

Lisa 1  
KINNITATUD  
Riigi Infosüsteemi Ameti  
peadirektori 25.01.2024  
käskkirjaga nr 1.1-2/24-005

RIIGI INFOSÜSTEEMI AMETI  
OHUENNETUSLIKU RIIKLIKU JÄRELEVALVE  
OHUPROGNOOS

Tallinn 2024

Vastavalt Riigi Infosüsteemi Ameti põhimääruse §-le 7 teostab 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 ohuprognosile tuginedes saab pidada võimalikuks olukorda, mille realiseerumisel tekib oht.

**Ohuprognosiooni 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 ohuprognosiooni funktsioon on anda järelevalve sekkumiseks kontrollitav ja arusaadav alus kodanikele, ettevõtjale ning Riigi Infosüsteemi Ametile. Ohuprognos 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 ohuprognos põhinema faktidel või korrakaitseorgani teaduslikel või tehnilistel teadmistel või Euroopa Liidu õigusaktist tuleneval järelevalvekohustusel ning lähtuma võrdse kohtlemise põhimõttest.

Tulenevalt eeltoodust on Riigi Infosüsteemi Ameti koostanud küberturvalisuse teenistuse ülesannetega kaetud tegevusvaldkondade ohte käsitlevad ohuprognosid. Käesoleva ohuprognos 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 ohuprognosis 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.

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

Käesolev ohuprognosis on koostatud ohuolukordade objektiivsete tunnuste alusel ja lähtutakse senise järelevalve tulemustest, kehtivatest nõuetest, CERT.EE-le ja AEO-le 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 ohuprognosis arvestatakse valdkondlikku kriitilisuse taset (riskitase) allpool väljatoodud riskimaatriksi abil, mille tulemusel selgub järelevalve teostamise prioriteedid ja meetodika 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 realiseerumisega kaasnev **potentsiaalne kahju** liigitub järgmiselt:

Tabel 1.

Kahju suurus	Kahju tagajärjed
Ähvardab organisatsiooni olemasolu	Võivad ulatuda katastroofilise tasemeni, mis ähvardab organisatsiooni olemasolu, st rohkem kui 1,5% aasta eelarvest.
Tõsine	Võivad olla tõsised, st kuni 1,5% aasta eelarvest.
Piiratud	On piiratud ja nendega saab hakkama.
Tühine	On väiksed ja saab jätta arvestamata.

**Riski realiseerumise võimalikkust** võib liigitada läbi sageduse määratud ajavahemiku (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.

	<b>Riskitase</b>	<b>Tegevus</b>
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.
Kõrge	Turvameetmed ei kaitse selle ohu eest piisavalt.	Riski vähendamine on prioriteet, selleks plaanitakse asjakohased tegevused, mida rakendada esimesel võimalusel.
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 ohu 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)	Ohuprognosi koostamise alus(ed)
1	Eesti maatumnusega seotud tipptaseme domeeninimed, sh tipptaseme nimeserveri teenuse osutamine	DNS teenuse pakkujad (nt Eesti Interneti Sihtasutus-EIS, Riigivõrk-ASO, Eesti Hariduse ja Teaduse andmesidevõrk EENET). 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 maatumnusega .ee Interneti infrastruktuur ja veebilehtede kompromiteerimine, kasutamise katkemine, õnnestunud küberrünne ja kogutud andmete tervikluse ja käideldavuse kadu. Turvanõrkustega välisvõrgu kaitse (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbe poliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvestimine ja haavatavuste seire. Turvanõrkustega veebileht. DNS teenuse pakkujal puudulik IT-riskihaldusprotsess ja riskide käsitluskava, st ettevõtte ei ole endale	harv	tõsine	keskmine	CERT-EE/ AEO laekunud intsidendi turvaanalüüs, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded, KorS §2, §4, §5 ja §49.

			<p>kõiki riske teadvustanud, mis omakorda toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. DNS teenuse, sh tiptaseme nimeserveri toimise 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 ohu realiseerumise tõenäosust küberrünnakuteks ja teenuse toimimise halvamiseks.</p>				
2	Eesti maatunnusega seotud tiptaseme domeeninimede registri haldamine	Tiptaseme domeeninimede registri omanik ja registripidaja EIS ning teised akrediteeritud registripidajad ( <a href="https://www.internet.ee/registripidajad/akrediteeritud-registripidajad">https://www.internet.ee/registripidajad/akrediteeritud-registripidajad</a> ), 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 küberrünnak ning ja kogutud andmete tervikluse ja käideldavuse kadu. Turvanõrkustega välisvõrgu kaitse (tulemüür) küberrünnakute 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	harv	tõsine	keskmine	CERT-EE/ AEO laekunud intsidendi turvaanalüüsi tulemused, asetleidnud intsidendi juurpõhjus ja selle mõjuulatu, KorS §2, §4, §5 ja §49.

			registripidaja teenuse, sh majutusteenuse toimise häirimisel või katkemisel on mõjutatud selle registripidaja juures domeenime registreerinud Eesti Interneti kasutajaskond. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust Eesti maatunnusega seotud tiptaseme nimeserveri küberrünnakuteks ja teenuse toimimise halvamiseks.				
3	Elektronpanganduse teenus pankadele kaardimaksede töötlemise ning ühiskasutuse süsteemi haldamisel ning makseteenuste vahendamisteenus.	(NETS Estonia AS, Maksekeskus jt). Teenuse osutamiseks IT-taristu (kasutatavad infosüsteemid ja- varad, arvutivõrk) turvalisuse tagamiseks kasutatud infotehnilised meetmed, sh haavatavuste ja turvanõrkuste tuvastamise seire meetmed ja nende piisavus.	Ohtudeks on elektronpanganduses kaarditehingute autoriseerimise, töötlemise, haldamise ja maksehingute korralduse katkemine, kompromiteerimine, õnnestunud küberrünne ning krediidiandmete tervikluse, konfidentsiaalsuse, käideldavuse kadu. Samuti riigisiseste pankade sh rahvusvaheliste kaardiorganisatsioonide (VISA, MasterCard, American Express) sularahautomaatide omavahelist riskasutust korraldava ühiskasutussüsteemi katkemine ja kompromiteerimine. Turvanõrkustega välisvõrgu kaitse (tulemüür) küberrünnete tuvastamiseks, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik IT-taristu turvatestimise ja haavatavuste seire. Turvanõrkustega veebileht.	keskmine	tõsine	keskmine	CERT-EE analüüsi tulemused, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, KorS §2, §4, §5 ja §49, Eesti Panga Presidendi 13.07.2018 määrus nr 7 „Makseteenuste ja sularaharingluse kirjeldus ja toimepidevuse nõuded“

			<p>Igasugune tehniline tõrge või kõrvalekalle elektronpanganduse teenuse osutaja teenustes, mõjutab igat Eestis tegutsevat teenuseosutajat ja tavainimesi, kes kasutavad teenuste eest tasumisel pangakaarti või teisi makseteenuseid vahendavaid teenuseid. Teenus on muutunud inimeste ja teenuseosutajate igapäevaelu korraldamise lahutamatuks osaks ja muutunud ühiskonna mugavusteenuste pakkumisel teenusest 24/7 sõltuvaks. Mõjutab otseselt elutähtsaid teenuseid nagu makseteenuseid (näiteks teenuseosutaja osutatavad pangasisesed maksed ja kaardimaksed ja teenuseosutaja vahelised maksed). 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.</p>				
4	Riigi osalusega ettevõtete avalikud teenused.	<p>Sihtasutused ja MTÜ-d, riigi osalusega äriühingud ja nende tütarettevõtted nimekirjade <a href="https://www.fin.ee/riigihanked-riigiabi-osalused-kinnisvara/riigi-osalused/ariuhingud">https://www.fin.ee/riigihanked-riigiabi-osalused-kinnisvara/riigi-osalused/ariuhingud</a> ja <a href="https://www.fin.ee/riigihanked-riigiabi-osalused-kinnisvara/riigi-osalused/sihtasutused">https://www.fin.ee/riigihanked-riigiabi-osalused-kinnisvara/riigi-osalused/sihtasutused</a> alusel. Teenuste osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid ja- varad, arvutivõrk); infosüsteemide turvalisuse</p>	<p>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</p>	sage	tõsine	kõrge	CERT-EE/ AEO laekunud intsidendi turvaanalüüs, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded,

		<p>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.</p>	<p>infoturbe poliitika, 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 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 ohu realiseerumise tõenäosust</p>				<p>KorS §2, §4, §5 ja §49.</p>
--	--	--	--	--	--	--	--------------------------------

			küberrünnakuteks ja teenuste toimimise halvamiseks.				
5	Küberturvalisuse seaduse § 3 lg 1 p 1 teenuste osutamine (Ühiskonna toimimise seisukohast olulised ja 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 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 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				CERT-EE/ AEO laekunud intsidendi turvaanalüüs, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevahtemenetluste 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	harv			tõsine	keskmine		
6. Mobiiltelefoniteenus;	harv			tõsine	keskmine		
7. andmesideteenus ;	harv			tõsine	keskmine		
8. elektrooniline isikutuvastamine ja digitaalne allkirjastamine	sage			tõsine	kõrge		
9. Vältimatu- ja kiirabi teenus;	sage			tõsine	kõrge		

	10. Makseteenus;		<p>ühiskonna toimimist ja ohtu võib sattuda</p> <p>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.</p> <p>Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatataavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu 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.</p>	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;			harv	tõsine	keskmine	
6	ESS-kohase elektroonilise side teenuse osutamine (sideteenus, kriitilise tähtsusega side teenus, mereraadioside,	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;	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	harv	tõsine	keskmine	CERT-EE/ AEO laekunud intsidendi turvaanalüüs, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste

	operatiivraadiosi de-võrgu teenus)	IT-riskihaldusprotsess ja riskide käsitluskava; turvaaudit; intsidentide haldus, väljast tellitud IT teenuslepingud.	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 teenustel üldsõnalised teenuslepingud. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine. Tegemist on ühiskonna poolt laialt kasutatavate 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 ohu realiseerumise tõenäosust küberrünnakuteks ja teenuste				tulemused, ametile laekunud vihjed ja pöördumised,  ESS §-s 87 <sup>2</sup> § 87 <sup>2</sup> lõike 6, § 100 <sup>3</sup> lõike 3, § 100 <sup>4</sup> lõike 2 ja § 100 <sup>5</sup> lõike 2, KorS §2, §4, §5 ja §49.
--	------------------------------------	--	--	--	--	--	--

			toimimise halvamiseks. Halvimal juhul võib tekkida võimalus eri- ja hädaolukorra tekkeks hädaolukorra seaduse mõistes.				
7	Tervishoiuteenuste korraldamine (haiglavõrku kuuluvate piirkondliku haigla ja keskhaigla pidaja statsionaarse eriarstiabi osutamine, kiirabibrigaadi pidaja kiirabi osutamine)	Kõik haiglad, kiirabid. Tervishoiuteenustes kasutava 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 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. 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 teatataavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja tervishoiuteenuste toimimise	sage	tõsine	kõrge	CERT-EE/ AEO laekunud intsidendi turvaanalüüs, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KÜTS nõuded. KorS §2, §4, §5 ja §49.

			<p>halvamiseks. Ohu 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 puutumatusse (riive privaatsusele), oht elule, või halvimal juhul kaasneda surm.</p>				
8	<p>Üldarstiabi teenuse korraldamine.</p>	<p>Perearstid. Tervishoiuteenustes üldarstiabi teenustes kasutava 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.</p>	<p>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 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 toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Turvanõrkustega ja</p>	sage	tõsine	kõrge	<p>CERT-EE/ AEO laekunud intsidendi turvaanalüüs, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded, KorS §2, §4, §5 ja §49.</p>

			<p>puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja tervishoiuteenuste toimimise halvamiseks. Ohu 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 puutumatusel (riive privaatsusele), oht elule, või halvimal juhul kaasneda surm.</p>				
9	<p>Raudteeinfrastruktuuri majandamine ja toimimise korraldamine, kauba ja reisijateveo ning veduriteenuse toimimise korraldamine</p>	<p>Raudteeinfrastruktuuri-ettevõtjad (AS Eesti Raudtee, Edelaraudtee Infrastruktuuri AS), kauba- või reisijateveo korraldajad. Raudteeinfrastruktuuri halduseks ja kauba ning reisijateveoks 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.</p>	<p>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 seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire.</p>	keskmine	Tõsine	keskmine	<p>CERT-EE/ AEO laekunud intsidendi turvaanalüüs, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded, KorS §2, §4, §5 ja §49.</p>

		<p>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.</p> <p>Tegemist on transpordivaldkonnas keskset 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 ohu realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.</p>			
--	--	---	--	--	--

10	Lennuliikluse teenindamine ja korraldamine	Lennuvälja käitaja ning Tallinna lennuinfoiirkonnas lennuliikluse teenindamist tagava aeronavigatsiooniteenuse osutaja. 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 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 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 teenustel üldsõnalised teenuslepingud. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatatavaks tulnud turvaaukude mitte parandamine.  Tegemist on transpordivaldkonnas olulist rolli kandva majandustegevusega, mille kaudu	harv	tõsine	keskmine	CERT-EE/ AEO laekunud intsidenti turvaanalüüs, asetleidnud intsidenti juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded, KorS §2, §4, §5 ja §49.

			<p>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 loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.</p>				
11	<p>Sadamateenuse korraldamine ja rahvusvahelise meresõidus sõitvate reisilaevade ning rannasõidus sõitvaid I kategooria laevade või A-klassi reisilaevade teenindamine</p>	<p>Sadamateenuse osutaja ja/või sadama omanik. Teenuste osutamiseks kasutatakse 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.</p>	<p>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</p>	harv	tõsine	keskmine	<p>CERT-EE/ AEO laekunud intsidenti turvaanalüüs, asetleidnud intsidenti juurpõhjus ja selle mõjuulatus, seniste järelevalvemenetluste tulemused, ametile laekunud vihjed ja pöördumised, KüTS nõuded, KorS §2, §4, §5 ja §49.</p>

			<p>(tulemüür) küberrünnete tuvastamiseks, nõrk infoturbe poliitika, kasinalt seadistatud või uuendamata tark- ja riistvara kasutamine, puudulik sisevõrgu ressursside turvatestimine ja haavatavuste seire.</p> <p>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 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 laevühenduste läbilaskevõime, inimeste julgeolek, elu ja tervis ning</p>			
--	--	--	--	--	--	--

			keskkonna puhtus. 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.				
12	ESS kohase Kaabelleviteenu se 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 tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus; väljast tellitud IT teenuslepingud.	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 (tulemüür) küberrünnete tuvastamiseks, nõrk infoturbe poliitika, 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 toovad kaasa ohte ja riske ennetavate ning leevendavate meetmete puudumise. Sisseostetud IT teenustel üldsõnalised teenuslepingud. Turvanõrkustega ja puuduliku turvalisusega IT-taristu	harv	tõsine	keskmine	CERT-EE/ AEO laekunud intsidendi turvaanalüüs, asetleidnud intsidendi juurpõhjus 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. 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 ringhäälinguvõrgutaristu, 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 loomine, kasutamine ning teatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.				
13	Digitaalse teenuse osutamine (internetipõhise kauplemiskoha, otsimootori ja	Teenuste osutamiseks kasutatav IT-taristu (kasutatavad infosüsteemid, infovarad, arvutivõrk); infosüsteemide turvalisuse tagamiseks kasutatavad alalised, infotehnilised ja organisatsioonilised turvameetmed, sh	Ohtudeks on digitaalse teenuse osutamisel kasutatava arvutivõrgu ja sellega seotud infosüsteemide töö ja toimimise häirimine, katkemine, kompromiteerimine, õnnestunud küberrünne ja kogutud andmete	harv	piiratud	madal	CERT-EE/ AEO laekunud intsidendi turvaanalüüs, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus,

	<p>pilveandmetöötl usteenuse osutamine)</p>	<p>haavatavuste ja turvanõrkuste tuvastamise seire meetmed; IT-riskihaldusprotsess ja riskide käsitluskava; intsidentide haldus. <b>NB! tehakse järelevalvet ainult siis, kui esitatakse kaebus.</b></p>	<p>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 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 toovad 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 kättesaadavuse nõue on teenuste tarbijate poolt peaaegu, et igapäevaelu korraldamiseks ja toimimiseks vajalik. Turvanõrkustega ja puuduliku turvalisusega IT-taristu loomine, kasutamine ning teatatavaks tulnud turvaaukude mitte parandamine tekitab soodsa olukorra ja tõstab ohu realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.</p>			<p>ametile laekunud vihjed ja pöördumised, KÜTS nõuded.</p>
--	---	--	---	--	--	---

14	<p>eIDAS- kohased usaldusteenused:</p> <p>1. E-allkirjade, e-templite või veebiserverite autentimise sertifikaatide väljastamine ja elutsükli haldus;</p> <p>2. Ajatempliteenus;</p> <p>3. E-allkirjade, e-templite sertifikaatide säilitamise teenus;</p> <p>4. E-allkirjade, e-templite valideerimise teenus;</p> <p>5. E-andmevahetuste enus</p>	<p>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.</p>	<p>Ohtudeks on usaldusteenuse 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.</p> <p>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 ohu realiseerumise tõenäosust küberrünnakuteks ja teenuste toimimise halvamiseks.</p> <p>Usaldusteenused on muutunud Eestis ühiskonna igapäevaste elu toimingutes vajalikuks osaks ning teenuse kasutajate hulk on valdavosa eesti kodanikest ja era-ning avalikest</p>	sage	tõsine	keskmine	<p>CERT-EE/ AEO laekunud intsidendi turvaanalüüs, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus, seniste järelevamenetluste tulemused. Ametile laekunud vihjed ja pöördumised. eIDAS ja EUTS nõuded, KorS §2, §4, §5 ja §49.</p>
----	---	---	--	------	--------	----------	--

			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 kuvab selle teenuse kasutajale vale mulje.				
15	Infosüsteemide andmevahetuskihiga liitumine	Infosüsteemide andmevahetuskihiga (edaspidi X-tee) liituda soovivad isikud ja liikmed. X-teeaga liitumiseks vajaliku taotluse ja liitumiskokkulepete olemasolu.	Nõuetekohase taotluse mitte esitamine ja liitumiskokkuleppe puudumine. Ohuks on illegaalne, tingimusteta ning vastutuseta andmete vahetamine (X-teeaga 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 <sup>9</sup> lg 1p 5 nõuded.
16	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). <b>Kestva ohu või ohukahtluse kõrvaldamine.</b>	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. Turvanõrkustega ja puuduliku turvalisusega IT-taristu	harv	tõsine	keskmine	CERT-EE/ AEO laekunud intsidendi turvaanalüüs, asetleidnud intsidendi juurpõhjus ja selle mõjuulatus. Ametile laekunud vihjed ja pöördumised. KorS §2, §4, §5 ja §49.

			<p>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 valdavosa eesti kodanikest ja era-ning avalikest teenustest, kes on ühtlasi ohu realiseerumisel mõjutatud.</p>				
--	--	--	---	--	--	--	--