Nabídka na

Reaudit kybernetické bezpečnosti

systémů ASDŘ

pro

Dopravní podnik hl. m. Prahy,

akciová společnost

Dopravní podnik
hlavního města Prahy

27. 8. 2025

Nabídka společnosti:

Blue Partners s.r.o.
Postupická 2931/9, 141 00 Praha 4

Obsah:

1 Zadání

Dopravní podnik hl. m. Prahy, akciová společnost (dále jen DPP) provedlo audit kybernetické bezpečnosti v roce 2023. DPP je povinno zajistit audit minimálně 1x 2 roky. DPP požaduje provedení reauditu kybernetické bezpečnosti čtyř systémů ASDŘ (ASDŘ-D, ASDŘ-E, ASDŘ-O a ASDŘ-T) se zaměřením na prověření splnění nápravných opatření vyplývajících z předchozího auditu, a to dle vyhlášky č. 82/2018 Sb. k zákonu č. 181/2014 Sb. Tento audit nebude hodnotit stav dle nového kybernetického zákona č. 260/2025 Sb.

2 Nabídka služeb

Součástí reauditu jsou následující klíčové aktivity zaměřené na komplexní prověření implementace nápravných opatření z předchozího auditu:

2.1 Analýza výchozí dokumentace

- Předání a komplexní analýza dokumentace z předchozího auditu z roku 2023
- Identifikace všech doporučených nápravných opatření
- Kategorizace opatření podle priorit a závažnosti
- Příprava kontrolních seznamů pro ověření implementace

2.2 Ověřovací pohovory s odpovědnými osobami

- Strukturované rozhovory s garanty aktiv jednotlivých systémů
- Ověření znalostí a dodržování bezpečnostních postupů
- Kontrola dokumentace procesů a jejich praktické aplikace
- Hodnocení efektivity zavedených opatření

2.3 Posouzení souladu s legislativou

- Kontrola souladu implementovaných opatření s požadavky vyhlášky č. 82/2018 Sb.
- Identifikace případných nedostatků nebo neúplné implementace

2.4 Identifikace nedokončených opatření

- Analýza stavu implementace každého doporučeného opatření
- Kategorizace podle stupně dokončení (provedeno/částečně/nezavedeno)
- Návrh doplňujících kroků pro nedokončená opatření

2.5 Závěrečná zpráva

Zpracování komplexní zprávy "Prověření plnění nápravných opatření" obsahující:

- **Exekutivní shrnutí** s celkovým hodnocením pokroku
- **Detailní analýzu každého opatření** včetně:
  - Stavu implementace (provedeno/částečně/nezavedeno)
  - Hodnocení účinnosti a úplnosti
  - Identifikace rizik spojených s neimplementovanými opatřeními
- **Doporučení pro dokončení** nebo optimalizaci jednotlivých opatření
- **Přílohy** s důkazními materiály

3 Postup

- Podpis smlouvy
- Předání dokumentace
- Řízené pohovory se zodpovědnými osobami za aktiva
- Draft zprávy
- Diskuse nad zprávou s garanty
- Prezentace výstupů a předání zprávy

4 Součinnost

- Zajištění schůzek pro řízené pohovory s garanty aktiv a dalšími osobami
- Dodání požadované dokumentace jako jsou např.
  - Organizační struktura a řád
  - Aktuální vnitřní předpisy a směrnice týkající se IT
  - Bezpečnostní dokumentace včetně bezpečnostní politiky
  - Přehled bezpečnostních opatření
  - Řízení přístupu a identit
  - Seznam aktiv
  - Analýza dopadů na podnikání (BIA)
  - Řízení aktiv a řízení rizik (analýza rizik)
  - Seznam poskytovaných IT služeb
  - Síťová architektura (perimetr, propojení lokalit, VLANy, principy)
  - Zálohovací plán a jeho popis
  - DR plán (plány obnovy)
  - BCP plán (plán kontinuity)
  - Technickou dokumentaci k systémům ASDŘ
  - Záznamy o bezpečnostních aktivitách
  - Přehled dodavatelských vztahů a hlavní smlouvy (2-3 významné smlouvy)

5 Harmonogram

Popis	Termín	Řádový termín
Podpis smlouvy	D	4.9.2025
Zaslání dokumentace	D + 5	11.9.2025
Základní analýza dokumentace	D + 15	25.9.2025
Řízené interview, diskuze	D + 45	6.11.2025
Závěrečná zpráva, prezentace	D + 60	27.11.2025

D je den podpisu smlouvy a číslo je počet pracovních dnů.

6 Odhad náročnosti

Odhad časové náročnosti reauditu byl stanoven na základě prostudování předchozí auditní zprávy z roku 2023, základní analýzy rozsahu a komplexnosti identifikovaných nápravných opatření, zkušeností z obdobných auditů kybernetické bezpečnosti v obdobných organizacích.

6.1 Přípravná fáze (12-15 hodin)

- Analýza dokumentace z předchozího auditu
- Příprava kontrolních seznamů a testovacích scénářů
- Koordinace s kontaktními osobami DPP

6.2 Fáze terénního ověření (80-100 hodin)

- Ověření stavu nápravy ASDŘ-D
- Ověření stavu nápravy ASDŘ-E
- Ověření stavu nápravy ASDŘ-O
- Ověření stavu nápravy ASDŘ-T

6.3 Fáze vyhodnocení a reportingu (33-40 hodin)

- Analýza získaných dat
- Zpracování závěrečné zprávy
- Diskuze
- Prezentace výsledků

7 Závazek dodržení termínů

🎯 **Předání reauditní zprávy** nejpozději do **1. 12. 2025**

8 Cena

Položka	Počet hodin	Sazba Kč/hod	Cena celkem Kč
Základní rozsah reauditu	125	2.000	250.000 Kč
Rezerva pro nepředvídané situace	25	2.000	50.000 Kč
Celková maximální cena	**150**	**-**	300.000 Kč

8.1 Cenové podmínky

- **Základní cena:** 250.000 Kč bez DPH
- **Maximální cena včetně rezervy:** 300.000 Kč bez DPH
- **Rezerva bude využita** v případě výrazně vyšší náročnosti reauditu oproti původnímu odhadu, v případě prodlev v součinnosti ze strany DPP (nedodání dokumentace, nedostupnost klíčových osob)
- **Fakturace:** po předání a odevzdání závěrečné zprávy
- **Platební podmínky:** 30 dnů od vystavení faktury

9 Komunikační plán

9.1 Měsíční reporting

Cílová role: vedoucí odboru interního auditu
Formát: fyzický/online meeting + email report
Trvání: do 30 minut
Obsah:

- Stav reauditu
- Identifikované problémy a jejich řešení
- Plán na následujících 14dní/měsíc
- Požadavky na součinnost

10 Vybrané reference (bezpečnost)

Český rozhlas (veřejnoprávní instituce) *1 500 zaměstnanců*	Audit IT v rámci organizace, bezpečnostní konzultant
FoxConn (výrobní podnik) *5 000 zaměstnanců*	Datová analýza a klasifikace dat pro DLP
DIA (státní správa) 250 zaměstnanců	Bezpečnostní analýza služby CzechPoint
FN Motol (zdravotnictví) *5 000 zaměstnanců*	Katalog služeb, analýza GDPR, riziková analýza kybernetické bezpečnosti, návrh opatření
OVB Allfinanz (finanční poradenství) *100 zaměstnanců, 2 000 spolupracovníků*	Bezpečnostní politika, aktiva, DR plán, BC plán, phishing, test zranitelnosti, vzdělávání, DORA
SSGH (školství) *80 zaměstnanců*	Audit IT největší soukromé školy, vytvoření dokumentace aplikací, směrnice, BC plán, test zranitelnosti, phishing, vzdělávání uživatelů
VŠPJ (školství) *200 zaměstnanců*	Bezpečnostní analýza, bezpečnostní konzultant, penetrační testování, phishing, vzdělávání uživatelů
Městská část Praha 4 (veřejná správa) *350 zaměstnanců*	Hodnocení bezpečnosti, aktiva, riziková analýza, dokumentace IT systémů, phishing, vzdělávání uživatelů, penetrační testování
Povodí Labe (státní podnik) *600 zaměstnanců*	Riziková analýza a zavedení GDPR do organizace, včetně zavedení směrnic
Česká obchodní inspekce (státní správa) *400 zaměstnanců*	Riziková analýza a zavedení GDPR do organizace, včetně zavedení směrnic
ZŠ a MŠ Praha 4 (školství) *Celkem cca 1 500 zaměstnanců*	Hodnocení kybernetické bezpečnosti Analýza dopadů a zavedení GDPR
Statutární město Kladno (město) *550 zaměstnanců*	Analýza dopadů a zavedení GDPR, dokumentace IT systémů, klasifikace dat
Ústav experimentální medicíny (věda a výzkum) *220 zaměstnanců*	Analýza bezpečnosti IT a soulad s NIS2, bezpečnostní dokumentace
LLP Group (sw development) *100 zaměstnanců*	Analýza bezpečnosti IT a soulad s NIS2 a DORA
RKO Group holding (odpadové hospodářství) *100 zaměstnanců*	Analýza bezpečnosti IT a soulad s NIS2, bezpečnostní dokumentace
Technické služby Vlašim (městský podnik) *55 zaměstnanců*	Analýza bezpečnosti IT a soulad s NIS2

11 Proč analýzu s BP

Disponujeme kvalifikovanými pracovníky s vysokými odbornými znalostmi.

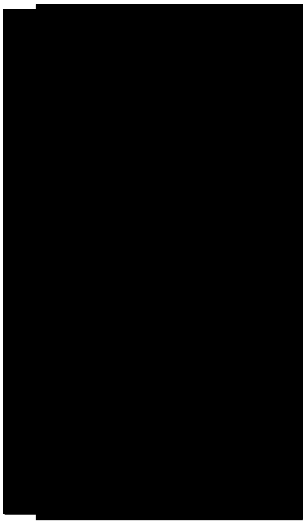
- více jak desetileté zkušenosti s vedením IT, analýzami, IT projekty a vývojem systémů
- 15 certifikovaných profesionálů s různým zaměřením (audity, procesy, řízení IT, infrastruktura, návrh a tvorba systémů, bezpečnost, vedení projektová kancelář),
- prověrka NBÚ na úroveň Důvěrné,
- vždy Vám otevřeně řekneme, co si o dané věci myslíme,
- děláme efektivní analýzy od malých firem po velké podniky, vždy s konkrétním zaměřením na danou firmu,
- máme široký záběr znalostí a problematik, které s analýzou IT přímo souvisí.

Nabízené plnění budou vykonávat osoby s následujícími kvalifikacemi:

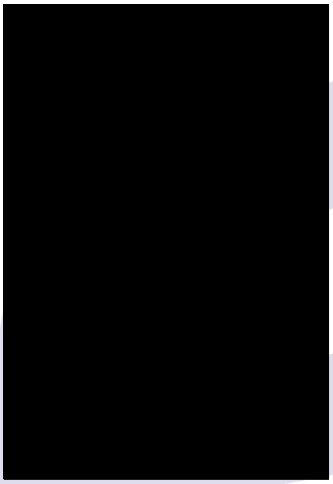
- Vysokoškolský titul
- Certifikace – ISMS lead auditor
- Certifikace – Manažer kybernetické bezpečnosti
- Certifikace – Auditor kybernetické bezpečnosti
- Certifikace – Architekt kybernetické bezpečnosti
- Certifikace – CIA – certifikovaný interní auditor

Doufáme, že Vás naše nabídka zaujala a těšíme se na případnou spolupráci. Pokud budete mít jakékoli dotazy, prosím, neváhejte nás kontaktovat na telefonním čísle [redacted]

Nebojte se nám svěřit.



Bezpečnost pro naše spokojené zákazníky.



12 Informace o společnosti

Společnost: **Blue Partners s.r.o.**
se sídlem: Postupická 2931/9, Záběhlice, 141 00 Praha 4
IČO: 27373622
Vedena u Městského soudu v Praze, oddíl C, vložka 109226

Profil společnosti:

Audit IT	Zjistíme, zda je ve vaší firmě řízeno IT optimálně. Prověříme, doporučíme, vysvětlíme.
Efektivní IT	Optimalizujeme fungování vašich informačních technologií. Zjednodušíme, zpřehledníme, zlevníme.
Outsourcing IT	Zbavíme vás starostí s IT. Přijedeme, dodáme, nastavíme, vyřešíme.
Projektová kancelář	Vedeme vaše projekty k úspěšné realizaci. Projektujeme, řídíme, kontrolujeme.
Vývoj aplikací	Proměníme vaše sny a přání do webové nebo mobilní aplikace. Naslouchámě, navrhneme, postavíme.

Certifikace společnosti:

ISO 9001 · ISO 20000 · ISO 27001 · PRINCE2 · CIA Certified Internal Auditor · Lead Auditor ISO 27001

Držitel osvědčení NBÚ č. 001683 Důvěrné (vznik)

Vybrané reference:

FN MOTOL · ČESKÁ OBCHODNÍ INSPEKCE · ZŠ A MŠ OHRADNÍ PRAHA 4, OHRADNÍ 49 · ÚZS VM · KLADNO MĚSTO PRO MODERNÍ ŽIVOT · Národní rozpočtová rada · TOYOTA LOUWMAN · Český rozhlas