Príloha č. 2 Podrobný opis predmetu zákazky

Názov predmetu zákazky

Školenie manažérov kybernetickej bezpečnosti a informačnej bezpečnosti (školiace aktivity)

Obsah

1 Úvod, účel a cieľ

Účelom tohto verejného obstarávania, realizovaného v rámci implementácie Reformy č. 5 Skvalitnenie vzdelávania a zabezpečenie spôsobilosti v oblasti KIB (Plán obnovy a odolnosti, Komponent 17: Digitálne Slovensko), je zabezpečiť zvyšovanie odbornosti v oblasti kybernetickej bezpečnosti ďalej definovanej cieľovej skupiny zamestnancov z prostredia verejnej a štátnej správy.

Cieľom verejného obstarávania je realizácia školiacich aktivít, a to formou školiacich aktivít, seminárov, ktoré budú realizované pre skupinu zamestnancov verejnej správy bližšie špecifikovanú v kapitole 2 (Cieľová skupina zamestnancov verejnej a štátnej správy) tohto dokumentu. Súčasťou realizácie školiacich aktivít bude aj poskytnutie podporných vzdelávacích materiálov pre školených zamestnancov verejnej správy. Verejný obstarávateľ požaduje realizáciu školiacich aktivít s poskytnutím podporných vzdelávacích materiálov maximálne po dobu 27 mesiacov od účinnosti zmluvy, ktorá bude výsledkom verejného obstarávania, resp. v súlade s harmonogramom zákazky, ktorý je opísaný v kapitole 5 tohto dokumentu.

1.1 Východiskový stav

Aktuálne nie sú v prostredí verejnej a štátnej správy dostupné školiace aktivity, ktoré by boli komplexne zamerané na zvýšenie znalostných štandardov v oblasti kybernetickej bezpečnosti u cieľovej skupiny zamestnancov špecifikovaných v kapitole 2 (Cieľová skupina zamestnancov verejnej a štátnej správy) tohto dokumentu na požadovanú úroveň.

1.2 Cieľ zákazky

Hlavným cieľom reformy Skvalitnenie vzdelávania a zabezpečenie spôsobilosti v oblasti KIB je zvýšiť znalostné štandardy v oblasti kybernetickej bezpečnosti, u definovanej cieľovej skupiny zamestnancov verejnej a štátnej správy špecifikovaných v kapitole 2 (Cieľová skupina zamestnancov verejnej a štátnej správy) tohto dokumentu, na požadovanú úroveň, a to prostredníctvom realizácie definovaných školiacich aktivít.

1.3 Definície a skratky

- EÚ - Európska únia
- KB - kybernetická bezpečnosť
- KIB - kybernetická a informačná bezpečnosť
- KIKSS - Klasifikácia informácií a kategorizácia systémov a sietí
- MKB - manažér kybernetickej bezpečnosti
- NBÚ - Národný bezpečnostný úrad
- OVM - orgán verejnej moci
- RR – riadenie rizík
- ZVO – Zákon č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

2 Podrobný opis predmetu zákazky

Verejný obstarávateľ požaduje zabezpečiť zvýšenie odbornosti v oblasti kybernetickej a informačnej bezpečnosti u definovanej cieľovej skupiny zamestnancov verejnej a štátnej správy špecifikovaných v kapitole 2 (Cieľová skupina zamestnancov verejnej správy) tohto dokumentu a to na, v tomto dokumente definovanú, požadovanú úroveň prostredníctvom nasledovných aktivít:

- realizácia školiacich aktivít pre cieľovú skupinu zamestnancov verejnej správy v oblasti kybernetickej a informačnej bezpečnosti, a
- dodanie podporných vzdelávacích materiálov pre cieľovú skupinu zamestnancov verejnej správy, ktoré budú obsahovať základné informácie a okruhy, ktoré budú predmetom realizácie vyššie uvedených školiacich aktivít.

Celkové trvanie zmluvy sa požaduje na obdobie 27 mesiacov odo dňa jej účinnosti, resp. v súlade s harmonogramom zákazky, ktorý je opísaný v kapitole 5 tohto dokumentu.

2.1 Cieľová skupina zamestnancov verejnej a štátnej správy

Cieľová skupina zamestnancov za oblasť kybernetickej a informačnej bezpečnosti pôsobiacich v orgánoch verejnej a štátnej správy je koncipovaná nasledovne:

- primárne: kategória používateľov *„manažér v kybernetickej bezpečnosti“,* a
- sekundárne: kategória používateľov *„IT manažér“, „informatik“, „zamestnanec v kybernetickej bezpečnosti“*[1].

Obsah, rozsah a úroveň školiacich aktivít budú teda primárne určené požiadavkami na znalostné štandardy[2] výhradne kategórie používateľov „manažér v kybernetickej bezpečnosti“, bez ohľadu na vyššie uvedené sekundárne kategórie skupiny zamestnancov, ktorí sa budú zúčastňovať školenia. Primárna kategória používateľov určuje požiadavky na obsah, rozsah a úroveň školiacich aktivít a podporných vzdelávacích materiálov.

Cieľová skupina zamestnancov z oblasti verejnej a štátnej správy pozostáva z celkového predpokladaného počtu 571 zamestnancov OVM (ide zároveň o maximálny počet preškolených zamestnancov, ktorí budú predmetom školiacich aktivít, z toho:

Modul 1: celkový predpokladaný a maximálny počet 200 zamestnancov,

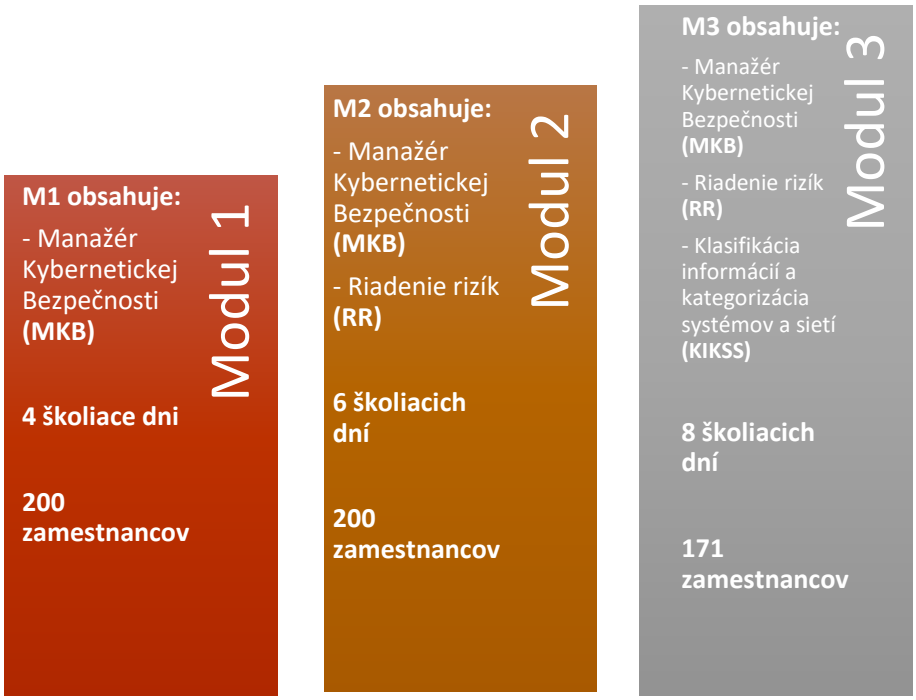
Modul 2: celkový predpokladaný a maximálny počet 200 zamestnancov,

Modul 3: celkový predpokladaný a maximálny 171 zamestnancov.

[1] Kategórie používateľov v zmysle prílohy č. 1 Vyhlášky Národného bezpečnostného úradu č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti

[2] Znalostné štandardy pre konkrétnu rolu sú uvedené v prílohe č. 5 s účinnosťou od 01.01.2024. Dostupné na: https://www.slov-lex.sk/pravne-predpisy/prilohy/SK/ZZ/2022/492/20240101_5495669-2.pdf

Každý zamestnanec OVM môže absolvovať max. jeden z modulov. Cieľ je preškoliť celkom 571 jednotlivcov s úspešným ukončením záverečného testu/skúšky. Pre vysvetlenie uvádzame, že obsahová náplň Modul 1 je súčasťou Modulu 2 a obsahová náplň Modul 2 je súčasťou Modulu 3 z tohto dôvodu nie je možné, aby rovnaký zamestnanec absolvoval viac ako jeden modul. Prihlásenie jednotlivých zamestnancov OVM na vzdelávacie aktivity podlieha schváleniu Osobného úradu (resp. ekvivalent podľa typu a organizačnej štruktúry OVM) každého OVM, ktorý verejný obstarávateľ vopred informuje o realizácii školení. Týmto krokom sa zamedzí prihlásenie uchádzačov, ktorí nespadajú do opisu cieľovej skupiny pre účely plnenia predmetu zmluvy.



Obrázok 1 Grafické znázornenie rozdelenia cieľovej skupiny zamestnancov OVM

2.2 Požiadavky na školiace aktivity

Verejný obstarávateľ požaduje, aby školiace aktivity boli realizované prezenčnou formou (napr. semináre a i.) a poskytované expertmi v oblasti kybernetickej bezpečnosti. Počet expertov zabezpečujúcich školiace aktivity ponecháva verejný obstarávateľ na uchádzačovi, tzn. či školenie bude realizovať v priebehu dňa jeden alebo viacerí lektori. Uvedené rovnako platí aj na jednotlivé časti modulov č. 1 až 3.

Verejný obstarávateľ požaduje, aby prvá školiaca aktivita bola realizovaná najneskôr do 1 mesiaca odo dňa účinnosti zmluvy, až po dobu ukončenia projektu, t. j. do uplynutia 27 mesiacov od účinnosti zmluvy.

Verejný obstarávateľ požaduje, aby školiace aktivity obsahovali všetky informácie nevyhnutné pre dosiahnutie špecifických cieľov zvyšovania znalostných štandardov, v súlade s tým ako je to definované v kapitole 3.1 (Požiadavky na obsahové náležitosti školiacich aktivít) tohto dokumentu.

Zároveň školiace aktivity musia zohľadňovať požiadavky vyplývajúce z legislatívneho rámca kybernetickej bezpečnosti a legislatívneho rámca ochrany osobných údajov, v súlade ako sú definované v kapitole 4 tohto dokumentu.

Každý zo školiacich seminárov musí spĺňať nasledovné náležitosti:

Verejný obstarávateľ bližšie špecifikuje metódy, formy a rozsahu vzdelávacích aktivít:

- **Modul 1:** Metóda výučby bude praktická s ukážkami a cvičeniami prezenčnou formou, podľa charakteru každého školenia.
  - v rozsahu 4 školiacich dní (t. j. v rozsahu 32 hodín) v štruktúre:
    - 2 dni formou školenia (zamerané na získanie teoretických znalostí),
    - 2 dni formou workshopu (interaktívna forma realizovaná s účastníkmi seminára zameraná na praktickú aplikáciu znalostí a zručností získaných v teoretickej časti semináru).
- **Modul 2:** Metóda výučby bude praktická s ukážkami a cvičeniami prezenčnou formou, podľa charakteru každého školenia.
  - v rozsahu 6 školiacich dní (t. j. v rozsahu 48 hodín) v štruktúre:
    - 3 dni formou školenia (zamerané na získanie teoretických znalostí),
    - 3 dni formou workshopu (interaktívna forma realizovaná s účastníkmi seminára zameraná na praktickú aplikáciu znalostí a zručností získaných v teoretickej časti semináru).
- **Modul 3:** Metóda výučby bude praktická s ukážkami a cvičeniami prezenčnou formou, podľa charakteru každého školenia.
  - v rozsahu 8 školiacich dní (t. j. v rozsahu 64 hodín) v štruktúre:
    - 4 dni formou školenia (zamerané na získanie teoretických znalostí),
    - 4 dni formou workshopu (interaktívna forma realizovaná s účastníkmi seminára zameraná na praktickú aplikáciu znalostí a zručností získaných v teoretickej časti semináru).

Pre vysvetlenie uvádzame doplňujúce požiadavky na predmet zákazky:

- jeden školiaci deň znamená spravidla 7 výukových hodín a navyše 1 hodinu prestávky na obed a/alebo občerstvenie,
- jazyk vzdelávacej aktivity bude slovenský jazyk alebo český jazyk,
- min. počet účastníkov jednej vzdelávacej aktivity 5 účastníkov a max. počet účastníkov jednej vzdelávacej aktivity 12,
- realizácia seminárov v pracovné dni v časovom rozmedzí od 08:00 do 18:00, v ktorom je zahrnutá aj obedňajšia prestávka v trvaní 60 min, ale nie je súčasťou rozsahu výukových hodín, výukovou hodinou sa rozumie 45 minút,
- realizácia seminárov vo všetkých ôsmych krajských mestách, pričom v každom krajskom meste sa bude seminár realizovať vo vyššie uvedenom predpokladanom min. alebo max. počte účastníkov a to v max. v šiestich termínoch v každom krajskom meste. Presné počty a alternatívne termíny konania školení v príslušných krajských mestách určí bližšie verejný obstarávateľ na základe záujmu zo strany účastníkov podľa záujmu v krajskom meste,
- zo strany verejného obstarávateľa je na základe vyššie uvedeného možná zmena predpokladaného počtu a zároveň maximálneho seminárov v jednotlivých krajských mestách bez vplyvu na cenovú ponuku,

- semináre sa bude môcť konať aj na inom mieste, ako je krajské mesto, so zreteľom na geografickú dostupnosť pre zamestnancov OVM,
- termíny vzdelávacích aktivít v rámci jednotlivých modulov budú dohodnuté po nadobudnutí účinnosti zmluvy, tak aby bol dodržaný predpoklad, že medzi jednotlivými školiacimi dňami rovnakej školiacej aktivity by nemal byť odstup viac ako 14 kalendárnych dní, ak sa účastníci nedohodnú inak,
- Online výučba bude prípustná len po výslovnom schválení verejného obstarávateľa. Rovnako, ako prezenčná forma výučby, nesmie celkovo presiahnuť maximálny počet 12 účastníkov. Online forma výučby môže dosiahnuť max. 25 % celkového rozsahu vzdelávacej aktivity. Verejný obstarávateľ však odporúča, aby každý termín seminára bol účastníkmi plne obsadený,
- prihlasovania sa zamestnancov z cieľovej skupiny špecifikovanej v kapitole 2 (Cieľová skupina zamestnancov verejnej a štátnej správy) v stanovených termínoch prostredníctvom elektronického rezervačného systému,
- rezervačný systém musí zabezpečovať nasledujúcu funkcionalitu z pohľadu zamestnanca: prihlásenie a odhlásenie zamestnanca na zvolený termín vzdelávacej aktivity, odosielanie potvrdzujúcich e-mailových správ o všetkých zmenách na prihláške k zvolenému termínu a taktiež musí zabrániť duplicitnej registrácii, prihlásení sa rovnakého zamestnanca na iné termíny. Po úspešnom prihlásení zamestnanca na vybraný termín vzdelávacej aktivity sa stav jeho prihlášky v rezervačnom systéme zmení na „prihlásený“,
- za jedinečný identifikátor zamestnanca sa pre účely tejto zákazky považuje e-mailová adresa zamestnanca,
- overenie každého prihláseného zamestnanca u zamestnávateľa (kontaktná osoba Osobného úradu alebo ekvivalent) v nasledovnom rozsahu: meno, priezvisko, názov zamestnávateľa a pracovné zaradenie, či zamestnanec spadá do cieľovej skupiny uvedenej v kapitole 2 (Cieľová skupina zamestnancov kybernetickej a informačnej bezpečnosti) tohto dokumentu. Po úspešnom overení sa stav prihlášky prihláseného zamestnanca v rezervačnom systéme zmení na „overený“,
- rezervačný systém musí zabezpečovať nasledujúcu funkcionalitu pre verejného obstarávateľa: prihlásenie a odhlásenie zamestnanca na zvolený termín vzdelávacej aktivity, schválenie, zamietnutie prihlášky zamestnanca na vybraný termín, export zoznamu účastníkov, zamestnancov vo formáte Microsoft Excel (*.xlsx), alebo ekvivalent (napr. formáty openoffice, *.csv). Po úspešnom schválení sa stav prihlášky prihláseného zamestnanca v rezervačnom systéme zmení na „schválený“.
- zamestnanec bol informovaný o každej zmene jeho prihlášky (prihlásený/odhlásený, overený/neoverený, schválený/neschválený) e-mailom. Zamestnanec sa môže zúčastniť vzdelávacej aktivity, iba po schválení verejným obstarávateľom,
- súčasťou každého semináru bude písomný záverečný test, ktorý zhodnotí nadobudnuté vedomosti a zručnosti individuálne pre každého z účastníkov. Za úspešné ukončenie vzdelávania a získanie osvedčenia k jednotlivým vzdelávacím seminárom sa považuje, ak účastník získa minimálne 70 % z celkového počtu (maximálne 60) bodov v záverečnom teste,
- písomný záverečný test musí obsahovať minimálne 30 otázok zameraných na obsahové náležitosti ako sú definované v kapitole 3.1 (Požiadavky na obsahové náležitosti podporných vzdelávacích materiálov a školiacich aktivít) tohto dokumentu,

— verejný obstarávateľ požaduje vyhotoviť min. tri rôzne varianty záverečného testu[3], každá otázka musí obsahovať aspoň 3 možné odpovede, pričom len jedna odpoveď je správna,
— každý účastník vzdelávacej aktivity má právo na jedno opakovanie záverečného testu, ktoré bude finančne kryté a zahrnuté v celkovej cene zákazky a verejnému obstarávateľovi nevzniknú iné nepredvídateľné náklady súvisiace s potvrdením uchádzačov pri absolvovaní kurzu,
— po úspešnom absolvovaní záverečného testu účastníkom seminára mu bude vydané písomné osvedčenie o absolvovaní tohto seminára.

Verejný obstarávateľ v súvislosti s každou školiacou aktivitou, seminárom zabezpečí nasledovné:

— zabezpečenie vhodného školiaceho priestoru pre max. 12 účastníkov a školiteľov na realizáciu školiaceho semináru (napr. prostredníctvom prenájmu školiaceho priestoru alebo vlastného školiaceho priestoru), vrátane príslušného technického zariadenia potrebného pre zabezpečenie prezentačných materiálov školiteľom (napr. notebook, projektor s plátnom alebo iné, v závislosti od potrieb vybavenia konkrétnej vzdelávacej aktivity),
— zvolený priestor bol dostupný hromadnou dopravou, a to maximálne do 30 min od najbližšej zastávky MHD a musí mať dostupnú kapacitu na parkovanie v počte zodpovedajúcom počtu účastníkov seminára alebo možnosťou parkovania v blízkom okolí maximálne do 500 m.
— zabezpečenie občerstvenia v každý školiaci deň počas celého semináru a pre všetkých účastníkov semináru (max. 12 + školitelia) (vrátane jeho príslušného finančného pokrytia) v min. rozsahu:
    - coffee break – 2 krát počas školenia
        - 7 g káva, cukor, kapucín
        - čaj - rôzne druhy, med, citrón
        - fl. 0,3 l minerálka perlivá/ neperlivá v pomere 50:50
        - fl. 0,25 l nealko ochutený nápoj /coca cola, cappy, vinea a pod./
        - 60 g slané kanapky/os.
        - 60 g sladké pečivo/os.
    - obed v min. rozsahu:
        - min. 0,33 l polievky - 2 druhy na výber
        - min. 250 g teplé jedlá 3 druhov s prílohou (minimálne dve mäsité jedlá s min. 150 g mäsa/os. a jedno bezmäsité jedlo)
        - min. 130 g zeleninový šalát alebo ovocný kompót (šalát z čerstvej zeleniny/sterilizovaný, ovocný kompót s podielom pevnej zložky minimálne 80 g),
        - chlieb, resp. pečivo 100 g/os.
        - Min. 90 g dezert/os.

Program vzdelávacej aktivity spolu s ponukou a možnosťou výberu stravovania pre účastníkov požadujeme zaslať min. 3 dni pred realizáciou vzdelávacej aktivity.

— Coffe breaky požadujeme zabezpečiť v rámci priestorov školenia. Obedy formou napr. bufetových stolov v mieste konania semináru alebo v jeho blízkom okolí do maximálnej vzdialenosti 500 m od miesta konania vzdelávacej aktivity.

[3] Príklady štruktúry otázok na skúšku manažéra kybernetickej bezpečnosti, aktuálne dostupné na: https://www.nbu.gov.sk/wp-content/uploads/2022/02/priklady-otazok-skuska-MKB.pdf

Vzdelávacie aktivity sa považujú za zrealizované vykonaním vzdelávacích aktivít v stanovenom počte a rozsahu. V prípade úspešného zvládnutia záverečného testu aj vydaním osvedčenia o absolvovaní vzdelávacej aktivity zamestnancovi cieľovej skupiny. Osvedčenie o absolvovaní vzdelávacej aktivity musí byť vydané účastníkovi vzdelávacej aktivity v posledný deň vzdelávacej aktivity a po úspešnom absolvovaní a vyhodnotení záverečného testu.

Úspešné absolvovanie záverečného testu nie je podmienkou pre ukončenie vzdelávacej aktivity, ale je potvrdenie, že účastník, zamestnanec zvládol preberanú tematiku v stanovenom štandarde. Každý zamestnanec je zodpovedný svojim prístupom k vzdelávacej aktivite a štúdiom tak, aby úspešne zvládol záverečný test podľa svojich možností a schopností. Ukončenie vzdelávacej aktivity bez úspešného ukončenia záverečného testu nie je prekážkou k úhrade za predmetné školenie za konkrétneho zamestnanca.

2.3 Požiadavky na podporné vzdelávacie materiály

Podporné vzdelávacie materiály budú:

- dostupné v písomnej forme, a to v papierovej podobe v počte 1 výtlačok pre účastníka školiaceho seminára. Podporné vzdelávacie materiály musia v maximálnej miere obsahovať požiadavky na obsahové náležitosti zahrnuté v bode 3.1 tohto dokumentu.
- vypracované a dodané pred samotnou realizáciou stanovených termínov školiacich aktivít v zmysle kapitoly 2.2 (Požiadavky na školiace aktivity) tohto dokumentu, t. j. najneskôr v deň začatia predmetného školiaceho seminára, ktorého sa príslušný zamestnanec z cieľovej skupiny zúčastní.
- obsahovať všetky informácie a náležitosti nevyhnutné pre dosiahnutie špecifických cieľov zvyšovania znalostných štandardov, ako sú definované v kapitole 3.1 (Požiadavky na obsahové náležitosti vzdelávacích materiálov a školiacich aktivít) tohto dokumentu.
- zohľadňovať požiadavky vyplývajúce z legislatívneho rámca kybernetickej bezpečnosti a legislatívneho rámca ochrany osobných údajov, ako sú definované v kapitole 4 (Legislatívne požiadavky) tohto dokumentu.

Verejný obstarávateľ požaduje dodanie, okrem vyššie uvedených podporných vzdelávacích materiálov v papierovej podobe aj v podobe elektronickej v rozsahu min. 30 normostrán (resp. minimálne 90 „slidov“ elektronickej prezentácie ku každému modulu, ktorý je uvedený v časti 2.2 (Požiadavky na školiace aktivity), v tlačenej farebnej verzii.

Verejný obstarávateľ požaduje najneskôr v deň realizácie prvej vzdelávacej aktivity doručiť elektronickou formou všetky podporné vzdelávacie materiály, vrátane testov a ostatných materiálov použitých. V prípade zmien, aktualizácii alebo inej úpravy vzdelávacích podporných materiálov je úspešný uchádzač povinný doručiť takto upravené materiály verejnému obstarávateľovi čo najskôr, najneskôr však v deň, kedy sa aktualizované verzie podporných vzdelávacích materiálov začnú používať.

3 Špecifické požiadavky

3.1 Požiadavky na obsahové náležitosti vzdelávacích materiálov a školiacich aktivít

Školiace aktivity, ako aj podporné vzdelávacie materiály, musia spĺňať všetky legislatívne požiadavky, ktoré sú nevyhnutné pre:

— naplnenie vzdelávacích cieľov pre kategóriu používateľov „manažér v kybernetickej bezpečnosti“ vrátane všetkých kategórií [4],
— zabezpečenie zvyšovania odbornosti k dosiahnutiu znalostných štandardov pre rolu „manažér kybernetickej bezpečnosti“[5], t. j. zabezpečenie získania príslušných vedomostí a nadobudnutia príslušných zručností, a
— zabezpečenie získania znalostí a zručností v zmysle Certifikačnej schémy overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti[6].

Informácie špecifikované vyššie v tejto kapitole dokumentu budú členené do nasledovných logických celkov, v zmysle požiadaviek certifikačnej schémy overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti:

Modul 1: Manažér KB

Vzdelávacie aktivity v rámci Modulu 1 sú zamerané minimálne na získanie znalosti a zručnosti týkajúcich sa:

— procesov a systému riadenia informačnej a kybernetickej bezpečnosti,
— zásad organizácie informačnej a kybernetickej bezpečnosti,
— zásad personálnej bezpečnosti,
— zásad riadenia prístupov a identít,
— spôsobu používania kryptografických bezpečnostných mechanizmov,
— princípov testovania kybernetickej bezpečnosti,
— právnych predpisov a noriem vzťahujúcich sa na oblasť kybernetickej bezpečnosti (bližšia špecifikácia viď kapitola 4 - Legislatívne požiadavky tohto dokumentu),
— právnych predpisov a požiadaviek na súlad vzťahujúcich sa na oblasť ochrany osobných údajov (bližšia špecifikácia viď kapitola 4 - Legislatívne požiadavky tohto dokumentu),
— návrhu a uplatňovania bezpečnostných stratégií a politík,
— procesov a metodík riadenia rizík,
— postupov analýzy rizík,

[4] Príloha č. 1 vyhlášky Národného bezpečnostného úradu č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti
[5] Príloha č. 5 vyhlášky Národného bezpečnostného úradu č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti
[6] Certifikačná schéma overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti, vydaná Národným bezpečnostným úradom, aktuálne dostupná na https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/NBU-Certifikacna_schema_20200319_v3.4.pdf

— typických hrozieb a postupov pre identifikáciu hrozieb a zraniteľností,
— bezpečnostných mechanizmov,
— princípov podnikovej architektúry, vrátane orientácie v bežne používaných architektúrnych rámcoch,
— procesov riešenia kybernetických bezpečnostných incidentov,
— princípov plánovania havarijnej obnovy prevádzky,
— procesov riadenia kontinuity činností,
— metód posudzovania rizík a schopnosť ich aplikovať v rámci organizácie,
— analýzy a kvantifikácie rizík,
— analýzy a hodnotenia bezpečnostných mechanizmov a riešení.

Modul 2: Manažér Kybernetickej Bezpečnosti (MKB) + riadenie rizík (RR)[7]

Vzdelávacie aktivity v rámci Modulu 2 sú zamerané minimálne na získanie:

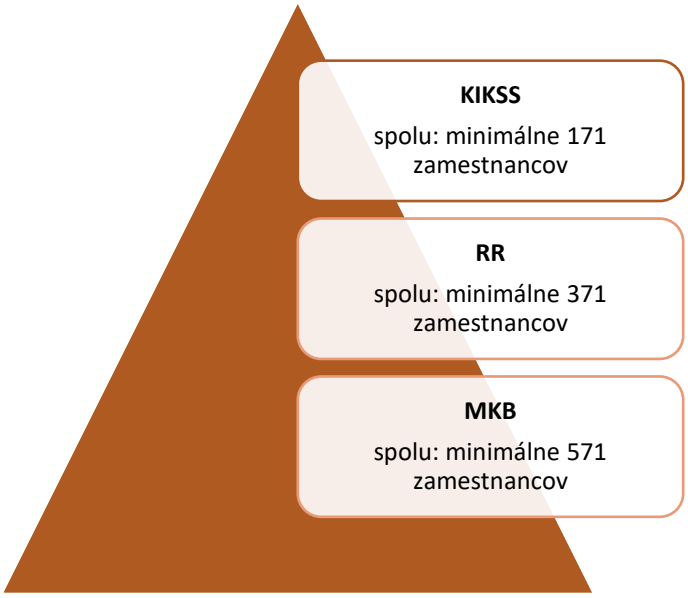
— znalosti uvedených v Module 1, a
— podrobných znalosti a postupov potrebných pre analýzu a riadenie rizík v kybernetickom priestore v zmysle platných právnych predpisov, metodických usmernení regulátora a technických noriem[8]. V rámci praktického workshopu Riadenie rizík v kybernetickej bezpečnosti je formou práce v skupinách osvojenie zručností pri nastavení procesu riadenia rizík a to od identifikácie aktív až po realizáciu vzorovej analýzy rizík s využitím bezpečnostného rámca ISO/IEC 27005.

Modul 3: Manažér Kybernetickej Bezpečnosti (MKB) + riadenie rizík (RR) + klasifikácia informácií a kategorizácia systémov a sietí (KIKSS)[9]

Vzdelávacie aktivity v rámci Modulu 3 sú zamerané minimálne na získanie:

— znalosti uvedených v Module 1 a 2, a
— podrobných znalosti a postupov potrebných pre úspešné uplatnenie klasifikácie informačných aktív a kategorizácie sietí a informačných systémov v organizácii v zmysle platných právnych predpisov, metodických usmernení regulátora a technických noriem. V rámci praktického workshopu Klasifikácia informácií a kategorizácia systémov a sietí (KIKSS) je cieľom poskytnúť uchádzačom základné zručnosti v oblasti, ktoré im umožnia stať sa plnohodnotnými členmi tímov zodpovedných za úspešné uplatnenie klasifikácie informačných aktív a kategorizácie sietí a informačných systémov v organizácii.

[7] Metodika riadenia rizík kybernetickej bezpečnosti – NBÚ, aktuálne dostupné na: https://www.nbu.gov.sk/wp-content/uploads/2021/12/Metodika_analyza_rizik_v1.0_12_2021.pdf
[8] Metodické usmernenie NBÚ, aktuálne dostupné na: https://www.nbu.gov.sk/kyberneticka-bezpecnost/riadenie-rizik/index.html
[9] Vyhláška č. 362/2018 Z. z. upravuje v prílohe č. 2 klasifikačnú schému – štruktúru klasifikácie informácií a kategorizácie sietí a informačných systémov, aktuálne dostupné na: https://www.slov-lex.sk/static/pdf/2018/362/ZZ_2018_362_20190101.pdf



Obrázok 2 Grafické znázornenie rozdelenia cieľovej skupiny zamestnancov OVM podľa plánovaného počtu odškolených zamestnancov v jednotlivých tématických celkoch

3.2 Autorské práva k dodaným podporným vzdelávacím materiálom

Verejný obstarávateľ požaduje, aby vzdelávacie materiály boli poskytnuté uchádzačom vzdelávania v zmysle bodu 2.3 (Požiadavky na podporné vzdelávacie materiály) tohto dokumentu, a taktiež požaduje, oprávnenosť použiť dodané dielo resp. ktorúkoľvek jeho časť (vrátane podporných vzdelávacích materiálov) na akýkoľvek účel v kontexte jemu zverených zákonných kompetencií. Autorské práva k dodaným podporným vzdelávacím materiálom sú predmetom dodania diela.

4 Legislatívne požiadavky

Školiace aktivity ako aj podporné vzdelávacie materiály špecifikované v kapitolách 2.2, 2.3 a 3.1 tohto dokumentu musia zohľadňovať legislatívny rámec pre oblasť kybernetickej bezpečnosti v Slovenskej republike, ktorý je daný najmä nasledovnými právnymi aktami:

a) Právne akty sekundárneho práva Európskej únie
   - Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Smernica NIS) – v kontexte jej transpozície do právneho poriadku Slovenskej republiky,
   - Nariadenie Európskeho parlamentu a Rady (EÚ) 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,
   - Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu,
   - Návrh znenia smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148 (Smernica NIS2) – v kontexte jej transpozície do právneho poriadku Slovenskej republiky
b) Všeobecne záväzné právne predpisy právneho poriadku Slovenskej republiky
   - Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
   - Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
   - Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a doplnení niektorých zákonov v znení neskorších predpisov,
   - Vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
   - Vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
   - Vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov,
   - 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,
   - Vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora,
   - Zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov,

- Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v znení neskorších predpisov,
- Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov,
- Vyhláška Národného bezpečnostného úradu č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti
- Vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti,

c) Ostatné relevantné akty a dokumenty
   - medzinárodné normy rady ISO/IEC 27000 „Informačné technológie - Bezpečnostné metódy - Systémy riadenia informačnej bezpečnosti“ alebo iný obdobný bezpečnostný rámec, spolu s jeho premapovaním na normy rady ISO/IEC 27000.
   - dodržanie Záväzného usmernenia NIKA v súvislosti s informovaním, komunikáciou a viditeľnosťou opatrení Plánu obnovy a odolnosti SR (https://www.planobnovy.sk/realizacia/dokumenty/ , časť Vizibilita) najmä pri príprave podporných vzdelávacích materiálov;

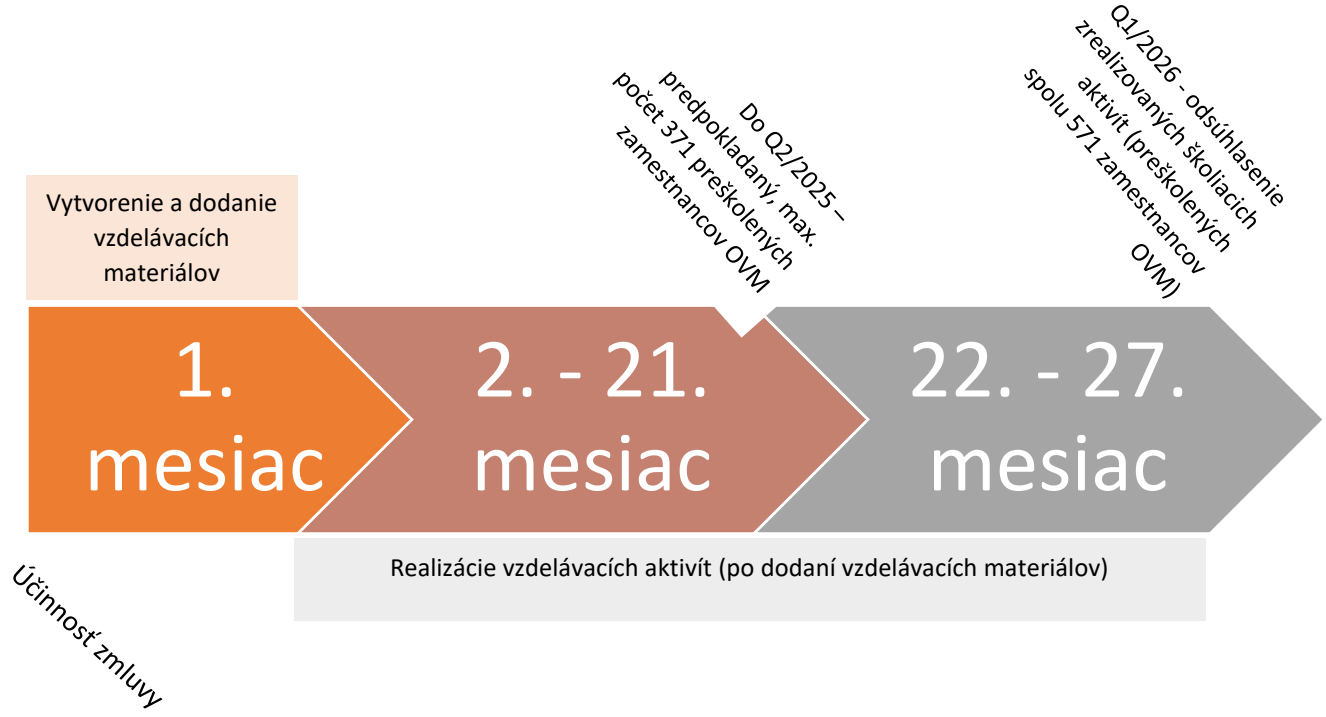
Školiace aktivity ako aj podporné vzdelávacie materiály špecifikované v kapitolách 2.2, 2.3 a 3.1 tohto dokumentu musia zohľadňovať legislatívny rámec pre oblasť ochrany osobných údajov v Slovenskej republike, ktorý je daný najmä nasledovnými právnymi aktami:

a) Právne akty sekundárneho práva Európskej únie
   - Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov),
   - Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) – v kontexte jej transpozície do právneho poriadku Slovenskej republiky
b) Všeobecne záväzné právne predpisy právneho poriadku Slovenskej republiky
   - zákon č. 18/2018 Z. z. o ochrane osobných údajov a o doplnení niektorých zákonov v znení neskorších predpisov,
   - Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov,
   - zákon č. 452/2021 Z. z. o elektronických komunikáciách zákonov v znení neskorších predpisov
c) Ostatné relevantné akty a dokumenty
   - príslušné metodické usmernenia Úradu na ochranu osobných údajov Slovenskej republiky,
   - príslušné metodické usmernenia Výboru na ochranu údajov (EÚ).

5 Harmonogram zákazky

Zákazka bude členená do nasledovných hlavných aktivít:

- vytvorenie podporných vzdelávacích materiálov úspešným uchádzačom /poskytovateľom na základe špecifikácií uvedených v tomto dokumente a ich dodanie účastníkom školiacich aktivít v lehote v zmysle kapitoly 2.3 (Požiadavky na podporné vzdelávacie materiály) tohto dokumentu,
- dodanie podporných vzdelávacích materiálov najneskôr do 1 mesiaca od dátumu účinnosti zmluvy,
- realizáciu školiacich aktivít na základe špecifikácií uvedených v tomto dokumente formou zrealizovania príslušných vzdelávacích aktivít, ktorých výsledkom bude osvedčenie o absolvovaní, ktoré musí vydať úspešný uchádzač príslušnému zamestnancovi (ak zamestnanec úspešne absolvuje záverečný test), pričom presný harmonogram termínov jednotlivých školiacich seminárov bude dohodnutý s víťazným uchádzačom po podpise zmluvy – jednotlivé vzdelávacie aktivity budú realizované v časovom rozmedzí so začiatkom od jedného mesiaca, resp. po dodaní podporných vzdelávacích materiálov, do dátumu konca účinnosti dohody a koncom korešpondujúcim s koncom projektu,
- kontrolný míľnik je stanovený najneskôr na koniec Q2/2025. Do skončenia tohto obdobia musí byť preškolených minimálne 371 zamestnancov OVM.
- odsúhlasenie zrealizovaných školiacich aktivít, do skončenia platnosti zmluvy, najneskôr však do konca Q1/2026 preškolených všetkých 571 zamestnancov OVM.



Obrázok 3 Predpokladaný časový harmonogram zákazky + kontrolné míľniky

6 Podmienky účasti

Splnenie podmienok účasti bude verejný obstarávateľ požadovať preukázať až v rámci riadne vyhláseného verejného obstarávania. Aktuálna výzva sa týka prípravných trhových konzultácií a určenia predpokladanej hodnoty zákazky, z uvedeného dôvodu v tejto fáze záujemca, ktorý bol oslovený so žiadosťou o zodpovedanie otázok v rámci PTK a predloženie cenovej ponuky, nepredkladá žiadne doklady za účelom preukázania splnenia podmienok účasti. (Uvedená informácia môže mať vplyv na určenie ceny, z uvedeného dôvodu je súčasťou tejto výzvy na predkladanie ponúk).

6.1 Požiadavky na kľúčových expertov

Verejný obstarávateľ požaduje od uchádzača údaje o odbornej praxi alebo odbornej kvalifikácii osôb zodpovedných za poskytnutie služby (kľúčových expertov) formou predloženia profesijných životopisov podpísaných dotknutou osobou a predložením požadovaných dokladov.

Každý uchádzačom predložený profesijný životopis alebo ekvivalentný doklad, podpísaný dotknutou osobou, musí obsahovať minimálne:

- meno a priezvisko príslušného kľúčového experta,
- najvyššie dosiahnuté vzdelanie príslušného kľúčového experta (inštitúcia, od-do, získaný titul/diplom),
- história zamestnania/odbornej praxe príslušného kľúčového experta (zamestnávateľ, trvanie pracovného pomeru/trvanie odbornej praxe/, rok a mesiac od – do, pozícia, ktorú príslušný kľúčový expert zastával),
- praktické skúsenosti príslušného kľúčového experta v oblasti zabezpečenia školenia kybernetickej a informačnej bezpečnosti (názov školenia, stručný opis školenia; obdobie rok a mesiac od - do, kontaktné údaje odberateľa najmä: názov, sídlo, emailový a telefonický kontakt, kde si bude môcť verejný obstarávateľ overiť informácie).
- dátum a podpis príslušného kľúčového experta.

Doklady a dokumenty, ktorými uchádzač preukazuje svoju technickú spôsobilosť alebo odbornú spôsobilosť vyhotovené v inom ako štátnom jazyku, t. j. v inom ako slovenskom jazyku, musia byť predložené v pôvodnom jazyku a súčasne musia byť úradne preložené do štátneho jazyka, t. j. do slovenského jazyka, okrem dokladov predložených v českom jazyku.

Kľúčoví experti, ktorí budú uvedení v ponuke uchádzača sa musia reálne podieľať na plnení predmetu príslušnej časti zákazky. V prípade, že Kľúčový expert nie je zamestnancom uchádzača, v takomto prípade musí uchádzač verejnému obstarávateľovi preukázať, že pri plnení zmluvy bude skutočne používať odborné kapacity tejto osoby, čo uchádzač preukáže zmluvou uzavretou s touto osobou, z ktorej musí vyplývať záväzok osoby, že poskytne plnenie počas celého trvania zmluvného vzťahu. V prípade, že počas plnenia zmluvy dôjde k nahradeniu Kľúčového experta inou osobou, nový Kľúčový expert musí spĺňať minimálnu požadovanú úroveň nahradeného Kľúčového experta vyžadovanú verejným obstarávateľom pri preukazovaní danej podmienky účasti technickej alebo odbornej spôsobilosti.

Uchádzač preukáže požadovaných expertov spôsobom, že na každého uvedeného experta bude prislúchať jedna osoba.

Verejný obstarávateľ požaduje predložiť doklady preukazujúce splnenie tejto podmienky účasti na nasledovných pozíciách:

a. Kľúčový expert pre kapitolu 2.2 (lektor/školiteľ kybernetickej bezpečnosti) (Požiadavky na školiace aktivity):

- minimálny počet 3 Kľúčových expertov (ktorí budú zodpovední za plnenie predmetu zákazky, a ktorí musia spĺňať nasledovné požiadavky:
- Minimálne ukončené vysokoškolské vzdelanie II. stupňa, preukazuje sa prostredníctvom kópie VŠ diplomu
- Musí mať znalosť slovenského alebo českého jazyka na úrovni pracovnej komunikácie (splnenie preukáže údajmi v životopise),
- Minimálne 4 roky odbornej praxe vo vzdelávaní dospelých v oblasti kybernetickej alebo informačnej bezpečnosti na pozícii lektora/školiteľa (splnenie preukáže údajmi v životopise s uvedením kontaktných osôb za účelom možného overenia),
- Expert na pozícii lektor/školiteľ musí spĺňať náležitosti uvádzané v prílohe č. 14 k vyhláške č. 492/2022 Z. z. Národného bezpečnostného úradu – Lektor kybernetickej bezpečnosti[10], preukazuje sa životopisom a uvedením referencií v oblasti lektorovania kybernetickej bezpečnosti
- Musí mať minimálne 5 praktických skúseností (získané v období predchádzajúcich štyroch rokov od vyhlásenia verejného obstarávania), kde v rámci každej skúsenosti s realizáciou školení v pozícií lektora/školiteľa (prezenčnou alebo distančnou formou), ktoré boli zamerané na kategóriu zamestnancov „manažér v kybernetickej bezpečnosti“ alebo minimálne 5 praktických skúseností pod zákazkami rovnakého alebo obdobného charakteru, ako je predmet zákazky (splnenie preukáže údajmi v životopise)
- Verejný obstarávateľ požaduje odbornú prax v minimálnom rozsahu 110 školiacich dní (1 školiaci deň = 7 výukových hodín) v priebehu posledných 4 rokov od vyhlásenia zákazky vo vzdelávaní dospelých (prezenčnou alebo dištančnou formou) v oblasti kybernetickej alebo informačnej bezpečnosti v skupinách s min. počtom 5 školených účastníkov.

b. Kľúčový expert pre kapitolu 2.3 - zodpovedný za vypracovanie podporných vzdelávacích materiálov (Požiadavky na podporné vzdelávacie materiály):

- minimálny počet 2 Kľúčových expertov ktorí musia spĺňať nasledovné požiadavky:
  - Minimálne ukončené vysokoškolské vzdelanie II. stupňa, preukazuje sa prostredníctvom kópie VŠ diplomu

[10] Príloha č. 14 k vyhláške č. 492/2022 Z. z. Národného bezpečnostného úradu – Lektor kybernetickej bezpečnosti, aktuálne dostupné na: https://www.slov-lex.sk/pravne-predpisy/prilohy/SK/ZZ/2022/492/20240101_5495696-2.pdf

- Minimálne dve praktické skúsenosti (získané v období predchádzajúcich štyroch rokov od vyhlásenia verejného obstarávania) s tvorbou metodiky a plánovaním výučby pre jednotlivcov alebo skupiny, učebné osnovy, ktoré sa venujú téme kybernetická alebo informačná bezpečnosť
- Minimálne jedna praktická skúsenosť (získaná v období predchádzajúcich štyroch rokov od vyhlásenia verejného obstarávania) s tvorbou e-learningových služieb na podporu vzdelávania s využitím vzdelávacích aktivít (napr. inštruktážne hry, interaktívne cvičenia, scenáre)
- Minimálne 4 roky odbornej praxe s tvorbou školiacich materiálov, ktorých obsah zahŕňa Úvod a terminológiu v kybernetickej alebo informačnej bezpečnosti, a/alebo Právna úprava vzťahujúca sa na kybernetickú alebo informačnú bezpečnosť, a/alebo na Bezpečnostné incidenty, a /alebo Digitálna identita, a/alebo Riadenie hrozieb a rizík, a/alebo Procesy a systémy riadenia informačnej a kybernetickej bezpečnosti, a/alebo Organizácia informačnej a kybernetickej bezpečnosti, a/alebo Personálna bezpečnosť alebo Riadenie prístupov a identít, a/alebo Princípov testovania kybernetickej bezpečnosti a pod.

V prípade uchádzača, ktorého tvorí skupina dodávateľov zúčastnená vo verejnom obstarávaní, tento preukazuje splnenie podmienok účasti týkajúcich sa technickej alebo odbornej spôsobilosti za všetkých členov skupiny spoločne.

Uchádzač môže na preukázanie technickej spôsobilosti alebo odbornej spôsobilosti využiť technické a odborné kapacity inej osoby, bez ohľadu na ich právny vzťah. V takomto prípade musí uchádzač verejnému obstarávateľovi preukázať, že pri plnení zmluvy bude skutočne používať kapacity osoby, ktorej spôsobilosť využíva na preukázanie technickej spôsobilosti alebo odbornej spôsobilosti.

6.2 Zoznam poskytovaných služieb obdobného charakteru

Verejný obstarávateľ požaduje od uchádzača predložiť zoznam poskytovaných služieb na podobný alebo porovnateľný predmet zákazky za predchádzajúce štyri roky od vyhlásenia verejného obstarávania s uvedením cien, lehôt dodania a odberateľov; dokladom je referencia, ak odberateľom bol verejný obstarávateľ alebo obstarávateľ podľa ZVO.

Zoznam poskytnutých služieb musí zahŕňať minimálne dve praktické skúsenosti z každej z nasledovných oblastí:

a) **realizácia školiacich aktivít** (prezenčnou alebo distančnou formou) zameraná na školenie pre oblasť kybernetickej alebo informačnej bezpečnosti, ktoré je prioritne definované pre pozíciu „manažér v kybernetickej bezpečnosti“ (Cyber Security Manager) a ktoré zahŕňa legislatívne požiadavky (smernice, právne predpisy, medzinárodné normy a štandardy súvisiace s informačnou a kybernetickou bezpečnosťou) a zvýšenie bezpečnostného povedomia a znalostných štandardov zamerané pre oblasť orgánov štátnej správy, zamestnancov z prostredia verejnej správy a pod., a to v minimálnej hodnote predpokladanej hodnoty zákazky € bez DPH za predchádzajúce 4 roky od vyhlásenia VO.

b) **tvorba podporných vzdelávacích materiálov** zahŕňa: tvorbu učebnej osnovy, učebných plánov vzdelávacieho materiálu v oblasti kybernetickej alebo informačnej bezpečnosti, jeho štruktúry, obsahovej náplne pre jednotlivcov alebo skupiny; alebo
   - tvorbu vzdelávacích aktivít a ich detailné rozpracovanie, ktoré sú zamerané na podporu vzdelávania (scenáre, inštruktážne hry, interaktívne cvičenia a pod.) v oblasti kybernetickej alebo informačnej bezpečnosti, ich merateľné ukazovatele a spôsob vyhodnocovania jednotlivých aktivít; alebo
   - tvorbu metodiky a plánovanie výučby, ktorá zahŕňa výchovno-vzdelávací proces (edukačný proces), ktorý sleduje zameranie, obsah a cesty výučby a vzdelávania a je komplexne zameraná na zvýšenie znalostných štandardov a princípov v oblasti kybernetickej alebo informačnej bezpečnosti ; alebo
   - tvorbu školiacich materiálov, ktorých obsah zahŕňa špecializované školenia kybernetickej bezpečnosti pre cieľovú skupinu „manažér kybernetickej bezpečnosti“ ako podporná pomôcka pre účastníkov, a to v podobe skrípt, pracovných zošitov a pod., ktoré boli vypracované na základe legislatívnych materiálov a medzinárodných noriem z oblasti kybernetickej bezpečnosti a/alebo informačnej bezpečnosti, ktoré uchádzač preukáže bez ohľadu na finančný limit.

Pod zákazkami rovnakého alebo obdobného charakteru ako predmet zákazky sa považujú zrealizované aktivity a to napríklad školenia, workshopy, konferencie zamerané na vzdelávanie a informovanosť ohľadom problematiky v oblasti kybernetickej alebo informačnej bezpečnosti, ktoré zahŕňali vysvetlenie základných pojmov a/alebo legislatívne požiadavky (smernice, právne predpisy, medzinárodné normy a štandardy súvisiace s informačnou a kybernetickou bezpečnosťou) a/alebo zvýšenie bezpečnostného povedomia a znalostných štandardov pre cieľové skupiny napríklad pre širokú verejnosť, ktoré spadá pod kategóriu používateľov „laici, bežní používatelia“, pre manažérov, podnikateľov a taktiež školenia zrealizované pre špecialistov KIB, príprava KIB expertov, audítorov KIB či za oblasť boja proti dezinformáciám a školenia realizované na kyberšikanu a pod.