



Nabídka

Vytvoření metodiky pro identifikaci a hodnocení aktiv
a pro hodnocení rizik informační bezpečnosti

Zákazník:	Generální finanční ředitelství
Číslo nabídky:	OP11951
Datum zpracování:	9.10.2019
Dodavatel:	IXPERTA s.r.o.
Verze:	1.3



1. Identifikační údaje

Název dokumentu:

Nabídka na vytvoření metodiky pro identifikaci a hodnocení aktiv a pro hodnocení rizik informační bezpečnosti

Identifikační údaje uchazeče (též Dodavatel):

Název / obchodní firma:

IXPERTA s.r.o.

Adresa sídla / místa podnikání:

Lihovarská 1060/12

190 00 Praha 9

Zapsaná v OR:

C 117991 vedená u Městského soudu v Praze

IČ:

27599523

DIČ:

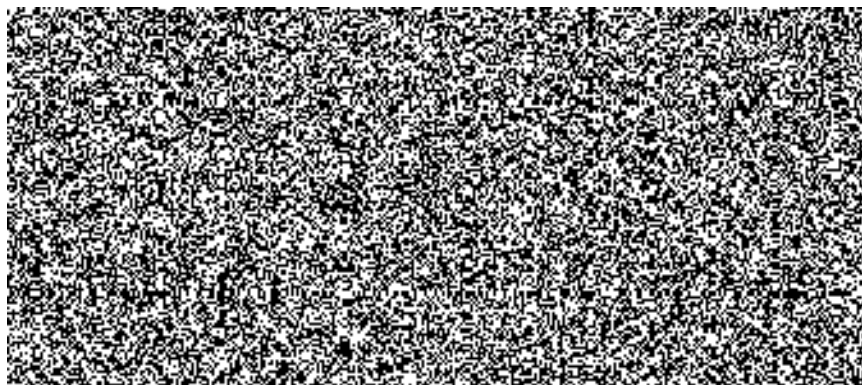
CZ27599523

Statutární orgán:

Bankovní spojení:

Web:

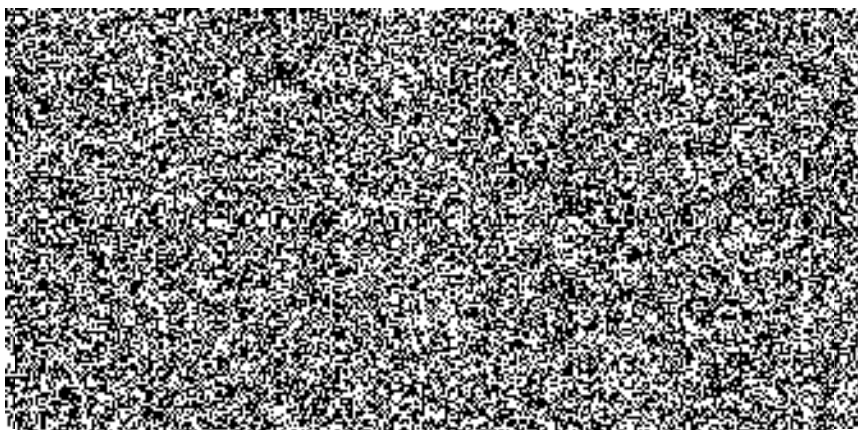
Kontaktní údaje:



Osoby oprávněné jednat jménem uchazeče:

Ve věcech smluvních:

Ve věcech technických:



2. Nabídka

2.1. Předmět a cíle projektu

Cílem projektu je vytvořit metodiku pro identifikaci a hodnocení aktiv a pro hodnocení rizik bezpečnosti informací pro Generální finanční ředitelství a jemu podřízené orgány finanční správy.

Metodika musí být v souladu s požadavky a možnostmi zákazníka tak, aby umožnila provádět řízení rizik v kontextu organizace Zákazníka, vč. materiálně technických a personálních možností.

Zákazník je vázán Zákonem č. 181/2014 Sb (Zákon o kybernetické bezpečnosti) a novelizovanou Vyhláškou o kybernetické bezpečnosti (vyhl. č. 82/2018). Metodika bude tuto legislativu plně respektovat. V oblastech nepokrytých touto legislativou bude vycházet z mezinárodních standardů rodiny ISO 27000, zejména normy ČSN ISO/IEC 27005:2019, příp. dalších aplikovatelných standardů.

Pokud jsou nyní již informační rizika hodnocena (předpokládáme, že jsou), vezme navržená metodika v oblasti hodnocení rizik v úvahu výstupy stávajícího hodnocení a jeho metodiky, aby byla zachována možnost srovnání vývoje rizik v organizaci Zákazníka v průběhu času.

Na základě vytvořené metodiky bude Zákazník, případně s využitím dodavatelů, provádět kontinuální řízení rizik informační bezpečnosti v rámci finanční správy.

2.2. Práce provedené společností IXPERTA

V rámci vytvoření metodiky pro identifikaci a hodnocení aktiv a pro hodnocení rizik budou za součinnosti Zákazníka provedeny následující činnosti. Tyto činnosti zahrnují jak workshopy s příslušnými pracovníky Zákazníka, tak i zpracování v kancelářích Dodavatele.

Vytvoření metodiky řízení rizik bezpečnosti informací:

- Kick-off meeting
- Workshop se zástupci Zákazníka – identifikace a odsouhlasení požadavků na metodiku
 - Dodavatel připraví základní obecné a předvídatelné požadavky a společně se Zákazníkem budou doplněny specifické požadavky
- Příprava draftu metodiky
 - Vč. nástrojů pro provádění hodnocení aktiv a rizik, jež poslouží pro ověření proveditelnosti a funkčnosti metodiky
- Předložení (prezentace) draftu metodiky k připomínkování Zákazníkem
 - V případě potřeby opakovaně
- Zpracování připomínek
 - V případě potřeby opakovaně
- Předání vypracované metodiky

Práce budou provedeny a výstupy dodány v českém jazyce.



2.3. Výstupy předané Zákazníkovi

V rámci vytvoření metodiky pro identifikaci a hodnocení aktiv a pro hodnocení rizik budou Zákazníkovi předány následující výstupy.

- Popis metodiky pro identifikaci a hodnocení aktiv a pro hodnocení rizik

2.4. Místo realizace

Práce budou provedeny buď v kancelářích Dodavatele (např. práce na výstupech) nebo v lokalitách Zákazníka (jednání, workshopy, koordinace postupu a prezentace výstupů):

Generální finanční ředitelství
Lazarská 15/7
117 22 Praha 1

Generální finanční ředitelství
Nábřeží Kapitána Jaroše 1000/7
170 00 Praha 7 – Holešovice

případně i další lokality Zákazníka v rámci Prahy.

Nabídka zahrnuje cestovní náklady Dodavatele do uvedených lokalit Zákazníka.

3. Potřebná součinnost (vstupy od) Zákazníka

V kalkulaci projektu není zahrnut podíl práce Zákazníka na následujících činnostech nutných pro uskutečnění projektu, které musí provést spolu s Dodavatelem Zákazník. Celkový rozsah těchto potřebných součinností lze zhruba odhadnout do 5 mandays (MD). Pokud není uvedeno jinak, předpokládáme poskytování součinnosti zejména:

- Odpovědnými manažery v oblasti kybernetické / informační bezpečnosti
- Pracovníky, kteří jsou v pozici zadavatele hodnocení rizika nebo budou s výstupy hodnocení rizik dále pracovat

Je požadováno:

- Poskytnutí stávající dokumentace týkající se řízení (identifikace, hodnocení, zvládnání, ...) aktiv a rizik bezpečnosti informací.
 - Vč. příp. stávající metodiky v současnosti používané Zákazníkem pro řízení rizik
- Účast na workshopu pro identifikaci a odsouhlasení požadavků na metodiku
- Účast na předání výstupů projektu
- Připomínkování výstupních dokumentů
- Akceptace výstupních dokumentů a jejich převzetí



4. Nabídka nezahrnuje

- › Činnosti požadované jako součinnost Zákazníka dle předchozí kapitoly
- › Zavedení metodiky do praxe vč.:
 - › Úpravy, nebo vytvoření postupů nebo procesů Zákazníka
 - › Úpravy, nebo vytvoření interních řídicích dokumentů (např. pokynů, směrnic) Zákazníka
 - › Úpravy, nebo vytvoření dokumentů a šablon záznamů Zákazníka mimo dokumentů uvedených v kapitole Výstupy předané Zákazníkovi
- › Provádění činností dle vytvořené metodiky (např. provedení analýzy rizik)
- › Změnové požadavky nad rámec nabídky



5. Cena a harmonogram

5.1. Cena

Cena za předmět díla je:

194 040,- Kč bez DPH

(234 788,- Kč vč. DPH)

Platnost nabídky: 1 měsíc od data vyhotovení.

Splatnost faktur IXPERTA je 30 dnů.

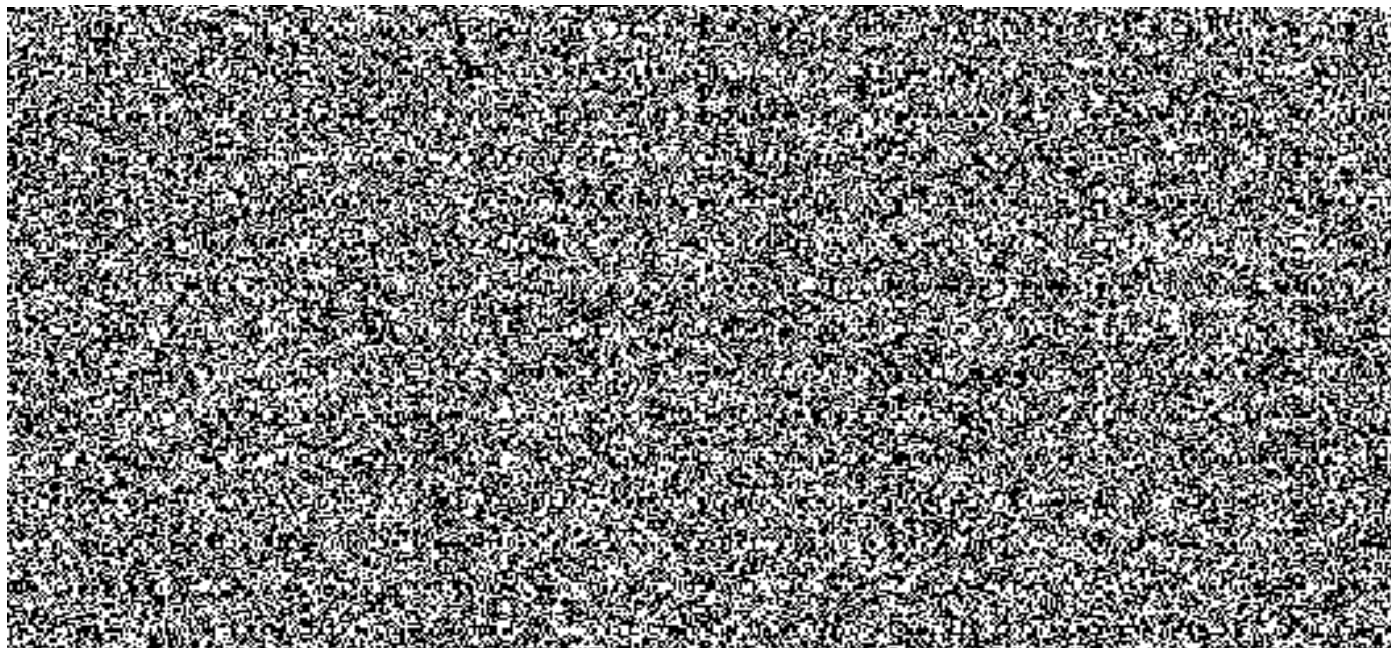
Fakturace po ukončení a předání projektu.

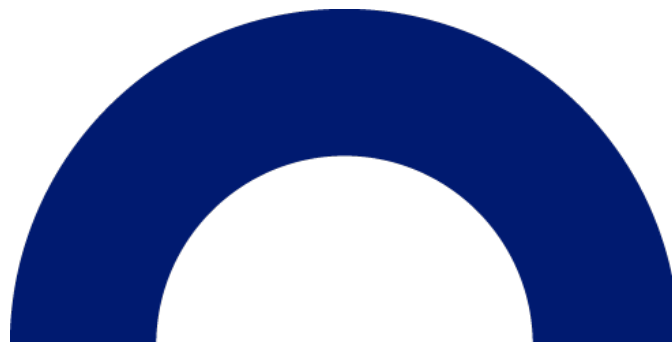
5.2. Orientační harmonogram prací

Za předpokladu optimální součinnosti Zákazníka budou práce provedeny cca do 6 týdnů. Zahájení projektu nejpozději do 2 týdnů od data objednání. Doporučujeme ponechat určitou projektovou rezervu.



6. Klíčoví členové realizačního týmu





O společnosti IXPERTA

Naše společnost IXPERTA působí na trhu informačních a komunikačních technologií 27 let. V našich týmech pracuje přes 250 expertů. Historicky jsme vznikli jako součást koncernu Siemens.

Propojujeme světy podnikových komunikací, infrastruktury, bezpečnosti a software. Máme certifikace od předních světových výrobců technologií a disponujeme vlastním vývojovým softwarovým centrem.

Zákazníky máme v České republice, na Slovensku, v Evropě, Asii a Severní Americe, a to ve všech typech organizací, od komerčních firem a výrobních podniků až po státní správu a finanční sektor.

