

## Manažer/manažerka kybernetické bezpečnosti (kód: 18-015-T)

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

### Odborná způsobilost

| Název                                                                                                              | Úroveň |
|--------------------------------------------------------------------------------------------------------------------|--------|
| Orientace v legislativě v oblasti kybernetické bezpečnosti pro potřeby manažera/manažerky kybernetické bezpečnosti | 7      |
| Uplatňování principů řízení kybernetické bezpečnosti                                                               | 7      |
| Supervize dokumentace řízení kybernetické bezpečnosti v organizaci                                                 | 7      |
| Řízení aktiv v kybernetické bezpečnosti                                                                            | 7      |
| Řízení rizik kybernetické bezpečnosti pro potřeby manažera/manažerky kybernetické bezpečnosti                      | 7      |
| Zajištění organizační bezpečnosti v oblasti kybernetické bezpečnosti                                               | 7      |
| Řízení rozvoje bezpečnostního povědomí organizace v oblasti kybernetické bezpečnosti                               | 7      |
| Řízení dodavatelů v oblasti kybernetické bezpečnosti                                                               | 7      |
| Řízení provozu a komunikací v oblasti kybernetické bezpečnosti                                                     | 7      |
| Řízení změn v rámci kybernetické bezpečnosti                                                                       | 7      |
| Řízení přístupu a identit v oblasti kybernetické bezpečnosti                                                       | 7      |
| Zajištění bezpečnosti v oblasti akvizice, vývoje a údržby kybernetické bezpečnosti                                 | 7      |
| Vyhodnocování bezpečnostních a provozních událostí v oblasti kybernetické bezpečnosti                              | 7      |
| Koordinace řízení kybernetických bezpečnostních incidentů                                                          | 7      |
| Zajišťování fyzické bezpečnosti v oblasti kybernetické bezpečnosti                                                 | 7      |
| Řízení bezpečnostních opatření v oblasti ochrany před škodlivým kódem v oboru kybernetické bezpečnosti             | 7      |
| Řízení kontinuity činností                                                                                         | 7      |

### Platnost standardu

Standard je platný od: 20.05.2025

## Kritéria a způsoby hodnocení

### Orientace v legislativě v oblasti kybernetické bezpečnosti pro potřeby manažera/manažerky 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 význam a vysvětlit členění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů                                                                                                                                                                                                                                                 | Ústní ověření   |
| d) Popsat alespoň dvě normy z řady ISO 27000, které souvisejí se systémem řízení bezpečnosti informací                                                                                                                                                                                                                                                                                                   | Ústní ověření   |
| e) Popsat význam a vysvětlit členění zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů                                                                                                                                                                                                                                    | Ústní ověření   |
| f) Popsat principy stanovené vyhláškou č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, ve znění pozdějších předpisů                                                                                                                                                                                                                                       | Ústní ověření   |
| g) Popsat a vysvětlit vyhlášku č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu, ve znění pozdějších předpisů                                                                                                                                                                                                                      | Ústní ověření   |

**Je třeba splnit všechna kritéria.**

### Uplatňování principů řízení kybernetické bezpečnosti

| Kritéria hodnocení                                                                                                                                                                                                                                                    | Způsoby ověření                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| a) Prokázat znalost plánování, řízení, měření a zlepšování procesů kybernetické bezpečnosti podle PDCA metodiky (plan-do-check-act/naplánuj-proveď-ověř-jednej)                                                                                                       | Písemné ověření                      |
| b) Graficky znázornit a popsat organizační začlenění kybernetické bezpečnosti v organizaci                                                                                                                                                                            | Písemné a ústní ověření              |
| c) Vysvětlit význam bezpečnostní politiky v oblasti systému řízení bezpečnosti informací                                                                                                                                                                              | Ústní ověření                        |
| d) Prezentovat obsah, formu a postup při návrhu systému řízení bezpečnosti informací včetně návrhů zlepšování podle konkrétního zadání (aplikovat systémový přístup řízení organizace, popsat úlohu vrcholového řízení, reportování systému kybernetické bezpečnosti) | Písemné a ústní ověření              |
| e) Popsat a vysvětlit principy těchto druhů auditů: interní audit, zákaznický audit, audit prováděné třetí stranou, audit procesu, audit služby                                                                                                                       | Ústní ověření                        |
| f) Nastavit alespoň 5 opatření z prohlášení o aplikovatelnosti a zdůvodnit jejich aplikaci v kontextu organizace                                                                                                                                                      | Praktické předvedení a ústní ověření |
| g) Popsat odvození nepřiměřených nákladů podle metodiky NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost)                                                                                                                                                | Ústní ověření                        |

**Je třeba splnit všechna kritéria.**

### Supervize dokumentace řízení kybernetické bezpečnosti v organizaci

| Kritéria hodnocení                                                                                                                                                                                                                                                                                                                                                                        | Způsoby ověření                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| a) Přezkoumat, analyzovat a vyhodnotit úplnost a kvalitu kompletního vzoru bezpečnostní dokumentace organizace v souladu s ustanovením hlavy III (Bezpečnostní politika a bezpečnostní dokumentace), § 30 (Bezpečnostní politika a bezpečnostní dokumentace), odst. (1) a (2) a přílohy 5, bodu 2. (Obsah bezpečnostní dokumentace) vyhlášky č. 82/2018 Sb., ve znění pozdějších předpisů | Praktické předvedení a ústní ověření |
| b) Vysvětlit principy tvorby, udržování a rozvíjení dokumentace systému řízení kybernetické bezpečnosti v organizaci podle konkrétního zadání, v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, ve znění pozdějších předpisů                                                                                | Ústní ověření                        |
| c) Popsat principy a techniky používané pro přezkoumání dokumentace                                                                                                                                                                                                                                                                                                                       | Ústní ověření                        |

**Je třeba splnit obě kritéria.**

### Řízení aktiv v kybernetické bezpečnosti

| Kritéria hodnocení                                                                                                                                                                                                                                                                                                                  | Způsoby ověření                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| a) Graficky znázornit a popsat členění aktiv podle § 2 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat a metodiku pro identifikaci a hodnocení aktiv, ve znění pozdějších předpisů | Písemné a ústní ověření              |
| b) Vyjmenovat a popsat oblasti, které mají být uvažovány při hodnocení aktiv                                                                                                                                                                                                                                                        | Ústní ověření                        |
| c) Určit hodnotu aktiv 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 |

**Je třeba splnit všechna kritéria.**

### Řízení rizik kybernetické bezpečnosti pro potřeby manažera/manažerky kybernetické bezpečnosti

| Kritéria hodnocení                                                                                                                                                                                                                                                                                                                                               | Způsoby ověření                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| a) Popsat metodiku hodnocení rizik podle 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                                                                                          | Ústní ověření                        |
| b) Popsat PDCA cyklus pro řízení rizik podle ISO/IEC 27005                                                                                                                                                                                                                                                                                                       | Ústní ověření                        |
| c) Stanovit hodnotu u aktiv organizace, identifikovat pro ně hrozby a zranitelnosti a vypočítat hodnotu rizika, a to 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.**

### Zajištění organizační bezpečnosti v oblasti kybernetické bezpečnosti

| Kritéria hodnocení                                                                                                                                                                                                                                                                                                        | Způsoby ověření         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| a) Prokázat znalost základních náležitostí a principů fungování systému řízení bezpečnosti informací                                                                                                                                                                                                                      | Písemné ověření         |
| b) Popsat bezpečnostní role podle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat a popsat jejich základní úkoly, pravomoci a odpovědnosti, ve znění pozdějších předpisů | Písemné a ústní ověření |
| c) Popsat a vysvětlit správné zařazení bezpečnostních rolí v organizační struktuře (organizačním řádu)                                                                                                                                                                                                                    | Ústní ověření           |

**Je třeba splnit všechna kritéria.**

### Řízení rozvoje bezpečnostního povědomí organizace v oblasti kybernetické bezpečnosti

| Kritéria hodnocení                                                                                                                                                                                                                                                                                                                                                           | Způsoby ověření                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| a) Vyjmenovat a popsat základní cíle zvyšování bezpečnostního povědomí 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                                                           | Písemné a ústní ověření              |
| b) Vyjmenovat a popsat různé způsoby a formy zvyšování bezpečnostního povědomí 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                                                   | Písemné a ústní ověření              |
| c) Popsat formální náležitosti vyplývající z vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat v oblasti zajištění bezpečnosti lidských zdrojů (především plán rozvoje bezpečnostního povědomí), ve znění pozdějších předpisů | Ústní ověření                        |
| d) Sestavit plán rozvoje bezpečnostního povědomí organizace                                                                                                                                                                                                                                                                                                                  | Praktické předvedení a ústní ověření |

**Je třeba splnit všechna kritéria.**

### Řízení dodavatelů v oblasti kybernetické bezpečnosti

| Kritéria hodnocení                                                                                                                                                                                                                                                                                                                                                                                                                                    | Způsoby ověření |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| a) Vyjmenovat základní povinnosti povinné osoby (v souvislosti se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů) pro řízení dodavatelů 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) Vyjmenovat povinnosti povinné osoby (v souvislosti se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů) pro významné dodavatele 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   |
| c) Podle konkrétního zadání uvést náležitosti zakotvené ve smluvních vztazích s významnými dodavateli a demonstrovat je, 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 provozu a komunikací v oblasti kybernetické bezpečnosti

| Kritéria hodnocení                                                                                                                                                                                                                                                                                                                                      | Způsoby ověření                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| a) Uvést alespoň pět pravidel a postupů v rámci řízení provozu a komunikací v organizaci podle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat a aplikovat tato pravidla, ve znění pozdějších předpisů | Praktické předvedení a ústní ověření |
| b) Popsat, na čem je založen soubor praxí ITIL (Information Technology Infrastructure Library)                                                                                                                                                                                                                                                          | Ústní ověření                        |
| c) Popsat problematiku poskytování služeb v cloudu s ohledem na zajištění vhodné úrovně kybernetické bezpečnosti                                                                                                                                                                                                                                        | Ústní ověření                        |

**Je třeba splnit všechna kritéria.**

### Řízení změn v rámci kybernetické bezpečnosti

| Kritéria hodnocení                                                                                                                                                                                                                                                                                                                | Způsoby ověření                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| a) Popsat význam termínu významná změna 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) Popsat analýzu rizik a zavedení opatření u významných změn 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                        |
| c) Popsat principy a účel penetračního testování a testování zranitelností 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) Rozhodnout o provedení penetračního testování a stanovit postup v rámci 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 |

**Je třeba splnit všechna kritéria.**

### Řízení přístupu a identit v oblasti kybernetické bezpečnosti

| Kritéria hodnocení                                                                                                                                                                                                                                                                                                           | Způsoby ověření |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| a) Popsat cíl a příklady opatření v oblasti řízení přístupů a identit 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) Uvést příklad možné implementace opatření v oblasti řízení přístupu a identit 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   |
| c) Uvést, jaké autentizační mechanismy a jejich vynucovací pravidla lze využít pro ověření identity                                                                                                                                                                                                                          | Ústní ověření   |

**Je třeba splnit všechna kritéria.**

### Zajištění bezpečnosti v oblasti akvizice, vývoje a údržby kybernetické bezpečnosti

| Kritéria hodnocení                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Způsoby ověření |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| a) Popsat cíl bezpečnostních opatření v oblasti akvizice, vývoje a údržby, 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, pro zadanou 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   |
| b) Popsat proces provádění bezpečnostního testování významných změn před jejich nasazením do provozu, 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 obě kritéria.**

### Vyhodnocování bezpečnostních a provozních událostí v oblasti kybernetické bezpečnosti

| Kritéria hodnocení                                                                                                                                                                                                                                                                                                                                                                                   | Způsoby ověření |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| a) Popsat cíl vyhodnocování bezpečnostních a provozních událostí v organizaci 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; demonstrovat na příkladu omezení případů nesprávného vyhodnocení událostí | Ústní ověření   |
| b) Popsat postupy pro detekci a vyhodnocování kybernetických bezpečnostních událostí a incidentů, jejich koordinaci a zvládání v organizaci 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 obě kritéria.**

### Koordinace řízení kybernetických bezpečnostních incidentů

| Kritéria hodnocení                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Způsoby ověření                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| a) Popsat metody detekce a zvládání kybernetických bezpečnostních incidentů                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Ústní ověření                        |
| b) Popsat metody zjišťování útoků na informační a komunikační technologie a metody monitorování kybernetické bezpečnosti, popsat vedení záznamů v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů a 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 | Písemné a ústní ověření              |
| c) Vysvětlit způsoby zvládání kybernetických bezpečnostních incidentů a způsoby vedení záznamů s tím souvisejících včetně návaznosti na ostatní procesy organizace                                                                                                                                                                                                                                                                                                                                                          | Ústní ověření                        |
| d) Demonstrovat zvládání kybernetického bezpečnostního incidentu, a to 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.**

### Zajišťování fyzické bezpečnosti v oblasti kybernetické bezpečnosti

| Kritéria hodnocení                                                                                                                                                                                                                                                                                               | Způsoby ověření |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| a) Popsat cíl bezpečnostních opatření v oblasti fyzické 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) Představit příklad možné aplikace vhodného bezpečnostního opatření                                                                                                                                                                                                                                            | Ústní ověření   |

**Je třeba splnit obě kritéria.**

### Řízení bezpečnostních opatření v oblasti ochrany před škodlivým kódem v oboru kybernetické bezpečnosti

| Kritéria hodnocení                                                                                                                                                                                                                                                                                                        | Způsoby ověření |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| a) Popsat cíl bezpečnostních opatření v oblasti ochrany před škodlivým kódem, 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) Popsat důvody pro pravidelnou aktualizaci nástroje pro ochranu před škodlivým kódem                                                                                                                                                                                                                                    | Ústní ověření   |
| c) Vyjmenovat alespoň 3 typy malware a krátce je popsat                                                                                                                                                                                                                                                                   | Ústní ověření   |

**Je třeba splnit všechna kritéria.**



## Řízení kontinuity činností

| Kritéria hodnocení                                             | Způsoby ověření |
|----------------------------------------------------------------|-----------------|
| a) Vysvětlit principy tvorby analýzy dopadů (BIA)              | Ústní ověření   |
| b) Objasnit tvorbu plánů kontinuity (BCP) a plánů obnovy (DRP) | Ústní ověření   |
| c) Představit základní typy testování BCP a DRP                | Ústní ověření   |

**Je třeba splnit všechna 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 započítáním 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 realizaci zkoušky popsané v hodnoticím standardu. Zkoušející tyto odborné způsobilosti neuznává jako již ověřené, pokud by tím nebylo zajištěno řádné ověření ostatních požadavků stanovených tímto hodnoticím 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 „**písemné ověření**“:

Uchazeč v první části zkoušky prokáže znalosti písemným testem (rozsah 45 minut, 20 otázek).

Pravidla pro aplikaci testů:

Musí přitom splňovat následující pravidla:

- Testy pro jednotlivé uchazeče musí být vygenerovány z dostatečně velkého souboru otázek, aby bylo možné vytvářet dostatečné počty různě sestavených testů.
- Při každé zkoušce musí být ověřeny všechny odborné způsobilosti.
- Každý uchazeč má ve svém testu pro každé kritérium, u kterého je uveden písemný způsob ověření, alespoň jednu otázku.

Za úspěšné splnění testu se považuje 70 % správně zodpovězených otázek s tím, že pro každé kritérium musí být správně zodpovězeno alespoň 50 % otázek.

Autorizovaná osoba vypracuje soubor 60 otázek, z nichž náhodným výběrem zvolí 20 testových otázek zaměřených na ověření znalostní složky vybrané odborné způsobilosti:

- *Uplatňování principů řízení kybernetické bezpečnosti*, kritérium a) 10 otázek z 30
- *Zajištění organizační bezpečnosti v oblasti kybernetické bezpečnosti*, kritérium a) 10 otázek z 30

Testové otázky budou uzavřené, sestavené ze tří variant odpovědí, z nichž pouze jedna je správná. Všechny otázky jsou bodově rovnocenné.

Autorizovaná osoba zajistí, aby všichni uchazeči plnili test zcela samostatně. V daném termínu před danou zkušební komisí mohou absolvovat test najednou všichni uchazeči. Přítomnost obou členů zkušební komise po celou dobu písemného ověřování je vyžadována.

Kritéria hodnocení, u kterých je jako způsob ověření uvedeno „**písemné ověření a ústní ověření**“:

Autorizovaná osoba vypracuje soubor 35 zadání určených pro splnění následujících kritérií ve složení:

- *Uplatňování principů řízení kybernetické bezpečnosti*, kritérium b) 5 zadání
- *Uplatňování principů řízení kybernetické bezpečnosti*, kritérium d) 5 zadání
- *Řízení aktiv v kybernetické bezpečnosti*, kritérium a) 5 zadání
- *Zajištění organizační bezpečnosti v oblasti kybernetické bezpečnosti*, kritérium b) 5 zadání
- *Zajištění bezpečnosti lidských zdrojů v oblasti kybernetické bezpečnosti*, kritérium a) 5 zadání
- *Zajištění bezpečnosti lidských zdrojů v oblasti kybernetické bezpečnosti*, kritérium b) 5 zadání
- *Koordinace řízení kybernetických bezpečnostních incidentů*, kritérium b) 5 zadání

Autorizovaná osoba zajistí náhodný výběr jednoho zadání pro každé z výše uvedených kritérií.

Uchazeč podle zadání vypracuje písemnou odpověď a obhájí ji v ústním ověření. Na vypracování písemných odpovědí má uchazeč 40 minut.

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,
- kritéria jsou ověřována prostřednictvím případové studie. Autorizovaná osoba vytváří celkem 10 případových studií, z nichž si uchazeč jednu vylosuje a ve kterých je vždy uvedeno:
  - 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,
  - definici informační a komunikační infrastruktury organizace,
  - přehled primárních a podpůrných aktiv organizace s uvedením vazeb.

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.

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 trvání zkoušky.

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 a přílohy č. 6 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 manažera 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](http://www.nukib.gov.cz).

## Nezbytné materiální a technické předpoklady pro provedení zkoušky

- Učebna odpovídající bezpečnostním a hygienickým předpisům, stoly, židle,
- psací potřeby, papír,
- soubor testových otázek a 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 9 hodin (hodinou se rozumí 60 minut). Celková doba trvání písemné části zkoušky jednoho uchazeče je 45 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