

Vastutav osakond: Strateegia- ja finantsosakond (SAFO)	Kinnitatud: kantsleri 25.07.2025 käskkirjaga nr 41
Protsessi koordinaator: Strateegia- ja finantsosakond, riskijuht	Versioon: 5

Rahandusministeeriumi riskijuhtimise kord

Andmed dokumendi muutmise kohta

Versioon	Jõustumise kuupäev	Muudatuse kirjeldus
Algne	01.10.2008	Algne versioon
Versioon 2	18.05.2010	Täiendati protsessiosaliste õigusi ja kohustusi.
Versioon 3	09.10.2013	Riskide hindamine integreeriti arengukava ja tegevuskava koostamise ja ülevaatamise protsessiga.
Versioon 4	04.11.2020	Täiendati olulises matus, protsessi koordineerijaks muudeti arendusosakond; lihtsustati tööprotsessi; määratleti riski hinde piir, millest alates maandamistegevused planeeritakse; protsessi kirjeldamiseks võeti kasutusele uus visuaal, mis kajastab ka kaasuvaid otsuseid, dokumente ja IT- süsteeme.
Versioon 5	25.07.2025	Dokumenti täiendati olulisel määral: riskijuhtimise protsessi koordineerijaks määrati strateegia- ja finantsosakond ning vastutajaks riskijuht. Määratleti RAM-i poolt aktsepteeritav riskitase, uuendati riskijuhtimise põhimõtted ja metoodika, tuginedes riskihalduse standarditele ning parimatele praktikatele, sh E-ITS riskihaldusjuhendile. Samuti täiendati valdkonnapõhiseid erisusi ja vastutusi riskihalduses.

Sisukord

1. Sissejuhatus ja eesmärk	1
2. Õiguslikud alused ja valdkondlikud erisused	2
3. Riskijuhtimise põhimõtted.....	3
4. Vajaduspõhine riskianalüüs	3
5. Riskihalduse metoodika.....	4
6. Riskiregister.....	5
7. Riskijuhtimise tööprotsessi tegevused ja rollijaotus.....	5
8. Kaasnevad dokumendid.....	8
9. Mõisted	8
Lisad	9

1. Sissejuhatus ja eesmärk

- 1.1. Rahandusministeeriumi (edaspidi RAM, asutus või ministeerium) riskijuhtimise korra eesmärk on kehtestada ministeeriumis ühtne riskijuhtimise raamistik, mis toetab strateegiliste eesmärkide saavutamist ning võimaluste teadlikku kasutamist, aidates kaasa asutuse jätkusuutlikule arengule ja tõhusamale toimimisele.
- 1.2. Riskijuhtimise eesmärk on viia asutuse tegevusega kaasnevad riskid aktsepteeritavale tasemele.

Vastutav osakond: Strateegia- ja finantsosakond (SAFO)	Kinnitatud: kantsleri 25.07.2025 käskkirjaga nr 41
Protsessi koordinaator: Strateegia- ja finantsosakond, riskijuht	Versioon: 5

2. Õiguslikud alused ja valdkondlikud erisused

- 2.1. Riskijuhtimise aluseks on mitmed siseriiklikud ja asutusesisesed õigusaktid, parimad praktikad ning organisatsiooni sisemised kokkulepped:
 - 2.1.1. Vabariigi valitsuse seaduse § 92 sätestab asutuse juhile kohustuse luua asutuses sisekontrolli süsteem - valitsusasutuse ja valitsusasutuse hallatava riigiasutuse juhtimisel rakendatav seaduslikkusele ja otstarbekusele suunatud terviklik abinõude kompleks, mis võimaldab tagada:
 - 2.1.1.1. õigusaktidest kinnipidamise;
 - 2.1.1.2. vara kaitstuse raiskamisest, ebasihipärasest kasutamisest, ebakompetentsest juhtimisest ja muust sarnasest tingitud kahju eest;
 - 2.1.1.3. asutuse tegevuse otstarbekuse asutuse ülesannete täitmisel;
 - 2.1.1.4. asutuse tegevusest tõese, õigeaegse ja usaldusväärse informatsiooni kogumise, säilitamise ja avaldamise.
- 2.2. Rahandusministeeriumi põhimäärus sätestab, et minister tagab sisekontrollisüsteemi rakendamise ja siseaudiitori kutsetegevuse korraldamise ministeeriumis ja ministeeriumi valitsemisalas olevates valitsusasutustes ning ministeeriumi hallatavates riigiasutustes.
- 2.3. Siseauditi roll riskijuhtimises on anda sõltumatut ja objektiivset hinnangut ning teha ettepanekuid riskijuhtimise ja sisekontrolli täiustamiseks. Siseauditi tööplaani koostamisel võetakse arvesse riskihindamise tulemusi, juhtkonna ja kõrgema juhtorgani ettepanekuid ning siseauditi üksuse eelarve suurust ja eelarvet.
- 2.4. Erandid, mille puhul riskijuhtimist reguleerivad täiendavalt eraldi õigusaktid või riskihindamise põhimõtted:
 - 2.4.1. Töökeskonna riskid kaardistatakse riskianalüüsina ja maandatakse tegevusplaani koostamisega vastavalt töötervishoiu ja tööohutuse seadusele. Riskide haldamise eest vastutab personali- ja õigusosakond koostöös ühisosakonnaga, tagades asutuseülese riskihindamise käigus, et asutuse riskinormi ületavad riskid kajastatakse asutuse riskiregistris.
 - 2.4.2. Füüsilise turvalisuse riskid kaardistatakse riskianalüüsi ja turvaplaanina vastavalt Vabariigi Valitsuse 23.09.2016 määruse nr 106 „Riigikaitseobjekti kaitse kord“ nõuetele. Riskide haldamise eest vastutab ühisosakond tagades asutuseülese riskihindamise käigus, et asutuse riskinormi ületavad riskid kajastatakse asutuse riskiregistris.
 - 2.4.3. Infoturvariske käsitletakse kooskõlas küberturvalisuse seaduse, selle alusel kehtestatud määruste, Eesti infoturbestandardi (E-ITS), pilvteenuse kasutamist reguleeriva määruse ning asutuse infoturbe- ja andmekaitsepoliitikaga, lähtudes ühtlasi RAM-i riskijuhtimise korrast. Infoturvariskide haldamise eest vastutab infoturbe eest vastutav töötaja, kes tagab asutuseülese riskihindamise käigus, et riskinormi ületavad riskid kajastuvad asutuse riskiregistris.

3. Riskijuhtimise põhimõtted

- 3.1. Riskijuhtimine on asutuse strateegilise juhtimise lahutamatu osa, toimub süstemaatiliselt ja järjepidevalt ning on integreeritud ministeeriumi juhtimis- ja tööprotsessidesse.
- 3.2. Riskijuhtimine on korraldatud kolmel tasandil, et tagada süsteemne ja sõltumatu riskide käsitlemine:
 - 3.2.1. Esmatasandil juhivad riske riskiomanikud oma igapäevases töös osakondades, kes tuvastavad, hindavad ja leevendavad riske oma vastutusvaldkonnas.
 - 3.2.2. Teisel tasandil toetavad ja kontrollivad riskijuhtimist juhtkond ning riskijuht, kes loovad ühtsed raamistikud, planeerivad riskihindamisi ning jälgivad leevendamistegevuste rakendamist.

Vastutav osakond: Strateegia- ja finantsosakond (SAFO)	Kinnitatud: kantsleri 25.07.2025 käskkirjaga nr 41
Protsessi koordinaator: Strateegia- ja finantsosakond, riskijuht	Versioon: 5

- 3.2.3. Kolmandal tasandil annab siseaudit, vajadusel välisaudiitorid ja teised kindlustandvate teenuste osutajad sõltumatu hinnangu riskijuhtimise ja sisekontrolli toimivusele.
- 3.3. Riskijuhtimises lähtutakse ennetavast lähenemisest, mis areneb dünaamiliselt vastavalt asutuse muutuvatele vajadustele ja ülesannetele.
- 3.4. Riskijuhtimise käigus kogutud infot, analüüse ja eksperthinnanguid kasutatakse nii ministeeriumi eesmärkide saavutamiseks kui ka kavandatavate tegevuste planeerimisel.
- 3.5. Riskide kirjeldamisel keskendutakse eelkõige riskidele, mis võivad oluliselt mõjutada eesmärkide saavutamist. Ülemäärase detailsuse ja väheolulise teabe esitamisest hoidutakse, et keskenduda juhtimisotsuseid toetavale sisule.
- 3.6. Asutuseülene riskide kaalutlemise ja käsitlemise ajakava ning seire on seotud strateegilise planeerimise ja aruandluse aastaringse tsükliga, mis tagab, et riskide hindamistulemusi arvestatakse enne järgmise perioodi tegevuste kavandamist.
- 3.7. Asutuseülene riskide kaalutlemine, riskikäsitus ning seire toimub üks kord aastas teenusepõhiselt. Vajadusel tehakse täiendav hindamine oluliste muutuste korral, mis võivad mõjutada riskide mõju või tõenäosust.
- 3.8. RAM riskijuhtimise tööprotsess, sealhulgas kord ja selle lisa, vaadatakse üle kord aastas riskihindamise tulemuste alusel ning parendatakse vastavalt vajadusele saadud kogemuste ja asjakohaste muudatuste põhjal, et tagada kooskõla strateegiliste eesmärkide ja muutuva keskkonnaga.

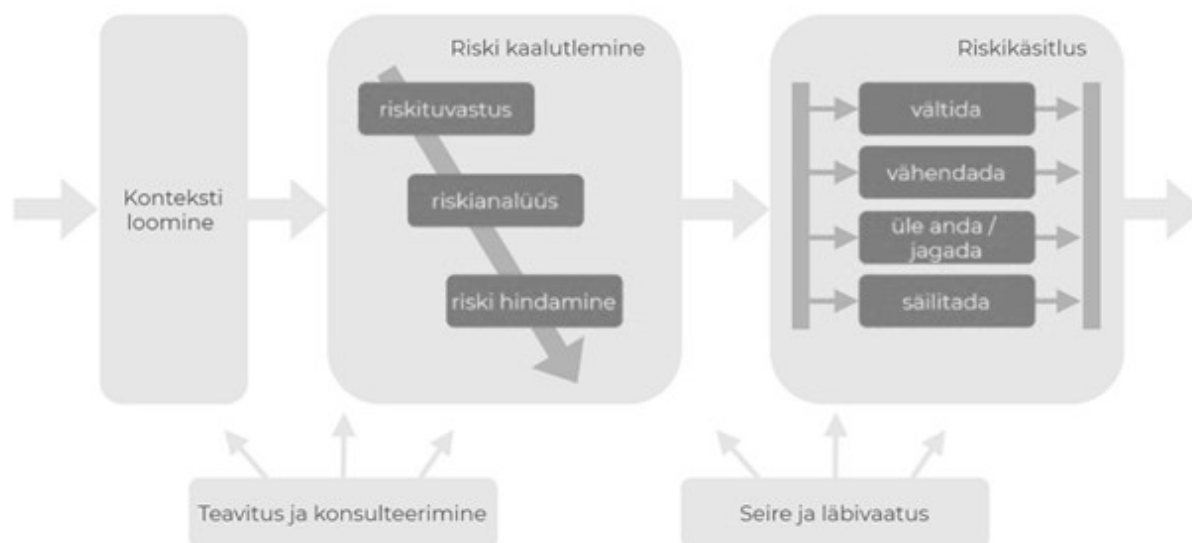
4. Vajaduspõhine riskianalüüs

- 4.1. Vajaduspõhine riskianalüüs on osa riskijuhtimisest ning seda tehakse siis, kui toimub muudatus, mis võib mõjutada eelkõige asutuse eesmärkide saavutamist, töökorraldust, andmete turvalisust või inimeste õigusi. Riskianalüüsi eesmärk on hinnata muudatusega kaasnevaid riske (nt sõltuvus teenusepakkujast, infoturberiskid, õiguslikud kohustused jms) ja kavandada sobivad riski leevendamise meetmed.
- 4.2. Riskianalüüs tuleb läbi viia vastavalt küberturvalisuse seadusele § 7 ning teistele asjakohastele õigusaktidele ja organisatsiooni sisemistele nõuetele, eelkõige siis, kui kasutusele võetakse uus infosüsteem või tehnoloogia (sh pilvtehnoloogia) või luuakse uus andmekogu. Riskianalüüsi algatamise eest vastutab muudatuse eest vastutav osakonnajuhataja, kaasates riskijuhi.
- 4.3. Juhul, kui riskianalüüsi käigus tuvastatakse, et isikuandmete töötlemine mõjutab inimese õigusi või privaatsust (nt tundlikud andmed, automatiseeritud otsused või tehisintellekti kasutamine), tuleb koostada andmekaitsealane mõjuhindang vastavalt isikuandmete kaitse seadusele § 38. Mõjuhindang võib olla riskianalüüsi osa või eraldiseisev dokument. Mõjuhindang koostatakse koostöös riskijuhiga kaasates vajadusel eksperdid vastavast valdkonnast.
- 4.4. Riskianalüüsi tulemusel tuvastatud riskinormi ületavad riskid kantakse riskiregistrisse ning kaasatakse asutuseülesse riskijuhtimise protsessi.

5. Riskihalduse metoodika

- 5.1. Riskihalduse metoodika kirjeldab protsessi, hõlmab konteksti loomist, riski kaalutlemist ja riskikäsitlust, mis moodustavad osa riskijuhtimise tööprotsessist ning kajastuvad alloleval joonisel 1.

Vastutav osakond: Strateegia- ja finantsosakond (SAFO)	Kinnitatud: kantsleri 25.07.2025 käskkirjaga nr 41
Protsessi koordinaator: Strateegia- ja finantsosakond, riskijuht	Versioon: 5



Joonis 1. Riskihaldus.

- 5.2. Riskihalduse konteksti määratlemisel võetakse arvesse asutuse strateegilisi eesmärke, RAM-i programme, auditite tulemusi, olulisi insidende, protsessidele määratud kaitsetarbeid ning sise- ja väliskeskkonna ohte. Need peamised tegurid aitavad mõista keskkonda, milles asutus tegutseb, ning tuvastada riske, mis võivad mõjutada eesmärkide saavutamist.
- 5.3. Riskide kaalutlemine koosneb kolmest sammust, milleks on riskide tuvastamine, analüüs ja hindamine.
- 5.4. Riske kaalutletakse ühtse metoodika alusel, kasutades mõju ja tõenäosuse skaalat ning riskihindamise maatriksit, mis on esitatud käesoleva korra lisas 1 (vt Exceli töölehte „Skaalad ja maatriks“).
- 5.5. RAM aktsepteerib riskinormina väga madala ja madala tasemega riske. Kõrgema tasemega riskide korral koostatakse riskikäsitluskava ning rakendatakse leevendusmeetmeid.
- 5.6. Riskianalüüsi käigus määratletakse riski võimalik mõju vähemalt ühes mõjuvaldkonnas ning analüüsitakse selle avaldumise viisi. Kui risk mõjutab mitut valdkonda, võetakse mõju hindamisel aluseks kõrgeim tuvastatud mõjutaseme hinnang. Mõjuanalüüsis hinnatakse riski mõju, lähtudes selle sisust ja kontekstist ning arvestades mõju ulatust ja tagajärgede olulisust. Mõjuvaldkondade vahel ei ole määratletud üldist tähtsuse järjekorda.
- 5.6.1. RAM-is kasutatakse riskide käsitlemiseks järgnevaid käsitusviise:
- 5.6.2. Vähendamine – aktsepteeritud riskitaset (riski normi) ületava riski vähendamine ehk leevendamine lisaturvameetmete abil.
- 5.6.3. Aktsepteerimine (säilitamine) – riski säilitamine samal tasemel, kui täiendavate riski vähendamise meetmete rakendamine osutub majanduslikult või muudel põhjustel ebaotstarbekaks. Riskinormi ületavate riskide aktsepteerimine vajab põhjendust ning asutuse juhi kinnitust.
- 5.6.4. Jagamine (üle andmine) – riski jagamine teiste osapooltega (kindlustus, välised teenusepakkujad). Riski jagamine ei võta organisatsioonilt andmete ja teiste varade kaitsmise kohustust ja vastutust seotud osapoolte ees.
- 5.6.5. Vältimine – riski põhjustavast tegevusest loobumine.
- 5.7. Riskikäsitluskava sisaldab rakendatavad leevendusmeetmed riskinormi ületavatele riskidele, vajadusel täiendava ressursikulu hinnangut ning riskikäsitluskavas kirjeldatud tegevuste täitmise tähtaega.
- 5.8. Riskide aktsepteerimise otsus tehakse riskikäsitluskava osana, tuginedes algsele riskihinnangule ja kavandatud riski leevendusmeetmetele. Väga madala ja madala riskitaseme korral loetakse risk automaatselt aktsepteerituks. Kui hinnatud riskitaseme on

Vastutav osakond: Strateegia- ja finantsosakond (SAFO)	Kinnitatud: kantsleri 25.07.2025 käskkirjaga nr 41
Protsessi koordinaator: Strateegia- ja finantsosakond, riskijuht	Versioon: 5

keskmise, kõrge, väga kõrge, siis on aktsepteerimiseks vajalik osakonnajuhi põhjendus ja kantsleri kinnitus. Kui risk ei ole aktsepteeritav, otsustatakse selle edasine käsitlemine, sealhulgas vajadus täiendavate leevendusmeetmete järele.

5.9. Jääkriski hinnatakse järgmise hindamistsükli käigus, kui on võimalik arvesse võtta rakendatud meetmete tegelikku mõju.

6. Riskiregister

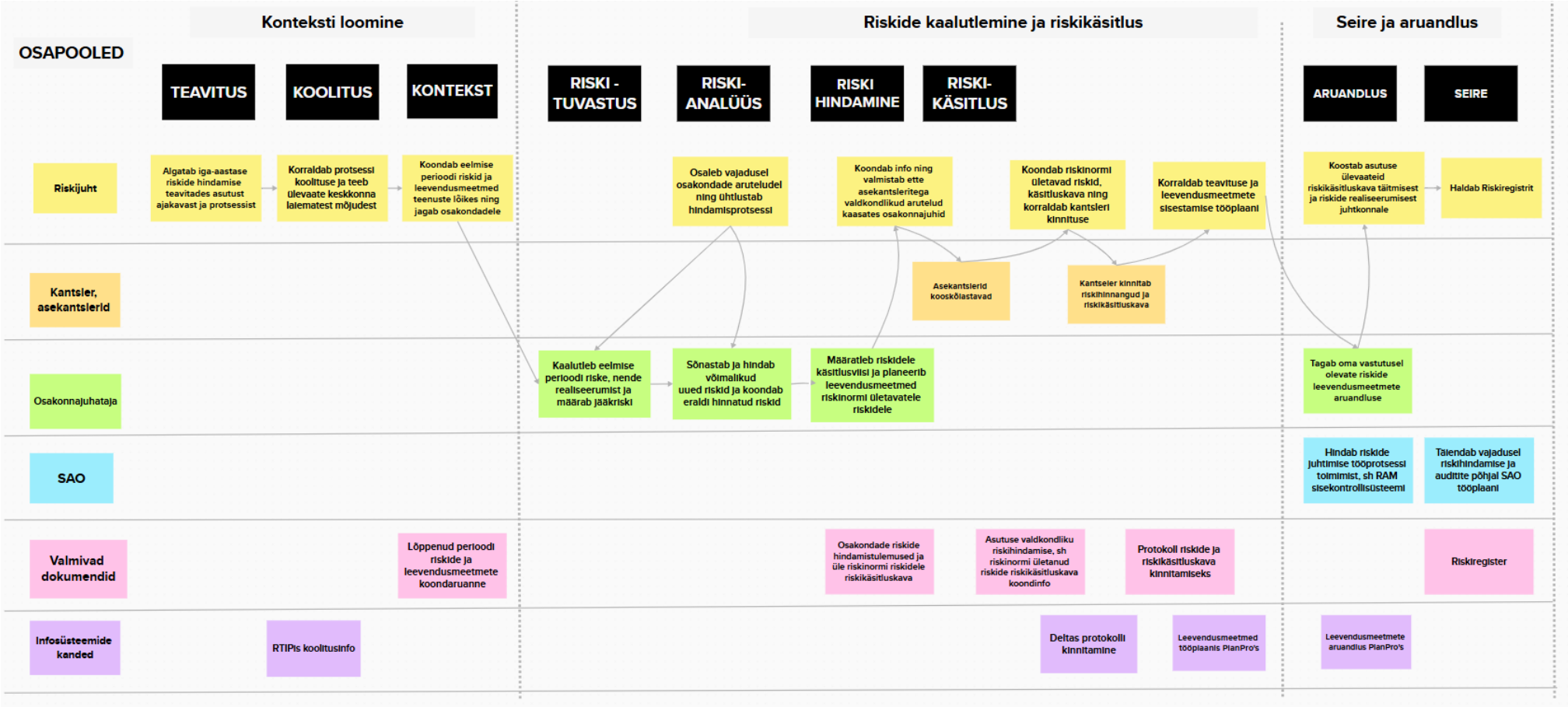
- 6.1. Asutuses peetakse riskiregistrit, mis on riskijuhtimise keskne töövahend.
- 6.2. Riskiregister sisaldab riskide ja nende käsitlemise andmeid vastavalt käesoleva korra lisa 1 struktuurile (vt Exceli tööleht „Riskihaldus“).
- 6.3. Peale riskihindamise ja riskikäsitluskava kinnitamist kantakse riskiregistris kirjeldatud riskinormi ületavate riskide leevendamistegevused edasi asutuse tegevuskava infosüsteemi.
- 6.4. Riskiregistri pidamise ja ajakohastamise eest vastutab RAM-i riskijuht, lähtudes riskijuhtimises kogutud teabest ning asutuse tegevuskava infosüsteemi andmetest. Riskiregister vaadatakse üle vähemalt kord aastas asutuseülese riskihindamise käigus ja ajakohastatakse.

7. Riskijuhtimise tööprotsessi tegevused ja rollijaotus

<i>Jrk</i>	<i>Vastutaja (ametikoht/roll/üksus)</i>	<i>Tegevuse kirjeldus</i>
7.1 ETTEVALMISTUS JA KONTEKSTI LOOMINE		
7.1.1	Riskijuht	Algatab iga-aastase riskide hindamise, saates osakonnajuhtidele teavituse koos ülesande, juhiste ja eelmise perioodi kokkuvõttega. Samuti korraldab riskijuhtimise koolituse ning teeb ülevaate keskkonnas laiemalt toimuvast, mis mõjutab riskide hindamist.
7.2 RISKIDE KAALUTLEMINE NING RISKIKÄSITLUS		
7.2.1	Osakonnajuhataja	Vaatab riskiomanikuna üle eelmisel perioodil hinnatud riskid ja nende käsitusviisid, analüüsides, kas riskid realiseerusid ja kas rakendatud meetmed olid piisavad ning hindab uuesti riski (jääkriski).
7.2.2	Osakonnajuhataja	Koondab punktis 2.4 ja peatükis 4 viidatud riskianalüüsides riskinormi ületavad riskid ning lisab planeeritud leevendusmeetmed.
7.2.3	Osakonnajuhataja	Sõnastab koostöös vajalike osapooltega võimalikud uued riskid, mis võivad ohustada seatud eesmärkide saavutamist ja planeeritud tegevuste elluviimist. Hindab määratletud riskide avaldumise tõenäosust ja mõju.
7.2.4	Osakonnajuhataja	Määratleb riskidele käsitusviisi ning asutuse riskinormi ületanud riskidele koostab riskikäsitluskava, määrates leevendamistegevused, vajaliku ressursi, tähtsajad ja vastutajad. Vajadusel teeb ettepanekuid riski aktsepteerimiseks, kui riskikäsitluse meetmete kulu ületab potentsiaalse kahju.
7.2.5	Riskijuht	Koondab osakondade määratletud riskid ning korraldab valdkondades hindamis- ja riskikäsitlusarutelud asekancleri ja osakonnajuhtidega.
7.3 RISIKIHINDAMISE TULEMUSTE JA RISIKIKÄSITLUSKAVA KINNITAMINE		
7.3.1	Riskijuht	Valmistab juhtkonnale ette riskihindamise tulemused ja riskikäsitluskava kinnitamiseks, vajadusel koondades või kategoriseerides riskid, mille mõju ulatub üle mitme osakonna või kogu asutuse.

Vastutav osakond: Strateegia- ja finantsosakond (SAFO)	Kinnitatud: kantsleri 25.07.2025 käskkirjaga nr 41
Protsessi koordinaator: Strateegia- ja finantsosakond, riskijuht	Versioon: 5

7.3.2	Juhtkond	Asekantslerid kooskõlastavad riskihindamise tulemused ja riskikäsitluskava ning kantsler kinnitab.
7.3.3	Riskijuht	Teavitab osakonnajuhte kinnitatud riskidest ja riskikäsitluskavast ning korraldab leevendamistegevuste sisestamise asutuse tegevuskava infosüsteemi. Haldab riskiregistrit.
7.4 SEIRE JA ARUANDLUS		
7.4.1	Osakonnajuhataja	Seirab oma valdkonnas asutuse riskinormi ületavaid riske ja nende leevendusmeetmeid ning raporteerib nende seisust asutuse tegevuskava infosüsteemis.
7.4.2	Riskijuht	Koostab asutuse tegevuskava infosüsteemist ülevaateid riskikäsitluskava täitmisest ja riskide realiseerumisest ning esitab need juhtkonnale. Haldab riskiregistrit.
7.4.3	SAO	Planeerib riskihindamise tulemuste ja siseauditi riskihinnangu põhjal SAO tööplaani siseauditid ja nõuandvad tööd.
7.4.4	SAO	Hindab siseauditite ja nõuandvate tööde käigus ning välisaudiitorite hinnangute põhjal RAM-i sisekontrollisüsteemi, sealhulgas riskide hindamise süsteemi toimimist erinevates valdkondades.
7.5 VAJADUSPÕHINE RISKIANALÜÜS		
7.5.1	Osakonnajuhataja	Algatab vajaduspõhise riskianalüüsi (sh vajadusel andmekaitsealase mõjuhinnangu) oma vastutusalas olevate muudatuste, teenuste või infosüsteemide puhul, kaasates riskijuhi.
7.5.2	Riskijuht	Vajadusel nõustab riskianalüüsi läbiviimist ning kaasab eksperdid vastavast valdkonnast. Korraldab riskianalüüsides tulemuste alusel riskinormi ületavate riskide integreerimise asutuse riskijuhtimisse.
7.5.3	Juhtkond	Valdkonna asekantsler kooskõlastab riskianalüüsi (sh vajadusel andmekaitsealase mõjuhinnangu) ning kantsler kinnitab.



Joonis 2. Riskijuhtimise tööprotsessi tegevused ja rollijaotus

Vastutav osakond: Strateegia- ja finantsosakond (SAFO)	Kinnitatud: kantsleri 25.07.2025 käskkirjaga nr 41
Protsessi koordinaator: Strateegia- ja finantsosakond, riskijuht	Versioon: 5

8. Kaasnevad dokumendid

Kaasnev dokument	Vastutaja	Asukoht	Säilitamise viis: paberil/ elektrooniliselt	Dok. tähis	Säilitustähtaeg
1. Riskihindamis- tulemused ja riskikäsitluskava	SAFO	DHS	Elektroonselt	1.1-8	Vastavalt dokumentide liigitusskeemile
2. Vajaduspõhised riskianalüüsid (sh andmekaitsealased mõjuhindangud)	SAFO	DHS	Elektroonselt	1.1-8	Vastavalt dokumentide liigitusskeemile

9. Mõisted

- 9.1. Riskijuhtimine - süsteemne ja koordineeritud tegevuste kogum, millega asutus juhib riskide haldust, nendega seotud otsuseid ja tegevusi eesmärkide saavutamiseks.
- 9.2. Riskihaldus on riskijuhtimise osa, mis keskendub konkreetsete riskide kaalutlemisele, tuvastamisele, hindamisele, leevendamisele ja seirele. Selle eesmärk on hoida riskid asutuse jaoks aktsepteeritaval tasemel.
- 9.3. Riskijuht - roll, kelle ülesanne on koordineerida riskijuhtimist organisatsioonis ning toetada juhtkonda ja üksusi riskide süsteemsel juhtimisel, sidudes riskijuhtimise strateegilise planeerimise ja aruandlusega.
- 9.4. Riskiomanik - roll, kelle vastutusalasse jääb riskist mõjutatud eesmärk, tegevusvaldkond või infovara ning kes vastutab riskikäsitluse eest, kaasates vajadusel teisi osapooli. Riskiomaniku rolli täidab tavaliselt teenuse, protsessi või infovara omanik (üldjuhul osakonnajuhataja).
- 9.5. Juhtkond – kantsler, asekanterid
- 9.6. Riski kaalutlemine - koondnimetus riskituvastuse, riskianalüüsi ja riski hindamise protsessidele.
- 9.7. Riskituvastus - riskiallikate (ohtude), sündmuste ning nende põhjuste ja võimalike tagajärgede kindlaks määramine.
- 9.8. Riski hindamine - riskianalüüsi tulemite ja riski kriteeriumide võrdlemine, eesmärgiga teha kindlaks, kas riskitase on talutav ning seeläbi aktsepteeritav.
- 9.9. Riskikäsitus - riski muutmise või kõrvaldamise või vältimise protsess, kus eelnevalt tuvastatud ja kategoriseeritud riskidele valitakse vastavad meetmed.
- 9.10. Riskikäsitluskava – riskide tuvastamise ja hindamise järgselt välja töötatud tegevusplaan riskikäsitluseks.
Riskikäsitusviis - riski suhtes ettevõetavate tegevuste haldamise viis.
- 9.11. Nõrkus - vara, süsteemi või protsessi kavandi, teostuse või käituse nõrk koht või puudus, mille kaudu riskiallikas võib tekitada tagajärgesid sündmuse.
- 9.12. Meede - abinõu, mis muudab riski, üldjuhul eesmärgiga seda vähendada.
- 9.13. Oht - võimaliku kahjustuse allikas.
- 9.14. Risk - määramatuse toime asutuse eesmärkidele. Väljendub sündmuse tekkimise tõenäosuse ja kahjutoime (tagajärgede) koosmõjuna. Eksisteerib relevantse ohu ning varaga seotud vastava nõrkuse olemasolul.
- 9.15. Võimalus - riski negatiivsele mõjule võib riskil olla ka positiivne mõju võimalusena, et toetada asutuse eesmärkide elluviimist.

Vastutav osakond: Strateegia- ja finantsosakond (SAFO)	Kinnitatud: kantsleri 25.07.2025 käskkirjaga nr 41
Protsessi koordinaator: Strateegia- ja finantsosakond, riskijuht	Versioon: 5

- 9.16. Riskitase - riski või riskide ühendi suurus, väljendatuna tagajärgede ja nende võimalikkuse kombinatsioonina.
- 9.17. Jääkrisk - pärast riskikäsitlust säiliv risk, mis jääb alles ka pärast olemasolevate või plaanitud kontrollimeetmete rakendamist.
- 9.18. Riskinorm - riskitase, mida organisatsioon soovib järgida või säilitada. Riskinorm määratleb organisatsiooni aktsepteeritava riskitaseme, mida ületades plaanitakse leevendusmeetmed.
- 9.19. Riski mõju - hinnanguline kahju suurus või ulatus, mida võib põhjustada konkreetse riski avaldumine asutuse eesmärkide saavutamisele.
- 9.20. Riski tõenäosus - riski realiseerimise võimalikkus ja sagedus.
- 9.21. Riskianalüüs - riski olemuse ja riskitaseme väljaselgitamine, arvestades tõenäosust, mõju ja olemasolevaid kontrollimeetmeid.
- 9.22. Riski mõjuvaldkond - kirjeldab, millist tüüpi tagajärgi riski realiseerumine võib kaasa tuua. See ei näita, kus risk tekib, vaid millele risk avaldab mõju. Mõjuvaldkonnad aitavad hinnata riski olulisust ja suunata sobivaid riskikäsitluse meetmeid.
- 9.23. Meede - abinõu, mis muudab riski (näiteks protsess, poliitika, vahend, tava või toiming).
- 9.24. Lisameede – täiendav abinõu, mida rakendatakse olemasolevate meetmete kõrval või kui risk suureneb.
- 9.25. Leevendusmeede - konkreetne samm või tegevus, mis viiakse ellu riski vähendamiseks.
- 9.26. Riskiregister - asutuse riskide ja nende käsitluste koondandmestik.
- 9.27. Infosüsteem - vahendite, inimeste, protsesside ja põhimõtete kogum, mille abil kogutakse, töödeldakse, säilitatakse ja väljastatakse andmeid ning mis koosneb erinevatest varadest, nagu riistvara, tarkvara, andmebaasid ja muud ressursid, mis toetavad infotöötlust.
- 9.28. Infoturvarisk - on infosüsteemide kasutamisel tekkida võivad riskid, mis ohustavad teabe konfidentsiaalsust, terviklust ja kättesaadavust ning mida hallatakse kooskõlas infoturbealaste nõuete ja standarditega.
- 9.29. Andmekaitsealane mõjuhinnang - protsess, mille käigus hinnatakse, kas kavandatav isikuandmete töötlemine võib põhjustada olulisi riske inimeste eraelu puutumatusele ning kirjeldatakse meetmeid nende riskide leevendamiseks.

Lisad

Lisa 1. Riskihalduse vorm