CERTIFIKAČNÁ SCHÉMA OVEROVANIA ODBORNEJ SPÔSOBILSOTI AUDÍTORA

I. ÚVOD

Certifikačnú schému overovania odbornej spôsobilosti audítora vydáva orgán dohľadu – Národný bezpečnostný úrad, ako vlastník schémy.

Certifikačná schéma poskytuje postup pri certifikácii audítora. V záujme zachovania kvality určuje všeobecné a osobitné požiadavky na certifikáciu audítora certifikačným orgánom podľa odporúčaní medzinárodne akceptovaných štandardov alebo iných vecne obdobných postupov[3]) príslušným na certifikáciu personálu v oblasti kybernetickej bezpečnosti.

Certifikačný orgán je oprávnený vydávať certifikát audítora, ak je akreditovaný Slovenskou národnou akreditačnou službou[1]) pre oblasť certifikácie audítorov v súlade s touto certifikačnou schémou.

II. ROZSAH

Predmet certifikácie	Audítor kybernetickej bezpečnosti podľa osobitného predpisu[2])
Opis práce a úloh	Preverenie účinnosti prijatých bezpečnostných opatrení a plnenie požiadaviek ustanovených zákonom a vykonávacími predpismi vykonaním auditu kybernetickej bezpečnosti.

III. KRITÉRIÁ CERTIFIKÁCIE

1. Všeobecné požiadavky na spôsobilosť

Minimálne požiadavky na úroveň vzdelania a prax žiadateľa o overenie odbornej spôsobilosti

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),

[1]) § 9 zákona č. 505/2009 Z. z. o akreditácii orgánov posudzovania zhody a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[2]) § 29 ods. 3 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a vyhlášky č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora

	- 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, doložené 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 (dokladá sa výpis z registra trestov nie starší ako 3 mesiace).

Kódex správania (etického, osobného):

- vyhlásenie (napríklad o nestrannosti, zachovaní mlčanlivosti).

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

2. Osobitné požiadavky na spôsobilosť

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. 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.

IV. TERMÍN A MIESTO VYKONANIA ODBORNEJ SKÚŠKY

Termín a miesto vykonania odbornej skúšky určuje certifikačný orgán. Ak sa žiadateľ na skúšku nedostaví, ale vopred sa ospravedlní, je automaticky zaradený a pozvaný na najbližší termín.

Odborná skúška

Odborná skúška sa vykonáva zo znalosti všeobecne záväzných právnych predpisov upravujúcich kybernetickú bezpečnosť, ochranu kritickej infraštruktúry a oblastí v rámci vzdelávacích štandardov pre kybernetickú bezpečnosť.

Národný bezpečnostný úrad na svojom webovom sídle zverejňuje

a) príklady otázok na vykonanie odbornej skúšky a usmernenie na ich používanie,
b) vzor žiadosti o vykonanie odbornej skúšky a

c) vzor certifikátu audítora.

Pozvánka na odbornú skúšku sa doručuje žiadateľovi spravidla v elektronickej podobe 15 dní pred termínom konania skúšky.

Odborná skúška sa skladá z písomného testu a prípadovej štúdie. Písomný test pozostáva z testových otázok zo znalosti všeobecne záväzných právnych predpisov o podmienkach výkonu činnosti audítora. Prípadovou štúdiou sa preukazuje aplikácia odborných predpisov, postupov a metodiky pri vypracúvaní úkonov auditu a odborné vedomosti na konkrétnom prípade.

Pred začatím odbornej skúšky žiadateľ preukáže svoju totožnosť dokladom totožnosti a certifikačný orgán ho poučí o pravidlách priebehu skúšky. Ak žiadateľ pred začatím odbornej skúšky nepreukáže svoju totožnosť alebo sa počas skúšky správa v rozpore s pravidlami priebehu skúšky a dobrými mravmi, vylúči sa zo skúšky a hľadí sa na neho akoby skúšku vykonal neúspešne.

Ak žiadateľ v odbornej skúške dosiahne v hodnotení najmenej 80%, vykoná skúšku úspešne.

Ak žiadateľ odbornej skúške dosiahne v hodnotení menej ako 80%, vykonal skúšku neúspešne. Opravnú odbornú skúšku môže žiadateľ vykonať najskôr po uplynutí šiestich mesiacov od neúspešného vykonania odbornej skúšky.

V. VYDANIE CERTIFIKÁTU AUDÍTORA

Informácie o žiadateľovi a výsledky odbornej skúšky sú podkladom na vydanie alebo nevydanie certifikátu audítora a rozhodovanie o tom je nezávislé a nestranné a prijíma ho kompetentná osoba v súlade s požiadavkami na certifikačný orgán podľa technickej normy[2)] a touto certifikačnou schémou.

Platnosť certifikátu audítora sa začína dňom vydania certifikátu audítora. Certifikát audítora sa zasiela žiadateľovi poštou, elektronicky alebo si ho môže prevziať osobne. Doba platnosti je 3 roky od jeho vydania. Audítor počas doby platnosti certifikátu audítora využíva svoj certifikát audítora v súlade s podmienkami a obmedzeniami v ňom uvedenými a udržiava stály kontakt s certifikačným orgánom a poskytuje mu pravdivé informácie a dokumenty požadované touto schémou. Svoju činnosť vykonáva audítor odborne a v súlade s dobrými mravmi.

VI. DOHĽAD NAD ČINNOSŤOU AUDÍTORA

Certifikačný orgán vykonáva podľa potreby a v súlade s požiadavkami Národného bezpečnostného úradu dohľad nad činnosťami vykonávanými audítormi.

V rámci dohľadu sa vykonáva:

- pohovor s audítorom s cieľom zistiť jeho znalosti v uplatňovaní postupov pri vykonávaní auditu kybernetickej bezpečnosti, zvyšovanie znalostí absolvovaním kurzov a pod.,
- kontrola vydávaných dokumentov audítora ,
- kontrola záznamov audítora o sťažnostiach zákazníkov, sťažnostiach Národného bezpečnostného úradu, ich vybavenie, nápravné opatrenia a ich účinnosť.

Ak je to potrebné môže sa pri dohľade vykonať posúdenie vlastného výkonu. Na tento účel certifikačný orgán využíva len vlastných zamestnancov. O vykonanom dohľade spracuje certifikačný orgán zápis, ktorý okrem zistených skutočností obsahuje aj termín predloženia nápravných opatrení na odstránenie zistených nedostatkov. Zápis prerokuje s audit, ktorá svojim podpisom potvrdí oboznámenie sa s protokolom, a ak s niektorými závermi nesúhlasí, uvedie svoje stanovisko (námietky, zdôvodnenie nesúhlasu). Záznamy z dohľadov sa evidujú v spise audítora.

VII. OBNOVA CERTIFIKÁTU A PREDĺŽENIE PLATNOSTI CERTIFIKÁTU

A: Obnova platnosti certifikátu audítora

O obnovu certifikátu audítora možno požiadať aj pred uplynutím doby platnosti aktuálne platného certifikátu audítora

a) ak to vyplýva zo všeobecne záväzných právnych predpisov,
b) na základe zmeny požiadaviek certifikačnej schémy,
c) vzhľadom na povahu a rozvinutosť priemyslu alebo odvetvia, v ktorom audítor pôsobí,
d) vzhľadom na prebiehajúce zmeny v technológiách a požiadavkách na audítorov alebo
e) na základe odôvodnenej požiadavky zainteresovaných strán.

Na žiadosť, konanie a na vydanie certifikátu audítora a na certifikát audítora sa vzťahujú ustanovenia o certifikácii audítora a certifikačná schéma.

B: Predĺženie platnosti certifikátu audítora

Pred uplynutím doby platnosti certifikátu audítora môže audítor požiadať o predĺženie platnosti svojho certifikátu audítora na ďalšie trojročné obdobie. Žiadosť sa podáva najneskôr tri mesiace pred skončením platnosti certifikátu audítora.
Podmienkou pre vydanie nového certifikátu audítora je, že audítor

a) počas doby platnosti certifikátu spĺňa podmienky certifikácie a
b) preukáže, že
   - si udržiava vedomosti a prax (udržiavanie praktických zručností doložením výkonu praxe audítora počas posledných troch rokov),
   - si zvyšuje kvalifikáciu v oblasti kybernetickej bezpečnosti najmenej v rozsahu absolvovania 120 hodín vzdelávania,
   - má znalosti auditovania v oblasti informačných systémov (dokladá sa platný certifikát na výkon auditu informačných systémov),
   - preukáže odbornú prax v oblasti auditu informačných systémov nie kratšiu ako tri roky (dokladá sa životopisom a zoznamom najmenej troch auditov spolu v rozsahu najmenej 10 dní auditov),
   - je nezávislý a predchádza konfliktu záujmov (dokladá sa prehlásením) a
   - dokladá nadobudnuté znalosti v oblasti kybernetickej bezpečnosti (dokladá sa praxou, vzdelávaním, auditmi).

Zvyšovanie kvalifikácie pozostáva napríklad z:

- účasti na školeniach v oblasti kybernetickej bezpečnosti (doložením rozsahu školenia v hodinách),
- publikačnej činnosti (akceptuje sa jedna hodina za každú normostranu publikácie),
- prednáškovej činnosti (akceptuje sa jedna hodina za každú odprednášanú hodinu, na prípravu prednášky je možné započítať trojnásobok času prednášania pri jedinečnom

obsahu prednášky a jedennásobok času prednášania pri opakovanom prednášaní prednášky).

Na žiadosť, konanie a na vydanie certifikátu audítora a na certifikát audítora sa vzťahujú ustanovenia o certifikácii audítora a certifikačná schéma okrem ustanovení o odbornej skúške.

VIII. POZASTAVENIE ALEBO ZRUŠENIE CERTIFIKÁTU AUDÍTORA

Certifikačný orgán pozastaví platnosť certifikátu audítora na základe podnetu Národného bezpečnostného úradu alebo pri porušovaní povinností podľa technickej normy.[3]) Ak nedôjde v lehote určenej certifikačným orgánom k náprave skutočností, ktoré viedli k pozastaveniu platnosti certifikátu audítora, certifikačný orgán zruší platnosť vydaného certifikátu audítora.

Certifikačný orgán uzatvorí s audítorom dohodu o tom, že audítor počas pozastavenia platnosti certifikátu audítora tento nevyužíva.

Certifikačný orgán uzatvorí s audítorom dohodu o zdržaní sa používania všetkých odkazov na certifikovaný status audítora, ak sa zruší platnosť certifikátu audítora.

IX. SPÔSOB OVEROVANIA A VYBAVOVANIA SŤAŽNOSTÍ NA VÝKON ČINNOSTI AUDÍTORA

Sťažnosti na výkon činnosti audítora spracúva a rieši certifikačný orgán podľa technickej normy. [3])

X. VEDENIE EVIDENCIÍ

Certifikačný orgán vedie evidenciu
a) žiadostí o vydanie certifikátu audítora,
b) dokumentácie priebehu a výsledkov odbornej skúšky,
c) dokladov preukazujúcich splnenie podmienok podľa certifikačnej schémy,
d) vydaných certifikátov audítora,
e) iných súvisiacich dokumentov.

XI. PRÍSTUP K CERTIFIKAČNEJ SCHÉME

Certifikačná schéma je verejný dokument, ktorý zverejňuje Národný bezpečnostný úrad na svojom webovom sídle.