INTEGROVANÝ OPERAČNÍ PROGRAM

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ

MINISTERSTVO PRO MÍSTNÍ ROZVOJ

Dodatečné informace č. 1

k nadlimitní veřejné zakázce „Elektronizace projektového řízení a nástroje komunikace“

Evidenční číslo ve VVZ: VZ 343904
VZ v E-ZAK: https://ezak.cnpk.cz/vz00001427

Dotaz 1:
Požadované dodatečné informace týkající se technické dokumentace:

- 2.4.13 Rozhraní: V jakém rozsahu mají být vazby implementovány?

Odpověď zadavatele:
Tento bod je napsán z naší strany trochu obecně (v Technické dokumentaci je uveden seznam informačních systémů, na něž má mít soutěžená aplikace vazby), neboť rozhraní od třetích stran dosud neexistuje, a proto není detailně popsáno ; ale už nyní avízujeme, jako technologií budou rozhraní popsána (SOAP).
Nicméně prakticky se jedná pouze o dotahování některých informací a dat (řádově půjde o jednotky webových služeb) z okolních systémů na základě informací vyplněných u projektu. Např. vrať majetek k danému projektu, vrať seznam faktur k danému projektu viz bod 2.4.5 TD . Pouze datové úložiště, které je součástí dodávky , by mělo disponovat rozsáhlejším a transakčním rozhraním viz 2.4.4 TD.

Dotaz 2:
Požadované dodatečné informace týkající se technické dokumentace:

- 4.1 Penetrační testy: Penetrační testy budou na naše náklady? Společnost si tedy můžeme vybrat sami?

Odpověď zadavatele:

Penetrační testy za účelem kontroly bezpečnosti informačních systémů Plzeňského kraje a Krajského úřadu Plzeňského kraje pro nás pravidelně realizuje vybraný externí odborný dodavatel.
Pokud jde o vyhodnocení bezpečnosti IS na projektové řízení , tato skutečnosti je popsána v návrhu smlouvy o dílo, která je nedílnou součástí zadávacích podmínek zadavatele.

Čl. 8. Bezpečnost díla

1. Objednatel upozorňuje zhotovitele, že aby mohl být informační systém (tj. dílo) zařazen do infrastruktury Plzeňského kraje, resp. Krajského úřadu Plzeňského kraje, tak musí splňovat bezpečnostní opatření, která zajistí, že informační systém projde penetračními testy dle metodiky: http://www.owasp.org/index.php/Category:OWASP_Project.

V odkazu jsou všechny techniky napadnutí, proti kterým musí být informační systém zabezpečen.

2. Zda informační systém tato bezpečností opatření splňuje, si objednatel ověří na vlastní náklady. Při zjištění bezpečnostních vad, je zhotovitel povinen tyto vady odstranit. Ještě jeden následný penetrační test po odstranění takových závad hradí objednatel. Pokud bezpečnostní chyby přetrvají, další penetrační testy bude hradit zhotovitel. Bezpečný průchod informačního systému penetračními testy je podmínkou pro akceptaci díla.

Dotaz 3:

Požadované dodatečné informace týkající se technické dokumentace:

- 4.3 Zálohování: Máme systém připravit na zálohování, které bude řízeno jiným systémem nebo management záloh má být také součástí systému (pravidelné spouštění, správa zálohovacích úloh,…)

Odpověď zadavatele:

V tuto chvíli používáme 2 způsoby zálohování:

1. Veeam Backup – kompletní virtuální stroje, včetně konzistentních záloh filesystému, SQL.

2. Symantec Backup Exec 2012 – jednotlivé zvláštní položky nebo SQL databáze samotné, vše opět konzistentně.

Pokud toto standardní zálohování nedostačuje pro korektní obnovení aplikace, je potřeba nastavit vlastní způsob zálohování a jeho výstup bude zálohován výše uvedeným SW v našem prostředí. Součástí musí být v každém případě popis řešení disaster recovery aplikace.