# 0 GAP analýza + architektura implementace opatření v rámci výzvy 10

Pro ověření detailního aktuálního stavu připravenosti úřadu na plnění požadavků zákona o kybernetické bezpečnosti a následnou přesnou definici detailní implementace opatření realizovaných v rámci tohoto projektu bude použita GAP analýza + architektura implementace opatření.

Metodika provedení rozdílové analýzy musí být založena na zjišťování stavu bezpečnostních opatření proti požadavkům jednotlivých paragrafů prováděcí vyhlášky kybernetického zákona č. 82 / 2018 Sb., detailním popisu stávajícího stavu.

* V první fázi proběhne rekognoskace prostředí krajského úřadu ve formě interview se správci a vlastníky aktiv, jejímž cílem je zmapování procesů a získání potřebných informací pro zpracování GAP analýzy. V této fázi proběhne intenzivní spolupráce odpovědných zaměstnanců krajského úřadu a smluvních partnerů s Dodavatelem.
* Ve druhé fázi jsou sesbíraná data porovnávána s požadavky ZKB, VKB a další platné legislativy a Dodavatel identifikuje a hodnotí zjištěné rozdíly.
* Na základě výsledků provedené rozdílové analýzy bude vypracován soubor dokumentů, který bude sloužit jako vodítko pro následnou realizaci jednotlivých dílčích celků projektu.

Výstupem bude:

1. Závěrečná auditní zpráva
2. Definice doporučených nápravných opatření s důrazem na opatření realizovaná v rámci výzvy č. 10
3. Doplněný / upravený plán zvládání rizik úřadu
4. Prováděcí dokumentaci implementace nápravných opatření realizovaných v rámci tohoto projektu, a to ve formě Low-level designu jednotlivých opatření.
5. Návrh jednotlivých akceptačních postupů pro jednotlivá realizovaná opatření projektu
6. Návrh akceptačních postupů pro souhrnné otestování dodaných a nakonfigurovaných opatření jako celku včetně penetračních testů a testů vulnerability

Prováděcí dokumentace musí obsahovat detailní popis realizace prováděných opatření včetně funkčního popisu konfigurací, ale i požadované úpravy, které bude nutné realizovat na stávající infrastruktuře, a to buď smluvním partnerem, nebo odpovědnými pracovníky zadavatele. (Tato dokumentace musí být rozčleněna dle funkčních celků a bude obsahovat požadavky na součinnost definované minimálně z pohledu lidských zdrojů, časového rozsahu a harmonogramu, spotřebního materiálu a omezení provozu.)

Akceptační postupy pro jednotlivá realizovaná opatření budou prováděna prostřednictvím automatizovaný scanů zranitelností pro jednotlivé opatření.

Souhrnné testování bezpečnosti na závěr celého projektu bude provedeno souborem penetračních testů ve formě whiteboxu, nebo greyboxu.

Následná implementace všech realizovaných nápravných opatření bude prováděna dle prováděcí dokumentace vytvořené v rámci této analýzy.

Soubor dokumentace je po schválení projektovým výborem zadavatele závazná pro další postup implementace. Jakékoli další změny projektové dokumentace budou možné pouze na základě schválení řídícího výboru projektu.

| *Požadavky na provedení činností* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| --- | --- | --- |
| **Seznámení se s prostředím Zadavatele** | | |
| Specifikace klíčových činností, procesů a struktur Zadavatele | ANO |  |
| Definice odpovědných osob na straně Zadavatele | ANO |  |
| Zpřesnění požadavků na součinnost odpovědných osob na straně Zadavatele | ANO |  |
| Omezení součinnosti jednotlivých pracovníků Zadavatele | max. 5 hodin týdne |  |
| Složení týmu provádějící realizaci opatření | min. 3 |  |
| Požadovaná odbornost člena týmu | min. 1x certifikovaný Lead Auditor |  |
| Požadovaná odbornost člena týmu | min. 1x certifikovaný Auditor |  |
| U každého jednání se Zadavatelem přítomni | min. 2 členové týmu |  |
| Písemná zpráva o stavu činnosti | min. 1x za týden, pokud není jednání v místě plnění |  |
| Jednání se Zadavatelem v místě plnění | min. 2x měsíčně |  |
| **Popis KII/VIS systému Zadavatele** | | |
| Detailní popis činností, procesů a ICT systémů vztažených k VIS | ANO |  |
| **Revize / Definice Aktiv ve smyslu ZKB** | | |
| Zjištění postupu definice Aktiv, jejich revize ve smyslu aktuálního ZKB (hodnocení z pohledu Důvěrnosti, Dostupnosti, Integrity) | ANO |  |
| Zjištění podpůrných aktiv systémů KII/VIS | ANO |  |
| **Sběr informací – místní šetření** | | |
| Kolektování informací Organizačních opatření | ANO |  |
| Kolektování informací Technických opatření ve vztahu k Aktivům ZKB | ANO |  |
| Zajištění informací dotčených třetích stran | ANO |  |
| **Revize / Definice Rizik ve smyslu ZKB** | | |
| Vypracování analýzy rizik | ANO |  |
| Plán zvládání rizik | ANO |  |
| Zhodnocení pokrytí rizik stávajícími technickými opatřeními | ANO |  |
| **Vyhodnocení a revize / definice nápravných opatření** | | |
| Zpracování závěrečné auditní zprávy | ANO |  |
| Definice doporučených nápravných opatření | ANO |  |
| Doplnění / úpravy plánu zvládání rizik úřadu | ANO |  |
| Vypracování prováděcí dokumentace doporučených nápravných opatření a podrobných technické vstupů ve formě low-level designu, pro implementaci technických opatření realizovaných v rámci projektu | ANO |  |
| Definice požadavků na součinnost odpovědných pracovníků zadavatele (lidské zdroje, časová náročnost, harmonogram, spotřební materiál a omezení provozu) | ANO |  |
| Definice požadavků na součinnost smluvních partnerů zadavatele (lidské zdroje, časová náročnost, harmonogram, spotřební materiál a omezení provozu) | ANO |  |
| Návrh jednotlivých akceptačních postupů pro jednotlivá realizovaná opatření projektu | ANO |  |
| Návrh akceptačních postupů pro souhrnné otestování dodaných a nakonfigurovaných opatření jako celku | ANO |  |
| Doba nutná pro provedení analytických prací včetně vyhotovení výsledných podkladů | Max. 90 dní |  |