projekt_991_Pristup_k_projektu_detailny

PRÍSTUP K PROJEKTU

(Project approach)

Identifikovanie požiadaviek **na technickú časť riešenia**

Identifikácia projektu

Povinná osoba	*NASES*
Názov projektu	*Detekcia zraniteľnosti koncových obslužných bodov*
Zodpovedná osoba za projekt	*Ing, Michal Seliga*
Realizátor projektu	*NASES*
Vlastník projektu	*NASES*

Schvaľovanie dokumentu

Položka	**Meno a priezvisko**	**Organizácia**	**Pracovná pozícia**	**Dátum**	**Podpis** (alebo elektronický súhlas)

Vypracoval	Michal Seliga	NASES	PM	12.2.2021	
Overil					

OBSAH

Nápoveda inštrukcie k vypĺňaniu dokumentu Prístup k projektu:

***Šedý text** v celom dokumente predstavuje nápovedu pre vyplnenie dokumentu, po vyplnení kapitol odporúčame text šedou farbou vymazať.*

***Zelenou farbou** je nápoveda pre prípravnú fázu projektu (ešte nečerpáte rozpočet) a modrou farbou pre iniciačnú fázu projektu (začínate alokovať pracovníkov na špecializovaných útvaroch – z dôvodu doplňania úvodných vstupov), rovnako ako v prípade šedého textu odporúčame po vyplnení mazať.*

***Pre prípravnú fázu**, prosím ukladajte dokumenty s prefixom P_XX (podľa vyhlášky) a pre iniciačnú fázu s prefixom I_XX.*

Finálna, schválená verzia dokumentácia z predošlej fázy musí byť na karte dokumentov v MetaIS uložená s koncovkou _FIN.

Poznámka: Odporúčame aby ste si VŠETKY TABUĽKOVÉ VSTUPY evidovali a spravovali v jednom centrálnom EXCELI – s cieľom minimalizovať budúcu prácnosť s aktualizáciou a udržiavaním obsahu.

PRÍSTUP K PROJEKTU V PRÍPRAVNEJ FÁZE PROJEKTU SPRACOVÁVATE ešte pred akýmkoľvek schvaľovaním a odsúhlasovaním vášho dokumentu vo vedení úradu (OVM) alebo u vašej autority, ktorá je zodpovedná za rozpočet.

PRÍSTUP K PROJEKTU V INICIAČNEJ FÁZE PROJEKTU SPRACOVÁVATE už po úvodnom odsúhlasení vedením organizácie, čím pokračujete v zdetailizovaní vášho dokumentu.

VZORY a ŠABLONY zdrojových súborov sú tu:
https://www.mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/riadenie-kvality-qa/index.html

1. ÚČEL DOKUMENTU

V PRÍPRAVNEJ FÁZE:

- ***V súlade s Vyhláškou 85/2020 Z.z. o riadení projektov*** - *je dokument* ***Prístup k projektu*** *pre prípravnú fázu určený na rozpracovanie informácií k projektu, aby bolo možné rozhodnúť o pokračovaní prípravy projektu, alokovaní rozpočtu, ľudských zdrojov a prechode do iniciačnej fázy.*

V INICIAČNEJ FÁZE:

- ***V súlade s Vyhláškou 85/2020 Z.z. o riadení projektov*** *- je dokument* ***Prístup k projektu*** *pre iniciačnú fázu určený na rozpracovanie detailných informácií prípravy projektu.*

Dokument Prístup k projektu v zmysle vyššie uvedenej vyhlášky má o.i popisovať riešenie projektu v oblastiach:

1. *Architektúry riešenia – aplikačná vrstva, technologická vrstva, ...*
2. *Požiadaviek na dátový model, dátové konverzie a migrácie*
3. *Požiadavky UX dizajn (front-end a back-end vizual)*
4. *Požiadaviek na vládny cloud, prípadne zdôvodnenie jeho použitia*
5. *Kapacitné požiadavky na HW, SW a licencie*
6. *Požiadaviek na bezpečnosť riešenia*
7. *Požiadavky na testovanie a akceptačné kritéria*
8. *Požiadavky na prevádzku, výkonnosť, dostupnosť a zálohovanie*
9. *Požiadavky na integrácie, rozhrania a spoločné komponenty*
10. *Požiadavky na dokumentáciu a školenia*

Projekt vychádza zo súčasného stavu kybernetickej bezpečnosti v SR a Operačného programu Integrovaná infraštruktúra - špecifický cieľ 7.9: Zvýšenie kybernetickej bezpečnosti v spoločnosti za účelom zabezpečenie komplexnej kybernetickej bezpečnosti v spoločnosti. Cieľom tejto štúdie uskutočniteľnosti je poskytnúť strategický rámec, plánovaný rozsah, očakávaný časový harmonogram a prípadné odporúčania ďalších aktivít, z ktorých je potrebné pri realizácii implementácie národného projektu vychádzať.

Na problematiku bezpečnosti informačných systémov a aplikácií sa dá pozerať z viacerých strán. V prvom rade je to bezpečnosť z pohľadu siete, t. j. chrániť infraštruktúru pred hrozbami prostredníctvom sieťových prvkov, ktoré vedia chrániť infraštruktúru až po 7 vrstvu OSI modelu, avšak táto ochrana nie je viazaná na aplikačnú logiku. Aplikačná logika sa dá teda považovať za ďalšiu možnosť nazerania na problematiku bezpečnosti. S uvedenými spôsobmi súvisí aj zvýšenie bezpečnosti aplikácie zavedením zásad bezpečného vývoja aplikácii. Prax ukázala, že väčšina útokov na web a mobilné aplikácie sa vykonáva mimo bezpečného prostredia inštitúcie, t.j. na strane klienta a to aj napriek snahe o zabezpečenie danej aplikácie a implementácie rôznych detekčných mechanizmov.

1.1 Konvencie používané v dokumentoch – označovanie požiadaviek

Zvoľte si konvenciu pre označovanie požiadaviek, súborov, atd.

Architektúrne požiadavky používajú konvenciu:

Napr.

A_AB_Oxx

- *A – architektúrna požiadavka*
- *AB – označenie systému (ak existuje členenie; môže byť vypustené)*
- *O – označenie požiadavky*
- *xx – číslo požiadavky*

Infraštruktúrne požiadavky používajú konvenciu:

Napr.

IP_nn_ORxx

- *IP – infraštruktúrna požiadavka*
- *nn – identifikácia (ak existuje členenie; môže byť vypustené)*
- *O – označenie požiadavky*
- *xx – číslo požiadavky*

Komunikačné požiadavky používajú konvenciu: ...

Bezpečnostné požiadavky používajú konvenciu: ...

Požiadavky na dodávateľa používajú konvenciu: ...

Prevádzkové požiadavky používajú konvenciu: ...

Ostatné technické požiadavky používajú konvenciu: ...

ID	**SKRATKA**	**POPIS**
1.	MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie
2.	NASES	Národná agentúra pre sieťové a elektronické služby
3.	mID	Aplikácie mobilné ID
4.	ESDV	Aplikácia eSlovenskoDoVrecka
5.	UPVS	Ústredný portál verejnej správy

6.	ESD	Systém pre detekciu hrozieb a prienikov na úrovni endpoint a session
7.	TXM	Systém pre detekciu hrozieb a prienikov na úrovni transakcií
8.	MITM	Man In The middle útok
9.	MITB	Main In the browser útok
10.	RAT	Remote Access Trojan
11.	API	Aplikačné rozhranie
12.	RASP	runtine application self-protection
13.	WAF	Web applikačný firewall
14.	SIEM	Security information and event management
15.	CSIRT	Computer Security Incident Response Team
16.	SOC	Security operational center
17.	SPA	Single page application
18.	ENISA	Agentúra Európskej únie pre kybernetickú bezpečnosť
19.	DDoS	Distribuované odmietnutie služby

2. OPIS NAVRHOVANÉHO RIEŠENIA

Opis navrhovaného riešenia sa spracováva až po definovaní vybranej alternatívy riešenia, t.j. v iniciačnej fáze projektu (Popis vybraného riešenia – popis TO-BE stavu - na základe výsledkov MCA z dokumentu projektový zámer).

Prax a štúdie ukázali, že väčšina útokov na web a mobilné aplikácie sa vykonáva mimo bezpečného prostredia inštitúcie, t.j. na strane klienta a to aj pri najväčšej snahe o zabezpečenie danej aplikácie a implementácie rôznych detekčných mechanizmov. Patria sem hrozby ako phishing, vhishing, RAT (remote access trojan), session hijacking, account takeover, credentials stealing, MITB, MIM, API scrapping a mnoho ďalších. Je možné konštatovať, že sa jedná o útoky na zariadenie klienta, z ktorého pristupuje klient na služby inštitúcie.

Najzraniteľnejším bodom komunikačnej reťaze je zariadenie klienta a samotný občan. Využívaním moderných architektúr (HTML5 a JS frameworkov, natívnych mobilných aplikácií) kedy sa dbá na vysokú užívateľskú skúsenosť, rýchly vývoj, sprístupňovanie API rozhraní do internetu sa prenáša veľká časť aplikačnej a business logiky z bezpečného prostredia dátového centra inštitúcie do nebezpečného prostredia internetu, zariadenia alebo infraštruktúry klienta odkiaľ daný klient využíva dané služby.

Navrhovaný modul detekcie hrozieb a prienikov zahŕňa kľúčové techniky pre ochranu aplikácií postavených na moderných architektúrach. Patrí sem samoochrana aplikácii a detekcia hrozieb na strane klienta napr. v podobe RASP (runtine application self-protection), detekcie malware (škodlivých aplikácií), detekcie zmien v správaní klienta (behavioral analysis) a zaradenie platformy na automatizáciu pravidelných bezpečnostných udalostí. Treba si uvedomiť, že Detekcia zraniteľnosti koncových obslužných bodov je iba doplnok a nie je to náhrada za bezpečnostné testovanie, bezpečný vývoj alebo implementáciu prvkov ako sú firewall a WAF. Navrhovaný modul detekcie hrozieb a prienikov rozšíri poskytované služby na GOVNETE.

Ako funguje Detekcia zraniteľnosti koncových obslužných bodov:

Techniky a architektúry detekcie zraniteľnosti koncových obslužných bodov chránia aplikáciu z vnútra, bez potreby inštalácie špecializovaného softvéru na strane klientskeho zariadenia (napr. antvirus) prostredníctvom implementácie resp. integrácie do aplikácií, ktoré bežia mimo bezpečného prostredia inštitúcie. Uvedené prostredie sa z princípu musí považovať za prostredia nebezpečné, bez kontroly. Z pohľadu aplikácie je to transparentné a bez dopadu na aplikačnú logiku, je to transparentné z pohľadu aplikácie.

Príklady fungovania detekcie zraniteľnosti koncových obslužných bodov nájdete na:
https://www.ibm.com/security/fraud-protection/trusteer

Samotná architektúra môže byť postavená na čisto aplikačnej logike, ktorá beží výlučne na strane klienta alebo aj v kombinácii so službami/komponentami bežiacimi na strane servera inštitúcie v bezpečnej infraštruktúre, kde je možné vykonávať hlbšie analýzy pre detekciu sofistikovanejších útokov alebo útokov v prípravnej fáze.

Navrhované riešenie projektu zahŕňa nasledovné techniky pre ochranu aplikácií/služieb:

Prevencia:
Jedná sa o pasívnu ochranu aplikácií, ktorá pozostáva najmä z code obfucation, white box crytpografia, pinning certifikátov, šifrovanie zdrojov, auto expirácia, vlastná klávesnica, polymorfizmus, odstránenie testovacích dát a nebezpečných aplikačných modulov. Prevencia je mandatórna a mala by byť súčasťou metodiky bezpečného vývoja, pričom neprináša žiadne detekčné mechanizmy.

Základná detekcia:
Detekcia je zameraná najmä na získanie rôznych atribútov prostredia, v ktorom beží aplikačná logika. Sem patrí napr. detekcia debugerov a emulácií, detekcia rootnutých alebo jailbrake-nutých zariadení, kontrola integrity, fingerprintig zariadenia resp. device binding, detekcia škodlivého kódu na zariadení.

Rozšírená detekcia:
Sofistikované útoky , resp. rôzne realtime útoky zväčša nie je možné detegovať základnými metódami a je nutná značná systémová a analytická podpora. Do rozšírených metód detekcie patrí detekcia botnetov, metódy na detekciu script injections, api injections, RASP, mutlifactor

adaptívna autentifikácia a autorizácia, behaviorálna analýza a detekcia crossesion útočných vektorov.

VÝHODY:

- Zisťovanie zraniteľností v reťazci služieb
- Možnosť proaktívneho začatia protiopatrení
- Zvyšovanie spokojnosti koncových používateľov / zákazníkov
- Skrátenie času a úsilia nápravy incidentov približne o 80% *(Zdroj: ENISA - Main incidents in the EU and worldwide From January 2019 to April 2020)*
- Eliminácia bezpečnostných incidentov o 75% *(Zdroj: ENISA - Main incidents in the EU and worldwide From January 2019 to April 2020)*

Základné princíp integrácie do nových a bežiacich aplikácií:

1. Udalosti musia byť integrované do SIEM systému NASES využívaných v SOC a následná analýza interným CSIRT tímom;
2. Robustný analytický nástroj pre detekciu komplexných útočných vektorov;
3. Možnosť integrácie do WEB-ových (vrátane SPA) a Mobilných aplikácií (Android, iOS);
4. Zabezpečenie multikanálového a multitentného prístupu.
5. Pre podporu multifaktor autentifikácie resp. risk based autentifikácie sys poskytne rizikové skóre. Aktuálne v štáte nie je multifaktor autentifikácie resp. risk based autentifikácie sys

Na základe vyššie uvedeného bude **hlavným cieľom projektu** vybudovať Modul pre detekciu hrozieb a prienikov na strane klienta a ceste mimo infraštruktúry NASES.

3. ARCHITEKTÚRA RIEŠENIA PROJEKTU

V tejto kapitole detailne rozpracujte kapitolu 3.5 Náhľad architektúry z dokumentu I_01 Projektový zámer.

Spracovanie a rozsah tejto kapitoly závisí od typu projektu – budovanie ISVS, rozvoj ISVS, migrácia do vládneho cloudu, nákup HW atď. Napríklad pri budovaní/rozvoji ISVS navrhujete všetky vrstvy architektúry (biznis, aplikačná, technologická), pri nákupe HW nie je potrebné popisovať biznis a aplikačnú vrstvu architektúry a pod.

*Architektúra navrhovaného riešenia projektu musí byť v súlade s funkčnými, nefunkčnými a technickými požiadavkami definovanými v katalógu požiadaviek (**I-01 – Príloha 1: Katalóg požiadaviek)**.*

V prípravnej fáze projektu popíšte súčasný stav (AS-IS) architektúry aj s príslušným architektonickým modelom.

V iniciačnej fáze projektu popíšte budúci stav (TO-BE) architektúry riešenia aj s príslušným architektonickým modelom.

AS IS architektúra a TO BE architektúra musia byť spracované tak, aby bol zreteľný výsledok projektu (zmena).

Vyžadujeme, aby návrh architektúry bol zakreslený pomocou modelovacieho jazyka Archimate minimálne vo verzii 3 (linka na špecifikáciu: https://www.opengroup.org/archimate-forum/archimate-overview). Pre modelovanie a popis existujúcej (As-Is) aj budúcej (To-Be) architektúry odporúčame použiť modelovací nástroj, ktorý podporuje export modelu do štandardizovaného formátu „The Open Group ArchiMate Model Exchange File Format Standard“. V návrhu zohľadnite usmernenia z používateľskej príručky centrálneho metainformačného systému verejnej správy (aktuálna verzia je zverejnená na linke: https://metais.vicepremier.gov.sk/help) pre popis, modelovanie a zápis informácií o komponentoch do metainformačného systému verejnej správy (METAIS). Pre detailnejší popis procesov, ktorých sa projekt týka je možné použiť tiež modelovací jazyk BPMN (ISO 19510). Pre detailnejší návrh riešenia v aplikačnej vrstve je možné použiť aj jazyk UML (ISO 19505).

Modely môžu obsahovať viac náhľadov na riešenú oblasť tak, aby dostatočne zrozumiteľne popisovali eGov komponenty, ktoré majú byť predmetom riešenia, ako aj ich vzťahy a závislosti navzájom a vzťahy na ostatné komponety eGov (napr. spoločné moduly ústredného portálu verejnej správy, iné vlastné alebo externé ISVS, služby alebo dátové registre).

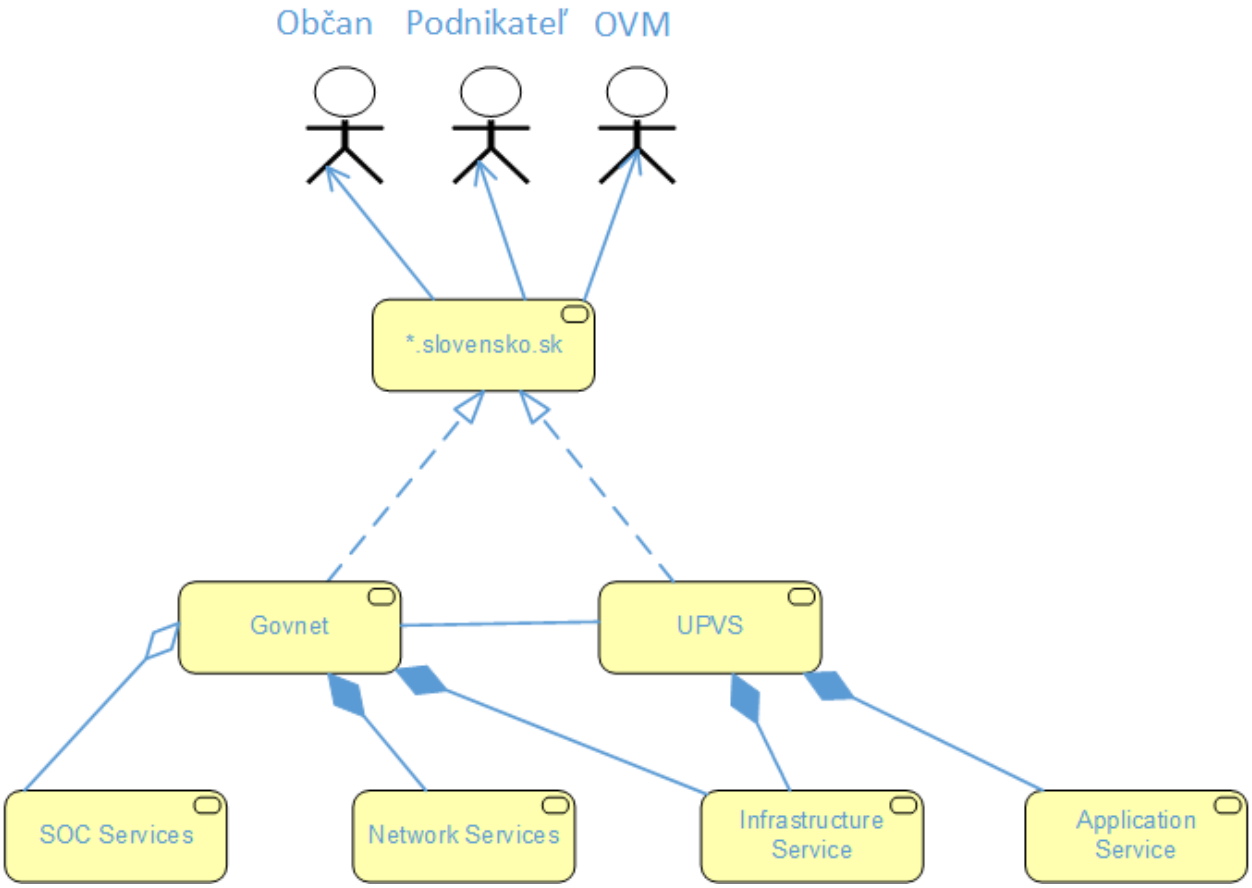
V tabuľke eGov komponentov uveďte všetky ISVS, AS, KS, ktoré sú výstupom projektu (rozvíjané alebo budované). eGovernment komponenty z tejto tabuľky musia korešpondovať s architektúrou TO BE a musia byť evidované v METAIS.

Tabuľka eGov komponenty (DOPLNIŤ VSTUPY v INICIAČNEJ FÁZE):

Typ (ISVS, AS, KS)	*Kód MetaIS*	*Názov*	*Budovaný / Rozvíjaný*
ISVS	isvs_404	Sieť GOVNET	Prevádzkovaný a plánujeme rozvíjať

Upozorňujeme: V prípade, že súčasťou projektu sú zmeny v biznis procesoch, musí byť technické riešenie postavené na aktualizovaných / redizajnovaných biznis procesoch s cieľom získať úspory v čase, napr. zrýchlením poskytnutia služby, v znížení nákladov atď.

Implementácia ESD riešenia dopĺňa službu GOVNET o nové možnosti detekcie zraniteľností a hrozieb pre služby poskytované Nasesom. Nedochádza k modifikácii business kontextu ani business procesom poskytovaných nadradenými službami, napr. www.slovensko.sk

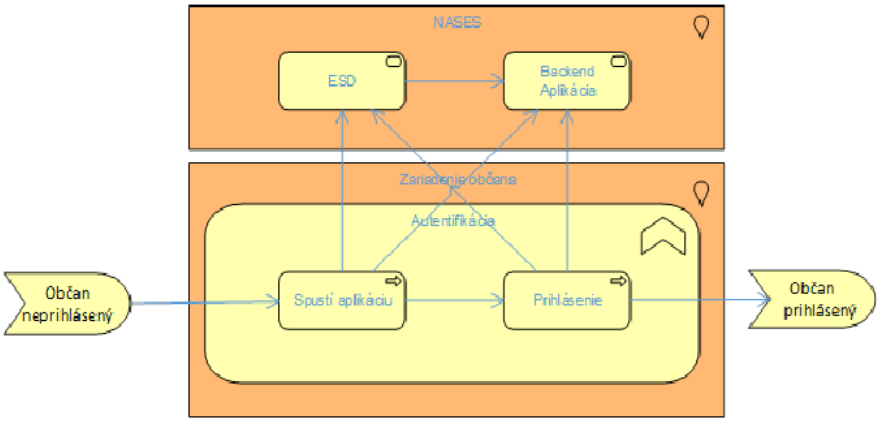


T.j. ESD riešenie z pohľadu business procesov aplikácie alebo riešenie môže ostať nezmenený alebo sa môže ľahko zmeniť aplikačná logika v závislosti na riziku.

Z pohľadu SOC a CSIRT sa dopĺňa ďalší zdroj udalostí pre analýzu a nápravne aktivity.

Implementácia ESD systému dopĺňa proces detekcie zraniteľností a hrozieb pre služby NASES-u.

Z pohľadu SOC a CSIRT sa dopĺňa ďalší zdroj udalostí pre analýzu a nápravne aktivity.



Obrázok popisuje generický scenár kedy dochádza k prihláseniu občana do aplikácie od momentu kedy si spustí aplikáciu (WEB, Mobile). Systém ESD monitoruje proaktívne atribúty a stav na úrovni koncového zariadenia, vykonáva „fingerprinting“ a behaviorálnu analýzu z pohľadu občana, zariadenia, lokality a session. Táto detekcia prebieha na pozadí a je nezávislá od interakcie občana s aplikáciou. V prípade zvýšenej hrozby je odoslaná správa do SOC, CSIRT. V prípade integrácie pri zvýšenom riziku je informovaná aplikácia z dôvodu obranných mechanizmov (zrušenie session ,zablokovanie , odhlásenie ..).

V zásade sa jedná o štatistické riešenie postavené na pravidlách alebo AI. Keďže riešenie môže bežať nezávisle od aplikácie, v tzv, silent móde (nie je priama interakcia medzi monitorovanou aplikáciou a systémom ESD), alebo aj v integrovanom móde (ESD vie priamo volať rozhrania monitorovanej aplikácie pre napr. zrušenie session, blokovanie používateľa …) je nutné zadefinovať základné rizikové parametre pre výberové konanie riešenia.

Riešením projektu je dosiahnuť ideálny scenár, a to je mat čo najnižšie False Positive Ratioa najvyššie Detection Rate, čo je technicky veľmi obtiažné a závislé od samotnej aplikácie, samotnej integrácie a riešenia pre detekciu hrozieb a prienikov. False Positive Ratio: pomer zle označených udalostí zo všetkých korektných udalostí, resp. sa jedná o nesprávne netegované prípady. Detection Rate, True positive: je citlivosť, tj. pomer správne detekovaných oproti všetkým čo mali byť detekovaný.

3.1 Biznis vrstva

IRELEVANTNÉ - z dôvodu, že samotná ESD nie je buisniss aplikácia ani komponentná z pohľadu koncového používateľa, je to iba jeden z ďalších zdrojov SOC/CSIRTu.

- *V prípravnej fáze projektu doplňte výstižné grafické zobrazenia (pohľady na model architektúry) a popis súčasného (AS-IS) stavu biznis vrstvy architektúry a krátky popis budúceho (TO-BE) stavu z pohľadu biznis architektúry*
- *V iniciačnej fáze projektu doplňte výstižné grafické zobrazenia (pohľady na model architektúry riešenia) a popis budúceho (TO-BE) stavu navrhovaného riešenia vybraného na základe MCA popísanej v Projektovom zámere. Navrhované riešenie musí korešpondovať s procesnými mapami v CBA a musí popisovať spôsob dosiahnutia a monitoringu prínosov uvedených v CBA.*
- *V popise riešenia urobte popis zmien medzi súčasným a budúcim stavom.*

3.2 Aplikačná vrstva

IRELEVANTNÉ- celá kapitola aj s podkapitolami irelevantná z dôvodu, že bezpečnostné riešenie nepracuje s dátovými objektmi.

- *V prípravnej fáze projektu uveďte model a popis súčasného (AS-IS) stavu* aplikačnej vrstvy architektúry.
- *V iniciačnej fáze projektu doplňte model a popis* budúceho (TO-BE) stavu navrhovaného riešenia aplikačnej vrstvy architektúry.
- *V popise budúceho stavu a jeho modeli popíšte, ako bude aplikačné riešenie podporovať procesy a prínosy uvedené v biznis vrstve.*
- *V popise riešenia urobte popis zmien medzi súčasným a budúcim stavom.*
- *V iniciačnej fáze projektu zohľadnite, modelujte a popíšte vzťahy na ostatné komponenty architektúry eGov (komponenty evidované v METAIS) ako sú spoločné moduly, iné ISVS a ich služby, referenčné registre*

V popise aplikačnej vrstvy sa pre každý budovaný/rozvíjaný ISVS jednoznačne vyjadrite k nasledovným bodom:

- *Použitie, alebo poskytovanie referenčných údajov (§ 49 – 55 zákona 305/2013*
- *Požiadavky na používanie registrovaných jednotných referencovateľných identifikátorov „URI“ (centrálny model údajov verejnej správy)*
- *Požiadavky na riešenie nariadenia (EU) 2016/679 - GDPR o ochrane osobných údajov – spôsob riešenia služby „Moje dáta“ (podľa konceptu Strategická priorita Manažment údajov (https://www.mirri.gov.sk/sekcie/strategicke-priority-nikvs/index.html)*
- *Požiadavky na riešenie zabezpečenia manažmentu zmluvných vzťahov pre poskytovanie služieb– vyplýva zo Zákona o ITVS 95/2019, §14, odsek 6 a automatizáciu monitorovania služieb a ich úrovne poskytovania*
- *Požiadavky na časť “Zoznam CI položiek (HW a SW) pre import do Servicedesku” (CMDB)*
- *Požiadavky “Automatizované monitorovanie služieb”– povinný výstup každého projektu.*

- *Požiadavky na časť "Poskytovanie analytických údajov a otvorených údajov (Open Data – detaily pre publikovanie na https://data.gov.sk/)"*
- *Požiadavky pre časť „aplikačné služby na externú integráciu" – prepájanie ISVS sa realizuje prostredníctvom vzťahu na úrovní 2 AS, ktoré nesmú poskytovať KS*
- *Požiadavka aby služby boli implementované tak, aby aj po nasadení do prevádzky fungovalo testovacie prostredie pre konzumentov a aby si integráciu mohol konzument otestovať aj s eID*
- *Požiadavky na návrh digitálnych služieb v súlade s Metodickým usmernením pre tvorbu používateľsky kvalitných elektronických služieb verejnej správy (https://www.mirri.gov.sk/wp-content/uploads/2020/10/Metodicke-usmernenie-pre-tvorbu-pouzivatelsky-kvalitnych-elektronickych-sluzieb-VS_7102020.pdf)*
- *Požiadavky na publikovanie elektronických služieb ISVS - aplikáciu odporúčaní z dokumentu Pravidlá publikovania elektronických služieb do multikanálového prostredia verejnej správy (https://www.mirri.gov.sk/wp-content/uploads/2018/10/Pravidla_Publikovania_Sluzieb_v1_0-1.pdf)*

Doplniť predpokladanú logickú architektúru schematicky a popisom (forma - použitím nástroja napr. ArchiMate v súlade so štandardom TOGAF – rovnako pre biznis procesy, aplikačnú a technologickú architektúru alebo UML diagramy (napr. Deployment Diagram)

Doplniť požiadavky na aplikačnú architektúru schematicky (rámcový návrh aplikačnej architektúry) a popisom, napr. v ponuke je potrebné uviesť:

- *logickú architektúru*
- *softvérovú (aplikačnú) architektúru riešenia v grafickej a textovej forme*
- *návrh logického členenia architektúry riešenia do modulov ISVS (detailnejší popis modulov a ich účelu)*
- *analytický dátový model na úrovni hlavných biznis objektov, ktoré sú premetom evidencie v riešení*

3.2.1 Popis aplikačnej architektúry riešenia na úrovni modulov ISVS a vzťahov medzi nimi

Popis modulov ISVS

Vysvetlenie účelu modulov ISVS

Funkčno-hierarchický model riešenia:

Doplniť model riešenia (forma - použitím nástroja napr. ArchiMate v súlade so štandardom TOGAF – rovnako pre biznis procesy, aplikačnú a technologickú architektúru alebo UML diagramy (napr. Deployment Diagram)

3.2.2 Popis dátovej architektúry riešenia na úrovni objektov evidencie a vzťahov medzi nimi

- *Logický dátový model*
- *Použité referenčné registre*
- *Prístup k riešeniu konceptu „Moje Dáta“ a GDPR*
- *Požiadavky na dátovú integráciu na CSRÚ (poskytovanie a konzumovanie údajov)*
- *Prístup k zabezpečeniu dátovej kvality a čistenie dát*
- *Prístup k príprave a zebezpečení testovacích dát*
- *Návrh dát, ktoré budú publikované ako Open Data*
- *Prístup k migrácii dát*

Použité dáta:

Popis požitých dát, popis štruktúr, tabuliek, dátových štruktúr a pamäťových blokov.

Pre každé zdieľané dáta s iným modulom a systémom ISVS je nutné uviesť

- *Dátové štruktúry*
- *Zoznam modulov ISVS, ktoré tieto dáta používajú*

Dátový model navrhovaného riešenia

Doplniť model riešenia (forma - použitím nástroja napr. ArchiMate v súlade so štandardom TOGAF – rovnako pre biznis procesy, aplikačnú a technologickú architektúru alebo UML diagramy (napr. Deployment Diagram)

3.3 Technologická vrstva

- Doplniť popis ASIS stavu
- Načrtnúť návrh TOBE stavu (+ popis alternatív)

Systémy ako ESD v súčasnosti NASES neprevádzkuje a pokiaľ je známe, z charakteru samotného systému je veľmi obtiažne zistiť či nejaké OVM podobný systém prevádzkuje.

Na trhu je množstvo systémov, ktoré môžu bežať v onPremise alebo sú ponúkané ako CLOUD riešenia, kde zákazník vykonáva iba základnú integráciu na úrovni ADC (Application delivery controller), v našom prípade sa jedná o F5 WAF/LB. V každom prípade ESD systém môže spracovávať veľké množstvo aj citlivých (vrátane osobných) údajov, môže analyzovať celá traffic prichádzajúcich a aj odchádzajúcich dát na úrovni session medzi používateľom a serverom. Z pohľadu priepustnosti sa jedná o systém spadajúci do kategória HPC, kedy je snaha v reálnom čase vypočítavať rizikové skóre session, koncového zariadenia, pripojenia či používateľa. Do výsledného deployment vstupujú spomenuté vlastnosti (throughput, spôsob integrácie, public cloud ...) a samotné potreby výťazného riešenia ktoré vyjde z súťaže VO.

V prípade OnPremise, požiadavky sú dané prevádzkovými štandardami NASES a systém bude interálnou súčasťou SOC, CSIRT (Je to zdroj bezpečnostných udalostí).

V požiadavkách pre časť „využívanie služieb vládneho cloudu“ doporučujeme zohľadniť:

- *Návrh aplikačnej a infraštruktúrnej architektúry v plnej miere zohľadňuje skutočnosť, že sú poskytované len služby uvedené v katalógu služieb Vládneho cloudu.*
- *Požiadavky na služby vládneho cloudu s93ú v plnej miere kompatibilné s aktuálnou verziou katalógu služieb vypublikovanej na https://www.sk.cloud alebo na* https://www.mirri.gov.sk/sekcie/informatizacia/egovernment/vladny-cloud/katalog-cloudovych-sluzieb/index.html

Požiadavky na služby vládneho cloudu doporučujeme mať ešte pred vyhlásením VO a následným spustením procesu migrácie – odkomunikované / odsúhlasené s prevádzkovateľom vládneho cloudu (MVSR)

Riešenia pre detekciu hrozieb a prienikov väčšinou fungujú autonómne. Vyžadujú si dedikovaný HW alebo môžu byť využívané ako cloud PaaS služby. Z dôvodu, že NASES prevádzkuje kritickú infraštruktúru, bude využívať riešenia inštalované prostredí resp. DC NASES. Predpokladom je, že súčasťou dodávky riešenia je dodávka infraštruktúrnych komponentov. K samotnému riešeniu následne sa bude pristupovať ako k „appliance“ t.j. ako hotovému, predkonfigurovanému riešeniu s jasne popísanými integračnými postupmi.

- Doplniť popis ASIS stavu
- Načrtnúť návrh TOBE stavu

Prostredia *(vyplní uchádzač):*

Súčasťou implementačného projektu je vybudovanie aj neprodukčného prostredia hlavne z dôvodu testovanie integrácie, testov patchovania a iných prevádzkových činností. Systém ESD je systém na detekciu hrozieb mimo chráneného perimetra, pričom testovanie alebo vývoj potencionálne chránených aplikácií beží v spravovanom prostredí a nie technicky možné nasimulovať reálne internetové prostredie. Neprodukčné prostredie (môže byť jedno pre deva je test) bude využívané čisto z dôvodu testov/ladenia prevádzkových činností, resp. potencionálnej integrácie.

Napr. v popise navrhovaného riešenia (vo forme štruktúrovanej tabuľky) uveďte parametre požadovaných prostredí:

- *produkčné (v zmysle požadovaného sizingu)*
- *testovacie (v minimálnom možnom sizingu) – určené pre testy nových modulov, úprav, zmenových požiadaviek a retesty na úrovni upgrade-ov (nie pre záťažové testovanie).*

V popise návrhu riešenia je požadované uviesť

- *sizing pre obidve prostredia*
- *požiadavky na integráciu*

*Poznámka: **doporučujeme**, aby ste si VŠETKY TABUĽKOVÉ VSTUPY evidovali a spravovali v jednom centrálnom EXCELI – s cieľom minimalizovať budúcu prácnosť s aktualizáciou a udržiavaním obsahu*

Štandardy a očakávané platformy na viacvrstvovom riešení:

Riešenie môže byť obstarané vo forme CLOUD služby ale aj môže byť implementované v onpremise prostredí. V prípade onpremise prostredia súťažné podklady budú obsahovať aktuálny štandard pre infraštruktúru budovania ISVS pri zohľadnení špecifík, atribútov a chovania bezpečnostných systémov a infraštruktúry.

Napr. pri použití vládneho cloudu ak navrhované riešenie v nejakej jeho časti zásadne nevyžaduje použitie iných platforiem, vyžadujeme uprednostnenie štandardov prostredia vládneho cloudu, v zmysle nasledujúceho prehľadu:

Napr.

Prehľad základných používaných štandardov v prostredí vládneho cloudu a OVM	
MS Windows 2012 R2	*= serverová platforma s diskovou storage-podporou (SAN)*
AIX 7.x	*= serverová platforma s diskovou storage-podporou (SAN)*
VMware ESX v xx.0	*= virtualizačná platforma pre servery*
MS SQL Server 2016	*= databázová (klástrová) platforma*
ORACLE 11g/12c	*= databázová platforma (alternatíva)*
.....	
MS ActiveDirectory 2012 R2	*= autorizačná platforma IAM (IdM) – vrátane podpory SSO*
MS Exchange 2016	*= e-mailový komunikačný systém*
.....	*= archivačná a zálohovacia platforma*
	= aktuálna platforma antivírusovej ochrany prostredia XYZ
MS Windows 10 *MS Office 2010 Std/Pro* *Internet Explorer IE v11, Chrome v62.x*	*= štandard vybavenia klientskej pracovnej stanice v prostredí XYZ (PC al. notebook s pripojením do LAN/WAN)*

Napr. Prehľad Open Source platforiem* akceptovateľných pre využitie v prostredí OVM	
ReadHat, Linux, ... a pod.	*= príklady serverových platforiem - operačný systém*
MySQL, PostgreSQL,... a pod.	*= príklady možných databázových platforiem*

*Poznámka: **doporučujeme**, aby ste si VŠETKY TABUĽKOVÉ VSTUPY evidovali a spravovali v jednom centrálnom EXCELI – s cieľom minimalizovať budúcu prácnosť s aktualizáciou a udržiavaním obsahu*

PRIKLAD:

IS bude využívať infraštruktúrne služby (IaaS) Vládneho cloudu podľa možností Katalógu služieb Vládneho cloudu:

- *Služby pripojenia do siete: Sieťové služby*
- *Služby výpočtového výkonu: Virtuálny server*
- *Architektúra CPU: x86-64, RISC*
- *Počet virtuálnych CPU: 1,2,4,8*
- *Veľkosť RAM: 1,2,4,8,16,32,64 GB*
- *Systémový diskový priestor: 20,32,40,80,100,128 GB*
- *Server OS (navrhované verzie OS musia byť podporované výrobcom v čase nasadenia projektu do produkčnej prevádzky min. 2 roky podľa oficiálneho „End-of-support" plánu dodávateľa):*
    - *x86: Windows server min. 2016*
    - *Red Hat Enterprise Linux min. 7,*
    - *RISK platforma: AIX min. 7.2 TL3 SP2 (64-bit)*
    - *CentOS: min. CentOS 7.3 (64-bit)*
- *Služby úložiska údajov: Diskový priestor TIER 1 (1 – 256 GB, max 1280 IOPS), TIER 2 (1 – 1000 GB, max 150 IOPS), TIER 3 (1 – 2000 GB, max 100 IOPS)*
- *Služby zálohovania*

PaaS Služby:

- *MDM: Talend MDM Platform, atď.*

Požiadavky na sizing

Riešenie môže byť obstarané vo forme CLOUD služby ale aj môže byť implementované v onpremise prostredí. V prípade onpremise prostredia súťažné podklady budú obsahovať aktuálny štandard pre infraštruktúru budovania ISVS pri zohľadnení špecifík, atribútov a chovania bezpečnostných systémov a infraštruktúry. Súčasťou ponuky vo VO musí byť kompletný detail požadovanej infraštruktúry aj so SLA parametrami, retenčnými politikami a kalkuláciou trendov.

Napr. požiadavka - súčasťou ponuky musí teda byť v technickej architektúre riešenia uvedený detailný popis HW a SW (OS, DB) komponentov

- *s úplným návrhom sizingu použitých komponentov, zohľadňujúcim členenie podľa jednotlivých častí/modulov/vrstiev a pre obidve tieto prostredia*
- *a s prihliadnutím na predpokladanú záťaž a rozvoj systému (min. na 6 rokov dopredu)*

doplniť nutný HW / komponenty pre projekt, doplniť popis technickej infraštruktúry potrebnej pre implementáciu navrhovaného riešenia.

ID	***Požadovaný HW*** *(stručný popis / názov)*	***Počet***
1.	*Doplň názov a stručný popis HW*	*Doplniť počet*
2.	*Doplň názov a stručný popis HW*	*Doplniť počet*
3.	*Doplň názov a stručný popis HW*	*Doplniť počet*

Výber služieb Vládneho cloudu (vyplní uchádzač)

Prostredie	*ID*	*Služba Vládneho cloudu (výber z katalógu služieb)*	*OS a verzia*	*Počet CPU*	*RAM (GB)*	*IS/modul/..*
Testovacie						
Predprodukčné						
Produkčné						

*Poznámka: **doporučujeme**, aby ste si VŠETKY TABUĽKOVÉ VSTUPY evidovali a spravovali v jednom centrálnom EXCELI – s cieľom minimalizovať budúcu prácnosť s aktualizáciou a udržiavaním obsahu*

Požiadavky na výkonnostné parametre, kapacitné požiadavky

Doplniť požiadavky, ktoré majú vplyv na výkon, sizing prostredí. Npr. Počet interných používateľov, počet externých používateľov, počet spracovávaných procesov, dokumentov,...

Komunikácia medzi vrstvami vládneho cloudu, využívanie sieťovej infraštruktúry (Govnet, LAN, VPN,...)

Komunikácia, sieťová a komunikačná infraštruktúra

Doplniť požiadavky na komunikáciu, napr. na výmenu dát, typ/spôsob pripojenia k sieti Internet, VPN, požiadavku na popis používaných TCP portov, nastavenia napr. Firewall-ov „..

Táto sekcia obsahuje všetko dôležité pre systémové procesy. Obsah závisí veľmi od použitého prostredia. Nasledujúce dve sekcie sú povinné, avšak je účelné vložiť aj iné sekcie.

Mapovanie procesov

Popis modulov použitých na tvorbu procesov v systéme.

HW mapping

Táto sekcia popisuje ako sú procesy replikované a ako sú distribuované v rámci HW prostredia .

Špeciálne požiadavky na SW konfiguráciu musia byť uvedené v tejto kapitole

3.3.2 ICloud HW a SW

Požiadavky na služby vládneho cloudu doporučujeme mať ešte pred vyhlásením VO a následným spustením procesu migrácie – odkomunikované / odsúhlasené s prevádzkovateľom vládneho cloudu (MVSR)

Stručný popis Cloud riešenia / zoznam HW komponentov (napríklad unix server, aplikačný server, PC ...) .

Všeobecný popis HW konfigurácie a vysvetlenie ako sú funkčné požiadavky mapované na HW. Špecifikácia, ktorý diagram ukazuje hlavné HW komponenty a relácie medzi nimi. Odkaz na externé manuály , ktoré detailne popisujú HW a SW prostredie.

3.3.3 Softvérová systémová infraštruktúra

Popísať požiadavky na systémové softvérové vybavenie (operačný systém, databázový systém, aplikačné platformy, ..)

3.3.4 Databázová štruktúra

Popisuje hlavné dátové bloky v databáze, ich štruktúru a relácie medzi nimi. Popisuje všetky špeciálne postupy použité v databáze a použitý DBMS. Popisuje ako sú mapované databázové polia na HW .

3.3.5 Hlavné riadiace toky

Rozdeľuje funkcie definované vo funkčnom dizajne na generické (logické) bloky a popisuje prepojenie každého generického bloku na systém. Sumarizuje procesy pre každý podsystém vrátane control flow diagramu medzi subsystémami.

3.3.6 Iné hľadiská dizajnu

Popis nasledovných ukazovateľov:

- *Technologické riziko*
- *Riešiteľnosť požiadaviek*
- *Bezpečnosť*
- *Ostatné regulačné a compliance podmienky*
- *Testovateľnosť*
- *Recovery*
- *Dostupnosť systému (24h)*
- *Životnosť a udržateľnosť systému*

3.3.7 Dátový model riešenia

3.3.8 Licencie

Doplniť požiadavky na licencie (nutný softvér), napr. aby ponuka obsahovala, aké licencie budú použité pre navrhovanú architektúru v členení:

- *aplikačný softvér*
- *systémový SW (operačné systémy, databázy a pod.)*
- *vlastné vyvíjané softvérové komponenty,*
- *treťostranné komponenty/moduly.*

ako aj v členení podľa prostredí, systémov, platforiem,...

Dôležité usmernenie pre oblasť zdrojových kódov:

- *Centrálny repozitár zdrojových kódov: https://www.zakonypreludi.sk/zz/2020-78/znenie-20200501#p31*
- *Overenie zdrojového kódu s cieľom jeho prepoužitia: https://www.zakonypreludi.sk/zz/2020-85/znenie-20200501#p7-3-c*
- *Spôsoby zverejňovania zdrojového kódu: https://www.zakonypreludi.sk/zz/2020-85/znenie-20200501#p8-9*
- *Inštrukcie k EUPL licenciám: https://joinup.ec.europa.eu/sites/default/files/inline-files/EUPL%201_1%20Guidelines%20SK%20Joinup.pdf*

Požadovať uviesť napr, názov, verziu, typ, počty a metriky potrebných licencií, atď.

ID	***IS/modul/komponent architektúry***	***Nutný SW*** *(stručný popis / názov)*	***Počet***	***Typ licencii***	***Poznámka***
1.	*Doplniť názov:* · *IS* · *Modul* · *Komponent architektúry*	*Doplň názov a stručný popis SW / názov licencie*	*Doplniť počet*	· *Užívateľ* · *CPU* · *systém*	
2.	*Doplniť názov:* · *IS* · *Modul* · *Komponent architektúry*	*Doplň názov a stručný popis SW / názov licencie*	*Doplniť počet*	· *Užívateľ* · *CPU* · *systém*	

*Poznámka: **odporúčame**, aby ste si VŠETKY TABUĽKOVÉ VSTUPY evidovali a spravovali v jednom centrálnom EXCELI – s cieľom minimalizovať budúcu prácnosť s aktualizáciou a udržiavaním obsahu*

3.3.9 Jazyková lokalizácia

Slovenský jazyk / Anglický jazyk

3.4 Bezpečnostná architektúra

- Doplniť popis ASIS stavu
- Načrtnúť návrh TOBE stavu (+ popis alternatív)

Stručne popísať postupy na dosiahnutie potrebnej úrovne bezpečnosti a spôsob zabezpečenia aktív projektu na jednotlivých vrstvách architektúry (dôvernosť, dostupnosť a integrita).

POUŽÍVATELIA SYSTÉMU:

Doplniť požiadavky na používateľské role a správu aplikácie

Interní používatelia (pracovníci ABC – administrácia , správa, podpora)

Externí používatelia (zákaznici, partneri tretie strany)

Bezpečnostná architektúra: Vzhľadom na skutočnosť, že riešenie spracováva aj citlivé dáta, je nutné zabezpečiť riadený a kontrolovaný mechanizmus na prístup k zdrojom riešenia ako aj k samotnému riešeniu.

Prístupy k riešeniu musia byť riadené na princípe RBAC a všetky aktivity používateľa musia byť logované v nezávislom audit logu.

3.5 SUMARIZÁCIA PREPOJENIA, INTEGRÁCIE a ROZHRANIA

DOPLNIŤ VSTUPY v INICIALIZAČNEJ FÁZE:

- *Do tabuľky nižšie uveďte MetaIS kód budovaného/rozvíjaného ISVS z projektu a piktogramom vyznačte, ktoré oblasti referenčnej architektúry bude ISVS využívať (implementované projekty/existujúce ISVS)*

- *Pokiaľ sa prepojenie alebo integrácia týka modulu, vzťah zaznačte pri materskom ISVS*

MetaIS kód ISVS z projektu	**Poskyt. Open data**	**Poskyt. ref. údajov**	**Konz. ref. údajov**	**Modul eSchránky**	**Platobný modul**	**Modul MED**	**Modul CEP**	**Modul MEF**	**GOVNET**
ISVS_404									✓

V požiadavkách na rozhrania, integrácie, importy a exporty, doporučujeme zohľadniť:

IRELEVANTNÉ- nižšie uvedené je irelevantné z dôvodu, že bezpečnostné riešenie nepracuje s dátovými objektmi, nejedná sa o agendový systém, nepracujeme s dátovými objektami.

- ***Vyhlášku úradu podpredsedu vlády SR pre investície a informatizáciu č. 78/2020 Z.z. štandardoch pre informačné technológie verejnej správy:*** *https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2020/78/*
- ***Požiadavky na časť "Otvorených údajov"***

Poskytovanie údajov

Konzumovanie údajov

- ***Požiadavka na časť "Referenčné údaje"***

Poskytovanie údajov

Konzumovanie údajov

- ***Požiadavky pre časť „Spoločné moduly UPVS"***

EXTERNÉ INTERFACES:

Externé businnes interfaces môžu byť kompletne definované vo funkčnej špecifikácii prípadne v externej dokumentácii. Táto sekcia má obsahovať zoznam interaces a názov dokumentácie, kde sú definované. Externé interfaces môžu byť definované nasledovne:

- *Interface typ (fyzický typ, operačný mód, prenosová rýchlosť...)*
- *Krížová referencia na procesné moduly*
- *Spoľahlivosť, bezpečnostné procesy, chybové stavy, recovery*

INTERNÉ INTERFACES:

Zoznam všetkých dát, ktoré sú použité ako interfaces medzi subsystémami. Interfaces väčšinou bývajú definované ako:

- *Procesné typy (dátové štruktúry správ a zdieľané oblasti pamäte)*
- *Procedúrne typy (dátové položky alebo štruktúry zasielané ako parametre)*

Pre každý procesný typ interface uveďte

- *Zoznam subsystémov, kde je použitý*
- *Referenciu na dátovú štruktúru*

Pre každý procedurálny typ uveďte

- *List zdieľaných parametrov, ich prístupové typy, a ich použitie*
- *Prípadnú referenciu na zdieľaný dátový typ*

Doplniť požiadavky na integráciu, napr.

- rozhrania medzi modulmi / komponentmi,
- rozhrania so systémami tretích strán – pokiaľ existujú,
- rozhrania na integrované backendové systémy– pokiaľ existujú,

ID	Požiadavka - Názov rozhrania	Popis rozhrania	Cieľ	Poznámka
1.	*Požiadavka - Doplň názov*	*Doplň popis*	*Doplň cieľ (výstup), ktorý chcete realizáciou rozhrania dosiahnuť*	
2.	*Požiadavka - Doplň názov*	*Doplň popis*	*Doplň cieľ (výstup), ktorý chcete realizáciou rozhrania dosiahnuť*	
3.	*Požiadavka - Doplň názov*	*Doplň popis*	*Doplň cieľ (výstup), ktorý chcete realizáciou rozhrania dosiahnuť*	

*Poznámka: **doporučujeme**, aby ste si VŠETKY TABUĽKOVÉ VSTUPY evidovali a spravovali v jednom centrálnom EXCELI – s cieľom minimalizovať budúcu prácnosť s aktualizáciou a udržiavaním obsahu*

TECHNICKÉ ROZHRANIA RIEŠENIA:

Doplniť blokovú schému riešenia (forma - použitím nástroja napr. ArchiMate v súlade so štandardom TOGAF – rovnako pre biznis procesy, aplikačnú a technologickú architektúru alebo UML diagramy (napr. Deployment Diagram, ...)

OPERAČNÉ / PREVÁDZKOVÉ ROZHRANIA RIEŠENIA:

Tento bod / kapitola bude obsahovať popis rozhraní na iné systémy, ktoré bude potrebné implementovať v projekte. (napr. budú riešené rozhrania na eTRUST a AD?). Pri riešení rozhraní na iné systémy bude popis obsahovať najmä:

- *Zoznam a popis existujúcich (ASIS) rozhraní (ak existujú)*
- *Zoznam a popis navrhovaných (TOBE) rozhraní*
- *Popis funkcionality rozhraní a modelu rozhraní*
- *Popis funkčných modulov rozhraní*
- *Popis procesov rozhraní*
- *Zoznam a popis existujúcich (ASIS) integrácií (ak existujú)*
- *Zoznam a popis navrhovaných (TOBE) integrácií*
- *Popis bezpečnosti (Metodika CSIRT)*
- *Spôsob nasadenia a pravidlá práce vo vývojom prostredí pripájaných systémov*
- *Spôsob nasadenia a pravidlá práce pre testovacie prostredia pripájaných systémov*
- *Ďalšie (doplňte podľa potreby)*

Pokiaľ je relevantné bude doplnené vizuálne (forma - použitím nástroja napr. ArchiMate v súlade so štandardom TOGAF – rovnako pre biznis procesy, aplikačnú a technologickú architektúru) a aj detailne popísaný biznis proces je vytvorený analytikom v interakcii/v komunikácii s koncovým užívateľom.

VÝMENA DÁT:

Doplniť požiadavky na výmenu dát, napr. použitie štandardných konektorov, web-services (webové služby)

Externá integrácia – s riešeniami a službami tretích strán

Mailová komunikácia – notifikácie

Adresárová služba Microsoft ActiveDirectory

SMS-messaging – notifikácie

Údajová základňa (štruktúra dát)

4. ZÁVISLOSTI NA OSTATNÉ IS / PROJEKTY

IRLEVANTNÉ - neevidujeme žiadnu súvislosť na iné IS/projekty

DOPLNIŤ VSTUPY v INICIALIZAČNEJ FÁZE:

- *Sumárny prehľad všetkých projektov a programov, ktoré sú v štádiu vývoja a v korelácii s pripravovaným projektom.*

Stakeholder	**Názov projektu**	**MetaIS kód projektu**	**Termín ukončenia**	**Popis závislosti**
Napr. MIRRI SR	*Projekt XY*	*Projekt_1234*	*04/2021*	*Vyplniť*

V popise závislostí per budovaný/rozvíjaný ISVS zohľadnite:

- *Požiadavky pre časť „Napojenie na API Gateway“ (volanie backendových služieb výlučne cez API Gateway, jednotné pripojenie a interakcia prístupových miest, frontendov cez ISVS prevádzkovateľa NASES)*
- *Požiadavky pre časť „Centrálne komponenty“ (centrálne bloky)*

*Poznámka: **odporúčame**, aby ste si VŠETKY TABUĽKOVÉ VSTUPY evidovali a spravovali v jednom centrálnom EXCELI – s cieľom minimalizovať budúcu prácnosť s aktualizáciou a udržiavaním obsahu.*

5. ZDROJOVÉ KÓDY

IRELEVANTNÉ – kupujeme konkrétny produkt (šnadarditovaný SW dostupny na trhu) bez možnosti uvedenia zdrojových kodov. Nerobíme vývoj SW

- *Doplniť požiadavky na zdrojové kódy (napr. zo vzorovej zmluvy). Aké druhy, formy a štruktúry zdrojových kódov požadujte odovzdať. Stručne popíšte aj spôsob ich preberania, periodicitu (pri akých míľnikoch) a spôsob archivácie.*
- *Doplniť pravidlá pre preberanie, správu a archiváciu zdrojových kódov.*
- *Tieto pravidlá následne preniesť do ZoD/SLA.*
- *Po uzatvorení zmluvy s dodávateľom rieešenia – zohľadniť ich aj v PIDe*
- *Doporučujeme naviazať preberanie/odovzdávanie zdrojových kód na fakturačné mílniky.*

Upozorňujeme: navrhnite spôsob, ako predísť „Vendor lock-in“ = t.j. dodávané riešenie musí byť v súlade so Zákonom o ITVS (ktorý „vendor lock-in“ nepovoľuje). Následne ustanovania predchádzaniu vendor-lockinu musia byť zahrnuté aj v ZoD a SLA.

6. PREVÁDZKA A ÚDRŽBA

- Doplniť popis ASIS stavu
- Načrtnúť návrh TOBE stavu (+ popis alternatív)
- Kompletný prehľad všetkých predpokladaných požiadaviek na prevádzku a údržbu cieľového riešenia
- doplňte Popis budúceho stavu, najmä oblasť Prevádzka
    - pre detailný popis je potrebné využiť **prílohy**
    - Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.
- *Charakterizujte spôsob podpory prevádzky aplikačných a technologických prostriedkov v súčasnom stave, ako aj po ukončení projektu a nasadení výstupov do prevádzky. Popíše sa teda aktuálny stav podpory prevádzky a úroveň poskytovania služieb (SLA), ako aj budúci stav podpory a úroveň poskytovania služieb podľa osobitného predpisu.*

Riešenie sa zvyčajne implementuje ako FailedOpen, t.j. výpadok tohto riešenia nespôsobuje výpadok hlavnej služby. Aj keď je riešenie designované ako FailedOpen, kedže sa jedná o prvok kritickej infraštruktúry tak v čase krízy je nutné zabezpečiť práve, hlavne tieto detekčné mechanizmy.

Navrhované nefunkčné parametre:

RTO ... 4h, t.j. po výpadku do 4h musí byť služba obnovená.

RPO ... 4h t.j. množstvo dát ktoré možno stratiť, keďže sa jedná o štatistické riešnie je možné väčšia strata dát.

Dostupnosť ... 99,95% za rok, t.j. 4h, 22min a 58s neplánovaných výpadkov ročne.

6.1 Prevádzkové požiadavky

- Doporučujeme vložiť popis L1 úrovne – požiadavky / očakávania
- Doporučujeme vložiť popis L2 úrovne – požiadavky / očakávania
- Doporučujeme vložiť popis L3 úrovne – požiadavky / očakávania

Štandardný čas podpory, čas/rýchlosť odstraňovania vád, dostupnosť systému, zálohovanie, plán obnovy systému, atď.

Požadované SLA na služby systémovej a aplikačnej podpory – servisné služby vzťahujúce sa na produkčné a testovacie prostredie IS

Rozsah zálohovania	vybrané údaje
Doba zotavenia (RTO)	4 hodiny
Je záloha pravidelne validovaná	N/A, Áno, Nie
Miera dostupnosti	99.95%

6.1.1 Úrovne podpory používateľov:

Help Desk bude realizovaný cez 3 úrovne podpory, s nasledujúcim označením:

- ***L1 podpory IS*** *(Level 1, priamy kontakt zákazníka) - jednotný kontaktný bod verejného obstarávateľa – IS Solution manager, ktorý je v správe verejného obstarávateľa a v prípade jeho nedostupnosti Centrum podpory používateľov (zabezpečuje prevádzkovateľ IS a DataCentrum).*

- ***L2 podpory IS*** *(Level 2, postúpenie požiadaviek od L1) - vybraná skupina garantov, so znalosťou IS (zabezpečuje prevádzkovateľ IS – verejný obstarávateľ).*

- ***L3 podpory IS*** *(Level 3, postúpenie požiadaviek od L2) - na základe zmluvy o podpore IS (zabezpečuje úspešný uchádzač).*

Definícia:

-

- ***Podpora L1 (podpora 1. stupňa)*** *- začiatočná úroveň podpory, ktorá je zodpovedná za riešenie základných problémov a požiadaviek koncových užívateľov a ďalšie služby vyžadujúce základnú úroveň technickej podpory. Základnou funkciou podpory 1. stupňa je zhromaždiť informácie, previesť základnú analýzu a určiť príčinu problému a jeho klasifikáciu. Typicky sú v úrovni L1 riešené priamočiare a jednoduché problémy a základné diagnostiky, overenie dostupnosti jednotlivých vrstiev infraštruktúry (sieťové, operačné, vizualizačné, aplikačné atď.) a základné užívateľské problémy (typicky zabudnutie hesla), overovanie nastavení SW a HW atď.*

- ***Podpora L2 (podpora 2. stupňa)*** *– riešiteľské tímy s hlbšou technologickou znalosťou danej oblasti. Riešitelia na úrovni Podpory L2 nekomunikujú priamo s koncovým užívateľom, ale sú zodpovední za poskytovanie súčinnosti riešiteľom 1. úrovne podpory pri riešení eskalovaného hlásenia, čo mimo iného obsahuje aj spätnú kontrolu a podrobnejšiu analýzu zistených dát predaných riešiteľom 1. úrovne podpory. Výstupom takejto kontroly môže byť potvrdenie, upresnenie, alebo prehodnotenie hlásenia v závislosti na potrebách Objednávateľa. Primárnym cieľom riešiteľov na úrovni Podpory L2 je dostať Hlásenie čo najskôr pod kontrolu a následne ho vyriešiť - s možnosťou eskalácie na vyššiu úroveň podpory – Podpora L3.*

- ***Podpora L3 (podpora 3. stupňa)*** *- Podpora 3. stupňa predstavuje najvyššiu úroveň podpory pre riešenie tých najobťiažnejších Hlásení, vrátane prevádzania hĺbkových analýz a riešenie extrémnych prípadov.*

Pre služby sú definované takéto SLA:

Help Desk je dostupný cez IS Solution manager a pre vybrané skupiny užívateľov cez telefón a email, incidenty sú evidované v IS Solution manager,

Dostupnosť L3 podpory pre IS je 12x5 (12 hodín x 5 dní od 8:00h do 16:00h počas pracovných dní),

Riešenie incidentov – SLA parametre

Za incident je považovaná chyba IS, t.j. správanie sa v rozpore s prevádzkovou a používateľskou dokumentáciou IS. Za incident nie je považovaná chyba, ktorá nastala mimo prostredia IS napr. výpadok poskytovania konkrétnej služby Vládneho cloudu alebo komunikačnej infraštruktúry.

- *Označenie naliehavosti incidentu:*

Označenie naliehavosti incidentu	***Závažnosť incidentu***	***Popis naliehavosti incidentu***
A	***Kritická***	*Kritické chyby, ktoré spôsobia úplné zlyhanie systému ako celku a nie je možné používať ani jednu jeho časť, nie je možné poskytnúť požadovaný výstup z IS.*
B	***Vysoká***	*Chyby a nedostatky, ktoré zapríčinia čiastočné zlyhanie systému a neumožňuje používať časť systému.*
C	***Stredná***	*Chyby a nedostatky, ktoré spôsobia čiastočné obmedzenia používania systému.*
D	***Nízka***	*Kozmetické a drobné chyby.*

možný dopad:

Označenie závažnosti incidentu	***Dopad***	***Popis dopadu***
1	***katastrofický***	*katastrofický dopad, priamy finančný dopad alebo strata dát,*
2	***značný***	*značný dopad alebo strata dát*
3	***malý***	*malý dopad alebo strata dát*

- *Výpočet priority incidentu je kombináciou dopadu a naliehavosti v súlade s best practices ITIL V3 uvedený v nasledovnej matici:*

Matica priority incidentov		***Dopad***		
		Katastrofický - 1	***Značný - 2***	***Malý - 3***
Naliehavosť	***Kritická - A***	*1*	*2*	*3*
	Vysoká - B	*2*	*3*	*3*
	Stredná - C	*2*	*3*	*4*
	Nízka - D	*3*	*4*	*4*

Vyžadované reakčné doby:

Označenie priority incidentu	***Reakčná doba(1) od nahlásenia incidentu po začiatok riešenia incidentu***	***Doba konečného vyriešenia incidentu od nahlásenia incidentu (DKVI) (2)***	***Spoľahlivosť' (3)*** *(počet incidentov za mesiac)*
1	*0,5 hod.*	*4 hodín*	*1*
2	*1 hod.*	*12 hodín*	*2*
3	*1 hod.*	*24 hodín*	*10*
4	*1 hod.*	*Vyriešené a nasadené v rámci plánovaných releasov*	

- *(1) Reakčná doba je čas medzi nahlásením incidentu verejným obstarávateľom (vrátane užívateľov IS, ktorí nie sú v pracovnoprávnom vzťahu s verejným obstarávateľom) na helpdesk úrovne L3 a jeho prevzatím na riešenie.*

- *(2) DKVI znamená obnovenie štandardnej prevádzky - čas medzi nahlásením incidentu verejným obstarávateľom a vyriešením incidentu úspešným uchádzačom (do doby, kedy je funkčnosť prostredia znovu obnovená v plnom rozsahu). Doba konečného vyriešenia incidentu od nahlásenia incidentu verejným obstarávateľom (DKVI) sa počíta počas*

celého dňa. Do tejto doby sa nezarátava čas potrebný na nevyhnutnú súčinnosť verejného obstarávateľa, ak je potrebná pre vyriešenie incidentu. V prípade potreby je úspešný uchádzač oprávnený požadovať od verejného obstarávateľa schválenie riešenia incidentu.

- *(3) Maximálny počet incidentov za kalendárny mesiac. Každá ďalšia chyba nad stanovený limit spoľahlivosti sa počíta ako začatý deň omeškania bez odstránenia vady alebo incidentu. Duplicitné alebo technicky súvisiace incidenty (zadané v rámci jedného pracovného dňa, počas pracovného času 8 hodín) sú považované ako jeden incident.*

- *(4) Incidenty nahlásené verejným obstarávateľom úspešnému uchádzačovi v rámci testovacieho prostredia*

1. *Majú prioritu 3 a nižšiu*
2. *Vzťahujú sa výhradne k dostupnosti testovacieho prostredia*
3. *Za incident na testovacom prostredí sa nepovažuje incident vztiahnutý k práve testovanej funkcionalite*

Vyššie uvedené SLA parametre nebudú použité pre nasledovné služby:

- *Služby systémovej podpory na požiadanie (nad paušál)*
- *Služby realizácie aplikačných zmien vyplývajúcich z legislatívnych a metodických zmien (nad paušál)*

Pre tieto služby budú dohodnuté osobitné parametre dodávky.

6.2 Požadovaná dostupnosť IS:

Popis	**Parameter**	**Poznámka**
Prevádzkové hodiny	24 hodín	
Servisné okno	4 hodiny	od 22:00 hod. - do 2:00 hod. utorok alebo štvrtok

Dostupnosť produkčného prostredia IS	99,95	· 98,5% z 24/7/365 t.j. max ročný výpadok je 66 hod. · Maximálny mesačný výpadok je 5,5 hodiny. · Vždy sa za takúto dobu považuje čas od 0.00 hod. do 23.59 hod. poča · Nedostupnosť IS sa počíta od nahlásenia incidentu Zákazníkom v čas na L3 v čase od 6:00 hod. - do 18:00 hod. počas pracovných dní). Do dost odstávky IS. · V prípade nedodržania dostupnosti IS bude každý ďalší začatý pracov odstránenia vady alebo incidentu.

TEXT pre inšpiráciu – vyberte si pre vás potrebné:

6.2.1 Dostupnosť (Availability)

Čo je Dostupnosť (Availability)

Dostupnosť (Availability) znamená, že dáta alebo iné zariadenie sú prístupné v okamihu jej potreby. Vyjadruje sa v percentách dostupného času.

***Dostupnosť* (Availability)** *je pojem z oblasti riadenia bezpečnosti v organizácii. Dostupnosť znamená, že dáta sú prístupné v okamihu jej potreby. Narušenie dostupnosti sa označuje ako nežiaduce zničenie (destruction) alebo nedostupnosť. Dostupnosť je zvyčajne vyjadrená ako percento času v danom období, obvykle za rok. Orientačný zoznam dostupnosti je uvedený v tabuľke:*

- ***90% dostupnosť*** *znamená výpadok 36,5 dňa*
- ***95% dostupnosť*** *znamená výpadok 18,25 dňa*
- ***98% dostupnosť*** *znamená výpadok 7,30 dňa*
- ***99% dostupnosť*** *znamená výpadok 3,65 dňa*
- ***99,5% dostupnosť*** *znamená výpadok 1,83 dňa*
- ***99,8% dostupnosť*** *znamená výpadok 17,52 hodín*
- ***99,9%*** *(“**tri deviatky**”)* ***dostupnosť*** *znamená výpadok 8,76 hodín*
- ***99,99%*** *(“**štyri deviatky**”)* ***dostupnosť*** *znamená výpadok 52,6 minút*
- ***99,999%*** *(“**päť deviatok**”)* ***dostupnosť*** *znamená výpadok 5,26 minút*
- ***99,9999%*** *(“**šesť deviatok**”)* ***dostupnosť*** *znamená výpadok 31,5 sekúnd*

Hoci je obvyklé uvádzať dostupnosť v percentách, presnejšie ukazovatele sú vyjadrením doby obnovenia systému a na množstvo dát, o ktoré môžeme prísť:

- *RTO (Recovery Time Objective) - doba obnovenia systému, t.j. za ako dlho po výpadku musí byť systém funkčný (pre bližšie info klik na nadpis)*
- *RPO (Recovery Point Objective) - aké množstvo dát môže byť stratené od vymedzeného okamihu*
- *Recovery Time - čas potrebný k obnove*

***Riešenie dostupnosti v praxi**: Nedostupnosť dát je jedným z rizík, ktorý môže postihnúť každú organizáciu. Dostupnosť je jedným s kľúčových požiadaviek na každý dôležitý informačný systém a vplyv na dostupnosť má mnoho faktorov, napríklad:*

- *Dostupnosť servera*
- *Dostupnosť pripojenie k internetu*
- *Dostupnosť databázy*
- *Dostupnosť webových stránok*

V prípade, že je časť softvér alebo infraštruktúra zabezpečovaná externe (napr. hosting, webhosting), prenáša sa zodpovednosť za dostupnosť týchto komponentov na dodávateľa. Potom je potrebné mať vhodným spôsobom ošetrenú úroveň dostupnosti, ktorú musí dodávateľ dodržať. Zvyčajne je dostupnosť súčasťou dohody o úrovni poskytovaných služieb (SLA).

Miera dostupnosti	99.95%

6.2.2 RTO (Recovery Time Objective)

RTO (Recovery Time Objective) je jeden z ukazovateľov dostupnosti dát. RTO vyjadruje množstvo času potrebné pre obnovenie dát a celého prevádzky nedostupného systému (softvér).

Recovery Time Objective *(zvyčajne sa požíva skratka RTO) je jeden z ukazovateľov dostupnosti dát. RTO vyjadruje množstvo času potrebné pre obnovenie dát a celej prevádzky nedostupného systému (softvér). Môže byť, v závislosti na použitej technológii, vyjadrené v sekundách, hodinách či dňoch.*

Využitie RTO v praxi*: Ukazovateľ RTO sa z pohľadu zákazníka využíva pre vyjadrenie doby pre obnovu dát. (napr. formou SLA). Na druhú stranu poskytovatelia dnes môžu voliť rôzne technológie zálohovanie, respektíve replikovanie dát a dobu obnovy dát znížiť až k nulovému výpadku. Existujúce technológie sa delia zhruba nasledovne:*

- *Tradičné zálohovanie - výpadok a obnova trvá cca hodiny až dni*
- *Asynchrónne replikácie dát - výpadok a obnova v poriadku sekúnd až minút*
- *Synchrónny replikácie dát - nulový výpadok*

Doba zotavenia (RTO)	4 hodiny

6.2.3 RPO (Recovery Point Objective)

RPO (Recovery Point Objective) je jeden z ukazovateľov dostupnosti dát. RPO vyjadruje, do akého stavu (bodu) v minulosti možno obnoviť dáta.

Recovery Point Objective *(zvyčajne sa požíva skratka RPO) je jeden z ukazovateľov dostupnosti dát. RPO vyjadruje, do akého stavu (bodu) v minulosti možno obnoviť dáta. Inými slovami množstvo dát, o ktoré môže organizácia prísť.*

Využitie RPO v praxi*: Ukazovateľ RPO sa z pohľadu zákazníka využíva pre vyjadrenie množstva obnoviteľných dát. (napr. formou SLA). Na druhú stranu poskytovatelia dnes môžu voliť rôzne technológie zálohovanie, respektíve replikovanie dát a bod obnovy dát znížiť až k nulovej strate. Existujúce technológie sa delia zhruba nasledovne:*

- *Tradičné zálohovanie - výpadok a obnova trvá cca hodiny až dni*
- *Asynchrónne replikácie dát - výpadok a obnova v poriadku sekúnd až minút, strata sa blíži k nule*
- *Synchrónny replikácie dát - nulová strata*

Maximálna strata dát (RPO)	4 hodiny

7. POŽIADAVKY NA PERSONÁL

- Doplniť požiadavky na projektové personálne zabezpečenie (projektové role a ich obsadenie)
- Doplniť rámcové požiadavky na obsadenie TOBE procesu
- Doplniť požiadavky potrebných školení a certifikátov

ID	Meno a Priezvisko	Pozícia	Oddelenie	Rola v projekte
1.	Michal Seliga	Projektový manažér za objednávateľa	NASES	
2.	Sekcia bezpečnosti	Kľúčový používateľ (end user)	NASES	
3.	Sekcia bezpečnosti	Špecialista na bezpečnosť	NASES	
4.	Sekcia bezpečnosti	Tester	NASES	
5.	Sekcia bezpečnosti	Analytik	NASES	
6.	Peter Žovák	IT Architekt	NASES	
7.	Sekcia bezpečnosti	Odborník pre IT Senior - Školiteľ IT	NASES	
8.	Sekcia bezpečnosti	Manažér kvality	NASES	
9.	Miloš Havrilla	Finančný manažér	NASES	
10.	SKIT	IT analytik	SKIT	
11.	SKIT	Špecialista pre bezpečnosť IT	SKIT	

12.	SKIT	Projektový manažér IT projektu	SKIT	
13.	SKIT	Špecialista pre infraštruktúrny/HW špecialista	SKIT	
14.	SKIT	IT architekt	SKIT	
15.	SKIT	IT programátor/vývojár	SKIT	
16.	SKIT	IT Tester	SKIT	

Mená pre projektové pozície budú doplnené po schválení projektového zámeru.

8. IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU

- Posúdenie spôsobov nasadzovania jednotlivých prístupov v praxi

V zmysle Vyhlášky 85/20202 Zz o projektovom riadení je potrebné posúdiť spôsob realizácie projektu metódou waterfall, agile alebo ich kombináciou.

V zmysle vyhlášky 85/2020 Zz o projektovom riadení je možné pristupovať k realizácii projektu prostredníctvom čiastkových plnení, t.j. inkrementov, a to:

- *Inkrement musí obsahovať z realizačnej fázy projektu aspoň etapu Implementácia a Testovanie a Nasadenia do produkcie; je možné ho realizovať viacerými iteráciami v závislosti od charakteru projektu a každý doručený inkrement projektu je nasadený na produkčnom prostredí informačnej technológie a je možné začať s dokončovacou fázou projektu, alebo pokračovať ďalším inkrementom*
- *Ak realizačná fáza veľkých projektov pozostáva z dodania jedného funkčného celku alebo dodania výlučne technických prostriedkov, objednávateľ v produkte P-03 Prístup k projektu - rámcový a I-03 Prístup k projektu - detailný s prílohou 1: Technická špecifikácia – rámcová, posúdi a vyhodnotí aj alternatívy rozdelenia na inkrementy na preukázanie ekonomickej nevýhodnosti alebo technických obmedzení rozdeliť projekt na inkrementy.*

*Poznámka: **odporúčame**, aby ste si VŠETKY TABUĽKOVÉ VSTUPY evidovali a spravovali v jednom centrálnom EXCELI – s cieľom minimalizovať budúcu prácnosť s aktualizáciou a udržiavaním obsahu.*

Riadiaci výbor sa zriaďuje ako najvyšší riadiaci orgán na účely realizácie Projektu „Detekcia zraniteľnosti koncových obslužných bodov“. Riadiaci výbor bude zostavený v nasledujúcom zložení:

Predseda RV	Pavel Karel	N
Podpredseda RV	Martin Sulík	N
zástupca vlastníkov procesov objednávateľa (biznis vlastník)	Pavel Karel	N
zástupca za MIRRI		M

Projektový tím pre projekt sa bude skladať s nasledujúcich zúčastnených strán:

1. NASES ako objednávateľ, vlastník a prevádzkovateľ riešenia modulu detekcie hrozieb
2. MIRRI

Metóda riadenia projektu:

Projekt bude realizovaný agilnými metóda s prihliadnutím na strategické priority podľa NKIVS. Projekt má udaný jasný cieľ a výstupy, ktoré budú priebežne konzultované s vlastníkom projektu.

Realizácia projektu je naplánovaná na 9 mesiacov. Nasledujúci harmonogram zobrazuje realizáciu projektu podľa jeho jednotlivých fáz:

ID	**FÁZA/AKTIVITA**	**ZAČIATOK (odhad termínu)**	**KONIEC (odhad termínu)**	**PO**
1.	Prípravná fáza	12/2020	02/2021	
2.	Iniciačná fáza	03/2021	04/2021	
3.	Realizačná fáza	06/2021	06/2022	
3a	Analýza a Dizajn	06/2021	07/2021	1 m
3b	Nákup technických prostriedkov, programových prostriedkov a služieb	06/2021	09/2021	3 m
3c	Implementácia a testovanie	09/2021	12/2021	3 m
3d	Nasadenie	01/2022	06/2022	5 m

4.	Dokončovacia fáza	07/2022	10/2022	3 m
5.	Podpora prevádzky (SLA)	napr. 01/2021	napr. 01/2025	N/A

9. PRÍLOHY

Príloha 1: Katalóg požiadaviek *(Excel) -* *https://www.mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/riadenie-kvality-qa/index.html*

Koniec dokumentu