Vysvětlení zadávací dokumentace č. 1

Název veřejné zakázky:
Nástroj pro řízení informačních rizik opakované znovuvyhlášení

Druh zadávacího řízení: zjednodušené podlimitní řízení (otevřená výzva)
Režim veřejné zakázky: podlimitní
Předmět veřejné zakázky: dodávky

Zadavatel: Nemocnice Pardubického kraje, a.s.
Sídlo: Kyjevská 44, 532 03 Pardubice
IČO: 27520536

V Pardubicích dne 20. 12. 2025

Zadavatel v souladu s ustanovením § 98, resp. § 99 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, (dále jen „zákon"), sděluje následující vysvětlení a změnu zadávací dokumentace vztahující se k výše uvedené veřejné zakázce.

Žádost o vysvětlení zadávací dokumentace

Dobrý den,
dovolujeme si vás požádat o vysvětlení následujících ustanovení zadávací dokumentace, která se nám jeví jako nejasná či potenciálně omezující hospodářskou soutěž.

Bod 1

1)
Ustanovení 10.3 ZD:
"seznam min. 4 významných služeb [...] min. jedna služba v hodnotě minimálně 3 000 000,- Kč bez DPH. V rozsahu nasazení systému řízení rizik více kategorií, minimálně pak řízení rizik dle ZoKB, řízení rizik BOZP a PO, rizik GDPR, Rizik Compliance, rizik Business Continuity managementu (BIA), rizik dodavatele a dodavatelského řetězce, finančních rizik dle zákona o vnitřní kontrole č.320/2001"

Otázka: Zadávací dokumentace požaduje, aby jedna referenční zakázka pokrývala současně minimálně 8 různých oblastí řízení rizik (ZoKB, BOZP, PO, GDPR, Compliance, BCM/BIA, dodavatelsky řetězec, finanční rizika). Takto formulovaný požadavek výrazně omezuje počet potenciálních dodavatelů, neboť kombinace všech těchto oblasti v rámci jedné zakázky je na trhu zcela výjimečná.

Dotaz

Žádáme o vysvětlení:
• Jaké konkrétní důvody vedly zadavatele ke kumulaci všech 8 oblasti řízení rizik v rámci jedné referenční zakázky?

Odpověď

Kombinace uvedených oblastí odpovídá běžným požadavkům na softwarové nástroje pro řízení obecných rizik v organizacích **obdobné velikosti a charakteru**, jakou je zadavatel. Pro zadavatele je zásadní, aby proces

řízení rizik byl podporován jedním integrovaným nástrojem, nikoli souborem vzájemně neprovázaných řešení.
Zadavatel proto požaduje řešení, které podporuje standardní a obecně uznávané procesy řízení rizik, například dle rámce ISO 31000, a které není funkčně omezeno pouze na oblast kybernetické či informační bezpečnosti, ale umožňuje jednotnou správu různých kategorií rizik v organizaci.

Záměrem zadavatele je tedy v organizaci realizovat jeden komplexní a konzistentní nástroj pro řízení rizik, založeném na data, asset (technické položky), údaje o lokaci, dodavatelích, o podnikových procesech atd. s možností vedení funkčních vazeb v jednom systému. Zadavatel zamýšlí řešit rizika na bázi jednotných procesů risk managementu omezeným týmem vlastních specialistů (omezené zdroje), kteří sdílí know-how nad jedním systémem.

Dotaz

Připouští zadavatel alternativně možnost prokázaní technické kvalifikace více referenčními zakázkami, z nichž každá pokrývá část požadovaných oblastí?

Odpověď

Z výše uvedeného důvodu ne, pokud jsou různé referenční zakázky řešeny různými systémy.

Dotaz

Zároveň:
Předmětem veřejné zakázky je dle bodu 2.1 ZD a Přílohy c. 2 (Technická specifikace)
"dodávka softwarových prostředků pro realizaci systému řízení informačních rizik a zvládaní bezpečnostních událostí"
Požadavek na referenční zakázku zahrnující realizaci těchto oblastí: "BOZP/PO, finanční rizika", se proto jeví jako nepřiměřený ve vztahu k předmětu plnění, neboť zadavatel tyto služby v rámci této zakázky nepoptává.
• Jaké konkrétní důvody vedly zadavatele k požadavku na reference zahrnující implementaci řízení BOZP/PO, když tato oblast není součástí předmětu plnění?

Odpověď

Jak je výše uvedeno:
Zadavatele k tomuto požadavku vede potřeba zavedení jednotného a dlouhodobě udržitelného nástroje pro řízení všech relevantních typů rizik v rámci organizace. Cílem je zajistit, aby pořizovaný systém nebyl omezen pouze na úzce vymezenou oblast, ale umožňoval jeho budoucí rozšíření i na další kategorie rizik, včetně oblasti BOZP/PO, finančních rizik aj. bez nutnosti pořizování samostatných řešení.

Tento přístup reflektuje princip řádného hospodáře, neboť umožňuje optimalizaci finančních nákladů na provoz a rozvoj informačních systémů a současně eliminuje riziko, že by zadavatel byl v budoucnu nucen vyhlašovat další veřejné zakázky na samostatné nástroje pro řízení jiných kategorií rizik.

Zadavatel k dotazu dále uvádí, že po realizaci požadovaných aspektů plnění uvedených v zadávací dokumentaci a po nabytí odborných znalosti s administrací systému a porozumění procesům bude v dalších aspektech, i v těch, kterých se týká dotaz (BOZP aj.), rozvíjet systém zejména vlastními

silami (případně s podporou vybraného dodavatele v rámci závazků dle servisní smlouvy, např. formou konzultací apod.). Cílem je ochrana a efektivní využití vložených investic a dalších interních zdrojů (zejména lidských) zadavatele.

Dotaz

Jaké konkrétní důvody vedly zadavatele k požadavku na reference zahrnující implementaci finančních rizik dle zákona č. 320/2001 Sb., když tato oblast není součástí předmětu plnění?

Odpověď

Zadavatel požadavek na reference zahrnující implementaci řízení finančních rizik dle zákona č. 320/2001 Sb. odůvodňuje tím, že řízení rizik je integrální součástí systému vnitřní kontroly podle zákona o finanční kontrole. Požadavek tak umožňuje ověřit, že dodavatel je schopen implementovat systém, který bude v budoucnu možné využít i pro podporu procesů řízení finančních rizik, čímž se zadavatel opět řídí principem řádného hospodáře a zajišťuje efektivní a jednotnou správu rizik v celé organizaci, jak již bylo uvedeno.

Dotaz

Může zadavatel potvrdit, že kvalifikační požadavky mají přiměřený vztah k předmětu veřejné zakázky?

Odpověď

S ohledem na výše uvedené odpovědi zadavatele odpovídají kvalifikační požadavky rozsahu, významu a důležitosti předmětu veřejné zakázky.

K bodu 1 jako celku zadavatel dále uvádí:

Zadavatel stanovil požadavky na referenční zakázku zahrnující všech osm oblastí řízení rizik z důvodu ověření, že dodavatel má **praktickou zkušenost s implementací komplexního, integrovaného systému řízení rizik v jedné organizaci**, nikoli pouze dílčí nebo tematicky omezené řešení.
Řízení rizik je zadavatelem myšleno jako **ucelený proces napříč organizací**, nikoli jako soubor izolovaných modulů.
Kumulace oblastí v jedné referenční zakázce prokazuje schopnost dodavatele:

- navrhnout jednotnou metodiku,
- zajistit provázanost jednotlivých typů rizik,
- implementovat systém použitelný v reálném provozu velké organizace,
- zajistit realizaci dlouhodobě udržitelného systému spravovaného efektivně pomocí omezených zdrojů zadavatele a postupně rozšiřovatelného na uvedené předmětné oblasti,
- zajistit následný rozvoj s akcentem na posílení a využití interních odborných zdrojů.

Bod 2

2)
Zadávací dokumentace stanovuje následující strukturu požadavku na reference:
• 1x zakázka min. 3 mil. Kč - systém řízení 8 kategorii rizik (ZoKB, BOZP, PO, GDPR, Compliance, BCM/BIA, dodavatelsky řetězec, finanční rizika)
• 1x zakázka min. 2 mil. Kč - řízení rizik dle ZoKB včetně auditu KB
• 1x zakázka min. 1 mil. Kč - řízení rizik dle ISO 27000
• 1x zakázka min. 1 mil. Kč - BCM

Zadavatel požaduje, aby Z TĚCHTO 4 referencí byly min. 2 realizovány pro zdravotnické zařízení a zároveň min. 2 pro systémy kritické informační infrastruktury.
Tato formulace znamená, že požadavky na zdravotnické zařízení a KII nejsou samostatné, ale musí byt splněny v rámci výše uvedených 4 referencí. Jinými slovy, dodavatel musí mít například:
• Zakázku na 3 mil. Kč (8 kategorií rizik) realizovanou pro KII, NEBO
• Zakázku na 2 mil. Kč (ZoKB + audit) realizovanou pro zdravotnické zařízení, atd.
Takto provázané požadavky jsou extrémně restriktivní, neboť vyžadují, aby dodavatel realizoval komplexní zakázky na řízení 8 kategorií rizik právě pro zdravotnické zařízení nebo provozovatele KII.

Dotaz

Žádáme o vysvětlení:
• Potvrzuje zadavatel, ze požadavek "Z toho" znamená, že reference pro zdravotnické zařízení a KII musí byt součástí výše uvedených 4 referencí (tj. nesmí se jednat o samostatné, dodatečné reference)?

Odpověď

Zadavatel uvádí, že nemusí.

Dotaz

Jaké konkrétní důvody vedly zadavatele k takto provázané formulaci požadavků?

Odpověď

Zajistit odborně způsobilého dodavatele pro plnění veřejné zakázky.

Dotaz

Připouští zadavatel alternativně možnost prokázat reference pro zdravotnické zařízení a KII samostatně, tj. mimo strukturu 4 specifických referencí?

Odpověď

Ano, připouští

K bodu 2 jako celku zadavatel uvádí:
Zadavatel požaduje, aby účastník doložit samostatné čtyři reference v daném finančním a funkčním rozsahu (první čtyři odrážky) konkrétně.
• 1x zakázka min. 3 mil. Kč - systém řízení 8 kategorii rizik (ZoKB, BOZP, PO, GDPR, Compliance, BCM/BIA, dodavatelsky řetězec, finanční rizika)
• 1x zakázka min. 2 mil. Kč - řízení rizik dle ZoKB včetně auditu KB
• 1x zakázka min. 1 mil. Kč - řízení rizik podle procesů definovaných normou ISO 27000
• 1x zakázka min. 1 mil. Kč - BCM
Samostatně může účastník doložit reference pro KII a zdravotnická zařízení; tyto nemusí být součástí prvních čtyř referencí.

Bod 3

3)
Ustanovení 10.3 ZD:
"min. dvě (2) významné zakázky musí byt realizovány pro systémy kritické informační infrastruktury"

Otázka: Kritická informační infrastruktura (KII) dle zákona c. 181/2014 Sb. a vyhlášky c. 437/2017 Sb. zahrnuje velmi omezeny okruh subjektu v České republice.
Zadavatel - Nemocnice Pardubického kraje - je provozovatelem základní služby ve smyslu zákona o kybernetické bezpečnosti, nikoliv provozovatelem KII. Požadavek na 2 reference pro KII se proto jeví jako nepřiměřený ve vztahu k charakteru zadavatele a předmětu plnění.

Dotaz

Žádáme o vysvětlení:
• Jaké konkrétní důvody vedly zadavatele k požadavku na reference pro systémy KII, když sám zadavatel není provozovatelem KII?

Odpověď

Zadavatel považuje své klíčové infrastrukturní systémy, které zajišťují kontinuitu poskytování IT služeb a informatickou podporu pro základní služby státu, za „kritické systémy“ a důvodně předjímá, že bude poskytovatelem regulované služby v režimu vyšších povinností (dále jen „povinná osoba“) a bude tímto směrem upravovat obsah bezpečnostních opatření a způsob jejich zavádění a provádění (viz. vyhláška 409/2025).
Zadavatel požadavek na reference zahrnující systémy kritické informační infrastruktury (KII) odůvodňuje tím, že související zkušenosti s implementací takových systémů jsou přínosné pro přípravu a adaptaci zdravotnických zařízení na novou regulatoriku, zejména dle nařízení CER a zákona č. 266/2025 Sb. (zákon o kritické infrastruktuře). Tyto zkušenosti zajišťují, že dodavatel disponuje kompetencemi potřebnými pro návrh a implementaci bezpečných systémů řízení rizik, které lze aplikovat i v prostředí zdravotnických zařízení podléhajících zvýšeným regulačním nárokům.

Dotaz

Připouští zadavatel alternativně reference pro provozovatele základní služby ve smyslu ZoKB, což odpovídá charakteru zadavatele?

Odpověď

Tento dotaz je pro zadavatele nejasný. Nerozumí termínu „alternativně reference pro provozovatele základní služby“.

Dotaz

Připouští zadavatel reference pro systémy informační infrastruktury zdravotnických zařízení, bez omezeni na KII?

Odpověď

ANO.

Bod 4

4)
Ustanovení 10.3 ZD - požadavky na realizační tým:
"Auditor kybernetické bezpečnosti - certifikace CISA a ISO 27000"
Otázka: Zadávací dokumentace požaduje, aby auditor kybernetické bezpečnosti disponoval současně certifikací CISA (Certified Information Systems Auditor) a certifikaci v oblasti ISO 27000 (pravděpodobně Lead Auditor ISO 27001). Obe certifikace pokrývají oblast auditu bezpečnosti informačních systémů a jejich současný požadavek se jeví jako duplicitní a nepřiměřeně omezující.
Právní rámec: Vyhláška c. 82/2018 Sb., o kybernetické bezpečnosti, v příloze c. 6 stanovuje požadavky na odbornou způsobilost bezpečnostních roli. Pro roli auditora kybernetické bezpečnosti uvádí následující certifikace jako alternativy (nikoliv kumulativní požadavky):
• Certified Information Systems Auditor (CISA)
• Certified Internal Auditor (CIA)
• Certified in Risk and Information Systems Control (CRISC)
• Lead Auditor Information Security Management System (Lead Auditor ISMS)
• Auditor BI (akreditační schéma CIA)
Vyhláška dále výslovně uvádí:
"Certifikace může byt i jiná než uvedená, jestliže certifikace dokládající odbornou způsobilost bezpečnostních roli splňuje požadavky ISO 17024."
Požadavek zadavatele na současné držení dvou konkrétních certifikaci (CISA a ISO 27000) je tedy v rozporu s duchem vyhlášky c. 82/2018 Sb., která tyto certifikace uvádí jako alternativy, a zároveň nepřipouští jiné rovnocenné certifikace dle ISO 17024.

Dotaz

Žádáme o vysvětlení:
• Jaké konkrétní důvody vedly zadavatele k požadavku na současné držení obou certifikací (CISA a ISO 27000), když obě pokrývají obdobnou oblast odbornosti?

Odpověď

Zadavatel opravuje v zadávací dokumentaci v bodě 10.3 Technická kvalifikace v části „Realizační tým“ požadavek na odbornou roli Auditor kybernetické bezpečnosti:

Auditor kybernetické bezpečnosti – ~~certifikace CISA a ISO 27000 – lead auditor, 3 roky praxe~~ certifikace CISA nebo Lead Auditor ISO 27001, 3 roky praxe

Dotaz

Připouští zadavatel v souladu s vyhláškou c. 82/2018 Sb. alternativně pouze jednu z uvedených certifikací (CISA nebo Lead Auditor ISO 27001)?

Odpověď

Ano, zadavatel připouští pouze jednu z uvedených certifikací, viz předchozí odpověď - certifikace CISA nebo Lead Auditor ISO 27001. Zadavatel upozorňuje, že se nejedná o ISO 27000 jako certifikaci na firmu (viz předchozí dotaz), ale o Lead Auditor ISO 27001.

Dotaz

Připouští zadavatel jiné certifikace?

Odpověď

Ano, záleží na konkrétní certifikaci. Zadavatel si vyhrazuje právo ji odmítnout v případě, že litera jiné certifikace nebude odpovídat dikci požadovaných certifikací.

Dotaz

Připouští zadavatel v souladu s vyhláškou c. 82/2018 Sb. i jiné certifikace splňující požadavky ISO 17024?

Odpověď

Alternativně lze doložit pouze jednu z uvedených certifikací, a to CISA nebo Lead Auditor ISO 27001.
Jiné certifikace mohou být akceptovány, záleží na konkrétní certifikaci a zadavatel si vyhrazuje právo ji odmítnout, pokud její obsah nebude odpovídat požadované odborné způsobilosti. Tímto způsobem zadavatel zachovává možnost ověřit odbornou způsobilost auditora kybernetické bezpečnosti a zároveň odstraňuje nepřiměřené omezení duplicitních požadavků.

Zadavatel prodlužuje lhůtu pro podání nabídek do 14. 1. 2026 do 10:00 hodin.

Oddělení veřejných zakázek
Nemocnice Pardubického kraje, a.s.