

projekt_2578_Projektovy_zamer_detailny

PROJEKTOVÝ ZÁMER

Vzor pre manažérsky výstup I-02

podľa vyhlášky MIRRI č. 401/2023 Z. z.

Povinná osoba	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR Pribinova 25 811 09 Bratislava
Názov projektu	Rozširovanie riadenia IT aktív – ITAM 2.0
Zodpovedná osoba za projekt	Igor Hladík Vedúci oddelenia pre správu licencií a centralizované obstarávanie IT komodít Sekcia informačných technológií verejnej správy
Realizátor projektu	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR
Vlastník projektu	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR

Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Vypracoval	Igor Hladík	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR	Vedúci oddelenia pre správu licencií a centralizované obstarávanie IT komodít	31.7.2024	

1. História DOKUMENTU

Tabuľka 1 – História dokumentu

Verzia	Dátum	Zmeny	Meno
1.0	31.07.2024	Vydanie dokumentu	Igor Hladík

2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

2.1 Použité skratky a pojmy

V nasledujúcej tabuľke sú uvedené skratky a pojmy použité v tomto dokumente a jeho prílohách.

Tabuľka 2 – Použité skratky a pojmy

SKRATKA/POJEM	POPIS
AI	Artificial Intelligence (Umelá inteligencia)
APM	Application Portfolio Management (Riadenie aplikačného portfólia)
BYOL	Bring your own license (Prines si vlastnú licenciu)
BYOD	Bring your own device (Prines si vlastné zariadenie)
CSIRT	Computer Security Incident Response Team
DNS	Dynamický nákupný systém
DP	Data privacy (ochrana údajov)
HW	Hardvér
EULA	End-user License Agreement (Licenčná zmluva s koncovým používateľom)
FinOps	Cloud Financial Management (Finančné riadenie nákladov na cloud)
GDPR	General Data Protection Regulation (Všeobecné nariadenie o ochrane údajov)
IaaS	Infrastructure as a Service (Infraštruktúra ako služba)
IEC	International Electrotechnical Commission
IS ITAM	Informačný systém riadenia IT aktív
ISO	International Organization for Standardization
IT	Informačné technológie
IT aktíva	IT aktíva v kontexte tejto stratégie predstavujú primárne softvérové aktíva.
ITAM	IT Asset Management (Riadenie IT aktív)
ITVS	Informačné technológie verejnej správy
MIRRI / MIRRI SR	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR
OPEX	Prevádzkové náklady
OVM	Orgán verejnej moci
PaaS	Platform as a Service (Platforma ako služba)
SSL	Bezpečnostný protokol - Secure Sockets Layer
SW	Softvér
ÚPVII	Úrad podpredsedu vlády SR pre investície a informatizáciu
VO	Verejné obstarávanie
VS	Verejná správa
XaaS	Everything as a Service (Všetko ako služba)

3. DEFINOVANIE PROJEKTU

3.1 Manažérske zhrnutie

Organizácie štátnej a verejnej správy vynakladajú nemalé finančné prostriedky na nákup hardvéru a softvérových licencií s cieľom využívať softvérové aplikácie alebo informačné systémy. Taktovo vynaložené výdavky zároveň predstavujú nezanedbateľnú časť rozpočtu útvarov zodpovedných za riadenie informačných technológií jednotlivých orgánov verejnej moci – typicky náklady na licencie predstavujú cca. 30-35% z celkového rozpočtu organizácií na informačné technológie (okrem toho ďalších 15-20% predstavujú náklady súvisiace s prevádzkou cloudovej infraštruktúry, resp. cloudových zdrojov, ktorých využívanie sa v podmienkach štátnej správy SR začína taktiež postupne etablovať). Bežnou praxou však je, že ich efektívnej správe sa následne už nevenuje dostatočná pozornosť. V dôsledku toho organizácie v mnohých prípadoch nemajú dostatočný prehľad o skutočnom využívaní hardvéru (a jeho životnom cykle) a softvérových licencií, ako ani aj o skutočnej potrebe využívania týchto softvérov a ani o súvisiacej licenčnej potrebe. Takýto stav vytvára podmienky pre neefektívne hospodárenie a správu IT majetku štátu. Inými slovami organizácie buď platia za licencie, ktoré nepotrebujú alebo majú licencií nedostatok, čím dochádza k nesúladu s licenčnými podmienkami SW výrobcu. Samotní SW výrobcovia sú si vedomí situácie predstavujúcej nesúlady s ich licenčnými podmienkami a preto najmä v posledných rokoch výrazne zvyšujú intenzitu softvérových auditov, ktoré pre nich predstavujú ďalší zdroj príjmov. Táto prax, samozrejme, neobchádza ani Slovenskú republiku, a „vdáčným“ cieľom takýchto auditov sú práve orgány verejnej moci.

Problematika efektívneho riadenia IT aktív vo verejnej a štátnej správe bola bližšie predstavená, resp. naštartovaná v roku 2018, kedy v rámci Úradu podpredsedu vlády SR pre investície a informatizáciu vznikli nasledujúce základné dokumenty:

- Reformný zámer – Riadenie IT aktív vo verejnej správe.
- Koncepcia riadenia IT aktív v štátnej správe.
- Štúdiá uskutočniteľnosti.

V nadväznosti na uvedené iniciovalo následne Ministerstvo investícií, regionálneho rozvoja a informatizácie SR v roku 2022 projekt vybudovania centrálnej kompetencie riadenia IT aktív, ktorý pozostáva z nasledujúcich častí (ďalej tiež ako ITAM 1.0):

1. Implementáciu informačného systému riadenia IT aktív (ďalej tiež ako „IS ITAM“) – ukončený v 12/2023 (prevádzka IS bude ukončená v zmysle platnej zmluvy v 10/2024).
2. Zabezpečenie expertných služieb v oblasti optimalizácie IT aktív (ktorá zahŕňa okrem iného aj vybudovanie centrálnej kompetencie riadenia IT aktív v štátnej správe) – ukončený v 08/2024.

V rámci neho boli stanovené nasledujúce najdôležitejšie ciele:

- Výrazné zníženie nákladov na obstarávanie a využívanie softvérov a súvisiacich licencií.
- Štandardizácia nástrojov na zber a evidenciu IT aktív
- Štandardizácia procesov týkajúcich sa životného cyklu IT aktív v rámci verejnej a štátnej správy.
- Centrálne evidencie nainštalovaných, využívaných a pripojených IT aktív aktualizovaných skoro v reálnom čase.
- Identifikácia nepovoleného hardvéru a softvéru pripojeného do internej siete verejnej správy.
- Možnosť centrálne vyhodnocovať bezpečnostné riziká, licenčný súlad a identifikovať potenciálne riziká nesúlady a pod.
- Optimalizácia IT aktív naprieč verejnou správou.
- Zvyšovanie povedomia, znalostí a kompetencií zamestnancov verejnej správy v oblasti licenčnej problematiky, súvisiacich rizikách ako aj jej efektívnom riadení.

V čase prípravy tohto dokumentu je implementácia IS ITAM dokončená, pričom k tejto kompetencii centrálneho riadenia IT aktív je pripojených 14 orgánov verejnej moci (ďalej tiež ako „OVM“), ktoré celkovo poskytujú dáta do IS ITAM približne z 30 000 zariadení vrátane osobných počítačov a serverov (fyzických a virtuálnych). Expertné služby pokračujú, pričom ich ukončenie v zmysle platnej zmluvy je stanovené na August 2024.

Už prvé dáta v IS ITAM a aktivity smerujúce k optimalizácii licenčného portfólia a zabezpečenia licenčného súladu ukazujú o významnej opodstatnenosti tejto iniciatívy, jej nevyhnutnom pokračovaní a ďalšom rozširovaní. Ako príklad možno uviesť niektoré úvodné zistenia z jedného pripojeného OVM:

- Potenciál na optimalizáciu jedného vybraného softvérového produktu jedného výrobcu softvéru vo výške takmer 160 000 EUR.
- Nainštalovaných 59 rôznych softvérov (vrátane rôznych verzií) na prácu s PDF súbormi.
- 2334 inštalácií rôznych softvérov, ktoré sú už bez podpory výrobcov týchto softvérov, čo z hľadiska riadenia kybernetickej bezpečnosti predstavuje významné bezpečnostné riziko.

V nadväznosti nielen na tieto úvodné zistenia, identifikované ďalšie prevádzkové potreby OVM v oblasti riadenia IT ale aj najnovšie globálne trendy v oblasti riadenia IT aktív, je predmetom tohto projektového zámeru:

- Pripájanie ďalších OVM k tejto centrálnej kompetencii riadenia IT aktív, pričom cieľový stav pripojených zariadení je stanovený na 150 000.
- Riadenie a optimalizácia aplikačného portfólia, ktorá okrem iného poskytne prepojenie fyzickej vrstvy softvérov dostupnej v IS ITAM s aplikačnou a biznis vrstvou zahŕňajúcou procesy, biznis služby a životné situácie (napr. v prostredí MetaIS), čím sa zabezpečia informácie v reálnom čase o technickom zdraví týchto aplikácií. Tie budú ďalej rozširované o biznis hodnotu, ktorú tieto aplikácie prinášajú svojím používateľom, čo je základom pre prípadnú optimalizáciu, konsolidáciu a modernizáciu aplikačného portfólia štátu.
- Riadenie softvérových zraniteľností, t.j. rozšírenie IS ITAM o modul riadenia softvérových zraniteľností a súvisiacu úpravu prevádzkového modelu riadenia IT aktív.
- Zabezpečenie efektívneho riadenia cloudových služieb a zavedenie finančného riadenia cloudových služieb, tzv. FinOps.

Implementácia týchto iniciatív predpokladá využitie finančných prostriedkov najmä z Programu Slovensko, pričom časový harmonogram ich implementácie je nastavený na obdobie 36 mesiacov (v období rokov 2025-2028) s predpokladanou finančnou potrebou vo výške **15 273 169 EUR bez DPH**. Okrem toho predložená CBA uvažuje s ďalšími nákladmi na interné zdroje MIRRI SR ako aj vybrané OVM v celkovej výške **474 179 EUR**. Tieto ďalšie náklady predstavujú náklady na ľudí, ktorí budú aktívne participovať na projekte (ako napr. projektový manažér za MIRRI SR, biznis vlastníka, vlastníka procesov, zástupca za riadenie architektúry, bezpečnosti a pod.) a nebudú hradení zo štátneho rozpočtu, ale podľa ich participácie na projekte, ktorá bude adekvátne hradená a bude obsiahnutá v Zmluve o spolupráci.

Už z povahy projektu a jeho záberu naprieč mnohými organizáciami štátnej a verejnej správy bude projekt realizovaný prostredníctvom národného projektu.

3.2 Motivácia a rozsah projektu

3.2.1 Motivácia a ciele

Problematika efektívneho riadenia IT aktív vo verejnej a štátnej správe bola bližšie predstavená, resp. naštartovaná v roku 2018, kedy v rámci Úradu podpredsedu vlády SR pre investície a informatizáciu (ďalej tiež ako „ÚPVII“) vznikli dva základné dokumenty:

- Reformný zámer – Riadenie IT aktív vo verejnej správe.
- Konceptia riadenia IT aktív v štátnej správe.

V rámci týchto dokumentov boli predstavené nasledujúce základné piliere riadenia IT aktív vrátane:

- Vybudovanie kompetencie riadenia IT aktív v štátnej správe.
- Riadenie IT aktív v štátnej správe:
 - Implementácia systému riadenia hardvérových aktív.
 - Implementácia systému riadenia softvérových aktív.

príčom sa predpokladalo, že riadenie IT aktív bude implementované v prostredí všetkých ústredných orgánov štátnej správy čo z hľadiska objemu predstavovalo v tom čase približne 150 000 zariadení vrátane stolných počítačov, notebookov, a serverov (fyzických, virtuálnych), pričom podľa v tom čase dostupných údajov všetky ústredné orgány štátnej správy vynakladali celkovo na softvér, čo zahŕňa poplatky za licencie, údržbu a podporu približne 100 000 000 EUR ročne.

V nadväznosti na uvedené pripravilo Ministerstvo investícií, regionálneho rozvoja a informatizácie SR (ďalej tiež ako „MIRRI SR“ alebo „MIRRI“) štúdiu uskutočniteľnosti, ktorá zastrešovala implementáciu informačného systému riadenia IT aktív (časť softvérové aktíva) a vybudovanie centrálnej kompetencie riadenia IT aktív vo verejnej správe, na základe ktorej vyhlásila v roku 2022 dve verejné obstarávania:

1. Implementácia informačného systému riadenia IT aktív.
2. Poradenské služby v oblasti optimalizácie IT aktív (ktorá zahŕňa okrem iného aj vybudovanie centrálnej kompetencie riadenia IT aktív v štátnej správe).

príčom celkový objem z hľadiska počtu pripojených a manažovaných zariadení bol stanovený na 40.000.

Dôvodom pre spustenie, resp. pokračovanie existujúceho projektu a jeho ďalšie rozširovanie je skutočnosť, že organizácie štátnej a verejnej správy, tak ako je uvedené vyššie, vynakladajú nemalé finančné prostriedky na nákup hardvéru a softvérových licencií s cieľom využívať softvérové aplikácie alebo informačné systémy. Takto vynaložené výdavky zároveň predstavujú nezanedbateľnú časť rozpočtu útvarov zodpovedných za riadenie informačných technológií jednotlivých orgánov verejnej moci – typicky predstavujú náklady na licencie cca. 30-35% z celkového rozpočtu organizácií na informačné technológie (okrem toho ďalších 15-20% predstavujú náklady súvisiace s prevádzkou cloudovej infraštruktúry, resp. cloudových zdrojov, ktorých využívanie sa v podmienkach štátnej správy SR začína taktiež postupne etablovať). Bežnou praxou však je, že ich efektívnej správe sa následne už nevenuje dostatočná pozornosť. V dôsledku toho organizácie v mnohých prípadoch nemajú dostatočný prehľad o skutočnom využívaní hardvéru (a jeho životnom cykle) a softvérových licencií, ako ani aj o skutočnej potrebe využívania týchto softvérov (ďalej len „SW“) alebo informačných systémov a aplikácií a ani o súvisiacej licenčnej potrebe. Takýto stav vytvára podmienky pre neefektívne hospodárenie a správu IT majetku štátu.

Inými slovami organizácie buď platia za licencie, ktoré nepotrebnú alebo majú licencií nedostatok, čím dochádza k nesúladu s licenčnými podmienkami SW výrobcu. Vyplýva to najmä zo skutočnosti, že po úvodnom nákupe licencií (napr. v prípade realizácie interných projektov rozširovania alebo zmeny IT infraštruktúry) sa ich následnej správe nevenuje dostatočná, resp. žiadna pozornosť, keďže jednotlivé OVM nemajú dostatočné personálne ani odborné kapacity, aby túto oblasť mohli pokrývať v požadovanom rozsahu a kvalite. Samotní SW výrobcovia sú si vedomí situácie predstavujúcej nesúlada s ich licenčnými podmienkami a preto najmä v posledných rokoch výrazne zvyšujú intenzitu softvérových auditov, ktoré pre nich predstavujú ďalší zdroj príjmov. Táto prax, samozrejme, neobchádza ani Slovenskú republiku, a „vďaka“ cieľom takýchto auditov sú práve OVM.

V tomto kontexte čiastkové ciele riadenia IT aktív zostávajú nezmenené, resp. sa ďalej rozširujú. Celkovo ich možno zhrnúť do nasledujúcich bodov:

- Výrazné zníženie nákladov na obstarávanie a využívanie softvérov a súvisiacich licencií.
- Štandardizáciu nástrojov na zber a evidenciu IT aktív v rámci verejnej a štátnej správy.
- Štandardizáciu procesov týkajúcich sa životného cyklu IT aktív v rámci verejnej a štátnej správy.
- Elimináciu manuálnych úloh a/alebo výrazné zníženie lokálnej administratívnej záťaže na úrovni jednotlivých OVM spojenej so životným cyklom IT aktív.
- Výrazné zníženie vplyvu ľudského faktora na sledovanie životného cyklu IT aktív na lokálnej úrovni.
- Centrálne evidenciu nainštalovaných, využívaných a pripojených IT aktív aktualizovanú skoro v reálnom čase.
- Možnosť centrálne vyhodnocovať bezpečnostné riziká vyplývajúce zo známych softvérových zraniteľností nainštalovaného softvéru.
- Možnosť centrálne vyhodnocovať licenčný súlad a identifikovať potenciálne riziká nesúladu.
- Možnosť využitia dostupných údajov pre ďalšiu analýzu a identifikáciu optimalizácie a znížovania nákladov na IT aktíva vo verejnej správe.
- Na základe centralizovaných údajov možnosť optimalizovať IT aktíva naprieč verejnou správou.
- Zvyšovanie povedomia, znalostí a kompetencií zamestnancov verejnej správy v oblasti licenčnej problematiky, súvisiacich rizikách ako aj jej efektívnym riadením.
- Meranie technického zdravia a biznis hodnoty softvérov a aplikácií používaných vo verejnej a štátnej správe v kontexte riadenia enterprise architektúry.

3.2.2 Rozsah projektu

V nadväznosti na informácie uvedené vyššie, identifikované ďalšie prevádzkové potreby OVM v oblasti riadenia IT ale aj najnovšie globálne trendy v oblasti riadenia IT aktív, je predmetom tohto projektového zámeru:

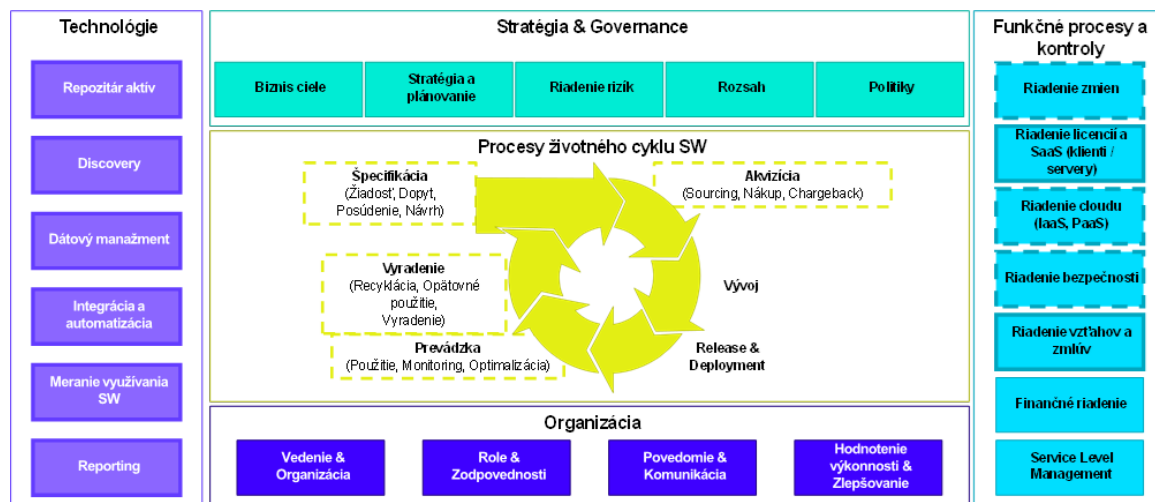
- Pripájanie ďalších OVM k tejto centrálnej kompetencii riadenia IT aktív, pričom cieľový stav pripojených zariadení je stanovený na 150 000.
- Riadenie a optimalizácia aplikačného portfólia, ktorá okrem iného poskytne prepojenie fyzickej vrstvy softvérov dostupnej v IS ITAM s aplikačnou a biznis vrstvou zahŕňajúcou procesy, biznis služby a životné situácie (napr. v prostredí MetalS), čím sa zabezpečia informácie v reálnom čase o technickom zdraví týchto aplikácií. Tie budú ďalej rozširované o biznis hodnotu, ktorú tieto aplikácie prinášajú svojim používateľom, čo je základom pre prípadnú optimalizáciu, konsolidáciu a modernizáciu aplikačného portfólia štátu. Súčasťou bude detailná analýza všetkých softvérových nákupov pripojených OVM na úrovni jednotlivých objednávok (za posledných 12 až 36 mesiacov) a ich mapovanie na identifikované softvéry a aplikácie v aplikačnom portfóliu OVM, ktoré budú ďalším vstupom pre návrh jednej z optimalizačných stratégií, tzv. 7Rs vrátane: Retain, Replatform, Rehost, Relicence, Retire, Refactor a Relocate.
- Riadenie softvérových zraniteľností, t.j. rozšírenie IS ITAM o modul riadenia softvérových zraniteľností a súvisiacu úpravu prevádzkového modelu riadenia IT aktív.
- Zabezpečenie efektívneho riadenia cloudových služieb a zavedenie finančného riadenia cloudových služieb, tzv. FinOps.

3.2.3 Biznis procesy / Koncové služby

Riadenia IT aktív v podmienkach Slovenskej republiky vychádza z globálneho rámca riadenia IT aktív spoločnosti SoftwareOne (dodávateľ projektu ITAM 1.0), ktorý je postavený na štandarde ISO/IEC 19770-1:2017 - Information technology — IT asset management (viď **Schéma 1 – Rámec pre riadenie IT aktív**), pričom tento rámec adresuje a ďalej rozširuje existujúce biznis procesy a koncové služby.

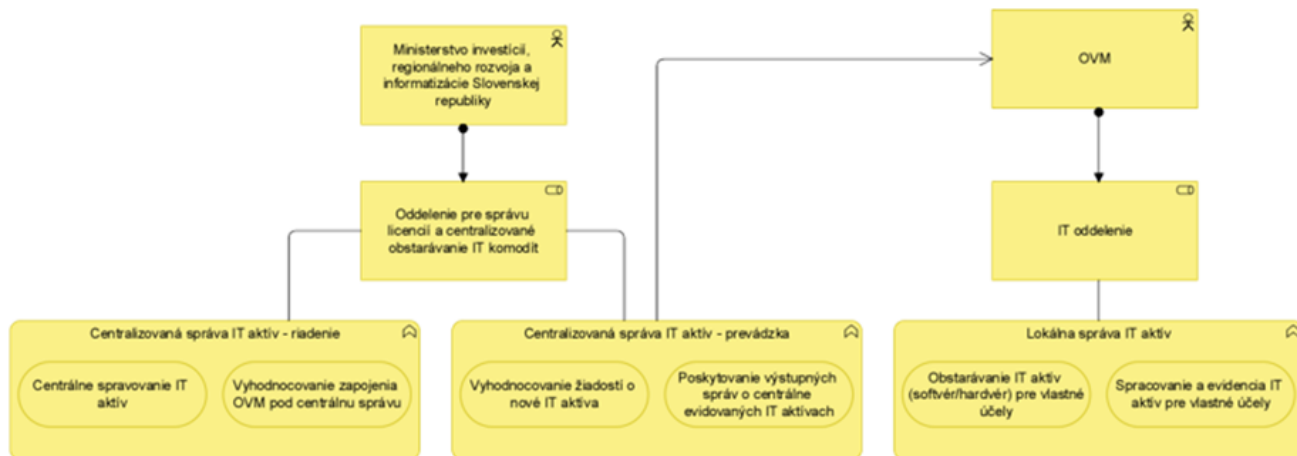
V kontexte zavedeného informačného systému riadenia IT aktív treba rozlišovať oblasti rámca, ktoré 1) sú priamo a plnohodnotne podporované zo strany IS ITAM (zvýraznené hrubou čiarou), 2) sú podporované zo strany IS ITAM len čiastočne (zvýraznené čiarokvanou čiarou), t.j. danú oblasť kvalitatívne dopĺňajú z pohľadu riadenia IT aktív, resp. existujú biznis procesy mimo IS ITAM, ktoré pre svoju potrebu čerpajú dáta z IS ITAM a 3) zo svojej povahy nie sú IS ITAM podporované vôbec, resp. sú pokryté organizačno-procesným zabezpečením mimo informačného systému.

Schéma 1 – Rámec pre riadenie IT aktív



Uvedený rámec riadenia IT aktív plne podporuje existujúce koncové služby, ktoré boli definované už pre projekt ITAM 1.0 a zároveň ich rozširuje o nové služby, ktoré reflektujú identifikované potreby uvedené v kapitole 3.2.2 Rozsah projektu. Takto je možné existujúce aj nové koncové služby graficky znázorniť nasledovne.

Schéma 2 – Schéma koncových služieb IS ITAM



V nasledujúcej tabuľke sú koncové služby bližšie popísané a namapované na konkrétne oblasti rámca riadenia ITAM

Tabuľka 3 – Namapovanie koncových služieb na rámec ITAM

Met a IS ID	Stav	Koncová služba	Oblasti koncovej služby	Oblasť rámca riadenia ITAM
ks_336642	Existujúca služba	Centrálné spravovanie IT aktív	Sken hardvérových aktív pripojených OVM	<ol style="list-style-type: none"> 1. Repozitár IT aktív 2. Discovery 3. Integrácia a automatizácia 4. Dátový manažment
			Sken softvérových aktív pripojených OVM	<ol style="list-style-type: none"> 1. Repozitár IT aktív 2. Discovery 3. Integrácia a automatizácia 4. Dátový manažment
			Jednotný prehľad o prevádzkovaných a využívaných cloudových službách SaaS.	<ol style="list-style-type: none"> 1. Riadenie licencií a SaaS 2. Špecifikácia 3. Reporting 4. Riadenie vzťahov a zmlúv
			Platforma pre zadanie nákupných dokladov	<ol style="list-style-type: none"> 1. Riadenie licencií a SaaS 2. Riadenie vzťahov a zmlúv 3. Dátový manažment

			Platforma pre zobrazenie licenčných rizík (t.j. identifikácia nainštalovaného softvéru, ktorý nie je pokrytý nákupným dokladom)	<ol style="list-style-type: none"> 1. Riadenie licencií a SaaS 2. Riadenie cloudu (IaaS/PaaS) 3. Reporting
			Platforma pre zobrazenie skutočného využívania nainštalovaného softvéru používateľom pre potreby optimalizácie budúcich nákupov.	<ol style="list-style-type: none"> 1. Riadenie licencií a SaaS 2. Riadenie cloudu (IaaS/PaaS) 3. Meranie využívania SW 4. Reporting 5. Odstránenie
			Platforma pre identifikáciu o aktuálnych softvérových zraniteľnostiach a ich mitigácií (Nová aplikačná služba, ktorá obohacuje koncové služby o tieto kapability).	<ol style="list-style-type: none"> 1. Riadenie bezpečnosti 2. Riadenie rizík 3. Riadenie zmien 4. Prevádzka 5. Vyraďovanie
			Platforma pre riadenie cloudových služieb a zdrojov (Nová aplikačná služba, ktorá obohacuje koncové služby o tieto kapability).	<ol style="list-style-type: none"> 1. Riadenie cloudu (IaaS, PaaS) 2. Finančné riadenie
			Platforma pre optimalizáciu aplikačného portfólia (Nová aplikačná služba, ktorá obohacuje koncové služby o tieto kapability).	<ol style="list-style-type: none"> 1. Špecifikácia 2. Akvizícia 3. Prevádzka 4. Vyraďovanie 5. Riadenie zmien 6. Dátový manažment
ks_336640	Existujúca služba	Poskytovanie výstupných správ o centrálne evidovaných IT aktívach	Zoznam používateľov jednotlivých aplikácií a náhľad posledného použitia aplikácie používateľom	<ol style="list-style-type: none"> 1. Reporting 2. Meranie využívania SW
			Náhľad maximálneho počtu a minimálneho počtu súbežných používateľov aplikácie pre licenčnú metriku súbežných používateľov	<ol style="list-style-type: none"> 1. Reporting 2. Riadenie licencií a SaaS 3. Riadenie cloudu (IaaS/PaaS)
			Sumár licenčného súladu	<ol style="list-style-type: none"> 1. Reporting 2. Riadenie licencií a SaaS
			Zobrazenie všetkých používateľských účtov na jednom zariadení, zoznamu aplikácií na jednom zariadení, celkovej ceny jedného zariadenia (hardvér + softvér), a dátumu posledného skenovania daného zariadenia	<ol style="list-style-type: none"> 1. Reporting
			Náhľad zobrazujúci celkový počet Microsoft Office 365 používateľov za obdobie minimálne posledných 12 mesiacov	<ol style="list-style-type: none"> 1. Reporting 2. Riadenie licencií a SaaS

			Náhľad zobrazujúci detaily využitia Microsoft Office 365 (používatelia, ktorí nevyužívajú svoj prístup, používatelia, ktorí by mali zmeniť úroveň svojho prístupu na základe využitia a cenu špecifickej úrovne prístupu)	<ol style="list-style-type: none"> 1. Reporting 2. Riadenie licencií a SaaS 3. Meranie využívania SW 4. Odstránenie
			Zobrazenie informácie o zostávajúcich voľných licenciách zvlášť pre každý softvér	<ol style="list-style-type: none"> 1. Reporting 2. Riadenie licencií a SaaS
			Sumárny náhľad / prehľad o všetkom softvéri na úrovni rodiny softvéru	<ol style="list-style-type: none"> 1. Reporting 2. Riadenie licencií a SaaS
			Náhľad zobrazujúci identifikované softvérové zraniteľnosti, ich kategorizáciu a prioritizáciu, skóre rizikovosti s návrhmi na ich mitigáciu	<ol style="list-style-type: none"> 1. Reporting 2. Riadenie bezpečnosti 3. Riadenie rizík 4. Riadenie zmien
			Náhľad zobrazujúci analytické údaje za účelom podpory riadenia cloudových služieb a zdrojov	<ol style="list-style-type: none"> 1. Reporting 2. Finančné riadenie 3. Riadenie cloudu (IaaS / PaaS)
			Prehľad o aktuálnom aplikačnom portfóliu, jeho prevádzkových nákladoch, kategorizácií z hľadiska biznis/IT stratégie a ďalšom rozvoji	<ol style="list-style-type: none"> 1. Reporting 2. Riadenie zmien 3. Riadenie licencií a SaaS (klienti / servery) 4. Finančné riadenie 5. Akvizícia 6. Stratégia a plánovanie
ks_336643	Existujúca služba	Vyhodnocovanie zapojenia OVM pod centrálnu správu	Vyhodnotenie pripravenosti a spôsobu možnosti pripojenia OVM pod centrálnu správu IT aktív	N/A
			Pravidelné vyhodnocovanie kvality údajov (aktuálnosť a kompletnosť dát zo skenov agentov, aktuálnosť a kompletnosť dát z konektorov, kompletnosť nákupných dokladov)	<ol style="list-style-type: none"> 1. Dátový manažment
ks_336641	Existujúca služba	Vyhodnocovanie žiadostí o nové IT aktíva	Zoznam používateľov jednotlivých aplikácií a náhľad posledného použitia aplikácie používateľom	<ol style="list-style-type: none"> 1. Špecifikácia 2. Riadenie bezpečnosti 3. Prevádzka 4. Odstránenie 5. Meranie využívania SW 6. Reporting

	Náhľad maximálneho počtu a minimálneho počtu súbežných používateľov aplikácie pre licenčnú metriku súbežných používateľov	<ol style="list-style-type: none"> 1. Špecifikácia 2. Riadenie bezpečnosti 3. Prevádzka 4. Odstránenie 5. Meranie využívania SW 6. Reporting
	Sumár licenčného súladu	<ol style="list-style-type: none"> 1. Reporting 2. Riadenie licencií a SaaS
	Náhľad zobrazujúci celkový počet Microsoft Office 365 používateľov za obdobie minimálne posledných 12 mesiacov	<ol style="list-style-type: none"> 1. Reporting 2. Riadenie licencií a SaaS
	Náhľad zobrazujúci detaily využitia Microsoft Office 365 (používatelia, ktorí nevyužívajú svoj prístup, používatelia, ktorí by mali zmeniť úroveň svojho prístupu na základe využitia a cenu špecifickej úrovne prístupu)	<ol style="list-style-type: none"> 1. Špecifikácia 2. Akvizícia 3. Prevádzka 4. Odstránenie 5. Meranie využívania SW
	Informácie o zostávajúcich voľných licenciách zvlášť pre každý softvér	<ol style="list-style-type: none"> 1. Reporting

3.3 Zainteresované strany/Stakeholderi

V nasledujúcej tabuľke sú uvedení hlavní aktéri pre projekt ITAM 2.0. V rámci nich sú to primárne organizačné útvary riadenia informačných technológií najmä IT prevádzky, IT architektúry a IT bezpečnosti.

Tabuľka 4 – Zainteresované osoby

ID	AKTÉR / STAKEHOLDER	SUBJEKT (názov / skratka)	ROLA (vlastník procesu/ vlastník dát /zákazník/ užívateľ člen tímu atď.)	Informačný systém (MetaIS kód a názov ISVS)
1.	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR	MIRRI	Poskytovateľ služieb centrálného riadenia IT aktív	isvs_9597 Centrálny informačný systém na riadenie IT aktív
2.	Ďalšie ústredné orgány štátnej správy (ktoré doposiaľ neboli pripojené ku kompetencii centrálného riadenia IT	N/A	Poskytovateľ údajov Konzument údajov a expertných služieb	-
3.	Vybrané podriadené organizácie ústredných orgánov štátnej správy a štátne podniky, ktorých vlastníkom, prípadne jediným akcionárom je Slovenská republika	N/A	Poskytovateľ údajov Konzument údajov a expertných služieb	-
4.	Vybrané krajské mestá a samosprávne kraje vrátane vybraných ich podriadených organizácií	N/A	Poskytovateľ údajov Konzument údajov a expertných služieb	-

3.4 Ciele projektu

Čiastkové ciele uvedené v 3.2.1 Motivácia a ciele možno zosumarizovať do formálnych cieľov projektu uvedených v nasledujúcej tabuľke:

Tabuľka 5 – Ciele projektu

ID	Názov cieľa	Názov strategického cieľa	Spôsob realizácie strategického cieľa
01	Zníženie nákladov na obstarávanie, využívanie softvérov, licenčného nesúladu a súvisiacich licencií	Optimalizovať náklady verejnej správy, prioritnej osi 3 –Efektívne IT	Implementácia IS ITAM s využitím expertných znalostí v oblasti licenčnej optimalizácie v prostredí vybraných OVM s max. počtom zariadení do celkového počtu: 150 000 zariadení
02	Štandardizácia nástrojov na zber a evidenciu IT aktív v rámci verejnej a štátnej správy	Zvýšiť úžitkovú hodnotu informačných systémov verejnej správy počas ich životného cyklu, prioritnej osi 3 – Efektívne IT	Implementácia IS ITAM do prostredia vybraných OVM s max. počtom zariadení do celkového počtu: 150 000 zariadení.
03	Centrálna evidencia nainštalovaných, využívaných a pripojených IT aktív	Skrátiť čas na prípravu a doručenie služieb a výsledkov informačných systémov VS, prioritnej osi 3 – Efektívne IT	Implementácia IS ITAM do prostredia vybraných OVM s max. počtom zariadení do celkového počtu: 150 000 zariadení vrátane zavedenia prevádzkového modelu centrálneho riadenia IT aktív.
04	Zvyšovanie kybernetickej bezpečnosti technologického prostredia	Kybernetická bezpečnosť- Zvýšenie schopnosti včasnej identifikácie kybernetických incidentov vo verejnej správe	Implementácia IS ITAM vrátane nasadenia modulu Snow Risk Monitor do prostredia vybraných OVM s max. počtom zariadení do výšky 150 000 s cieľom identifikácie nepovoleného softvéru, identifikácie známych softvérových zraniteľností nainštalovaného softvéru a pod.
05	Optimalizácia a konsolidácia aplikačného portfólia prostredníctvom meranie technického zdravia, biznis hodnoty softvérov a aplikácií a duplicitných funkčností	Optimalizovať náklady verejnej správy, prioritnej osi 3 – Efektívne IT	Implementácia IS ITAM vrátane rozšírenia a využitia platformy Bizdesign Horizon v prostredí vybraných OVM s max. počtom zariadení do celkového počtu: 150 000 s využitím expertných znalostí v oblasti riadenia aplikačného portfólia.
06	Optimalizácia a znižovanie nákladov cloudových zdrojov	Optimalizovať náklady verejnej správy, prioritnej osi - 3 Efektívne IT	Implementácia IS ITAM vrátane nástroja pre riadenie cloudových zdrojov s využitím expertných znalostí v oblasti v oblasti FinOps v prostredí vybraných OVM s max. počtom zariadení do celkového počtu: 150 000 zariadení.
07	Poskytovanie úplných a spoľahlivých údajov o prostredí	Digitálna transformácia a lepšie údaje - Dobudovať digitálne prostredie založené na zdieľaní údajov vo verejnej správe	Implementácia IS ITAM do prostredia vybraných OVM s max. počtom zariadení do celkového počtu: 150 000 zariadení, vrátane nastavenia štandardných reportov a dashboardov o softvérovom ale aj hardvérovom stave IT prostredia.
08	Znížiť administratívnu záťaž pri spravovaní nástroja na riadenie IT aktív	Znížiť interakcie osôb a zložitosť pri používaní služieb verejnej správy, prioritnej osi 1 - Lepšie služby	Implementácia IS ITAM do prostredia vybraných OVM s max. počtom zariadení do celkového počtu: 150 000 zariadení vrátane zavedenia prevádzkového modelu centrálneho riadenia IT aktív.

3.5 Merateľné ukazovatele (KPI)

Ciele uvedené v predchádzajúcej kapitole možné adresovať prostredníctvom nasledujúcich merateľných ukazovateľov:

Tabuľka 6 – Merateľné ukazovatele projektu ITAM 2.0

ID	ID /Názov cieľa	Názov ukazovateľa (KPI)	Popis ukazovateľa	Merná jednotka	AS IS merné hodnoty (aktuálne)	TO BE Merné hodnoty (cieľové hodnoty)	Spôsob ich merania	Pozn.
01	01 - 08	Počet nových optimalizovaných úsekov verejnej správy – ústredné orgány verejnej správy a /alebo podriadené organizácie, VÚC, mesto/obec	Zapojenie ďalších ústredných orgánov verejnej moci vrátane ich podriadených organizácií, VÚC, obec/mesto do 2027	OVN, VÚC, obec /mesto	14	40	IS ITAM	-
02	01	Zníženie nákladov na licencie	Zníženie nákladov zapojených OVM na licencie, údržbu a podporu	financie (€)	0	5%	Správa z licenčného posúdenia	Kvantifikovaná ročná úspora na základe priemerných ročných nákladov (za posl. 3 roky), ktoré budú známe v rámci realizácie projektu

03	01	Zníženie rizika licenčného nesúladu	Zníženie licenčného nesúladu z dôvodu nedodržiavania licenčných podmienok	financie (€)	0	20%	Správa z licenčného posúdenia	Kvantifikovaný licenčný nesúlad bude známy v rámci realizácie projektu
04	05	Zníženie počtu aplikácií	Zníženie počtu aplikácií využívaných OVM	Počet systémov a aplikácií	0	5%	IS ITAM	Súčasný počet aplikácií využívaných OVM bude známy po implementácii IS ITAM

3.6 Špecifikácia potrieb koncového používateľa

IS ITAM ako aj Bizdesign Horizon sú etablované riešenia v prostredí štátnej a verejnej správy SR. Okrem toho bude predstavená aj platforma FinOps na efektívne riadenie cloudových zdrojov. Ani jeden z uvedených systémov neprestavuje systém, s ktorým by do priameho kontaktu prichádzali občania alebo podnikatelia a zároveň sa nejedná o agendové informačné systémy. Hlavnými používateľmi týchto systémov sú dedikovaní pracovníci z organizačných útvarov riadenia IT z jednotlivých OVM najmä IT prevádzky, IT bezpečnosti, IT architektúry.

V prípade IS ITAM a Bizdesign Horizon sa jedná len o ďalšie rozširovanie a adopciu týchto riešení v prostredí štátnej a verejnej správy SR.

3.7 Riziká a závislosti

V nasledujúcej tabuľke sú uvedené riziká, ktoré môžu ovplyvniť úspešnosť realizácie projektu. Uvedené vychádza zo skúseností projektového tímu, ktorý sa podieľal na realizácii projektu ITAM 1.0:

Tabuľka 7 – Riziká a závislosti

ID	NÁZOV RIZIKA a ZÁVISLOSTI (O)	Kategória rizika a závislosti A1, A2, B1 - vysoká závažnosť A3, B2, C1 - stredná závažnosť B3, C2, C3 - nízka závažnosť	POPIS / NÁSLEDOK	MITIGAČNÉ OPATRENIA (ako - saurh riešenia)	ZODPOVEDNÝ (I/O)	TERMÍN	Pravdepodobnosť vzniku rizika / závislosti V - vysoká S - stredná N - nízka	Dopad rizika / závislosti F - Fatálny V - Významný S - stredný N - Nevýznamný	Odhad nákladov / Rozsah škôd pri vzniku rizika / závislosti (kaľka - hodnota v EUR)	Poznámka
1	Nedostatočné zapojenie organizácií do centrálneho riadenia ITAM a ich angažovanosť (poskytovanie informácií, pomáha nasaďovanie IS ITAM do prostredia OVM, dlhé odzvy predstavitel'ov OVM a pod.)	B2	Nenaplnenie cieľov a KPI projektu	1) Vysvetľovanie prínosov projektu, 2) Flexibilita v možných architektonických modeloch nasadenia IS ITAM, 3) Realizácia programu adopcie, 4) Komunikácia a podpora projektu od najvyššieho vedenia MBRRI	Igor Hladik (MBRRI SR)	TBD	S	V	TBD	

3.8 Stanovenie alternatív v biznisovej vrstve architektúry

Tak ako je uvedené vyššie, projekt ITAM 2.0 je len rozšírením a doplnením už existujúceho riešenia, preto nie je potrebné posudzovať rôzne alternatívy v biznisovej vrstve architektúry. Bližšie informácie k tejto časti sú uvedené v Detailnom návrhu riešenia IS ITAM – kapitola 5 Procesy podporované navrhovaným riešením a kapitola 6 Biznis architektúra riešenia.

Uvedené vychádza zo schválenej stratégie budúceho smerovania ITAMu v podmienkach verejnej správy SR, ktorý reflektuje na najnovšie potreby a trendy v oblasti IT a riadenia IT aktív. Navrhované komponenty a aplikačné služby taktiež vychádzajú z konkrétnych potrieb, ktoré boli identifikované u z zapojených OVM v rámci realizácie ITAM 1.0.

Snow Risk Monitor - Riadenie softvérových zraniteľností

Je to modul platformy Snow, Snow Risk Monitor. Snow Risk Monitor pomáha mitigovať bezpečnostné riziká tým, že porovnáva všetky softvéri inštalované v prostredí OVM s databázou známych softvérových zraniteľností NIST (National Institute of Standards and Technology). Riadenie softvérových zraniteľností, t.j. rozšírenie IS ITAM o modul riadenia softvérových zraniteľností a súvisiacu úpravu prevádzkového modelu riadenia IT aktív. Mať prehľad o nainštalovanom softvéri zahŕňa mať prehľad aj o rizikách, ktoré sú s ním spojené. Implementácia IS ITAM do prostredia jednotlivých OVM preukázala veľké množstvo nainštalovaných softvérov, ktoré sú už po dobe svojej životnosti čo predstavuje bezpečnostné riziko. Na uvedené zistenia a s nimi spojené bezpečnostné riziká je potrebné nadviazať ďalšou úrovňou riadenia ITAM, ktorou je poskytovanie informácií o všetkých zraniteľnostiach, ktoré sú s daným softvérom spojené, a ktoré je potrebné eliminovať, prípadne iným spôsobom mitigovať. Keďže komplexné a automatizované riadenie softvérových zraniteľností v prostredí verejnej a štátnej správy neexistuje, súčasťou ďalšieho rozvoja kompetencie ITAM by malo byť doplnenie modulu Snow Risk Monitor k súčasnej implementácii IS ITAM a zároveň v rámci prevádzkového modelu riadenia ITAM, nastavenie bližšej spolupráce medzi prevádzkou IT, resp. útvarmi zodpovednými za IT bezpečnosť pripojených OVM a nominovanými kľúčovými používateľmi ITAM za OVM, aby informácie zo Snow Risk Monitor boli efektívne využívané na zvyšovanie kybernetickej bezpečnosti pripojeného OVM.

FinOps – Riadenie cloudových zdrojov:

FinOps nástroj bude doplnený ako SaaS služba k existujúcemu IS ITAM. FinOps slúži na zabezpečenie efektívneho riadenia cloudových služieb a zavedenie finančného riadenia cloudových služieb. Potreba FinOps vychádza zo zvyšujúcej sa potreby zdrojov verejného cloudu a kopíruje najnovšie trendy s nástupom cloudových riešení a s celosvetovým trendom prechodu z on-premise riešení, resp. vlastných dátových centier do prostredia cloudu a využívania služieb IaaS alebo PaaS. Práve preto je rozšírenie ITAMu smerom k zabezpečeniu čo najefektívnejšieho využívania cloudových zdrojov nevyhnutné. V tomto kontexte bol etablovaný ako celosvetový štandard efektívneho riadenia cloudových zdrojov FinOps8 (z anj. Cloud Financial Management). Potreba komplexného a efektívneho riadenia cloudových zdrojov vychádza najmä z praxe, keďže skúsenosti so sveta ukazujú, že organizácie majú s riadením nákladov súvisiacich s cloudovou infraštruktúrou problémy. Priamu nadväznosť na tieto pravidlá, štandardy a konvencie má FinOps, ktorý predstavuje disciplínu, kombinujúcu princípy finančného riadenia s cloudovým inžinierstvom a jeho prevádzkou s cieľom poskytnúť organizáciám lepšie pochopenie ich výdavkov na cloud. Pomáha im tiež prijímať rozhodnutia o tom, ako pridelovať a spravovať svoje náklady na cloud, a zároveň umožňuje kontrolovať výdavky na cloud pri zachovaní úrovne výkonu, spoľahlivosti a zabezpečenia potrebnej na podporu ich biznis operácií.

Bizzdesign Horizon – Optimalizácia aplikačného portfólia:

Rozšírenie využitia platformy Bizzdesign Horizon, pričom z architektonického hľadiska nedochádza k žiadnym zmenám. Platforma Bizzdesign Horizon je už nasadená v prostredí štátnej a verejnej správy SR (napr. MIRRI, Ministerstvo financií SR a iné). V súčasnosti je využívaná najmä ako centrálny architektonický repozitár (aj pre potreby systému MetalS), pričom zameranie je na modelovanie biznis vrstvy ako sú napr. procesy, biznis služby a životné situácie a modelovanie referenčných architektur. Túto platformu je možné rozvinúť aj smerom k riadeniu aplikačného portfólia a tým maximalizovať jej pridanú hodnotu, keďže jej integrálnou súčasťou je aj komponent podporujúci kompetenciu Riadenia aplikačného portfólia. Z uvedeného vyplýva, že nie je potrebné zavádzať žiadnu novú APM technológiu, ktorá by v budúcnosti podporovala ITAM pilier. Platforma Bizzdesign je menovaná lídrom medzi nástrojmi pre enterprise architecture podľa spoločnosti Gartner (September 2023).

3.9 Multikriteriálna analýza

Neaplikované - viď predchádzajúcu kapitolu.

3.10 Stanovenie alternatív v aplikačnej vrstve architektúry

Tak ako je uvedené vyššie, projekt ITAM 2.0 je len rozšírením a doplnením už existujúceho riešenia, preto nie je potrebné posudzovať rôzne alternatívy v aplikačnej vrstve architektúry. Bližšie informácie k tejto časti sú uvedené v Detailnom návrhu riešenia IS ITAM – kapitola 10 Aplikačná architektúra.

Okrem architektonického riešenia uvedeného v Detailnom návrhu riešenia IS ITAM, t.j. riešenia postaveného na jednom centrálnom informačnom systéme, bude v rámci projektu ITAM 2.0 predstavený architektonický model umožňujúci implementáciu aj tzv. rezortných ITAM systémov, ktoré budú konsolidovať informácie za rezort. Informácie z týchto čiastkových ITAM systémov sa budú pre účely licenčnej optimalizácie naprieč všetkými OVM následne konsolidovať prostredníctvom analytických reportov na úrovni všetkých pripojených OVM.

Tak ako je uvedené v predchádzajúcom odseku, architektonicky platforma Snow, na ktorej je IS ITAM postavený umožňuje implementáciu aj tzv. rezortných ITAM systémov, ktoré budú fyzicky aj logicky oddelené od ostatných ITAM systémov, pričom tieto môžu byť implementované do prostredia verejného vládneho cloudu alebo aj do prostredia samotného OVM (na úrovni rezortu). Rezortný IS ITAM bude mať vytvorené všetky tri časti - zbernú (tzv. Inventory Manager), aplikačnú aj databázovú, ktoré budú úplne oddelené od ostatných OVM, pričom bude zabezpečená aj oddelená správa daného systému.

V kontexte doplnenia nových modulov, projekt ITAM 2.0 zabezpečí nasledovné:

- Rozšírenie využitia platformy Bizzdesign Horizon, pričom z architektonického hľadiska nedochádza k žiadnym zmenám.
- Snow Risk Monitor bude doplnený ako SaaS služba k existujúcemu IS ITAM.
- FinOps nástroj bude doplnený ako SaaS služba k existujúcemu IS ITAM.

3.11 Stanovenie alternatív v technologickej vrstve architektúry

Tak ako je uvedené vyššie, projekt ITAM 2.0 je len rozšírením a doplnením už existujúceho riešenia, preto nie je potrebné posudzovať rôzne alternatívy v technologickej vrstve architektúry. Súčasný IS ITAM je prevádzkovaný vo verejnej časti vládneho cloudu. Bližšie informácie k tejto časti sú uvedené v Detailnom návrhu riešenia IS ITAM – kapitola 11 Fyzická vrstva. Na technologickej vrstve nedochádza k žiadnym zmenám.

Zároveň je potrebné uviesť, že v prípade implementácie tzv. rezortných ITAM systémov bude mať dané OVM na výber, či bude preferovať jeho implementáciu v prostredí vlastného dátového centra, vo vlastnom tenante verejného cloudu (verejnej časti vládneho cloudu) alebo využije tenant MIRRI vo verejnej časti vládneho cloudu, tak ako je implementovaný aj centrálny IS ITAM. V prípade využitia kapacít vlastného dátového centra, alebo vlastného tenantu verejnej časti vládneho cloudu, bude OVM znášať náklady na zabezpečenie potrebného výpočtového výkonu. V prípade využitia tenantu MIRRI, budú náklady súvisiace s využívaním potrebných cloudových zdrojov znášané MIRRI.

4. POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

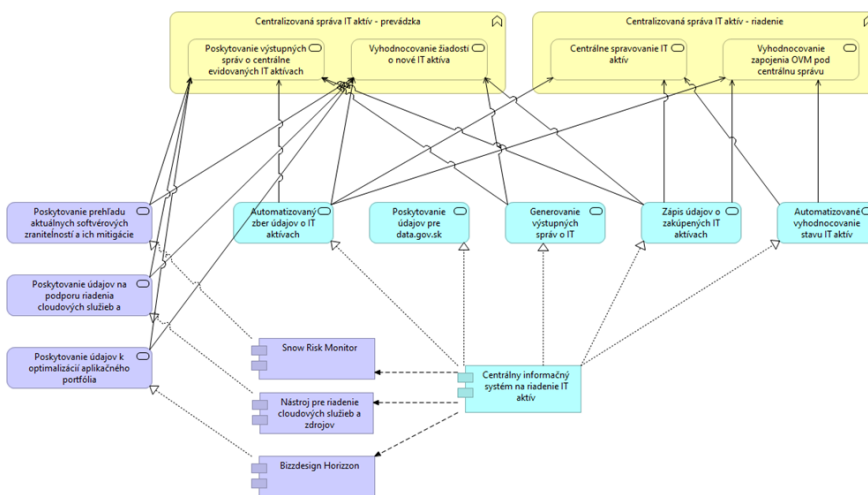
Výstupy projektu možno rozdeliť do nasledujúcich skupín:

1. Výstupy v zmysle vyhlášky 401/2023 o riadení projektov. Tieto výstupy už boli spracované v rámci realizácie projektu ITAM 1.0 – viď Projektový iniciálny dokument Implementácie informačného systému riadenia IT aktív a poskytovania aplikačnej podpory[1]. Tieto budú v rámci ITAM 2.0 aktualizované a doplnené o špecifiká tohto projektu.
2. IS ITAM vrátane rezortných IS ITAM nasadených do prostredia jednotlivých OVM
3. Snow Risk Monitor nasadený ako SaaS
4. Platforma FinOps nasadená ako SaaS
5. Expertné výstupy:
 - a. Úvodné zhodnotenie vspielosti riadenia ITAM pre jednotlivé OVM
 - b. Záverečné zhodnotenie vspielosti riadenia ITAM pre jednotlivé OVM
 - c. Stratégia rozvoja ITAM (aktualizácia)
 - d. Prevádzkový model (aktualizácia)
 - e. Správy o licenčnej pozícii jednotlivých výrobcov SW za OVM jednotlivo - polročne
 - f. Správy o zraniteľnostiach SW - polročne
 - g. Správy o riadení (finančných nákladoch) cloudových zdrojov – kvartálne
 - h. Manažérske dashboards – za OVM a konsolidované za všetky OVM (redukcia nákladov, eliminácia budúcich nákladov, znižovanie licenčných nesúladov a pod.) - mesačne
 - i. Školenia – licencie / IS ITAM
 - j. Metodika, prevádzkový model a nástroj riadenia cloudových zdrojov v zmysle FinOps
 - k. Správy z konsolidácie aplikačného portfólia atď. pre každé OVM

5. NÁHĽAD ARCHITEKTÚRY

Na nasledujúcej schéme je zobrazená architektúra súčasného prostredia IS ITAM v kombinácii s budúcimi novými aplikáciami – Snow Risk Monitor, Bizdesign Horizon a nástroj pre riadenie cloudových zdrojov – platforma FinOps:

Schéma 3 – Architektúra ITAM 2.0



Jednotlivé súčasné komponenty IS ITAM sú bližšie popísané v Detailnom návrh riešenia IS ITAM. Okrem toho v rámci realizácie projektu ITAM 2.0, budú do existujúceho riešenia doplnené nasledujúce komponenty:

- Snow Risk Monitor, štandardný softvér, ktorý pomáha mitigovať bezpečnostné riziká tým, že porovnáva všetky softvéri inštalované v prostredí OVM s databázou známych softvérových zraniteľností NIST (National Institute of Standards and Technology). Snow Risk Monitor poskytuje ďalej nasledujúce funkcionality:
 - Identifikuje zraniteľnosti naprieč celým aplikačným portfóliom.
 - Kategorizuje a prioritizuje riziká spojené s týmito zraniteľnosťami.
 - Identifikuje možné úniky údajov.
 - Poskytuje detailný návod ako identifikované zraniteľnosti odstrániť.
 - Priorizuje nápravné činnosti na základe stupňa závažnosti.
 - Monitoruje a chráni osobné údaje prostredníctvom:
 - Identifikácie aplikácií, ktoré spracúvajú osobné údaje.
 - Identifikácie typov osobných údajov, ktoré tieto aplikácie spracovávajú.
 - Poskytuje informácie o celkovom rizikovom skóre organizácie.
- BizDesign Horizon – zavedená platforma, ktorá podporuje tému riadenia aplikačného portfólia.
- FinOps certifikovaný nástroj, štandardný softvér, pre riadenie cloudových zdrojov pokrývajúci min. nasledujúce oblasti:
 - Riadenie rozpočtu a prognózovanie
 - „Chargeback“ a integrácia s IT financiami
 - Cloud politiky a governance
 - Alokácia nákladov
 - Analýza dáta a „showback“
 - Riadenie prístupu
 - Zakladanie rozhodovacích štruktúr a štruktúr zodpovednosti v zmysle FinOps
 - Analýza cloudových sadzieb
 - Podpora multi-cloud
 - Využitie zdrojov a „right-sizing“
 - Optimalizácia sadzieb – „right-costing“

Špecifikácia minimálnych funkčných požiadaviek Snow Risk Monitor a FinOps nástroja je uvedená v prílohe 1. Keďže sa jedná o štandardné (krabicové) nástroje, nepredpokladá sa žiadny vývoj ale skôr len nastavenie a konfigurácia týchto nástrojov do podmienok verejnej a štátnej správy SR, resp. aby sa naplnili požiadavky a ciele definované na projekte ITAM 2.0.

5.1 Prehľad e-Government komponentov

5.1.1 Prehľad koncových služieb – budúci stav:

Tabuľka 8 – Prehľad koncových služieb

Kód KS (z Metals)	Názov KS	Používateľ KS (G2C/G2B/G2G/G2A)	Životná situácia (+ kód z Metals)	Úroveň elektronizácie KS
n/a	n/a	n/a	n/a	Vyberte jednu z možností
n/a	n/a	n/a	n/a	Vyberte jednu z možností

5.1.2 Prehľad budovaných/rozvíjaných ISVS v projekte – budúci stav:

Tabuľka 9 – Prehľad budovaných / rozvíjaných ISVS

Kód ISVS (z Metals)	Názov ISVS	Modul ISVS (zaškrtnite ak ISVS je modulom)	Stav IS VS	Typ IS VS	Kód nadradeného ISVS (v prípade zaškrtnutého checkboxu pre modul ISVS)
isvs_9597	Centrálny informačný systém na riadenie IT aktív		Prevádzkovaný a plánujem rozvíjať	Ekonomický a administratívny chod inštitúcie	
tbd	BizzDesign Horizon		Prevádzkovaný a plánujem rozvíjať	Agendový	
tbd	Snow Risk Monitor		Plánujem budovať	Ekonomický a administratívny chod inštitúcie	
tbd	Nástroj pre riadenie cloudových zdrojov (FinOps)		Plánujem budovať	Ekonomický a administratívny chod inštitúcie	

5.1.3 Prehľad budovaných aplikačných služieb – budúci stav:

Tabuľka 10 – Prehľad budovaných aplikačných služieb

Kód AS (z MetalS)	Názov AS	ISVS/modul ISVS (kód z MetalS)	Aplikačná služba realizuje KS (kód KS z MetalS)
65976	Poskytovanie prehľadu aktuálnych softvérových zraniteľností a ich mitigácie	9597	ks_336642 ks_336640
65977	Poskytovanie údajov na podporu riadenia cloudových služieb a zdrojov	9597	ks_336642 ks_336640
65978	Poskytovanie údajov k optimalizácií aplikačného portfólia	9597	ks_336642 ks_336640

5.1.4 Prehľad integrácií ISVS na spoločné ISVS^[2] a ISVS iných OVM alebo IS tretích strán

Predmetný projekt svojim rozsahom a zameraním nepredpokladá vytvorenie / budovanie aplikačných služieb poskytovaných na externú integráciu, integráciu na nadrezortné centrálné bloky, integráciu na Spoločné moduly ÚPVS, integráciu na Modul procesnej integrácie a integrácie údajov (IS CSRÚ), či integráciu na centrálny API GW Modul úradnej komunikácie.

Tabuľka 11 – Prehľad integrácií ISVS

Kód ISVS (z MetalS)	Názov ISVS	Kód integrovaného ISVS (z MetalS)	Názov integrovaného ISVS
n/a	n/a	n/a	n/a
n/a	n/a	n/a	n/a

5.1.5 Aplikačné služby na integráciu

Predmetný projekt svojim rozsahom a zameraním nepredpokladá vytvorenie / budovanie aplikačných služieb poskytovaných na externú integráciu, integráciu na nadrezortné centrálné bloky, integráciu na Spoločné moduly ÚPVS, integráciu na Modul procesnej integrácie a integrácie údajov (IS CSRÚ), či integráciu na centrálny API GW Modul úradnej komunikácie.

Tabuľka 12 – Prehľad aplikačných služieb na integráciu

AS (Kód MetalS)	Názov AS	Realizuje ISVS (kód MetalS)	Poskytujúca alebo Konzumujúca	Integrácia cez CAMP	Integrácia s IS tretích strán	SaaS	Integrácia na AS poskytovateľa (kód MetalS)
n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

5.1.6 Poskytovanie údajov z ISVS do IS CSRÚ

Predmetný projekt svojim rozsahom a zameraním nepredpokladá využitie ani vytvorenie referenčných údajov.

Tabuľka 13 – Prehľad poskytovania údajov z ISVS do IS CSRÚ

ID OE	Názov (poskytovaného) objektu evidencie	Kód ISVS poskytovajúceho OE	Názov ISVS poskytovajúceho OE
n/a	n/a	n/a	n/a
n/a	n/a	n/a	n/a

n/a	n/a	n/a	n/a
-----	-----	-----	-----

5.1.7 Konzumovanie údajov z IS CSRÚ

Predmetný projekt svojím rozsahom a zameraním nepredpokladá využitie ani vytvorenie referenčných údajov.

Tabuľka 14 – Prehľad konzumovania údajov z IS CSRÚ

ID OE	Názov (konzumovaného) objektu evidencie	Kód a názov ISVS konzumujúceho OE z IS CSRÚ	Kód zdrojového ISVS v MetaIS
n/a	n/a	n/a	n/a
n/a	n/a	n/a	n/a
n/a	n/a	n/a	n/a

5.1.8 Prehľad plánovaného využívania infraštruktúrnych služieb (cloudových služieb) – budúci stav:

Tabuľka 15 – Prehľad plánované využívania infraštruktúrnych cloudových služieb

Kód infraštruktúrnej služby (z MetaIS)	Názov infraštruktúrnej služby	Kód využívajúceho ISVS (z MetaIS)	Názov využívajúceho ISVS
infra_sluzba_598	Microsoft Azure Backup	isvs_9597	Centrálny informačný systém na riadenie IT aktív
infra_sluzba_625	Virtual Network	isvs_9597	Centrálny informačný systém na riadenie IT aktív
infra_sluzba_637	Virtual Machines	isvs_9597	Centrálny informačný systém na riadenie IT aktív
infra_sluzba_627	API management	isvs_9597	Centrálny informačný systém na riadenie IT aktív
infra_sluzba_609	Azure Storage	isvs_9597	Centrálny informačný systém na riadenie IT aktív
infra_sluzba_613	Azure DNS	isvs_9597	Centrálny informačný systém na riadenie IT aktív
infra_sluzba_590	SQL Server on Virtual Machines	isvs_9597	Centrálny informačný systém na riadenie IT aktív

6. LEGISLATÍVA

Projekt ITAM 2.0 nevyžaduje žiadne legislatívne zmeny.

7. ROZPOČET A PRÍNOSY

7.1 Sumarizácia nákladov a prínosov

Náklady	Spolu	Centrálny informačný systém na riadenie IT aktív	Snow Risk Monitor	BizzDesign / APM	FinOps platforma

Náklady s DPH	30 731 388 €	23 832 899 €	1 879 226 €	4 401 361 €	617 902 €
IT - CAPEX	7 179 289 €	6 210 918 €	653 470 €	203 470 €	111 431 €
Aplikácie	3 014 370 €	2 516 999 €	203 470 €	203 470 €	90 431 €
SW	4 164 919 €	3 693 919 €	450 000 €	- €	21 000 €
HW	- €	- €	- €	- €	- €
IT - OPEX- prevádzka	23 538 994 €	17 613 878 €	1 225 037 €	4 194 073 €	506 007 €
Aplikácie	9 799 850 €	5 008 733 €	175 037 €	4 194 073 €	422 007 €
SW	11 279 145 €	10 145 145 €	1 050 000 €	- €	84 000 €
HW	2 460 000 €	2 460 000 €	- €	- €	- €
Riadenie projektu	13 104 €	8 102 €	719 €	3 819 €	463 €
Výstupné náklady	- €	- €	- €	- €	- €
Prínosy	51 985 604 €	51 985 604 €	- €	- €	- €
Finančné prínosy	- €	- €	- €	- €	- €
Administratívne poplatky	- €	- €	- €	- €	- €
Ostatné daňové a nedaňové príjmy	- €	- €	- €	- €	- €
Ekonomické prínosy	51 985 604 €	51 985 604 €	- €	- €	- €
Občania (€)	- €	- €	- €	- €	- €
Úradníci (€)	35 324 315 €	35 324 315 €	- €	- €	- €
Úradníci (FTE)	N/A	N/A	N/A	N/A	N/A
Kvalitatívne prínosy	16 661 289 €	16 661 289 €	- €	- €	- €

Vzhľadom na architektúru celého riešenia, boli skalkulované prínosy kumulované do Centrálného informačného systému na riadenie IT aktív aj za ostatné modulu/aplikácie navrhovaného riešenia.

8. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU a METÓDA JEHO RIADENIA

V nasledujúcej tabuľke je uvedený indikatívny harmonogram implementácia ITAM 2.0, ktorý zohľadňuje špecifiká týchto projektov a postupného nasadzovania riešenia do prostredí jednotlivých OVM:

Tabuľka 7 – Harmonogram projektu

ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu)	KONIEC (odhad termínu)	POZNÁMKA
1.	Prípravná fáza a Iniciačná fáza	01/2024	03/2025	
2.	Realizačná fáza	04/2025	03/2028	Postupné zapájanie jednotlivých OVM.
2a	Analýza a Dizajn	04/2025	03/2027	
2b	Nákup technických prostriedkov, programových prostriedkov a služieb	04/2025	03/2027	Postupne, podľa potreby.
2c	Implementácia a testovanie	04/2025	03/2027	Realizované per jednotlivé OVM.
2d	Nasadenie a PIP	04/2025	03/2027	Realizované per jednotlivé OVM.
3.	Dokončovacia fáza	04/2025	03/2027	Realizované per jednotlivé OVM.

4.	Podpora prevádzky (SLA)	06/2025	03/2028	Prevádzka začína pripojením prvého OVM a postupne sa rozširuje na ostatné OVM.
----	-------------------------	---------	---------	--

9. PROJEKTOVÝ TÍM

Projektový tím MIRRI bude konkrétnejšie definovaný až v ďalších fázach v rámci prípravných prác projektu ITAM 2.0. Avšak vzhľadom na skúsenosti z projektu ITAM 1.0 bude projektový tím za stranu MIRRI SR pozostávať z rovnakých rolí ako sú uvedené v Projektovom iniciálnom dokumente k projektu implementácie informačného systému riadenia IT aktív a poskytovania aplikačnej podpory, kapitola 6.2 Riadenie projektu a kapitola 6.3 Pracovný tím.

Riadiaci výbor projektu tvorí predseda riadiaceho výboru projektu a vlastníci procesov alebo nimi poverení zástupcovia.

Riadiaci výbor sa riadi "Štatútom riadiaceho výboru", ktorý je popísaný v dokumente Štatút RV projektu ako najvyšší riadiaci orgán na účely realizácie projektu na základe schválenej projektovej dokumentácie.

Štatút Riadiaceho výboru upravuje najmä jeho pôsobnosť, úlohy, zloženie, zasadnutie a hlasovanie. Členom riadiaceho výboru projektu môže byť aj zástupca dodávateľa. Väčšina členov riadiaceho výboru projektu s hlasovacím právom sú osoby navrhnuté objednávatelom a zastupujú záujmy objednávatelä. Riadiaci výbor projektu dozerá na hospodárnosť, efektívnosť a účelové využívanie finančných prostriedkov a môže prispôsobiť štandardy projektového riadenia na realizovaný projekt.

- Projektový manažér Objednávatelä – dohliada a riadi projekt v zmysle Zmluvy, dohliada na plnenia Dodávateľa, predkladá návrh akceptácie plnení Dodávateľa.
- Projektový manažér Dodávateľa – riadi dodávanie častí diela v zmysle Zmluvy na strane Dodávateľa, predkladá plnenia za Dodávateľa.
- Analytický tím Dodávateľa – analyzuje a navrhuje riešenia pre implementáciu požiadaviek.
- Vývojový tím Dodávateľa – implementuje požiadavky v zmysle schválených návrhov.
- Testovací tím Dodávateľa – overuje funkčnosť implementovaných požiadaviek.
- Tím UAT Objednávatelä – overuje funkčnosť a správnosť implementovaných požiadaviek.

Projektové role:

- Projektový manažér
- Kľúčový používateľ
- Analytik IT
- Architekt IT
- ID Tester
- Dátový špecialista
- Manažér kybernetickej a informačnej bezpečnosti

Ďalšie projektové role:

- Finančný manažér
- Manažér kvality
- Asistent PM

9.1 PRACOVNÉ NÁPLNE

Pracovné náplne jednotlivých členov projektového tímu MIRRI SR budú definované až v ďalších fázach v rámci prípravných prác projektu ITAM 2.0.

Projektová rola:	PROJEKTOVÝ MANAŽÉR
Stručný popis:	· zodpovedá za riadenie projektu počas celého životného cyklu projektu. Riadi projektové (ľudské a finančné) zdroje, zabezpečuje tvorbu obsahu, neustále odôvodňovanie projektu (aktualizuje BC/CBA) a predkladá vstupy na rokovanie Riadiaceho výboru. Zodpovedá za riadenie všetkých (ľudských a finančných) zdrojov, členov projektovému tímu objednávatelä a za efektívnu komunikáciu s dodávateľom alebo stanovených zástupcom dodávateľa.

	<ul style="list-style-type: none"> · zodpovedá za riadenie prideleného projektu - stanovenie cieľov, spracovanie harmonogramu prác, koordináciu členov projektového tímu, sledovanie dodržiavania harmonogramu prác a rozpočtu, hodnotenie a prezentáciu výsledkov a za riadenie s tým súvisiacich rizík. Projektový manažér vedie špecifikáciu a implementáciu projektov v súlade s firemnými štandardami, zásadami a princípmi projektového riadenia. · zodpovedá za plnenie projektových/programových cieľov v rámci stanovených kvalitatívnych, časových a rozpočtových plánov a za riadenie s tým súvisiacich rizík. V prípade externých kontraktov sa vedúci projektu/ projektový manažér obvykle podieľa na ich plánovaní a vyjednávaní a je hlavnou kontaktnou osobou pre zákazníka.
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	<p>Zodpovedný za:</p> <ul style="list-style-type: none"> · Riadenie projektu podľa pravidiel stanovených vo Vyhláške 85/2020 Z.z. · Riadenie prípravy, inicializácie a realizácie projektu · Identifikovanie kritických miest projektu a navrhovanie ciest k ich eliminácii · Plánovanie, organizovanie, motivovanie projektového tímu a monitorovanie projektu · Zabezpečenie efektívneho riadenia všetkých projektových zdrojov s cieľom vytvorenia a dodania obsahu a zabezpečenie naplnenie cieľov projektu · Určenie pravidiel, spôsobov, metód a nástrojov riadenia projektu a získanie podpory Riadiaceho výboru (RV) pre riadenie, plánovanie a kontrolu projektu a využívanie projektových zdrojov · Zabezpečenie vypracovania manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 · Zabezpečenie realizácie projektu podľa štandardov definovaných vo Vyhláške 78/2020 Z.z. · Zabezpečenie priebežnej aktualizácie a verzionovania manažérskej a špecializovanej dokumentácie v minimálnom rozsahu Vyhlášky 85/2020 Z.z., Prílohy č.1 · Vypracovanie, pravidelné predkladanie a zabezpečovanie prezentácie stavov projektu, reportov, návrhov riešení problémov a odsúhlasovania manažérskej a špecializovanej dokumentácie v rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 na rokovaní RV · Riadenie a operatívne riešenie a odstraňovanie strategických / projektových rizík a závislostí · Predkladanie návrhov na zlepšenia na rokovaní Riadiaceho výboru (RV) · Zabezpečenie vytvorenia a pravidelnej aktualizácie BC/CBA a priebežné zdôvodňovanie projektu a predkladanie na rokovaní RV · Celkovú alokáciu a efektívne využívanie ľudských a finančných zdrojov v projekte · Celkový postup prác v projekte a realizuje nápravné kroky v prípade potreby · Vypracovanie požiadaviek na zmenu (CR), návrh ich prioritizácie a predkladanie zmenových požiadaviek na rokovaní RV · Riadenie zmeny (CR) a prípadné požadované riadenie konfigurácií a ich zmien · Riadenie implementačných a prevádzkových aktivít v rámci projektov. · Aktívne komunikuje s dodávateľom, zástupcom dodávateľa a projektovým manažérom dodávateľa s cieľom zabezpečiť úspešné dodanie a nasadenie požadovaných projektových výstupov, · Formálnu administráciu projektu, riadenie centrálného projektového úložiska, správu a archiváciu projektovej dokumentácie · Kontrolu dodržiavania a plnenia míľnikov v zmysle zmluvy s dodávateľom, · Dodržiavanie metodík projektového riadenia, · Predkladanie požiadaviek dodávateľa na rokovaní Riadiaceho výboru (RV), · Vecnú a procesnú administráciu zúčtovania dodávateľských faktúr
	<ul style="list-style-type: none"> · Certifikácia - Prince 2

Odporúčané kvalifikačné predpoklady	<ul style="list-style-type: none"> · Certifikácia - PMI PMP · Certifikácia - IPMA <p>Certifikát vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou.</p>
Poznámka	<p>V prípade, ak v projekte tíme NIE SÚ vytvorené projektové role Manažér zmien (Change manager) a Implementačný manažér (Release manager), tak rozsah a povinnosti týchto rolí vykonáva rola Projektový manažér</p> <p>Poznámka: Prekopírujte do popisu role pre Projektového manažéra, popisy rolí Change managera a Release managera.</p>

Projektová rola:	KĽUČOVÝ POUŽÍVATEĽ (end user)
Stručný popis:	<ul style="list-style-type: none"> · zodpovedný za reprezentáciu záujmov budúcich používateľov projektových produktov alebo projektových výstupov a za overenie kvality produktu. · zodpovedný za návrh a špecifikáciu funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu, požiadaviek koncových používateľov na prínos systému a požiadaviek na bezpečnosť. · Kľúčový používateľ (end user) navrhuje a definuje akceptačné kritériá, je zodpovedný za akceptačné testovanie a návrh na akceptáciu projektových produktov alebo projektových výstupov a návrh na spustenie do produkčnej prevádzky. Predkladá požiadavky na zmenu funkcionalít produktov a je súčasťou projektových tímov
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	<p>Zodpovedný za:</p> <ul style="list-style-type: none"> · Návrh a špecifikáciu funkčných a technických požiadaviek · Jednoznačnú špecifikáciu požiadaviek na jednotlivé projektové výstupy (špecializované produkty a výstupy) z pohľadu vecno-procesného a legislatívny · Vytvorenie špecifikácie, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu, · Špecifikáciu požiadaviek koncových používateľov na prínos systému · Špecifikáciu požiadaviek na bezpečnosť, · Návrh a definovanie akceptačných kritérií, · Vykonanie používateľského testovania funkčného používateľského rozhrania (UX testovania) · Finálne odsúhlasenie používateľského rozhrania · Vykonanie akceptačného testovania (UAT) · Finálne odsúhlasenie a akceptáciu manažérskych a špecializovaných produktov alebo projektových výstupov · Finálny návrh na spustenie do produkčnej prevádzky, · Predkladanie požiadaviek na zmenu funkcionalít produktov · Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 · Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

Odporúčané kvalifikačné predpoklady	<ul style="list-style-type: none"> doplňte podľa potreby alebo vymažte
Poznámka	<p>V prípade, ak v projekte tíme NIE SÚ vytvorené projektové role UX DIZAJNÉRA, tak rozsah a povinnosti tejto role vykonáva rola KLÚČOVÝ POUŽÍVATEĽ.</p> <p>Prekopírujte do popisu role pre KLÚČOVÉHO POUŽÍVATEĽA, popis role UX DIZAJNÉRA.</p>

Projektová rola:	IT ARCHITEKT
Stručný popis:	<ul style="list-style-type: none"> zodpovedá za návrh architektúry riešenia IS a implementáciu technológií predovšetkým z pohľadu udržateľnosti, kvality a nákladov, za riešenie architektonických cieľov projektu dizajnu IS a súlad s architektonickými princípmi. vykonáva, prípadne riadi vysoko odborné tvorivé činnosti v oblasti návrhu IT. Študuje a stanovuje smery technického rozvoja informačných technológií, navrhuje riešenia na optimalizáciu a zvýšenie efektívnosti prostriedkov výpočtovej techniky. Navrhuje základnú architektúru informačných systémov, ich komponentov a vzájomných väzieb. Zabezpečuje projektovanie dizajnu, architektúry IT štruktúry, špecifikácie jej prvkov a parametrov, vhodnej softvérovej a hardvérovej infraštruktúry podľa základnej špecifikácie riešenia. zodpovedá za spracovanie a správu projektovej dokumentácie a za kontrolu súladu implementácie s dokumentáciou. Môže tiež poskytovať konzultácie, poradenstvo a vzdelávanie v oblasti svojej špecializácie. IT architekt, projektant analyzuje, vytvára a konzultuje so zákazníkom riešenia na úrovni komplexných IT systémov a IT architektúr, najmä na úrovni aplikačného vybavenia, infraštruktúrnych systémov, sietí a pod. Zaručuje, že návrh architektúry a/alebo riešenia zodpovedá zmluvne dohodnutým požiadavkám zákazníka v zmysle rozsahu, kvality a ceny celej služby/riešenia.
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	<p>Zodpovedný za:</p> <ul style="list-style-type: none"> Navrhovanie architektúry IT riešení s cieľom dosiahnuť najlepšiu efektívnosť. Transformovanie cieľov, príslubov a zámerov projektu do tvorby reálnych návrhov a riešení. Navrhovanie takých riešení, aby poskytovali čo najvyššiu funkčnosť a flexibilitu. Posudzovanie vhodnosti navrhnutých riešení s ohľadom na požiadavky projektu. Zodpovednosť za technické navrhnutie a realizáciu projektu. Zodpovednosť za vytvorenie technickej IT dokumentácie a jej následná kontrola. Zodpovednosť za definovanie integračných vzorov, menných konvencií, spôsobov návrhu a spôsobu programovania. Definovanie architektúry systému, technických požiadaviek a funkčného modelu (Proof Of Concept.) Vytvorenie požiadaviek na HW/SW infraštruktúru IS Udržiavanie a rozvoj konzistentnej architektúry s dôrazom na architektúru aplikačnú, dátovú a infraštruktúru Analýzu a odhad náročnosti technických požiadaviek na vytvorenie IS alebo vykonanie zmien v IS Navrhovanie riešení zohľadňujúce architektonické štandardy, časové a zdrojové obmedzenia, Navrhovanie dátových transformácií medzi dátovými skladmi a aplikáciami Vyhodnocovanie implementačných alternatív z pohľadu celkovej IT architektúry Ladenie dátových štruktúr za účelom dosiahnutia optimálneho výkonu

	<ul style="list-style-type: none"> · Prípravu akceptačných kritérií · Analýza nových nástrojov, produktov a technológií · Správa, rozvoj a dohľad nad dodržiavaním integračných štandardov · Priebežné posudzovanie vecných výstupov dodávateľa v rámci analýzy, návrhu riešenia vrátane Detailného návrhu riešenia (DNR) z pohľadu analýzy a návrhu riešenia architektúry IS · Vykonať posudzovanie a úpravu testovacej stratégie, testovacích scenárov, plánov testov, samotné testovanie a účasť na viacerých druhoch testovania · Vykonalie záťažových, výkonnostných a integračných testov a navrhnutie následných nápravných · Nasadenie a otestovanie migrácie, overenie kvality dát a navrhnutie nápravných opatrení · Participáciu na výkone bezpečnostných testov, · Participáciu na výkone UAT testov, · Posúdenie prevádzkovo-infraštruktúrnej dokumentácie pred akceptáciou a prevzatím od dodávateľa · Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 · Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu
Odporúčané kvalifikačné predpoklady	<ul style="list-style-type: none"> · Certifikácia - Togaf · Certifikácia - ArchiMate <p>Certifikát vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou.</p>
Poznámka	<p>V prípade, ak v projekte tíme NIE JE vytvorená projektová rola INTEGRAČNÝ MANAŽÉR, tak rozsah a povinnosti tejto role vykonáva rola IT ARCHITEKT</p> <p>Poznámka: Prekopírujte do popisu role pre IT ARCHITEKTA, popis role INTEGRAČNÉHO MANAŽÉRA.</p>
Projektová rola:	IT ANALYTIK
Stručný popis:	<ul style="list-style-type: none"> · zodpovedá za zber a analyzovanie funkčných požiadaviek, analyzovanie a spracovanie dokumentácie z pohľadu procesov, metodiky, technických možností a inej dokumentácie. Podieľa sa na návrhu riešenia vrátane návrhu zmien procesov v oblasti biznis analýzy a analýzy softvérových riešení. Zodpovedá za výkon analýzy IS, koordináciu a dohľad nad činnosťou SW analytikov. · analyzuje požiadavky na informačný systém/softvérový systém, formálnym spôsobom zaznamenáva činnosti/procesy, vytvára analytický model systému, okrem analýzy realizuje aj návrh systému, ten vyjadruje návrhovým modelom. · Analytik informačných technológií pripravuje špecifikáciu cieľového systému od procesnej až po technickú rovinu. Mapuje a analyzuje existujúce podnikateľské a procesné prostredie, analyzuje biznis požiadavky na informačný systém, špecifikuje požiadavky na informačnú podporu procesov, navrhuje koncept riešenia a pripravuje podklady pre architektov a vývojárov riešenia, participuje na realizácii zmien, dohliada na realizáciu požiadaviek v cieľovom riešení, spolupracuje pri ich preberaní (akceptácie) používateľom. · Pri návrhu IT systémov využíva odbornú špecializáciu IT architektov a projektantov. Študuje a analyzuje dokumentáciu, požiadavky klientov, legislatívne a technické podmienky a možnosti zvyšovania efektívnosti a výkonnosti riadiacich a informačných procesov. Navrhuje a prerokúva koncepcie riešenia informačných systémov a analyzuje ich efekty a dopady. Zabezpečuje spracovanie analyticko-projektovú špecifikáciu s návrhom dátových a objektových štruktúr a ich väzieb, užívateľského rozhrania a ostatných podkladov pre projektovanie nových riešení.

	<ul style="list-style-type: none"> Spolupracuje na projektovaní a implementácii návrhov. Môže tiež poskytovať poradenstvo v oblasti svojej špecializácie. Zodpovedá za návrhovú (design) časť IT - pôsobí ako medzičlánok medzi používateľmi informačných systémov (biznis pohľad) a ich realizátormi (technologický pohľad).
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	<p>Zodpovedný za:</p> <ul style="list-style-type: none"> Vykonanie analýzy procesných a ďalších požiadaviek a vytvorenie špecifikácie súčasného alebo budúceho užívateľa softwaru („zákazníka“) a následne navrhuje dizajn a programátorské riešenie. Participáciu na vývoji nových, ale i vylepšovaní existujúcich aplikácií v rámci celého vývojového cyklu – systémová analýza, dizajn, kódovanie, užívateľské testovanie, implementácia, podpora, dokumentácia. Úzko spolupracuje aj s IT architektom. Analýza potrieb zákazníka vrátane tvorby úplnej analytickej dokumentácie a vstupov do verejného obstarávania (VO). Mapovanie požiadaviek do návrhu funkčných riešení. Návrh a správa katalóg požiadaviek - registra požiadaviek riešenia Analýza funkčných a nefunkčných požiadaviek, Návrh fyzického a logického modelu, Návrh testovacích scenárov, V priebehu implementácie robí dohľad nad zhodou výstupov s pôvodným analytickým zadaním. Zodpovednosť za dodržiavanie správnej metodiky pri postupe analýzy Definovanie akceptačných kritérií v projekte Odsúhlasenie opisu produktov, ktoré predstavujú vstupy alebo výstupy (priebežné alebo konečné) úloh dodávateľov, alebo ktoré ich priamo ovplyvňujú a zabezpečovať akceptáciu produktov po ich dokončení Priraduje priority a poskytuje stanoviská používateľov na rozhodnutia Riadiaceho výboru projektu – k realizácii zmenových požiadaviek Poskytuje merania aktuálneho stavu pre potreby porovnania s výsledkami projektu vzhľadom na realizáciu prínosov Rieši požiadavky používateľov a konflikty iných priorít Posúdenie prevádzkovo-infraštruktúrnej dokumentácie pred akceptáciou a prevzatím od dodávateľa Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu
Odporúčané kvalifikačné predpoklady	<ul style="list-style-type: none"> Certifikácia - OMG-Certified UML (Unified Modeling Language) alebo ekvivalent <p>Certifikát vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou.</p>
Poznámka	

Projektová rola:	MANAŽÉR KVALITY
Stručný popis:	<ul style="list-style-type: none"> zodpovedá za priebežné vyžadovanie, hodnotenie a kontrolu kvality (vecnej aj formálnej) počas celého projektu. Je zodpovedný za úvodné nastavenie pravidiel riadenia kvality a za následné dodržiavanie a kontrolu kvality jednotlivých projektových výstupov. Sleduje a hodnotí kvalitatívne ukazovatele projektových výstupov a o zisteniach informuje projektového manažéra objednávateľa formou pravidelných alebo nepravidelných správ/záznamov.

	<ul style="list-style-type: none"> · plánuje, koordinuje, riadi a kontroluje systém manažérstva kvality, monitoruje a meria procesy a identifikuje príležitosti na trvalé zlepšovanie systému manažérstva kvality v organizácii v súlade s platnými normami. Zabezpečuje tvorbu cieľov a koncepcie kvality, vrátane kontroly ich plnenia a vykonáva interné a externé audity kvality v súlade s plánom. · Počas celej doby realizácie projektu zabezpečuje zhodu kvality projektových výstupov s požiadavkami. Realizuje postupy riadenia kvality tak, aby výsledkom boli projektové výstupy spĺňajúce požiadavky objednávateľa. Kontroluje, či sa riadenie a proces zabezpečenia kvality vykonáva správnym spôsobom, v správnom čase a správnymi osobami.
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	<p>Zodpovedný za:</p> <ul style="list-style-type: none"> · Návrh a zavádzanie do praxe postupov, techník, nástrojov a pravidiel, ktoré maximalizujú efektivitu práce a kvalitatívne parametre vývoja softwaru/produktu/IS, resp. IT projektu · Definovanie politiky kvality (stratégie kvality), meranie kvality, analýzu a spracovanie plánov kvality, · Riadenie a monitorovanie dosahovania cieľov kvality, · Špecifikáciu požiadaviek na kvalitu vyvíjaných funkcionalít systému · Špecifikáciu požiadaviek pre ďalší rozvoj, · Definovanie akceptačných kritérií · Zabezpečenie súladu so štandardmi, normami, právnymi požiadavkami, požiadavkami užívateľov a prevádzkovateľov systémov, · Posúdenie BC/CBA – odôvodnení projektu · Kontrolu kvalitu plnenia vecných požiadaviek definovaných v Zmluve s dodávateľom alebo v požiadavkách na zmenu, · Akceptáciu splnenia vecných a kvalitatívnych požiadaviek v projekte svojím podpisom na akceptačnom protokole pri odovzdávaní jednotlivých fáz projektu/čiastkových projektov alebo pri odovzdávaní zmien vykonaných v rámci zmenových konaní, · Aktívnu účasť rokovaniach a participáciu na riešení vecných požiadaviek členov projektového tímu, · Monitoring a vyhodnocovanie kvality údajov a návrh nápravných opatrení za účelom zabezpečenia správnosti a konzistentnosti údajov · Definovanie postupov, navrhovanie a vyjadrovanie sa k plánom testov a testovacích scenárov · Analyzovanie výsledkov testovania. · Kontrolu plnenia projektových úloh a časového harmonogramu projektu · Kontrolu plnenia finančného plánu projektu · Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 · Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu
Odporúčané kvalifikačné predpoklady	<ul style="list-style-type: none"> · Certifikácia - Prince 2, PMI PMP, IPMA · Certifikácia - Togaf alebo ekvivalent · Certifikácia - ISO 9001 alebo ekvivalent <p>Certifikát vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou.</p>
Poznámka	<p>V prípade, ak v projekte tíme NIE JE vytvorená projektová rola VLASTNÍK PROCESOV (biznis vlastník) a VLASTNÍK ÚDAJOV, tak rozsah zodpovedností a povinností týchto rolí vykonáva rola MANAŽER KVALITY.</p> <p>Poznámka: Prekopírujte do popisu role pre MANAŽÉRA KVALITY, popis role VLASTNÍK PROCESOV (biznis vlastník) a VLASTNÍK ÚDAJOV.</p>

Projektová rola:	VLASTNÍK PROCESOV (biznis vlastník)
Stručný popis:	<ul style="list-style-type: none"> · zodpovedá za proces - jeho výstupy i celkový priebeh poskytnutia služby alebo produktu konečnému užívateľovi. Kľúčová rola na strane zákazníka (verejného obstarávateľa), ktorá schvaľuje biznis požiadavky a zodpovedá za výsledné riešenie, prínos požadovanú hodnotu a naplnenie merateľných ukazovateľov. Úlohou tejto roly je definovať na užívateľa orientované položky (user-stories), ktoré budú zaradované a prioritizované v produktovom zásobníku. Zodpovedá za priebežné posudzovanie vecných výstupov dodávateľa v rámci analýzy, návrhu riešenia vrátane DNR z pohľadu analýzy a návrhu riešenia aplikácii IS. · zodpovedný za schválenie funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu. Definuje očakávania na kvalitu projektu, kvalitu projektových produktov, prínosy pre koncových používateľov a požiadavky na bezpečnosť. Definuje merateľné výkonnostné ukazovatele projektov a prvkov. Vlastník procesov schvaľuje akceptačné kritériá, rozsah kvalitu dodávaných projektových výstupov pri dosiahnutí platobných míľnikov, odsúhlasuje spustenie výstupov projektu do produkčnej prevádzky a dostupnosť ľudských zdrojov alokovaných na realizáciu projektu.
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	Zodpovedný za: <ul style="list-style-type: none"> · Realizáciu dohľadu nad súladom projektových výstupov s požiadavkami koncových používateľov. · Spoluprácu pri riešení odpovedí na otvorené otázky a riziká projektu. · Posudzovanie, pripomienkovanie, testovanie a protokolárne odsúhlasovanie projektových výstupov v príslušnej oblasti (v biznis procese) po vecnej stránke (najmä procesnej a legislatívnej) · Riešenie problémov a požiadaviek v spolupráci s odbornými garantmi, · Spoluprácu pri špecifikácii a poskytuje súčinnosť pri riešení zmenových požiadaviek · Schválenie funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu z pohľadu používateľov koncového produktu · Definovanie očakávaní na kvalitu projektu, kritérií kvality projektových produktov, prínosov pre koncových používateľova požiadaviek na bezpečnosť, · Definovanie merateľných výkonnostných ukazovateľov projektov a prvkov, · Sledovanie a odsúhlasovanie nákladovosti, efektívnosti vynakladania finančných prostriedkov a priebežné monitorovanie a kontrolu odôvodnenia projektu (BC/CBA) · Schválenie akceptačných kritérií, · Riešenie problémov používateľov · Akceptáciu rozsahu a kvality dodávaných projektových výstupov pri dosiahnutí platobných míľnikov, · Vykonanie UX a UAT testovania · Odsúhlasenie spustenia výstupov projektu do produkčnej prevádzky, · Dostupnosť a efektívne využitie ľudských zdrojov alokovaných na realizáciu projektu, · Vykonávanie monitorovania a hodnotenia procesov v plánovaných intervaloch. · Poskytovanie vyjadrení k zmenovým požiadavkám, k ich opodstatnenosti a prioritizácii · Zisťovanie efektívneho spôsobu riadenia a optimalizácie zvereného procesu, vrátane analyzovanie všetkých vyskytujúcich sa nezhôd, · Okrem zvažovaní rizík prevádzkových alebo podporných procesov súčasne vlastník napomáha identifikovať príležitosti, · Zlepšovanie a optimalizáciu procesov v spolupráci s ďalšími prepojenými vlastníkmi procesov a manažérom kvality, · Odsúhlasenie akceptačných protokolov zmenových konaní

	<ul style="list-style-type: none"> · Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 · plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu
Odporúčané kvalifikačné predpoklady	· doplňte podľa potreby alebo vymažte
Poznámka	Rola VLASTNÍK PROCESOV je biznis vlastník , ide o kľúčovú rolu v rámci projektového tímu.

Projektová rola:	VLASTNÍK ÚDAJOV / VLASTNÍK DÁT
Stručný popis:	<ul style="list-style-type: none"> · zodpovedá za udržiavanie databázy, spravuje používateľské účty/prístupy, zálohuje a optimalizuje chod databázy, identifikuje problémové oblasti a navrhuje riešenia na ich odstránenie. Správca databáz vykonáva, prípadne riadi odborné činnosti v oblasti správy bázy dát a dátových súborov IKT. · zabezpečuje inštaláciu, testovanie, oživovanie a nastavenie parametrov a následnú správu databázy vrátane prostriedkov a aplikácií na jej využitie. Zabezpečuje migráciu dát, generovanie výstupov, vytváranie relácií a spájanie dát, zálohovanie dát a správu používateľských účtov/prístupov. · zabezpečuje monitoring prevádzky bázy dát, administratívne a dokumentačné práce súvisiace so správou databázy a riešenie neštandardných situácií. Poskytuje inštrukcie a poradenstvo používateľom databázových systémov · celý rozsah svojej agendy rieši v súlade s legislatívou o dátových štandardoch – Vyhláškou 78/2020 Zz o dátových štandardoch
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	<p>Zodpovedný za:</p> <ul style="list-style-type: none"> · Realizáciu dohľadu nad súladom projektových výstupov s požiadavkami na dátovú kvalitu. · Spoluprácu pri riešení odpovedí na otvorené otázky a riziká projektu. · Posudzovanie, pripomienkovanie, testovanie a protokolárne odsúhlasovanie projektových výstupov v príslušnej oblasti – dátových štandardov · Riešenie problémov a požiadaviek v spolupráci s odbornými garantmi, · Spoluprácu pri špecifikácii a poskytuje súčinnosť pri riešení zmenových požiadaviek · Schválenie funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu z pohľadu používateľov koncového produktu · Spolupráca pri definovaní merateľných výkonnostných ukazovateľov projektov a prvkov, · Konzultovanie akceptačných kritérií, · Spolupráca na realizácii UAT testovania z pohľadu dodržania dátových štandardov · Odsúhlasenie spustenia výstupov projektu do produkčnej prevádzky, · Dostupnosť a efektívne využitie ľudských zdrojov alokovaných na realizáciu projektu, · Poskytovanie vyjadrení k zmenovým požiadavkám, k ich opodstatnenosti a prioritizácii · Zisťovanie efektívneho spôsobu riadenia a optimalizácie zvereného procesu, vrátane analyzovanie všetkých vyskytujúcich sa nezhôd, · Odsúhlasenie akceptačných protokolov zmenových konaní

	<ul style="list-style-type: none"> · Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1 · plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu
Odporúčané kvalifikačné predpoklady	· doplňte podľa potreby alebo vymažte
Poznámka	<p>V prípade, ak v projekte tíme NIE SÚ vytvorené projektové role VLASTNÍK DÁT, tak rozsah a povinnosti tejto role vykonáva rola VLASTNÍK PROCESOV (biznis vlastník).</p> <p>Prekopírujte do popisu role pre VLASTNÍKA PROCESOV (biznis vlastník), popis role VLASTNÍKA DÁT.</p>

Projektová rola:	MANAŽER KYBERNETICKEJ BEZPEČNOSTI (KIB) a IT BEZPEČNOSTI (ITB)
Stručný popis:	<ul style="list-style-type: none"> · zodpovedá za dodržanie princípov a štandardov na kybernetickú a IT bezpečnosť, za kontrolu a audit správnosti riešenia v oblasti bezpečnosti. · koordinuje a riadi činnosť v oblasti bezpečnosti prevádzky IT, spolupracuje na projektoch, na rozvoji nástrojov a postupov k optimalizácii bezpečnostných systémov a opatrení. Stanovuje základné požiadavky, podmienky a štandardy pre oblasť bezpečnosti programov, systémov, databázy či sieti. Spracováva a kontroluje príslušné interné predpisy a dohliada nad plnením týchto štandardov a predpisov. Kontroluje a riadi činnosť nad bezpečnostnými testami, bezpečnostnými incidentmi v prevádzke IT. Poskytuje inštrukcie a poradenstvo používateľom počítačov a informačných systémov pre oblasť bezpečnosti <p>PODMIENKY SPRÁVNEHO a EFEKTÍVNEHO VÝKONU ČINNOSTI role Manažér KIB a ITB:</p> <p>1) neobmedzený aktívny prístup ku všetkým projektovým dokumentom, nástrojom a výstupom projektu, v ktorých sa opisuje predmet projektu z hľadiska jeho architektúry, funkcií, procesov, manažmentu informačnej bezpečnosti a spôsobov spracúvania dát, ako aj dát samotných.</p> <p>2) rola manažér Kybernetickej a IT bezpečnosti si vyžaduje mať sprístupnené všetky informácie o bezpečnostných opatreniach zavádzaných projektom v zmysle:</p> <p>a) § 20 zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov</p> <p>b) ustanovení zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov</p>
Detailný popis rozsahu zodpovednosti, povinností a kompetencií	<p>Zodpovedný za:</p> <ul style="list-style-type: none"> · špecifikovanie štandardov, princípov a stratégií v oblasti ITB a KIB, · ak je projekt primárne zameraný na problematiku ITB a KIB – je priamo zodpovedný za špecifikáciu a analýzu funkčných požiadaviek na ITB a KIB, · špecifikovanie požiadaviek na ITB a KIB, kontroluje ich implementáciu v realizovanom projekte, · špecifikovanie požiadaviek na bezpečnosť vývojového, testovacieho a produkčného prostredia, · špecifikovanie funkčných a nefunkčných požiadaviek pre oblasť ITB a KIB, · špecifikovanie požiadaviek na bezpečnosť v rámci bezpečnostnej vrstvy, · špecifikovanie požiadaviek na školenia pre oblasť ITB a KIB, · špecifikovanie požiadaviek na bezpečnostnú architektúru riešenia a technickú infraštruktúru pre oblasť ITB a KIB, · špecifikovanie požiadaviek na dostupnosť, zálohovanie, archiváciu a obnovu IS vzťahujúce sa na ITB a KIB, · realizáciu posúdenie požiadaviek agendy ITB a KIB na integrácie a procesov konverzie a migrácie, identifikácia nesúladu a návrh riešenia

- špecifikovanie požiadaviek na ITB a KIB, bezpečnostný projekt a riadenie prístupu,
- špecifikovanie požiadaviek na testovanie z hľadiska ITB a KIB, realizáciu kontroly zapracovania a retestu,
- špecifikovanie požiadaviek na obsah dokumentácie v zmysle legislatívnych požiadaviek pre oblasť ITB a KIB, ako aj v zmysle "best practies",
- špecifikovanie požiadaviek na dodanie potrebnej dokumentácie súvisiacej s ITB a KIB kontroluje ich implementáciu v realizovanom projekte,
- špecifikovanie požiadaviek a konzultácie pri návrhu riešenia za agendu ITB a KIB v rámci procesu „Mapovanie a analýza technických požiadaviek - detailný návrh riešenia (DNR)“,
- špecifikáciu požiadaviek na bezpečnosť IT a KIB v rámci procesu "akceptácie, odovzdania a správy zdroj. kódov"
- špecifikáciu akceptačných kritérií za oblasť ITB a KIB,
- špecifikáciu pravidiel pre publicitu a informovanosť s ohľadom na ITB a KIB,
- poskytovanie konzultácií pri tvorbe šablón a vzorov dokumentácie pre oblasť ITB a KIB,
- získavanie informácií nutných pre plnenie úloh v oblasti ITB a KIB,
- špecifikáciu podmienok na testovanie, reviduje výsledky a výstupy z testovania za oblasť ITB a KIB,
- konzultácie a vykonávanie kontrolnej činnosť zameranej na obsah a komplexnosť dok. z hľadiska ITB a KIB,
- špecifikáciu požiadaviek na bezpečnostný projekt pre oblasť ITB a KIB,
- realizáciu kontroly zameranej na naplnenie požiadaviek definovaných v bezp. projekte za oblasť ITB a KIB
- realizáciu kontroly zameranú na správnosť nastavení a konfigurácii bezpečnosti jednotlivých prostredí,
- realizáciu kontroly zameranú realizáciu procesu posudzovania a komplexnosti bezpečnostných rizík, bezpečnosť a kompletný popis rozhraní, správnu identifikácia závislostí,
- realizáciu kontroly naplnenia definovaných požiadaviek pre oblasť ITB a KIB,
- realizáciu kontroly zameranú na implementovaný proces v priamom súvisi s ITB a KIB,
- realizáciu kontroly súladu s planou legislatívou v oblasti ITB a KIB (obsahuje aj kontrolu leg. požiadaviek)
- realizáciu kontroly zameranú zabezpečenie procesu, interfejsov, integrácii, kompletného popisu rozhraní a spoločných komponentov a posúdenia z pohľadu bezpečnosti,
- poskytovanie konzultácií a súčinnosti pre problematiku ITB a KIB,
- získavanie a spracovanie informácií nutných pre plnenie úloh v oblasti ITB a KIB,
- aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 85/2020 Z.z., Prílohou č.1
- plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

Odporúčané kvalifikačné predpoklady

- doplňte podľa potreby alebo vymažte
- Certifikát vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou.

10. ODKAZY

Neaplikovateľné – pre tento projektový zámer nie sú uvedené žiadne relevantné odkazy na externé dokumenty alebo informačné zdroje.

11. PRÍLOHY

Príloha 1: Katalóg požiadaviek (Excel)

Príloha 2: Zoznam rizík a závislostí (Excel)

Príloha 3: Stratégia rozvoja ITAM

Príloha 4: Detailný návrh riešenia – Implementácia informačného systému riadenia IT aktív a poskytovanie aplikačnej podpory (na vyžiadanie z dôvodu obsahu citlivých údajov)

Príloha 5: CBA

Príloha 6: Rozdielová analýza

-

Koniec dokumentu

[1] Pozn.: Projektový iniciálny dokument je dostupný na vyžiadanie.

[2] Spoločné moduly podľa zákona č. 305/2013 e-Governmente