Lisa 1
KINNITATUD
peadirektori 07.02.2025
käskkirjaga nr 1.1-2/25-008

RIIGI INFOSÜSTEEMI AMETI
OHUENNETUSLIKU RIIKLIKU JÄRELEVALVE
OHUPROGNOOS

Tallinn 2025

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 3 kohaselt on küberintsident süsteemis toimuv sündmus, mis ohustab või kahjustab arvutivõrgu- 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 1).

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.

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 ohuprognoosile tuginedes saab pidada võimalikuks olukorda, mille realiseerumisel tekib oht.

Ohuprognoosi 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 ohuprognoosi funktsioon on anda järelevalve sekkumiseks kontrollitav ja arusaadav alus kodanikele, ettevõtjale ning Riigi Infosüsteemi Ametile. Ohuprognoos on ühtlasi aluseks ka iga jooksva kalendriaasta järelevalve tööplaani koostamisele, mis omakorda täpsustab valimit millist kirjeldatud olukordadest jooksval aastal kontrollitakse.

Vastavalt KorS § 24 lg 2 peab ohuprognoos 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 ohuprognoosid. Käesolev ohuprognoos sisaldab nimekirja erinevates valdkondades võimalikest realiseeruda võivatest ohukahtlustest või ohtudest, milliste ennetamiseks on kohane juhinduda KorS § 2, § 4 ja § 5 sätestatust, mis on aluseks RIA-le KüTS §-des 12 ja 14 nimetatud ülesannete täitmiseks.

Lisaks sisaldab käesolev ohuprognoos ka laiaulatusliku tarbijaskonnaga ja ühiskonnas igapäevaelu toimimiseks vajalike baasteenustega seotud ohtude prognoose. 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.

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

Käesolev ohuprognoos on koostatud ohuolukordade objektiivsete tunnuste alusel ja lähtutakse senise järelevalve tulemustest, kehtivatest nõuetest, CERT.EE-le, kriitilise infrastruktuuri küberkaitse osakonna (edaspidi KIKK) sektoriaalsed riskianalüüsid ja analüüsi- ja ennetusosakonnale (edaspidi AEO) laekunud intsidentide turvaanalüüside tulemustest, asetleidnud intsidendi 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 prognoosib oodatavaid kahjusid ja mõjusid.

Käesolevas ohuprognoosis 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 küberintsidendi 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 osutuda 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.


Potentsiaalne kahju
Ähvardab organistsiooni olemasolu
Tõsine
Piiratud
Tühine
Keskmine
Kõrge
Väga kõrge
Väga kõrge
Keskmine
Keskmine
Kõrge
Väga kõrge
Madal
Keskmine
Keskmine
Kõrge
Madal
Madal
Keskmine
Keskmine
Harv
Keskmine
Sage
Väga sage
Riski realiseerumise sagedus
Vajab kohest sekkumist
Vajab sekkumist esimesel võimalusel
Kõrgendatud prioriteediga seire
Aksepteeritav

Riski realiseerumise võimalikkuse tabel.

Jrk nr	**Valdkond**	**Kontrolliese**	**Ohuolukorra kirjeldus, võimalikud tagajärjed**	**Tekkimise tõenäosus ehk realiseerumise võimalikkus** (väga sage/sage/ keskmine/harv) vt Tabel 2	**Mõju ehk potentsiaalne kahju** (ähvardab organisatsiooni: tõsine/piiratud/tühine) vt Tabel 1	**Kriitilisuse tase** (riski tase) vt Joonis 1	**Ohuprognoosi koostamise alus(ed)**
1	Eesti maatunnusega seotud tipptaseme domeeninimede, sh tipptaseme nimeserveri 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 ettevõte 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	Eesti maatunnusega seotud tipptaseme domeeninimede registri haldamine	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 piisavus. Väljast tellitud IT teenuslepingud.	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

		Kestva ohu või ohukahtluse kõrvaldamine.	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 tipptaseme 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	Sihtasutused ja MTÜ-d, riigi osalusega äriühingud ja nende tütarettevõtted nimekirjade https://www.fin.ee/riigihanked-riigiabi-osalused-kinnisvara/riigi-osalused/ariuhingud ja https://www.fin.ee/riigihanked-riigiabi-osalused-kinnisvara/riigi-osalused/sihtasutused alusel. 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 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.

			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	Küberturvalisuse seaduse § 3 lg 1 p 1 teenuste osutamine (ühiskonna toimimise seisukohast olulised ja	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	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				CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale

	elutähtsad teenused)**:**	tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus, väljast tellitud IT teenuslepingud.	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 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				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;			harv	tõsine	keskmine	
	9. vältimatu- ja kiirabi teenus;			harv	tõsine	keskmine	
	10. makseteenus;			keskmine	tõsine	keskmine	
	11. sularaharinglus;			harv	tõsine	keskmine	
	12. kaugküttega varustamine;			sage	tõsine	kõrge	
	13. kohaliku tee sõidetavuse tagamine;			keskmine	tõsine	keskmine	

	14. veega varustamine ja kanalisatsioon;		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.	sage	tõsine	kõrge	
5	ESS-kohase elektroonilise side teenuse osutamine (sideteenus, kriitilise tähtsusega side teenus, mereraadioside, operatiivraadiosi devõrgu teenus)	Sideettevõtjad. Teenuste osutamiseks 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.	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-	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,

			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 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.				ESS §-s 87^2 § 87^2 lõike 6, § 100^3 lõike 3, § 100^4 lõike 2 ja § 100^5 lõike 2, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.
6	Tervishoiuteenuste korraldamine (haiglavõrku kuuluvate piirkondliku haigla ja keskhaigla pidaja statsionaarse eriarstiabi	Kõik haiglad, kiirabid. Tervishoiuteenustes kasutatava võrgu- ja infosüsteemide 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	Ohtudeks on tervishoiuteenuste 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	sage	tõsine	kõrge	CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv,

	osutamine, kiirabibrigaadi pidaja kiirabi osutamine)	riskide käsitluskava; intsidentide haldus, väljast tellitud IT teenuslepingud.	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. 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 tervishoiuasutuse 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 puutumatusele (riive privaatsusele), oht elule või halvimal juhul kaasneda surm.				asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded. KorS § 2, § 4, § 5 ja § 49.

7	Üldarstiabi teenuse korraldamine	Perearstid. Tervishoiuteenustes üldarstiabi teenustes 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 tervishoiuteenuste 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-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 tervishoiuasutuse teenuseid. Üldise ohuolukorra võimaliku tagajärjena võib saada muuta	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, KorS § 2, § 4, § 5 ja § 49.

			eriliigilisi isiku- ja terviseandmeid (patsiendiandmed) või need sattuda kolmandate isikute valdusesse, tekkida kahju inimese tervisele, oht eraelu puutumatusele (riive privaatsusele), oht elule, või halvimal juhul kaasneda surm.				
8	Raudteeinfrastruktuuri majandamine ja toimimise korraldamine, 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 haldus; väljast tellitud IT teenuslepingud.	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 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	sage	piiratud	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, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

			tulnud turvaaukude mitte parandamine. Tegemist on transpordivaldkonnas keskset rolli kandva majandustegevusega, mille kaudu tagatakse õiglane konkurentsiolukord 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.				
9	Lennuliikluse teenindamine ja korraldamine	Lennuvälja käitaja ning Tallinna lennuinfopiirkonnas lennuliikluse teenindamist tagav aeronavigatsiooniteenuse osutaja. Teenuste osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste	Ohtudeks on lennuvälja käitaja 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	harv	tõsine	keskmine	CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud

		tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud.	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 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 lennuliikluse teenindamise turvalisus, sh kavandatud lennuühenduste läbilaskevõime, inimeste julgeolek, elu ja tervis. Turvanõrkustega ja puuduliku turvalisusega IT-taristu				intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

			loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.				
10	Sadamateenuse korraldamine ja rahvusvahelise meresõidus sõitvate reisilaevade ning rannasõidus sõitvaid I kategooria laevade või A-klassi reisilaevade teenindamine	Sadamateenuse osutaja ja/või sadama omanik. 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.	Ohtudeks on sadamateenuses või rahvusvahelise meresõidus sõitvate reisilaevade ning rannasõidus 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	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, KüTS nõuded, KorS § 2, § 4, § 5 ja § 49.

			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 elavat juriidilist ning füüsilist isikut, samuti ka välispartnereid. Ohtu võib sattuda kogu EV veeliikluse teeninduse turvalisus, sh kavandatud laevaühenduste 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.				
11	ESS kohase kaabelleviteenuse osutamine ja ringhäälinguvõrgu teenuse osutamine	Kaabelleviteenuse ja ringhäälinguvõrgu teenuse osutaja (AS STV, Levira AS, Elisa Eesti AS, Telia Eesti AS jne). Teenuste osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh haavatavuste ja turvanõrkuste	Ohtudeks on kaabelleviteenuse ja ringhäälinguvõrgu 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	harv	tõsine	keskmine	CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus

		tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud.	(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- riskianalüüs 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 laiaulatuslikult kasutusele võetud meedialahendusi, sh raadioprogrammide- ja telekanalite edastamist, teleülekannete tootmist pakkuva majandustegevusega, mis on informatsiooni jagamisel eluliselt väga tähtsal kohal ning mille katkemine mõjutab oluliselt ühiskonna toimimist, riigi julgeolekut, igat Eestis tegutsevat ja elavat juriidilist ning füüsilist isikut, samuti ka välispartnereid. Ohtu võib sattuda Eesti territooriumit katva ringhäälinguvõrgu taristu, sh ca 280 000 kasutajaga digi-TV levivõrgu ja nende vahendusel teleprogrammide ja kanalite edastamise toimivus, turvalisus ning inimeste julgeolek, elu ja tervis. Turvanõrkustega ja puuduliku turvalisusega IT-taristu				ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded, ESS (§ 87-2 lg 6), KorS § 2, § 4, § 5 ja § 49.

			loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab riski realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.				
12	Digitaalse teenuse osutamine (internetipõhise kauplemiskoha, otsimootori ja pilveandmetöötlusteenuse 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! tehakse järelevalvet ainult siis, kui esitatakse kaebus.	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	CERT-EE/ AEO küberteemalised statistilised aruanded, laekunud intsidendi turvaanalüüs, KIKK sektoriaalsed riskianalüüsid, valdkonnale suunatud küberrünnete kasv, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, ametile laekunud vihjed ja pöördumised, KüTS nõuded.

			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.				

13	eIDAS- kohased 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-andmevahetuste enus 6. e-allkirja või e-templi kaugloomise vahendite haldamise teenus; 7. elektrooniliste tõendite väljastamise teenus; 8. elektrooniliste tõendite	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	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. eIDAS-e ja selle alusel antud rakendusaktide ning EUTS nõuded, KorS § 2, § 4, § 5 ja § 49.

	valideerimise teenus; 9. registreeritud e-andmevahetuste enuse kaudu edastatud andmete ja nendega seotud tõendite valideerimise teenus 10.elektroonilise 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.				
14	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.
15	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). 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	harv	tõsine	keskmine	CERT-EE/ AEO asetleidnud intsidendi juurpõhjus ja selle mõjuulatus. Ametile laekunud vihjed ja pöördumised. KorS § 2, § 4, § 5 ja § 49.

			kasutamine. Turvanõrkustega veebileht. 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.				