Vysvetlenie SP č. 1

Verejnému obstarávateľovi bola v lehote na predkladanie ponúk doručená žiadosť o vysvetlenie informácií uvedených v súťažných podkladoch. V súlade s § 48 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov Vám poskytujeme nasledovné vysvetlenie:

Žiadosť o vysvetlenie č.1

Konkrétně bychom Vás chtěli požádat o vysvětlení níž uvedené skutečnosti:
V Zadávací dokumentaci: Podmínky Účasti uchazečů – část 2. Technická a odborná způsobilost - bod. 3 uvádí Zadavatel požadavky na Experta č. 4 – Specialistu pro IT bezpečnost:
a) minimálne 3 roky odbornej praxe s implementáciou bezpečnosti aplikačnej infraštruktúry informačných systémov,
b) minimálne 2 profesionálne praktické skúsenosti v oblasti návrhu bezpečnosti informačných systémov v rámci projektov realizácie informačných systémov,
c) platný certifikát Audítora Kybernetickej bezpečnosti podľa zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti alebo ekvivalentného právneho predpisu platného v danom štáte,
d) platný certifikát Audítora ISO 22301 Lead Auditor BCM
e) preukazuje sa životopisom alebo údajom o odbornej praxi preukazujúcim splnenie podmienok účasti a kópiou príslušného certifikátu.
Tímto žádáme zadavatele o vysvětlení/ upřesnění požadavku d) tedy certifikát ISO 22301.
Vzhledem k požadavku na držení certifikátu Audítora Kybernetickej bezpečnosti podľa zákona č. 69/2018 Z.z. a zároveň dle předpokládaného předmět plnění experta č. 4 není z našeho pohledu v žádném případě relevantní, aby daný člen realizačního týmu musel být jeho držitelem. V současnosti TÜV SÜD Slovakia s.r.o (jeden ze dvou certifikačních orgánů pro certifikaci osob dle Audítora Kybernetickej bezpečnosti podľa zákona č. 69/2018 Z.z.) eviduje ve svých databázích pouze 19 osob, kteří jsou jeho držitelem a tím pádem by po uplatnění požadavku dle bodu d) došlo k výrazné diskriminaci volné soutěže, přičemž po jeho aplikaci dojde k výraznému omezení potencionálních kandidátů na jednotky osob.
Tímto zadavatele žádáme s ohledem na podporu podmínek volné soutěže, aby akceptoval dle bodu d) i alternativní certifikace, případně umožnil prokázání daného požadavku například 3 roky odborné praxe v oblasti zavádění BCMS.

ODPOVEĎ

Ďakujem za vašu otázku ohľadne verejného obstarávania „Definovanie metodiky na Business Continuity Management a integrácie bezpečnosti do životného cyklu vývoja systému SDLC (SystemDevelopmentLifeCycle)“.
Z našich skúseností so zákonom 69/2018 o kybernetickej bezpečnosti a prislúchajúcej vyhlášky 362/2018 Z.z. respektíve jej novelizovanej verzie 264/2023 Z.z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, máme za to, že oblasť Business Continuity je najkritickejšia a najviac podceňovaná oblasť v rámci bezpečnostných opatrení definovaných v zákone č. 69/2018 Z.z. o kybernetickej bezpečnosti.
Z tohto dôvodu požadujeme expertov, ktorí majú skúsenosť so zákonom 69/2018 Z.z. o kybernetickej bezpečnosti nie len ako konzultant, manažér ale aj ako audítor. Tak isto požiadavky na certifikát Audítora ISO 22301 Lead Auditor BCM, sú pre nás relevantné na naplnenie požiadaviek nášho projektu v nadväznosti aj na jeho čerpanie z výzvy „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS“. Komentár ohľadne relevantnosti audítora kybernetickej bezpečnosti podľa zákona 69/2018 Z.z. nie je relevantný, keďže počet certifikovaných audítorov na Slovensku je vyšší, ako vami uvádzaná

hodnota 19. Na Slovensku máme viacero certifikačných autorít a počet audítorov kybernetickej bezpečnosti podľa zákona 69/2018 Z.z. je viac ako 60.

Žiadosť o vysvetlenie č.2

OTÁZKA č. 1

Verejný obstarávateľ v súťažných podkladov v kapitole „ČASŤ A2.“ na strane 22 uvádza požiadavky na splnenie podmienok účasti “ Expert č.1 :” uvádza:

„d) platný certifikát CISM, CEH08 alebo ekvivalent daného certifikátu od inej akreditovanej autority (Napr.: NBU)

e) platný certifikát Auditora Kybernetickej bezpečnosti podľa zákona 69/2018 Z.z.“

Zároveň verejný obstarávateľ požiadavky “platný certifikát CISM alebo ekvivalent” uvádza aj pri expertovi “Expert č.3 – Expert pre bezpečnosť informácií” Takisto požiadavku “platný certifikát Auditora Kybernetickej bezpečnosti podľa zákona 69/2018 Z.z. “ uvádza pri expertovi “Expert č.4 – Špecialista pre IT bezpečnosť – senior:” Zároveň “platný certifikát Audítora ISO 22301 Lead Auditor BCM” je nelogicky vyžadovaný pri expertovi č 4, napriek tomu že skúsenosti s implmentáciou BCMS sú vyžadované pri expertovi č.1

Podotázka 1:

Bude preto verejný obstarávateľ akceptovať ak uchádzač preukáže plnenie týchto pozícií (expert č 1., 3 a 4) jedným expertom ?

Podotázka 2:

Takisto vzhľadom na to že sa nejedná o vykonanie auditu, nie je zrejmé z akého dôvodu sú vyžadované certifikáty „platný certifikát Auditora Kybernetickej bezpečnosti“ a „platný certifikát Audítora ISO 22301 Lead Auditor BCM“. Bude preto verejný obstarávateľ považovať za splnenie podmienok účasti aj v prípade ak používateľ preukáže skúsenosti s tvorbou implementácie BCM a kybernetickej bezpečnosti?

ODPOVEĎ

Nie. Na vykonávanie aktivít v rámci času, ktorý mame, je potrebné viacero expertov, z ktorých je každý expert na jednu oblasť. Preto požadujeme popísané vedomosti u viacerých expertov. Je požadovaných dostatočné množstvo man days, ktoré treba naplniť paralelnými aktivitami a expertami.

Podotázka 2:

Takisto vzhľadom na to že sa nejedná o vykonanie auditu, nie je zrejmé z akého dôvodu sú vyžadované certifikáty „platný certifikát Auditora Kybernetickej bezpečnosti“ a „platný certifikát Audítora ISO 22301 Lead Auditor BCM“. Bude preto verejný obstarávateľ považovať za splnenie podmienok účasti aj v prípade ak používateľ preukáže skúsenosti s tvorbou implementácie BCM a kybernetickej bezpečnosti ?

Odpoveď

Z našich skúseností so zákonom 69/2018 o kybernetickej bezpečnosti a prislúchajúcej vyhlášky 362/2018 Z.z. respektívejej novelizovanej verzie 264/2023 Z.z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, mame za to, že oblasť Business Continuity je najkritickejšia a najviac podceňovaná oblasť v rámci bezpečnostných opatrenídefinovaných v zákone o kybernetickej bezpečnosti 69/2018 Z.z.

S tohto dôvodu požadujeme expertov, ktorý majú skúsenosť so zákonom 69/2018 Z.z. o kybernetickej bezpečnosti nie len ako konzultant, manažér ale aj ako auditor. Tak isto požiadavky na certifikát Audítora ISO 22301 Lead Auditor BCM, sú pre nás relevantné na

naplnenie požiadaviek nášho projektu v spojení aj na jeho čerpanie z výzvy „„Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS

OTÁZKA č. 2

Verejný obstarávateľ v súťažných podkladov v dokumente „ČASŤ B1. OPIS PREDMETU ZÁKAZKY“ v kapitole „iii. Požiadavky na systém:“ uvádza :

„• v prípade potreby a rozhodnutia URHH a Manažéra KB musí byť systém schopný zastrešiť všetky evidenčné a procesné oblasti riadenia KB nezávisle od iných systémov a bez potreby integrácie na iné systémy. “

Vie verejný obstarávateľ vysvetliť ktoré všetky evidenčné a procesné oblasti plánuje zastrešiť, ktoré nie sú uvedené v rámci opisu predmetu zákazky ? Jedná sa o to že verejný obstarávateľ obstaráva SW v zmysle opisu predmetu zákazky a ak sú požadované aj iné požiadavky je ich nevyhnutné definovať.

ODPOVEĎ

Rozsah je definovaný povinnými aktivitami, ktoré má zabezpečovať poskytovateľ základnej služby v zmysle Zákona č. 69/2018 o Kybernetickej bezpečnosti a súvisiacich vyhláškach.

Minimálne však v rozsahu:

- Evidencia informačných aktív, ich vyhodnotenie a riadenie
- Evidencia a riadenie rizík, plánov zvládania rizík
- Evidencia a riadenie hrozieb KB
- Evidencia a riadenie zraniteľností KB
- Evidencia a riešenie incidentov KB
- Evidencia výsledkov auditov KB
- Evidencia výsledkov bezpečnostných testov a kontrol
- Evidencia riadenie rizík dodávateľov s vplyvom na KB
- Evidencia technických bezpečnostných opatrení
- Evidencia a riadenie bezpečnostnej dokumentácie
- Evidencia a riadenie procesov vzdelávania v oblasti KB

OTÁZKA č. 3

Verejný obstarávateľ v súťažných podkladov v dokumente „ČASŤ B1. OPIS PREDMETU ZÁKAZKY“ v kapitole „iii. Požiadavky na systém:“ uvádza :

„systém nesmie byť zložený s viacerých samostatných špecifických systémov – požadované jednotné riešenie a jednotná technológia v rámci všetkých definovaných funkcionalít.“

Vie verejný obstarávateľ definovať, čo znamená, že systém nemá byť zložený z viacerých samostatných špecifických systémov a jednotná technológia? Jedná sa o to že už v rámci samostatných požiadaviek sú definované požiadavky, ktoré túto funkčnú požiadavku negujú. (napr. musí umožňovať pracovať aj s databázami, ktoré nie potrebné priebežne platiť – kde databáza je samostatný špecifický systém.). Takisto sa môže jednať o Preto žiadame verejného obstarávateľa o jasné špecifikovanie požiadaviek tak aby boli jednoznačné.

Takisto žiadame verejného obstarávateľa o definovanie požiadavky na jednotnú technológiu. Jedná sa o jednotnú technológiu na úrovni frontendu, backendu, API. Alebo sa jedná o obmedzenie na niektoré konkrétne frameworky, napr Spring a podobne? Alebo sa jedná o jednotnú technológiu na úrovni orchestrácie kontajnerov kde všetky moduly a mikroservicy musia bežať v rámci jednotného clustra worker nodov ?

ODPOVEĎ

Verejný obstarávateľ požaduje jedno softvérové riešenie, ktoré bude zastrešovať všetky požadované funkcionality a nebude zložený z viacerých softvérových komponentov, ktoré zo svojej podstaty netvoria jeden funkčný celok.

OTÁZKA č. 4

Verejný obstarávateľ v súťažných podkladov v dokumente „ČASŤ B1. OPIS PREDMETU ZÁKAZKY“ v kapitole „iii. Požiadavky na systém:“ uvádza :

„• nástroj musí umožňovať úpravy existujúcich modulov a rolí/oprávnení podľa požiadaviek Zadávateľa.“

Vie verejný obstarávateľ definovať akých existujúcich modulov ? Vie ich verejný obstarávateľ vymenovať.? Vie verejný obstarávateľ definovať aké úpravy plánuje realizovať a ktoré musí aplikácia podporovať ?

ODPOVEĎ

Verejný obstarávateľ požaduje nástroj, ktorý má jednotlivé funkcionality ako je napríklad risk manažment a správa aktiv ako separátne moduly. Tieto moduly by mali byt modifikovateľné podľa potrieb a interných procesov obstarávateľa.

OTÁZKA č. 5

Verejný obstarávateľ v súťažných podkladov v dokumente „ČASŤ B1. OPIS PREDMETU ZÁKAZKY“ v kapitole „iii. Požiadavky na systém:“ uvádza :

„• možnosť prepojiť so service deskom, alebo CMDB databázou“

Vie verejný obstarávateľ definovať aký service desk využíva a aký spôsob prepojenia požaduje ?

ODPOVEĎ

Požiadavka je primárne určená, aby systém obsahoval integračné, napr. API rozhranie ktoré je možné konfigurovať, resp. upraviť podľa vzniknutých potrieb.

OTÁZKA č. 6

Verejný obstarávateľ v súťažných podkladov v dokumente „ČASŤ B1. OPIS PREDMETU ZÁKAZKY“ v kapitole „iii. Požiadavky na systém:“ uvádza :

„• možnosť využívať API rozhranie“

Vie verejný obstarávateľ definovať aký API akých systémov a za akým účelom plánuje využívať ?

ODPOVEĎ

Primárne ide o pripojenie so service deskom, alebo CMDB databázou.

OTÁZKA č. 7

Verejný obstarávateľ v súťažných podkladov v dokumente „ČASŤ B1. OPIS PREDMETU ZÁKAZKY“ v kapitole „iii. Požiadavky na systém:“ uvádza :

„• integrovaná OLAP kocka minimálne na úrovni pohľadov na informačné aktíva, systémové aktíva, hrozby, zraniteľnosti, opatrenia, riziká, nezhody a ich vzájomné súvislosti v danom okamihu.“

Vzhľadom na to že z uvedených príkladov pohľadov jednoznačne nevyplýva explicitná potreba na implementáciu OLAP kocky keďže sa jedná skôr o prehľady ako o multidimenziánálne analytické dáta. Vie preto verejný obstarávateľ definovať aké príklady aké dimenzie a ich rozsah požaduje pri jednotlivých OLAP kockách a aký spôsob agregácie a výpočtu ukazovateľov bude požadovať. (napr. aspoň súhrný počet vypočítaných ukazovateľov) ? V prípade že jedná len o jednoduché prehľady a nie o analytické dáta OLAP prosíme o úpravu požiadavky.

ODPOVEĎ

Definovať prehľad o vzájomných prejdeniach a väzbách v rámci systému, no minimálne na úrovni:

- Informačných aktív
- Technických aktív (tzv. podporných aktív)
- Súvisiacich bezpečnostných opatreniach
- Súvisiacich rizík a kritickosti rizík, hodnôt, úrovní
- Súvisiacich hrozieb
- Súvisiacich incidentov
- Súvisiacich zraniteľností

+ možnosť dynamicky pridávať ďalšie parametre obsiahnuté v systéme.

Ak je dodávateľ schopný túto funkcionalitu a informácie poskytnúť inou formou ako OLAP, bude akceptovaný aj ekvivalent OLAP kocky.

Z dôvodu, že nedochádza k zmene podkladov pre vypracovanie ponuky, verejný obstarávateľ nepredĺžil lehotu na predkladanie ponúk.

V Bratislave, 24.10.2023