I-02 Projektový zámer (projektovy_zamer)

naposledy upravil Juraj Kottner

- 2025/02/25 15:54

Obsah

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

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

Povinná osoba	Ministerstvo kultúry Slovenskej republiky
Názov projektu	Zvýšenie úrovne kybernetickej a informačnej bezpečnosti MKSR
Zodpovedná osoba za projekt	Ing. Juraj Kottner
Realizátor projektu	Ministerstvo kultúry Slovenskej republiky
Vlastník projektu	Ministerstvo kultúry Slovenskej republiky

Schvaľovanie dokumentu

Položka	**Meno a priezvisko**	**Organizácia**	**Pracovná pozícia**	**Dátum**	**Podpis** (alebo elektronický súhlas)
Vypracoval	Ing. Juraj Kottner	Ministerstvo kultúry Slovenskej republiky	Riaditeľ odboru informačných systémov	2.1.2025	

1.História DOKUMENTU

Verzia	Dátum	Zmeny	Meno
0.1	04.11.2024	Pracovný návrh	Kolektív Žiadateľa
0.7	09.12.2024	Prvá verzia na kontrolu	Kolektív Žiadateľa
0.9	27.12.2024	Verzia na schválenie	Kolektív Žiadateľa
1.0	02.01.2025	Final verzia na odovzdanie	Kolektív Žiadateľa
1.1	20.01.2025	Zapracovanie pripomienok od MIRRI	Kolektív Žiadateľa

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.

Dokument Projektový zámer v zmysle vyššie uvedenej vyhlášky obsahuje manažérske zhrnutie, rozsah, ciele a motiváciu na realizáciu projektu, zainteresované strany, alternatívy, návrh merateľných ukazovateľov, detailný opis požadovaných projektových výstupov, detailný opis obmedzení, predpokladov, tolerancií a návrh organizačného zabezpečenia projektu, detailný opis rozpočtu projektu a jeho prínosov, náhľad architektúry a harmonogram projektu so zoznamom rizík a závislostí.

2.1Použité skratky a pojmy

SKRATKA/POJEM	POPIS
IS	Informačný systém
EÚ	Európska únia
HW	Hardware
SW	Software
MCA	Multikriteriálna analýza
MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
NAC	Network Access Control
NBÚ	Národný bezpečnostný úrad
NDR	Network detection and response
PAM	Privileged Access Management
SIEM	Security Information and Event Management
TCO	Total cost of ownership
VO	Verejné obstarávanie
ZoKB	Zákon o kybernetickej bezpečnosti
ŽoNFP	Žiadosť o nenávratný finančný príspevok
NKIVS	Národná koncepcia informatizácie verejnej správy
OOÚ	Ochrana osobných údajov
PO	Plán obnovy a odolnosti
OVM	Orgán verejnej moci
PaaS	Platform as a service
PILOT	PILOT - Prevádzka riešenia na vybraných aktéroch na produkčnom prostredí.
PoC	PoC - Implementovaný prototyp riešenia
PR	Projektové riadenie
RFO	Register fyzických osôb
RPO	Register právnických osôb
SDL	Security development lifecycle
SLA	Service level agreement
SOAR	Security orchestration, automation and response

2.2Konvencie pre typy požiadaviek (príklady)

Hlavné kategórie požiadaviek v zmysle katalógu požiadaviek, sú rozdelené na funkčné (funkcionálne), nefunkčné (kvalitatívne, výkonové a pod.). Podskupiny v hlavných kategóriách je možné rozšíriť podľa potrieb projektu, napríklad:

Funkcionálne (používateľské) požiadavky majú konvenciu:

FRxx

U – užívateľská požiadavka

R – označenie požiadavky

xx – číslo požiadavky

V rámci projektu a katalógu požiadaviek neboli uvedené nefunkčné požiadavky, ale v prípade, že v rámci fázy Analýza a Dizajn budú v rámci revízie požiadaviek pridané, budú mať označenie uvedené nižšie.

Nefunkčné (kvalitatívne, výkonové - Non Functional Requirements - NFR) požiadavky budú mať nasledovnú konvenciu:

NRxx

N – nefukčná požiadavka (NFR)

R – označenie požiadavky

xx – číslo požiadavky

Ostatné typy požiadaviek môžu byť ďalej definované objednávateľom/PM.

3.DEFINOVANIE PROJEKTU

3.1Manažérske zhrnutie

Predkladaný projekt je vypracovaný v súlade s:

- Vyhláškou č. 401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy;
- Výzvou č. PSK-MIRRI-616-2024-DV-EFRR na predkladanie Žiadostí o poskytnutie nenávratného finančného príspevku so zameraním na „Zvýšenie úrovne kybernetickej a informačnej bezpečnosti“.

Výzva č. PSK-MIRRI-616-2024-DV-EFRR definuje:

- Priorita -1P1 Veda, výskum a inovácie
- Špecifický cieľ - RSO 1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy
- Opatrenie - 1.2.1 Podpora v oblasti informatizácie a digitálnej transformácie (Oblasť - Kybernetická a informačná bezpečnosť)

Ministerstvo kultúry Slovenskej republiky, Nám. SNP č. 33, 813 31 Bratislava – Staré Mesto (ďalej len „MKSR") je zapísané do registra prevádzkovateľov základnej služby a je povinné plniť povinnosti vyplývajúce zo zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a zákona č. 95/2019 Z.z. o informačných technológiách verejnej správy (ITVS).

Práve prostredníctvom predkladaného projektu môže MKSR tieto primárne oblasti aktualizovať v značnej miere tak odstrániť zistené nedostatky.

Realizáciou aktivít projektu MKSR dosiahne naplnenie hlavného opatrenia v oblasti Kybernetická a informačná bezpečnosť. Prostredníctvom navrhovaných riešení je zámerom MKSR minimalizovať negatívne dopady v prípade výskytu kybernetického incidentu a útokov na informačné systémy MKSR prostredníctvom zavádzania systémov riadenia a nástrojov v oblasti IB a KyB.

V súlade s § 29 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „ZoKB“) bol 29.04.2024 odovzdaný audit kybernetickej bezpečnosti. Následne bola odovzdaná finálna verzia záverečnej správy o výsledkoch auditu. V súlade s §29 ods. 5 ako prevádzkovateľ základnej služby v zákonom stanovenej lehote bola zaslaná záverečná správa o výsledkoch auditu NBÚ spolu s opatreniami na nápravu a s lehotami na ich odstránenie. Tento projekt rieši vybrané návrhy a opatrenia na nápravu nesúladov, ktoré majú pre Žiadateľa najvyššiu prioritu a zabezpečia zvýšenie úrovne kybernetickej a informačnej bezpečnosti.

Indikatívna výška finančných prostriedkov predstavuje **2 621 943 €.** a projekt bude financovaný z **Programu Slovensko**.

V rámci projektu budú dosiahnuté nasledovné kvantitatívne ako aj kvalitatívne prínosy.

Kvantitatívne prínosy v rámci navrhovaného projektu sú:

- Zníženie nákladov súvisiacich s odstraňovaním preventívnych kybernetických incidentov.
- Zníženie nákladov súvisiacich s odstraňovaním reaktívnych kybernetických incidentov.

Kvalitatívne prínosy vychádzajú z princípov NKIVS:

Prioritná os 4 Kybernetická a informačná bezpečnosť a čiastkovým cieľom **Zvýšenie schopnosti včasnej identifikácie kybernetických incidentov vo verejnej správe**.

Ďalšie uvažované kvalitatívne prínosy v rámci navrhovaného projektu sú:

- Zníženie miery rizika vzniku kybernetického incidentu.
- Zvýšenie miery súladu s platnou legislatívou.
- Zvýšenie úrovne kybernetickej a informačnej bezpečnosti.
- Zvýšenie detekcie kybernetických bezpečnostných incidentov.
- Zvýšená spokojnosť a dôvera používateľov.

Harmonogram projektu je nastavený na **17** mesiacov od času T0.

Predkladaný projekt je vo vecnom súlade s **typmi akcie**:

- **Zlepšovanie technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti KIB v prostredí orgánov štátnej a verejnej správy**
- **Podpora včasnej detekcie a zvýšenie schopnosti reakcie na kybernetické bezpečnostné incidenty a na adaptáciu najmodernejších technológií, na zvýšenie odolnosti základných služieb pred kybernetickými hrozbami, vrátane podpory inovatívnych produktov a služieb až po úroveň TRL 9**

V rámci oprávneného typu akcie je oprávnená nasledovná **hlavná aktivita:**

- **Zvýšenie úrovne informačnej a kybernetickej bezpečnosti prostredníctvom nákupu hardvéru a bezpečnostného softvéru**

3.2Motivácia a rozsah projektu

Hlavnou motiváciou na realizáciu projektu a zvýšenie úrovne informačnej a kybernetickej bezpečnosti je aktuálny stav kybernetickej a informačnej bezpečnosti podporený výsledkami z auditu kybernetickej bezpečnosti Žiadateľa. Infraštruktúra žiadateľa je zastaralá, nespĺňajúce aktuálne požiadavky a štandardy a v niektorých dôležitých oblastiach predstavuje bezpečnostné riziko. V rámci motivácie uvádzame dôvody, ktorých realizácia je oprávnená v rámci aktivít projektu:

Nesúlad voči zákonu č. 69/2018 Z. z

Výsledky z auditu kybernetickej bezpečnosti z roku 2024 preukázali veľké nedostatky a to najmä v oblastiach uvedených nižšie. Žiadateľ je povinný vykonať opatrenia, ktoré mu ukladá zákon.

Nedostatková oblasť Sieťová a komunikačná bezpečnosť

Žiadateľ aktuálne využíva bezpečnostné prvky ako Firewall 4 ks a sieťové switche 4ks dlho po dobe životnosti. Zároveň v rámci infraštruktúry absentuje aktívna forma kontroly a systém, ktorý by dokázal včas upozorniť Žiadateľa o možnom probléme alebo útoku. Jedná sa o veľmi vysoké riziko s veľmi závažným dopadom.

Nedostatková oblasť Zaznamenávanie udalostí a monitorovanie

Žiadateľ nemá centrálny systém zaznamenávania logov a nemá možnosť získavať plošné oznámenia o stave infraštruktúry. Existujú čiastkové riešenia v zmysle jednotlivých projektov, avšak v prípade kybernetického incidentu by bolo veľmi náročné dohľadávať informácie a následne ich analyzovať.

Nedostatková oblasť Kontinuita prevádzky

Žiadateľ disponuje čiastkovým riešením zálohovania avšak ten nepostačuje na komplexné zabezpečenie kontinuity prevádzky. Nie je zabezpečený komplexný a jednotný systém zálohovania, obnovy a testovania týchto procesov. V prípade rozsiahleho ransomware útoku nie je možné garantovať obnovu všetkých dát a ani kontrolu integrity všetkých obnovených dát.

Nedostatková oblasť Riešenie kybernetických bezpečnostných incidentov

Žiadateľ nemá zabezpečenú oblasť riadenia a správy kybernetických incidentov, čo okrem iného z dlhodobého hľadiska predstavuje veľké riziko nevhodného pristupovania počas a po kybernetickom útoku, zároveň zamedzuje tak vhodne pristúpiť k riešeniu kritickej situácií.

Nedostatková oblasť Riadenie rizík

Žiadateľ nemá zabezpečenú oblasť riadenia a správy rizík a zraniteľností, ako aj správu aktív a z toho vyplývajúcich problémov. Žiadateľ nemá zabezpečenú možnosť dostatočne včas preventívne reagovať na možné riziká a zraniteľnosti a zamedziť tak skutočnému potenciálnemu kybernetickému incidentu.

Nedostatková oblasť Bezpečnosť pri prevádzke informačných systémov a sietí

Žiadateľ nemá zabezpečenú oblasť správy prevádzky informačných systémov do takej miery, aby bolo možné efektívne využívať moderné systémy na správu infraštruktúrneho vybavenia, konfigurácií, dokumentácií a znalostných databáz a zabezpečiť tak best practice pri prevádzke informačných systémov.

Nedostatková oblasť Riadenie prístupov

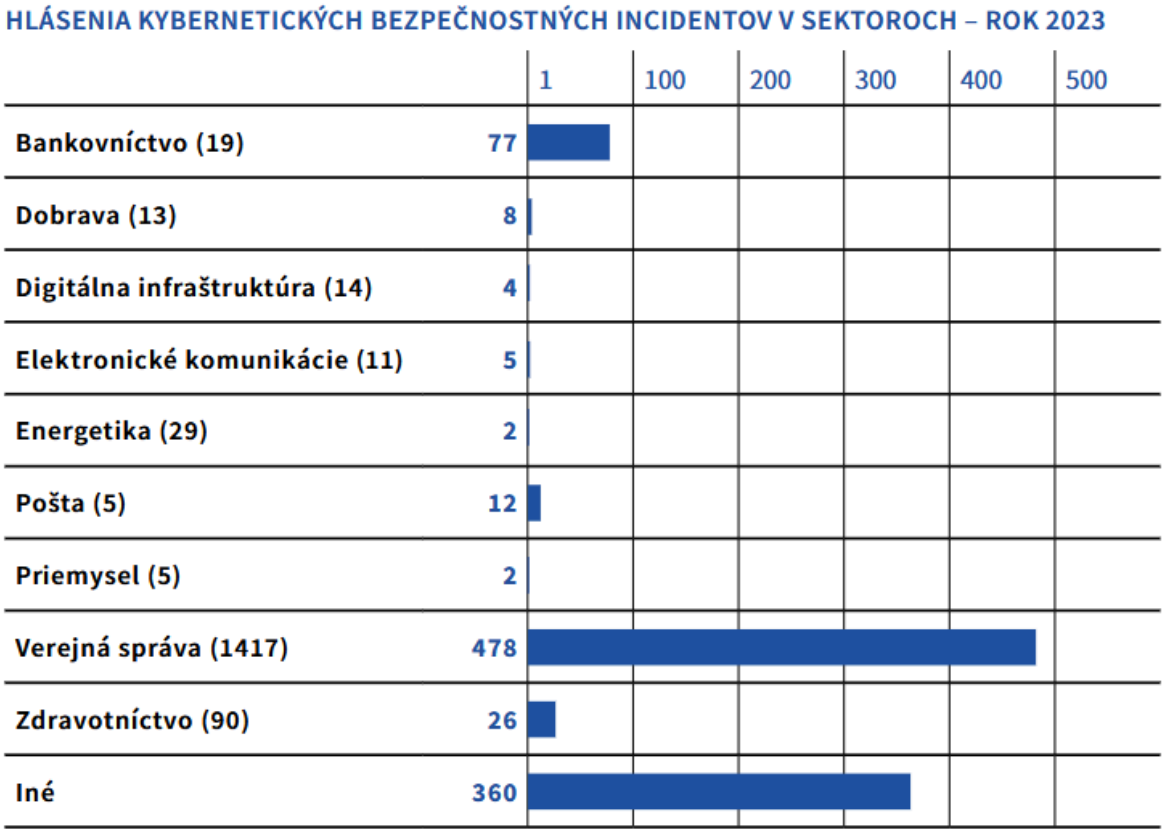
Žiadateľ nemá zavedený komplexný systém riadenia prístupov, ktorý by vedel zabezpečiť dodržiavanie oprávnení v zmysle požiadaviek na jednotlivé systémy. Existujúce formy riadenia sú prevažne lokálneho charakteru bez možnosti centrálnej správy a centrálneho sledovania. Vzhľadom na potreby Žiadateľa sa jedná o veľký nedostatok zabezpečiť bezpečný efektívny prístup k dátam a systémom pre tých ktorý ho v čase potrebujú bez ohrozenia všeobecnej bezpečnosti daných dát a systémov.

Poznámka: Konkrétne výsledky auditu nie sú v rámci verejne dostupnej dokumentácie z bezpečnostných dôvodov priložené.

Všeobecnou motiváciou na realizáciu projektu a zvýšenie úrovne informačnej a kybernetickej bezpečnosti je aj aktuálny stav a trend vývoja kybernetických útokov a incidentov a ich následné negatívne dopady, ktoré sú stále na vzostupe a negatívne ovplyvňujú životne dôležité sektory nevyhnutné pre chod spoločnosti. Pre názorný prehľad je využitá Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2023, zdroj: https://www.nbu.gov.sk/data/att/2855.pdf. Kde sa uvádza:

Najviac hlásení v roku 2023 pochádzalo zo sektorov verejná správa, bankovníctvo a zdravotníctvo. Vyšší počet hlásení implikuje viac incidentov v sektore a vyššiu úroveň zrelosti a povedomia hlásiaceho subjektu (nebojí sa hlásiť, komunikuje, hlási aj dobrovoľne a pod).

Je však potrebné brať do úvahy rozdielne počty subjektov v jednotlivých sektoroch aj atraktívnosť potenciálnych ziskov v prípade aktivít škodlivých aktérov. Takisto s prichádzajúcou novelou zákona v nadväznosti na NIS 2 je možné do ďalších rokov očakávať nárast hlásení, pretože novela rozšíri pôsobnosť na ďalšie subjekty.



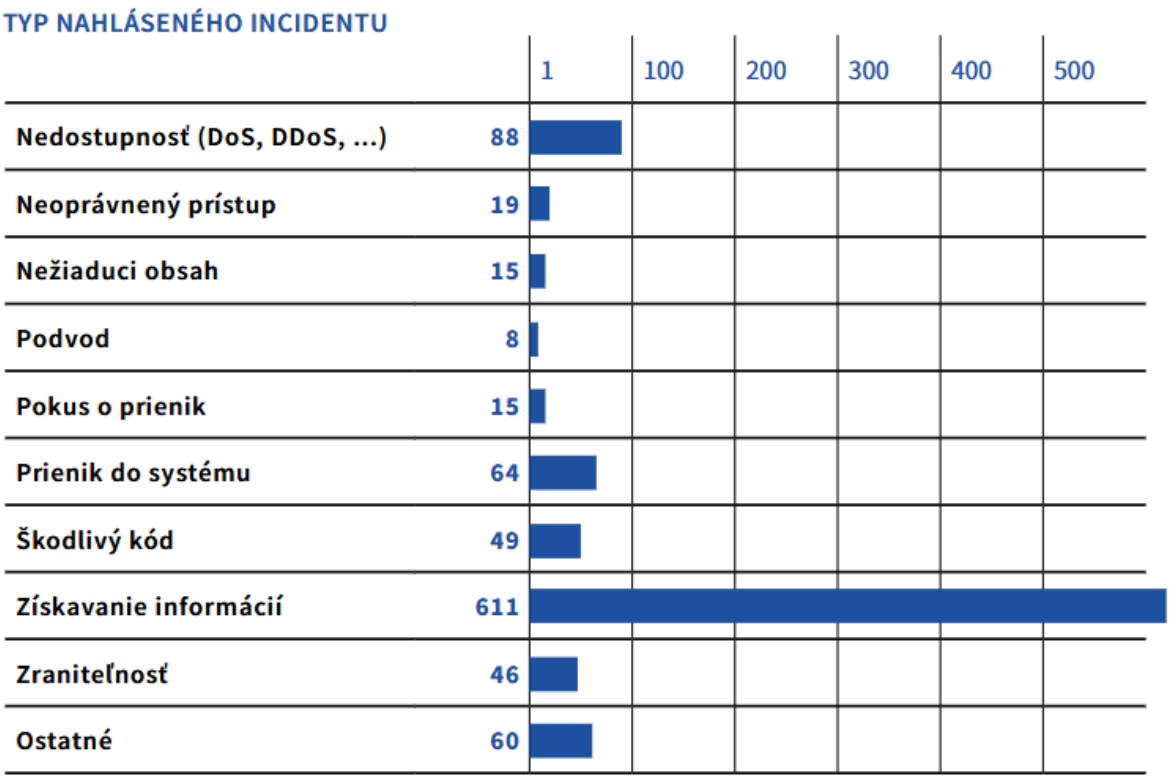
Zdroj: https://www.nbu.gov.sk/data/att/2855.pdf

V sektore verejná správa, konkrétne v podsektore informačné systémy verejnej správy, sa kybernetická bezpečnosť dlhodobo nemení napriek najväčšiemu počtu prevádzkovateľov. V niektorých prípadoch je zanedbaná až kriticky. Najmä samosprávy a menší prevádzkovatelia si neuvedomujú jej dôležitosť.

Na základe údajov o počte závažných kybernetických bezpečnostných incidentov, ktoré VJ CSIRT riešila, sa ich počet v uplynulých rokoch významne zvýšil. Významný zlom nastal po roku 2018. Za uplynulý rok 2022 sa počet závažných incidentov v riešení VJ CSIRT zvýšil na 1 012 s medziročným nárastom o 19 %, k čomu významne prispeli vyššia miera detekcie a nahlasovania incidentov, vypuknutie vojenského konfliktu medzi Ruskom a Ukrajinou a významný nárast aktivity štátom podporovaných skupín. Vplyvom pokračovania konfliktu a pretrvávajúcej podpory Ukrajiny možno očakávať podobný vývoj aj v nasledujúcom období. Medzi najčastejšie tipy závažných incidentov v roku 2022 patrili: získavanie informácií – phishing, social engineering... (55 %), malvér (18 %) a botnet (7 %). Zdroj https://csirt.sk/.

Štatistický prehľad incidentov za rok 2023

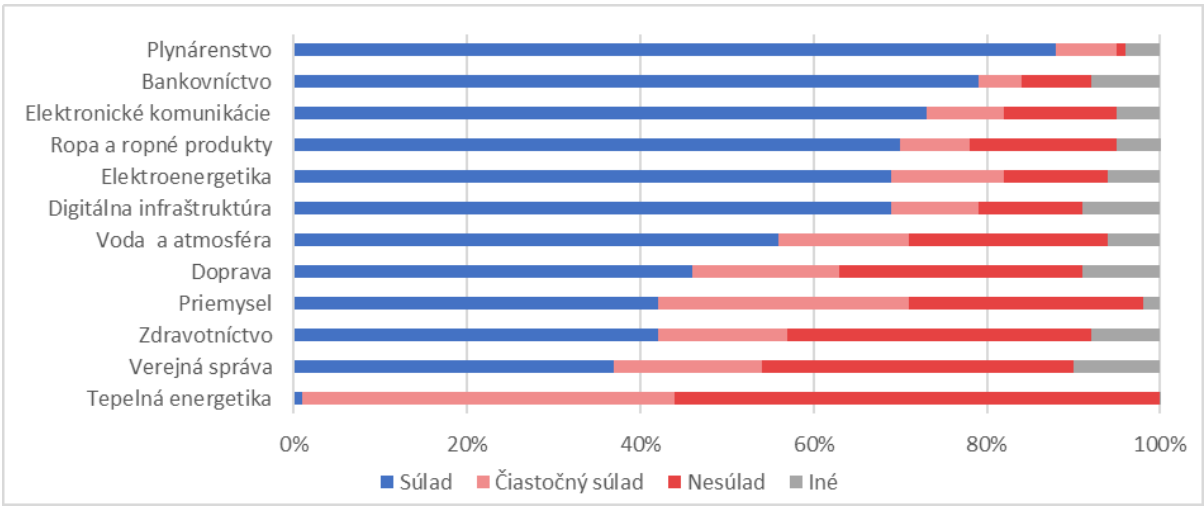
Národné centrum kybernetickej bezpečnosti plnilo úlohy na úseku monitorovania slovenského kybernetického priestoru. Pracovalo na zhromažďovaní a analyzovaní informácií z prijímaných hlásení o kybernetických bezpečnostných incidentoch. Oproti minulým rokom nastala zmena v štatistickom vyhodnocovaní zaznamenaných incidentov, v ktorom sa zhromažďujú údaje len o incidentoch nahlásených NCKB.



Zdroj: https://www.nbu.gov.sk/data/att/2855.pdf

V roku 2023 dominovali technické typy útokov, ako sú získavanie informácií, nedostupnosť, prienik do systému, škodlivý kód a zraniteľnosť. Phishing bol stále najrozšírenejšou a najúspešnejšou metódou získavania citlivých údajov a šírenia škodlivého obsahu. Nedostupnosť v sebe zahŕňa aj nedostupnosť systémov, ktorá nie je následkom kybernetického útoku (viď vyššie). Oproti predchádzajúcemu roku sme zaznamenali nárast ransomvérovej a malvérovej aktivity.

Sektor Verejná správa vykazuje dlhodobo veľmi zlé výsledky súladu s auditnými požiadavkami. Pritom je to jeden z najväčších sektorov z pohľadu počtu prevádzkovateľov základných služieb (ďalej aj „PZS"), ktorých je aktuálne 1 410. Horšie výsledky vykazuje už len odvetvie tepelnej energetiky. Podrobný prehľad stavu súladu, resp. nesúladu s auditnými požiadavkami z pohľadu jednotlivých sektorov zobrazuje obrázok nižšie. Dáta za rok 2022, zdroj: Doručené správy auditu KB za rok 2022, NBÚ.

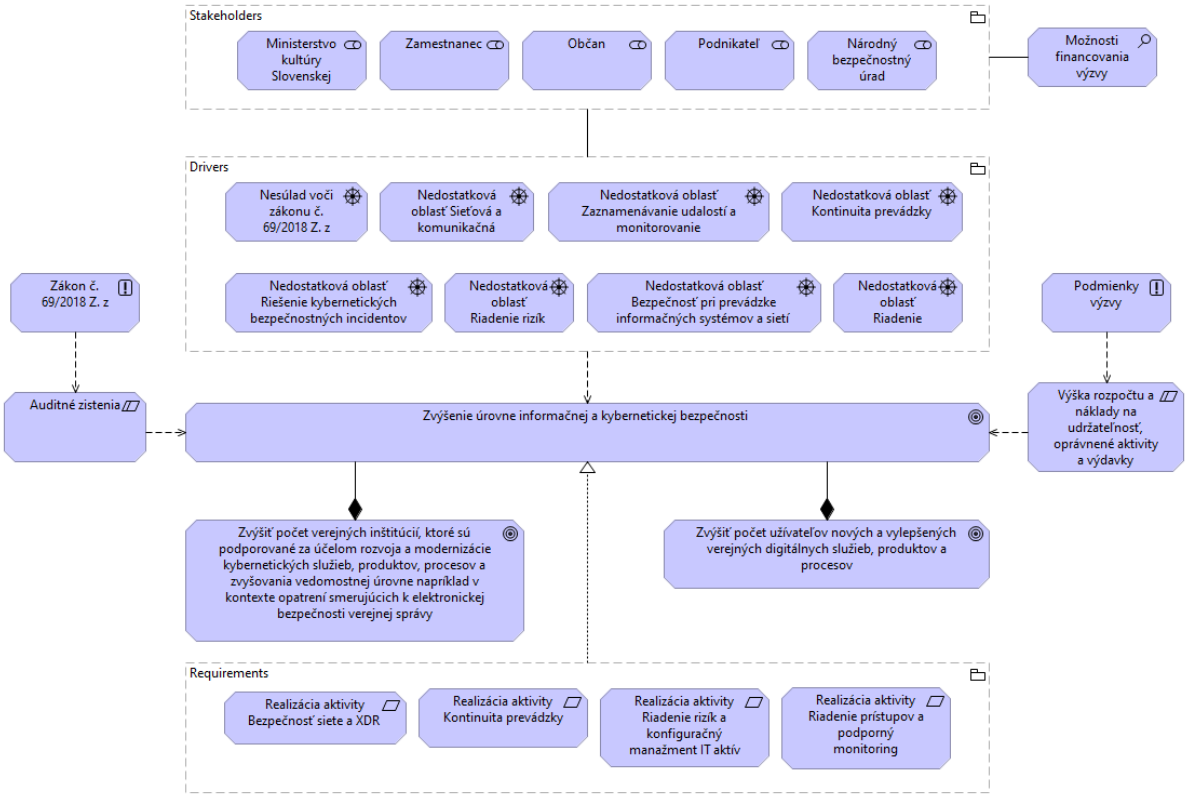


Obrázok 2: Stav súladu podľa vykonaných auditov KB v jednotlivých odvetviach za rok 2022 (Zdroj: Doručené správy auditu KB za rok 2022, NBÚ)

Ministerstvo kultúry Slovenskej republiky, Nám. SNP č. 33, 813 31 Bratislava – Staré Mesto (ďalej len „MKSR") je zapísané do registra prevádzkovateľov základnej služby a je povinné plniť povinnosti vyplývajúce zo zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a zákona č. 95/2019 Z.z. o informačných technológiách verejnej správy (ITVS). Medzi základné povinnosti patrí prijatie a dodržiavanie všeobecných bezpečnostných opatrení pre nasledovné oblasti:

- organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,
- riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
- personálnej bezpečnosti,
- riadenia prístupov,
- riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
- bezpečnosti pri prevádzke informačných systémov a sietí,
- hodnotenia zraniteľností a bezpečnostných aktualizácií,
- ochrany proti škodlivému kódu,
- sieťovej a komunikačnej bezpečnosti,
- akvizície, vývoja a údržby informačných sietí a informačných systémov,
- zaznamenávania udalostí a monitorovania,
- fyzickej bezpečnosti a bezpečnosti prostredia,
- riešenia kybernetických bezpečnostných incidentov,
- kryptografických opatrení,
- kontinuity prevádzky,
- auditu, riadenia súladu a kontrolných činností.

Všetky uvedené bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu. Žiadateľ je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom vykonaním auditu kybernetickej bezpečnosti v stanovenom rozsahu.



Žiadateľ deklaruje, že ku dňu predloženia ŽoNFP má vykonaný **audit kybernetickej bezpečnosti podľa § 29 zákona č. 69/2018 Z. z..**

Predmetom auditu kybernetickej bezpečnosti boli informačné systémy a príslušné podporné informačné systémy a informačné siete a prvky infraštruktúry.

Žiadateľ deklaruje, že nečerpal finančné prostriedky z výziev:

- **Podporu budovania bezpečnostných dohľadových centier v prostredí verejnej správy (17I06-04-V01)**
- **Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS (kód ITMS2014+ OPII-2021/7/16-DOP)**
- **Zvýšenie úrovne informačnej a kybernetickej bezpečnosti v podsektore ISVS / ITVS (kód ITMS2014+ OPII-2019/7/8-DOP)**
- **Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejná správa (kód PSK-MIRRI-611-2024-DV-EFRR)**

3.2.1 Problémy ktoré majú byť riešené v rámci predloženého projektu sú v oblastiach, ktoré sú namapované na jednotlivé hlavné aktivity a vychádzajú priamo zo záverov auditu kybernetickej bezpečnosti a zároveň ktoré sú v súlade s oprávnenými aktivitami v rámci výzvy

Oblasť	Aktivita
Sieťová a komunikačná bezpečnosť	Bezpečnosť siete a XDR
Zaznamenávanie udalostí a monitorovanie	
Riešenie kybernetických bezpečnostných incidentov	
Kontinuita prevádzky	Kontinuita prevádzky
Riadenie rizík	Riadenie rizík a konfiguračný manažment IT aktív
Bezpečnosť pri prevádzke informačných systémov a sietí	
Riadenie prístupov	Riadenie prístupov

3.2.1.1Prvá skupina oblastí z vysokým nesúladom na základe auditu, ktoré sú v súlade s podmienkami výzvy projektu

- **Sieťová a komunikačná bezpečnosť**
  - Implementácia nástrojov na ochranu integrity sietí, ktoré zabezpečujú riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami, implementácia segmentácie sietí, implementácia alebo obnova firewall-u, revízia firewall pravidiel;
  - zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a vzdialený prístup, napríklad implementáciou dvojfaktorovej autentizácie alebo kryptografických prostriedkov;
  - segmentácie sietí v súlade s pravidlami klasifikácie a kategorizácie;
  - implementácia automatizovaného nástroja na identifikáciu neoprávnených sieťových spojení na hranici s vonkajšou sieťou, na blokovanie neoprávnených spojení, na monitorovanie bezpečnosti, na detekciu prienikov a prevenciu prienikov identifikáciou nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky a ďalších povinností alebo vo forme funkcionalít, prípadne licencií iných už existujúcich nástrojov;
  - implementácia sond detekcie a prevencie prieniku, najmä na serveroch podporujúcich základné služby informačných technológií verejnej správy.
- **Zaznamenávanie udalostí a monitorovanie**
  - Implementácia centrálneho Log manažment systému pre zber a ukladanie logov z jednotlivých informačných systémov;
  - implementácia centrálneho nástroja na zaznamenávanie činností sietí a informačných systémov a používateľov a identifikovanie bezpečnostných incidentov (SIEM);
  - implementácia automatizovaných systémov vykonávajúcich dohľad pred neoprávnenými zásahmi, neautorizovaným prístupom, najmä pred zmenami a zničením a návrh adekvátnych opatrení na ukladanie záznamov a systému logovania.
- **Riešenie kybernetických bezpečnostných incidentov**
  - Obstaranie nástroja na monitorovania a analyzovania udalostí v sieťach a informačných systémoch vrátane detekcie, zberu relevantných informácií, vyhodnocovania a riešenia zistených kybernetických bezpečnostných incidentoch a vykonávania napr. forenzných analýz v snahe minimalizovať výskyt a dopad kybernetických bezpečnostných incidentov;
  - implementácia nástroja na detekciu, nástroja na zber a nepretržité vyhodnocovanie a evidenciu kybernetických bezpečnostných udalostí.

Prvá aktivita - Bezpečnosť siete a XDR

Uvedené oblasti plánuje Žiadateľ zabezpečiť XDR systémom spolu s Log managementom, SIEM a SOAR s perpetuálnou licenciu pre dlhodobú udržateľnosť a súlad s oprávnenosťou výdavkov v rámci výzvy spolu s 4 x HW sonda a min. 50 virtuálnych senzorov/sond, výmenou 4 zastaralých a bez podpory FW a Switchov, implementáciou 2FA pre potreby VPN prístupu a celkovo autentifikácie, VPN koncentrátora pre vzdialený prístup a potrebné prepojenia do infraštruktúry a pre sprístupnenie systémov Žiadateľa prevádzkovaného na NG FW a to pre celú organizáciu a infraštruktúru Žiadateľa. Jednotlivé položky korešpondujúce s výdavkami v rozpočte sú nasledovné.

- Riešenie bezpečnosti siete - SW riešenie podporujúce funkcie XDR, NDR, LOGMANAŽMENT, SIEM, SOAR, 50 virtual sensor/sonda - perpetuálna licencia
- Data Collector (server)
- 2 x HW sonda 1 Gbps

- 2 x HW sonda 512 Mbps
- Implementácia a zaškolenie XDR, NDR, LOGMANAŽMENT, SIEM, SOAR
- Core switche 4ks – náhrada za 3850
- NG Firewall 4ks s vpn (pocet VPN 1000)
- Implementácia VPN a multifaktor 2FA - Inštalačné a konfiguračné aktivity v zmysle opisu predmetu
- Implementácia segmentácie na nových SW a implementácia 802.1x - Inštalačné a konfiguračné aktivity v zmysle opisu predmetu

3.2.1.2Druhá skupina oblastí z vysokým nesúladom na základe auditu, ktoré sú v súlade s podmienkami výzvy

- **Kontinuita prevádzky**
  - Obstaranie nástroja na zabezpečenie kontinuity prevádzky a zabezpečenia testov plánov kontinuity prevádzky v reálnom prostredí organizácie a zapracovanie nedostatkov z výsledkov testovania; implementácia systému zálohovania.
  - implementácia systému zálohovania.

Druhá aktivita – Kontinuita prevádzky

Uvedenú oblasť plánuje žiadateľ zabezpečiť obstaraním rozšírenia existujúceho diskového poľa, pridaním nového diskového poľa, každé v inej lokalite, primárna a sekundárna a využije sa funkcia replikácie dát medzi poľami, vďaka čomu sa zabezpečí schopnosť rýchlej synchronizácie a aj možnosť presunu virtuálnych serverov medzi lokalitami a zabezpečí sa tak vyššia dostupnosť virtuálnych diskov pre hypervisor, obstaraním dvoch zálohovacích serverov s nasadením nástrojov na zálohovanie, uloženie záloh a obnovy záloh v kombinácií s zvýšením bezpečnostných opatrení v oblastí zálohovania a kontinuity prevádzky, obstaraním dvoch páskových knižníc na dlhodobú archiváciu dát, cold backup. Všetky prvky sú zdvojené vzhľadom na využitie primárnej a sekundárnej lokality, ktoré sú aktuálne obe využívané na prevádzku IS.

- Rozšírením existujúceho diskového poľa a pridaním nového diskového poľa s celkovou použiteľnou kapacitou 100 TB
- Prepojením týchto dvoch polí, každé v inej lokalite, primárna a sekundárna a využitie funkcie replikácie dát medzi poľami, vďaka čomu sa zabezpečí schopnosť rýchlej synchronizácie a aj možnosť presunu virtuálnych serverov medzi lokalitami a zabezpečí sa tak vyššia dostupnosť virtuálnych diskov pre hypervisor.
- Implementácia 2 x backup server, každý pre jednu z lokalít, primárnu a sekundárnu.
- Backup a restore systém bude obsahovať nástroj na kontrolu záloh, na prítomnosť škodlivého kódu, aj na úrovni diskového poľa, vrátane natívnej integrácia s používanými technológiami a ochranou proti ransomware.
- Implementácia 2x pásková knižnica, každá pre jednu z lokalít, primárnu a sekundárnu pre ďalší stupeň zálohovania v podobe dlhodobej archivácie, cold backup.
- Implementácia procesov zálohovania na obnovu siete a informačných systémov, vrátane pravidelného testovania obnovy záloh

Aktivity pre naplnenie tejto aktivity

- Analýza existujúcich systémov z pohľadu business continuity, disaster continuity, definovanie recovery point objective (RPO), recovery time objective (RTO) a zálohovacej politiky
- Implementácia HW, SW nástrojov pre zabezpečenie definovanej zálohovacej politiky, replikácie záloh medzi dátovými centrami, procesov obnovy:
- Nasadenie a testovanie implementovanej zálohovacej politiky, vrátane obnovy informačných systémov

Realizáciou tejto aktivity bude zabezpečená kontinuita prevádzka a testov plánov kontinuity prevádzky v reálnom prostredí organizácie a zapracovanie nedostatkov z výsledkov testovania.

3.2.1.3Tretia skupina oblastí z vysokým nesúladom na základe auditu, ktoré sú v súlade s podmienkami výzvy

- **Riadenie rizík**
  - Implementáciu centrálneho systému pre identifikáciu a inventarizáciu aktív, podľa ich hodnoty vrátane určenia ich vlastníka, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu.

- **Bezpečnosť pri prevádzke informačných systémov a sietí**
    - Implementácia technických riešení podporujúcich riadenie bezpečnosti pri prevádzke, napr. nástroj pre riadenie, evidenciu a schvaľovanie zmien, evidenciu bezpečnostných incidentov, konfiguračný manažment bezpečnostných nastavení;

Tretia aktivita – Riadenie rizík a konfiguračný manažment IT aktív

Prvú oblasť plánuje Žiadateľ zabezpečiť implementáciou SW nástroja na analýzu rizík a teda na manažment zraniteľností kybernetickej bezpečnosti a riadenie záplat a aktualizácií za účelom zabezpečiť konzistentné nasadzovanie potrebných softvérových opráv a aktualizácií. Druhú oblasť plánuje Žiadateľ zabezpečiť updatom existujúceho (Open Source CMDB) nástroja pre manažment konfigurácií počítačových sietí a IT aktív, zoznam ich vlastníkov/správcov, vzájomných väzieb, súvisiacej dokumentácie a zoznam a opis prostredí, v ktorom sú aktíva umiestnené a prevádzkované, tzv. CMDB, ktorý upgradne a rozšíri o procesy a odporúčania vychádzajúce z ITILv4 a tak, aby boli v súlade s požiadavkami výzvy. Jednotlivé položky korešpondujúce s výdavkami v rozpočte sú nasledovné.

- Update a upgrade CMDB (existujúce neaktualizované riešenie) v zmysle ITILv4 procesov a odporúčaní - VM bude bežať na Management serveri uvedenom v aktivite 4 Riadenie prístupov a podporný monitoring, update sa predpokladá ideálne na najnovšiu stabilnú verziu a v prípade upgrade plánujeme využiť dostupné rozšírenia
- SW na analýzu a riadenie rizík - inštalácia bude v rámci VM bežiacej na Management serveri uvedenom v aktivite 4 Riadenie prístupov a podporný monitoring
- Implementácia SW na analýzu rizík - Inštalačné a konfiguračné aktivity v zmysle opisu predmetu

3.2.1.4Štvrtá skupina oblastí z vysokým nesúladom na základe auditu, ktoré sú v súlade s podmienkami výzvy

- **Riadenie prístupov**
    - zavedenie, implementácia alebo aktualizácia centrálneho nástroja na správu a overovanie identity, nástroja na riadenie prístupových oprávnení vrátane privilegovaných prístupových práv a kontroly prístupových účtov a prístupových oprávnení;

Štvrtá aktivita - Riadenie prístupov a podporný management

Uvedenú oblasť plánuje Žiadateľ zabezpečiť implementáciou AD s vysokou dostupnosťou v podobe 3 x server, 1 x server pre management a podporný monitoring, virtualizačná platforma VMware vSphere Standard 8 pre synergický efekt z už existujúcou pôvodnou technologickou infraštruktúrou žiadateľa v rozsahu počtu fyzických jadier tzv. Core. Jednotlivé položky korešpondujúce s výdavkami v rozpočte sú nasledovné.

- VMWARE licecnie - VMware vSphere Standard 8, 256 cores - licencie na každý zo štyroch serverov počte 2 x CPU slot x počet fyzických jadier. Virtualizačná platforma pre dosiahnutie synergického efektu s existujúcou infraštruktúrou, požiadavkami na technologickú architektúru Žiadateľa a aj vzhľadom na ostatné aktivity v rámci hlavných aktivít projektu.
- Server pre AD 3x - servery pre riadenie prístupov v zapojení a konfiguráciou s vysokou dostupnosťou, virtualizačná platformu pre dosiahnutie synergického efektu s existujúcou infraštruktúrou, požiadavkami na technologickú architektúru Žiadateľa a aj vzhľadom na ostatné aktivity v rámci hlavných aktivít projektu. (vystavané servery budú využité v zmysle zvýšenia úrovne informačnej a kybernetickej bezpečnosti aj pre ďalšie bežné aktivity počas a po ukončení projektu v období udržateľnosti)
- Management server 1x server pre management, správu a riadenie rizík a prevádzky a podporný monitoring, virtualizačná platforma pre dosiahnutie synergického efektu s existujúcou infraštruktúrou, požiadavkami na technologickú architektúru Žiadateľa a aj vzhľadom na ostatné aktivity v rámci hlavných aktivít projektu. (vystavaný server bude využitý v zmysle zvýšenia úrovne informačnej a kybernetickej bezpečnosti aj pre ďalšie bežné aktivity počas a po ukončení projektu v období udržateľnosti)
- Implementácia riešenia - Inštalačné a konfiguračné aktivity v zmysle opisu predmetu

3.2.2Súlad projektu

Táto kapitola predstavuje súhrn opatrení, ktoré sú detailnejšie vysvetlené v kapitole 3.2.1 a jedná sa o zhrnutie k akým opatreniam a cieľom PSK a NKIVS projekt prispieva. Uvedené je v zmysle výzvy povinné, keďže predpisuje konkrétny špecifický cieľ a opatrenie a pre naplnenie súladu s podmienkami výzvy, konkrétne bod 2 Podmienka splnenie kritérií pre výber projektov – vylučujúce kritéria, uvedené v prílohe č. 8 Výzvy „Minimálne náležitosti

manažérskych produktov“ a zároveň pre preukázanie súladu podmienky výzvy č. 3 Podmienka oprávnenosti aktivít projektu, konkrétne súlad s predpísaným typom akcie a hlavnej aktivity.

Predkladaný projekt je v súlade s Chartou základných práv EÚ, zabezpečuje a presadzuje rodovú rovnosť, nediskrimináciu a prístupnosť pre osoby so zdravotným postihnutím, konkrétne: - navrhovaný projekt zabezpečuje dodržiavanie základných práv a súlad s Chartou základných práv EÚ, - v navrhovanom projekte je zohľadňovaná a presadzovaná rovnosť mužov a žien, uplatňuje a začleňuje sa hľadisko rodovej rovnosti, - v navrhovanom projekte sú prijaté opatrenia na zabránenie akejkoľvek diskriminácie, - navrhovaný projekt zabezpečuje a zohľadňuje prístupnosť pre osoby so zdravotným postihnutím.

Projektom realizované aktivity prispievajú k cieľom a aktivitám intervenčnej stratégie programu Slovensko 2021 – 2027

v nasledovných oblastiach:

- **Súlad projektu so špecifickým cieľom: RSO1.2 (opatrenie 1.2.1),**
- **Súlad s očakávanými výsledkami definovanými v Partnerskej dohode pre špecifický cieľ RSO 1.2,**
- **súlad s definovanými typmi oprávnených aktivít v rámci výzvy.**

Konkrétne:

1.2.1 Podpora v oblasti informatizácie a digitálnej transformácie (Kybernetická a informačná bezpečnosť):

- **Zlepšovanie technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti KIB v prostredí orgánov štátnej a verejnej správy**
- **podporu včasnej detekcie a zvýšenie schopnosti reakcie na kybernetické bezpečnostné incidenty a na adaptáciu najmodernejších technológií, na zvýšenie odolnosti základných služieb pred kybernetickými hrozbami, vrátane podpory inovatívnych produktov a služieb až po úroveň TRL 9**

V rámci oprávneného typu akcie je oprávnená nasledovná **hlavná aktivita:**

- **Zvýšenie úrovne informačnej a kybernetickej bezpečnosti prostredníctvom nákupu hardvéru a bezpečnostného softvéru**

Predkladaný projektu je v súlade s platnou Národnou koncepciou informatizácie verejnej správy Slovenskej republiky (ďalej ako „NKIVS“) a to konkrétne v **prioritnej osi 4 Kybernetická a informačná bezpečnosť** a čiastkovým cieľom **Zvýšenie schopnosti včasnej identifikácie kybernetických incidentov vo verejnej správe**.

Projektom navrhované výdavky projektu spĺňajú všetky podmienky oprávnenosti definované vo výzve v časti upravujúcej oblasť oprávnenosti výdavkov (vecná oprávnenosť a účelnosť výdavkov, hospodárnosť a efektívnosť výdavkov, územná oprávnenosť výdavkov, časová oprávnenosť výdavkov a pod.). Uvedené je podložené vypracovaným dokumentom **I_02_BC_CBA_PRILOHA ktorá obsahuje aj rozpočet a TCO**. Nepriame výdavky na podporné aktivít **nepresahujú 7 %** z celkových priamych výdavkov v zmysle výzvy. **Žiadateľom predložený rozpočet v najlepšej možnej miere reflektuje požiadavky definované projektom a jeho hlavnými a podpornými aktivitami a skutočná výška nákladov bude výsledkom úspešného Verejného obstarávania.**

Projektom predložené dopady a miery rizík obsiahnuté v prílohe P_01_a_I_01_a_M_02_1_PRILOHA_1_REGISTER_RIZIK-a-ZAVISLOSTI **nepresahujú pre riziká s vysokou závažnosťou hranicu 50 %.** V rámci projektu bolo identifikovaných s vysokou závažnosťou, ktoré ohrozujú úspešnú realizáciu projektu **menej ako 10 % rizík** z celkového počtu identifikovaných rizík.

Žiadateľ v rámci projektu **disponuje** (v súlade s podmienkami výzvy) dostatočnými odbornými kapacitami s náležitou odbornou spôsobilosťou a know-how na riadenie a implementáciu projektu v danej oblasti.

3.2.3Zabezpečenie základných činností v oblasti kybernetickej a informačnej bezpečnosti v organizácii žiadateľa

Žiadateľ v rámci projektu plánuje zabezpečiť:

- **Implementácia nástrojov pre zavedenie zálohovania na obnovu siete a informačného systému vrátane pravidelného testovania obnovy záloh – Aktivita Kontinuita prevádzky**, aktivitu plánuje Žiadateľ zabezpečiť obstaraním rozšírenia existujúceho diskového poľa, pridaním nového diskového poľa, každé v inej lokalite, primárna a sekundárna a využije sa funkcia replikácie dát medzi poľami, vďaka čomu sa zabezpečí schopnosť rýchlej synchronizácie a aj možnosť presunu virtuálnych serverov medzi lokalitami a zabezpečí sa tak vyššia dostupnosť virtuálnych diskov pre hypervisor, obstaraním dvoch zálohovacích serverov s nasadením nástrojov na zálohovanie, uloženie záloh a obnovy záloh v kombinácií s zvýšením bezpečnostných opatrení v oblastí zálohovania a kontinuity prevádzky, obstaraním dvoch páskových knižníc na dlhodobú archiváciu dát, cold backup. Všetky prvky sú zdvojené vzhľadom na využitie primárnej a sekundárnej lokality, ktoré sú aktuálne obe využívané na prevádzku IS. Zároveň **Aktivita Bezpečnosť siete a XDR**, kde sa plánujú NG FW a Switche v HA módoch pre zabezpečenie vysokej dostupnosti a zabezpečenie proti výpadkom jednotlivých nodov.
- **Implementácia nástrojov pre manažment konfigurácií počítačových sietí a IT aktív, zoznam ich vlastníkov/správcov, vzájomných väzieb, súvisiacej dokumentácie a zoznam a opis prostredí, v ktorom sú aktíva umiestnené a prevádzkované (tzv. CMDB), ktorý sa viaže na inventarizáciu IT aktív – Aktivita Riadenie rizík a konfiguračný manažment IT aktív**, kde sa plánuje update existujúceho (Open Source CMDB) nástroja pre manažment konfigurácií počítačových sietí a IT aktív, ktorý sa upgradne a rozšíri o procesy a odporúčania vychádzajúce z ITILv4.
- **Implementácia nástrojov na manažment zraniteľností kybernetickej bezpečnosti a riadenie záplat a aktualizácií za účelom zabezpečiť konzistentné nasadzovanie potrebných softvérových opráv a aktualizácií – Aktivita Riadenie rizík a konfiguračný manažment IT aktív**, kde sa plánuje implementácia SW nástroja na analýzu rizík a teda spomínaný manažment zraniteľností kybernetickej bezpečnosti a riadenie záplat a aktualizácií

3.2.3Zabezpečenie vybraných činností zameraných na prevenciu pred kybernetickými bezpečnostnými incidentmi v organizácii žiadateľa

Žiadateľ v rámci projektu plánuje zabezpečiť:

- **Implementáciu nástrojov pre zavedenie viacfaktorovej autentifikácie – Aktivita Bezpečnosť siete a XDR**, kde s plánuje zavedenie dvojfaktorovej (2FA) autentifikácie pre VPN prístup, konkrétne výmenou 4 zastaralých a bez podpory FW a Switchov, implementáciou 2FA pre potreby VPN prístupu a celkovo autentifikácie, VPN koncentrátora pre vzdialený prístup a potrebné prepojenia do infraštruktúry a pre sprístupnenie systémov Žiadateľa prevádzkovaného na NG FW a to pre celú organizáciu a infraštruktúru Žiadateľa.
- **Implementácia nástrojov, ktorých cieľom je zvýšiť schopnosť detekcie škodlivých aktivít a bezpečnostných incidentov, resp. ochrana koncových bodov, dát, dátových prenosov a sieťovej komunikácie, alebo ktorých cieľom je zvýšenie ochrany pred kybernetickými útokmi z externého prostredia - Aktivita Bezpečnosť siete a XDR**, kde sa plánuje implementovať XDR systém spolu s Log managementom, SIEM a SOAR s perpetuálnou licenciu pre dlhodobú udržateľnosť a súlad s oprávnenosťou výdavkov v rámci výzvy spolu s 4 x HW sonda a min. 50 virtuálnych senzorov/sond, výmenou 4 zastaralých a bez podpory FW a Switchov, implementáciou 2FA pre potreby VPN prístupu, VPN koncentrátora pre vzdialený prístup a potrebné prepojenia do infraštruktúry a pre sprístupnenie systémov Žiadateľa prevádzkovaného na NG FW a to pre celú organizáciu a infraštruktúru Žiadateľa.

3.3Zainteresované strany/Stakeholderi

- *Doplňte KTO (zoznam subjektov/osôb) sa zúčastňuje projektu a akú rolu zastáva*

ID	AKTÉR / STAKEHOLDER	SUBJEKT (názov / skratka)	ROLA (vlastník procesu/ vlastník dát/zákazník/ užívateľ .... člen tímu atď.)	Informačný systém (MetaIS kód a názov ISVS)
1.	Ministerstvo kultúry Slovenskej republiky	MKSR	Prevádzkovateľ IS, užívateľ IS, Vlastník procesov, Vlastník dát	isvs_331 IS CAIR, isvs_365 Dotačný systém MK SR, isvs_333 CEMUZ, isvs_367 Centrálny jednotný ekonomický systém SOFTIP

			PROFIT, isvs_372 Informačný systém MK SR, isvs_361 Elektronický systém štatistického zisťovania KULT, množstvo webových sídel uvedených v METAIS,
2.	Zamestnanec	Člen tímu, užívateľ	isvs_331 IS CAIR, isvs_365 Dotačný systém MK SR, isvs_333 CEMUZ, isvs_367 Centrálny jednotný ekonomický systém SOFTIP PROFIT, isvs_372 Informačný systém MK SR, isvs_361 Elektronický systém štatistického zisťovania KULT, množstvo webových sídel uvedených v METAIS,
3.	Občan	Užívateľ	množstvo webových sídel uvedených v METAIS
5.	Podnikateľ	Užívateľ	množstvo webových sídel uvedených v METAIS
6.	Národný bezpečnostný úrad NBÚ		

3.4Ciele projektu

Do tabuliek nižšie doplniť CIEĽ /CIELE 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
1.	Zvýšenie úrovne informačnej a kybernetickej bezpečnosti	Zvýšenie schopnosti včasnej identifikácie kybernetických incidentov vo verejnej správe	Implementácia projektom navrhovaných aktivít

3.5Merateľné ukazovatele (KPI)

Merateľné ukazovatele vychádzajú z podmienok výzvy č. PSK-MIRRI-616-2024-DV-EFRR a jej prílohy č. 4.

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.
1.	1. - Zvýšenie úrovne	Verejné inštitúcie	Počet verejných	verejné inštitúcie	0	1	Overenie stavu	Spadá pod oprávnenú

	informačnej a kybernetickej bezpečnosti	podporované v rozvoji kybernetických služieb, produktov a procesov (PO095 / PSKPSOI12)	inštitúcií, ktoré sú podporované za účelom rozvoja a modernizácie kybernetických služieb, produktov, procesov a zvyšovania vedomostnej úrovne napríklad v kontexte opatrení smerujúcich k elektronickej bezpečnosti verejnej správy				hodnoty ku koncu realizácie hlavných aktivít projektu	aktivitu: Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti
2.	1. - Zvýšenie úrovne informačnej a kybernetickej bezpečnosti	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov (PR017 / PSKPRCR11)	Počet užívateľov nových a vylepšených verejných digitálnych služieb, produktov a procesov	používatelia / rok	0	1 400 (počet užívateľov registratúry, 350 MKSR, zvyšok 1 050 rezort s podriadenými organizáciam, aj neumelecký pracovníc v administratívei)	Kontinuálne overovanie v rámci udržateľnosti projektu	Spadá pod oprávnenú aktivitu: Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti

3.6Špecifikácia potrieb koncového používateľa

Výstupy a ciele projektu nie sú zamerané na priamy vývoj nových alebo rozvoj existujúcich ISVS/s, alebo elektronických služieb, ktoré majú grafické alebo iné používateľské rozhranie a sú určené pre občanov/ podnikateľov (alebo aj pracovníkov verejnej správy pracujúcich s agendovým systémom), ďalej označených ako koncoví používatelia a je zameraný na zvýšenie úrovne kybernetickej bezpečnosti v rámci organizácie Žiadateľa.

3.7Riziká a závislosti

Projektom predložené dopady a miery rizík obsiahnuté v prílohe P_01_a_I_01_a_M_02_1_PRILOHA_1_REGISTER_RIZIK-a-ZAVISLOSTI **nepresahujú pre riziká s vysokou závažnosťou hranicu 50 %.** V rámci projektu bolo identifikovaných s vysokou závažnosťou, ktoré ohrozujú úspešnú realizáciu projektu **menej ako 10 % rizík** z celkového počtu identifikovaných rizík.

Detailný popis rizík a závislostí sú v priloženej prílohe P_01_a_I_01_a_M_02_1_PRILOHA_1_REGISTER_RIZIK-a-ZAVISLOSTI.

3.8Stanovenie alternatív v biznisovej vrstve architektúry

Alternatíva 1:

Biznis alternatíva 1 predstavuje ponechanie existujúceho stavu informačnej a kybernetickej bezpečnosti Žiadateľa a nevýhodou je ponechanie stavu, konkrétne:

- **Nesúlad voči zákonu č. 69/2018 Z. z -** Výsledky z auditu kybernetickej bezpečnosti preukázali veľké nedostatky a to najmä v oblastiach uvedených nižšie. Žiadateľ je povinný vykonať opatrenia, ktoré mu ukladá zákon.
- **Nedostatková oblasť Sieťová a komunikačná bezpečnosť -** Žiadateľ aktuálne využíva bezpečnostné prvky ako Firewall 4 ks a sieťové switche 4ks dlho po dobe životnosti, bez oficiálnej podpory výrobcu a s už dlhdoobo známimi bezpečnostnými zraniteľnosťami, na ktoré už výrobca neposkytuje bezpečnostnú aktualizáciu. Zároveň v rámci infraštruktúry absentuje aktívna forma kontroly a systém, ktorý by dokázal včas upozorniť Žiadateľa o možnom probléme alebo útoku. Jedná sa o veľmi vysoké riziko a veľmi závažným dopadom.
- **Nedostatková oblasť Zaznamenávanie udalostí a monitorovanie -** Žiadateľ nemá centrálny systém zaznamenávania logov a nemá možnosť získavať plošné oznámenia o stave infraštruktúry. Existujú čiastkové riešenia v zmysle jednotlivých projektov, avšak v prípade kybernetického incidentu by bolo veľmi náročné dohľadávať informácie a následne ich analyzovať.
- **Nedostatková oblasť Kontinuita prevádzky -** Žiadateľ disponuje čiastkovým riešením zálohovania avšak ten nepostačuje na komplexné zabezpečenie kontinuity prevádzky. Nie je zabezpečený komplexný a jednotný systém zálohovania, obnovy a testovania týchto procesov. V prípade rozsiahleho ransomware útoku nie je možné garantovať obnovu všetkých dát a ani kontrolu integrity všetkých obnovených dát.
- **Nedostatková oblasť Riešenie kybernetických bezpečnostných incidentov -** Žiadateľ nemá zabezpečenú oblasť riadenia a správy kybenretických incidentov čo okrem iného z dhodobého hľadiska predstavuje veľké riziko nevhodného pristupovania počas a po kybernetickom útoku a zamedzuje tak vhodne pristúpiť k riešeniu kritickej situácií.
- **Nedostatková oblasť Riadenie rizík -** Žiadateľ nemá zabezpečenú oblasť riadenia a správy rízík a zraniteľností, ako aj správu aktív a z toho vyplývajúcich problémov. Žiadateľ nemá zabezpečenú možnosť dostatočne včas preventívne reagovať na možné riziká a zraniteľnosti a zamedziť tak skutočnému potenciálnemu kybernetickému incidentu.
- **Nedostatková oblasť Bezpečnosť pri prevádzke informačných systémov a sietí -** Žiadateľ nemá zabezpečenú oblasť správy prevádzky informačných systémov do takej miery, aby bolo možné efektívne využívať moderné systémy na správu infraštruktúrneho vybavenia, konfigurácií, dokumentácií a znalostných databáz a zabezpečiť tak best practice pri prevádzke informačných systémov.
- **Nedostatková oblasť Riadenie prístupov -** Žiadateľ nema zavedený komplexný systém riadenia prístupov, ktorý by vedel zabezpečiť dodržiavanie oprávnení v zmysle požiadaviek na jednmotlivé systémy. Existujúce formy riadenia sú prevažne lokálneho charakteru bez možnosti centrálnej správy a yeda aj centrálneho sledovania. Vzhľadom na potreby Žiadateľa sa jedná o veľký nedostatok zabezpečiť bezpečný efektívny prístup k dátam a systémom pre tých ktorý ho v čase potrebujú bez ohrozenia všeobecnej bezpečnosti daných dát a systémov.

Výhodou alternatívy je žiadny náklad na preventívne opatrenia a zamedzovaniu kybernetickým incidentom.

Alternatíva 2:

Biznis alternatíva 2 predstavuje implementáciu všetkých projektom navrhovaných aktivít:

- **Prvá aktivita – Bezpečnosť siete a XDR**
- **Druhá aktivita – Kontinuita prevádzky**
- **Tretia aktivita – Riadenie rizík a konfiguračný manažment IT aktív**
- **Štvrtá aktivita - Riadenie prístupov a podporný management**

Pre pokrytie všetkých nedostatkových oblastí:

- **Sieťová a komunikačná bezpečnosť**
- **Zaznamenávanie udalostí a monitorovanie**
- **Riešenie kybernetických bezpečnostných incidentov**
- **Kontinuita prevádzky**
- **Riadenie rizík**
- **Bezpečnosť pri prevádzke informačných systémov a sietí**
- **Riadenie prístupov**

Výhodou alternatívy je väčšie percento splnenia súladu voči zákonu č. 69/2018 Z. z, ako aj zabezpečenie vyššej miery kybernetickej bezpečnosti oproti aktuálnemu stavu, zavedenie nových systémov na ochranu voči kybernetickým útokom, možnosť obnovy dát, zníženie času výpadku systémov znížením času obnovenia prevádzky a zabezpečenia tak kontinuity prevádzky, včas a adekvátne reagovať na kritické situácie, podporenie bezpečnosti

a prevádzky informačných systémov, podporenie správy znalostnej databázy a správy konfigurácie a riadenie rizík, riadenie prístupov a zabezpečenie prístupu k systémom a dátam pre tých ktorý ho v čase potrebujú bez ohrozenia všeobecnej bezpečnosti.

Nevýhodou alternatívy je vyššia obstarávacia cena a následná cena prevádzky ako pre alternatívu 3, potreba zvýšenia kvalifikácie IT technických zamestnancov a potreba zavedenia nových bezpečnostných štandardov do procesov a pracovného výkonu.

Alternatíva 3:

Biznis alternatíva 3 predstavuje implementáciu podmnožiny projektom navrhovaných aktivít:

- **Druhá aktivita – Kontinuita prevádzky**
- **Tretia aktivita – Riadenie rizík a konfiguračný manažment IT aktív**

pre pokrytie vybraných nedostatkových oblastí:

- **Kontinuita prevádzky**
- **Riadenie rizík**
- **Bezpečnosť pri prevádzke informačných systémov a sietí**

Výhodou alternatívy je navýšenie percenta splnenia súladu voči zákonu č. 69/2018 Z. z, ako aj zabezpečenie vyššej miery kybernetickej bezpečnosti oproti aktuálnemu stavu, podporenie bezpečnosti a prevádzky informačných systémov, podporenie správy znalostnej databázy a správy konfigurácie a riadenie rizík, riadenie prístupov a zabezpečenie prístupu k systémom a dátam pre tých ktorý ho v čase potrebujú bez ohrozenia všeobecnej bezpečnosti. a nižšia obstarávacie a prevádzkové náklady oproti alternatíve 2.

Nevýhodou alternatívy je obstarávacia cena a následná cena prevádzky, potreba zvýšenia kvalifikácie IT technických zamestnancov a potreba zavedenia nových bezpečnostných štandardov do procesov a pracovného výkonu.

3.9Multikriteriálna analýza

Spracovanie MCA:

	KRITÉRIUM	ZDÔVODNENIE KRIÉRIA	Žiadateľ	Zamestnanec	Občan/Podnikateľ
BIZNIS VRSTVA	Zvýšiť percento súladu a odstrániť tak niektoré najkritickejšie zistenia a zabezpečiť systémy Žiadateľa s povinnosťami vyplývajúcimi zo zákona č.69/2018 Z.z A (KO)	Ministerstvo kultúry Slovenskej republiky, Nám. SNP č. 33, 813 31 Bratislava – Staré Mesto (ďalej len „MKSR") je zapísané do registra prevádzkovateľov základnej služby	X	X	
	Súlad s výzvou a jej podmienkami a najmä výška NFP B (KO)	Projekt je v súlade s výzvou a nie je možné v prípade ŽoNFP nespĺňať jej stanovené kritéria pre úspešné získanie NFP	X	X	
	Zvýšenie úrovne informačnej a kybernetickej bezpečnosti C (KO)	Jedná sa o hlavný sieľ projektu na ktorý sú nmapované jho merateľné ukazovatele	X	X	X

	a všetky aktivity projektu			
Zabezpečiť oblasť Sieťová a komunikačná bezpečnosť D	Jedná sa o oblasť s vysokým nesúladom predstavujúcu vážne bezpečnostné riziko	X	X	X
Zabezpečiť oblasť Zaznamenávanie udalostí a monitorovanie E	Jedná sa o oblasť s vysokým nesúladom predstavujúcu vážne bezpečnostné riziko	X	X	
Zabezpečiť oblasť Kontinuita prevádzky F	Jedná sa o oblasť s vysokým nesúladom predstavujúcu vážne bezpečnostné riziko	X	X	X
Zabezpečiť oblasť Riešenie kybernetických bezpečnostných incidentov G	Jedná sa o oblasť s vysokým nesúladom predstavujúcu vážne bezpečnostné riziko	X	X	X
Zabezpečiť oblasť Riadenie rizík H	Jedná sa o oblasť s vysokým nesúladom predstavujúcu vážne bezpečnostné riziko	X	X	
Zabezpečiť oblasť Bezpečnosť pri prevádzke informačných systémov a sietí I	Jedná sa o oblasť s vysokým nesúladom predstavujúcu vážne bezpečnostné riziko	X	X	
Zabezpečiť oblasť Riadenie prístupov J	Jedná sa o oblasť s vysokým nesúladom predstavujúcu vážne bezpečnostné riziko	X	X	
Nezvyšovať nároky na kvalifikáciu IT technických zamestnancov K	Nutnosť navýšenia znalostí pre obsluhu nových IS a HW	X	X	
Neovplyvňovať a nezasahovať do pracovných návykov a procesov zamestnancov Žiadateľa L	Ovplyvnenie výkonu práce, zvýšenie bezpečnostných opatrení často spôsobuje zníženie efektivity a nutnosť postupovať podľa určených postupov a predpisov	X	X	

Vyhodnotenie MCA:

Zoznam kritérií	Alternatíva 1	Spôsob dosiahnutia	Alternatíva 2	Spôsob dosiahnutia	Alternatíva 3	Spôsob dosiahnutia

Kritérium A	Nie	Nedosahuje	Áno	Zvýši sa percento súladu a odstránia sa niektoré kritické nedostatky z auditu v zmysle zákona č.69/2018 Z.z	Áno	Zvýši sa percento súladu a odstránia sa niektoré kritické nedostatky z auditu v zmysle zákona č.69/2018 Z.z
Kritérium B	Áno	Nie je v rozpore sa nezapojiť do výzvy	Áno	Je v súlade s podmienkami výzvy	Áno	Je v súlade s podmienkami výzvy
Kritérium C	Nie	Nedosahuje	Áno	Úroven informačnej a kybernetickej bezpečnosti sa zvýši	Áno	Úroven informačnej a kybernetickej bezpečnosti sa zvýši
Kritérium D	Nie	Nedosahuje	Áno	Implementácia aktivity Bezpečnosť siete a XDR	Nie	Nedosahuje
Kritérium E	Nie	Nedosahuje	Áno	Implementácia aktivity Bezpečnosť siete a XDR	Nie	Nedosahuje
Kritérium F	Nie	Nedosahuje	Áno	Implementácia aktivity Kontinuita prevádzky	Nie	Nedosahuje
Kritérium G	Nie	Nedosahuje	Áno	Implementácia aktivity Bezpečnosť siete a XDR	Nie	Nedosahuje
Kritérium H	Nie	Nedosahuje	Áno	Implementácia aktivity Riadenie rizík a konfiguračný manažment IT aktív	Áno	Implementácia aktivity Riadenie rizík a konfiguračný manažment IT aktív
Kritérium I	Nie	Nedosahuje	Áno	Implementácia aktivity Riadenie rizík a konfiguračný manažment IT aktív	Áno	Implementácia aktivity Riadenie rizík a konfiguračný manažment IT aktív
Kritérium J	Nie	Nedosahuje	Áno	Implementácia aktivity Riadenie prístupov a podporný management	Áno	Implementácia aktivity Riadenie prístupov a podporný management
Kritérium K	Áno	Nie je potrebné zvyšovať kvalifikáciu, ostáva aktuálny stav	Nie	Nedosahuje	Nie	Nedosahuje
Kritérium L	Áno	Nie je potrebné meniť návyky a zavádzať nové bezpečnostné opatrenia a procesy, ostáva aktuálny stav	Nie	Nedosahuje	Nie	Nedosahuje

Prostredníctvom MCA zostavenej na základe kapitoly Motivácia, ktorá obsahuje ciele stakeholderov, ich požiadavky a obmedzenia pre dosiahnutie uvedených cieľov vychádza ako **najvhodnejšia Alternatíva 2**, ktorá predstavuje implementáciu Žiadateľom navrhovaného projektu v plnom rozsahu po zohľadnení všetkých nážetostí a obmedzení daných výzvou. Aj napriek zvýšeniu nárokov na technickú kvalifikáciu, možný negaívny dopad na výkon, ako aj zvýšené prevádzkové náklady, je situáciu potrebné brať zodpovedne, venovať sa téme bezpečnosti a využiť tak možnosti financovania z výzvy na naplnenie cieľov a požiadaviek.

3.10Stanovenie alternatív v aplikačnej vrstve architektúry

V rámci biznis vrstvy vyšla na základe KO kritérií a vhodnosti jedna alternatíva a nie je nutné ju naďalej porovnávať na aplikačnej úrovni a to aj z dôvodu, že Žiadateľ sa pridržiava odporúčaniami vyplývajúcimi z auditu kybernetickej bezpečnosti. V rámci aplikačnej vrstvy Žiadateľ nepredpisuje konkrétne produkty a služby ale len popis minimálnych požiadaviek na tieto systémy a proces Verejného obstarávania zabezpečí ekonomicky najvhodnejšiu alternatívu.

3.11Stanovenie alternatív v technologickej vrstve architektúry

V rámci biznis vrstvy vyšla na základe KO kritérií a vhodnosti jedna alternatíva a nie je nutné ju naďalej porovnávať na technologickej úrovni a to aj z dôvodu, že Žiadateľ sa pridržiava odporúčaniami vyplývajúcimi z auditu kybernetickej bezpečnosti. a ich výber je vzhľadom na existujúcu infraštruktúru a technologické prostredie zvolený tak, aby zabezpečil ekonomicky najvýhodnejšie riešenia a aby bola jeho obsluha a správa zabezpečená v čo najvyššej miere internými kapacitami. V rámci novej časti technologickej vrstvy Žiadateľ nepredpisuje konkrétne produkty a služby ale len popis minimálnych požiadaviek na tieto systémy a proces Verejného obstarávania zabezpečí ekonomicky najvhodnejšiu alternatívu.

4.POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

Realizáciou projektu sa dosiahne zvýšenie úrovne informačnej a kybernetickej bezpečnosti a zabezpečia sa systémy Žiadateľa s povinnosťami vyplývajúcimi zo zákona č.69/2018 Z.z.. Realizáciou aktivít:

- **Prvá aktivita – Bezpečnosť siete a XDR**
- **Druhá aktivita – Kontinuita prevádzky**
- **Tretia aktivita – Riadenie rizík a konfiguračný manažment IT aktív**
- **Štvrtá aktivita - Riadenie prístupov a podporný management**

Sa zabezpečí:

- **Sieťová a komunikačná bezpečnosť**
- **Zaznamenávanie udalostí a monitorovanie**
- **Riešenie kybernetických bezpečnostných incidentov**
- **Kontinuita prevádzky**
- **Riadenie rizík**
- **Bezpečnosť pri prevádzke informačných systémov a sietí**
- **Riadenie prístupov**

Projekt, jeho realizácia a všetky jeho projektové výstupy budú v súlade s vyhláškou 401/2023 o riadení projektov.

ID	**Prehľad projektových výstupov**	**nad 1.000.000 EUR**
	Výstupy vytvárané PRIEBEŽNE počas celého projektu	**Projekt a zmenová požiadavka v prevádzke**
M-01	**Plán etapy/Plán fázy**	**ÁNO**
M-02	**Manažérske správy, plány, reporty, zoznamy, odporúčania a požiadavky:**	
	(1) Zoznam otvorených otázok	**ÁNO**

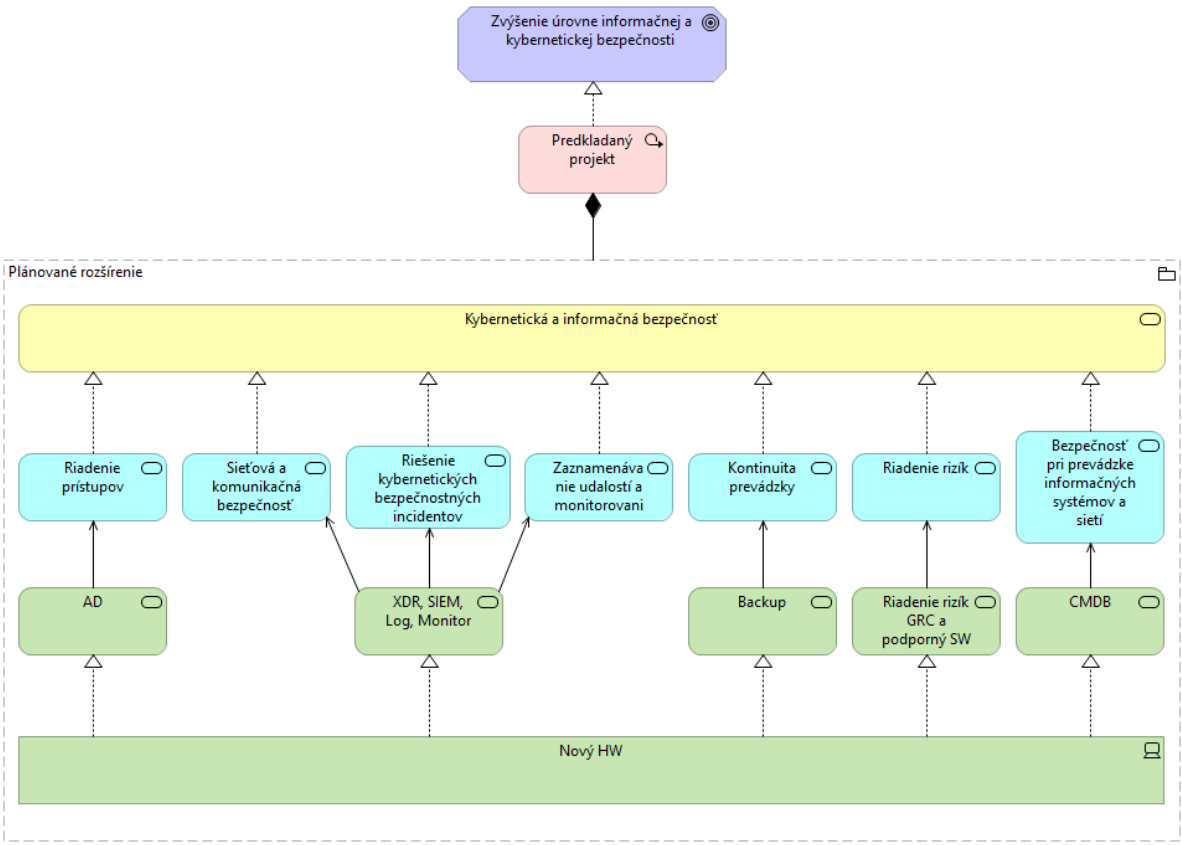
	(2) Zoznam funkčných zdrojových kódov	**ÁNO, v závislosti od technického riešenia**
	(3) Zoznam licencií	**ÁNO**
	(4) Správa o stave projektu (Status report)	**ÁNO**
	(5) Požiadavka na zmenu (CR)	**ÁNO**
M-03	**Akceptačný protokol**	**ÁNO**
M-04	**Audit kvality**	**ÁNO, v závislosti od technického riešenia**
M-05	**Analýza nákladov a prínosov**	**ÁNO**
M-06	**Evidencia e-Government komponentov v MetaIS, vrátane architektonických modelov**	**ÁNO**
	PRÍPRAVNÁ A INICIAČNÁ FÁZA	
I-01	**Ideový zámer**	**ÁNO**
I-02	**Projektový zámer**	**ÁNO**
I-03	**Prístup k projektu**	**ÁNO**
I-04	**Katalóg požiadaviek**	**ÁNO**
MÍĽNIK - ukončenie obstarávania alebo uzatvorenie zmluvy s dodávateľom		
	REALIZAČNÁ FÁZA	
R1	**ANALÝZA A DIZAJN**	
R-01	**Projektový iniciálny dokument (PID)**	**ÁNO**
	Akceptačné kritériá	**ÁNO**
R1-1	**Detailný návrh riešenia (DNR)** (1) Zámer riešenia, analýza požiadaviek, používateľský prieskum a motivačná architektúra (2) Popis postupu analýzy a návrhu riešenia (3) Biznis architektúra* a. Existujúca a cieľová biznis architektúra b. Procesy podporované navrhovaným riešením c. Vytvorenie informačnej architektúry a mapovanie používateľskej cesty d. Vytvorenie grafického návrhu a prototypu používateľského rozhrania (UX, UI) – Pre projekt nerelevantné e. Prípady použitia (use case model) (4) Dátová architektúra (5) Aplikačná architektúra* a. Existujúca a budúca aplikačná architektúra b. Aplikačné komponenty a ich vzťah k biznis komponentom a funkčným požiadavkám c. Integrácie – Komunikácia medzi komponentami (OpenAPI) (6) Technologická architektúra* a. Existujúca a budúca technologická architektúra b. Technologické komponenty riešenia a ich vzťah k aplikačným komponentom (7) Softvérové licencie a zdrojové kódy	**ÁNO, v závislosti od technického riešenia**

	(8) Požiadavky na úrovne služieb (SLA) a výkonnosť (9) Zabezpečenie dostupnosti, zálohovanie a obnova riešenia (10 Bezpečnosť – riešenie požiadaviek na bezpečnosť (11) Migrácia dát (12) Harmonogram realizácie a nasadenia, závislosti	
R1-2	**Plán a stratégia testovania**	**ÁNO**
	(1) Testovacie prípady (UC/TC) (2) Testovacie prostredia (3) Testovacie dáta (4) Defekt manažment, monitoring a reporting testov	**ÁNO, v závislosti od technického riešenia**
R2	**NÁKUP TECHNICKÝCH PROSTRIEDKOV, PROGRAMOVÝCH PROSTRIEDKOV A SLUŽIEB**	
R2-1	**Obstaranie technických prostriedkov**	**ÁNO**
R2-2	**Obstaranie programových prostriedkov a služieb**	**ÁNO**
R3	**IMPLEMENTÁCIA A TESTOVANIE**	
R3-1	**Vývoj, migrácia údajov a integrácia**	**ÁNO**
R3-2	**Testovanie**	
	(1) Funkčné testovanie (FAT)	**ÁNO**
	(2) Systémové a integračné testovanie (SIT)	**ÁNO**
	(3) Záťažové a výkonnostné testovanie	**ÁNO**
	(4) Bezpečnostné testovanie (SW/HW a kybernetická bezpečnosť)	**ÁNO**
	(5) Používateľské testy funkčného používateľského rozhrania (UX)	**ÁNO, v závislosti od technického riešenia**
	(6) Používateľské akceptačné testovanie (UAT)	**ÁNO, v závislosti od technického riešenia**
R3-3	**Školenia personálu**	**ÁNO**
R3-4	**Dokumentácia**	
	(1) Aplikačná príručka, vrátane aktualizovanej dokumentácie architektúry v rozsahu podľa položiek 3 až 10 Detailného návrhu riešenia R1-1	**ÁNO**
	(2) Integračná príručka	**ÁNO, v závislosti od technického riešenia**
	(3) Používateľská príručka	**ÁNO**
	(4) Zdrojové kódy a licencie	**ÁNO, v závislosti od technického riešenia**
	(5) Inštalačná a konfiguračná príručka	**ÁNO**
	(6) Prevádzkový opis a pokyny	**ÁNO**

	pre diagnostiku, servis a údržbu	
	(7) Pokyny na obnovu pri výpadku alebo havárii (Havarijný plán)	**ÁNO**
	(8) Bezpečnostný projekt	**ÁNO, v závislosti od technického riešenia**
	(9) Údaje o monitorovaní úrovne poskytovaných služieb (SLA) aktív IT	**ÁNO**
R4	**NASADENIE a POSTIMPLEMENTAČNÁ PODPORA (PIP)**	
R4-1	**Nasadenie do produkčnej prevádzky** (vyhodnotenie)	**ÁNO**
R4-2	**Akceptácia spustenia do produkčnej prevádzky** (vyhodnotenie)	**ÁNO**
	MÍĽNIK - UZATVORENIE Zmluvy v prevádzke (SLA zmluva)	
	DOKONČOVACIA FÁZA	
M-02	**Manažérske správy, plány, reporty, zoznamy, odporúčania a požiadavky:**	
	(1) Správa o dokončení projektu (etapy/fázy)	**ÁNO**
	(2) Plán kontroly po odovzdaní projektu	**ÁNO**
	(3) Odporúčanie nadväzných krokov	**ÁNO**
	(4) Plán monitorovania a hodnotenia po odovzdaní projektu	**ÁNO**

5.NÁHĽAD ARCHITEKTÚRY

Hlavným cieľom a teda predmetom projektu je zvýšenie úrovne kybernetickej a informačnej bezpečnosti Žiadateľa. Na nasledujúcom diagrame je znázornená High Level architektúra riešenia. Všetky bližšie detaily jednotlivých vrstiev architektúry sú dostupné v dokumente I-03 Prístup k projektu.



1. Aplikačná služba Riadenie prístupov bude priradená pod novú technologickú službu Active Directory.
2. Aplikačná služba Sieťová a komunikačná bezpečnosť, Riešenie kybernetických bezpečnostných incidentov a Zaznamenávanie udalostí a monitorovanie bude priradená pod novú technologickú službu XDR, SIEM, Log, Monitor.
3. Aplikačná služba Kontinuita prevádzky bude priradená pod novú technologickú službu Backup.
4. Aplikačná služba Riadenie rizík bude priradená pod novú technologickú službu Riadenie rizík GRC a podporný SW.
5. Aplikačná služba Bezpečnosť pri prevádzke informačných systémov a sietí bude priradená pod novo upravenú technologickú službu CMDB.
6. Všetky novo vytvorené technologické služby budú realizované na novom HW spolu s potrebným SW.
7. Všetky aplikačné služby budú spolu tvoriť novú biznis službu Kybernetickej a informačnej bezpečnosti.

Všetky bližšie detaily jednotlivých vrstiev architektúry sú dostupné v dokumente I-03 Prístup k projektu.

5.1Prehľad e-Government komponentov

Obsah kapitoly je spravovaný spracovaný v dokumente I-03 Prístup k projektu.

6.LEGISLATÍVA

V rámci predkladaného projektu a ani po jeho ukončení počas obdobia udržateľnosti sa neočakáva úprava alebo priama zmena zákona vyplývajúca z aktivít projektu a teda úspešná realizácia projektu nie je ovplyvnená žiadnymi vyžadovanými zmenami v legislatíve.

Z pohľadu predmetu projektu je dotknutá nasledovná legislatíva v rámci SR:

- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy v znení neskorších predpisov;
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;
- Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v znení neskorších predpisov;
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky 401/2023 o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 85/2020 Z. z. o riadení projektov v znení neskorších predpisov.

7.ROZPOČET A PRÍNOSY

7.1Sumarizácia nákladov a prínosov

Náklady CAPEX a OPEX na 10 rokov:

TO BE - AS IS (€, SUM)

			Spolu	Modul 1
Náklady s DPH			4 129 499 €	4 129 499 €
	Všeobecný materiál		- €	- €
	IT - CAPEX		2 450 414 €	2 450 414 €
		Aplikácie	- €	- €
		SW	73 431 €	73 431 €
		HW	2 376 983 €	2 376 983 €
	IT - OPEX		1 507 556 €	1 507 556 €
		Aplikácie	- €	- €
		SW	43 856 €	43 856 €
		HW	1 463 700 €	1 463 700 €
	Riadenie projektu		171 529 €	171 529 €
	Výstupné náklady		- €	- €
Prínosy			6 074 523 €	6 074 523 €
	Finančné prínosy		- €	- €
		Administratívne poplatky	- €	- €
		Ostatné daňové a nedaňové príjmy	- €	
	Ekonomické prínosy		6 074 523 €	6 074 523 €
		Občania (€)	- €	- €
		Úradníci (€)	- €	- €
		Úradníci (FTE)	N/A	N/A
		Kvalitatívne prínosy	6 074 523 €	6 074 523 €

Uvedený projekt nerozdelujeme na inkrementy z dôvodu, že v rámci vyhlášky 401/2023 (https://www.slov-lex.sk/ezbierky-fe/pravne-predpisy/SK/ZZ/2023/401/#paragraf-4.odsek-5.pismeno-b) sa uvádza, že „realizačné fázy viacerých inkrementov nie je možné realizovať súbežne a realizačná fáza ďalšieho inkrementu sa začína až po ukončení realizačnej fázy predchádzajúceho inkrementu“, kde z charakteru projektu, kde sa neplánuje štandardne vývoj softvéru, ale jedná sa o nákup HW a licencovaného a OS softvéru by rozdelení spôsobovalo problémy pri samotnej implementácii, kedy sa jedná o osadenie a konfiguráciu HW, ktorá môže prebiehať súbežne

v dohodnutých časoch odstávok a vzájomne sa nijako neovplyvňuje. Nasadenie zálohovania sa neovplyvňuje s implementáciou nových FW a bolo by kontraproduktívne takto rozdeľovať infraštruktúrne úpravy. Samozrejme je dôležité aby sa nevykonávali všetky kritické zmeny v tom istom čase, ale v logickom slede, ale nie až vždy po úplnom ukončení nejakej aktivity v rámci iného inkrementu.

Náklady na projekt predstavujú náklady na obstaranie HW, SW, externé a interné inštalačné a konfiguračné práce. Riadenie projektu spadá pod nepriame náklady projektu. V rámci katalógu požiadaviek nevyužívame UCP odhad nákladov na realizáciu funkčných požiadaviek. Cena je určená v rámci záložky Rozpočet - HW a licencie priamo z PHZ na všetky položky rozpočtu. Interné náklady sú určené predpokladaným odhadom prácnosti.

Náklady na prevádzku sú započítané od t4 vzhľadom na obstaranie 3 ročnej (3 Y) podpory na všetky HW a SW položky rozpočtu, kde rátame s implementáciou v čase t1.

7.2Výpočet prínosov

7.2.1Kvantitatívne prínosy

Kvantitatívne prínosy v rámci navrhovaného projektu sú:

- Zníženie nákladov súvisiacich s odstraňovaním preventívnych kybernetických incidentov.
- Zníženie nákladov súvisiacich s odstraňovaním reaktívnych kybernetických incidentov.

V rámci výpočtu a monetizácie prínosov je využitá kombinácia:

1. Nákladov cenu práce pri obmedzení výkonu internými zamestnancami
2. Náklady na výšku škody kybernetického incidentu

Cenu práce pri obmedzení výkonu internými zamestnancami – 1 incident ročne

Do výpočtu vstupuje priemerná mesačná hrubá mzda vo verejnej správe za 3. Q./2024 (obdobie aktualizovať k času predloženia dokumentu), podľa ŠÚ SR na úrovni 1984,00 € z čoho vyplýva pri zohľadnení fondu pracovnej doby v štátnej správe hodinová super hrubá mzda 16,44 €.V prípade 1 400 interných a externých zamestnancov (využívajúcich registratúru je 1 400) s trojdňovým výpadkom 3 x 7,5 h (3 Pracovné dni predstavujú konzervatívny prístup k odhadu, kde vstupujú krátke útoky v hodinách ako napr. DDoS až po rozsiahlejšie ako Ransomware, kde sa zotavenie z útoku pohybuje od niekoľkých dní až po niekoľko mesiacov. Priemerne v zmysle štatistík napr. (https://www.cigent.com/blog/ransomware-and-recovery-time-what-you-should-expect) sa uvádza priemerná hodnota 21 dní. Pre potreby preukázania prínosvo sme konzervatívne zvolili hodnotu 3 dni ako priemer všetkých závažnejších útokov), čo predstavuje 22,5 hodinový výpadok je pre prvý rok 517 974,51 €. So započítaním zákonného nárastu miezd zamestnancov v štátnej a verejnej správe (valorizácia miezd) + 1% ročne nasledovné:

Cena výpadkov pre roky t3 až t10	Hodnota
t2	517 974,51 €
t3	523 154,26 €
t4	528 385,80 €
t5	533 669,66 €
t6	539 006,35 €
t7	544 396,42 €
t8	549 840,38 €
t9	555 338,78 €
t10	560 892,17 €

Výšku škody kybernetického incidentu - 1 incident ročne

Výpočet vychádza z odhadu, že ekonomické škody kybernetických útokov predstavujú 0,5% z HDP (priemerná hodnota). Pri vysoko príjmových krajinách dosahujú až 1,1% z HDP . Zdroj: https://www.csis.org/analysis/economic-impact-cybercrime, https://www.rand.org/pubs/research_reports/RR2299.html. V rámci výpočtu uvažujeme o hodnote 0,5% z výšky štátneho rozpočtu za rok 2023 v hodnote 23 688 600 000 €, zdroj:https://www.mfsr.sk/sk/media/tlacove-spravy/bilancia-statneho-rozpoctu-k-31-12-2023.html. Odhad nákladov na kybernetické incidenty

vo verejnej správe za rok vychádza na 118 443 000,00 €. Počet útokov na verejnú správu za rok 2023 je určený na hodnotu 478, zdroj NBU: https://www.nbu.gov.sk/data/att/2855.pdf. Z toho vyplýva, že pri tejto metodike je výška jedného incidentu v hodnote 247 788,70 €. Pri zohľadnení konzervatívneho prístupu, je vo výpočte prínosov použitá polovičná hodnota vo výške 123 894,35 € za prvý rok. Pri započítaní odhadu rastu HDP a teda celkovo ekonomiky SR to predstavuje nasledovné:

Cena kyberneticéhi incidentu raz ročne pre organizáciu od t3 do t10	Hodnota	Rast HDP, do roku 2027 v zmysle výboru, realistický odhad, zvyšok 2 % (odhad je nad 2 %), Zdroj: https://www.mfsr.sk/files/sk/financie/institut-financnej-politiky/strategicke-materialy/program-stability/program-stability-sr-roky-2024-2027_final.pdf
t2	123 894,35 €	1
t3	126 991,71 €	1,025
t4	130 166,50 €	1,025
t5	133 290,50 €	1,024
t6	135 956,31 €	1,02
t7	138 675,44 €	1,02
t8	141 448,94 €	1,02
t9	144 277,92 €	1,02
t10	147 163,48 €	1,02

Súhrnné kvantitatívne prínosy:

Sumár nákladov na jeden kybernetický incident ročne pre potreby prínosov v CBA	Hodnota
t1	0
t2	641 868,86 €s
t3	650 145,97 €
t4	658 552,30 €
t5	666 960,16 €
t6	674 962,66 €
t7	683 071,85 €
t8	691 289,32 €
t9	699 616,71 €
t10	708 055,65 €

Vzhľadom na implementáciu HW a SW v t1, predpokladáme prínosy už od roku t2.

Poznámka: V rámci CBA boli do karty Parametre - Agendové IS premietnuté kvantitatívne prínosy v časti pre kvalitatívne prínosy a premenované pre potreby tohto projektu.

7.2.2Kvalitatívne prínosy

Kvalitatívne prínosy vychádzajú z princípov NKIVS:

Prioritná os 4 Kybernetická a informačná bezpečnosť a čiastkovým cieľom **Zvýšenie schopnosti včasnej identifikácie kybernetických incidentov vo verejnej správe**.

Ďalšie uvažované kvalitatívne prínosy v rámci navrhovaného projektu sú:

- Zníženie miery rizika vzniku kybernetického incidentu.
- Zvýšenie miery súladu s platnou legislatívou.
- Zvýšenie úrovne kybernetickej a informačnej bezpečnosti.
- Zvýšenie detekcie kybernetických bezpečnostných incidentov.
- Zvýšená spokojnosť a dôvera používateľov.

7.2.3Výsledky CBA

Výsledok CBA		*Výsledná hodnota*	*Minimálna hodnota*
BCR	pomer prínosov a nákladov	1,28	**1,00**
FIRR	finančná vnútorná výnosová miera (%)	#NUM!	-
EIRR	ekonomická vnútorná výnosová miera (%)	20,9%	5,0%
FNPV	finančná čistá súčasná hodnota (eur s DPH)	-3 808 095	-
ENPV	ekonomická čistá súčasná hodnota (eur bez DPH)	1 659 046	0

Rok návratu investície: **t6**

7.2.4Analýza citlivosti a kritických premenných

Zvýšenie nákladov - TCO celkovo		**Zvýšenie CAPEX**		**Zníženie kvantitatívnych prínosov KyB (pôvodné Kvalitatívne)**	
%	**BCR**	**%**	**BCR**	**%**	**BCR**
0%	1,28	**0%**	1,28	**0%**	1,28
10%	1,16	**10%**	1,20	**-10%**	1,15
20%	1,06	**20%**	1,13	**-20%**	1,02
30%	0,98	**30%**	1,07	**-30%**	0,89
40%	0,91	**40%**	1,01	**-40%**	0,77
50%	0,85	**50%**	0,96	**-50%**	0,64
60%	0,80	**60%**	0,92	**-60%**	0,51
70%	0,75	**70%**	0,88	**-70%**	0,38
80%	0,71	**80%**	0,84	**-80%**	0,26
90%	0,67	**90%**	0,80	**-90%**	0,13
100%	0,64	**100%**	0,77	**-100%**	0,00

Z uvedeného vyplýva, že charakter kritickej premennej vykazuje Zníženie kvantitatívnych prínosov KyB, ktorej zníženie o danú percentuálnu hodnotu vykazuje o čosi väčšie percentuálne zníženie BCR.

		Zníženie počtu podaní v budúcom stave										
	1,28	**0%**	**-10%**	**-20%**	**-30%**	**-40%**	**-50%**	**-60%**	**-70%**	**-80%**	**-90%**	**-100%**
Zvýšenie CAPEX	**0%**	1,28	1,28	1,28	1,28	1,28	1,28	1,28	1,28	1,28	1,28	1,28
	10%	1,20	1,20	1,20	1,20	1,20	1,20	1,20	1,20	1,20	1,20	1,20
	20%	1,13	1,13	1,13	1,13	1,13	1,13	1,13	1,13	1,13	1,13	1,13
	30%	1,07	1,07	1,07	1,07	1,07	1,07	1,07	1,07	1,07	1,07	1,07
	40%	1,01	1,01	1,01	1,01	1,01	1,01	1,01	1,01	1,01	1,01	1,01
	50%	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96
	60%	0,92	0,92	0,92	0,92	0,92	0,92	0,92	0,92	0,92	0,92	0,92
	70%	0,88	0,88	0,88	0,88	0,88	0,88	0,88	0,88	0,88	0,88	0,88
	80%	0,84	0,84	0,84	0,84	0,84	0,84	0,84	0,84	0,84	0,84	0,84
	90%	0,80	0,80	0,80	0,80	0,80	0,80	0,80	0,80	0,80	0,80	0,80
	100%	0,77	0,77	0,77	0,77	0,77	0,77	0,77	0,77	0,77	0,77	0,77

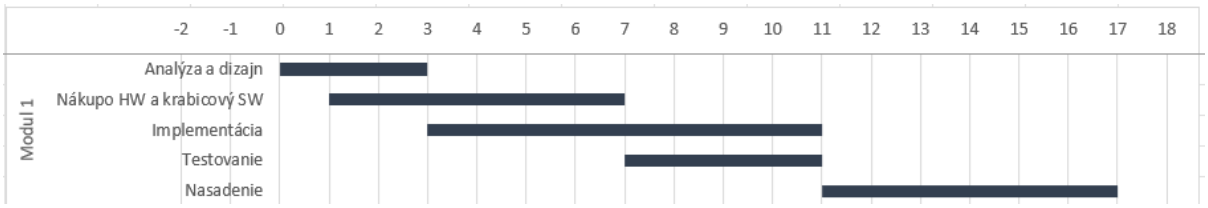
V rámci CBA bola testovaná kombinácia premenných, z ktorých jedna nie je relevantná a ukazuje sa tak dôležitosť práve zvýšenie CAPEX.

8.HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU a METÓDA JEHO RIADENIA

Celkový harmonogram jednotlivých fáz projektu:

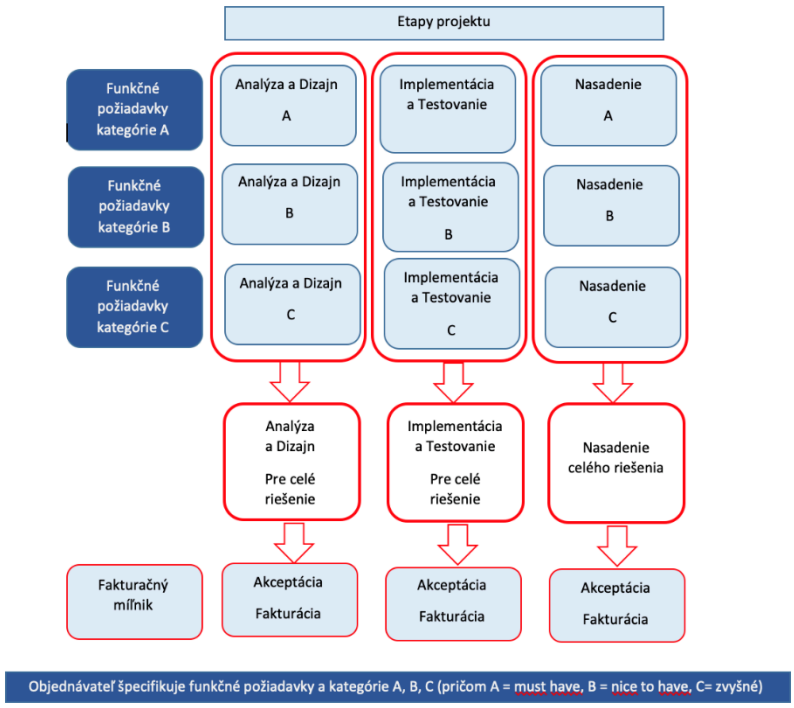
ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu)	KONIEC (odhad termínu)	POZNÁMKA
1.	Prípravná fáza a Iniciačná fáza	11/2024	4/2025	
2.	Realizačná fáza	05/2025	09/2026	
2a	Analýza a Dizajn	05/2025	07/2025	Kontrola PHZ, overenie požiadaviek, štart projektu, úvodné projektové výstupy a dokumentácia
2b	Nákup technických prostriedkov, programových prostriedkov a služieb	06/2025	11/2025	Obstaranie dodávateľa, licencií HW. Predpokladáme prípravy na VO ešte pred podpisom Zmluvy o NFP, ešte počas ŽoNFP, v zmluve o dodávke bude odkladacia podmienka o účinnosti zmluvy až po podpise Zmluvy o NFP.
2c	Implementácia a testovanie	08/2025	3/2026	Implementácia a testovanie aktivít bez značného dopadu na výkon Žiadateľa
2d	Nasadenie a PIP	04/2026	07/2026	Nasadenie aktivít bez značného dopadu na výkon Žiadateľa
3.	Dokončovacia fáza	08/2026	09/2026	Záverečná dokumentácia, záverečná správa s ukončením projektu
4.	Podpora prevádzky (SLA)	8/2026	12/2031	Minimálne 5 rokov a viac, následné predĺženie po prehodnotení stavu

Indikatívny harmonogram realizačnej fázy jednotlivých častí projektu z CBA. Detailný harmonogram bude vytvorený v rámci Projektového iniciálneho dokumentu.



Projekt a jeho realizácia a všetky jeho projektové výstupy budú v súlade s vyhláškou 401/2023 o riadení projektov. Pre projekt bola vzhľadom na jeho povahu vybraná ako najvhodnejšia metóda 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.



9.PROJEKTOVÝ TÍM

Projektový tím bude vytvorený v súlade s vyhláškou 401/2023 o riadení projektov. Bude vytvorený riadiaci výbor a projektový tím na strane objednávateľa.

Riadiaci výbor bude tvorený:

1. Predseda riadiaceho výboru projektu,
2. Zástupca biznis vlastníkov,
3. Zástupca kľúčových používateľov,
4. Projektový manažér objednávateľa,
5. Zástupca Dodávateľa v zmysle Zmluvy o dielo

ID	Meno a Priezvisko	Pozícia	Oddelenie	Rola v projekte
1.	Bude definovaný v iniciačnej fáze	Bude definovaný v iniciačnej fáze	NA	Predseda riadiaceho výboru projektu s HP
2.	Bude definovaný v iniciačnej fáze	Bude definovaný v iniciačnej fáze	NA	Zástupca biznis vlastníkov s HP
3.	Bude definovaný v iniciačnej fáze	Predpokladá sa nominácia Manažéra kybernetickej a informačnej bezpečnosti	NA	Zástupca kľúčových používateľov s HP
4.	Bude definovaný v iniciačnej fáze	Bude definovaný v iniciačnej fáze	NA	Projektový manažér objednávateľa s HP

5.	Bude definovaný v iniciačnej fáze	Bude definovaný v iniciačnej fáze	NA	Zástupca Dodávateľa v zmysle Zmluvy o dielo bez HP

Na návrh určeného projektového manažéra bude vymenovaný projektový tím, pričom predseda riadiaceho výboru projektu alebo projektový manažér objednávateľa na základe poverenia plánujú minimálne nasledovné pozície:

1. Projektový manažér,
2. Manažér kybernetickej a informačnej bezpečnosti,
3. Kľúčový používateľ,
4. Odborný zamestnanec IT,
5. Finančný manažér,
6. Vlastník procesov

ID	Meno a Priezvisko	Pozícia	Oddelenie	Rola v projekte
1.	Bude definovaný v úvode realizačnej fázy	Bude definovaný v úvode realizačnej fázy	NA	Projektový manažér
2.	Bude definovaný v úvode realizačnej fázy	Bude definovaný v úvode realizačnej fázy	NA	Manažér kybernetickej a informačnej bezpečnosti (Tím manažér)
3.	Bude definovaný v úvode realizačnej fázy	Bude definovaný v úvode realizačnej fázy	NA	Kľúčový používateľ
4.	Bude definovaný v úvode realizačnej fázy	Očakáva sa Systémovým alebo Sieťový administrátor	NA	Odborný zamestnanec IT
5.	Bude definovaný v úvode realizačnej fázy	Bude definovaný v úvode realizačnej fázy	NA	Finančný manažér
6.	Bude definovaný v úvode realizačnej fázy	Bude definovaný v úvode realizačnej fázy	NA	Vlastník procesov

Členovia tímu sa budú zodpovedať Tím manažérovi s rolou Manažér kybernetickej a informačnej bezpečnosti a Tím manažér sa zodpovedá roly Projektový manažér. Následne projektový manažér sa bude zodpovedať Riadiacemu výboru.

9.1 PRACOVNÉ NÁPLNE

Riadiaci výbor projektu tvorí predseda riadiaceho výboru projektu, zástupca prevádzky a biznis vlastníci alebo nimi poverení zástupcovia. Členom riadiaceho výboru projektu môže byť aj zástupca dodávateľa. Člen riadiaceho výboru projektu za dodávateľa môže mať hlasovacie právo. Väčšina členov riadiaceho výboru projektu s hlasovacím právom sú osoby navrhnuté objednávateľom a zastupujúce záujmy objednávateľa.

Riadiaci výbor projektu zasadá pravidelne, najmenej jedenkrát za tri mesiace.

Projektový manažér

- Zodpovedá za riadenie projektu počas celého životného cyklu projektu. Riadi projektové (ľudské a finančné) zdroje, zabezpečuje tvorbu obsahu, neustále odôvodňovanie projektu (aktualizuje BC/CBA) a predkladá vstupy na rokovanie Riadiaceho výboru. Zodpovedá za riadenie všetkých (ľudských a finančných) zdrojov, členov projektovému tím objednávateľa a za efektívnu komunikáciu s dodávateľom alebo stanovených zástupcom dodávateľa.
- Zodpovedá za riadenie prideleného projektu - stanovenie cieľov, spracovanie harmonogramu prác, koordináciu členov projektového tímu, sledovanie dodržiavania harmonogramu prác a rozpočtu, hodnotenie a prezentáciu výsledkov a za riadenie s tým súvisiacich rizík. Projektový manažér vedie špecifikáciu a implementáciu projektov v súlade s firemnými štandardami, zásadami a princípmi projektového riadenia.
- Zodpovedá za plnenie projektových/programových cieľov v rámci stanovených kvalitatívnych, časových a rozpočtovým plánov a za riadenie s tým súvisiacich rizík. V prípade externých kontraktov sa vedúci projektu/

projektový manažér obvykle podieľa na ich plánovaní a vyjednávaní a je hlavnou kontaktnou osobou pre zákazníka.

Kľúčový používateľ

- Zodpovedný za reprezentáciu záujmov budúcich používateľov projektových produktov alebo projektových výstupov a za overenie kvality produktu.
- Zodpovedný za návrh a špecifikáciu funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu, požiadaviek koncových používateľov na prínos systému a požiadaviek na bezpečnosť.
- Kľúčový používateľ (end user) navrhuje a definuje akceptačné kritériá, je zodpovedný za akceptačné testovanie a návrh na akceptáciu projektových produktov alebo projektových výstupov a návrh na spustenie do produkčnej prevádzky. Predkladá požiadavky na zmenu funkcionalít produktov a je súčasťou projektových tímov

Manažér kybernetickej a informačnej bezpečnosti

- Zodpovedá za dodržanie princípov a štandardov v oblasti informačnej a kybernetickej bezpečnosti a za kontrolu a audit implementovaných bezpečnostných opatrení (technológií, procesov atď.).
- Koordinuje a riadi činnosť v oblasti bezpečnosti prevádzky IT, spolupracuje na projektoch, na rozvoji nástrojov a postupov k optimalizácii bezpečnostných systémov a opatrení. Stanovuje základné požiadavky, podmienky a štandardy pre oblasť bezpečnosti programov, systémov, databázy či sieti. Spracováva a kontroluje príslušné interné predpisy a dohliada nad plnením týchto štandardov a predpisov. Kontroluje a riadi činnosť nad bezpečnostnými testami, bezpečnostnými incidentmi v prevádzke IT. Poskytuje inštrukcie a poradenstvo používateľom počítačov a informačných systémov pre oblasť bezpečnosti.

Podmienky správneho a efektívneho výkonu činnosti role Manažér KIB a ITB:

1) neobmedzený aktívny prístup ku všetkým projektovým dokumentom, nástrojom a výstupom projektu, v ktorých sa opisuje predmet projektu z hľadiska jeho architektúry, funkcií, procesov, manažmentu informačnej bezpečnosti a spôsobov spracúvania dát, ako aj dát samotných.

2) rola manažér Kybernetickej a IT bezpečnosti si vyžaduje mať sprístupnené všetky informácie o bezpečnostných opatreniach zavádzaných projektom v zmysle:

a) § 20 zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

b) ustanovení zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov

Vlastník procesov

- Zodpovedá za proces - jeho výstupy i celkový priebeh poskytnutia služby alebo produktu konečnému užívateľovi. Kľúčová rola na strane zákazníka (verejného obstarávateľa), ktorá schvaľuje biznis požiadavky a zodpovedá za výsledné riešenie, prínos požadovanú hodnotu a naplnenie merateľných ukazovateľov. Úlohou tejto roly je definovať na užívateľa orientované položky (user-stories), ktoré budú zaradzované a prioritizované v produktovom zásobníku. Zodpovedá za priebežné posudzovanie vecných výstupov dodávateľa v rámci analýzy, návrhu riešenia vrátane DNR z pohľadu analýzy a návrhu riešenia aplikácii IS.
- Zodpovedný za schválenie funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu. Definuje očakávania na kvalitu projektu, kvalitu projektových produktov, prínosy pre koncových používateľov a požiadavky na bezpečnosť. Definuje merateľné výkonnostné ukazovatele projektov a prvkov. Vlastník procesov schvaľuje akceptačné kritériá, rozsah a kvalitu dodávaných projektových výstupov pri dosiahnutí platobných míľnikov, odsúhlasuje spustenie výstupov projektu do produkčnej prevádzky a dostupnosť ľudských zdrojov alokovaných na realizáciu projektu.

Ostatné role a ich pracovné náplne:

Odborný zamestnanec IT

Zabezpečuje správu infraštruktúry Žiadateľa.

Finančný manažér

Zabezpečuje finančnú správu a kontrolu projektu.

Administratívny pracovník

Vykonáva administratívne úkony a to najmä podporné aktivity pre projektového a finančného manažéra projektu.

10.ODKAZY

Nie je relevantné pre projekt.

11.PRÍLOHY

1. **Príloha :** Zoznam rizík a závislostí (Excel)