma auditi läbi asjatundlikult ja nõuetekohase professionaalse hoolega. Audit annab mõistliku kindluse auditeeritava protseduuride tõhususe kohta, võttes arvesse auditi riski, et isegi suhteliselt olulised eeskirjade eiramised ja rikkumised võivad jääda avastamata. Eeldasime, et meile edastatud teave ei olnud vale ega eksitav. Oleksime saanud teistsugust või täiendavat teavet, oleksime võinud tõstatada teistsuguseid tähelepanekuid.

3.1 Metoodika

Töö teostamise käigus viisime läbi intervjuud RVT, RIA, SMIT-i ja MKM-i esindajatega. Valimiste infosüsteemide ja nendega seotud protsesside turvalisuse tervikliku auditeerimise teostamisel lähtusime hinnangu andmisel meile teatavaks tehtud ja kasutamiseks võimaldatud teabest.

Töö käigus osapooltelt saadud ning audiitorite poolt analüüsitud dokumentide loetelu on välja toodud käesolevas aruandes **Lisa 1**.

Valimiste infosüsteemide ja nendega seotud protsesside turvalisuse tervikliku auditeerimise käigus andsid meile informatsiooni (intervjuude või teiste suhtluskanalite kaudu) järgmised isikud:

- | | |
|---|---|
| 1) Raul Rikk - riikliku küberturvalisuse juht (MKM) | 8) Alo Einla - valimiste infosüsteemide arenduse osakonnajuhataja (RIA) |
| 2) Martin Sepp - küberriskide halduse juht (MKM) | 9) Tarmo Hanga - riigi infosüsteemi teenistuse peaarhitekt (RIA) |
| 3) Raavo Palu - küberturvalisuse õigusnõunik (MKM) | 10) Priit Parmakson - tehnoloogia osakonna vanemarhitekt (RIA) |
| 4) Oliver Grauberg - küberturvalisuse õigusnõunik (MKM) | 11) Arne Koitmäe - riigi valimisteenistuse juht (RVT) |
| 5) Kristel Neier - valimiste tooteomanik (SMIT) | 12) Indrek Leesi - riigi valimisteenistuse nõunik (RVT) |
| 6) Kairit Pabstel - meeskonnajuht (SMIT) | |
| 7) Mairis Kungla - rahvastiku toimingute osakond, osakonnajuhataja asetäitja (SMIT) | |

3.1.1 Standardid ja õigusaktid

Valimiste infosüsteemide ja nendega seotud protsesside turvalisuse auditi teostamisel tugineti järgmistele standarditele, õigusaktidele ja suunistele:

- 1) ISO/IEC 27001:2013 - Information security management
- 2) ISO/IEC 27005:2018 - Information security risk management
- 3) Infosüsteemide turvameetmete süsteem ISKE <https://www.ria.ee/et/kuberturvalisus/iske/juhendid-ja-materjalid.html>
- 4) Recommendation CM/Rec(2017)5[1] of the Committee of Ministers to member States on standards for e-voting
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680726f6f>
- 5) OSCE/ODIHR-i valimiste hindamise missiooni aruanne 2011
<https://www.osce.org/files/f/documents/7/3/165836.pdf>
- 6) e-valimiste tööühma koondaruanne 12.12.2019 <https://mkm.ee/digiriik-ja-uhenduvus/kuberturvalisus/valimiste-kuberturvalisus>
- 7) Isikut tõendavate dokumentide seadus (peatükk 5¹ reguleerib digitaalset isikutunnistust, mida kasutatakse valija tuvastamiseks) <https://www.riigiteataja.ee/akt/115102021003?leiaKehtiv>;
- 8) RIA põhimäärus (§ 8 lg 3 p 1 tõttu) – <https://www.riigiteataja.ee/akt/128092021003?leiaKehtiv>
- 9) Riigikogu kantselei põhimäärus (viimati kinnitatud 22.02.2018; peatükk VII² reguleerib RVT-d)
<https://www.riigikogu.ee/wpcms/wp-content/uploads/2014/11/Riigikogu-Kantselei-p%C3%B5him%C3%A4%C3%A4rus-2.pdf>
- 10) RVT põhimäärus (kinnitatud 22.12.2016) - <https://www.riigikogu.ee/wpcms/wp-content/uploads/2014/11/Riigi-valimisteenistuse-p%C3%B5him%C3%A4%C3%A4rus-1.pdf>
- 11) VVK 08.10.2018 otsus nr 57 „Hääletamissedeli ja elektroonilise hääle vormi kehtestamine Riigikogu valimisteks“ - <https://www.riigiteataja.ee/akt/310102018001>
- 12) VVK 08.10.2018 otsus nr 59 „Hääletamissedeli ja elektroonilise hääle vormi kehtestamine Euroopa Parlamendi valimisteks“ - <https://www.riigiteataja.ee/akt/310102018002>
- 13) VVK 03.12.2020 otsus nr 2 „Vabariigi Valimiskomisjoni töökord“
<https://www.riigiteataja.ee/akt/308122020008>

- 14) VVK 25.01.2021 otsus nr 3 „Tehnilised nõuded elektroonilise hääletamise üldpõhimõtete tagamiseks“ <https://www.riigiteataja.ee/akt/327012021006>
- 15) VVK 03.02.2021 otsus nr 4 „Elektroonilise hääletamise organisatsiooni kirjeldus“ <https://www.riigiteataja.ee/akt/305022021001>
- 16) VVK 05.03.2021 otsus nr 6 „Hääletamissedeli ja elektroonilise hääle vormi kehtestamine kohaliku omavalitsuse volikogu valimisteks“ - <https://www.riigiteataja.ee/akt/309032021010>
- 17) RVT 08.10.2021 käskkiri nr 12-8/21-12 „Elektroonilise hääletamise protokollistiku ja süsteemi tehniliste juhendite kinnitamine“ <https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/3e26aadf-361c-41f9-8678-2a903efeb282>
- 18) RVT 04.09.2021 käskkiri nr 12-8/21-6 „Elektroonilise hääletamise süsteemi testimise ajakava ja ulatus 2021. a kohaliku omavalitsuse volikogu valimistel“ <https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/4f31b350-ca01-4523-ab66-660932b26c10>
- 19) RVT 04.09.2021 käskkiri nr 12-8/21-5 „Elektrooniliselt antud hääle lugemise juures viibivate riigi valimisteenistuse esindajate määramine ning elektrooniliste hääle avamise võtme ligipääsuvahendite jaotamine riigi valimisteenistuse esindajate vahel“ <https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/8f08e295-8d97-4ff7-959e-b8a908b8cf9a>
- 20) RVT 04.09.2021 käskkiri nr 12-8/21-4 „Elektrooniliste hääle salastamiseks kasutatava krüptoalgoritmi määramine 2021. a kohaliku omavalitsuse volikogu valimistel“ <https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/7cf162ec-798b-4cbe-98c4-e114db7f1f0f>
- 21) RVT 04.09.2021 käskkiri nr 12-8/21-3 „Elektroonilise hääletamise rakkerühma liikmete nimetamine 2021. a kohaliku omavalitsuse volikogu valimisteks“ <https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/3e30e57e-e293-46e8-a835-72799bc7d0fb>
- 22) RVT 04.09.2021 käskkiri nr 12-8/21-1 „Hääletamise korraldamise ja valimistulemuste kindlakstegemise juhendi kinnitamine kohaliku omavalitsuse volikogu valimisteks 2021. aastal“ - <https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/b2021b6f-cc4b-4bf5-8c1d-da936a9bbdcd>
- 23) RVT 29.05.2019 käskkiri nr 12-8/19-20 „Elektroonilise hääletamise käsiraamatu kinnitamine“ <https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/ca4bcef2-786e-451e-a681-f2d5debd6818>
- 24) RVT 21.01.2019 käskkiri nr 12-8/19-8 „Elektroonilist hääletamist takistavate juhtumite ehk intsidentide haldamise põhimõtted“ <https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/5c0ba67d-59ef-4c44-8f88-187b9e0061c8>
- 25) RVT 29.05.2017 käskkiri nr 12-8/17-3 "Elektroonilise hääletamise üldraamistik ja selle kasutamine Eesti riiklikel valimistel“ <https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/cbe7bdc8-61f1-4d0e-84e6-2ec61bc64656>

3.1.2 Riskide hindamise metoodika

Auditi käigus tuvastatud infoturvariskide määratlemisel lähtusime infoturvariski standardist ISO/IEC 27005:2018 ning tuginesime KPMG audiitorite varasemale töökogemusele. All olevates tabelites on välja toodud auditi käigus kasutatud riski hindamise metoodika.

Riskiklassid koos kirjeldustega

Riskiklass	Kirjeldus
Väga kõrge (20-25)	Nõuab kohest reageerimist. Lubamatu risk. Kui risk on hinnatud väga kõrgeks, vajab see viivitamatut ja ennetavate ning tagajärgi leevendavate meetmete planeerimist ja rakendamist.
Kõrge (15-16)	Tegevused esimesel võimalusel. Oluline risk. Riski vähendamine on vajalik esimesel võimalusel. Tuleb koostada riski vähendamise meetmete kava ning see rakendada kiireloomuliste tegevuste kompleksina.
Keskmine (9-12)	Meetmete rakendamine planeeritakse. Soovimatu risk. Vajalik kaaluda meetmete rakendamist riski vähendamiseks. Tuleb koostada kava ning seada tegevustele prioriteedid. Meetmed on vajalik rakendada mõistliku aja jooksul.
Madal (5-8)	Võetakse teadmiseks. Talutav risk. Riski teadvustatakse, kuid selle edasiseks vähendamiseks ei pruugita rakendada täiendavaid meetmeid. Tuleb kaaluda vajadust rakendada riski ennetavaid ja/või tagajärgi leevendavaid turvameetmeid ning hinnata, kas meetmete rakendamine on kasumlikum kui riski aktsepteerimine.
Väga madal (1-4)	Aktsepteeritakse. Tühine risk. Turvameetmete rakendamine ei ole kohustuslik, kuid riski tuleb jälgida ja regulaarselt hinnata.

Riskimaatriks ja riskiklassi kirjeldus

		MÕJU (IMPACT)				
		Vähetähtis 1	Kerge 2	Raske 3	Väga raske 4	Katastroofiline 5
TÖENÄOSUS (PROBABILITY)	(Peaaegu) kindel 5					
	Tõenäoline 4					
	Võimalik 3					
	Vähetõenäoline 2					
	Väga harv 1					

Riski tõenäosuse skaala

Tõenäosus	Skaala	Aeg	Kirjeldus
(Peaaegu) kindel	5	kuu	Riski avaldumine lähitulevikus on kindel
Tõenäoline	4	6 kuud	Riski avaldumine lähitulevikus on tõenäoline
Võimalik	3	aasta	On tõenäoline, et see riskistsenaarium millalgi realiseerub
Vähetõenäoline	2	5 aastat	Selliste riskide realiseerumine on üldjuhul väga harv, aga on võimalik, et mingil hetkel tulevikus see realiseerub
Väga harv	1	10+ aastat	Teoreetiliselt võimalik, aga suure tõenäosusega ei realiseeru see riskistsenaarium kunagi

Riski mõju skaala

Mõju	Skaala	Kirjeldus
Katastroofiline	5	• kaasnevad katastroofilised (missioonikriitilised) kahjud; • ohu realiseerumine (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab teenuse pikaajase katkemise või seab ohtu e-valimiste läbiviimise või tekitab katastroofilisi tagajärgi keskkonnale või kriitilisi rahalisi kaotusi; • äärmiselt vaenulik avalikkuse ja meedia tähelepanu, mis kestab püsivalt kuude kaupa ning põhjustab valijate loobumise e-valimiste teenuse kasutamisest; • võivad tekkida pikaajased katkestused e-valimiste infosüsteemi töös või vahetu oht säärase olukorra tekkeks; • e-valimiste läbiviimine on häiritud 80–100% ulatuses.
Väga raske	4	• kaasnevad olulised kahjud; • ohu realiseerumine (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab e-valimiste infosüsteemi töös olulise katkemise või keskkonnasaastet või väga olulisi rahalisi kaotusi; • märkimisväärne negatiivne avalikkuse tähelepanu, mis kestab nädalaid ning võib esile kutsuda valijate loobumise teenuse kasutamisest; • e-valimistega seotud teiste infosüsteemide töö on oluliselt häiritud või on vahetu oht säärase olukorra tekkeks; • e-valimiste läbiviimine on häiritud 50–80% ulatuses.
Raske	3	• kaasnevad keskmised kahjud; • ohu realiseerumine (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) võib põhjustada katkestuse e-valimiste infosüsteemi töös, toimepidevuse töös või keskkonnale või olulisi rahalisi kaotusi; • negatiivne tähelepanu, mis kestab päevi ning mis võib hiljem korduda; • häiritud võib olla teiste e-valimistega seotud infosüsteemide töö või on vahetu oht säärase olukorra tekkeks; • e-valimiste läbiviimine on häiritud 30–50% ulatuses.
Kerge	2	• kaasnevad väheolulised kahjud; • ohu realiseerumine (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt märkimisväärseid takistusi e-valimiste funktsiooni täitmisele või märkimisväärseid rahalisi kaotusi; • negatiivne tähelepanu, mis on ajaliselt piiratud ühe päevaga; • e-valimiste läbiviimine võib olla häiritud 10–30% ulatuses.
Vähetähtis	1	• ei kaasne märkimisväärseid kahjusid või kahjud puuduvad; • ohu realiseerumine (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) ei põhjusta olulisi takistusi organisatsiooni funktsiooni täitmisele; • põgus negatiivne tähelepanu, mis väljendub mõnes meediasõnumis.

4 Eelnevate auditiaruannete analüüs

4.1 E-valimiste turvalisuse tööühma koondaruande hetkehinnang

Oma auditi käigus tutvusime ka E-valimiste turvalisuse tööühma koondaruande¹ soovitusetega ning viisime läbi intervjuud koondaruandes välja toodud punktide eest vastutavate osapooltega (asutustega). Käesolevas punktis anname audiitorite hinnangu koondaruandes välja toodud 25 tähelepaneku hetkeolukorrale. Oma hinnangu andmisel oleme lähtunud intervjuude käigus saadud informatsioonist ning audiitoritele edastatud dokumentatsioonist.

Nr.	Tähelepanek	Hetkeolukorra hinnang
1	Tagada süsteemi hoolduse ja arenduse jaoks piisav ja jätkusuutlik rahastamine	Protsessiauditi käigus erinevatelt osapooltelt kogutud informatsiooni ja tõendite põhjal saame väita, et hetkel ei ole tagatud süsteemi hoolduse ja arendamise jaoks piisav ning jätkusuutlik rahastamine. Vabariigi Valitsus ei ole eraldanud valimiste süsteemi hoolduse ja arendamise jaoks piisavalt ressursse, mis võimaldaks jätkusuutlikku arendamist pikemas vaates. Valimiste perioodiks (passiivne periood 6 kuud enne valimispäeva ja aktiivne periood valimiste ajal) raha eraldamine testimiste ja arenduste läbiviimiseks ei ole jätkusuutlikku arengut võimaldav lahendus. Lisaks eelnevale on oluline, et RIA ja RVT ülesanded oleksid valimisi reguleerivates seadustes selgelt ja üheselt mõistetavalt piiritletud.
2	Parandada süsteemi arusaadavust vaatlejatele ja avalikkusele	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et hetkel on ajakohastatud ainult osa dokumentatsioonist, teavitusmaterjalidest ja alamlehekülgedest, mis puudutavad e-valimiste infosüsteemi ja veebilehte (www.valimised.ee). Informatsioon valimiste veebilehel pärineb kohati 2017. aastast kui mitte isegi varasemast ajast. Lisandunud on mõned videod ja selgitused, kuid audiitorite hinnangul vajaks kogu veebilehel olev informatsioon huvigruppe arvestades täiendavat läbitöötamist ja selgitusmaterjalide paremat visualiseerimist. Ühe konkreetse näitena saame välja tuua valijarakenduse kontrollimise juhendi, mis ei ole tavakasutaja vaatest selgelt mõistetav ja arusaadav.
3	Selgitada avalikkusele e-valimiste süsteemi arendamisel tehtud valikuid	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et hetkel on loodud selgitavad materjalid veebilehele www.valimised.ee selgitamaks hääletamisprotsessi kui tervikut ning selle juurde kuuluvaid komponente. Kokkuvõtlikku süsteemi disaini valikuid detailselt põhjendavat dokumentatsiooni ei ole koostatud.
4	Suurendada e-valimiste turvalisuse tagamisega seotud inimeste arvu	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et e-valimiste turvalisuse tagamisega seotud inimeste arvu ei ole märgatavalt tõstetud. Peamine aspekt, mille tõttu inimressurssi ei ole suurendatud, taandub rahalise ressursi eraldamisele. Vabariigi Valitsus ei ole võimaldanud e-valimiste jätkusuutlikuks arendamiseks rahalist ressursi, mis tagaks ka inimressursi suurendamise võimekuse. Akadeemiliste organisatsioonidega tehakse koostööd teaduslikus vaates.

¹<https://mkm.ee/digiriik-ja-uhendus/kuberturvalisus/valimiste-kuberturvalisus>

5	Suurendada e-valimiste sõltumatu kontrolliga tegelevate audiitorite arvu	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et e-valimiste kontrolliga tegelevate sõltumatute audiitorite arvu ei ole suurendatud põhjusel, et täiendavate audiitorite lisamisest tulenev lisandväärtus valimisi läbiviivate organsatsioonide hinnangul on marginaalne.
6	Suurendada pädevate vaatlejate arvu	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et vaatlemine on vabatahtlik tegevus ning et vaatlejate arvu suurendamine sõltub huvigruppidest ja isikutest endist. Vaatlejate jaotamine akrediteeritud ja tavavaatlejateks ei ole toetust leidnud, kuna kõik vaatlejad on seni saanud osaleda koolitusel, mille käigus tutvustatakse süsteemi ülesehitust ning räägitakse valimiste protsessidest. 2021. aasta valimiste käigus rakendati tagasiside küsimise punkti, mis on toodud välja e-valimiste tööühma aruandes. Auditi läbiviimise lõppfaasiks ei olnud vaatlejatelt tagasisidet RVT-le edastatud. Eraldi kokkuleppeid erasektori ja ajakirjanduse ning rahvusvaheliste vaatlejate kaasamiseks ei ole sõlmitud.
7	Tõsta krüptosüsteemide jätkusuutlikkuse tagamise võimekust	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et teadaolevalt ei ole MKM ega ka Haridus- ja Teadusministeerium toetanud ideed teaduse võimekuse tõstmiseks krüptograafia vallas. MKM nägemus on, et krüptograafia kasutamine on igakordse teenuse kasutamise otsus ning riik ei ole seotud konkreetse valdkonna arendamise tagamisega.
8	Kasutada dubleeritud erinevaid tarkvarakomponente häälte kokkulugemise protsessis	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et RVT ja RIA ei ole näinud vajadust viia läbi põhjalik analüüs dubleeriva tarkvara loomiseks koos kaasnevate kulude kalkulatsiooniga kuna olemasolev süsteem on RVT hinnangul piisavalt hea ning täidab oma funktsiooni. Alternatiivse tarkvara loomise kulud on kaudselt hinnatud ning antud kulud oleksid samas suurusjärgus olemasoleva süsteemi arenduskuludega. Seetõttu ei ole alternatiivse tarkvara loomine rahaliselt põhjendatud. RVT-le annab lisakindlust see, et tarkvarakomponendid, mida kasutatakse valimiste protsessi käigus, on dubleeritud erinevatesse asukohtadesse, mis tagab süsteemile kehtestatud käideldavusnõuded (õigel ajal kättesaadav ja kasutuskõlblik).
9	Vähendada valija arvuti ja arvutikasutuskusega seotud ohtusid	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et RVT ja RIA on lisanud tarkvara autentsuse tõendamise lisavõimaluse kui täiendava kaitsemeetme valijarakenduses. Arvutikasutajate ja valijate ohutu arvutikasutuse osas viib RIA koostöös teiste ametkondadega läbi järjepidevaid teadlikkuse tõstmise kampaaniaid.
10	Võimaldada mobiiliga hääletamist	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et analüüs, millele e-valimiste tööühma koondaruandes viidatakse, on lõpetatud, analüüsi tulemitena on jätkatud töötamist, ning käivad pidevad arutelud leidmaks sobivaim ja turvalisim lahendus mobiiliga hääletamiseks.
11	Tagada e-hääletajale võimalus kontrollida oma hääle lugemisele jõudmist	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et RVT on arendanud funktsionaalsuse ning sellekohane juhend on leitav veebilehelt www.valimised.ee .
12	Viia läbi hääletamist reguleerivate õigusaktide revisjon	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et Justiitsministeerium tegeleb antud valdkonna õiguslike küsimustega ning valimisi reguleerivate seaduste täiendamisega.

13	Muuta i-hääle liikumine audiitoritele ja vaatlejatele kogu tsükli ulatuses vaadeldavaks (kogu protsessi vaadeldavus-kontrollitavus)	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et VVK on koostanud juhendid avalikkusele kui ka audiitoritele, mis selgitavad täpselt e-hääletamise protsessi ning hääle liikumist ja kontrollimist (https://www.valimised.ee/et/e-haaletamine).
14	Sätetada e-hääle andmekoosseis seadusega	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et Justiitsministeerium tegeleb antud valdkonna õiguslike küsimustega ning valimisi reguleerivate seaduste täiendamisega.
15	Reguleerida i-hääletamisega seotud andmete hävitamise protseduur senisest täpsemalt	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et RVT ja RIA on dokumenteerinud e-hääletuse majutuskeskkonna sulgemise, sealsete andmete kustutamise protseduuri, häälte hävitamise protseduuri, salajase võtme osakute loomise/hävitamise/haldamise protseduuri. Dokumentatsiooni on viimati uuendatud mais 2019, seega saame järeldada, et töörühmas käsitletud täpsustusi ja uuendusi ei ole sisse viidud.
16	Luua i-hääletuse logimist ja logide kasutamist reguleeriv protseduur	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et logide kättesaadavaks tegemise korda ei ole kinnitatud ega sätestatud. Küll on dokumenteeritud e-hääletuse logimise seadistused, logi tootva teenuse logimise korraldus ja logide kogumisteenuse korraldus.
17	Täiendada e-valimiste infosüsteemi tarkvara komponentide järelkontrollitavuse protseduuri	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et järelkontrollitavuse protseduuri rakendatakse kuni kohtuvaidluste protsessi ametliku lõppemiseni ning seejärel kustutatakse. Arhiveerimismeetodit ei rakendata, kuna selleks puudub täiendav vajadus.
18	Sätetada i-hääletusele hääletuskabiini puudumist kompenseerivad meetmed	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et eraldi juhendit ja täiendusi valijarakendusse sisse viidud ei ole, tagamaks privaatseid valimistoiminguid. Küll aga on e-hääletanul võimalik soovi korral muuta oma häält e-hääletamise jooksul ning ka valimispäeval valimisjaoskonnas hääletades. Kehtima jääb viimasena antud häält.
19	Pikendada i-hääletamise tõendusmaterjali säilitusaega	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et hetkel lähtutakse valimiste ühetaolisuse printsiibist, kehtivast seadusandlusest ning põhimõttest, et e-hääled hävitatakse samadel alustel paberhääletagega.
20	Rakendada i-häälte töötlemisel protokollimist	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et i-häälte töötlemisel on rakendatud protokollimist. Valimisi auditeerinud audiitorite tulemid on avalikustatud veebilehel www.valimised.ee .
21	Ühtlustada hääletusajad ja piirata hääle muutmisvõimalust	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et hääletusaegu on võrreldes 2019. aasta hääletamisega kohandatud, kuid kehtima on jäänud olemasolev protseduur. Teisisõnu on võimalik oma häält muuta valimispäeval valimisjaoskonnas hääletamisega.
22	Ühtlustada e-valimiste tulemuste teatavaks tegemise viis ja kiirus võrreldes pabervalimistega	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et protseduuri uuendus on ellu viidud ja rakendatud ning e-häälte teatavaks tegemise viis ja kiirus muutusid 2021. aasta valimistel.

23	Vähendada e-valimiste usalduse polariseeritust	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et e-valimiste tööühma koondaruandes välja toodud punktid on olnud arutlusel või võetud töösse ning sellest tulenevalt peaks suurenema ka usaldus e-valimiste vastu.
24	Võimaldada Smart-ID kasutamist	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et Smart-ID kasutamine valimistel on olnud arutlusel, kuid 2021. aasta valimistel otsustati antud lahendust mitte kasutusele võtta. Arutlused antud süsteemi kasutuselevõtuks 2023. aasta valimisteks on auditi ajal käimas ning lõppresultaadini jõutud ei ole.
25	Viia e-hääletus vastavusse käibivate otsast lõpuni kontrollitavuse nõuetega	Protsessiauditi käigus kogutud informatsiooni ja tõendite põhjal saame väita, et Justiitsministeerium tegeleb antud valdkonna õiguslike küsimuste ja valimisi reguleerivate seaduste täiendamisega.

4.2 Recommendation CM/Rec(2017)5[1] of the Committee of Ministers to member States on standards for e-voting

EU CM/Rec(2017)5[1] of the Committee of Ministers standardis² on välja toodud üldised suunised valimiste demokraatlikuks läbiviimiseks ning valimiste (sh tulemuste) ja kodanike valimisõiguste jälgimiseks ja tagamiseks.

Audiitorite hinnangul ei ole me tuvastanud olulisi vastuolusid EU Committee of Ministers standardis väljatoodud suuniste osas.

4.3 OSCE/ODIHR-i valimiste hindamise missiooni aruanne 2011

OSCE lähetas 2015. aastal demokraatlike institutsioonide ja inimõiguste büroo (OSCE/ODIHR) 15. veebruaril valimiste eksperdirühma (EET) vaatlema 1. märtsil toimunud Riigikogu valimisi. OSCE/ODIHREET keskendus vaid teatud valimistega seotud aspektidele – interneti teel hääletamisele, erakondade ja valimiskampaaniate rahastamisele ning rahvusvähemuste osalusele valimistel.

Audiitorite hinnangul on enamus antud aruandes³ välja toodud soovitusi valimiste infosüsteemides rakendatud. Valimiste infosüsteemid võimaldavad: 1. Kontrollida, kas valija poolt antud hääle on loetud samal kujul, kui see on valimiste infosüsteemi salvestatud. 2. *end-to-end* sertifitseerimine teostatakse sõltumatu asutuse poolt. 3. Valimiste käigus toimub demokraatlik vaatlusprotsess, kõik kes soovivad, võivad osaleda valimiste vaatluses, kui on end eelnevalt registreerinud. 4. **Erakondade Rahastamise Järelevalve Komisjon (edaspidi ERJK) volitusi ei ole aruande soovitude kohaselt rakendatud ning ERJK-l puuduvad selged volitused rikkumiste korral uuringute läbiviimiseks ning vajadusel trahvide väljastamiseks**⁴. 5. Audiitorite hinnangul ei ole aruandes välja toodud soovitus nr 5 täielikult rakendatud ning nõuab täiendavaid pingutusi. Aruande soovitus nr 5 „*Ametkonnad peaksid säilitama ja jätkama püüdlusi naturalisatsiooni korras kodakondsuse saamise stimuleerimiseks endiselt suure hulga määratlemata kodakondsusega isikute seas, eesmärgiga anda neile Riigikogu valimistel valimisõigus*“.

OSCE aruandes välja toodud muude soovitude osas on audiitorite hinnangul toimunud edasimineku, kuid käesolevas aruandes on välja toodud sarnased soovitud, mis hõlmavad valimiste infosüsteemide täiendavat edasiarendamist, et tagada e-hääletamise jätkuv turvalisus.

OSCE aruandes välja toodud soovitude osas ei ole audiitorite hinnangul hetkel riski e-hääletamise ja valimiste infosüsteemide turvalisusele.

² <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680726f6f>

³ <https://www.osce.org/files/f/documents/7/3/165836.pdf>

⁴ <https://www.erjk.ee/et/komisjon-ja-kontaktid/erakondade-rahastamise-jarelevalve-komisjoni-tookord>

5 Tähelepanekud

Antud peatükis on välja toodud auditi käigus tuvastatud tähelepanekud koos riskitasemetega, riskikirjeldustega, soovitud, vastutajate (mitme vastutaja korral on peavastutaja loetelus esimesena välja toodud osapool nt RVT/RIA puhul on peavastutajaks RVT) ja teostamise soovituslike tähtaegadega (lõplikud tähtajad määravad teemadega tegelevad osapooled).

Tähelepanek 1 – Puudulik turvatestimise protsessi kirjeldus arendustsükli

Keskmine	Tähelepanek 1: Turvatestimise nõue ei ole VIS3 ja EHS (sh valijarakendus) arenduse protsessis dokumenteeritud piisava täpsusega: ▪ VIS3 osas on välja toodud: „<i>turvatestimine viiakse läbi enne toodangu esmakordset avalikustamist või enne suuremate muudatuste reliis</i>“. Auditi läbiviimise käigus, ei ole tuvastatud, kuidas täpselt defineeritakse VIS3 infosüsteemis suuremat muudatust, millele tuleb tellida turvatestimine. ▪ EHS materjalides ning e-hääletamise infoturbe poliitikas ei ole kirjeldatud nõue turvatestide läbiviimiseks. Ei ole selgelt määratletud turvatestide läbiviimise ulatus (skoop), mis sagedusega turvatestide tuleb läbi viia, kes vastutab turvatestide läbiviimise ja leitud puuduste kõrvaldamise eest. Vastavalt ISO 27001:2017 standardi turvameetmete punktile A12.6 tuleb vältida tehniliste nõrkuste ärakasutamist ning ISO 27002:2017 standardi turvameetmete punkti A18.2 kohaselt tuleb läbi viia tehniliste nõrkuste testimine.
	Riskikirjeldus: VIS3 ja EHS puudulike turvatestimise läbiviimise protsesside kirjelduste tõttu võivad olulised turvanõrkused jääda õigeaegselt tuvastamata. Tuvastamata turvanõrkused võivad tulevikus kompromiteerida e-valimiste infosüsteeme ning seetõttu ei ole võimalik e-häält anda.
	Soovitus: Viia läbi regulaarseid nõrkuseanalüüse ja EHS-i (sh valijarakendus) turvatestimist. Antud nõue tuleks dokumenteerida EHS süsteemi nõudena. VIS3 ja EHS osas tuleks dokumenteerida turvatestide läbiviimise ulatus, sagedus ning vastutajad, kes korraldavad turvatestide läbiviimist ja tegelevad leitud puuduste kõrvaldamisega. VIS3 süsteemi dokumentatsioonis on soovitatav kirjeldada süsteemi mõistes definitsioon „suur muudatus“.
	Vastutaja(d): RVT/RIA
	Tähtaeg: 31.12.2022 (antud tähtaeg on eelduslik, lõplik tähtaeg selgub peale hanke läbiviimist, samas tuleb arvestada 2023 toimuvate Riigikogu valimistega)

Tähelepanek 2 – VIS3 infosüsteemi seansihalduse sessiooni pikkus ei ole kooskõlas parimate praktikatega

Keskmine	Tähelepanek 2: VIS3 süsteemi seansihalduse osas oleme tuvastanud mittevastavuse seansihalduse parimate praktikatega. RIA Confluence alamlehe Moodulid-> SEA (seansihaldur)⁵ kohaselt on VIS3 süsteemi maksimaalseks seansipikkuseks määratud 9h. Audiitorite hinnangul on nii pikk seansipikkus põhjendamatu ning tuleks üle hinnata, võttes arvesse parimaid praktikaid (<i>OWASP session timeout best practice - common idle timeouts ranges are 2-5 minutes for high-value applications and 15-30 minutes for low risk applications</i>) seansipikkuse osas. RIA kommentaar nii pika seansipikkuse osas oli, et vastav aeg on määratud, kuna valimiste süsteemi kasutava töötaja tööpäev on 9h.
	Riskikirjeldus: Pikk seansiaeg suurendab riski ja võimalust, et ründaja (pahatahtlik kasutaja) suudab tuvastada seansi identifikaatori (sessioon ID).
	Soovitus: VIS3 seansihalduse sessioon tuleks viia vastavusse parimate praktikatega, seansi sessioon ei tohiks olla pikem kui 30 minutit, mille järel peaks süsteemi kasutaja end uuesti autentima.
	Vastutaja(d): RVT/RIA
	Tähtaeg: 31.12.2022 (antud tähtaeg on eelduslik, samas tuleb arvestada 2023 toimuvate Riigikogu valimistega)

Tähelepanek 3 – Puudused riskianalüüside läbiviimisel

Keskmine	Tähelepanek 3: RIA-s viiakse läbi riskianalüüse vastavalt RIA-s rakendatud riskianalüüsi juhendile. Juhendi kohaselt on kohustuslik läbi viia riskianalüüs iga tähtsa infosüsteemi osas ja iga märkimisväärse muudatuse või arenduse puhul. RIA-s teostatakse organisatsiooniülest riskianalüüsi, mis hõlmab ka VIS3 süsteemi, aga parimate praktikate kohaselt tuleks kõrge riskiga infosüsteemi osas läbi viia spetsiifiline infosüsteemipõhine riskianalüüs. Audiitoritele võimaldati ligipääs ja võimalus kontrollida RIA Confluence arenduskeskkonnas⁶ spetsiifilist VIS3 süsteemi komponentidele tehtud riskianalüüsi, nt sedeliväljastuse, PostgreSQL ja OWASPTop10 osas, aga mainitud analüüside käigus ei ole hinnatud VIS3 süsteemi spetsiifilisi riske järgides parimaid praktikaid (nt ISO 27005⁷) riskianalüüsi läbiviimisel ning riskide kirjeldamise ja maandamise osas. EHS (sh valijarakendus) riskianalüüs on viimati RVT poolt läbi viidud 2017. aastal. Peale 2017. aastat ei ole EHSi (valijarakenduse) osas ohtu ja nõrkuseid uuesti hinnatud.
	Riskikirjeldus: Ilma põhjaliku riskianalüüsita ei võimalik tuvastada ega ennetada riske, mida vastava analüüsi läbiviimise käigus oleks võimalik tuvastada ning neile reageerida. Riskide mittekäsitlemine võib negatiivselt mõjutada e-valimisete läbiviimise protsesside ja süsteemide toimivust ning turvalisust.

⁵ <https://confluence.ria.ee/pages/viewpage.action?pageId=102469672>

⁶ <https://confluence.ria.ee/pages/viewpage.action?pageId=140117992>

⁷ <https://www.iso.org/standard/75281.html>

Soovitus: Tuleks läbi viia VIS3 ja EHS (sh valijarakendus) põhised riskianalüüsid, mis sisaldaksid infot riskide hindamise metoodika kohta, ülevaadet ohtudest ja turvanõrkustest koos riskihinnanguga ning riskide maandamise plaaniga. Riskianalüüsi tulemusena tuleks koostada riskiraport, mida tuleks esitleda süsteemi eest vastutavatele isikutele ja teistele vajalikele osapooltele. Riskide hindamise ja maandamistegevuste osas on soovitatav korraldada järelkontrolle (nt siseauditi raames või välise sõltumatu audiitori poolt) veendumaks, et tuvastatud riskid ning tegevuskava riskide maandamiseks on ajakohased ja tegevuskava jätkuvalt efektiivne.

Täiendavalt tuleks audiitorite hinnangul RVT-s juurutada riskianalüüsi läbiviimise kord ning RIA riskianalüüsi juhendit täiendada selliselt, mis sätestaks selged nõuded viia läbi valimiste infosüsteemide (VIS3 ja EHS) spetsiifilised riskianalüüsid. Mainitud infosüsteemide osas on soovitatav läbi viia riskianalüüsid esimesel võimalusel.

Täiendavalt tuleks riskianalüüsi dokumentatsiooni uuendada kord aastas tagamaks riskide ajakohasus (ohud muutuvad pidevalt) ning sobilikud leevendusmeetmed.

Vastutaja(d): RVT (teema vastutaja) / RIA (kaasatud osapool)

Tähtaeg: 31.01.2023 (antud tähtaeg on eelduslik, lõplik tähtaeg selgub peale hanke läbiviimist)

Tähelepanek 4 – RVT ja RIA vastutusalad ei ole selgelt piiritletud

Tähelepanek 4: Audiitorid tutvusid RVT ja RIA elektrooniliste valimiste rollijaotusega, mis on kehtiva õiguse alusel kehtestatud. Kuigi RIA põhimääruse kohaselt on RIA vastutusel valimiste infosüsteemide teenuse arendamine, haldamine, majutamine ning nende kasutamise koordineerimine, ei ole selleks RIA üldeelarves eraldatud jätkusuutlikku finantsressurssi, et tagada määruuses sätestatud kohustuste täitmine.

RVT põhimääruse kohaselt on RVT vastutusalas korraldada valimiste läbiviimiseks vajalike tehniliste lahenduste arendus ja haldus, kuid RVT-l puudub selleks vajalik arendusosakond. Vajalikud arendused tuleb tellida RIA-st, kes omakorda korraldab vajaliku arenduspartneri leidmise.

Audiitorite hinnangul on määrustega RVT-le ja RIA-le määratud kohustused, mida ei ole olemasoleva inimressursi ning eelarvega võimalik täita.

2019. aasta e-valimiste tööühma koondaruande⁸ ettepanek 1 on täpsustada RIA ja RVT ülesandeid. Auditi läbiviimise ajaks ei ole audiitorite hinnangul ning osapoolte (RIA ja RVT) kinnitusel valimisi reguleerivaid seadusi täpsustatud ega eespool mainitud asutuste ülesandeid ja vastutusalasid selgelt piiritletud.

Audiitoritele edastatud informatsiooni kohaselt on Justiitsministeeriumi juhtimise all käsil valimisi reguleerivate seaduste muutmise projekt, mille peamine eesmärk oleks RIA ja RVT rollijaotuse selgem kajastamine. Eelnõu esialgne mustand on koostatud, kuid töögrupis käivad veel arutelud eelnõu osas. Peamine muudatus oleks, et RIA roll oleks seaduses selgemalt kajastatud, mitte ei tuleneks pelgalt Vabariigi Valimiskomisjoni volitusnormide alusel tehtud otsustest. Peamine diskussioon seisneb RIA rolli osas.

Riskikirjeldus: Ebaselged vastutusalad osapoolte vahel võivad valimiste ettevalmistamise ja läbiviimise käigus takistusi tekitada, kuna puudub ühene arusaam rollide jaotuse ja vastutusalade osas.

⁸ <https://mkm.ee/digiriik-ja-uhendus/kuberturvalisus/valimiste-kuberturvalisus>

Soovitus: Piiritleda selgelt RIA ja RVT vastutusalad ja ülesanded, et erinevate asutuste vastutusalade piirid oleksid üheselt mõistetavad.

- Kindlaks määrata kellel on valimiste infosüsteemide kehtestamise pädevus, antud asutus peaks omama vastutust valimiste ja hääletamise (sh elektroonilise) organiseerimisel.

Soovituslik rollide jaotus oleks järgnev:

- MKM-i üldine vastutus valimiste infosüsteemide toimimise ja vajalike ressursside organiseerimise eest RVT-le ja RIA-le e-valimiste läbiviimiseks ning vajalikeks arendustöödeks, sh turvalisuse tagamiseks vajalikud kulud;
- RVT on valimiste infosüsteemide omanik ning peab tagama, et süsteemide osas viiakse läbi vajalikud analüüsid, turvatestimised, koodianalüüs ohtude ja nõrkuste tuvastamiseks. Tulemuste põhjal esitatakse vajalikud arendus- või muudatustööde tellimused RIA-le. Analüüside ja auditite läbiviimiseks peaks olema RVT-le tagatud vajalikud inim- ja finantsressursid;
- RIA vastutusalas on valimiste infosüsteemide arendustööd, majutusteenuse osutamine või haldus, süsteemide hooldustööd, vajalike muudatuste ja täiendustööde teostamine vastavalt RVT poolt esitatud tellimustele. Valimiste infosüsteemide arendustöödeks, majutuseks koos vajaliku personaliga tuleks tagada vajalikud finantsressursid.

Vastutaja(d): JuM/VVK

Tähtaeg: 31.12.2023 (eelduslik tähtaeg, lõplik tähtaeg selgub järgmise valimistsükli käigus)

Tähelepanek 5 – Jätkusuutliku arendamise puudumine

Tähelepanek 5: Intervjuude käigus kogutud informatsiooni põhjal ei ole e-valimiste töörühma koondaruandes⁹ ettepanekut 1 arvestatud ega seeläbi tagatud valimiste jätkusuutlikuks arendamiseks vajalikke finantsressursse.

Auditi intervjuude käigus tõstatasid mitmed asutused antud probleemkoha, rõhutades nii sellest tulenevaid ressursialaseid piiranguid vastavate vajalike arenduste tegemisel kui ka piisava inimressursi puudumist. RVT-l on puudu valijarakendusega tegelevatest IT-spetsialistidest, kes tegeleks tootearenduse ja turbeteemadega. RIA-l on peamiseks küsimuseks finantsressursi vajadus, et teostada plaanitud arendusi (nt m-hääletamine), hallata e-hääletamise majutuskeskkondi ning palgata vajalikku inimressurssi sellega tegelema jne.

Madal

Audiitoritele on tehtud kättesaadavaks RVT ja RIA 2023–2026 eelarve taotlused valimiste infosüsteemide osas. Audiitorite hinnangul on taotlustes välja toodud summad realistlikud. Jätkusuutliku arendamise ja turvalisuse tagamiseks tuleks arvestada järgnevate tööde ja kuludega:

- m-valimiste rakenduse majutamiseks, hooldustöödeks ning väiksemateks jätkuarendusteks 1,6–1,7 miljonit eurot (ilma km-ta, periood 2023–2026);
- 2023. aasta Riigikogu valimiste arendustöödeks personalikulud (RK23 valimiste arendustööd, m-valimiste POC/MVP) 1,5 miljonit eurot (ilma km-ta, periood 2023–2026);
- VIS3 jätkusuutlikuks toimimiseks, hooldustöödeks ja väiksemateks arendusteks 3,1 miljonit eurot (ilma km-ta, periood 2023–2026);
- VIS3 m-valimiste arendustööd ja turvatestide auditid, valimiste perioodil klienditeenindus, teavituskampaaniad, käesolevas aruandes välja toodud puuduste eemaldamine, VIS ja EHS koodiauditid, muud arendustööd kokku on eeldatavalt 10 miljonit eurot (ilma km-ta, periood 2023–2026);

⁹ <https://mkm.ee/digiriik-ja-uhendus/kuberturvalisus/valimiste-kuberturvalisus>

	Pidevalt toimiva avaliku valimiste läbiviimise teenuse ärianalüüs (teenust saaks riigis kasutada nt ülikooli rektori valimiseks jmt), väiksemad arendustööd, vajaliku personali palkamine (tootejuht, kliendihaldurid) eelduslikult 800 000 eurot (ilma km-ta, periood 2023–2025). Ilma vajaliku rahalise ja inimressursita ei ole võimalik tagada e-valimiste infosüsteemide küberturvalisust ega jätkusuutlikkust. Valimiste eel Vabariigi Valitsuse reservfondist ressursside taotlemine ei ole jätkusuutlik, kuna on risk, et fondile ei ole eraldatud piisavalt rahalisi ressursse. Lisaks, valimiste-eelsel perioodil antud teemaga tegeledes ei pruugi leida vajalikke arenduspartnereid liiga lühikese etteteatamisega.
	Riskikirjeldus: Ebapiisav ressursside olemasolu võib viia süsteemi ja protsessi nõrkusteni, mis võivad mõjutada e-valimiste efektiivsust ja turvalisust (nt ühilduvusprobleemid).
	Soovitus: Vabariigi Valitsus peaks tagama e-valimiste süsteemi jätkusuutliku finantseerimise selleks, et jõuda olukorda, kus valimised (sh e-valimised) oleksid e-riigi alusteenusena soovijatele pidevalt kasutatavad. Oluline on tagada e-valimiste turvalisuse tase ning töötajate olemasolu vastavasisulislike kriitiliste teenuste jaoks.
	Vastutaja(d): VVK/RVT (vastutavad osapooled) / MKM (kaasatud osapool)
	Tähtaeg: 31.12.2023 (eelduslik tähtaeg, lõplik tähtaeg selgub peale riigieelarve ning asutuste 2023-2026 eelarve taotluste kinnitamist)

Tähelepanek 6 – Mittetäielik testimine enne valimisi

Madal	Tähelepanek 6: Audiitoritele edastatud informatsiooni põhjal ei viida erinevaid testimisi enne aktiivset valimiste perioodi läbi piisavas mahu. Valijarakenduse funktsionaalsuse testimise käigus ei testitud rakendust kõikidel laialt levinud operatsioonisüsteemidel, mis avaldus ka 2021. aasta valimistel, kui valijatel ei õnnestunud Mac OS operatsioonisüsteemil hääletada (tootjapoolne turvauuendus peale valijarakenduse testimist). Lisaks eelnevale on audiitorid täheldanud, et VIS3 andmete importimise testimisel kasutatakse väikeses mahu testandmeid. Aktiivsel valimisperioodil suuremahuliste andmete päring tekitab valimiste infosüsteemi töös tõrkeid. Päringu andmete mahu suur erinevus testimisel ja aktiivsel valimisperioodil, ei võimalda esile tuua ega ennetada süsteemi poolt tehtavate päringute käigus tekkivaid võimalikke vigu. SMIT-i poolt viidi enne valimisi läbi testimisi, kuid Rahvastikuregistri testandmete puudumise tõttu ei olnud võimalik läbi viia valijate nimekirja testimist.
	Riskikirjeldus: Ilma põhjaliku testimiseta on suur tõenäosus, et realiseeruvad turvariskid (käideldavus ja terviklus). Varasemalt on mõlemad tähelepaneku all välja toodud riskid realiseerunud. Riskitaset maandab asjaolu, et globaalselt on Mac OS kasutajaid ca 16% maailma arvutikasutajate hulgas võrreldes 75% Windows operatsiooni süsteemi kasutajate osakaaluga. MacOS-ga seotud risk realiseerus 2021 KOV valimiste käigus, kui paljudel MacOSi uusima platvormi kasutajatel ei toiminud valijarakendus koos ID-kaardiga. Andmemahu vähene testimine võib valimisperioodil valimiste infosüsteemi maha kukutada.
	Soovitus: Enne aktiivset valimiste perioodi tuleks viia läbi erinevate stsenaariumite teste, tagamaks nii valijarakenduse ja valimiste infosüsteemide toimimine erinevatel operatsioonisüsteemidel kui ka testida piisavas või samaväärse andmemahuga päringuid erinevate asutuste infosüsteemide vahel. Tuleks luua Rahvastikuregistri andmete põhjal testbaas, kus oleks võimalik testida testvalijate nimekirja Rahvastikuregistri andmetega.

Vastutaja(d): RVT/RIA/SMIT
Tähtaeg: 31.01.2023 (antud tähtaeg on eelduslik, lõplik tähtaeg sõltub valimistsüklist ning hangetest)

Tähelepanek 7 – Vaatlemise protsessi ebatäpsused

Madal	Tähelepanek 7: Valimiste juurde kuuluva vaatlemise protsessi käigus on audiitorid täheldanud, et vaatlejatele on veebi vahendusel esitletud tühistatud e-häälte näitamise käigus kodanike isikuandmeid. Audiitorite hinnangul ei ole hetkel tagatud videoülekande käigus edastatavate andmete piisav turvalisus, kuna esitatakse ka tühistatud häälte juurde kuuluvaid isikuandmeid (nimi jmt). Isikuandmeid esitledes võidakse mõjutada hääletusel osalenud inimese privaatsust. Samuti ei ole piiritletud, kas vaatlejana osalenu võib salvestada ekraanivideot ja seda levitada olenemata sellest, kas see sisaldab isikuandmeid või mitte.
	Riskikirjeldus: Vaatlemise käigus on võimalik näha valija poolt antud häält, mis rikub valija seaduslikku õigust salajasele hääletamisele. Iga valija peab saama hääletada nii, et keegi ei saaks tema tahte vastaselt teada seda, kuidas ta hääletas ja kas ta hääletas.
	Soovitus: Leida sobilik lahendus enne 2023. aastal toimuvaid valimisi tagamaks isikuandmete anonümiseerimine või piirata turvakaalutlustel isikuandmete edastamist videoülekande teel. Vaatlemise protsessi uuendamine aitaks leevendada väljatoodud riski. Reeglitega hääletamisruumis ja hääletamiskabiiniga tuleb tagada hääle saladus, sh elektroonilise hääletamise korral tuleb tagada salajasus ka hääle muutmise võimaluse ja paberhääle ülimuslikkusega.
	Vastutaja(d): VVK/RVT
	Tähtaeg: 30.12.2022 (antud tähtaeg on eelduslik, samas tuleb arvestada 2023 toimuvate Riigikogu valimistega)

Tähelepanek 8 – Ebapiisav kommunikatsioon enne valimisi

Väga madal	Tähelepanek 8: Valimistega seotud protsessidega tutvumisel ning intervjuude läbiviimisel on selgunud, et erinevad osapooled hindavad kommunikatsiooni ning protsessi toimimist väga erinevalt. Valimiste protsessi edukaks läbiviimiseks tuleks kommunikatsiooni parandada erinevate osapoolte vahel ning alustada oluliselt varem valimiste protsessis osalevate asutustega suhtlust. Audiitorite hinnangul ei ole auditi läbiviimise hetkel selgelt piiritletud, millal alustatakse valimiste protsessi ettevalmistamist ning informatsiooni vahetus erinevate osapoolte vahel enne aktiivset valimiste perioodi ei ole piisav. RIA poolt kutsuti 30.09.20 alates kokku töörühm, et koordineerida valimiste (sh e-valimiste) korralduslikke ja tehnilisi küsimusi. Antud töörühma koostöö aluseks on RIA, RVT ja MKM-i koostööleping.
	Riskikirjeldus: Puudulik või ebapiisav kommunikatsioon kõigi valimistega seotud osapoolte vahel võib tekitada arusaamatusi, mis mõjutab negatiivselt valimiste mainet või tekitab tõrkeid valimiste läbiviimisel.

Soovitus: Valimiste ettevalmistamist tuleks alustada vähemalt üks aasta enne valimiste läbiviimist, kohtumisaegad eri osapoolte vahel tuleks kokku leppida oluliselt varem ning kommunikatsiooni tuleks parandada.

Antud töörühma tuleks ametlikult lisada kõik valimiste läbiviimisega seotud osapooled. Töörühmas tuleks lisaks tehnilistele aspektidele (tootmisteemad) jagada ka valimistega seotud osapooltele vajalikku informatsiooni.

Vastutaja(d): RVT

Tähtaeg: 30.06.2022 (antud tähtaeg on eelduslik)

Tähelepanek 9 – Valimiste veebilehe informatsioon on aegunud

Väga madal

Tähelepanek 9: Audit käigus oleme tutvunud valimiste veebilehel (www.valimised.ee) avaldatud informatsiooni ning alamlehtedelt leitavate juhistega. Valimiste veebilehe informatsiooni on peale 2019. aasta Riigikogu valimisi minimaalselt muudetud. Täiendatud on üksikuid alamlehti nagu näiteks valimiste meespea alamleht „valijate nimekiri“, kuid veebilehte tuleks järjepidevalt uuendada.

Valimiste veebilehel on oluline teha täiendusi, uuendada tuleks „valijarakendused ja usaldusväarsuse kontrollimine“¹⁰ ja alamlehte. Antud alamlehel ei ole lihtsustatud kujul üldsusele selgitatud, kuidas on võimalik kontrollida valijarakendusi ning nende usaldusväarsust.

E-valimiste töörühma koondaruandes on vastav üldine ettepanek välja toodud ettepanek nr 9 all.

Riskikirjeldus: Kui valimiste ametlikku veebilehte ei ole uuendatud ning puuduvad või on aegunud e-hääletamiseks vajalikud juhendid, võib tekkida olukord, kus rikutakse valija õigust saada asjakohast informatsiooni ning tuge e-hääle andmisel.

Soovitus: Tagamaks üldsusele selgem ja ühtsem arusaam valimistest on oluline täiendada valimistega seotud veebilehte järjepidevalt eelkõige enne valimisi. Uuendada tuleks „valijarakendused ja usaldusväarsuse kontrollimine“ alamlehte.

Enne valimisi tuleks üle kontrollida, et e-hääletamise juhendite ning valimiste meespea alamlehed on uuendatud arvestades IT arendusi ning muudatusi ja järgmiste valimiste konteksti.

Vastutaja(d): RVT

Tähtaeg: 30.12.2022 (antud tähtaeg on eelduslik)

¹⁰ <https://www.valimised.ee/et/e-haaleamine/e-haaleamise-juhised/valijarakendused-ja-usaldusvaarsuse-kontrollimine>

Tähelepanek 10 – Dokumentatsiooni puudused

Väga madal	Tähelepanek 10: Audiitorid märganud ebatäpsusi nii RIA (VIS3), SMIT kui ka RVT dokumentatsioonis. - RIA VIS3 dokumentatsioonis on audiitorid leidnud ebatäpsuseid ning puuduseid selgitustes ja põhjendustes. Näiteks RIA siseveebis Confluence lehel ei ole alamlehel Arhitektuur-> Aspektid-> Aeg¹¹ dokumenteeritud ajaparametrid punktides 9-15. Audiitoritele teadaoleva informatsiooni kohaselt on mainitud Confluence leht RIA poolt uuendamisel, kuid audititoimingute läbiviimise ajal ei olnud see lõpuni viidud. - SMIT-i protsessi dokumendis „SMIT RR Klienditoe pöördumiste halduse protsess“ leidsid audiitorid puudujääke ja ebatäpsuseid. Antud dokumendi ametlik uuendamise protsess ei ole paigas, dokument ei ole ametlikult kinnitatud ja puudub dokumendi versioonihalduse viide koos viimase ülevaatuse aja ning muudatuste nimekirjaga. Hetkel ei vasta antud dokumendi haldus parimatele praktikatele. - RVT edastatud dokumentatsioonis ei kattu versioonide numbrid ja sisu nt dokumendis „Dok IVXV-AR-EN-1.4.0 ning Dok IVXV-AR-1.7.6“.
	Riskikirjeldus: Ebatäpsused protseduuride dokumentatsioonis võivad viia arusaamatusteni valimistega seotud osapoolte vahel, mis võib tekitada takistusi valimiste sujuvaks läbiviimiseks, mõjutada negatiivselt mainet ja vähendada usaldusvärsust.
	Soovitus: Tähelepaneku all välja toodud puudused dokumentatsioonis tuleks osapooltel esimesel võimalusel parandada, et tagada dokumentatsiooni vastavus ja selgelt mõistetavus järgmiste valimiste toimumise ajaks. Valimiste protsesside dokumentatsioon tuleks iga-aastaselt üle vaadata. Kõik muudatused tuleks kajastada dokumendi versioonihalduses koos muudatuste nimekirjaga k.a juhul, kui muudatusi ei tehtud.
	Vastutaja(d): RVT, RIA, SMIT
	Tähtaeg: 31.12.2022 (antud tähtaeg on eelduslik, samas tuleb arvestada 2023 toimuvate Riigikogu valimistega)

Tähelepanek 11 – Volitusnormi puudumine õigusaktides

Väga madal	Tähelepanek 11: Oleme tutvunud olemasolevate õigusaktidega, mis reguleerivad valimisi. Analüüsi tulemusena oleme tuvastanud alljärgnevad puudused õigusaktides. Riigikogu valimise seaduses¹² ei ole volitusnorm piisavalt selgelt sõnastatud, mis annab Riigi valimisteenistusele õiguse valimiste infosüsteemi kehtestamiseks. Seaduse § 15 lg 2 p 5 sätestab järgmist: „Ülesannete täitmiseks riigi valimisteenistus: /---/ 5) /---/ haldab valimiste infosüsteemi ja valijate elektroonilise nimekirja infosüsteemi.“ Sõnadel „haldab“ ja „kehtestab“ ei ole sama tähendus. Puudub valimiste infosüsteemi definitsioon, samuti puudub üheselt mõistetav selgitus, mida valimiste infosüsteemi all antud seaduse tähenduses mõeldakse. Seaduses puudub volitusnorm valimiste infosüsteemi loomiseks.
-------------------	--

¹¹ <https://confluence.ria.ee/display/VIS3/Aeg>

¹² [Riigikogu valimise seadus–Riigi Teataja](#)

	Enne 01.01.2017 kehtinud RKVS-is oli volitusnorm olemas nii VIS-le kui ka EHS-le. Elektroonilise hääletamise süsteemi põhimäärus on alates 01.01.2017 kehtetu¹³. Lisaks sellele tekib küsitavus seoses Hea õigusloome ja normitehnika eeskirja¹⁴ (HÖNTE) §-ga 12, mille kohaselt: „Volitusnorm ei tohi sisaldada volitust reguleerida valdkonda, mida Eesti Vabariigi põhiseaduse kohaselt saab reguleerida üksnes seadusega. Volitusnormis ei tohi volitada kehtestama regulatsiooni näiteks järgmistes küsimustes: /---/ 3) Vabariigi Presidendi, Riigikogu ja kohaliku omavalitsuse volikogu valimiste kord /---/“
	Riskikirjeldus: Volitusnormi puudumine ei tekita riski konkreetse hääletamistoimingu suhtes valija poolt. Küll aga tekib risk hääletamise tervikuna vaidlustamiseks. Isegi kui kaebus lükatakse tagasi, siis valimistulemuste väljakuulutamise ikkagi viibib.
	Soovitused: Hetkel kehtivat õigusruumi tuleks parendada tulenevalt järgnevatest soovitustest: 1) Kontrollida olemasoleva volituse koostõla HÖNTE §-ga 12. 2) Viia riigikogu valimiste seadusesse sisse muudatused selliselt, et definitsioonid oleks seaduses õigesti paigutatud ning täpsustatud. Volitusnorm ja valimiste infosüsteem peavad olema üheselt mõistetavad. Volitusnorm peab olema nähtav ja jälgitav mõlemas suunas – volituse andvast normist kuni selle alusel vastu võetud normini.
	Vastutaja(d): JuM/VVK
	Tähtaeg: 31.12.2023 (eelduslik tähtaeg, lõplik tähtaeg selgub järgmise valimistsükli käigus)

Tähelepanek 12 – Õigusaktide ebatäpsused

Väga madal	Tähelepanek 12: Vastavalt kehtivatele õigusaktidele oleme tuvastanud järgmised ebatäpsused. Kohaliku omavalitsuse volikogu valimise seaduses¹⁵, Euroopa Parlamendi valimise seaduses¹⁶ ja rahvahääletuse seaduses¹⁷ puudub viide valimiste infosüsteemi kasutamisele. Kõikides loetletud seadustes on küll viited Riigikogu valimise seaduse peatükile 7¹, mis omakorda viitab teistele sama seaduse sätetele, mille kaudu jõuab lõpuks hääletamistulemuste VIS-i sisestamiseni. Samas ei ole riigikogu valimise seaduse selget volitusnormi VIS-i kehtestamiseks (vt Tähelepanek 11). Arvestades, et valimiste puhul on tehniline korraldus kattuv, siis tekib küsimus nelja erineva valimisi reguleeriva seaduse vajalikkuses.
	Riskikirjeldus: Viidete puudumine ei tekita riski konkreetse hääletamistoimingu suhtes valija poolt. Küll aga tekib risk hääletamise tervikuna vaidlustamiseks. Isegi kui kaebus lükatakse tagasi, siis valimistulemuste väljakuulutamise ikkagi viibib.
	Soovitus: Viia nimetatud seadustesse sisse viide riigikogu valimiste seaduse valimiste infosüsteemi sätete kohaldamisele. Kaaluda kõikide valimiste korraldamise nõuete koondamist ühte seadusesse, et oleks üheselt mõistetav valimisnõudeid reguleeriv seadus.

¹³ Elektroonilise hääletamise süsteemi põhimäärus–Riigi Teataja

¹⁴ Hea õigusloome ja normitehnika eeskiri–Riigi Teataja

¹⁵ Kohaliku omavalitsuse volikogu valimise seadus–Riigi Teataja

¹⁶ Euroopa Parlamendi valimise seadus–Riigi Teataja

¹⁷ Rahvahääletuse seadus–Riigi Teataja

Vastutaja(d): JuM/VVK
Tähtaeg: 31.12.2023 (eelduslik tähtaeg, lõplik tähtaeg selgub järgmise valimistsükli käigus)

Tähelepanek 13 – Valijarakenduse veateade ei viita õigele lehele

Väga madal	Tähelepanek 13: Vastavalt valimiste veebilehe juhiste lehele on antud e-häält peale hääle andmist võimalik poole tunni jooksul kontrollida kuni kolm korda¹⁸. Audiitorid viisid läbi e-valimiste hääletamise valijarakenduse testimise, mille käigus kontrolliti, kas valijarakenduse kaudu antud hääle on süsteemi poolt edukalt loetud. Süsteem võimaldab antud häält rakenduse kaudu kontrollida kolm korda poole tunni jooksul, neljandal korral süsteem blokeerib päringu. Kui antud e-häält kontrollida neli korda, kuvab valijarakendus veateade koos Abiinfo valikuga. Mainitud link aga viib kasutaja üldabiinfo lehele, mitte ei viita valimiste lehel e-hääle kontrollimise juhendile, et saada täpsemat infot veateade kohta või valimiste korraldaja abiinfot.
	Riskikirjeldus: Valimiste turvalisusele mainitud puudus otseselt riski ei kujuta, risk on pigem mainekahju, kui valijal ei õnnestu leida vajalikku abiinfot.
	Soovitus: Valijarakenduse veateated koos linkidega tuleks üle kontrollida ning veenduda, et kasutaja suunatakse vastava veateade lehele, kus leidub lisainfo ja vajadusel kontaktid abi saamiseks.
	Vastutaja(d): RVT/RIA
	Tähtaeg: 30.12.2022 (antud tähtaeg on eelduslik, samas tuleb arvestada 2023 toimuvate Riigikogu valimistega)

Tähelepanek 14 – Kasutajat ei verifitseerita kontrollrakenduses

Väga madal	Tähelepanek 14: Kontrollrakendusega saab valija poolt antud häält kontrollida ilma kasutajat (valijat) verifitseerimata. Kui pahatahtlik kasutaja saab enda kätte valija nutiseadme, mis ei ole kaitstud PIN-koodi või biomeetriaga, on võimalik vaadata teise isiku (valija) poolt antud häält. Lisaks tuvastasid audiitorid, et peale hääle andmist valijarakenduses kuvatav QR kood ei aegu, st kood jääb ekraanil näha, kui avada valijarakendus uuesti ilma vana sessiooni lõpetamata ning uuesti hääletades. Eelmise sessiooni QR kood jääb kehtima ning poole tunni jooksul on võimalik kontrollida nii viimast kui eelmise sessiooni käigus antud häält (kandidaati). Peale poolt tundi jääb QR kood nähtavaks, kuid on kehtetu, st kontrollrakendusega ei ole võimalik enam häält kontrollida. RVT kommentaar QR koodi mitteaegumise või sessiooni sundlõpetamise osas on, et QR kood sisaldab infot hääletamise protsessi etappide kohta ning see on vajalik infoallikas, kui kodanikul ei õnnestu häält anda ja pööratakse IT-toe poole.
	Riskikirjeldus: Valimiste läbiviimise turvalisusele mainitud puudus olulist riski ei kujuta, risk on valija seaduslike õiguste rikkumine, kui valija hääle ei ole piisavalt turvaliselt kaitstud ning pahatahtlik kasutaja võib tuvastada, kelle poolt isik on hääletanud ja avaldada selle näiteks sotsiaalmeedias.

¹⁸ <https://www.valimised.ee/et/e-haaletamine/e-haaletamise-juhised/e-haale-kontrollimine>

Soovitus: Kontrollrakenduses tuleks antud hääle avamiseks isik verifitseerida või küsida nutiseadme PIN-koodi/biomeetrilist kinnitust.

Pärast hääle andmist tuleks valijarakenduse sessioon lõpetada 15 minuti jooksul, et piirata QR koodi lugemise võimalust võõra kasutaja poolt. Valija hääle salajasust aitab tagada valijarakenduse sessiooni piiramine ning antud olukorras ei ole vajalik QR koodi osas rakendada aegumist või kuvamise piiramist rakenduses.

Vastutaja(d): RVT/RIA

Tähtaeg: 30.12.2022 (eelduslik tähtaeg, lõplik tähtaeg selgub järgmise valimistsükli käigus)

6 Kokkuvõte

Valimiste infosüsteemide ja nendega seotud protsesside turvalisuse tervikliku auditeerimise käigus oleme hinnanud valimiste infosüsteemide ja nendega seotud protsesside turvalisust.

Valimiste infosüsteemide ja nendega seotud protsesside turvalisuse auditeerimise käigus viisime läbi intervjuud MKM, RVT, RIA ja SMIT esindajatega. Tutvusime RVT, RIA, SMIT ja MKM poolt edastatud dokumentatsiooniga sh elektroonilise hääletamise infosüsteemi (EHS) valijarakenduse, valimiste infosüsteemi (VIS3), Rahvastikuregistri ja selle kasutajatoe protsessi ning loetletud osapoolte vahel sõlmitud omavaheliste kokkulepete dokumentatsiooniga.

Protsessi auditi käigus tutvutud dokumentatsiooni ja edastatud tõendite põhjal saame väita, et valimiste infosüsteemides ja nendega seotud protsessides ei esine väga kõrge ega kõrge riskitasemega puudusi. Väga kõrge ja kõrge riskitasemega puudusteks loetakse puuduseid, mis võivad mõjutada protsesside korrektset toimimist, valimistulemuste korrektsust, valimiste infosüsteemide turvalisust, valijate isikuandmete ja tehtud valikute avalikuks tulekut jt.

Valimiste infosüsteemide ja nendega seotud protsesside osas oleme tuvastanud 14 puudust ja mittevastavust, millest 3 puudust on keskmise riskitasemega, 4 puudust on madala riskitasemega ning 7 väga madala riskitasemega.

Keskmise riskitasemega puudusteks antud auditi kontekstis on: dokumentatsioonis esinevad ebatäpsused ja puudused, mis võivad mõjutada protsessi kui terviku turvalisust; ebapiisava tihedusega riskianalüüsi läbiviimine, kuna riskid on pidevas muutumises sõltuvalt kasutuses olevatest tehnoloogiatest ja sealt leitud vigadest; parimate praktikate järgimine seansihalduse sessiooni pikkuse osas ei ole tagatud, millest tulenevalt võib tekkida süsteemile suurenenud koormus ning tõuseb tõenäosus süsteemi rikkeks.

Madala ja väga madala riskitasemega puudusteks antud auditi kontekstis on: vastutusalade selge piiritlemine, mis ei ole hetkel kõigile osapooltele selgelt arusaadav ja üheselt mõistetav; ebapiisavate vahendite eraldamine valimiste jätkusuutlikkuse tagamiseks; turvatestimise protsessi kirjelduse ja dokumentatsiooni puudused; vaatlemise protsessi ebatäpsused, kus veebi vahendusel on esitletud tühistatud e-häälte näitamise käigus kodanike isikuandmeid; ebapiisav kommunikatsioon valimistega seotud osapoolte vahel; vananenud informatsioon valimiste veebilehel¹⁹; ebatäpsused sisemises protsessi dokumentatsioonis, dokumentidel puudub kinnituse kuupäev või täpsed vastused väljatoodud punktidele ei ole leitavad; volitusnormi puudumine õigusaktides, mis näiteks annab Riigi valimisteestistusele õiguse valimiste infosüsteemi kehtestamiseks; ebatäpsused õigusaktides, kus puudub viide valimiste infosüsteemi kasutamisele; valijarakenduse veateade ei viita õigele lehele, päring blokeeritakse, mitte ei suunata kasutajat edasi infolehele; kasutaja verifitseerimata jätmine kontrollrakenduses, kus pahatahtlik isik võib vaadata teise isiku (valija) poolt antud häält.

Lõppkokkuvõtteks võime väita, et protsessi auditi käigus tutvutud dokumentatsiooni ja edastatud tõendite põhjal on valimiste infosüsteemid ja nendega seotud protsessid piisavalt turvalised, et tagada e-valimise protsesside korrektset toimimist, valimistulemuste korrektsust, valimiste infosüsteemide turvalisust vältimaks valijate isikuandmete ja tehtud valikute avalikuks tulekut.

Viisime oma auditi läbi asjatundlikult ja nõuetekohase professionaalse hoolega. Audit annab mõistliku kindluse auditeeritava protsesside tõhususe kohta, võttes arvesse auditi riski, et isegi suhteliselt olulised eeskirjade eiramised ja rikkumised võivad jääda avastamata. Eeldasime, et meile edastatud teave ei olnud vale ega eksitav. Oleksime saanud teistsugust või täiendavat teavet, oleksime võinud tõstatada teistsuguseid tähelepanekuid.

¹⁹ www.valimised.ee

Lisa 1 - Edastatud dokumentatsioon

Töö teostamisel kogusime ja oleme tutvunud järgnevate dokumentidega:

1) RIA VIS3 arenduskeskkonna dokumentatsioon (olulisemad viited)

- a. Äriarhitektuur <https://confluence.ria.ee/pages/viewpage.action?pageId=95585791>
- b. Evitusarhitektuur <https://confluence.ria.ee/display/VIS3/Evitusarhitektuur>
- c. API-d ja UI-d <https://confluence.ria.ee/display/VIS3/API-d+ja+UI-d>
- d. Hostinimed ja IP-d <https://confluence.ria.ee/display/VIS3/Hostinimed+ja+IP-d>
- e. VIS3-EHS liideste spetsifikatsioonid <https://github.com/e-gov/VIS3-EHS>
- f. Analüüs > Välisliidesed > Rahvastikuregister
<https://confluence.ria.ee/display/VIS3/Rahvastikuregister>
- g. Testimine <https://confluence.ria.ee/display/VIS3/Testimine>
- h. Juhendid <https://confluence.ria.ee/display/VIS3/Juhendid>
- i. VIS3 ja EHS andmevahetuses usalduse loomine (võtmete vahetamine) – protseduuri dokument (tellimus)
- j. Taustateavet saab VIS3 ja EHS andmevahetuse spetsifikatsioonist (<https://github.com/e-gov/VIS3-EHS>)
- k. RIA IKT 2023-2026 taotlused – RIA e-valimiste toetava rolli, arenduses VIS3 ja M-valimiste rakendused, valimiste korraldamisega seotud kulud jaoks (igakordselt valimiste sõlmitud leping)

2) SMIT poolt edastatud dokumentatsioon

- a. 07.10.21-17.10.21_statistika_SMIT.xlsx
- b. Algnimekirja_päringu_intsident.pdf
- c. Failistruktuur.pdf
- d. Muudatuste_pärimise_intsident.pdf
- e. Pöördumiste halduse protsess_RR_Klienditugi.docx
- f. Teenused+andmete+küsimiseks+VIS3.pdf
- g. Valijate+nimekirja+X-tee+teenus+VIS3ga.pdf

3) RVT poolt edastatud dokumentatsioon

- | | |
|---|---|
| a. IVXV-TP-1.2_e-haaletamise_infoturbe poliitika.pdf | o. IVXV-API.pdf |
| b. RVT korraldus nr 3 (E-haaletamise rakkerühm).pdf | p. IVXV-audiitor.pdf |
| c. RVT korraldus nr 4 (KOV krüptoalgoritm).pdf | q. IVXV-haldusteenuse-juhend.pdf |
| d. RVT korraldus nr 5 (KOV lugemise juures viibivad isikud).pdf | r. IVXV-kogumisteenuse-haldusjuhend.pdf |
| e. RVT korraldus nr 6 (KOV testimise ajakava).pdf | s. IVXV-seadistuste-koostejuhend.pdf |
| f. RVT korraldus nr 9 (e-haaletamise infoturbe poliitika).pdf | t. IVXV-valijarakendus.pdf |
| g. RVT korraldus nr 12 (EHS tehniline dokumentatsioon).pdf | u. IVXV-valijarakenduse-pakendamine.pdf |
| h. IVXV-dokumentatsiooni-uldisukord.pdf | v. IVXV-architecture-diff.pdf |
| i. IVXV-architecture.pdf | w. IVXV-arhitektuur-diff.pdf |
| j. IVXV-arhitektuur.pdf | x. IVXV-audiitor-diff.pdf |
| k. IVXV-kasutusmallid.pdf | y. IVXV-dokumentatsiooni-uldisukord-diff.pdf |
| l. IVXV-protocols.pdf | z. IVXV-haldusteenuse-juhend-diff.pdf |
| m. IVXV-protokollid.pdf | aa. IVXV-kasutusmallid-diff.pdf |
| n. IVXV-votmerakendus.pdf | bb. IVXV-kogumisteenuse-haldusjuhend-diff.pdf |
| | cc. IVXV-protocols-diff.pdf |
| | dd. IVXV-protokollid-diff.pdf |
| | ee. IVXV-seadistuste-koostejuhend-diff.pdf |

Kontakt

Ivar Anton

IT audit Team Lead

+372 6 268 700

ivaranton@kpmg.com

Mihkel Kukk

Head of Cyber and IT audit

+372 6 268 700

mihkelkukk@kpmg.com

Tarmo Toiger

Partner

+372 6 268 700

ttoiger@kpmg.com

KPMG Baltics OÜ

Narva mnt 5

10117 Tallinn

Estonia

kpmg.ee

© 2022 KPMG Baltics OÜ, an Estonian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

KPMG name and logo are registered trademarks or trademarks of the KPMG International Cooperative ("KPMG International").

