

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)	<ul style="list-style-type: none">- 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)	<ul style="list-style-type: none">- 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)	<ul style="list-style-type: none">- 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 normy³⁾ 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),
- objektivnosť (absencia uznaných sťažností na objektivnosť 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.

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