Kinnitatud
peadirektori käskkirjaga 27.10.2025 nr 1-1/25/49-1

IT ja infoturbe riskide haldamise kord (K34)

Protsess: IT ja infoturbe riskide haldamine

Protsessi omanik: infoturbe spetsialist

Versioon: 1

IT ja infoturbe riskide haldamise kord sisaldab:

1. Sissejuhatus ja dokumendi eesmärk

Käesolev kord kirjeldab IT ja infoturbe riskide haldamise protsessi Riigi Tugiteenuste Keskuses (edaspidi RTK) ning sätestab IT ja infoturbe riskide haldamise aluspõhimõtted. Käesolev kord on osa RTK infoturbe halduse süsteemist (edaspidi ISMS).

IT ja infoturbe riskide haldamise eesmärk on viia organisatsiooni tegevusega kaasnevad IT ja infoturbe riskid juhtkonnale aktsepteeritavale tasemele. Tõhus riskide haldamine suurendab juhtkonna kindlustunnet, et organisatsiooni eesmärgid saavutatakse. Käesolev kord toetab organisatsiooni üldist riskide haldamise protsessi, keskendudes IT ja infoturbe riskidele.

Käesoleva korra kaasajastatuna hoidmise eest vastutab RTK infoturbe spetsialist, kes vaatab korra perioodiliselt üle (vähemalt 1 kord aastas) ning teeb vajadusel täiendusi. Korra ja selle muudatused kinnitab RTK peadirektor.

2. Mõisted

- **Jääkrisk** on pärast riskikäsitlust säiliv risk.
- **Meede** on abinõu, mis muudab riski, üldjuhul eesmärgiga seda vähendada.

- **Nõrkus** on vara, süsteemi või protsessi kavandi, teostuse või käituse nõrk koht või puudus, mille kaudu riskiallikas võib tekitada tagajärjega sündmuse.
- **Oht** on võimaliku kahjustuse allikas.
- **RACI maatriks** kirjeldab igale rollile või isikule määratud vastutust projekti täitmisel.
- **Risk** on määramatuse toime organisatsiooni eesmärkidele. Väljendub sündmuse tekkimise tõenäosuse ja kahjutoime (tagajärgede) koosmõjuna. Eksisteerib relevantse ohu ning varaga seotud vastava nõrkuse olemasolul.
- **Riski hindamine** on riskianalüüsi tulemite ja riski kriteeriumide võrdlemine, eesmärgiga teha kindlaks, kas riskitase on talutav ning seeläbi aktsepteeritav.
- **Riski kaalutlemine** on koondnimetus riskituvastuse, riskianalüüsi ja riski hindamise protsessidele.
- **Riskianalüüs** on (eelnevalt tuvastatud) riski iseloomu ja riskitaseme väljaselgitamine.
- **Riskide haldamine** on omavahel kooskõlalised tegevused organisatsiooni suunamiseks ja juhtimiseks riski suhtes.
- **Riskikäsitlus** on riski muutmise või kõrvaldamise või vältimise protsess; riskide haldamise protsessi viimane järk, kus eelnevalt tuvastatud ja kategoriseeritud riskidele valitakse vastavad meetmed.
- **Riskinorm** on riskitase või tüüp, mida organisatsioon soovib järgida või säilitada.
- **Riskitase** on riski või riskide ühendi suurus, väljendatuna tagajärgede ja nende võimalikkuse kombinatsioonina.
- **Riskituvastus** on riskiallikate (ohtude), sündmuste ning nende põhjuste ja võimalike tagajärgede kindlaks määramine.

3. Vastutused ja rollid

RTK infoturbe spetsialist vastutab IT ja infoturbe riskide kaalutlemise läbi viimise ning infoturbe riskide haldamise protsessi toimimise eest. Teenuseomanik vastutab tema vastutusel oleva vara või protsessiga seotud tuvastatud riskide käsitluse eest riskiomaniku rollis. RTK juhtkond kinnitab riskide nimekirja ning aktsepteerib jääkriski.

Detailsemad IT ja infoturbe riskide haldamise protsessi rollid ja vastutused on esitatud allpool RACI maatriksis:

Tegevus	Infoturbe spetsialist	ISO juht	Kvaliteedijuht	Teenuse omanik	Tippjuhtkond
Riskide haldamise protsessi korraldamine	R	I	C	I	A
Riskikaalutlemise korraldamine	R	C	A	C	I
Riskide tuvastamine	R	C	A	C	I
Nõrkuste ja rakendatud meetmete tuvastamine	R	C	A	C	I
Riskide hindamise läbi viimine	R	C	A	C	I
Riskianalüüsi teostamine	R	C	A	C	I
Riskikäsitlusplaani koostamine ja teostamine	C	C	A	R	I
Riskide nimekirja kinnitamine	C	I	C	I	R/A
Jääkriski aktsepteerimine	C	I	C	I	R/A
Riskide nimekirjapidamine ja riskide monitooring	R	C	A	C	I
Riskidest raporteerimine	R	I	A	I	I

Tabel 1. Rollid ja vastutused RACI

- **Teostaja (*responsible – R*)** – täidab tööülesandeid. Igale ülesandele määratakse vähemalt üks isik.
- **Vastutaja (*accountable – A*)** – vastutab tegevuste täitmise eest. Ülesanne on juhtida ja kontrollida teostaja(te) tööd. Ühe ülesande jaoks ei tohiks olla rohkem kui üks vastutaja.
- **Nõustaja (*consulted – C*)** – jagab teavet ja/või annab nõu vastutajatele ja teostajatele. Nõustajaid võivad töö tulemused mõjutada ning nendega suheldakse kogu protsessi vältel.
- **Informeeritav (*informed – I*)** – teavitatakse otsustest ja töötulemustest kas teostaja või vastutaja poolt üldjuhul peale tegevuse lõpetamist.

4. IT ja infoturbe riskide haldamise ja riskide kaalutlemise läbiviimise põhimõtted

RTK poolt rakendatud ISMS põhineb Eesti infoturbe standardil (edaspidi E-ITS), mis on etalonturbepõhine. IT ja infoturbe riskide haldamisel tuginetakse E-ITS riskihaldusjuhendis väljatoodud metoodikale.

RTK on teostanud IT ja infoturbe riskidele etalonturbe välise riskianalüüsi E-ITS juurutamisel lähtudes organisatsiooni ametiprotsessidele määratud kaitsetarbest. Edaspidi viib RTK infoturbe spetsialist läbi perioodilist organisatsiooniülest IT ja infoturbe riskide kaalutlemist vähemalt kord aastas või vajadusel sagedamini (ametiprotsesside ja varade muudatuste või oluliste turvaintsidentide ilmnemise puhul). Riski kaalutlemise läbi viimisel lähtutakse käesoleva dokumendi peatükis 5 kirjeldatud metoodikast.

RTK infoturbe spetsialist koostab ja hoiab kaasajastatuna organisatsiooni IT ja infoturberiskide registrit, mille abil teostab riskide seiret ning uute riskide ilmnemisel või olemasolevate riskide muutmisel, täiendab riskiregistrit.

Infoturbe spetsialist raporteerib riskinormi ületavad riskid organisatsiooni kvaliteedijuhile, kes lisab neid organisatsiooniülesesse riskide nimekirja RTK riskidest täieliku ülevaate saamiseks.

RTK infoturbe spetsialist raporteerib RTK juhtkonnale organisatsiooni IT ja infoturbe riskidest vähemalt kord kvartalis, milles muuhulgas annab ülevaate riskikäsitlusplaanide täitmise ning ilmnenud uute riskide kohta.

Riskinorm

RTK aktsepteerib väga madala ja madala riskitasemega riske. Madalast kõrgema riskitasemega riskid suunatakse kohustuslikus korras riskikäsitlusse. Riskide nimekirja kinnitab ning jääkriske aktsepteerib RTK juhtkond.

Riskikäsitlusse suunatud riskile peab olema määratud riskiomanik, kelleks on üldiselt riskiga seotud vara või protsessi omanik, kes infoturbe spetsialistiga konsulteerides valib riskikäsitlusviisi ning koostab riskikäsitlusplaani.

RTK-s IT ja infoturberiskide käsitlemiseks kasutatakse järgnevaid käsitlusviise:

- **Vähendamine** – aktsepteeritud riskitaset (riski normi) ületava riski vähendamine lisaturvameetmete abil.
- **Aktsepteerimine** (säilitamine) – riski säilitamine samal tasemel, kui täiendavate riski vähendamise meetmete rakendamine osutub majanduslikult või muudel

põhjustel ebaotstarbekaks. Riskinormi ületavate riskide aktsepteerimine vajab detailse põhjenduse ning organisatsiooni juhtkonna kinnitust.

- **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.
- **Vältimine** – riski põhjustavast tegevusest loobumine.

IT ja infoturbe riskide kaalutlemisel lähtub RTK alljärgnevatest skaaladest ja riskimaatriksist:

Tõenäosus	Skaala	Aeg	Kirjeldus
(Peaaegu) kindel	5	Kuu	Riski avaldumine lähitulevikus on kindel.
Tõenäoline	4	6 kuud	Riski avaldumine lähitulevikus on tõenäoline, küsimus on ajas.
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.

***Tabel 2**. Riski realiseerumise tõenäosuse 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 pikaaegse katkemise või seab ohtu riigi julgeoleku või suure hulga inimeste elud või tekitab katastroofilisi tagajärgi keskkonnale või kriitilisi rahalisi kaotusi; • äärmiselt vaenulik avalikkuse ja meedia tähelepanu, mis kestab püsivalt kuid ning põhjustab klientide loobumise teenuse kasutamisest; • võivad tekkida pikaaegsed katkestused teiste teenuste toimimises või vahetu oht säärase olukorra tekkeks; • **teenus 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 teenuse olulise katkemise või seab ohtu riigi julgeoleku või põhjustab ohtu inimelule või keskkonnasaastet või väga olulisi rahalisi kaotusi; • märkimisväärne negatiivne avalikkuse tähelepanu, mis kestab nädalaid ning võib esile kutsuda klientide loobumise teenuse kasutamisest; • teiste teenuste pakkumine on oluliselt häiritud või on vahetu oht säärase olukorra tekkeks; • **teenus 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 teenuse toimepidevuse töös või põhjustab ohtu inimeste tervisele või keskkonnale või olulisi rahalisi kaotusi; • negatiivne tähelepanu, mis kestab päevi ning mis võib hiljem korduda; • häiritud võib olla teiste teenuste pakkumine või on vahetu oht säärase olukorra tekkeks; • **teenus 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 organisatsiooni funktsiooni täitmisele või märkimisväärseid rahalisi kaotusi; • negatiivne tähelepanu, mis on ajaliselt piiratud ühe päevaga; • **teenuse osutamine 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;

***Tabel 3**. Riski realiseerumisega kaasneva mõju skaala*

		Mõju				
Tõenäosus		**Vähetähtis - 1**	**Kerge - 2**	**Raske - 3**	**V. Raske - 4**	**Katastroofiline - 5**
	(Peaaegu) Kindel - 5	Madal - 5	Keskmine - 10	Kõrge - 15	V. Kõrge - 20	V. Kõrge - 25
	Tõenäoline - 4	V. Madal - 4	Madal - 8	Keskmine - 12	Kõrge – 16	V. Kõrge - 20
	Võimalik - 3	V. Madal - 3	Madal - 6	Keskmine - 9	Keskmine - 12	Kõrge - 15
	Vähetõenäoline - 2	V. Madal - 2	V. Madal - 4	Madal - 6	Madal – 8	Keskmine - 10
	V. Harv - 1	V. Madal - 1	V. Madal - 2	V. Madal - 3	V. Madal - 4	Madal - 5

***Tabel 4**. Riskimaatriks*

Riskiklass	Kirjeldus
Väga kõrge (20-25)	**Nõuab kohest reageerimist**. Lubamatu risk. Kui risk on hinnatud väga kõrgeks, vajab see viivitamatut tegutsemist 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 kiireloomulise 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 kasulikum kui riski aktsepteerimine.
Väga madal (1-4)	**Aktsepteeritakse**. Tühine risk. Turvameetmete rakendamine ei ole kohustuslik, kuid riski tuleb jälgida ja regulaarselt hinnata.

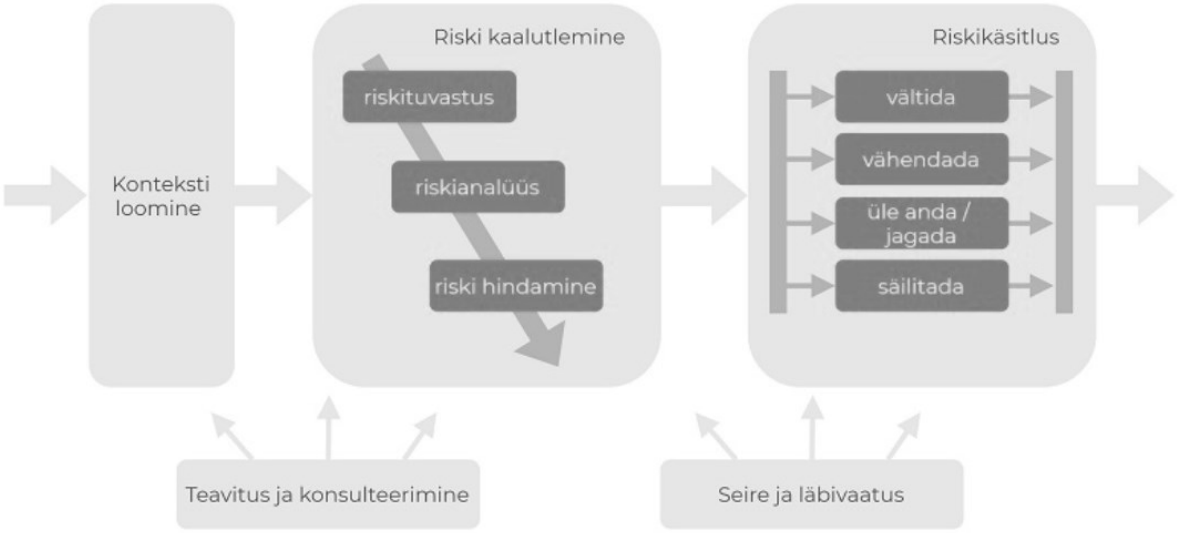
***Tabel 5**. Riski hindamise kriteeriumid*

5. IT ja infoturbe riskide kaalutlemise läbiviimise metoodika

RTK viib läbi IT ja infoturbe riskide kaalutlemist, tuginedes E-ITS riskihaldusjuhendis kirjeldatud metoodikale.

RTK infoturbe spetsialist teostab IT ja infoturbe riskide kaalutlemist vähemalt kord aastas või oluliste muudatuste korral (sh uute infosüsteemide kasutuselevõtt, uute IT lepingute sõlmimine ning IT lepingumuudatuste teostamine, uute projektide alustamine), tagamaks, et kõik riskid on tuvastatud, analüüsitud ja tehtud teatavaks juhtkonnale.

RTK IT ja infoturbe riskide kaalutlemise protsess koosneb kolmest sammust, milleks on 1) riskide tuvastamine, 2) analüüs ja 3) hindamine. Riskide kaalutlemise protsessi oluliseks sisendit andvaks eeltööks on konteksti loomine. Riski kaalutlemise väljund on sisendiks riskikäsitluse protsessile.



***Joonis 1**. E-ITS riskihalduse protsess*

5.1 Riski kaalutlemise protsessi eeltööd, ehk konteksti loomine

Kõikide RTK infosüsteemide puhul arvestab riskide kaalutlemine järgmisi seisukohti:

- IT ja infoturbe riskide haldamise protsessi ulatus (E-ITS rakendamisel võrdub kaitsealaga).
- Infosüsteemidele ja nendele tuginevatele ametiprotsessidele määratud kaitsetarve.
- Asjakohaste haavatavuste tuvastamine infosüsteemides, ametiprotsessides, ja infotöötlus asukohtades.
- Asjakohaste turvameetmete tuvastamine süsteemides ja infotöötlus asukohtades.
- Rakendatud turvameetmete efektiivsuse hindamine asjakohaste testimismeetodite abil (meetmete rakendamise läbivaatused, auditid, turvatestimised jne).

5.2 Riskide tuvastamine

Organisatsiooni riskituvastuse eesmärk on kindlaks määrata, mis võib põhjustada potentsiaalset kahju ja saada ülevaade kuidas, kus ja miks kahju võib tekkida. **Riskide tuvastamine hõlmab riske, olenemata sellest, kas nende allikas on RTK kontrolli all.** Allpool kirjeldatud RTK riskituvastuse protsessi sammud on sisendandmete kogumiseks järgnevale riskianalüüsi tegevusele.

a) Varade tuvastamine

RTK infoturbe spetsialist tuvastab IT ja infoturbe riskide kaitselasse kuuluvad varad ning hoiab varade nimekirja kaasajastatuna. E-ITS rakendamisel kasutatakse varade nimekirjana E-ITS sihtobjektide nimekirja. Varade tuvastamisel teevad koostööd IT juht, varade ja protsesside omanikud ning infosüsteemide peakasutajad. Protsessi koordineerib infoturbe spetsialist. Varade tuvastamine viiakse läbi organisatsioonile sobiva detailsuse tasemega. RTK rühmitab vajadusel sarnased varad riskianalüüsi protsessi sisendiks.

b) Ohtude tuvastamine

RTK infoturbe spetsialist tuvastab ja dokumenteerib kõik IT ja infoturbe riskihalduse ulatuses olevad ohud ja nende allikad, mis võivad mõjutada varasid, nagu organisatsiooni teave, protsessid ja infosüsteemid. Ohtude tuvastusel lähtub RTK E-ITS alusohtude kataloogist, millele vajadusel lisab infoturbe spetsialist asjakohased moodulispetsiifilised ohud. Vajadusel rühmitab RTK asjakohased ohud riskianalüüsi protsessi sisendiks.

c) Rakendatud turvameetmete tuvastamine

RTK infoturbe spetsialist on tuvastanud ja dokumenteerinud kõik olemasolevad ja kavandatavad turvameetmed, nende rakendamise ja kasutamise staatuse E-ITS infoturbe meetmete rakendamisplaanis (vajadusel ka E-ITS välised lisameetmed). Riskianalüüsi sisendiks vastandab RTK infoturbe meetmete rakendamisplaanis olevad meetmed ohtude tuvastuse sammus tuvastatud ohtudega, E-ITS alusohtude puhul kasutab RTK E-ITS alusohtude viitetabelit.

d) Nõrkuste tuvastamine

RTK infoturbe spetsialist tuvastab ja dokumenteerib nõrkused protsessides ja varades, mida võidakse ära kasutada, et põhjustada kahju varadele või organisatsioonile, ning mis soodustavad ohuga seotud riskistsenaariumite realiseerumist.

Risk eksisteerib kui on olemas asjakohase ohu ja seotud nõrkuse koosesinemine.

RISK = OHT x NÕRKUS

5.3 Riskianalüüs

RTK infoturbe spetsialist viib läbi riskianalüüsi, võttes arvesse teavet infovarade kriitilisusest, protsesside ja varade teadaolevatest nõrkustest (ka planeeritud aga rakendamata või osaliselt rakendatud meetmed), rakendatud meetmetest, varasematest organisatsioonis toimunud (turva)intsidentidest.

RTK teenusejuhid analüüsivad tuvastatud riske, kasutades kvalitatiivset meetodit. Lähtudes käesoleva dokumendi peatükis 4 välja toodud skaaladest, hinnatakse iga tuvastatud riski realiseerumise mõju (tagajärge) ning tõenäosust.

Tuvastatud riski realiseerumise tõenäosuse ja mõju alusel määratakse igale tuvastatud riskile riskiklass. Riskiklassi arvutamiseks kasutab RTK järgmist valemit:

RISKITASE = TÕENÄOSUS x MÕJU

5.4 Riskide hindamine

RTK hindab ja prioriseerib IT ja infoturbe riske lähtudes riski hindamise kriteeriumitest ja riskimaatriksist, mis on välja toodud käesoleva dokumendi peatükis 4.

Riskinormi piires olevad riskid aktsepteeritakse, riskinormi ületavad riskid suunatakse riskikäsitlusse. RTK riskinormi kirjeldus on välja toodud käesoleva dokumendi peatükis 4.

5.5 Riskikäsitlus

Kõikidele riskikäsitlusse suunatud riskidele määratakse riskiomanik (üldjuhul teenuse omanik). Riskiomanik määrab riskikäsitlusviisi, lähtudes peatükis 4 välja toodud

nimekirjast ning koostab detailse riskikäsitlusplaani. Riskikäsitlusplaan sisaldab rakendatavad lisameetmed, täiendava ressursikulu hinnangut (vajadusel) ning tegevuste täitmise tähtaega. Riski aktsepteerimise ettepaneku tegemisel lisab riskiomanik detailse põhjenduse.

Riskikäsitlusplaani kinnitab ning riski aktsepteerimisele lõpliku otsuse langetab RTK juhtkond.

RTK infoturbe spetsialist analüüsib ja hindab jääkriski, mis säilib peale riskikäsitluse läbi viimist ja riskikäsitlusplaani rakendamist. Tõhusa riskikäsitluse eesmärk on viia risk organisatsioonile aktsepteeritavale tasemele.