SOTSIAALKINDLUSTUSAMET

KÄSKKIRI

05.12.2024 nr 171

Sotsiaalkindlustusameti riskihaldusjuhendi kinnitamine

Alused: korruptsioonivastane seadus (KVS); küberturvalisuse seaduse (KüTS) § 7 lg 2 p 1 ja KüTS alusel ettevõtlus- ja infotehnoloogiaministri 16.12.2022 määrusega nr 101 kehtestatud „Eesti infoturbestandard“; hädaolukorra seaduse § 39 lg 5 alusel kehtestatud Vabariigi Valitsuse 29.07.2021 määrus nr 75 „Elutähtsa teenuse toimepidevuse riskianalüüsi ja plaani nõuded, nende koostamise ning plaani kasutuselevõtmise nõuded ja kord1“ ning selle alusel Riigikantselei poolt välja antud „Toimepidevuse riskianalüüsi ja plaani koostamise juhend 2024“; töötervishoiu ja tööohutuse seaduse (TTOS) § 13’4; raamatupidamise seaduse § 24 lg 3; sotsiaalkaitseministri 30.01.2019 määrusega nr 2 „Sotsiaalkindlustusameti põhimääruse“ § 10 lg 1 p 6 ja lg 2; sotsiaalkindlustusameti peadirektori 12.05.2024 käskkirjaga nr 67 kinnitatud „Eesti infoturbestandardi rakendamine ja äriprotsessidele kaitsetarbe määramine“; peadirektori 18.06.2024 käskkirjaga nr 80 kinnitatud „Sotsiaalkindlustusameti kriisiplaan“; peadirektori 01.07.2024 käskkirjaga nr 87 kinnitatud „Sotsiaalkindlustusameti infoturvapoliitika“

Sotsiaalkindlustusameti poolt pakutavate teenuste toimivust ohustavate riskide kaardistamiseks ning riskide mõju ja tõenäosuse hindamiseks ning teenuste toimepidevuse tagamiseks

1. Kinnitan Sotsiaalkindlustusameti riskihaldusjuhendi vastavalt käskkirja lisale 1.

2. Juhendis esitatud põhimõtted kehtivad tagasiulatuvalt alates 1. jaanuarist 2024.a., juhend jõustub käesoleva käskkirja kinnitamisest.

(allkirjastatud digitaalselt)
Maret Maripuu
Peadirektor

Lisa 1

Kinnitatud 05.12.2024

Käskkirjaga nr 171

Sotsiaalkindlustusameti riskihaldusjuhend

1. Juhendi eesmärk, ulatus ja kasutatavad põhimõisted

1.1. Käesoleva juhendi eesmärk on kirjeldada asutuse riskihalduse protsessi ja anda juhiseid riskide tuvastamiseks, hindamiseks ja maandamiseks Sotsiaalkindlustusameti (edaspidi SKA) teenuste toimivust ohustavate riskide kaardistamiseks ning riskide mõju ja tõenäosuse hindamiseks ja teenuste toimepidevuse tagamiseks, et seeläbi parandada organisatsiooni üldist turvalisust ja vastupanuvõimet.

1.2. SKA riskihaldus on korraldatud asutuse äriprotsesside põhiselt, arvestades põhi- ja tugiteenuste jaotust ning eripärasid.

1.3. Teenusepõhise või äriprotsessi riskihalduse loomise, rakendamise ning käesoleva juhendi aja- ja asjakohasena hoidmise eest vastutab peadirektori poolt määratud SKA teenistuja lähtuvalt ametijuhendist või peadirektori käskkirjaga määratud ühekordsest teenistusülesandest.

1.4. Juhendis kasutatavad mõisted lähtuvad juhendi kehtestamisel aluseks olevates õigusaktides nimetatud legaaldefinitsioonidest ja Eesti Infoturbestandardi (E-ITS) põhiterminitest[1].

2. SKA riskikategooriad

2.1. Riskide hindamisel tuleb määrata riskidele kategooriad, et oleks võimalik riske grupeerida.

2.2. Risk kategoriseeritakse, pidades silmas, et riskid võivad liikuda ühest kategooriast teise ja kuuluda samaaegselt mitmesse kategooriasse. Riskikategooriad on järgnevad:

2.2.1. strateegiline risk – risk, mis realiseerumisel seab ohtu SKA strateegiliste eesmärkide saavutamise, näiteks vale planeerimine või koostöö puudumine huvigruppidega jmt;

2.2.2. tegevusrisk – risk, mis tuleneb ebapiisavatest või puuduvatest protsessidest või tegevustest asutuse sees, näiteks ebatõhus juhtimine või valed otsused, IT-riskid, personaliga seotud riskid, töökeskkonna riskid, inimlikud eksimused jmt;

2.2.3. mainerisk – risk, mis realiseerumisel mõjutab negatiivselt asutuse tajumist kolmandate isikute poolt, reputatsiooni avalikkuse silmis, näiteks ebaõige info avaldamine, konfidentsiaalse info lekkimine, negatiivne meediakajastus jmt;

[1] Eesti infoturbestandardi seletav sõnaraamat veebiväljaandena https://eits.ria.ee/et/abimaterjalid/seletav-soonaraamat

2.2.4. finantsrisk – risk, mis realiseerumisel ähvardab kaasa tuua (tõsiseid) rahalisi kaotusi, näiteks ebaõige finantsplaneerimine või aruandlus, finantskahju jmt;
2.2.5. aruandlusrisk – risk, mille tulemusena võib juhtkond langetada valesid juhtimisotsuseid, näiteks ebaõige alusinfo aruandluse koostamisel, väära mulje kujunemine aruandluse tõlgendamisel jmt;
2.2.6. vastavusrisk – risk, mille realiseerumisel ei vasta asutuse tegevus õigusaktides sätestatud nõuetele ja ei ole tagatud nende järgimine, näiteks õigusruumi ebaõige tõlgendamine tegevuse käigus või selle arvestamata jätmine, teadaoleva audititulemuse arvestamata jätmine jmt;
2.2.7. väliskeskkonna risk – risk, mis tuleneb asutuse välisest tegevusest ja mille haldamine ei ole asutuse töötajate võimuses, näiteks vääramatu jõud, planeerimata õigusruumi muudatus jmt;
2.2.8. pettuse risk – risk, mis hõlmab ebaseaduslikke tegusid, mis võidakse korda saata organisatsiooni kasuks või kahjuks ja nii organisatsioonisiseste või-väliste isikute poolt ja mida iseloomustab tahtlus, näiteks korruptsioon, õigusakti rikkumine jmt.

3. Teenuste riskihalduse protsess üldiselt

3.1. SKA teenuste riskihaldus toimub lähtudes teenuste strateegilistest eesmärkidest, mis on kinnitatud riiklike arengukavadega Vabariigi Valitsuse või Sotsiaalministeeriumi tasandil.

3.2. Riskihaldus algab organisatsiooni sisemise ja välise keskkonna mõistmisest, sealhulgas sotsiaalsete, poliitiliste, majanduslike ja tehnoloogiliste tegurite arvestamisest.

3.3. Riskide tuvastamine hõlmab teenuse või äriprotsessiga seotud võimalike ohtude ja nende mõju kindlakstegemist. Riskide tuvastamiseks kasutatakse erinevaid meetodeid ja tööriistu, nt dokumentide ülevaatus, intervjuud, organisatsiooniülesed küsimustikud, töökoha või tööprotsessi vaatlus.
3.3.1. Dokumentide ülevaatuse käigus analüüsitakse olemasolevaid dokumente, sh töökorrad, juhendid, varasemad riskihinnangud, auditite aruanded, protseduurid ja poliitikad, et tuvastada võimalikud riskid;
3.3.2. Intervjuu käigus vesteldakse teenistujate ja juhtidega, et saada ülevaade võimalikest riskidest. Intervjuu tulemused vormistatakse vähemalt kirjalikku taasesitamist võimaldavas vormis (nt e-kirjaga);
3.3.3. Küsitlused suunatakse vastamiseks kõigile SKA teenistujatele või konkreetsele teenusega või äriprotsessiga seotud teenistujate grupile, et koguda laiemat arvamust ja tuvastada riske, mida muidu ei pruugi märgata või mida üks teenistuja ei puugi osata välja tuua;
3.3.4. Töökoha või tööprotsessi või töökeskkonna vaatlus teostatakse, et tuvasta võimalikke ohte ja riske. See meetod on eriti kasulik füüsiliste ja operatiivsete riskide tuvastamiseks.
3.3.5. Lisaks eeltoodule on ohtude või riskide tuvastamiseks kasutada ajurünnakuid, kus osalevad erinevate osakondade teenistujad, sest see aitab tuvastada riske erinevates vaatenurkades. Samuti SWOT analüüsi, et tuvastata organisatsiooni tugevused, nõrkused, võimaluse ja ohud. Täiendavalt saab kasutada väliseid allikaid, sh valdkonna aruandeid,

teadusuuringuid, konsultantide soovitusi või ka organisatsiooni tulemuslikkuse näitajaid, et tuvastada kõrvalekaldeid ja võimalikke riske.

3.4. Pärast ohtude kindlakstegemist toimub teenuse või äriprotsessiga seotud riskide hindamine.

3.4.1. Riskide hindamis abil määratakse riskide esinemise tõenäosus ja riski realiseerumisel avalduv võimalik mõju, sh kahju organisatsiooni, teenuse ja/või inimeste vaates.

3.4.2. Riskide hindamine võib olla kvantitatiivne (numbriline) või kvalitatiivne (kirjeldav) hindamine. Riskide hindamiseks kasutatakse riskimaatriksit 4 x 4 või 5 x 5 süsteemis või muud konkreetse teenuse või protsessiga sobivat süsteemi.

3.4.3. Riskide hindamisel riskimaatriksi abil paigutatakse riskid maatriksisse, kus üks telg näitab riski tõenäosust ja teine telg riski mõju.

3.4.4. Riskitaseme määramise võetakse aluseks Vabariigi Valitsuse määrus „Elutähtsateenuse toimepidevuse riskianalüüsi ja plaani nõuded, nende koostamise ning plaani kasutuselevõtmise nõuded ja kord“ Lisa 3: Stsenaariumi realiseerumise tagajärje hindamine".

3.4.5. Riskide prioritiseeritakse nende olulisuse alusel, st riskimaatriksi kasutamisel asetuvad kõrge tõenäosuse ja suure mõjuga riskid maatriksis kõrge prioriteediga alale.

3.5. Pärast riskide prioritiseerimist analüüsitakse, kui palju riske organisatsioon on valmis taluma. See aitab määrata, millised riskid vajavad kiiret sekkumist ja millised võivad oodata, sh

3.5.1. Teenuse või äriprotsessi eest vastutava osakonna juhataja esitab riskihindamise tulemused ja sellest tulenevad ettepanekud SKA juhtgrupile kahe nädala jooksul arvates hindamistulemuste saamisest.

3.5.2. SKA juhtgrupp arutab ja määrab riskide prioriteetsuse, võttes arvesse organisatsiooni strateegilisi eesmärke ja ressursse ning kinnitab protokollilise otsusega lõpptulemuse.

3.6. Pärast riskide hindamist töötatakse välja ja rakendatakse meetmed riskide realiseerumise ennetamiseks, realiseerunud riskide mõju vähendamiseks või mõju leevendamiseks. Suuremahuliste tegevuste elluviimiseks lisatakse meetmete rakendamise ülesanne SKA või teenuse eest vastutava osakonna tööplaani või määratakse konkreetse teenistuja ülesandena.

3.7. Riskide maandamiseks kasutatakse ühte või mitut strateegiat, meetodit või tegevust, sh

3.7.1. Riskide vältimine – teadlik tegevuste või projektide vältimine, mis võivad kaasa tuua SKA jaoks suuri riske;

3.7.2. Riskide vähendamine – meetmete rakendamine riskide esinemise tõenäosuse või mõju vähendamiseks. Näiteks turvameetmete tugevdamine tööruumides või IT-süsteemides, teenistujate teadlikkuse tõstmine (koolituste või infotundide või selgitavate materjalide abil);

3.7.3. Riskide ülekandmine - riskide üleandmine kolmandale osapoolele lepingu kaudu;

3.7.4. Riskide aktsepteerimine – teatud riskide teadlik aktsepteerimine, kui nende mõju on väike või nende vältimine on liiga kulukas. Ettepaneku riski aktsepteerimiseks teeb teenuse eest vastutava osakonna juhataja SKA

juhtgrupile. Riski aktsepteerimise otsuse teeb SKA juhtgrupp, vormistades selle protokollilise otsusena;

3.7.5. Riskide hajutamine – investeeringute või tegevuste mitmekesistamine või jaotamine, et vähendada ühe riski mõju kogu organisatsioonile.

3.8. Riskihaldus on pidev protsess, mis nõuab regulaarset järelevalvet ja ülevaatust, et tagada meetmete tõhusus ja vajadusel teha kohandus. SKA riskihaldusprotessi aluseid vaadatakse üle ja vajadusel kohandatakse vähemalt üks kord kahe aasta jooksul.

4. Riskihaldusega seotud rollid ja vastutus

4.1. SKA peadirektor koostöös juhtgrupiga, kuhu kuuluvad osakondade juhatajad ja peadirektori nõunikud:

4.1.1. Määratleb ja kinnitab riskihalduse strateegia ja poliitika;

4.1.2. Tagab, et riskihaldus on integreeritud organisatsiooni strateegiliste eesmärkidega;

4.1.3. Jälgib ja hindab perioodiliselt riskihalduse tõhusust tervikuna.

4.2. Kriisireguleerimise osakond (kuni 31.12.2024.a) või sotsiaalhoolekande toimepidevuse osakond (alates1.12.2025.a), kelle põhiülesannete hulka kuulub muuhulgas ameti enda ja ameti osutatavate teenuste toimepidevuse tagamise toetamine, koostöös kriisijuhi ning teiste osakondadega ja peadirektori nõunikuga (sisekontrolli valdkonnas)

4.2.1. Koordineerib riskihalduse protsessi ja tegevusi;

4.2.2. Tuvastab, hindab ja jälgib organisatsiooniüleseid riske;

4.2.3. Arendab ja rakendab riskide maandamise plaane teenuste toimepidevuse vaates.

4.3. Riskiomanikud ehk SKA-s osakonna juhatajad, talituse juhatajad, juhtivspetsialistid ja teenuseomanikud ning portfellihaldurid või peadirektori poolt määratud teenistujad (ametijuhendi või muu asutusesisese õigusakti kaudu)

4.3.1. Vastutavad konkreetsete riskide juhtimise eest oma valdkonnas;

4.3.2. Rakendavad riskide maandamise meetmeid ja jälgivad nende tõhusust.

4.4. SKA sisekontrolliülesandega teenistujad

4.4.1. Hindavad riskihalduse protsessi ja kontrollimeetmete tõhusust määratud teenuste või äriprotsesside ulatuses;

4.4.2. Annavad sõltumatut tagasisidet ja soovitusi riskihalduse parandamiseks.

4.5. Iga SKA teenistuja

4.5.1. Teadvustab ja jälgib riskihalduse poliitikaid ja protseduure.

4.5.2. Teavitab vahetut juhti või talituse juhatajat või osakonna juhatajat või peadirektori nõunikku (sisekontrolli valdkonnas) või peadirektorit võimalikest riskidest ja intsidentidest, mis mõjutavad teenus(t)e toimivust.

Intsidentidest teavitamine toimub vastavalt intsidentide käsitlemise korrale.

5. Spetsiifilise riskihalduse rollid ja erisused üldisest riskihaldusest

5.1. E-ITS riskihaldus toimub lähtudes E-ITS riskihaldusjuhendi[2] põhimõtetest ning asutusesisestest töökordadest ja juhenditest (nt Infoturvapoliitika), sh

5.1.1. E-ITS riskihaldus on korraldatud äriprotsesside põhiselt ja toimub juhtimistarkvaras PlanPro.

5.1.2. E-ITS riskihalduse protsessi loomise ja rakendamise eest vastutab SKA infoturbespetsialist. Seejuures võib infoturbespetsialist nõustada riskide hindamisel, kuid ei tohi osaleda infoturbega seotud riskide hindamise tulemuste kinnitamisel enda vastutusalas olevate konkreetsete riskide osas.

5.1.3. E-ITS rakendamise eest füüsilise turbe vaates vastutab personaliosakonna (kuni 31.12.2024.a) või personali- ja haldusosakonna (alates 1.01.2025.a) halduse juhtivspetsialist, peaspetsialist või spetsialist talle määratud ulatuses. Seejuures võib füüsilise turbe eest vastutav teenistuja nõustada riskide hindamisel, kuid ei tohi osaleda füüsilise turbega seotud riskide hindamise tulemuste kinnitamisel enda vastutusalas olevate konkreetsete riskide osas.

5.1.4. E-ITS riskihalduse metoodika:

Riskitaseme määravad kahju suurus ja riski realiseerumise võimalikkus. Arvesse võetakse infoturbe rakendusplaani meetmed, mis on juba teostatud kui ka rakendamisele määratud meetmed.

Riskitase tuvastatakse riskimaatriksi abil 4 x 4 süsteemis, sh

5.1.4.1. Riski mõju jaguneb neljaks:

Mõju	Hinne	Kirjeldus
Tähtsusetu	1	Riski avaldumine ei häiri käimasolevaid ja planeeritavaid tegevusi ning eesmärkide saavutamist.
Vähene	2	Riski avaldumisel on tegevused ja eesmärkide saavutamine küll mõningal määral häiritud, kuid eesmärgid on saavutatavad ja lisaressursse vajatakse vähesel määral, sh võib piisav olla asutusesisene ressursside ümberjaotamine. Asutuse tööd on võimalik jätkata. Märkimisväärset mainekahju ei kaasne, see on kontrollitav. Kriitilised asukohad, teenused ei ole mõjutatud
Oluline	3	Riski avaldumisel on tegevused ja eesmärkide saavutamine olulisel määral häiritud. Eesmärkide saavutamiseks on vaja olulisel määral lisaressursse. Esineb negatiivset meediakajastust, mis nõuab asutuse poolset sekkumist. Kriitilised asukohad, teenused on mõjutatud. Teenuse toimimine on takistatud üle SLAs märgitud aja, mõjutatud on ka asutuse põhiprotsesside toimimine. Kriitilisi teenuseid on võimalik osutada alternatiivsete vahendite abil.
Kahjustav	4	Riski avaldumisel ei ole võimalik tegevusi jätkata ja/või eesmärke saavutada. Kahjude likvideerimine nõuab olulisi ressursse. Ulatuslik negatiivne meediakajastus, mis ei ole (täielikult) kontrollitav. Mõjutatud on mitmed asukohad, teenused, sh kriitilised. Suuremahuline teenuste katkestus üle SLA-s märgitud aja. Mõjutatud on asutuse põhiprotsesside toimimine.

[2] E-ITS riskihaldusejuhend veebiväljaandena https://eits.ria.ee/et/abimaterjalid/riskihaldusjuhend/juhend

5.1.4.2. Riski tõenäosus jaguneb neljaks:

Tõenäosus	Hinne	Kirjeldus
Vähetõenäoline	1	Riski avaldumine on teoreetiliselt võimalik, kuid praktiliselt üliharva juhtuv.
Võimalik	2	Riski avaldumine on võimalik, kuid praktilisi juhtumeid on üksikuid.
Tõenäoline	3	Riski avaldumine on suure tõenäosusega ja on olemas kindlad tõendusmaterjalid riski avaldumise kohta.
Kindel	4	Risk on juba avaldunud või riski avaldumine tulevikus on vältimatu.

5.1.4.3. Riski mõju ja tõenäosuse hindamise tulemusena leitakse nende koostoimes **riskitase,** lähtudes järgnevast riskimaatriksist (kasutatud värvid tulenevad PlanPro süsteemist):

MÕJU	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
Riskimaatriks numbriline		1	2	3	4
		TÕENÄOSUS			

MÕJU	Kahjustav	Keskmine	Kõrge	Väga kõrge	Väga kõrge
	Oluline	Keskmine	Keskmine	Kõrge	Väga kõrge
	Vähene	Madal	Keskmine	Keskmine	Kõrge
	Tähtsusetu	Madal	Madal	Keskmine	Keskmine
Riskimaatriks sõnaline		Vähetõenäoline	Võimalik	Tõenäoline	Kindel
		TÕENÄOSUS			

5.1.4.4. Riskimaatriksi alusel tuvastatakse riskiskoor, mille alusel seatakse riskide käsitlemiseks prioriteedid:

Riskitase	Skoor	Olulisuse määratlus
Madal	1-2	Turvameetmed annavad piisava kaitse. Praktikas väiksed riskid tavaliselt aktsepteeritakse, kuid ikkagi ohtu seirates. Hallatakse rutiinsete turbeprotsessi seiretegevuste käigus.

Keskmine	3-6	Turvameetmed võivad osutuda ebapiisavateks. Kõrgendatud tähelepanuga seire, olukorra muutudes võib vajada kohest sekkumist. Oluline on riski teadvustamine.
Kõrge	8-9	Turvameetmed ei kaitse selle ohu eest piisavalt. Riski vähendamine on prioriteet, selleks plaanitakse asjakohased tegevused, mida rakendada esimesel võimalusel.
Väga kõrge	12-16	Turvameetmed ei kaitse selle ohu eest piisavalt. Väga suurt riski praktikas ei aktsepteerita, sellega tuleb (käitlusjärgus) eraldi tegeleda. Vajab kohest sekkumist, et vähendada riski talutava piirini.

5.1.4.5. E-ITS riskide hindamise ja seire eest vastutavad teenistujad, nende tegevused ja tähtajad kinnitatakse osakonna tööplaaniga või eraldi peadirektori käskkirjaga ning lisatakse PlanPro süsteemi iga kalendriaasta kohta tegevuste elluviimise kalendriaasta 31. jaanuariks.

5.2. SKA töökeskkonna riskihaldus toimub lähtudes töötervishoiu ja tööohutuse seaduse ja selle alamaktides sätestatud põhimõtetest ning asutusesisestest töökordadest ja juhenditest, sh

5.2.1. Töökeskkonna riskihalduse eest vastutab personaliosakonna (kuni 31.12.2024.a) või personali- ja haldusosakonna (alates 1.01.2025.a) töökeskkonna- ja heaolu partner koostöös töökeskkonnavolinike ning töökeskkonnanõukogu liikmetega.

5.2.2. Töökeskkonna riskihaldus toimub Tööinspektsiooni iseteeninduskeskkonna https://iseteenindus.ti.ee/login riskianalüüsi töövahendi abil tuginedes viidatud keskkonna toimemudelile ja riskihalduse süsteemile[3].

5.2.3. Töökeskkonna riskide hindamise ja seire eest vastutavad teenistujad, nende tegevused ja tähtajad kinnitatakse peadirektori käskkirjaga iga kalendriaasta kohta tegevuste elluviimise kalendriaasta 31. jaanuariks.

5.3. Korruptsiooni ja huvide konflikti riskihaldus toimub lähtudes Justiitsministeeriumi koostatud riskide haldamise ja hindamise juhendist[4] ning asutusesisestest töökordadest ja juhenditest, sh

5.3.1. Korruptsiooni ja huvide konflikti riskihalduse eest vastutab peadirektori nõunik (sisekontrolli valdkonnas).

5.3.2. Korruptsiooni ja huvide konflikti riskihaldus toimub dokumendihaldussüsteemis Delta ning riigitöötaja iseteeninduse portaalis RTIP.

5.3.3. Korruptsiooni ja huvide konflikti riskide analüüsimise alusohud on:

5.3.3.1. Organisatsiooni tasandil

- Nõrk organisatsioonikultuur ja juhtimine;

[3] Iseteeninduskeskkonna kasutusjuhend veebiväljaandena https://www.ti.ee/sites/default/files/documents/2023-02/TI_iseteeninduse_kasutusjuhend_ET_02.2023.pdf

[4] Justiitsministeeriumi juhend „Korruptsiooni ja huvide konflikti riskide hindamine“ veebiväljaandena https://www.korruptsioon.ee/sites/default/files/2024-01/Korruptsiooni%20ja%20huvide%20konflikti%20riskide%20hindamine.pdf

- Nõrk kontrollikeskkond;
- Teadlikkuse tõstmisega mittetegelemine ja nõrk kommunikatsioon.

5.3.3.2. Ametiisiku tasandil (teenistujad)

- Korruptiivne tulu;
- Ametiseisundi korruptiivne kasutamine;
- Avaliku vahendi korruptiivne kasutamine;
- Mõju korruptiivne kasutamine;
- Siseteabe korruptiivne kasutamine;
- Tegevus- ja toimingupiirangute rikkumine.

5.3.4. Korruptsiooni ja huvide konflikti riskide analüüsimiseks:

5.3.4.1. Tuvastatakse ohud teenuste, protsesside, struktuuriüksuste või ametikohtade vaates;

5.3.4.2. Tuvastatakse võimalikud nõrkused ja haavatavused;

5.3.4.3. Hinnatakse üle kasutatavate kontrollimehhanismide tõhusus;

5.3.5. Metoodika: Riskitaseme määravad kahju suurus ja riski realiseerumise võimalikkus. Arvesse võetakse korruptsiooni ja huvide konflikti ennetamise meetmed, mis on juba teostatud kui ka rakendamisele määratud meetmed. Riskitase tuvastatakse riskimaatriksi abil 4 x 4 süsteemis.

5.3.6. Korruptsiooni ja huvide konflikti riskide hindamise ja seire eest vastutavad teenistujad, nende tegevused ja tähtajad kinnitatakse peadirektori käskkirjaga iga kalendriaasta kohta tegevuste elluviimise kalendriaasta 31. jaanuariks.

5.4. SKA teenuste toimepidevuse riskihaldus toimub lähtudes Vabariigi Valitsuse 29.07.2021 määruse nr 75 „Elutähtsa teenuse toimepidevuse riskianalüüsi ja plaani nõuded, nende koostamise ning plaani kasutuselevõtmise nõuded ja kord1“ ning Riigikantselei koostatud toimepidevuse riskianalüüsi ja plaani koostamise juhendi aluspõhimõtetest ning asutusesisestest töökordadest ja juhenditest.

5.4.1. Teenuste toimepidevuse riskihalduse eest vastutab kriisireguleerimise osakond (kuni 31.12.2024.a) või sotsiaalhoolekande toimepidevuse osakond (alates1.12.2025.a), kelle põhiülesannete hulka kuulub muuhulgas ameti enda ja ameti osutatavate teenuste toimepidevuse tagamise toetamine, koostöös kriisijuhi ning teiste osakondadega.

5.4.2. Teenuste toimepidevuse riskihaldus toimub dokumendihaldussüsteemis Delta ning teenusepõhiselt *Confluence* keskkonnas (wiki).

5.4.3. Metoodika: Riskitaseme määravad kahju suurus ja riski realiseerumise võimalikkus. Arvesse võetakse meetmed, mis on juba teostatud kui ka rakendamisele määratud meetmed.

5.4.4. Teenuse toimepidevuse riskitase tuvastatakse riskimaatriksi abil 5 x 5 süsteemis, kus

	TÕENÄOSUS					RISKISKOOR | 1 – 25
MÕJU		1	2	3	4	5	
	1	1	2	3	4	5	1 – 2 EBAOLULINE
	2	2	4	6	8	10	3 – 7 MADAL
	3	3	6	9	12	15	8 – 12 KESKMINE
	4	4	8	12	16	20	15 – 19 KÕRGE
	5	5	10	15	20	25	20 – 25 KRIITILINE

1 – väga väike, 2 – väike, 3 – keskmine, 4 – suur, 5 – väga suur

6. Teabevahetus ja aruandlus
   - 6.1. Riskihalduse tulemused edastatakse vastutava teenistuja poolt perioodiliselt vähemalt kirjalikku taasesitamist võimaldavas vormis või aruandena peadirektorile ja SKA juhtgrupi liikmetele ning esitletakse juhtgrupi koosolekul vähemalt üks kord kalendriaastas.
     - 6.1.1. E-ITS riskihalduse tulemused ja tegevuste ülevaate annavad infoturbespetsialistid või füüsilise turbe eest vastutavad teenistujad üks kord kuus ettekande vormis juhtgrupi koosolekul.

7. Dokumentatsioon ja arhiiv
   - 7.1. Riskihaldusega seotud dokumente säilitatakse ja hallatakse lähtuvalt SKA teabehalduse korrast ning teenuse spetsiifiliselt lähtuvalt teenusega seotud sisemistest kordadest.

8. Koolitus ja teadlikkus
   - 8.1. Riskihaldusega seotud teadlikkuse tõstmiseks kavandatakse ja viiakse iga-aastaselt läbi SKA teenistujatele suunatud sise- ja tellimuskoolitusi lähtudes SKA teenistujate arendamise ning koolituse põhimõtetest.
   - 8.2. Riskihaldusega seotud koolituse kavandamise ja tellimise eest vastutavad kriisijuht, sotsiaalhoolekande toimepidevuse osakond, teiste osakondade juhatajad, talituse juhatajad ja juhtivspetsialistid, infoturbespetsialistid või peadirektori nõunik (sisekontrolli valdkonnas) osakonna põhimäärusest või teenistuja ametijuhendist või muust asutuse sisemist töökorraldust reguleerivas õigusaktis nimetatud pädevuse piire arvestades