ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2022

Vyhlásené: 23. 12. 2022 Časová verzia predpisu účinná od: 1. 9.2026

Obsah dokumentu je právne záväzný.

493

VYHLÁŠKA
Národného bezpečnostného úradu
z 19. decembra 2022
o audite kybernetickej bezpečnosti

Národný bezpečnostný úrad (ďalej len „úrad“) podľa § 32 ods. 1 písm. f) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 287/2021 Z. z. (ďalej len „zákon“) ustanovuje:

§ 1

(1) Audit kybernetickej bezpečnosti (ďalej len „audit“) sa vykonáva odborne, objektívne, nestranne a na základe dôkazov. Za správnosť a úplnosť záverečnej správy o výsledkoch auditu zodpovedá certifikovaný audítor kybernetickej bezpečnosti podľa § 29 ods. 3 zákona (ďalej len „audítor“).

(2) Samohodnotenie sa vykonáva odborne, objektívne a na základe dôkazov. Za správnosť a úplnosť správy o vykonaní samohodnotenia zodpovedá manažér kybernetickej bezpečnosti (ďalej len „manažér“).

(3) Časový rozsah trvania auditu sa určuje tak, že je dostatočný na posúdenie plnenia povinností podľa zákona a účinnosti prijatých bezpečnostných opatrení. Ak nie je možné v rámci rozsahu trvania auditu hodnotiť každé jednotlivé opatrenie na veľkej populácii prvkov, hodnotí sa ich stav formou vzorkovania, pričom rozsah vzoriek sa určuje s ohľadom na vykonanú klasifikáciu informácií, vykonanú analýzu rizík kybernetickej bezpečnosti a na vypovedaciu schopnosť auditu. Audit alebo samohodnotenie sa vykonáva v časovom rozsahu a periodicite podľa prílohy č. 2.

(4) Pri výkone auditu sa

a) prijíma žiadosť o vykonanie auditu v rozsahu minimálnych náležitostí uvedených v prílohe č. 1 a posudzuje kompletnosť údajov v žiadosti; môžu vyžadovať ďalšie informácie potrebné na prípravu a výkon auditu,

b) pripravuje harmonogram výkonu auditu, ktorý obsahuje najmä

1. identifikáciu organizačných útvarov, procesov, auditovaných sietí, informačných systémov a operačných technológií a fyzických lokalít prevádzkovateľa základnej služby s uvedením času a

2. meno, priezvisko a kontaktné údaje zodpovedného zamestnanca prevádzkovateľa základnej služby, ktorý poskytuje audítorovi počas auditu požadovanú súčinnosť,

c) určuje rozsah auditu spôsobom podľa prílohy č. 2,

d) určujú metódy auditu,

e) pripravujú podklady a pracovné dokumenty potrebné na zaznamenávanie výkonu auditu, ktoré sú prílohou záverečnej správy o výsledkoch auditu, a to najmä

1. zápisy zo stretnutí,
2. evidencia predložených dôkazov,
3. evidencia účastníkov auditu,
4. evidencia navštívených lokalít,

f) preskúmava bezpečnostná dokumentácia a vyhodnocujú bezpečnostné opatrenia a vypracúva kontrolný záznam auditovaných bezpečnostných opatrení (ďalej len „kontrolný záznam“) podľa prílohy č. 3,

g) zbierajú, sústreďujú a vyhodnocujú dôkazy o zisteniach auditu,

h) oboznamuje zodpovedný zamestnanec prevádzkovateľa základnej služby so zistenými nedostatkami a zostavuje súbor odporúčaných opatrení na ich odstránenie,

i) vypracúva záverečná správa o výsledkoch auditu podľa vzoru uvedeného v štandarde na výkon auditu kybernetickej bezpečnosti zverejnenom na webovom sídle úradu.

(5) Pri samohodnotení sa

a) preskúmava bezpečnostná dokumentácia, vyhodnocujú prijaté bezpečnostné opatrenia a plnenie požiadaviek podľa zákona,

b) zbierajú, sústreďujú a vyhodnocujú dôkazy o zisteniach samohodnotenia,

c) vypracúva správa o vykonaní samohodnotenia.

§ 2

(1) V záverečnej správe o výsledkoch auditu sa hodnotí výsledok auditu a uvedú sa dôkazy, ktoré sa viažu k jednotlivým zisteniam auditu.

(2) Záverečná správa o výsledkoch auditu obsahuje najmä

a) meno, priezvisko, číslo certifikátu audítora, dátum vyhotovenia správy, certifikačnú značku audítora a jeho vlastnoručný podpis alebo kvalifikovaný elektronický podpis,

b) vymedzenie rozsahu vykonaného auditu,

c) cieľ auditu,

d) metódy auditu,

e) zhrnutie zistení výsledkov auditu a konštatovanie súladu, čiastočného súladu alebo nesúladu s požiadavkami na bezpečnosť sietí, informačných systémov a operačných technológií,

f) odporúčané nápravné opatrenia pri zistení nedostatkov,

g) dokumenty, najmä

1. kópiu certifikátu audítora,
2. kópiu žiadosti o vykonanie auditu,
3. výpočet rozsahu trvania auditu a zdôvodnenie jeho skrátenia alebo predĺženia,
4. kontrolný záznam,
5. vyjadrenie prevádzkovateľa základnej služby k zisteniam auditu,
6. harmonogram auditu,
7. zoznam evidovaných dôkazov,

8. uvedenie a zdôvodnenie zmien a rozdielov uskutočnenia auditu oproti plánovanému harmonogramu,
9. zhodnotenie plnenia povinností podľa zákona a celkového stavu prijatých bezpečnostných opatrení informačných systémov, vyslovenie súladu, čiastočného súladu alebo nesúladu s požiadavkami na bezpečnosť sietí, informačných systémov a operačných technológií a konkrétne uvedenie nedostatkov.

(3) Prílohou záverečnej správy o výsledkoch auditu je pri zistení nesúladu alebo čiastočného súladu s požiadavkami na bezpečnosť sietí, informačných systémov a operačných technológií aj správa o zistených nedostatkoch, pri ktorých sa uvádza termín vykonania nápravných opatrení na zabezpečenie súladu s požiadavkami na bezpečnosť sietí, informačných systémov a operačných technológií. Nápravné opatrenia sa prijímajú tak, že je možné ich zahrnúť do záverečnej správy o výsledkoch auditu.

(4) Ak sú niektoré zistené nedostatky odstránené do termínu vyjadrenia prevádzkovateľa základnej služby k zisteniam auditu pred spracovaním záverečnej správy o výsledkoch auditu, je možné v tejto záverečnej správe o výsledkoch auditu konštatovať pre plnenie daných požiadaviek súlad s požiadavkami na bezpečnosť sietí, informačných systémov a operačných technológií.

(5) Audit je ukončený odovzdaním záverečnej správy o výsledkoch auditu prevádzkovateľovi základnej služby. Maximálna doba výkonu auditu je 12 po sebe nasledujúcich mesiacov.

(6) Správa o vykonaní samohodnotenia obsahuje najmä

a) identifikačné údaje manažéra v rozsahu meno a priezvisko,

b) dátum vykonania samohodnotenia,

c) zhrnutie zistení výsledkov samohodnotenia s vyhodnotením požiadaviek na bezpečnosť sietí, informačných systémov a operačných technológií,

d) zoznam evidovaných dôkazov.

(7) Správa o vykonaní samohodnotenia sa úradu predkladá prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.

§ 3

(1) Audit kybernetickej bezpečnosti vykonaný podľa doterajších predpisov sa považuje za audit kybernetickej bezpečnosti podľa tejto vyhlášky.

(2) Audit kybernetickej bezpečnosti začatý a neukončený do 31. decembra 2022 sa dokončí podľa tejto vyhlášky.

§ 3a
Prechodné ustanovenia k úpravám účinným od 1. septembra 2026

(1) Audit začatý a neukončený do 31. augusta 2026 sa dokončí podľa doterajších predpisov.

(2) Audit začatý do 31. decembra 2026 sa môže vykonať aj podľa doterajších predpisov.

§ 4

Zrušuje sa vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.

§ 5

Táto vyhláška nadobúda účinnosť 1. januára 2023.

Roman Konečný v. r.

Príloha č. 1
k vyhláške č. 493/2022 Z. z.

MINIMÁLNE NÁLEŽITOSTI ŽIADOSTI O VYKONANIE AUDITU

1. Informácie o prevádzkovateľovi základnej služby:
   a) názov alebo obchodné meno, sídlo právnickej osoby alebo miesto podnikania fyzickej osoby – podnikateľa a identifikačné číslo organizácie prevádzkovateľa základnej služby,
   b) informácia, či je prevádzkovateľ základnej služby prevádzkovateľom kritickej základnej služby,
   c) identifikačné údaje a kontaktné údaje zodpovedného zamestnanca prevádzkovateľa základnej služby, ktorý poskytne audítorovi počas výkonu auditu súčinnosť v rozsahu meno a priezvisko, telefónne číslo a emailová adresa,
   d) identifikačné údaje a kontaktné údaje štatutárneho orgánu prevádzkovateľa základnej služby alebo splnomocneného zamestnanca alebo inej splnomocnenej osoby, ktorému sa záverečná správa o výsledkoch auditu odovzdáva v rozsahu meno a priezvisko, telefónne číslo a emailová adresa.
2. Informácie o zamestnancoch a osobách vykonávajúcich činnosť pre prevádzkovateľa základnej služby:
   a) počet všetkých zamestnancov prevádzkovateľa základnej služby,
   b) počet zamestnancov a osôb vykonávajúcich činnosť pre prevádzkovateľa základnej služby zúčastňujúcich sa na zabezpečovaní bezpečnostných opatrení sietí, informačných systémov a operačných technológií prevádzkovateľa základnej služby.
3. Počet dodávateľov na výkon činností, ktoré priamo súvisia s prevádzkou sietí, informačných systémov a operačných technológií pre prevádzkovateľa základnej služby (ďalej len „tretia strana“) a názov poskytovanej služby treťou stranou.
4. Počet zamestnancov tretej strany a počet osôb vykonávajúcich činnosť pre tretiu stranu zúčastňujúcich sa na zabezpečovaní bezpečnostných opatrení sietí, informačných systémov a operačných technológií prevádzkovateľa základnej služby.
5. Počet zamestnancov a osôb vykonávajúcich činnosť pre prevádzkovateľa základnej služby a počet zamestnancov a osôb vykonávajúcich činnosť pre tretiu stranu, ktorí vykonávajú určité identické činnosti a typ tejto činnosti.
6. Informácie o počte lokalít prevádzkovateľa základnej služby, v ktorých prevádzkovateľ základnej služby vykonáva svoje činnosti s
   a) neopakujúcimi sa poskytovanými službami s uvedením okresu alebo kraja lokalít spolu s počtom zamestnancov a osôb vykonávajúcich činnosť na lokalite zúčastňujúcich sa na prevádzke sietí, informačných systémov a operačných technológií prevádzkovateľa základnej služby,
   b) opakujúcimi sa poskytovanými službami spolu s počtom zamestnancov a osôb vykonávajúcich činnosť na lokalite zúčastňujúcich sa na prevádzke sietí, informačných systémov a operačných technológií prevádzkovateľa základnej služby.
7. Informácie o počte informačných systémov prevádzkovateľa základnej služby určených ako IKT alebo OT.
8. Informácia o analýze rizík kybernetickej bezpečnosti a bezpečnostných opatreniach podľa osobitného predpisu:[1])
   a) informácia o vykonaní analýzy rizík kybernetickej bezpečnosti a dátume jej poslednej zmeny,

[1]) Vyhláška Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach.

b) informácia o existencii zadokumentovaného rozsahu a prijatí bezpečnostných opatrení.

9. Zoznam bezpečnostnej dokumentácie podľa § 20 ods. 3 zákona alebo osobitného predpisu[2]) a úroveň vykonávania bezpečnostných opatrení prevádzkovateľa základnej služby.

10. Informácia o počte regulácií[3]) v oblasti kybernetickej bezpečnosti; okrem zákona, ktorým podlieha prevádzkovateľ základnej služby.

11. Počet a názvy poskytovaných služieb prevádzkovateľa základnej služby.

12. Informácia o certifikácii siete alebo informačného systému prevádzkovateľa základnej služby podľa požiadaviek na certifikáciu kybernetickej bezpečnosti informačných a komunikačných technológií[4]) alebo podľa inej certifikačnej schémy.

13. Počet používateľov sietí, informačných systémov a operačných technológií prevádzkovateľa základnej služby.

---

[2]) Napríklad zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov.

[3]) Napríklad vykonávacie nariadenie Komisie (EÚ) 2024/2690 zo 17. októbra 2024, ktorým sa stanovujú pravidlá uplatňovania smernice (EÚ) 2022/2555, pokiaľ ide o technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík a o bližšie určenie prípadov, v ktorých sa incident považuje za významný, vo vzťahu k poskytovateľom služieb DNS, správcom názvov TLD, poskytovateľom služieb cloud computingu, poskytovateľom služieb dátového centra, poskytovateľom sietí na sprístupňovanie obsahu, poskytovateľom riadených služieb, poskytovateľom riadených bezpečnostných služieb, poskytovateľom online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete a poskytovateľom dôveryhodných služieb (Ú. v. EÚ L, 2024/2690, 18. 10. 2024), nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (Ú. v. EÚ L 333, 27. 12. 2022), nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti) (Ú. v. EÚ L, 2024/2847, 20. 11. 2024) v platnom znení, zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 95/2019 Z. z. v znení neskorších predpisov, vyhláška Ministerstva dopravy Slovenskej republiky č. 111/2026 Z. z., ktorou sa ustanovujú sektorové bezpečnostné opatrenia v pôsobnosti Ministerstva dopravy Slovenskej republiky.

[4]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7. 6. 2019) v platnom znení.

Príloha č. 2
k vyhláške č. 493/2022 Z. z.

ČASOVÝ ROZSAH A PERIODICITA VYKONÁVANIA AUDITU ALEBO SAMOHODNOTENIA

A. ČASOVÝ ROZSAH VYKONÁVANIA AUDITU

1. Pred začiatkom auditu sa určí dĺžka jeho trvania na naplánovanie a vykonanie úplného a efektívneho auditu, s cieľom dostatočne posúdiť predmet auditu.
2. Pri určovaní času potrebného na výkon auditu na mieste a celkového času potrebného na audit sa vychádza z údajov uvedených v tabuľke č. 1. Rozsah auditu ustanovený v tabuľke č. 1 je len východiskom pre určenie adekvátneho rozsahu príslušného auditu. Pri určovaní konečného rozsahu auditu sa vždy zohľadňujú aj špecifické podmienky prevádzkovateľa základnej služby.
3. Ak je vymenovaný audítorský tím, do časového rozsahu trvania auditu sa započítava čas audítora pri prvotnom posúdení dokumentácie prevádzkovateľa základnej služby, doručení vyžiadaných dodatočných podkladov, predbežnej analýze plnenia povinností, posúdení povinnej dokumentácie v rámci spracovania návrhu správy z auditu a pri spracovaní záverečnej správy o výsledkoch auditu, a to spolu najviac v rozsahu 30 % celkovej dĺžky trvania auditu. Vypočítaný čas na plánovanie a vypracovanie správy nesmie znížiť celkový čas auditu na mieste na menej ako 70 % vypočítaného času. Ak je na plánovanie a písanie správy potrebný ďalší čas, nesmie to byť dôvodom na skrátenie času auditu na mieste. Čas audítora na cestovanie nie je zahrnutý v tomto čase a je doplňujúci k vypočítanému času auditu. Do rozsahu trvania auditu sa započítava len čas audítora.
4. Pri výpočte dĺžky trvania auditu sa zohľadňujú informácie zo žiadosti o vykonanie auditu a dodatočne vyžiadané informácie od prevádzkovateľa základnej služby.
5. Výpočet dní trvania auditu sa vykonáva celkovo pre prostredie prevádzkovateľa základnej služby v tomto poradí úkonov:

a) Výpočet základnej dĺžky trvania auditu

Základná dĺžka trvania auditu sa určuje v človeko-dňoch, ktorá je daná efektívnym počtom zamestnancov a osôb vykonávajúcich činnosť pre prevádzkovateľa základnej služby a tretiu stranu, ktorí sa zúčastňujú na zabezpečovaní bezpečnostných opatrení sietí, informačných systémov a operačných technológií prevádzkovateľa základnej služby. Na účely výpočtu základnej dĺžky trvania auditu sa do výpočtu zahŕňajú tieto informácie zo žiadosti:

1. počet zamestnancov a osôb vykonávajúcich činnosť pre prevádzkovateľa základnej služby zúčastňujúcich sa na zabezpečovaní bezpečnostných opatrení sietí, informačných systémov a operačných technológií prevádzkovateľa základnej služby a
2. počet zamestnancov a osôb vykonávajúcich činnosť pre tretiu stranu zúčastňujúcich sa na zabezpečovaní bezpečnostných opatrení sietí, informačných systémov a operačných technológií.

Ak nadpolovičná väčšina zamestnancov alebo osôb vykonávajúcich činnosť pre prevádzkovateľa základnej služby a tretiu stranu vykonáva určité identické činnosti, je povolené zníženie vstupného počtu osôb na výpočet dĺžky trvania auditu.

Pre určenie efektívneho počtu osôb na výpočet trvania auditu môže byť použitá druhá odmocnina z počtu osôb vykonávajúcich jednotlivú identickú činnosť zaokrúhlená nahor na najbližšie celé číslo. Toto číslo musí byť maximálnym povoleným zníženým počtom osôb. Efektívny počet zamestnancov a osôb vykonávajúcich činnosť pre prevádzkovateľa základnej služby a tretiu stranu sa vypočíta spočítaním zamestnancov a osôb vykonávajúcich činnosť pre prevádzkovateľa základnej služby a tretiu stranu, ktorí nevykonávajú identické činnosti, a druhej odmocniny zamestnancov a osôb vykonávajúcich činnosť pre prevádzkovateľa základnej služby a tretiu stranu, ktorí vykonávajú identické činnosti.

Tabuľka č. 1: Určenie základného rozsahu trvania auditu

Počet zamestnancov a osôb vykonávajúcich činnosť, zúčastňujúcich sa na zabezpečovaní bezpečnostných opatrení sietí, informačných systémov a operačných technológií prevádzkovateľa základnej služby	**Základný rozsah auditu v človeko-dňoch**
1 – 10	5
11 – 15	6
16 – 25	7
26 – 45	8,5
46 – 65	10
66 – 85	11
86 – 125	12
126 – 175	13
176 – 275	14
276 – 425	15
426 – 625	16,5
626 – 875	17,5
876 – 1 175	18,5
1 176 – 1 550	19,5
1 551 – 2 025	21
2 026 – 2 675	22
2 676 – 3 450	23
3 451 – 4 350	24
4 351 – 5 450	25
5 451 – 6 800	26
6 801 – 8 500	27
8 501 – 10 700	28
viac ako 10 700	ďalej podľa vzťahu vyššie

b) Výpočet dĺžky trvania auditu na lokalitách prevádzkovateľa základnej služby

Všetky lokality prevádzkovateľa základnej služby, na ktorých sa vykonávajú činnosti súvisiace s poskytovanou službou, je potrebné posúdiť a zahrnúť do auditu. Vo výpočte základnej dĺžky trvania auditu je zohľadnený celkový počet zamestnancov a osôb vykonávajúcich činnosti pre prevádzkovateľa základnej služby ako aj zamestnancov a osôb tretej strany bez ohľadu na ich umiestnenie.

Výber vzorky lokality:

Za výber vzorky lokality je zodpovedný audítor. Lokality sa vyberajú podľa týchto pravidiel:

1. lokalita s neopakujúcimi sa poskytovanými službami prevádzkovateľa základnej služby je vždy súčasťou auditu spolu s centrálou,
2. lokalita s opakujúcimi sa poskytovanými službami prevádzkovateľa základnej služby – audítor je zodpovedný za výber lokalít na základe ich rizikovosti, veľkosti a počtu prevádzkovaných sietí, informačných systémov a operačných technológií. Počet je definovaný ako odmocnina počtu všetkých lokalít s opakujúcimi sa poskytovanými službami.

Pre definovanie dĺžky trvania auditu na vybraných lokalitách sa vychádza z počtu zamestnancov a osôb vykonávajúcich činnosť pre prevádzkovateľa základnej služby, ktorí pôsobia na danej lokalite.

c) Faktory, ktoré vplývajú na rozsah auditu

Celková dĺžka auditu je počet človeko-dní základnej dĺžky auditu. Táto celková dĺžka auditu môže byť znížená alebo zvýšená o faktory, ktoré vplývajú na dĺžku trvania auditu.

Krok 1: Určenie faktora súvisiaceho s poskytovanou službou: Identifikuje sa zodpovedajúci stupeň pre každú z kategórií uvedených v tabuľke č. 2 a výsledok sa spočíta.

Tabuľka č. 2: Faktor súvisiaci so službou a procesmi

Kategória	**Opis**	**Stupeň**
Počet regulácií v oblasti kybernetickej bezpečnosti	1. Prevádzkovateľ základnej služby podlieha regulácii v oblasti kybernetickej bezpečnosti len podľa zákona	**1**
	2. Prevádzkovateľ základnej služby podlieha dvom reguláciám v oblasti kybernetickej bezpečnosti	**2**
	3. Prevádzkovateľ základnej služby podlieha trom a viac reguláciám v oblasti kybernetickej bezpečnosti	**3**
Poskytovaná služba a procesy	1. Jedna až dve poskytované služby a proces so štandardnými a opakujúcimi sa činnosťami	**1**
	2. Dve až päť poskytovaných služieb a neopakujúce sa procesy a činnosti	**2**
	3. Šesť a viac poskytovaných služieb alebo 50 lokalít a viac	**3**
Úroveň vykonávania bezpečnostných opatrení	1. Prevádzkovateľ základnej služby vykonáva bezpečnostné opatrenia na úrovni 75 % a viac	**1**
	2. Prevádzkovateľ základnej služby vykonáva bezpečnostné opatrenia v rozsahu od 40 % do 74 %	**2**
	3. Prevádzkovateľ základnej služby vykonáva bezpečnostné opatrenia na úrovni menej ako 40 %	**3**

Tabuľka č. 3: Faktor súvisiaci s prostredím IKT alebo OT

Kategória	**Opis**	**Stupeň**
Komplexnosť IKT infraštruktúry	1. Prevádzkovateľ základnej služby má určené siete, informačné systémy a operačné technológie v kategórii IKT v počte: 1 – 5	**1**
	2. Prevádzkovateľ základnej služby má určené siete, informačné systémy a operačné technológie v kategórii IKT v počte: 6 – 15	**2**
	3. Prevádzkovateľ základnej služby má určené siete, informačné systémy a operačné technológie v kategórii IKT v počte: 16 a viac	**3**
Závislosť na tretej strane	1. Prevádzkovateľ základnej služby nemá žiadnu tretiu stranu s významným vplyvom na	**1**

	prevádzkovateľa základnej služby, s vplyvom na prevádzku sietí, informačných systémov a operačných technológií prevádzkovateľa základnej služby	
	2. Prevádzkovateľ základnej služby má aspoň jednu tretiu stranu s významným vplyvom na prevádzkovateľa základnej služby, s vplyvom na prevádzku sietí, informačných systémov a operačných technológií alebo tretia strana sa zúčastňuje na zabezpečovaní bezpečnostných opatrení sietí, informačných systémov a operačných technológií prevádzkovateľa základnej služby	**2**
	3. Prevádzkovateľ základnej služby má dve a viac tretích strán s významným vplyvom na prevádzkovateľa základnej služby s vplyvom na prevádzku sietí, informačných systémov a operačných technológií alebo dve a viac tretích strán sa zúčastňuje na zabezpečovaní bezpečnostných opatrení sietí, informačných systémov a operačných technológií prevádzkovateľa základnej služby	**3**
Komplexnosť OT infraštruktúry	1. Prevádzkovateľ základnej služby má určené siete, informačné systémy a operačné technológie v kategórii OT v počte: 0	**1**
	2. Prevádzkovateľ základnej služby má určené siete, informačné systémy a operačné technológie v kategórii OT v počte: 1 – 2	**2**
	3. Prevádzkovateľ základnej služby má určené siete, informačné systémy a operačné technológie v kategórii OT v počte: 3 a viac	**3**

Krok 3: Na základe výsledkov z krokov 1 a 2 sa identifikuje vplyv faktorov na čas trvania auditu výberom zodpovedajúceho údaja v tabuľke č. 4.

Tabuľka č. 4: Vplyv faktorov na čas auditu

		Komplexnosť IKT a OT		
		Nízka (od 3 do 4)	**Stredná (od 5 do 6)**	**Vysoká (od 7 do 9)**
Komplexnosť poskytovanej služby	**Vysoká (od 7 do 9)**	**1,12**	**1,30**	**1,40**
	Stredná (od 5 do 6)	**0,92**	**1,00**	**1,30**
	Nízka (od 3 do 4)	**0,80**	**0,92**	**1,12**

Krok 4: Záverečný výpočet: Počet človeko-dní základnej dĺžky auditu sa vynásobí faktorom vypočítaným v kroku 3. Tento výsledok je konečným počtom dní trvania auditu.

d) Uplatnenie subjektívneho názoru audítora

Audítor môže na základe odôvodneného rozhodnutia a po predchádzajúcej konzultácii s prevádzkovateľom základnej služby dodatočne upraviť rozsah trvania auditu určený postupom podľa písmen a) až c) na iný rozsah trvania auditu v rozmedzí -30 % až +30 %,

ak s týmto postupom prevádzkovateľ základnej služby vopred súhlasí.

e) Audit vykonávaný na diaľku

Ak sa vykonáva audit lokalít prevádzkovateľa základnej služby na diaľku, rozsah trvania auditu na diaľku neprekročí 30 % plánovaného času trvania auditu na mieste. Čas trvania auditu na mieste sa odvodzuje od času trvania auditov určených pre jednotlivé lokality prevádzkovateľa základnej služby.

B. PERIODICITA VYKONÁVANIA AUDITU ALEBO SAMOHODNOTENIA

(1) Audit sa vykonáva a ukončuje najneskôr do konca

a) tretieho kalendárneho roka nasledujúceho po roku, v ktorom bol posledný audit ukončený, alebo

b) piateho kalendárneho roka nasledujúceho po roku, v ktorom bol posledný audit ukončený, ak ide o prevádzkovateľa základnej služby, ktorý nie je prevádzkovateľom kritickej základnej služby a ktorý vykonáva samohodnotenie podľa § 29 ods. 8 zákona v intervale podľa odseku 3.

(2) Audit sa vykonáva pri každej významnej zmene, najneskôr do šiestich mesiacov, odkedy má zmena významný vplyv na realizované bezpečnostné opatrenia.

(3) Samohodnotenie sa vykonáva každé dva roky. Správa o vykonaní samohodnotenia sa predkladá najneskôr do konca kalendárneho roka, v ktorom sa samohodnotenie vykonáva.

Príloha č. 3
k vyhláške č. 493/2022 Z. z.

KONTROLNÝ ZÁZNAM AUDITOVANÝCH BEZPEČNOSTNÝCH OPATRENÍ

Kontrolný záznam obsahuje súbor požiadaviek na bezpečnosť sietí, informačných systémov a operačných technológií podľa zákona a jeho vykonávacích predpisov a osobitných predpisov. Pri spoločných požiadavkách na prevádzkovateľa základnej služby sa vyplní spoločný kontrolný záznam za všetky siete, informačné systémy a operačné technológie relevantné pre audit. Bezpečnostné opatrenia, ktoré sú odlišné pre jednotlivé auditované siete, informačné systémy a operačné technológie, sa vyplnia samostatne pre každú sieť, informačný systém alebo operačnú technológiu.

V kontrolnom zázname sa uvedie

a) súlad, čiastočný súlad alebo nesúlad s požiadavkami na bezpečnosť sietí, informačných systémov a operačných technológií na prijaté bezpečnostné opatrenia,

b) zistenia auditu pre jednotlivé požiadavky na bezpečnosť sietí, informačných systémov a operačných technológií,

c) získané dôkazy podporujúce uvedené zistenia a

d) referencia na použitú metódu auditu, napríklad

1. pozorovanie činností a stavu bezpečnostných opatrení,
2. analýza predložených záznamov,
3. analýza predložených postupov, predpisov a dokumentov,
4. rozhovory a dotazníky.

Súčasťou kontrolného záznamu je aj overenie úplnosti požadovanej bezpečnostnej dokumentácie a overenie klasifikácie informácií a kategorizácie sietí, informačných systémov a operačných technológií.

Ak sú auditované siete, informačné systémy a operačné technológie, pre ktoré platia dodatočné požiadavky nad rámec bezpečnostných opatrení uvedených v zákone alebo v osobitnom predpise,[4]) uvedie sa v kontrolnom zázname spôsob plnenia podľa požiadaviek, ktoré sa aplikujú na prevádzkovateľa základnej služby.

So zistenými nedostatkami je priebežne oboznámený zodpovedný pracovník prevádzkovateľa základnej služby počas auditu a zároveň dokumentuje odporúčané opatrenia na odstránenie nedostatkov.

Kontrolný záznam sa uchováva s odbornou starostlivosťou a s ohľadom na citlivosť informácií dva roky od skončenia auditu.

Vydavateľ Zbierky zákonov Slovenskej republiky, správca obsahu a prevádzkovateľ právneho a informačného portálu Slov-Lex dostupného na webovom sídle www.slov-lex.sk je
Ministerstvo spravodlivosti Slovenskej republiky, Račianska 71, 813 11 Bratislava,
tel.: +421 2 888 91 864, +421 2 888 91 865, e-mail: helpdesk@slov-lex.sk.