Příloha č. 1
Podrobná specifikace Předmětu smlouvy

Předmětem smlouvy je provedení auditu Systému řízení bezpečnosti informací SPÚ na shodu tohoto systému řízení s požadavky zákona č. 181/2014 Sb., ve znění pozdějších předpisů, a návazné vyhlášky č. 82/2018 Sb. (o kybernetické bezpečnosti), v rozsahu povinností správce a provozovatele „významného informačního systému" dle § 3 písm. e) zákona.

Audit se skládá se z částí:

1. Příprava auditu

Na úvodních jednáních smluvních stran je projednána a oboustranně schválena příprava auditu, zejména v následujících oblastech:

- specifikace níže uvedených bodů 1, 3 – 5 (viz část 3. - Zpráva z auditu),
- věcně časový návrh „Plánu auditu SŘBI",
- Projednání specifik SPÚ a z toho plynoucích omezení a diferencí v provedení auditu mezi ústředím SPÚ a vybranými lokalitami SPÚ (kraje a pobočky krajů).

2. Vlastní provedení auditu

Fáze I. Audit dokumentovaných informací

V této části auditor/auditoři přezkoumává/jí zpřístupněnou základní dokumentaci k SŘBI. Nálezy z této fáze I. jsou prezentovány oprávněné osobě SPÚ před započetím fáze II. k případnému vyjasnění indikovaných neshod a možných sporných bodů.

Pozn.: zpřístupnění dokumentovaných informací z provozu, včetně případných náhledů do informačních systémů Objednatele, je prováděno při auditu na místě (ústředí SPÚ).

Fáze II. Audit na místě

Ve druhé části je auditor/auditoři seznámen/seznámeni na místech (viz bod 3.3 Smlouvy) s vlastním výkonem provozu SŘBI. Na základě auditních metod a postupů sbírají důkazy z provozu SŘBI, včetně auditních pohovorů se zaměstnanci SPÚ. Pro nezbytnou součinnost doprovodu auditorů na jednotlivých pracovištích/lokalitách jsou určeni zaměstnanci SPÚ. Tito průvodci mohou/nemusí být zároveň i auditovanými osobami.

V průběhu obou fází probíhá na základě komunikační matice nezbytná komunikace mezi oprávněnými osobami SPÚ a vedoucím auditorem, zejména k zajištění a zpřístupnění auditory požadovaných informací, a k zajištění další nezbytné součinnosti, zejména řešení nutnosti ad-hoc změn oproti schválenému plánu auditu (např. neplánovaná nepřítomnost auditovaných apod.).

3. Zpráva z auditu

Výstupem auditu je „Zpráva z auditu SŘBI", která obsahuje minimálně:

1. Základní informace (tým auditorů, oprávněné osoby SPÚ a jejich odpovědnost v rámci auditu, komunikační matice, aj.).
2. Stanovení cílů, předmětů, kritérií auditu a metrik hodnocení:
   - Cíl auditu

   Nezávislé kvalifikované ověření shody na SPÚ provozovaného SŘBI s požadavky zákona č. 181/2014 Sb. a návazné vyhlášky č. 82/2018 Sb. (o kybernetické bezpečnosti).

- Předmět auditu

Dokumentovaný a provozovaný Systém řízení bezpečnosti informací (SŘBI) v organizaci SPÚ – ústředí a vybrané další lokality.

- Kritéria auditu

Kritériem pro hodnocení SŘBI je plnění zákona č. 181/2014 Sb. (ZKB) a návazné vyhl. č. 82/2018 Sb. (VKB), o kybernetické bezpečnosti, na úrovni relevantních požadavků této legislativy, kladených na správce a provozovatele „významného informačního systému“ (VIS).

- Metriky hodnocení

Shoda = dokumentováno / prováděno (SPÚ plní požadavek ZKB/VKB pro kategorii VIS).

Neshoda = není dokumentováno / není prováděno (SPÚ neplní požadavek ZKB/VKB pro kategorii VIS).

Zaváděno = plnění požadavku ZKB/VKB pro kategorii VIS je v procesu zavádění (v plánu nebo v procesu implementace).

NR/NA = není relevantní/aplikovatelné pro SPÚ (jako správce a provozovatele VIS)

3. Metody a postupy auditu (navrhuje vedoucí auditor, odsouhlasí oprávněná osoba SPÚ).
4. Seznam požadovaných a seznam zpřístupněných dokumentovaných informací – tj. řídící dokumentace, plány a záznamy o jejich plnění a ostatní relevantní informace (navrhuje vedoucí auditor, odsouhlasí oprávněná osoba).
5. Proveditelnost a rizika auditu, opatření k jejich minimalizaci (identifikují a odsouhlasí obě strany).
6. Stanovený věcně-časový „Plán auditu SŘBI“ a jeho následné plnění (plán navrhuje vedoucí auditor, odsouhlasí oprávněná osoba SPÚ).
7. Zjištění z auditu – kompletní kontrolní tabulky („checklists“) stanovených požadavků ZKB/VKB, auditní zjištění a jejich vyhodnocení podle stanovených metrik hodnocení pro I. a II. fázi auditu.
8. Přezkoumání nalezených neshod s oprávněnou osobou SPÚ a (vyjádření SPÚ k neshodám a případné doplnění důkazů k jejich eliminaci).
9. Případné nevyřešené názorové rozdíly (konstatování „bez názorových rozdílů mezi auditory a oprávněnými osobami SPÚ“, nebo výčet nevyřešených názorových rozdílů mezi auditory a oprávněnými osobami SPÚ).
10. Návrhy auditu na další zlepšení (příležitosti ke zlepšení systému SŘBI).
11. Manažerské shrnutí pro vrcholové vedení SPÚ (shrnující manažerská SWOT tabulka a celkové stručné shrnutí výsledků auditu).

4. Distribuce zprávy z auditu

Distribuci finální Zprávy z auditu zajišťuje vedoucí auditor oprávněné osobě SPÚ v elektronické (PDF) a listinné podobě.

5. Prezentace výsledku auditu vrcholovému vedení SPÚ

V případě zájmu ze strany vrcholového vedení SPÚ provede vedoucí auditor prezentaci Zprávy z auditu.

6. Ukončení auditu a fakturace

Po splnění předchozích bodů a podpisu akceptačního protokolu ze strany oprávněné osoby SPÚ je provedena fakturace a úhrada faktury podle článku 5 Smlouvy.