PŘÍLOHA SMLOUVY O POSKYTOVÁNÍ SLUŽEB

SPECIFIKACE SLUŽEB INTERNÍHO AUDITU V OBLASTI INFORMAČNÍCH A KOMUNIKAČNÍCH SYSTÉMŮ A INFORMAČNÍ A KYBERNETICKÉ BEZPEČNOSTI V SZIF

A Provádění jednotlivých auditů

Během platnosti smlouvy budou provedeny 3 plnohodnotné samostatné interní audity v oblasti informačních a komunikačních systémů a informační a kybernetické bezpečnosti v SZIF (ve smyslu kapitoly 9. 2 „Interní audit" normy ČSN ISO/IEC 27001, v platném znění), vždy jeden v jednotlivých letech 2023 – 2025. Dle zkušeností pro provedení jednoho auditu je časový rozsah cca 20 MD (Man-day). Audity budou prováděny v souladu s metodikou Objednatele na základě parametrů definovaných v plánovací fázi respektive uvedených na objednávce a budou obsahovat minimálně tyto klíčové aktivity:

- plánovací příprava
- shromažďování informací
- hodnocení informačních a komunikačních systémů a informační a kybernetické bezpečnosti v SZIF
- prezentace výstupů.

Dle povahy auditu, především u auditů technického rázu, může dojít k rozšíření těchto metodik o metodiky a auditní manuály související s auditovaným prostředím/technologií.

V rámci poskytovaných Služeb bude Objednateli Poskytovatelem předána auditní dokumentace dle interních standardů Objednatele, případně dle interní metodologie Poskytovatele. Její součástí je především:

- organizace a interní předpisová základna
- plánování
- použité metodologie
- popis technologií a systémová schémata
- popis aplikací a aplikačních vazeb
- dokumentace auditních prací
- auditní zjištění
- návrh zprávy
- závěrečná zpráva.

Publikace zpráv bude prováděna dvoukolově:

- **Návrh zprávy** odsouhlasený interním auditem Objednatele bude distribuován představitelům auditovaných útvarů pro zpracování jejich připomínek, námětů a reakcí na auditní zjištění.
- **Závěrečná Zpráva** bude distribuovaná všem zainteresovaným osobám dle zvyklostí a postupů Objednatele.

Zpráva z auditu bude členěna rovněž v souladu s postupy Objednatele a bude obsahovat minimálně tyto komponenty:

- definici auditu (rozsah auditu)
- manažerské shrnutí
- přehled zjištěných nedostatků vč. identifikovaných rizik a navržených doporučení
- popis provedené auditorské práce
- auditní doložku.

Přesnější členění a formát výsledných zpráv bude dohodnut v rámci spolupráce.

Poskytovatel zajistí toto plnění nejméně dvěma auditory s tím, že každý z nich bude mít minimálně 6 let praxe (doloží životopisem) s prováděním auditů informačních a komunikačních systémů a informační a kybernetické bezpečnosti a alespoň jeden bude držitelem platného certifikátu Lead auditor ISMS, a alespoň jeden držitelem platného certifikátu CISA/CRISC/CISSP.

B Volné hodiny

Poskytovatel poskytne v průběhu trvání smlouvy auditory pro potřeby auditorského týmu Odboru interního auditu a vnitřní kontrola Objednatele v rozsahu až 360 pracovních hodin (tj. 45 člověkodní), kdy auditor Poskytovatele bude na vyžádání spolupracovat s interními auditory Objednatele i na ostatních interních auditech, jejichž cíle se mohou týkat prověření oblastí informačních a komunikačních systémů, bezpečnosti informací nebo kybernetické bezpečnosti. Kapacita auditorů může být Objednatelem též využita ve smyslu konzultací či školení poskytovaných k problematice uvedených oblastí. Objednatel požadovanou kapacitu auditorů oznámí Poskytovateli nejpozději 10 pracovních dní před plánovaným uskutečněním auditu či konzultace, pokud se s Poskytovatelem nedohodne jinak. Z vykonané činnosti vznikne výkaz práce a akceptační protokol, případně jiný výstup dle dohody smluvních stran.

Volné hodiny auditorů Poskytovatele jsou k dispozici Objednateli dle jeho potřeby.
Pro objednávání volných hodin auditorů Poskytovatele bude využíván následující mechanizmus:

- ohlášení potřeby minimálně 10 pracovních dní před plánovaným uskutečněním auditu či konzultace a dohodnutí parametrů poskytovaných služeb – například předmět služeb, termíny, případně další požadavky na poskytované služby
- vytvoření objednávky
- provedení služeb
- potvrzení poskytnutých služeb schválením definovaného výstupu
- fakturace

Poskytovatel zajistí toto plnění alespoň jedním auditorem, který bude držitelem platného certifikátu Lead auditor ISMS, platného certifikátu CISA/CRISC/CISSP (s ohledem na požadovanou potřebu) a bude mít minimálně 6 let praxe (doloží životopisem) s prováděním auditů informačních a komunikačních systémů a informační a kybernetické bezpečnosti.