

Lisa 1
KINNITATUD
peadirektori XX.XX.2026
käskkirjaga nr 1.1-2/26-XXX

RIIGI INFOSÜSTEEMI AMETI
OHUENNETUSLIKU RIIKLIKU JÄRELEVALVE
OHUPROGNOOS

Tallinn 2026

Vastavalt Riigi Infosüsteemi Ameti põhimääruse §-le 7 täidab amet õigusaktidega sätestatud ulatuses tema pädevuses olevaid ülesandeid riigi infosüsteemi ja küberturvalisuse valdkonnas.

Küberturvalisuse seaduse (KüTS) § 12 lg 1 kohaselt koordineerib Riigi Infosüsteemi Amet seaduses sätestatud ulatuses küberturvalisuse tagamist ning küberintsidendi ennetamist ja lahendamist ning teostab ka turvameetmete rakendamise üle järelevalvet.

KüTS § 2 p 19 kohaselt on küberintsident võrgu- ja infosüsteemis toimuv sündmus, mis ohustab või kahjustab võrgu- ja infosüsteemi turvalisust.

Ohuks loetakse sündmust või asjaolu, mis asjakohaste kaitsemeetmete puudumisel võib põhjustada turvarikkeid, katkestusi teenuse toimepidevuses või kahjustab infovara muul viisil.

Ohu tõrjumine ja ennetamine on riikliku järelevalve ülesandeks, mille üldiseid põhimõtteid reguleerib korrakaitseseadus (KorS).

Ohutõrjeliseks järelevalveks loetakse avaliku korra kaitsealas oleva õigusnormi või isiku subjektiivse õiguse rikkumise või õigushüve kahjustamist puudutava korrarikkumise kõrvaldamist, sh ohukahtluse korral ohu väljaselgitamist (KorS § 5 lg-ed 1 kuni 6).

Ohu ennetavaks järelevalveks loetakse seda osa korrakaitsest, kus puudub ohukahtlus, kuid saab pidada võimalikuks olukorda, mille realiseerumisel tekib ohukahtlus või oht. Ohu ennetamine on muu hulgas teabe kogumine, vahetamine ja analüüs, toimingute kavandamine ja elluviimine ning riikliku järelevalve meetmete kohaldamine avalikku korda tulevikus ähvardada võivate ohtude tõrjumiseks, sealhulgas süütegude ennetamine (KorS § 5 lg 7).

Tulenevalt KorS § 6 lg-st 1 ja KüTS § 14 lg 1 on Riigi Infosüsteemi Amet riiklikku järelevalve ülesannet täitma volitatud asutus ehk korrakaitseorgan. Riigi Infosüsteemi Amet teeb riiklikku järelevalvet küberturvalisuse seaduse ja selle alusel kehtestatud õigusaktides sätestatud nõuete täitmise üle.

KorS § 24 lg 1 alusel on korrakaitseorganil lubatud kohaldada riikliku järelevalve erimeedet ohu ennetamiseks, kui ohuproгноosile tuginedes saab pidada võimalikuks olukorda, mille realiseerumisel tekib oht.

Ohuproгноosi funktsioon on ohuennetusliku riikliku järelevalve aluse tekitamine, mille laiem kasutamise eesmärk on järelevalvetoimingutega tagada oluliste teenuste igapäevane turvaline toimimine läbi kehtestatud nõuete täitmise ja teadliku küberkäitumise. Käesoleva ohuproгноosi funktsioon on anda järelevalve sekkumiseks kontrollitav ja arusaadav alus kodanikele, ettevõtjale ning Riigi Infosüsteemi Ametile. Ohuproгноos on ühtlasi aluseks ka iga jooksva kalendriaasta järelevalve tööplaani koostamisele, mis omakorda täpsustab valimit millist kirjeldatud olukordadest jooksva aastal kontrollitakse.

Vastavalt KorS § 24 lg 2 peab ohuproгноos põhinema faktidel või korrakaitseorgani teaduslikel või tehnilistel teadmistel või Euroopa Liidu õigusaktist tuleneval järelevalvekohustusel ning lähtuma võrdse kohtlemise põhimõttest.

Tulenevalt eeltoodust on Riigi Infosüsteemi Amet koostanud küberturvalisuse teenistuse ülesannetega kaetud tegevusvaldkondade ohte käsitlevad ohuproгноosid. Käesolev ohuproгноos sisaldab nimekirja erinevates valdkondades võimalikest realiseeruda võivatest ohukahtlustest või ohtudest, milliste ennetamiseks on kohane juhendada KorS § 2, § 4 ja § 5 sätestatust, mis on aluseks RIA-le KüTS §-des 12 ja 14 nimetatud ülesannete täitmiseks.

Lisaks sisaldab käesolev ohuproгноos ka laiaulatusliku tarbijaskonnaga ja ühiskonnas igapäevaelu toimimiseks vajalike baasteenustega seotud ohtude progноose. Käsitletud on sellised baasteenused ja nendega seotud ohud, mille arvutivõrgu- ja infosüsteemide turvalisus ning toimepidevuse toimimine on ühiskonna igapäeva toimetuste juures väga olulised ning nende ohtude realiseerumine toob kaasa laiaulatusliku mõju ja tagajärgedega kahju tekitamise olukorra.

Ohuproгноosis sisalduvate potentsiaalsete ohtlike olukordade ja neid puudutavate teenuste nimekiri ei ole lõplik, sest kõiki ohuolukordi ei ole võimalik ette näha. Käesoleva ohuproгноosi ajakohasust hinnatakse järjepidevalt, vähemalt üks kord aastas, st jooksva aasta viimasel kalendrikuul, ning tehakse selles uue ohuolukorra tekkimisel muudatusi.

Käesolev ohuproгноos on koostatud ohuolukordade objektiivsete tunnuste alusel ja lähtutakse senise järelevalve tulemustest, kehtivatest nõuetest, CERT.EE-le, kriitilise infrastruktuuri küberkaitse osakonna (edaspidi KIKK) sektoriaalsetest riskianalüüsides ja analüüsi- ja ennetusosakonnale (edaspidi AEO) laekunud intsidentide turvaanalüüsides tulemustest, asetleidnud intsidentide juurpõhjusest ja selle mõjuulatusest, teadus- ja erialakirjanduses avaldatud käsitlustest ja ülevaadetest. Ohtude realiseerumise tegelik sagedus sõltub ohu tüübist, turvaaugu „suurusest“ ning objekti iseärasustest, näiteks andmete tundlikkusest. Seega hindab Riigi Infosüsteemi Amet küberintsidentide ennetamisele suunatud järelevalvetegevusel ja asjakohaste turvameetmete valimisel ohu tegeliku toimumise tõenäosust ning progноosis oodatavaid kahjusid ja mõjusid.

Käesolevas ohuproгноosis arvestatakse valdkondlikku kriitilisuse taset (riskitase) allpool väljatoodud riskimaatriksi abil, mille tulemusel selguvad järelevalve teostamise prioriteedid ja metoodika ohu ennetamiseks või kõrvaldamiseks.

Risk on määramatuse toime organisatsiooni eesmärkidele. Risk kujuneb ohu poolt nõrkuse ärakasutamise tõenäosuse ja tekkida võiva küberintsidentide tagajärgede kombinatsioonist ja mille funktsiooniks on riskitase. Riskitaseme sisendparameetrite väärtusteks on potentsiaalne kahju ja riski realiseerumise võimalikkus.

Riski mõju all mõistame kahju või tagajärge, mida konkreetse riski avaldumine/realiseerumine kaasa tuua võib.

Riski realiseerumisega kaasnev **potentsiaalne kahju** liigitub järgmiselt:

Tabel 1.

Kahju suurus	Kahju tagajärjed
Ähvardab organisatsiooni olemasolu	Ülisuur rahaline kaotus, ülisuur mõjuulatus, sh piiriülene, kahjud, mis ulatuvad katastroofilise tasemeni, mis ähvardab organisatsiooni olemasolu, ülisuur maine kadu, surmavad vigastused.
Tõsine	Suur rahaline kahju, suur mõjuulatus, sh piiriülene, toimimise ristsõltuvus, tõsine maine kaotus, vigastuste/ohvrite oht.
Piiratud	Keskmine rahaline kahju, vähene maine kadu, tegevus on lühiajaliselt piiratud, kuid saab hakkama.
Tühine	Tähtsusetud kahjud, mis on väiksed ja saab jätta arvestamata.

Riski tõenäosuse all mõistame konkreetse riski avaldumise võimalikkust/sagedust. **Riski realiseerumise võimalikkust** võib liigitada läbi realiseerimise sageduse määratud ajavahemiku jooksul (võttes arvesse organisatsiooni nõrkusi ja turvameetmeid).

Tabel 2.

Realiseerumise võimalikkus / kirjeldus	
Väga sage	Sündmus toimub mitu korda kuus.
Sage	Sündmus toimub kord kuus kuni kord aastas.
Keskmine	Sündmus toimub üks kord iga ühe kuni viie aasta kohta.
Harv	Senise teadmuse põhjal võib sündmus toimuda maksimaalselt üks kord viie aasta jooksul.

Riskitaseme määravad ära kahju suurus ja riski realiseerumise võimalikkus.

Tabel 3.

Riskitase		Tegevus
Väga kõrge	Turvameetmed ei kaitse selle ohu eest piisavalt. Väga suurt riski praktikas ei aktsepteerita, sellega tuleb (käsitlusjärgus) eraldi tegeleda.	Vajab kohest sekkumist, et vähendada riski talutava piirini. Tegutse kohe!
Kõrge	Turvameetmed ei kaitse selle ohu eest piisavalt.	Riski vähendamine on prioriteet, selleks plaanitakse asjakohased tegevused, mida rakendada esimesel võimalusel. Riskide pidev jälgimine.
Keskmine	Turvameetmed võivad osutada ebapiisavateks.	Kõrgendatud tähelepanuga seire, olukorra muutudes võib vajada kohest sekkumist. Oluline on riski teadvustamine.
Madal	Turvameetmed annavad piisava kaitse. Praktikas väikesed riskid tavaliselt aktsepteeritakse, kuid ikkagi ohtu seirates.	Hallatakse rutiinsete turbeprotsessi seiretegevuste käigus.

Riskitase tuvastatakse **riskimaatriksi** abil, mille tulemusel on võimalik kindlaks teha kõige kriitilisemad valdkonnad antud hindamise perioodil.

Riskimaatriks.



Riski realiseerumise võimalikkuse tabel.

Jrk nr	Valdkond	Kontrolliese	Ohuolukorra kirjeldus, võimalikud tagajärjed	Tekkimise tõenäosus ehk realiseerumise võimalikkus (väga sage/sage/keskmine/harv)	Mõju ehk potentsiaalne kahju (ähvardab organisatsiooni: tõsine/piiratud/tühine)	Kriitilisuse tase (riski tase)	Ohuproгноosi koostamise alus(ed)
1.	Digitaalse teenuse (Eesti maatunnusega seotud tipptaseme domeeninimede süsteemi teenuse) osutamine	DNS teenuse pakkujad (nt Eesti Interneti Sihtasutus-EIS, Eesti Hariduse ja Teaduse ministeeriumi hallatav EENET ehk Eesti Hariduse ja Teaduse Andmesidevõrk). Teenuste osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid ja-varad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised meetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsessi ja riskide käsitluskava, intsidentide haldus, väljast tellitud IT teenuslepingud.	Ohtudeks on EESTI maatunnusega .ee Interneti infrastruktuur ja veebilehtede kompromiteerimine, kasutamise katkemine, õnnestunud küberrünne ja kogutud andmete tervikluse ja käideldavuse kadu. Turvanõrkustega välisvõrgu kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. DNS teenuse pakkujal puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st ettevõtte ei ole endale	sage	tõsine	kõrge	CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KÜTS nõuded,

			kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. DNS teenuse, sh tipptaseme nimeserveri toimimise häirimisel või katkemisel on mõjutatud kogu Eesti Interneti kasutajaskond, sh riigiasutuste, hallatavate asutuste, riigi osalusega ettevõtete, elutähtsate teenuste osutajate või nendele alusteenuseid osutavate teenuseosutajate teenused ja töö. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuse toimimise halvamiseks.				KorS § 2, § 4, § 5 ja § 49.
2.	Digitaalse teenuse (Eesti maatunnusega seotud tipptaseme domeeninimede registreerimine ja tippdomeeninimede registri haldamine) osutamine	Tipptaseme domeeninimede registri omanik ja registripidaja EIS ning teised akrediteeritud registripidajad (https://www.internet.ee/registripidaja/akrediteeritud-registripidajad), sh Zone Media OÜ, RIKS, Telia Eesti AS, Spin TEK AS jne). Teenuse osutamiseks IT-taristu (kasutatavad infosüsteemid ja- varad, arvutivõrk) turvalisuse tagamiseks kasutatud infotehnilised meetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed ja nende	Ohtudeks on EESTI.ee Interneti infrastruktuuri ja veebilehtede kompromiteerimine, kasutamise katkemine, õnnestunud küberrünne ja kogutud andmete tervikluse ja käideldavuse kadu. Turvanõrkustega välisvõrgu kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik IT-taristu turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. Sisseostetud IT teenustel üldsõnalised teenuslepingud. DNS sekundaarse	sage	tõsine	kõrge	CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste

		piisavus. Väljast tellitud IT teenuslepingud.	registripidaja teenuse, sh majutusteenuse toimimise häirimisel või katkemisel on mõjutatud selle registripidaja juures domeeninime registreerinud Eesti Interneti kasutajaskond. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust Eesti maatunnusega seotud tiptaseme nimeserveri küberrünnakuteks ja teenuse toimimise halvamiseks.				järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised. KorS § 2, § 4, § 5 ja § 49.
3.	Riigi osalusega ettevõtete avalikud teenused tegevuste osas, mis on reguleeritud KüTS §-is 3.	Sihtasutused ja MTÜ-d, riigi osalusega äriühingud ja nende tütarettevõtted nimekirjade alusel https://www.fin.ee/riigihanked-riigiabi-osalused/riigi-osalused . Teenuste osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid ja -varad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised meetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava, intsidentide haldus, väljast tellitud IT teenuslepingud.	Ohtudeks on avalikest huvidest tulenevate ülesannete (haldusülesanded) korraldamiseks vajalike arvutivõrgu- ja infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine, õnnestunud küberrünne ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega välisvõrgu kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu IT-taristu turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. Asutuse nimel korduvalt saadetud pahavara levitavad kirjad. Riigi osalusega asutusel puudulik IT-riskihaldusprotsess ja riskide	sage	tõsine	kõrge	CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidenti turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidenti juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

			käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Ohu realiseerumine mõjutab Riiki ennast ja igat Eestis elavat ja tegutsevat füüsilist- ja juriidilist isikut, kes tarbib avalikust huvist lähtuvaid riiklike teenuseid. Teenuste hulgas on ka eluks vajalikke fundamentaalseid teenuseid, mis mõjutavad inimeste põhiseadusest tulenevaid kaitsevajadusi, elukvaliteeti, tervist ja ühiskonna toimimist jms. Samuti on mõjutatud riigi maksu- ja finantskohustuste halduskorraldus - riigikassa, riigieelarve kujunemine. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.				
4.	Vedelkütusevaru moodustamine ja haldamine	HOS § 18¹ lg 1 alusel määratud riigi äriühing e varu haldaja, kelle põhikirjalise tegevuse eesmärk on varu moodustamine ja haldamine. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse	Ohtudeks on ühiskonna toimimise seisukohast oluliste ja elutähtsate teenuste korraldamiseks vajalike võrgu- ja infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektorიაalsed riskianalüüsid, valdkonnale

		tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	kadu. Turvanõrkustega välisvõrgu kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbe poliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Tegemist on riigi varustuskindluse, julgeoleku ja majanduse toimimiseks vajaliku teenusega, sh on tegemist strateegilise ressurssiga, mille roll muutub oluliseks kriiside ja hädaolukordade ajal, mil tavapärased tarneaheldad on häiritud. Ohu realiseerumisel turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja vedelkütusevaru haldamise toimimise halvamiseks. Selle teenuse katkemise tagajärjed võivad olla ulatuslikud ja				suunatud küberrünnete kasv, asetleidnud intsidentide juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, vedelkütusevaru seaduse §1 lg 2 ja § 4 § KüTS nõuded. KorS § 2, § 4, § 5 ja § 49. 2. Järeelkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
--	--	---	---	--	--	--	--

			pikaajalised nii ühiskonnale, majandusele kui ka riigi julgeolekule.				
5.	Küberturvalisuse seaduse § 3 lg 2 p 2 teenuste osutamine (ühiskonna toimimise seisukohast elutähtsad teenused):	Elutähtsa teenuse osutamiseks võrgu- ja infosüsteemide pidamise nõuded; IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus, väljast tellitud IT teenuslepingud.	Ohtudeks on ühiskonna toimimise seisukohast oluliste ja elutähtsate teenuste korraldamiseks vajalike võrgu- ja infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega välisvõrgu kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Ohu realiseerumine mõjutab igat Eestis tegutsevat ja elavat juriidilist- ning füüsilist isikut, kes tarbib neid teenuseid. Teenuste hulgas on ka eluks vajalikke fundamentaalseid teenuseid, mille				CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded, HOS nõuded. KorS § 2, § 4, § 5 ja § 49.
	1. elektriga varustamine;			harv	tõsine	keskmine	
	2. maagaasiga varustamine			harv	tõsine	keskmine	
	3. vedelkütusega varustamine ;			harv	tõsine	keskmine	
	4. riigitee sõidetavuse tagamine;			harv	piiratud	madal	
	5. telefoniteenus			sage	tõsine	kõrge	
	6. mobiiltelefoniteenus;			sage	tõsine	kõrge	
	7. andmesideteenus;			sage	tõsine	kõrge	
	8. elektrooniline isikutuvastamine ja digitaalne allkirjastamine;			sage	tõsine	kõrge	
	9. vältimatu- ja kiirabi teenus;			harv	tõsine	keskmine	
	12. kaugküttega varustamine;			harv	tõsine	keskmine	

	13. kohaliku tee sõidetavuse tagamine;		katkemine või häired teenuse kasutamises mõjutavad oluliselt ühiskonna toimimist ja ohtu võib sattuda inimeste elu või tervis või teise elutähtsa teenuse või üldhuviteenuse toimimine. Oluline tagada igapäevaste teenuste toimimiseks vajalike infosüsteemide turvalisus selliselt, et oleks välistatud igasugune küberrünnete tekkevõimalus, masinatega manipuleerimine ning arvestada sõltuvustega, mis tulenevad teistest infosüsteemidest ja elutähtsate teenuste toimimisest. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja ühiskonna toimimise seisukohast oluliste ja elutähtsate teenuste toimimise halvamiseks. Halvimal juhul võib tekkida võimalus eri- või hädaolukorra tekkeks hädaolukorra seaduse mõistes.	keskmine	tõsine	keskmine	
	14. veega varustamine ja kanalisatsioon;			harv	tõsine	keskmine	
6.	ESS-kohase üldkasutatava elektroonilise side võrgu ja üldkasutatava side teenuse osutamine (ülioluline üksus)	Suuremad sideettevõtjad (majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot) . Teenuste osutamiseks üldkasutatava sidevõrgu- ja teenuste turvalisuse ning tervikluse tagamise nõuded; IT-taristu	Ohtudeks on elektroonilise side teenuste osutamiseks vajaliku sidevõrgu- ja sellega seotud infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine, õnnestunud küberrünne ja kogutud andmete tervikluse, konfidentsiaalsuse ja	harv	tõsine	keskmine	CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektorიაalsed riskianalüüsid, valdkonnale

		(kasutatavad infosüsteemid, infovarad, sidevõrk); sidevõrkude ja teenuste turvalisuse tagamiseks kasutatavad infotehnilised turvameetmed, turvaeskirjad, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; turvaaudit; intsidentide haldus, väljast tellitud IT teenuslepingud.	käideldavuse kadu. Turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbe poliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisestatud IT teenustel üldsõnalised teenuslepingud. Tegemist on ühiskonna poolt laiaulatuslikult kasutusele võetud ja eluliselt tähtsate teenustega, mille katkemine mõjutab oluliselt ühiskonna toimimist, riigi julgeolekut, igat Eestis tegutsevat ja elavat juriidilist- ning füüsilist isikut. Ohtu võib sattuda inimeste elu ja tervisele. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks. Halvimal juhul võib tekkida võimalus eri- ja hädaolukorra tekkeks hädaolukorra				suunatud küberrünnete kasv, aset leidnud intsidentide juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, ESS §-s 87² § 87² lõike 6, § 100³ lõike 3, § 100⁴ lõike 2 ja § 100⁵ lõike 2, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
--	--	--	---	--	--	--	---

			seaduse mõistes.				
7.	ESS-kohase üldkasutatava elektroonilise side võrgu ja üldkasutatava side teenuse osutamine (oluline üksus)	Väiksemad sideettevõtjad (majandusaasta jooksul vähem kui 50 töötajat ja kelle aastabilansimaht või aastakäive on väiksem kui 10 miljonit eurot). Teenuste osutamiseks üldkasutatava sidevõrgu- ja teenuste turvalisuse ning tervikluse tagamise nõuded; IT-taristu (kasutatavad infosüsteemid, infovarad, sidevõrk); sidevõrkude ja teenuste turvalisuse tagamiseks kasutatavad infotehnilised turvameetmed, turvaeeskirjad, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; turvaaudit; intsidentide haldus, väljast tellitud IT teenuslepingud. NB! Riiklikus järelevalves rakendatakse ainult järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on elektroonilise side teenuste osutamiseks vajaliku sidevõrgu- ja sellega seotud infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine, õnnestunud küberrünne ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Tegemist on ühiskonna poolt laiaulatuslikult kasutusele võetud ja eluliselt tähtsate teenustega, mille katkemine mõjutab oluliselt ühiskonna toimimist, riigi julgeolekut, igat Eestis tegutsevat ja elavat juriidilist- ning füüsilist isikut. Ohtu võib sattuda inimeste elu ja tervisele. Turvanõrkustega ja puuduliku	harv	tõsine	keskmine	Ametile laekunud vihjed ja pöördumised võimalike turvanõrkuste rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

			turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks. Halvimal juhul võib tekkida võimalus eri- ja hädaolukorra tekkeks hädaolukorra seaduse mõistes.				
8.	ESS-kohase kriitilise tähtsusega side teenus, mereraadioside, operatiivraadioside võrgu teenus)	Kriitilise tähtsusega side, mereraadioside, operatiivraadiosidevõrguteenus. Teenuste osutamiseks sidevõrgu- ja mereraadioside, operatiivraadiosidevõrguteenuste turvalisuse ning tervikluse tagamise nõuded; IT-taristu (kasutatavad infosüsteemid, infovarad, sidevõrk); sidevõrkude ja teenuste turvalisuse tagamiseks kasutatavad infotehnilised turvameetmed, turvaeeskirjad, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; turvaaudit; intsidentide haldus, väljast tellitud IT teenuslepingud.	Ohtudeks on Eesti kriitilise tähtsusega side, mereraadioside, operatiivraadiosidevõrguteenuste osutamiseks vajaliku sidevõrgu- ja sellega seotud infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine, õnnestunud küberrünne ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT	harv	tõsine	keskmine	CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidenti turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidenti juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, ESS §-s § 100 ³ , § 100 ⁴ ja § 100 ⁵ , KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

			teenustel üldsõnalised teenuslepingud. Tegemist on ühiskonna poolt laiaulatuslikult kasutusele võetud ja eluliselt tähtsate teenustega, mille katkemine mõjutab oluliselt ühiskonna toimimist, riigi julgeolekut, igat Eestis tegutsevat ja elavat juriidilist- ning füüsilist isikut. Ohtu võib sattuda inimeste elu ja tervis. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks. Halvimal juhul võib tekkida võimalus eri- ja hädaolukorra tekkeks hädaolukorra seaduse mõistes.				
9.	Perearstiabi osutamine	Perearstiabi osutaja (perearstid ja nendega koos töötavad tervishoiutöötajad). Perearstiabi teenuses kasutatava võrgu- ja infosüsteemide pidamise nõuded; IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud.	Ohtudeks on perearstiabi teenuse korraldamiseks vajalike võrgu- ja infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega välisvõrgu kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Teenuse osutajatel puudulik IT-	harv	piiratud	madal	Ametile laekunud vihjed ja pöördumised võimalike turvanõrkuste rikkumise kohta, KÜTS nõuded, KorS § 2, § 4, § 5 ja § 49.

		NB! Riiklikus järelevalves rakendatakse ainult järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KÜTS §-des 7 ja 8 nõudeid.	riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja tervishoiuteenuste toimimise halvamiseks. Riski realiseerumine mõjutab pea igat kodanikku, kes tarbib perearsti teenuseid. Üldise ohuolukorra võimaliku tagajärjena võib saada muuta eriliigilisi isiku- ja terviseandmeid (patsiendiandmed) või need sattuda kolmandate isikute valdusesse, tekkida kahju inimese tervisele, oht eraelu puutumatusle (riive privaatsusele), oht elule, või halvimal juhul kaasneda surm.				
10.	Rahvatervise hädaolukorras esmatahtsa meditsiiniseadme tootmine	Rahvatervise hädaolukorras esmatahtsa meditsiiniseadme tootjad. Tootmises kasutatava võrgu- ja infosüsteemide pidamise nõuded; IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja	Ohtudeks on rahvatervise hädaolukorras esmatahtsa meditsiiniseadmete tootmisel võrgu- ja infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega välisvõrgu kaitse (tulemüür) küberrünnete	harv	tõsine	keskmine	1. CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv,

		turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meetet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	tuvastamiseks, nõrk infoturbe poliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja meditsiiniseadmete eesmärgipäraseks kasutamiseks. Riski realiseerumine mõjutab pea igat kodanikku, kes tarbib konkreetseid meditsiiniseadmeid. Tegemist on tõsise patsiendiohutuse ja rahvatervise riskiga. Kõige raskema ohuolukorra stsenaariumi tagajärjena saab meditsiiniseadme parameetrite muutmist juhtida selleks volitamata isikud ja muuta selle seadme kasutamine inimese tervisele ohtlikuks, ohustada tema eraelu puutumatust (riive privaatsusele),				asetleidnud intsidenti juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, Euroopa Parlamendi ja nõukogu määruse (EL) 2022/123 artikkel 22, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvaõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
--	--	--	--	--	--	--	--

			ohtu elule, halvimal juhul kaasneda surm.				
11.	Euroopa Parlamendi ja nõukogu määruse (EL) 2017/745 artikli 2 punktis 1 loetletud meditsiiniseadmete ja Euroopa Parlamendi ja nõukogu määruse (EL) 2017/746 artikli 2 punktis 2 loetletud in vitro diagnostikameditsiiniseadmete tootmine	Meditsiiniseadme tootja. Tootmises kasutatava võrgu- ja infosüsteemide pidamise nõuded; IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Rakendatakse ainult järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on rahvatervise hädaolukorras esmatahtsa meditsiiniseadmete tootmisel võrgu- ja infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega välisvõrgu kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja meditsiiniseadmete eesmärgipäraseks kasutamiseks. Riski realiseerumine mõjutab pea igat kodanikku, kes	harv	piiratud	madal	Ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

			tarbib konkreetseid meditsiiniseadmeid. Tegemist on tõsise patsiendiohutuse ja rahvatervise riskiga. Kõige raskema ohuolukorra stsenaariumi tagajärjena saab meditsiiniseadme parameetrite muutmist juhtida selleks volitamata isikud ja muuta selle seadme kasutamine inimese tervisele ohtlikuks, ohustada tema eraelu puutumatust (riive privaatsusele), ohtu elule, halvimal juhul kaasneda surm.				
12.	Euroopa Liidu majanduse tegevusalade statistilise klassifikaatori NACE Revision 2 C jao osas 21 osutatud põhifarmaatsiatoote ja ravimpreparaadi tootmine, sh vere töötlemine.	Euroopa Liidu majanduse tegevusalade statistilise klassifikaatori NACE Revision 2 C jao osas 21 osutatud põhifarmaatsiatoote ja ravimpreparaadi tootjad, sh apteegid. Tootmises kasutatava võrgu- ja infosüsteemide pidamise nõuded; IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud.	Ohtudeks on kõnealuste põhifarmaatsiatoote ja ravimpreparaadi tootmiseks vajalike võrgu- ja infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega välisvõrgu kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, Majanduse tegevusalade statistiline klassifikaator – NACE Revision 2 C

		NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	teenustel üldsõnalised teenuslepingud. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks farmaatsiatoote ja ravimipreparaadi tootmisel. Riski realiseerumine mõjutab pea igat kodanikku, kes tarbib konkreetseid farmaatsiatooteid. Tegemist on tõsise patsiendiohutuse ja rahvatervise riskiga. Kõige raskema ohuolukorra stsenaariumi tagajärjena saab farmaatsiatoote ja ravimipreparaadi tootmist juhtida selleks volitamata isikud ja muuta toodetud preparaadid inimese tervisele ohtlikuks, tekkida kahju inimese tervisele, oht elule, või halvimal juhul kaasneda surm.				jagu 21 , KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järeldkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
13.	Ravimi, va veterinaarravimi uurimine ja arendamine	Ravimi uurimise ja arendamisega tegelev juriidiline või füüsiline isik. Uurimises või arendamises kasutatava võrgu- ja infosüsteemide pidamise nõuded; IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide	Ohtudeks on kõnealuste põhifarmaatsiatoote ja ravimipreparaadi tootmiseks vajalike võrgu- ja infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega välisvõrgu kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbe poliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste

		haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	sisevõrgu ressursside turvatestimine ja haavatavuste seire. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberründeks ja uurimise ja arendamise tööde toimimise halvamiseks.				järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, ravimiseaduse § 2 lg 1, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
14.	Raudteeinfrastruktuuri majandamine, käitamine, hooldamine ja uuendamine kauba ja reisijateveo ning veduriteenuse toimimise korraldamine	Raudteeinfrastruktuuri-ettevõtjad (AS Eesti Raudtee, Edelaraudtee Infrastruktuuri AS), kauba- või reisijaveo korraldajad. Raudteeinfrastruktuuri halduseks ja kauba ning reisijaveoks kasutatava võrgu- ja infosüsteemide pidamise nõuded; IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide	Ohtudeks on raudteeinfrastruktuuri halduses ja kauba ja reisijateveo ning veduriteenuse kasutatavate arvutivõrgu- ja sellega seotud infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine, õnnestunud küberrünne ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbe poliitika, kasinalt riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire.	sage	piiratud	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja

		haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelekontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine. Tegemist on transpordivaldkonnas kesksel rolli kandva majandustegevusega, mille kaudu tagatakse õiglane konkurentsiolekord nii kauba- kui ka reisijateveol. Tegemist on ühiskonna poolt laiaulatuslikult kasutusele võetud ja eluliselt tähtsate teenustega, mille katkemine mõjutab oluliselt ühiskonna toimimist, riigi julgeolekut, igat Eestis tegutsevat ja elavat juriidilist ning füüsilist isikut. Ohtu võib sattuda raudteeinfrastruktuuri kavandatud läbilaskevõime, inimeste elu ja tervis. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.				pöördumised, raudteeseaduse § 2 p 14 KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
--	--	---	--	--	--	--	--

15.	Lennujuhtimisteenus osutamine	Lennuliikluskorraldusettevõtja. Teenuste osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seiremeetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelekontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on lennujuhtimises kasutatavate arvutivõrgu- ja lennuliikluse teenindamist tagava aeronavigatsiooniteenuse toimimiseks kasutatava arvutivõrgu ja sellega seotud infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine, õnnestunud küberrünne ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Tegemist on transpordivaldkonnas olulist rolli kandva majandustegevusega, mille kaudu tagatakse turvaline EV õhuruumi kasutamine ja lennuliikluse teeninduse tagamine nii kauba- kui ka reisijateveol. Tegemist on ühiskonna poolt laiaulatuslikult kasutusele	harv	tõsine	keskmine	1.CERT-EE/AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, Euroopa Parlamendi ja nõukogu määruse (EL) 2024/2803 artikkel 2 p 6, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

			võetud ja eluliselt tähtsate teenustega, mille katkemine mõjutab oluliselt ühiskonna toimimist, riigi julgeolekut, igat Eestis tegutsevat ja elavat juriidilist- ning füüsilist isikut, samuti ka välispartnereid. Ohtu võib sattuda kogu EV õhuruumi lennujuhtimise teenindamise turvalisus, sh kavandatud lennuühenduste läbilaskevõime, lendude kokkupõrgete vältimine, inimeste julgeolek, elu ja tervis. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.				
16.	Lennujaama taristu juhtimine ja koordineerimine(haldamine)	Lennujaama haldaja. Teenuste osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitleuskava; intsidentide haldus; väljast tellitud IT teenuslepingud.	Ohtudeks on lennujaama taristu haldamiseks kasutatavate arvutivõrgu- ja lennuliikluse teenindamist tagava aeronavigatsiooniteenuse toimimiseks kasutatava arvutivõrgu ja sellega seotud infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine, õnnestunud küberrünne ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile

		NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Tegemist on ühiskonna poolt laiaulatuslikult kasutusele võetud ja eluliselt tähtsa teenusega, mille katkemine mõjutab oluliselt ühiskonna toimimist, riigi julgeolekut, igat Eestis tegutsevat ja elavat juriidilist- ning füüsilist isikut, samuti ka välispartnereid. Ohtu võib sattuda kogu EV õhuruumi lennuliikluse teenindamise turvalisus, sh kavandatud lennuühenduste läbilaskevõime, inimeste julgeolek, elu ja tervis. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.				laekunud vihjed ja pöördumised, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järellkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
17.	Sadama tegevuse e sadama teenuse korraldamine ja veesõidukite	Sadama pidaja ja sadamarajatise valdaja. sadama omanik. Teenuste osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid,	Ohtudeks on sadamateenuses või rahvusvahelise meresõidus sõitvate reisilaevade ning rannasõidus	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi

	(reisilaevade ning rannasõidus sõitvate laevade) teenindamine	infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	sõitvaid I kategooria laevade või A-klassi reisilaevade teenindamises kasutatava arvutivõrgu ja sellega seotud infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine, õnnestunud küberrünne ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Tegemist on transpordivaldkonnas olulist rolli kandva majandustegevusega, mille kaudu tagatakse EV territoriaal- ja sisemeres ohutu ning turvaline veeliikluse ja sadamateenuse teenindus nii kauba- kui ka reisijateveol. Tegemist on ühiskonna poolt laiaulatuslikult kasutusele võetud ja eluliselt tähtsate teenustega, mille katkemine mõjutab oluliselt ühiskonna toimimist, riigi julgeolekut, igat Eestis tegutsevat ja				turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, sadamaseaduse § 2 p 3 ja § 3, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järellkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
--	--	--	--	--	--	--	--

			elavat juriidilist ning füüsilist isikut, samuti ka välispartnereid. Ohtu võib sattuda kogu EV veeliikluse teeninduse turvalisus, sh kavandatud laevaihenduste läbilaskevõime, inimeste julgeolek, elu ja tervis ning keskkonna puhtus. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.				
18.	Mereveoteenus, reisijate ja kauba vedamiseks sisevetes, merel ja rannavetes	Reisijate ja kauba vedaja merel ja rannavetes. Teenuste osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA	Ohtudeks on reisijate ja kaubavedude korraldamisel kasutatava arvutivõrgu ja sellega seotud infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine, õnnestunud küberrünne ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 725/2004,

		järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Tegemist on transpordivaldkonnas olulist rolli kandva majandustegevusega, mille kaudu tagatakse EV territoriaal- ja sisemeres ohutu ning turvaline veeliiklus kauba- kui ka reisijateveol. Tegemist on ühiskonna poolt laiaulatuslikult kasutusele võetud ja eluliselt tähtsa teenusega, mis puudutab igat Eestis tegutsevat ja elavat juriidilist ning füüsilist isikut, samuti ka välispartnereid. Ohu realiseerumisel on mõjutatud kogu EV veeliikluse teeninduse turvalisus, sh inimeste julgeolek, elu ja tervis ning keskkonna puhtus. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.				KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
19.	Maanteetranspordis liikluskorralduses ja liikuvuse juhtimiseks kasutava intelligentse	Intelligentse transpordisüsteemi omanik ja haldaja. Teenuste osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised,	Ohtudeks on intelligentse transpordisüsteemiga seotud infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine, õnnestunud küberrünne ja kogutud andmete tervikluse, konfidentsiaalsuse ja	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektorიაalsed riskianalüüsid,

	transpordisüsteemi käitamine	infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	käideldavuse kadu. Turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Tegemist on transpordivaldkonnas olulist rolli kandva majandustegevusega, mille kaudu tagatakse EV maanteetranspordis ja liideste jaoks teiste transpordiliikidega ohutu ning turvaline maanteeliiklus. Tegemist on ühiskonna poolt laiaulatuslikult kasutusele võetud ja eluliselt tähtsa teenusega, mis puudutab igat Eestis tegutsevat ja elavat juriidilist ning füüsilist isikut, samuti ka välispartnereid. Ohu realiseerumisel on mõjutatud kogu EV maanteeliikluse teeninduse turvalisus, sh inimeste julgeolek, elu ja tervis. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud				valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, Liiklusseaduse § 6¹ lg 1, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järellkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
--	---	--	---	--	--	--	--

			turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja intelligentse transpordisüsteemi haldamise halvamiseks.				
20.	Digitalse teenuse (pilvandmetöötluste enuse osutamine, sisulevivõrguteenus e osutamine, internetipõhise kauplemiskoha pidaja ja veebipõhise otsingumootori või sotsiaalmeediaplatformi pidaja) osutamine	Teenuste osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus. NB! Rakendatakse ainult järelkontrolli meedet, kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on digitaalse teenuse osutamisel kasutatava arvutivõrgu ja sellega seotud infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine, õnnestunud küberrünne ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu. Turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu IT-taristu turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toob kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Digitaalse teenuse vahendusel on tekkinud igapäevane Eesti riigi, majanduse ja elanikkonna ulatuslik sõltuvus info- ja kommunikatsioonitehnoloogiast (IKT-st) ja e-teenustest, sh e-teenuste platvormidest, mille toimivuse ja	harv	piiratud	madal	Ametile laekunud vihjed ja pöördumised võimalike turvanõrkuste rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

			kättesaadavuse nõue on teenuste tarbijate poolt peaaegu et igapäevaelu korraldamiseks ja toimimiseks vajalik. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.				
--	--	--	---	--	--	--	--

21.	eIDAS- kohased kvalifitseeritud usaldusteenused: 1.e-allkirjade, e-templite või veebiserverite autentimise sertifikaatide väljastamine ja elutsükli haldus; 2. ajatempliteenus; 3. e-allkirjade, e-templite sertifikaatide säilitamise teenus; 4. e-allkirjade, e-templite valideerimise teenus; 5. e-andmevahetusteenus 6. e-allkirja või e-templi kaugloomise vahendite haldamise teenus; 7. elektrooniliste tõendite väljastamise teenus; 8. elektrooniliste tõendite valideerimise teenus; 9. registreeritud e-andmevahetusteenuse kaudu edastatud	Usaldusteenuse osutamiseks vajaliku tegevusloa olemasolu, teenuste osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk) ja selle turvalisuse vastavus nõuetele; infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; usaldusmärgi nõuetekohane kasutamine; väljast tellitud IT teenuslepingud.	Ohtudeks on usaldusteenuse osutamisel kasutatava arvutivõrgu ja sellega seotud infosüsteemide töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbepoliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks. Usaldusteenused on muutunud Eestis ühiskonna igapäevaste elu toimingutes vajalikuks osaks ning teenuse kasutajate hulk on valdav osa Eesti kodanikest ja era- ning avalikest	sage	tõsine	kõrge	CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused. Ametile laekunud vihjed ja pöördumised. eIDAS-e ja selle alusel antud rakendusaktide ning EUTS nõuded, KÜTS nõuded, KorS § 2, § 4, § 5 ja § 49.
-----	--	--	---	------	--------	-------	--

	andmete ja nendega seotud tõendite valideerimise teenus 10.elektronilise arvestusraamatu teenus.		teenustest. Loata tegutsemise puhul ei ole kontrollitud usaldusteenuse vastavust teenusele kehtestatud nõuetele, mis seab otseselt ohtu nõutud turvalisuse tasemega teenuse tagamise usaldusteenuse kasutajale e-tehingutes. Usaldusmärgi väärkasutamine tekitab selle teenuse kasutajale vale mulje teenuse turvalisuse tasemest.				
22.	eIDAS- kohased mitte kvalifitseeritud usaldusteenused: 1.e-allkirjade, e-templite või veebiserverite autentimise sertifikaatide väljastamine ja elutsükli haldus; 2. ajatempliteenus; 3. e-allkirjade, e-templite sertifikaatide säilitamise teenus; 4. e-allkirjade, e-templite valideerimise teenus; 5. e-andmevahetusteenus	Mitte kvalifitseeritud usaldusteenuse osutajad. Teenuste osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk) ja selle turvalisuse vastavus nõuetele; infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; usaldusmärgi nõuetekohane kasutamine; väljast tellitud IT teenuslepingud. NB! Riiklikus järelevalves rakendatakse ainult järelkontrolli meedet, kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel kasutatava arvutivõrgu ja sellega seotud infosüsteemide töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne ja kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbe poliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT	harv	piiratud	madal	Ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, eIDAS-e ja selle alusel antud rakendusaktide ning EUTS nõuded, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

	6. e-allkirja või e-templi kaugloomise vahendite haldamise teenus; 7. elektrooniliste tõendite väljastamise teenus; 8. elektrooniliste tõendite valideerimise teenus; 9. registreeritud e-andmevahetusteenuse kaudu edastatud andmete ja nendega seotud tõendite valideerimise teenus 10.elektroonilise arvestusraamatu teenus.		teenustel üldsõnalised teenuslepingud. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.				
23.	Infosüsteemide andmevahetuskihiga liitumine	Infosüsteemide andmevahetuskihiga (edaspidi X-tee) liituda soovivad isikud ja liikmed. X-teega liitumiseks vajaliku taotluse ja liitumiskokkulepete olemasolu.	Nõuetekohase taotluse mitte esitamine ja liitumiskokkuleppe puudumine. Ohuks on illegaalne, tingimusteta ning vastutuseta andmete vahetamine (X-teega on ühendatud ettevõtete infosüsteemid kellel puudub keskusega liitumiskokkulepe).	harv	piiratud	madal	X-tee osakonnalt laekunud teave potentsiaalsete liitujate osas, ametile laekunud vihjed ja pöördumised, AvTS § 43 ⁹ lg 1p 5 nõuded.

24.	Avaliku korra e ühiskonna seisundi tagamine	Avaliku korra e ühiskonna seisundi tagamiseks vajalike võrgu- ja infosüsteemide, teenusplatvormide pakkujad/omanikud, arendajad, haldajad, (eraettevõtted). Teenuse osutamiseks kasutatav IT-taristu turvaline tehniline lahendus (kasutatavad infosüsteemid, infovarad, arvutivõrk). NB! Ainult kestva ohu või ohukahtluse kõrvaldamine.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks. Teenuse- ja rakenduspõhised infosüsteemid on muutunud Eestis ühiskonna igapäevaste elu toimingutes vajalikuks osaks ning teenuse kasutajate hulk on valdav osa Eesti kodanikest ja era- ning avalikest teenustest, kes on ühtlasi ohu realiseerumisel mõjutatud.	harv	tõsine	keskmine	CERT-EE/ AEO asetleidnud intsidendi juurpõhjus ja selle mõjuulatus. Ametile laekunud vihjed ja pöördumised. KorS § 2, § 4, § 5 ja § 49.
-----	---	--	---	------	--------	----------	--

25.	Digitaaalse teenuse (Andmekeskusteenuse) osutamine	Andmekeskusteenuse osutaja. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seiremeetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meetet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks. Andmekeskusteenus on muutunud Eestis ühiskonna igapäevaste elu toimingutes vajalikuks osaks digitaalsete andmete töötlemisel ja nende turvalisel säilitamisel. Teenuse kasutajate hulk on valdav osa era-	harv	tõsine	keskmine	1. CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

			ning avalikest teenustest, kes on ühtlasi ohu realiseerumisel mõjutatud. Kaudselt mõjutab teenuse ebaturvalisus igat Eesti kodanikku, kelle andmeid andmekeskustes töödeldakse ja säilitatakse.				
26.	Elektrienergia hulgimüüjatele või lõpptarbijatele elektrienergia müümine	Elektrienergia müüja e teenuse osutaja. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkumine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks. Elektrienergia müümine on muutunud Eestis ühiskonna igapäevase elu toimimise osa.	harv	tõsine	keskmine	CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, elektrituruseadus § 6 lg 1 p 7, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järellkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta,

			Teenuse kasutajate hulk on valdav osa elektrienergia hulgimüüjad ja lõpptarbijad, kes on ohu realiseerumisel mõjutatud.				KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
27.	Elektrienergia tootmine	Elektrienergia tootja e teenuse osutaja. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks. Elektrienergia tootmine on muutunud Eestis ühiskonna igapäevaste elu toimingutes vajalikuks osaks. Teenuse kasutajate hulk on valdav osa elektrienergia hulgimüüjad ja	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, elektrituruseadus §3 p 24, § 6 lg 1 p 1, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

			lõpptarbijad, kes on ohu realiseerumisel mõjutatud.				
28.	Elektrisõiduki laadimispunkti haldamine ja käitamine	Elektrisõiduki laadimispunkti käitamise/haldamise teenuse osutaja. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meetet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.	harv	piiratud	madal	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, elektrituruseadus §3 p 13¹, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

29.	Jaotusvõrgu teenuse osutamine	Jaotusvõrguettevõtja elektrituruseaduse tähenduses. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meetet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks. Elektrienergia edastamine jaotusvõrgu kaudu on muutunud Eestis ühiskonna igapäevaste elu toimingutes vajalikuks osaks. Teenuse kasutajate hulk on valdav osa elektrienergia hulgimüüjad ja lõpptarbijad, kes on ohu realiseerumisel mõjutatud.	harv	tõsine	keskmine	1. CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektorიაalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, elektrituruseadus §3 p 11, § 8 lg 3, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
-----	--------------------------------------	---	---	------	--------	----------	---

30.	Määratud elektriturukorraldamine	Määratud elektriturukorraldaja. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seiremeetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meetet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenuse toimimise halvamiseks. Teenuse kasutajate hulk on valdav osa elektrienergia hulgimüüjad ja lõpptarbijad, kes on ohu realiseerumisel mõjutatud.	harv	tõsine	keskmine	1. CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidenti turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidenti juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, Euroopa Parlamendi ja nõukogu määruse (EL) 2019/943 artikkel 2 p 8, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
-----	----------------------------------	--	---	------	--------	----------	--

31.	Põhivõrgu teenuse osutamine	Põhivõrguettevõtja. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenuse toimimise halvamiseks. Teenuse kasutajate hulk on valdav osa elektrienergia hulgimüüjad ja lõpptarbijad, kes on ohu realiseerumisel mõjutatud.	harv	Tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektorიაalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, elektrituruseadus § 3 p 21, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelikontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
32.	Agregeerimine, elektri tarbimise koormuse juhtimine	Agregaatorid ning tarbimiskaja ja energiasalvestusega tegelevad ettevõtjad. Teenuse osutamiseks	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed,	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded,

	(tarbimiskaja) või elektrienergia salvestamine.	kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meetet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenuse toimimise halvamiseks. Teenuse kasutajate hulk on valdav osa elektrienergia hulgimüüjad ja lõpptarbijad, kes on ohu realiseerumisel mõjutatud.				laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, elektrituruseadus § 3 p-id 1², 1³, 8², 23³, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
33.	Joogivee varustamine	Joogiveega varustav joogivee käitleja. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised,	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed

		infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja joogivee varustamisega, sh jaotamisega seotud tegevuste toimimise halvamiseks. Joogiveega varustamine on ühiskonna elukorralduses inimeste igapäevaelu toimimise alustala. Üldise ohuolukorra võimaliku tagajärjena võib saastatud joogivee jagamisel tekkida kahju inimese tervisele, oht elule või halvimal juhul kaasneda surm. Joogivee tarbijateks on iga Eesti juriidiline- ja füüsiline isik e kodanik, kes saab ohu realiseerumisel mõjutatud.				riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, veeseaduse § 17 lg 1, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järellkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
34.	Asulareovee, olmereovee või tööstusreovee	Asulareovee, olmereovee või tööstusreovee kogumise, ärajuhtimise või puhastamise teenuse osutaja.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded,

	kogumine, ärajuhtimine või puhastamine	Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seiremeetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja asulareovee korraldamisega seotud tegevuste toimimise halvamiseks. Asulareovee korraldamine on ühiskonna igapäevaste elukeskkonna toimingutes vajalikuks osaks. Teenuse kasutajate hulk on iga Eesti kodanik, kes saab ohu realiseerumisel mõjutatud.				laekunud intsidendi turvaanalüüs, KIKK sektorიალsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, nõukogu direktiivi 91/271/EMÜ asulareovee puhastamise kohta (EÜT L 135, 30.05.1991, lk 40–52) artikkel 2 punktid 1, 2 ja 3, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
--	---	--	---	--	--	--	---

35.	Maagaasi tootmine, importimine, ülekande, jaotamine, hoiustamine või müümine	Gaasiettevõtja maagaasiseaduse tähenduses. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja maagaasi tootmisega, importimisega, ülekande jaotamisega, hoiustamisega või müümisega seotud tegevuste toimimise halvamiseks. Gaasi tootmine, importimine, ülekande jaotamine, hoiustamine ja müük on ühiskonna igapäevaste eluks vajalike toimingute osaks. Teenuse kasutajateks on pea iga Eesti kodanik,	harv	tõsine	keskmine	1. CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektorიაalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, maagaasiseadus § 4, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
-----	--	--	--	------	--------	----------	--

			kes saab ohu realiseerumisel mõjutatud.				
36.	Maagaasi hoiustamine ja kasutusse andmine (hoidlatevõrgu haldamine)	Hoidlatevõrgu haldur (Maagaasi hoiustamise ülesande täitja ja gaasihoidla nõuetekohase kasutamise eest vastutav ettevõtte). Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja gaasi hoidlatevõrgu haldamisega seotud tegevuste toimimise halvamiseks.	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektorიაalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, maagaasiseadus § 2 lg 17 ja § 17², KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

37.	Veeldatud maagaasi terminali teenuse korraldamine ja haldamine	Veeldatud maagaasi terminali haldur. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja veeldatud maagaasi terminali haldamisega seotud tegevuste toimimise halvamiseks.	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektorიაalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, maagaasiseadus, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järellkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
38.	Maagaasi rafineerimise ja töötlemise rajatise käitamine	Maagaasi rafineerimise ja töötlemise rajatise käitaja. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk);	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi

		infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meetet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	häärimine, katkumine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja maagaasi rafineerimise ja töötlemisega seotud tegevuste toimimise halvamiseks.				turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järellkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
39.	Digitalse teenuse (haldusteenuse või infoturbeteenuse) osutamine	Kliendi ruumides või kaugjuhtimise teel IKT-toodete, võrkude, taristu, rakenduste või muude võrgu- ja infosüsteemide paigaldamist, aktiivset haldamist, käitamist või hooldamistuge pakkuv ettevõtte. Infoturbeteenuse osutamisel riskide juhtimise tuge pakkuv ja selle	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkumine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja	harv	tõsine	keskmine	CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale

		elluviija teenuse osutaja. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja haldusteenuse või infoturbeteenuse osutamisega seotud tegevuste toimimise halvamiseks.				suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 2 punkt 13, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järeelkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
40.	Interneti sõlmpunkti osutamine	Interneti sõlmpunkti teenuse osutaja. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkumine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektorიალsed riskianalüüsid, valdkonnale suunatud

		meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Tegemist on andmesidevaldkonnas olulist rolli kandva majandustegevusega, mille kaudu tagatakse EV territooriumil andmesidevõrgu omavahelised ühendused ja internetiliiklus. Tegemist on eluliselt tähtsa teenusega, mille katkemine mõjutab oluliselt ühiskonna toimimist, riigi julgeolekut, igat Eestis tegutsevat ja elavat juriidilist- ning füüsilist isikut. Ohtu võib sattuda inimeste elu ja tervis, samuti ka välispartnerite vaheline infovahetus. Ohu realiseerumisel on mõjutatud kogu EV internetivõrkude vahelised ühendused ja info liikumine. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.				küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
--	--	--	--	--	--	--	---

41.	Kaugkütte käitamine	Kaugkütte käitamise teenuse osutaja. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seiremeetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meetet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Tegemist on eluliselt tähtsa teenusega, mille katkemine mõjutab oluliselt ühiskonna igapäeva elu, riigi julgeolekut, igat Eestis tegutsevat ja elavat juriidilist- ning füüsilist isikut. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu	harv	tõsine	keskmine	1. CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidenti turvaanalüüs, KIKK sektorიაalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidenti juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, kaugkütteseadus §2 p 2, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
-----	------------------------	---	--	------	--------	----------	--

			realiseerumise tõenäosust küberrünnakuteks ja kaugkütte- ja kaugjahutussüsteemi käitamisega seotud tegevuste toimimise halvamiseks.				
42.	Väärtpaberite kauplemiskoha (reguleeritud väärtpaberiturg, mitmepoolne kauplemissüsteem ja organiseeritud kauplemissüsteem) korraldamine	Väärtpaberite kauplemiskoha korraldaja väärtpaberituru seaduse tähenduses (investeeringusühing ja reguleeritud väärtpaberi turu korraldaja). Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meetet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Tegemist on eluliselt tähtsa teenusega, millel turvanõrkus kujundab märkimisväärset finants-, õiguslikke riske kauplemiskoha kasutajatele ning mõjutab ka kogu finantsturu stabiilsust. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, väärtpaberituru seaduse § 3 KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta,

			väärtpaberite kauplemiskoha korraldamisega seotud tegevuste toimimise halvamiseks.				KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
43.	Kosmosepõhise teenuse osutamist toetava Eesti Vabariigi või eraõigusliku isiku omandis oleva, hallatava või käitatava maapealse taristu käitamine	Kosmosepõhise teenuse osutamist toetava maapealse taristu (nt satelliitside maajaamad, andmetöötluskeskused, juhtimiskeskused) käitaja. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meetet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Tegemist on eluliselt ja ühiskonnale olulist rolli kandva majandustegevusega, sest need võimaldavad toimida mitmetel igapäevaelu ja riigikaitse jaoks hädavajalikel süsteemidel. Kosmosepõhise teenusel toetava maapealse taristu kaudu tagatakse EV territooriumil side ja andmeside toimimine, sh tagatakse kaugemate piirkondade internetiühendus, mereside ja lennundusside toimimine ning varuside kriisiolukordades.	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, väärtpaberituruseaduse § 3 KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelekontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

			Tegemist on eluliselt tähtsa teenusega, mille katkemine mõjutab oluliselt ühiskonna toimimist, riigi julgeolekut, igat Eestis tegutsevat ja elavat juriidilist- ning füüsilist isikut. Ohtu võib sattuda inimeste elu ja tervis, samuti ka välispartnerite vaheline infovahetus. Ohustatud on ka näiteks navigatsioon ja ajasünkroonimine, mille tagajärjel on mõjutatud kõik teenused, kes sõltuvad GPS- ja muud GNSS-süsteemide täpsest ajast ja andmevahetusest (pangatehingud, elektrivõrkude tööd, mobiilsidevõrgud, logistika, transport jne). Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.				
44.	Hoiuste või muude tagasimakstavate vahendite vastuvõtmine avalikkuselt ja laenu andmine, investeerimisteenused (kauplemine oma arvel ja finantsinstrumentide ja/või finantsinstrumentide emissiooni	Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 artikkel 4 p1 kohased krediitiasutused . Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus,

	tagamine kindla kohustuse alusel) osutamine	haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Tegemist on eluliselt tähtsa teenusega, millel turvanõrkus kujundab märkimisväärset finants-, õiguslikke riske laenu andmisel teenuse tarbijatele. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenuse toimimise halvamiseks.				seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 artikkel 4 p1, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
45.	Nafta tootmine, rafineerimise ja töötlemise rajatiste käitamine ning nafta hoiustamine ja ülekandmine	Nafta tootmise, rafineerimise ja töötlemise rajatiste käitamine ning nafta hoiustamise ja ülekandmise teenuse osutamine. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus,

		riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenusega seotud tegevuste toimimise halvamiseks.				seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
46.	Vesiniku tootmine, hoiustamine ja ülekandmine	Vesiniku tootmise, hoiustamise ja ülekandmisega tegelev ettevõtja. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole	harv	tõsine	keskmine	1.CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidenti turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidenti juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja

		NB! Ettevõtja suhtes, kellel on majandusaasta jooksul 50 või rohkem töötajat ja kelle aastabilansimaht või aastakäive ületab 10 miljonit eurot rakendatakse riiklikus järelevalves järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja vesiniku tootmise, hoiustamise ja ülekandmisega seotud tegevuste toimimise halvamiseks.				pöördumised, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49. 2. Järelkontrolli korral ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
47.	Jäätmete käitlemine (jäätmete kogumine, vedamine, taaskasutamine, sealhulgas sortimine, ja kõrvaldamine, sealhulgas vahendamine või edasimüümine)	Jäätmekäitlemisega tegelev ettevõtte. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Riiklikus järelevalves rakendatakse järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine,	harv	piiratud	madal	Ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, jäätmeseadus § 13, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49

			kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja jäätmete käitlemisega seotud tegevuste toimimise halvamiseks.				
48.	Kemikaalide tootmine ja turustamine	Kemikaalide tootmisega ja turustamisega tegelev ettevõtte. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Riiklikus järelevalves rakendatakse ainult järelkontrolli meetet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja kemikaalide tootmise ja turustamisega seotud tegevuste toimimise halvamiseks.	harv	piiratud	madal	Ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 1907/2006 artikkel 3 punktid 3 ja 9 , KüTS nõuded, KorS § 2, § 4, § 5 ja § 49

49.	Toidu, va alkoholi hulгимүүк, tööstuslik tootmine ja/või tööstuslik töötlemine	Toidukäitlemisettevõtte (toidu tootmis-, töötlemis- või turustamisega tegelev ettevõtte), kelle nimetatud tegevusest saadav aastakäive on vähemalt 50 protsenti tema aastakäibest. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Riiklikus järelevalves rakendatakse ainult järelkontrolli meetet, kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja toidukäitlemisega seotud tegevuste toimimise halvamiseks.	harv	piiratud	madal	Ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 178/2002 artikkel 3 punkt 2 KüTS nõuded, KorS § 2, § 4, § 5 ja § 49
50.	osa 26: arvutite, elektroonika- ja optikaseadmete tootmine; - osa 27: elektriseadmete tootmine; - osa 28: mujal liigitamata	Euroopa Liidu majanduse tegevusalade statistilise klassifikaatori NACE Revision 2 C jao osades 26–30 osutatud majandustegevusega tegelev ettevõtja.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete	harv	piiratud	madal	Ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta,

	masinate ja seadmete tootmine; - osa 29: mootorsõidukite, haagiste ja poolhaagiste tootmine; - osa 30: muude transpordivahendite tootmine"	Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud. NB! Riiklikus järelevalves rakendatakse järelkontrolli meedet, kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	tervkluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenusega seotud tegevuste toimimise halvamiseks.				KüTS nõuded, KorS § 2, § 4, § 5 ja § 49
51.	Postisaadetiste kogumine, sorteerimine, vedu ja saajale kättetoimetamine (adresseeritud postisaadetiste edastamine)	Postiteenuse ja kulleriteenuse osutajad. Teenuse osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud	harv	piiratud	madal	Ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49

		NB! Riiklikus järelevalves rakendatakse ainult järelekontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KüTS §-des 7 ja 8 nõudeid.	või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja postiteenusega seotud tegevuste toimimise halvamiseks.				
52.	Teadus- ja arendustegevus	Asutused, mille põhikirjajärgseks põhitegevuseks on teadus- ja arendustegevus. Teaduse- ja arendustegevuseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud.	Ohtudeks on teenuse osutamisel: kasutatava IT-taristu komponendi (infovarad, võrguseadmed, infosüsteemid jne) töö ja toimimise häirimine, katkemine, manipuleerimine, kompromiteerimine, õnnestunud küberrünne, kogutud andmete tervikluse, konfidentsiaalsuse ja käideldavuse kadu, turvanõrkustega võrgu välisühendus(t)e kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine. Turvanõrkustega veebileht. Teenuse osutajatel puudulik IT- riskihaldusprotsess ja	harv	piiratud	madal	Ametile laekunud vihjed ja pöördumised võimalike turvanõuete rikkumise kohta, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

		NB! Riiklikus järelevalves rakendatakse ainult järelkontrolli meedet, st kui RIA järelevalveosakonnal on alust arvata, et teenuse osutaja ei järgi KÜTS §-des 7 ja 8 nõudeid.	riskide käsitluskava, st asutus ei ole endale kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teadustööga seotud tegevuste toimimise halvamiseks.				
--	--	---	--	--	--	--	--