PŘÍLOHA SMLOUVY O POSKYTOVÁNÍ SLUŽEB

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

A Plánování auditů

Ve spolupráci se zaměstnanci Odboru interního auditu Objednatele připraví Poskytovatel podklady pro plánování činnosti interního auditu v oblasti informačních a komunikačních systémů a informační a kybernetické bezpečnosti v SZIF na období 2018 – 2020. Pro roky 2018, 2019 a 2020 se Poskytovatel bude podílet na sestavení ročního plánu činnosti Odboru interního auditu upřesněním tříletého plánu pro dané roky, a to vždy v prosinci roku předcházejícího[1].

Plán interních auditů bude založen na základě posouzení specifických rizik. Prvotní posouzení rizik určí specifické oblasti, procesy nebo činnosti, které představují nejvyšší rizika. Hlavním výstupem bude plánovací dokumentace obsahující:

- identifikaci a zhodnocení rizikových oblastí IT prostředí
- cíl a rozsah interního auditu
- časový harmonogram auditů v předmětném období.

Podrobnosti této dokumentace budou dohodnuty v průběhu spolupráce. Výběr oblastí/procesů k samostatným auditům je v kompetenci Objednatele na základě doporučení Poskytovatele. Jednotlivé audity budou zadány formou samostatné objednávky, kde budou uvedeny základní parametry auditu.

Vzhledem k certifikaci Objednatele dle normy ČSN ISO/IEC 27001: 2014 budou pro plánování auditů v oblasti bezpečnosti informací primárně využity Zásady dobré praxe dle ČSN ISO/IEC 27001: 2014 a rozdělení bezpečnostních oblastí dle této normy při zohlednění podmínky zauditování všech prvků ISMS zavedeného v SZIF dle ČSN ISO/IEC 27001: 2014 do provedení prodlužovacího auditu certifikačním místem, tj. v průběhu tříletého období. Současně bude při plánování zohledněn rozsah normy ČSN ISO/IEC 20000-1:2012 spolu s požadavky zákona č. 181/2014 Sb. o kybernetické bezpečnosti.

Poskytovatel zajistí plnění této části zakázky alespoň jedním auditorem, který bude držitelem platného certifikátu Lead auditor ISMS a/nebo platného certifikátu CISA/CRISC/CISSP a bude mít minimálně 3 roky praxe (doloží životopisem) s prováděním auditů informačních a komunikačních systémů a informační a kybernetické bezpečnosti.

B Provádění jednotlivých auditů

Během platnosti smlouvy budou provedeny 3 plnohodnotné samostatné audity v oblasti informačních a komunikačních systémů a informační a kybernetické bezpečnosti v SZIF, vždy jeden v jednotlivých letech 2018 – 2020. Audity budou prováděny v souladu s metodikou Objednatele a metodikou provádění auditů ČSN EN ISO 19011:2003 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.

[1] Pro rok 2018 bude toto upřesnění součástí Plánu auditů na období 2018 až 2020.

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 dodávky 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 Odborem interního auditu 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
- manažerské shrnutí
- přehled zjištěných nedostatků vč. identifikovaných rizik a navržených doporučení
- detailní popis auditorské práce
- auditní doložku.

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

Poskytovatel zajistí plnění této části zakázky nejméně dvěma auditory, s tím, že alespoň 1 bude držitelem platného certifikátu Lead auditor ISMS a/nebo platného certifikátu CISA/CRISC/CISSP. Každý z auditorů bude mít minimálně 3 roky praxe (doloží životopisem) s prováděním auditů informačních a komunikačních systémů a informační a kybernetické bezpečnosti

C Volné hodiny

Poskytovatel poskytne v průběhu trvání smlouvy auditory pro potřeby auditorského týmu Odboru interního auditu Objednatele v rozsahu až 280 pracovních hodin (tj. 35 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 poskytovaných k problematice uvedených oblastí. Objednatel požadovanou kapacitu auditorů oznámí poskytovateli nejpozději 10 pracovních dní před plánovaným uskutečněním auditu či konzultace, pokud se se Poskytovatelem nedohodne jinak. Z vykonané činnosti vznikne výkaz práce a akceptační protokol, případně jiný výstup dle dohody.

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

- ohlášení potřeby a dohodnutí parametrů – definovat shodu nad osobami, předmětem prací, termíny případně parametry dodávky
- vytvoření objednávky dle dohodnutých parametrů
- provedení prací čerpáním hodin

- potvrzení dodávky schválením definovaného výstupu
- fakturace dle objednávky.

Poskytovatel zajistí plnění této části zakázky alespoň jedním auditorem, který bude držitelem platného certifikátu Lead auditor ISMS a/nebo platného certifikátu CISA/CRISC/CISSP a bude mít minimálně 3 roky praxe (doloží životopisem) s prováděním auditů informačních a komunikačních systémů a informační a kybernetické bezpečnosti.

D Harmonogram plnění zakázky

Bližší popis trvání jednotlivých fází je uveden v časovém harmonogramu dle jednotlivých let.

období	činnost
2018	Zpracování plánu na období 2018 – 2020
	1 x samostatný audit
	Upřesnění plánu pro rok 2019
	Samostatné hodiny dle potřeby
2019	1 x samostatný audit
	Upřesnění plánu pro rok 2020
	Samostatné hodiny dle potřeby
2020	1 x samostatný audit
	Samostatné hodiny dle potřeby