Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Postupy posudzovania účinnosti opatrení

Riadenie súladu a kontrolné činnosti (Blok II)
Kurz: Manažér kybernetickej bezpečnosti

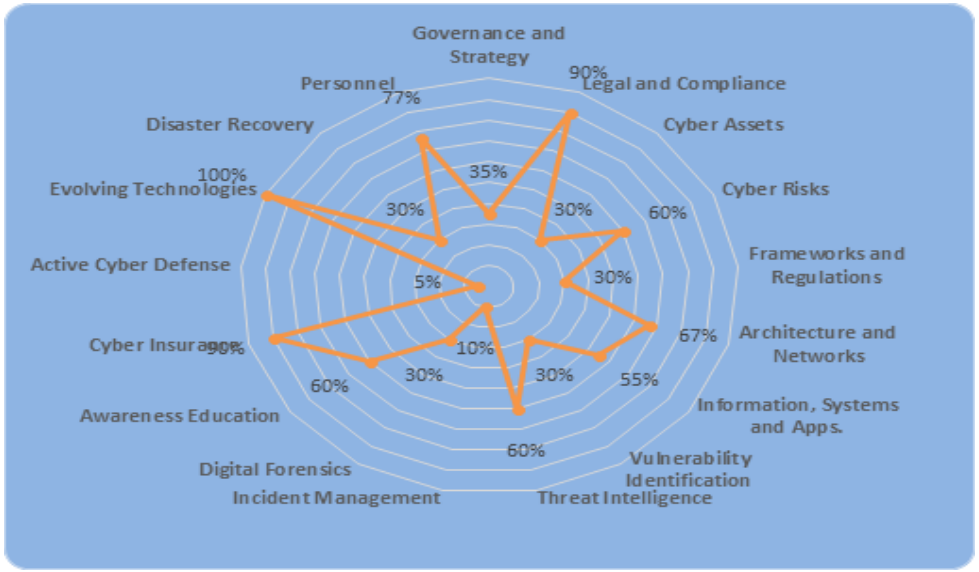
Doc. Ing. Katarína Kampová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Katarina.Kampova@uniza.sk

Definícia auditu (ISO 19011 / ISO 9000 / ISO/IEC 27007)

- Audit je systematický, nezávislý a zdokumentovaný proces získavania objektívnych dôkazov a ich objektívneho hodnotenia s cieľom určiť rozsah splnenia auditových kritérií.
- 👉 V praxi to znamená, že audit skúma, či sú napríklad procesy, systémy alebo produkty v súlade s požiadavkami (napr. normy, zákony, interné smernice) a či sa správne implementujú a udržiavajú.



Typy auditov

- Podľa ISO štandardov sa audity zvyčajne delia takto:

1. **Interný audit (prvá strana / first-party audit)**
    1. vykonáva sa vo vlastnej organizácii (napr. audit kvality, bezpečnosti, IT)
    2. cieľ: preveriť súlad s internými požiadavkami a pripraviť sa na externé audity
2. **Externý audit (druhá alebo tretia strana)**
    1. **Druhá strana (second-party audit)**
        1. vykonáva napr. zákazník voči dodávateľovi (audit dodávateľov)
    2. **Tretia strana (third-party audit)**
        1. vykonáva nezávislá certifikačná alebo dozorná organizácia
        2. cieľ: certifikácia (napr. ISO 9001, ISO/IEC 27001) alebo akreditácia

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďalšie delenia auditov

- **Podľa predmetu**:
  - audit systému (napr. ISMS, QMS, EMS)
  - audit procesu (napr. výrobný proces, softvérový proces)
  - audit produktu (napr. vyhovuje finálny produkt požiadavkám?)
- **Podľa účelu:**
  - audit zhody (compliance audit)
  - audit výkonnosti (performance audit)
  - audit bezpečnosti (security audit)
  - audit environmentálneho manažmentu (environmental audit)
- **Podľa rozsahu / hĺbky:**
  - kompletný audit (full audit)
  - čiastočný audit (partial audit)
  - kontrolný / následný audit (follow-up audit)

Čo je audit kybernetickej bezpečnosti?

- Auditom kybernetickej bezpečnosti sa rozumie overenie plnenia povinností podľa tohto zákona, posúdenie zhody prijatých bezpečnostných opatrení s požiadavkami podľa tohto zákona a osobitných predpisov, ktoré sa vzťahujú na bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby pre jednotlivé siete a informačné systémy služby a pre prostriedky, ktoré podporujú služby.
- Cieľom auditu kybernetickej bezpečnosti je zabezpečiť požadovanú úroveň kybernetickej bezpečnosti, predchádzať kybernetickým bezpečnostným incidentom a identifikovať nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby na navrhnutie a prijatie opatrení na ich odstránenie, nápravu existujúceho stavu a na predchádzanie kybernetickým bezpečnostným.

Prečo robiť audit kybernetickej bezpečnosti?

- Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek ustanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti do dvoch rokov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov základnej služby.
- Prevádzkovateľ základnej služby, ktorý nie je prevádzkovateľom kritickej základnej služby, môže zabezpečiť plnenie povinnosti vykonať audit kybernetickej bezpečnosti v lehote podľa predchádzajúcej vety preverením účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených týmto zákonom samohodnotením prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.

Samohodnotenie PZS

Samohodnotenie PZS

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Samohodnotenie v zmysle zákona o kybernetickej bezpečnosti

Vážený prevádzkovateľ základnej služby (PZS),

tento formulár samohodnotenia je určený pre tých PZS, ktorí:

1. majú v období od 1. augusta 2021 do 31. decembra 2023 povinnosť auditu podľa zákona č. 69/2018 Z.z. vo kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“),
2. majú len informačné systémy kategórie I. a II. podľa vyhlášky Národného bezpečnostného úradu č. 362/2018 Z.z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška č. 362/2018 Z. z.“) a
3. majú určeného manažéra kybernetickej bezpečnosti.

Tento formulár vypĺňa za PZS určený manažér kybernetickej bezpečnosti na základe aktuálneho stavu v prostredí PZS pravdivo a tak aby uvedené odpovede bolo možné v prípade potreby preveriť.
K jednotlivým otázkam je odporúčané pripojiť dokumenty podporujúce vyplnené tvrdenia.

K vyplnenému formuláru je potrebné priložiť plán implementácie opatrení kybernetickej bezpečnosti na nasledujúce obdobie schválené štatutárom.

Vyplnený formulár s plánom implementácie opatrení je potrebné elektronicky podpísať kvalifikovaným elektronickým podpisom štatutára a zaslať e-mailom na podatelna@nbu.gov.sk, prípadne zaslať do elektronickej schránky Národného bezpečnostného úradu (NBÚ) prostredníctvom ÚPVS (slovensko.sk).

Časť A: Identifikácia PZS

Identifikácia prevádzkovateľa základných služieb.

A.1 Názov PZS

A.2 Sídlo PZS

Ulica

Číslo ulice

Mesto

PSČ

Časť C: Manažér KB

Identifikácia určeného manažéra kybernetickej bezpečnosti a vyjadrenie sa k popisu jeho právomocí, povinností a zodpovedností, ktoré sú súčasťou jeho pracovnej náplne alebo obdobného opisu jeho pracovných činností.

C.1 Meno určeného manažéra KB

C.2 Dátum určenia do funkcie manažéra KB

C.3

Vyplýva z pozície Vami určeného manažéra KB jeho možnosť predkladať návrhy a oznamovať informácie v oblasti KB priamo štatutárnemu orgánu danej PZS a jeho nezávislosť od riadenia prevádzky a vývoja služieb informačných technológií?

○ Áno ○ Nie

Kedy realizujeme audit KB?

- PZS je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti v rozsahu stanovenom podľa všeobecne záväzného právneho predpisu, ktorý vydá úrad, a to po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale.
- Prevádzkovateľ základnej služby, ktorý nie je prevádzkovateľom kritickej základnej služby, môže v periodicite ustanovenej podľa § 32 ods. 1 písm. d) zabezpečiť plnenie povinnosti vykonať audit kybernetickej bezpečnosti vykonaním samohodnotenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.
- Samohodnotenie vykonáva manažér kybernetickej bezpečnosti. Takýto prevádzkovateľ základnej služby je povinný podrobiť sa auditu kybernetickej bezpečnosti do piatich rokov odo dňa zaradenia do registra prevádzkovateľov základnej služby a následne podľa periodicity ustanovenej podľa § 32 ods. 1 písm. d). V čase povinnosti vykonať audit kybernetickej bezpečnosti sa samohodnotenie nevykonáva.

Kým sa vykonáva audit kybernetickej bezpečnosti?

- Audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti, ktorým je:
  - fyzická osoba,
  - spoločník,
  - štatutárny orgán
  - alebo zamestnanec právnickej osoby.
- Certifikáciu audítora kybernetickej bezpečnosti vykonáva subjekt verejnej správy akreditovaný podľa osobitného predpisu ako orgán certifikujúci osoby (ďalej len „orgán certifikujúci osoby“) v oblasti kybernetickej bezpečnosti.

Kým sa vykonáva audit kybernetickej bezpečnosti?

- Právnická osoba zabezpečuje audit kybernetickej bezpečnosti prostredníctvom certifikovaného audítora kybernetickej bezpečnosti alebo certifikovaných audítorov kybernetickej bezpečnosti. Zabezpečovanie auditu kybernetickej bezpečnosti právnickou osobou je podnikaním podľa obchodného zákonníka.
- Ak právnická osoba zabezpečuje audit prostredníctvom certifikovaného audítora kybernetickej bezpečnosti, zodpovedá za škodu spôsobenú pri výkone auditu kybernetickej bezpečnosti táto právnická osoba.
- Fyzická osoba

ZOZNAM VIAZANÝCH ŽIVNOSTÍ

Por. čís.	Živnosť	Preukaz spôsobilosti	Poznámka	Zoz-nam
99.	Certifikovaný audítor kybernetickej bezpečnosti	- certifikát audítora kybernetickej bezpečnosti	§ 29 ods. 3 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov	

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zoznam certifikovaných audítorov

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

ÚRAD | OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ A LIMITOVANÝCH INFORMÁCIÍ | ŠIFROVÁ OCHRANA INFORMÁCIÍ

Kybernetická bezpečnosť » Audit » Informatívny zoznam audítorov

Informatívny zoznam audítorov

Informatívny zoznam audítorov ako **fyzických osôb** je hypertextovým odkazom na webové sídlo certifikačného orgánu; za jeho aktuálnosť a správnosť úrad nezodpovedá.

Fyzické osoby

- audítori certifikovaní Kompetenčným a certifikačným centrom kybernetickej bezpečnosti
- audítori certifikovaní TÜV SÜD Slovakia s.r.o.

Právnické osoby

(zoznam sa aktualizuje)

Právnická osoba zabezpečuje audit kybernetickej bezpečnosti prostredníctvom certifikovaného audítora kybernetickej bezpečnosti alebo certifikovaných audítorov kybernetickej bezpečnosti.

Zoznam držiteľov certifikátov ku dňu 14.04.2025:

Meno, priezvisko, titul	Číslo certifikátu	Platnosť certifikátu
Ing. Ivan Makatura, CRISC, CDPSE	001/O-024:2023	28.04.2026
Ing. Tomáš Hettych, CISA, CISM, CGEIT, CRISC, CDPSE	002/O-024:2023	28.04.2026
Mgr. Anton Horváth, CISA, CISM	003/O-024:2023	28.04.2026
Ing. Michal Ďorda, CISA, CISSP	004/O-024:2023	30.05.2026
Mgr. Peter Borák, CISM, CISA, CGEIT, CRISC, CISSP	005/O-024:2023	30.05.2026
Ing. Marián Illovský, CISA, CIA, CDPSE	006/O-024:2023	30.05.2026
Ing. David Dvořák, CISA, CISM, CRISC	007/O-024:2023	05.06.2026
Ing. Katarína Géciová, CISA	008/O-024:2023	05.06.2026
Ing. Mikuláš Zalai, CISA, CGEIT, CRISC, CCISO	009/O-024:2023	05.06.2026
Ing. Marek Uličný	010/O-024:2023	05.06.2026
Ing. Adrian Bagala	011/ O-024:2023	19.06.2026
Ing. Luděk Novák, PhD, CISA, CISSP, CGEIT, CRISC, CSX-P	012/ O-024:2023	21.08.2026

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Požiadavky na audit kybernetickej bezpečnosti

§ 29 Audit

(1) Auditom kybernetickej bezpečnosti sa rozumie overenie plnenia povinností podľa tohto zákona, posúdenie zhody prijatých bezpečnostných opatrení s požiadavkami podľa tohto zákona a osobitných predpisov, ktoré sa vzťahujú na bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby pre jednotlivé siete a informačné systémy služby a pre prostriedky, ktoré podporujú služby. Cieľom auditu kybernetickej bezpečnosti je zabezpečiť požadovanú úroveň kybernetickej bezpečnosti, predchádzať kybernetickým bezpečnostným incidentom a identifikovať nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby na navrhnutie a prijatie opatrení na ich odstránenie, nápravu existujúceho stavu a na predchádzanie kybernetickým bezpečnostným incidentom. Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek ustanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti do dvoch rokov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov základnej služby. Prevádzkovateľ základnej služby, ktorý nie je prevádzkovateľom kritickej základnej služby, môže zabezpečiť plnenie povinnosti vykonať audit kybernetickej bezpečnosti v lehote podľa predchádzajúcej vety preverením účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených týmto zákonom samohodnotením prostredníctvom jednotného informačného systému kybernetickej bezpečnosti spôsobom podľa odseku 8.

Požiadavky na audit kybernetickej bezpečnosti

(2) Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti v rozsahu stanovenom podľa všeobecne záväzného právneho predpisu, ktorý vydá úrad, a to po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale.

(3) Audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti,[31]) ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby. Certifikáciu audítora kybernetickej bezpečnosti vykonáva subjekt verejnej správy podľa osobitného predpisu[31aa]) akreditovaný podľa osobitného predpisu[31a]) ako orgán certifikujúci osoby[31b]) (ďalej len „orgán certifikujúci osoby“) v oblasti kybernetickej bezpečnosti.

(4) Právnická osoba zabezpečuje audit kybernetickej bezpečnosti prostredníctvom certifikovaného audítora kybernetickej bezpečnosti alebo certifikovaných audítorov kybernetickej bezpečnosti. Zabezpečovanie auditu kybernetickej bezpečnosti právnickou osobou je podnikaním podľa osobitného predpisu.[31c]) Ak právnická osoba zabezpečuje audit prostredníctvom certifikovaného audítora kybernetickej bezpečnosti, zodpovedá za škodu spôsobenú pri výkone auditu kybernetickej bezpečnosti táto právnická osoba.

Požiadavky na audit kybernetickej bezpečnosti

(5) Prevádzkovateľ základnej služby je povinný predložiť záverečnú správu o výsledkoch auditu úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu.

(6) Úrad môže kedykoľvek vykonať audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby alebo požiadať certifikovaného audítora kybernetickej bezpečnosti, aby vykonal takýto audit u prevádzkovateľa základnej služby s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom.

(7) Náklady na audit kybernetickej bezpečnosti podľa odseku 1 znáša prevádzkovateľ základnej služby a náklady na audit kybernetickej bezpečnosti podľa odseku 6 znáša úrad.

(8) Prevádzkovateľ základnej služby, ktorý nie je prevádzkovateľom kritickej základnej služby, môže v periodicite ustanovenej podľa **§ 32 ods. 1 písm. d)** zabezpečiť plnenie povinnosti vykonať audit kybernetickej bezpečnosti vykonaním samohodnotenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. Samohodnotenie vykonáva manažér kybernetickej bezpečnosti. Takýto prevádzkovateľ základnej služby je povinný podrobiť sa auditu kybernetickej bezpečnosti do piatich rokov odo dňa zaradenia do registra prevádzkovateľov základnej služby a následne podľa periodicity ustanovenej podľa **§ 32 ods. 1 písm. d)**. V čase povinnosti vykonať audit kybernetickej bezpečnosti sa samohodnotenie nevykonáva.

(9) Prevádzkovateľ základnej služby, na ktorého sa vzťahuje nariadenie (EÚ) 2022/2554, vykonáva preverenie účinnosti prijatých bezpečnostných opatrení podľa nariadenia (EÚ) 2022/2554, osobou podľa odseku 3.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zhrnutie požiadaviek k auditu KB

Č.	Oblasť	Kontrolné body
1	Účel auditu	✓ Overenie plnenia povinností podľa zákona č. 69/2018 Z. z. ✓ Posúdenie zhody opatrení s požiadavkami zákona a predpisov ✓ Preverenie sietí, IS a podporných prostriedkov ✓ Zabezpečenie úrovne bezpečnosti, prevencia incidentov, identifikácia nedostatkov a návrhy opatrení
2	Povinnosť auditu	✓ Do 2 rokov od zaradenia do registra PZS ✓ Po významných zmenách s dopadom na opatrenia ✓ V intervaloch podľa vyhlášky (min. raz za 2 roky) ✓ Ne-kritické PZS: samohodnotenie cez systém, ale raz za 5 rokov riadny audit
3	Audítor	✓ Certifikovaný audítor kybernetickej bezpečnosti (fyzická osoba, štatutár, zamestnanec právnickej osoby) ✓ Certifikácia akreditovaným orgánom ✓ Pri audite cez právnickú osobu: právnická osoba zodpovedá za prípadnú škodu
4	Záverečná správa	✓ Vypracovanie záverečnej správy ✓ Návrh opatrení a lehôt na odstránenie nedostatkov ✓ Predloženie správy úradu do 30 dní od ukončenia auditu
5	Mimoriadny audit úradu	✓ Úrad môže kedykoľvek vykonať audit alebo poveriť audítora ✓ Cieľ: potvrdiť účinnosť opatrení a súlad s požiadavkami zákona
6	Náklady	✓ Audit podľa ods. 1 → hradí prevádzkovateľ základnej služby ✓ Audit podľa ods. 6 → hradí úrad
7	Samohodnotenie (iba PZS)	✓ Samohodnotenie cez informačný systém KB ✓ Vykonáva manažér kybernetickej bezpečnosti ✓ Najneskôr raz za 5 rokov riadny audit (v tom čase sa samohodnotenie nevykonáva)
8	Špeciálne prípady (EÚ nariadenie)	✓ PZS podliehajúce nariadeniu EÚ 2022/2554 preverujú účinnosť opatrení podľa tohto nariadenia a osobami podľa ods. 3

Vyhláška č. 493/2022 Z.z. a audit kybernetickej bezpečnosti

493

VYHLÁŠKA

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

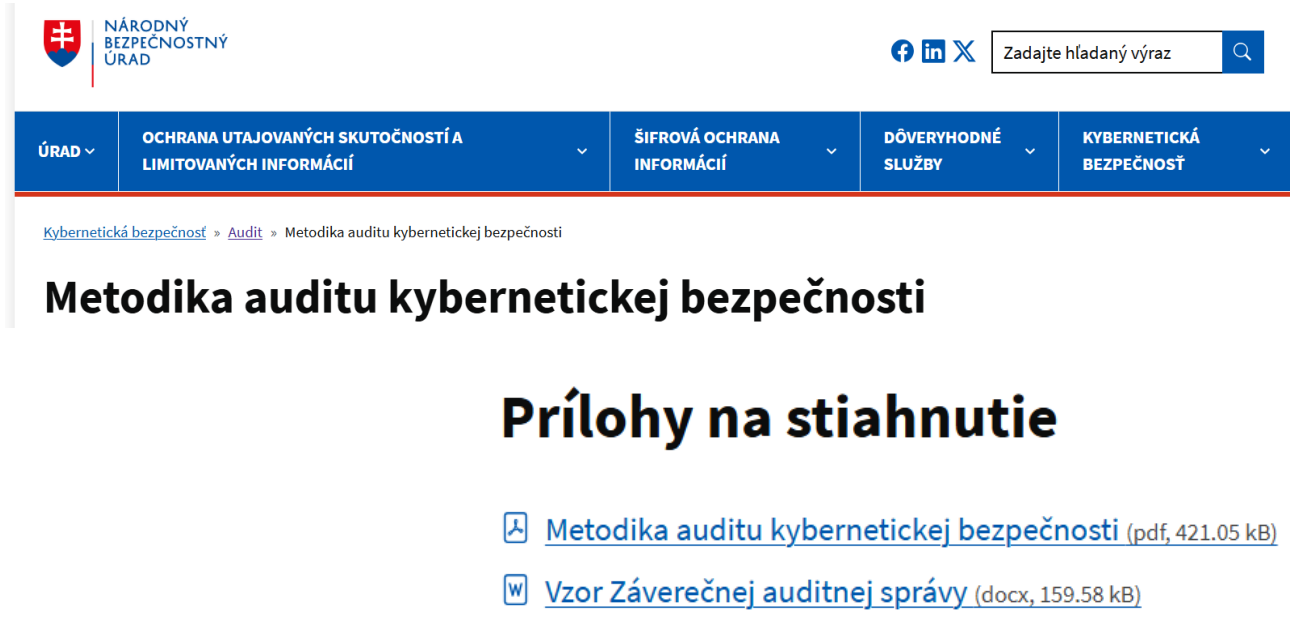
Národný bezpečnostný úrad (ďalej len „úrad“) podľa **§ 32 ods. 1 písm. f) zákona č. 69/2018 Z. z.** o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 287/2021 Z. z. (ďalej len „zákon“) ustanovuje:

§ 1

(1) Auditom kybernetickej bezpečnosti (ďalej len „audit“) sa overuje plnenie povinností podľa zákona a posudzuje sa zhoda prijatých bezpečnostných opatrení s požiadavkami podľa zákona a súvisiacich osobitných predpisov vzťahujúcich sa na bezpečnosť sietí a informačných systémov[1]) prevádzkovateľa základnej služby pre jednotlivé siete a informačné systémy základnej služby a pre tie, ktoré podporujú základné služby, s cieľom zabezpečiť požadovanú úroveň kybernetickej bezpečnosti a predchádzať kybernetickým bezpečnostným incidentom. Auditom sa identifikujú nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby s cieľom prijať opatrenia na ich odstránenie a nápravu a na predchádzanie kybernetickým bezpečnostným incidentom.

Metodika auditu kybernetickej bezpečnosti

- Účelom metodiky auditu je zaručiť kompatibilitu postupov audítorov a jednotnosť formátu záverečných správ auditu.
- https://www.nbu.gov.sk/metodika-auditu-kybernetickej-bezpecnosti/



Činnosti pri výkone auditu podľa vyhlášky č. 493/2022 Z.z.

Krok auditu	Opis činnosti
a) Prijatie žiadosti	Prijatie žiadosti podľa prílohy č. 1; kontrola kompletnosti údajov; prípadné vyžiadanie ďalších informácií.
b) Príprava harmonogramu	Obsahuje: 1. Identifikácia organizačných útvarov, procesov, auditovaných sietí, IS a lokalít s časom. 2. Meno, priezvisko, kontakt zodpovedného zamestnanca prevádzkovateľa.
c) Určenie rozsahu auditu	Určenie rozsahu podľa prílohy č. 2.
d) Určenie metód auditu	Výber vhodných metód auditu.
e) Príprava podkladov a dokumentov	Pracovné dokumenty, ktoré sú prílohou záverečnej správy, najmä: 1. Zápisy zo stretnutí. 2. Evidencia dôkazov. 3. Evidencia účastníkov. 4. Evidencia lokalít.
f) Preskúmanie dokumentácie a opatrení	Preskúmanie bezpečnostnej dokumentácie, vyhodnotenie opatrení a vypracovanie kontrolného záznamu podľa prílohy č. 3.
g) Zber a vyhodnotenie dôkazov	Zbieranie, sústreďovanie a vyhodnocovanie dôkazov o zisteniach.
h) Oboznámenie so zisteniami	Informovanie zodpovedného zamestnanca o nedostatkoch; zostavenie odporúčaných opatrení.
i) Vypracovanie záverečnej správy	Spracovanie správy podľa vzoru zo štandardu na výkon auditu kybernetickej bezpečnosti zverejneného na webovom sídle úradu.

Minimálne náležitosti žiadosti o vykonanie auditu KB

1. Identifikácia prevádzkovateľa základnej služby
2. Identifikácia základných služieb a auditovaných IS a sietí
3. Počet zamestnancov prevádzkovateľa základnej služby
4. Zoznam IS a klasifikácia s väzbou na základnú službu, vrátane:
   - Organizačné útvary a počet zamestnancov
   - Väzba IS a sietí na základnú službu, vplyv výpadku
   - Počet užívateľov, teritoriálne rozloženie, dôsledky výpadku
   - Systém správy, dodávatelia, SLA
   - Sieťová architektúra a prepojenia
   - Zoznam aktív, technológií, klasifikácia
   - Správa z penetračných testov (ak sú vykonané)
   - Správa z predošlého auditu
5. Kontaktná osoba (meno, priezvisko, kontakt)
6. Evidencia incidentov s dopadom na základné služby (od posledného auditu alebo za posledné 2 roky pri prvom audite)
7. Rozhodnutie o pokute, ďalšie porušenia povinností
8. Bezpečnostná dokumentácia (§ 20 ods. 5 zákona alebo osobitného predpisu)
9. Číslo platného potvrdenia o priemyselnej bezpečnosti (ak je vydané)

Žiadosť o výkon auditu kybernetickej bezpečnosti

doc. Ing. Katarína Kampová, PhD.
audítorka kybernetickej bezpečnosti

Vec
Žiadosť o výkon auditu kybernetickej bezpečnosti

Vážená audítorka,

zasielame Vám formálnu žiadosť na výkon auditu kybernetickej bezpečnosti podľa Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej len „Zákon") v súlade s prílohou č. 1 k vyhláške Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti.

1. Identifikácia prevádzkovateľa základnej služby (PZS)	
Obchodné meno	
Sídlo	
Prevádzka(y)	
IČO	
Štatutárny orgán	
Zodpovedný zástupca (kontaktná osoba)	

2. Identifikácia základných služieb podporených auditovanými informačnými systémami a sieťami	
Základná služba	
Sektor	
Podsektor	

3. Počet zamestnancov PZS	
Počet zamestnancov	

4. Zoznam informačných systémov a ich klasifikácia s väzbou na základnú službu a pre každý z nich najmenej informácie o informačnom systéme a	
Zoznam informačných systémov a ich klasifikácia s väzbou na základnú službu	Základná služba: ▪ Informačný systém 1 (Kategória X.) ▪ Informačný systém 2 (Kategória X.) ▪ …
a) *identifikácia organizačných útvarov PZS a počet zamestnancov prevádzkujúcich informačné systémy a siete, pri externom zabezpečovaní činností správy informačných systémov rozsah využívaných služieb v človekodňoch; pri doložení výsledkov auditu na externe zabezpečované činnosti sa externí pracovníci nezapočítavajú,*	Zoznam externých poskytovateľov správy informačných systémov a súvisiace zmluvy nie sú súčasťou žiadosti o výkon auditu kybernetickej bezpečnosti – Príloha č. X.
b) *väzba siete a informačného systému na prevádzkovanú základnú službu; ktorá základná služba je závislá od informačného systému, aký je vplyv výpadku informačného systému na základnú službu,*	Priama väzba. Závislosť základných služieb od informačných systémov nie je súčasťou žiadosti o výkon auditu kybernetickej bezpečnosti – Príloha č. X.
c) *počet užívateľov základnej služby, teritoriálne rozloženie a dôsledky pri výpadku základnej služby na jej užívateľov,*	Presný počet užívateľov základnej služby nie je možné identifikovať. Pri výpadku základnej služby by boli postihnutí užívatelia prevažne v regióne … a organizácie v zriaďovateľskej pôsobnosti …
d) *systém správy, interné a externé zdroje, identifikácia kľúčových dodávateľov a zmlúv a dohôd o úrovni poskytovaných služieb,*	Centralizovaná správa. Identifikácia kľúčových dodávateľov a zmlúv a dohôd nie je súčasťou žiadosti o výkon auditu kybernetickej bezpečnosti – Príloha č. X.
e) *schéma sieťovej architektúry s uvedením miest prepojení sietí a pripojenia voči externým sieťam,*	Je súčasťou žiadosti o výkon auditu kybernetickej bezpečnosti – Príloha č. X.
f) *zoznam aktív a používaných technológií so závislosťami od iných informačných systémov a služieb dodávateľov s uvedením vlastníkov týchto aktív a identifikáciou citlivosti podľa osobitného predpisu,*	Je súčasťou žiadosti o výkon auditu kybernetickej bezpečnosti – Príloha č. X.
g) *organizačné útvary a počty zamestnancov prevádzkujúcich informačné systémy a siete vrátane počtu dodávateľov,*	Je súčasťou žiadosti o výkon auditu kybernetickej bezpečnosti – Príloha č. X.
h) *správa z posledného penetračného testovania informačného systému, použitá*	Je súčasťou žiadosti o výkon auditu kybernetickej bezpečnosti – Príloha č. X.

Určenie rozsahu trvania auditu KB

- Pred začiatkom auditu sa určí dĺžka jeho trvania s cieľom dostatočne posúdiť predmet auditu. Pri výpočte trvania dĺžky auditu sa zohľadňujú informácie zo žiadosti o vykonanie auditu kybernetickej bezpečnosti a dodatočne vyžiadané informácie, najmä:

Faktor / kategória	Popis a význam pre audit
Počet interných zamestnancov a externých dodávateľov	Koľko ľudí spravuje siete a systémy. Viac ľudí → **zložitejší audit.**
Kategorizácia sietí a informačných systémov	Ako sú siete a systémy dôležité/kritické. Vyššia kategória → **dôkladnejšie preverenie.**
Systémová architektúra prostredia	Či je prostredie centralizované alebo decentralizované. Decentralizácia → **náročnejší a dlhší audit.**
Množstvo, rozsah a komplexnosť dokumentácie	Počet a náročnosť dokumentov (politiky, záznamy, výsledky auditov, analýzy rizík). Viac dokumentov → **dlhší audit.**
Počet tretích strán	Koľko externých firiem sa podieľa na prevádzke systémov. Viac strán → **vyššia náročnosť preverenia.**
Počet lokalít	Počet miest/pobočiek, ktoré podporujú základnú službu. Viac lokalít → **viac dní auditu.**

Určenie rozsahu trvania auditu KB

Celkový počet zamestnancov zúčastňujúcich sa na prevádzke IS a bezpečnosti	Základný rozsah auditu (človeko-dni)
1 – 10	5
11 – 20	6
21 – 30	7
31 – 40	8
41 – 50	9
51 – 60	10
> 60	+1 deň za každých ďalších 10 zamestnancov

- **Špeciálne pravidlá (nezvyšujú auditný čas)**
  - Ak sa zamestnanci z iných lokalít pripájajú len **vzdialene** → auditný čas sa nezvyšuje.
  - Ak viaceré systémy spravujú **tie isté osoby a auditujú sa súčasne** → auditný čas sa nezvyšuje.
- Zvyšujúce faktory (viď. Prílohu vyhlášky)
- Znižujúce faktory (viď. Prílohu vyhlášky)
- Do časového rozsahu trvania auditu sa započítava spolu najviac v rozsahu **1/3 celkového potrebného časového rozsahu trvania auditu.** Tento čas je na prípravu auditu, záverečnej správy a posúdenie povinnej dokumentácie

Plán auditu

- Kroky v rámci plánovania auditu:
  - Auditný program
  - Určenie zdrojov v programe auditu
  - Začatie auditu
  - Poverenie výkonom auditu
  - Ustanovenie pre plán auditu

Určenie zdrojov programu auditu

Oblasť	Čo zvážiť
💰 Finančné a časové zdroje	Príprava, riadenie a zlepšovanie auditu (rozpočet, časové rezervy)
🛠️ Metódy auditu	Aké metódy sa použijú (rozhovory, kontrola dokumentácie, testovanie, pozorovanie)
👥 Dostupnosť audítorov a expertov	Kto má potrebné kompetencie na určité úlohy v rámci auditu
📏 Rozsah, riziká a príležitosti programu	Aký veľký je program, aké riziká a príležitosti z neho plynú
✈️ Cestovanie a ubytovanie	Čas a náklady na dopravu, ubytovanie, stravu, technické zabezpečenie na mieste
🌎 Časové pásma	Ak má organizácia geograficky vzdialené služby, treba zladiť časové pásma
💻 Technológie na vzdialenú spoluprácu	Napr. cloudové riešenia, telekonferenčné systémy, nástroje na zdieľanie dokumentov
🔧 Potrebné nástroje a zariadenia	Aké špeciálne vybavenie a technológie sú nevyhnutné na vykonanie auditu
📄 Dostupnosť dokumentácie	Aké dokumenty sú potrebné a či sú k dispozícii počas tvorby programu auditu
🔐 Bezpečnostné previerky a kryptografia	Požiadavky na prístup, zabezpečovacie mechanizmy, kryptografické opatrenia

Harmonogram auditu KB

📅 Harmonogram auditu (audit schedule)

- Je to **konkrétny časový plán auditu**.
- Obsahuje:
  - dátumy a časy auditu,
  - presné aktivity (napr. otvorenie auditu, preskúmanie dokumentácie, návšteva lokalít, rozhovory, ukončenie auditu),
  - mená kontaktných osôb,
  - informáciu, kedy a kde sa bude čo diať.
- **Príklad:**
  - 9:00 – 9:30: Otváracie stretnutie
  - 10:00 – 12:00: Preskúmanie bezpečnostnej dokumentácie
  - 13:00 – 15:00: Prehliadka serverovne
  - 15:30 – 16:00: Ukončovacie stretnutie

Harmonogram auditu

1. Identifikácia prevádzkovateľa základnej služby (PZS)	
Obchodné meno	
Sídlo	
Prevádzka(y)	
IČO	
Štatutárny orgán	
Zodpovedný zástupca (kontaktná osoba)	

2. Identifikácia základných služieb podporených auditovanými informačnými systémami a sieťami	
Základná služba	
Sektor	
Podsektor	

3. Ciele auditu	
Vyžadovaný audit kybernetickej bezpečnosti zo strany PZS	Overenie plnenia povinností podľa Zákona č. 69/2018 Z. z. a posúdenie zhody prijatých bezpečnostných opatrení s požiadavkami podľa zákona a súvisiacich osobitných predpisov vzťahujúcich sa na bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby pre jednotlivé siete a informačné systémy základnej služby a pre tie, ktoré podporujú základné služby, s cieľom zabezpečiť požadovanú úroveň kybernetickej bezpečnosti a predchádzať kybernetickým bezpečnostným incidentom. Auditom sa identifikujú nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby s cieľom prijať opatrenia na ich odstránenie a nápravu a na predchádzanie kybernetickým bezpečnostným incidentom.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Začatie auditu

- Audítor má zaistiť vykonanie kontaktu s auditovaným PZS na:

a) prípadne doplnenie a finálne odsúhlasenie žiadosti o vykonanie auditu;

b) odsúhlasenie harmonogramu a výpočtu rozsahu trvania auditu;

c) potvrdenie komunikačných kanálov s predstaviteľmi auditovaného PZS;

d) potvrdenie právomoci na vykonanie auditu;

e) poskytnutie relevantných informácií o cieľoch, predmete, kritériách, metódach auditu a o zložení audítorského tímu vrátane akýchkoľvek technických expertov;

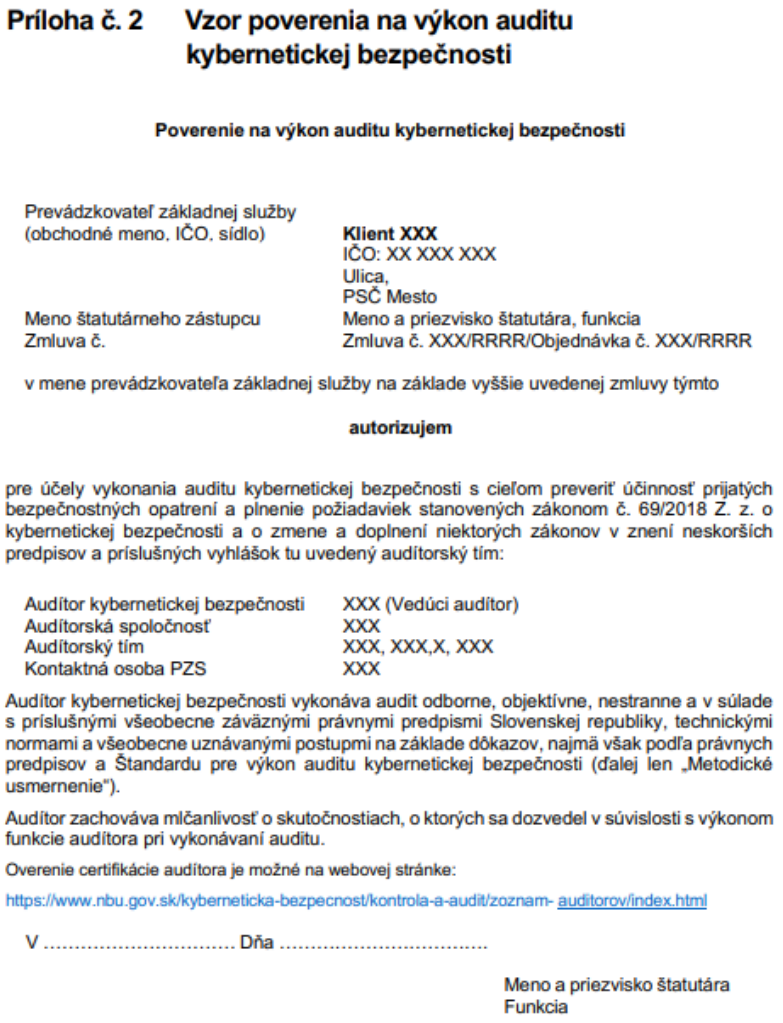
f) vyžiadanie prístupu k relevantným informáciám na účely plánovania vrátane informácií o rizikách a príležitostiach, ktoré PZS identifikoval, a o tom, ako sa zvládajú;

g) potvrdenie dohody s auditovaným PZS, ktorá sa týka rozsahu zachovania mlčanlivosti a zaobchádzania s dôvernými informáciami;

h) určenie akýchkoľvek špecifických požiadaviek na prístup, na bezpečnosť a ochranu zdravia, na bezpečnosť, dôvernosť alebo na ďalšie požiadavky.

Poverenie výkonom auditu

- Poverenie obsahuje najmä:
  - Určenie rozsahu auditu
  - Menovanie vedúceho audítora
  - Vyhlásenie PZS o záväzku vykonať audit kybernetickej bezpečnosti
  - Meno kontaktnej osoby (osôb), ktorá je v mene PZS povinná poskytnúť audítorovi súčinnosť
  - Predpokladaný začiatok a koniec auditu
- Vzor poverenia na výkon auditu kybernetickej bezpečnosti je v Prílohe č. 2 tejto metodiky.



Príloha č. 2 Vzor poverenia na výkon auditu kybernetickej bezpečnosti

Poverenie na výkon auditu kybernetickej bezpečnosti

Prevádzkovateľ základnej služby (obchodné meno, IČO, sídlo)	**Klient XXX** IČO: XX XXX XXX Ulica, PSČ Mesto
Meno štatutárneho zástupcu	Meno a priezvisko štatutára, funkcia
Zmluva č.	Zmluva č. XXX/RRRR/Objednávka č. XXX/RRRR

v mene prevádzkovateľa základnej služby na základe vyššie uvedenej zmluvy týmto

autorizujem

pre účely vykonania auditu kybernetickej bezpečnosti s cieľom preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a príslušných vyhlášok tu uvedený audítorský tím:

Audítor kybernetickej bezpečnosti	XXX (Vedúci audítor)
Audítorská spoločnosť	XXX
Audítorský tím	XXX, XXX,X, XXX
Kontaktná osoba PZS	XXX

Audítor kybernetickej bezpečnosti vykonáva audit odborne, objektívne, nestranne a v súlade s príslušnými všeobecne záväznými právnymi predpismi Slovenskej republiky, technickými normami a všeobecne uznávanými postupmi na základe dôkazov, najmä však podľa právnych predpisov a Štandardu pre výkon auditu kybernetickej bezpečnosti (ďalej len „Metodické usmernenie").

Audítor zachováva mlčanlivosť o skutočnostiach, o ktorých sa dozvedel v súvislosti s výkonom funkcie audítora pri vykonávaní auditu.

Overenie certifikácie audítora je možné na webovej stránke:

https://www.nbu.gov.sk/kyberneticka-bezpecnost/kontrola-a-audit/zoznam- auditorov/index.html

V ..... Dňa .....

Meno a priezvisko štatutára
Funkcia

Priebeh auditu KB - Otváracie stretnutie

- **Kedy a ako:**
  - Realizuje sa až po podpise poverenia audítora.
  - Termín a účasť dohodne vedúci audítor.
- **Účel stretnutia:**
  - Potvrdiť dohodu všetkých strán (PZS a audítorského tímu) s plánom auditu.
  - Predstaviť audítorský tím a jeho roly.
  - Uistiť sa, že všetky činnosti auditu môžu byť vykonané.
- **Účastníci:**
  - Manažment PZS.
  - Podľa potreby zodpovední za základné služby.
- **Vedúci stretnutia:**
  - Certifikovaný audítor kybernetickej bezpečnosti.
  - Pri audite tímu → vedúci musí byť certifikovaný audítor.
- **Čo sa má overiť:**
  - Ciele, predmet a kritériá auditu.
  - Plán auditu, dátumy stretnutí, potrebné zmeny.
  - Oficiálne komunikačné kanály.
  - Jazyk auditu.
  - Spôsoby podávania informácií.
  - Dostupnosť zdrojov a zariadení pre audítorov.
  - Otázky dôvery a informačnej bezpečnosti.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Priebeh auditu KB - Získanie a overenie informácií

- **Cieľ:** Zhromažďovať a overovať informácie o cieľoch, predmete a kritériách auditu, vrátane rozhraní medzi funkciami, činnosťami a procesmi.
- **Zásady overovania:**
  - Akceptujú sa iba overiteľné informácie.
  - Pri nedostatočnej miere overenia → audítor využíva profesijný úsudok.
  - Každý dôkaz vedúci k zisteniu sa zaznamenáva.
  - Nové alebo zmenené zistenia → posúdiť vplyv na súlad/nesúlad.
- **Metódy zberu informácií:**
  - Rozhovory
  - Pozorovania
  - Dotazníky
  - Preskúmanie dokumentov
- **Dôležité pravidlá:**
  - Žiadny zásah do IS alebo sietí.
  - Informácie dodáva zodpovedný zamestnanec PZS cez dohodnutý kanál.
  - Zakázané: penetračné a výkonnostné testy počas auditu.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Priebeh auditu KB - Vzorkovanie pri audite

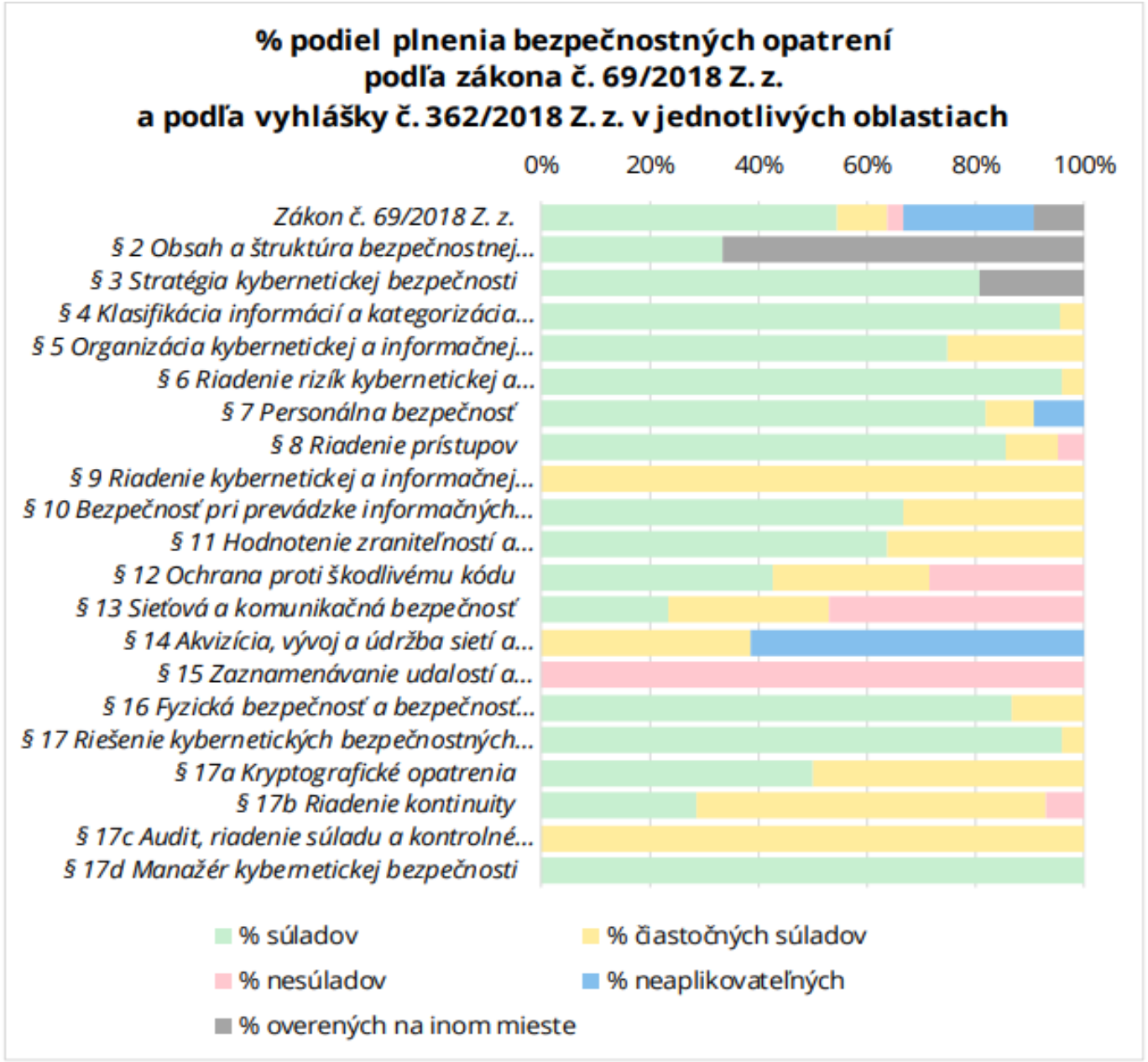
- **Čo to znamená:**
  - Výber menej ako 100 % položiek zo základného dátového súboru.
  - Cieľ → získať a vyhodnotiť dôkazy, aby bolo možné formulovať závery.
- **Kedy sa používa:**
  - Ak nie je praktické alebo efektívne preveriť všetky dostupné informácie.
  - Napr. záznamy sú príliš početné alebo rozptýlené.
- **Cieľ vzorkovania:**
  - Poskytnúť audítorovi istotu, že ciele auditu môžu byť (alebo budú) dosiahnuté.
  - Audítor zodpovedá za výber vzorky.
- 📊 **Kroky vzorkovania:**

1. Vypracovanie cieľov odberu vzorky
2. Výber rozsahu a zloženia základného súboru
3. Výber metódy odberu vzorky
4. Určenie veľkosti vzorky
5. Vykonanie odberu vzorky
6. Vyhodnotenie, vykazovanie, dokumentovanie výsledkov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Priebeh auditu KB - Kritéria auditu

- Auditom sa identifikujú nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby.
- Súlad, čiastočný súlad alebo nesúlad sa identifikuje pre:
  - jednotlivé požiadavky Zákona, všeobecné bezpečnostné opatrenia a sektorové bezpečnostné opatrenia ak existujú a sú prijaté pri ich aplikovaní nad jednotlivými sieťami a IS základnej služby a ich podpornými komponentami.
- Kritériami auditu kybernetickej bezpečnosti je overenie a posúdenie:
  - plnenia povinností prevádzkovateľa základnej služby podľa § 19 Zákona,
  - plnenia ostatných povinností prevádzkovateľa základnej služby uvedených v § 20, ...
  - súladu prijatých všeobecných bezpečnostných opatrení s požiadavkami podľa § 20 Zákona a príslušnej vykonávacej vyhlášky, ktorou sú definované všeobecné bezpečnostné opatrenia,
  - súladu so všeobecne záväzným právnym predpisom, ktorý vydal Ústredný orgán v spolupráci s Úradom a ktorým ustanovia sektorové bezpečnostné opatrenia.


% podiel plnenia bezpečnostných opatrení
podľa zákona č. 69/2018 Z. z.
a podľa vyhlášky č. 362/2018 Z. z. v jednotlivých oblastiach
0%
20%
40%
60%
80%
100%
Zákon č. 69/2018 Z. z.
§ 2 Obsah a štruktúra bezpečnostnej...
§ 3 Stratégia kybernetickej bezpečnosti
§ 4 Klasifikácia informácií a kategorizácia...
§ 5 Organizácia kybernetickej a informačnej...
§ 6 Riadenie rizík kybernetickej a...
§ 7 Personálna bezpečnosť
§ 8 Riadenie prístupov
§ 9 Riadenie kybernetickej a informačnej...
§ 10 Bezpečnosť pri prevádzke informačných...
§ 11 Hodnotenie zraniteľností a...
§ 12 Ochrana proti škodlivému kódu
§ 13 Sieťová a komunikačná bezpečnosť
§ 14 Akvizícia, vývoj a údržba sietí a...
§ 15 Zaznamenávanie udalostí a...
§ 16 Fyzická bezpečnosť a bezpečnosť...
§ 17 Riešenie kybernetických bezpečnostných...
§ 17a Kryptografické opatrenia
§ 17b Riadenie kontinuity
§ 17c Audit, riadenie súladu a kontrolné...
§ 17d Manažér kybernetickej bezpečnosti
% súladov
% čiastočných súladov
% nesúladov
% neaplikovateľných
% overených na inom mieste

Čo sa posudzuje?

Komponent	Predmet posúdenia
Funkcia	Akým spôsobom sú plnené základné funkcie v kontexte auditného kritéria
Dokumentácia	Ako je bezpečnostné kritérium zdokumentované, či existuje príslušná politika a či politika je zverejnená
Roly	Ako sú pre auditné kritérium definované a obsadené jednotlivé roly, rozsah ich právomocí a zodpovedností
Činnosti	Či sú v súvislosti s auditným kritériom vykonávané všetky činnosti, odporúčané podľa dobrej praxe
Nástroj	Ak je auditným kritériom nástroj, posúdiť, ako spĺňa kvalita nástroja požiadavky dobrej praxe
Údaje	Aká je kvalita údajov, ktorými je zdokumentované auditné kritérium
Metrika	Ako sú stanovené kritériá pre meranie kvality príslušného auditného kritéria, ako sa tieto merania spracovávajú a vyhodnocujú

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Tvorba zistení auditu

- Auditný dôkaz sa má vyhodnocovať oproti stanoveným kritériám auditu, s cieľom objektívne určiť zistenia auditu. Zistenia auditu sú uvádzané ako:

Súlad	ak je kritérium auditu plnene a audítor neidentifikoval riziko	
Čiastočný súlad	ak je kritérium auditu plnene iba čiastočne	
Nesúlad	Ak kritérium auditu nie je splnené, alebo ak audítor identifikoval riziko súvisiace s daným kritériom	

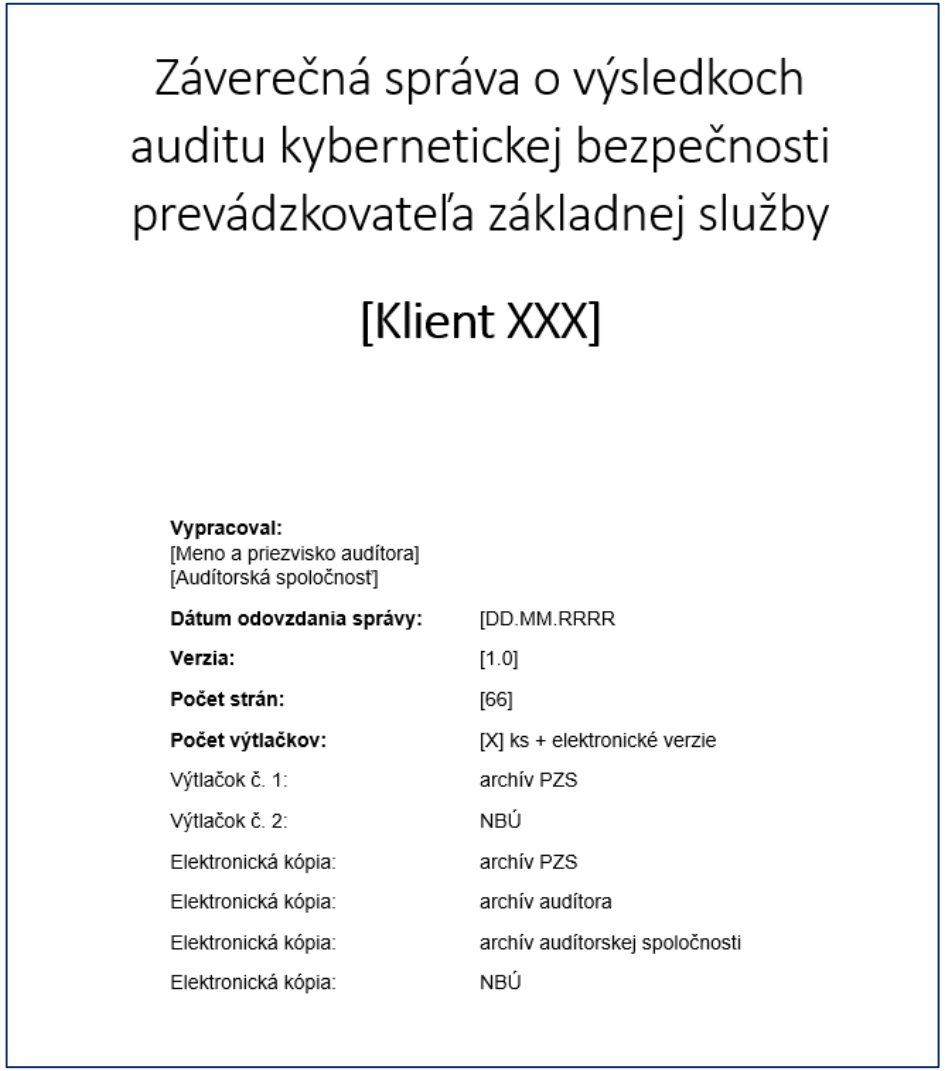
- V prípade, že kritérium auditu nie je relevantné pre PZS alebo jeho prostredie, audítor vyhodnotí príslušnú požiadavku v kontrolnom zázname ako „NEAPLIKOVATEĽNÉ“

Ukončenie auditu - Obsah a formát správy z auditu

- Audítor má spracovať správu auditu kybernetickej bezpečnosti, ktorej súčasťou je kontrolný záznam o výsledkoch auditu podľa prílohy č. 3 k vyhláške č. 493/2022 Z. z.
- Vzor formátu správy auditu kybernetickej bezpečnosti, vrátane vzoru kontrolného záznamu o výsledkoch auditu je v Prílohe č. 4 tejto metodiky.
- V prípade elektronickej verzie správy z auditu, audítor podpisuje správu svojim kvalifikovaným elektronickým podpisom (KEP).
- Audítor uchováva auditnú správu s odbornou starostlivosťou a s ohľadom na citlivosť informácií počas dvoch rokov od skončenia auditu.

Kontrolný záznam a záverečná správa

- Sprava z auditu ma poskytnuť uplny, presny, stručny a jasny zaznam priebehu auditu a ma zahŕňať najmä:
  - Úvodnú časť
  - Nálezovú časť
  - Zhodnotenie auditu
  - Prílohy
  - Vyjadrenie PZS
  - Zoznam nedostatkov odstránených počas auditu



Záverečná správa o výsledkoch auditu kybernetickej bezpečnosti prevádzkovateľa základnej služby

[Klient XXX]

Vypracoval:
[Meno a priezvisko audítora]
[Audítorská spoločnosť]

Dátum odovzdania správy:	[DD.MM.RRRR
Verzia:	[1.0]
Počet strán:	[66]
Počet výtlačkov:	[X] ks + elektronické verzie
Výtlačok č. 1:	archív PZS
Výtlačok č. 2:	NBÚ
Elektronická kópia:	archív PZS
Elektronická kópia:	archív audítora
Elektronická kópia:	archív audítorskej spoločnosti
Elektronická kópia:	NBÚ

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Riadenie súladu a kontrolné činnosti (Blok II)
Kurz: Manažér kybernetickej bezpečnosti

Doc. Ing. Katarína Kampová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Katarina.Kampova@uniza.sk