projekt_2578_Pristup_k_projektu_detailny

PRÍSTUP K PROJEKTU

Vzor pre manažérsky výstup I-03

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	30.4.2024	

1. História dokumentu

Verzia	Dátum	Zmeny	Meno
1.0	30.04.2024	Vydanie dokumentu	Igor Hladík

2. Účel dokumentu

V súlade s Vyhláškou 401/2023 Z.z. je dokument I-03 Prístup k projektu určený na rozpracovanie detailných informácií prípravy projektu z pohľadu aktuálneho stavu, budúceho stavu a navrhovaného riešenia.

Dokument Prístup k projektu v zmysle vyššie uvedenej vyhlášky obsahuje opis navrhovaného riešenia, architektúru riešenia projektu na úrovni biznis vrstvy, aplikačnej vrstvy, dátovej vrstvy, technologickej vrstvy, infraštruktúry navrhovaného riešenia, bezpečnostnej architektúry, špecifikáciu údajov spracovaných v projekte, čistenie údajov, prevádzku a údržbu výstupov projektu, prevádzkové požiadavky, požiadavky na zdrojové kódy. Zároveň opisuje aj implementáciu projektu a preberanie výstupov projektu.

Vzhľadom na skutočnosť, že projekt Rozširovania riadenia IT aktív - ITAM 2.0 (ďalej tiež ako „ITAM 2.0) je len pokračovaním a rozšírením pôvodného projektu vybudovania centrálnej kompetencie riadenia IT aktív, ktorý pozostával z implementácie informačného systému riadenia IT aktív a zabezpečenia expertných služieb v oblasti optimalizácie IT aktív (ďalej tiež ako „ITAM 1.0“), tento dokument sa, tam kde je to relevantné, len odkazuje na iné dokumenty, ktoré boli spracované v rámci ITAM 1.0 a poskytujú informácie požadované týmto dokumentom.

Súčasná iniciatíva budovania centrálnej kompetencie riadenia ITAM vo verejnej a štátnej správe predstavuje základný pilier budovania efektívneho ITAM. Ten treba ďalej rozvíjať smerom na ďalšie OVM a zároveň ho dopĺňať o ďalšie oblasti, prostredníctvom ktorých sa súčasné nastavenie a rozsah ITAM priblíži k najmodernejším programom týkajúcich sa zabezpečovania softvéru a celkového riadenia portfólia (ďalej tiež ako „SSPM“ z anj. Software Sourcing and Portfolio Management).

Budúce smerovanie ITAM (Predkladaný projektový zámer):

1. Zapájanie ďalších OVM k centrálnemu riadeniu ITAM.
2. Hlavné iniciatívy rozširovania kompetencií ITAM vrátane:

- Riadenia a optimalizácia aplikačného portfólia
- Riadenie softvérových zraniteľností
- Optimalizácia nákupu softvérových licencií Tier 3
- Riadenie cloudových služieb (IaaS/Paas) a FinOps

2.1 Použité skratky a pojmy

SKRATKA/POJEM	POPIS
AI	Artifical 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 as 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. Popis navrhovaného riešenia

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.

Pre manažérsky sumár navrhovaného riešenia viď kapitoly 3.1 a 3.2 Projektového zámeru.

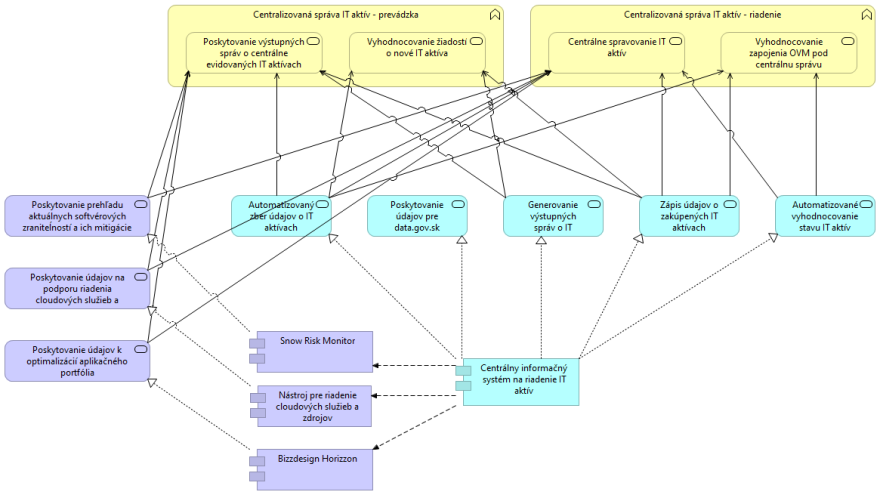
4. Architektúra riešenia projektu

4.1 Biznis vrstva

Biznis architektúra predkladaného riešenia je detailne rozpracovaná v rámci Detailného návrhu riešenia projektu ITAM 1.0 – kapitola 6, ktorá je doplnená o architektonický návrh budúceho riešenia v rámci projektu ITAM 2.0 – viď kapitolu 5 Projektového zámeru.

Náhľad architektúry:

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



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 zraniteľnosti NIST (National Institute of Standards and Technology). Snow Risk Monitor poskytuje ďalej nasledujúce funkcionality:
    - Identifikuje zraniteľnosti naprieč celým aplikačným portfóliom.
    - Kategorizuje a priorizuje 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.
- BizzDesign 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“

Pri Snow Risk Monitor a FinOps 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 projektom ITAM 2.0.

4.1.1 Prehľad koncových služieb – budúci stav:

Projekt ITAM 2.0 neuvažuje so žiadnymi novými koncovými službami.

4.1.2 Jazyková podpora a lokalizácia

Požadované používateľské rozhrania všetkých požadovaných komponentov ITAM budú v slovenskom aj anglickom jazyku.

4.2 Aplikačná vrstva

Aplikačná architektúra predkladaného riešenia je detailne rozpracovaná v rámci Detailného návrhu riešenia projektu ITAM 1.0 – kapitola 10, ktorá je doplnená o architektonický návrh budúceho riešenia v rámci projektu ITAM 2.0 – viď kapitolu 5 Projektového zámeru.

Projekt ITAM 2.0 uvažuje s troma novými aplikačnými službami, tak ako je uvedené v kapitole 5.1.3 Projektového zámeru.

3 nové aplikačné služby:

- Rozšírenie využitia platformy Bizzdesign Horizzon, 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.

Kľúčovým komponentom v rámci ITAM 2.0 je IS ITAM.

IS ITAM je založený na riešení Snow Software Box. Architektúra platformy SNOW navrhnutá pre projekt ITAM je schopná zbierať a vyhodnocovať údaje až pre 75000 zariadení bez úprav. Celé riešenie je škálovateľné a v prípade väčšieho počtu zariadení je možné rozšíriť rozsah zberu údajov o ďalší aplikačný server. Prostredie je rozdelené na dve časti:

- Centrálne produkčné riešenie, ktoré obsahuje hlavný aplikačný a databázový server a zhromažďuje všetky údaje. Obsahuje centrálnu aplikáciu pre prístup používateľov k prostrediu IS ITAM.

- Server Snow Gateway umiestnený v každej pripojenej organizácii. Používa sa na zber údajov v internej sieti organizácie a na komunikáciu s centrálnym riešením. V prípade integrácie centrálneho riešenia s internou aplikáciou komunikuje s aplikačným serverom Snow License Manager pomocou rozhrania API.

V prípade pripojenia externých systémov, nasadenia novej verzie alebo hromadnej práce s údajmi bude k dispozícii aj samostatné testovacie prostredie, ktoré sa použije na overenie testovacích scenárov pri nasadzovaní IS ITAM pre nové organizácie, ako aj na testovanie správy opráv IS ITAM, prípadne na testovanie integračných scenárov pre externé aplikácie.

KOMPONENTY CENTRÁLNEHO RIEŠENIA:

Aplikačný server: Snow License Manager

Hlavný aplikačný server pre prístup používateľov k informáciám IS ITAM. Aplikácia je prístupná prostredníctvom štandardných webových prehliadačov na adrese https:\\app.itam.sk. Prístup je zabezpečený protokolom https s definovaným certifikátom. Používateľ využíva služby len na základe autentifikácie v aplikácii, prístup neautentifikovaných používateľov nie je povolený.

Zabezpečenie prístupu je riadené sieťovou vrstvou fyzickej infraštruktúry.

Aplikačný server obsahuje rozhranie na integráciu s okolitými systémami vo forme rozhrania API. Používanie API je možné len pre definované systémy a len na základe overenia.

Aplikačný server: Snow Inventory Server

Server určený na zber údajov z jednotlivých organizácií a zber údajov z cloudových služieb. Komunikácia s jednotlivými OVM sa zabezpečuje prostredníctvom webovej služby na adrese https:\\inv.itam.sk.

Databázový server

Databázový server obsahuje dve databázy pre hlavné aplikačné servery, databázu Snow License Manager a databázu Inventory server.

Databázy sú plne spravované aplikačnou vrstvou. Služby databázového servera zabezpečujú pravidelné zálohovanie, indexovanie databáz a údržbu s cieľom zachovať integritu oboch databáz.

Aplikačný server v prostredí pripojenej organizácie

Organizácia bude komunikovať s centrálnym riešením pomocou aplikačného servera Snow Gateway. Server zabezpečuje zber údajov v rámci organizácie od agentov a konektorov. Poskytuje internú komunikáciu prostredníctvom webovej služby nakonfigurovanej na internú sieťovú adresu.

Údaje sa do centrálneho riešenia odosielajú v automatizovanej šifrovanej forme. Komunikáciu zabezpečujú služby centrálneho riešenia https:\\api.itam.sk.

Klienti

Klienti aplikácie pracujú s centrálnym aplikačným serverom Snow Linceses Manager iba prostredníctvom webového prehliadača. Prístup k aplikácii sa zabezpečuje prostredníctvom overovacieho formulára. Aplikácia riadi prístup k jednotlivým informáciám na základe pridelenej role a organizácie.

Snow Agent

Agent Snow je aplikácia, ktorá zhromažďuje SW a HW údaje z koncových zariadení a servera. Možno ho nainštalovať na serveroch so systémami Windows, Linux, UNIX, AIX a macOS. Agent komunikuje s centrálnym riešením pred bránou Snow Gateway (alebo priamo s inventárnym serverom). Cieľom agenta je tiež zhromažďovať údaje o používaní softvéru a cloudových služieb na koncových zariadeniach. Komunikácia s centrálnym riešením prebieha prostredníctvom webových služieb a je šifrovaná. Výstupom agenta je zašifrovaný súbor, ktorý sa dešifruje až v centrálnom riešení uložením do databázy.

Snow Integration Manager

Aplikácia vykonáva zber údajov z iných systémov (VMware, Hyper-V, SCCM, ILMT a ďalších). V prípade pripojenia k iteratívnym aplikáciám organizácie sa nachádza na serveri Snow GW. Aplikácia získava informácie väčšinou pomocou funkcií API aplikácií, výstupom sú zašifrované súbory.

V prípade získavania informácií o overených cloudových službách (O365, Adobe Cloud atď.) je aplikácia umiestnená na aplikačnom serveri Snow Inventory Server a poskytuje zber informácií o cloudových službách pomocou rozhraní API.

4.2.1 Rozsah informačných systémov – AS IS

Viď nasledujúcu kapitolu.

4.2.2 Rozsah informačných systémov – TO BE

AS-IS aj TO-BE informačné systémy sú uvedené v rámci Projektového zámeru – kapitola 5.1.2

4.2.3 Využívanie nadrezortných a spoločných ISVS – AS IS

Projekt ITAM 2.0 nevyužíva žiadne nadrezortné a spoločné ISVS.

4.2.4 Prehľad plánovaných integrácií ISVS na nadrezortné ISVS – spoločné moduly podľa zákona č. 305 /2013 e-Governmente – TO BE

Projekt ITAM 2.0 neuvažuje s integráciou na žiadne nadrezortné a spoločné ISVS. V prípade potenciálneho dopytu po dátach uložených v rámci ITAM 2.0 bude využité štandardné API rozhranie.

4.2.5 Prehľad plánovaného využívania iných ISVS (integrácie) – TO BE

Viď predchádzajúcu kapitolu.

4.2.6 Aplikačné služby pre realizáciu koncových služieb – TO BE

Viď kapitolu 5.1.3 Projektového zámeru.

4.2.7 Aplikačné služby na integráciu – TO BE

Predmetný projekt svojím rozsahom a zameraním nepredpokladá vytvorenie / budovanie aplikačných služieb poskytovaných na externú integráciu, integráciu na nadrezortné centrálne 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.

4.2.8 Poskytovanie údajov z ISVS do IS CSRÚ – TO BE

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

4.2.9 Konzumovanie údajov z IS CSRU – TO BE

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

4.3 Dátová vrstva

Pre účely spracovania dátovej architektúry, resp. dátovej vrstvy riešenia treba poznamenať, že predmetný projekt svojím rozsahom a zameraním nerieši životné situácie, nepredpokladá poskytovanie koncových služieb občanom, príp. podnikateľom, ako ani nevyužíva služby poskytované nadrezortnými / podpornými centrálnymi blokmi.

Z pohľadu údajov nepredpokladá využitie, resp. vytváranie referenčných, analytických a ani mojich údajov.

ITAM 2.0 predpokladá využitie štandardných riešení, tzv. Commercial off-the-shelf softvérov (ďalej tiež ako „COTS“), t.j. neuvažuje nad vývojom v dátovej vrstve.

Dátové entity v rozsahu projektu ITAM 1.0 sú bližšie popísané v rámci Prílohy 4 Projektového zámeru - Detailný návrh riešenia – kapitola 7.

4.3.1 Údaje v správe organizácie

Princípy dátovej architektúry majú za cieľ uspokojiť informačné potreby všetkých zainteresovaných strán z hľadiska dostupnosti informácií, bezpečnosti a kvality. Vo všeobecnosti sa dátová architektúra riadi nasledujúcimi princípmi:

- Údaje a informácie sú aktívom pre MIRRI SR a ostatné OVM pripojené k projektu ITAM 2.0;
- Údaje je potrebné spravovať opatrne ako aktívum zabezpečením:
    - primeranej kvality,
    - dôvernosti, t.j. informácie sú sprístupnené alebo zverejnené len oprávneným jednotlivcom, subjektom alebo procesom prostredníctvom autentifikácie (t.j. identifikácie používateľa) a autorizácie (t.j. určením úrovní prístupu k dátovým zdrojom, resp. zdrojom systému),
    - integrity, t.j. zabezpečenie presnosti a úplnosti údajov počas celého ich životného cyklu,
    - dostupnosti, t.j. informácie musia byť dostupné vtedy, keď sú potrebné,
    - auditných záznamov, t.j. sledovania aktivít v systéme.
    - pochopenia a efektívneho využívania.
- Zodpovednosť za správu údajov zdieľajú správcovia biznis údajov.

4.3.2 Dátový rozsah projektu - Prehľad objektov evidencie - TO BE

Viď kapitolu 4.3.4

4.3.3 Referenčné údaje

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

4.3.3.1 Objekty evidencie z pohľadu procesu ich vyhlásenia za referenčné

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

4.3.3.2 Identifikácia údajov pre konzumovanie alebo poskytovanie údajov do/z CSRU

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

4.3.4 Kvalita a čistenie údajov

4.3.4.1 Zhodnotenie objektov evidencie z pohľadu dátovej kvality

V súlade s navrhovaným prevádzkovým modelom pre riadenie centrálnej kompetencie ITAM, riadenie dátovej kvality vychádza z medzinárodného štandardu ISO/IEC 19770-1:2017 - IT asset management systems.

V tomto kontexte je cieľom riadenia kvality dát 1) zabezpečiť, aby požadované údaje o všetkých relevantných IT aktívach boli presne a úplne zaznamenané počas celého životného cyklu a aby pre všetky IT aktíva existovali zdokumentované informácie o tom, či sú alebo nie sú autorizované, a 2) zabezpečiť, aby existovali primerané procesy overovania úplnosti údajov s cieľom dosiahnuť dôveryhodné údaje, ktoré môžu napríklad znížiť riziko neoprávneného nasadenia softvéru a vďaka úplnej dôvere v inventárne údaje smerovať k lepším biznis rozhodnutiam o budúcich nákupoch softvéru a k potenciálnym úsporám a zamedzeniu zbytočných nákladov.

Na nasledujúcom obrázku sú uvedené atribúty dátovej kvality v kontexte riadenia ITAM:

Zber, vyhodnocovanie a riadenie procesov zberu dát do centrálneho IS ITAM sú založené na troch základných pilieroch uvedených nižšie. Okrem toho existujú aj ďalšie IT aktíva, ktoré predstavujú špecificky konsolidované aktíva typu Datacentrum, použité pre virtualizáciu alebo ďalšie rozširujúce aktíva ako napr. firewally, sieťové prvky a pod. Špeciálnu kategóriu tvoria mobilné zariadenia alebo iné užívateľské zariadenia, ktoré nie sú osobným počítačom.

Hardvérové aktíva

IT vybavenie, ktoré je evidované ako spravovaný majetok OVM a je možné vykonávať jeho automatizovaný sken. Patria sem:

- servery (fyzické, virtuálne alebo v prenájme),
- koncové zariadenia (desktopy, laptopy),
- virtuálne stanice a
- všetky zariadenia obstarané ako IaaS.

Z hľadiska softvérovej evidencie je tiež potrebné evidovať všetky vlastnosti o zariadeniach, na ktorých je softvér nainštalovaný s ohľadom na možný vplyv na licenčné podmienky.

Pri hardvérových aktívach sa evidujú: číslo na štítku, sériové číslo, výrobca, model, umiestnenie a vlastník. Uvedené je determinované skenovacími agentami IS ITAM (platforma Snow).

Softvérové aktíva

Všetok softvér používaný používateľmi na jednotlivých hardvérových zariadeniach alebo ako SaaS. Tieto aktíva obsahujú nasledovné informácie:

- Názov, verzia vydania alebo jasná identifikácia.
- Metriky licencií na meranie počtu potrebných licencií.
- Odkaz na zariadenie a používateľa.
- Interná a externá kategorizácia.
- Meranie skutočného využitia (t.j. počet SW štartov používateľom).
- Väzba na špecifiká prostredia (terminálové servery, virtuálna pracovná plocha atď.).
- Ďalšie merateľné a skenovateľné atribúty agentami IS ITAM.
- Zraniteľnosti naprieč celým aplikačným portfóliom, ich kategorizácia, prioritizácia a návrh mitigácie.
- Metamodel, koncepty definované modelovacím jazykom Archimate, ako napr. aplikácia, aplikačné služby relevantné z pohľadu APM a pod.

Ďalej sem patria nadobúdacie doklady vrátane objednávok, faktúr, dodacích listov ako aj metrík a podmienok, licenčné modely a pod.

Používateľ

Interný alebo externý pracovník OVM, prípadne iná osoba, ktorá využíva akékoľvek IT prostriedky v organizácii a je možné ju na úrovni IT prostriedkov identifikovať (najčastejšie používateľským účtom):

- Aktívni používatelia sú priradení k použitým softvérovým aktívam.
- Špecifiká použitia (používateľský model, súbežný server a iné).
- Prehľad použitia a ich kategorizácie (vnútorné, externé).
- Presná identifikácia osoby na odstránenie možných duplicít.
- Kategorizácia podľa požiadaviek na správne vykazovanie (oddelenie, funkcia, typ a podpora).

4.3.4.2 Roly a predbežné personálne zabezpečenie pri riadení dátovej kvality

Rola	Činnosti	Pozícia zodpovedná za danú činnosť (správca ISVS / dodávateľ)
ITAM analytik	Evidencia požiadaviek na dátovú kvalitu, monitoring a riadenie procesu Práca s IS ITAM, analýza dát dostupných v IS ITAM, generovanie reportov umožňujúcich rozhodovanie o optimalizácii softvérových výdavkov na základe dát. Poskytovanie podpory pri sledovaní a správe fyzických IT aktív, zabezpečení správneho záznamu a evidencii aktív, udržiavanie inventárnych záznamov.	ITAM analytik (Oddelenie pre správu licencií a centralizované obstarávanie IT komodít)
Databázový špecialista	Analyzuje požiadavky na dáta, modeluje obsah procedúr	Dodávateľ
Dátový špecialista pre dátovú kvalitu	Spracovanie výstupov merania, interpretácie, zápis biznis pravidiel, hodnotiace správy z merania	Dodávateľ

4.3.5 Otvorené údaje

V nasledujúcej tabuľke sú uvedené objekty evidencie, ktoré budú realizáciou projektu sprístupnené ako otvorené údaje.

Názov objektu evidencie / datasetu *(uvádzať OE z tabuľky v kap. 4.3.2)*	Požadovaná interoperabilita (*3 - 5)*	Periodicita publikovania *(týždenne, mesačne, polročne, ročne)*
Softvérové aktíva – celkové ročné náklady na Tier 1 výrobcov SW	3	Polročne

4.3.6 Analytické údaje

Predmetný projekt svojim rozsahom a zameraním nepredpokladá prácu s analytickými údajmi.

4.3.7 Moje údaje

Predmetný projekt svojim rozsahom a zameraním nepredpokladá prácu s Mojimi údajmi.

.

4.3.8 Prehľad jednotlivých kategórií údajov

Predmetný projekt svojim rozsahom a zameraním nerieši životné situácie ani neposkytuje koncové služby pre občanov, resp. podnikateľov.

4.4 Technologická vrstva

4.4.1 Prehľad technologického stavu - AS IS

Technologická architektúra predkladaného riešenia je detailne rozpracovaná v rámci Prílohy 4 Projektového zámeru - Detailný návrh riešenia projektu ITAM 1.0 – kapitola 11, ktorá je doplnená o architektonický návrh budúceho riešenia v rámci projektu ITAM 2.0 – viď kapitolu 5 Projektového zámeru.

V prípade nových komponentov Snow Risk Monitor a platformy FinOps, tie budú dostupné pre projekt ITAM 2.0 vo forme SaaS. Z tohto dôvodu nie je potrebné uvažovať s novými požiadavkami v oblasti technologickej architektúry.

4.4.2 Požiadavky na výkonnostné parametre, kapacitné požiadavky – TO BE

Tak ako je uvedené v Projektovom zámere – kapitola 3.11, 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, ktorý je definované v Prílohe 4 Projektového zámeru - Detailný návrh riešenia projektu ITAM 1.0 - kapitola 11.

4.4.3 Návrh riešenia technologickej architektúry

Viď 4.4.1

4.4.4 Využívanie služieb z katalógu služieb vládneho cloudu

V nasledujúcej tabuľke je uvedený prehľad plánovaného využívania infraštruktúrnych cloudových služieb:

Kód infraštruktúrnej služby *(z MetaIS)*	Názov infraštruktúrnej služby	**Kód využívajúceho ISVS** *(z MetaIS)*	**Názov integrovaného 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
infra_sluzba_598	Microsoft Azure Backup	isvs_9597	Centrálny informačný systém na riadenie IT aktív

Ďalšie informácie týkajúce sa testovacieho a produkčného prostredia sú uvedené v rámci Prílohy 4 Projektového zámeru - Detailný návrh riešenia projektu ITAM 1.0 – kapitola 11.

Projekt ITAM 2.0 nepredpokladá využívanie vývojového prostredia ani pri jednom z navrhovaných/požadovaných komponentov riešenia.

4.5 Bezpečnostná architektúra

Bezpečnostná architektúra pre existujúce riešenie je spracovaná v rámci Prílohy 4 Projektového zámeru - Detailný návrh riešenia projektu ITAM 1.0 – kapitola 15. Okrem toho bol pre projekt ITAM 1.0 spracovaný Bezpečnostný projekt, ktorý je dostupný na vyžiadanie na Oddelení pre správu licencií a centralizované obstarávanie IT komodít (MIRRI SR).

Nové komponenty riešenia – Snow Risk Monitor a platforma FinOps budú dostupné ako SaaS služba.

5. Závislosti na ostatné ISVS / projekty

Nie sú známe žiadne závislosti na ostatných ISVS / projektoch.

6. Zdrojové kódy

Keďže navrhované riešenie predpokladá využitie štandardných softvérov – COTS, požiadavka na dostupnosť a odovzdanie zdrojových kódov nie je opodstatnená. V prípade vývoja na mieru podľa požiadaviek MIRRI, táto časť kódu bude odovzdaná v zmysle požiadaviek definovaných budúcou zmluvou o implementácii ITAM 2.0 (obdobným spôsobom ako v prípade projektu 1.0).

7. Prevádzka a údržba

Viď Prílohu 1 - Prevádzkový opis a pokyny pre servis a údržbu, ktorý bol spracovaný v rámci projektu ITAM 1.0. Ostatné – nové komponenty predkladaného riešenia budú dostupné vo forme SaaS a z hľadiska požiadaviek na dostupnosť alebo prevádzkové služby budú kopírovať požiadavky kladené na IS ITAM.

7.1 Prevádzkové požiadavky

Viď Prílohu 1 - Prevádzkový opis a pokyny pre servis a údržbu.

7.1.1 Úrovne podpory používateľov

Viď Prílohu 4 Projektového zámeru - Detailný návrh riešenia – Kapitola 14 a Prílohu 1 tohto dokumentu - Prevádzkový opis – kapitola 17.

7.1.2 Riešenie incidentov – SLA parametre

Viď Prílohu 4 Projektového zámeru - Detailný návrh riešenia – Kapitola 14 a Prílohu 1 tohto dokumentu - Prevádzkový opis – kapitola 17.

7.2 Požadovaná dostupnosť IS:

7.2.1 Dostupnosť (Availability)

Viď Prílohu 4 Projektového zámeru - Detailný návrh riešenia – Kapitola 14.

7.2.2 RTO (Recovery Time Objective)

Recovery Time Objective = 24hod

7.2.3 RPO (Recovery Point Objective)

Recovery Point Objective = 48hod

8. Požiadavky na personál

Požiadavky na personál budú obdobné ako pri realizácii projektu ITAM 1.0. Bližšie informácie sú uvedené v rámci Projektového iniciačného dokumentu (kapitoly 2.2.3 a 6), ktorý bol spracovaný v rámci projektu ITAM 1.0 a bude aktualizovaný pre potreby projektu ITAM 2.0 počas jeho realizácie. Okrem toho v rámci realizácie služieb týkajúcich sa riadenia aplikačného portfólia, bude nevyhnutná komunikácia s kľúčovými používateľmi systémov za jednotlivé OVM, ktoré budú súčasťou riadenia aplikačného portfólia.

9. Implementácia a preberanie výstupov projektu

Implementácia a preberanie výstupov projektu budú obdobné ako pri realizácii projektu ITAM 1.0. Bližšie informácie sú uvedené v rámci dokumentu - Projektový iniciačný dokument – kapitola 10, ktorý je dostupný na vyžiadanie.

10. Prílohy

Príloha 1 - Prevádzkový opis a pokyny pre servis a údržbu