TERVIKTEKST
03.04.2025 käskkiri nr 24 (esialgne)
13.06.2025 käskkiri nr 40 (muudatus)
01.12.2025 käskkiri nr 90 (muudatus)

JUSTIITS- JA DIGIMINISTEERIUM

MINISTRI KÄSKKIRI

Toetus riikliku küberturvalisuse tugevdamiseks

Käskkiri kehtestatakse Vabariigi Valituse 29.09.2022 protokollilise otsuse nr 58 päevakorrapunkti 8 otsustuspunktide 1 ja 5 alusel ning kooskõlas Vabariigi Valitsuse 31.07.2014 määrusega nr 123 „Vabariigi Valitsuse reservist vahendite eraldamise ja eraldatud vahendite kasutamise kord“ (edaspidi *määrus*).

1. Reguleerimisala ja eesmärk

1.1. Käskkirjaga reguleeritakse sihtotstarbelise reservi info- ja kommunikatsioonitehnoloogia (edaspidi *IKT*) küberturvalisuse probleemide lahendamiseks toetuse andmise ja kasutamise tingimusi ja korda (edaspidi *meede*).

1.2. Toetusega panustatakse Küberturvalisuse strateegia 2024–2030 „Läbivalt IT-vaatlikum Eesti“ ja riigieelarve seaduse § 20 lõike 4 kohaselt kinnitatud digiühiskonna programmi tulemuste saavutamisesse.

1.3. Käskkirja rakendamisega panustatakse Riigikogu 12.05.2021. a otsuse „Riigi pikaajalise arengustrateegia „Eesti 2035“ heakskiitmine“ aluspõhimõtete hoidmisesse ning strateegilise sihi „Riigivalitsemine“ saavutamisse, hoolitsedes selle eest, et digitaalse ühiskonna küberriskid oleksid hästi hallatud ning Eesti küberruum kõrge usaldusväärsusega.

1.4. Toetuse andmise eesmärk on Eesti ühiskonna toimimise seisukohast oluliste erakorraliste ja kriitiliste võrgu- ja infosüsteemide küberintsidentide ja -ohtude kiire leevendamine, kahjulike mõjude minimiseerimine ning nende ennetamine.

2. Meetme rakendamine

2.1. Meetme väljatöötamise ja rakendamise, sh taotlusvoorude väljakuulutamise ning läbiviimise, sh taotluste menetlemise, eest vastutab Justiits- ja Digiministeeriumi riikliku küberturvalisuse talitus (edaspidi RKT).

2.2. Taotlusi toetuse väljamaksmiseks menetleb ja toetuse väljamakseid teeb Rahandusministeerium RKT otsuse ja määruse § 3 lõike 3 alusel.

3. Mõisted

3.1. Kübersündmus on iga intsident või toiming, mis leiab aset võrgu- ja infosüsteemis või digitaalses keskkonnas ning millel on mõju võrgu- ja infosüsteemi käideldavusele, autentsusele, terviklusele ja konfidentsiaalsusele. Kübersündmusena käsitletakse meetmes nii tahtlikku kui tahtmatut punktides 3.2. ja 3.3. nimetatud küberintsidenti või tarkvaralist toimingut.

3.2. Küberintsident on süsteemis toimuv sündmus, mis ohustab või kahjustab süsteemi turvalisust.

3.3. Tarkvaraline toiming on tarkvara või andmeid sisaldava riistvara mittetoimimine ning veebilehe või teenuse ootamatu katkestus.

3.4. Küberrisk on küberintsidendist tingitud kahju või häire võimekus, mida tuleb väljendada sellise kahju või katkestuse ulatust ja kõnealuse küberintsidendi esinemise võimalikkust arvesse võtva kombineeritud näitajana.

3.5. Partner on määruse §-s 2 nimetatud riigiasutus, kes osaleb toetatavas tegevuses ja kellel tekivad selle käigus kulud.

4. Toetatavad ja mittetoetatavad tegevused

4.1. Erakorraliste ja kriitiliste kübersündmuste lahendamise taotlusvooru raames toetatakse:
4.1.1. erakorralise kübersündmuse tulemusena tekkinud olukorra lahendamist;
4.1.2. taotlusele eelnenud 12 kuu jooksul avastatud kriitilise turvanõrkuse (zeroday – kriitiliste null-päeva turvanõrkuste) ja küberintsidendi mõju ärahoidmist;
4.1.3. ootamatute küberriskide eskaleerumise (näiteks olulise mõjuga küberintsidendid, tarneahela risk, ilmnenud seos riskiriigiga) vältimist;
4.1.4. taotlusele eelnenud 12 kuu jooksul toimunud kriitilise küberintsidendi järelmite lahendamist, kui tegevus ei ole edasilükatav ega rahastatav muudest kinnitatud eelarvetest.

4.2. Punktis 4.1. nimetatud projektide raames toetatakse muuhulgas järgmisi tegevusi:
4.2.1. tarkvara ja riistvara komponentide turvauuendus või väljavahetus;
4.2.2. olemasolevate või uute kesksete skaleeritavate lahenduste kasutuselevõtmine;
4.2.3. lahendused, mis hoiavad ära oluliste ühiskondlike funktsioonide häirimist, näiteks riigi e-teenuste toimimist või kahjustavad majandusliku ja kodanike heaolu.

4.3. Punktis 4.1. nimetatud projektide raames ei toetata järgmisi tegevusi, välja arvatud kui need on kübersündmuse lahendamise parimad lahendused:
4.3.1. koolituste ettevalmistamist ja läbiviimist;
4.3.2. töötajate värbamist ja töötasude maksmist;
4.3.3. teenuse, toote, tarkvara elukaare planeerimist;
4.3.4. teenuse, toote, tarkvara tavapärase toimepidevuse tagamist ja haldust;
4.3.5. püsikulusid, sh püsivaid majandamiskulusid;
4.3.6. litsentside uuendamist ja kallinemist;
4.3.7. *kehtetu* (*muudetud 01.12.2025 käskkirjaga nr 90*).
4.3.8. puuduliku riskianalüüsi või Eesti Infoturbestandardi (või ISO/IEC 27001) kohuslasena selle rakendamata jätmise tagajärgi;
4.3.9. Riigi Infosüsteemi Ameti (*edaspidi* RIA) turvaohu teavitusele mittereageerimise tagajärgi.

4.3[1]. Punktis 4.1. nimetatud projektide raames ei toetata lunaraha maksmist.

4.4. Oluliste ühiskondlike funktsioonide häiringute ennetamise taotlusvooru raames toetatakse:
4.4.1. turvaauditi tulemuste rakendamist ulatusliku positiivse mõju tagamiseks;
4.4.2. koolitused ja õppused küberkriisi ennetamiseks;
4.4.3. tegevusi kriitilise küberturvalisuse ohu ärahoidmiseks või toimunud kriisijuhtumi mõju lõpetamiseks;
4.4.4. infoturbe halduse süsteemi meetmete rakendamist;
4.4.5. taakvara väljavahetamist.

4.5. Punktis 4.4. nimetatud projektide raames ei toetata järgmisi tegevusi:
4.5.1. litsentside uuendamist ja kallinemist;
4.5.2. Eesti infoturbestrandardi (või ISO/IEC 27001) rakendamise konsulteerimist ja auditeerimist;
4.5.3. personali värbamist ja töötasude maksmist;
4.5.4. ühiskondliku mõjuta teenuse, toote, tarkvara elukaare planeerimist.

5. Projekti kestvus

5.1. Punktis 4.4 sätestatud projekti maksimaalne kestvus on jooksva kalendriaasta 31. detsember.

5.2. Punktis 5.1 sätestatud projekti maksimaalset kestvust võib RKT põhjendatud juhul pikendada. Pikenduse eelduseks on toetuse saaja põhjendatud taotlus.

6. Toetuse suurus

6.1. Taotlusvooru avamisest antakse potentsiaalsetele taotlejatele e-posti teel teada meetme taotlusvooru eelarve maht.

6.2. Toetuse minimaalne suurus projekti kohta on 15 000 eurot.

6.3. Toetuse maksimaalne suurus on taotlusvooru eelarve maht.

6.4. Punkti 4.1 projektil kohustuslik omafinantseering puudub.

6.5. Punkti 4.4. projekti minimaalne omafinantseeringu määr on 10% projekti maksumusest.

7. Kulude abikõlblikkus

7.1. Abikõlblikud on projekti kestvuse jooksul tehtud põhjendatud kulud.

7.2. Kulu loetakse põhjendatuks, kui kulu on sobiv, vajalik ja tõhus taotluse rahuldamise otsuses toodud tulemuse saavutamiseks ning see tekib taotluse rahuldamise otsuses nimetatud toetatavate tegevuste käigus.

7.3. Kulu abikõlblikkuse üle otsustab RKT.

8. Nõuded taotlusele

8.1. Ministeerium ja Riigikantselei saavad esitada ühe koondtaotluse oma valitsemis- ja haldusala ja valdkonna jaoks.

8.2. Riigikogu Kantselei, Vabariigi Presidendi Kantselei, Riigikontroll, Õiguskantsleri Kantselei ning Riigikohus enda ja oma haldusala asutuse jaoks saavad esitada ühe koondtaotluse.

8.3. Taotluses esitatakse vähemalt järgmine teave:
8.3.1. taotleja ja partneri(te) andmed;
8.3.2. projekti eesmärk;
8.3.3. projekti tegevuste kirjeldus;
8.3.4. teave projekti peamiste sihtrühmade ja nende suuruse kohta;
8.3.5. teave projekti tulemuste jätkusuutlikkuse kohta, sealhulgas projekti jätkutegevuste kohta pärast projekti lõppu;
8.3.6. projekti ajakava;
8.3.7. projekti eelarve, sealhulgas kulude loetelu tegevuste ja alategevuste kaupa;
8.3.8. taotletav toetuse summa;
8.3.9. projekti omafinantseeringu suurus ja allikad;
8.3.10. teave, kui taotleja on projektile või projekti tegevustele taotlenud toetust samal ajal muudest riigieelarvelistest, Euroopa Liidu või muudest välisabi toetusmeetmetest;
8.3.11. teave selle kohta, mis vahenditest kaetakse taotluseobjekti edasised haldus- ja arenduskulud projekti elluviimise järel;
8.3.12. taotluse hindamiseks vajalik muu teave.

8.4. Punktis 4.4. nimetatud taotlusega koos tuleb esitada projekti elluviija täidetud RIA F4SLE infoturbe küpsushindamise tulemuse.

9. Taotluse esitamine ja menetlemine

9.1. Taotluse saab esitada taotleja seaduslik esindaja RKT e-postile kybertoetus@justdigi.ee taotlusvoorus ette antud taotlusvormil:
9.1.1. punktis 4.1. nimetatud taotlusvoorus võetakse taotlusi vastu jooksvalt nende saabumise järjekorras, aga hiljemalt 12 kuu jooksul erakorralise ja kriitilise kübersündmuse toimumisest või muu erakorralise küberohu avastamisest.
9.1.2. punktis 4.4. nimetatud taotlusi võetakse vastu taotlusvooru tähtpäevaks.

9.2. Taotluste vastuvõtmise alustamisest ning taotlusvooru tähtajast teavitab RKT määruse §-s 2 nimetatud riigiasutuste e-posti aadressidele ning Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu listi e-posti kaudu.

9.3. Taotluse menetlemine koosneb taotluse ja taotleja nõuetele vastavuse kontrollist, taotluse hindamisest ning taotluse rahuldamisest, osalisest või kõrvaltingimustega rahuldamisest või rahuldamata jätmisest.

9.4. RKT võib taotluse menetlemise käigus nõuda taotlejalt selgitusi ja lisadokumente taotluses esitatud teabe kohta, samuti taotluse täiendamist või muutmist, kui leiab, et taotlus ei ole piisavalt selge või selles esinevad puudused.

9.5. Punktis 4.1. nimetatud taotlus võetakse menetlusse jooksvalt ning vaadatakse läbi ja tehakse otsus esimesel võimalusel, aga hiljemalt seitsme tööpäeva jooksul taotluse esitamisest arvates (*muudetud 13.06.2025 käskkirjaga nr 40*).

9.6. Punktis 4.4. nimetatud taotlused võetakse menetlusse taotlusvooru väljakuulutamisest alates ning otsus tehakse hiljemalt 15 tööpäeva jooksul taotlusvooru tähtpäevast arvates.

9.7. Kui taotluses avastatakse puudusi, teatatakse sellest viitamata taotlejale ja antakse puuduste kõrvaldamiseks üldjuhul mitte rohkem kui viis tööpäeva, mille võrra pikeneb taotluse menetlemise tähtaeg.

10. Taotluste hindamine, hindamiskriteeriumid ja -metoodika

10.1. Nõuetele vastavaid taotlusi hindab kantsleri käskkirjaga moodustatud hindamiskomisjon, kuhu kuulub ka Riigi Infosüsteemi Ameti esindaja(d). Vajadusel kaasatakse teisi eksperte.

10.2. Hindamiskomisjoni liikmed peavad deklareerima oma erapooletust ja sõltumatust hinnatavatest projektidest, taotlejatest ja partneritest.

10.3. Punktis 4.1. nimetatud taotlused hinnatakse lisas 1 sätestatud hindamismetoodika alusel.

10.4. Punktis 4.4. nimetatud taotlused hinnatakse lisa 2 sätestatud hindamismetoodika alusel.

11. Taotluse rahuldamine, osaline rahuldamine, kõrvaltingimustega rahuldamine või rahuldamata jätmine

11.1. RKT otsus taotluse rahuldamiseks, osaliseks rahuldamiseks ja kõrvaltingimustega rahuldamiseks on aluseks Rahandusministeeriumile taotluse esitamiseks reservist vahendite eraldamiseks.

11.2. RKT otsused vormistatakse protokollina.

11.3. RKT jätab taotluse rahuldamata, kui taotleja või taotlus ei vasta nõuetele ning puudusi ei kõrvaldata või taotluse rahuldamise kõrvaltingimusi ei täideta RKT määratud ajal või kui taotleja ei nõustu taotluse osalise või kõrvaltingimustega rahastamise ettepanekuga.

11.4. Teave taotluse rahastamise või rahastamata jätmise kohta saadetakse taotlejale esimesel võimalusel taotluses näidatud e-posti aadressile.

12. Toetuse saaja kohustused

12.1. Toetuse saaja kohustub:
12.1.1. tagama taotluses ja taotluse rahuldamise otsuses sätestatud tingimuste täitmise;
12.1.2. tagama otsuses ette nähtud omafinantseeringuks vajalike vahendite olemasolu;
12.1.3. esitama RKT poolt ette nähtud vormis, viisil ja tähtaja jooksul nõutud teabe;
12.1.4. kooskõlastama RKT-ga projekti tegevuste muutmise enne nende muudatuste tegemist;
12.1.5. teavitama RKT-d ning tagastama Rahandusministeeriumile eraldatud toetuse juhul, kui seda kasutati taotlusest või taotluse rahuldamise otsusest teistel eesmärkidel või teistele tegevustele.

(allkirjastatud digitaalselt)

Liisa-Ly Pakosta
Justiits- ja digiminister

KINNITATUD

Justiits- ja Digiministri 03.04.2025 käskkirjaga 24
Lisa 1

ERAKORRALISTE JA KRIITILISTE KÜBERSÜNDMUSTE LAHENDAMISE TAOTLUSVOORU HINDAMISMETOODIKA

1. Taotluste hindamine

1.1. Nõuetele vastavaid taotlusi hindab käskkirja punktis 10.1. nimetatud hindamiskomisjon, kaasates vajadusel teisi eksperte.

1.2. Hindamiskomisjon hindab nõuetele vastavaid taotlusi järgmiste hindamiskriteeriumite alusel:

nr	Hindamiskriteeriumid	JAH / EI
1	Taotluse eesmärgi asjakohasus	
2	Probleemi erakorralisus ja kriitilisus	
3	Taotluse rahastamata jätmise tagajärjed	

1.3. Hindamiseks esitab RKT hindamiskomisjoni liikmetele:
1.3.1. taotluse;
1.3.2. hindamismetoodika;
1.3.3. hindamislehe;
1.3.4. hindamise seisukohast olulise muu teabe.

1.4. Taotlus kuulub rahastamisele, kui kõik siinse lisa punktis 1.2. sätestatud hindamiskriteeriumid on täidetud.

1.5. Hindamiskomisjoni liikmete hinnangute erinevuste korral on otsustavaks hindamiskomisjoni esimehe hinnang. Vajadusel tellitakse taotlusele täiendav ekspertiis.

2. **Hindamiskriteeriumid projektitaotluste hindamiseks**

Hindamiskriteerium 1: TAOTLUSE EESMÄRGI ASJAKOHASUS Hinnatakse:	JAH	EI
• Kas taotlus on suunatud erakorralise kübersündmuse lahendamisele?		
• Kas taotlus aitab vältida ootamatu küberriski eskaleerumist?		
• Kas taotlus on suunatud taotlusele eelnenud 12 kuu jooksul avastatud turvanõrkuse või küberintsidendi järelmite likvideerimiseks?		
Kui kasvõi ühele küsimustest on vastus „jah“, peetakse 1. kriteerium täidetuks.		

Hindamiskriteerium 2: PROBLEEMI ERAKORRALISUS JA KRIITILISUS Hinnatakse:	JAH	EI
• Kas taotlusega lahendatav kübersündmus või küberrisk on ettenägematu?		
• Kas taotlusega lahendatav kübersündmus või küberrisk on toimunud / selgunud taotlusele eelnenud 12 kuu jooksul?		
• Kas taotlusega lahendatav kübersündmus või küberrisk on ühiskonna toimimise või julgeoleku seisukohast oluline? (*muudetud 13.06.2026 käskkirjaga nr 40*)		
Kui kõigile kolmele küsimusele on vastus „jah“, peetakse 2. kriteerium täidetuks.		

Hindamiskriteerium 3: RAHASTAMATA JÄTMISE TAGAJÄRJED Hinnatakse:	JAH	EI
• Kas taotluses toodud kübersündmuse või küberriski lahendamist on võimalik rahastada muust eelarvest või toetusmeetmest?		
• Kas taotluses toodud kübersündmuse või küberriski lahendamist on võimalik oluliste tagajärgedeta (ilma oluliste ühiskondlike funktsioonide häiringuteta) edasi lükata (näiteks kuueks kuuks, üheks aastaks vms)?		
• Kas taotluses toodud kübersündmuse või küberriski lahendamata jätmisega seotud riskide realiseerumise tõenäosus on väike?		
Kui vähemalt kahele küsimusele on vastus „ei“, siis peetakse 3. kriteerium täidetuks.		

KINNITATUD
Justiits- ja Digiministri 03.04.2025 käskkirjaga 24
Lisa 2

OLULISTE ÜHISKONDLIKE FUNKTSIOONIDE HÄIRINGUTE ENNETAMISE TAOTLUSVOORU HINDAMISMETOODIKA

1. Taotluste hindamine

1.1. Nõuetele vastavaid taotlusi hindab käskkirja punktis 10.1. nimetatud hindamiskomisjon, kaasates vajadusel teisi eksperte.

1.2. Kui vooru esitatakse erakorralise ja kriitilise iseloomuga taotlusi, siis nende hindamiseks kasutatakse käskkirja lisas 1 toodud metoodikat ning neid rahastatakse esimese prioriteedina.

1.3. Erakorralise ja kriitilise iseloomuga taotluste rahastamisest kalendriaasta jooksul kasutamata jäänud vahenditest toetuse saajate välja selgitamiseks hindab hindamiskomisjon esitatud taotlusi järgmiste hindamiskriteeriumite alusel:

Nr	Hindamiskriteeriumid	Hindamis-kriteeriumite osakaalud
1	Projekti mõju meetme eesmärgi saavutamiseks	50%
2	Projekti olulisus probleemi lahendamiseks	25%
3	Projekti rahastamata jätmise tagajärjed	15%
4	Omafinantseeringu olemasolu	10%
		100%

1.4. Hindamise läbiviimiseks esitab RKT hindamiskomisjoni liikmetele:
1.4.1. taotluse;
1.4.2. hindamismetoodika;
1.4.3. hindamislehe;
1.4.4. hindamise seisukohast olulise muu teabe.

1.5. Hindamiskomisjoni liikmete hinnangute erinevuste korral on otsustavaks hindamiskomisjoni esimehe hinnang. Vajadusel tellitakse taotlusele täiendav ekspertiis.

1.6. Taotlust hinnatakse skaalal 0–3, millest kõrgeim hinne on 3 ja madalaim 0. Hindamine toimub täisarvudes (0; 1; 2; 3). Esimesest kuni kolmanda hindamiskriteeriumini hinne kujuneb hindamiskomisjoni liikmete antud hinnanguväärtuste keskmisest. Taotluse koondhinne moodustub järgmiselt: hindamiskomisjoni liikmete igale kriteeriumile antud hinnanguväärtuste keskmised korrutatakse läbi hindamiskriteeriumi osakaaluga, hindamiskriteeriumide hinded liidetakse ning saadud summale lisatakse juurde neljanda kriteeriumi punktid.

1.7. Kui hindamiskomisjoni liikmete ühe kriteeriumi hinne erineb 2 punkti võrra, vaadatakse kriteeriumi hinded ja põhjendused hindamiskomisjoni liikmete poolt ühiselt üle ja vajadusel korrigeeritakse.

1.8. Hinnang taotlusele loetakse negatiivseks kui hindamiskriteeriumide 1–3 hinnanguväärtuste keskmiste summa on võrdne ühega või sellest väiksem.

1.9. Punktis 1.8 nimetamata juhtudel loetakse hinnang taotlusele positiivseks.

1.10. Positiivse hinnangu saanud taotlused järjestatakse punktis 1.6 nimetatud koondhinde alusel pingeritta. Juhul, kui mitme projekti tulemuste koondsumma on võrdne, eelistatakse projekte, mis said hindamiskriteeriumis nr 1 kõrgema hinde.

2. Hindamiskriteeriumid projektitaotluste hindamiseks

Hindamiskriteerium 1: PROJEKTI MÕJU MEETME EESMÄRGI SAAVUTAMISEKS	
Hindamiskriteeriumi kaal: 50%.	
Hinnatakse: • Kas ja kuidas panustab projekt baaskübervõimete (taakvara osakaalu vähendamine, logide haldus, küberturvalisuse alane teadlikkus, identiteedihalduse tõhustamine, pilvteenuste kasutus ja riskide dokumenteerimine) parandamisse? • Kas ja mis ulatuses panustab projekt mõne õigusakti nõuete täitmisesse või Eesti infoturbestrandardi (või ISO/IEC 27001) ülevõtmisesse? • Milline on projektiga lahendatava probleemi (nt küberturvalisuse taseme, kriisihalduse võimekuse tõstmine) mõju ulatus (ühe asutuse mõjuga, ühe ministeeriumi valitsemisala mõjuga, üleriikliku mõjuga, riigi ülese mõjuga)?	
Hinne	Taseme kirjeldus
3	- Projekt panustab mitme baaskübervõime parandamisse, õigusakti(de) või standardi ülevõtmisesse. Projekti tulemusel suureneb nii taotleja kui riigi tervikuna küberturvalisuse taseme tõus. Projekti tulemusel suureneb vähemalt üleriiklik kriisihalduse võimekus.
2	- Vahepealne hinne, kus täidetud on enamus, kuid mitte kõik hinde 3 kirjelduse asjaoludest ning ei esine ühtegi hinde 0 kirjelduste asjaolu.
1	- Vahepealne hinne, kus täitmata on enamus hinde 3 kirjelduse asjaoludest või esineb hinde 0 kirjelduse asjaolusid.
0	- Projekt ei panusta ühtegi baaskübervõime parandamisse, õigusakti või standardi ülevõtmisesse. Projekt ei panusta küberturvalisuse taseme tõstmisesse või see panus ei ole ilmselge või see panus on piiratud ühest asutusest väiksema üksusega. Projekti tulemusel ei parane riiklik kriisihalduse võimekus. Projekti mõju meetme eesmärgi saavutamisele on ebaselge.

Hindamiskriteerium 2: PROJEKTI OLULISUS PROBLEEMI LAHENDAMISEKS	
Hindamiskriteeriumi kaal: 25%.	
Hinnatakse: • Kas projektiga valitud lahendus on parim projekti eesmärgi saavutamiseks? • Kas antud projektiga lahendatakse probleemi täielikult või osaliselt? • Kas projekt vajab jätkurahastust tulevikus?	
Hinne	Taseme kirjeldus
3	- Projektiga valitud lahendus on parim võimalik projekti eesmärgi saavutamiseks. Projektiga lahendatakse probleemi tervikuna ning jätkurahastust projekti tegevused ei vaja.
2	- Vahepealne hinne, kus täidetud on enamus, kuid mitte kõik hinde 3 kirjelduse asjaoludest ning ei esine ühtegi hinde 0 kirjelduste asjaolu.
1	- Vahepealne hinne, kus täitmata on enamus hinde 3 kirjelduse asjaoludest või esineb hinde 0 kirjelduse asjaolusid.
0	- Projektiga valitud lahendus ei ole üheti arusaadav või selle olulisus probleemi lahendamiseks on kaheldav või ei ole ilmselge. Projektis kirjeldatu probleemi lahendatakse osaliselt ning projekti tegevused vajavad jätkurahastust.

Hindamiskriteerium 3: PROJEKTI RAHASTAMATA JÄTMISE TAGAJÄRJED

Hindamiskriteeriumi kaal: 15%.

Hinnatakse:

- Kas taotluses toodud küberturvalisuse probleemi lahendamist on võimalik rahastada muust eelarvest või toetusmeetmest?
- Kas taotluses toodud küberturvalisuse probleemi rahastamist on võimalik oluliste tagajärgedeta (oluline mõju riikliku küberturvalisuse tagamisele, ühiskonna toimimisele, või kriitilise teenuse osutamisele) edasi lükata (nt 6 kuuks, 1 aastaks vms)?
- Kas taotluses toodud küberturvalisuse probleemi lahendamata jätmise oluliste riskide realiseerimise tõenäosus on väike?

Hinne	Taseme kirjeldus
3	- Projekti rahastamata jätmisel on rasked tagajärjed riikliku küberturvalisuse tagamisele. Projekti rahastamise edasi lükkamine seab ohtu mõne olulise objekti või teenuse osutamise küberturvalisust. Projekti ei ole võimalik rahastada muudest vahenditest ning mitterahastamise tagajärg on kriitiliselt valulik.
2	- Vahepealne hinne, kus täidetud on enamus, kuid mitte kõik hinde 3 kirjelduse asjaoludest ning ei esine ühtegi hinde 0 kirjelduste asjaolu.
1	- Vahepealne hinne, kus täitmata on enamus hinde 3 kirjelduse asjaoludest või esineb hinde 0 kirjelduse asjaolusid.
0	- Projekti võib rahastada muudest eelarvetest / toetusmeetmetest või tegevuste elluviimist on võimalik edasi lükata järgmisesse aastasse ning sellega ei kaasne olulist mõju riiklikule küberturvalisusele.

Hindamiskriteerium 4: PROJEKTI OMAFINANTSEERINGU OLEMASOLU

Hindamiskriteeriumi kaal: 10%.

Hinnatakse:

- Taotleja omafinantseeringu osakaal projekti eelarvest (omafinantseeringu määra (%) suurus projekti eelarvest protsentides).

Vooru taotlused omafinantseeringu määraga 10% saavad kriteeriumi hindeks „1“. Ülejäänud vooru taotlused reastatakse omafinantseeringu määra suuruse järgi, parim pool saab kriteeriumi hindeks 3, nõrgem pool saab kriteeriumi hindeks 2.
NB! Sama omafinantseeringu määraga taotlused kuuluvad samasse poolde.

Hinne	Taseme kirjeldus
3	- Omafinantseeringu määr mahub parimasse (kõige suurema omafinantseeringu osakaaluga) poolde.
2	- Omafinantseeringu määr mahub nõrgemasse (parimast poolest väiksema omafinantseeringu osakaaluga) poolde.
1	- Omafinantseeringu määr 10%.