

# PROJEKTOVÝ ZÁMER

## Vzor pre manažérsky výstup I-02 podľa vyhlášky MIRRI č. 401/2023 Z. z.

<b>Povinná osoba</b>	Regionálny úrad verejného zdravotníctva so sídlom v Dolnom Kubíne
<b>Názov projektu</b>	Podpora v oblasti kybernetickej a informačnej bezpečnosti RÚVZ
<b>Zodpovedná osoba za projekt</b>	Ing. Jana Grňo Mikulášiová, manažér kybernetickej bezpečnosti
<b>Realizátor projektu</b>	Úrad verejného zdravotníctva SR
<b>Vlastník projektu</b>	Ing. Jana Grňo Mikulášiová, manažér kybernetickej bezpečnosti

### Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Vypracoval		RÚVZ Dolný Kubín			

## 1. HISTÓRIA DOKUMENTU

Verzia	Dátum	Zmeny	Meno
1.0.	01.07.2024	Vypracovanie dokumentu	
1.0	22.12.2023	Zapracovanie súladu s vyhláškou č. 401/2023 Z. z.	

## 2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

V súlade s Vyhláškou 401/2023 Z.z. je dokument I-02 Projektový zámer určený na rozpracovanie detailných informácií prípravy projektu, aby bolo možné rozhodnúť o pokračovaní prípravy projektu, pláne realizácie, alokovaní rozpočtu a ľudských zdrojov.

V súlade s Vyhláškou MIRRI SR č. 401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke IT VS je dokument 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. Dodávané riešenie bude v súlade so zákonom. Zároveň opisuje aj implementáciu projektu a preberanie výstupov projektu.

Hlavnou motiváciou je realizácia kyberbezpečnostných opatrení definovaných v Z.z. 69/2018 a v zákone o ISVS.

Prioritne jedná o tie opatrenia, ktoré vykazujú najväčší nesúlad s uvedenými právnymi normami a vyhláškou 362/2018 Z. z.. V dôsledku realizácie týchto opatrení budú ÚVZ SR chránené v maximálnej možnej miere pred kybernetickým incidentom, ktorý by mohol mať na poskytovanie služieb a prevádzku ÚVZ SR.

Medzi základné povinnosti je prijatie a dodržiavanie všeobecných bezpečnostných opatrení pre nasledovné oblasti, ktoré sú obsahom projektu:

1. Prehodnotení SM-03 Bezpečnostná politika a stratégia Úradu verejného zdravotníctva s ohľadom na požiadavky nového zákona o KB a príslušných vykonávacích predpisov,
2. Dopracovanú smernicu pre oblasti riadenia bezpečnosti prevádzky sietí a IS/APP,
3. Aktualizovanú SM-25 Smernica, ktorou sa upravuje práca s informačnými technológiami,
4. Nasadený nástroj na automatizáciu analýzy rizík a prehodnotenie a aktualizácia analýzy rizík podľa požiadaviek nového zákona o KB,
5. Spracovávanie inventarizácie aktív a ich klasifikáciu s ohľadom na IS ÚVZ a dokumentovanie vzťahov a závislostí medzi IS ÚVZ a ostatnými používanými systémami a aplikáciami na ÚVZ SR,

6. Prehodnotenú a spracovanú novú SOA (Security Operations Architecture) s ohľadom na novú legislatívu a jej plnenie pre oblasť kybernetickej bezpečnosti,
7. Zavedenú kontrolu dodržiavania bezpečnostných politík zo strany zamestnancov, administrátorov a osôb zastávajúcich niektorú z bezpečnostných rolí,
8. Implementovaný nástroj na detekciu kybernetických bezpečnostných incidentov, ktorý spĺňa všetky požiadavky Vyhlášky § 17, ods. 03 a ods. 04,
9. Navrhnutý a zdokumentovaný efektívny spôsob kontroly pre účely zaručenia, že prevádzka, používanie a manažment siete a informačného systému je v súlade s vnútornými predpismi a zmluvnými záväzkami,
10. Prehodnotenú a aktualizovanú smernicu v oblasti SM-51 Smernica Riadenie kontinuity procesov a činností a spracované nové BCP/DRP plány potrebné na zabezpečenie kontinuity činností podľa nového zákona o KB,
11. Aktualizovaná SM-44 Smernica o klasifikácii informácií na Úrade verejného zdravotníctva Slovenskej republiky,
12. Zanalyzované existujúce prostredie ÚVZ SR s ohľadom na vzniknutý systém IS ÚVZ a vytvorené záznamy o identifikovaných vzťahoch a súvislostiach,
13. Zanalyzovaný spôsob efektívnej realizácie monitoringu zariadení, činností, sietí, IS a APP v prostredí ÚVZ SR a zabezpečenú podporu pre vybrané riešenie pri jeho nasadení a spustení do prevádzky.

Cieľom projektu je, aby po jeho realizácii naša inštitúcia dosiahla čo možno najväčší súlad s NIS2, Zákomom o kyberbezpečnosti, ako aj Zákomom o ISVS.

## 2.1 Použité skratky a pojmy

SKRATKA/POJEM	POPIS
KIB	Kybernetická a informačná bezpečnosť
IT	Informačné technológie
VS	Verejná správa
ITVS	Informačné technológie verejnej správy
NFP	Nenávratný finančný príspevok
OP SK	Operačný program SLOvensko
ÚVZ SR	Úrad verejného zdravotníctva SR
RÚVZ	Regionálny úrad verejného zdravotníctva
MZ SR	Ministerstvo zdravotníctva SR
NKIVS	Národná koncepcia informatizácie verejnej správy
ZoBK	Zákon o kybernetickej bezpečnosti
SOA	Security Operations Architecture
SOC	Security Operation Center

## 2.2 Konvencie pre typy požiadaviek (príklady)

Zvoľte si konvenciu pre označovanie požiadaviek, súborov, atď. Hlavné kategórie požiadaviek v zmysle katalógu požiadaviek, rozdeľujeme na funkčné (funkcionálne), nefunkčné (kvalitatívne, výkonové a pod.). Podskupiny v hlavných kategóriách je možné rozšíriť podľa potrieb projektu, napríklad:

**Funkcionálne (používateľské) požiadavky** majú nasledovnú konvenciu:

**FRxx**

- U – užívateľská požiadavka
- R – označenie požiadavky
- xx – číslo požiadavky

**Nefunkčné (kvalitatívne, výkonové - Non Functional Requirements - NFR) požiadavky** majú nasledovnú konvenciu:

**NRxx**

- N – nefunkčná požiadavka (NFR)
- R – označenie požiadavky
- xx – číslo požiadavky

Ostatné typy požiadaviek môžu byť ďalej definované objednávateľom/PM.

### 3. DEFINOVANIE PROJEKTU

#### 3.1 Manažérske zhrnutie

Úrad verejného zdravotníctva SR ako prevádzkovateľ základnej služby zapísanej v registri prevádzkovateľov základných služieb má povinnosti, ktoré vyplývajú zo ZoKB. Medzi základné povinnosti je prijatie a dodržiavanie všeobecných bezpečnostných opatrení pre nasledovné oblasti:

1. Prehodnotenú SM-03 Bezpečnostná politika a stratégia Úradu verejného zdravotníctva s ohľadom na požiadavky nového zákona o KB a príslušných vykonávacích predpisov,
2. Dopracovanú smernicu pre oblasti riadenia bezpečnosti prevádzky sietí a IS/APP,
3. Aktualizovanú SM-25 Smernica, ktorou sa upravuje práca s informačnými technológiami,
4. Nasadený nástroj na automatizáciu analýzy rizík a prehodnotenie a aktualizácia analýzy rizík podľa požiadaviek nového zákona o KB,
5. Spracovávanie inventarizácie aktív a ich klasifikáciu s ohľadom na IS ÚVZ a dokumentovanie vzťahov a závislostí medzi IS ÚVZ a ostatnými používanými systémami a aplikáciami na ÚVZ SR,
6. Prehodnotenú a spracovanú novú SOA (Security Operations Architecture) s ohľadom na novú legislatívu a jej plnenie pre oblasť kybernetickej bezpečnosti,
7. Zavedenú kontrolu dodržiavania bezpečnostných politík zo strany zamestnancov, administrátorov a osôb zastávajúcich niektorú z bezpečnostných rolí,
8. Implementovaný nástroj na detekciu kybernetických bezpečnostných incidentov, ktorý spĺňa všetky požiadavky Vyhlášky § 17, ods. 03 a ods. 04,
9. Navrhnutý a zdokumentovaný efektívny spôsob kontroly pre účely zaručenia, že prevádzka, používanie a manažment siete a informačného systému je v súlade s vnútornými predpismi a zmluvnými záväzkami,
10. Prehodnotenú a aktualizovanú smernicu v oblasti SM-51 Smernica Riadenie kontinuity procesov a činností a spracované nové BCP/DRP plány potrebné na zabezpečenie kontinuity činností podľa nového zákona o KB,
11. Aktualizovaná SM-44 Smernica o klasifikácii informácií na Úrade verejného zdravotníctva Slovenskej republiky,
12. Zanalyzované existujúce prostredie ÚVZ SR s ohľadom na vzniknutý systém IS ÚVZ a vytvorené záznamy o identifikovaných vzťahoch a súvislostiach,
13. Zanalyzovaný spôsob efektívnej realizácie monitoringu zariadení, činností, sietí, IS a APP v prostredí ÚVZ SR a zabezpečenú podporu pre vybrané riešenie pri jeho nasadení a spustení do prevádzky

**Jednotlivé organizačné jednotky (OZ), teda regionálne úrady verejného zdravotníctva (ktorých je 36) využívajú centrálny informačný systém (IS ÚVZ), tzn. že každá OZ, ak sa stane terčom kybernetického útoku, ohrozuje fungovanie IS ÚVZ ako celku a môže spôsobiť odstavenie celého systému. V dôsledku toho je nevyhnutné, aby navrhovaným systémom disponovalo nie len ÚVZ, ale aj všetky RÚVZ.**

Zasielané udalosti sú v jednotlivých organizáciách na vstupe prijaté, označované a parsované podľa technológie. Následne sú buď vhodnými základnými pravidlami produktu a implementačnými pravidlami na mieru spracované, aby bolo možné s nimi vytvárať potrebné navrhnuté scenáre. Ďalej sú uložené a vizualizované buď prostredníctvom základných nástrojov, alebo v budúcnosti vyššou formou pomocou integračnej platformy. Implementácia zahŕňa vytvorenie prístupových oprávnení v súlade s požiadavkami na viditeľnosť a spracovanie dát a následnú vizualizáciu.

Prevádzkové informácie budú zobrazovať aktuálne informácie o stave logovaných ICT systémov jednotlivých organizácií. Nad týmito logmi bude vykonané parsovanie a následne sa uložia do centrálného dátového skladu, kde bude možné s týmito dátami ďalej pracovať. Primárne sa jedná o nepretržitý zber logov a monitorovanie prevádzky ICT technológií, systémov, aplikácií, stavu kybernetického a fyzického zabezpečenia a poskytovanie dát a informácií pre riešenie odchýlok a nápravných opatrení. Všetky údaje uložené v dátovom sklade budú podrobené procesu sledovania a vyhodnocovania podľa nižšie uvedených scenárov. Tým bude zabezpečené sledovanie jednotlivých systémov podľa nariadenia NIS2. Jednotlivé zistenia budú automaticky evidované v systéme na riadenie bezpečnosti, ktorý riadi všetky zistené riziká a navrhuje vhodné opatrenia. Takto evidované a riadené sledovanie logov povedie k včasnej detekcii rizík a ich okamžitej náprave.

Z pohľadu kompletného zberu logov bude vyhodnocované:

- prihlasovanie a odhlasovanie ku všetkým účtom, vrátane neúspešných pokusov

- vykonanie a neúspešný pokus o vykonanie privilegovanej činnosti
- manipulácia a neúspešný pokus o manipuláciu s účtami, oprávneniami a právami
- neuskutočnenie činností v dôsledku nedostatku prístupových práv alebo oprávnení
- začatie a ukončenie činností technických aktív
- kritické a chybové hlásenia technických aktív
- prístup a neúspešný pokus o prístup k záznamom udalostí
- manipulácia a neúspešný pokus o manipuláciu so záznamami udalostí
- zmenu a neúspešný pokus o zmenu nastavení nástrojov na zaznamenávanie udalostí
- ďalšie činnosti používateľov, ktoré môžu mať vplyv na bezpečnosť regulovanej služby.

### **Výsledky projektu a cieľový stav (manažérske produkty)**

#### **Čiastková aktivita a) Organizácia KB,**

Na základe zistených nedostatkov v oblasti riadenia kybernetickej a informačnej bezpečnosti v organizácii sa určuje nasledovný cieľový stav:

Komplexná bezpečnostná dokumentácia bude novo vypracovaná, pričom zohľadňuje predchádzajúcu dokumentáciu a jej aktualizácie vrátane rozsahu a metód dodržiavania všeobecných bezpečnostných opatrení.

Budú novo sa vyvinuté a implementované špecifické interné riadiace akty pre vybrané oblasti kybernetickej a informačnej bezpečnosti.

Bude aktualizovaný stav bezpečnostného výboru organizácie.

Bude vypracovaný bezpečnostný projekt komplexnej ochrany informačného systému verejnej správy.

#### **Čiastková činnosť b) Riadenie rizík KB,**

Na základe zistených nedostatkov v oblasti riadenia rizík kybernetickej a informačnej bezpečnosti v organizácii sa určuje nasledovný cieľový stav:

Všetky aktíva súvisiace so spracovaním informácií a centrálnym inventárnym záznamovým zariadením budú identifikované ich hodnotou a s označením ich vlastníka, ktorý definuje ich požiadavky na dôvernosť, dostupnosť a integritu (EAM).

Riadenie rizík bude automatizované pomocou nástroja, pozostávajúce z identifikácie zraniteľnosti, identifikácie hrozieb, identifikácie rizík a analýzy rizík s ohľadom na aktíva, určenia vlastníka rizika a implementácie organizačných a technických bezpečnostných opatrení, funkčnej analýzy dopadov a pravidelného prehodnocovania identifikovaných rizík v závislosti od aktualizácie prijatých bezpečnostných opatrení.

Bude implementovaný automatizovaný systém správy a registrácie pre inventarizáciu majetku (EAM/).

Bude implementovaný automatizovaný systém riadenia a registrácie pre katalogizáciu hrozieb.

Bude zavedený sa automatizovaný systém riadenia a registrácie pre katalogizáciu rizík a opatrení.

#### **Čiastková činnosť c) Personálna bezpečnosť,**

Na základe zistených nedostatkov v oblasti personálnej bezpečnosti v organizácii je stanovený nasledovný cieľový stav:

Bude vyvinutý postup na priradenie osoby k jednej z rolí zabezpečenia

Bude zavedený plán na rozvoj bezpečnostného povedomia a vzdelávania

Bude vyvinutá metóda hodnotenia účinnosti rozvojového plánu bezpečnostného povedomia

Budú určené pravidlá a postupy pri riešení porušení bezpečnostnej politiky

Budú zavedené postupy na ukončenie pracovného pomeru

Budú zavedené postupy pre prípady porušenia bezpečnostných politík

Bude vypracovaný a aktualizovaný akt vnútorného riadenia s bezpečnostnými zásadami pre koncových používateľov

Postupy a procesy, ktorými sa riadi personálna bezpečnosť organizácie, budú vypracované a implementované prostredníctvom interného riadiaceho aktu.

Bude vyhotovený automatizovaný systém riadenia a evidencie pre prácu s organizačnou štruktúrou je implementovaný s prepojením na technické získavanie existujúcich informácií z dostupných technických zdrojov – najmä MS AD.

#### **Čiastková aktivita k) Zaznamenávanie udalostí a monitoring sietí a IS,**

Na základe zistených nedostatkov v oblasti zaznamenávania a monitorovania udalostí je stanovený nasledovný cieľový stav:

Implementovaný bude centrálny log management systém pre zber a ukladanie logov z jednotlivých informačných systémov s podporou napojenia na riadiace systémy a poskytovania potrebných podporných dát.

Bude vypracovaná dokumentácia metód monitorovania a fungovania systému správy log a centrálného nástroja na monitorovanie bezpečnosti a bude definovaný spôsob evidencie prevádzkových záznamov, ich vyhodnocovanie, spôsoby hlásenia podozrivej činnosti, zodpovedné osoby a ďalšie povinnosti.

Vytvorí sa špecifikácia všetkých udalostí, ktoré sa musia zaznamenávať, a súvisiaca konfigurácia prvkov informačných technológií verejnej správy vrátane dokumentácie rozsahu údajov zaznamenaných v protokolových súboroch.

Bude vypracovaný vnútorný zákon o riadení, ktorý obsahuje a upravuje povinnosti stanovené platnou legislatívou.

### 3.2 Ciele projektu

Do tabuliek nižšie doplniť CIEĽ /CIEĽE PROJEKTU, ich mapovanie na strategické ciele (napr. z NKIVS, KRIT a iných strategických dokumentov) a súvisiace merateľné ukazovatele (KPI- key performance indicators). Ciele musia byť S.M.A.R.T. - konkrétne, merateľné, dosiahnuteľné, relevantné, časovo ohraničené.

ID	Názov cieľa	Názov strategického cieľa	Spôsob realizácie strategického cieľa
...		...	...
...		...	...

### 3.3 Merateľné ukazovatele (KPI)

ID	ID/Názov cieľa	Názov ukazovateľa (KPI)	Popis ukazovateľa	Merná jednotka	AS IS merateľné hodnoty (aktuálne)	TO BE Merateľné hodnoty (cieľové hodnoty)	Spôsob ich merania	Pozn.
...		...	...	...	...	...	...	...
...		...	...	...	...	...	...	...
...		...	...	...	...	...	...	...

Vysvetlivky k vyplneniu tabuľky:

- Vzory merateľných ukazovateľov pre projekt sú publikované v Checkliste pre agendu Merateľné ukazovatele/KPI (<https://www.mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-ga/riadenie-kvality-ga/index.html> )
- **AS IS merateľné ukazovatele** – t. j. popíšte, aké merateľné ukazovatele máte teraz (vpište výsledky meraní – v merateľných jednotkách) .
- **TO BE merateľné ukazovatele** – t. j. popíšte cieľové merateľné ukazovatele, ktoré chcete dosiahnuť.
- Odporúčame, aby váš budúci IS mal automatizovaný monitoring (na pravidelnej báze, napr. týždenne) vami stanovených merateľných ukazovateľov – s cieľom, aby ste mohli riadiť službu, produkt, proces, ľudí
- V prípade financovania cez zdroje EÚ uvádzať aj Projektové merateľné ukazovatele z operačného programu (špecifické ciele, merateľné ukazovatele atď).

### 3.4 Riziká a závislosti

**Zoznam rizík a závislostí realizácie projektu:**

**Realizácia projektu na zabezpečenie kyberbezpečnosti financovaného z fondov EÚ môže čeliť viacerým rizikám.**

#### 1. Nedodržanie harmonogramu aktivít

Riziko spočíva v nedodržovaní harmonogramu aktivít projektu, ktoré by vyústilo do oneskorenia projektu.

Opatrenia na elimináciu:

V rámci prípravy projektu bol harmonogram jednotlivých aktivít zostavený tak aby zodpovedal možnostiam žiadateľa.

Na elimináciu rizika nedodržania harmonogramu aktivít projektu je potrebné prijať niekoľko opatrení, ktoré zabezpečia efektívne riadenie času a zdrojov. Tu sú niektoré z nich:

a) Dôkladné plánovanie:

- žiadateľ má vypracovaný detailný projektový plán so všetkými aktivitami, úlohami a milníkmi.
- žiadateľ využil osvedčené metódy plánovania, ako sú Ganttove diagramy alebo PERT (Program Evaluation and Review Technique).

b) Realistické časové odhady:

- v rámci žiadosti boli stanovené realistické časové rámce pre jednotlivé aktivity na základe skúseností a po porade s odbornými konzultantmi,
- do riadenia a plánovania bol zapojený projektový tím, ktorý bude úlohy vykonávať, aby sa zabezpečila realističnosť odhadov.

c) Identifikácia kritických ciest:

- žiadateľ určil kritické cesty (critical paths) v projekte, ktoré majú najväčší vplyv na celkový harmonogram.
- žiadateľ bude pravidelne sledovať postup na týchto kritických cestách a zabezpečí, aby nedošlo k žiadnym oneskoreniam.

d) Rezervy na nepredvídané udalosti:

- žiadateľ v rámci stanovenia aktivity projektu zahrnul do plánu časové rezervy (buffer times) na pokrytie nepredvídaných udalostí alebo oneskorení.
- projektový a odborný tím žiadateľa je pripravený flexibilne prispôsobiť plán pri výskyte neočakávaných situácií.

e) Pravidelný monitoring a kontrola:

- žiadateľ bude mať v rámci realizácie projektu zavedený zavedený systém pravidelného monitorovania postupu projektu a porovnávania s harmonogramom.
- súčasne budú používané softvérové nástroje na riadenie projektov, ktoré umožňujú sledovanie priebehu v reálnom čase.

f) Efektívna komunikácia:

- žiadateľ má zavedené pravidelné stretnutia projektového tímu na hodnotenie postupu a riešenie problémov.
- žiadateľ zabezpečí udržiavať otvorenú a transparentnú komunikáciu medzi všetkými členmi tímu a zainteresovanými stranami.

g) Riadenie rizík:

- žiadateľ identifikoval potenciálne riziká, ktoré by mohli ovplyvniť harmonogram, a vypracovať plány na ich zmiernenie.
- žiadateľ bude pravidelne aktualizovať rizikový register a prijímať preventívne opatrenia.

h) Dostatočné zdroje:

- žiadateľ má zabezpečené, aby mal projektový tím k dispozícii všetky potrebné zdroje vrátane personálu, technológií a financií.
- žiadateľ bude riešiť prípadné nedostatky zdrojov čo najskôr, aby nedošlo k oneskoreniam.

i) Flexibilita a adaptabilita:

- žiadateľ je pripravený prispôsobiť harmonogram podľa aktuálnych podmienok a vývoja situácie.
- žiadateľ bude mať zavedené spolu s projektovými tímom procesy pre rýchlu reakciu na zmeny a úpravu plánov.

**Závažnosť tohto rizika však považujeme za nízku, vzhľadom na zabezpečenie účinných opatrení na elimináciu.**

## **2. Nedosiahnutie plánovaných hodnôt merateľných ukazovateľov**

Hoci v rámci projektu sa nesledujú také merateľné ukazovatele, ktoré by boli merateľnými ukazovateľmi s príznakom, žiadateľ si uvedomuje možné riziká súvisiace s nenaplnením merateľných ukazovateľov.

### Opatrenia na elimináciu rizika:

Keďže merateľné ukazovatele sú odrazom úspešného naplnenia jednotlivých aktivít, prijímateľ prijal alebo prijme najmä nasledovné opatrenia:

Prijímateľ dlhoročne realizuje projekty financované s fondov EÚ. Samotný projekt vyplýva z jeho dlhodobých plánov a preto celé jeho nastavenie je podrobne analyzované vrátane nastavenia časového harmonogramu a cieľových hodnôt merateľných ukazovateľov. Prijímateľ do realizácie projektu zapojil odborných zamestnancov spoločnosti, aby bolo zaručené dosiahnutie plánovaných výsledkov.

Aby sa eliminovalo riziko nedosiahnutia plánovaných hodnôt merateľných ukazovateľov v rámci projektu, môžu byť prijaté nasledujúce opatrenia:

a) Precízne plánovanie a nastavenie realistických cieľov:

- V projekte sú definované jasné a realistické ciele a merateľné ukazovatele (KPIs) na základe dôkladnej analýzy, prípravy projektu a prieskumu trhu.
- Žiadateľ využil historické údaje a osvedčené metódy na stanovenie cieľov.

b) Pravidelný monitoring a hodnotenie:

- žiadateľ zavedie v rámci realizácie projektu systém pravidelného monitoringu a hodnotenia postupu dosahovania cieľov.
- žiadateľ zavedie v rámci realizácie projektu mechanizmy na pravidelné správy a analýzy progresu.

c) Flexibilita a adaptabilita:

- projektový tím žiadateľa je pripravený prispôbiť plány a stratégie na základe zistení z monitoringu.
- žiadateľ počas realizácie projektu zavedie procesy pre rýchlu reakciu na neočakávané udalosti alebo zmeny v externom prostredí.

d) Zabezpečenie potrebných zdrojov:

- žiadateľ identifikoval a zabezpečil všetky potrebné zdroje vrátane finančných, ľudských a technologických potrebných na úspešnú realizáciu projektu,
- žiadateľ bude pravidelne preverovať dostupnosť zdrojov a riešiť prípadné nedostatky.

e) Kvalitný projektový manažment:

- žiadateľ disponuje skúsenými a certifikovanými projektovými manažérmi, ktorých skúsenosti sú uvedené v časti 7.4. ŽoNFP,
- žiadateľ bude využívať pri realizácii projektu osvedčené metodiky projektového riadenia, ako sú PRINCE2, PMI alebo Agile.

f) Zapojenie všetkých zainteresovaných strán:

- žiadateľ prostredníctvom projektového tímu zabezpečí, aby všetci zainteresovaní boli dostatočne informovaní a zapojení do projektu.
- žiadateľ plánuje organizovať pravidelné stretnutia a konzultácie s projektovým tímom a relevantnými stranami na získanie spätnej väzby a podpory pri realizácii projektu,

g) Rizikový manažment:

- Identifikovať potenciálne riziká spojené s dosahovaním ukazovateľov a vypracovať plány na ich zmiernenie.
- Pravidelne aktualizovať rizikový register a prijímať preventívne opatrenia.

h) Komunikácia a transparentnosť:

- Zabezpečiť otvorenú a transparentnú komunikáciu o postupoch a výsledkoch.
- Informovať tím a vedenie o aktuálnom stave a prípadných problémoch.

i) Kontrola a audit:

- Zaviesť interné a externé kontroly a audity na preverenie plnenia merateľných ukazovateľov.
- Implementovať odporúčania z auditov na zlepšenie procesov a výkonnosti.

**Závažnosť tohto rizika však považujeme za nízku, vzhľadom na zabezpečenie účinných opatrení na elimináciu.**

### **3. Nedostatky v dodávkach od externých dodávateľov**

Nedodržovanie termínov zo strany externých dodávateľov služieb a tovarov. Dodávateľ(ia) služieb a tovarov, ktorý vziđe z procesu verejného obstarávania nebude dodržiavať harmonogram prác a dodávok, resp. bude v omeškani.

**Opatrenia na elimináciu rizika:**

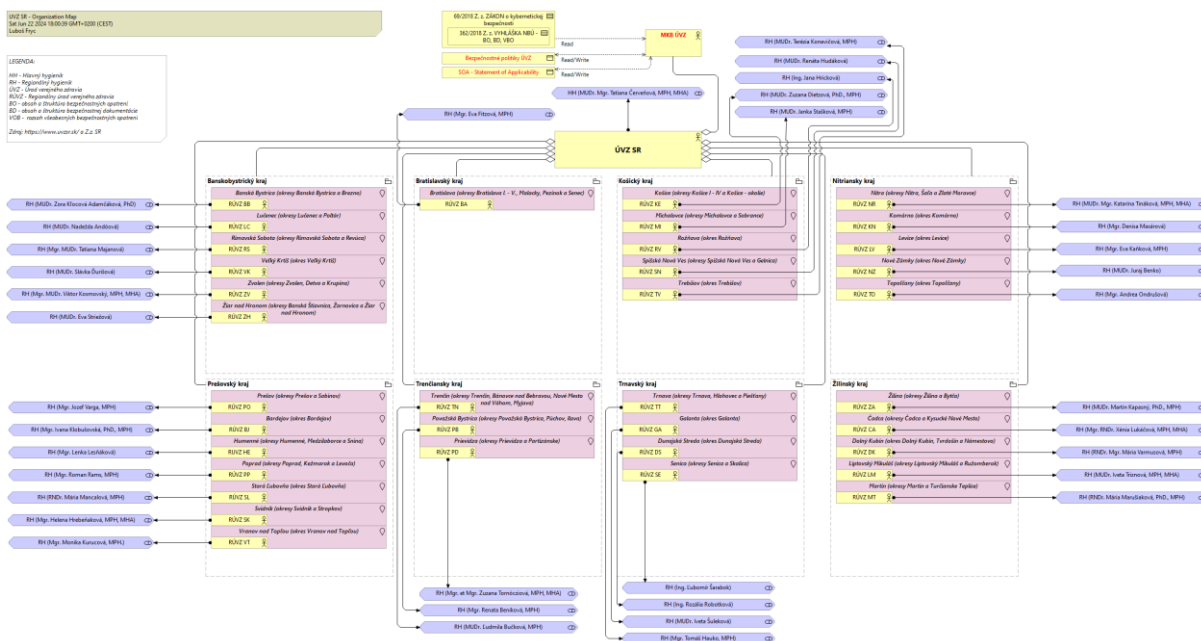
Projektový manažér bude pravidelne komunikovať s dodávateľom, konzultovať prípadné omeškania, hľadať riešenia. V rámci realizácie projektu budú organizované pravidelné zasadnutia Riadiaceho výboru. Postihy za škody a omeškania budú definované v rámci zmluvy o dodávke tovaru, resp. poskytnutí služieb. Ďalším opatrením je už dnes realizovaná kontrola kvality externých dodávateľov zo strany žiadateľa. Súčasne bude žiadateľ starostlivo vyberať dodávateľov na základe ich schopností a referencií. V rámci procesu verejného obstarávania budú zavedené jasné zmluvné podmienky a dohodnúť si pravidelné kontroly plnenia záväzkov, vrátane finančných sankcií. Žiadateľ bude sa bude usilovať o diverzifikovanie dodávateľov, aby sa minimalizovala závislosť na jedinom zdroji. Podmienkou žiadateľa bude implementovať osvedčené technológie a riešenia, ktoré sú už overené na trhu. Žiadateľ zároveň plánuje investovať do školení a certifikácií pre zamestnancov, aby mali potrebné zručnosti a vedomosti.

Závažnosť tohto rizika však považujeme za nízku, vzhľadom na zabezpečenie účinných opatrení na elimináciu.

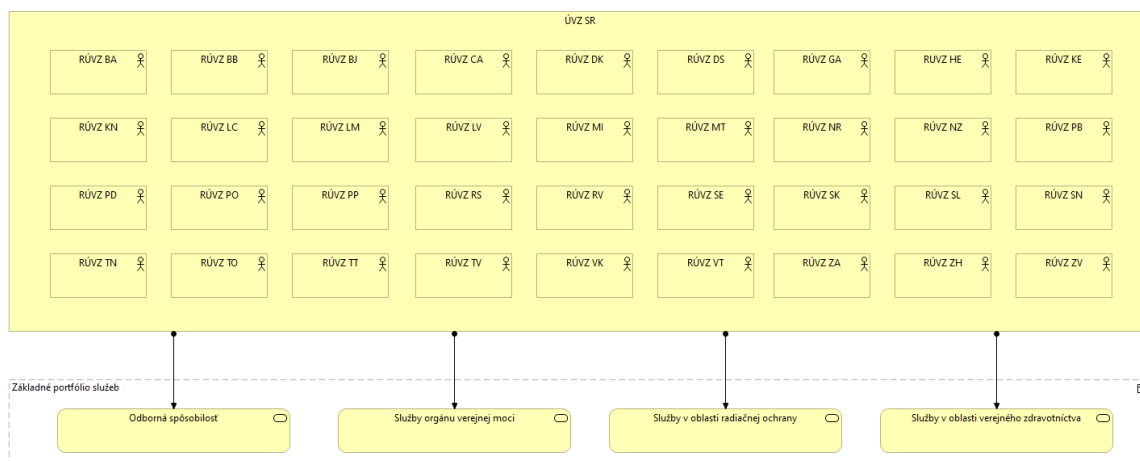
**Na základe vykonanej analýzy rizík ohrozujúcich úspešnú realizáciu projektu možno konštatovať, že menej ako 10 % rizík z celkového počtu identifikovaných rizík v ŽoNFP je s vysokou závažnosťou, ktoré ohrozujú úspešnú realizáciu projektu.**

**4. SÚČASNÁ ARCHITEKTÚRA PREVÁDZKOVANÝCH IS**

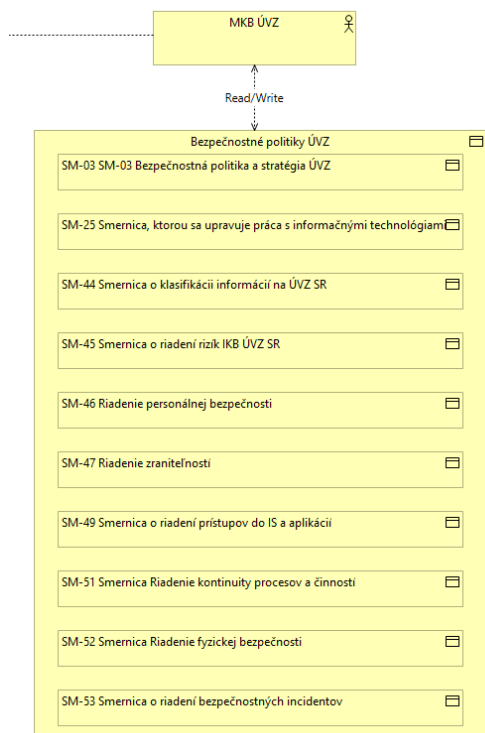
**ÚVZ SR, ako aj jednotlivé RÚVZ spoločne používajú IS ÚVZ.**







LEGENDA:  
ÚVZ - Úrad verejného zdravia  
RÚVZ xx - Regionálny úrad verejného zdravia  
Zdroj: <https://www.uvzsr.sk/>



## 5. ROZPOČET A PRÍNOSY

Rozpočet projektu je detailne špecifikovaný v časti 11. Rozpočet projektu v rám ci predloženej ŽoNFP.

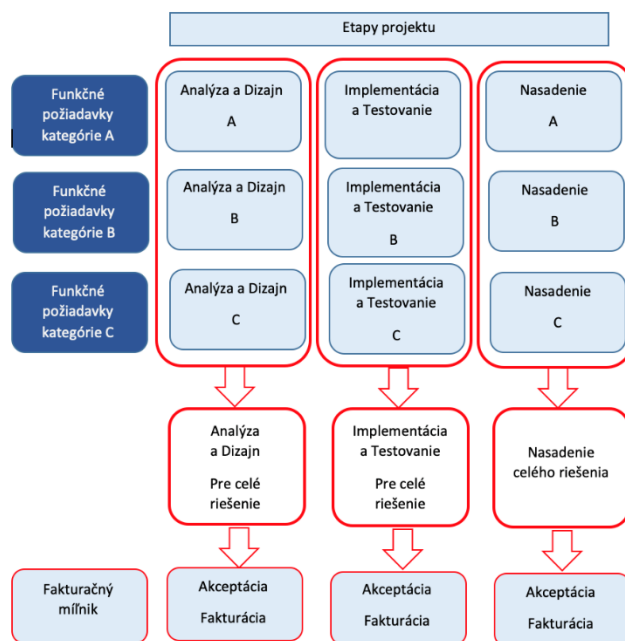
## 6. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU A METÓDA JEHO RIADENIA

Harmonogram projektu je uvedený v časti 9. Harmonogram realizácie aktivít predloženej ŽoNFP.

Projekt bude realizovaný metódou Waterfall:

Waterfall - vodopádový prístup počíta s detailným naplánovaním jednotlivých krokov a následnom dodržiavaní postupu pri vývoji alebo realizácii projekty. Projektovému tímu je daný minimálny priestor na zmeny v priebehu realizácie. Vodopádový prístup je vhodný a užitočný v projektoch, ktorý majú jasný cieľ a jasne definovateľný postup a rozdelenie prác.

*Objednávateľ projektu vypracuje funkčnú a technickú špecifikáciu,*



Objednávateľ špecifikuje funkčné požiadavky a kategórie A, B, C (pričom A = must have, B = nice to have, C= zvýšené)

Dokumenty obsahujúce informácie klasifikované ako chránené a prísne chránené podľa Vyhlášky č.362/2018 Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení budú v rámci projektu odovzdávané v elektronickej podobe šifrovane pomocou PGP kľúčov, ktoré si žiadateľ a dodávateľ na začiatku projektu vymenia.

Pri akceptácii budú vyhotovované vopred definované akceptačné kritéria a požiadavky z katalógu funkčných a nefunkčných požiadaviek vzťahujúce sa k jednotlivým míľnikom projektu.

Metóda riadenia "Waterfall" (vodopád) je jedným z najtradičnejších prístupov k riadeniu projektov v oblasti IT. Tento model je lineárny a sekvenčný, čo znamená, že každá fáza projektu musí byť dokončená pred začiatkom ďalšej. Tieto fázy sú nasledovné:

### 1. Požiadavky (Requirements):\*

- V tejto počiatočnej fáze sú zhromaždené všetky požiadavky na systém. Ide o veľmi dôležitý krok, pretože chyby v

požiadavkách môžu mať vážne následky v neskorších fázach. Dokumentujú sa všetky požiadavky zákazníka, funkčné aj nefunkčné, a výsledkom je detailná špecifikácia požiadaviek.

#### 2. Analýza systému (System Design):

- Po dokončení zhromažďovania požiadaviek sa prejde k analýze systému a návrhu. Táto fáza zahŕňa vytvorenie architektúry systému, technických špecifikácií a návrhu softvéru, ktorý bude schopný splniť všetky definované požiadavky.

#### 3. Implementácia (Implementation):

- Po schválení návrhu systému sa začne s implementáciou, teda s programovaním a kódovaním systému podľa navrhnutých špecifikácií. Výsledkom tejto fázy je hotový softvér.

#### 4. Integrácia a testovanie (Integration and Testing):

- V tejto fáze sa jednotlivé komponenty systému integrujú a testujú sa ako celok, aby sa overilo, či systém funguje podľa očakávaní a spĺňa všetky špecifikované požiadavky. Testovanie zahŕňa rôzne typy testov, vrátane funkčných, integračných a systémových testov.

#### 5. Nasadenie (Deployment):

- Po úspešnom testovaní sa systém nasadí do produkčného prostredia. Táto fáza môže zahŕňať aj školenie používateľov a prípravu dokumentácie pre používateľov.

#### 6. Údržba (Maintenance):

- Po nasadení systému začína fáza údržby, ktorá zahŕňa opravy chýb, aktualizácie a vylepšenia systému na základe spätnej väzby od používateľov a meniace sa požiadavky.

#### **Výhody Waterfall modelu:**

- Jednoduchosť a jasná štruktúra: \*Každá fáza má jasne definovaný začiatok a koniec.
- Dobre zdokumentovaný proces: Všetky požiadavky a kroky sú detailne zdokumentované.
- Jednoduché riadenie: \*Jednoduché plánovanie a sledovanie pokroku projektu.

Waterfall model je ideálny pre projekty, kde sú požiadavky jasne definované a stabilné, a kde sa očakáva, že projekt prebehne bez veľkých zmien. V súčasnosti sa však stále častejšie využívajú agilné prístupy, ktoré lepšie vyhovujú dynamickým a meniacim sa požiadavkám projektov.

#### **Kvantitatívne prínosy projektu:**

- Zníženie nákladov spojených so sanáciou KBU/KBI
- Zníženie nákladov spojených s elimináciou následkov reaktívnych KBI

#### **Kvalitatívne prínosy projektu:**

- Zníženie rizika KBI,
- Zvýšenie súladu s platnou legislatívou,
- Zvyšovanie úrovne kybernetickej a informačnej bezpečnosti,
- Zvýšenie detekcie KBI,
- Zvýšte spokojnosť a dôveru používateľov,

#### **Popis cieľového stavu**

##### **Základné ciele projektu:**

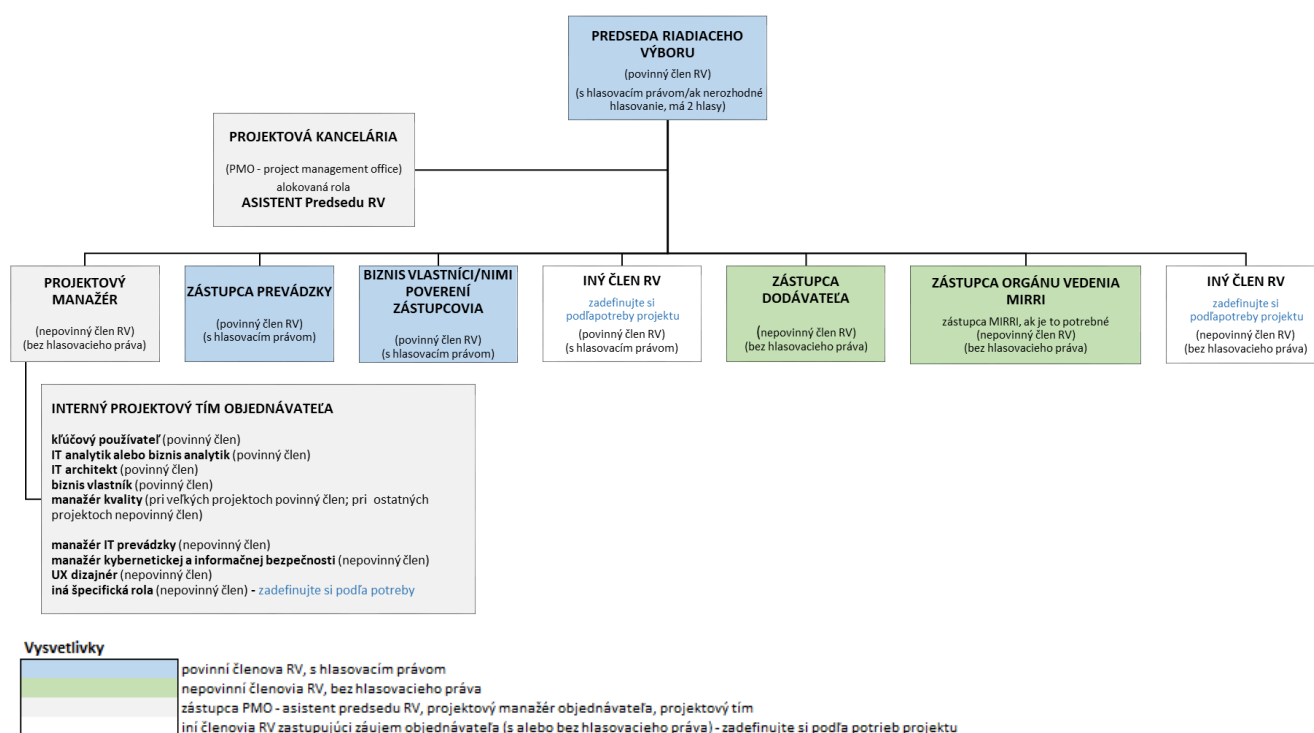
- Aktualizácia stratégie kybernetickej bezpečnosti,
- Aktualizácie bezpečnostnej politiky KB vrátane implementačnej dokumentácie, v súlade s Príloha – Manažérske Produkty,
- Vykonávanie inventarizácie aktív, klasifikácie informácií a kategorizácie sietí a interných systémov,
- Stabilizácia riadenia rizík – aktualizácia analýzy rizík a analýzy dopadov a nasadenie nástroja Asset Inventory, Threats, Risks and Measures (EAM/),
- Implementácia nástroja na zaznamenávanie a monitorovanie udalostí (Log Management)
- Implementácia auditu KB, procesu riadenia a kontroly dodržiavania predpisov.

## 7. PROJEKTOVÝ TÍM

**Projektový tím je detailne popísaný v predloženej ŽoNFP, časť 7.5 Prevádzková kapacita žiadateľa.**

ID	Meno a Priezvisko	Pozícia	Oddelenie	Rola v projekte
1.	Doplniť meno a priezvisko	Doplniť pozíciu (pracovné zaradenie v línii)	Doplniť názov org. útvaru	Doplniť rolu v projekte
2.	Doplniť meno a priezvisko	Doplniť pozíciu (pracovné zaradenie v línii)	Doplniť názov org. útvaru	Doplniť rolu v projekte
3.	Doplniť meno a priezvisko	Doplniť pozíciu (pracovné zaradenie v línii)	Doplniť názov org. útvaru	Doplniť rolu v projekte

Vzor organizačnej štruktúry



## 8. VÝSLEDKY PROJEKTU

VÝSLEDKOM PROJEKTU JE ZABEZPEČENIE SÚLADU SO SMERNICOU NIS2 a Zákomom o kybernetickej bezpečnosti Slovenskej republiky (Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti)

Realizáciou vyššie uvedenej aktivity, dosiahne žiadateľ súlad so Smernicou NIS2 a Zákomom o kybernetickej bezpečnosti Slovenskej republiky (Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti). Tieto aktivity pokrývajú širokú škálu oblastí vrátane bezpečnostnej politiky, správy rizík, ochrany proti škodlivému kódu, inventarizácie aktív, bezpečnosti sietí a informačných systémov, kontroly prístupu, riadenia zraniteľností, monitoringu, kontinuity činností a incident managementu.

Tu je prehľad, ako tieto aktivity pomáhajú dosiahnuť súlad:

**1. Bezpečnostná politika a stratégia:** Prehodnotenie a aktualizácia bezpečnostnej politiky a stratégie zabezpečuje, že organizácia má správne nastavený rámec pre kybernetickú bezpečnosť v súlade s legislatívou.

2. Smernice a procesy : Aktualizácia a vytváranie nových smerníc pre rôzne oblasti kybernetickej bezpečnosti zabezpečuje, že všetky činnosti sú vykonávané v súlade s novými požiadavkami Zákona a NIS2.

3. Riadenie rizík: Nasadenie nástrojov na automatizáciu analýzy rizík a aktualizácia analýzy rizík zabezpečuje, že riziká sú riadne identifikované, hodnotené a riadené.

4. Inventarizácia aktív: Spracovanie inventarizácie aktív a ich klasifikácia pomáha organizácii identifikovať a spravovať svoje informačné aktíva, čo je kľúčové pre ochranu citlivých informácií.

5. Log management: Implementácia nástrojov a procesov na detekciu a riadenie kybernetických bezpečnostných incidentov zabezpečuje, že organizácia môže efektívne zvládať incidenty a minimalizovať ich dopad.

Realizácia týchto aktivít predstavuje komplexný prístup k dosiahnutiu súladu s NIS2 a Zákonom o kybernetickej bezpečnosti, čím sa zabezpečuje ochrana kritickej infraštruktúry a citlivých informácií v súlade s aktuálnymi požiadavkami.

## **9. PRÍLOHY**

**Príloha** : Zoznam rizík a závislostí (Excel): <https://www.mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/riadenie-kvality-qa/index.html>