



PÔDOHOSPODÁRSKA PLATOBNÁ AGENTÚRA

Hraničná 12, 815 26 Bratislava

Odbor verejného obstarávania

Naše číslo:

47697/2021/108

Vybavuje/Tel.

Mgr. Pavel Piliar/+421 918612497

V Bratislave

26.04.2021

Vysvetlenie informácií potrebných na vypracovanie ponuky

Predmet zákazky: „Informačná a kybernetická bezpečnosť - zavedenie bezpečnostných opatrení a postupov II.“

Druh postupu: Zákazka s nízkou hodnotou § 117 ZVO

Na základe doručenej žiadosti o vysvetlenie informácií potrebných na vypracovanie ponuky poskytuje verejný obstarávateľ toto vysvetlenie informácií potrebných na vypracovanie ponuky pre vyššie uvedený predmet zákazky.

Vysvetlenie informácií potrebných na vypracovanie ponuky:

1. Otázka:

„Aké majú opodstatnenie Vaše požiadavky na certifikáty:

- ITIL® Practitioner alebo ekvivalent,*
- PRINCE2® Practitioner alebo ekvivalent,*
- podniková architektúra (TOGAF®, COBIT®, resp. CGEIT certifikácia alebo ekvivalent),*
- vedúci / externý audítor ISMS podľa normy ISO/IEC 27001:2013 alebo certifikovaný audítor kybernetickej bezpečnosti vedený v zozname NBÚ.*

s plnením predmetu „Informačná a kybernetická bezpečnosť - zavedenie bezpečnostných opatrení a postupov II.“

Dané požiadavky resp. špecialisti s požadovanými certifikátmi sú podľa nášho názoru len eliminačným kritériom na potenciálnych dodávateľov bez opodstatnenia.

Ďakujem za vysvetlenie. „

1. Odpoveď:

Verejný obstarávateľ požaduje, aby uchádzač splnil požiadavky uvedené vo Výzve na predkladanie ponúk. Keďže sa jedná o komplexnú implementáciu organizačných opatrení podľa požiadaviek Zákona o kybernetickej bezpečnosti, ktoré vyplývajú z nálezov Auditu KB, tak požiadavky na kvalifikáciu členov implementačného tímu sú podľa nás na mieste.

PPA ako inštitúcia bankového charakteru spravujúca európske financie s dôrazom na protikorupčné opatrenia prechádza procesom kompletnej digitalizácie a tak najvyššia kvalita pri implementácii je pre nás nevyhnutná.

Súčasne verejný obstarávateľ na základe doručenej žiadosti o vysvetlenie požiadavky prehodnotil a upúšťa od požiadavky na certifikáciu PRINCE2, nakoľko po zvážení predmetu zákazky je zrejmé, že pri poskytovaní kontrahovanej služby nebude priamo realizovaná projektová aktivita a ako verejný obstarávateľ sme v pozícii konzumenta a nie sme tak súčasťou projektového tímu.

2. Otázka:

„Ešte jedna pripomienka a to konkrétne k Vašej požiadavke:

- *vedúci / externý audítor ISMS podľa normy ISO/IEC 27001:2013 alebo certifikovaný audítor kybernetickej bezpečnosti vedený v zozname NBÚ.*

Vašu požiadavku som konzultoval aj s NBÚ SR a ich stanovisko je, že :

- *obstarávateľ sa nemôže odvolávať na zoznam NBU, NBU žiadny zoznam, ktorý je referenčný NEVEDIE a ani NESMIE VIESŤ (nemá na to oporu v zákone ani nemá takú ambíciu)*
- *obstarávateľ sa nemôže odvolať na tento zoznam (ak tak robí, je to protizákonné). Zoznam na stránke NBU sa aj volá informatívny“*

2. Odpoveď:

Národný bezpečnostný úrad síce nezverejňuje na svojom webe zoznam certifikovaných audítorov, ale zverejňuje URL zoznamov. Samostatné zoznamy sú vedené a zverejňované orgánmi na posudzovanie zhody , na základe ich povinnosti , vyplývajúcej z ich akreditácie.

Ustupujeme teda od požiadavky účasti certifikovaného audítora kybernetickej bezpečnosti v projekte, najmä však z dôvodu udržania nezávislosti certifikovaných audítorov kybernetickej bezpečnosti. Pokrytie potreby zodpovedajúcej roly v projekte požadujeme aby člen projektového tímu disponoval certifikátom manažérstva informačnej bezpečnosti podľa ISO 27001, vydaným akreditovanou certifikačnou autoritou, alebo certifikátom profesionála informačnej bezpečnosti s certifikátom CISA (ISACA) , bez uznania akejkoľvek ekvivalencie iných certifikátov.

Dôvodom, prečo je nutné trvať na účasti audítora informačnej bezpečnosti , je nutný dohľad kvalifikovaného audítora nad úlohami projektu. Výstupy z projektu musia byť striktné v súlade s požiadavkami na bezpečnosť informácií v zmysle zákona 69/2018 Z.z. o kybernetickej bezpečnosti. Nejestvuje iná projektová rola , ktorá by bola spôsobilá na posudzovanie účinnosti implementovaných organizačných a technických bezpečnostných opatrení, vrátane odstránení nálezov vyplývajúcich zo záverečnej správy auditu kybernetickej bezpečnosti ktorý sme absolvovali v tomto roku.

V skratke teda požadujeme: Certifikát manažérstva informačnej bezpečnosti podľa ISO 27001 (lead audítor podľa ISO 27001) vydaným akreditovanou certifikačnou autoritou alebo certifikát profesionála informačnej bezpečnosti s certifikátom CISA (ISACA) pre oblasť systému riadenia IB, bez uznania akejkoľvek ekvivalencie iných certifikátov.

Vzhľadom na vyššie uvedené nastáva zmena vo Výzve na predkladanie ponúk v časti Obsah ponuky, bode 4. nasledovne:

4. Certifikáty konzultantov /skeny/: Uchádzač, resp. ním poskytnutí konzultanti/experti, musia vzhľadom na požadovaný rozsah, komplexnosť a najmä odbornosť aktivít, disponovať nasledovnými certifikátmi:

- ITIL® Practitioner alebo ekvivalent,
- podniková architektúra (TOGAF®, COBIT®, resp. CGEIT certifikácia alebo ekvivalent),
- Certifikát manažérstva informačnej bezpečnosti podľa ISO 27001 (lead audítor podľa ISO 27001) vydaným akreditovanou certifikačnou autoritou alebo certifikát profesionála informačnej bezpečnosti s certifikátom CISA (ISACA) pre oblasť systému riadenia IB, bez uznania akejkoľvek ekvivalencie iných certifikátov.

Uvedený zoznam certifikátov je možné kumulatívne splniť všetkými expertmi, podieľajúcimi sa na plnení predmetu zákazky.

Na základe vyššie uvedeného verejný obstarávateľ posúva lehotu na predkladanie ponúk na 3.5.2021 do 12:00 hod.