

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Příloha č. 2 - Požadavky na procesy poskytování EKIS MV a ISoSS

Česká republika – Ministerstvo vnitra

Obsah

1	Přehled procesů poskytování EKIS MV a ISoSS.....	3
1.1	Řízení provozu a reporting	3
1.1.1	Typy jednání	4
1.1.2	Typy reportů.....	7
1.2	Řízení požadavků a incidentů	9
1.2.1	Aplikační podpora – řízení incidentů	9
1.2.2	Aplikační podpora – řízení požadavků na rozvoj	10
1.3	Řízení rizik vyplývajících z provozu.....	10
1.3.1	Registr rizik	10
1.3.2	Procedura řízení rizik.....	11
1.4	Řízení dostupnosti služeb.....	13
1.4.1	Zavedení a změny monitoringu dostupnosti služeb	13
1.4.2	Operativní dohled dostupnosti a iniciace řešení	14
1.4.3	Reporting dostupnosti služeb.....	14
1.4.4	Plánování dostupnosti služeb	14
1.5	Řízení reklamací	15
1.6	Řízení architektury	15
1.6.1	Plánování rozvoje architektury.....	16
1.7	Řízení dodavatelů	16
1.8	Change Management.....	16
1.9	Řízení problémů	17
1.10	Release Management	17
1.11	Test Management	17
1.12	Řízení aktiv a konfiguračních položek	18
1.13	Řízení přístupu	18
1.14	IT Service Continuity Management.....	18

1 Přehled procesů poskytování EKIS MV a ISoSS

V rámci tohoto dokumentu jsou vymezena základní pravidla a požadavky na řízení procesů poskytování služeb provozu a rozvoje EKIS MV a Informačního systému o státní službě, dále jen „ISoSS“ (dále souhrnně označeno jen Systém). Poskytovatel je povinen v rámci těchto procesů poskytovat maximální součinnost. Jedná se o tyto procesy:

- Řízení provozu a reporting
- Aplikační podpora – řízení incidentů
- Aplikační podpora – řízení požadavků na rozvoj
- Řízení rizik vyplývajících z provozu
- Řízení dostupnosti služeb
- Řízení reklamací
- Řízení architektury
- Řízení dodavatelů
- Change Management
- Řízení problémů
- Release Management
- Test Management
- Řízení aktiv a konfiguračních položek
- Řízení přístupů
- IT Service Continuity Management

1.1 Řízení provozu a reporting

V této kapitole je popsán způsob řízení služeb prostřednictvím definovaných řídicích struktur, jednotlivých typů jednání a reportů zpracovávaných Poskytovatelem.

Pro účely řízení služeb je ustanovena následující řídicí struktura:

Úroveň řízení	Strana Objednatele	Strana Poskytovatele
Strategická úroveň	Náměstek ministra vnitra pro řízení sekce ekonomiky a provozu (předseda Řídicí komise EKIS MV, předseda Řídicího výboru ISoSS), náměstek ministra vnitra pro státní službu, ředitel OPRE	Zodpovědný statutární zástupce

Úroveň řízení	Strana Objednatele	Strana Poskytovatele
Řídící úroveň	Manažer EKIS Objednatele (ředitel odboru provozu a rozvoje EKIS), garanti primárních aktiv EKIS a ISoSS, Servisní manažeři Objednatele (vedoucí oddělení příp. projektový manažer)	Vedoucí sekce Obchod Poskytovatele Servisní manažeři Poskytovatele
Výkonná úroveň	Servisní manažeři Objednatele (vedoucí oddělení příp. projektový manažer), zástupci věcných správců EKIS MV a ISoSS, architekt Objednatele bezp. manažer Objednatele	Servisní manažeři Poskytovatele, projektoví manažeři Poskytovatele, architekt Poskytovatele
Operativní úroveň – realizační týmy	Manažeři nastavení EKIS MV a ISoSS, zástupci věcných správců EKIS MV a ISoSS	Konzultanti Poskytovatele

V případě neshod, nebo pokud řešená záležitost přesahuje kompetence dané řídicí úrovně je stanovena následující eskalační hierarchie:

Eskalační úroveň	1. eskalační úroveň	2. eskalační úroveň	3. eskalační úroveň
Řídící úroveň	Výkonná úroveň	Řídící úroveň	Strategická úroveň

Podněty na eskalace jsou postoupeny na vyšší řídicí úroveň pouze v případě, kdy eskalující řídicí úroveň není schopna daný podnět vyřešit.

1.1.1 Typy jednání

Řízení poskytování služeb se standardně odehrává na formalizovaných jednáních v následujícím vymezení:

Jednání	Popis	Frekvence	Účastníci	Vstupy /výstupy
Řídící Komise EKIS MV Řídící výbor ISoSS	<p>Cílem jednání je schválení strategických projektů rozvoje, řešení eskalací, které nebylo možné vyřešit na nižších řídicích úrovních projektu a případná revize finančního zabezpečení.</p> <p>Předmětem je také autorizace změn smlouvy.</p> <p>Jednání organizuje Objednatel.</p>	Ad hoc	Strategická úroveň	<p>Vstupy:</p> <p>Registr rizik</p> <p>Plán rozvoje</p> <p>Náměty na eskalace</p> <p>Výstupy:</p> <p>Zápis ŘK EKIS, ŘV ISoSS</p>
Jednání Řídící rady EKIS MV / ISoSS	<p>Cílem jednání je projednat stavy rozvojových projektů a poskytovaných služeb, změny a eskalace z výkonné a operativní úrovně řízení.</p> <p>Předmětem jednání je zejména stav připravovaných a probíhajících projektů a případné eskalace ve vztahu k poskytovaným službám.</p> <p>Jednání organizuje Objednatel ve spolupráci s Poskytovatelem.</p>	1x za kvartál	Řídící úroveň, Výkonná úroveň	<p>Vstupy:</p> <p>Stav projektů za uplynulé období</p> <p>Doporučení ze strany architektů, pokud je pro jednání relevantní</p> <p>Eskalace</p> <p>Výstupy:</p> <p>Zápis</p> <p>Plány rozvoje pro další období</p>
Jednání servisních manažerů (SM)	Předmětem jednání je stav poskytovaných služeb, rozvoj, koordinace a pánování aktivit na	Ad hoc	Servisní manažeři Objednatele a Poskytovatele	<p>Vstupy:</p> <p>Stav projektů za uplynulé období</p>

Jednání	Popis	Frekvence	Účastníci	Vstupy /výstupy
	<p>další období, projednání výsledků poskytování služeb v uplynulém období (zejména úrovně služeb, vytížení kapacit, realizovaný rozvoj, rizika).</p> <p>Jednání organizuje a vede Servisní manažer Poskytovatele nebo Objednatele.</p>			<p>Doporučení ze strany architektů, pokud je pro jednání relevantní</p> <p>Výstupy:</p> <p>Výstupem jednání jsou plány pro další období</p> <p>Zápis</p>
Risk workshop	<p>Předmětem risk workshopu je proaktivní identifikace rizik v rámci provozu a rozvoje služeb.</p> <p>Jednání organizuje a vede Objednatel ve spolupráci s Poskytovatelem.</p>	2x za rok	Výkonná úroveň	<p>Vstupy:</p> <p>Stávající registr rizik</p> <p>Výstupy:</p> <p>Aktualizovaný registr rizik</p> <p>Zápis</p>
Architektonický / integrační board	<p>Předmětem architektonického boardu je příprava a schválení plánu rozvoje architektury.</p> <p>Závěry jsou případně projednány na jednání Řídící rady EKIS, Řídícího výboru ISoSS</p> <p>Jednání organizuje a vede Objednatel ve spolupráci s Poskytovatelem.</p>	2x za rok	Výkonná úroveň	<p>Výstupy:</p> <p>Zápis</p> <p>Doporučení pro Řídící radu EKIS, Řídící výbor ISoSS</p>
Schůzky operativní úrovně	Schůzky organizuje a vede Objednatel anebo Poskytovatel, dle toho, kdo konkrétní schůzku svolává.	Ad hoc	Realizační týmy	<p>Výstupy:</p> <p>Dle dohody účastníků</p> <p>(zápis, informační mail)</p>

1.1.2 Typy reportů

Klíčové informace o poskytování služeb jsou za jednotlivé procesy agregovány do souhrnných pravidelných reportů zpracovaných zvlášť pro EKIS MV a ISoSS:

Report	Popis	Frekvence	Adresáti
Souhrnný měsíční výkaz	<p>Zpráva zahrnuje:</p> <ul style="list-style-type: none"> - Přehledy (tabulka) dosahovaných úrovní služeb (SLA) - Komentář k hlavním výpadkům služeb v období - Komentář k realizovaným a plánovaným aktivitám rozvoje - Stav realizovaných projektů (ukončené – probíhající – plánované) - Statistiku čerpání člověkohodin - Významná rizika a jejich stav <p>Přílohou zprávy jsou:</p> <ul style="list-style-type: none"> - Detailní reporty o úrovni služeb a plnění SLA - Detailní reporty spotřeby práce na drobný rozvoj a konzultace, připravené pracovníky Objednatele a zaslané na Servisního manažera Poskytovatele <p>SMV připravuje Servisní manažer Poskytovatele v rozlišení informací pro EKIS a pro ISoSS.</p> <p>SMV schvaluje ředitel OPRE a servisní manažer Poskytovatele. Následně je podkladem pro výpočet penalizací a fakturaci služeb.</p>	Měsíční	Výkonná úroveň Řídící úroveň

Report	Popis	Frekvence	Adresáti
Zápis z jednání Řídící rady EKIS / Řídícího výboru ISoSS	<p>Závěry a změny vyplývající z řídicí rady</p> <p>Dosahované úrovně služeb</p> <p>Informace o plnění SLA</p> <p>Stav realizovaných projektů</p> <p>Plán rozvojových aktivit na další období</p> <p>Komentář k plánovaným a realizovaným aktivitám rozvoje</p> <p>Rizika provozu a rozvoje služeb</p> <p>Požadavek na odstávku systému mimo dohodnutý režim</p>	1x za kvartál	Řídící úroveň a další účastníci
Zápis z jednání Servisních manažerů	Závěry a změny vyplývající z jednání servisních manažerů, plán pro další období	Ad hoc,	Účastníci jednání Servisních manažerů
Zápis z Risk worshopu	Závěry a změny vyplývající z Risk workshopu	2x za rok	Účastníci Risk worshopu
Registr rizik	<p>Evidence rizik s pravděpodobností jejich výskytu a dopadem. K registru rizik je dedikován Risk workshop 2 x za rok, nicméně významná rizika jsou uvedena v souhrnném měsíčním výkazu.</p> <p>Registr rizik je uložen na SHP Objednatele. Přístupy řídí a přiděluje odpovědný pracovník Objednatele.</p>	2x za rok	<p>Řídící úroveň</p> <p>Vybraní zaměstnanci Objednatele a Poskytovatele</p>
Zápis z architektonického / integračního boardu	Závěry a změny vyplývající z architektonického / integračního boardu	2 x za rok	Řídící úroveň Účastníci Architektonického / integračního boardu

Níže je uvedeno schéma znázorňující vazby mezi vstupy do jednání, jednáními a výstupy z jednání:

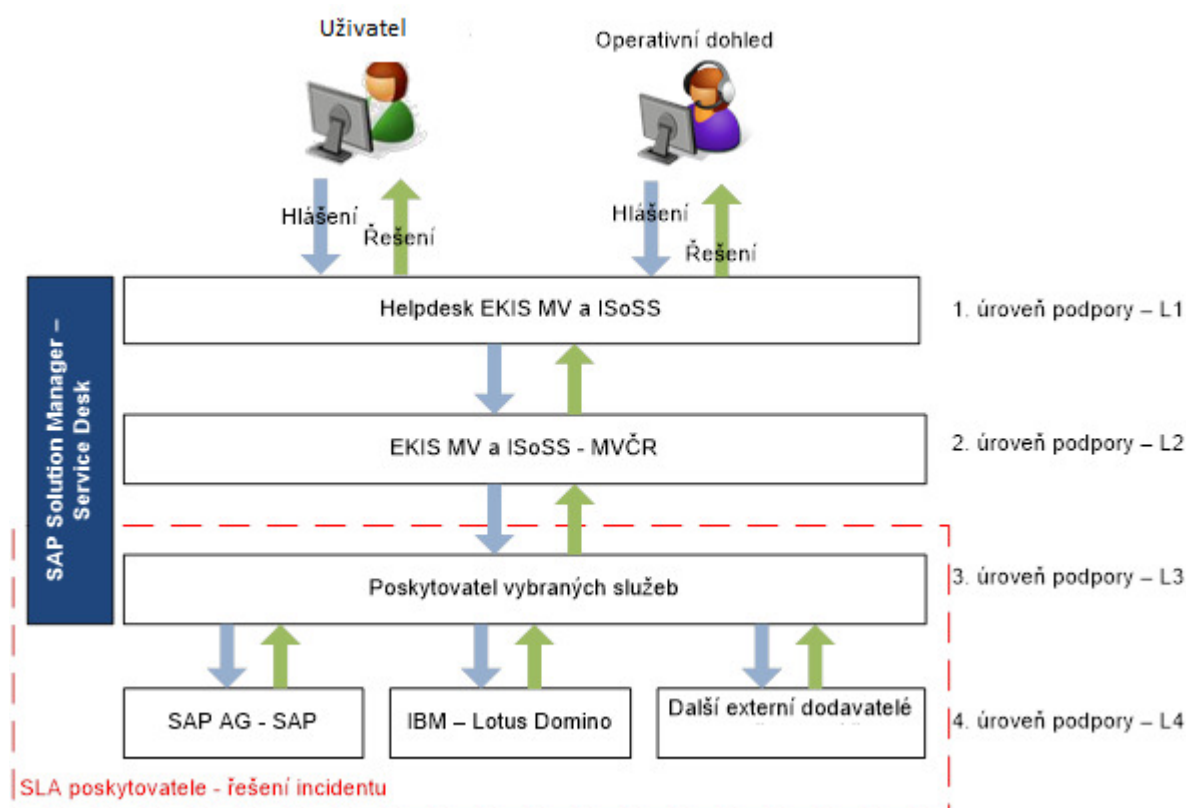
1.2 Řízení požadavků a incidentů

Incidenty a Požadavky založené uživateli jsou automaticky evidovány a zpracovávány v systému Solution Manager Objednatele.

Pro hlášení a dotazy obdržené e-mailem nebo telefonicky založí v odůvodněných případech pracovník Service Desku EKIS MV nebo ISoSS („operativní dohled“) hlášení v systému Solution Manager manuálně.

Tato úroveň je označována jako 1. úroveň podpory uživatelů – L1.

Bližší informace k procesům řízení incidentů a požadavků je uvedeno v podkapitolách níže.



Hlášení je v rámci analýzy v první úrovni podpory (L1) kategorizováno manažerem nastavení EKIS MV nebo ISoSS jako **incident** nebo jako **požadavek** s následným postoupením k řešení dle odpovídajícího procesu.

1.2.1 Aplikační podpora – řízení incidentů

Aplikační podpora v rámci provozu spočívá především v řešení incidentů, eskalovaných na třetí úroveň podpory, resp. řešení incidentů pro daný Systém nebo jeho komponentu.

V rámci aplikační podpory se Poskytovatel zavazuje zajistit řešení incidentu formou spolupráce v rámci řešitelského týmu. Pro daný incident Poskytovatel zajistí analýzu a diagnostiku incidentu, posouzení a ohodnocení chyb, návrh řešení incidentu, eventuálně návrh změn, popisu chyby a hledání náhradního řešení incidentu. Při řešení spolupracuje s konzultanty třetích stran, pokud je to potřebné.

Každý incident bez ohledu na to, kdo ho identifikoval, musí být zadán do Solution Manager. V případě, že incident není možné řešit interními zdroji Objednatelem je eskalován na 3. úroveň podpory zajišťovanou Poskytovatelem. Poskytovatel po vyřešení incidentu předá řešení příslušnému manažerovi nastavení EKIS MV nebo ISoSS k otestování. V případě, že je testováním ověřeno, že incident byl odstraněn, dochází k uzavření tiketu pro daný incident v Solution Manager a proces je ukončen. V případě neúspěšného testování je incident vrácen k řešení Poskytovateli až do jeho opětovného vyřešení. V případě, že konzultant Poskytovatele není schopen incident vyřešit vlastními silami, zabezpečí eskalaci incidentu na 4. úroveň podpory. Poskytovatel nadále nese vůči Objednateli zodpovědnost za vyřešení uvedeného incidentu. Při eskalaci na 4. úroveň podpory Objednatel zajistí na základě žádosti Poskytovatele přístupy pro požadované prostředí (v případě nutnosti i pro produktivní prostředí).

1.2.2 Aplikační podpora – řízení požadavků na rozvoj

Aplikační podpora v rámci rozvoje spočívá především v řešení požadavků na rozvoj.

Rozvoj systémů může obsahovat jakýkoliv vývoj nebo konfiguraci spojenou s aplikacemi, které jsou provozovány Objednatelem. Součástí rozvojové aplikační podpory je také řešení rozvoje EKIS MV a ISoSS na základě legislativních změn.

Požadavky na rozvoj mohou být definovány věcným správcem / metodikem nebo manažery nastavení. Všechny požadavky na rozvoj budou manažerem nastavení Objednatele před zahájením realizace zadány do Solution Manager a předány Poskytovateli, který provede následující úkony:

- Rámcově navrhne způsob řešení;
- Odhadne / zpřesní počet člověkodů potřebných k realizaci;
- Rámcově popíše dopady změny do systému.

Před realizací musí být požadavek schválen manažerem nastavení Objednatele.

V případě, že se jedná svým rozsahem a komplexností o projekt, Poskytovatel v součinnosti s Objednatelem zajistí přípravu plánu projektu a zahájí tvorbu cílového konceptu (resp. aktualizaci existujících cílových konceptů) a po jeho schválení realizaci úprav.

Po ukončení realizace je změna předána k akceptačním testům a po akceptaci manažerem nastavení EKIS / ISoSS nebo věcným správcem a servisním manažerem Objednatele může být změna přenesena do produktivního prostředí.

Plánování a čerpání člověkodů na realizaci požadavků na rozvoj je evidováno pomocí nástroje Solution Manager.

1.3 Řízení rizik vyplývajících z provozu

Všechna podstatná rizika musí být dokumentována a analyzována, ke každému riziku musí být naplánována a implementována přiměřená reakce.

1.3.1 Registr rizik

Všechna identifikovaná rizika musí být zaznamenána v registru rizik. Registr rizik spravuje Servisní manažer Poskytovatele. Registr rizik schvaluje odpovědný zástupce Objednatele a Poskytovatele.

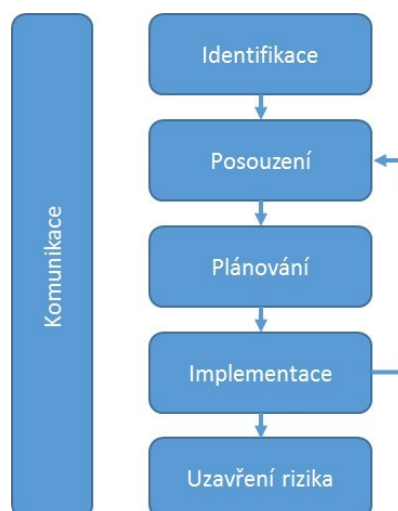
Registr rizik je uložen na SHP Objednatele, přístupy k registru přiděluje a řídí Objednatel.

Registr rizik obsahuje následující údaje:

- Kdo identifikoval riziko	- Dopad vč. kvantifikace
- Kdy bylo riziko identifikováno	- Kategorie reakce na riziko
- Kategorie rizika	- Popis aktivit reakce na riziko
- Popis rizika (příčina, k jaké události je vázáno, co se může stát)	- Status rizika
- Pravděpodobnost	- Vlastník rizika
	- Vykonavatel aktivit

1.3.2 Procedura řízení rizik

Procedura řízení rizik zahrnuje Identifikaci, posouzení, plánování, implementaci a komunikaci. Posloupnost kroků zachycuje následující schéma.



1.3.2.1 Identifikace

Cílem identifikace rizik je rozpoznání hrozeb/zranitelností (rizik), které mohou negativně ovlivnit provoz a rozvoj systému EKIS a ISoSS.

Rizika mohou být hlášena ad-hoc kterýmkoliv pracovníkem Objednatele a Poskytovatele. Rizika jsou rovněž identifikována proaktivně formou Risk workshopů (četnost viz Typy jednání).

V rámci identifikace rizika jsou dokumentovány tyto aspekty:

- Možná příčina, resp. zdroj rizika;
- Popis události nebo oblasti, ke které se riziko váže;
- Popis možných dopadů rizika, tj. co se může stát, pokud riziko nastane.

1.3.2.2 Posouzení

Předmětem posouzení rizika je odhad pravděpodobnosti hrozby/zranitelnosti a dopadu rizika na aktivitu.

<p>Kategorie pravděpodobnosti hrozby/zranitelnosti:</p> <ul style="list-style-type: none"> - Nízká - Střední - Vysoká - Kritická 	<p>Kategorie dopadu rizika na aktivitu:</p> <ul style="list-style-type: none"> - Nízký (riziko ohrožuje aktivitu na úrovni části modulu systému EKIS MV nebo ISoSS, cíl či harmonogram dílčí aktivity v rámci etapy projektu) - Střední (riziko ohrožuje aktivitu na úrovni celého modulu systému EKIS MV nebo ISoSS, cíl či harmonogram dílčí části/etapy projektu nebo rozvojového projektu) - Vysoký (riziko ohrožuje aktivitu na úrovni celého systému EKIS MV nebo ISoSS, cíl, projektu, harmonogram či rozpočet) - Kritický (riziko narušení dostupnosti aktivity není přípustné, a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktivita je považována za kritickou.)
--	--

Posouzení rizika navrhuje Servisní manažer Poskytovatele. Návrh posouzení rizika vč. plánu jeho ošetření je projednán a schválen na nejbližším Risk workshopu.

Rizika, která jsou posouzena v obou kategoriích současně jako vysoká nebo kritická, musí být eskalována na řídicí úroveň.

Rizika, která jsou posouzena v obou kategoriích současně jako střední nebo nízká jsou řešena na úrovni jednání Risk workshopu.

1.3.2.3 Plánování

Předmětem plánování je zvolení přiměřené reakce na riziko, stanovení zodpovědných rolí a naplánování příslušných aktivit (plán zvládnutí rizik). Při plánování je riziku přidělena jedna z následujících kategorií reakce na riziko:

- Zamezení rizika – předmětem je opatření nebo změna, která riziko zcela vyloučí.
- Snížení rizika – předmětem je opatření nebo změna, která sníží úroveň dopadu nebo pravděpodobnosti rizika.
- Záložní plán – předmětem je návrh postupu (plánu), který ošetří dopady rizika v případě, kdy riziko nastane.
- Přenesení rizika – předmětem je přenesení některých finančních dopadů rizika na třetí stranu.
- Přijetí rizika – přijetí rozhodnutí, že možné dopady rizika jsou nižší než nároky jeho ošetření. Riziko bude nadále monitorováno.

1.3.2.4 Implementace

Předmětem ošetření rizika je vykonání naplánovaných aktivit reakce na riziko a průběžné monitorování stavu a parametrů rizika. Jsou definovány následující zodpovědnosti rolí, které byly nominovány v rámci plánování rizik:

- **Vlastník rizika** – osoba zodpovědná za řízení, monitoring a kontrolu všech aspektů daného rizika včetně implementace plánovaných aktivit reakce na riziko.
- **Vykonavatel aktivit** – osoba zodpovědná za realizaci naplánovaného opatření k danému riziku. Jeho úkolem je podporovat a realizovat úkoly od vlastníka rizika směřující k ošetření rizika a minimalizaci jeho dopadů.

Vlastník rizika a vykonavatel aktivit může být jedna a tatáž osoba.

Po implementaci může být riziko uzavřeno nebo se proces vrací do fáze Posouzení.

1.3.2.5 Komunikace

Významná rizika (vysoká a velmi vysoká) jsou zahrnuta do souhrnného měsíčního výkazu.

Pokud je to nutné, komunikují zodpovědní Servisní manažeři Objednatele vhodnou formou informace o rizicích zástupcům dotčených skupin uživatelů. Komunikace probíhá v průběhu celého procesu řízení rizik.

1.4 Řízení dostupnosti služeb

Řízení dostupnosti je zaměřeno především na proaktivní identifikaci výpadků dostupnosti, snižování jejich počtu, dopadů a délky jejich trvání. V dlouhodobém měřítku je cílem dosažení nákladově optimální úrovně dostupnosti služeb při současném splnění obchodních požadavků na jejich dostupnost. V neposlední řadě poskytuje proces řízení dostupnosti podklady pro vyhodnocení úrovně služeb a vyúčtování služeb.

Řízení dostupnosti se skládá z následujících aktivit:

- Zavedení a změny monitoringu dostupnosti služeb
- Operativní dohled dostupnosti a iniciace řešení
- Roční přehled dostupnosti služeb
- Schvalování plánovaných výpadků dostupnosti
- Plánování dostupnosti služeb

1.4.1 Zavedení a změny monitoringu dostupnosti služeb

Nastavení monitoringu dostupnosti by mělo být realizováno v rámci změnového řízení zavedení nebo změny služby.

Požadovaná úroveň dostupnosti ICT služby a způsob jejího vykazování by měly být definovány v rámci návrhové fáze řízení změny zavedení nebo změny služby. Návrh požadované úrovně dostupnosti musí být konzultován se zodpovědným servisním manažerem s cílem nalezení optimální rovnováhy mezi úrovní dostupnosti a celkové nákladovosti řešení služby.

Na základě požadavků je zpracován návrh monitoringu dostupnosti služby, který zahrnuje především:

- Určení technické metody monitoringu

- Definice notifikací
- Zpracování podkladů pro dohled systému a popis reakcí na zjištěné události.

Vlastní nastavení monitoringu se skládá z:

- Zavedení monitoringu dostupnosti služby pro účely operativního dohledu služby (detekce a identifikace poruchových stavů, zahájení řešení, minimalizace doby výpadku).
- Zavedení služby do reportu dostupnosti.

Po zavedení monitoringu je kontinuálně vyhodnocována kvalita dostupnosti služby a prováděny korekce nastavení monitoringu.

Návrh monitoringu dostupnosti služeb zpracovává Poskytovatel služby. Zavedení a změny monitoringu dostupnosti služby jsou předmětem schválení ze strany zodpovědného servisního manažera Objednatele.

1.4.2 Operativní dohled dostupnosti a iniciace řešení

Úlohou operativního dohledu dostupnosti služeb je sledování nestandardních stavů zjištěných automatickými monitorovacími systémy nebo na základě definovaných manuálních kontrol, identifikace výpadků a iniciace jejich řešení s cílem minimalizovat nedostupnost ICT služeb.

Zajišťování operativního dohledu služeb je zodpovědností Objednatele a Poskytovatel by měl poskytnout minimálně následující činnosti:

- Poskytování součinnosti řešitelům incidentu při identifikaci příčin a dopadů výpadku.

1.4.3 Reporting dostupnosti služeb

Proces řízení dostupnosti zajišťuje periodické vyhodnocování parametrů dostupnosti definovaných v rámci katalogu služeb a je přílohou Souhrnného měsíčního výkazu.

Podkladem pro zpracování přehledu dostupnosti služeb je seznam všech naměřených výpadků doplněný o seznam výpadků nahlášených formou incidentu, které nebyly pokryty automatickým měřením.

Report má dvě úrovně podrobnosti – celkový přehled dostupnosti služeb a detailní rozbor výpočtu dostupnosti služby.

Sestavení reportu a vyhodnocení dostupnosti by měl obsahovat tyto dílčí činnosti:

- Přehled naměřených výpadků
- Identifikace chybně naměřených výpadků, které neměly dopad na dostupnost služby
- Identifikace nahlášených incidentů, které způsobily výpadek služby, který nebyl zachycen monitorovacími systémy
- Schválení reportu dostupnosti a návrh korekcí Poskytovatelem
- Zajištění podpory Poskytovateli při interpretaci a obhajobě vykázané dostupnosti

Report dostupnosti je součástí pravidelné měsíční zprávy o poskytování služeb. Následně se stává jedním z podkladů pro vyúčtování služeb.

1.4.4 Plánování dostupnosti služeb

Jednou ročně se zpracovává Plán dostupnosti.

Plán dostupnosti má následující obsah:

- Stanovení metody měření dostupnosti služeb
- Dosahované hodnoty dostupnosti služeb a přehled příčin výpadků
- Návrh opatření pro zvýšení dostupnosti služeb a prevenci výpadků
- Roční plán servisních odstávek

1.5 Řízení reklamací

Ze smluvních vztahů mezi Objednatelem a Poskytovatelem vyplývají lhůty na reklamaci, které se vztahují jak k celkovému dílu, tak k dílčím dílům vzniklým na základě rozvoje služeb.

Vada, která má charakter incidentu, je řešena stejným způsobem jako ostatní incidenty. Za předpokladu, že řešení vady nevyžaduje čerpání prostředků z rozpočtu rozvoje, není mezi standardním incidentem a vadou rozdíl.

Pokud má vada závažnější charakter a je řešena formou požadavku na rozvoj, jdou náklady na vynaložené zdroje k tíži Poskytovatele služeb a neměly by být zahrnuty do čerpání rozpočtu rozvoje.

Rozhodnutí je předmětem dohody zodpovědného Servisního manažera Objednatele a Servisního manažera Poskytovatele. V případě neshody je uplatněno standardní eskalační řízení.

K řešené vadě se vztahují lhůty pro odstranění vady a slevy z těchto lhůt vyplývající z Přílohy č. 3 Smlouvy. Ty mohou být uplatněny souběžně s uplatněním penalizací za snížení úrovně poskytovaných služeb (např. v rámci parametrů dostupnosti služeb).

1.6 Řízení architektury

Řízení, udržování a dokumentování architektury zahrnuje systémy EKIS MV a ISoSS. Architektura zahrnuje následující dílčí architektonické vrstvy:

- Motivační architektura (zajišťuje Objednatel)
- Business architektura (zajišťuje Objednatel)
- Architektura informačního systému (zajišťuje Poskytovatel)
 - Datová architektura
 - Aplikační architektura
 - Definice požadavků na technologickou infrastrukturu (*pozn. realizaci těchto požadavků zajišťuje Objednatel*)

Každý změnový požadavek, který má dopad na architekturu systémů, by měl být posouzen architektem v případě, že se dotkne některého z níže uvedených témat a navržené řešení by mělo být v souladu s principy a pravidly navržené architektury.

Architektura je povinna zabývat se těmito tématy:

- Integrace mezi službami.

- Dopady a vazby na strategie MV (ISVS, RPP, JIP, KAAS, ISZR, centrální místo služeb, SOCCR, Datové schránky).
- Dopady a vazby na strategie mimo rezort MV (ČNB, IISSP, CRAB a další)
- Požadavky s přesahem definovaných služeb, tj. nad rámec smluvních vztahů mezi Objednatel a Poskytovatelem.
- Vedení a aktualizace dokumentace v Archimate.

1.6.1 Plánování rozvoje architektury

Pro účely plánování rozvoje architektury je ustanoven Architektonický board.

Architektonický board je veden hlavním architektem Poskytovatele a účastní se jej vybraní pracovníci Poskytovatele a Objednatele (standardně servisní manažeři a manažeři nastavení).

Cílem Architektonického boardu je sestavování plánu rozvoje architektury. Podkladem pro plán rozvoje architektury jsou především následující aspekty:

- Identifikované koncepční nedostatky stávající architektury (např. v oblasti zajištění požadované dostupnosti služeb atp.).
- Předpokládané rozvojové požadavky EKIS MV a ISoSS (např. plánované změny legislativy, uživatelské požadavky atp.).
- Plány rozvoje okolních informačních systémů (ostatní IS resortu MV, centrální registry atp.).
- Plány výrobců SW na další rozvoj a podporu produktů využívaných v systémech EKIS MV a ISoSS.
- Trendy na trhu a best practices z jiných projektů.

1.7 Řízení dodavatelů

Řízení dílčích dodávek je plně v kompetenci Poskytovatele, který je zodpovědný za přenesení podmínek a parametrů provozu a rozvoje služeb EKIS MV a ISoSS, včetně zajištění všech bezpečnostních pravidel i na případné subdodavatele.

V kontextu smluvního zajištění provozu a rozvoje EKIS MV a ISoSS se nepředpokládá, že by si Objednatel najímal dílčí dodávky samostatně a separátně od kontraktu s Poskytovatelem. Výjimkou mohou být projekty realizované v rámci operačních programů Evropské unie a přímý dokup SW licencí.

1.8 Change Management

Cílem procesu je řídit celý životní cyklus veškerých změn v provozovaných systémech za co nejnižšího omezení provozu.

Relevantní požadavky budou zadány k analýze, přičemž, v rámci této analýzy Poskytovatel stanoví pracnost, návrh termínu realizace, požadavky na součinnost a dopad do stávající infrastruktury/provozu.

Požadavek musí být schválen Objednatel.

Požadavky jsou schvalovány také zástupci architektury Objednatele a Poskytovatele z pohledu dopadů do infrastruktury a celkové koncepce řešení. Objednatel určuje, jestli požadavky budou řešeny z drobného rozvoje nebo dílčí smlouvou.

V rámci Change Managementu je realizován proces transportu změn do produktivního prostředí pouze prostřednictvím Solution Managera (pokud je to technicky možné) dle požadavku zapsaného v systému Solution Manager.

Jakýkoli transport mimo Solution Manager, pokud se smluvní strany nedohodnou jinak, je považován za bezpečnostní incident. Transport je realizován směrem vývoj → test → produkce. Výjimky jsou pouze v mimořádných situacích, kdy se po akci provede záznam do Solution Managera.

1.9 Řízení problémů

Problém je příčinou jednoho nebo více incidentů a cílem procesu je problémy detekovat, evidovat a následně zabránit jejich opakovanému výskytu. Podstatou procesu je znalostní báze o známých incidentech a řízení jejich životních cyklů. Budou evidovány náhradní postupy, pokud není možné incident odstranit okamžitě.

1.10 Release Management

Cílem procesu je řídit přípravu a uvolňování jednotlivých release. Release Management obsahuje následující fáze:

- Plánování release
- Vývoj
- Testování release
- Nasazení
- Vyhodnocení a uzavření.

1.11 Test Management

Test Management je možné považovat za součást Release Managementu, nicméně proces je vzhledem k jeho komplexnosti popsán zvlášť.

Testování je rozděleno do 3 fází:

- Příprava testů: V této fázi je potřeba zajistit, aby byly zajištěny veškeré předpoklady pro realizaci testů (připravená prostředí, testovací scénáře, testovací data, nástroje pro testování apod.) a dále stanovit nezbytné role na straně Poskytovatele a Objednatele (testeři, vedoucí testování, designéři testovacích scénářů, analytici apod.).
- Realizace testů: Jedná se o samotné testování, musí být stanoven způsob evidence nálezů a proces jejich vypořádání.
- Vyhodnocení testů: V rámci vyhodnocení testů musí být jednoznačně stanoven výsledek testování. Je rozhodnuto o opakování testů případně o nasazení testované verze Do prostředí Produkce. V tomto případě jsou testy formálně uzavřeny.

Proces Test Management (výše uvedené 3 fáze) je v kompetenci a odpovědnosti Objednatele, pokud samozřejmě není testování součástí procesu zajišťované podpory, drobného rozvoje

a realizace rozvojových projektů. To je zpravidla v zodpovědnosti Poskytovatele, pokud není dohodnuto jinak. Součástí Test managementu je vždy poskytování součinnosti druhou stranou.

1.12 Řízení aktiv a konfiguračních položek

Cílem procesu je řízení aktiv nezbytných pro provoz IT služeb.

Nejvyšší úroveň aktiv je zachycena v Příloze č. 5 Architektura EKIS MV a ISOSS.

Konfigurační položka je aktivum nezbytné pro provoz služby (například jiné aplikační služby IT, SW, lidé, dokumentace apod.) O konfiguračních položkách budou v centrální evidenci vedeny a aktualizovány záznamy, aby bylo možné určit jejich stav. V případě, že je stav nevyhovující, je nutné přijmout reakční opatření.

Za evidenci aktiv a konfiguračních položek odpovídá Objednavatel. Poskytovatel poskytuje součinnost – informuje o realizovaných změnách, které provádí po předchozím souhlasu Objednavatele.

1.13 Řízení přístupu

Tento proces patří do oblasti bezpečnosti. Cílem procesu je zajistit, že k datům a službám budou přistupovat pouze oprávnění uživatelé. Řízení přístupu musí zohledňovat bezpečnostní politiky Objednavatele. Kdo má mít přístup k aktivu (služba či data), rozhoduje vlastník tohoto aktiva. Proces se skládá z následujících činností:

- Příjem požadavků na zřízení / změnu / zrušení přístupu
- Ověření identity uživatele a ověření oprávněnosti nakládání s požadovaným aktivem včetně druhu oprávnění (čtení /změnu)
- Monitoring přístupů uživatelů k aktivům dle jejich přístupových práv
- Případná iniciace odejmutí oprávnění
- Správa bezpečnostních incidentů.

Řízení přístupu je plně v kompetenci a odpovědnosti Objednavatele a proces je popsán v Bezpečnostní dokumentaci.

1.14 IT Service Continuity Management

Cílem procesu je obnova funkčnosti služeb Systému po rozsáhlém výpadku. Je požadováno definovat strategie obnovy a zpracovat plány Disaster recovery těchto služeb a implementace zvolených opatření.

Zpracovává Objednavatel v součinnosti s Poskytovatelem.

