



Vysvětlení zadávacích podmínek č. 4

1. Specifikace zakázky a zadavatele

Číslo zakázky (pod kterým byla uveřejněna na www.esfcr.cz)	10866
Název zakázky	Provedení certifikace dle ISO/IEC 27001
Registrační číslo projektu	CZ.03.4.74/0.0/0.0/16_033/0002813
Název projektu	Profesionální a bezpečný úřad
Název / obchodní firma zadavatele	Kraj Vysočina
Sídlo zadavatele	Žižkova 57, Jihlava
IČO zadavatele / DIČ zadavatele	70890749
Jméno a příjmení osoby oprávněné jednat za zadavatele	Ing. Vladimír Novotný, náměstek hejtmana

Zadavatel obdržel dne 7. 11. 2016 další dotaz na vysvětlení nabídky:

Otázka:

Začátek otázky

Ačkoli jste tyto odpovědi zhodnotili jako nerelevantní pro stanovení nabídky, pro mě jsou to velmi důležité informace pro stanovení rizika Vaší organizace a odvíjí se od toho délka auditu a tudíž i cena. Pokud tato otázka č. 9 nebude zodpovězena, nebudu schopna stanovit konečnou cenu, pouze odhad, který se může při odkrytí skutečností lišit od navržené ceny.

1) Úroveň rizika a komplexita:

9a Úroveň rizika: Prosím, určete-zaškrtněte míru rizika (vysoké, střední nebo nízké) pro každou ze tří kategorií níže (právo a požadavky, obchodní kontinuita a schopnost, držené/řízení informace).

	Nízké	Střední	Vysoké	L	M	H
Právní a regulační požadavky	Nesoulad pravděpodobně povede k menšímu peněžitému trestu či poškození dobrého jména	Nesoulad pravděpodobně povede k významnějšímu peněžitému trestu či poškození dobrého jména	Nesoulad pravděpodobně povede k soudnímu stíhání			
Obchodní kontinuita a dostupnost	Dopad omezen na obchodní / provozní nepřijemnosti	Nedostatek či výpadek má významný dopad na základní služby, jako je zdravotní péče - výpadky budou mít	Informace musí být neustále dostupné (např. krizová národní infrastruktura)			



		pravděpodobně odezvu od opatření havarijního plánování národních / místních vládních organizací			
Držené/řízené informace	Informace obecné povahy	Citlivé a osobní identifikační informace (poznámka: obsahuje informace o zaměstnancích)	Vysoce hodnocené vládní informace, např. tajné a výše; vládní nouzové vysílání		
Příklady	Obchodní organizace, klasické podniky, které tvoří podstatnou součást dodavatelských řetězců nebo partnerství se středními a vysoce rizikovými organizacemi. Poznámka: Aby společnost měla „nízké“ riziko, nesmí držet žádné osobní identifikační informace o zaměstnancích	Nemocnice, peněžní sektor (banky, místní úřady, telekomunikační poskytovatelé a další, kteří drží osobní nebo citlivé identifikační informace	Vládní ministerstva, krizové národní infrastruktury (např. vysílání)		

Odpověď:

Pro zpracování nabídky není nezbytné.

9b: hodnocení komplexity

Faktor komplexity	Kategorie jednoduchá („S“)	Kategorie složitá („C“)	Hodnocení „S“ nebo „C“	
Počet zaměstnanců a agenturních zaměstnanců	<1000	>=1000		
Počet uživatelů	<1 milion	>=1 milion		
Počet provozoven	<5	>=5		
Počet serverů	<100	>=100		
Počet pracovních stanic + PC + laptopů	<300	>=300		
Počet vývojářů aplikací a pracovníků údržby	<100	>=100		

Odpověď:

Pro zpracování nabídky není nezbytné.

Dále se prosím o upřesnění předmětu certifikace „Řízení informační bezpečnosti“ – to je název certifikace. Předmět certifikace odráží činnost certifikované organizace. Co organizace dělá. Má odrážet činnosti, které jsou kryty certifikací ISO 27001. Zde uvádím příklady z jiných certifikátů:



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Služby v oblasti informačních technologií, včetně projektování a realizace sítí, servisních činností, systémové integrace a vývoje softwaru
Vývoj, návrh, výroba, instalace, údržba, opravy, modifikace a konstrukční změny leteckých pozemních zařízení

[Konec otázky](#)

Odpověď

Úroveň rizika a komplexita:

9a Úroveň rizika: Prosím, určete-zaškrtněte míru rizika (vysoké, střední nebo nízké) pro každou ze tří kategorií níže (právo a požadavky, obchodní kontinuita a schopnost, držené/řízení informace).

	Nízké	Střední	Vysoké	L	M	H
Právní a regulační požadavky	Nesoulad pravděpodobně povede k menšímu peněžitému trestu či poškození dobrého jména	Nesoulad pravděpodobně povede k významnějšímu peněžitému trestu či poškození dobrého jména	Nesoulad pravděpodobně povede k soudnímu stíhání		x	
Obchodní kontinuita a dostupnost	Dopad omezen na obchodní / provozní nepříjemnosti	Nedostatek či výpadek má významný dopad na základní služby, jako je zdravotní péče - výpadky budou mít pravděpodobně odezvu od opatření havarijního plánování národních / místních vládních organizací	Informace musí být neustále dostupné (např. krizová národní infrastruktura)		x	
Držené/řízené informace	Informace obecné povahy	Citlivé a osobní identifikační informace (poznámka: obsahuje informace o zaměstnancích)	Vysoce hodnocené vládní informace, např. tajné a výše; vládní nouzové vysílání		x	
Příklady	Obchodní organizace, klasické podniky, které tvoří podstatnou součást dodavatelských řetězců nebo partnerství se středními a vysoce rizikovými organizacemi. Poznámka: Aby	Nemocnice, peněžní sektor (banky, místní úřady, telekomunikační poskytovatelé a další, kteří drží osobní nebo citlivé identifikační informace	Vládní ministerstva, krizové národní infrastruktury (např. vysílání)			



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

	společnost měla „nízké“ riziko, nesmí držet žádné osobní identifikační informace o zaměstnancích				
--	--	--	--	--	--

Upřesnění odpovědi k bodu Obchodní kontinuity a dostupnost:

Dle poznámky v příkladu nemůžeme spadat pod nízké riziko kvůli držení identifikačních údajů o zaměstnancích, nicméně popis středního rizika pro nás není příliš výstižný. Rovněž závisí na výpadku konkrétního systému, době výpadku a rozsahu. Formulace otázky a standardní odpovědi neumožňuje adekvátní odpověď z naší strany.

9b: hodnocení komplexity

Faktor komplexity	Kategorie jednoduchá („S“)	Kategorie složité („C“)	Hodnocení „S“ nebo „C“	
Počet zaměstnanců a agenturních zaměstnanců	<1000	>=1000	x	
Počet uživatelů	<1 milion	>=1 milion	x	
Počet provozoven	<5	>=5	x	
Počet serverů	<100	>=100		x
Počet pracovních stanic + PC + laptopů	<300	>=300	x	
Počet vývojářů aplikací a pracovníků údržby	<100	>=100	x	

Upřesnění odpovědi k bodu Počet provozoven:

Není specifikováno, co je míněno provozovnou. Certifikace se bude týkat jednoho úřadu, který sídlí v hlavním areálu (4 budovy) a v dalších čtyřech samostatných budovách/pracovištích.

Dotaz už byl zodpovídan

Upřesnění odpovědi k bodu Počet serverů:

Není uvedeno, zda se jedná o počet virtuálních či fyzických strojů. Odpověď zahrnuje i virtuální stroje.

Předmět certifikace:

Řízení informační bezpečnosti

Dotaz už byl zodpovídan

Pozn.: Činnost kraje jako vyššího územně samosprávného celku vychází z již v předchozích vysvětleních nabídky zmiňovaného zákona č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů. Uvádění citace obecně závazných právních předpisů do vysvětlení zadávacích podmínek považujeme za neúčelné.

S ohledem na charakter otázek zadavatel nepovažuje za nutné prodlužovat lhůtu pro podání nabídek.



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Datum a podpis osoby oprávněné
jednat za zadavatele

V Jihlavě dne 8. 11. 2016

Elektronicky podepsáno
Ind. Dana Buřičová
Vedoucí odboru analýz a podpory řízení