

TIEKĖJŲ RIZIKOS VERTINIMO KLAUSIMYNAS

Paslaugos tiekėjo rizikos laipsnis (toliau – Rizikos laipsnis) – laipsnis, priskiriamas atsižvelgiant į tiekėjų rizikos vertinimo, apimančio atitiktą Kibernetinio saugumo įstatymui (toliau – KSI) ir Kibernetinio saugumo reikalavimų aprašui (toliau – OTR), finansinę, reputacijos, paslaugų kokybės bei veiklos istorijos situaciją, rezultatus ir apskaičiuojamą bendrą rizikos balą.

Paslaugos tiekėjo rizikos vertinimas – tiekėjų rizikos analizė, kurios metu potenciali tiekėjų rizika vertinama atitikties KSI ir OTR, finansinės, reputacijos, paslaugų kokybės bei veiklos istorijos situacijos atžvilgiu, rizikai suteikiama skaitinė reikšmė, apskaičiuojamas bendras rizikos balas, nustatomas rizikos laipsnis.

Paslaugų tiekėjo rizikos valdymas – veiksmai, kuriais, atsižvelgiant į tiekėjų rizikos laipsnį ir tiekėjų kritiškumą, riziką siekiama koordinuoti ir kontroliuoti.

		Eil. Nr.	Klausimas	Atsakymas		
				TAIP	IŠ DALIES	NE
Atitiktis kibernetinio saugumo reikalavimams	Saugumo politika	1.	Ar Organizacijoje yra patvirtintas kibernetinio saugumo politikos dokumentas (-ai), atitinkantis (-ys) KSI ir OTR reikalavimus?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		2.	Ar Organizacijos vadovo patvirtintas Saugumo politikos dokumentas (-ai) yra peržiūrimas (-i) ir atnaujinamas (-i) ne rečiau kaip kartą per metus arba pasikeitus aplinkybėms?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Kibernetinio saugumo rizikos analizė	3.	Ar Organizacijoje yra patvirtinta tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarka?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		4.	Ar Organizacijoje yra paskirtas už rizikos vertinimą, rizikos vertinimo proceso priežiūrą bei nuolatinį tobulinimą atsakingas asmuo?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		5.	Ar Organizacijoje taikomas rizikos vertinimo ir valdymo procesas apima tinklų ir informacinių sistemų identifikavimą ir klasifikavimą, rizikos analizę ir rizikos valdymo priemonių pasirinkimą?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		6.	Ar rizikos vertinimas Organizacijoje atliekamas ne rečiau kaip kartą per metus, įvykus esminiems organizaciniais ar kitiems reikšmingiems pokyčiams, taip pat įvykus dideliame kibernetiniame incidentui?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		7.	Ar rizikos vertinimo metu Organizacijoje rengiama rizikos vertinimo ataskaita ir, jei rizikos vertinimo metu yra nustatoma šalinamų trūkumų, rizikos valdymo planas?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Eil. Nr.	Klausimas	Atsakymas		
			TAIP	IŠ DALIES	NE
Už kibernetinį saugumą atsakingi asmenys	8.	Ar Organizacijoje yra paskirtas (-i) asmuo (-enys), atsakingas (-i) už kibernetinį saugumą (pvz.: Kibernetinio saugumo vadovas, Saugos įgaliotinis ir pan.)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	9.	Ar visi Organizacijos darbuotojai yra informuoti apie už kibernetinį saugumą paskirtą (-us) asmenį (-is)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	10.	Ar Organizacijoje yra paskirtas (-i) asmuo (-enys), atsakingas (-i) už tinklų ir informacinių sistemų priežiūrą, veikimo užtikrinimą (pvz.: IT administratorius, IS administratorius ir pan.)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kibernetinių incidentų valdymas	11.	Ar Organizacijoje yra patvirtintas kibernetinių incidentų valdymo planas, atitinkantis LR Vyriausybės patvirtinto Nacionalinio kibernetinių incidentų valdymo plano nuostatas?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	12.	Jei Organizacijai tinklų ir informacinių sistemų paslaugas, susijusias su kibernetinių incidentų valdymu, teikia paslaugų teikėjai, ar patvirtintas kibernetinių incidentų valdymo planas yra suderintas su paslaugų teikėju?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	13.	Ar Organizacijoje patvirtintas kibernetinių incidentų valdymo plano veiksmingumas yra reguliariai išbandomas ir ar yra parengiama veiksmingumo išbandymo ataskaita?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	14.	Ar Organizacijoje yra nustatyti žurnalinių įrašų (angl. <i>log</i>) administravimo ir saugojimo, įsibrovimų aptikimo ir prevencijos reikalavimai?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	15.	Ar Organizacijoje yra įgyvendinti techniniai reikalavimai, nurodyti OTR Lentelėje 1?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Veiklos tęstinumo valdymas	16.	Ar Organizacijoje yra patvirtintas veiklos tęstinumo valdymo planas?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	17.	Ar Organizacijoje yra parengtas detalus tinklų ir informacinių sistemų veiklos atkūrimo planas, apimantis atsakingus asmenis, veiksmų atlikimo terminus ir pan.?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	18.	Ar Organizacijoje yra nustatytas tinklų ir informacinių sistemų ar jų dalies atkūrimo laikotarpis (angl. <i>Recovery time objective, RTO</i>) ir ar jis yra reguliariai išbandomas?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	19.	Ar Organizacijoje yra nustatytas tinklų ir informacinių sistemų ar jų dalies duomenų praradimo laikas (angl. <i>Recovery point objective, RPO</i>) ir ar jis yra reguliariai išbandomas?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Eil. Nr.	Klausimas	Atsakymas		
			TAIP	IŠ DALIES	NE
	20.	Ar Organizacijoje yra nustatyti atsarginių duomenų kopijų kūrimo, saugojimo ir duomenų atkūrimo iš jų reikalavimai ir ar yra aiškiai apibrėžti atsarginio kopijavimo mastas ir dažnis?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	21.	Ar Organizacijoje yra įgyvendinti techniniai reikalavimai, nurodyti OTR Lentelėje 2?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tiekimo grandinės saugumo užtikrinimas	22.	Ar Organizacijoje yra nustatyta tiekimo grandinės saugumo valdymo tvarka, taikoma paslaugų, darbų ar įrangos pirkimams, susijusiems su tinklų ir informacinių sistemų projektavimu, kūrimu, diegimu, naudojimu, priežiūra, modernizavimu ir (ar) kibernetinio saugumo užtikrinimu?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	23.	Ar Organizacijoje yra numatyti tinklų ir informacinių sistemų tiekėjų atrankos kriterijai apimantys atitiktą KSI, kokybės reikalavimus ir prieigų valdymą?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	24.	Ar Organizacija sutartyse su tiekėjais (įskaitant subtiekejus), kiek tai susiję su teikiamomis paslaugomis, numato reikalavimus, apimančius atitiktą KSI, reikiamus personalo įgūdžius, sertifikatus ar kvalifikacijas, įsipareigojimus pranešti apie įvykusius kibernetinius incidentus ir pan.?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	25.	Ar Organizacija yra numčiusi tinklų ir informacinių sistemų paslaugų teikėjų rizikos vertinimo reikalavimus ir ar remdamasi jais reguliariai atlieka tiekėjų kontrolę (vertinimą, sutarčių peržiūrą, planinius ir (ar) neplaninius auditus)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	26.	Ar Organizacija su interneto paslaugos, jei duomenų perdavimo paslauga yra esminė paslaugai teikti, teikėju yra sudariusi sutartį (-is), kurioje (-iose) numatyta: reagavimas į kibernetinius incidentus įprastomis darbo valandomis, reagavimas į kibernetinius incidentus po darbo valandų, nepertraukiamas interneto paslaugos teikimas: 24 valandas per parą, 7 dienas per savaitę, paslaugos sutrikimų registravimas: 24 valandas per parą, 7 dienas per savaitę, ir apsaugos nuo tinklų ir informacinės sistemos trikdymo taikymas (angl. <i>Denial of Service, DoS; Distributed Denial of Service, DDoS</i>)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Saugus tinklų ir informacinių sistemų įsigijimas,	27.	Ar Organizacijoje yra nustatyta tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo užtikrinimo tvarka?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	28.	Ar Organizacijoje yra nustatytos tinklų ir informacinių sistemų pokyčių, pataisų ir spragų valdymo tvarkos?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Eil. Nr.	Klausimas	Atsakymas		
			TAIP	IŠ DALIES	NE
plėtojimas ir priežiūra	29.	Ar Organizacijoje yra rengiamas, ne rečiau nei kartą per metus peržiūrimas ir atjauninamas leistinos programinės įrangos sąrašas?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	30.	Ar Organizacijoje programinę įrangą diegia, reikiamus pokyčius, pataisas ir spragų taisymą atlieka tik Organizacijos įgalioti asmenys?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	31.	Ar Organizacijoje yra reguliariai atliekamas spragų skenavimas, o visos tinklų informacinės sistemos spragų skenavimas ne rečiau kaip kas 6 mėnesius?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	32.	Ar Organizacijoje yra įgyvendinti techniniai reikalavimai, nurodyti OTR Lentelėje 3?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kibernetinio saugumo reikalavimų veiksmingumo vertinimas	33.	Ar Organizacijoje yra nustatyta kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarka?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	34.	Ar Organizacijoje, ne rečiau nei kartą per metus, yra atliekamas atitikties KSI, OTR ir (ar) Organizacijos patvirtintiems Saugumo politikos dokumentams vertinimas?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	35.	Ar Organizacijoje, ne rečiau kaip kartą per 3 metus, yra atliekamas kibernetinio saugumo auditas, vadovaujantis KSI 14 straipsnio 8 punkto nuostatomis?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kibernetinės higienos praktika	36.	Ar Organizacijoje yra nustatyta kibernetinės higienos praktikos organizavimo ir kibernetinio saugumo mokymų organizavimo ir vykdymo tvarka?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	37.	Ar Organizacijoje, ne rečiau nei kartą per metus, visi Organizacijos darbuotojai išklauso kibernetinės higienos praktikos mokymus?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	38.	Ar Organizacijos darbuotojai yra reguliariai informuojami apie kibernetinio saugumo aktualijas?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kriptografijos ir šifravimo naudojimo politika	39.	Ar Organizacijoje yra nustatyta kriptografijos ir šifravimo naudojimo tvarka?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	40.	Ar Organizacijoje yra įgyvendinti techniniai reikalavimai, nurodyti OTR Lentelėje 4?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Žmogiškųjų išteklių saugumas, fizinės prieigos politika ir	41.	Ar Organizacijoje yra nustatyta žmogiškųjų išteklių saugumo tvarka?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	42.	Ar Organizacijoje prieiga prie tinklų ir informacinių sistemų Organizacijos darbuotojams ir trečiosioms šalims suteikiama tik susipažinus su kibernetinio saugumo dokumentais ir sutikus jų laikytis?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

		Eil. Nr.	Klausimas	Atsakymas		
				TAIP	IŠ DALIES	NE
Bendrieji veiklos rodikliai	turto valdymas	43.	Ar Organizacijoje prieigą prie tinklų ir informacinių sistemų turintys Organizacijos darbuotojai ir trečiosios šalys privalo pasirašyti konfidencialumo ir (ar) informacijos neatskleidimo sutartį, pasižadėjimą?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		44.	Ar Organizacijoje yra nustatyta fizinės prieigos tvarka, numatanti saugomas Organizacijos patalpas, užtikrinanti saugomų patalpų fizinės apsaugos kontrolę ir tik įgaliotų asmenų patekimą?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		45.	Ar Organizacijoje yra įgyvendinti techniniai reikalavimai, nurodyti OTR Lentelėje 5?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		46.	Ar Organizacijoje yra nustatyta turto valdymo tvarka, numatanti turto sąrašą, saugaus turto naudojimo tvarką Organizacijoje ir už Organizacijos ribų?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		47.	Ar Organizacijoje tinklų ir informacinių sistemų gedimai yra registruojami, o jų tvarkymą atlieka tik Organizacijos įgalioti kvalifikuoti specialistai?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		48.	Ar Organizacijoje yra įgyvendinti techniniai reikalavimai, nurodyti OTR Lentelėje 6?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Prieigos valdymas	49.	Ar Organizacijoje yra nustatyta prieigos valdymo tvarka, numatanti prieigos naudotojams, administratoriams ir tretiesiems asmenims suteikimą, keitimą, naikinimą, jų tapatybės nustatymą ir pan.?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		50.	Ar Organizacijoje yra nustatyta saugaus slaptažodžio kūrimo ir naudojimo tvarka, numatanti saugaus slaptažodžio reikalavimus, nurodanti, kad slaptažodžius draudžiama atskleisti kitiems asmenims, juos perduoti atviru tekstu ir pan.?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		51.	Ar Organizacijoje yra nustatyta kelių veiksmų tapatumo priemonių naudojimo tvarka ir ar tokios priemonės yra naudojamos?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		52.	Ar Organizacijoje yra įgyvendinti techniniai reikalavimai, nurodyti OTR Lentelėje 7?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Finansinė būklė	53.	Ar, per paskutinius 12 mėnesių, Organizacija nepatyrė / nepatiria finansinių sunkumų?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		54.	Ar, per paskutinius 12 mėnesių, Organizacija turėjo / turi palankų skolų ir nuosavo kapitalo santykį?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		55.	Ar, per paskutinius 12 mėnesių, Organizacija neturėjo / neturi skolų valstybinėms institucijoms?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

		Eil. Nr.	Klausimas	Atsakymas		
				TAIP	IŠ DALIES	NE
	Reputacija	56.	Ar, per paskutinius 12 mėnesių, Organizacija nepatyrė / nepatiria žalos reputacijai?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Paslaugų kokybė	57.	Ar Organizacija atlieka pastovią paslaugų kokybės analizę?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		58.	Ar, per paskutinius 12 mėnesių, Organizacija sulaukė/sulaukia teigiamų vartotojų atsiliepimų apie paslaugų kokybę?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Veiklos istorija	59.	Ar, per paskutinius 12 mėnesių, Organizacijoje neįvyko / nevyksta didelių kibernetinių incidentų, trikdžiusių / trikdančių Organizacijos veiklą?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		60.	Ar, per paskutinius 12 mėnesių, Organizacijoje neįvyko / nevyksta nedidelių ir (ar) vos neįvykusių kibernetinių incidentų?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>