Odpoveď na žiadosť o vysvetlenie č. 1

Identifikácia verejného obstarávateľa:

Obchodné meno:	Záchranná zdravotná služba Bratislava
Sídlo:	Antolská 11, 850 07 Bratislava 57
IČO:	17336210
Názov zákazky:	Rozvoj kybernetickej bezpečnosti v ZZS Bratislava

Odkaz na zverejnené dokumenty: https://josephine.proebiz.com/sk/tender/77018/summary

Otázka č. 1:

Žiadame o poskytnutie vysvetlenia, na základe akých požiadaviek na predmet zákazky stanovil verejný obstarávateľ rôzne trvanie období, za ktoré má záujemca/uchádzač preukázať splnenie podmienok účasti pri jednotlivých expertoch. Špeciálne u experta č. 4 žiada splnenie podmienok účasti s dvomi rôznymi dĺžkami rozhodných období. Žiadame o odstránenie požiadavky na viazanosť praktických skúseností so stanoveným obdobím kalendárnych rokov.

Odpoveď č. 1:

Verejný obstarávateľ k stanoveniu dĺžky rozhodných období pri expertoch č. 1 až 4 uvádza nasledovné vecné odôvodnenie:

Stanovenie rozhodného obdobia, za ktoré má uchádzač preukázať praktické skúsenosti jednotlivých expertov, vychádza z princípu proporcionality podľa § 10 ods. 2 zákona č. 343/2015 Z. z. o verejnom obstarávaní (ďalej len „**ZVO**") v spojení s § 38 ods. 5 ZVO, podľa ktorého musia byť podmienky účasti týkajúce sa technickej alebo odbornej spôsobilosti primerané a musia súvisieť s predmetom zákazky. Diferenciácia rozhodných období odráža objektívne odlišnú povahu úloh jednotlivých expertov, technologickú dynamiku príslušných odborných oblastí a životný cyklus relevantných nástrojov, ktoré sú predmetom verejného obstarávania. Verejný obstarávateľ pri ich stanovení postupoval tak, aby na jednej strane zabezpečil dostatočnú referenčnú vzorku skúseností a na strane druhej aktuálnosť týchto skúseností vo vzťahu k súčasnému stavu technológií a hrozieb.

Verejný obstarávateľ nad rámec ďalej uvedených dôvodov uvádza, že rozhodné obdobie, za ktoré žiada preukázať požadované skúsenosti, určil v dĺžke 3 až 5 rokov, čo je dostatočne dlhá doba na preukázanie, že expert má v danej oblasti dostatočné a aktuálne praktické skúsenosti. Kým verejný obstarávateľ stanovil požiadavku 3 praktických skúseností za obdobie troch či piatich rokov (pozn. požiadavka zodpovedá periodicite 1 skúsenosť za približne každého 1 až 1,5 roka), experti, ktorí sa aktívne venujú implementácii uvedených bezpečnostných nástrojov, môžu preukázať aj niekoľko praktických skúseností v jednom kalendárnom roku.

Okrem toho, verejný obstarávateľ predĺžením rozhodných období až na obdobie 5 rokov v tých prípadoch, kde to z vecnej stránky je možné, umožňuje širšiu súťaž hospodárskych subjektov. Ak by naopak boli požiadavky stanovené pre každého experta rovnako prísne (preukázanie požadovaných skúseností v období posledných 3 rokov), bez ohľadu na vecné hľadisko, dochádzalo by zbytočne ku sprísneniu súťažných podmienok a zúženiu hospodárskej súťaže.

Verejný obstarávateľ v neposlednom rade upozorňuje na to, že na zabezpečenie dostatočnej hospodárskej súťaže, priaznivých a nediskriminačných podmienok, bude v rámci preukazovania technickej a odbornej spôsobilosti akceptovať, aby odborné požiadavky pre každú požadovanú pozíciu kľúčového experta boli splnené kombináciou viacerých osôb, maximálne však dvomi, ktoré spoločne v súhrne pokrývajú všetky stanovené požiadavky na danú pozíciu.

K expertovi č. 1 (5 rokov) – Senior konzultant pre súlad s bezpečnostnými požiadavkami a dokumentáciu IKB:

Ide o konzultačnú pozíciu metodicko-procesného charakteru, ktorej výstupom je dokumentácia organizácie a riadenia informačnej a kybernetickej bezpečnosti. Príslušné regulatórne a normatívne rámce (zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a jeho vykonávacie vyhlášky, normy radu ISO/IEC 27000) sú metodologicky relatívne stabilné a ich aplikačná prax je viacročná. Päťročné obdobie zabezpečí dostatočnú hĺbku a šírku referenčných skúseností pri zachovaní ich aktuálnosti voči platnému regulatórnemu rámcu.

K expertovi č. 2 (5 rokov) – Senior technik bezpečnosti perimetra: Nástroje perimetrovej bezpečnosti (NGFW, IPS/IDS, WAF a obdobné) majú relatívne dlhší životný cyklus a stabilnejšiu architektonickú bázu. Skúsenosti s ich implementáciou zostávajú odborne relevantné aj v dlhšom časovom horizonte. Päťročné rozhodné obdobie považuje verejný obstarávateľ za primerané vo vzťahu k povahe a technologickej dynamike tohto segmentu.

K expertovi č. 3 (4 roky) – Senior technik pre ochranu kritických prvkov a bezpečnostný monitoring: Oblasť ochrany kritických prvkov a bezpečnostného monitoringu (EDR/XDR, SIEM a obdobné) je technologicky výrazne dynamickejším segmentom než perimetrová bezpečnosť. Funkcionalita, architektúra (prechod od on-premise riešení k cloud-native a SaaS platformám) aj detekčné metodiky (MITRE ATT&CK, behaviorálna a UEBA analytika, korelačné pravidlá) prešli v posledných rokoch výrazným vývojom. Kratšie štvorročné obdobie zabezpečí, že expert disponuje aktuálnou skúsenosťou s technológiami a metodikami zodpovedajúcimi súčasnému stavu poznania, a nie skúsenosťami s riešeniami, ktoré sú dnes prekonané, resp. postupy ich implementácie sú odlišné. Požiadavka disponovať aktuálnejšími skúsenosťami tiež reflektuje dôležitosť a komplexitu dodávaného bezpečnostného nástroja (ide o technicky najpokročilejší komponent z opisu predmetu zákazky).

K Expertovi č. 4 (3 + 5 rokov) – Konzultant pre bezpečnostné testovanie: Dvojaké rozhodné obdobie pri tomto expertovi nepredstavuje vnútorný rozpor, ale je dôsledkom objektívne odlišnej povahy dvoch zložiek bezpečnostného testovania:

- *3 roky pri skenovaní zraniteľností a/alebo penetračnom testovaní* – ide o oblasť s najvyššou technologickou dynamikou/dynamikou hrozieb. Spektrum aktívne zneužívaných zraniteľností a útočných techník (napr. priebežné aktualizácie OWASP Top 10, MITRE ATT&CK, CVE) sa mení v horizonte mesiacov. Trojročné obdobie zabezpečí, že expert má aktuálne skúsenosti. Navyše, experti, ktorí sa profesionálne a aktívne venujú bezpečnostnému testovaniu IT systémov, vykonávajú bežne niekoľko testovaní ročne, na trhu sú obvyklé.

- *5 rokov pri bezpečnostnom testovaní zamestnancov* – metodika testovania bezpečnostného povedomia (phishingové kampane, sociálne inžinierstvo) je z metodologického hľadiska

podstatne stabilnejšia. Päťročné obdobie zabezpečí dostatočnú referenčnú vzorku skúseností pri zachovaní ich odbornej relevantnosti. Verejný obstarávateľ má za to, že akceptovaním dlhšieho obdobia zároveň stanovil priaznivejšie podmienky pre uchádzačov a umožnil nimi širšiu hospodársku súťaž.

K návrhu na odstránenie viazanosti praktických skúseností na rozhodné obdobie:

Verejný obstarávateľ návrhu na úplné odstránenie časového vymedzenia praktických skúseností nevyhovuje. Stanovenie rozhodného obdobia je v súlade s § 38 ods. 5 ZVO. Úplná absencia časového vymedzenia by mohla viesť k tomu, že uchádzač preukáže spôsobilosť skúsenosťami, ktoré sú vo vzťahu k aktuálnemu stavu technológií, hrozieb a postupov v oblasti kybernetickej bezpečnosti neaktuálne. Takýto stav by bol v rozpore s účelom podmienok účasti aj s oprávneným záujmom verejného obstarávateľa na riadnom a kvalitnom plnení predmetu zákazky, tým viac, ak ide o citlivú oblasť kybernetickej bezpečnosti.

Stanovené rozhodné obdobia považuje verejný obstarávateľ za vecne odôvodnené, primerané povahe predmetu zákazky, nediskriminačné a v súlade so základnými princípmi verejného obstarávania.

Verejný obstarávateľ podmienky účasti v predmetnej časti nemení.

Otázka č. 2:

Certifikát MKB je jediná štátnou schémou regulovaná a akreditovaná osobná certifikácia v oblasti kybernetickej bezpečnosti na Slovensku (vydávaná v súlade s § 28 a nasl. zákona č. 69/2018 Z. z.), žiadame uviesť, akým spôsobom verejný obstarávateľ zohľadnil túto skutočnosť pri nastavovaní podmienok účasti a prečo preferuje kumuláciu troch komerčných ISO certifikátov pred štátnou certifikáciou MKB, ktorá má vyššiu relevanciu pre súlad s národnou legislatívou.

Vzhľadom na tú skutočnosť, že certifikácia Manažér kybernetickej bezpečnosti (MKB) podľa certifikačnej schémy Národného bezpečnostného úradu SR (v zmysle zákona č. 69/2018 Z. z. a akreditovaná podľa ISO/IEC 17024) explicitne zahŕňa znalosti a zručnosti v oblastiach budovania a riadenia systému manažérstva informačnej / kybernetickej bezpečnosti (analogicky ISMS podľa ISO/IEC 27001), identifikácie, analýzy a ošetrovania rizík (analogicky ISO/IEC 27005), zabezpečovania odolnosti a kontinuity činnosti organizácie v kontexte kybernetických hrozieb (analogicky princípy ISO 22301 v rozsahu relevantnom pre kybernetickú bezpečnosť),

žiadame verejného obstarávateľa o vysvetlenie, či bude akceptovať certifikát MKB (vydaný akreditovaným certifikačný morgánom – napr. TÜV SÜD, Cyber Competence a pod.) ako plnohodnotnú náhradu za kumulatívne držanie osobných certifikátov ISO/IEC 27001:2022, ISO/IEC 27005:2018 a ISO 22301:2019 u experta č. 1Senior konzultant pre posúdenie súladu s bezpečnostnými požiadavkami a spracovanie základnej dokumentácie pre organizáciu a riadenie IKB?

Ak nie, žiadame o odôvodnenie neprijatia ekvivalentu k požadovanej podmienke účasti a stanovisko k nasledovným otázkam.

Otázka č. 2B

Ak verejný obstarávateľ trvá na kumulatívnom držaní troch samostatných ISO certifikátov, žiadame uviesť konkrétne časti Opisu predmetu zákazky / technickej špecifikácie, ktoré vyžadujú znalosti nad rámec toho, čo pokrýva certifikačná schéma MKB podľa aktuálnej verzie schválené NBÚ (verzia 1.2 z roku 2024 alebo neskoršia).

Otázka č. 2C

Žiadame prehodnotiť proporcionalitu požiadavky na kumuláciu troch ISO certifikátov v jednej osobe vzhľadom na skutočnosť, že certifikát MKB je štátom regulovaná a akreditovaná odborná spôsobilosť priamo viazaná na slovenskú legislatívu kybernetickej bezpečnosti (vrátane požiadaviek vyplývajúcich z implementácie NIS2), MKB zahŕňa integrovaný pohľad na ISMS, riadenie rizík a odolnosť / kontinuitu v kybernetickom prostredí, v praxi sa MKB bežne uplatňuje práve pri implementácii a prevádzke bezpečnostných technológií (firewall, XDR, SIEM, MFA, sieťová segmentácia atď.).

Prečo verejný obstarávateľ nepovažuje certifikát MKB + preukázateľné praktické skúsenosti s implementáciou uvedených technológií za postačujúci na zabezpečenie súladu s legislatívou a riadneho plnenia technologickej časti projektu?

Účelom určenia podmienok účasti týkajúcich sa technickej alebo odbornej spôsobilosti je overiť si z týchto hľadísk postavenie uchádzača alebo záujemcu a uistiť sa, že plnenie zmluvy v požadovanom rozsahu a kvalite bude zabezpečované spôsobilým zmluvným partnerom. Stanovené podmienky účasti svojím rozsahom a charakterom musia mať priamu súvislosť s predmetom zákazky a musia objektívne vyjadrovať odôvodniteľné požiadavky na spôsobilosť záujemcov k jeho plneniu. Verejný obstarávateľ môže vymedziť minimálnu úroveň podmienok účasti iba takým spôsobom, aby bola primeraná a zodpovedala druhu, rozsahu, zložitosti a charakteru (povahe) konkrétneho predmetu zákazky. Verejný obstarávateľ má prostredníctvom minimálnej úrovne podmienok účasti overiť spôsobilosť záujemcu splniť zákazku, nie vytvárať neodôvodnené prekážky pre účasť záujemcov vo verejnom obstarávaní.

Stanovením neprimeraných podmienok účasti sa verejný obstarávateľ môže dopustiť konania, prostredníctvom ktorého obmedzí okruh potencionálnych záujemcov a znemožní im účasť vo verejnom obstarávaní. Za formu neprípustnej diskriminácie (skrytej) je potrebné považovať i taký postup verejného obstarávateľa, ktorým verejný obstarávateľ znemožní niektorým záujemcom uchádzať sa o zákazku nastavením takej minimálnej úrovne podmienky účasti, ktorá je zjavne neprimeraná k predmetu zákazky, pričom je zrejmé, že ju môžu splniť len niektorí z potencionálnych záujemcov, hoci by inak boli k plneniu predmetu zákazky objektívne spôsobilí.

Odpoveď č. 2:

Odpoveď verejného obstarávateľa na žiadosť o vysvetlenie č. 2 (vrátane podotázok 2B a 2C):

Verejný obstarávateľ k otázke akceptácie certifikátu Manažér kybernetickej bezpečnosti (MKB) ako náhrady za kumuláciu troch certifikátov (ISO/IEC 27001:2022 – interný audítor, ISO/IEC 27005:2018 – manažér riadenia rizík a ISO/IEC 22301:2019 – manažér BCMS / interný audítor) u Experta č. 1 a k súvisiacim podotázkam uvádza nasledovné:

Verejný obstarávateľ kvalitu status certifikačnej schémy Manažér kybernetickej bezpečnosti, vydávanej akreditovanými certifikačnými orgánmi v zmysle § 28 a nasl. zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, plne uznáva. Súťažné podklady v časti A.2 (technická a odborná

spôsobilosť) výslovne umožňujú nahradenie každého z požadovaných certifikátov ekvivalentom, ktorý zodpovedá požadovanému odbornému zameraniu, rozsahu a úrovni znalostí, je vydaný akreditovaným certifikačným orgánom a je platný a overiteľný. MKB tieto formálne kritériá akreditácie spĺňa.

K otázke č. 2 – MKB ako ekvivalent kumulácie troch certifikátov

Verejný obstarávateľ MKB ako plnohodnotnú náhradu za kumulatívne držanie všetkých troch požadovaných certifikátov v jednej osobe akceptovať nemôže, a to z dôvodu, že certifikačná schéma MKB poskytuje integrovaný manažérsky prehľad naprieč viacerými oblasťami kybernetickej bezpečnosti (ISMS, riadenie rizík, kontinuita, sieťová a aplikačná bezpečnosť, incident manažment, personálna a fyzická bezpečnosť, overovanie súladu a pod.). Ide o certifikáciu prierezovú, ktorá overuje, že manažér KB ovláda celé spektrum domén na úrovni potrebnej pre riadenie KB vo vnútri organizácie.

Naproti tomu tri požadované ISO certifikáty overujú špecializovanú spôsobilosť do hĺbky v troch odlišných odborných doménach:

- ISO/IEC 27001:2022 (interný audítor) overuje špecificky spôsobilosť vo vzťahu k ISMS – t. j. schopnosť posudzovať súlad systému riadenia s normou a viesť interný audit podľa stanovenej metodiky.
- ISO/IEC 27005:2018 overuje špecificky spôsobilosť v oblasti riadenia rizík kybernetickej bezpečnosti podľa konkrétnej normalizovanej metodiky.
- ISO/IEC 22301:2019 overuje špecificky spôsobilosť v oblasti systému manažérstva kontinuity činnosti (BCMS) vrátane metodiky Business Impact Analysis (BIA).

Vzťah medzi MKB a uvedenými ISO certifikátmi nie je teda vzťahom dvoch ekvivalentov, ale o požadovanej hĺbke spôsobilostí. MKB s každou z týchto domén pracuje, avšak na úrovni potrebnej pre manažérsky rozhľad, nie na úrovni kumulatívne špecializovaného audítora ISMS, špecializovaného manažéra rizík podľa ISO/IEC 27005, ani špecializovaného manažéra BCMS podľa ISO/IEC 22301. Schéma MKB neoveruje a ani nemá za cieľ overiť hĺbkové metodické zvládnutie auditu ISMS, metodiky ISO/IEC 27005 a metodiky BCMS podľa ISO/IEC 22301 samostatne – overuje integrovaný prehľad manažéra.

K otázke č. 2B – konkrétne väzby požadovaných certifikátov na predmet zákazky

Verejný obstarávateľ uvádza nasledovné konkrétne väzby medzi jednotlivými certifikátmi a explicitnými požiadavkami Opisu predmetu zákazky (príloha č. 1):

K ISO/IEC 27001:2022 (interný audítor): Modul č. 1, aktivita 1.1 – Posúdenie súladu s bezpečnostnými požiadavkami – výslovne požaduje vypracovanie *„kontrolného zoznamu plnenia všetkých relevantných požiadaviek podľa zákona o KB a vykonávacích predpisov, ich súladu s aktuálnym stavom IKB v ZZS Bratislava, vrátane overenia skutočne implementovaných bezpečnostných opatrení*". Ide o aktivitu povahy, ktorá si vyžaduje špecificky spôsobilosť na overenie súladu. Súvisiaca aktivita 1.2 d) ďalej zahŕňa vypracovanie Smernice pre riadenie informačnej bezpečnosti (ISMS) podľa medzinárodných štandardov radu ISO 27000, ktoré sú v OPZ explicitne uvedené ako východisko.

K ISO/IEC 27005:2018: Modul č. 1, aktivita 1.2 c) výslovne požaduje *„aktualizáciu analýzy rizík kybernetickej bezpečnosti a analýzy dopadov (AR/BIA), ktorá je založená na Metodike analýzy rizík kybernetickej bezpečnosti, verzia 2.0 alebo novšia, vydanej NBÚ dňa 01. septembra 2025, a ktorá je plne v súlade s medzinárodným štandardom ISO 27005"*. Aktivita 1.2 d) ďalej zahŕňa vypracovanie Smernice pre riadenie aktív a rizík vrátane AR/BIA metodiky. Požiadavka na špecializovanú spôsobilosť podľa ISO/IEC 27005 je teda v OPZ priamo a doslovne uvedená.

K ISO/IEC 22301:2019: Modul č. 1, aktivita 1.2 c) výslovne zahŕňa analýzu dopadov (BIA – Business Impact Analysis), ktorá je základom systému manažérstva kontinuity činnosti podľa ISO/IEC 22301. Vyhláška NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach, na ktorú OPZ priamo odkazuje, takisto zahŕňa požiadavky na riadenie kontinuity činností. Pre verejného obstarávateľa, ktorý je prevádzkovateľom základnej služby v sektore zdravotníctvo, je kontinuita prevádzky kľúčová a nevyhnutná. Špecializovaná spôsobilosť v oblasti BCMS podľa ISO/IEC 22301 je preto vo vzťahu k povahe predmetu zákazky aj mimo požiadaviek vyhlášky NBÚ objektívne zrejmá.

K otázke č. 2C – proporcionalita podmienky účasti

Verejný obstarávateľ pri stanovovaní podmienok účasti postupoval v súlade s § 38 ods. 5 ZVO a princípmi podľa § 10 ods. 2 ZVO. Trvá na tom, že požiadavka na tri špecializované certifikáty u Experta č. 1 nie je neproporcionálna, a to vzhľadom na nasledovné objektívne skutočnosti:

- Predmetom zákazky nie je len implementácia technológií, ale aj komplexné spracovanie procesnej dokumentácie pre prevádzkovateľa základnej služby, vrátane stratégie, bezpečnostnej politiky a ôsmich smerníc pokrývajúcich celý rámec ISMS, rizík, kontinuity, aktív, klasifikácie informácií, prístupov, dodávateľov a SSDLC.

- Verejný obstarávateľ je prevádzkovateľom základnej služby v sektore so zvýšenými nárokmi na kontinuitu činnosti, ktorej ohrozenie môže mať závažné prevádzkové a finančné dopady na organizáciu.

- OPZ priamo odkazuje na medzinárodné štandardy ISO 27000, ISO 27005, na metodiku NBÚ verzia 2.0 z 01. 09. 2025 a na vyhlášku NBÚ č. 227/2025 Z. z. Požadované certifikáty sú vo vzťahu k týmto referenčným rámcom priamo previazané.

- Súťažné podklady umožňujú kombináciu dvoch osôb na jednu pozíciu kľúčového experta, čo uchádzačovi umožňuje rozdeliť požadované certifikácie medzi dvoch špecialistov. Táto možnosť výrazne znižuje bariéru účasti a nepredpokladá kumuláciu všetkých troch certifikátov u jednej fyzickej osoby.

- Súťažné podklady zároveň umožňujú akceptáciu ekvivalentov pri každom z certifikátov, ak spĺňajú stanovené kritériá zamerania, rozsahu, úrovne, akreditácie a overiteľnosti.

Argument záujemcu, že podmienka účasti by mohla predstavovať skrytú diskrimináciu, verejný obstarávateľ neprijíma. Skrytá diskriminácia predpokladá taký postup, ktorý objektívne spôsobilým hospodárskym subjektom znemožňuje účasť bez vecnej súvislosti s predmetom zákazky. V tomto prípade je každá z požadovaných certifikácií objektívne previazaná s konkrétnym, výslovne pomenovaným výstupom OPZ, a možnosť ich pokrytia kombináciou dvoch expertov resp. ekvivalentnými certifikátmi, je výslovne zachovaná.

Verejný obstarávateľ s ohľadom na čo najširšiu hospodársku súťaž vo veci akceptácie ekvivalentov jednotlivých certifikácií uvádza nasledovné:

- Certifikát MKB, vydaný akreditovaným certifikačným orgánom, môže byť akceptovaný ako ekvivalent certifikátu ISO/IEC 27001:2022 – interný audítor, a to vzhľadom na vecné prekrytie domén ISMS a auditu v rámci certifikačnej schémy MKB.
- Pri certifikátoch ISO/IEC 27005:2018 a ISO/IEC 22301:2019 verejný obstarávateľ trvá na požiadavke špecializovanej osobnej certifikácie alebo iného ekvivalentu, ktorý overuje spôsobilosť práve v týchto doménach, nakoľko MKB sám o sebe nepokrýva tieto špecializované metodiky v rozsahu a hĺbke požadovaných výstupov OPZ (AR/BIA podľa ISO 27005, BIA podľa BCMS).

Verejný obstarávateľ podmienky účasti v predmetnej časti nemení.