MAJANDUS- JA
KOMMUNIKATSIOONI-
MINISTEERIUM

KÄSKKIRI

19.02.2025 nr 8

Majandus- ja Kommunikatsiooniministeeriumi riskijuhtimise kord

Vabariigi Valitsuse 23. oktoobri 2002. a määruse nr 323 „Majandus- ja Kommunikatsiooniministeeriumi põhimäärus“ § 25 lõike 2 punkti 3 alusel kinnitan „Majandus- ja Kommunikatsiooniministeeriumi riskijuhtimise korra“ (lisatud).

(allkirjastatud digitaalselt)
Ahti Kuningas
kantsler

KINNITATUD
kantsleri 19.02.2025 käskkirjaga nr 8
Lisa

MAJANDUS- JA KOMMUNIKATSIOONIMINISTEERIUMI RISKIJUHTIMISE KORD

1. Üldpõhimõtted

1.1.1 Riskijuhtimise korra (edaspidi *kord*) eesmärk on kehtestada Majandus- ja Kommunikatsiooniministeeriumi (edaspidi MKM) ühtsed reeglid riskijuhtimise korraldamiseks. Riskijuhtimise eesmärk on viia organisatsiooni tegevusega kaasnevad riskid juhtkonnale aktsepteeritava tasemeni.
1.1.2 Korra nõuded lähtuvad riskijuhtimise valdkonna spetsiifikast, rahvusvahelistest ja riigisisestest regulatsioonidest ning valdkonna parimast praktikast ning on kooskõlas MKM-is rakendatava infoturbestandardiga.
1.1.3 Riskihalduse tagamisel ja rakendamisel tuleb, nii palju kui võimalik, lähtuda kohustuste lahususe põhimõttest.
1.1.4 Korra täitmist korraldab infoturbejuht või kantsleri nimetatud isik.

1.2 Riskijuhtimise korraldamise eelduseks on, et turvameetmed kõigest vähendavad turvariski. Seega on tõenäoline, et andmete terviklus, käideldavus või konfidentsiaalsus saavad kahjustada. Infosüsteemi turvalisus loetakse piisavaks, kui jääkrisk on MKM-i jaoks aktsepteeritaval tasemel võrreldes varade väärtusega ja turvameetmete maksumusega. Kui infosüsteemi funktsionaalsus on MKM-i tegevuses kriitilise tähtsusega, infosüsteemi asendus- ja arenduskulud on ebamõistlikult suured või kui infovarasid ähvardab kõrge risk, viiakse vajadusel läbi detailne riskianalüüs.

1.3 MKM tagab kõikide enda käsutuses olevate infovarade kaitse vastavalt ohtude realiseerumise tõenäosusele ja kaitstavate varade väärtusele.

1.4 MKM-i riskide koordineerimise eest vastutab riskijuht või kantsleri nimetatud isik.

1.5 MKM rakendab oma ülesannete täitmiseks turvameetmeid, mis on majanduslikult põhjendatud ning proportsionaalsed kaitstavate infovarade turvaklassiga.

1.6 MKM-i infovarade haldamise eest vastutavad välised koostööpartnerid ja MKM-i infovarad on kirjeldatud koostööpartnerite infovarade haldamise süsteemides. Kõigi infovarade kohta on koostatud infovarade loend.

1.7 MKM rakendab riskide vähendamiseks Eesti infoturbestandardi (edaspidi E-ITS) turvameetmeid vastavalt infovaradele määratud turvaklassile ja E-ITS rakendusjuhendile. Kui mõnda E-ITS turvameedet ei ole võimalik või otstarbekas täita, rakendab MKM alternatiivseid meetmeid (lisaturvameetmed) riski maandamiseks või aktsepteerib kantsler kirjalikult meetme.

1.8 Kantsler, lähtuvalt riskide hindamisest, võtab vastu kirjalikke otsuseid riskide maandamiseks ja aktsepteerib jääkriskid. Riski aktsepteerimiseks või maandamiseks teeb kirjaliku ettepaneku riskiomanik.

1.9 Käesolevas korras kasutatud mõisted ja rollid on kirjeldatud E-ITS kodulehel, mis on kättesaadav aadressil: https://eits.ria.ee/et/abimaterjalid/seletav-soonaraamat.

2. Kasutusulatus ja vastutus

Riskijuhtimise kord on täitmiseks kõigile MKM-i ametnikele ja töötajatele, praktikantidele, lepingu alusel teenust osutavatele isikutele ning kõigile teistele isikutele, kes osalevad MKM-i töös ja kehtib kõikides MKM-i füüsilistes asukohtades. Käesoleva korra sätteid kohaldatakse ka rakenduste, registrite, andmekogude ja andmebaaside (edaspidi *välised rakendused*) kasutamise korral, kui vastavate väliste rakenduste kasutamise kordades või põhimäärustes ei ole sätestatud teisiti.

3. Riskihaldus

3.1 Riskihaldus on terviklik protsess (lisa 2), mis tagab asjakohase infoturvariskidega tegelemise MKMis.

3.2. Riski kaalutlemine – kogu riskituvastuse, riskianalüüsi ja riski hindamise protsess tervikuna:
3.2.1 riskituvastus – riskide kaardistamine. Eesmärk on leida nõrkused ja ohud, millel on mõju MKM-i äriprotsessidele või varadele. Tuvastamisel kasutatakse E-ITS etalonturbe alusohtude kataloogi (kättesaadav E-ITS). Riskide loetelus esitatakse riskide kirjeldus koos tuvastatud nõrkuste ja ohtudega;
3.2.2 riskianalüüs – protsess riski iseloomu väljaselgitamiseks ja riskitaseme määramiseks. Tuvastatud riskidele määratakse kaalukus riskimaatriksi (lisa 1) abil. Tõenäosuse ja tagajärgede koosmõju väljendatakse riskimaatriksi abil leitud kaalukuse hinnanguga;
3.2.3 riski hindamine – riskianalüüsi tulemite ja riski kriteeriumite võrdlemise protsess eesmärgiga teha kindlaks, kas risk ja/või selle suurus on aktsepteeritav või talutav. MKM koostab riskide loetelu koos riskiomaniku otsusega riski käsitlemiseks või säilitamiseks. Vajadusel määratakse riskide käsitlemise prioriteet. Riskinormist väiksema riski korral riski käsitlemisel lisaturvameetmeid ei ole vaja määrata (risk aktsepteeritakse).

3.3. Riskikäsitlus – riski muutmise protsess, mis tegeleb iga riskiga eraldi ning määrab meetmed kahju vähendamiseks:
3.3.1 turvameetmete valimine riskikäsitluseks – riski käsitlemiseks määratakse lisaturvameetmed, mis aitavad riski muutes saavutada riskinormile vastava taseme. Sobiva etalonturbe kataloogi mooduli olemasolul kasutatakse lisaturvameetmete määramisel selle kõrgmeetmeid lähtuvalt infoturbe põhikomponentidest (C-I-A ehk konfidentsiaalsus, terviklus, käideldavus);
3.3.2 iga turvameetme kulude võrdlus eeldatava kahjuga või otsese väärtusega ja otsus meetme teostuse poolt või vastu – lõplik turvameetmete koosmõju, kulukuse jm aspektide hindamine ning jääkriskide aktsepteerimine toimub etalonturbe protsessis turvameetmete kinnitamise sammus;
3.3.3 turvameetmete rakendamine – soovitud riskitaseme saavutamiseks võib olla tarvilik rakendada rohkem kui ühte lisaturvameedet (nt võib ka tuvastatud riski taseme astet vähendada). Kõige otstarbekamaks võib erandjuhtudel osutuda riski säilitamine samal tasemel;
3.3.4 jääkriskide uurimine, käsitlusvariantide määratlemine – kas aktsepteerimine on talutav riskiomaniku ja kantsleri poolt.

3.4. Riskide seire ja aruandlus – turvameetmete või käsitlusvariantide korrigeerimine käituse vältel.

4. Riskiregister

4.1 MKM dokumenteerib teadaolevad riskid koos ohtude ja nõrkustega MKM-i sisemise töökorralduse vajadusteks loodud riskiregistris, mida peetakse elektroonilises halduskeskkonnas.

4.2 Seire korral kasutatakse riskide seisust ülevaate saamiseks riskiregistrit.

4.3 Riskiregistri osaks on 4x4 riskimaatriks (lisa 1).

4.4 Aktsepteeritud riskid on riskimaatriksis rohelised, nendele ei ole vaja lisaturvameetmeid määrata.

4.5 Keskmised riskid on riskimaatriksis kollased, mille puhul on otsustatud, millised neist on aktsepteeritud ning milliste puhul on määratud lisaturvameetmed.

4.6 Riskinormist suuremad riskid on riskimaatriksis oranžid ja punased ning neile on määratud lisaturvameetmed.

5. Riski seire

5.1 Riskijuht või kantsleri nimetatud isik vaatab riske üle perioodiliselt (vähemalt kord aastas), kuna riski tase võib ajas muutuda ning tuua kaasa vajaduse täiendavaks riskianalüüsiks. Riskide seiramisel hinnatakse ka riskikäsitluse käigus määratud meetmeid, mille efektiivsus võib ajas muutuda.

5.2 Riskide seire hõlmab pidevat tagasisidet infoturbeintsidentidest.

5.3 Riske seiratakse kasutades ministeeriumisisest riskiaruandlust. Riskidega tegelevad osakonnad (nt rakendavad meetmeid) protokollivad/dokumenteerivad protsesside seisu analüüsimiseks.

5.4 Riskide seire käigus teostatakse:
5.4.1 infoturbemeetmete ajakohastamist;
5.4.2 regulatsioonide ja dokumentatsiooni perioodilist läbivaatust;
5.4.3 töökeskkonna regulaarset seiret;
5.4.4 infoturbe valdkonda või MKM-i töökeskkonda puudutavatele muudatustele reageerimist;
5.4.5 infoturbeintsidentide analüüsi;
5.4.6 auditeerimist.

6. Riskianalüüs

6.1 MKM-i tegevust kahjulikult mõjutada võivate toimingute ja sündmuste pidevaks hindamiseks teostatakse riskianalüüse.

6.2 Riskianalüüsi viib läbi riskijuht infoturbejuhi või kantsleri nimetatud isiku korraldusel.

6.3 Riskianalüüsi tuleb teostada vähemalt üks kord aastas ja enne igat suuremat muudatust IT-keskkonnas (nt intsidendid).

6.4 Riskianalüüs viiakse läbi vastavalt käesolevale korrale.

6.5 MKM-i riskihaldus põhineb ISO 27005 standardil ja E-ITS kolmastmelise etalonturbe metoodikal.

6.6 Riski vähendamiseks rakendatakse E-ITS turvameetmeid vastavalt infovaradele määratud turvaklassile ja E-ITS rakendusjuhendile.

6.7 Riskide puhul hinnatakse selle esinemise tõenäosust, tagajärgede mõju, likvideerimise kulu ja riski maandamise kulu. Maandatakse riskid, mis tõenäoliselt juhtuvad (4-punkti skaalal 2 või enam) või mille tagajärgede mõju likvideerimise kulu on suurem riski maandamise kulust. Juhtkonna otsusega on lubatud aktsepteerida riski, mis juhtkonna hinnangul on väikese tõenäosusega (4-punkti skaalal 1) või mille maandamiseks pole asutusel eelarvet. Viimasel juhul kaalutakse alternatiivseid riski vähendamise võimalusi.

6.8 Riskianalüüsiga määratakse riskisündmustele astmelised hinnangud: a) tõenäosus; b) tagajärjed. Tõenäosuse ja tagajärgede koosmõju väljendatakse riskimaatriksi (lisa 1) abil leitud kaalukuse hinnanguga.

Riskimaatriks

		TAGAJÄRG			
TÕENÄOSUS		**Kerge (A)**	**Raske (B)**	**Väga raske (C)**	**Katastroofiline (D)**
	Väga suur (4)	Keskmine **(R^3)**	Kõrge **(R^4)**	Väga kõrge **(R^5)**	Väga kõrge **(R^5)**
	Suur (3)	Madal **(R^2)**	Keskmine **(R^3)**	Kõrge **(R^4)**	Väga kõrge **(R^5)**
	Keskmine (2)	Madal **(R^2)**	Keskmine **(R^3)**	Kõrge **(R^4)**	Kõrge **(R^4)**
	Väike (1)	Madal **(R^2)**	Madal **(R^2)**	Keskmine **(R^3)**	Kõrge **(R^4)**

MAJANDUS- JA KOMMUNIKATSIOONIMINISTEERIUMI RISKIJUHTIMISE KORD
Lisa 2

Protsessijoonis