Auditor/auditorka kybernetické bezpečnosti (kód: 18-019-T)

Autorizující orgán: Národní úřad pro kybernetickou a informační bezpečnost
Skupina oborů: Informatické obory (kód: 18)
Týká se povolání: Auditor kybernetické bezpečnosti
Kvalifikační úroveň NSK - EQF: 7

Odborná způsobilost

Název	Úroveň
Orientace v legislativě v oblasti kybernetické bezpečnosti pro potřeby auditora/auditorky kybernetické bezpečnosti	7
Uplatňování zásad auditu kybernetické bezpečnosti	7
Orientace v pojmech a definicích v oblasti auditu kybernetické bezpečnosti	7
Plánování auditu kybernetické bezpečnosti	7
Provádění auditu kybernetické bezpečnosti	7
Strategické a taktické řízení ICT	7
Řízení provozu a komunikací ICT	7
Ochrana aktiv v rámci kybernetické bezpečnosti	7
Řízení rizik kybernetické bezpečnosti pro potřeby auditora/auditorky kybernetické bezpečnosti	7
Tvorba scénářů pro zjišťování připravenosti na kritické situace, příprava, vedení a vyhodnocení kontrolních cvičení v oblasti kybernetické bezpečnosti	7

Platnost standardu

Standard je platný od: 20.05.2025 do: 05.07.2026

Kritéria a způsoby hodnocení

Orientace v legislativě v oblasti kybernetické bezpečnosti pro potřeby auditora/auditorky kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Popsat význam a vysvětlit členění zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů	Ústní ověření
b) Popsat a vysvětlit prováděcí předpisy vztahující se k zákonu č. 181/2014 Sb., (vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury), ve znění pozdějších předpisů	Ústní ověření
c) Popsat a vysvětlit cíle evropského nařízení GDPR (nařízení Evropského parlamentu a Rady EU 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES - obecné nařízení o ochraně osobních údajů), ve znění pozdějších předpisů a jeho vztah k ochraně informací v organizaci	Ústní ověření
d) Definovat legislativní rámec pro vyspecifikovanou povinnou osobu v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů	Ústní ověření

Je třeba splnit všechna kritéria.

Uplatňování zásad auditu kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Popsat metodiku auditu kybernetické bezpečnosti v souladu s vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů	Ústní ověření
b) Identifikovat a aplikovat principy auditování v oblasti kybernetické bezpečnosti podle zadaného příkladu	Praktické předvedení a ústní ověření

Je třeba splnit obě kritéria.

Orientace v pojmech a definicích v oblasti auditu kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Definovat a popsat pojmy vztahující se k auditu/auditorovi kybernetické bezpečnosti: program auditu, plán auditu, předmět auditu, auditor, odborná způsobilost auditora, tým auditorů bezpečnosti, technický expert auditu, překladatel auditu, klient auditu	Ústní ověření
b) Popsat a vysvětlit pojmy vztahující se k auditu/auditorovi kybernetické bezpečnosti: kritéria auditu, cíle auditu, zjištění z auditu, objektivní důkaz, závěr z auditu	Ústní ověření
c) Popsat a vysvětlit pojmy vztahující se k auditu/auditorovi kybernetické bezpečnosti: etické chování, nezávislost auditora, průkaznost, techniky auditování, prezentování výsledků auditu	Ústní ověření

Je třeba splnit všechna kritéria.

Plánování auditu kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Určit činnosti, které je nezbytné provést při stanovení programu auditu kybernetické bezpečnosti	Ústní ověření
b) Navrhnout program auditu kybernetické bezpečnosti	Praktické předvedení a ústní ověření
c) Popsat způsob stanovení odpovědností a požadavků na zdroje (lidské, materiální) v rámci programu auditu kybernetické bezpečnosti	Ústní ověření

Je třeba splnit všechna kritéria.

Provádění auditu kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Popsat přípravné činnosti, které musí auditní tým uskutečnit před zahájením auditu kybernetické bezpečnosti	Ústní ověření
b) Vysvětlit a zdůvodnit nutnost přezkoumání dokumentů před zahájením auditu kybernetické bezpečnosti	Ústní ověření
c) Popsat způsob hledání důkazů (shoda/neshoda), hodnocení situací, vedení interview v rámci kybernetické bezpečnosti	Ústní ověření
d) Popsat praktické prověření při vzorkování v rámci kybernetické bezpečnosti	Ústní ověření
e) Popsat průběh dokončení auditu kybernetické bezpečnosti a závěrečných jednání	Ústní ověření
f) Popsat obsah prezentace výsledků auditu kybernetické bezpečnosti managementu organizace	Ústní ověření
g) Vyjmenovat a demonstrovat činnosti vykonávané při zahájení auditu kybernetické bezpečnosti na místě, při jeho provádění a činnosti související s tvorbou zprávy z auditu kybernetické bezpečnosti	Praktické předvedení a ústní ověření

Je třeba splnit všechna kritéria.

Strategické a taktické řízení ICT

Kritéria hodnocení	Způsoby ověření
a) Zařadit pozici vedoucího IT oddělení do organizační struktury organizace a zdůvodnit toto začlenění	Praktické předvedení a ústní ověření
b) Uvést a popsat standardy a normy používané při řízení ICT v organizaci	Ústní ověření
c) Popsat řízení zdrojů (lidské, finanční, časové) v rámci IT oddělení	Ústní ověření
d) Popsat a demonstrovat principy projektového řízení; určit, na který z parametrů trojimperativu je v projektu kladen největší důraz	Praktické předvedení a ústní ověření
e) Popsat a vytvořit plánování IT rozpočtu	Ústní ověření
f) Uvést a popsat postupy při koordinaci provozu ICT	Ústní ověření
g) Popsat provádění řízení změn s ohledem na zajištění kontinuity organizace	Ústní ověření

Je třeba splnit všechna kritéria.

Řízení provozu a komunikací ICT

Kritéria hodnocení	Způsoby ověření
a) Popsat, na čem je založen soubor praxí ITIL (Information Technology Infrastructure Library)	Ústní ověření
b) Popsat význam frameworku COBIT (Control Objectives for Information and related Technology). Navrhnout konkrétní aplikaci procesů ve 4 doménách	Praktické předvedení a ústní ověření
c) Podle konkrétního zadání navrhnout zálohovací schéma a metodiku kontroly záloh	Ústní ověření

Je třeba splnit všechna kritéria.

Ochrana aktiv v rámci kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Identifikovat a ohodnotit aktiva organizace v souladu s vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů	Praktické předvedení a ústní ověření
b) Určit hodnotu aktiv v souladu s vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů	Praktické předvedení a ústní ověření
c) Popsat způsoby likvidace aktiv v souladu s vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů	Ústní ověření
d) Popsat pravidla pro manipulaci s aktivy s ohledem na úroveň aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv v souladu s vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů	Ústní ověření

Je třeba splnit všechna kritéria.

Řízení rizik kybernetické bezpečnosti pro potřeby auditora/auditorky kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Definovat a popsat metodiky řízení rizik kybernetické bezpečnosti	Ústní ověření
b) Vyjmenovat a popsat základní metody analýzy rizik kybernetické bezpečnosti	Ústní ověření
c) Stanovit hodnotu u aktiv, identifikovat pro ně hrozby a zranitelnosti a vypočítat hodnotu rizika, v souladu s vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů	Praktické předvedení a ústní ověření

Je třeba splnit všechna kritéria

Tvorba scénářů pro zjišťování připravenosti na kritické situace, příprava, vedení a vyhodnocení kontrolních cvičení v oblasti kybernetické bezpečnosti

Kritéria hodnocení	Způsoby ověření
a) Připravit scénáře a cvičení v souladu s normou ISO 22398:2013, ve znění pozdějších předpisů, vést je a vyhodnotit	Praktické předvedení a ústní ověření
b) Vysvětlit smysl a způsob implementace cyklu PDCA	Ústní ověření

Je třeba splnit obě kritéria.

Organizační a metodické pokyny

Pokyny k realizaci zkoušky

1. Vstupní předpoklady pro účast na zkoušce

Uchazečem o zkoušku může být každá fyzická osoba starší 18 let, která získala alespoň základy vzdělání, nebo účastník rekvalifikace podle zákona č. 435/2004 Sb., zákon o zaměstnanosti.

Zdravotní způsobilost není vyžadována.

Autorizovaná osoba zároveň s odesláním pozvánky ke zkoušce písemnou formou sdělí, kde a jakým způsobem se uchazeč může informovat o svých povinnostech a průběhu zkoušky a které doklady/dokumenty musí uchazeč předložit bezprostředně před započetím zkoušky.

Autorizovaná osoba informuje žadatele písemnou formou v předstihu minimálně 7 dní o vybraných technologiích (HW a SW) a platformách zvolených pro vykonání zkoušky.

2. Průběh zkoušky

Před zahájením zkoušky uchazeč předloží zkoušejícímu průkaz totožnosti a případně další dokumenty opravňující k připuštění ke zkoušce uvedené v části 1. Vstupní předpoklady pro účast na zkoušce.

Bezprostředně před zahájením zkoušky autorizovaná osoba seznámí uchazeče s pracovištěm, s organizací zkoušky, s jeho právy a povinnostmi v rámci zkoušky podle zákona č. 179/2006 Sb., a s požadavky bezpečnosti a ochrany zdraví při práci (BOZP) a požární ochrany (PO), o čemž autorizovaná osoba vyhotoví a uchazeč podepíše písemný záznam.

Zkoušející uzná, a tedy nemusí ověřovat, ty odborné způsobilosti, které byly již dříve u uchazeče ověřeny v rámci zkoušky z jiné profesní kvalifikace (nutno doložit osvědčením o získání profesní kvalifikace), a které jsou shodné svým rozsahem i obsahem. Rozsah a obsah odborné způsobilosti určují její jednotlivá kritéria a pokyny k provedení zkoušky popsané v hodnoticím standardu. Zkoušející tyto odborné způsobilosti neuzná jako již ověřené, pokud by tím nebylo zajištěno řádné ověření ostatních požadavků stanovených tímto hodnotícím standardem (například při nutnosti dodržení technologických postupů a časové souslednosti různých činností).

Zkouška se koná v českém jazyce.

Zkouška je veřejná. Praktická část zkoušky a praktická zkouška není veřejná v případech, kdy to je nutné z hygienických důvodů nebo z důvodu ochrany zdraví a bezpečnosti práce.

Pokyny k jednotlivým způsobům ověřování:

Kritéria hodnocení, u kterých je jako způsob ověření uvedeno „***ústní ověření***":

- jsou ověřována formou individuálního pohovoru obou členů zkušební komise s uchazečem, tj. s vyloučením možnosti, že by odpovědi aktuálně zkoušeného uchazeče slyšel jiný uchazeč / ostatní uchazeči,
- tato kritéria se ověřují například v odděleném samostatném prostoru (místnosti) nebo takovým způsobem, kdy je zaručeno individuální zkoušení uchazeče,
- přítomnost obou členů zkušební komise po celou dobu ústního ověřování je vyžadována.

Kritéria hodnocení, u kterých je jako způsob ověření uvedeno „***praktické předvedení a ústní ověření***":

- jsou ověřována tak, že uchazeč nejprve prakticky předvede požadovanou činnost a poté (nikoliv však nutně bezprostředně) na pokyn zkušební komise svou činnost obhájí, odpoví na otázky,
- přítomnost obou členů zkušební komise po celou dobu ověřování formou praktického předvedení a ústního ověření je vyžadována.
- Jednotlivá tato kritéria budou přezkoušena v rámci případové studie. Autorizovaná osoba vytváří celkem 10 případových studií, z nichž si uchazeč jednu vylosuje a v nichž jsou vždy uvedeny:
  - předmět činnosti fiktivní organizace,
  - strategie rozvoje ICT organizace s uvedením priorit na další účetní období,
  - organizační struktura organizace,
  - charakteristiky útvaru, kde má být proveden audit,
  - definice informační a komunikační infrastruktury organizace,
  - přehled primárních a podpůrných aktiv organizace s uvedením vazeb.

Autorizovaná osoba, resp. autorizovaný zástupce autorizované osoby je oprávněný předčasně ukončit zkoušku, pokud vyhodnotí, že v důsledku činnosti uchazeče bezprostředně došlo k ohrožení nebo bezprostředně hrozí nebezpečí ohrožení zdraví, života a majetku či životního prostředí. Zdůvodnění předčasného ukončení zkoušky uvede autorizovaná osoba do záznamu o průběhu a výsledku zkoušky. Uchazeč může ukončit zkoušku kdykoliv v jejím průběhu, a to na vlastní žádost.

Výsledné hodnocení

Zkoušející hodnotí uchazeče zvlášť pro každou odbornou způsobilost a výsledek zapisuje do záznamu o průběhu a výsledku zkoušky.

Výsledné hodnocení pro danou odbornou způsobilost musí znít:
- „splnil“, nebo
- „nesplnil“, v závislosti na stanovení závaznosti, resp. nezávaznosti jednotlivých kritérií u každé odborné způsobilosti.

Výsledné hodnocení zkoušky zní buď:
- „vyhověl“, pokud uchazeč splnil všechny odborné způsobilosti, nebo
- „nevyhověl“, pokud uchazeč některou odbornou způsobilost nesplnil. Při hodnocení „nevyhověl“ uvádí autorizovaná osoba vždy zdůvodnění, které uchazeč svým podpisem bere na vědomí.

Počet zkoušejících

Zkouška probíhá před zkušební komisí složenou z dvou členů. Všichni členové komise musí být přítomni u zkoušky po celou dobu jejího trvání.

Zkoušející je povinen provádět ověřování odborných způsobilostí při zkoušce přesně podle všech ustanovení tohoto hodnoticího standardu.

Požadavky na odbornou způsobilost autorizované osoby, resp. autorizovaného zástupce autorizované osoby

Autorizovaná osoba, resp. autorizovaný zástupce autorizované osoby musí splňovat tento požadavek:

Vysokoškolské vzdělání magisterského stupně, vyškolení dle požadavků § 7 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů (např. certifikace uvedené v příloze č. 6 vyhlášky) a nejméně 5 let prokázané odborné praxe v činnostech auditora kybernetické bezpečnosti.

Žadatel o udělení autorizace prokazuje splnění požadavků na odbornou způsobilost a praxi v povolání autorizujícímu orgánu, a to předložením dokladu nebo dokladů o získání odborné způsobilosti a praxe v povolání v souladu s hodnoticím standardem této profesní kvalifikace, nebo takovým postupem, který je v souladu s požadavky uvedenými v hodnoticím standardu této profesní kvalifikace autorizujícím orgánem stanoven.

Žádost o udělení autorizace naleznete na internetových stránkách autorizujícího orgánu: Národní úřad pro kybernetickou a informační bezpečnost, www.nukib.gov.cz.

Nezbytné materiální a technické předpoklady pro provedení zkoušky

- Učebna odpovídající bezpečnostním a hygienickým předpisům, stoly, židle,
- psací potřeby, papír,
- soubor 10 případových studií,
- stolní počítač nebo notebook (dostatečně výkonný natolik, aby zajistil plynulý provoz aplikací) s aktuálním operačním systémem, kancelářský software, internetové připojení,
- dataprojektor, plátno, flip-chart.

Uchazeč musí mít na zkušebním zařízení udělena administrátorská práva z důvodu doplnění instalace SW, který používá (zohlednění jeho osobní preference).

K žádosti o udělení autorizace žadatel přiloží seznam materiálně-technického vybavení dokládající soulad s požadavky uvedenými v hodnoticím standardu pro účely zkoušky. Zajištění vhodných prostor pro provádění zkoušky prokazuje žadatel odpovídajícím dokladem (např. výpis z katastru nemovitostí, nájemní smlouva, dohoda).

Doba přípravy na zkoušku

Uchazeč má nárok na celkovou dobu přípravy na zkoušku v trvání 10 minut. Do doby přípravy na zkoušku se nezapočítává doba na seznámení uchazeče s pracovištěm, s organizací zkoušky, s požadavky BOZP a PO a s právy a povinnostmi uchazeče v rámci zkoušky podle zákona č. 179/2006 Sb.

Doba pro vykonání zkoušky

Celková doba trvání vlastní zkoušky jednoho uchazeče (bez času na přípravu a přestávky) je 8 až 10 hodin (hodinou se rozumí 60 minut).

Autoři standardu

Autoři hodnoticího standardu

Hodnoticí standard profesní kvalifikace připravila SR pro informační technologie a elektronické komunikace , ustavená a licencovaná pro tuto činnost HK ČR a SP ČR.

Na tvorbě se dále podílely subjekty zastoupené v pracovní skupině:

- Network Security Monitoring Cluster, družstvo
- AXENTA a. s.
- Jihomoravský kraj