KCCKB Verejné

Druh dokumentu: Metodika

ŠTANDARD NA VÝKON AUDITU KYBERNETICKEJ BEZPEČNOSTI

Číslo: 03
Verzia: 7.0

Zverejnený: 30.4.2021
Účinný od: 1.5.2021

Záväzný pre: *CERTIFIKOVANÍ ADÍTORI KYBERNETICKEJ BEZPEČNOSTI*
Prístupný pre: *ODBORNÁ VEREJNOSŤ*

Vydal útvar: *ODBOR AUDITU A AUTORIZOVANÝCH ČINNOSTÍ*
Autori: Tomáš Hettych
Spoluautori: Marián Illovský, Katarína Geciová, Michal Ďorda

Schválil: Ivan Makatura, generálny riaditeľ

Obsah:

1 Úvod

1.1 Normatívne odkazy

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

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

[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

[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

[5] Vyhláška Národného bezpečnostného úradu č. 436/2019 Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora

[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

[8] STN EN ISO / IEC 27000, Informačné technológie - Bezpečnostné metódy - Systém riadenia informačnej bezpečnosti systémy - prehľad a slovník

[9] STN EN ISO / IEC 27001, Informačné technológie - Bezpečnostné metódy - Systém riadenia informačnej bezpečnosti systémy - požiadavky

[10] STN EN ISO / IEC 27002 Informačné technológie - Bezpečnostné metódy - Pravidlá dobrej praxe riadenia informačnej bezpečnosti

[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

1.2 Termíny a definície

termín	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
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 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.
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 zistenej nezhody
auditný dôkaz		záznamy, konštatovania skutočnosti alebo ďalšie informácie, ktoré sa týkajú kritérií auditu a sú verifikovateľné [ISO 19011: 2018, čl. 3.9]
auditný záver		výsledok auditu po zvážení cieľov auditu a všetkých zistení auditu [ISO 9000: 2015, čl. 3.13.10]
audítor kybernetickej bezpečnosti		orgán posudzovania zhody podľa osobitného predpisu, ktorý je certifikovaný ako orgán príslušný na posudzovanie zhody v oblasti kybernetickej bezpečnosti
audítorská spoločnosť		zamestnávateľ audítora kybernetickej bezpečnosti, ak pracuje ako zamestnanec spoločnosti, ktorá môže sprostredkovať 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
cieľ auditu		definícia toho, čo sa má dosiahnuť individuálnym auditom
efektívnosť		miera, v akej sa realizovali plánované činnosti a dosiahli plánované výsledky [ISO 19011: 2018, čl. 3.26]
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]

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
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 organizácia vykonáva prácu alebo poskytuje službu pomocou on-line nástrojov, ktoré umožňujú jednotlivcom vykonávať procesy bez ohľadu na fyzické umiestnenie. [ISO 19011: 2018, čl. 3.5]
prevádzkovateľ základnej služby	PZS	orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa §3 písm. k) 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
stav nezhody / nezhoda / nesúlad		nesplnenie požiadavky; požiadavkami v kontexte auditu kybernetickej bezpečnosti sú požiadavky vykonávacích predpisov k Zákonu [ISO 19011: 2018, čl. 3.20]
stav zhody / zhoda / súlad		splnenie požiadavky; požiadavkami v kontexte auditu kybernetickej bezpečnosti sú požiadavky vykonávacích predpisov k Zákonu [ISO 19011: 2018, čl. 3.20]
technický expert		osoba, ktorá poskytuje audítorskému tímu špecifické poznatky alebo odborné vedomosti [ISO 19011: 2018, čl. 3.16]
Úrad		Národný bezpečnostný úrad
vedúci audítor kybernetickej bezpečnosti		certifikovaný audítor kybernetickej bezpečnosti zodpovedný sa výkon auditu, ktorý garantuje odbornosť a správnosť auditu a podpisuje záverečnú správu auditu kybernetickej bezpečnosti
zistenia auditu		výsledky hodnotenia zozbieraných dôkazov auditu v porovnaní s kritériami auditu; Zistenia auditu preukazujú zhodu alebo nezhodu [ISO 19011: 2018, čl. 3.10]

1.3 Všeobecné zásady auditu kybernetickej bezpečnosti

Auditom kybernetickej bezpečnosti sa určuje efektívnosť implementácie opatrení, vykonávania opatrení ako aj prípadne existujúce nedostatky implementovaných opatrení v prostredí PZS v oblasti IT a oblasti kybernetickej bezpečnosti v zmysle platnej regulácie a bezpečnostného rámca.

Audit kybernetickej bezpečnosti musí dodržiavať 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

Zásada etiky

Audítor kybernetickej bezpečnosti má vykonávať audit poctivo a zodpovedne, objektívnym a nezaujatým spôsobom. Kdekoľvek je to možné, audítor má byť nezávislý od objektu posudzovania a má vo všetkých prípadoch konať spôsobom, ktorý vylúči tendenčnosť a konflikt záujmov.

Prístup založený na dôkazoch

Musia 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.

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.

Prístup založený na riziku

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

Zásada relevantnosti

Audítor má 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).

Zásada úplnosti a správnosti

Audítor je zodpovedný, že všetky dôkazy, ktoré získa a používa počas auditu sú správne a úplne. Všetky získané auditné dôkazy musia byť uchované, aby sa ku rovnakým výsledkom vedel dostať aj iný a nezávislý audítor pri opakovanom výkone auditu.

Zásada proporcionality a primeranej starostlivosti

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

Audítor sa musí vyhnúť akýmkoľvek aktivitám, ktoré by mohli viesť k znehodnoteniu potenciálnych dôkazov na základe úmyselného či neúmyselného konania. Audítor napríklad nesmie pristupovať ku zariadeniam, ak nemá potrebné schopnosti a nie je pripravený využiť spoľahlivé a overené postupy.

1.4 Metódy 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, implementáciu 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 auditovanej organizácie. Činnosti auditu na diaľku sa vykonávajú na ktoromkoľvek inom mieste než je sídlo auditovanej organizácie, bez ohľadu na vzdialenosť.

Činnosti auditu **pri osobnej vzájomnej súčinnosti** zahŕňajú vzťah medzi pracovníkmi auditovanej organizácie a audítorským tímom. Činnosti auditu **bez osobnej vzájomnej súčinnosti** nezahŕňajú žiadnu osobnú vzájomnú súčinnosť s osobami zastupujúcimi auditovanú organizáciu, 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 auditovanej organizácie 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 Plán auditu

2.1 Auditný program

Generickým cieľom auditu kybernetickej bezpečnosti je overiť plnenie povinností podľa Zákona a posúdiť zhodu 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.

2.2 Určenie rozsahu auditu kybernetickej bezpečnosti

Rozsah auditu je určený v prílohe Príloha č. 3 k vyhláške č. 436/2019 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 auditu je aj výber metód auditu, voľba procedúr, výber nástrojov potrebných pre audit a výber kritérií pre vyhodnotenie auditných dôkazov.

Návrh programu auditu audítor spracuje na základe informácií, ktoré získal zo žiadosti o vykonanie auditu.

2.3 Určenie zdrojov programu auditu

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

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.

2.4 Stanovenie vykonateľnosti auditu

Vykonateľnosť auditu má zaručiť poskytnutie primeraného uistenia, že môžu byť dosiahnuté ciele auditu. Určenie vykonateľnosti má vziať do úvahy tieto faktory:

a) dostupnosť dostatočných a vhodných informácií na plánovanie a vykonanie auditu;
b) primeranú spoluprácu s prevádzkovateľom základnej služby
c) primeraný čas a zdroje na vykonanie auditu.

Ak sa audit nedá vykonať, potom sa má prevádzkovateľovi základnej služby odporučiť odklad výkonu auditu až do doby relevantnej zmeny, ktorá poskytne predpoklad nového stanovenia vykonateľnosti auditu.

2.5 Začatie auditu

Audítor má zaistiť vykonanie kontaktu s auditovanou organizáciou na:

a) potvrdenie komunikačných kanálov s predstaviteľmi auditovanej organizácie;
b) potvrdenie právomoci na vykonanie auditu;
c) poskytnutie relevantných informácií o cieľoch, predmete, kritériách, metódach auditu a o zložení audítorského tímu vrátane akýchkoľvek technických expertov;
d) vyžiadanie prístupu k relevantným informáciám na účely plánovania vrátane informácií o rizikách a príležitostiach, ktoré organizácia identifikovala, a o tom, ako sa zvládajú;
e) určenie aplikovateľných požiadaviek predpisov, regulačných požiadaviek a ďalších požiadaviek relevantných pre činnosti, procesy, produkty a služby auditovanej organizácie;
f) potvrdenie dohody s auditovanou organizáciou, ktorá sa týka rozsahu zachovania mlčanlivosti a zaobchádzania s dôvernými informáciami;
g) spracovanie usporiadaní auditu vrátane harmonogramu;
h) určenie akýchkoľvek špecifických požiadaviek na prístup, na bezpečnosť a ochranu zdravia, na bezpečnosť, dôvernosť alebo na ďalšie požiadavky;

2.6 Poverenie výkonom auditu

Vedúci audítor dohodne s auditovanou organizáciou vystavenie poverenia ako potvrdenia právomoci na vykonanie auditu.

Poverenie musí obsahovať najmä:

- Určenie rozsahu auditu
- Menovanie vedúceho audítora
- Zoznam členov audítorského tímu
- Vyhlásenie PZS o záväzku vykonať audit kybernetickej bezpečnosti
- Zoznam osôb, ktoré sú v mene PZS povinné poskytnúť audítorovi súčinnosť
- Program auditu
- Harmonogram auditu

Ak je audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby vykonávaný v zmysle §29 ods. 5) Zákona s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek

stanovených Zákonom na základe požiadania Úradu, poverenie vystavuje Úrad, alebo certifikačný orgán.

Vzor poverenia na výkon auditu kybernetickej bezpečnosti je v prílohe č. 2.

3 Priebeh auditu kybernetickej bezpečnosti

3.1 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 (auditovanej organizácie 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 auditovanej organizácie.

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 auditovanou organizáciou, 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;

3.2 Získanie a verifikácia informácií

Počas auditu pomocou vhodného 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 majú akceptovať iba tie informácie, ktoré sa dajú aspoň do určitej miery verifikovať. **Ak použiteľná miera verifikácie 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 zhodu, alebo nezhodu.

Metódy zhromažďovania informácií zahŕňajú, ale nie sú nimi limitované

- rozhovory;
- pozorovania;
- dotazníky,

- preskúmania zdokumentovaných informácií

Ak sa informácie poskytli iným spôsobom, ako sa očakávalo (napr. rozdielnymi jednotlivcami, alternatívnymi médiami), úplnosť dôkazu sa má posúdiť aj dodatočne.

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.

Riziko spojené so vzorkovaním je, že vzorky nemusia byť reprezentatívne pre základný súbor, z ktorého boli vybraté. Tým môže byť záver audítora skreslený a odlišný od toho záveru, ktorý by sa dosiahol, keby sa preskúmal celý základný súbor. Môžu existovať ďalšie riziká v závislosti od variability v základnom súbore, z ktorého sa vybrala vzorka a metóda vzorkovania.

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 nezhodu, resp. nedostatočnú účinnosť opatrenia, alebo nejestvujúce, alebo neefektívne dodatočné opatrenie, je na jeho rozhodnutí, či bude skúmať novú vzorku, alebo uzatvorí danú požiadavku ako nezhodu.

3.3 Kritériá auditu

Auditom sa identifikujú nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby. Zhoda alebo nezhoda sa identifikuje pre:

- jednotlivé siete a informačné systémy základnej služby
- siete a informačné systémy ktoré podporujú základné služby

Kritériami auditu kybernetickej bezpečnosti je overenie a posúdenie:

- plnenia povinností prevádzkovateľa základnej služby podľa §19 Zákona
- zhody prijatých bezpečnostných opatrení s požiadavkami podľa §20 Zákona

- zhody prijatých bezpečnostných opatrení podľa súvisiacich osobitných predpisov vzťahujúcich sa na bezpečnosť sietí a informačných systémov

3.4 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**.

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:

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. 3 je uvedený príklad hodnotenia vyspelosti jednotlivých komponentov bezpečnostnej architektúry.

3.5 Tvorba zistení auditu

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

ZHODA - ak je kritérium auditu plnené a audítor neidentifikoval riziko, ani príležitosť na zlepšenie

ČIASTOČNÁ ZHODA - ak je kritérium auditu plnené iba čiastočne, alebo ak audítor identifikoval príležitosť na zlepšenie

NEZHODA - ak je kritérium auditu nie je plnené, alebo ak audítor identifikoval riziko súvisiace s daným kritériom

Ak to špecifikuje plán auditu, jednotlivé zistenia auditu majú zahŕňať okrem určenia zhody aj dobrú prax spolu s podpornými dôkazmi, príležitosti na zlepšovanie a akékoľvek odporúčania pre prevádzkovateľa základnej služby.

4 Ukončenie auditu

4.1 Určovanie záverov auditu

Závery auditu majú obsahovať nasledujúce náležitosti:

a) rozsah zhody s kritériami auditu vrátane efektívnosti implementovaných opatrení v plnení zamýšľaných bezpečnostných cieľov,
b) identifikácia rizík a primeranosti implementovaných opatrení na zvládanie rizík;
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.

Ak to plán auditu špecifikuje, potom závery auditu môžu viesť k odporúčaniam na opatrenia, alebo k odporúčaniam na činnosti budúceho auditu.

4.2 Obsah a formát správy z auditu

Audítor má spracovať správu auditu kybernetickej bezpečnosti, ktorej súčasťou je kontrolný záznam o výsledkoch auditu podľa Prílohy č. 4 k vyhláške č. 436/2019 Z. z.

Vzor formátu správy auditu kybernetickej bezpečnosti, vrátane vzoru kontrolného záznamu o výsledkoch auditu je v Prílohe č. 1.

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

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 (auditovanej organizácie), 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 auditovanej organizácie pri audite

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.

Nálezová časť správy z auditu PZS (kontrolný záznam) s návrhom konkrétnych opatrení je z hľadiska dôvernosti klasifikovaný stupňom „Interné“. Prístupný je pre:
- Úrad,
- Certifikačný orgán,
- Certifikovaných audítorov kybernetickej bezpečnosti, ktorí kontrolný zíznam vykonali,
- Členov auditorského tímu
- Štatutárny organ PZS

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

Zhodnotenie auditu

Zhodnotenie plnenia povinností podľa Zákona a celkového stavu prijatých bezpečnostných opatrení každého informačného systému súvisiaceho so základnou službou, vyslovenie 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 auditovanou organizáciou,
- akékoľvek dôsledky pre program auditu alebo nasledujúce audity.

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. kontrolný záznam s vyjadrením prevádzkovateľa základnej služby ku zisteniam auditu.

Povinnou súčasťou správy auditu na jej poslednom liste je **vyhlásenie audítora**. Vzor textu vyhlásenia je súčasťou Prílohy č. 1.

Vyjadrenie PZS

Po ukončení auditných stretnutí audítor pripraví draft správy, ktorú poskytne na vyjadrenie zástupcovi prevádzkovateľa základnej služby.

Súčasťou záverečnej správy o výsledkoch auditu je pri zistení nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov aj správa o zistených nedostatkoch, pri ktorých prevádzkovateľ základnej služby uvádza termín vykonania nápravných opatrení na zabezpečenie požadovaného súladu s požiadavkami na bezpečnosť sietí a informačných systémov. Nápravné opatrenia sa prijímajú tak, že je možné ich zahrnúť do záverečnej správy o výsledkoch auditu.

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

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 zhodu s požiadavkami na bezpečnosť sietí a informačných systémov.

4.3 Záverečné stretnutie

Záverečné stretnutie („Kick-out meeting“) sa má uskutočniť na prezentáciu zistení a záverov auditu.

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 auditovanou organizáciou.

Vedúci audítorského tímu má oboznámiť auditovanú organizáciu so situáciami vzniknutými v priebehu auditu, ktoré by mohli viesť k zníženiu dôveryhodnosti záverov auditu. Ak je definované

v platnom systéme manažérstva alebo v dohode s klientom auditu, účastníci majú schváliť časový rámec na prijatie plánu opatrení na zvládnutie zistení auditu.

Stupeň podrobností má vziať do úvahy efektívnosť systému manažérstva v dosahovaní cieľov auditovanej organizácie vrátane zvažovania jej súvislostí, rizík a príležitostí.

Ak je to potrebné, pri záverečnom stretnutí sa auditovanej organizácii má vysvetliť

a) informácia, že zhromažďovanie dôkazov auditu sa založilo na vzorke dostupných informácií a nevyhnutne nepredstavuje celkovú efektívnosť procesov auditovanej organizácie,
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 a uznal manažment PZS,
f) akékoľvek súvisiace následné činnosti po audite (napr. implementácia a preskúmanie nápravných opatrení, zvládnutie sťažností auditu, procesu odvolania).

Majú sa prediskutovať, a ak je to možné vyriešiť akékoľvek rozporné názory týkajúce sa zistení alebo záverov auditu medzi audítorským tímom a auditovanou organizáciou. Ak sa nevyriešili, tak sa majú zaznamenať.

4.4 Distribúcia správy z auditu

Správa z auditu má mať uvedený dátum, má sa primerane preskúmať a schváliť v súlade s plánom auditu.

Správu z auditu má audítor distribuovať relevantným zainteresovaným stranám definovaným v programe auditu alebo v pláne auditu, najneskôr do 30 dní od záverečného stretnutia.

Záverečnú správu o výsledkoch auditu je povinný úradu predložiť PZS, do 30 dní od ukončenia auditu. Za termín ukončenia auditu sa považuje termín doručenia správy z auditu.

Pri distribúcii správy z auditu musia byť prijaté primerané opatrenia na zaistenie dôvernosti správy.

Príloha č. 1 Vzor správy auditu kybernetickej bezpečnosti

Správa auditu kybernetickej bezpečnosti

MENO A PRIEZVISKO AUDÍTORA	
EVIDENČNÉ ČÍSLO PLATNÉHO CERTIFIKÁTU AUDÍTORA, DÁTUM VYDANIA	
IDENTIFIKÁCIA PREVÁDZKOVATEĽA ZÁKLADNEJ SLUŽBY (OBCHODNÉ MENO, IČO, SÍDLO, MENO ŠTATUTÁRNEHO ZÁSTUPCU)	
AUDITOVANÉ ZÁKLADNÉ SLUŽBY	
DÁTUMY A MIESTA, KDE SA VYKONÁVALI ČINNOSTI AUDITU	
METÓDY VYKONANÉHO AUDITU	
IDENTIFIKÁCIA AUDÍTORSKÉHO TÍMU	
IDENTIFIKÁCIA ÚČASTNÍKOV Z AUDITOVANEJ ORGANIZÁCIE PRI AUDITE	
POČET STRÁN, VRÁTANE PRÍLOH	
DÁTUM ODOVZDANIA	

Manažérske zhrnutie

Zhrnutie hlavných zistení pre potreby štatutárneho vedenia PZS...

Hodnotenie dosiahnutia cieľov auditu

Záverečné slovné zhrnutie splnenia kritérií auditu...

Zhrnutie úrovne poskytnutej súčinnosti z pohľadu audítora...

Zhrnutie procesu auditu vrátane akýchkoľvek zistených prekážok, ktoré môžu znížiť spoľahlivosť záverov auditu...

Potvrdenie, že sa dosiahli ciele auditu v rámci predmetu auditu v súlade s plánom auditu...

Súvisiace audity...

Popis zistení z rôznych auditovaných oblastí, alebo z predchádzajúcich auditov (napr. audit ISMS. ITSM, a i.)...

Dodatočné požiadavky

Ak sú auditované informačné systémy, pre ktoré platia dodatočné požiadavky nad rámec bezpečnostných opatrení uvedených v Zákone alebo v osobitnom predpise (napr. zákon č. 95/2019 Z. z. o ITVS, vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov), audítor uvedie v kontrolnom zázname spôsob plnenia v súlade s platnými požiadavkami aplikovanými na prevádzkovateľa základnej služby...

Klasifikácia informácií a kategorizácia IS

Overenie úplnosti požadovanej bezpečnostnej dokumentácie a overenie klasifikácie informácií a kategorizácie sietí a informačných systémov...

Kontrolný záznam o výsledkoch auditu

§	Ods.	Písm.	Ustanovenie	Stav súladu	Zistenia / identifikované odchýlky / opis rizík	Súvisiace auditné dôkazy	Odporúčané nápravné opatrenia

Správa o zistených nedostatkoch (stavy nesúladu a závažné auditné zistenia)

§	Ods.	Písm.	Ustanovenie	Zistenia / identifikované odchýlky / opis rizík	Súvisiace auditné dôkazy	Odporúčané nápravné opatrenia audítora

Zoznam použitých dokumentov

§	Ods.	Písm.	Ustanovenie	Dokument

Vyhlásenie audítora

Správu auditu som vypracoval/a ako certifikovaný audítor kybernetickej bezpečnosti, evidenčné číslo certifikátu xxx/O-xxx v zmysle platnej metodiky vlastníka certifikačnej schémy.

Vyhlasujem, že som nezávislý/á pri posudzovaní bezpečnostných opatrení a že som sa počas posledných troch rokov pred konaním auditu nezúčastňoval/a na riadení alebo prevádzke auditovaných informačných systémov.

Prehlasujem, že audit som vykonal/a objektívne a že si nie som vedomý/á žiadnych uznaných sťažností na objektívnosť počas vykonávanej praxe. Som si vedomý/á následkov vedome nepravdivej auditnej správy.

Certifikačná značka (pečiatka) audítora

Podpis audítora

Príloha č. 2 Vzor poverenia na výkon auditu kybernetickej bezpečnosti

Autorizačný list / Poverenie na výkon auditu kybernetickej bezpečnosti

PREVÁDZKOVATEĽ ZÁKLADNEJ SLUŽBY (OBCHODNÉ MENO, IČO, SÍDLO)	
MENO ŠTATUTÁRNEHO ZÁSTUPCU	
ZMLUVA Č.	

v mene prevádzkovateľa základnej služby na základe vyššie uvedenej zmluvy týmto

autorizujem

pre účely vykonania auditu kybernetickej bezpečnosti s cieľom preveriť účinnosti prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených Zákonom č. 69/2018 Z.z. o kybernetickej bezpečnosti (ďalej len „Zákon“) a príslušných vyhlášok tu uvedený audítorský tím:

AUDÍTOR KYBERNETICKEJ BEZPEČNOSTI (VEDÚCI AUDÍTOR) AUDÍTORSKÁ SPOLOČNOSŤ	
AUDÍTORSKÝ TÍM	
ASISTENTI AUDÍTORA	
TECHNICKÍ EXPERTI	
ZAMESTANCI PZS ÚČASTNÍ PRI AUDITE	

Všetci vyššie uvedení členovia auditorského tímu spĺňajú kritéria Vyhlášky č. 436/2019 Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora (ďalej len „Vyhláška“).

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 Zákona, Vyhlášky a Štandardu pre výkon auditu kybernetickej bezpečnosti (ďalej len „Metodické usmernenie“).

Certifikačným orgánom pre účely auditov kybernetickej bezpečnosti je KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI a overenie certifikácie audítora je možné na webovej stránke: https://cybercompetence.sk .

Dátum

Meno a podpis štatutárneho zástupcu PZS

Príloha č. 3 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