NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Metodika auditu kybernetickej bezpečnosti

Štandard na výkon auditu kybernetickej bezpečnosti
v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Verzia	3.0
Dátum vydania	23. októbra 2023
Dátum účinnosti	1. novembra 2023
Právny stav ku dňu	1.septembra 2023
Záväzný pre	Certifikovaní audítori kybernetickej bezpečnosti
Prístupný pre	Verejnosť

Obsah

1 Úvod

1.1 Zoznam príloh

Príloha	Názov prílohy
Príloha č. 1	Vzor žiadosti o audit kybernetickej bezpečnosti
Príloha č. 2	Vzor poverenia na výkon auditu kybernetickej bezpečnosti
Príloha č. 3	Vzor vyjadrenia PZS ku auditnej správe
Príloha č. 4	Vzor záverečnej auditnej správy
Príloha č. 5	Matica vyspelosti komponentov bezpečnostnej architektúry

1.2 Normatívne odkazy

[1] Zákon č. 69/2018 Z. z o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „Zákon“)

[2] Vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z. ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby) (ďalej len „vyhláška č. 164/2018 Z. z.“)

[3] Vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z. ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov (ďalej len „vyhláška č. 165/2018 Z. z.“)

[4] Vyhláška Národného bezpečnostného úradu č. 362/2018 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.“)

[5] Vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti (ďalej len „vyhláška č. 493/2022 Z. z.“)

[6] Nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93

[7] Zákon č. 56/2018 Z. z. o posudzovaní zhody výrobku, sprístupňovaní určeného výrobku na trhu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

[8] STN EN ISO / IEC 27000:2023, Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000: 2018)

[9] STN ISO / IEC 27001:2023, Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Systémy manažérstva informačnej bezpečnosti. Požiadavky. (ISO/IEC 27001: 2022)

[10] STN EN ISO / IEC 27002:2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Riadenie informačnej bezpečnosti (ISO/IEC 27002: 2022)

[11] ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[12] ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

[13] ISO/IEC 27008:2019 Information technology — Security techniques — Guidelines for the assessment of information security controls

[14] STN/ EN ISO 19011: 2018 Návod na auditovanie systémov manažérstva

[15] ISO / IEC 27037 - Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence

[16] ISO/TR 15801:2017 Document management — Electronically stored information — Recommendations for trustworthiness and reliability

[17] ISO / IEC 17020, Conformity assessment — Requirements for the operation of various types of bodies performing inspection

[18] Guidelines on assessing DSP and OES compliance to the NISD security requirements, ENISA, 11/2018

[19] ITAF™: A Professional Practices Framework for IS Audit/ Assurance, 3rd Edition. ISACA

[20] COBIT5 (Control Objectives for Information and Related Technologies), ISACA

[21] ISO/IEC 18045:2008 Information technology — Security techniques — Methodology for IT security evaluation

[22] ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for it security — Part 1: Introduction and general model

[23] ISO/IEC 15408-2: Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components

[24] ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for it security — Part 3: Security assurance components

[25] ISO/IEC 15504-5:2012 Information technology — Process assessment — Part 5: An exemplar software life cycle process assessment model

[26] ISO/IEC TS 15504-10:2011 Information technology — Process assessment — Part 10: Safety extension

[27] NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security

[28] ISO/IEC TR 19791:2010 Information technology — Security techniques — Security assessment of operational systems

1.3 Definície a kľúčové pojmy

Pojem	Skratka	Výklad
	ISO	International Organization for Standardization
	NIST	National Institute of Standards and Technology
	ISA	International Society of Automation
	IEC	International Electrotechnical Commission
akreditačný orgán		autoritatívny orgán, ktorý vykonáva akreditáciu na základe právomoci, ktorú mu udelil štát
audit		systematický, nezávislý a zdokumentovaný proces získavania objektívnych dôkazov a ich objektívne vyhodnotenie, aby sa určila miera, v akej sa plnia kritériá auditu [ISO 19011: 2018, čl. 3.1]
audit kybernetickej bezpečnosti		overenie plnenia povinností podľa Zákona a posúdenie súladu 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.

Pojem	Skratka	Výklad
auditné nástroje		softvérové, alebo hardvérové automatizačné prostriedky a aplikácie, ktoré napomáhajú preskúmať, alebo vyhodnotiť aplikované bezpečnostné opatrenia extrahovaním a preskúmaním údajov relevantných pre audit
auditné odporúčanie		návrh audítora na zmiernenie rizika a/ alebo odstránenie zisteného nesúladu
auditný dôkaz		záznamy, konštatovania skutočnosti alebo ďalšie informácie, ktoré sa týkajú kritérií auditu a sú verifikovateľné [ISO 19011: 2018, čl. 3.9]
auditný návrh na zlepšenie		návrh audítora na zvýšenie úrovne bezpečnosti a/alebo zvýšenie efektívnosti prijatých opatrení nad rámec požiadaviek zákona/vyhlášky
auditný záver		výsledok auditu po zvážení cieľov auditu a všetkých zistení auditu [ISO 9000: 2015, čl. 3.13.10]
audítor kybernetickej bezpečnosti		orgán posudzovania súladu podľa osobitného predpisu, ktorý je certifikovaný ako orgán príslušný na posudzovanie súladu v oblasti kybernetickej bezpečnosti
audítorská spoločnosť		právnická osoba zabezpečujúca audit kybernetickej bezpečnosti prostredníctvom certifikovaného audítora kybernetickej bezpečnosti
audítorský tím		jedna osoba alebo viaceré osoby vykonávajúce audit, podporované v prípade potreby technickými expertmi; jeden audítor v audítorskom tíme je vedúcim audítorského tímu [ISO 19011: 2018, čl. 3.14]
certifikačný orgán	CAB	orgán ktorý vykonáva služby posudzovania zhody
efektívnosť		miera, v akej sa realizovali plánované činnosti a dosiahli plánované výsledky [ISO 19011: 2018, čl. 3.26]
harmonogram auditu		Viď „plán auditu“
kritériá auditu		súbor požiadaviek, oproti ktorým sa porovnávajú objektívne dôkazy (požiadavky môžu zahŕňať politiky, štandardy, postupy, pracovné inštrukcie, právne požiadavky, zmluvné záväzky a pod.) [ISO 19011: 2018, čl. 3.7]
objekt posudzovania		akýkoľvek konkrétny materiál, produkt, inštalácia, proces, systém, osobu alebo orgán, ktorých sa týka posudzovanie v rámci auditu; z dôvodov zjednodušenia sa v rámci tejto metodiky používa výraz „objekt posudzovania“ alebo „objekt posudzovania zhody“ ako spoločný odkaz na ktorúkoľvek z týchto zložiek.
plán auditu		opis činností a usporiadaní auditu [ISO 9000: 2015, čl. 3.13.6]
posudzovanie zhody		dokazovanie, že sa splnili určené požiadavky týkajúce sa produktu, procesu, systému, osoby alebo orgánu [ISO/IEC 17000: 2004 čl. 2.1]
požiadavka		potreba alebo očakávanie, ktoré sa určia, všeobecne sa predpokladajú alebo sú povinné; požiadavkami v kontexte auditu kybernetickej bezpečnosti sú požiadavky vykonávacích predpisov k Zákonu

Pojem	Skratka	Výklad
predmet auditu		rozsah a hranice auditu; predmet auditu zvyčajne obsahuje opis fyzických a virtuálnych prostredí, funkcií, organizačných jednotiek, činností a procesov, ako aj predpokladaného časového intervalu; virtuálne prostredie je miesto, kde PZS vykonáva prácu alebo poskytuje službu pomocou on-line nástrojov, ktoré umožňujú jednotlivcom vykonávať procesy bez ohľadu na fyzické umiestnenie a ktoré ako celok predstavujú základnú službu podľa Zákona.
prevádzkovateľ základnej služby	PZS	orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa § 3 písm. l) Zákona
proces		súbor vzájomne súvisiacich alebo vzájomne pôsobiacich činností, ktoré používajú vstupy na dodávanie zamýšľaných výsledkov [ISO 19011: 2018, čl. 3.24]
program auditu		usporiadanie pre súbor jedného, alebo viacerých auditov plánovaných na konkrétny časový úsek a zameraných na konkrétny cieľ [ISO 19011: 2018, čl. 3.4]
skúšanie (testovanie):		určenie jednej alebo viacerých charakteristík objektu posudzovania zhody podľa vopred definovaného postupu
technický expert		osoba, ktorá poskytuje audítorskému tímu špecifické poznatky alebo odborné vedomosti [ISO 19011: 2018, čl. 3.16]
Úrad		Národný bezpečnostný úrad
Ústredný orgán		Úrad, Ministerstvo dopravy a výstavby Slovenskej republiky, Ministerstvo financií Slovenskej republiky, Ministerstvo hospodárstva Slovenskej republiky, Ministerstvo obrany Slovenskej republiky, Ministerstvo vnútra Slovenskej republiky, Ministerstvo zdravotníctva Slovenskej republiky, Ministerstvo životného prostredia Slovenskej republiky, Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
vedúci audítor kybernetickej bezpečnosti		certifikovaný audítor kybernetickej bezpečnosti zodpovedný za výkon auditu, ktorý garantuje odbornosť a správnosť auditu a podpisuje záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti
zistenia auditu		výsledky hodnotenia zozbieraných dôkazov auditu v porovnaní s kritériami auditu; Zistenia auditu preukazujú súlad alebo nesúlad [ISO 19011: 2018, čl. 3.10]
súlad		splnenie požiadavky; požiadavkami v kontexte auditu kybernetickej bezpečnosti sú požiadavky vykonávacích predpisov k Zákonu [ISO 19011: 2018, čl. 3.20]
čiastočný súlad		čiastočné splnenie požiadavky; požiadavkami pokiaľ ide o audit kybernetickej bezpečnosti sú požiadavky vykonávacích predpisov k Zákonu; stav Čiastočný súlad je z pohľadu požiadaviek Zákona považovaný za nesúlad s jeho požiadavkami.
nesúlad		nesplnenie požiadavky; požiadavkami v kontexte auditu kybernetickej bezpečnosti sú požiadavky vykonávacích predpisov k Zákonu [ISO 19011: 2018, čl. 3.20]

1.4 Všeobecné zásady auditu kybernetickej bezpečnosti

Auditom kybernetickej bezpečnosti (ďalej len „audit“) sa určuje efektívnosť implementácie opatrení, vykonávania opatrení ako aj prípadne existujúce nedostatky implementovaných opatrení v prostredí PZS v oblasti informačno-komunikačných technológií (IKT) a v oblasti kybernetickej bezpečnosti v zmysle platnej regulácie a bezpečnostného rámca.

V rámci auditu sa dodržiavajú nasledujúce všeobecné zásady:

- Zásada etiky
- Prístup založený na dôkazoch
- Procesný prístup
- Prístup založený na riziku
- Zásada relevantnosti
- Zásada úplnosti a správnosti
- Zásada proporcionality a primeranej starostlivosti

1.4.1 Zásada etiky

Audítor kybernetickej bezpečnosti má vykonávať audit poctivo a zodpovedne, objektívnym a nezaujatým spôsobom. Pokiaľ je to možné, audítor má byť nezávislý od objektu posudzovania a má vo všetkých prípadoch konať spôsobom, ktorý vylúči tendenčnosť a konflikt záujmov. Primárnym a základným právom a zároveň primárnou a základnou povinnosťou audítora musí byť aj zachovanie mlčanlivosti.

1.4.2 Prístup založený na dôkazoch

V rámci auditu majú byť použité racionálne metódy, ktorých cieľom je v systematickom procese auditovania dosiahnuť spoľahlivé a reprodukovateľné závery auditu.

Keďže audit sa vykonáva počas stanoveného časového intervalu a s obmedzenými zdrojmi, auditný dôkaz sa zakladá na vzorkách dostupných informácií. Dôveryhodnosť záverov auditu je úzko spojená s použitím primeraného vzorkovania.

1.4.3 Procesný prístup

Výsledky auditu sa dosiahnu efektívnejšie, ak audítor pochopí procesy PZS a ich celkové vzájomné pôsobenie ako súvisiacich činností, ktoré sú vykonávané ako kompaktný, holistický systém. Vlastnosti systému nemožno určiť len pomocou popisu vlastností jeho častí. Naopak celok ovplyvňuje podobu a fungovanie jeho jednotlivých častí.

1.4.4 Prístup založený na riziku

Audit má byť zameraný na skutočnosti významné pre auditovaného PZS a na dosiahnutie cieľov programu auditu, berúc do úvahy identifikované riziká a opatrenia primerané rizikám.

1.4.5 Zásada relevantnosti

Audítor musí vedieť preukázať, že získané dôkazy sú relevantné pre audit - t. j. že obsahujú informácie, ktoré majú význam pre posúdenie a že existuje dobrý dôvod, prečo boli získané. (Relevantnosť je vlastnosť dôkazného prostriedku, keď tento má poslúžiť na preukázanie alebo vyvrátenie časti konkrétnej informácie).

1.4.6 Zásada úplnosti a správnosti

Audítor je zodpovedný za to, že všetky dôkazy, ktoré získa a používa počas auditu sú správne a úplne. Všetky získané auditné dôkazy musia byť uchované po dobu najmenej **dva roky** od skončenia auditu.

1.4.7 Zásada proporcionality a primeranej starostlivosti

Zásada proporcionality upravuje, ako má audítor vykonávať svoje právomoci. Podľa zásady proporcionality platí, že audítor vykoná na dosiahnutie cieľov auditu kroky len v takom rozsahu, ktoré sú nevyhnutné na dosiahnutie daného cieľa.

Audítor v rámci auditu zároveň vykonáva iba také úkony, ktoré nevedú k znehodnoteniu dôkazov či už jeho úmyselným alebo neúmyselným konaním. Na základe úmyselného či neúmyselného konania,

napríklad audítorovi nie je dovolené pristupovať k takým zariadeniam, na obsluhu ktorých nemá potrebné spôsobilosti a nie je pripravený využiť spoľahlivé a overené postupy.

1.4.8 Zásada opakovateľnosti a reprodukovateľnosti

Všetky postupy používané pri manipulácii s auditnými dôkazmi by mali byť opakovateľné (Opakovateľnosť je vlastnosť procesu vykonaného s cieľom získať rovnaké výsledky testov v rovnakom testovacom prostredí – t.j. rovnaký počítač, pevný disk, režim prevádzky atď.).

Výsledky postupov by mali byť zároveň reprodukovateľné. (Reprodukovateľnosť je vlastnosť procesu získať rovnaké výsledky testov v inom testovacom prostredí - t.j. iný počítač, pevný disk, operátor atď.).

1.5 Metódy výkonu auditu kybernetickej bezpečnosti

Audit sa môže vykonať využitím rôznych metód. Zvolené metódy auditu závisia od definovaných cieľov, od predmetu a kritérií auditu a aj od jeho trvania a miesta. Cieľom auditu je overiť dizajn, nasadenie a spôsob vykonávania (prevádzkovú účinnosť) bezpečnostných opatrení u prevádzkovateľa základnej služby.

Je potrebné zamedziť možným nepresnostiam auditných zistení vyplývajúcich zo zvolených metód auditu. Kombinácia rôznych metód auditu môže zvýšiť efektívnosť procesu auditu.

V tabuľke sú uvedené príklady metód auditu, ktoré sa môžu použiť samostatne alebo vo vzájomnej kombinácii na dosiahnutie cieľov auditu.

Rozsah zapojenia audítora a PZS	**Spôsob výkonu činností audítora**	
	Na mieste	**Na diaľku**
Osobná vzájomná súčinnosť	• Vykonanie rozhovorov • Doplnenie kontrolných záznamov a dotazníkov za spoluúčasti PZS • Vykonanie preskúmania objektu posúdenia za spoluúčasti PZS • Vzorkovanie	• Cez interaktívne komunikačné prostriedky: – vykonanie rozhovorov; – pozorovanie vykonávania práce s diaľkovým navádzaním; – doplnenie kontrolných záznamov a dotazníkov; – vykonanie preskúmania objektu posúdenia za spoluúčasti PZS
Bez osobnej vzájomnej súčinnosti	• Vykonanie preskúmania objektu posúdenia (napr. záznamy a analýza údajov). Pozorovanie vykonania práce. • Vykonanie návštevy na mieste. Doplnenie kontrolného zoznamu. Vzorkovanie (napr. produktov)	• Vykonanie preskúmania objektu posúdenia • Pozorovanie výkonu práce pomocou prostriedkov dohľadu, • Posúdenie predpisov a regulačných požiadaviek. • Analýza údajov

Činnosti auditu na mieste sa vykonávajú v sídle auditovaného PZS. Činnosti auditu na diaľku sa vykonávajú na ktoromkoľvek inom mieste než je sídlo auditovaného PZS.

Činnosti auditu **pri osobnej vzájomnej súčinnosti** zahŕňajú vzťah medzi pracovníkmi auditovaného PZS a audítorským tímom. Činnosti auditu **bez osobnej vzájomnej súčinnosti** nezahŕňajú žiadnu osobnú vzájomnú súčinnosť s osobami zastupujúcimi auditovaného PZS, avšak zahŕňajú vzájomnú súčinnosť so zariadeniami, s vybavením a dokumentáciou.

Vykonateľnosť činností auditu na diaľku závisí od niekoľkých faktorov (napr. od úrovne rizika na dosiahnutie cieľov auditu, od úrovne dôvery medzi audítorom a pracovníkmi auditovaného PZS a od regulačných požiadaviek).

Na úrovni programu auditu sa má zaistiť vhodné a vyvážené použitie aplikácie metód auditu, či už na diaľku, alebo na mieste tak, aby sa zaistilo uspokojivé dosiahnutie cieľov programu auditu.

2 Určenie rozsahu trvania auditu kybernetickej bezpečnosti

Rozsah trvania auditu sa vypočíta na základe kritérií uvedených v prílohe č. 2 k vyhláške č. 493/2022 Z. z. [5]

Určenie rozsahu trvania auditu audítor spracuje na základe informácií, ktoré získal zo žiadosti o vykonanie auditu. Minimálne náležitosti žiadosti o vykonanie auditu sú uvedené v prílohe č. 1 vyhlášky č. 493/2022 Z. z. [5].

Audítor určuje časový rozsah trvania auditu tak, že je dostatočný na posúdenie plnenia povinností podľa Zákona a účinnosti prijatých bezpečnostných opatrení a ich stav hodnotí formou vzorkovania, pričom rozsah vzoriek určuje s ohľadom na vykonanú klasifikáciu informácií a kategorizáciu sietí a informačných systémov, vykonanú analýzu rizík kybernetickej bezpečnosti a na vypovedaciu schopnosť auditu.

Súčasťou určenia rozsahu trvania auditu je aj výber metód auditu, voľba postupov, výber nástrojov potrebných pre audit a výber kritérií pre vyhodnotenie auditných dôkazov.

Ak je audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby vykonávaný v zmysle § 29 ods. 6 Zákona s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených Zákonom na základe požiadania Úradu, je rozsah trvania auditu určený na základe informácií poskytnutých PZS pri prvom stretnutí, prípadne na základe informácií Úradu.

Žiadosť o výkon auditu podľa § 29 ods. 6 Zákona musí byť podpísaná štatutárnym orgánom Úradu alebo ním poverenou osobou.

3 Plán auditu

3.1 Auditný program

Generickým cieľom auditu kybernetickej bezpečnosti je overiť plnenie povinností podľa Zákona a posúdiť súlad 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 nesúlady s požiadavkami Zákona a súvisiacich osobitných predpisov pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby s cieľom prijať opatrenia na ich odstránenie a nápravu a na predchádzanie kybernetickým bezpečnostným incidentom.

3.2 Určenie zdrojov programu auditu

Pri určovaní zdrojov programu auditu audítor kybernetickej bezpečnosti, ktorý riadi program auditu, má zvažovať najmä:

a) finančné a časové zdroje nevyhnutné na prípravu, riadenie a zlepšovanie auditu,

b) metódy auditu,

c) individuálnu a celkovú dostupnosť iných audítorov a technických expertov, ktorí majú vhodné kompetencie na určité čiastkové ciele programu auditu,

d) rozsah programu auditu, riziká a príležitosti programu auditu,

e) čas a náklady na cestu, ubytovanie a ďalšie potreby auditovania,

f) vplyv rozdielnych časových pásem v prípade, že klient auditu prevádzkuje geograficky vzdialené služby a lokácie,

g) dostupnosť technológií podporujúcich vzdialenú spoluprácu pri audite na diaľku (napr. cloudové

riešenia, telekonferenčné systémy, atď.),

h) dostupnosť akýchkoľvek požadovaných nástrojov, zariadení a technológií potrebných pre výkon auditu,

i) dostupnosť nevyhnutných zdokumentovaných informácií určených v priebehu tvorby programu auditu,

j) požiadavky týkajúce sa bezpečnostných previerok, zabezpečovacích zariadení, a kryptografických mechanizmov.

3.3 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.

3.4 Poverenie výkonom auditu

Ak je audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby vykonávaný v zmysle § 29 ods. 6) Zákona s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených Zákonom na základe požiadania Úradu, poverenie vystavuje Úrad, alebo Úradom oslovená audítorská spoločnosť.

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.

3.5 Ustanovenia pre plán auditu vykonávanom v zmysle § 29 ods. 6 Zákona

Ak je audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby vykonávaný v zmysle § 29 ods. 6 Zákona s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených Zákonom na základe žiadosti Úradu, Úrad poskytne kontaktné údaje zástupcu PZS audítorovi.

Audítor kontaktuje PZS a postupuje v súlade s vyššie uvedenými bodmi.

V prípade, že PZS do 7 pracovných dní od doručenia žiadosti audítora nezareaguje na audítorove požiadavky alebo neposkytne požadovanú súčinnosť, audítor je povinný bezodkladne informovať Úrad o vzniknutej situácii.

4 Priebeh auditu kybernetickej bezpečnosti

4.1 Otváracie stretnutie

Otváracie stretnutie môže byť vykonané až po podpise poverenia audítora výkonom auditu. Termín otváracieho stretnutia a účasť na stretnutí dohodne s príslušnými osobami vedúci audítor.

Účelom otváracieho stretnutia je:

a) potvrdenie dohody všetkých strán (auditovaného PZS a audítorského tímu) s plánom auditu;

b) predstavenie audítorského tímu a rolí členov tímu;

c) uistenie, že všetky plánované činnosti auditu môžu byť vykonané.

Otváracie stretnutie sa má realizovať s manažmentom PZS alebo, ak treba, za prítomnosti tých, ktorí zodpovedajú za základné služby, ktoré majú byť predmetom auditu. Stupeň detailu sa má zhodovať so zvyklosťami procesu auditu auditovaného PZS.

Prvé stretnutie má viesť certifikovaný audítor kybernetickej bezpečnosti. V prípade, že audit je vykonávaný tímom audítorov, vedúci audítorského tímu musí byť certifikovaný audítor kybernetickej bezpečnosti.

Podľa potreby sa má vziať do úvahy overenie:

- cieľov, predmetu a kritérií auditu;
- plánu auditu a ďalších súvisiacich opatrení s auditovaným PZS, napr. dátum a čas záverečného stretnutia, akékoľvek priebežné stretnutia audítorského tímu s manažmentom auditovanej organizácie a akékoľvek potrebné zmeny;
- oficiálnych komunikačných kanálov medzi audítorským tímom a auditovanou organizáciou;
- jazyka, ktorý sa bude používať v priebehu auditu;
- spôsobu podávania informácií o postupe a priebehu auditu v auditovanej organizácii;
- dostupnosti potrebných zdrojov a zariadení audítorskému tímu;
- skutočností súvisiacich s dôverou a informačnou bezpečnosťou;

4.2 Získanie a overenie informácií

Počas auditu pomocou vzorkovania sa majú zhromažďovať a overovať použiteľné informácie týkajúce sa cieľov, predmetu a kritérií auditu vrátane informácií súvisiacich s rozhraním medzi funkciami, činnosťami a procesmi.

Ako dôkaz auditu sa môžu **akceptovať iba tie informácie, ktoré sa dajú overiť**. Ak použiteľná miera overenia nie je dostatočná, audítor má použiť vlastný profesijný úsudok.

Zaznamenať sa má každý dôkaz auditu, ktorý vedie k zisteniu. Ak sa v priebehu zhromažďovania objektívnych dôkazov vyskytnú akékoľvek nové alebo zmenené skutočnosti, riziká alebo príležitostí (t. j. nové zistenia), je potrebné aj pre tieto posúdiť, aký majú vplyv na súlad, alebo nesúlad.

Metódy zhromažďovania informácií zahŕňajú najmä:

- rozhovory;
- pozorovania;
- dotazníky,
- preskúmania zdokumentovaných informácií

Ak sa informácie zhromaždili iným spôsobom, ako je uvedené vyššie (napr. rozdielnymi jednotlivcami, alternatívnymi médiami), úplnosť dôkazu sa má posúdiť aj dodatočne.

Zhromažďovanie informácií pri audite sa uskutočňuje výhradne bez zásahu audítora do auditovaného informačného systému alebo siete. Požadované informácie je povinný dodať zodpovedný zamestnanec PZS s výmenou cez predom dohodnutý kanál.

Činnosti priamo ovplyvňujúce činnosť auditovaného informačného systému alebo siete ako napríklad výkon penetračných testov, výkonnostných testov a podobne, je zakázané vykonávať pri audite.

V prípade, že je dostupná správa z predchádzajúceho auditu kybernetickej bezpečnosti PZS alebo z iných relevantných auditov, v ktorých sú overené niektoré z požiadaviek Zákona, audítor môže po overení aktuálnosti a platnosti informácií uvedených v tejto správe, využiť túto správu ako zdroj informácií a uvedie ju v zozname dôkazov.

Vzorkovanie pri audite sa vykonáva vtedy, ak nie je praktické alebo efektívne preverenie všetkých dostupných informácií v priebehu auditu, napr. záznamy sú príliš početné alebo príliš rozptýlené na posúdenie každej položky v základnom súbore. Vzorkovanie pri audite veľkého súboru je proces výberu menej ako 100 % položiek z celkového dostupného dátového súboru (základného súboru) na získanie a vyhodnotenie dôkazov o nejakej vlastnosti základného súboru s cieľom formulácie záverov týkajúcich sa základného súboru.

Cieľom výberu vzorky je poskytnúť informácie audítorovi, aby získal istotu, že ciele auditu môžu byť alebo budú dosiahnuté. Výber vzorky je zodpovednosťou audítora a môže byť vykonaný na základe posúdenia jestvujúceho opatrenia.

Výber vzorky obyčajne zahŕňa tieto kroky:

a) vypracovanie cieľov odberu vzorky

b) výber rozsahu a zloženia základného súboru, z ktorého sa vzorka odoberie

c) výber metódy odberu vzorky

d) určenie veľkosti vzorky

e) vykonanie odberu vzorky

f) zostavovanie, vyhodnocovanie, vykazovanie a zdokumentovanie výsledkov

Pri odbere vzorky sa má zvažovať kvalita dostupných údajov. Ak je odber vzorky nedostatočný a nepresný, údaje nezaručia relevantné zistenia. Výber vhodnej vzorky sa má zakladať tak na výbere metódy odberu vzorky, ako aj na type požadovaných údajov, napr. na odvodení konkrétnych vzorov správania alebo na vyvodení záverov v rámci základného súboru.

Podávanie správ o vybratej vzorke by malo vziať do úvahy veľkosť vzorky, metódu výberu, odhady vykonané na základe vyhodnotenia vzorky.

Ak audítor na základe získanej vzorky identifikuje nesúlad, resp. nedostatočnú účinnosť opatrenia, alebo nejestvujúce, alebo neefektívne dodatočné opatrenie, je na jeho rozhodnutí, či bude skúmať novú vzorku, alebo uzatvorí danú požiadavku ako nesúlad.

Audítor môže pri uchovávaní dôkazov využiť hashovací nástroj na zabezpečenie integrity poskytnutých dôkazov. V tom prípade je súčasťou zoznamu príslušných dôkazov, ktorý je uvedený v Správe z auditu, aj príslušný hash jednotlivých dôkazov.

4.3 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 § 17, § 18, § 20, § 24a, § 27 a § 29,
- 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.

4.4 Komponenty bezpečnostnej architektúry

Audítori majú zvažovať, či získané a verifikované informácie poskytujú dostatočné objektívne dôkazy na preukázanie, že sú plnené kritériá auditu.

Bezpečnostné opatrenia podľa § 20 Zákona sú typickými komponentami na jednotlivých vrstvách bezpečnostnej architektúry. S cieľom **objektivizovať tvorbu zistení, ak to špecifikuje plán auditu**, môže audítor vyhodnocovať jednotlivé kritériá auditu v kontexte príslušného komponentu bezpečnostnej architektúry.

4.4.1 Posudzované komponenty

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

Na vyhnutie sa zovšeobecneniu a dosiahnutie vyššieho detailu a objektivizácie rozhodnutia o súlade, čiastočnom súlade, alebo nesúlade môže audítor identifikovať aj úroveň vyspelosti príslušného hodnoteného komponentu. Jednotlivé komponenty môžu typicky nadobúdať hodnoty vyspelosti podľa modelu reprezentácie CMMI (z angl. Capability Maturity Model Integration).

V tomto modeli sú úrovne vyspelosti dosiahnutých bezpečnostných cieľov alebo úrovne bezpečnostných opatrení hodnotené v 5-hodnotovej stupnici nasledovne podľa tabuľky 4.4.2.

4.4.2 Úrovne vyspelosti

#	Úroveň slovne	Výklad
0	„absentujúci“	bezpečnostný cieľ nie je splnený, alebo neexistuje dôkaz o dostatočnej vyspelosti procesu alebo opatrenia (typicky sa v hodnotení neuvádza).
1	„počiatočný“	cieľ je dosahovaný (opatrenie je aplikované) ad-hoc, intuitívne, bez vopred stanovených aktivít a procedúr, závislý na individuálnom prístupe a na konkrétnych osobách ktoré disponujú expertízou v danej oblasti.
2	„opakovateľný“	cieľ je ustanovený (opatrenie implementované), výkon prebieha väčšinou rovnakým spôsobom, informácie sú prístupné celému tímu. Sú prítomné isté známky plánovania, procesná disciplína sa opiera o predchádzajúce výsledky, chýba dokumentácia, metrika a optimalizácia.
3	„formalizovaný“	cieľ je ustanovený (opatrenie implementované), prebieha rovnakým spôsobom, prístup k vykonávaniu procesu (uplatneniu opatrenia) je zdokumentovaný a štandardizovaný. Skúsenosti sa v tíme navzájom distribuujú, organizácia má prehľad o vstupoch a výstupoch procesu, proces je integrovaný do ostatných procesov, chýba však metrika a optimalizácia.
4	„riadený“	cieľ (opatrenie) sú plne riadené, obsahujú potrebné formálne prvky. O výkone sú zbierané dáta, meraná je účinnosť a produktivita, výstupy sú systematicky kvantitatívne a kvalitatívne vyhodnocované.
5	„optimalizovaný“	cieľ (opatrenie) sú plne riadené, obsahujú potrebné formálne prvky, meraná je účinnosť a produktivita. V organizácii funguje mechanizmus neustálej optimalizácie voči jasne definovaným a dosiahnuteľným úrovniam, na základe spätnej väzby.

V Prílohe č. 5 tejto metodiky je uvedený príklad hodnotenia vyspelosti jednotlivých komponentov bezpečnostnej architektúry.

4.5 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 plnené a audítor neidentifikoval riziko
ČIASTOČNÝ SÚLAD	ak je kritérium auditu plnené iba čiastočne
NESÚLAD	ak kritérium auditu nie je plnené, alebo ak audítor identifikoval riziko súvisiace s daným kritériom

Ak to špecifikuje plán auditu, jednotlivé zistenia auditu môžu zahŕňať okrem určenia súladu aj dobrú prax spolu s podpornými dôkazmi, návrhmi na zlepšenie a akékoľvek odporúčania pre prevádzkovateľa základnej služby.

V prípade, že kritérium auditu nie je relevantné pre PZS alebo jeho prostredie, audítor vyhodnotí príslušnú požiadavku v kontrolnom zázname ako „NEAPLIKOVATEĽNÉ“ (napr. v § 7 ods. 1 písm. h) vyhlášky č. 362/2018 Z. z., ak PZS nevykonáva žiadne činnosti s informáciami pre vojenské spravodajstvo, je stav súladu označený ako „NEAPLIKOVATEĽNÉ“).

4.6 Ustanovenia pre priebeh auditu vykonávanom v zmysle § 29 ods. 6 Zákona

V prípade, že PZS do 7 pracovných dní od doručenia žiadosti audítora nezareaguje na audítorove požiadavky alebo neposkytne očakávanú súčinnosť, audítor je povinný v čo najkratšom čase informovať Úrad o vzniknutej situácii.

5 Ukončenie auditu

5.1 Určovanie záverov auditu

Závery auditu majú obsahovať nasledujúce náležitosti:

a) počty súladov, čiastočných súladov a nesúladov s kritériami auditu vrátane efektívnosti implementovaných opatrení v plnení zamýšľaných bezpečnostných cieľov,

b) identifikácia rizík a primeranosti implementovaných opatrení na zvládanie rizík pre jednotlivé kritéria auditu;

c) dosiahnutie cieľov auditu, pokrytie predmetu auditu a splnenie kritérií auditu;

d) podobné zistenia z rôznych oblastí, ktoré sa auditovali, alebo zo spoločného auditu alebo z predchádzajúceho auditu za účelom identifikácie trendov

e) odporúčania a prípadne návrhy na zlepšenie za jednotlivé oblasti, ktoré boli relevantné pre audit.

5.2 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.

Správa z auditu má poskytnúť úplný, presný, stručný a jasný záznam priebehu auditu a má zahŕňať

najmä:

- Úvodnú časť
- Nálezovú časť
- Zhodnotenie auditu
- Prílohy
- Vyjadrenie PZS
- Zoznam nedostatkov odstránených počas auditu

5.2.1 Úvodná časť

Úvodná časť správy z auditu obsahuje:

a) meno, priezvisko, číslo platného certifikátu audítora, dátum vyhotovenia a jeho podpis,

b) vymedzenie rozsahu vykonaného auditu, identifikáciu organizácie (auditovaného PZS), auditovaných základných služieb

c) cieľ auditu,

d) dátumy a miesta, kde sa vykonávali činnosti auditu

e) referencie na použité metódy auditu

f) identifikáciu audítorského tímu a účastníkov z auditovaného PZS pri audite

5.2.2 Nálezová časť

Nálezová časť správy z auditu (kontrolný záznam) obsahuje:

a) zhrnutie zistení výsledkov auditu a konštatovanie súladu alebo nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov, pre súbor požiadaviek na bezpečnosť sietí a informačných systémov podľa Zákona a jeho vykonávacích predpisov a osobitných predpisov

b) zistenia auditu pre jednotlivé požiadavky na bezpečnosť sietí a informačných systémov, vrátane odkazu na získané auditné dôkazy podporujúce uvedené zistenia,

c) odporúčané nápravné opatrenia audítora pri zistení nedostatkov,

V samostatnom zozname je možné uviesť vybrané stavy nesúladu a závažné auditné zistenia.

Pri spoločných požiadavkách na prevádzkovateľa základnej služby sa vyplní spoločný kontrolný záznam za všetky informačné systémy relevantné pre audit. Bezpečnostné opatrenia, ktoré sú odlišné pre jednotlivé auditované základné služby, sa vyplnia samostatne.

Vzor nálezovej časti správy z auditu (kontrolný záznam) s návrhom typických opatrení je z hľadiska dôvernosti klasifikovaný stupňom „Interné“. Prístupný je pre:

- Úrad,
- Certifikačný orgán
- Certifikovaných audítorov kybernetickej bezpečnosti.

Na sprístupnenie kontrolného záznamu tretím stranám je potrebné schválenie zo strany vlastníka informácie.

5.2.3 Zhodnotenie auditu

Zhodnotenie plnenia povinností podľa Zákona a celkového stavu prijatých bezpečnostných opatrení každého informačného systému súvisiaceho so základnou službou, vyslovenie súladu, čiastočného súladu, alebo nesúladu s jednotlivými požiadavkami na bezpečnosť sietí a informačných systémov a konkrétne uvedenie nedostatkov, informáciu o stave vykonaných nápravných opatrení, ak prevádzkovateľ základnej služby na základe predchádzajúceho auditu mal tieto nápravné opatrenia prijať.

Podľa potreby môže správa z auditu v časti zhodnotenie zahŕňať alebo odkazovať aj na:

- akékoľvek neauditované oblasti uvedené v predmete auditu vrátane záležitostí spojených s

nedostupnosťou dôkazov, zdrojov alebo dôvernosťou, a to aj so súvisiacimi zdôvodneniami,

- identifikovanú dobrú prax,
- schválené plány následných opatrení, ak nejaké sú,
- vyjadrenie o dôvernosti obsahu,
- akékoľvek nevyriešené rozporné názory medzi audítorským tímom a auditovaným PZS
- akékoľvek dôsledky pre program auditu alebo nasledujúce audity.

5.2.4 Prílohy

Prílohy správy z auditu vo forme dokumentov, najmä:

1. kópia certifikátu audítora,
2. kópia formálnej časti žiadosti o vykonanie auditu,
3. výpočet rozsahu trvania auditu a zdôvodnenie jeho skrátenia alebo predĺženia,
4. schválený harmonogram auditu,
5. zoznam posúdenej dokumentácie,
6. uvedenie a zdôvodnenie zmien a rozdielov priebehu auditu oproti plánovanému harmonogramu,
7. vyjadrenie prevádzkovateľa základnej služby ku správe z auditu a zisteniam auditu.

Povinnou súčasťou správy auditu je **vyhlásenie audítora**. Text vyhlásenia je súčasťou Prílohy č. 3 tejto metodiky.

5.2.5 Nedostatky odstránené počas auditu

Audítor oboznamuje zodpovedného pracovníka prevádzkovateľa základnej služby so zistenými nedostatkami počas celého priebehu auditu a zároveň dokumentuje odporúčané opatrenia na odstránenie nedostatkov.

Ak sú všetky zistené nedostatky odstránené do dohodnutého času pred spracovaním záverečnej správy o výsledkoch auditu, je možné v tejto záverečnej správe o výsledkoch auditu konštatovať súlad s požiadavkami na bezpečnosť sietí a informačných systémov.

5.2.6 Vyjadrenie PZS

Po ukončení auditných stretnutí audítor pripraví draft správy, ktorú poskytne na vyjadrenie zástupcovi prevádzkovateľa základnej služby. Dátum odovzdania draftu správy by mal byť stanovený a odsúhlasený oboma stranami (či už v zmluve alebo na úvodnom stretnutí).

Prevádzkovateľ základnej služby má právo vyjadriť sa k správe z auditu a toto vyjadrenie sa vkladá do správy. Vyjadrenie prevádzkovateľa základnej služby sa vydáva len v jednej iterácii.

Akékoľvek rozporné názory týkajúce sa zistení alebo záverov auditu medzi audítorským tímom a PZS je nutné prediskutovať a ak je to možné vyriešiť. Ak to nie je možné vyriešiť PZS má právo uviesť svoj názor, spolu so zdôvodnením nesúhlasu, priamo vo vyššie uvedenom vyjadrení.

Prevádzkovateľ základnej služby sa môže vzdať vyjadrenia ku správe auditu, v takom prípade audítor uvedie túto skutočnosť v časti Zhodnotenie auditu.

V prípade, že PZS nezašle vyjadrenie v termíne do 7 pracovných dní od odovzdania draftu správy, audítor má právo vytvoriť finálnu verziu správy z auditu, kde v časti Zhodnotenie auditu uvedie túto skutočnosť.

Po doručení formálneho vyjadrenia PZS, audítor pripraví finálnu verziu správy, ktorú následne odovzdá PZS vo formáte a počte dohodnutom s PZS. Po dohode s PZS môže byť dátum vydania finálnej verzie správy rovnaký ako dátum záverečného stretnutia.

Dátum vydania finálnej verzie správy je považovaný za dátum ukončenia auditu.

Súčasťou finálnej správy o výsledkoch auditu, ktorú je PZS povinný odovzdať Úradu v súlade s požiadavkami Zákona, sú pri zistení nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov aj príslušné nápravné opatrenia na zabezpečenie požadovaného súladu s požiadavkami na bezpečnosť sietí a informačných systémov a termín ich vykonania zo strany PZS.

Ak má PZS pripravené tieto opatrenia pred vypracovaním finálnej verzie správy z auditu, audítor tieto opatrenia uvedie priamo v správe. Ak určenie týchto nápravných opatrení zo strany PZS vyžaduje viacej času, audítor uvedie v správe v časti Nápravné opatrenia, že PZS je povinný priložiť k auditnej správe zoznam prijatých nápravných opatrení a tento zoznam tvorí prílohu auditnej správy.

5.3 Záverečné stretnutie

Záverečné stretnutie („Kick-out meeting“) je voliteľná súčasť výkonu auditu, ak sa v pláne auditu na ňom dohodne audítor a PZS. Primárnym cieľom tohto stretnutia má byť prezentácia zistení a záverov auditu a prípadné odovzdanie finálnej verzie správy.

Záverečnému stretnutiu má predsedať certifikovaný audítor, vedúci audítorského tímu za prítomnosti manažmentu PZS, a ak je potrebné, aj za prítomnosti

- pracovníkov zodpovedných za funkcie alebo procesy, ktoré boli predmetom auditu;
- ďalších členov audítorského tímu;
- ďalších relevantných zainteresovaných strán určených klientom auditu alebo auditovaným PZS.

Vedúci audítorského tímu má oboznámiť auditovaného PZS so situáciami vzniknutými v priebehu auditu, ktoré by mohli viesť k zníženiu dôveryhodnosti záverov auditu.

Ak je to potrebné, pri záverečnom stretnutí sa auditovanému PZS má vysvetliť

a) informácia, že zhromažďovanie dôkazov auditu sa založilo na vzorke dostupných informácií a nevyhnutne nepredstavuje celkovú efektívnosť procesov auditovaného PZS,
b) metóda podávania správy,
c) že zistenie auditu sa zvládlo na základe odsúhlaseného a Zákonom stanoveného procesu,
d) možné následky neprimerane zvládnutých zistení auditu,
e) prezentácia zistení a záverov auditu takým spôsobom, aby ich pochopil manažment PZS,
f) akékoľvek súvisiace následné činnosti po audite (napr. implementácia a preskúmanie nápravných opatrení, zvládnutie sťažností auditu, procesu odvolania).

5.4 Distribúcia správy z auditu

Správu z auditu má audítor distribuovať vopred dohodnutým a odsúhlaseným spôsobom relevantným zainteresovaným stranám definovaným v programe auditu, v pláne auditu alebo v zmluve/objednávke, najneskôr do 3 dní od vydania finálnej správy z auditu.

Záverečnú správu o výsledkoch auditu je povinný úradu predložiť PZS do 30 dní od ukončenia auditu spolu so zoznamom prijatých nápravných opatrení a termínom ich splnenia.

Pri distribúcii správy z auditu musia byť prijaté primerané opatrenia na zaistenie dôvernosti správy. Rozpracované verzie správy a finálna správa z auditu je z hľadiska dôvernosti klasifikovaný stupňom „Interné“. Prístupný je pre:

- Úrad,
- Certifikačný orgán,
- Certifikovaných audítorov kybernetickej bezpečnosti, ktorí vypracovali danú správu,
- Členov audítorského tímu
- Štatutárny orgán PZS a ním poverené osoby

Odovzdaním finálnej verzie prechádza vlastníctvo informácie z vedúceho audítora na štatutára PZS.

Na sprístupnenie kontrolného záznamu tretím stranám je potrebné schválenie zo strany vlastníka informácie.

5.5 Sprístupnenie správy z auditu

5.5.1 Povinnosti audítora sprístupňovať záverečnú správy

Audítor KB nie je povinnou osobou v zmysle § 2 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (zákon o slobode informácií).

Audítor KB je voči PZS viazaný povinnosťou mlčanlivosti v zmysle § 12 Zákona.

Audítor KB nie je povinný sprístupniť záverečnú správu ani v prípade, keby mu na to PZS dal súhlas (t. j. zbavil ho mlčanlivosti).

5.5.2 Povinnosti PZS sprístupňovať záverečnú správy

Pre PZS v súvislosti so sprístupňovaním správ auditu na základe dožiadania podľa zákona o slobode informácií platí:

- PZS je povinný záverečnú správu sprístupniť, iba v prípade, že je povinnou osobou v zmysle § 2 zákona o slobode informácií
- PZS môže sprístupnenie záverečnej správy odmietnuť, ak:
  - sprístupnenie by to bolo v rozpore s právne záväznými aktmi Európskych spoločenstiev a Európskej únie alebo s medzinárodnou zmluvou, ktorou je Slovenská republika viazaná,
  - záverečná správa sa týka výkonu kontroly, dohľadu alebo dozoru orgánom verejnej moci podľa osobitných predpisov (t. j. napríklad auditu nariadeného Úradom podľa § 29 ods. 5 Zákona)
  - ide o dokumentáciu, ktorá obsahuje informácie, ktorých zverejnenie by sa mohlo použiť spôsobiť narušenie objektov osobitnej dôležitosti a ďalších dôležitých objektov podľa osobitných predpisov, najmä podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre znení neskorších predpisov.

5.6 Ustanovenia pre ukončenie auditu vykonávanom v zmysle § 29 ods. 6 Zákona

V prípade, že PZS do 7 pracovných dní nezareaguje na audítorove požiadavky alebo neposkytne očakávanú súčinnosť, audítor je povinný v čo najkratšom čase informovať Úrad o vzniknutej situácii.

Záverečnú správu v prípade auditov nariadených podľa § 29 ods. 6 Zákona Úradom audítor zasiela Úradu.

Príloha č. 1 Vzor žiadosti o audit kybernetickej bezpečnosti

PZS hlavička, adresa sídla

Pre:
[Meno a priezvisko vedúceho certifikovaného audítora] Certifikovaný audítor kybernetickej bezpečnosti

Vec:
Žiadosť o audit kybernetickej bezpečnosti

Vážený audítor,

Zasielame Vám formálnu žiadosť na výkon auditu kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej ako „Zákon“) v súlade s prílohou č. 2 k vyhláške Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.

1. Identifikácia prevádzkovateľa základnej služby:
2. Identifikácia základných služieb

Prevádzkovateľ základnej služby (obchodné meno, IČO, sídlo)	**Klient XXX** IČO: XX XXX XXX Ulica, PSČ Mesto
Meno štatutárneho zástupcu	
Základná/é služba/y	
	Základná služba č. 1
	Základná služba č. 2
	Základná služba č. 3
Sektor	Sektor podľa Zákona
Podsektor	Podsektor podľa Zákona

Príloha č. X: Oznámenie podľa § 17 ods. 1 Zákona

3. Počet zamestnancov prevádzkovateľa základnej služby

XXX

4. Zoznam informačných systémov a ich klasifikácia s väzbou na základnú službu

Príloha č. X: Zoznam aktív, zoznam informačných systémov

a. identifikácia organizačných útvarov prevádzkovateľa základnej služby 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,

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,

Príloha č. X: Zoznam aktív, zoznam informačných systémov Príloha č. X: Bezpečnostná dokumentácia

c. počet užívateľov základnej služby, teritoriálne rozloženie a dôsledky pri výpadku základnej služby na jej užívateľov,

XXX používateľov naprieč celým Slovenskom

d. systém správy; interné a externé zdroje, identifikácia kľúčových dodávateľov a zmlúv a dohôd o úrovni poskytovaných služieb,

Informačné systémy, ktoré za zúčastňujú na realizácii základnej služby, zabezpečujeme interne. Dodávateľsky zabezpečujeme:
XXX, firma....

e. schéma sieťovej architektúry s uvedením miest prepojení sietí a pripojenia voči externým sieťam,

Príloha č. X: Schéma sieťovej architektúry

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,

Máme/nemáme

g. organizačné útvary a počty zamestnancov prevádzkujúcich informačné systémy a siete vrátane počtu dodávateľov; pri prítomnosti zamestnancov dodávateľa na pracovisku prevádzkovateľa počas auditu sa lokality dodávateľov nezapočítavajú,

Príloha č. X: Organizačná schéma s vyznačením útvarov a ľudí zúčastňujúcich sa na realizácií základnej služby

h. správa z posledného penetračného testovania informačného systému, použitá metodika a rozsah testovania a doloženie kvalifikácie zamestnancov vykonávajúcich penetračné testy, ak sú penetračné testy vykonané.

Príloha č. X: xxx

5. Meno, priezvisko a kontaktné údaje zodpovedného zamestnanca prevádzkovateľa základnej služby, ktorý poskytne audítorovi počas výkonu auditu požadovanú súčinnosť a bude ho sprevádzať.

XXX (Manažér KB)

6. Evidencia záznamov o kybernetických bezpečnostných incidentoch s vplyvom na poskytovanie základných služieb od doby vykonania posledného auditu alebo za posledné dva roky pri prvom audite.

Príloha č. X – bezpečnostné incidenty za posledné dva roky

7. Rozhodnutie o uložení pokuty na úseku kybernetickej bezpečnosti, ak bola uložená, a ďalšie prípady porušenia povinností podľa Zákona, ak k porušeniam došlo.

k uvedenej situácii neprišlo/udialo sa dňa XXX

8. Bezpečnostná dokumentácia podľa § 20 ods. 5 Zákona alebo osobitného predpisu.

Príloha č. X: Bezpečnostná dokumentácia – zoznam + samotné dokumenty Príloha č. X: xxxxx

9. Číslo platného potvrdenia o priemyselnej bezpečnosti, ak je vydané.
nemáme

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

Príloha č. 3 Vzor vyjadrenia PZS ku auditnej správe

PZS hlavička, adresa sídla

Pre:
[Meno a priezvisko vedúceho certifikovaného audítora]
Certifikovaný audítor kybernetickej bezpečnosti

Vec:
Vyjadrenie prevádzkovateľa základnej služby k správe z auditu kybernetickej bezpečnosti

Vážený audítor,

na základe auditu kybernetickej bezpečnosti podľa § 29 ods. 1 zákona č. 69/2018

Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov Vám zasielame naše vyjadrenie s priebehom výkonu auditu kybernetickej bezpečnosti a draftu záverečnej správy o výsledkoch auditu prevádzkovateľa základnej služby. K priebehu auditu a nálezom z preverovaných oblastí **máme/nemáme** výhrady* a so záverečnou správou **súhlasíme**.

* Zoznam výhrad:

S pozdravom

Meno a priezvisko štatutára
Funkcia

Príloha č. 4 Vzor záverečnej auditnej správy

Vzor záverečnej auditnej správy vo formáte MS Word je samostatnou prílohou.

Príloha č. 5 Matica vyspelosti komponentov bezpečnostnej architektúry

Úroveň vyspelosti	Funkcia	Dokumentácia	Roly	Činnosti	Nástroj	Údaje	Metrika
0	Nie je plnená	Neexistuje	Nie sú definované	Nie sú vykonávané	Neexistuje	Neexistujú	Metrika nie je stanovená
1	Je plnená iba malá časť funkcií	Iba základné, nejednotné informácie	Roly sú vykonávané iba ad-hoc dostupnými pracovníkmi	Sú vykonávané iba niektoré základné činnosti	Využívajú sa len jednoduché pomôcky	Využívajú sa len náhodné zdroje údajov	Neexistujú podklady, vykonávané sú len zriedkavé merania
2	Sú plnené niektoré zo základných funkcií	Dokumentácia je čiastočná, bez jednotného prístupu	Sú priradené osoby do základných rolí	Väčšina základných činností je vykonávaná	Podporované sú výhradne základné funkčnosti nástroja	Proces využíva vlastné oddelené údaje	Neexistuje špecifická metrika, merania sú vykonávané nepriamo
3	V plnom rozsahu sú plnené základné funkcie	Štruktúra dokumentácie je definovaná, obsahovo môže byť dokumentácia čiastočne neúplná	Väčšina rolí je definovaná a majú priradené osoby	Vykonávané sú všetky základné činnosti	Nástroj je schopný plne podporovať cieľ, avšak bez ďalšej integrácie	Údaje sú dostupné, majú požadovanú kvalitu, nie sú zdieľané	Existuje špecifická metrika, sú vykonávané len čiastočné merania
4	Všetky funkcie sú plnené	Dokumentácia pokrýva všetky potreby	Všetky potrebné roly sú definované, majú priradené osoby	Všetky činnosti sú plne vykonávané	Plne funkčný nástroj, s čiastočnou integráciou do iných procesov (opatrení, nástrojov)	Existuje jednotná údajová základňa	Merania sú vykonávané v odporúčanom rozsahu
5	Funkcie sú plnené a optimalizované	Kompletná dokumentácia, vrátane definovaného životného cyklu	Roly sú definované, majú priradené osoby a právomoci	Všetky činnosti sú vykonávané; je definovaný systém zlepšovania	Nástroj plne a efektívne podporuje prostredie a ciele	Jednotná údajová základňa s plánom rozvoja	Merania sú pravidelné a využívané sú k optimalizácii