

**Dotazník za účelom odhadu rozsahu prác**

Spoločnosť	Národná diaľničná spoločnosť, a. s.
Zodpovedný zamestnanec (meno, email, tel. číslo)	XXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXX

Č.	Otázka	Odpoveď
1	Ste prevádzkovateľom prvku kritickej infraštruktúry ¹ ?	
2	Ste prevádzkovateľom základnej služby („PZS“)?	
2.1	Ak áno, aké základné služby prevádzkujete?	
3	Počet užívateľov Siete a Informačného Systému ² s väzbou na základné služby? (ďalej len IS) <i>Príklad: 1500 interných 3000 externých</i>	
4	Počet IS pre jednotlivé základné služby?	
5	Počet zamestnancov zúčastňujúcich na prevádzke IS s väzbou na základnú službu?	
6	Štruktúra správy IS s väzbou na základnú službu <i>Centralizovaná verus distribuovaná</i>	
7	Počet externých pracovísk, kde je prevádzkovaný samostatný IS s väzbou na základnú službu, iný ako na ostatných pracoviskách?	
8	Máte s tretími stranami uzavreté akékoľvek zmluvy na výkon činností, ktoré priamo súvisia s prevádzkou IS s väzbou na základné služby (<i>ak áno, počet a typ služieb</i>)? <i>Príklad: 1 x dodávateľ podpory užívateľských staníc 1 x dodávateľ IS zariadení 1 x dodávateľ laboratórnych zariadení</i>	
9	Počet zamestnancov tretích strán zúčastňujúcich na prevádzke IS s väzbou na základnú službu?	
10	Máte vypracovanú bezpečnostnú dokumentáciu týkajúcu sa Vašich IS (<i>ak áno, akú a z ktorého roku</i>)?	-
11	Máte určenú rolu manažéra kybernetickej bezpečnosti? (<i>CISO</i>)	
12	Máte zadokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení?	
13	Máte schválenú bezpečnostnú stratégiu kybernetickej bezpečnosti?	
14	Máte zadanú klasifikáciu informácií?	
15	Vykonalí ste kategorizáciu IS podľa požiadaviek Zákona?	
15.1	Ak áno, sú IS zaradené do:	
15.2	I. kategórie	
15.3	II. kategórie	
15.4	III. kategórie	

1 § 2 písm. a) zákona č. 45/2011 Z.z. o kritickej infraštruktúre
2§ 3 písm. a) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti



16	Máte záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti podľa § 29 zákona.	
17	Máte vypracované postupy a procesy pre riadenie aktív, hrozieb a rizík?	
18	Máte identifikované a evidované aktíva využívané pre základnú službu?	
19	Máte vypracované a zavedené riadenie personálnej bezpečnosti?	
20	Máte vypracované a zavedené riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov?	
21	Máte zavedený systém a procesy na identifikáciu technických zraniteľností v IS s väzbou na základnú službu?	
22	Máte zavedené prvky riadenia bezpečnosti sietí a informačných systémov?	
23	Máte zavedené praktiky riadenia prevádzky?	
24	Máte zavedené riadenie prístupov osôb alebo systémov do IS s väzbou na základnú službu?	
25	Máte vypracované a zavedené kryptografické opatrenia?	
26	Máte vypracovaný a zavedený postup riešenia kybernetických incidentov?	
27	Vyskytol sa závažný kybernetický bezpečnostný incident za posledné 2 roky?	
28	Porušili ste povinnosti ZoKB, prípadne bola udelená pokuta? <i>(ak áno, aké)</i>	
29	Máte zavedený centralizovaný bezpečnostný dohľad nad IS s väzbou na základnú službu?	
30	Máte zavedenú fyzickú bezpečnosť a bezpečnosť prostredia v súvislosti s IS s väzbou na základnú službu?	
31	Máte vypracované a zavedené pravidlá a postupy riadenia kontinuity procesov v súvislosti s IS s väzbou na základnú službu?	
32	Máte vypracované a pravidelné testované krízové plány v súvislosti s IS s väzbou na základnú službu?	
33	Máte vypracované, zavedené a pravidelne testované postupy zálohovania a obnovy siete a informačného systému?	
34	Ste držiteľom certifikátu podľa technickej normy (napr. ISO 27001) a certifikovaná oblasť zahŕňa IS s väzbou na základnú službu? <i>(uvedte aj podľa akej normy)</i>	
35	Máte potvrdenie o priemyselnej bezpečnosti? <i>(ak áno, uveďte číslo)</i>	
36	Ďalšie informácie	-