ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2019

Vyhlásené: 19. 12. 2019 Časová verzia predpisu účinná od: 1. 1.2020 do: 31.12.2022

436

VYHLÁŠKA
Národného bezpečnostného úradu
z 11. decembra 2019,
o audite kybernetickej bezpečnosti a znalostnom štandarde audítora

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

§ 1

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

(2) Audit vykonáva orgán posudzovania zhody podľa § 29 ods. 3 zákona, ktorým je audítor kybernetickej bezpečnosti (ďalej len „audítor“).

(3) Na vykonanie auditu audítor spĺňa podmienky znalostného štandardu podľa prílohy č. 1 overené skúškou doloženou podľa odporúčaní medzinárodne akceptovaných technických noriem[2]) alebo iných, týmto štandardom vecne obdobných a všeobecne uznávaných postupov.

(4) Audítor zodpovedá za správnosť, rozsah a odbornosť pri výkone auditu a spracovaní záverečnej správy o výsledkoch auditu.

(5) Audítor vykonáva audit odborne, objektívne, nestranne, na základe dôkazov podľa odporúčaní technických noriem[2]) alebo iných vecne obdobných a všeobecne uznávaných postupov.

(6) 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 podľa odseku 1.

(7) Audítor pri výkone auditu najmä

a) prijíma žiadosť o vykonanie auditu v rozsahu minimálnych náležitostí uvedených v prílohe č. 2 a posudzuje kompletnosť údajov v žiadosti; môže si vyžiadať ďalšie informácie potrebné na prípravu a výkon auditu,

b) pripravuje harmonogram výkonu auditu, ktorý obsahuje najmä

1. identifikáciu organizačných útvarov, procesov, auditovaných sietí a informačných systémov a fyzických lokalít prevádzkovateľa základnej služby s uvedením času a
2. meno, priezvisko a kontaktné údaje zodpovedného zamestnanca prevádzkovateľa základnej služby, ktorý poskytuje audítorovi počas auditu požadovanú súčinnosť,

c) určuje rozsah auditu spôsobom podľa prílohy č. 3,

d) určuje metódy auditu podľa prílohy č. 4,

e) pripravuje podklady a pracovné dokumenty potrebné na výkon auditu,

f) preskúmava bezpečnostnú dokumentáciu a vyhodnocuje bezpečnostné opatrenia a vypracúva kontrolný záznam auditovaných bezpečnostných opatrení (ďalej len „kontrolný záznam“) podľa prílohy č. 4,

g) zbiera, sústreďuje a vyhodnocuje dôkazy o zisteniach auditu,

h) písomne oboznamuje zodpovedného zamestnanca prevádzkovateľa základnej služby so zistenými nedostatkami a zostavuje súbor odporúčaných opatrení na ich odstránenie,

i) vypracúva záverečnú správu o výsledkoch auditu.

§ 2

(1) V záverečnej správe o výsledkoch auditu sa hodnotí výsledok auditu a uvedú sa dôkazy, na základe ktorých sa hodnotenie vykonalo.

(2) Záverečná správa o výsledkoch auditu obsahuje najmä

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

b) vymedzenie rozsahu vykonaného auditu,

c) cieľ auditu,

d) metódy vykonaného auditu,

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

f) odporúčané nápravné opatrenia audítora pri zistení nedostatkov,

g) dokumenty, najmä

1. kópiu certifikátu audítora,
2. kópiu žiadosti o vykonanie auditu,
3. výpočet rozsahu trvania auditu a zdôvodnenie jeho skrátenia alebo predĺženia,
4. kontrolný záznam s vyjadrením prevádzkovateľa základnej služby so zisteniami auditu,
5. harmonogram auditu,
6. zoznam posúdenej dokumentácie,
7. uvedenie a zdôvodnenie zmien a rozdielov priebehu auditu oproti plánovanému harmonogramu,
8. zhodnotenie plnenia povinností podľa zákona a celkového stavu prijatých bezpečnostných

opatrení každého informačného systému súvisiaceho so základnou službou, vyslovenie súladu alebo nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov a konkrétne uvedenie nedostatkov,

h) informáciu o stave vykonaných nápravných opatrení, ak prevádzkovateľ základnej služby na základe predchádzajúceho auditu mal tieto nápravné opatrenia prijať.

(3) 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.

(4) 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.

§ 3

Táto vyhláška nadobúda účinnosť 1. januára 2020.

Roman Konečný v. r.

Príloha č. 1
k vyhláške č. 436/2019 Z. z.

ZNALOSTNÝ ŠTANDARD AUDÍTORA

1. Všeobecné požiadavky

Minimálne požiadavky na úroveň vzdelania a prax audítora:

Vzdelanie a požadovaný doklad	Prax a spôsob jej preukázania (alternatívy predložených dokumentov)
Úplné stredné všeobecné vzdelanie a úplné stredné odborné vzdelanie (doklad o získanom stupni vzdelania a o získanej kvalifikácii)	- skúsenosti v oblasti informačných technológií, kybernetickej bezpečnosti - najmenej 10 rokov praxe (životopis s uvedením kontaktu na overiteľnú referenciu, zoznam vykonaných auditov s uvedením kontaktu na overiteľnú referenciu), - skúsenosti v oblasti auditu informačných systémov - najmenej sedem rokov praxe (medzinárodný certifikát z oblasti auditu informačných systémov, zoznam vykonaných auditov s uvedením kontaktu na overiteľnú referenciu)
Vysokoškolské vzdelanie prvého stupňa (doklady o absolvovaní štúdia)	- skúsenosti v oblasti informačných technológií, kybernetickej bezpečnosti - najmenej sedem rokov praxe (životopis s uvedením kontaktu na overiteľnú referenciu, zoznam auditov), - skúsenosti v oblasti auditu informačných systémov - najmenej päť rokov praxe (medzinárodný certifikát z oblasti auditu informačných systémov, zoznam vykonaných auditov s uvedením kontaktu na overiteľnú referenciu)
Vysokoškolské vzdelanie druhého stupňa (doklady o absolvovaní štúdia)	- skúsenosti v oblasti informačných technológií, kybernetickej bezpečnosti - najmenej päť rokov praxe (životopis s uvedením kontaktu na overiteľnú referenciu, zoznam auditov), - skúsenosti v oblasti auditu informačných systémov - najmenej tri roky praxe (medzinárodný certifikát z oblasti auditu informačných systémov, zoznam vykonaných auditov s uvedením kontaktu na overiteľnú referenciu)

Vedomosti:

- Znalosť auditu kybernetickej bezpečnosti alebo informačnej bezpečnosti, alebo auditu informačných systémov sa preukazuje osvedčením certifikačného audítora podľa technickej normy[3]) alebo ekvivalentným osvedčením o spôsobilosti vykonávať audit informačnej alebo kybernetickej bezpečnosti doloženým medzinárodne platným certifikátom audítora.

Predpoklady:

- nezávislosť (audítor je nezávislý pri posudzovaní bezpečnostných opatrení, ak sa počas posledných troch rokov pred konaním auditu nezúčastňoval na riadení alebo prevádzke auditovaných informačných systémov; dokladá sa vyhlásením pri každom audite),
- objektívnosť (absencia uznaných sťažností na objektívnosť počas vykonávanej praxe),
- bezúhonnosť.

2. Osobitné požiadavky

Minimálne požiadavky na úroveň odbornej spôsobilosti audítora

Názov role	Oblasť/proces	Znalosti, schopnosti a predpoklady
Audítor	audit kybernetickej bezpečnosti	Znalosť procesov a systému riadenia informačnej a kybernetickej bezpečnosti. Znalosť zásad organizácie informačnej a kybernetickej bezpečnosti. Znalosť zásad personálnej bezpečnosti. Znalosť zásad riadenia prístupov a identít. Znalosti o spôsobe používania kryptografických bezpečnostných mechanizmov. Znalosť princípov testovania kybernetickej bezpečnosti. Znalosť zásad auditu kybernetickej bezpečnosti. Znalosť právnych predpisov, politík, požiadaviek na súlad a noriem vzťahujúcich sa na kybernetickú bezpečnosť. Znalosť právnych predpisov, politík, požiadaviek na súlad a noriem vzťahujúcich sa na ochranu osobných údajov. Znalosť politík a noriem vzťahujúcich sa na informačnú a kybernetickú bezpečnosť. Znalosť politík a noriem vzťahujúcich sa na ochranu osobných údajov. Znalosť zásad ochrany osobných údajov. Schopnosť navrhovať a uplatniť bezpečnostné stratégie a politiky. Znalosť procesov a metodík riadenia rizík.

[3]) Napríklad STN EN ISO/IEC 27001, STN ISO/IEC 20000-1.

		Znalosť postupov analýzy rizík. Znalosť typických hrozieb a postupov pre identifikáciu hrozieb a zraniteľností. Znalosť bezpečnostných mechanizmov. Znalosť metodík podnikovej architektúry. Znalosť procesov riešenia kybernetických bezpečnostných incidentov. Znalosť princípov plánovania havarijnej obnovy prevádzky. Znalosť procesov riadenia kontinuity činností a princípov plánovania havarijnej obnovy. Znalosť princípov logovania a bezpečnostného monitorovania. Znalosť zásad riadenia fyzickej a objektovej bezpečnosti. Znalosť bezpečnostných mechanizmov vo fyzickej a objektovej bezpečnosti. Znalosť princípov riadenia služieb v oblasti informačných technológií. Znalosť princípov riadenia nákladov a rozpočtových pravidiel. Schopnosť prioritizácie úloh a efektívneho priraďovania zdrojov. Znalosť princípov riadenia ľudských zdrojov. Znalosť konceptov počítačových sietí. Znalosť zásad riadenia projektov. Znalosť zásad riadenia dodávateľských služieb. Znalosť zásad navrhovania a vývoja aplikácií a informačných systémov. Znalosť zásad obstarávania informačných systémov. Znalosť zásad aplikačnej bezpečnosti. Znalosť princípov a procesov auditovania. Technické vedomosti o auditovaných systémoch. Znalosť metód posudzovania rizík dostatočná pre vyhodnotenie rizík auditu a posúdenia hodnotenia rizík, kategorizácie informačných systémov prevádzkovateľov. Znalosť požiadaviek zákona a príslušných vyhlášok. Schopnosť posúdiť dôkazy. Schopnosť analyzovať riziká. Schopnosť spracovať úplnú a prehľadnú záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti. Schopnosť analyzovať a hodnotiť bezpečnostné mechanizmy a riešenia.

Príloha č. 2
k vyhláške č. 436/2019 Z. z.

MINIMÁLNE NÁLEŽITOSTI ŽIADOSTI O VYKONANIE AUDITU KYBERNETICKEJ BEZPEČNOSTI

1. Identifikácia prevádzkovateľa základnej služby.
2. Identifikácia základných služieb podporených auditovanými informačnými systémami a sieťami.
3. Počet zamestnancov prevádzkovateľa základnej služby.
4. Zoznam informačných systémov a ich klasifikácia s väzbou na základnú službu a pre každý z nich najmenej informácie o informačnom systéme a
   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,
   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,
   c) počet užívateľov základnej služby, teritoriálne rozloženie a dôsledky pri výpadku základnej služby na jej užívateľov,
   d) systém správy; interné a externé zdroje, identifikácia kľúčových dodávateľov a zmlúv a dohôd o úrovni poskytovaných služieb,
   e) schéma sieťovej architektúry s uvedením miest prepojení sietí a pripojenia voči externým sieťam,
   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,[4])
   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,
   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.
5. Meno, priezvisko a kontaktné údaje zodpovedného zamestnanca prevádzkovateľa základnej služby, ktorý poskytne audítorovi počas výkonu auditu požadovanú súčinnosť a bude ho sprevádzať.
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.
7. Rozhodnutie o uložení pokuty na úseku kybernetickej bezpečnosti, ak bola uložená, a ďalšie prípady porušenia povinností podľa zákona, ak k porušeniam došlo.
8. Bezpečnostná dokumentácia podľa § 20 ods. 5 zákona alebo osobitného predpisu.[5])
9. Číslo platného potvrdenia o priemyselnej bezpečnosti, ak je vydané.

Príloha č. 3
k vyhláške č. 436/2019 Z. z.

ROZSAH TRVANIA A ČASOVÝ INTERVAL AUDITU KYBERNETICKEJ BEZPEČNOSTI

A: URČENIE ROZSAHU TRVANIA AUDITU

Audítor zodpovedá za určenie dĺžky trvania auditu na dostatočné posúdenie predmetu auditu. Pri výpočte trvania dĺžky auditu audítor zohľadňuje informácie zo žiadosti o vykonanie auditu kybernetickej bezpečnosti a dodatočne vyžiadaných informácií, predovšetkým z

a) počtu používateľov sietí a informačného systému,
b) počtu zamestnancov zúčastňujúcich sa na prevádzke sietí a informačného systému,
c) kategorizácie sietí a informačných systémov,
d) rozsahu účasti tretích strán na prevádzke informačného systému a zabezpečovaní bezpečnostných opatrení,
e) množstva, rozsahu a komplexnosti dokumentácie súvisiacej s prevádzkou informačného systému a zabezpečovaním bezpečnostných opatrení vrátane výsledkov predchádzajúcich auditov a vykonaných analýz rizík.

Výpočet dní trvania auditu pre každý informačný systém a lokalitu prevádzkovateľa samostatne.

Počet zamestnancov zúčastňujúcich sa na prevádzke systému a zabezpečovaní bezpečnostných opatrení	**Audit v človeko-dňoch**
1~10	5
11~20	6
21~30	7
31~50	8
51~70	9
71~90	10
>90	+1 deň za každých ďalších 20 zamestnancov

Za každý ďalší informačný systém sa považuje súbor súvisiacich a navzájom závislých aktív (hardvér, softvér, služby dodávateľov), ktoré podporujú ďalšiu základnú službu, alebo je prevádzka informačných systémov a sietí vykonávaná inými zamestnancami, alebo organizačným útvarom, alebo je na inej lokalite. Pri prítomnosti alebo účasti zamestnancov z iných lokalít (dodávateľ pri externe zabezpečovaných činnostiach) podieľajúcich sa na

prevádzke rovnakého informačného systému formou vzdialeného pripojenia nie je potrebné zvyšovať počet dní auditu.

Ak za niekoľko informačných systémov a zabezpečenie bezpečnostných opatrení sú zodpovedné tie isté osoby, nezvyšuje sa počet dní auditu, ak budú viaceré informačné systémy auditované súčasne.

Faktory znižujúce rozsah auditu (najviac na 1/3 uvedeného rozsahu pri kombinácii faktorov).

Trvanie auditu sa od výpočtu dní podľa predchádzajúcej tabuľky znižuje

a) na 1/3, ak má audítor k priamej dispozícii záverečnú správu o výsledkoch auditu z predchádzajúceho auditu kybernetickej bezpečnosti vykonaného v súlade s touto vyhláškou a nevyskytli sa žiadne zmeny v počtoch zamestnancov spravujúcich systémy, v aktívach, použitých technológiách a základných službách podporovaných informačnými systémami v záverečnej správe o výsledkoch auditu. Audítor sa venuje predovšetkým prevereniu skutočnosti, či uvedené zmeny nenastali, a zároveň oblastiam označeným v kontrolnom zázname, ktoré sú povinné pre každý audit,
b) na ½, ak sú všetky informačné systémy zaradené do kategórie citlivosti I,
c) na ½, ak je prevádzkovateľ základnej služby držiteľom certifikátu podľa technickej normy[6]) a certifikovaná oblasť zahŕňa auditované informačné systémy,
d) na ½, ak je auditovaný informačný systém certifikovaný v súlade s požiadavkami na certifikáciu kybernetickej bezpečnosti[7]) informačných technológií,
e) na iný rozsah podľa rozhodnutia audítora; audítor musí svoje rozhodnutie riadne zdôvodniť.

Faktory zvyšujúce rozsah auditu

Trvanie auditu sa od výpočtu dní podľa predchádzajúcej tabuľky zvyšuje

a) na dvojnásobok, ak sú informačné systémy zaradené do kategórie citlivosti III,
b) na dvojnásobok, ak sa vyskytol závažný kybernetický bezpečnostný incident od doby vykonania posledného auditu alebo je uložená pokuta za porušenie povinností podľa zákona,
c) na iný rozsah podľa rozhodnutia audítora po predošlej konzultácii s prevádzkovateľom základnej služby; audítor musí svoje rozhodnutie riadne zdôvodniť.

Do časového rozsahu trvania auditu sa započítava čas audítora pri posúdení žiadosti o vykonanie auditu kybernetickej bezpečnosti, doručenie vyžiadaných dodatočných podkladov, predbežná analýza plnenia povinností, posúdenie povinnej dokumentácie a spracovanie záverečnej správy o výsledkoch auditu, a to spolu najviac v rozsahu 1/3 celkového potrebného časového rozsahu trvania auditu.

B: URČENIE ČASOVÉHO INTERVALU AUDITU

Audit sa vykonáva

---

[6]) Napríklad STN EN ISO/IEC 27001 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky (ISO/IEC 27001: 2013 vrátane Cor. 1: 2014 a Cor. 2: 2015).

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

a) každé dva roky a
b) pri každej významnej zmene, najneskôr do dvoch mesiacov odkedy má zmena významný vplyv na realizované bezpečnostné opatrenia.

Významným vplyvom sa rozumie najmä
a) vplyv na prijatú klasifikáciu informácií a kategorizáciu sietí a informačných systémov,
b) zmena dopadových kritérií základnej služby,
c) zmena alebo výmena informačného systému a prevádzkových parametrov základnej služby,
d) zavedenie novej siete alebo nového informačného systému, od ktorých je závislá základná služba, alebo
e) zavedenie novej technológie, od ktorej je závislá základná služba.

Príloha č. 4
k vyhláške č. 436/2019 Z. z.

KONTROLNÝ ZÁZNAM AUDITOVANÝCH BEZPEČNOSTNÝCH OPATRENÍ

Kontrolný záznam obsahuje súbor požiadaviek na bezpečnosť sietí a informačných systémov podľa zákona a jeho vykonávacích predpisov a osobitných predpisov. 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 informačné systémy, sa vyplnia samostatne pre každý informačný systém alebo sieť.

V kontrolnom zázname audítor uvedie

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

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

c) získané dôkazy podporujúce uvedené zistenia a

d) referenciu na použitú metódu auditu, napríklad
- pozorovanie činností a stavu bezpečnostných opatrení,
- analýzu predložených záznamov,
- analýzu predložených postupov, predpisov a dokumentov,
- rozhovory a dotazníky.

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

Ak sú auditované informačné systémy, pre ktoré platia dodatočné požiadavky nad rámec bezpečnostných opatrení uvedených v zákone alebo v osobitnom predpise,[5]) audítor uvedie v kontrolnom zázname spôsob plnenia v súlade s platnými požiadavkami aplikovanými na prevádzkovateľa základnej služby.

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

Audítor uchováva kontrolný záznam s odbornou starostlivosťou a s ohľadom na citlivosť informácií počas dvoch rokov od skončenia auditu.

1) Napríklad § 2 zákona Národnej rady Slovenskej republiky č. 566/1992 Zb. o Národnej banke Slovenska v znení neskorších predpisov, § 14 zákona č. 429/2002 Z. z. o burze cenných papierov v znení neskorších predpisov, zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 2 ods. 9 zákona č. 747/2004 Z. z. o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov v znení zákona č. 132/2013 Z. z., zákon č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov, zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.

2) Napríklad STN EN ISO/IEC 17024 Posudzovanie zhody. Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb (ISO/IEC 17024:2012).

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) Napríklad zákon č. 95/2019 Z. z., vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov.

Vydavateľ Zbierky zákonov Slovenskej republiky, správca obsahu a prevádzkovateľ právneho a informačného portálu Slov-Lex dostupného na webovom sídle www.slov-lex.sk je
Úrad vlády Slovenskej republiky, Námestie slobody 1, 813 70 Bratislava,
tel.: 02 888 91 131, e-mail: helpdesk@slov-lex.sk.