Prílohy

1. Zoznam zvolených cloudových služieb

Údaje sa vypĺňajú manuálne.

MetalS kód	Názov služby z katalógu služieb	Požadovaná úroveň

2. Riziká projektu

Údaje sa vypĺňajú manuálne.

R2 Pri zachovaní súčasného stavu nie je možné efektívne plniť ciele súvisiace so vzdelávaním, výskumom a vývojom definované v koncepcii kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020. R3 Nedostatočné technické vybavenie pre zabezpečenie nosných služieb Centra. R4 Nedostatočná vzdelanostná úroveň v oblasti kybernetickej bezpečnosti.

ID	Názov rizika	Pravdepodobnosť	Dosah	Návrh mitigácie
R_X		Takmer isté riziko - výskyt rizika treba v každom prípade očakávať. Pravdepodobné riziko - existuje vysoká pravdepodobnosť, že sa riziko vyskytne. Stredné riziko - riziko sa môže vyskytnúť. Slabé riziko - riziko sa môže vyskytnúť za veľmi špecifických okolností. Nepravdepodobné riziko - výskyt rizika sa neočakáva.	Extrémny dosah - znemožní realizáciu projektu. Vysoký dosah - ovplyvní pokračovanie projektu Stredný dosah - vyžiada si úpravy projektu Nízky dosah - ovplyvní efektívnosť projektu v niektorých aspektoch. Zanedbateľný dosah - dosah sa minimalizuje bežnou činnosťou v rámci projektu.	
R_1	R1 Splnenie KPI definovaných v rámci tejto štúdie	Pravdepodobné riziko - existuje vysoká pravdepodobnosť, že sa riziko vyskytne	Nízky dosah - ovplyvní efektívnosť projektu v niektorých aspektoch	Výberom vhodnej alternatívy riešenia. Projektovou kontrolou naplnenia KPI
R_2	Pri zachovaní súčasného stavu nie je možné efektívne plniť ciele súvisiace so vzdelávaním, výskumom a vývojom definované v koncepcii kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020.	Stredné riziko - riziko sa môže vyskytnúť.	Stredný dosah - vyžiada si úpravy projektu	
R_3	Nedostatočné technické vybavenie pre zabezpečenie nosných služieb Centra	Pravdepodobné riziko - existuje vysoká pravdepodobnosť, že sa riziko vyskytne.	Stredný dosah - vyžiada si úpravy projektu	Implementovať navrhované riešenie
R_4	Nedostatočná vzdelanostná úroveň v oblasti kybernetickej bezpečnosti.	Stredné riziko - riziko sa môže vyskytnúť	Zanedbateľný dosah - dosah sa minimalizuje bežnou činnosťou v rámci projektu.	Paralelne s prípravou projektu sa musí čo najskôr začať s náborom a zaškolením kvalifikovaným zdrojov.
R_5	Pri zachovaní súčasného stavu technologických komponentov sa nepokryjú všetky činnosti definované v legislatívnych požiadavkách	Stredné riziko - riziko sa môže vyskytnúť	Nízky dosah - ovplyvní efektívnosť projektu v niektorých aspektoch	Výberom vhodnej alternatívy riešenia. Projektovou kontrolou naplnenia KPI
R_6	Nie všetky informačné systémy a moduly budú vybudované systematickým spôsobom	Pravdepodobné riziko - existuje vysoká pravdepodobnosť, že sa riziko vyskytne	Zanedbateľný dosah - dosah sa minimalizuje bežnou činnosťou v rámci projektu.	Plánovanie a priebežná transparentná komunikácia. Kontrola plánovaných úloh pri realizácii.

R_7	Prevádzka súčasného riešenia je obmedzovaná nedostatočným personálnym, znalostným a technickým (hardvérovým a softvérovým) vybavením	Stredné riziko - riziko sa môže vyskytnúť	Nízky dosah - ovplyvní efektívnosť projektu v niektorých aspektoch	Včas definovať požiadavky na organizačné zabezpečenie podpory. Už počas budovania riešenia vytvoriť návrh riešenia budúcej podpory a kvantifikovať personálne ako aj technické požiadavky na podporu.
R_8	Legislatívna príprava bude meškať, respektíve výsledné znenia nových právnych predpisov budú obsahovať ustanovenia, ktoré môžu mať vplyv na národný projekt	Stredné riziko - riziko sa môže vyskytnúť	Stredný dosah - vyžiada si úpravy projektu	Identifikovať potrebné zmeny v úvodných analytických fázach projektu a spustiť čo najskôr legislatívny proces.
R_9	Politické riziko pri zmene vlády	Stredné riziko - riziko sa môže vyskytnúť	Stredný dosah - vyžiada si úpravy projektu	Zahrnúť projekt medzi dlhodobé strategické ciele reformy verejnej správy.
R_10	Riešenie bude náročne na biznis (kapacitne a vedomostne)	Slabé riziko - riziko sa môže vyskytnúť za veľmi špecifických okolností	Zanedbateľný dosah - dosah sa minimalizuje bežnou činnosťou v rámci projektu.	Implementovať riešenie.
R_11	Riešenie nebude dostatočne flexibilné	Slabé riziko - riziko sa môže vyskytnúť za veľmi špecifických okolností	Zanedbateľný dosah - dosah sa minimalizuje bežnou činnosťou v rámci projektu.	Vo fáze analýzy a dizajnu projektu je potrebné definovať požiadavky na systém tak, aby bol schopný reagovať na časté zmeny, umožňoval integráciu dát prostredníctvom rôznych formátov a rozhraní.
R_12	Interná integrácia tréningových pracovísk na ústredné tréningové centrum.	Stredné riziko - riziko sa môže vyskytnúť	Stredný dosah - vyžiada si úpravy projektu	Eliminácia tohto rizika správnym návrhom jednotlivých komponentov riešenia
R_13	Spolupráca zúčastnených strán nebude na dostatočnej úrovni	Slabé riziko - riziko sa môže vyskytnúť za veľmi špecifických okolností	Zanedbateľný dosah - dosah sa minimalizuje bežnou činnosťou v rámci projektu.	Je nevyhnutné dostatočné zapojenie organizácií do projektu a je nevyhnutné stanoviť projektu vysokú prioritu a dôležitosť a vyžadovať súčinnosť zúčastnených strán.
R_14	Centrum nebude plne vyladené do času uvedenia do produkčnej prevádzky	Stredné riziko - riziko sa môže vyskytnúť	Nízky dosah - ovplyvní efektívnosť projektu v niektorých aspektoch	Priebežne budovať interné kapacity a definovať pracovníkov dedikovaných pre prevádzku riešenia. Vykonať školenia a dokumentáciu pracovných postupov.
R_15	Nedodržiavanie organizačných bezpečnostných opatrení a procesov	Slabé riziko - riziko sa môže vyskytnúť za veľmi špecifických okolností	Nízky dosah - ovplyvní efektívnosť projektu v niektorých aspektoch	Počas projektu vytvoriť prostredie s najvyššou možnou úrovňou bezpečnosti.
R_16	Nedostatok finančných prostriedkov na pokrytie prevádzky	Stredné riziko - riziko sa môže vyskytnúť	Stredný dosah - vyžiada si úpravy projektu	1. Kontrolovať výšku nákladov na prevádzku a údržbu po nasadení systému. 2. Zahrnúť výdavky na prevádzku a údržbu do návrhu rozpočtu. 3. Vyhodnocovať KPI a dosahovanie očakávaných prínosov riešenia a použiť ako argumentáciu.
R_17	Nepodarí sa dosiahnuť preukázateľné úspory podľa plánu	Slabé riziko - riziko sa môže vyskytnúť za veľmi špecifických okolností	Nízky dosah - ovplyvní efektívnosť projektu v niektorých aspektoch	Ciele projektu musia byť previazané s úsporami. Reálne úspory budú neustále vyhodnocované tak, aby boli prípadné problémy v čas rozoznané.
R_18	Náklady na vybudovanie alebo prevádzku sa vymknú kontrole / presiahnu plánovanou hodnotu	Slabé riziko - riziko sa môže vyskytnúť za veľmi špecifických okolností	Stredný dosah - vyžiada si úpravy projektu	Odhad nákladov projektu je vykonaný vzhľadom na znalosť súčasného stavu a požiadaviek na systém so zohľadnením rizikovej prirážky. Efektívne vynaloženie verejných prostriedkov zabezpečí následne verejné obstarávanie vykonávané riadne a v súlade so záväznými normami.

3. Výstupy projektu a kritériá kvality

Údaje sa vypĺňajú manuálne.

ID	Výstup projektu	Kritérium kvality a spôsob dosiahnutia
VP_1	Legislatíva tobe	Súlad s legislatívou - spustiť čo najskôr legislatívny proces
VP_2	Biznis architektúra tobe	Miera úplnosti a optimalizácie procesov v rámci Centra - správnym návrhom jednotlivých komponentov riešenia
VP_3	Architektúra informačných systémov tobe	Interná integrácia tréningových pracovísk na ústredné tréningové centrum - Výsledky integračných testov

VP_4	Implementácia a migrácia	Dodržiavanie plánu národného projektu -Implementácia riešenia v súlade s navrhnutým harmonogramom
VP_5	Implementácia a migrácia	Funkčné projektové registre a manažment zmien - Dôsledné dodržiavanie projektových princípov (Prince2)
VP_6	Implementácia a migrácia	Definované produkty s konkrétnymi a merateľnými kritériami - Product breakdown structure a akceptačné kritériá
VP_7	Bezpečnostná architektúra tobe	Akceptovateľný výsledok bezpečnostného auditu - Výsledky auditu
VP_8	Prevádzka tobe	Zníženie počtu prevádzkových incidentov v procese prevádzky Centra - V rámci prevádzky riešenia je potrebné vytvoriť stabilizovaný tím podpory

4. Legislatívna analýza

Údaje sa vypĺňajú manuálne.

Zmena nie je potrebná

ID	Typ	Názov	Zdôvodnenie	Návrh zmeny
LA_X	Vid. Vysvetlenie typov právnych v metodickom usmernení Aproximačné nariadenia vlády SR Zákon Nariadenia vlády SR Vyhlášky / výnosy / opatrenia Uznesenia vlády SR Vnútorné riadiace predpisy Zmluvy Technické normy		Zdôvodnenie zaradenia	Zdôvodnenie zmeny
LA_1	Smernica	smernica Európskeho parlamentu a rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii		
LA_2	Vykonávacie nariadenie Komisie (EÚ) smernice Európskeho parlamentu a Rady (EÚ) 2016/1148	vykonávacie nariadenie Komisie (EÚ) 2018/151 z 30. januára 2018, ktorým sa stanovujú pravidlá uplatňovania	Pokiaľ ide o bližšiu špecifikáciu prvkov, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri riadení rizík v oblasti bezpečnosti sietí a informačných systémov, a parametrov na posudzovanie toho, či má incident závažný vplyv	Zmena nie je potrebná
LA_3	Zákon	zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov		Zmena nie je potrebná
LA_4	Vyhláška	vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),		Zmena nie je potrebná

LA_5	Vyhláška	vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov	Zmena nie je potrebná
LA_6	Vyhláška	vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov	Zmena nie je potrebná
LA_7	Vyhláška	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	Zmena nie je potrebná
LA_8	Zákon	zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov	Zmena nie je potrebná
LA_9	Zákon	zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov	Zmena nie je potrebná
LA_10	Koncepčný dokument	Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020	Zmena nie je potrebná
LA_11	Koncepčný dokument	Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020	Zmena nie je potrebná

5. Zainteresovaní

Rola jednotlivca, tímu alebo organizácie (alebo ich skupín), ktorá reprezentuje ich záujmy vo vzťahu k výstupom architektúry a dosiahnutým cieľom. Údaje sa vypĺňajú manuálne.

ID	Zainteresovaný	Popis
1	UPVII	UPVII je inštitúcia zodpovedná za sektor verejnej správy podľa zákona o KyB.
2	NBÚ	NBÚ je podľa zákona o KyB národná autorita v oblasti kybernetickej bezpečnosti.
3	SIS	SIS je partnerom projektu.
4	ústredné orgány štátnej správy	Ústredné orgány štátnej správy budú vysielať svojich zamestnancov (špecialistov KyB) na tréningy a všetkých zamestnancov na školenia v oblasti KyB.
5	ostatné OVM	Zamestnanci ostatných OVM budú absolvovať pravidelné školenia zamerané na oblasť KyB.

6. Ciele OP II - PO7

Ktoré ciele OPII projekt rieši a či je k nim vypracovaný reformný zámer podľa vzoru EVS.
Údaje sa vypĺňajú v MetaIS, do tabuľky sa generujú.

ID cieľa	Meno cieľa	Reformný zámer EVS (A/N/NA)	Spôsob naplnenia cieľa
OPII/OPEVS			

ciel_po7_9	Zvýšenie kybernetickej bezpečnosti v spoločnosti	Informačné systémy a siete budú posudzované z pohľadu naplnenia zadefinovaných bezpečnostných cieľov a súladu s legislatívou. Budú sa implementovať a vylepšovať opatrenia na riadenie bezpečnostných rizík, predovšetkým pre systémy verejnej správy patriace do kritickej infraštruktúry. Zvýši sa transparentnosť informovania o bezpečnostných incidentoch jednotlivcov, ktorých osobné údaje boli stratené, ukradnuté alebo pozmenené. Celkovo sa zvýši dôvera v digitálny priestor a povedomie o spôsobe riešenia kybernetických útokov. Prispeje k tomu tiež nasadenie platformy pre zber údajov a opatrení a pre posielanie výstrah súvisiacich s kybernetickou bezpečnosťou. Táto platforma bude interoperabilná s európskym riešením a napojená na Európske centrum pre kybernetický zločin.

7. Architektonické ciele

Koncový stav, prínos.
Údaje sa vypĺňajú v MetaIS, do tabuľky sa generujú.

MetaIS kód	Cieľ	Spôsob naplnenia cieľa	Zainteresovaní
X		Bližšie spresnenie.	ID zainteresovaných z prílohy Zainteresovaný

8. Architektonické princípy

Relevantné princípy NKIVS treba zaevidovať pre danú štúdiu v MetaIS. Do prílohy štúdie sa následne vygenerujú. Údaje sa vypĺňajú v MetaIS, do tabuľky sa generujú.

MetaIS kód	Typ	Názov	Popis	Spôsob plnenia
princip_19	Princíp	TECHNOLOGICKÁ INTEROPERABILITA	Softvér a hardvér vo verejnej správe musí byť v súlade s definovanými štandardami, ktoré podporujú interoperabilitu údajov, aplikácií a technológií, a to v celom európskom priestore.	
princip_12	Princíp	SPÄTNÁ VÄZBA	Používatelia môžu poskytnúť spätnú väzbu o službe, nahlásiť chyby, navrhovať zlepšenia a podobne. Poskytovateľ služieb môže použiť tento vstup pre zlepšenie kvality služby. Týmto spôsobom majú používatelia možnosť konštruktívne presadzovať svoje záujmy.	
princip_3	Princíp	PROAKTIVITA	Verejná správa ponúkne všade tam, kde je to možné, poskytovanie takých služieb, ktoré používateľ v danom okamihu potrebuje, prípadne ich bude vykonávať z vlastnej iniciatívy s možnosťou odmietnutia toho postupu zo strany používateľa.	
princip_6	Princíp	UNIFORMITA	Z pohľadu používateľa je obsluha používateľa cez akýkoľvek kanál jednotná a používa štandardné postupy a riešenia.	
princip_9	Princíp	TRANSPARENTNÝ PRÍSTUP K SLUŽBÁM	Používatelia majú pri používaní elektronických služieb prístup ku všetkým relevantným informáciám s výnimkou tých, ktorých sprístupňovanie je zo zákona obmedzené alebo zamietnuté. Pred, počas a po poskytnutí služby poskytovateľ informuje používateľa o postupe riešenia, o maximálnom čase jej vybavenia, použitých informáciách a výsledku. V prípade, \nže ide o službu komplexnú (to je pozostávajúcu z viacerých nadväzujúcich aktivít) a je to relevantné, \nje klient informovaný o zmene stavu jeho požiadavky (to znamená, že počas vybavovania jeho požiadavky vie zistiť, v akom stave sa práve nachádza).	
princip_2	Princíp	ORIENTÁCIA NA SLUŽBY	Architektúra verejnej správy je založená na definícii služieb, ktoré odrážajú procesy reálneho sveta. To znamená, že akákoľvek vrstva architektúry verejnej správy (vrstva procesov, IS, technológií) komunikuje s okolitým svetom prostredníctvom služieb , ktoré sú konzumované prostredníctvom rôznych kanálov (rozhraní). Zámerom je podporiť digitálnu transformáciu verejnej správy, ktoré bude poskytovať používateľsky prívetivé elektronické služby ako štandard, a to aj pre cezhraničné vybavovanie životných situácií.	
princip_20	Princíp	OTVORENÉ ŠTANDARDY	Prednostne sa používajú otvorené štandardy a formáty a dôraz sa kladie nazabezpečenie technologickej neutrálnosti.	
princip_24	Princíp	TRANSPARENTNOSŤ	Riadenie informačnej bezpečnosti, najmä výkon dohľadu a kontroly, musí byť zabezpečený postupmi, ktoré garantujú ich transparentnosť a opakovateľnosť.	
princip_5	Princíp	PRÍSTUPNOSŤ	Služba je ľahko prístupná pre každého občana Európskej únie, aj zdravotne, sociálne, či inak znevýhodneného používateľa. Poskytovatelia služieb musia prispôsobiť ich prístupnosť k preferovaným metódam používateľa. Ide teda aj o výber komunikačných kanálov, času, kedy je kontakt možný a používateľskú prívetivosť metód komunikácie.	

princip_25	Princíp	AUDITOVATEĽNOSŤ	Riadenie informačnej bezpečnosti rovnako ako aj iných aktivít vo verejnej správe musí používať princípy a pravidlá, ktoré umožňujú výkon kontroly a zároveň umožňujú generovanie auditných a iných log záznamov s požadovanou úrovňou ich ochrany.
princip_11	Princíp	KVALITA A SPOĽAHLIVOSŤ	Používatelia sa môžu spoľahnúť, že poskytovateľ služieb bude garantovať kvalitu, dostupnosť a spoľahlivosť služieb. Napríklad akákoľvek poskytnutá informácia musí byť správna, autentická, aktuálna a úplná.
princip_1	Princíp	ZODPOVEDNOSŤ A SPRÁVA SLUŽIEB	Každá služba, či už jednoduchá alebo komplexná musí mať jasne definovaného správcu, ktorý zodpovedá za jej poskytovanie, rozvoj a údržbu.
princip_4	Princíp	JEDNODUCHÁ NAVIGÁCIA	Používatelia jednoducho nájdu požadovanú službu, ktorú následne môžu jednoduchým spôsobom použiť.
princip_8	Princíp	OKAMŽITÉ VYBAVENIE	Všade tam, kde je to možné, alebo kde to bude možné po úprave legislatívy, budú poskytované samoobslužné online služby, v rámci ktorých sú podania vybavované okamžite. V ostatných prípadoch, keď je nevyhnutná akcia zamestnanca verejnej správy, sú podania vybavované v čo najkratšom možnom čase.
princip_17	Princíp	SPOLOČNÉ POUŽÍVANIE APLIKÁCIÍ	Aplikácie, ktoré sú jednotne používané v rámci celej verejnej správy sú preferované pred používaním obdobných aplikácií alebo pred vývojom duplicitných aplikácií.
princip_10	Princíp	JEDEN KRÁT A DOSŤ	Pri interakcii s verejnou správou bude verejná správa od žiadateľa vyžadovať len údaje, ktoré sú nové a verejná správa nimi ešte nedisponuje. Tento princíp bude platiť na úrovni celej Európskej únie a bude zabezpečovaný pomocou platformy dátovej integrácie. Zároveň bude umožnené elektronické zdieľanie rozhodnutí, ktoré vydala verejná správa.
princip_22	Princíp	BEZPEČNOSŤ ÚDAJOV	Údaje sú chránené najmä pred neoprávneným prístupom, manipuláciou, použitím a zverejnením (zachovanie dôvernosti údajov), ich úmyselnou alebo neúmyselnou modifikáciou (zachovanie integrity údajov) a sú dostupné v požadovanom čase a v požadovanej kvalite (zachovanie dostupnosti údajov).
princip_18	Princíp	JEDNODUCHÉ POUŽÍVANIE APLIKÁCIÍ	Aplikácie verejnej správy sú jednoduché na použitie pre koncového používateľa, či už z technického alebo obsahového hľadiska. Použitá technológia je pre používateľa používateľsky prívetivá, takže sa môže sústrediť na úlohy, ktoré pomocou aplikácií rieši.
princip_27	Princíp	ORIENTÁCIA NA KLIENTA	Verejná správa aktívne pracuje so skupinami klientov s cieľom vytvoriť také služby, ktoré sú klientmi vyžadované alebo preferované, a sú pre klienta jednoducho použiteľné. Verejná správa vzdeláva klientov svojich služieb o tom, aké služby sú vytvorené, ako sa používajú. Za klientov sú považovaní občania, podnikatelia ale i úradníci, ktorí sa službám venujú.
princip_28	Princíp	PARTICIPÁCIA	Verejná správa v procese informatizácie verejnej správy aktívne spolupracuje s verejnosťou.
princip_29	Princíp	TRANSPARENTNÉ ROZHODOVANIE	Verejná správa v procese informatizácie transparentne a včas informuje o budúcich zámeroch a aktívne žiada o vstupy verejnosti.
princip_30	Princíp	EFEKTÍVNOSŤ A PRIDANÁ HODNOTA	Informatizácia verejnej správy sleduje najvyššiu hodnotu za peniaze a prebieha na základe kontinuálneho vyhodnocovania nákladov a prínosov.
princip_31	Princíp	OTVORENÉ API	Aplikačné rozhrania elektronických služieb sú verejné pre dôveryhodné aplikácie tretích strán. Aplikačné rozhrania v informačných systémov sú budované spôsobom umožňujúcim ich použitie komukoľvek (po splnení určených podmienok). Špecificky všetky služby informačných systémov, ktoré sú dostupné grafickým rozhraním majú byť dostupné aj otvoreným aplikačným rozhraním.
princip_32	Princíp	MODULÁRNOSŤ	Aplikácie IKT sú členené na menšie samostatné časti, ktoré sú prepojené dobre definovanými rozhraniami s cieľom zvýšiť flexibilitu riešení.

9. Koncové služby

Koncové služby, ktoré budú výstupom projektu.
Údaje sa vypĺňajú do eGovernment komponentov MetaIS. Do prílohy štúdie sa generujú.

10. Zoznam pôvodných KS, ktoré budú po ukončení projektu zrušené

Údaje sa vypĺňajú manuálne.

11. Informačné systémy (ISVS)

Príloha nie je aplikovateľná, keďže sa nevytvára ISVS.
Údaje sa vypĺňajú do eGovernment komponentov MetaIS. Do prílohy štúdie sa následne generujú.

MetaIS kód	Názov informačného systému	Modul ISVS - kód	Modul ISVS - názov

12. Aplikačné služby

Príloha nie je aplikovateľná, keďže sa nevytvára ISVS.
Údaje sa vypĺňajú do eGovernment komponentov MetaIS. Do prílohy štúdie sa následne generujú.

13. Prevádzka

Príloha nie je aplikovateľná, keďže sa nevytvára ISVS. Údaje sa vypĺňajú manuálne.

Rozsah zálohovania	N/A, všetko, vybrané údaje
Doba zotavenia (RTO)	N/A, alebo čas v hodinách
Je záloha pravidelne validovaná	N/A, Áno, Nie
Miera dostupnosti	N/A, alebo 90% - 99.999%

14. Harmonogram projektu

Údaje sa vypĺňajú manuálne.

ID	Aktivita	Dĺžka trvania (v mesiacoch)

15. Test štátnej pomoci

Kontrolné otázky pre hodnotenie testu štátnej pomoci. Údaje sa vypĺňajú manuálne.

ID	Kontrolná otázka	A/N/NA	Bližšia špecifikácia odpovede
1	Je možné oprávnené aktivity, resp. činnosti žiadateľov v danej výzve kvalifikovať ako činnosti „nehospodárskeho" charakteru v zmysle pravidiel štátnej pomoci?	A	Áno. Cieľovým zákazníkom projektu je výhradne sektor verejnej správy, projekt by sa teda z tohto pohľadu dal nazvať "interným" projektom.
2	Je možné oprávnené aktivity resp. činnosti žiadateľov v danej výzve kvalifikovať ako „hospodárske" v zmysle pravidiel štátnej pomoci?	N	Nie. Cieľovým zákazníkom projektu je výhradne sektor verejnej správy, projekt by sa teda z tohto pohľadu dal nazvať "interným" projektom. Navyše podobná hospodárska aktivita sa na území SR ani nenachádza.

3	Sú splnené všetky kritéria (kumulovane) definované článkom 107 ods. 1 Zmluvy o fungovaní EÚ: a) prevod verejných zdrojov a pripísateľnosť štátu, b) ekonomické zvýhodnenie príjemcu pomoci, c) selektívnosť poskytnutej pomoci, d) narušenie hospodárskej súťaže alebo hrozba narušenia hospodárskej súťaže a vplyv na vnútorný obchod medzi členskými štátmi?	NA	Nie je aplikovateľné, keďže sa jedná o aktivitu nehospodárskeho charakteru.
4	Sú splnené všetky kritéria (kumulovane) definované pre služby všeobecného hospodárskeho záujmu (v zmysle rozsudku Altmark C-280/00) vrátane osobitného charakteru služby: a) podnik, ktorému bola poskytnutá pomoc bol poverený realizáciou záväzkov služby vo verejnom záujme a tieto záväzky boli jasne definované, b) kritériá, na základe ktorých je vypočítaná kompenzácia boli vopred určené objektívnym a transparentným spôsobom , c) kompenzácia nepresahuje sumu nevyhnutnú na pokrytie všetkých výdavkov alebo ich časti vzniknutých pri plnení záväzkov služieb vo verejnom záujme, zohľadniac pri tom súvisiace príjmy ako aj primeraný zisk d) ak sa výber podniku povereného realizáciou záväzkov služieb vo verejnom záujme neuskutočnil prostredníctvom výberového konania v rámci verejnej súťaže, výška nevyhnutnej kompenzácie je určená na základe analýzy výdavkov, ktoré by stredne veľký podnik, dobre riadený a primerane vybavený prostriedkami vynaložil pri realizácii týchto záväzkov, zohľadniac pri tom súvisiace príjmy ako aj primeraný zisk pri realizácii týchto záväzkov?	NA	Nie je aplikovateľné, keďže sa jedná o aktivitu nehospodárskeho charakteru.
5	Je možné pomoc zo strany poskytovateľa pomoci definovať v rámci podmienok minimálnej pomoci?	NA	Nie je aplikovateľné, keďže sa jedná o aktivitu nehospodárskeho charakteru.

Vyhodnotenie

(V závislosti od hodnotenia poskytovateľ pomoci uvedie či ide o "štátnu pomoc"; "pravidlá štátnej pomoci sa neuplatňujú"; "nie je štátna pomoc"; "SVHZ"; "pomoc de minimis"; "pomoc de minimis - SVHZ")