- Zpráva o ukončení projektu

Role a odpovědnosti:

- Programový management – určuje tolerance projektu.
- Sponzor – určuje tolerance na etapu, rozhoduje o Plánu realizace výjimek.
- Projektový vedoucí – monitoruje postup a porovnává jej proti plánu, autorizuje balíky práce.
- Týmový manažer – přijímá (schvaluje) Balíky práce, informuje Projektovou podporu o dokončených činnostech v rámci kvality, informuje projektového vedoucího o všech odchylkách.
- Projektový dohled – ověřuje obchodní případ s ohledem na externí vlivy, potvrzuje, že postup etapy/projektu je v souladu s dohodnutými tolerancemi.

2.3 Objednávka

Detailní proces je pospán v Rámcové dohodě – uzavírání objednávek. Zde jsou uvedeny pouze základní procesní kroky k uzavření objednávky.

1. Jednotlivé dohody o dílčím plnění na poskytování Plnění budou uzavírány na základě písemné výzvy k podání nabídek adresované ze strany Objednatele všem dodavatelům dle § 135 odst. 1 písm. a) ZZVZ
2. Objednatel se zavazuje zaslat Dodavateli Výzvu prostřednictvím elektronického nástroje Tender arena (https://www.tenderarena.cz/). Objednatel je oprávněn změnit elektronický nástroj, musí však o každé změně vyrozumět písemně Dodavatele. Změna elektronického nástroje je vůči Dodavateli účinná okamžikem, kdy o ní byl písemně vyrozuměn.
3. Výzva bude obsahovat minimálně:
   a. vymezení a popis požadovaného Plnění v souladu s přílohou č. 1 Rámcové dohody;
   b. místo a dobu realizace Plnění;
   c. závazný návrh Objednávky dle podmínek konkrétního Plnění;
   d. lhůtu, způsob a místo pro podání nabídek; délka lhůty pro podání nabídek bude přiměřená charakteru a náročnosti úkonů vyžadovaných od Dodavatele pro přípravu jeho nabídky;
   e. údaje o kritériích hodnocení a metodě hodnocení; způsob výběru nejvýhodnější nabídky bude vycházet ze Zadávací dokumentace.
4. Dodavatel je povinen v případě svého zájmu na základě Výzvy podat nabídku (dále jen „Nabídka“) ve lhůtě stanovené ve Výzvě, a to prostřednictvím elektronického nástroje dle odst. 4.2 Rámcové dohody.

2.4 Realizace projektu

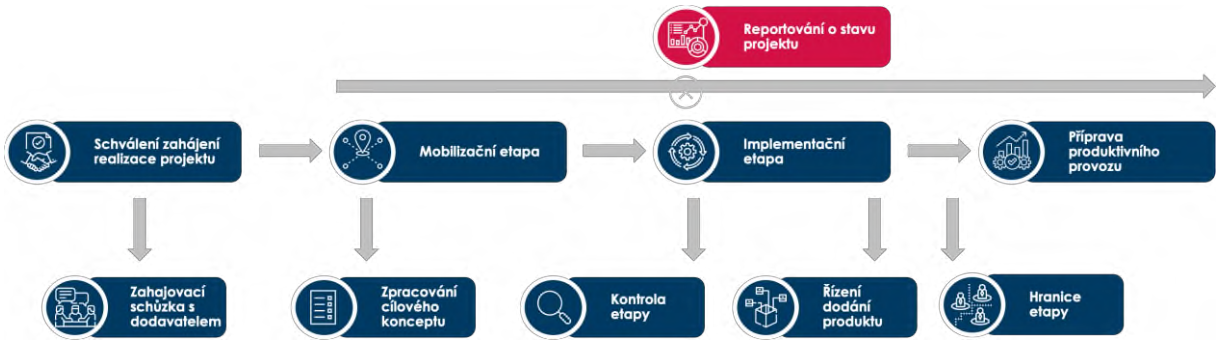
Realizace projektu je fáze v projektovém řízení, ve které se plány a strategie, které byly připraveny v předchozích fázích, přeměňují do skutečného výsledku nebo produktu. Tato fáze zahrnuje **mobilizační etapu, implementační etapu, přípravu produktivního provozu a průběžné monitorování a reportování pokroku a správu zdrojů**. Fáze realizace projektu je zahájena po

schválení připravených podkladů k řízení projektu a v případě konání VZ, tak po podpisu smlouvy s dodavatelem.

Vstupním procesem fáze realizace projektu je schválení zahájení realizace projektu.

Realizace projektu se skládá ze **3 základních etap**:

1. Mobilizační etapa (zpracování prováděcího projektu)
2. Implementační etapa (kontrola etapy, řízení dodání produktu, hranice etapy)
3. Příprava produktivního provozu



2.4.1 Schválení zahájení realizace projektu

Tento krok je možný uskutečnit až **po podpisu smlouvy s vítězným uchazečem** (dále jen dodavatelem).

Výkonný výbor schvaluje:

- **Výsledky výběrového řízení**
- **Plán projektu**
- **Organizační strukturu a role** (včetně zástupců uživatelů a dodavatelů v realizačním týmu)

Následně **Sponzor projektu informuje Výkonný výbor** o zahájení realizace projektu.

Dalším krokem v rámci realizace projektu je zorganizování zahajovací schůzky s dodavatelem. Před uskutečněním zahajovací schůzky s dodavatelem projektový vedoucí požádá o přípravu prezentace na tuto schůzku. Prezentace by měla obsahovat tyto údaje:

- **Představení dodavatele**
- **Rozsah prací**
- **Harmonogram**
- **Kontaktní matice dodavatele**
- **Požadované součinnosti**
- **Další kroky**

Tato schůzka slouží především k představení dodavatele a seznámení se se základním rámcem a informacemi o projektu.

Projektový vedoucí zašle informace na projektovou kancelář, která aktualizuje kontaktní matici a všem členům týmu zajistí přístup do společného úložiště.

2.4.2 Mobilizační etapa

Mobilizační etapa je zahájena předáním šablony „**Prováděcí projekt**“ dodavateli s požadavkem o jeho vypracování.

Prováděcí projekt je ústředním dokumentem pro realizaci projektu a obsahuje:

- Detailní analýzu
- Analýzu současného stavu
- Analýzu nových požadavků
- Návrh řešení
- Technologické zajištění provozu
- Organizační zajištění provozu
- Katalog požadavků
- Definici datového rozhraní
- Systémovou a bezpečnostní politiku
- Požadovanou součinnost.

Dodavatel vypracuje prováděcí projekt v **požadované struktuře včetně testovacích scénářů.** Jeho činnost je koordinována projektovým manažerem dle schváleného plánu projektu a smlouvy s dodavatelem.

Následně je dokument zaslán do připomínkovacího řízení a je spuštěn proces připomínkování.

Prováděcí projekt je schválen Sponzorem projektu a Klíčovým uživatelem. Po schválení je zahájen proces akceptačního řízení. Projektový manažer připraví Předávací protokol a Akceptační protokol. Společně s manažerem dodavatele jej vyplní a zajistí podepsání obou dokumentů. Podepsané protokoly jsou společně s Prováděcím projektem vloženy na MS Teams / SharePoint.

Projektový manažer aktualizuje Plán projektu na základě schváleného prováděcího projektu. Dodefinuje jednotlivé etapy s termíny po konzultaci s klíčovým uživatelem a hlavním dodavatelem v souladu se smlouvou s dodavatelem.

2.4.3 Kontrola etapy

Kontrola etapy probíhá průběžně v rámci řízení etapy a zahrnuje:

- každodenní práci projektového manažera – **přidělování, monitoring a kontrola úkolů**.

- **řízení rizik a otevřených bodů** – eviduje je, analyzuje a vyhodnocuje, nastavuje opatření, případně eskaluje výkonnému výboru.
- **reportování zprávy o stavu etapy** výkonnému výboru a **eskalace otevřených bodů a rizik** (v případě, kdy hrozí překročení tolerancí etapy).

Kontrola etapy obsahuje níže uvedené procesy:

2.4.3.1 Řízení úkolů

Detailně je tento proces popsán v kapitole registr úkolů.

2.4.3.2 Řízení rizik

Detailně je tento proces popsán v kapitole řízení rizik.

2.4.3.3 Řízení otevřených bodů

Detailně je tento proces popsán v kapitole řízení otevřených bodů.

2.4.3.4 Řízení změn

Detailně je tento proces popsán v kapitole řízení změn.

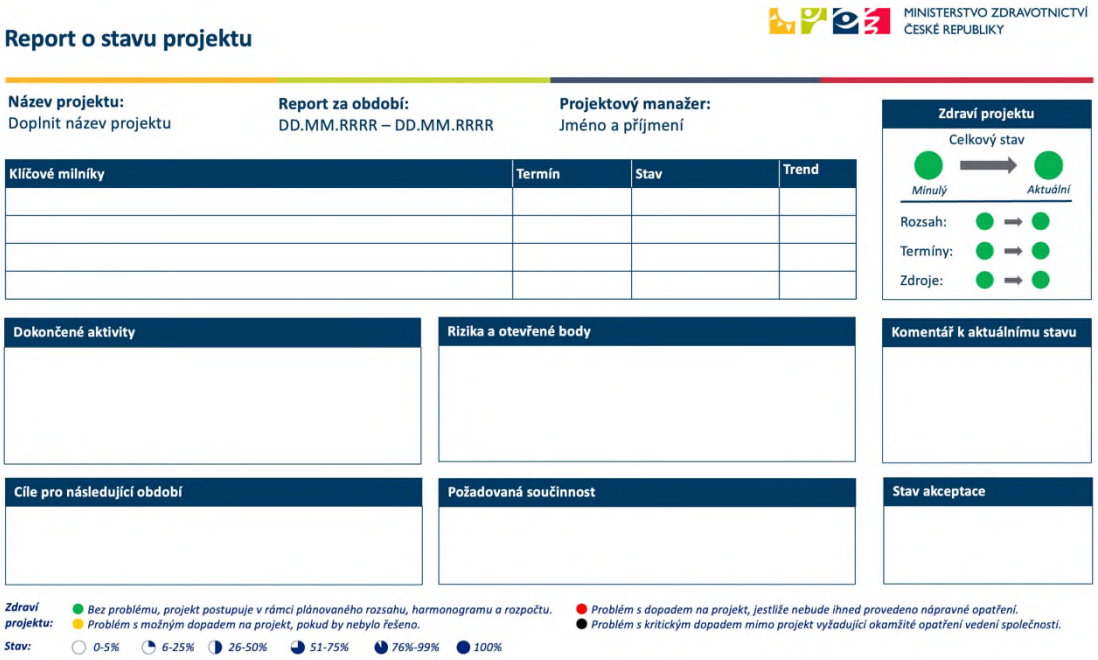
2.4.3.5 Reportování o stavu projektu

V rámci této činnosti připravuje projektový manažer šablonu „**Report o stavu projektu**“. Zpráva poskytuje výkonnému výboru v předem daných intervalech souhrnné informace o projektu.

Účelem reportu je poskytnout výkonnému výboru (nebo jiným zainteresovaným stranám) souhrnnou informaci o stavu projektu v pravidelných intervalech. Používá se k monitorování postupu a signalizování potenciálních problémů výkonnému výboru.

Zpráva je vytvářena v 7denní frekvenci nebo dle dohody.

2.4.3.5.1 Report o stavu projektu



Report o stavu projektu

MINISTERSTVO ZDRAVOTNICTVÍ ČESKÉ REPUBLIKY

Název projektu: Doplnit název projektu

Report za období: DD.MM.RRRR – DD.MM.RRRR

Projektový manažer: Jméno a příjmení

Klíčové milníky	Termín	Stav	Trend

Zdraví projektu

Celkový stav — Minulý → Aktuální

Rozsah: → Termíny: → Zdroje: →

Dokončené aktivity

Rizika a otevřené body

Komentář k aktuálnímu stavu

Cíle pro následující období

Požadovaná součinnost

Stav akceptace

Zdraví projektu: Bez problému, projekt postupuje v rámci plánovaného rozsahu, harmonogramu a rozpočtu. / Problém s možným dopadem na projekt, pokud by nebylo řešeno. / Problém s dopadem na projekt, jestliže nebude ihned provedeno nápravné opatření. / Problém s kritickým dopadem mimo projekt vyžadující okamžité opatření vedení společnosti.

Stav: 0-5% / 6-25% / 26-50% / 51-75% / 76%-99% / 100%

2.4.3.5.2 Zdraví projektu

Zdraví projektu odkazuje na celkový stav a výkonnost projektu v průběhu jeho realizace. Je to komplexní hodnocení různých aspektů projektu, které zahrnuje: celkový stav, rozsah, termíny a zdroje.

V rámci zdraví projektu je využívána čtyř barevná škála:

- Bez problému, projekt postupuje v rámci plánovaného rozsahu, harmonogramu a rozpočtu.
- Problém s možným dopadem na projekt, pokud by nebylo řešeno.
- Problém s dopadem na projekt, jestliže nebude ihned provedeno nápravné opatření.
- Problém s kritickým dopadem na projekt vyžadující okamžité opatření vedení společnosti.

Projektový vedoucí vždy aktualizuje zdraví projektu jak pro minulé reportovací období, tak i aktuální.

2.4.3.5.3 Klíčové milníky

Projektový vedoucí doplní klíčové milníky. Jedná se o termíny, které označují dokončení klíčové fáze nebo dosažení klíčového cíle projektu (většinou jsou definované ve smlouvě).

V rámci sledování plnění klíčových milníků projektový vedoucí pravidelně aktualizuje stav a trend. Samotné klíčové milníky a jejich termín je neměnný.

2.4.3.5.4 Stav

pro sledování stavu plnění klíčového milníku je používána procentuální hodnota plnění.

Ta je vypočítává následujícím způsobem:

$$\left(\frac{Stav\ přípravy\ výstupů}{Celkový\ plánovaný\ stav\ přípravy\ výstupů}\right) x\ 100 = Procentuální\ plnění$$

Dle procentuálního plnění je doplněn jeden z uvedených stavů:

○	0-5 %
◔	6-25 %
◑	26-50 %

◕	51-75 %
◕	76-99 %
●	100 %

Dále projektový vedoucí doplní trend, dle kterého bude probíhat plnění klíčového milníků.

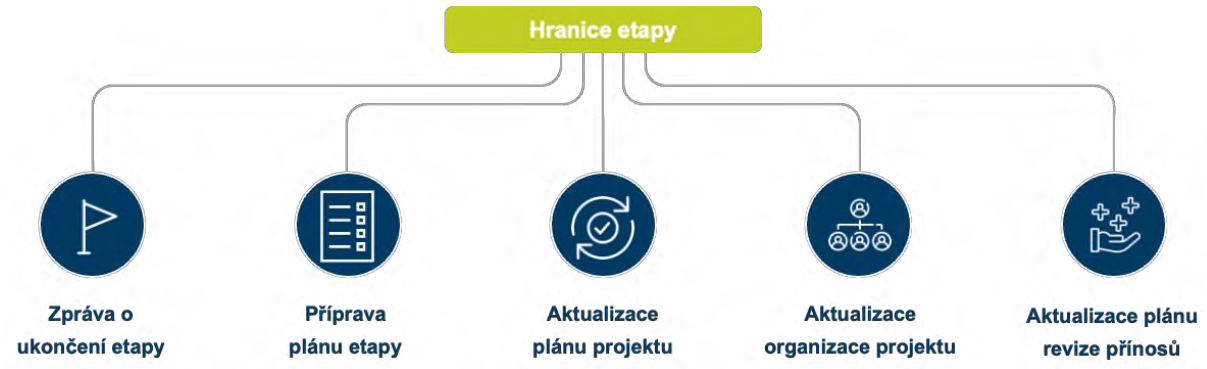
2.4.4 Hranice etapy

Hranice etapy jsou strategickými body v průběhu projektu, kde se provádí **hodnocení dosažených výsledků, plánů pro další fázi a celkového stavu projektu**.

Účelem procesu řízení hranice etapy je:

- **Dokončení a vyhodnocení stávající etapy.**
- **Detailní plánování následující etapy.**
- Aktualizace Projektového plánu.
- **Posouzení stavu rizik.**
- Příprava zprávy pro Výkonný výbor.
- **Zpracování monitorovací zprávy pro řídící orgán.**

V rámci hranice etapy je nutné provést 5 základních kroků:



2.4.4.1 Zpráva o ukončení etapy

V rámci této aktivity připravuje projektový vedoucí pro Výkonný výbor Zprávu o ukončení etapy. V rámci reportování ukončené etapy posuzuje stav rizik, otevřených bodů a kvality, vyhodnocuje plnění rozpočtu a harmonogramu. Zpráva slouží jako podklad pro čerpání finančních prostředků/ platby dílčích faktur dodavatele. Pro přípravu zprávy je využívána šablona „Zpráva o ukončení etapy“.

2.4.4.2 Příprava plánu etapy

Pro každou etapu je zpracováván detailní plán etapy. Jedná se o harmonogram vycházející z projektového plánu rozpracovaný do větších detailů tak, aby bylo možné etapy dobře kontrolovat a řídit. Zkrácením plánovacího horizontu je možné dosáhnout efektivnějšího a přesnějšího plánování. Plán etapy obsahuje termíny pro etapu, produkty, které budou dodané v této etapě. Plán etapy zpracovává projektový vedoucí a je využívána šablona „Plán etapy“.

2.4.4.3 Aktualizace plánu projektu

Projektový vedoucí po vypracování plánu etapy aktualizuje a zreviduje plán projektu. Promítne do něj změny a upřesnění.

2.4.4.4 Aktualizace organizace projektu

Projektový vedoucí po vypracování plánu etapy aktualizuje a zreviduje organizaci projektu. Promítne do ní plánované produkty a aktivity následující etapy, resp. potřebné kvalifikace pro jejich dodání a posouzení.

2.4.4.5 Aktualizace plánu revize přínosů

V rámci této aktivity projektový vedoucí aktualizuje dokument plán revize přínosů o dosažené částečné přínosy (bylo-li dosaženo některých z plánovaných cílů/indikátorů).

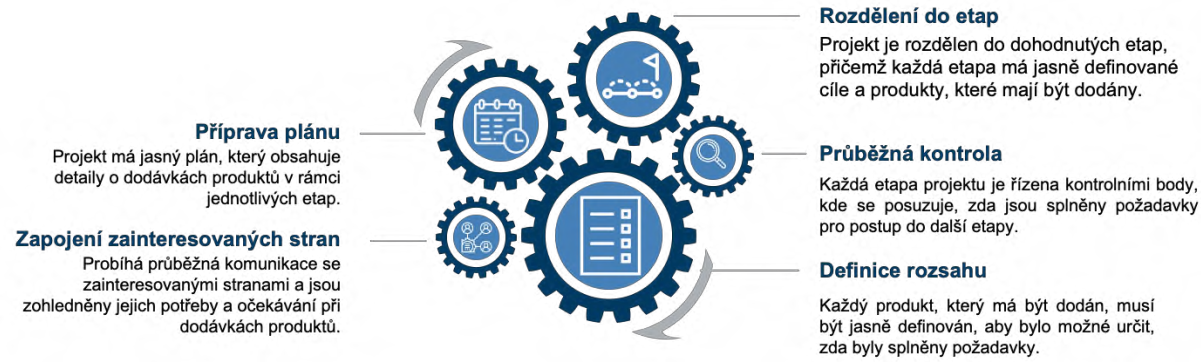
2.4.5 Řízení dodání produktu

Jedná se v projektové hierarchii o **nejnižší proces řízení.** Slouží k oddělení práce projektového manažera od práce odborné. **Zahrnuje tvorbu/výrobu a schválení jednotlivých produktů/výstupů.**

Projektový manažer je odpovědný za schválení/přidělení úkolu, přijetí dokončené práce a za provedení záznamů o otevřených bodech nebo rizicích předložených Týmovým manažerem/členem týmu (v rámci procesu kontroly etapy).

Týmový manažer/člen týmu je odpovědný za provedení úkolu (dohlíží, zda je práce provedena po odborné stránce). O realizaci průběžně informuje projektového manažera v rámci kontrolingových schůzek.

Aby bylo řízení dodání produktu úspěšné je nutné držet se pěti základních parametrů:



Po dokončení řízení dodání produktu je zahájena aktivita schválení a předání produktů / výstupů uživateli / uživatelům.

V rámci této aktivity probíhá **schválení a předávání produktů uživatelům**. Na základě výsledků testování a kontroly kvality je sepsán **akceptační protokol** (viz kapitola Akceptační řízení). Akceptační protokol je podepsán klíčovým uživatelem, sponzorem projektu a hlavním dodavatelem (zástupce dodavatele). Projektový manažer zaznamená výsledky do registru kvality a podepsané akceptační protokoly uloží na úložiště.

Zdrojové kódy jsou ukládány do úložiště kódu MZ využívající nástroje Microsoft DevOps Server. Dodavatel na základě odsouhlasení instalace (report provedených testů ve vývojovém prostředí dodavatele) do prostředí MZ (produkční i neprodukční) je povinen provést uložení a předání zdrojového kódu instalované verze aplikace. Zdrojový kód musí být předán v kompletní buildovatelné podobě (včetně projektu, nebo nastavení vývojového prostředí) a to jak pro neprodukční, tak i pro produkční prostředí. Verze pro produkční i neprodukční prostředí jsou tvořeny jedním zdrojovým kódem, liší se pouze v konfiguracích (parametrech buildu) pro produkční a neprodukční prostředí.

Součástí nové verze vždy musí být popis změn, resp. úprav verze, tzv. Release notes a dále musí být dodána instalační příručka (případně ostatní povinná dokumentace).

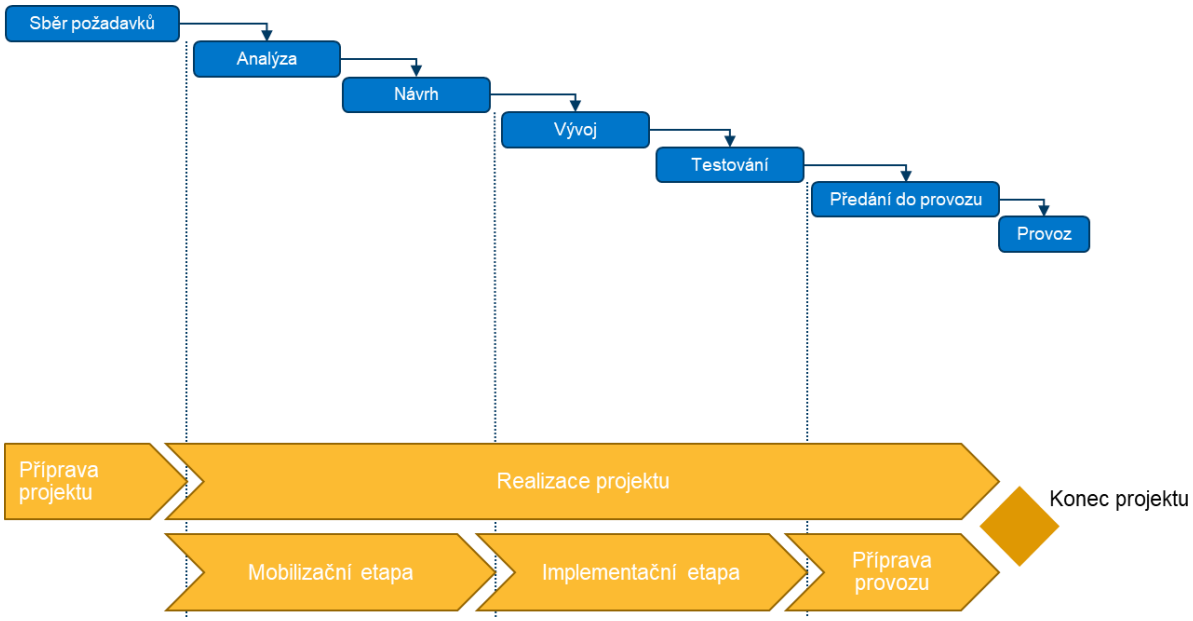
2.4.5.1 Návaznost procesů vývoje SW na projektové řízení

Metodika projektového řízení MZČR včetně PRINCE2, ze které vychází, jsou schopné pokrýt široké spektrum realizovaných (nejen) IT projektů.

Pro účely této metodiky vycházíme z **tzv. vodopádového (waterfall) životního cyklu vývoje software**. Jedná se o lineární a sekvenční přístup kdy je každý krok závislý na výstupu předchozího kroku. Způsob, jakým se tyto projekty rozvíjejí, má lineární průběh.

Celkově je předpokládáno, že projekty budou řízeny dle metodiky Prince2, ale zároveň má dodavatel volnost v začlenění agilních principů jako jsou například Sprinty, Stand-up, ...

Vodopádový životní cyklu je znázorněný na následujícím obrázku:



Projekty založené na vodopádovém modelu jsou dobře definované, předvídatelné a mají specifickou dokumentaci. Užití tohoto přístupu je výhodné zejména v případech kdy:

- **jsou definované požadavky;**
- **je stanovena pevná časová osa;**
- **jsou dané a srozumitelné technologie a**
- **pravděpodobně nebudou vyžadovány výrazné změny v průběhu projektu.**

2.4.5.1.1 Mobilizační etapa – Realizační projekt

Z pohledu řízení projektu vstupujeme do **realizační části projektu** s popisem aplikace, tj. definovanými požadavky (funkčními i nefunkčními), kvalitativními požadavky a způsoby jejich ověření, a to ve formě Karty projektu a Popisu produktu.

V rámci první realizační etapy označované jako Mobilizační etapa je vpracován tzv. **Prováděcí projekt zahrnující fázi Analýzy (Detailní analýzy) a Návrhu systému.**

V průběhu analytické fáze jsou funkční požadavky na aplikaci **analyzovány, ověřovány a formálně zpracovány do podoby Funkční specifikace** (definice use case – případů užití). Funkční specifikace je formální dokument používaný k podrobnému popisu zamýšlených schopností produktu, vzhledu a

interakcí s uživateli pro vývojáře softwaru (v případě, že se jedná o rozšíření stávající aplikace, je také analyzován současný stav).

S ohledem na skutečnost, že funkční specifikace detailně popisuje chování aplikace, je obvyklé, že po dokončení funkční specifikace vznikne i **dokument popisující způsob jejího ověření v podobě Testovacích scénářů.**

V průběhu fáze návrhu (designu) vzniká dokument **technická specifikace, aby popsal technický návrh aplikace** – její technickou architekturu (použití schválených arch. paternů, provozní platforma atp.), služeb, integrací na okolní systémy, definicí datového rozhraní, datových modelů a dalších technických detailů.

Realizační projekt dále musí obsahovat **popis technologického a organizačního zajištění provozu** (viz. etapa Předání do produkčního provozu).

V neposlední řadě je nezbytné zajistit odpovídající **bezpečnost aplikace** (součást analýzy i návrhu) a to včetně zpracování systémové a bezpečnostní politiky.

Samostatnou kapitolu pak tvoří sada povinné dokumentace (požadavek ze strany objednatele), které bude součástí dodávky (Uživatelská příručka, admin. příručka atp.)

Prováděcí projekt také definuje **požadavky na součinnost ze strany objednatele**, tak aby bylo možné efektivně řídit zdroje na straně objednatele.

Na základě schváleného prováděcího projektu je pak možné aktualizovat Projektový plán a následně zahájit Implementaci systému.

2.4.5.1.2 Implementační etapa

V průběhu projektové Implementační fáze **probíhá vlastní vývoj aplikace** (kódování / implementace), která je standardně řízenou projektovou etapou – přidělování balíků práce, úkolování, kontrola plnění atp. Realizace je na straně dodavatele a obvykle v jeho vývojovém prostředí. **Průběh této etapy je možné monitorovat na základě tzv. unit testů, tj. testů na úrovni aplikačních modulů, tak jak jsou postupně zadávány k realizaci.**

Po dokončení fáze vývoje aplikace nastává **fáze testování,** tj. ověření, zda byly naplněny veškeré funkční i nefunkční požadavky na aplikace, tj. zda byla naplněna kvalita dodávky (aplikace).

Pro ověření funkčních požadavků jsou z analytické fáze připraveny testovací scénáře detailně popisující očekávané chování aplikace. Pro testování nefunkčních požadavků jsou připraveny specifické testovací postupy a nástroje připravené již ve fázi návrhu, nebo v rámci definování testovací strategie. Jedná se například o výkonové testy, kapacitní testy, testy na odolnost proti výpadky aplikace, resp. ztráty dat, nebo penetrační (bezpečnostní testy).

Vlastní vyhodnocení testů (kvality aplikace) je posuzována s ohledem na celkovou funkčnost aplikace. Výsledky testů, resp. chyby aplikace jsou kategorizovány, např. kategorie A – kritický dopad, systém je zcela nefunkční, kategorie B – závažný dopad, hlavní části systému jsou funkční, nebo funkční

s omezením, kategorie C – ostatní. Pro vyhodnocení – akceptaci aplikace pak slouží počty možných chyb aplikace dané kategorie – např. 0 chyb kategorie A, 5 chyb kategorie B a 20 chyb kategorie C, které jsou definované již v rámci kvalitativních parametrů a v rámci smlouvy s dodavatelem.

Pro způsob a postup testování není možné navrhnout jednotný postup, který vždy závisí na konkrétních požadavcích charakteru vlastní aplikace. Jako příklad je možné uvést následující postup:

a) **Aplikace je připravena k testování –** dodavatel hlásí připravenost k instalaci aplikace do testovacího prostředí objednatele a předkládá kompletní protokol o provedených unit a funkčních testech ve vývojovém prostředí (bez integračních vazeb) pro ověření připravenosti. Současně předkládá instalační postup a zdrojové kódy k uložení do DevOps prostředí objednatele.
b) Specialisté dodavatele provedou instalaci aplikace dle předaného instalačního postupu **a ověří základní funkčnost aplikace** (obvykle hlavní proces, tzv. smoke testy). Instalace je provedena do testovacího prostředí objednatele, a to včetně integračních vazeb (datové zdroje). Je vypracován instalační protokol (instalaci může provést i dodavatel). Takto připravený systém je předán testovacímu týmu – Test manažerovy.
c) **Testovací tým provádí funkční testy** (systémové a integrační) podle připravených detailních testovacích scénářů. V případě odlišného chování aplikace je tato skutečnost zaznamenána jako chyba včetně návrhu její kategorie z pohledu testera. Dále jsou doplněny nezbytné informace potřebné k analýze chyby. Zaznamenaná chyba je předána testovacímu manažerovy, který ji předá na dodavatele k dalšímu zpracování. Dodavatel si k reportované chybě může vyžádat doplňující informace, případně může chybu odmítnout jako neodůvodněnou. Dodavatel má obvykle definován čas na analýzu chyby a na její odstranění, a to v závislosti na její kategorii.
d) V případě, že kvalita aplikace neodpovídá stanoveným kritériím dodavatel připravuje novou verzi aplikace s opravenými chybami (viz. termíny dle kritičnosti chyby).
e) Dodavatel hlásí připravenost k opakovanému testování aplikace, zejména pak jako kontrola opravy chybových stavů. Deklaruje opravu identifikovaných chybových stavů a předkládá novu verzi aplikace – zdrojový kód a instalační příručku.
f) Následují opakující se kroky b), c) d) a e) do doby naplnění kvalitativních kritérií, případně do rozhodnutí o Ukončení projektu.
g) Výše uvedené funkční testy jsou realizovány testovacím týmem, tj. speciality, kteří s aplikací nebudou cílově pracovat. Proto po dosažení akceptačních kritérií je naplánována série funkční testů, realizována koncovými uživateli (tzv. end user testy). Testování je v tomto případě realizováno již ne striktně podle připravených testovacích scénářů. Identifikace chybových stavů, jejich evidence, předání na dodavatele, vydání nové verze se opakuje, stejně jako v případě testovacího týmu.
h) Samostatnou kapitolou jsou pak testy nefunkčních vlastností aplikace (systému). I výsledky těchto testů se započítávají do celkového scóre kvality aplikace.

Jedná se např. o:

- Zátěžové testy – na aplikaci je generována zátěž a je průběžně sledována odezva aplikace, případně odezvy různých části aplikace.
- Kapacitní testy – zjišťuje se při jakém počtu uživatel / zátěže dojde ke zpomalení nebo kolapsu aplikace.
- HA/DR testy – testy ověřující chování aplikace k mezních stavech, jako je výpadek aplikačního node, realizovatelnost překlopení do záložního datového centra atp.
- Bezpečnosti (penetrační) testy – testy aplikace z pohledu její odolnosti proti kybernetickým hrozbám a zranitelnostem (obvykle provádí nezávislá odborná společnost).

Problematika testování je podrobněji popsaná v příloze

2.4.5.1.3 Předání do produkce

Fáze předání aplikace do produkce je nedílnou a nesmírně důležitou součástí projektu. V rámci projektové metodiky je předání do produkce nastaveno jako poslední projektová etapa, před uzavřením projektu.

2.5 Příprava produktivního provozu

Cílem tohoto procesu je:

- **Předání provozní dokumentace.**
- **Nastavení produkčních konfigurací.**
- **Nasazení systému do produktivního prostředí.**
- **Potvrzení připravenosti aplikace pro spuštění produktivního provozu (Provozně technické kontrolní seznamy (checklisty), kontrolní seznamy (checklisty) shody se systémem řízení kvality).**

Hlavním procesem přípravy produktivního provozu je příprava nasazení systému do produktivního prostředí.

Integrační tým provede posouzení shody dodaného díla/aplikace s provozně-technickými požadavky a požadavky systému řízení kvality.

Nesoulady s požadavky jsou zaznamenávány do Registru otevřených bodů. Následně je výsledek předán výkonnému výboru k rozhodnutí o dalším postupu (spuštění produktivního provozu, opravy/zajištění souladu).

Příprava produktivního provozu se řídí plánem etapy. V této etapě jsou využívány níže uvedené šablony:

2.6 Ukončení projektu

Cílem této fáze je:

- Formální převzetí do provozu (uživateli) a spuštění produktivního provozu
- Formální ukončení projektu

Ukončení projektu zahrnuje:

- Posouzení, zda všechny cíle popsané v kartě projektu byly naplněny
- Posouzení, zda všechny **výstupy byly dodány a akceptovány** uživatelem nebo provozem
- Popis, **co by mělo být zajištěno provozem** a jeho podporou po ukončení projektu (vč. monitoringu ukazatelů, udržitelnosti, provozní dokumentace)
- **Předání dokumentace pro provoz**
- **Aktualizace Enterprise architektury**
- Ověření, že **Plán revize přínosů[2] zohledňuje požadované testování přínosů** po ukončení projektu a jsou přiřazeny odpovědné osoby za provedení měření
- **Osoby odpovědné** za měření přínosů po skončení projektu (provoz) jsou v rámci ukončení projektu oficiálně pověřeny tímto měřením.
- Stanovení následných akcí
- Zpracování **závěrečné zprávy** projektu a závěrečná MZ a ŽoP
- **Sběr získaných poznatků** z projektu a zapracování do zprávy o získaných poznatcích
- Analýza rizik přetrvávajících po skončení projektu
- **Archivace** projektových dokumentů (dle skartačního řádu)

[2] Centralizovaná evidence monitorovaných ukazatelů udržovaná za všechny projekty

- Příprava oznámení o ukončení projektu pro výkonný výbor

2.7 Uvedení do provozu

Etapa uvedení do provozu je koncipována jako standardní projektová etapa, ale je uvažována jako povinná, **před ukončení projektu. Důvodem zavedení této povinné etapy je zajištění dlouhodobé udržitelnosti produktů projektu (např. informačního systému), které je obvykle vyžadované na základě dotačního titulu.**

Již od počátku plánování projektu, v případě implementace informačního systému je potřeba neopomenout, že kromě koncových uživatelů systému (tj. skupiny lidí, kteří se systémem ve výsledku pracují) je zde další skupina lidí, kteří systém provozují a podporují, případně dále rozvíjejí. To je důvodem proč i oddělení provozu/provozní obsluha systému náleží do projektové role uživatel a stejně jako koncový uživatel systému stejně tak musí mít možnost si definovat funkční i nefunkční požadavky na systém/produkt ze svého pohledu.

Ne všechny projekty dodávají informační systém, tj. programový kód „běžící“ někde v datacentru. Stejně tak je důležité **uvažovat i o uvedení do provozu u výstupů typu dokument např. popisující fungování nových procesů, směrnic apod. a správně plánovat funkční i nefunkční požadavky na produkt projektu směřující k jeho plánovanému užití a následné možnosti měření jeho přínosu.**

Přestože je etapa Uvedení do provozu poslední v pořadí projektových etap (před Ukončením projektu) její vstupy musí být definovány již jako součástí etapy zahájení a také nastavení produktu (někdy i předprojektové etapy – projektový záměr), kde vznikají Projektový plán i Popisy produktů apod.

Vzhledem ke skutečnosti, že žádný informační systém není stejný, tj. není možné vzorově definovat provozní požadavky je níže uváděn seznam vybraných příkladů, které je vždy nezbytné přizpůsobit konkrétní situaci (stejné platí i pro produkty typu dokument).

Pro nový informační systém zajistit/ověřit že:

- **existují dostatečné výpočetní zdroje** – z pohledu výkonnosti, objemu zpracovávaných dat, dostupnosti, kybernetické bezpečnosti.
- je k dispozici **dostatek lidských zdrojů** s odpovídající kvalifikací.
- bude dodána **instalační dokumentace, případně migrační strategie a dokumentace včetně instalačního protokolu.**
- bude dodána **dokumentace s detailními požadavky konfigurace na provozní infrastrukturu.**
- bude dodána **provozní a admin dokumentace.**
- bude dodána **dokumentace pro provozní troubleshooting.**
- **zaškolení** provozního personálu včetně relevantních úrovní Helpdesku/ServiceDesku.

- bude **zajištěna smlouva o podpoře a údržbě (SLA)** včetně dostupnosti dodavatelského Helpdesku, ověřit služby podpory a údržby dle standardu.

Jak bylo uvedeno v úvodu, jedná se o standardní projektovou etapu, tedy jsou vyžívány standardní projektové postupy – řízení dodávky pomocí Balíků práce (řízení kvality, rizik atp.), reportování o ukončení etapy / Zpráva o ukončení etapy, Schválení ukončení projektu.

Proces obsahuje tři základní procesy, které je nutné dodržet:

2.7.1 Předání aplikace a příprava spuštění produktivního provozu

Výstupem tohoto procesu je produktivně provozovaná aplikace.

2.7.2 Akceptace díla a zahájení produktivního provozu

Formální akceptace aplikace (viz kapitola akceptační řízení). A formální schválení zahájení produktivního provozu.

Schválení spuštění produktivního provozu na základě Provozně technického checklistu a checklistu shody se systémem řízení kvality.

2.8 Ukončení projektu

Jedná se o **oficiální uzavření a dokončení všech činností a fází, které byly plánovány a prováděny v rámci projektu.** Tato fáze zahrnuje formální ukončení všech projektových činností, hodnocení dosažených výsledků, zpracování závěrečných dokumentů a informování stakeholderů o dokončení projektu. Ukončení projektu je důležitým krokem, který umožňuje zajištění, že projekt byl úspěšně dokončen a dosáhl svých cílů.

Proces obsahuje šest základních procesů, které je nutné dodržet:

2.8.1 Aktualizace přehledu získaných poznatků

Finální aktualizace a předání registru získaných zkušeností na projektovou kancelář Programu EZ.

2.8.2 (Zpracování závěrečné MZ a ŽoP)

V rámci této aktivity je zpracována **závěrečná Monitorovací zpráva a Žádost o platbu** (Je-li projekt financován finančním mechanismem vyžadujícím zpracování těchto dokumentů. Formát dokumentů je definován poskytovatelem dotace). Obecně se jedná o závěrečnou monitorovací zprávu a o závěrečnou žádost o platbu.

Je nutné zkontrolovat podmínky poskytovatele dotace, a dle toho upravit připravované podklady.

2.8.3 Aktualizace plánu revize přínosů

Finální aktualizace plánu revize přínosů pro následné monitorování přínosů a monitorovacích indikátorů v průběhu provozu aplikace v rámci procesu Monitoring/měření přínosů zajišťovaného na úrovni portfolia projektů a aplikací (viz kapitola plán revize přínosů).

2.8.4 Archivace dokumentace

V rámci této aktivity probíhá **archivace dokumentace**. Na základě skartačního řádu bude provedena archivace odpovědnými osobami.

Elektronická dokumentace MS Sharepoint slouží dále jako zdroj informací po skončení realizace projektu (např. pro další projekty, změny v rámci provozu apod.)

2.8.5 Předání dokumentace k řízení projektu

Projektový vedoucí formálně předá dokumentaci dokončeného projektu na úroveň Programu EZ.

2.8.6 Vyhodnocení projektu

Projektový vedoucí v rámci této aktivity provádí **vyhodnocení projektu.** V rámci Zprávy o ukončení projektu informuje, zda cíle definované v projektové dokumentaci byly dosaženy.

Pro přípravu zprávy je využívána šablona „Zpráva o ukončení projektu“.

3 POVINNÁ DOKUMENTACE

V průběhu projektů budou projektové týmy vypracovávat dokumentaci, která bude sloužit k řádnému dokumentování projektových aktivit, popisu výstupů a po projektových procesů. Níže je definovaná dokumentace, která bude povinnou součástí všech projektů, které budou navrhovat a vyvíjet technická řešení. Každý projekt může nad tuto povinnou sadu dokumentů připravit i dodatečné dokumenty podle svého uvážení.

3.1 Analytická dokumentace

Analýza požadavků na nový/upravený produkt. Analýza zahrnuje jak funkční, tak nefunkční požadavky. Funkční požadavky popisují požadované funkce a chování systému, včetně definice nutných aktivit a akcí, které musí být vykonány. Nefunkční požadavky definují ostatní vlastnosti produktů jako jsou výkonové požadavky, požadavky na dostupnost a odolnost systému, požadavky na design, technologické požadavky atp.

3.2 Návrhová dokumentace (Design)

Detailní funkční specifikace – dokument definuje, co přesně systém dělá a shrnuje artefakty. Definuje funkční pravidla, případy užití (use-cases), uživatelské příběhy (user stories) nebo modely/prototypy uživatelského rozhraní.

Detailní technické specifikace – definují detailní technickou architekturu (s využitím schválených architektonických vzorů), návrh integrací a integračních vazeb poskytovaných, nebo využívaných dotčenými systémy, design databázových modelů, katalog poskytovaných služeb, atp.

Testovací scénáře – v návaznosti na detailní funkční specifikaci jsou vytvořeny podrobné testovací scénáře ve vazbě na jednotlivé případy užití (use-case) obsahující zejména vstupní data do testovacího scénáře a očekávané výsledky/chování aplikace.

3.3 Uživatelská dokumentace

Je určena pro samotné uživatele vytvořeného systému. Uživatelská dokumentace může být realizována v různých formách např.:

- referenční příručka,
- průvodce aplikací/systémem (podle případu užití),
- podpora uživatele – časté dotazy
- **výukový a školící materiál** (pomocí něhož mohou uživatelé získat potřebné znalosti)

Rozsah uživatelské dokumentace závisí na charakteru dodávaného řešení/aplikace a bude upřesněn již ve fázi zadání.

3.4 Provozní/Servisní dokumentace

Je určena především provoznímu/servisnímu personálu. Obsahuje popis pravidelných provozních činností k zajištění spolehlivého a bezproblémového provozu (pravidelné provozní aktivity, kontrola aplikačních a systémových logů, provozní a bezpečnostní záplatování, zálohování, atd). Provozní dokumentace dále musí obsahovat popis, nebo lépe průvodce při odstraňování drobných nestandardních provozních stavů (čištění front po restartu atp.), problémů a dalších výjimečných situací.

3.5 Systémová dokumentace

Cílem této dokumentace je poskytnout vývojářům, resp. servisním vývojářům ucelený přehled o celém systému. Hlavními částmi dokumentu je zejména aplikační architektura s detailním popisem jednotlivých aplikačních modulů a jejich parametrů. V kombinaci s dokumentovaným zdrojovým kódem umožní pochopit účel modulu/metody/třídy, tak aby bylo možné provést jeho nezávislou úpravu.

Pro případ potřeby pro pochopení je možné využít i návrhovou část dokumentace.

3.6 Administrátorská dokumentace

Dokumentace popisující veškeré administrátorské činnosti pro vytvořený systém včetně stanovení četnosti a způsobu provádění nezbytných administrátorských činností. Nedílnou součástí provozní dokumentace je popis konfigurace jak SW, tak HW částí řešení.

3.7 Bezpečnostní dokumentace

Analýza rizik, případně Model hrozeb (Threat Model) zpracovaný pro vytvářený systém, tak aby byly efektivně navrženy relevantní bezpečnostní opatření (bezpečnostní architektura – aplikační, nastavení infrastruktury, organizační opatření atp.).

Bezpečnostní architektura – popis způsobu implementace jednotlivých bezpečnostních opatření s cílem efektivně eliminovat identifikované bezpečnostní hrozby.

Plán obnovy (IT Disaster Recovery Plan) – IT plán obnovy systému po havárii v rámci zachování kontinuity obchodní činnosti.

3.8 Ostatní dokumentace

Report z penetračního testování – výsledky testování, jako součást akceptačního řízení. Penetrační/bezpečnostní testování dle metodiky OWASP (ideálně nezávislou stranou).

Výsledky z výkonových / kapacitních testů – součást akceptačního řízení

Výsledky z funkčních testů – výsledky ze všech úrovní testů (unit, systémové, integrační, UAT, …).

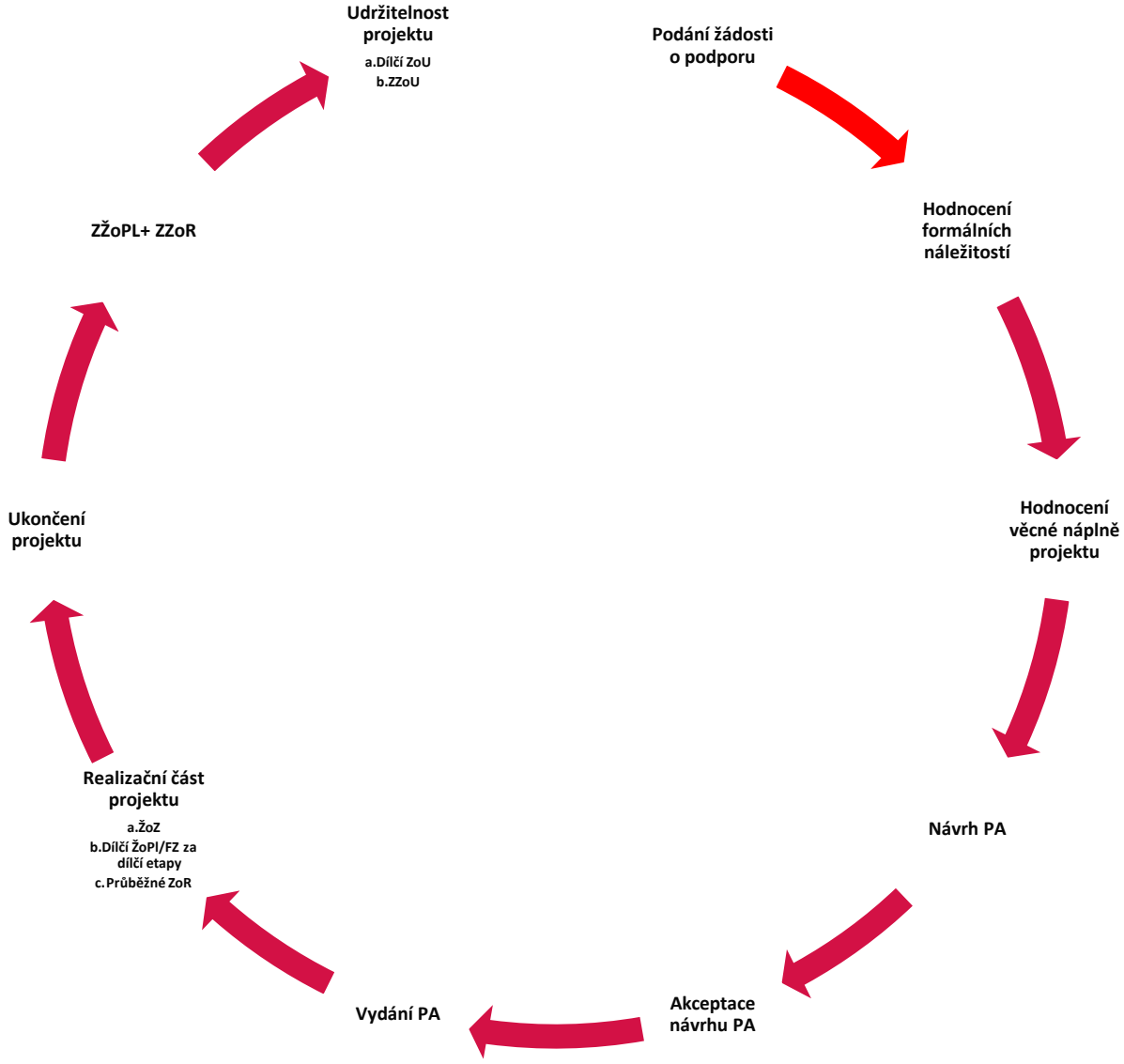
4 FINANCOVÁNÍ A VÝKAZNICTVÍ EU/NPO

4.1 Financování dotačního projektu

Tato kapitola je rozdělena na několik základních oblastí, které jsou stěžejní ve fázi realizace dotačních projektů. Realizace projektu po schválení Žádosti o podporu v sobě zahrnuje mnoho úkonů a kroků, které jsou úzce spjaty s mnoha dalšími povinnostmi a pravidly napříč celým projektem. Předložení podkladů k Žádosti o platbu je až jedním z posledních kroků. Každý projekt je jedinečný a je třeba dbát na jeho individuální vývoj a specifické nároky. V průběhu realizace projektu se objevují doplňující požadavky a nové informace vztahující se k novým pravidlům či konkrétním projektům, na které je třeba ve stanoveném času reagovat a implementovat do svých interních procesů. Je třeba mít povědomí o provázanosti s výběrovým řízením. Je třeba rozumět pravidlům a řešit provázanosti s realizační částí.

4.2 Národní plán obnovy

Národní plán obnovy, zkráceně NPO, vznikl v reakci na krizi způsobenou pandemií COVID-19, jehož cílem je pomocí investic a reformních opatření zajistit mj. zvýšení digitalizace České republiky. Aktuálně je NPO rozšířen o reformní prvky reagující na energetickou krizi.


Udržitelnost projektu
a.Dílčí ZoU
b.ZZoU
Podání žádosti o podporu
Hodnocení formálních náležitostí
Hodnocení věcné náplně projektu
Návrh PA
Akceptace návrhu PA
Vydání PA
Realizační část projektu
a.ŽoZ
b.Dílčí ŽoPl/FZ za dílčí etapy
c. Průběžné ZoR
Ukončení projektu
ZŽoPL+ ZZoR

4.2.1 Podání žádosti o podporu

Na základě požadavků řídícího orgánu (dále ŘO) je sepsán Podnikatelský záměr či Studie proveditelnosti, kde je velmi podrobně popsán cíl a řešení plánovaného projektu. Žádost o podporu je obvykle podávána prostřednictvím informačního systému (nejčastěji ISKP14+, ISKP21+, AIS SFŽP ČR) a obsahuje formální přílohy. Veškeré náležitosti a přílohy jsou definovány konkrétní Výzvou k podání žádosti o podporu, případně Pravidly pro žadatele a příjemce.

Podání žádosti o podporu zajišťuje Dotační specialista ve spolupráci s Hlavním vedoucím projektu.

Termín podání je stanoven konkrétní Výzvou.

4.2.2 Hodnocení formálních náležitostí

Řídící orgán nebo jeho zastupující subjekt provedou tzn. hodnocení formálních náležitostí projektu. Tento krok probíhá bez účasti žadatele, přičemž ale může být ŘO vyzván k doplnění formálních náležitostí. Za doplnění žádosti o podporu je odpovědný dotační specialista a Hlavní vedoucí projektu.

4.2.3 Hodnocení věcné náplně projektu

Řídící orgán nebo jeho zastupující subjekt provedou tzn. hodnocení věcných náležitostí projektu. Tento krok probíhá bez účasti žadatele, přičemž ale může být ŘO vyzván k doplnění formálních náležitostí. Za doplnění žádosti o podporu je odpovědný dotační specialista a Hlavní vedoucí projektu.

4.2.4 Návrh Právního aktu

Po schválení projektu, tj. splnění formálních i věcných náležitostí a po kladném hodnocení Výběrové komise, je vydán návrh Právního aktu (dále PA). O vydání návrhu je žadatel zpravidla informován v informačním systému.

4.2.5 Akceptace návrhu Právního aktu

Návrh PA je zaslán žadateli, který zkontroluje veškeré údaje a v případě, že s uvedenými podmínkami souhlasí a uvedené údaje jsou správné, zašle řídícímu orgánu „akceptaci“ PA. Ta je zasílána obvykle formou depeše v informačním systému.

Termín pro zaslání akceptační depeše stanovuje vždy konkrétní projektový manažer ŘO.

4.2.6 Vydání Právního aktu

Pokud je návrh PA žadatelem akceptován, je Řídícím orgánem vydán platný Právní akt. O vydání je žadatel informován prostřednictvím informačního systému. V tento okamžik se z žadatele o dotaci stává příjemce dotační podpory.

4.2.7 Realizační část projektu

Realizační fáze projektu je z celého jeho životního cyklu nejdelší, obvykle trvá dva až tři roky dle jeho zaměření a maximální lhůty, kterou Výzva stanovuje. Je třeba postupovat v souladu s projektovou žádostí a dle stanoveného harmonogramu. Za realizační část projektu zodpovídá Projektový vedoucí.

4.2.8 Žádosti o změnu

S ohledem na dlouhé schvalovací lhůty a dlouhou realizační dobu projektu není neobvyklé, že dochází k částečným změnám projektu, a to jak z pohledu rozpočtu, harmonogramu i věcné náplně. Všechny tyto změny je třeba konzultovat buď s dotačním specialistou nebo přímo s ŘO. Žádost o změnu je vždy nezbytné podat v informačním systému a ŘO ji musí schválit. Většina změn by měla být schválena před jejich realizací – v případě, že budou vynaloženy výdaje na neschválenou změnu, tyto výdaje se automaticky stávají nezpůsobilými. Za řádné podání Žádosti o změnu zodpovídá Dotační specialista ve spolupráci s Projektovým vedoucím.

Termín pro podání Žádosti o změnu je vždy nejpozději v den, kdy má být daná povinnost splněna.

4.2.9 Dílčí žádosti o platbu/finanční zprávy za dílčí etapy

V závislosti na způsobu financování projektu (ex-ante/předem versus ex-post/zpětně) se podávají žádosti o platbu/finanční zprávy, obvykle jedna etapa rovná se jedna žádost o platbu/finanční zpráva. Za podání Žádosti o platbu/finanční zprávy zodpovídá Dotační specialista, který obdrží potřebné podklady od ostatních útvarů dle charakteru požadované dokumentace.

Termín pro podání Žádosti o platbu/finanční zprávy je stanoven ve finančním plánu, obvykle však činí 2 měsíce od konce příslušné etapy. Zároveň Pokyn Vlastníka komponenty stanovuje, že se ŽoPl/FZ podává 2x ročně, a to za I. a II. pololetí.

4.2.10 Průběžné monitorovací zprávy o realizaci

Zprávy o realizaci jsou přímo navázány na termíny pro podání žádostí o platbu/finanční zprávy, jedno bez druhého tedy podat nelze. Ve Zprávě o realizaci se obvykle dokládá dodržení pravidel pro publicitu, doplňuje se popis průběhu dané etapy a dokládá se průběžné plnění závazných indikátorů, případně další informace, které stanovuje Výzva. Za podání Zprávy o realizaci zodpovídá Dotační specialista, který obdrží potřebné podklady od ostatních útvarů dle charakteru požadované dokumentace.

Termín pro podání Zprávy o realizaci je stanoven ve finančním plánu, obvykle však činí 2 měsíce od konce příslušné etapy.

4.2.11 Ukončení projektu

Plánované datum ukončení projektu je pevně dané a váže se k němu několik povinností – viz níže. Toto datum je možné posunout jen výjimečně na základě odůvodněných okolností a obvykle pouze do maxima stanoveného Výzvou. V ojedinělých případech může poskytovatel dotace projekt prodloužit i za toto maximum. Naopak příjemce může projekt ukončit kdykoli před plánovaným koncem projektu, nicméně musí splnit všechny povinnosti, ke kterým se zavázal.

Za splnění všech povinností stanovených PA zodpovídá Projektový vedoucí.

4.2.12 Závěrečná žádost o platbu/Závěrečná finanční zpráva + Závěrečná monitorovací zpráva o realizaci

Závěrečná žádost o platbu (dále ZŽoP)/Závěrečná finanční zpráva (dále ZFZ) a Závěrečná zpráva o realizaci (dále ZZoR) jsou svým rozsahem a obsahem obdobné jako Žádosti a Zprávy průběžné. Navíc je v tomto případě třeba doložit splnění všech závazných indikátorů a dalších povinností vyplývajících z PA. Za podání Závěrečné žádosti o platbu/Závěrečné finanční zprávy a Zprávy o realizaci zodpovídá Dotační specialista, který obdrží potřebné podklady od ostatních útvarů dle charakteru požadované dokumentace.

Dle pravidel NPO je příjemce povinen podat ZŽoP/ZFZ a ZZoR do dvou měsíců od plánovaného konce projektu, pokud bude projekt ukončen dříve, lze i ZŽoP/ZFZ a ZZoR podat dříve.

4.2.13 Udržitelnost projektu

Obvykle v závislosti na velikosti příjemce je stanovena délka doby udržitelnosti, přičemž nejčastěji je to pro malý a střední podnik 3 roky a pro velké podniky 5 let. Po celou tuto dobu se nezbytné nadále plnit veškeré povinnosti stanovené PA, případně další metodikou. Za řádné plnění doby udržitelnosti zodpovídá Projektový vedoucí.

4.2.14 Dílčí Zprávy o udržitelnosti

Jednou za rok dle harmonogramu stanoveného ŘO je příjemce povinen předkládat v informačním systému Zprávy o realizaci. V této Zprávě příjemce popíše průběh projektu v daném monitorovacím období, doloží plnění publicity a případnou změnu v hodnotě závazného indikátoru. Za podání Zprávy o udržitelnosti zodpovídá Dotační specialista, který obdrží potřebné podklady od ostatních útvarů dle charakteru požadované dokumentace.

Termín pro podání Zprávy o udržitelnosti je zpravidla deset kalendářních dnů po konci monitorovacího období dle harmonogramu stanoveného ŘO.

4.2.15 Závěrečná Zpráva o udržitelnosti

Po skončení doby udržitelnosti, dle typu příjemce tedy po dalších třech až pěti letech, se podává poslední Závěrečná Zprávy o udržitelnosti. Svým rozsahem a obsahem je obdobná, jako Zprávy předchozí. Za podání Zprávy o udržitelnosti zodpovídá Dotační specialista, který obdrží potřebné podklady od ostatních útvarů dle charakteru požadované dokumentace.

Termín pro podání Zprávy o udržitelnosti je zpravidla deset kalendářních dnů po konci monitorovacího období dle harmonogramu stanoveného ŘO.

4.3 Seznam osob/orgánů ke spolupráci na zajištění realizace dotačního projektu

- Hlavní vedoucí projektu – vede a koordinuje všechny Manažery skupiny projektů

- Manažer skupiny projektů – osoba mající přehled o předem stanovené skupině projektů, dohlíží na klíčové milníky projektů, vede a koordinuje Projektové vedoucí, reportuje Hlavnímu vedoucímu projektu
- Projektový vedoucí – osoba, která má o projektu kompletní přehled a koordinuje další osoby a orgány, zodpovídá se Manažerovi skupiny projektů
- Realizační tým projektu – osoby a pozice zapojené do projektu dle projektové žádosti, zodpovídají se Projektovému vedoucímu
- Účetní oddělení – zajišťuje oddělené účetnictví, sestavy, zodpovídá se Projektovému vedoucímu
- Finanční oddělení – proplácí faktury, mzdové výdaje, zodpovídá se Projektovému vedoucímu
- Mzdové oddělení – zajišťuje mzdové podklady – PS, DPP, Čestná prohlášení zaměstnanců, zaměstnavatele, výkazy práce, mzdové listy apod., zodpovídá se Projektovému vedoucímu
- IT oddělení – odpovídá za technické zajištění projektu, zodpovídá se Projektovému vedoucímu
- Právní oddělení – zajišťuje veřejné zakázky, kontrolu uzavřených smluv, zodpovídá se Projektovému vedoucímu
- Marketingové oddělení – zajišťuje publicitu, zodpovídá se Projektovému vedoucímu
- Interní dotační specialista – zpracovává podklady od ostatních oddělení do požadované podoby ŘO (tato pozice může být buď skutečně interní nebo zajištěna prostřednictvím poradenské agentury/externistou, v tom případě bude pak mimo interní organizační strukturu)

4.4 Seznam obecných podkladů k žádostem o platbu

- Pracovní smlouvy, Dohody o práci mimo hlavní pracovní poměr
- Výkazy práce
- Mzdové listy
- Čestná prohlášení každého zaměstnance o souhlasu s kofinancováním mzdy ze zdrojů EU
- Čestné prohlášení zaměstnavatele, že úvazky osob zapojených do projektu nepřesahují úvazek 1,0 u zaměstnavatele za všechny vykonávané činnosti
- Dokumentace k veřejným zakázkám

- Smlouvy s dodavateli
- Objednávky
- Nabídky
- Dodací listy, předávací protokoly
- Protokoly o zaškolení
- Faktury s číslem projektu
- Sestavy z odděleného účetnictví – např. účetní deník
- Inventární karty
- Čestné prohlášení o neuplatňování nároku na odpočet DPH/Čestné prohlášení o výši koeficientu pro odpočet DPH – pouze v případě, kdy je DPH způsobilým výdajem
- Daňová přiznání, kontrolní hlášení, výpisy z účtu o úhradě DPH – pouze pokud je DPH způsobilým výdajem
- Doklady o úhradě nárokovaných faktur
- Fotodokumentace pořízeného majetku vč. SW
- Fotodokumentace publicity na webu příjemce a partnerů, fotografie publicity v místě realizace projektu
- Popis průběhu etapy/projektu
- Finanční výkazy za poslední uzavřený rok
- Dokumentace k indikátorům/výstupům projektu
- Ostatní dokumentace specifická pro danou výzvu

4.5 Výňatek z povinností konečného příjemce dle Právního aktu

- Termínem ukončení realizace projektu se rozumí dosažení účelu projektu, tj. poskytnutí všech služeb, dodávek a ostatních aktivit souvisejících s projektem, potvrzená v předávacím protokolu nebo datum úhrady poslední dlužné částky dodavatelům (rozhodné je datum, které nastane později), a to nejpozději do data uvedeného v Dopisu o schválení finanční podpory.
- KP je povinen při realizaci projektu uskutečňovat zadávání veřejných zakázek v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, vlastním interním aktem, vydaným k zadávání veřejných zakázek, případně Pokynem pro zadávání VZMR pro NPO (nemá-li KP vydán vlastní interní akt), vydaný vlastníkem komponenty. Postup předkládání zadávání veřejných zakázek ke kontrole vlastníkovi komponenty bude upraven platným Pokynem pro příjemce finanční podpory.
- KP je povinen pravidelně předkládat vlastníkovi komponenty pravdivé a úplné informace o průběhu realizace projektu.
- KP je povinen oznámit vlastníkovi komponenty všechny změny a skutečnosti, které mají vliv na plnění Dopisu o schválení finanční podpory a Podmínek nebo skutečnosti s tím související. Podstatné změny projektu vyžadují předchozí písemný souhlas vlastníka komponenty, KP je musí oznámit vlastníkovi komponenty před jejich realizací. Výjimku tvoří změny způsobené force majeure, které KP oznamuje neprodleně. KP nesmí provést změnu vydané Řídící dokumentace bez předchozího souhlasu vlastníka komponenty s podstatnou změnou projektu. Nepodstatné změny projektu nevyžadují předchozí písemný souhlas vlastníka komponenty. Oznamují se v rámci nejbližší monitorovací zprávy o projektu. Ustanovení týkající se změn platí i v době udržitelnosti, je-li stanovena.
- KP je povinen nejpozději při podání závěrečné zprávy prokázat naplnění účelu, na který mu byly peněžní prostředky poskytnuty, a splnění indikátorů uvedených v Dopise o schválení finanční podpory.
- KP je povinen zachovat výsledky realizace projektu po dobu 5 let od ukončení realizace projektu, a to minimálně do konce roku 2026, kdy končí implementace celého NPO. Povinnosti KP v době udržitelnosti budou upraveny Pokynem pro příjemce finanční podpory.
- KP je povinen v průběhu realizace a po dobu deseti let od ukončení realizace projektu, za účelem ověřování plnění povinností vyplývajících z Dopisu o schválení finanční podpory a těchto Podmínek, poskytovat požadované informace a dokumentaci zaměstnancům nebo zmocněncům pověřených orgánů (Ministerstvo vnitra, Ministerstva průmyslu a obchodu, Ministerstva financí, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy, Evropské komisi) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost. KP je též povinen zajistit, aby obdobné povinnosti ve vztahu k projektu plnili také dodavatelé a subdodavatelé podílející se na realizaci projektu.

- KP je povinen pečovat o pořízený majetek s péčí řádného hospodáře. Po dobu realizace a v době udržitelnosti KP není oprávněn majetek financovaný z prostředků na financování projektu prodat, pronajmout ani jinak zatížit ve prospěch třetí osoby bez souhlasu vlastníka komponenty.
- KP je povinen řádně uchovávat veškerou dokumentaci související s realizací projektu včetně účetních dokladů podle českých právních předpisů nejméně po dobu 10 let od schválení závěrečné zprávy o projektu. Každý originální účetní doklad musí obsahovat informaci, že se jedná o projekt financovaný z NPO a být označen specifickým identifikátorem. KP je povinen zajistit, aby obdobné povinnosti ve vztahu k projektu plnili také dodavatelé a subdodavatelé podílející se na realizaci projektu. Pokud není tato povinnost stanovena přímo v dodavatelské smlouvě, je KP povinen doložit, jakým jiným způsobem byli partneři a dodavatelé k této povinnosti zavázáni (např. formou vlastní dohody KP – dodavatel).
- KP se zavazuje, že na stejné způsobilé výdaje nebo jejich části nesmí čerpat jinou veřejnou podporu.
- KP je povinen vést oddělenou účetní evidenci o projektu v souladu se zákonem č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.
- KP je povinen provádět propagaci účasti prostředků NPO v souladu s Pokynem pro příjemce finanční podpory.
- KP je povinen zveřejnit účetní závěrku ve Sbírce listin Obchodního rejstříku (nebo obdobném registru) dle zákona č. 563/1991 Sb. o účetnictví, ve znění pozdějších předpisů, případně poskytnout tyto informace jinou formou (např. zasláním nebo vložením do monitorovacího systému). Povinnost zveřejňování účetních závěrek se týká těch subjektů, které mají takové povinnosti uloženy zákonem o účetnictví v §21a.
- KP je povinen dodržovat zásadu „významně nepoškozovat“, tedy nepodporovat nebo nevykonávat hospodářské činnosti, které významně poškozují kterýkoli environmentální cíl, případně ve smyslu článku 17 Nařízení (EU) 2020/8521 a dále ve smyslu Oznámení Komise.
- KP je povinen v rámci realizace projektu vyloučit jakékoliv riziko střetu zájmů

5 NÁSTROJ PRO SPRÁVU DOKUMENTŮ A OBECNÉ ŠABLONY

Základním nástrojem pro správu dokumentů Programu EZ jsou MS Teams a SharePoint. Správu a administraci zajišťuje Projektová kancelář Programu EZ.

V současné době probíhá rozhodování o použití dalších nástrojů jako je např. Confluence a JIRA. Tato kapitola bude aktualizována po finálním rozhodnutí o použitých nástrojích pro správu dokumentace Programu EZ.

5.1 Seznam obecných šablon

6 ZÁKLADNÍ PRAVIDLA ZABEZPEČENÍ

Dodavatelé projektů v rámci programu Elektronizace zdravotnictví uvedených v seznamu projektů podle kapitoly 1.1 jsou identifikováni jako významní dodavatelé dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZoKB“) a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „VoKB“). Dodavatelé proto musí dodržovat všechny povinnosti vyplývající ze ZoKB, VoKB a souvisejících právních předpisů. V této souvislosti je nutné zdůraznit, že MZ má právo provádět u dodavatelů bezpečnostní audit. Požadavky jsou uvedeny a upřesněny v rámci smluvního ujednání mezi dodavatelem a Ministerstvem zdravotnictví. Bezpečnostní požadavky mohou být na základě analýzy rizik dodavatelského řetězce v průběhu realizace projektů aktualizovány.

Každá osoba je povinna dodržovat základní pravidla zabezpečení pro ochranu údajů a informací, které by mohly být potenciálně citlivé.

Web strategie: https://ncez.mzcr.cz/

Citace dle ČSN ISO 690:2022:

MINISTERSTVO ZDRAVOTNICTVÍ ČESKÉ REPUBLIKY. Elektronizace zdravotnictví – Stanovení podmínek realizace, verze dokumentu 0.1. Praha, 2024. Licencováno pod CC BY 4.0, licenční podmínky dostupné z: http://creativecommons.org/licenses/by/4.0/.

Realizační požadavek

Název projektu	dsadasa		
Číslo projektu			
Identifikátor objednávky		Identifikátor požadavku	
Název požadavku			
Požadované datum dokončení			
Specifikace úkolů	*Detailní popis požadavku, včetně popisu formy výstupu*		

Odhady nákladů realizace požadavku

Role	Počet MD
Celkem MD	**0**

Specifické požadavky	

Schvalovací doložka

Řídící výbor	☐		Dne		
Výkonný výbor	☐		Dne		
Projektový výbor	☐		Dne		
Ředitel NCEZ	☐	Dne		Podpis	
Vedoucí NCEZ	☐	Dne		Podpis	
Projektový vedoucí	☐	Dne		Podpis	

*Rozsah schválení Realizačního požadavku se řídí platnou maticí odpovědností.

Potvrzení Realizačního požadavku Dodavatelem

Název projektu			
Číslo projektu			
Identifikátor objednávky		Identifikátor požadavku	
Název požadavku			

Role	Jméno pověřené osoby k plnění Realizačního požadavku

Požadavky na součinnost	
Varianty řešení	
Ostatní	

Analýza dopadu

Oblast	Dopad změny Ano/Ne
Model EA architektury (specifikujte)**	
Model Solution architektury komponenty (specifikujte)**	
Metodika *(specifikujte)*	
Dokumentace architektury EA/Solution	
Systémová dokumentace	
Uživatelská dokumentace	
Programátorská dokumentace	
Bezpečnostní dokumentace	
Zdrojový kód*	
Ostatní realizační úkoly / projekty *(specifikujte)***	
Vlastnické, užívací právo a standardní software ***	

** Dokumentace změny zdrojového kódu musí obsahovat podrobný popis a komentář každého zásahu do zdrojového kódu.*

*** V případě, že realizace požadavku ovlivní jiný realizační úkol nebo projekt, je třeba v analýze dopadu jasně a detailně specifikovat, jakým způsobem se dopad projeví.*

**** V případě, že je součástí požadavku změna týkající se těchto oblastí, bude příslušným způsobem doplněno.*

Specifikace dopadů		
Schvalovací doložka		
Dodavatel potvrzuje, že Realizační požadavek je schopen splnit dle specifikace a požadovaném harmonogramu	Odpovědná osoba za dodavatele	Jméno a prijmení
	Datum	
	Podpis	

Výkaz práce

Název projektu					
Číslo projektu					
Identifikátor objednávky			Identifikátor požadavku		
Název požadavku					
Jméno pracovníka			Role		
Rok		Měsíc		Celkem odpracovaných dní	0,0

Datum	Počet hodin	Činnost

Součet hodin 0

Datum			Podpis pracovníka	

Výhrady k Výkazu práce Ano ☐ Ne ☐

Výkaz práce převzal a schválil	Datum	Podpis

Národní plán obnovy

Financováno Evropskou unií
NextGenerationEU

NÁRODNÍ CENTRUM ELEKTRONICKÉHO ZDRAVOTNICTVÍ

MINISTERSTVO ZDRAVOTNICTVÍ ČESKÉ REPUBLIKY

Metodika testování aplikací

Projekt Národní centrum elektronického zdravotnictví (registrační číslo CZ.31.1.01/MV/22_05/0000005)

Součást Metodiky řízení kvality na projektech MZČR/NCEZ/NPO

Obsah

Historie verzí

Verze	Datum	Autor	Popis změn	Označení změn
1.0	18.6.2024		Metodika testování, výchozí verze	Finální

Seznam zkratek a pojmů

Zkratka	Význam
MZČR, MZ	Ministerstvo zdravotnictví České republiky
SW	Software je souhrnný název pro všechny programy a aplikace.
Use Case	Označení pro případ užití, termín používaný v softwarovém inženýrství a systémové analýze k popisu interakcí mezi uživatelem (nebo aktérem) a systémem, které vedou k dosažení konkrétního cíle.
PM	Projektový manažer
NCEZ	Národní centrum elektronického zdravotnictví
MKB	Manažer Kybernetické bezpečnosti
N/A	Zkratka z anglického "Not Available", což v překladu znamená "Není k dispozici" nebo "Není aplikovatelné".
Git	Git je distribuovaný systém pro správu verzí, který se používá k sledování změn v kódu a řízení verzí softwarových projektů
DDoS	Distributed Denial of Service je typ kybernetického útoku, při kterém jsou zasílány velké množství žádostí na cílový server, službu nebo síť ze spousty různých zdrojů současně.
ISTQB	International Software Testing Qualifications Board, je mezinárodní nezisková organizace, založená v roce 1998 a její systém certifikování testerů se stal předním světovým systémem certifikace v oblasti testování softwaru.

Seznam příloh

Příloha č.	
Příloha č. 1	EZ_Testovaci_scenar.xlsx – šablona testovacích scénářů

1 ÚVOD

Cílem tohoto dokumentu je stanovit metodická pravidla a metody pro přípravu a realizaci procesu testování informačních systémů a aplikací dodávaných ve formě služeb. Testy budou probíhat na projektech financovaných v rámci Národního plánu obnovy týkající se elektronizace zdravotnictví. Cílem provádění testů systémů a aplikací je ověření funkčnosti, stability, výkonu a úrovně ochrany kybernetické bezpečnosti.

Dokument neobsahuje konkrétní testovací případy a scénáře a ani specifikace testovacích dat, ty jsou předmětem definic v rámci konkrétních realizačních projektů.

1.1 Určení dokumentu

Tento dokument je určen pro zhotovitele aplikací či systémů a popisuje pravidla a metody, které pro testování je povinen použít Dodavatel v rámci projektu. MZČR si může ad-hoc provádět samostatné testy v jednotlivých oblastech, nebo může zadat provedení těchto testů jako samostatný projekt se specifickými metodami a pravidly uvedených v zadání a platnými jen pro tento samostatný projekt.

2 Strategie testování

Testování je klíčovou součástí projektu vývoje a dodávky nového systému. Cílem testování je zajištění kvality systému a ověření jeho funkčnosti, spolehlivosti a výkonu.

Mezi cíle testování v projektu patří:

- Ohodnotit pracovní produkty, jako jsou požadavky, uživatelské scénáře, návrh a kód.
- Ověřit, zda byly splněny všechny specifikované požadavky.
- Potvrdit, že je testovaný objekt kompletní a funguje tak, jak uživatelé a zainteresované strany očekávají.
- Vytvořit důvěru v danou úroveň kvality testovaného objektu.
- Předcházet defektům.
- Odhalit selhání a defekty.
- Poskytnout informace zúčastněným stranám v dostatečné míře tak, aby mohly činit kvalifikovaná rozhodnutí, zejména pokud jde o úroveň kvality testovaného objektu.
- Snížit úroveň rizika nízké kvality softwaru (např. dříve neodhalená selhání, která se projeví v provozu).
- Ověřit zda jsou dodrženy zákonné normy jako například ISVS a ZkOB.
- Dodržet smluvní, právní nebo regulatorní požadavky nebo normy a/nebo ověřit, zda testovaný objekt dosahuje shody s takovými požadavky nebo normami.

Je preferováno využití automatizovaných testů, které jsou rychlé, opakovatelné a umožňují efektivní pokrytí scénářů testování. Dodavatel pro automatizaci testů navrhne a dodá/zapůjčí příslušný nástroj.

3 Testování SW aplikací / systémů

Základní požadavky na ověření kvality Produktu projektu (viz. PRINCE2, Metodika řízení projektů MZČR, Metodika řízení kvality NCEZ), resp. dodávané SW aplikace jsou definovány již v rámci přípravy Prováděcího projektu. Již zde musí být jasné, že systém bude akceptován na základě funkčních a nefunkčních testů. Rozsah a typy testů by měly být definovány nejpozději jako vstup pro výběrové řízení (může ovlivnit rozsah pracnosti atp.).

Testování – ověřováni kvality probíhá dle strategie řízení kvality a každá aktivita je zaznamenána do Registru kvality.

V první realizační projektové fázi – zpracování Prováděcího projektu je pro účely testování zpracován Testovací plán, testovací scénáře a šablona testovacího reportu.

3.1 Testovací plán

Dokument, který definuje přístup, rozsah, zdroje a harmonogram testovacích aktivit zaměřených na software nebo systém. Obsahuje informace o cílech testování, testovacích scénářích, strategiích, zdrojích a dalších podrobnostech potřebných k úspěšnému provedení testů. Plán testů pomáhá zajistit, aby všechny aspekty testování byly dobře promyšlené a provedené systematicky. Typicky zahrnuje následující položky:

- Úvod a účel. Manažerské shrnutí: Stručný přehled dokumentu a vysvětlení, proč je testovací plán vytvořen a jaký je jeho hlavní cíl. Zahrnuje identifikaci rozsahu plánu ve vztahu k projektovému plánu, rozpočtová omezení a omezení zdrojů, rozsah testování, vymezení vazby testování na ostatní aktivity a případně proces změnového řízení, pravidla pro komunikaci a koordinaci klíčových aktivit.
- Reference: Seznam všech dokumentů, které plán testování podporují, nebo se k němu vztahují. Může se jednat o projektový plán, specifikace požadavků, designové specifikace, standardy pro proces vývoje software a testování metodologické příručky a příklady, podnikové standardy a směrnice, apod.
- Rozsah testování: Přesné vymezení toho, co bude a nebude testováno (moduly, funkce, komponenty apod.). U vymezení co není předmětem testování se uvádí zdůvodnění, proč nebudou testovány.
- Cíle testování: Konkrétní cíle, které mají být testováním dosaženy, například ověření funkčnosti, výkonnosti, bezpečnosti nebo kompatibility.
- Testovací strategie: Metody a přístupy, které budou použity k provedení testů, včetně typů testů (např. manuální, automatizované, funkční, nefunkční).
- Testovací prostředí: Detaily o hardwaru, softwaru, síťových konfiguracích a dalších prvcích potřebných pro testování.

- Součásti dodávky za testování: Seznam součástí dodávky ze strany testovacího týmu. Součástí dodávky mohou být kromě testovacího plánu a testovacích scénářů, výstupy z nástrojů pro podporu testování, simulátory, statické a dynamické generátory, test logy, reporty defektů, reporty o stavu testování a další.
- Kritéria pro zahájení a ukončení testů: Podmínky, které musí být splněny, aby mohlo být testování zahájeno a ukončeno (např. dostupnost testovacích prostředí, stabilita softwaru).
- Kritéria pro přerušení a požadavky na následnou obnovu: Definice podmínek, při kterých je nutné přerušit testování. Specifikují akceptovatelnou úroveň defektů, které ještě umožní pokračovat v testování po předchozích defektech. Dále specifikuje aktivity, které je nutné opakovat při obnově testování.
- Harmonogram testování: Časový plán jednotlivých testovacích aktivit, včetně milníků a termínů pro dokončení testů.
- Role a odpovědnosti: Seznam členů testovacího týmu a jejich specifické role a odpovědnosti v rámci testování.
- Testovací scénáře a případy: Podrobný popis testovacích scénářů a případů, které budou provedeny, včetně vstupů, očekávaných výstupů a kroků k provedení testů.
- Kritéria pro přijetí: Měření a ukazatele, které určují, zda software splňuje požadavky a je připraven pro nasazení.
- Plán správy defektů: Proces pro identifikaci, zaznamenávání, sledování a řešení defektů nalezených během testování.
- Rizika a zmírňování rizik: Identifikace potenciálních rizik spojených s testováním a strategie pro jejich zmírnění.
- Plán komunikace: Jak budou výsledky testování, zprávy a další důležité informace komunikovány mezi členy týmu a zainteresovanými stranami.
- Zdroje: Seznam všech potřebných zdrojů, včetně nástrojů, infrastruktury a lidských zdrojů potřebných k provedení testování.
- Požadavky na testovací prostředí a infrastrukturu pro testování: Specifikace nezbytných a požadovaných vlastností testovacího prostředí a testovacích dat, což může zahrnovat požadavky na speciální hardware i software, podpůrné nástroje, databáze, platformy, lidské zdroje, nastavení prostředí před zahájením testování a další potřeby.
- Součinnosti: Identifikace vztahů a dodávaných pracovních produktů mezi testovacím týmem a ostatními osobami či odděleními.
- Znalostní báze: Jaké znalosti a zkušenosti mají mít testeři, školení a dokumentace podporující provedení testů.
- Terminologický slovník: Seznam termínů a zkratek používaných v plánu testování a obecně v oboru testování spolu s vysvětlením jejich významů

- Závěrečné poznámky: Jakékoliv další relevantní informace, které nebyly zahrnuty v předchozích částech.

S ohledem na různorodost požadavků / aplikací je nutné, aby projekt měl Testovací plán. Testovací plán je živý dokument, který se může měnit a upravovat podle potřeby během celého testovacího cyklu, aby odrážel aktuální potřeby a zjištění.

Testovací plán vytváří Dodavatel a Zákazník připomínkuje a schvaluje.

Obsah Testovacího plánu může přesahovat výše uvedená témata. Vzorové Testovací plány lze nalézt v normě ISO/IEC/IEEE 29119-3.

3.2 Testovací scénář

Dokument v první části popisuje předpoklady k provedení testu, kroky testera (krok za krokem) – co musí udělat a jaký výsledek je očekávaný. K testovacím scénářům vznikne jejich seznam, ve kterém bude zaznamenána vazba na požadavek, který má testovací scénář ověřit. Obdobně do seznamu funkčních a nefunkčních požadavků bude přidána vazba na testovací scénáře které požadavek ověřují. Druhá část dokumentu je určena pro zaznamenání detailních výsledků testu s popisem odchylky/chyby od očekávaného výsledku a vazbou na ticket k jejímu odstranění. Testovací scénáře, zejména pro funkční testy by měly být vytvořeny na základě funkční specifikace a měla by zde být vazba na jednotlivé případy užití (Use Case). Testovací scénáře se připravují i pro nefunkční požadavky – testy výkonových, nebo bezpečnostních parametrů. Plnění druhé části dokumentu se provádí v průběhu testování SW aplikace ve fázi testování.

Dokument připravuje Dodavatel v rámci realizační fáze.

Součástí přípravy první části testovacího scénářů je příprava testovacích dat za součinnosti Zadavatele a to jak na úrovni dat který se při testech do testovaného systému budou vkládat, tak dat, která systém bude obsahovat pro úspěšné provedení reportu v druhé části.

Formát testovacích scénářů pro ruční testy v minimalistické verzi bude v Excelu nebo je na vyzvání Dodavatel nahraje do nástroje určeného na správu testů. Nástroj na správu a řízení testů instaluje a provozuje Zadavatel.

Automatizované testovací scénáře Dodavatel nahraje do automatizačního testovacího nástroje a zdrojové soubory včetně popisu budou předané v textové formě, jakož i návod na nahrání a provozování testovacího nástroje.

3.3 Testovací report

Jedná se o excel tabulku nebo výstup z nástroje pro řízení a správu testů se seznamem jednotlivých Testovacích scénářů, kam se zapisují souhrnné výsledky z testování (jednotlivých testovacích kol). Report obsahuje zejména výsledek testovacího případu, závažnost chyby, typ testů, identifikace testovacího kola a relevantní osoby – tester, test manager, kvality manager, PM MZ.

Test report dává přehled o aktuálním „stavu“ testování a na základě vyhodnocení jednotlivých kol je možné sledovat trendy v počtu a závažnosti chyb s ohledem na plán release. Testovací report se na základě požadavků a specifik dotčeného projektu může změnit.

Testovací report připravuje strana, která provádí testovaní, protistrana poskytuje na vyzvání součinnost. Například, když test provádí Zadavatel, tak report připravuje Zadavatel a Dodavatel na vyzvání poskytuje relevantní informace, jako třeba stav řešení vad a jejich výhled na odstranění.

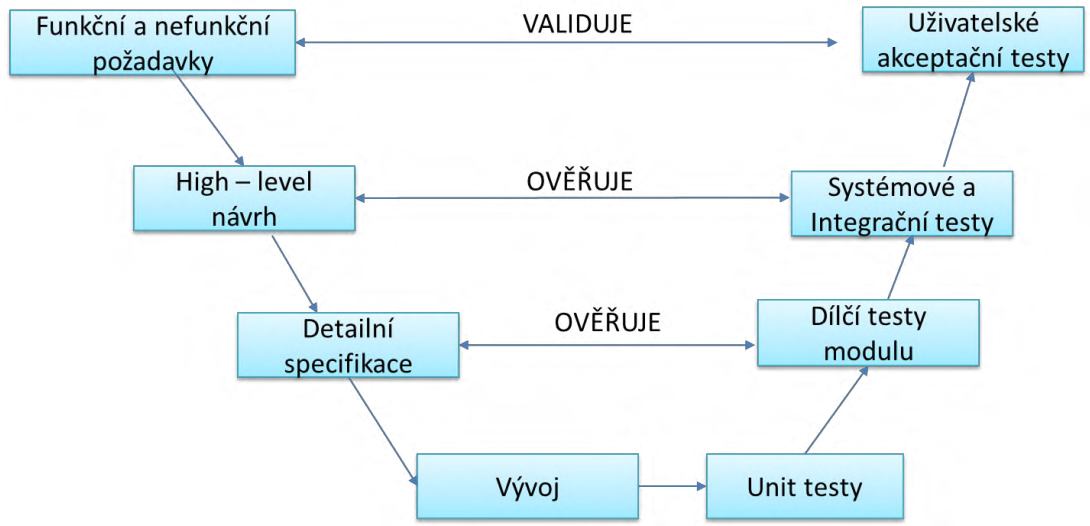
4 Umístění testů na projektu

Testy na projektu vycházejí z metodologie vývoje softwaru a testování (Viz. ISO 9001, ISO/IEC 12207, ISO/IEC 20000 , ISO/IEC/IEEE 29119, NIST Special Publication 800-84 a best practice -ITIL, ISTQB), která zdůrazňuje paralelní vztah mezi fázemi vývoje a testování. Tento model je rozšířením tradičního vodopádového modelu a jeho název je odvozen od tvaru písmena "V", které vzniká při znázornění modelu, kdy jsou testovací fáze umístěny paralelně k fázím vývoje.

V-Model testování charakterizuje:

- Každá fáze vývoje má svou odpovídající testovací fázi.
- Požadavky na software jsou testovány pomocí akceptačních testů.
- Návrh systému je testován systémovými testy.
- Návrh architektury je testován integračními testy.
- Detailní návrh (design) je testován jednotkovými testy.

Souvislost mezi testy a vývojem aplikace v průběhu projektu zachycuje následující obrázek.



Obrázek 1 - V model testů

Použití V modelu v testech pomáhá zajistit, že každý krok vývoje je systematicky ověřován, čímž se minimalizuje riziko chyb a nedostatků ve finálním produktu.

5 Akceptace testů

Hodnoty a dopady výstupu testů posuzuje v rámci akceptačního řízení Řídící popřípadě Výkonný výbor, min dostává pro info, že testy byly dokončeny a s jakým výsledkem.

Testy jsou součástí akceptačního řízení – kompetence PM NCEZ, pro rozhodnutí o akceptaci testů dostává výsledky testů autorizované:

- Garantem aktiva
- Architektem NCEZ
- MKB NCEZ (pokud součástí byly KB testy)
- Klíčovým uživatelem NCEZ (pokud byl definován)
- Odbornou společností (pokud byla definována)
- Případně další osobou určenou MZČR/NCEZ

Podklady připravuje Dodavatel za součinnosti Zadavatele, k autorizaci předkládá a zajišťuje Zadavatel osobou určenou na projektu (typicky Testovací manažer Zadavatele)

Podrobněji v dokumentu zabývajícím se zajištěním kvality a v smluvních dokumentech projektu.

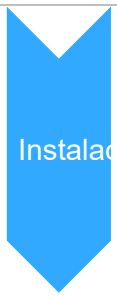
6 Proces testování

Proces	Prostředí	Tým	Popis	Výstup
	Vývojové prostředí Dodavatele	Vývojový tým Dodavatele	Vývoj aplikace dle schváleného plánu, kvalita zdrojového kódu odpovídá standardu MZ, nebo best practise. Průběžné provádění Unit testů aplikačních modulů.	N/A
	N/A	Vývojový tým Dodavatele	Ukončení vývojové fáze – dokončeny všechny funkční i nefunkční části. Vytvořen build pro nasazení do testovacího prostředí k ověření funkčnosti.	N/A
	Testovací prostředí Dodavatele	Testovací tým Dodavatele	Cílem je provést co největší rozsah funkčních a nefunkčních testů (s ohledem na neexistující integrace a data, nebo pouze dummy – simulovaná). Pro testy využije Dodavatel v maximální míře integraci, tam kde je to možné. Dodavatel dokládá MZ připravenost systému k testování na straně MZ formou reportu o provedených testech.	Výstup: Report Dodavatele o provedených testech a připravenosti systému k uživatelským testům (KPI nejsou, ale systém by měl být testovatelný).
	N/A	Vývojový tým Dodavatele	Vytvořen build pro nasazení do testovacího prostředí MZ. Build uložen do repository.	Výstup: Předávací protokol k aktuální verzi aplikace, Release notes.
	Testovací prostředí MZ	Admin tým MZ za podpory Dodavatele, nebo tým Dodavatele	Z repository MZ je provedena instalace aplikace do testovacího prostředí MZ. Správnost a funkčnost aplikace ověřena tzv. smoke testy (ověření vybraných/hlavních use case, integrací nebo pouze kontrola logů atp., může být různé). Odpovídá Dodavatel.	N/A

	Testovací prostředí MZ	Admin tým MZ za podpory Dodavatele, nebo tým Dodavatele	Předání instalované verze systému.	Výstup: Instalační protokol
	Testovací prostředí MZ	Dodavatel za podpory Admin /tech.tým MZ (připravuje Dodavatel, provádí MZ, za 3.stranu zajišťuje MZ pokud není dohodnuto jinak)	Integrační testy mají za cíl ověřit správnou integraci jednotlivých komponent a modulů systému. Během integračních testů budou testována rozhraní mezi jednotlivými částmi /moduly systému, včetně externích systémů, a bude ověřována jejich bezproblémová komunikace (autentizace, komunikace atp.).	Výstup: Testovací report, aktualizace Registru kvality Exit kritérium: dosažení KPI
	Testovací prostředí MZ	Testovací tým MZ	Uživatelské funkční testy ověřují funkčnost systému z pohledu uživatelů a prověřují pokrytí všech zadaných procesů a splnění všech funkčních požadavků na systém. Nedílnou součástí funkčních testů je i testování kvality a úplnosti datové migrace. Testy jsou obvykle koncipovány jako více kolové.	Výstup: Testovací report, aktualizace Registru kvality Exit kritérium: dosažení KPI (KPI mohou být stanovené i pro opravy chyb)
	Vývojové prostředí Dodavatele	Vývojový tým Dodavatele	Oprava zjištěných a akceptovaných chyb.	Výstup: Report Dodavatele o provedených testech – v rámci dotčených testovacích scénářů.
	N/A	Vývojový tým Dodavatele	Vytvořen build s opravami pro nasazení do testovacího prostředí MZ. Build uložen do repository MZ.	Výstup: Předávací protokol k aktuální verzi aplikace, Release Notes.
	Testovací prostředí MZ	Admin tým MZ za podpory Dodavatele, nebo tým Dodavatele	Z repository MZ je provedena instalace aplikace do testovacího prostředí MZ. Správnost a funkčnost aplikace ověřena tzv. smoke testy. Odpovídá Dodavatel.	N/A

	Testovací prostředí MZ	Admin tým MZ za podpory Dodavatele, nebo tým Dodavatele	Předání instalované verze systému.	Výstup: Instalační protokol
Pozn.	*Počet testovacích kol se stanovuje v závislosti na složitosti systému. V rámci harmonogramu je nezbytné počítat jak s vlastním testováním, tak i s časem nezbytný pro opravy, interní testy Dodavatele, příprava buildu a instalace nové verze. Doporučujeme minimálně týdenní testovací cyklus. Testování se provádí v naplánovaném rozsahu, nebo do doby dosažení KPI.*			
	testovací prostředí MZ	Testovací tým MZ	Uživatelské funkční testy ověřují funkčnost systému z pohledu uživatelů a prověřují pokrytí všech zadaných procesů a splnění všech funkčních požadavků na systém. Nedílnou součástí funkčních testů je i testování kvality a úplnosti datové migrace. Testy jsou obvykle koncipovány jako více kolové.	Výstup: Testovací report, Update Registr kvality Exit kritérium: dosažení KPI
	Vývojové prostředí Dodavatele	Vývojový tým Dodavatele	Oprava zjištěných a akceptovaných chyb.	Výstup: Report Dodavatele o provedených testech – v rámci dotčených testovacích scénářů.
	N/A	Vývojový tým Dodavatele	Vytvořen build s opravami pro nasazení do prostředí MZ. Build uložen do repository MZ.	Výstup: Předávací protokol k aktuální verzi aplikace, Release Notes
	Testovací prostředí MZ, nebo prostředí pro výkonové testy	Admin tým MZ za podpory Dodavatele, nebo tým Dodavatele	Z repository MZ je provedena instalace aplikace do testovacího prostředí MZ. Správnost a funkčnost aplikace ověřena tzv. smoke testy. Odpovídá Dodavatel.	N/A

	Testovací prostředí MZ, nebo prostředí pro výkonové testy	Admin tým MZ za podpory Dodavatele, nebo tým Dodavatele	Předání instalované verze systému.	Výstup: Instalační protokol
	Testovací prostředí MZ, nebo prostředí pro výkonové testy	Dodavatel za podpory Testovací/ Technický tým MZ (připravuje Dodavatel včetně zapůjčení podpůrných nástrojů, provádí MZ)	Výkonové (nebo výkonové a kapacitní testy) – cílem je ověřit výkonové požadavky na odezvy a reakce systému (odezva systému – přechod mezi obrazovkami při současném zatížení XY uživatelů, kontrola objemu ukládaných dat, testy, pro jakém počtu uživatelů dojde k nepřiměřenému prodloužení odezvy uživatelům atp.)	Výstup: Testovací report, Aktualizace Registru kvality Exit kritérium: dosažení KPI
	Testovací prostředí MZ, nebo prostředí pro bezpečnostní testy	Testovací / Technický tým MZ, nebo nezávislá specializovaná organizace	Bezpečnostní (penetrační) testy – obvykle black box režim.	Výstup: Testovací report, Update Registr kvality Exit kritérium: dosažení KPI (nemá kritické, závažné a ani střední zranitelnosti)
	Testovací prostředí MZ, nebo prostředí pro ostatní testy	Dle typu testů	Další specifické testy – dle charakteru systému, nebo požadavků Zadavatele (testy k ověření správnosti instalačního postupu, provozních postupů, testy migrace dat, test Disaster recovery planu, atp.).	Výstup: Testovací report, Update Registr kvality
Pozn.	*Výkonové, bezpečnostní (penetrační), případně ostatní tesy se provádí na otestovaném systému, v prostředí co nejvíce simulujícím finální produkční prostředí (např. se provádí na druhém node produkčního systému). Testy se také mohou opakovat v případě, že systém nesplní požadovaná kritéria.* *Každá identifikovaná chyba vyžaduje opravu a ověření opravené chyby.* *Předpokládejme, že nemáme další chyby (byly opraveny, včetně ověření správnosti opravy).*			

	Testovací prostředí MZ	Testovací tým uživatelů	UAT (User Acceptance Test) jsou prováděny skupinou koncových uživatelů systému a je ověřována funkčnost systému z pohledu koncového uživatele. Součástí UAT testu je i tzv. free testing.	Výstup: Testovací report, Update Registr kvality
	Vývojové prostředí Dodavatele	Vývojový tým Dodavatele	Oprava zjištěných a akceptovaných chyb.	Výstup: Report Dodavatele o provedených testech – v rámci dotčených testovacích scénářů.
	N/A	Vývojový tým Dodavatele	Vytvořen build pro produkční prostředí a pro testovací/prostředí provozní podpory. Buildy uložen do repository MZ.	Výstup: Předávací protokol k aktuální verzi aplikace, Release Notes
	Testovací prostředí MZ	Testovací tým uživatelů	UAT (User Acceptance Test) jsou prováděny skupinou koncových uživatelů systému a je ověřována provedená oprava chyb funkčnosti systému z pohledu koncového uživatele. Může být proveden regresní test. Součástí testu je i tzv. free testing.	Výstup: Testovací report, Update Registr kvality Exit kritérium: dosažení KPI
	Produkční prostředí	Admin tým MZ za zvýšené podpory Dodavatele,	Z repository MZ je provedena instalace aplikace do produkčního prostředí MZ. Správnost a funkčnost aplikace ověřena tzv. smoke testy. Odpovídá Dodavatel.	Šablona: Instalační protokol Výstup: Instalační protokol
	Produkční prostředí	Zvýšená podpora ze strany MZ a Dodavatele (čeká se na první špičku)	Systém spuštěn do produkčního provozu. Přechod na Služby podpory ze strany Dodavatele, SLA a jejich vyhodnocování.	

Instalac	Testovací Prostředí, nebo prostředí pro provozní podporu	Admin tým MZ za podpory Dodavatele,	Z repository MZ je provedena instalace aplikace do prostředí provozní podpory MZ. Správnost a funkčnost aplikace ověřena tzv. smoke testy. Odpovídá Dodavatel.	Výstup: Instalační protokol
	Testovací Prostředí, nebo prostředí pro provozní podporu	Zvýšená podpora ze strany MZ a Dodavatele (čeká se na první špičku)	Systém spuštěn pro účely provozní podpory.	
	N/A	N/A	Akceptace	Výstup: Akceptační protokol

Vysvětlivky – popis prostředí:

Vývojové prostředí Dodavatele – prostředí Dodavatele, kde probíhá vývoj aplikace / SW vybavení. Prostředí je obvykle neřízeno a minimálně omezeno. Externí systémy – intergace – jsou dostupné v omezené míře, nebo pouze jako dummy.

Testovací prostředí Dodavatele – prostředí Dodavatele určené pro ověřování kvality systému, prostředí bývá obvykle řízené (bez vývojářského přístupu), prostředí může a nemusí mít externí vazby, ne vždy je možné ověřit integrace (obvykle).

Testovací prostředí MZ – prostředí objednatele určené pro ověřování kvality dodávané SW aplikace, jedná se o řízené prostředí včetně nezbytných integrací a externích systémů. Testovací prostředí také obsahuje datovou sadu nezbytnou pro plánované testy (pro všechny kola – nutná data obnovovat).

„jiné“ testovací/neprodukční prostředí – jedná se obvykle o prostředí pro účely specializovaných testů – výkonových, penetračních, testů releasu pro nasazení oprav na produkční prostředí atp., kde je nezbytná co největší podobnost se systémem produkčním.

Produkční prostředí MZ – standardní produkční prostředí pod provozní podporou MZ.

7 Druhy testu

Pod jednotlivými druhy testu rozumíme veškeré testování, které má za cíl ověřit naplnění funkčních a nefunkčních požadavků na dílo.

Testovací scénáře a data pro testing připraví Dodavatel, který bude zodpovídat za to, že tyto scénáře pokryjí všechny funkční a nefunkční požadavky uvedené v zadávací dokumentaci a specifikaci projektu. Zadavatel na přípravě poskytuje součinnost a reviduje jednotlivé výstupy.

Příprava scénářů a dat integračních a systémových testů proběhne ve spolupráci Dodavatele, Zadavatele a třetí stranou. Každý z účastníků testů připravuje testovací scénáře a data za svou stranu.

7.1 Unit testing

Jednotkové testy (unit tests) jsou základní formou testování softwaru, která se zaměřuje na ověřování správné funkčnosti jednotlivých částí kódu, typicky jednotlivých funkcí, metod nebo modulů. Cílem jednotkových testů je izolovat a ověřit chování každé menší části softwaru nezávisle na ostatních částech systému.

Klíčové aspekty jednotkových testů

- Izolace: Jednotkové testy jsou navrženy tak, aby testovaly jen jednu jednotku kódu najednou, bez závislosti na jiných modulech nebo funkcích.
- Automatizace: Jednotkové testy jsou obvykle automatizované, což znamená, že mohou být opakovaně spouštěny bez zásahu člověka.
- Opakovatelnost: Testy by měly být opakovatelné a konzistentní, tedy stejné testy by měly dávat stejné výsledky bez ohledu na to, kolikrát jsou spuštěny.

Výhody jednotkových testů

- Rychlá detekce chyb: Díky izolaci a specifickému zaměření mohou jednotkové testy rychle identifikovat chyby v kódu.
- Usnadnění refaktoringu: Když je kód pokryt jednotkovými testy, vývojáři mohou provádět změny a refaktorovat kód s jistotou, že neporuší existující funkcionalitu.
- Dokumentace kódu: Jednotkové testy mohou sloužit jako forma dokumentace, která ukazuje, jak má být daný kód používán a jaké jsou jeho očekávané výsledky.

Za provedení unit testingu bude zodpovědný Dodavatel.

7.2 Integrační testy

Integrační testy budou společně prováděny Dodavatelem, Zadavatelem a třetí stranou, a mají za cíl ověřit správnou integraci jednotlivých komponent a modulů systému. Během integračních testů budou testována rozhraní, včetně externích systémů, a bude ověřována jejich bezproblémová komunikace.

Klíčové aspekty integračních testů

- Testování rozhraní: Integrační testy ověřují, zda jednotlivé moduly správně komunikují přes definovaná rozhraní (API).
- Reálné prostředí: Tyto testy se často provádějí v prostředí, které simuluje reálné podmínky, pod kterými bude systém fungovat.
- Detekce chyb v interakci: Integrační testy jsou zaměřeny na identifikaci chyb, které se mohou vyskytnout při interakci mezi různými částmi systému, což jednotkové testy nemusí odhalit.

7.3 Uživatelské funkční testy

Uživatelské funkční testy ověřují funkčnost systému z pohledu uživatelů a prověřují pokrytí všech zadaných procesů a splnění všech funkčních požadavků na systém.

Nedílnou součástí funkčních testů je i testování kvality a úplnosti datové migrace.

Uživatelské testy provádí tým Zadavatele, který na tuto činnost musí být předem důkladně proškolen Dodavatelem.

7.4 Testy výjimek

Tento typ testování simuluje nesprávné chování uživatele, jako např. používání nekorektních dat apod. Tento typ testu má za úkol prověřit systém tak, aby nedošlo ke kolapsu systému, nedošlo ke zpracovávání nekorektních dat, aby docházelo ke korektnímu zápisu příčin problémů do logu.

7.5 Akceptační testy

Akceptační testy (UAT) budou prováděny na testovacím prostředí (resp. na prostředí, které bude nastaveno stejně jako budoucí provozní prostředí). Součástí akceptačního testu bude i ověření instalace systému podle schváleného rollout plánu.

Akceptační testy ověří, zda nový systém splňuje všechny funkční a nefunkční požadavky na systém uvedené v zadávací dokumentaci a specifikaci projektu. UAT včetně přípravy testovacích scénářů a dat provádí Zadavatel za podpory Dodavatele, s využitím testovacích scénářů připravených pro funkční testy.

Každý testovací scénář musí obsahovat jednoznačné akceptační kritérium.

Při provádění akceptačních testů projektový tým trvale monitoruje stav testování a informuje Projektový výbor o procentu úspěšně akceptovaných scénářů. Po akceptaci všech scénářů a doručení všech výstupů Dodavatelského projektu

7.6 Penetrační testy

Penetrační testy slouží k prověření a zhodnocení odolnosti systému proti vnějšímu nebo vnitřnímu útoku. Cílem je zdokumentovat slabá místa systému a dodat informace Dodavateli případně Zadavateli pro jejich odstranění.

Penetrační testy jsou prováděny v souladu s Českým Zákonem o kybernetické bezpečnosti, a zejména jeho prováděcí vyhláškou č. 316/2014 Sb., ISO27002 a nařízením (EU) 2016/679 (GDPR) a ISO27034.

Budou provedeny minimálně následující testy:

- Test infrastruktury (např. otevřené porty)
- Test uživatelského portálu
- Test interních uživatelů – pro všechny definované uživatelské role
- Simulovaný útok s cílem přetížit služby systému (DDoS).
- Testování bezpečnosti aplikací (bezpečnostní chyby v designu i ve skutečné implementaci)
- Revize zdrojového kódu, je-li projektem vyžadováno

Penetrační test se bude provádět některou z metodik OSSTMM, OWASP, NIST, PTES, nebo ISSAF. Dodavatel připraví návrh penetračních testů, ten je schvalován Zadavatelem. Následně Dodavatel penetrační test provede za přítomnosti Zadavatele a o provedeném testu Dodavatel vyhotoví protokol, který Zadavatel podepisuje.

Zadavatel se může rozhodnout svěřit provedení penetračních testů třetí straně (bezpečnostně zaměřené společnosti mající příslušné certifikace). V takovém případě Dodavatel poskytuje třetí straně skrze Zadavatele podporu.

Pokud budou identifikovány chyby v systému, které budou identifikovány jako závažné, bude test (minimálně v oblasti ovlivněné závažnými chybami) po jejich odstranění opakován.

Po nasazení systému do provozního prostředí bude test zopakován na žádost bezpečnostního oddělení.

7.7 Zátěžové testy

Zátěžové testy budou prováděny Dodavatelem a zaměří se na testování výkonu a odolnosti systému za extrémních zátěžových podmínek. Tyto testy mají za cíl ověřit, jak systém reaguje a udržuje výkonnost při zvýšeném počtu uživatelů, transakcí nebo při velkém objemu dat.

Testovací scénáře a podpůrné nástroje (specializovaný software) připraví Dodavatel, pokud nebude dohodnuto jinak.

Důležitým požadavkem na testovací scénáře je, aby věrně kopírovali maximální reálnou zátěž v každé z operací. Je tedy třeba počítat s nejhorší možnou, ale stále ještě reálnou kombinací požadavků na systém (např. je možné, že se ve stejnou chvíli přihlásí do systému všichni uživatelé z daného časového pásma, ale už nereálné, tedy mimo scénář testu je, že se najednou přihlásí, nebo provedou konkrétní operaci všichni uživatelé ze všech zastupitelských úřadů).

Zátěžový test nepředpokládá útok typu DDoS, odolnost proti cílenému útoku bude ověřována v rámci penetračního testu.

Pro realizaci zátěžového testu bude využit specializovaný software, aby bylo možno monitorovat spouštěné akce, jejich trvání a zátěž klíčových komponent systému (procesory, paměť, síť atd.). Veličiny typicky měříme v transakcích za sekundu, dobou odezvy, počtem současně pracujících klientů, úrovní využití zdrojů atd.

Zátěžovému testování aplikací se věnuje standard ISO/IEC/IEEE 29119-4. Vychází z dřívější normy IEEE 829-2008 či ještě dřívějšího BS 7925-2.

7.8 Typy zátěžového testování aplikace

Standardy pro testování popisují několik základních technik zátěžového testování aplikací. Budou provedené všechny dávající smysl pro dodávané dílo.

Testování aplikace zátěží

Testování aplikace zátěží se obvykle provádí pro zjištění chování systému (například jeho výkon a spolehlivost) při specifickém předpokládaném zatížení. Tato zátěž může být způsobena očekávaným souběžným počtem uživatelů v aplikaci, která provádí určitý počet transakcí v rámci stanovené doby trvání. Tento test zjistí dobu odezvy pro důležité transakce. Databáze, aplikační server apod. mohou být během testu sledovány, což pomůže při identifikaci úzkých míst v aplikačním softwaru a hardwaru, na němž je software nainstalován.

Stresové testování

Stresové testování se obvykle používá k pochopení horních limitů kapacity v systému. Tento typ testu slouží k určení robustnosti systému z hlediska extrémního zatížení a pomáhá administrátorům aplikací ověřit, zda systém bude fungovat dostatečně, pokud aktuální zatížení překročí očekávanou maximální hodnotu.

Testování odolnosti

Testy odolnosti, se obvykle provádí k zjištění, zda systém dokáže vydržet nepřetržité jisté významné zatížení a jak se během něj a po něm chová. Během testů odolnosti se typicky monitoruje využití paměti pro detekci potenciálních paměťových úniků. Důležitým parametrem je degradace výkonu, tj. zjištění, zda výkonnost a doba odezvy po určité dlouhé době trvalé aktivity jsou stejně dobré nebo lepší než na začátku testu.

Testování špiček

Testování špiček se provádí náhlým zvýšením nebo snížením zatížení generovaného velkým počtem uživatelů a sledováním chování systému. Cílem je zjistit, zda výkon významně poklesne, jestli systém selže, nebo naopak je schopen zvládnout dramatické změny zatížení.

Objemové testování

Objemové testování je zaměřeno na posouzení výkonu systému při zadání zpracování specifického objemu údajů. Může například zahrnovat hodnocení systému, pokud je její databáze zaplněna z její téměř maximální kapacity.

Testování škálovatelnosti

Testování škálovatelnosti je zaměřeno na posouzení, jak bude systém fungovat za podmínek, které budou muset být v budoucnu podporovány. To může například zahrnovat posouzení, jaká úroveň dodatečných zdrojů (např. paměť, kapacita disku, šířka pásma sítě) budou muset být přidány pro očekávané budoucí zatížení.

7.9 Sledovaná kritéria

Určení sledovaných kritérií musí být vždy součástí zadání testování. Kritéria se budou lišit v závislosti na technologii a účelu systému. Příklady sledovaných kritérií mohou být následující:

Souběžnost a propustnost

Pokud systém identifikuje koncové uživatele nějakou formou přihlašovací procedury, je vhodné se zaměřit na kritérium souběžnosti. Podle definice je to největší počet souběžných uživatelů systému, které je systém schopen v daném okamžiku podporovat. Předpis pracovní skriptované transakce může mít vliv na změřenou souběžnost, zejména pokud obsahuje aktivitu přihlášení a odhlášení.

Pokud systém nemá koncept identifikace koncových uživatelů, pak je toto kritérium typicky založeno na maximální propustnosti nebo počtu transakcí za jednotku času.

Doba odezvy serveru

Doba odezvy serveru je čas, kdy jeden uzel systému odpovídá na žádost jiného. Jednoduchým příkladem je žádost HTTP GET od klienta prohlížeče na webový server. V konkrétních případech může být důležité nastavit kritéria pro měření času odezvy serveru mezi různými, či všemi uzly systému.

Doba odezvy vykreslení

Testovací nástroje mají většinou potíž s měřením doby odezvy vykreslení, neboť se obecně zaměřují na rozpoznání doby, kdy neexistuje žádná aktivita v komunikaci. K měření doby odezvy vykreslení je obecně nutné do scénáře testů zahrnout funkční testovací skripty.

7.10 Automatizovaná kontrola zdrojového kódu

V rámci procesu CI/CD je zdrojový kód při každém nasazení automaticky otestován (pozn. rozšíření continuous integration o tzv. continuous inspection) některým z nástrojů pro statickou analýzu kódu (př. SonarQube), integrovaným na Git Zadavatele. Tyto reporty jsou automaticky odesílány Zadavateli. Součástí reportu jsou základní ukazatele, zejména přidané řádky kódu, automaticky zjištěné bugy, duplicity, poměr komentovaných řádků kódu.

7.11 Regresní testy

Provádí se s cílem ověřit, že nově provedené změny v kódu neovlivnily negativně existující funkčnost systému. Jsou zaměřeny na zajištění toho, že po úpravách, opravách chyb nebo přidání nových funkcí stále fungují stávající funkcionality tak, jak mají.

Regresní testy se provádějí v následujících situacích:

- Po úpravách kódu: Kdykoli se provádí změny v kódu, ať už se jedná o opravy chyb, přidání nových funkcí nebo optimalizace kódu, je nutné provést regresní testy, aby se ověřilo, že tyto změny neporušily stávající funkčnost.
- Po aktualizaci knihoven nebo frameworků: Když se aktualizují závislosti projektu (například knihovny nebo frameworky), může to mít vliv na fungování aplikace. Regresní testy pomáhají ověřit, že aktualizace nezpůsobily problémy.
- Po integraci nového kódu: Pokud se nový kód integruje do stávajícího kódu (například při použití Continuous Integration/Continuous Deployment – CI/CD procesů), regresní testy se použijí k ověření, že integrace proběhla bez problémů.
- Před nasazením do produkčního prostředí: Regresní testy jsou často poslední kontrolou před nasazením nového kódu do produkčního prostředí, aby se minimalizovalo riziko, že se do produkce dostane chybový kód.

Druhy regresních testů

Automatizované regresní testy: Tyto testy se provádějí pomocí automatizačních nástrojů a jsou vhodné pro opakující se testovací scénáře. Automatizované testy jsou efektivní pro velké projekty s častými změnami, protože se dají rychle a opakovaně spouštět.

Manuální regresní testy: Tyto testy se provádějí ručně a jsou vhodné pro scénáře, které jsou těžké automatizovat nebo vyžadují lidský úsudek. Jsou také užitečné pro kontrolu nových funkcionalit, které ještě nebyly zahrnuty do automatizovaných testů.

Regresní testy navrhuje Dodavatel a Zadavatel připomínkuje a schvaluje. Regresní testy provádí Dodavatel a o jejich provedení vyhotovuje report který je součástí schvalování Zadavatelem na provedení změny v prostředích Zadavatele.

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Název dokumentu: Architektonické principy a vzory			
Název projektu:	**Projekt Národní centrum elektronického zdravotnictví**	**Identifikace projektu:**	
Verze dokumentu:	**1.0**	**Datum vytvoření:**	30.01.2024
Klasifikace:	**Veřejný ☐ Interní☐ Důvěrný ☐ Pouze určeným osobám ☐**		

Vysvětlení zkratek a pojmů	
Zkratka / pojem	**Význam**
Principy KB	Principy kybernetické bezpečnosti
Principy OHA	Principy Hlavního architekta eGovernmentu
Principy GDPR	Principy GDRP (Ochrana osobních údajů)
Interní principy MZ	Interní principy Ministerstva zdravotnictví ČR

Historie změn			
Pořadí změny	**Provedené dne**	**Zpracoval**	**Schválil**

Rozdělovník				
Jméno Příjmení	**Organizace/ útvar**	**Účel** (na vědomí, ke schválení, ke zpracování)	**Datum**	**Podpis**

ID principu	Typ požadavku	Kategorie	Název požadavku	Popis požadavku	Účel požadavku	Zdroj požadavku
K01	Funkční	Bezpečnostní požadavky	Zajištění segmentace sítě oddělením prostředí	Prostředí musí být odděleno minimálně na: Provozní, Zálohovací, Vývojové, Testovací a případně jiné specifické prostředí.	Soulad s legislativou	VKB §18 - Bezpečnost komunikačních sítí
K02	Funkční	Bezpečnostní požadavky	Řízení vzdáleného přístupu ke komunikační síti	Bude povolována pouze nezbytná komunikace v rámci vzdáleného přístupu.	Soulad s legislativou	VKB §18 - Bezpečnost komunikačních sítí
K03	Funkční	Bezpečnostní požadavky	Zajištění důvěrnosti a integrity při přenosu informací a dat v rámci komunikační sítě	Za pomocí aktuálně odolných kryptografických algoritmů je zajištěna nemožnost čtení či změny dat v komunikační síti.	Soulad s legislativou	VKB §18 - Bezpečnost komunikačních sítí
K04	Funkční	Bezpečnostní požadavky	Ověření identity před zahájením jejich aktivit	Každý uživatel musí být spolehlivě identifikován pře tím než zahájí jakoukoliv aktivitu na zařízení	Soulad s legislativou	VKB §19 - Správa a ověřování identit
K05	Funkční	Bezpečnostní požadavky	Řízení maximálního počtu možných neúspěšných pokusů o přihlášení	Po překročení počtu neúspěšných pokusů bude účet zablokován a bude ho moci odblokovat pouze administrátor.	Soulad s legislativou	VKB §19 - Správa a ověřování identit
K06	Funkční	Bezpečnostní požadavky	Odolnost uložených a přenášených autentizačních údajů vůči hrozbám a zranitelnostem, které by mohly narušit jejich důvěrnost nebo integritu		Soulad s legislativou	VKB §19 - Správa a ověřování identit
K07	Funkční	Bezpečnostní požadavky	Centralizovaná správa identit	Centrální nástroj pro správu, ověřování a ukládání identit uživatelů, administrátorů a technických aktiv	Soulad s legislativou	VKB §19 - Správa a ověřování identit
K08	Funkční	Bezpečnostní požadavky	Řízení oprávnění pro přístup k jednotlivým aktivům	Na základě pravidla "Need to know" jsou přiřazována uživatelská oprávnění pouze k aktivům, která jsou pro jejich práci relevantní.	Soulad s legislativou	VKB §20 - Řízení přístupových oprávnění
K09	Funkční	Bezpečnostní požadavky	Řízení oprávnění pro čtení dat, zápis dat a změnu oprávnění.	Na základě pravidla "Need to know" jsou přiřazována uživatelská oprávnění pouze k datům, která jsou pro jejich práci relevantní.	Soulad s legislativou	VKB §20 - Řízení přístupových oprávnění
K10	Funkční	Bezpečnostní požadavky	Zaznamenávání bezpečnostních a relevantních provozních událostí pomocí centrálního nástroje	Zaznamenává zejména následující informace o událostí: a) datum a čas včetně specifikace časového pásma, b) typ činnosti, c) jednoznačnou identifikaci technického aktiva, které činnost zaznamenalo, d) jednoznačnou identifikaci účtu, pod kterým byla činnost provedena, e) jednoznačnou identifikaci zařízení původce a f) úspěšnost nebo neúspěšnost činnosti.	Soulad s legislativou	VKB §22 - Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
K11	Funkční	Bezpečnostní požadavky	Zajištění důvěrnosti a integrity zaznamenaných logů a ochrana před jejím neoprávněným čtením a změnou	Zajištění důvěrnosti a integrity logů pomocí řízení oprávnění a použití kryptografických prostředků	Soulad s legislativou	VKB §22 - Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
K12	Funkční	Bezpečnostní požadavky	Zaznamenávání zejména všech událostí z §23 VoKB	Zaznamenává zejména následující události: a) přihlášení a odhlášení ke všem účtům a to včetně neúspěšných, b) provedení a neúspěšný pokus o provedení privilegovaných činností, c) manipulace a neúspěšný pokus o manipulaci s účty a oprávněními, d) Neprovedení činnosti v důsledku nedostatku přístupových práv, e) zahájení a ukončení činnosti technických aktiv, f) kritická a chybová hlášení technických aktiv, g) Přístup a neúspěšný přístup k záznamům událostí, h) Manipulace a neúspěšný pokus o manipulaci se záznamy událostí, ch) změnu a neúspěšnou změnu nástrojů pro zaznamenávání událostí a i) Další činnosti uživatelů, které mohou mít vliv na bezpečnost.	Soulad s legislativou	VKB §22 - Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
K13	Funkční	Bezpečnostní požadavky	Zajištění trvalé ochrany aplikací, informací, transakcí a identifikátorů relací	Znemožnění provedení neoprávněné činnosti nebo popřením provedení činnosti na těchto aktivech.	Soulad s legislativou	VKB §25 - Aplikační bezpečnost
K14	Funkční	Bezpečnostní požadavky	Zajištění kryptografické ochrany aktiv a komunikace	Budou využívány aktuálně odolné kryptografické prostředky a budou zohledněny doporučení a metodiky v oblasti kryptografických algoritmů vydané NUKIBem. Tato ochrana zajistí bezpečnost pro hlasovou, audiovizuální, textovou, emailovou a nouzovou (v rámci organizace) komunikaci.	Soulad s legislativou	VKB §26 - Kryptografické prostředky
K15	Nefunkční	Specifické požadavky Bezpečnost	Zamezení neoprávněného vstupu dle stanoveného bezpečnostního perimetru aktiva	Použití elektronické kontroly vstupu nebo jiných prvku fyzické bezpečnosti pro zamezení neoprávněného vstupu do stanoveného bezpečnostního perimetru.	Soulad s legislativou	VKB §17 - Fyzická bezpečnost
K16	Nefunkční	Specifické požadavky Bezpečnost	Zamezení poškození dle stanoveného perimetru aktiva	Použití elektronické kontroly vstupu nebo jiných prvku fyzické bezpečnosti pro zamezení poškození aktiva ve stanoveného bezpečnostního perimetru.	Soulad s legislativou	VKB §17 - Fyzická bezpečnost
K17	Nefunkční	Specifické požadavky Bezpečnost	Zamezení neoprávněným zásahům dle stanoveného bezpečnostního perimetru aktiva	Použití elektronické kontroly vstupu nebo jiných prvku fyzické bezpečnosti pro zamezení neoprávněným zásahům do stanoveného bezpečnostního perimetru.	Soulad s legislativou	VKB §17 - Fyzická bezpečnost
K18	Nefunkční	Specifické požadavky Bezpečnost	Zajištění fyzické ochrany na úrovni objektů		Soulad s legislativou	VKB §17 - Fyzická bezpečnost
K19	Nefunkční	Specifické požadavky Bezpečnost	Zajištění fyzické ochrany v rámci objektů		Soulad s legislativou	VKB §17 - Fyzická bezpečnost
K20	Nefunkční	Specifické požadavky Bezpečnost	Zajištění detekce narušení fyzického bezpečnostního perimetru		Soulad s legislativou	VKB §17 - Fyzická bezpečnost
K21	Nefunkční	Specifické požadavky Bezpečnost	Evidence přístupů do fyzického bezpečnostního perimetru	Všechny informace o přístupech do fyzického bezpečnostního perimetru jsou evidovány v k tomu určené a zabezpečené databázi.	Soulad s legislativou	VKB §17 - Fyzická bezpečnost
K22	Nefunkční	Bezpečnostní požadavky	Řízení komunikace v rámci komunikační sítě		Soulad s legislativou	VKB §18 - Bezpečnost komunikačních sítí
K23	Nefunkční	Bezpečnostní požadavky	Řízení vzdálené správy technických aktiv	Bude povolována pouze nezbytná komunikace v rámci vzdálené správy technických aktiv.	Soulad s legislativou	VKB §18 - Bezpečnost komunikačních sítí
K24	Nefunkční	Bezpečnostní požadavky	Využití nástroje, který zajistí ochranu integrity komunikační sítě		Soulad s legislativou	VKB §18 - Bezpečnost komunikačních sítí
K25	Nefunkční	Bezpečnostní požadavky	Vedení evidence technických aktiv, účtů a autentizačních mechanismů, které nesplňují požadavky na správu a ověření identit	Odpovědná osoba je povinna vést evidenci technických aktiv, která nesplňují požadavky na správu a ověření identit, a to včetně odůvodnění	Soulad s legislativou	VKB §19 - Správa a ověřování identit
K26	Nefunkční	Bezpečnostní požadavky	Dodržení důvěrnosti při vytváření výchozích autentizačních údajů a při obnově přístupu		Soulad s legislativou	VKB §19 - Správa a ověřování identit
K27	Nefunkční	Bezpečnostní požadavky	Opětovné ověření identity	Po stanovené době nečinnosti bude požadované opětovné ověření identity uživatele	Soulad s legislativou	VKB §19 - Správa a ověřování identit
K28	Nefunkční	Bezpečnostní požadavky	Vícefaktorová autentizace s nejméně dvěma různými typy faktorů		Soulad s legislativou	VKB §19 - Správa a ověřování identit
K29	Nefunkční	Bezpečnostní požadavky	Využití centralizovaného nástroje pro řízení přístupových oprávnění s ohledem na vazby mezi aktivy		Soulad s legislativou	VKB §20 - Řízení přístupových oprávnění
K30	Nefunkční	Bezpečnostní požadavky	Použití nástroje pro detekci KBI v rámci KS	Tento nástroj bude ověřovat a kontrolovat přenášená data v KS, mezi jednotlivými KS a v síťovém perimetru. Také bude blokovat nežádoucí komunikaci.	Soulad s legislativou	VKB §21 - Ochrana před škodlivým kódem
K31	Nefunkční	Bezpečnostní požadavky	Použití centrálně spravovaného nástroje pro detekci KBI	Tento nástroj by měl zajišťovat nepřetržitou a automatickou ochranu před škodlivým kódem, řízení a sledování používání vyměnitelných zařízení a datových nosičů, řízení automatického spouštění obsahu vyměnitelných zařízení a datových nosičů, řízení oprávnění ke spouštění kódu a detekci na základě chování uživatelů technického aktiva a aplikací.	Soulad s legislativou	VKB §21 - Ochrana před škodlivým kódem

K32	Nefunkční	Bezpečnostní požadavky	Aktualizace rozsahu určených technických aktiv	Na základě hodnocení důležitosti aktiv aktualizuje rozsah aktiv, u kterých je zaznamenávání bezpečnostních a provozních událostí prováděno.	Soulad s legislativou	VKB §22 - Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
K33	Nefunkční	Bezpečnostní požadavky	Zajištění jednoznačné síťové identifikace	U každého záznamu události musí být jednoznačně identifikován uživatel a zařízení, na kterém událost vznikla.	Soulad s legislativou	VKB §22 - Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
K34	Nefunkční	Bezpečnostní požadavky	Uchovávání záznamů událostí	Uchovávání záznamů událostí nejméně po dobu 18 měsíců	Soulad s legislativou	VKB §22 - Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
K35	Nefunkční	Bezpečnostní požadavky	Používání nástroje pro nepřetržité vyhodnocování detekovaných KBU a KBI	Tento nástroj musí: a) sbírat, vyhledávat a seskupovat související záznamy za účelem detekce KBU, b) dále musí varovat a podávat nepřetržité informace o detekovaných KBU, c) vyhodnocovat KBU s cílem identifikovat KBI, d) omezit případy nesprávného či nežádoucího vyhodnocení KBU, e) pravidelně aktualizovat nastavení včetně pravidel pro detekci a vyhodnocování KBU a pro poskytování informací o detekovaných KBU. f) využívání informací získaných nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí pro optimální nastavení bezpečnostních opatření informačního a komunikačního systému.	Soulad s legislativou	VKB §23 - Detekce kybernetických bezpečnostních událostí; § 24 - Sběr a vyhodnocování kybernetických bezpečnostních událostí
K36	Nefunkční	Bezpečnostní požadavky	Ochrana technických aktiv	Zajištění bezodkladných bezpečnostních aktualizací vydaných dodavatelem podporovaných technických aktiv nebo pokud není dané aktivum již podporováno, tak jsou zavedena opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti těchto aktiv.	Soulad s legislativou	VKB §25 - Aplikační bezpečnost
K37	Nefunkční	Bezpečnostní požadavky	Provádění pravidelného skenování zranitelností	Toto skenování je prováděno alespoň jednou ročně z interní a externí KS.	Soulad s legislativou	VKB §25 - Aplikační bezpečnost
K38	Nefunkční	Bezpečnostní požadavky	Penetrační testování technických aktiv	S ohledem na hodnocení technických aktiv a hodnocení rizik je prováděno penetrační testování z interní a externí KS. Dále před jejich uvedením do provozu a v souvislosti s významnou změnou.	Soulad s legislativou	VKB §25 - Aplikační bezpečnost
K39	Nefunkční	Bezpečnostní požadavky	Opětovné testování zranitelností	Provádění opětovného otestování nálezu zajištěného na základě skenování zranitelností nebo penetračním testováním za účelem ověření funkčnosti zavedených bezpečnostních opatření.	Soulad s legislativou	VKB §25 - Aplikační bezpečnost
K40	Nefunkční	Bezpečnostní požadavky	Certifikáty a kryptografické klíče	Budou použity pouze odolné kryptografické klíče a certifikáty. Bude využíván systém správy klíčů a certifikátů, který zajistí generování, distribuci, ukládání, změny, omezení platnosti a zneplatnění certifikátů a řádnou likvidaci kryptografických klíčů. Dále umožní kontrolu a audit a zároveň zajistí důvěrnosti a integritu kryptografických klíčů.	Soulad s legislativou	VKB §26 - Kryptografické prostředky
K41	Nefunkční	Bezpečnostní požadavky	Zajištění dostupnosti	Vytváření pravidelných záloh nastavení tech. aktiv, informací a dat nezbytných pro obnovení služby. Tyto zálohy musí být chráněny před narušením integrity a důvěrnosti a dostupnosti. dále budou pravidelně testovány na jejich integritu, dostupnost a obnovitelnost a výsledky testů jsou dokumentovány. Dostupnost služeb je stanovena dle řízení kontinuity činností a služba musí být odolná proti hrozbám a zranitelnostem, které ohrožují její dostupnost. U aktiv nezbytných pro zajištění dostupnosti služby musí být zajištěna redundance. Za účelem omezení šíření KBI a snížení jeho dopadu je zálohovací prostředí odděleno od jiných prostředí.	Soulad s legislativou	VKB §27- Zajišťování úrovně dostupnosti informací
K42	Nefunkční	Bezpečnostní požadavky	Zajištění kybernetické bezpečnosti specifických technických aktiv	Pro toto zajištění se omezí fyzický přístup a zároveň jsou omezena i oprávnění k přístupu k těmto aktivům. Dále je zajištěna segmentace sítí těchto aktiv od jiných prostředí. Dále jsou tato aktiva chráněna před využitím známých hrozeb a zranitelností a je zajištěna obnova dostupnosti.	Soulad s legislativou	VKB §28 - Průmyslové, řídicí a obdobné specifické systém
K43	Nefunkční	Bezpečnostní požadavky	Bezpečný vývoj aplikací	Při vývoji nového vízového systému budou respektována pravidla bezpečného vývoje aplikací (např. OWASP), pomocí kterých se ošetří běžná bezpečnostní rizika, jako je vsunutí škodlivého kódu, prolomení autentizace, zpřístupnění citlivých dat, nedostatečná kontrola přístupu a XSS skriptování, známé zranitelnosti či nedostatečné logování.	Soulad s legislativou	VKB §25 - Aplikační bezpečnost

ID principu	Typ požadavku	Kategorie	Název požadavku	Popis požadavku	Účel požadavku	Zdroj požadavku
P1	Nefunkční	Požadavky OHA	Standardně digitalizované	Orgány veřejné správy mají poskytovat služby primárně digitálně a samoobslužně, zároveň musí udržovat otevřené i další kanály pro ty, kteří nemohou buď z vlastního rozhodnutí, lidských nebo technických důvodů využívat digitální služby.	Soulad s legislativou	OHA
P2	Nefunkční	Požadavky OHA	Pouze jednou	Orgány veřejné správy musí zaručit, že občané a podniky poskytují stejné informace celé veřejné správě pouze jednou. Orgány veřejné správy využívají při výkonu působnosti tyto sdílené údaje opakovaně, přičemž musí dodržovat pravidla ochrany údajů.	Soulad s legislativou	OHA
P3	Nefunkční	Požadavky OHA	Podpora začlenění a přístupnost	Orgány veřejné správy musí digitální veřejné služby koncipovat tak, aby standardně podporovaly začlenění a vyhovovaly z pohledu funkcí, UX/UI designu a způsobem ovládání specifickým potřebám nejrůznějších skupin klientů z pohledu jejich věku, schopností nebo lidem s různými formami zdravotního postižení.	Soulad s legislativou	OHA
P4	Nefunkční	Požadavky OHA	Otevřenost a transparentnost	Orgány veřejné správy mezi sebou mají sdílet informace a data a musí občanům a podnikům umožnit přístup ke kontrole vlastních údajů a možné opravě. Musí uživatelům umožnit sledování správních procesů, které se jich týkají a musí do koncipování a poskytování služeb zapojit zúčastněné strany jak z komerční, akademické i občanské sféry a spolupracovat s nimi.	Soulad s legislativou	OHA
P5	Nefunkční	Požadavky OHA	Přeshraniční přístup jako standard	Orgány veřejné správy mají relevantní digitální služby zpřístupnit napříč hranicemi a mají zabránit dalšímu růstu jejich fragmentace, a tím usnadnit mobilitu na jednotném trhu.	Soulad s legislativou	OHA
P6	Nefunkční	Požadavky OHA	Interoperabilita jako standard	Veřejné služby mají být koncipovány tak, aby hladce fungovaly v rámci celého jednotného trhu a napříč různými organizačními jednotkami, a opíraly se o volný pohyb údajů a digitálních služeb v Evropské unii. Současně je nezbytné zajistit interoperabilitu veřejných služeb uvnitř veřejné správy ČR jako předpoklad odstranění místní příslušnosti a snížení omezujícího vlivu věcné příslušnosti služeb VS na jejich klienty.	Soulad s legislativou	OHA
P7	Nefunkční	Požadavky OHA	Důvěryhodnost a bezpečnost	Všechny iniciativy mají přesahovat pouhé dodržování právního rámce pro ochranu osobních údajů, soukromí a bezpečnost informačních technologií a mají tyto prvky zahrnout již do fáze přípravy architektury výkonu služeb veřejné správy.	Soulad s legislativou	OHA
P8	Nefunkční	Požadavky OHA	Jeden stát	Všechny iniciativy a veřejné služby mají být postaveny na společném přístupu ministerstev a dalších OVM k vytvoření a poskytování služeb veřejné správy a postupném odbourávání nežádoucího resortismu a tvorby duplicit. Zásadou je sdílení služeb, nezbytné infrastruktury a standardů pro realizaci jednotlivých služeb na všech úrovních veřejné správy i mezi nimi. Přestože je zodpovědnost za jednotlivé služby rozdělená, výsledek musí být z pohledu klienta jednotný.	Soulad s legislativou	OHA
P9	Nefunkční	Požadavky OHA	Sdílené služby veřejné správy	Budování a využívání sdílených služeb ve veřejné správě je jednou ze základních priorit eGovernmentu. Pokud bude výsledkem nové či upravované legislativy služba veřejné správy, má být koncipována jako služba sdílená nebo s využitím existujících sdílených služeb.	Soulad s legislativou	OHA
P10	Nefunkční	Požadavky OHA	Připravenost na změny	Procesy poskytování služeb veřejné správy i IT řešení jejich podpory musí být navrhovány tak, aby umožňovaly efektivně implementovat rozhodnutí reagující pružně na změnu zákonných parametrů služeb, změnu technologie, změnu dodavatele a další přicházející změny a potřeby.	Soulad s legislativou	OHA
P11	Nefunkční	Požadavky OHA	eGovernment jako platforma	Digitalizované procesy, požadavky a služby veřejné správy, stejně jako technické prostředky pro jejich naplnění, musí být navrženy tak, aby umožnily klientům veřejné správy, především velkým organizacím, integrovat tyto služby do svých ICT řešení tak, aby pro ně bylo co nejsnazší dostát svým povinnostem vůči veřejné správě a dosáhnout svých práv.	Soulad s legislativou	OHA
P12	Nefunkční	Požadavky OHA	Vnitřně pouze digitální	Veškerá komunikace uvnitř úřadů i mezi úřady navzájem musí být pouze digitální. Od přijetí podání až do vypravení a doručení rozhodnutí nebo jiného výstupu, musí být všechny interní provozní procesy veřejné správy plně elektronické, bezpapírové – pokud není jejich zavedení v této podobě nehospodárné (3E).	Soulad s legislativou	OHA
P13	Nefunkční	Požadavky OHA	Otevřená data jako standard	Veřejné údaje evidované orgány veřejné správy ve spravovaných ISVS musí být zveřejňovány jako otevřená data. Pro neveřejné údaje musí být jako otevřená data zveřejňována jejich anonymizovaná podoba, souhrn nebo statistika, nebo obdobná forma, pokud může mít význam pro uživatele těchto dat. V případě, že orgány veřejné správy sdílejí veřejné údaje, včetně anonymizované podoby neveřejných údajů, souhrnů nebo statistik, musí je sdílet jako otevřená data.	Soulad s legislativou	OHA
P14	Nefunkční	Požadavky OHA	Technologická neutralita	Digitální služby veřejné správy musí být technologicky nezávislé a neutrální. Musí být garantováno, že přístup k veřejným službám není závislý na konkrétní (předem určené) platformě či technologii. Což neznamená, že musí být podporovány všechny existující a okrajové technologie.,	Soulad s legislativou	OHA
P15	Nefunkční	Požadavky OHA	Uživatelská přívětivost	Musí být kladen důraz na uživatelskou přívětivost zaváděných digitálních služeb veřejné správy pro různé skupiny uživatelů. Služby musí být na prvním místě srozumitelné, uzpůsobené rozdílným požadavkům různých cílových skupin uživatelů v populaci. Služby mají být z hlediska uživatelského rozhraní otevřené, nesmí se omezovat na proprietární rozhraní nebo jediný standard a předjímat jediný způsob využití.	Soulad s legislativou	OHA
P16	Nefunkční	Požadavky OHA	Konsolidace a propojování	Je nutno budovat ISVS efektivně a snažit se využívat v maximální míře již vytvořené a sdílené procesně a funkčně ucelené komponenty pro řešení obdobných požadavků napříč agendami a úřady. Stejně nezbytné je zajistit propojování ISVS a jejich údajů v případech, pokud jsou potřebné pro výkon agend.	Soulad s legislativou	OHA
P17	Nefunkční	Požadavky OHA	Omezení budování monolitických systémů	Soutěženy musí být menší vzájemně provázané celky, aby se možnost dodávat státu otevřela i pro menší spolehlivé dodavatele. Cílem je soutěžit nejlepší řešení v dané oblasti, ne největší řešení na trhu.	Soulad s legislativou	OHA
P18	Nefunkční	Požadavky OHA	Datová suverenita a nezávislost	Každý úřad má neustálý a plný přístup a kontrolu vůči všem datům informačních systémů ve své správě.	Soulad s legislativou	OHA
P19	Nefunkční	Požadavky OHA	Otevřená řešení	Digitální služby a komponenty informačních systémů, realizované na míru objednatele, včetně nadstaveb a rozšíření balíkového SW, musí být vytvořeny v podobě a s licencí umožňující jejich sdílení a uveřejněny ve státním úložišti otevřeného zdrojového kódu a to nejpozději v den uvolnění první verze služby do produktivního provozu.	Soulad s legislativou	OHA
P20	Nefunkční	Požadavky OHA	Metriky digitálních služeb	Každý nový nebo podstatně změněný proces veřejné správy a každý nový nebo podstatně změněný informační systém na jeho podporu musí být navržen tak, aby umožňoval měřit využívání, výkon a efektivitu všech agend a služeb VS.	Soulad s legislativou	OHA

P21	Nefunkční	Požadavky OHA	Udržitelnost digitálních služeb a zařízení	Každé nové nebo podstatně změněné řešení pro digitální služby bude využívat udržitelných digitálních technologií, které mají minimální negativní dopad na životní prostředí a na společnost; budeme i ve VS podporovat standardy a označení udržitelnosti pro digitální produkty a služby.	Soulad s legislativou	OHA
P22	Nefunkční	Požadavky OHA	Svoboda volby	Každý by měl mít možnost využívat u služeb VS výhod algoritmických systémů a systémů umělé inteligence, a to i tím, že bude činit vlastní informovaná rozhodnutí v digitálním prostředí, přičemž bude chráněn před riziky a újmou, pokud jde o jeho zdraví, bezpečí a základní práva.	Soulad s legislativou	OHA

ID principu	Typ požadavku	Kategorie	Název požadavku	Popis požadavku	Účel požadavku	Zdroj požadavku
G01	Funkční	Požadavky GDPR	Informování subjektů údajů o incidentech v ochraně OÚ	Subjekt údajů má právo získat osobní údaje, které se ho týkají a které poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, je-li to technicky možné, a může požadovat, aby MU tam, kde tomu nebrání zákonná překážka, předala osobní údaje předem určenému správci	Soulad s legislativou	GDPR
G02	Funkční	Požadavky GDPR	Údržba záznamů o předávání OÚ	Zásady zpracování osobních údajů Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně, zákonným a transparentním způsobem . Osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely, a k jinému účelu jen, dal-li k tomu subjekt údajů souhlas .	Soulad s legislativou	GDPR
G03	Funkční	Požadavky GDPR	Údržba dokumentace k informování subjektů údajů o zpracování OÚ	Pokud bude zpracování probíhat na základě souhlasu, musí jej získat ještě předtím, než začne s daty pracovat.	Soulad s legislativou	GDPR
G03	Funkční	Požadavky GDPR	Plnění práv subjektů OÚ na žádost	•právo na informace o zpracování osobních údajů (OÚ) •právo na přístup subjektu k OÚ •právo na opravu •právo na výmaz („právo být zapomenut") •právo na omezení zpracování •právo na přenositelnost údajů •právo vznést námitku •právo nebýt předmětem automatizovaného rozhodnutí.	Soulad s legislativou	GDPR
			Pozn., ostatní povinnosti nařízení? např logování, Agendové systémy pro zajištění práv subjektu údajů			

ID principu	Typ požadavku	Kategorie	Název požadavku	Popis požadavku	Účel požadavku	Zdroj požadavku
I01	Funkční	Interní pravidla MZČR	Shoda s technologickým standardem MZČR	Nově budované či implementované informační systémy či aplikace jsou provozovatelné v souladu s technologickým standardem MZČR	Soulad s interními standardy a nařízeními	Interní standard MZČR

ID principu	Typ požadavku	Kategorie	Název požadavku	Popis požadavku	Účel požadavku	Zdroj požadavku
M01	Nefunkční	Požadavky SEZ	Přínos pro pacienta	Primárním cílem rozvoje elektronického zdravotnictví musí být přínos pro pacienty a kvalitu zdravotní péče.	Naplnění NSEZ	Národní strategie elektronického zdravotnictví
M02	Nefunkční	Požadavky SEZ	Právo pacienta	Právo pacienta na zajištění odpovídající péče, ochranu osobní důstojnosti a ochranu osobních údajů nesmí být zaváděním prostředků elektronického zdravotnictví oslabeno, ale naopak posilováno.	Naplnění NSEZ	Národní strategie elektronického zdravotnictví
M03	Nefunkční	Požadavky SEZ	Zapojení odborných zdravotnických pracovníků	Lékaři a další odborní pracovníci ve zdravotnictví musí být zapojováni do projektů již ve fázi přípravy záměrů, při plánování a tvorbě návrhů řešení. Názory odborné veřejnosti musí být v rámci projektů aktivně získávány a přiměřeně zohledňovány.	Naplnění NSEZ	Národní strategie elektronického zdravotnictví
M04	Nefunkční	Požadavky SEZ	Kvalita služeb EZ	Před zavedením nových nástrojů a služeb elektronického zdravotnictví do praxe musí být vždy dostatečným způsobem ověřena a vyhodnocena jejich použitelnost, kvalita, stabilita a výkonnost.	Naplnění NSEZ	Národní strategie elektronického zdravotnictví
M05	Nefunkční	Požadavky SEZ	Motivace zavádění SEZ	Zavádění elektronického zdravotnictví na základě plošně stanovené povinnosti je principiálně nesprávné. Při zavádění nových služeb a nástrojů elektronického zdravotnictví je třeba využívat především pozitivní motivace a zavádět nové technologie postupně a uvážlivě tak, aby nedošlo k ohrožení plynulosti a bezpečnosti provozu, ohrožení pacienta nebo zhoršení podmínek práce zdravotníků.	Naplnění NSEZ	Národní strategie elektronického zdravotnictví
M06	Nefunkční	Požadavky SEZ	Dodržování ověřených standardů a technologií	Všude, kde je to možné a účelné, je třeba při tvorbě nových řešení využívat veškeré dostupné vědecko-výzkumné poznatky a ověřené technologie, včetně standardů pro výměnu a zobrazování zdravotnických informací.	Naplnění NSEZ	Národní strategie elektronického zdravotnictví
M07	Nefunkční	Požadavky SEZ		Princip validity informací pro potřeby plánování dostupnosti a hodnocení kvality péče	Naplnění NSEZ	Národní strategie elektronického zdravotnictví
M08	Nefunkční	Požadavky SEZ		Princip použitelnosti nástrojů – jednoduché navigačně nativní uživatelské prostředí	Naplnění NSEZ	Národní strategie elektronického zdravotnictví
M09	Nefunkční	Požadavky SEZ		Princip integrace nových funkcí do používaných klinických informačních systémů	Naplnění NSEZ	Národní strategie elektronického zdravotnictví
M10	Nefunkční	Požadavky SEZ		Princip důvěryhodnosti – zdravotníci musí být v konečném důsledku ujištěni a přesvědčeni, že sdílené informace jsou bezpečně přenášeny a ukládány a nedochází k jejich zneužívání	Naplnění NSEZ	Národní strategie elektronického zdravotnictví

ID principu	Typ požadavku	Kategorie	Název požadavku	Popis požadavku	Ucel pozadavku	Zdroj požadavku
E01	Funkční	Požadavky SEZ	Služby vytvářející důvěru	Oprávněnou osobou může být pouze poskytovatel zdravotních služeb nebo poskytovatel sociálních služeb.	Soulad s legislativou	Zákon č. 325/2021 Sb.
E02	Funkční	Požadavky SEZ	Autentizace uživatele	Autentizace uživatele k veřejným službám probíhá pomocí Národní identity občana (NIA) nebo bankovní identity (SoNIA)	Soulad s eGovernment ČR	Služby eGovernmentu ČR
E03	Funkční	Požadavky SEZ	Autentizace uživatele	Zajištění jednotného přístupu ke službám elektronického zdravotnictví v souladu s principy eGovernmentu	Soulad s eGovernment ČR	Služby eGovernmentu ČR

ID principu	Typ požadavku	Kategorie	Název požadavku	Popis požadavku	Účel požadavku	Zdroj požadavku
S01						

Ministerstvo zdravotnictví České republiky
Palackého nám. č 4, 128 01 Praha 2, IČ: 00024341

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Verze: v0/01
Platnost nové verze od: 27.02.2024
Spisový znak: XX.X.X
Skartační znak a lhůta: X/X

ZPRACOVÁNÍ METODIK TVORBY NÁSTROJŮ PRO IMPLEMENTACI NÁRODNÍ STRATEGIE EZ

Metodika tvorby, správy a užití Enterprise Architektury v resortu Ministerstva zdravotnictví ČR

Pořadí revize	Provedené dne	Zpracoval	Schválil
0.			
1.			
2.			

Obsah

Seznam zkratek a pojmů

Zkratka	Význam
ABB	Architektonický stavební prvek (Architecture building Block)
ADM	Architecture Development Method
ArchiMate	Modelovací jazyk pro popis podnikové architektury
COBIT	Control Objectives for Information and Related Technology, rámec pro řízení IT
ČR	Česká republika
EA	Podniková architektura
FPR	Katalog funkcí, procesů a obslužných rozhraní veřejné správy
ID	identifikátor
ITIL	Information Technology Infrastructure Library, rámec pro řízení IT služeb
JAR	Katalog organizačních jednotek, aktérů a rolí
KAK	Katalog aplikačních komponent a klíčových aplikačních funkcí
KAP	Katalog architektonických principů
KBP	Katalog balíčků práce
KDE	Katalog základních datových entit
KGP	Katalog GAP
KIK	katalog infrastrukturních komunikačních komponent, funkcí a klíčových služeb
KPL	Katalog Plateau – ustálené stavy architektury, které zachycují stav každé etapy rozvoje architektury v organizaci
KRB	Katalog prvků vertikální domény rizik a bezpečnosti
KSP	Katalog prvků vertikální domény shody s pravidly
KSS	Katalog prvků vertikální domény strategie a směřování
KTK	Katalog technologických komponent a klíčových funkcí nebo služeb
KVK	Katalog prvků vertikální domény výkonnosti a kvality
KZS	Katalog zainteresovaných stran (stakeholders)
KS	Katalog služeb
MV ČR	Ministerstvo vnitra České republiky
MZ ČR	Ministerstvo zdravotnictví České republiky
NA	Národní architektura
NAP	Národní architektonický plán

Zkratka	Význam
NAR	Národní architektonický rámec
OLA	Operational-level agreement
RACI	Matice zodpovědností (Responsibility assignment matrix)
SBB	Stavební prvek řešení (Solution Building Block)
SLA	Service-level agreement
TOGAF	The Open Group Architecture Framework, mezinárodní architektonický rámec
ÚZIS	Ústav zdravotnických informací a statistiky ČR
VS	Veřejná správa

Pojem	Výklad
Doména architektury	Zájmová oblast architektury. TOGAF rozlišuje domény architektury: byznys, data, aplikace a technologie. Další rámce přidávají další domény pro oblasti motivace ke změně.
Hledisko a Pohled	Definuje perspektivu, ze které je možné vidět pohled. Pohled na model systému organizace je konkrétní artefakt (katalog, matice a zejména diagram). Hledisko říká, jak má diagram vypadat a co má prezentovat uživateli.
Metamodel	Model definující, jakým způsobem bude architektura popsána, ze kterých typových prvků a jejich vazeb bude popis architektury sestaven a podle jakých pravidel.
Metodika	Definovaná a opakovatelná sada kroků pro vyřešení daného úkolu. Zaměřuje se na proces samotný, ale může obsahovat i definici požadovaného obsahu.
Model	Model představuje účelově zjednodušenou reprezentaci předmětu zájmu a je nástrojem pro porozumění. Účelem modelu je potom prezentovat ty aspekty organizace, které jsou podstatné z pohledu zainteresovaných subjektů.
Modelování	Modelování je proces, při kterém se vytváří model předmětu, vždy s ohledem na zamýšlené použití modelu.
Zainteresovaný	Jednotlivec, tým nebo organizace, která má zájem na přínosu architektury.

Seznam obrázků

1 ÚVOD

1.1 Účel dokumentu

Tento dokument obsahuje popis metodiky pro tvorbu a správu modelů architektury resortu Ministerstva zdravotnictví ČR.
Účelem tohoto dokumentu je poskytnout návod, jak modelovat architekturu resortu/úřadu, aby se všechny jednotlivě vzniklé modely vzájemně doplňovaly a zapadly do Národní architektury VS ČR.
Účelem metodiky v širším slova smyslu je být východiskem pro modelování architektur úřadu pro jakékoli použití při plánování a rozvoji služeb a jejich informační podpory.

1.2 Definice architektury

Ve standardu TOGAF má “architektura” dva doplňující se významy podle kontextu:
Formální popis systému nebo plánu systému na úrovni jeho komponent jako vodítko pro jeho implementaci.
Struktura komponent, jejich vzájemných vazeb a principů a návodů řídících jejich návrh a vývoj v čase.
Definice pro potřeby české veřejné správy:
Enterprise Architecture (architektura úřadu), jako manažerská metoda, je prostředkem pokorného a celostního poznávání organizace na podporu rozhodování, zejména při plánování strategických změn.

Jednoduše řečeno:
Architektura úřadu představuje popis struktury a chování úřadu (kdo jsme), plánovaných změn (odkud a kam jdeme) a jejich informační podpory (k čemu nám je a má být ICT).
Architektonický rámec obsahuje rady pro:

- Popis architektury: jak zachytit jednotlivé obrazy architektury podle potřeb zájmových skupin.
- Metodu tvorby architektury: návrh cyklu tvorby architektury rozděleného do fází a organizovaného podle domén s rozdílnými výstupy.
- Organizaci architektonického týmu: jaká má být struktura týmu, jeho dovednosti, znalosti, způsob řízení a kontroly.

1.3 Vysvětlení klíčových pojmů

Pro orientaci v této koncepci jsou klíčové tři pojmy a jejich zkratky:

- **Národní architektura (NA, NAVSČR)** – je uplatnění metod a myšlení podnikové architektury na veřejnou správu státu, konkrétně ČR. Představuje dva významy současně, jak existující a

plánovanou skutečnou architekturu VS, tak její popis. Představuje také souhrn lokálních architektur OVM a centrálních architektur eGovernmentu.

- **Národní architektonický rámec (NAR)** – představuje myšlenkový koncept, metodiku postupu, sadu standardů, pomůcek a návodů pro tvorbu a údržbu NA a NAP.
- **Národní architektonický plán (NAP)** – je popisem plánovaného cílového stavu NA v určitém časovém horizontu a plánem cesty, tj. implementačních kroků (programů a projektů), vedoucích ze současného stavu k dosažení stavu cílového. NAP je také soubor architektonických dat (modelů) a diagramů, udržovaných společně OHA a jednotlivými OVM, členěný na: architektury úřadů a architektury sdílených řešení.

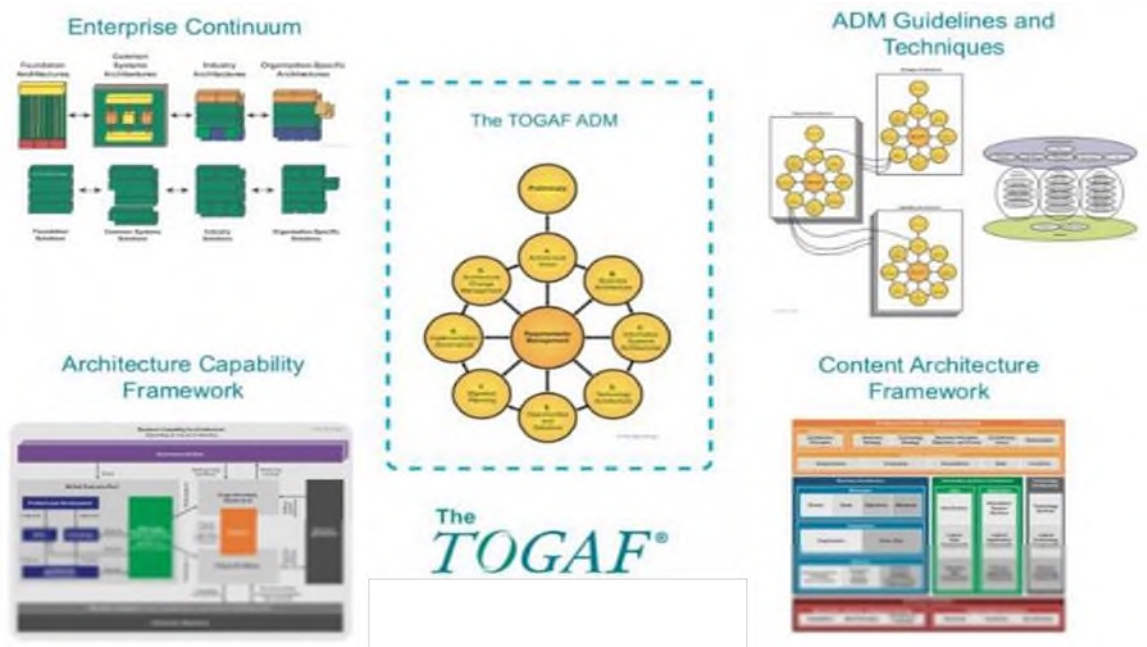
1.4 Východiska pro návrh metodiky

Navržená metodika čerpá z metodiky pro modelování architektur odboru Hlavního architekta eGovernmentu Ministerstva vnitra ČR a dalších, veřejně dostupných dokumentů, zveřejněných uvedeným odborem.

Stejně jako metodika odboru Hlavního architekta i tato metodika se opírá o dva základní pilíře používané v oblasti návrhu moderní ICT Architektury:

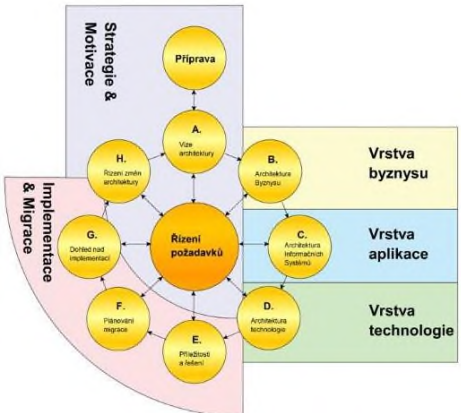
- TOGAF – je mezinárodně uznávaný rámec pro řízení tvorby Enterprise architektury ve společnostech využívajících prostředků informačních technologií. Původní koncept vznikl v USA, ale již více než deset let se používá po celém světě včetně České republiky. Oficiální dokumentace standardu TOGAF se nachází na adrese http://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html.
- ArchiMate® - je nezávislý grafický modelovací jazyk. O jeho správu se stará konsorcium Open Group, které ArchiMate® vyhlásilo jako standard pro popis Enterprise architektury. Obecné standardy pro modelování v jazyce ArchiMate jsou dostupné na adrese http://pubs.opengroup.org/architecture/archimate2-doc/.

Rozšíření jazyka ArchiMate® ve verzi 3.0.1 je v souladu s metodikou TOGAF. Tři hlavní vrstvy ArchiMate®, tj. procesní vrstva, aplikační vrstva a technologická vrstva odpovídají fázím TOGAF ADM cyklu – B. (procesní architektura), C. (architektura informačních systémů), D. (technologická architektura). Některé oblasti TOGAF ale nejsou v jazyce ArchiMate® obsaženy. Je to pochopitelné, protože TOGAF je rámec a má mnohem širší záběr než ArchiMate®, který je jazykem pro modelování architektury. Dále existuje Implementační a migrační oblast rozšíření ArchiMate®, která koresponduje s TOGAF ADM fázemi E. (příležitosti a řešení), F. (plánování migrace) a G. (zavedení řízení).

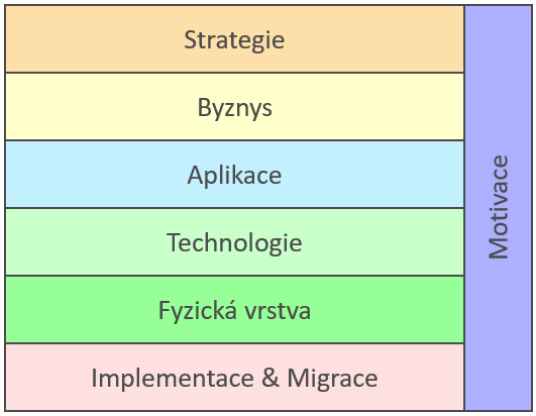


Obrázek 1 The TOGAF® Standard a jeho hlavní části (The Open Group, 2022)

Standard TOGAF 9.2 byl aktualizován s důrazem na byznys architekturu a restrukturalizován tak, aby plně podporoval knihovnu rámců TOGAF.



Obrázek 3 mapování domén ArchiMate® na TOGAF®



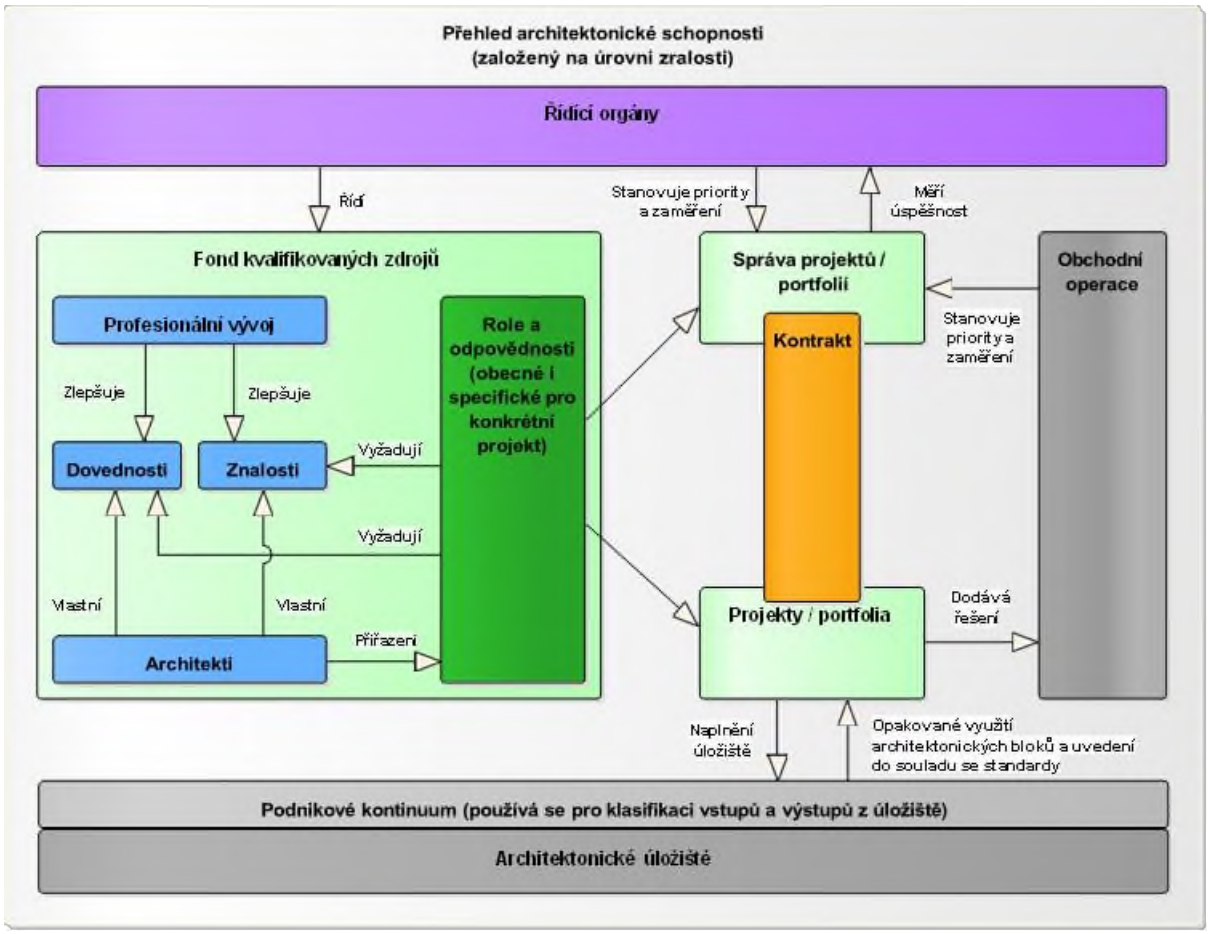
Obrázek 2 domény jazyka ArchiMate, verze 3.0.1, publikovaná v listopadu 2017

Standard ArchiMate® 3.0.1. byl doplněn o strategickou vrstvu, některé byznys elementy byly přesunuty do motivační domény, byly doplněny další elementy do aplikační a technologické vrstvě a přibyla nová fyzická vrstva.

Více informací o základních principech metodiky architektonického rámce TOGAF® a architektonického modelovacího jazyka ArchiMate lze nalézt v přílohách 10.1 Základy rámce TOGAF® a 10.2 Základy jazyka ArchiMate® tohoto dokumentu.

2 ORGANIZACE A ARCHITEKTONICKÉ SCHOPNOSTI

Pro zajištění architektonických funkcí v organizaci je nutné vytvořit příslušnou organizační strukturu, procesy, role, zodpovědnosti a znalosti. Architecture Capability Framework poskytuje referenční model a návod, jak takové organizační změny provést.



Obrázek 4 Zavedení architektonické schopnosti do organizace

2.1 Vybudování architektonické schopnosti

Vybudování architektonické schopnosti není jednorázový projekt, ale spíše průběžná činnost, která poskytuje kontext, prostředí a zdroje k řízení udržitelné architektonické praxe.

Vybudování architektonické schopnosti vyžaduje změny v architektuře organizace, ve které se má schopnost zavádět.

Organizace by měla mít k dispozici kvalifikovaný architektonický tým, který má schopnost a znalosti potřebné k plánování, navrhování a implementaci architektonických řešení.

Organizace by měla definovat efektivní architektonický proces, který zahrnuje stanovení směrnic, postupů a nástrojů pro správu a řízení architektury v organizaci.
Organizace by měla pravidelně sledovat a spravovat své architektonické aktivity, včetně hodnocení aktuálního stavu architektury, identifikace a analýzy potenciálních problémů a rizik a plánování budoucích architektonických iniciativ.
Je nutné zajištění podpory vedení organizace, aby architektonická schopnost měla podporu a angažovanost vedení organizace, které poskytuje potřebné zdroje pro realizaci architektonických iniciativ.
Na úrovni byznys architektury je především zapotřebí ustanovit útvar architektury, vydefinovat jeho role, zodpovědnosti a činnosti. Dále je pak potřeba zajistit procesy správy architektonického úložiště. Na úrovni datové architektury je potřeba stanovit strukturu architektonického úložiště a artefakty, které v něm budou uloženy.
Na úrovni aplikační architektury je potřeba zvolit architektonické úložiště a podpůrné nástroje pro řízení architektury.
Na úrovni technologické a infrastrukturní architektury je potřeba stanovit technologické komponenty a infrastrukturu pro podporu aplikací.

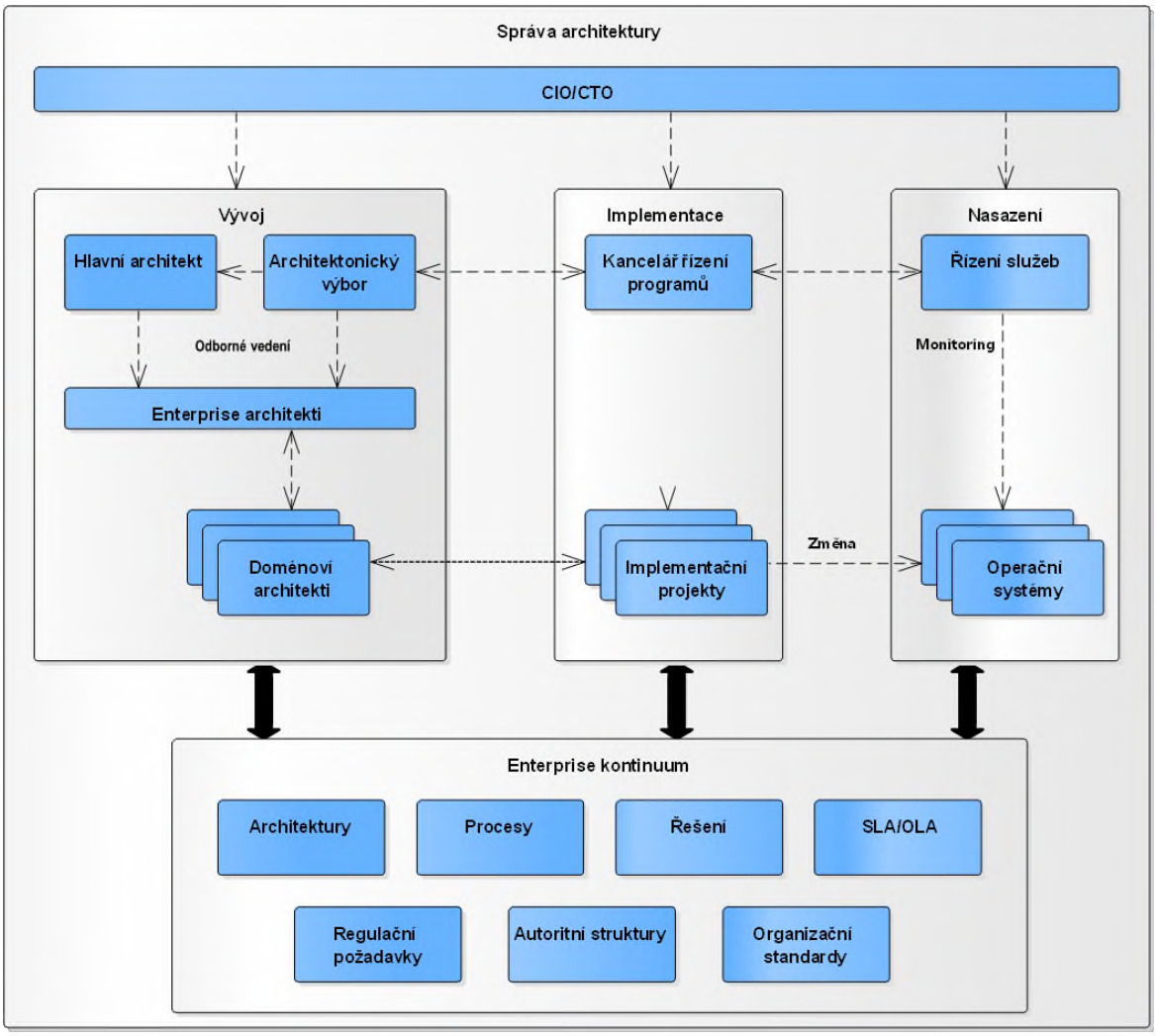
2.2 Útvar architektury MZ

Útvar architektury je orgán, jehož hlavní náplní je zastávat nejméně těchto pět rozdílných, ale vzájemně se doplňujících a podmiňujících funkcí:

1. Kontrolní orgán předběžně kontrolující vybrané vlastnosti v rámci resortu předkládaných IT projektů vůči zásadám NAP a vůči vyhlášeným standardům architektury řešení.
2. Auditní orgán stanovující požadovanou úroveň architektonické zralosti jednotlivých organizací resortu, jejich architektonického oddělení a jeho procesů a governance a orgán kontrolující dosažení této úrovně v požadovaném čase a její zachování.
3. Enterprise a Solution Architect architektur (byznys, aplikačních, datových i technologických) centrálních sdílených (nebo jednotných) služeb a centrálních sdílených (nebo standardizovaných) systémů Governmentu (eGovernmentu) na úrovni resortu.
4. Přirozený vzor a leader (metodik) tvorby Enterprise a Solution architektur v jednotlivých OVM v resortu, tj. tvůrce a vykladač přizpůsobené metodiky, správce resortních sdílených znalostí (vzory, návody, referenční modely a praktické příklady) a správce prostředků pro sdílení architektonických znalostí (architektonické úložiště, portál, wiki, diskusní fóra, …).
5. Lokální (interní) Enterprise Architekt úřadu a těch organizací resortu, které jej o to požádají a kde nepostačí předchozí role rádce.

2.2.1 Složení útvaru architektury

Útvar architektury se skládá z architektonického výboru a architektonického týmu (hlavní architekt, enterprise architekti a solution architekti).



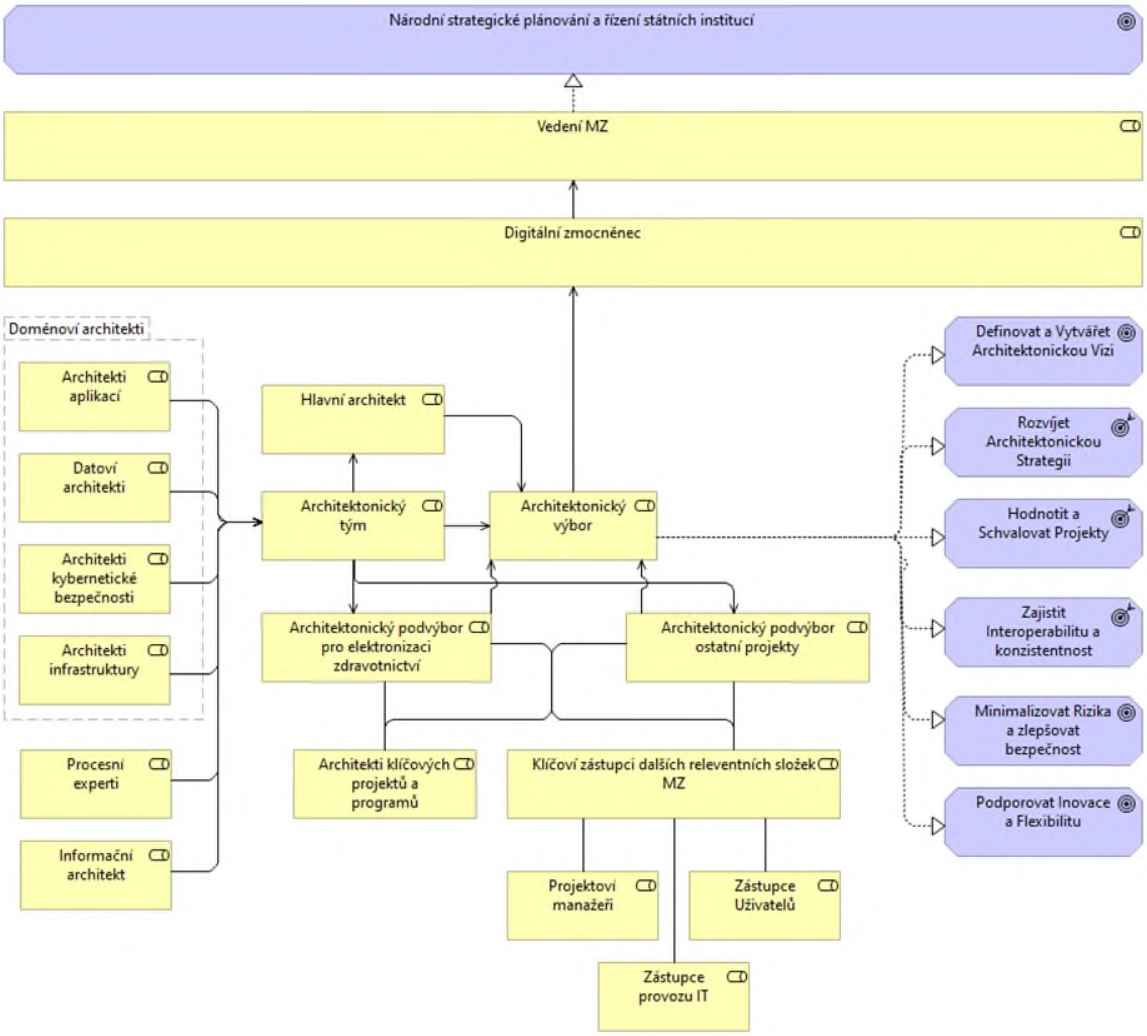
Obrázek 5 Architecture Governance Framework – organizační struktura

2.2.2 Architektonický výbor

Architektonický výbor zajišťuje, aby všechny informační systémy a technologické projekty v organizaci byly v souladu s definovanými architektonickými principy a standardy. To pomáhá zajistit konzistenci a integritu celkové informační architektury organizace. Architektonický výbor pomáhá formulovat a podporovat strategické cíle organizace prostřednictvím architektonických rozhodnutí a doporučení.

2.2.2.1 Struktura architektonického výboru

Architektonický výbor na Ministerstvu zdravotnictví ČR je tvořen různými klíčovými členy a podporován širokou škálou odborných rolí, které mají různé znalosti a zkušenosti.



Obrázek 6 Struktura a zapojení architektonického výboru

Cíle, struktura, odpovědnosti architektonického výboru a životní cyklus správy požadavků na architektonické změny jsou popsány v samostatném metodickém dokumentu Organizace a řízení podnikové architektury Ministerstva zdravotnictví ČR.

2.2.3 Zodpovědnosti útvaru architektury

Útvar architektury je typicky zodpovědný za dosažení následujících cílů:

- Poskytnutí principů a standardů pro všechna rozhodnutí týkající se architektury
- Zaručení aplikace nejlepších praktik na tvorbu architektury
- Zajištění konzistence mezi architekturami
- Určení znovupoužitelných komponent
- Zajištění flexibility architektury (aby vyhovovala byznys potřebám, aby vhodně využívala nové technologie)

- Vynucení souladu s architekturou
- Rozvoj architektonické zralosti v organizaci
- Poskytování architektonického poradenství
- Rozvoj a správu architektonického rámce

Z hlediska operativy je útvar architektury zodpovědný za:

- Monitoring a kontrolu dodržení architektonického kontraktu
- Zajištění efektivní a konzistentní správy a implementace architektur
- Řešení eskalovaných nejasností, problémů a konfliktů
- Poskytování doporučení
- Zaručení souladu s architekturami a udělování výjimek
- Zaručení řízeného přístupu ke všem relevantním informacím pro implementaci architektury
- Validace reportovaných SLA, úspor apod.
- Aktualizaci a správu architektonických dokumentů
- Komunikaci a spolupráci s týmy a stakeholdery
- Implementace architektonických směrnic
- Řešení architektonických problémů

Z hlediska řízení je útvar architektury zodpovědný za:

- Tvorbu použitelných řídících materiálů a provozování řídících aktivit
- Poskytnutí základního kontrolního mechanizmu pro zaručení efektivní implementace architektury
- Včasnou identifikaci odchylek (neshody) od architektury a naplánování aktivit pro nápravu
- Vybudování vazby mezi implementací architektury, architektonickou strategií a cíli obsaženými v enterprise architektuře a strategickými cíli resortu
- Řízení změn v architektuře ve spolupráci s architektonickým výborem a jeho podvýbory, který je popsán v samostatném metodickém dokumentu Organizace a řízení podnikové architektury Ministerstva zdravotnictví ČR

K prosazování architektonických rozhodnutí musí Ministerstvo zdravotnictví ČR vydat závaznou směrnice zodpovědnosti související s rozhodnutím AV.

2.2.4 Role a kapacity v útvaru architektury

Očekávané funkce útvaru architektury je potřebné naplnit kapacitami zaměstnanců (i zlomkovými) s odpovídajícími schopnostmi, kteří budou vstupovat do níže uvedených rolí. Přičemž jeden zaměstnanec může plnit více rolí a některé role mohou být trvale či dočasně zajištěny externě.

- Vedoucí (ředitel) útvaru architektury úřadu
- Hlavní architekt úřadu (Enterprise Architect)
- Metodik architektury úřadu (Enterprise Architect)
- Doménový architekt úřadu (Enterprise Architect)

- Byznys (procesní) architekt úřadu
- Aplikační architekt úřadu
- Datový architekt úřadu
- Technologický (IT) architekt úřadu
- Bezpečnostní (IT) architekt úřadu
- Hlavní architekt řešení projektů eGovernmentu a ostatních změnových projektů
- Doménový architekt řešení (Solution Architect)
- Byznys (procesní) architekt řešení
- Aplikační architekt řešení
- Datový architekt řešení
- Technologický (IT) architekt řešení
- Bezpečnostní (IT) architekt řešení
- Architekt významných řešení – napříč doménami (Solution Architect), například:
- Architekt pro všechny součásti související s eHealth
- Architekt všech řešení na platformě xyz
- Architekt průřezových IT služeb (DMS, Knowledge Management, Workflow apod.)
- Specialista legislativy a analýz architektury eGovernmentu ČR a EU
- Metodik architektonického vzdělávání, osobního rozvoje a sdílení arch. znalostí v resortu

2.3 Dodržování souladu výstupů s architekturou úřadu

Zajištění souladu individuálních výstupů projektů s architekturou úřadu je nezbytným aspektem řízení architektury. Za tímto účelem vykonává obvykle řízení IT následující činnosti:

- Zadání přípravy projektových architektur neboli projektově specifických pohledů, které ilustrují, jaký má Enterprise Architektura vliv na hlavní projekty v organizaci.
- Formální proces review, jehož cílem je posoudit soulad připravených projektových architektur s architekturou úřadu.
- Formální zpracování požadavků na Architektonický výbor a jeho podvýbory, které je popsáno v samostatném metodickém dokumentu Organizace a řízení podnikové architektury Ministerstva zdravotnictví ČR.

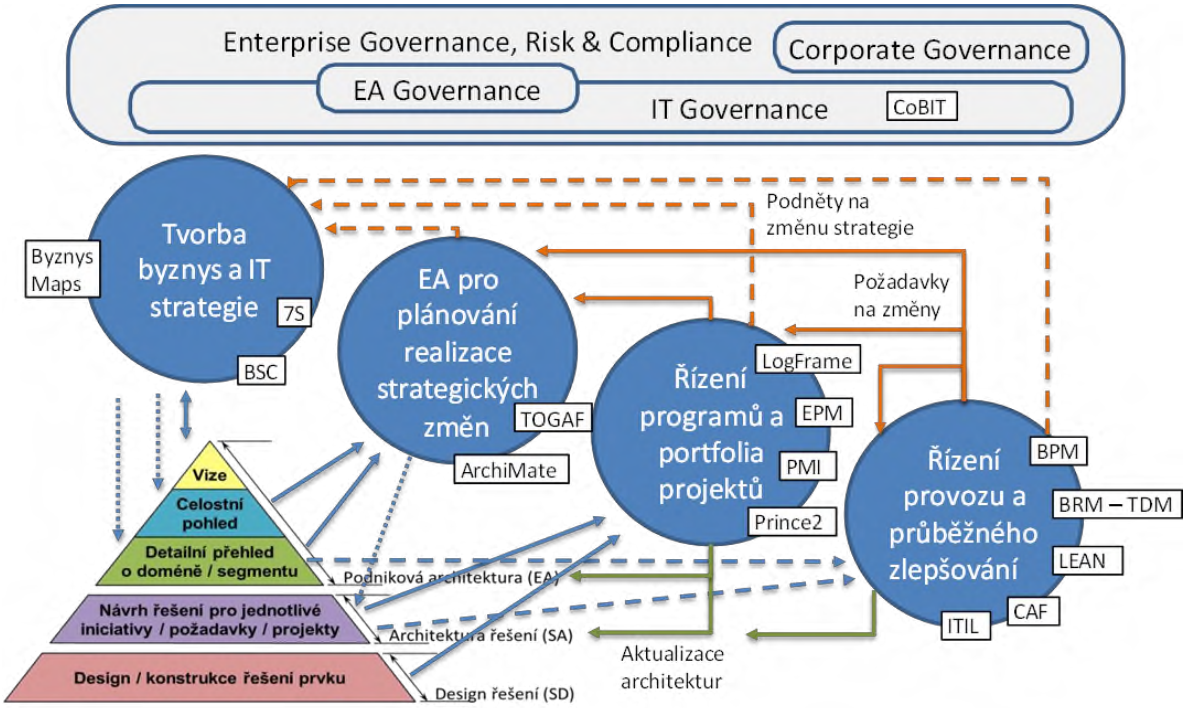
Být „v souladu“ znamená:

- Podporovat stanovenou strategii a budoucí směr
- Dodržovat stanovené standardy
- Poskytovat stanovené funkcionality
- Dodržovat stanovené principy, referenční modely a vzory
- Pro usnadnění vyhodnocení souladuarchitektury projektu s architekturou úřadu doporučujeme vytvořit kontrolní seznamy

- Respektovat architektonická rozhodnutí architektonického výboru a jeho podvýboru popsaných v samostatném metodickém dokumentu Organizace a řízení podnikové architektury Ministerstva zdravotnictví ČR
- Pravidelně hodnotit a aktualizovat architekturu

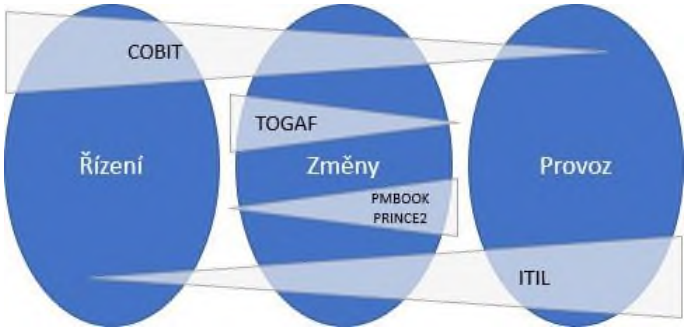
3 VZTAH ARCHITEKTONICKÉHO RÁMCE A OSTATNÍCH MANAŽERSKÝCH DISCIPLÍN

TOGAF je obecný, technologicky nezávislý rámec, který je určený pro užití v rozličných prostředích. Díky tomu je flexibilní a rozšiřitelný a může být použit sám o sobě, nebo může být doplněn jinými standardními rámci jako je například ITIL, COBIT a PRINCE2. Následující obrázek ilustruje, jak známé rámce zapadají do podnikových procesů.



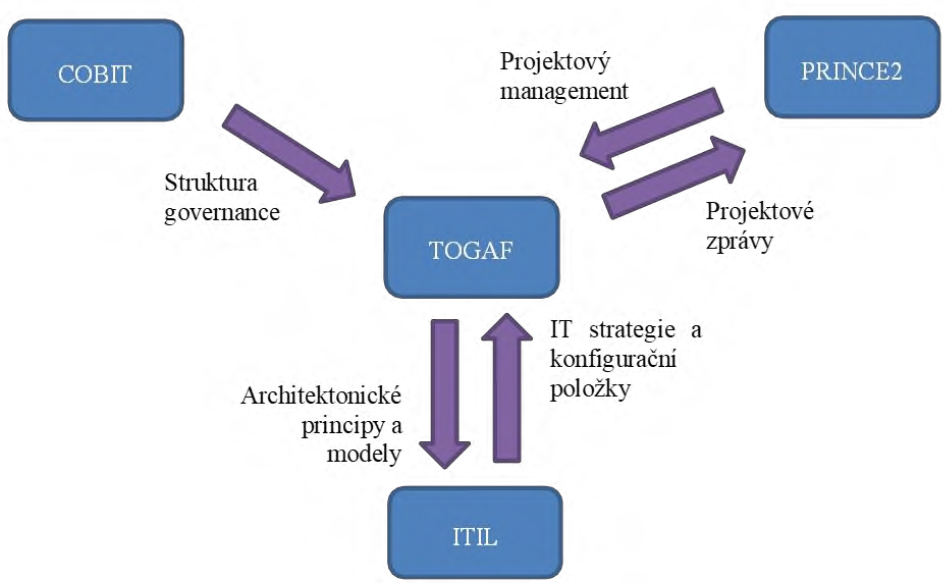
Obrázek 7 Architektonický rámec a ostatní manažerské disciplíny, zdroj: NA VSČR

V této kapitole je popsán vztah architektonického rámce TOGAF s rámci, které jsou nejčastěji doporučeny pro jeho doplnění. Jedná se o rámce COBIT, ITIL a PRINCE2.



Obrázek 8 Překryv užívaných podnikových, architektonických, projektových a provozních rámců, Zdroj: ITpreneurs.com

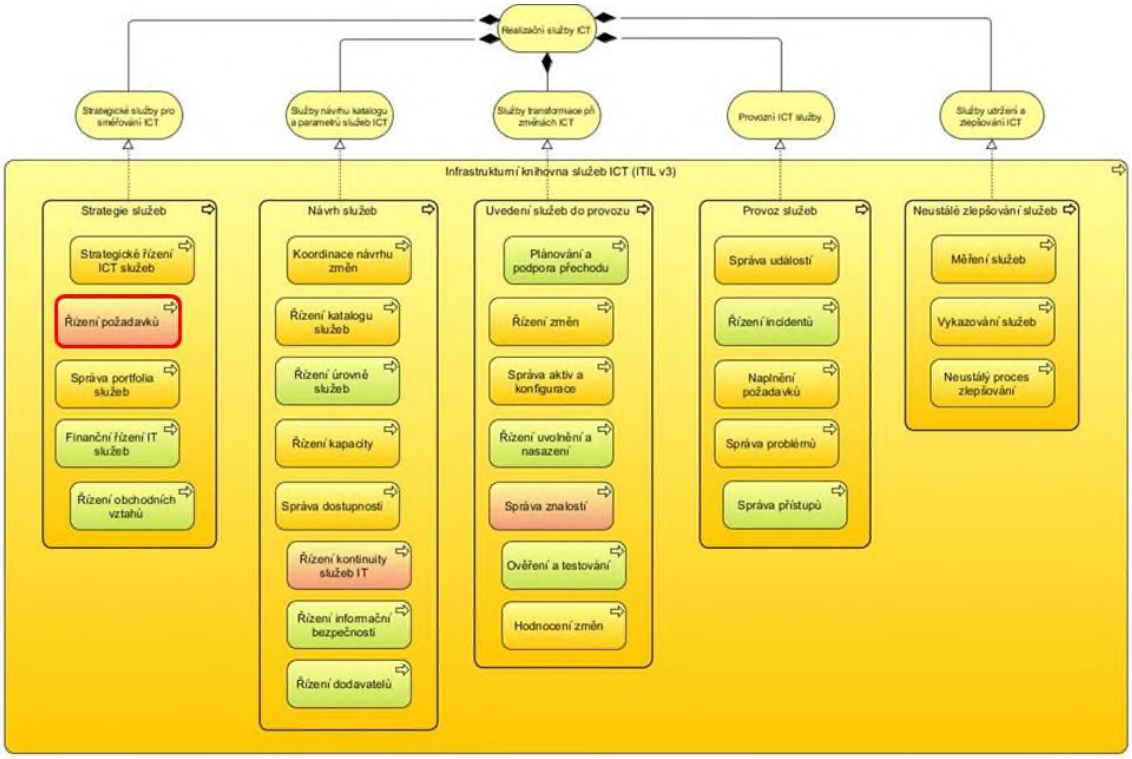
Hlavní interakce (výměna informací) mezi rámci je uveden na obrázku níže.



Obrázek 9 Hlavní interakce mezi rámci

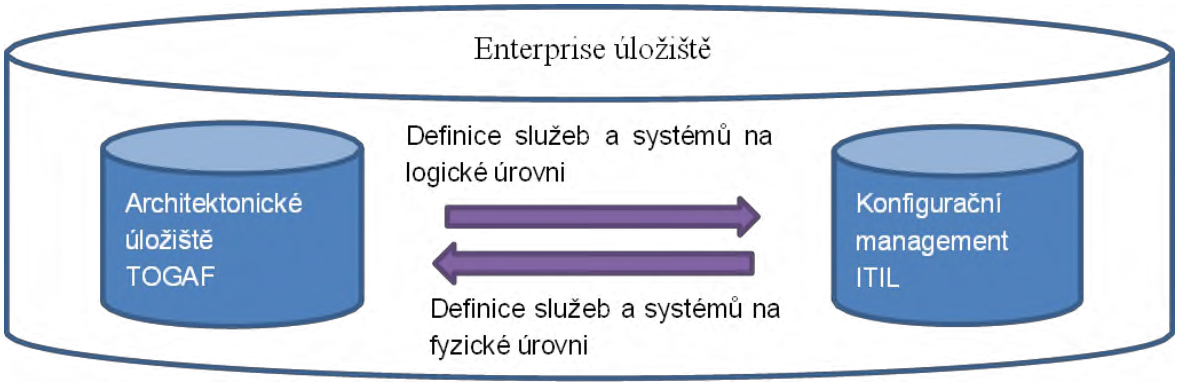
3.1 Vazba TOGAF na ITIL

Information Technology Infrastructure Library (ITIL, norma ČSN/ISO 20000) je rámec pro řízení IT služeb. Základní princip ITIL je postaven na řízení životního cyklu IT služby a řízení hodnoty, kterou informační technologie poskytují zákazníkům – tj. odběratelům IT služeb. ITIL obsahuje soubor praxí prověřených konceptů a postupů.



Obrázek 10 Pohled na metodický rámec ITIL v jazyce ArchiMate®

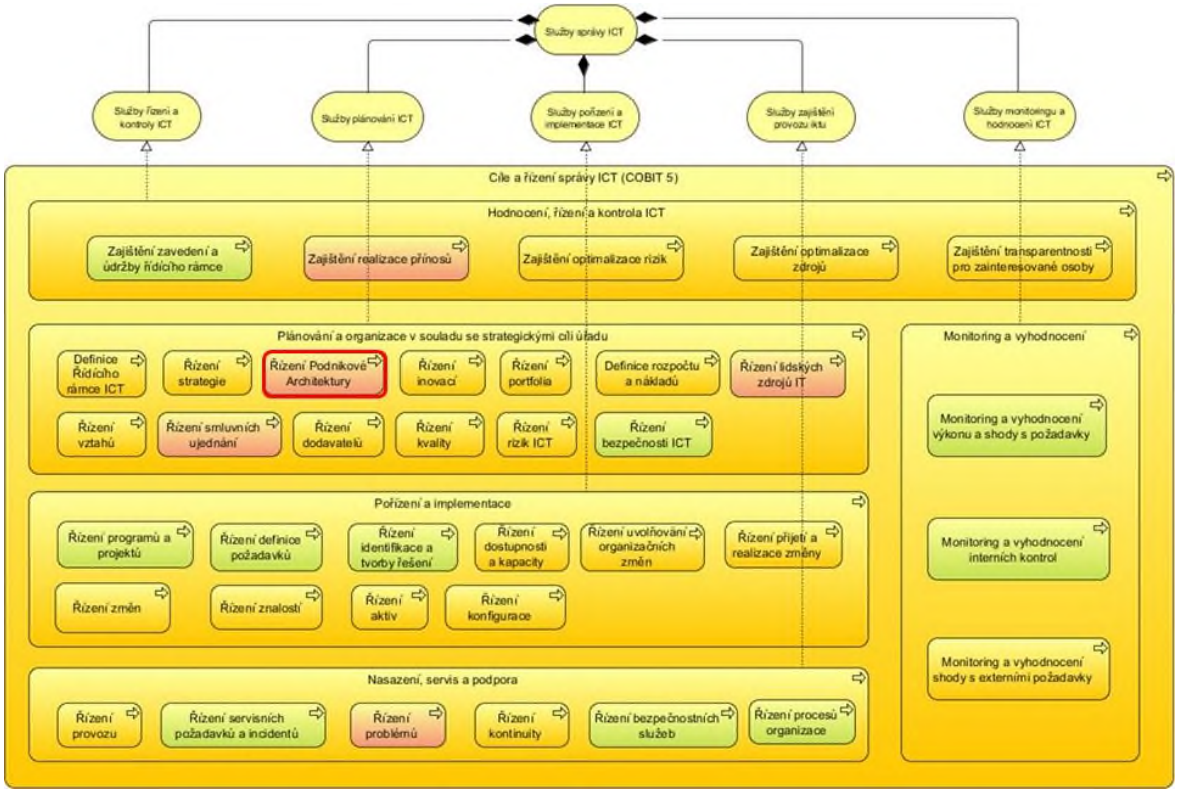
Úložiště pro podporu procesů vedených podle ITIL, včetně správy konfiguračních prvků souvisí s architektonickým úložištěm TOGAF (dominantně v oblasti Řízení požadavků) a měly by se vzájemně doplňovat. Architektura vytvořená pomocí rámce TOGAF poskytuje vstupy do procesů ITIL a využívá jejich výstupy.



Obrázek 11 Vztah mezi úložišti

3.2 Vazba TOGAF na COBIT

Control Objectives for Information and related Technology (COBIT) je rámec pro správu a řízení IT (IT Governance). Jedná se o soubor praktik, které by měly umožnit dosažení strategických cílů organizace díky efektivnímu využití dostupných zdrojů a minimalizaci IT rizik. COBIT byl ve své páté verzi upraven tak, aby byl plně kompatibilní s rámci TOGAF, ITIL a PRINCE2, a vytváří tak zastřešující rámec („umbrella framework“).



Obrázek 12 Pohled na metodický rámec COBIT v jazyce ArchiMate®

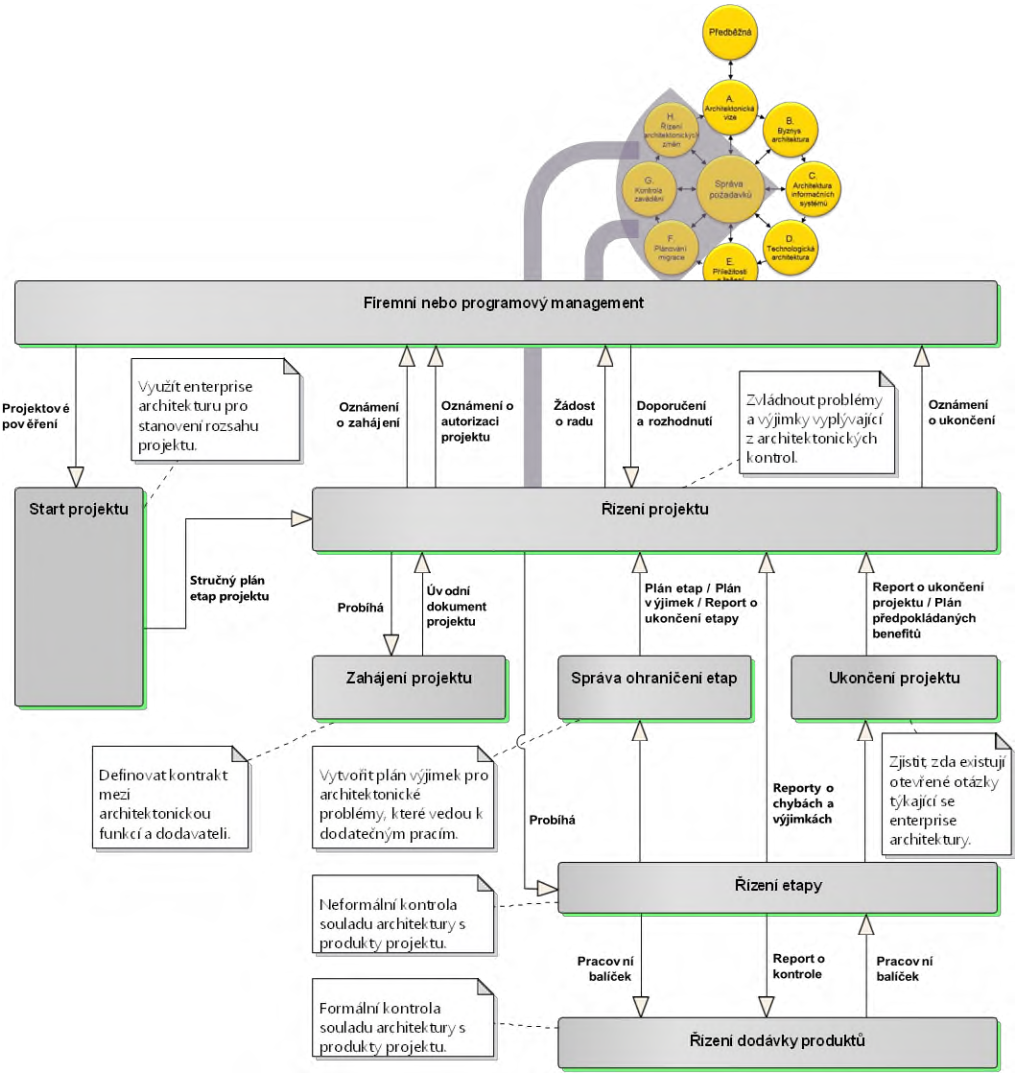
COBIT pokrývá většinu aktivit definovaných rámcem TOGAF. V rámci plánování a organizace definuje přímo proces Řízení Podnikové Architektury, čímž dochází k propojení obou rámců. COBIT dále obohacuje aktivity rámce TOGAF o:

- vztahuje je k obecným IT cílům a doprovodným metrikám,
- přidává architektonicky-specifické procesní cíle a doprovodné metriky,
- definuje zodpovědnosti za aktivity TOGAF formou matice přiřazení zodpovědnosti (RACI).

COBIT dává TOGAF do kontextu tím, že propojuje procesy architektury s ostatními procesy organizace, řízením změn projekty a poskytováním ICT služeb.

3.3 Vazba TOGAF na PRINCE2

Projects In Controlled Environment 2 (PRINCE2) je strukturovaná metoda pro řízení projektů.
TOGAF definuje aktivity, praktiky a výstupy pro projektový management. Nedoporučuje se používat samotný TOGAF jako rámec pro řízení projektu. Pro řízení architektonického projektu je možno použít



Obrázek 13 Vztah mezi procesy PRINCE2 a TOGAF

standardní projektové rámce jako PRINCE2 nebo PMBOK. Architektura vytvořená pomocí TOGAF by měla určovat specifikaci projektu, protože dává do relace základní požadavky s jednotlivými komponentami, které jsou vyjádřeny v modelech architektury. Specifikace jednotlivých projektů by měly být v souladu s architekturami vytvořenými pomocí TOGAF.

4 STRUKTURA MODELOVÝCH ARCHITEKTUR

V této kapitole se vysvětluje „Co se modeluje a proč“.

4.1 Architektury podle účelu a podrobnosti

Vrstvy architektury podniku se dělí podle míry detailu následujícím způsobem, viz také Obrázek 12:

- Vrstvy podnikové architektury
- Architektonická vize
- Celostní modely architektur podniku – Strategická architektura, slovník pojmů
- Segmentové, schopnostní a doménové modely architektur podniku
- Vrstva architektur řešení
- Doménové a projektové průřezové architektury řešení
- Vrstva designu konkrétních řešení
- Design a konstrukce realizace dílčích prvků řešení

Obrázek 14 Model vrstev architektur podniku/úřadu podle rozdílné míry detailu obsahu, zdroj: NA VSČR

Architektonická vize je první vrstvou agregovaných informací, sloužících k předání základních poselství o poznání organizace, jejího stávajícího, ale především cílového stavu. Tato vrstva nemusí souviset přímo s jednotlivými poznanými dílčími prvky organizace. Modely zpracované v rámci architektonické vize představují vizualizaci vybraných odpovědí na strategické otázky **Kam? a Proč?** se organizace vydává.

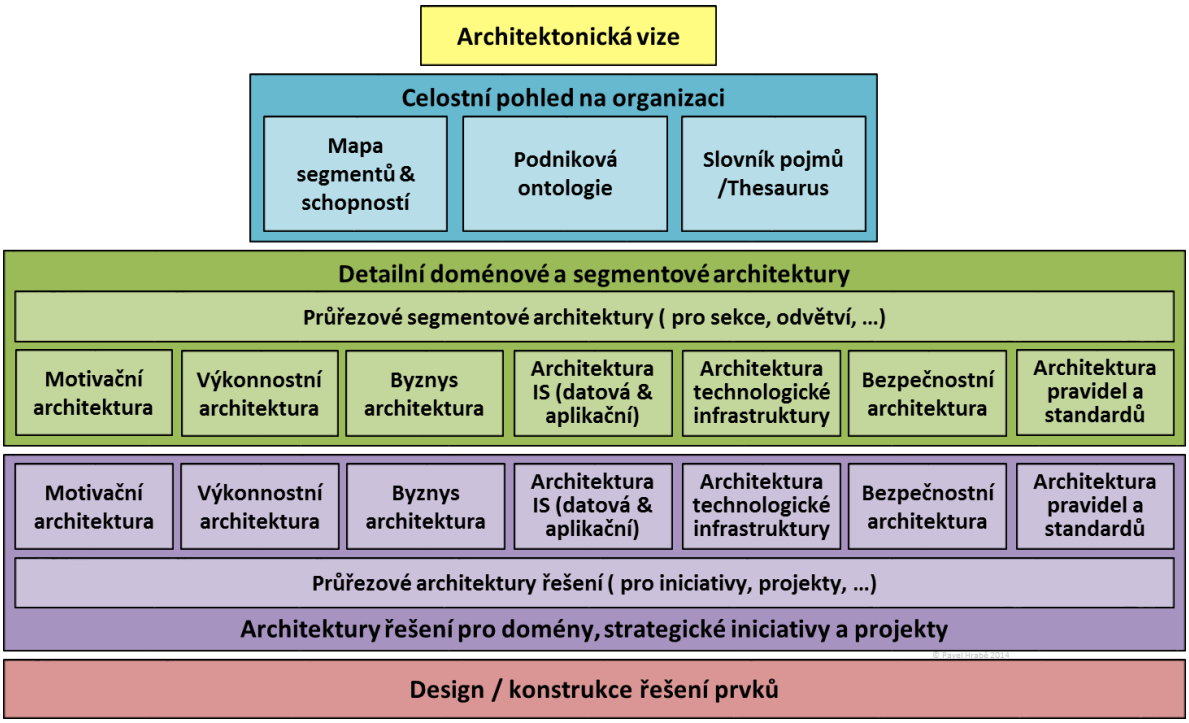
Druhá a třetí vrstva spolu s vizí představují podnikovou architekturu**, architekturu úřadu (EA).** V těchto vrstvách je zachycena inventarizace, vizualizace a porozumění tomu, co všechno se v organizaci

nachází a v jakých vazbách. Modely těchto vrstev představují vizualizaci na otázky **Co? a Jaké prvky?** organizaci tvoří.

Celostní podniková architektura je nositelem celostního pohledu na podnik. Představuje výčet všech typových prvků (objektů či konceptů), které se v organizaci vyskytují. Přehled typů objektů je základem pro slovník pojmů spojovaných s architekturou, tedy se strukturou a chováním organizace. Současně je tato struktura organizace vyjádřena jejím úplným meta-modelem (nebo jinak zvaným ontologickým modelem). Tato vrstva by mohla být označena jako meta-architektura podniku. Z tohoto modelu organizace jsou postupně vybírány objekty (například proces, služba aplikace, organizační jednotka atp.), které jsou předmětem inventarizace současného stavu a plánování stavu budoucího.

Třetí vrstva podnikové architektury je průřezová nebo doménová podniková architektura, která představuje těžiště obsahu popisu podnikové architektury, viz Obrázek 13 - zelená vrstva.

Tyto vrstvy popisují výhradně existenciální aspekty všech prvků architektury podniku a jejich vazeb (že existují, jak jsou staré, odkud pocházejí, kdo za jejich existenci odpovídá, jak dlouho budou ještě k dispozici apod.).



Obrázek 15 Pyramidální model architektur úřadu / podniku podle účelu a míry podrobnosti informací, zdroj: NA VSČR

Jako základ, demonstrující tento princip návrhu, byly do otevřené vrstvy doménových architektur pro běžné použití zařazeny:

- Výkonnostní architektura (dle vzoru FEAF)
- Motivační architektura (samostatně dle ArchiMate)

- Byznys Architektura (dle TOGAF, zde vyjma Motivační architektury, osamostatněné výše)
- Architektura IS (Datová a Aplikační)
- Architektura technologické infrastruktury (všechny ve smyslu definic dle TOGAF)
- Bezpečnostní architektura
- Řídicí doména (Governance)
- Architektura shody s pravidly, předpisy a standardy

Architektura řešení představuje vrstvu architektury vysvětlující, jak prvky tvořící organizaci fungují, jaká je jejich vnitřní výstavba, jak společně reagují na konkrétní potřebu (řeší ji). Její modely tedy představují vizualizaci odpovědí zejména na otázku **Jak funguje?** Architektury řešení musí vyhovovat architektonickým principům podnikových architektur z vyšších vrstev pyramidálního modelu.

Architektury řešení jsou obvykle dílčí, pokrývající část řešených problémů a změn organizace (program, projekt), které odpovídají jednotlivým dílčím potřebám a řeší požadované změny Architektury řešení. Jdou často napříč více architektonickými doménami, ale mohou být i uvnitř jediné z nich. Jsou typicky platné pro dílčí část segmentu.

Domény architektur řešení mohou přesně odpovídat doménám podnikové architektury, viz Obrázek 13, kde žlutě orámované domény fialové vrstvy odpovídají detailnímu rozpracování tradičních domén TOGAF. Domény architektur řešení v řadě případů budou odpovídat dílčím manažerským disciplínám, jako je BPM, EPM nebo QM.

Design řešení představuje vrstvu architektury přinášející detailní poznání o tom, jak lze dílčí prvek architektury vytvořit, vyrobit, jak uvést do provozu jednotlivý konkrétní prvek architektury podniku. Může jít o návrh změny pracovního postupu (proces), zadání programování SW komponenty, vzorec pro výpočet ukazatele výkonnosti apod. Architektonické modely řešení představují vizualizaci odpovědí na otázku **Jak je to udělané?**

4.2 Architektonické domény

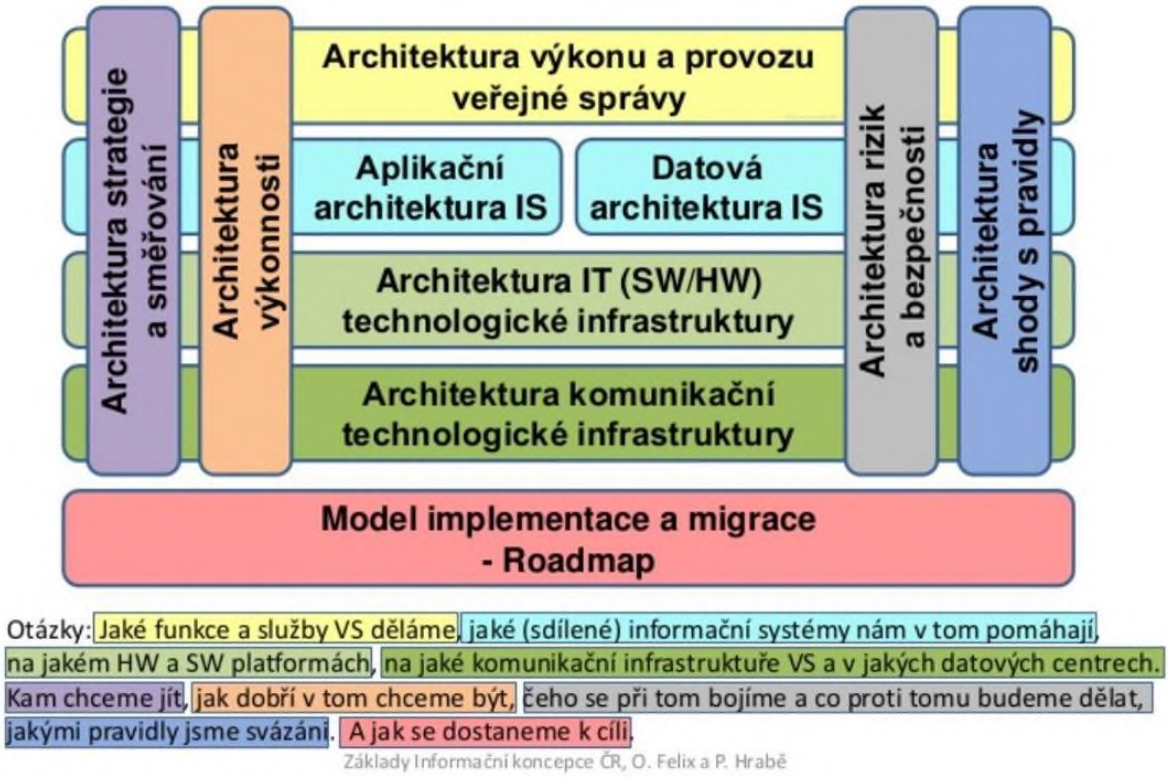
Zaměření a obsah národních architektur v jednotlivých zemích se vzájemně liší a časem se mění. Pro Národní architekturu VS ČR je navrženo již od počátku zahrnout do rámce NAR následující architektonické domény, viz také Obrázek 14:

- Architektura strategického směrování, tzv. motivační
- Architektura výkonnosti, měřící dosahování strategie i provozní efektivity
- Byznys architektura – tedy architektura všech součástí výkonu veřejné správy a podpůrných funkcí, zejména zaměřená na procesy, služby, organizaci, role a zodpovědnosti
- Architektura informačních systémů, členěná na Informační (datovou) a Aplikační architekturu
- Technologická architektura, pro potřeby VS ČR dělená dle čtyřvrstvé vize architektury na: architekturu IT technologií, tzv. platformou, architekturu komunikační infrastruktury.
- Bezpečnostní architektura – postihující specifické bezpečnostní atributy napříč doménami
- Řídicí doména (Governance)

- Architektura shody s pravidly a udržitelnosti

V tomto rozdělení je navrženo mimo jiné to, že do samostatné domény architektury strategie a směrování jsou z byznys architektury přesunuty koncepty motivace. Z oblastí, které například TOGAF považuje za součást obsahu metamodelu obsahu, ale nemodeluje je jako architekturu, viz Obrázek 28, byly do domény architektury „Shody s pravidly“ převzaty negativně motivující (limitující) koncepty, jako jsou omezení a předpoklady. V případě architektury pro VS ČR se zejména jedná o zákony formulující obsah tzv. agend. Následně jsou v téže doméně umístěny formulované (prohlášené) závazné standardy architektury.

Tento návrh struktury domén architektonického rámce výhodný zejména proto, že jako kombinace dvou ve veřejných správách nejvíce užívaných standardů TOGAF a FEAF (v nejnovější modifikaci pro GEA-NZ 3.1).



Obrázek 16 Rozvržení domén obsahu architektonického rámce NA VS ČR, zdroj: NA VSČR

Barevnost rozvržení domén NA VS ČR, viz Obrázek 14, není náhodná. Barvy tradičních domén dle TOGAF/ArchiMate přebírají barevnost vrstev jazyka ArchiMate (Lankhorst & al., 2009). Barvy vertikálních domén jsou převzaty ze schématu referenčních modelů GEA-NZ 3.0 (Deleu, 2014).

4.3 Architektury podle míry obecnosti a závaznosti

Typy modelů:

- Metamodel
- Referenční modely
- Společné (sdílené) modely, včetně modelů povinných vzorů
- Zobecněné (anonymizované) příklady
- Individuální modely

Některé výstupy architektury, např. standardy komunikace IS nebo standardy porovnávání výkonnosti procesů VS nebo přímo řízených organizací ústředních orgánů, budou závazné napříč celou veřejnou správou. Jiné budou závazné například jenom pro výkon státní správy, ale už nikoli pro územní samosprávy. Některé části obsahu architektury nebudou závazné nikde a
budou mít pouze popisný a doporučující charakter. Takové koncepci se v zahraničí říká
„federativní architektura“ a povinnosti dané zákony jsou v ní dobře patrné.
Z hlediska obecnosti, jednoty a účelu jednotlivých modelů bude obsah architektury členěn na:

- **Referenční modely (RM)** – vyjadřují obecné modely, které se dále využívají pro popisování reálných organizací nebo jejich částí. Na této úrovni se nevyskytují žádné konkrétní obsahy architektur (ani As-Is ani To-Be). Tato vrstva je povinně referenční na meta-úrovni, tj. přináší povinné klasifikace a povinné formy vyjádření modelů. Zkráceně: referenční forma modelování.
- **Společný (sdílený) obsah** – modely zahrnující ty součásti architektonických modelů, které organizace na různých úrovních veřejné správy musí nebo mohou sdílet. Tato vrstva je povinně i dobrovolně referenční pro obsahy To-Be architektur a je prostředkem zajištění konzistence celkové To-Be architektury veřejné správy. Zkráceně: referenční obsah architektury.
- **Individuální modely (IM)** - modely vyjadřující koncepce rozvoje jednotlivých organizací, vytvořené dle této metodiky vycházející z Národního architektonického rámce (NAR).

Výše uvedenou strukturu modelů doplňují ještě pro akceleraci zavedení EA velmi žádané praktické příklady. Svým charakterem jsou to individuální modely, ale mnohdy budou zobecněné, anonymizované, takže už u nich nebude patrný konkrétní modelovaný úřad. Tyto modely nejsou pro nikoho závazné. Slouží pro inspiraci jako nositelé praktické zkušenosti.

5 PROCESY TVORBY ARCHITEKTUR (TOGAF)

Proces tvorby architektur stanovuje, jak se má postupovat v celém životním cyklu architektury.

Z dvojice **disciplín 1) management architektury** a **2) governance architektury** se tato kapitola zaměřuje na procesy obou, ale struktury, orgány a vybrané funkce governance jsou v samostatné kapitole.

Pro proces tvorby architektur je převzala tato metodika cyklus z metodiky TOGAF ADM. Ten je rozdělen na fáze a ty dále na kroky, vysvětlené v popisu jednotlivých fází. V každé fázi je třeba vždy kontrolovat, zda výstupy a výsledky fáze odpovídají očekávání celého angažmá a metodickým požadavkům na danou fázi. V cyklu metodiky ADM se nacházejí následující fáze:

Předběžná fáze (Preliminary Phase), která popisuje přípravu a zahájení činností potřebných pro promítnutí business potřeb do architektury, včetně přizpůsobení architektonického rámce a definice principů a okrajových podmínek.

Fáze A: Architektonická vize (Architecture Vision) popisuje úvodní fázi architektonického cyklu. Zahrnuje definici rozsahu, poznání zájmových skupin, vytvoření architektonické vize a získání souhlasů k architektonickému záměru.

Fáze B: Business architektura (Business Architecture) popisuje vývoj architektury podnikání, poslání organizace na podporu dosažení stanovené vize.

Fáze C: Architektura IS (Information Systems Architectures) popisuje postup vývoje architektury IS, zahrnující aplikační a datovou architekturu.

Fáze D: Technologická architektura (Technology Architecture) popisuje vývoj architektury IT technologické infrastruktury.

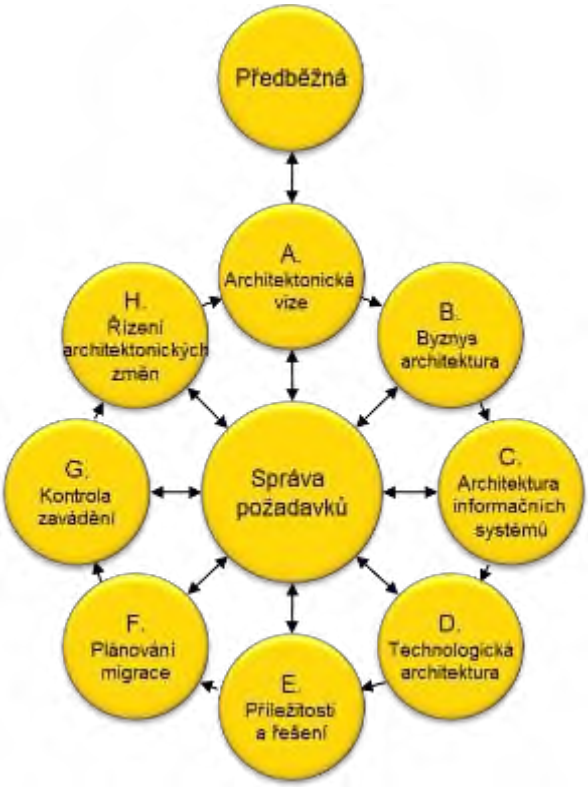
Fáze E: Příležitosti a řešení (Opportunities & Solutions) provede počáteční plánování implementace a identifikaci prostředků dodávky architektonických změn, definovaných v předchozích fázích.

Fáze F: Plánování přechodu (Migration Planning) představuje detailní plánování potřebných implementačních kroků.

Fáze G: Kontrola (řízení) implementace (Implementation Governance) představuje architektonický dohled nad průběhem implementace.

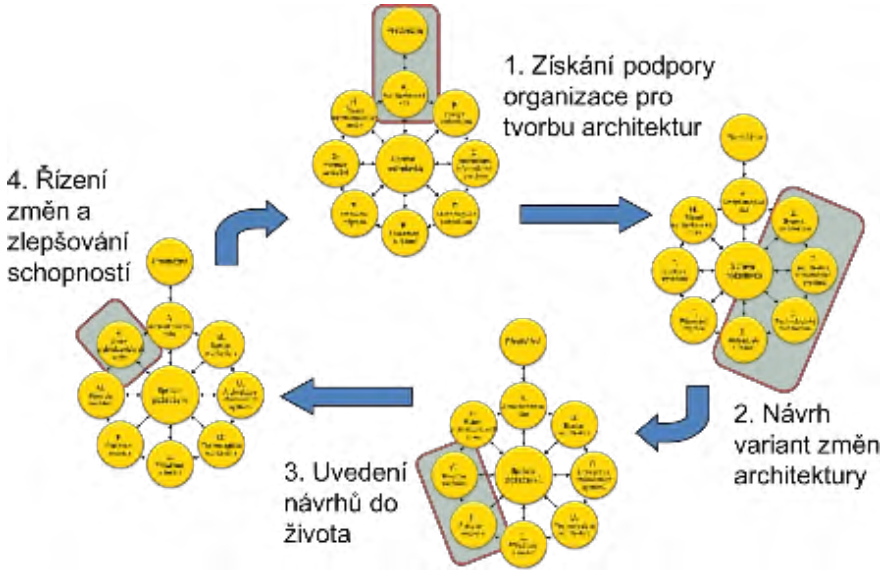
Fáze H: Řízení architektonických změn (Architecture Change Management) ustavuje procedury pro řízení změn architektury.

Správa požadavků (Requirements Management) představuje vazbu procesů řízení IT požadavků a procesů řízení změn architektury. Fáze Správy (architektonických) požadavků je průběžná. Výstupy jedné fáze mohou (nebo dokonce mají) být upraveny fázemi následujícími.



Obrázek 17 Přehled fází tvorby architektury dle TOGAF ADM (The Open Group, 2022)

Metodika TOGAF ADM je postavena na iteraci mezi jednotlivými procesy. Cílem těchto iterací je vybudovat optimální architekturu. Každá iterace je při tvorbě architektury uvozena rozhodnutím o tom, co by mělo být pokryto v dané fázi, jaká úroveň detailu je požadována a v jakém časovém výhledu by se mělo dojít k cílové architektuře (výsledku iterace). Pochopitelně je zároveň specifikováno, jakých architektonických standardů bude využito a za jakých omezujících podmínek.



Obrázek 18 Seskupení fází cyklu ADM vývoje architektur (The Open Group, 2022)

Podrobnější popis rámce TOGAF a fází ADM se nachází v příloze 10.1 Základy rámce TOGAF.

5.1 Přizpůsobení cyklu metodiky ADM pro architekturu resortu zdravotnictví

Metodika TOGAF ADM předpokládá, že bude upravena na míru organizace, což platí i pro českou veřejnou správu. Základní úprava metodiky ADM je obsažena v této metodice.
Před zahájením každé dílčí architektonické práce v úřadu je třeba znovu provést níže uvedená rozhodnutí a nastavit parametry tohoto angažmá.

5.1.1 Nastavení rozsahu architektonického angažmá

Metodika ADM je iterativní proces, s iteracemi mezi fázemi i uvnitř každé fáze. Pro každou iteraci v ADM, pro každé jednotlivé nové architektonické zadání (angažmá) v úřadu/ organizaci musí být předem, v **Požadavku na architektonickou práci, stanoveno:**

- šířka pokrytí úřadu/podniku architektonickým angažmá,
- požadovaná míra (hloubka) modelovaného detailu,
- časový horizont architektury,
- modelované domény,
- architektonické vstupy, ať již to jsou výsledky předchozích fází nebo předchozích cyklů v úřadu nebo architektonické materiály odkudkoli, třeba referenční modely z OHA MV nebo ze světa.

Tato metodika stanovuje nad rámec standardu TOGAF, aby byly v Požadavku na architektonickou práci specifikovány základní zájmové skupiny (stakeholders) vedle sponzora, a dále výstupy, kterými mohou být naplněna očekávání sponzorů.

Definitivní a závaznou specifikaci výstupů přinese vždy až schválené tzv. **Zadání pro architektonickou práci** („Statement of architecture work“), které zpracuje architektonický výbor organizace.

5.1.2 Rozhodnutí o šířce rozsahu

Primárně se jedná o rozhodnutí, zda na požadovaný záměr zadavatele odpovídá architektura uvnitř úřadu/ organizace (enterprise) nebo jeho části (segmentu), anebo bude modelován tzv. rozšířený úřad/ organizace společně s externími partnery, dodavateli a úřady. Je tedy podstatné, zda se v daném architektonickém angažmá bude jednat o vlastní organizaci úřadu, nebo architekturu úřadu společně se všemi podřízenými organizacemi, nebo architekturu rozšířeného řetězce dodávky veřejné služby.
Při každém architektonickém zadání pro individuální nebo referenční modely uvnitř úřadu (enterprise) je třeba rozhodnout, zda se bude jednat o celostní, strategickou architekturu, nebo segmentovou architekturu, či dokonce schopnostní architekturu.

5.1.3 Rozhodnutí o hloubce obsahu

Pro modely v rámci NA VS ČR platí, že nebude-li v Požadavku na architektonickou práci specificky odůvodněno jinak, modelují se **všechny výskyty procesů**, aplikací, platforem apod. dle předdefinovaných metamodelů, které se v daném rozsahu organizace aktuálně nacházejí nebo cílově mají nacházet.
U každého inventarizovaného nebo projektovaného objektu se ale model ptá pouze po jeho existenci a existencí zásadně spojených atributech. Například zda je aplikační komponenta zakoupena nebo naprogramována, od koho, kdy vznikla a kdy bez podpory zanikne, případně zda je součástí strategické infrastruktury státu atp.
U změn vznikají **architektury řešení**, s úrovní podrobnosti **„Solution Architecture“.** Tyto architektury odpovídají na otázku: „Jak to má fungovat (uvnitř – funkce a vně – služby)?“
Výsledkem je úplná funkční nebo ne-funkční specifikace, katalogů služeb a dalších detailních architektonických artefaktů (potřebné pro výběr a uzavření smlouvy s interním nebo externím dodavatelem realizace změn.
Konkrétní **návrh řešení (Solution Design)** se již v zodpovědnosti útvarů architektury úřadu nikdy netvoří.

5.1.4 Rozhodnutí o časovém horizontu architektury

Při každém architektonickém angažmá je třeba rozhodnout, v jakém časovém horizontu (za jak dlouho) se má plánovat cílová navrhovaná architektura. Délku požadovaného horizontu na jedné straně prodlužuje požadavek dlouhodobé stability návrhu, na druhé straně ji zkracuje přirozená neschopnost predikovat cokoli na dobu delší tří let (zejména pak v IT oblasti).
Vedle toho je třeba, aby architektura úřadu vždy přinášela dostatečný informační předstih a podklad pro rozhodování. Proto tato koncepce stanovuje, že jako další milník cílové architektury se musí používat **horizont klouzavý** (relativní), stanovený na do dobu **5 let** od předložení architektury ke schválení.

Realizace architektur se děje po krocích odpovídajících rozvojovým programům a projektům. Každý z nich po úspěšném završení posouvá stávající stav do nejbližšího projektovaného budoucího stavu architektury. Takovým časovým řezům architektur se říká **přechodové architektury**. Vzhledem k přetrvávajícímu ročnímu řídícím (a rozpočtovému) cyklu ve VS ČR a k omezené míře předvídatelnosti věcí budoucích je stanoveno, že cesta k cílovému horizontu architektury úřadu (2025 a 5 let) musí být povinně rozdělena přinejmenším do přechodových architektur odpovídajících **1. a 2. roku** jejich realizace. Vedle toho musí být možné prezentovat z architektonického modelu v úložišti úřadu (nebo posléze v centrálním národním úložišti) projektovanou přechodovou architekturu úřadu ke každému **milníku dokončení realizačního projektu či programu.**

Pro všechny architektury úřadu/podniku v rámci NA VS ČR platí, že budou s týmž klouzavým (relativním) horizontem (5 let, odpovídajících **rozpočtovému výhledu**) aktualizovány **na úrovni strategické architektury úřadu** pravidelně **každý rok** tak, aby identifikované (a upřesněné) transformační projekty na následující rok mohly sloužit jako kvalifikovaný podklad pro vyjednávání o struktuře a výši **rozpočtu**.

5.1.5 Rozhodnutí o doménách při tvorbě architektur

Pro modely architektury v úřadech se v rámci koncepce NA VS ČR předpokládá, že budou **vždy** obsahovat popis architektury (modely a artefakty**) ve všech** jejích **doménách**. To platí přinejmenším bez výjimek pro pravidelně aktualizovanou strategickou architekturu úřadu.

Ne vždy budou úřady disponovat dostatečným časem, schopnostmi, kapacitami či prostředky na to, aby navrhly (nebo si nechaly navrhnout) všechny dílčí architektury ve všech doménách. Proto není nutné navrhovat všechny domény architektur úřadu, pokud to není potřebné pro naplnění požadavků sponzora nebo zadavatele. Nenavrhované domény je však vždy třeba mít alespoň okrajově na zřeteli.

Je však důležité definovat hranice mezi jednotlivými doménami. To znamená určit, jaké části organizace nebo procesy patří do každé domény a jak jsou mezi sebou propojeny.

Pro každou identifikovanou doménu je důležité stanovit odpovědnosti a pravomoci. To zahrnuje určení, kdo je zodpovědný za správu, rozvoj a řízení dané domény, stejně jako vztahy mezi různými doménami. Je důležité také vyhodnotit, jak jednotlivé domény spolu interagují a jaké jsou závislosti mezi nimi. To umožní lépe porozumět celkové architektuře a zajistit, aby byla navržena optimální řešení.

Při tvorbě architektur je tak důležité přijímat rozhodnutí o doménách, identifikovat a definovat různé oblasti, které ovlivňují architekturu informačních systémů a technologií v organizaci, protože tato rozhodnutí jsou klíčová pro správné řízení a rozvoj architektury.

Příklad: Je-li zadáním sponzora navrhnout, které technologické platformové komponenty mohou být přesunuty do dvou cílových virtualizovaných datových center kraje, a které dokonce do jednoho z NDC, pak IT technologická vrstva a komunikační vrstva musí být úplná. Aplikační vrstva stačí jenom naznačená a datová, byznys, motivační a výkonnostní vrstva nemusí být modelována vůbec. Předpokládá se, že se aplikační služby a data vůči byznys a vyšším vrstvám se změnou technologických vrstev nesmí změnit.

5.1.6 Rozhodnutí o použitých vstupech

Tato metodika ve svých aktualizacích stanovuje postupně narůstající sadu povinných a doporučených akcelerátorů (vzorů, taxonomií a referenčních modelů, návodů, příkladů). Ty podle míry závaznosti musí nebo mohou být použity ve všech odpovídajících modelech.

Pokud je možnost volby, je potřebné, aby každé zadání bylo zpřesněno i odkazem na vstupy pro něj stanovené.

Obdobně to platí i pro již existující architektonické artefakty. V každém zadání by mělo být stanoveno, na jaké architektonické dřívější artefakty a výstupy má navázat, zpřesnit je nebo nahradit.

5.1.7 Rozhodnutí o volbě hledisek podle zainteresovaných

Již před zahájením modelování architektury musí být v Požadavku na architektonickou práci identifikovány klíčové zájmové skupiny (stakeholders), jejich požadavky, potřeby a architektonické artefakty (pohledy na model).

Jde o to, že vedoucí organizací budou muset v souvislosti s vytvořenou architekturou (na základě jeho výsledků) činit investiční rozhodnutí o realizaci změn.

6 STANOVENÍ RÁMCE OBSAHU A VÝSTUPU ARCHITEKTUR

Tato kapitola stanovuje přesně, jaké objekty architektury úřadu jsou předmětem zájmu při sestavování modelu a jeho architektonických výstupů. Určuje způsob popisu obrazu architektury úřadu.
Kapitola se zejména zaměřuje na prvky metamodelu a na formální (předměty dodávky) a neformální (artefakty) architektonické výstupy.
Vlastní rámec obsahu a definice výstupů architektur je průběžně určován Architektonickým výborem.

6.1 Předměty modelování – architektonický metamodel

Metamodel je předpis a logika používání jazyka pro modelování architektury v praxi. Při tvorbě architektury budou vytvářeny modely v jazyce ArchiMate podle předem schváleného metamodelu. Užití Metamodelu je plně v souladu se specifikacemi jazyka **ArchiMate** a architektonického rámce **TOGAF**. Metamodel architektury jednoznačně definuje, jaké elementy z jazyka ArchiMate a jaké vazby mezi nimi jsou použity.
Důvody a pravidla pro používání metamodelů při tvorbě konkrétních modelů jsou následující:

- Metamodel **je abstraktním modelem**, důležitým pro správné zachycení a zvýraznění objektů a vazeb v modelu úřadu (co a jak modelovat),
- Metamodel **podporuje určitou metodu** nebo konkrétní postup tvorby modelů (předepisuje modelovací jazyk, použité elementy a možné vazby).

6.1.1 Použití jazyka ArchiMate pro modelování

6.1.1.1 Vrstvy a struktura modelů

V diagramech je třeba rozlišit jednotlivé vrstvy (příp. strukturu) modelů pomocí vizuálního uspořádání. Základní elementy vrstev modelu (byznys – procesní, aplikační a datová, technologická, infrastrukturní) budou vždy **odlišeny barevně**. Jednotlivé elementy pohledů jsou vertikálně (shora dolů) propojeny **logickými vazbami.**
Metodika předpokládá, že výraznou informací, obsaženou v pohledech na model je i umístění prvků modelu v jeho ploše, v tzv. mapách. Pro jednotnou logiku umisťování prvků poslouží postupně sestavené referenční modely k jednotlivým vrstvám architektury a k jednotlivým pohledům.

6.1.1.2 Barvy elementů

Definovaná struktura meta – modelu ArchiMate je členěna na tři vrstvy, které jsou pro účely respektování čtyřvrstvé vize architektury eGovernmentu ČR rozšířeny na čtyři vrstvy. Každá vrstva má barevnou interpretaci dle originální ArchiMate specifikace, podle které lze určit, o jakou vrstvu se jedná. Tento barevný standard je nutno respektovat a dodržovat.

- **Procesní vrstva** a všechny elementy v této vrstvě jazykem ArchiMate® definované budou **žluté**.
- **Aplikační a datová vrstva** a všechny elementy v této vrstvě jazykem ArchiMate® definované budou **tyrkysové**.
- **Technologická vrstva** a všechny elementy v této vrstvě jazykem ArchiMate® definovanou budou **zelené**.
- **Infrastrukturní vrstva** a všechny elementy v této vrstvě jazykem ArchiMate® definovanou budou **zelené**.

Komponenty obou vrstev vize čtyřvrstvé architektury VS (technologické a infrastrukturní) budou v téže zelené, neboť ve skutečnosti tyto vrstvy jsou pouze speciálním rozdělením jednotné technologické architektury dle standardu ArchiMate pro české potřeby řízení zodpovědnosti za rozdílné technologické služby.

V souladu se specifikací ArchiMate a NAR se nebude používat barevné vzájemné rozdělení tzv. aspektů v jednotlivých vrstvách (aktivní prvky, chování a pasivní prvky) – barevné odlišení není nutné, a když, tak jedině stupni šedé.

6.1.1.3 Tabulka definice barev dle standardu NAR

Barvy vychází ze standardu NAR a Archimate 3.1, který v tento moment NAR využívá.

Doména	Název barvy	Červená (R)	Zelená (G)	Modrá (B)
Motivační	Fialová	204	204	255
Strategická	Okrová	245	222	170
Byznys	Žlutá	255	255	175
Aplikační	Tyrkysová	175	255	255
Technologická	Zelená	175	255	175
Fyzická	Zelená	175	255	175
Implementační a migrační	Světle červená	255	224	224
Kompozitní	Světle zelená	224	255	224
	Bez barvy (bílá)	- (255)	- (255)	- (255)
	Oranžová	255	185	115

Poslední verze standardu ArchiMate 3.1 zavedla nové barvy pro nové domény (strategickou a fyzickou) a přesunula řadu prvků z byznys domény do strategické. Tím došlo k rozporu v barevnosti prvků vůči původnímu barevnému ladění domén NAR.

Tento rozpor se ještě bude na úrovni NAR muset řešit. Problém je v tom, že na jedné straně NAR a tato metodiky počítá s doménami a prvky, které ještě ve standardu ArchiMate nejsou a až se v něm (pravděpodobně) objeví, mohou mít jinou barvu, než nyní plánuje NAR. Současně je problémem

efektivní užívání modelovacích nástrojů, kde nejjednodušší je ponechávat prvkům jejich originální ArchiMate barvu.

6.1.1.4 Tvary elementů

Elementy ve všech vrstvách budou zobrazeny tak, jak je jazyk ArchiMate® definuje. Je nepřípustné upravovat jejich tvary dané standardem Open Group.

Vedle toho (a navíc) je ale možné vytvářet na základě korektně zachyceného modelu úřadu libovolné a rozmanité tzv. laické diagramy, představující model netrénovaným čtenářům prostřednictvím intuitivních (často naivních a naturálních) ikon a animací.

6.2 Celkový metamodel

6.2.1 Maximální metamodel

Maximální metamodel architektury úřadů jako součástí Národní architektury je pro první období jejího zavádění stanoven jako plný a nezměněný rozsah standardní specifikace ArchiMate 3.1 (ten aktuálně NAR využívá), případně vyšší.

Protože metamodel ArchiMate a TOGAF ještě není vzájemně 100% shodný, přebírá NAR některé objekty metamodelu i z TOGAF, a to objekty Organizační jednotka, Logická a fyzická aplikační komponenta, Logická a fyzická technologická komponenta.

Vedle toho zavádí NAR nové koncepty pro objekty typické pro českou veřejnou správu, a to Právní předpis, Agendu a Informační systém (logický, ISVS).

Nad rámec standardní specifikace ArchiMate 3.1 jsou pro metamodel NA VS ČR zavedeny následující specializované koncepty (objekty metamodelu), tzv. «stereotypy», postihující:

potřeby veřejné správy je to „právní předpis“ jako «Předpis», «Agenda» a «IS»,

obecně chybějící koncepty „organizační jednotka“ jako «Organizace» (dle TOGAF) a «Útvar », pro standardizaci «Standard»,

potřeby odděleně postihnout a vyhodnotit prvky komunikační infrastruktury jsou to volitelně «Komunikační služby», «Komunikační funkce» apod. (z čtyřvrstvé vize),

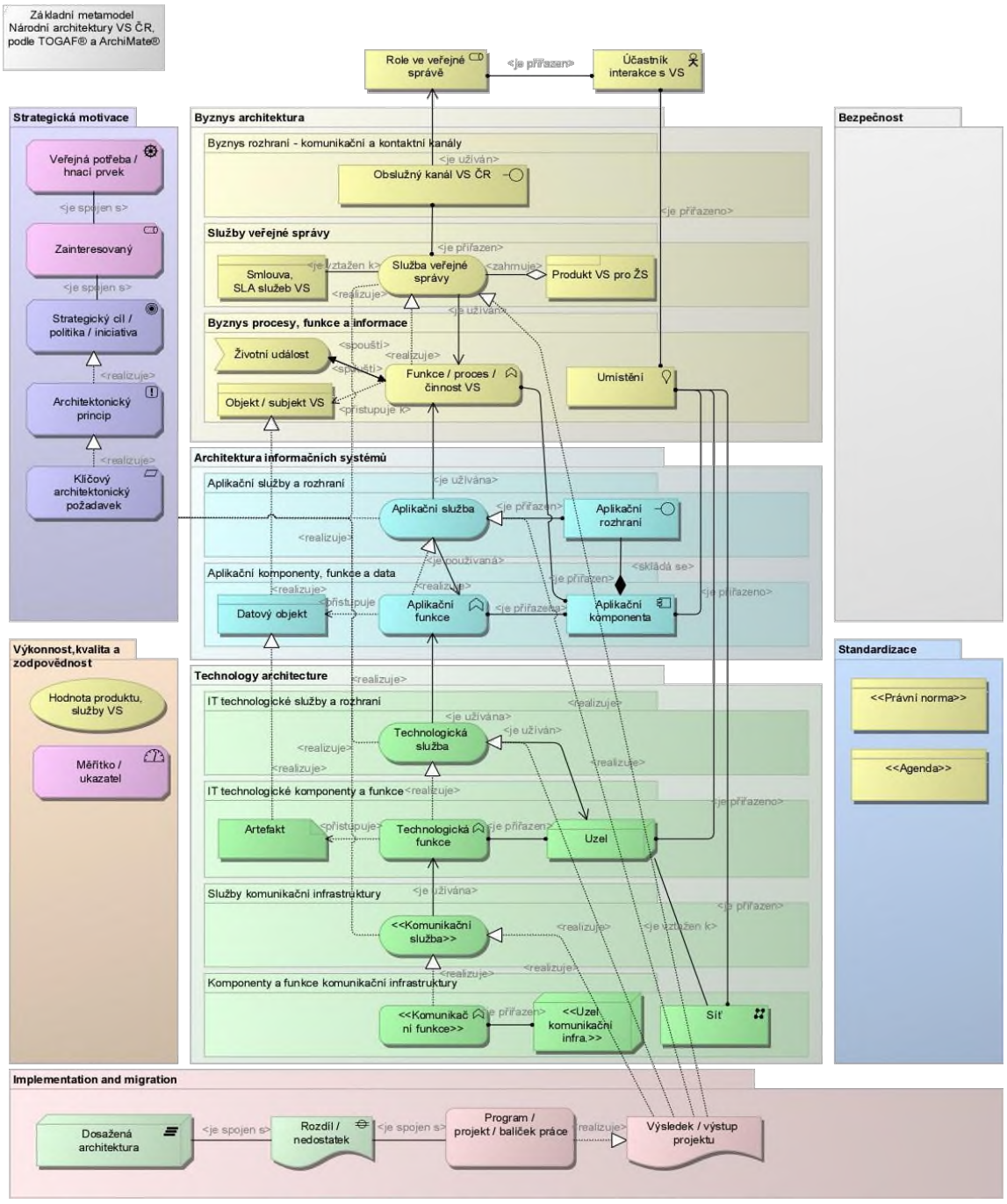
potřeby odlišit «Logické aplikační komponenty» a «Fyzické aplikační komponenty» (z TOGAF).

Není povinné specializovat prvky z doplněné vrstvy Komunikační a fyzické infrastruktury, ale je to přípustné.

Teprve praktická zkušenost ukáže, zda není výhodné některé objekty metamodelu pro zjednodušení zakázat a jiné specializací původních doplnit.

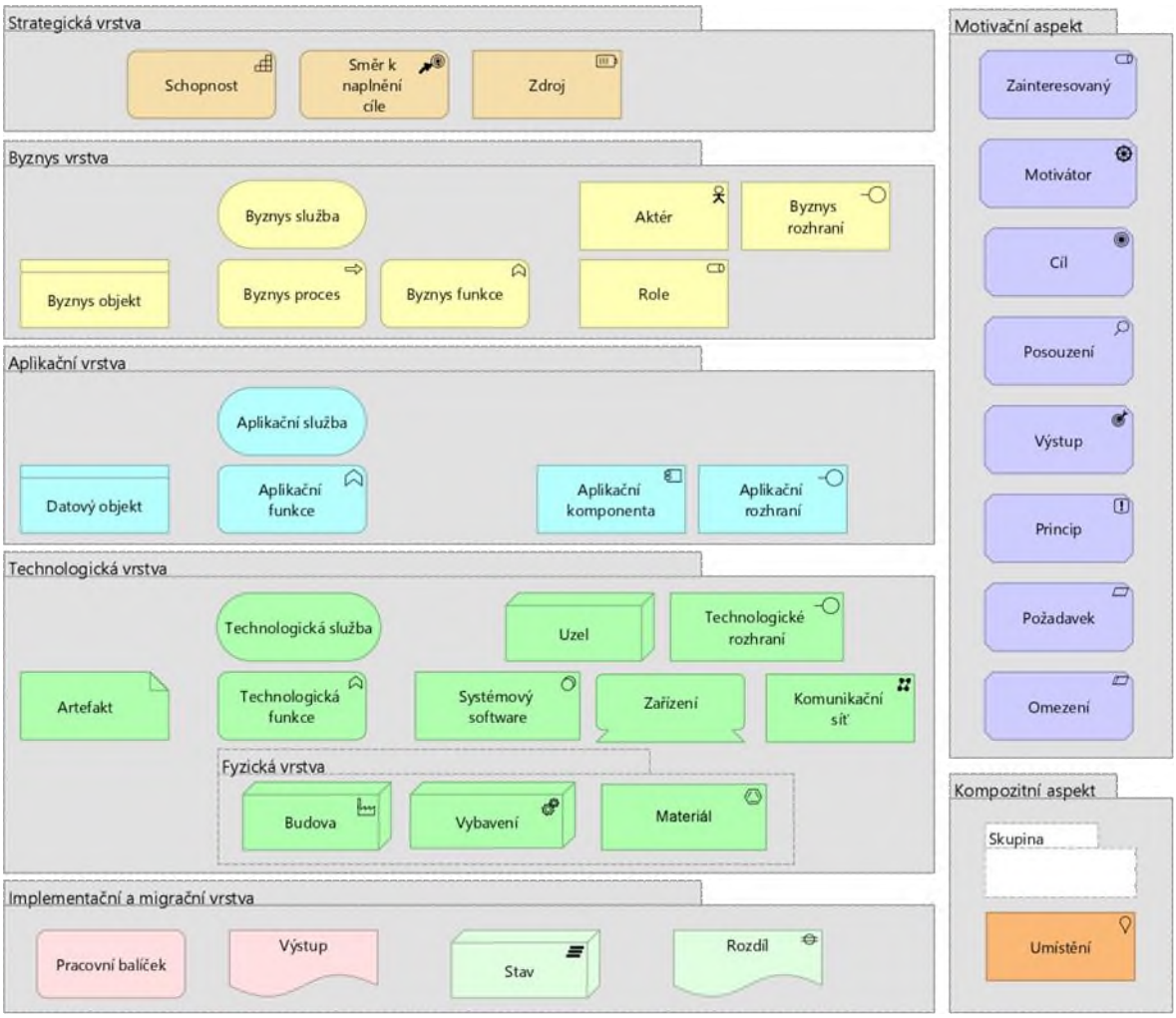
6.2.2 Základní metamodel

Doporučený redukovaný (základní) metamodel je představen souhrnně na schématu uvedeném níže a současně vždy u jednotlivých doménových metamodelů.



Obrázek 19 Základní metamodel národní architektury veřejné správy České republiky, zdroj: NA VSČR

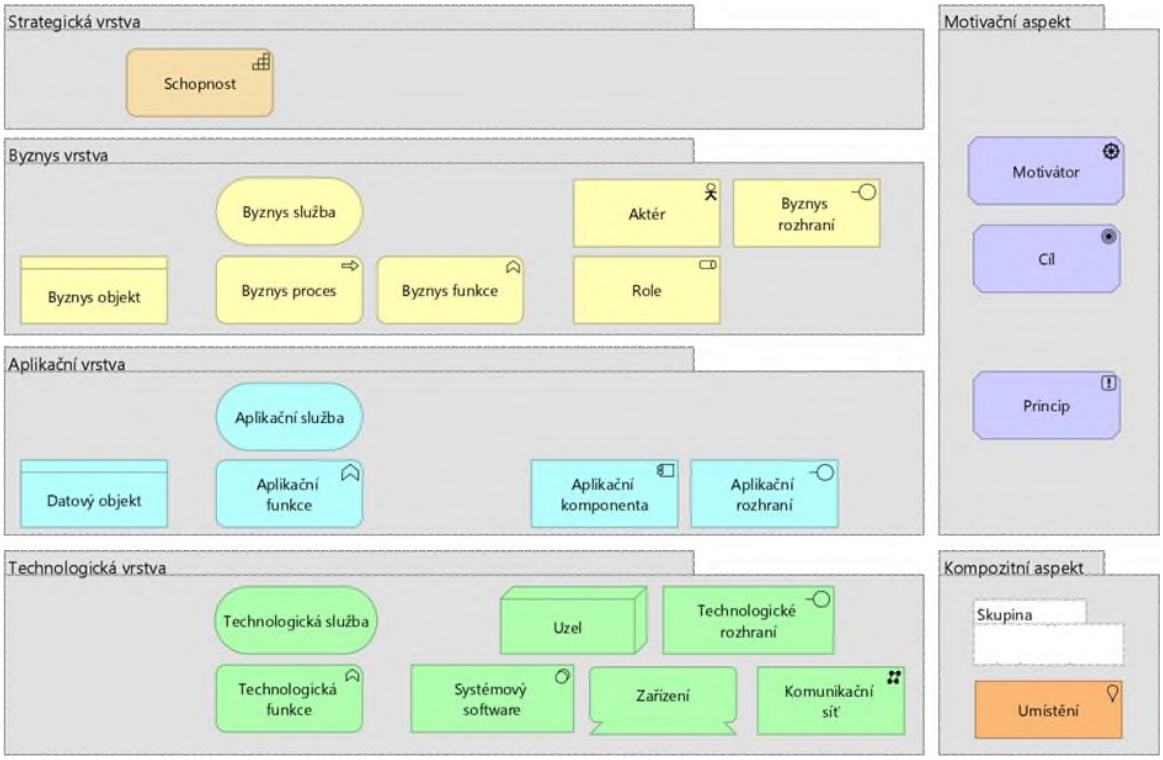
V jednotlivých typizovaných (a legislativním nebo metodickým předpisem upravených) architektonických angažmá, jako je právě seznámení OHA s plánovaným IT projektem (tzv. žádost) bude samostatným metodickým postupem doporučen pro zjednodušení ještě dále redukovaný metamodel.
Doporučené redukované (zjednodušené) metamodely jednotlivých vrstev architektury jsou uvedeny v následujících částech.



Obrázek 20 Základní (redukovaný) výběr prvků metamodelu NA ze standardu ArchiMate 3.1 (bez specializovaných stereotypů), zdroj: NA VSČR

6.2.3 Zjednodušený metamodel základních doporučených prvků

Celkový, již redukovaný základní (natož maximální) metamodel definující architekturu NA, obsahuje ještě stále značné množství vazeb a rozšiřujících oblastí. Pro přehlednost a lepší pochopení je na Obrázku níže schematicky znázorněn dále zjednodušený metamodel základních doporučených prvků. Z úplného metamodelu byly vybrány pouze nejzásadnější objekty a vazby z nerozšířeného standardu ArchiMate.



Obrázek 21 : Zjednodušený metamodel základních doporučených prvků, zdroj: NA VSČR

6.2.4 Principy a příklady lokálních rozšíření metamodelu

Dle NAR: Každá z budoucích tzv. povinných organizací (OVS) bude pravděpodobně moci architekturu úřadu modelovat nad rámec povinného rozsahu, definovaného touto metodikou a udržovaného v centrálním architektonickém úložišti. Do něj však budou po kontrole přebírány pouze modely přesně stanoveného rozsahu.

Pro svoje interní účely smí OVS rozšiřovat metamodel architektury, jak v notaci ArchiMate specializací objektů, kdy vznikají nové tzv. stereotypy, tak provázáním objektů do detailních modelů v jiných notacích, např. UML, BPMN, DMN nebo Citizen Journey Map).

Definice lokálních rozšíření metamodelu je plně v gesci rozhodnutí Architektonického výboru pro případné budoucí použití.

6.2.5 Povinný rozsah modelů

Povinný rozsah modelů není stanoven souhrnně touto metodikou, ale je dán typy architektonických angažmá. Jim budou odpovídat dílčí metodické pokyny a rozšiřující metodiky typu „Jak na to?“. Například tabulky a vysvětlení ve formuláři a metodickém pokynu žádosti o stanovisko OHA k ICT projektům jednoznačně stanovují, které objekty modelů musí být zahrnuty a prakticky o tomto povinném rozsahu rozhoduje Architektonický výbor, případně jsou definovány na úrovni projektů v zadávací dokumentaci.

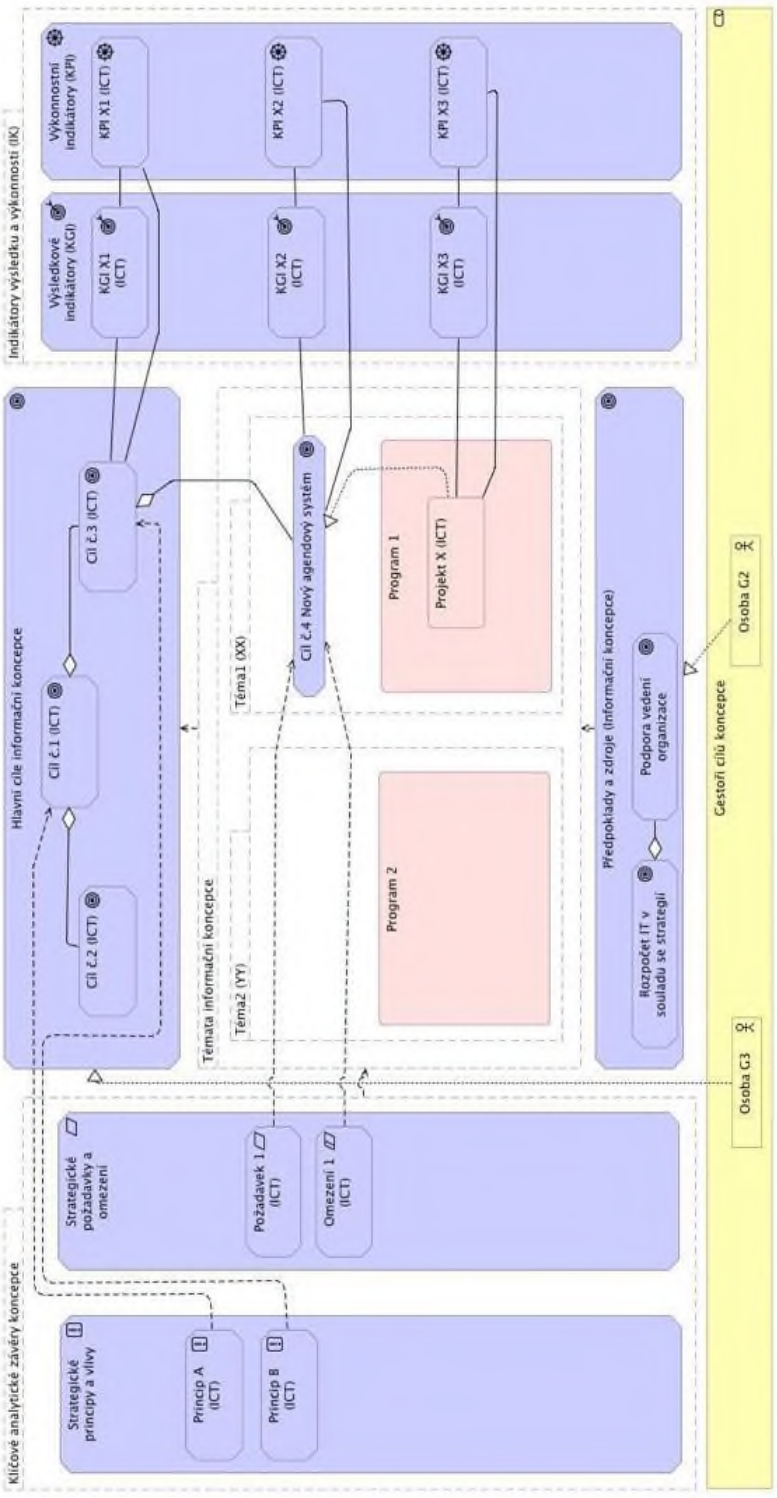
6.3 Dílčí doménové metamodely

6.3.1 Motivační vrstva, strategie, registr záměrů a projektů, migrace

6.3.1.1 Koncepce a „business“ strategie, motivace a výkonnost

Diagram je určen všem členům vedení organizace / úřadu / rezortu / kraje / magistrátu – potenciálně i včetně politického vedení úřadu i ostatních členů reprezentace. Dalšími adresáty je odborná veřejnost a se základním obsahem / sumářem by měli být seznámeni i zaměstnanci.

Poznámka: obrázky v následujících kapitolách, u kterých není uveden titulek, pocházejí z modelů zveřejněných na stránkách MVČR, Odboru hlavního architekta.



Obrázek 22 Dílčí a specifické strategie (2.úroveň strategie), zdroj: metodika DAIN s.r.o.

Diagram odpovídá na otázky, **jakou vizí / prioritami se organizace řídí, co motivuje hlavní změny a jak je strukturován strategický plán** jak vnitřního rozvoje organizace / rezortu / kraje / magistrátu, tak cíle ovlivňující celou oblast působnosti organizace a v důsledku rozvoj společnosti.

Koncepce a „business" strategie organizace reprezentuje diagram – mapu vzniklou převodem základních koncepčních dokumentů organizace do strukturovaného modelu – vyhovujícímu moderním manažerským metodikám BSC / CAF (a popsané notací ArchiMate). V menší míře by měly být obsaženy cíle z kompetenčního zákona (v případě úřadu), ve větší míře dlouhodobý plán rozvoje / vlivu organizace na zákazníky a rozvoj společnosti. Obsahem cílů by měl být rovněž závazek vedení zlepšovat efektivitu a výkonnost organizace (obecně směřování k excelenci, jak jí definuje CAF).

Struktura modelu motivace vychází z „best-practices" metodiky BSC (Balanced-Scorecard), která je „de-facto" standardem pro kauzální modelování strategií. Určitým zvoleným zjednodušením je volba jen 2 skupin cílů proti 4 „perspektivám" klasického BSC. Umožňuje to **jednodušší agregaci dílčích strategií** do celkové koncepce / strategie organizace tak, že vrcholové cíle specializovaných strategií tvoří „nižší patro" dílčích cílů koncepce / strategie celé organizace.

Popis, principy a hlavní prvky diagramu:

- Koncepce „Strategická mapa" by měla celkově (z důvodu přehlednosti a srozumitelnosti) obsahovat řádově desítky objektů.
- Součástí grafické reprezentace modelu nemusí být nutně zpracování principů a vlivů (často se pro definici cílů užívá jiná struktura vstupních analýz – např. SWOT, různé kvantitativní a kvalitativní analýzy apod.).
- Počet vrcholových cílů by neměl překročit cca deset (nicméně není to dogma). Velký počet cílů indikuje potřebu jejich přemístění o úroveň níže do dílčích – specializovaných strategií.
- Principy a vlivy se vážou na jednotlivé cíle vazbou typu ovlivnění (influence).
- Cíle jsou vzájemně spojeny vazbou typu kompozice, která ukazuje **směr hlavní kauzality příčina -> důsledek** (splnění cílů 2 a 3 je podmínkou splnění cíle 1; plnění cíle 4 je podmínkou / předpokladem splnění cíle 3).
- Z hlediska návazných dílčích strategií (např. IT strategie) se jejich vrcholové cíle vážou do strategické úrovně dílčích cílů organizace (vrcholový cíl diagramu IT strategie bude obvykle dílčím cílem v koncepčním – vrcholovém diagramu celé organizace). Obdobným způsobem se agregují cíle mezi subjekty organizace. Vrcholové cíle jednotlivých subjektů ovšem mohou tvořit jak vrcholové, tak dílčí cíle celé struktury mateřské a zřizovaných organizací (celku).
- Každý cíl, který není automaticky (s)plněn naplněním podřízených / dílčích cílů musí být vybaven indikátorem (měřítkem) výsledku (**KGI-Key Goal Indicator**) definujícím, jak je měřeno (s)plnění cíle. Rovněž je důležité definovat výkonnostní indikátor (**KPI – Key Performance Indicator**), pokud lze takový nalézt. Hodnota KPI se určuje plánem, je manažersky ovlivnitelná a správné hodnoty přispívají k plnění výsledku (KGI – Key Goal Indicators).

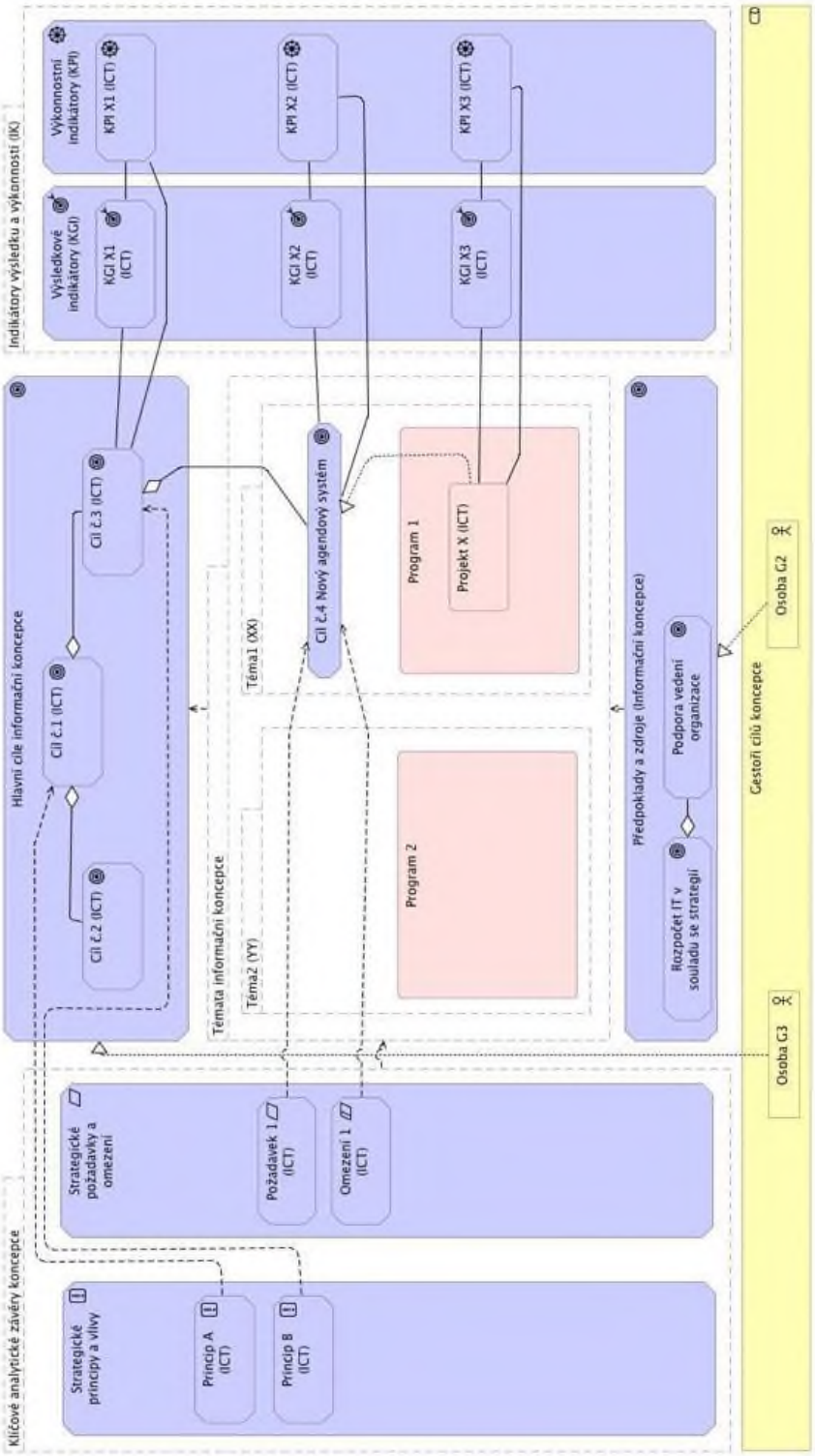
- K naplnění cílů jsou kromě indikátorů definovány témata, programy, projekty a další iniciativy (např. akční plány v podobě souboru úkolů). Na úrovni koncepce by se mělo jednat o několik jednotek klíčových střednědobých až dlouhodobých projektů s dopadem na celou organizaci.
- Mimo diagram, přesto klíčovou informaci, tvoří odpovědnost – přiřazení indikátorů a odpovědnosti za měření / reporting (nejlépe osobám managementu).

6.3.1.2 Dílčí a specifické strategie (2.úroveň strategie)

Dílčí strategie / koncepce jako např. **Informační koncepce** jsou určeny všem členům vedení organizace a těm zaměstnancům, které dílčí strategie přímo nebo nepřímo ovlivňuje. Diagramy určují **vrcholové cíle, prioritních témata (oblastí) a „předpokladové“ cíle** (způsobilost, zdroje), včetně priorit v alokaci zdrojů. Témata je vhodné dekomponovat na cíle a programy, které vedou k jejich naplnění.

2. úroveň strategie obsahuje detailnější rozpracování výše uvedeného 1. úrovně strategie z předchozí kapitoly.

Cíle této dekompozice a zvyšující se agregační úrovně (hloubky) je postupně doplňovat detailní zasazení témat informační koncepce do programu (**viz Program 1 a Program 2**). Přesně identifkovat a pojmenovat konkrétní Strategické principy a vlivy, Strategické požadavky a omezení, Výsledkové indikátory (KGI) a Výkonnostní indikátory (KPI). Všechny tyto čtyři veličiny vstupují a ovlivňují definovaný projekt v rámci programu (Projekt X (ICT)).



Obrázek 23 Dílčí a specifické strategie (2.úroveň strategie), zdroj: metodika DAIN s.r.o.

Důležité je zapracovat (přenést) vrcholové cíle dílčích strategií do celkové strategie organizace (do skupiny témat a „předpokladových“ cílů) tak, **aby byl dvojúrovňový model jako celek konzistentní,** nebo alespoň doplnit vazby mezi cíli obou úrovní.

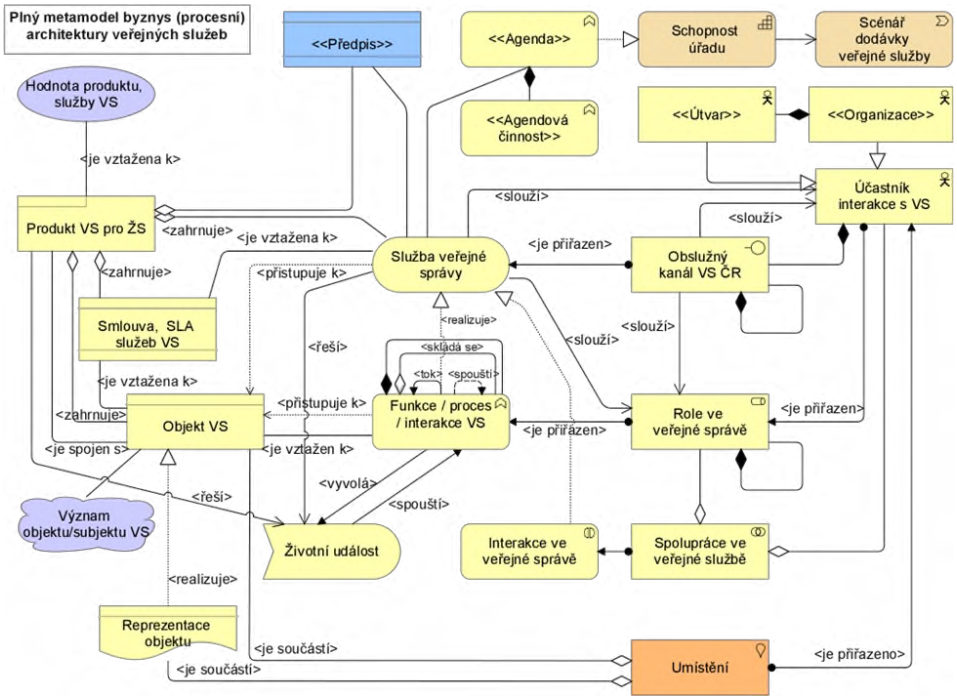
Dílčí strategie se zpracovávají dle požadavku managementu organizace, nicméně některé oblasti jsou nepřímo vyžadovány / regulovány zákony (v případě úřadu). Jedná se například o následující:

- Informační koncepce dle požadavků zákona 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
- Personální strategie, kvalifikace, motivace a zvyšování efektivity.
- Bezpečnostní politika dle požadavků zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Státní energetická koncepce a další oblasti dle potřeby.

Další dílčí strategie je vhodné definovat podle „best-practices“. Poměrně zanedbávanou oblastí je oblast kvality a zvyšování výkonnosti – obecně dosahování excelence.

6.3.2 Metamodel byznys architektury

V rámci této části je definován metamodel organizační architektury, a to jak v plné, tak i redukované verzi a v minimální verzi

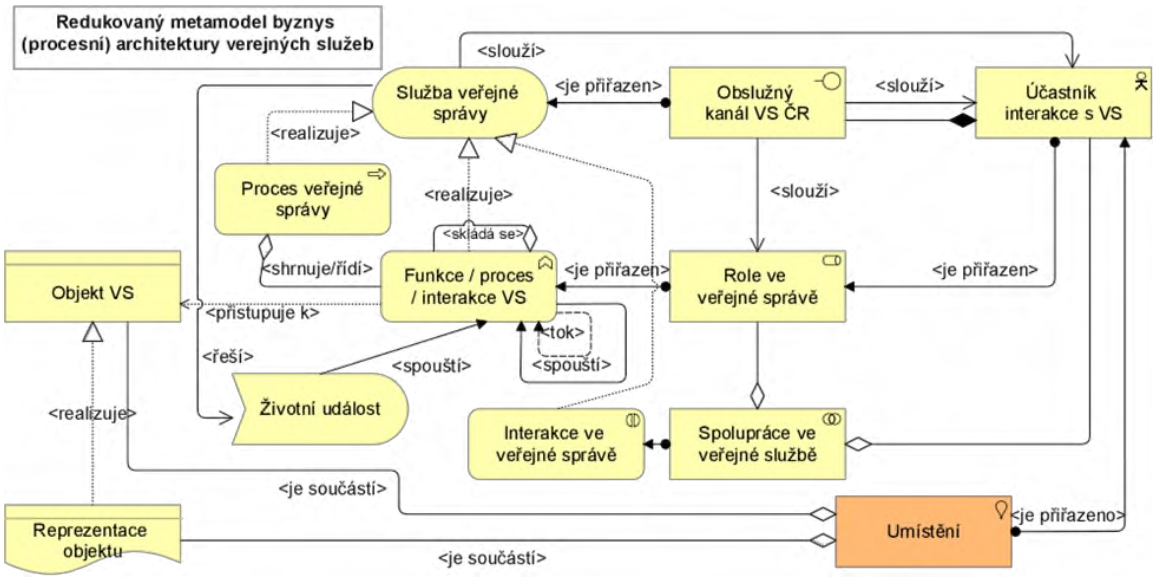


Obrázek 24 Plný metamodel byznys architektury

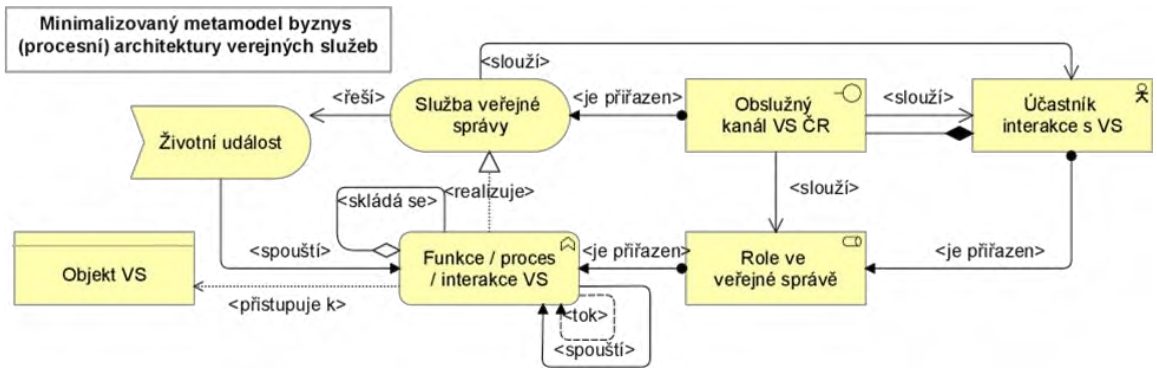
Součástí metamodelu BA, jak je zobrazen, jsou i koncepty metamodelu patřící podle NAR nebo ArchiMate do jiných domén, protože jsou důležitou součástí celkového pohledu na výkon služeb veřejné správy (tj. Byznys). Myslí se tím koncepty:

- ze strategické domény: Schopnost úřadu, Scénář dodávky veřejné služby a Umístění
- z motivační domény: Hodnota produktu/služby VS a Význam objektu VS
- z domény shody s předpisy: Předpis.

Vedle lokalizovaných označení pro VS ČR, například „Účastník interakce s VS“, je možné pro zjednodušení v profesní komunitě vždy používat i originální označení, zde „aktér“. Některé zmíněné pro byznys důležité koncepty byly ve verzi 3.1 ArchiMate přesunuty do jiných domén, proto mají jiné barvy, ale zde jsou i nadále uvedeny.



Obrázek 25 Redukovaný metamodel byznys architektury

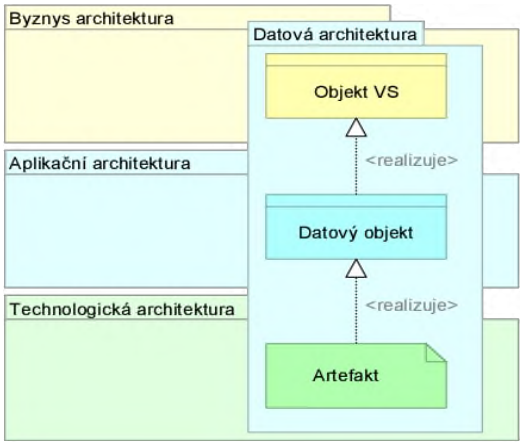


Obrázek 26 Minimalizovaný metamodel byznys architektury

6.3.3 Metamodel architektury IS – informační (datové) architektury (DA)

Datová architektura dle TOGAF v notaci ArchiMate nemá vlastní vrstvu, její objekty jsou rozloženy ve všech třech vrstvách. Představují pasivní prvky, tedy o čem jsou systémy a s čím zachází. Vždy se jedná o tři úrovně abstrakce.

Zatímco datové modelování hovoří o konceptuálních, logických a fyzických datových objektech, TOGAF hovoří o datových entitách, logických a fyzických informačních komponentách, používá ArchiMate následující vyjádření, viz obr. vlevo.



Obrázek 27 Struktura datové architektury

Objekt / subjekt veřejné správy (orig. Business Object) představuje všechny věci, které v prostředí veřejné správy prostě jsou. A některé z nich jsou pro nás zajímavé do té míry, že si o nich vedeme datové záznamy. Objekt v modelu představuje konceptuální úroveň datového modelování.

Datový objekt je logickým obrazem skutečného objektu promítnutého do vrstvy informačních systémů. Vypovídá o struktuře údajů vedených v IS a představuje logickou úroveň datového modelování.

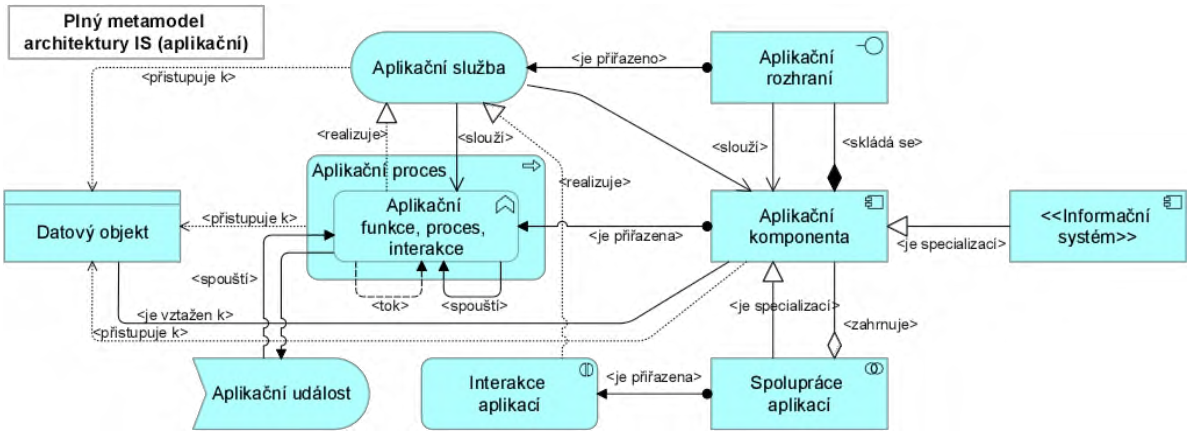
Datový artefakt, tedy soubor, tabulka, záznam na disku je fyzickou reprezentací dat o objektu. Artefakt je také používán jako fyzická reprezentace SW, ať již aplikační komponenty nebo systémového SW.

Datová architektura má pouze pasivní prvky, nemá žádné aktivní ani vlastní kompozitní prvky a ani prvky chování. Může s výhodou využívat kompozitní koncept Seskupení.

6.3.4 Metamodel architektury IS – aplikační architektury (AA)

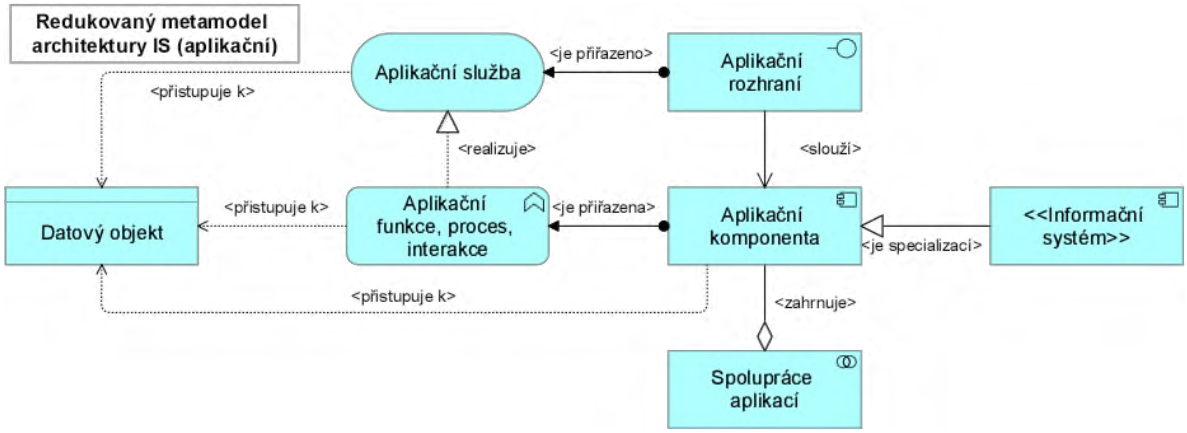
V rámci této části je definován metamodel architektury aplikací a to jak v plné, tak i redukované verzi.

Struktura prvků metamodelu (konceptů) plně odpovídá základním aspektům jazyka ArchiMate, obdobně jako v ostatních základních vrstvách.



Obrázek 28 Plný metamodel architektury IS

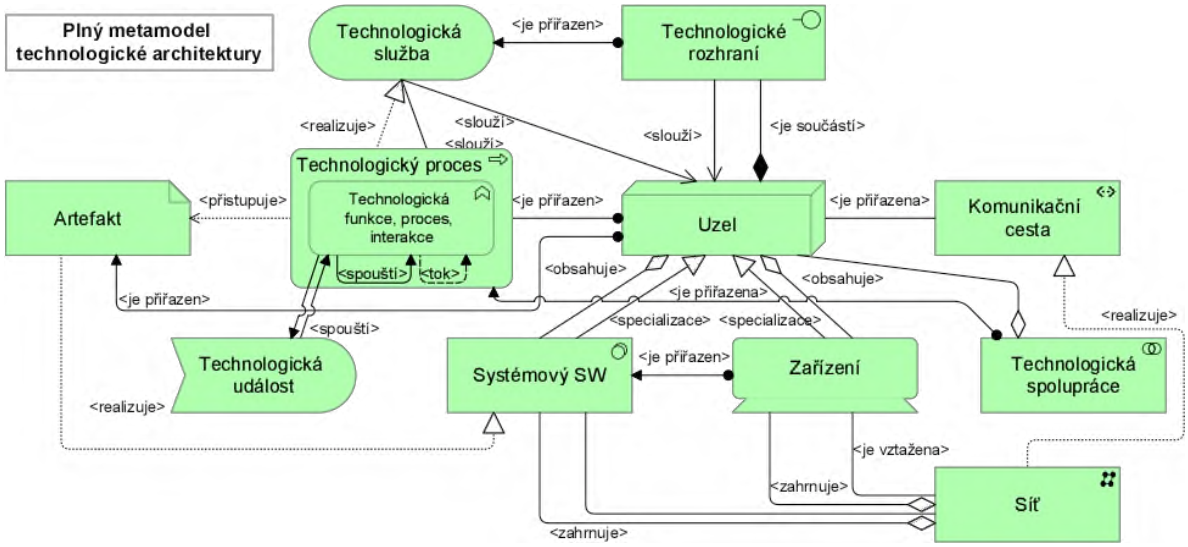
Předpokládáme, že v praxi bude užitečné redukovat, jak počet typů prvků modelů, tak počet typů povolených vazeb. Aktuálně doporučenou redukci metamodelu AA, současně považovanou za minimální možnou, ukazuje následující schéma:



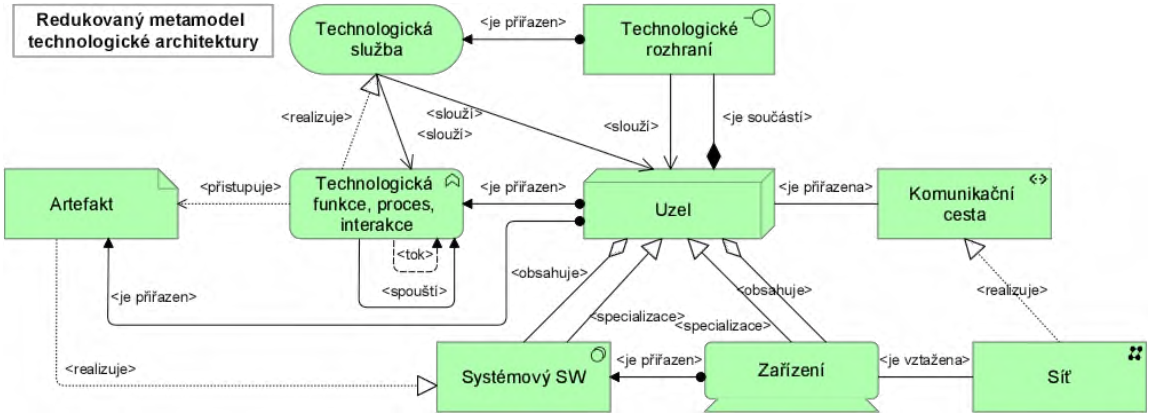
Obrázek 29 Redukovaný metamodel architektury IS

6.3.5 Metamodel ICT technologické architektury – IT infrastruktury (TA)

V rámci této části je definován plný a zjednodušený metamodel technologické architektury.



Obrázek 30 Plný metamodel technologické architektury

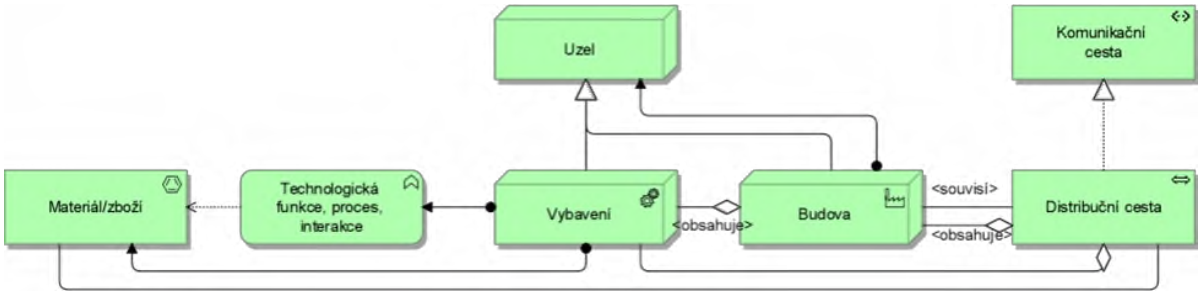


Obrázek 31 Redukovaný metamodel technologické architektury

6.3.6 Metamodel komunikační a fyzické infrastruktury (KI)

Metamodel komunikační infrastruktury je totožný jako metamodel jakékoli ostatní ICT technologické infrastruktury. V architektonických výstupech bude převážně představovat samostatný pohled nebo bude součástí pohledu čtyřvrstvé architektury eGovernmentu.

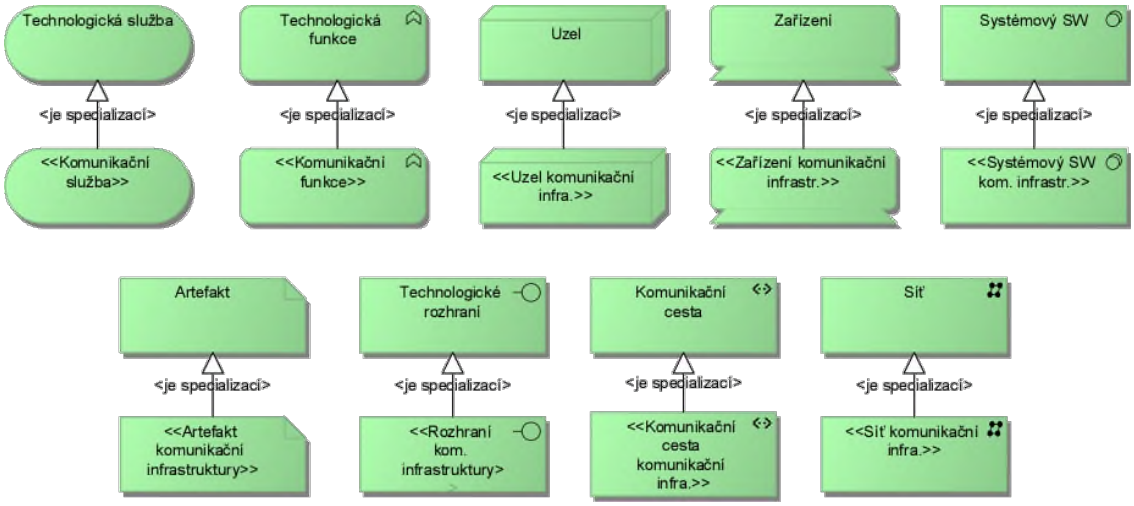
Po rozšíření standardu ArchiMate o prvky fyzického světa (non-IT) jsou tyto prvky součástí této architektonické domény NAR, neboť velmi blízce odpovídající jejímu původnímu účelu v rámci vize čtyřvrstvé architektury.



Obrázek 32 Metamodel fyzické architektury

6.3.6.1 Specializace prvků metamodelu komunikační infrastruktury

Pokud bude potřeba zdůraznit na úrovni metamodelu odlišnost komunikační infrastruktury, budou moci být všechny použité koncepty metamodelu tzv. specializovány, viz obr. níže.



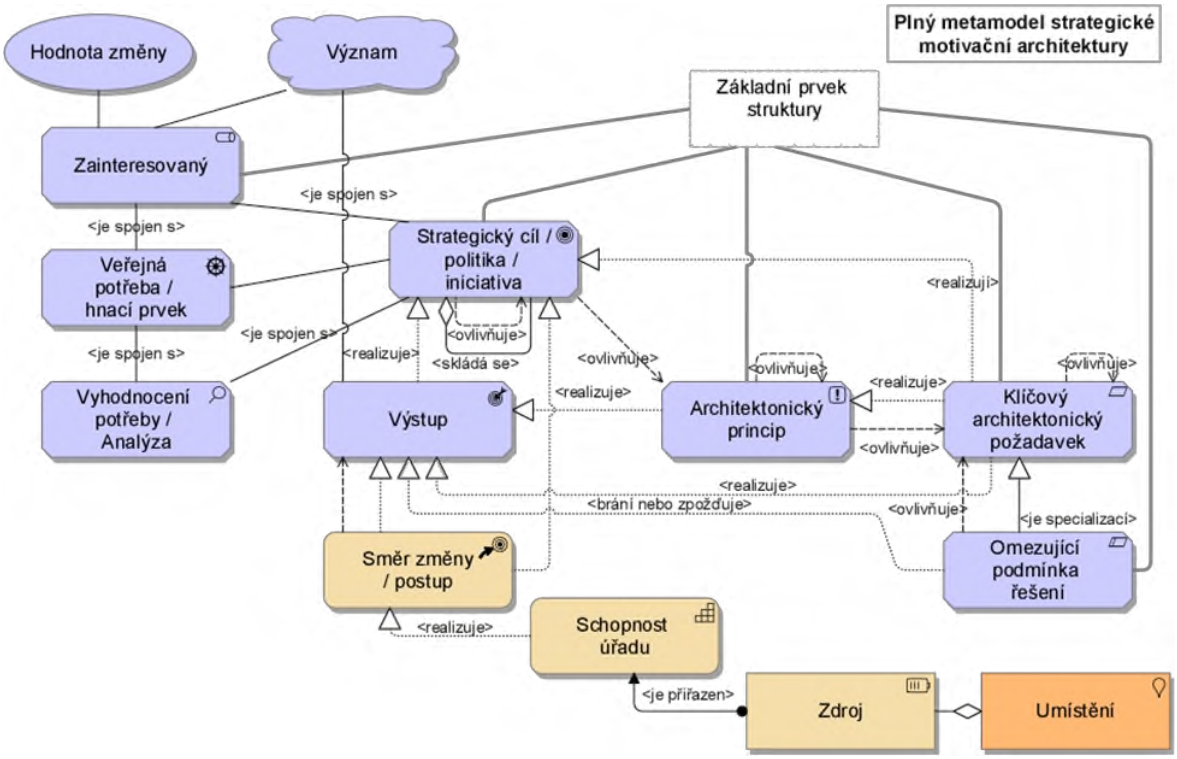
Obrázek 33 Prvky metamodelu komunikační infrastruktury

Pro běžné použití ve zde výše uvedených typech angažmá se ale specializace pro prvky technologické infrastruktury nepředpokládá a nevyžaduje.

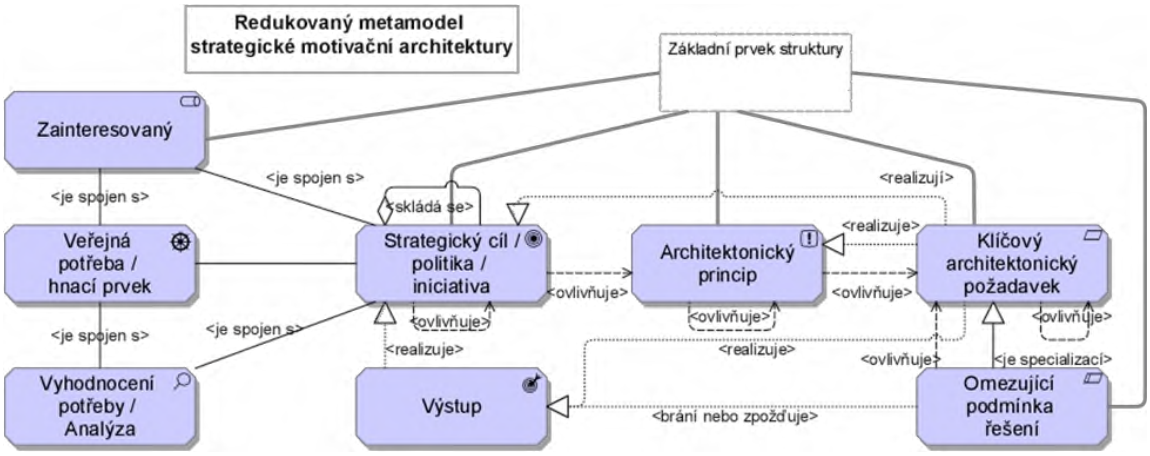
6.3.7 Metamodel architektury strategie a směřování (MA)

Strategická architektura dle NAR je první, nejdůležitější a aktuálně nejobsažnější doménou z oblasti jednotlivých motivačních architektur – vertikálních domén.

Spojuje v sobě motivační architekturu dle TOGAF13) a tzv. motivační a strategickou14) vrstvu dle ArchiMate. To je důvodem, proč jsou v metamodelu domény strategické a směřování v NAR kombinovány prvky více barev.



Obrázek 34 Plný metamodel strategické motivační architektury



Obrázek 35 Redukovaný metamodel strategické motivační architektury

Metamodel neobsahuje všechny možné vazby, protože každý prvek v motivačním rozlišení může být agregací/specializací prvku stejného typu (např. cíl se může agregovat na dílčí cíle).

6.3.8 Metamodel výkonnostní architektury (PA)

Výkonnostní architektura NA VS ČR zatím nemá definované žádné specifické prvky metamodelu. Předpokládáme, že v následujících verzích jazyka ArchiMate se objeví volnější použití objektu Metrika

(KGI, KPI) (zejména TCO), PPI20), než je tomu v současnosti jakožto měřítko výsledku vyhodnocení potřeby, motivátoru, v motivační architektuře.

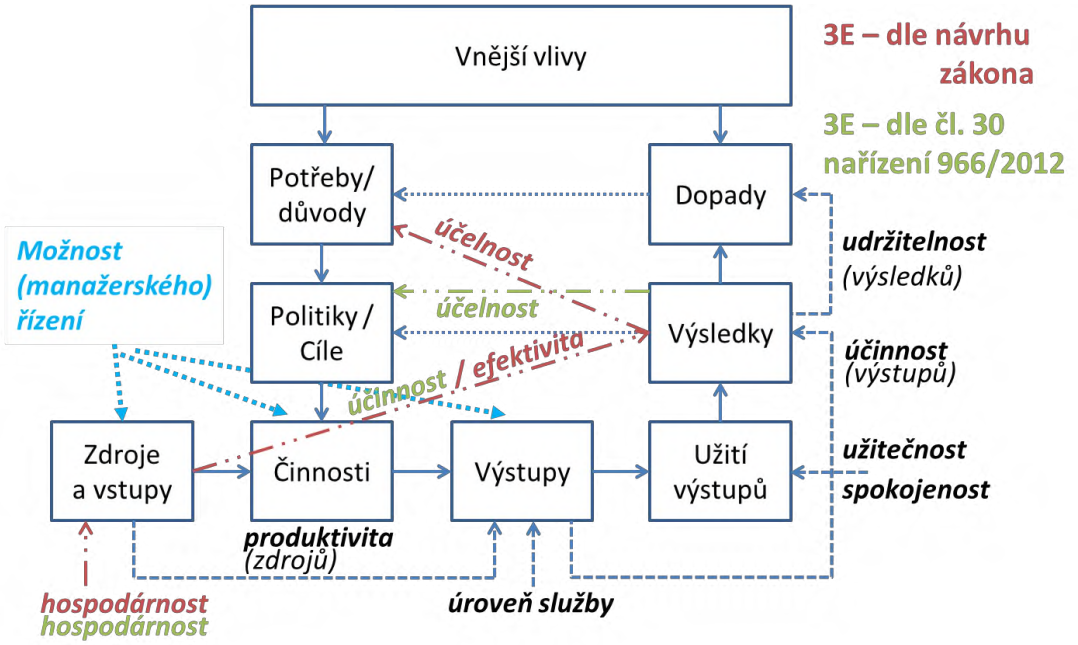
Doposud každý objekt modelu může mít metriky přiřazeny v profilu atributů. Typy ukazatelů výkonnosti se zatím nemodelují.

Architektura výkonnosti, kvality a zodpovědnosti by měla sloužit na podporu řízení výkonnosti, kvality a zodpovědnosti v orgánech veřejné správy. Řízení výkonnosti, kvality a zodpovědnosti ve veřejné správě je spojeno zejména se snahou organizace dělat správné věci správně, tj. kvalitně, efektivně, hospodárně a včas.

Základní tři sady ukazatelů se obvykle ukrývají pod akronymem 3E:

- **Hospodárnost (Economy)** – vztahuje se k nákladům na zdroje pro spotřebovávané vstupy. Metriky hospodárnost se používají k posouzení, zda za pořízení nezbytných zdrojů je placena odpovídající cena.
- **Účinnost (Efficiency)** – účinnost představuje vztah mezi vstupy a výstupy, je poměrem dosažených výstupů ke spotřebovaným vstupům. Účinnost je výrazem dimenze „dělat věci správně“ a ukazuje na výkonnost ve smyslu způsobu, jakým je činnost uskutečňována.
- **Účelnost (Effectiveness)** – je výrazem míry jakou produkované výstupy vedou k očekávaným výsledkům. Metriky účelnosti se zaměřují na sílu vztahu mezi provedenou intervencí a dosaženým výsledkem. Účelnost je výrazem dimenze „dělat správné věci“ a ukazuje na výkonnost ve smyslu volby činnosti, která je uskutečňována.

S tím souvisí i tzv. Logický model řízení výkonnosti, vypracovaný na základě podkladů Evropského účetního dvora a MF ČR:

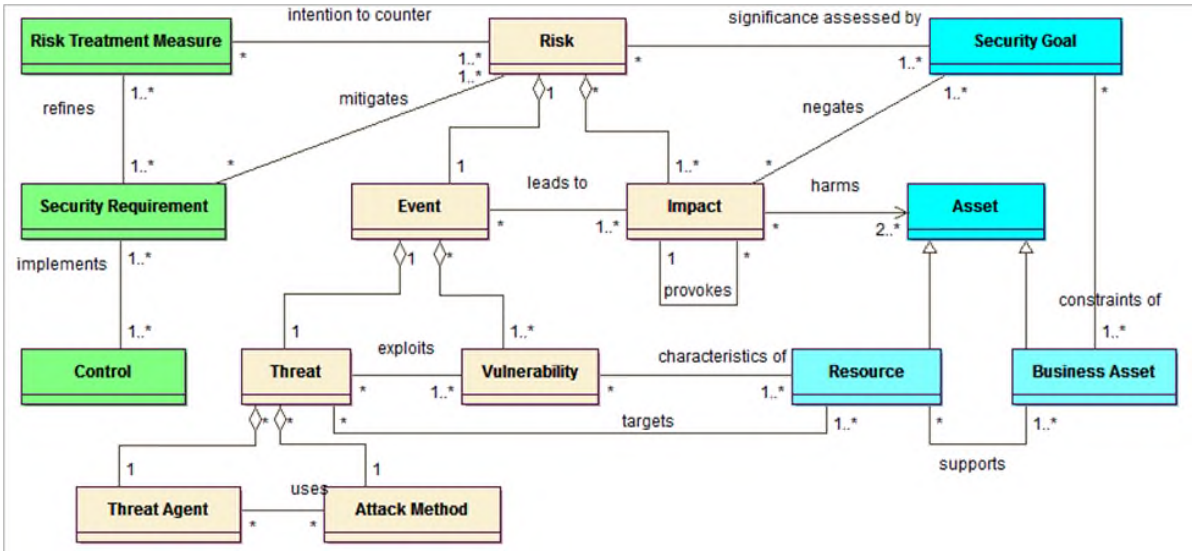


Obrázek 36 Metamodel výkonnostní architektury

Pro řízení výkonnosti, kvality a zodpovědnosti platí obdobné paradigma jako níže u bezpečnosti:
Není možné řídit výkonnost a kvalitu prvků systému úřadu a zodpovědnost za ně, bez toho, že bychom je dobře poznali a porozuměli jim, například prostřednictvím architektury úřadu.
Doména výkonnosti k základním objektům architektury úřadu přidává několik specifických prvků (cílů, ukazatelů, vyhodnocení, opatření). Ty jsou do značné míry modelovatelné pomocí konceptů byznys a motivační architektury, jejich specializací nebo do budoucna samostatných specifických konceptů, obdobně jako u bezpečnostní architektury.

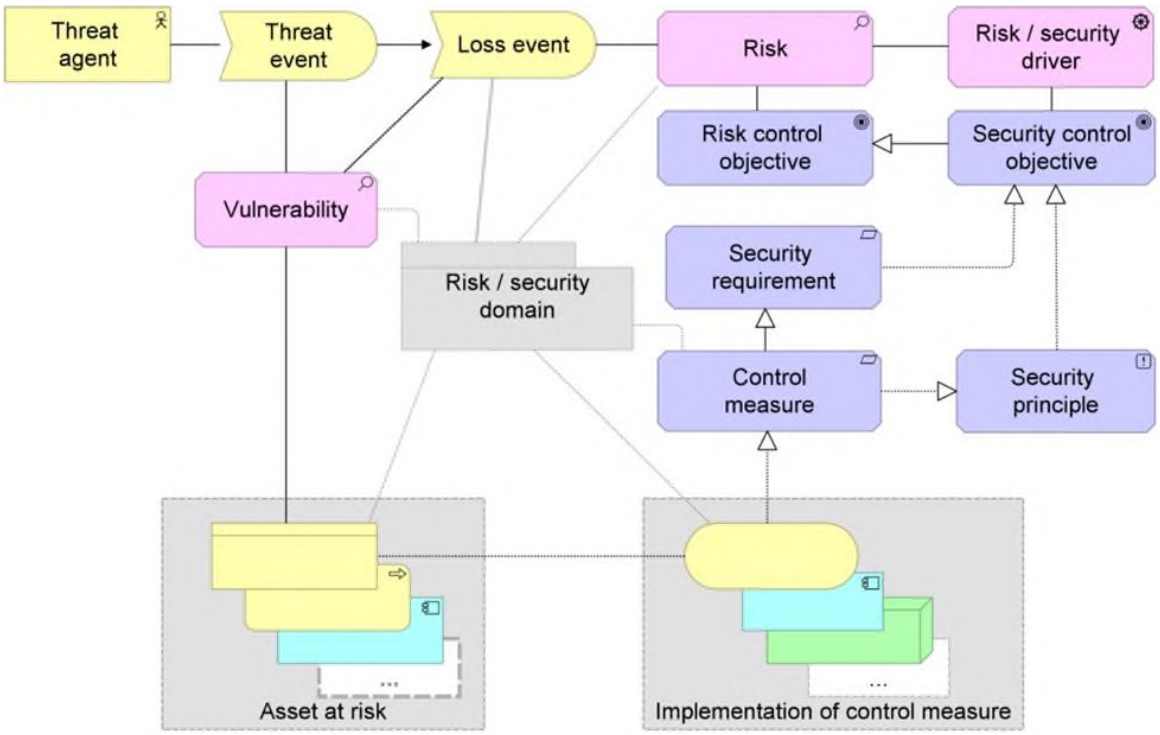
6.3.9 Metamodel bezpečnostní architektury (SA)

Bezpečnostní architektura NA VS ČR zatím nemá definované žádné specifické prvky metamodelu. Předpokládáme, že jimi budou později rizika a opatření spojená s hlavními objekty modelu.
Lze předpokládat podle Whitepaperu The Open Group a vývoje některých modelovacích nástrojů, že jazyk ArchiMate a standard TOGAF v budoucnu přidá tyto koncepty.



Obrázek 37 Metamodel bezpečnostní architektury (SA)

Specifické koncepty bezpečnosti a řízení rizik se dají v aktuálním standardu ArchiMate modelovat s pomocí konceptů byznys a motivační architektury nebo jejich specializovaných stereotypů, viz schéma:



Obrázek 38 Příklad ArchiMate modelu

Diagram mimo jiné zdůrazňuje základní princip bezpečnostní architektury:
Vše, co je součástí systému organizace a co modelujeme v ostatních doménách, může být ohroženo a je potřeba to chránit, ale současně téměř vše z toho je současně pro jiné věci prostředkem takové ochrany.
Z toho také plyne, že dobrý model základních prvků architektury úřadu je nezbytným předpokladem a vstupem její bezpečnostní architektury.

6.3.10 Metamodel architektury standardizace, shody s předpisy a udržitelnosti

Oblast standardizace a udržitelnosti NA VS ČR zatím nemá v mezinárodních standardech definované žádné specifické prvky metamodelu. Předpokládáme, že dle potřeb budou využity specializované prvky byznys a motivační architektury, ve smyslu cílů, požadavků či omezujících podmínek.
Vedle toho bude obsah standardizace vyjadřován prohlášením každého jednotlivého prvku architektury nebo jejich kombinace za architektonický stavební blok (ABB), za stavební blok řešení (SBB) nebo za architektonický vzor (pattern).
Tato doména se v souladu se svým názvem zaměřuje na oblasti řízení, které regulují činnost úřadů (OVS), a to konkrétně:

- **Shoda s předpisy;** Podle Ústavy a ZLPS smí veřejné správy v oblasti výkonu veřejné moci konat jenom to, co je jí výslovně předepsáno zákonem, respektive podzákonnými předpisy.

- **Standardizace;** Veřejná správa omezuje prostor pro samostatné rozhodování, a tím i komplexitu svého prostředí tím, že „dobrovolně“ vydává standardy (procesů, IT, služeb, bezpečnosti apod.) nebo přebírá nezávislé externí standardy (ISO, ČSN apod.).
- **Udržitelnost;** Veřejná správa si pro oblasti své regulace (agendy) i pro svoji vlastní organizaci a interní činnosti stanovuje kritéria (limity) udržitelnosti, a to v oblasti ekonomické, sociální a environmentální. Typickou iniciativou v této oblasti je CSR.

Základním objektem shody s předpisy je objekt „právní předpis“. Tento objekt není standardní součástí specifikace ArchiMate, proto NAR navrhuje používat specializaci objektu „Kontrakt“ do podoby: «Předpis». Vše ostatní, co tvoří strukturu systému úřadu, musí být ve shodě s právními předpisy. Pokud by tomu tak nebylo, jde o nežádoucí stav. Míru shody není třeba vyjadřovat dalšími koncepty, v rámci NAR stačí objekty modelu, typicky agendy nebo služby, propojit asociační vazbou s objekty «předpis», viz následující obrázek:

Obrázek 39 <<Předpis>>

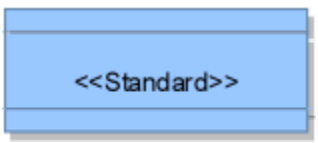
Objekty předpis mohou být libovolně specializovány/agregovány, přes dílčí úrovně předpisu: článek, paragraf, odstavec, písmeno. Jinou specializací je struktura předpisů nižší právní síly (prováděcí právní předpisy, podzákonné právní normy či sekundární právní předpisy), tj. typicky vyhlášky a metodické pokyny. Pro tyto druhy specializace obsahu konceptu «předpis» je v této verzi NAR nežádoucí vytvářet další stereotypy.

6.3.10.1 Metamodel architektury standardizace

V oblasti standardizace se vyskytují standardy dvou typů:

- **Standard jako dokument,** který vyjadřuje vůli signatářů (autorů standardu) definovat a užívat některé „věci“ jednotně stejně.
- **Prohlášený standard,** který vzniká tak, že nějakou existující věc (typicky typ výrobku, formát dat apod.) z modelu své vlastní architektury prohlásím standardem.

V metamodelu architektury standardizace je potřebné zachytit jediný nový prvek, a to objekt představující obraz standardizačního dokumentu, například ISO 27000. Pro takovéto objekty navrhuje NAR také specializaci konceptu jazyka ArchiMate „kontrakt“ do podoby «standard», viz následující obrázek:



Obrázek 40 <<Standard>>

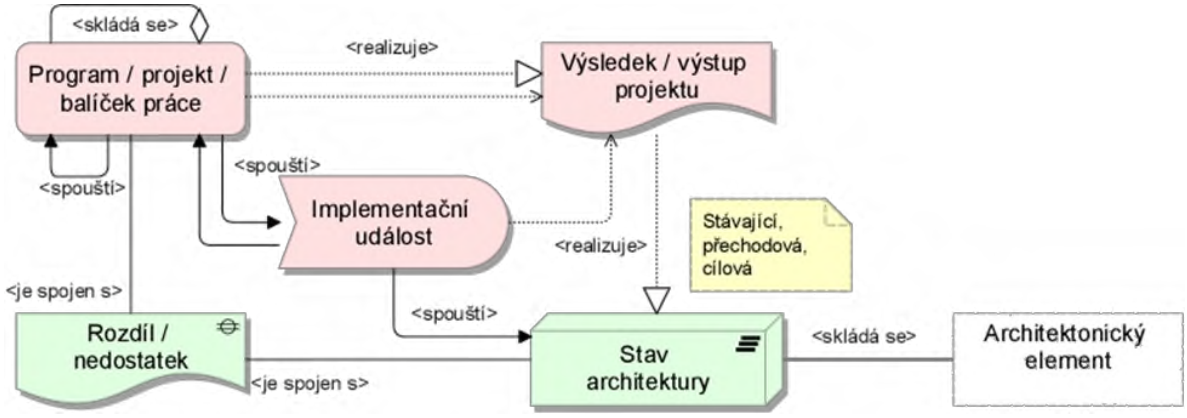
6.3.10.2 Metamodel architektury dlouhodobé udržitelnosti

Architektura dlouhodobé udržitelnosti pro NA VS ČR zatím nemá definované žádné specifické prvky metamodelu. Předpokládáme, že v následujících verzích jazyka ArchiMate se objeví volnější použití objektu Metrika (KPI) než je tomu v současnosti jakožto měřítko výsledku vyhodnocení potřeby, motivátoru, v motivační architektuře. Předpokládáme, že Metrika bude vhodným konceptem i pro architekturu dlouhodobé udržitelnost.

Dalšími vhodnými atributy mohou být například Architektonický princip, Architektonický požadavek nebo Omezující podmínka, případně jejich specializované stereotypy.

6.3.11 Metamodel architektury implementace a migrace

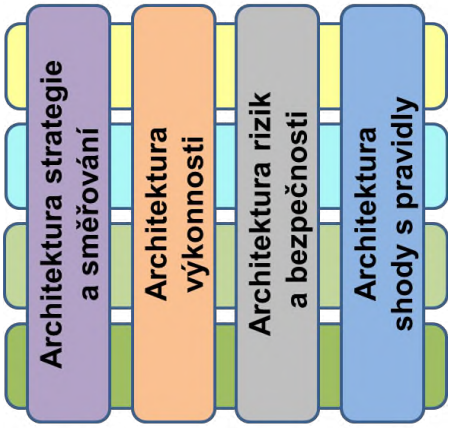
Na obrázku níže je znázorněn metamodel implementačního a migračního rozšíření.



Obrázek 41 Metamodel implementačního a migračního rozšíření

6.3.12 Metamodely vertikálních domén NAVSČR

Architektura vertikálních domén definovaných na Obrázek 14: Rozvržení domén obsahu architektonického rámce NA VS ČR zatím nemá definované žádné specifické prvky metamodelu.



Obrázek 42 Vertikální domény architektury NA VSČR, zdroj: NA VSČR

Vertikální domény představují všechny formy (složky) motivace organizace ke konání veřejné služby a k její změně. Jsou to:

- **Strategie a směrování** – Kam chceme jít? - jaké politiky si úřad naplánoval a proč
- **Výkonnost** – Jak dobří chceme být v tom, co děláme? – jaká máme měřítka výkonnosti a Jakosti
- **Rizika a bezpečnost** – Čeho se chceme vyvarovat a jak se proti tomu bráníme?
- **Shoda s pravidly** – Jaká pravidla jsme si pro svou cestu stanovili (či nám byla dána)?

Tyto vertikální domény vycházejí z NA VS ČR a nic nebrání jejímu využití i pro potřeby rezortu Zdravotnictví. Uvedené metamodely níže vycházejí z konzultací s MV OHA a rozšiřují tedy výše uvedené základní schéma vertikálních domén.

MVČR předpokládalo (předpoklad z roku 2024 z doby platného standardu ArchiMate verze 3.1), že v následujících verzích jazyka ArchiMate se objeví volnější použití objektu Metrika (KPI), než je tomu v současnosti jakožto měřítko výsledku vyhodnocení potřeby, motivátoru, v motivační architektuře. Doposud každý objekt modelu může mít metriky přiřazeny v profilu atributů. Typy ukazatelů výkonnosti se zatím nemodelují.

Bezpečnostní architektura NA VS ČR zatím nemá definované žádné specifické prvky metamodelu. MVČR předpokládalo (předpoklad z doby platného standardu ArchiMate verze 3.1), že jimi budou později rizika a opatření spojená s hlavními objekty modelu.

Oblast standardizace a udržitelnosti NA VS ČR zatím nemá definované žádné specifické prvky metamodelu. MVČR předpokládalo (předpoklad z doby platného standardu ArchiMate verze 3.1), že dle potřeb to budou specializované prvky motivační architektury, ve smyslu cílů, požadavků či omezujících podmínek.

Za stavu, že **nejsou definovány** metamodely vertikálních domén NAR VS **ČR a reálné potřebě vytvářet** tyto průřezové individuální pohledy pro zainteresované osoby na strategické, výkonnostní a bezpečnostní prvky architektury. Dávat je do shody s platnými pravidly, zákony a vyhláškami, které mají významné dopady právě na architekturu organizace, si resort zdravotnictví definuje vlastní patterny (vzory) vertikálních domén.

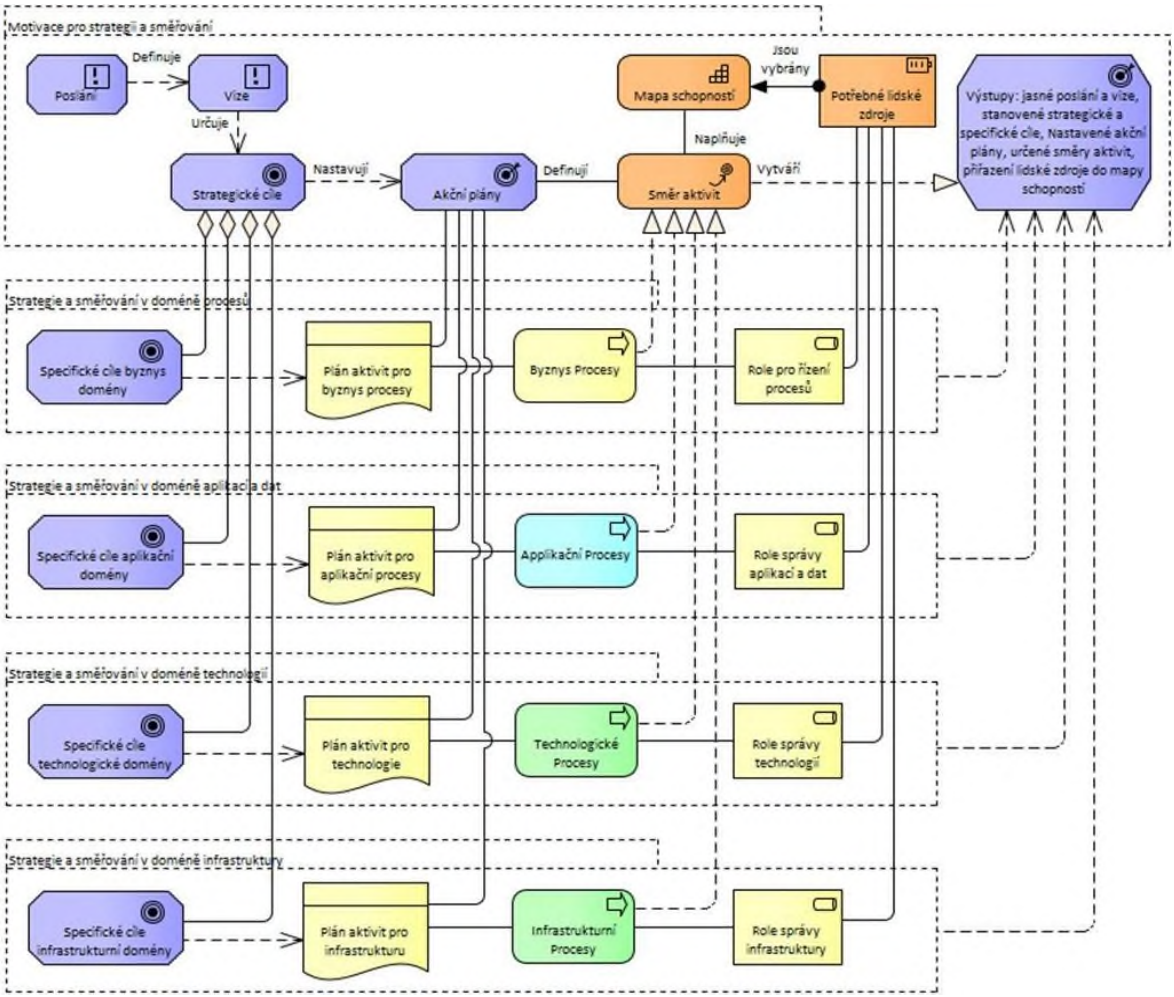
Navrhované patterny budou praxí a užíváním v resortu zdravotnictví postupně zpřesňovány a mohou se v budoucnu transformovat na závazné metamodely vertikálních domén architektury zdravotnictví a přispět tak i k definici obecných cílových metamodelů vertikálních domén NA VSČR.

6.3.12.1 Vzor pro budoucí metamodel architektury strategie a směřování (DSS)

Tento návrhový vzor si klade otázky: Jaké poslání a jakou vizi máme? Jaké strategické a na ně navázané specifické cíle jsou určeny? Jaké dílčí byznys, aplikační, technologické a infrastrukturní plány aktivit máme popsány? Jaké byznys, aplikační, technologické a infrastrukturní procesy tvoří společně provázané aktivity v akčních plánech? Definují akční plány, potřebný směr aktivit pro naplnění společné

mapy schopností? Jaké lidské zdroje a jejich vlastnosti jsou vybrány pro pokrytí jednotlivých schopností? Jsou popsány role požadovaných lidských zdrojů a způsob jejich zapojení do procesů řízení a správy, a to na všech úrovních architektury? Jak je vyhodnocováno dosahování jednotlivých specifických a strategických cílů strategie ve všech doménách architektury?

Návrh obsahuje jasné poslání a vizi, stanovené strategické a specifické cíle, nastavené akční plány, určené směry aktivit, definované potřebné lidské zdroje a schopnosti, které mají mít pro zajištění provozu a rozvoje architektury v resortu zdravotnictví.



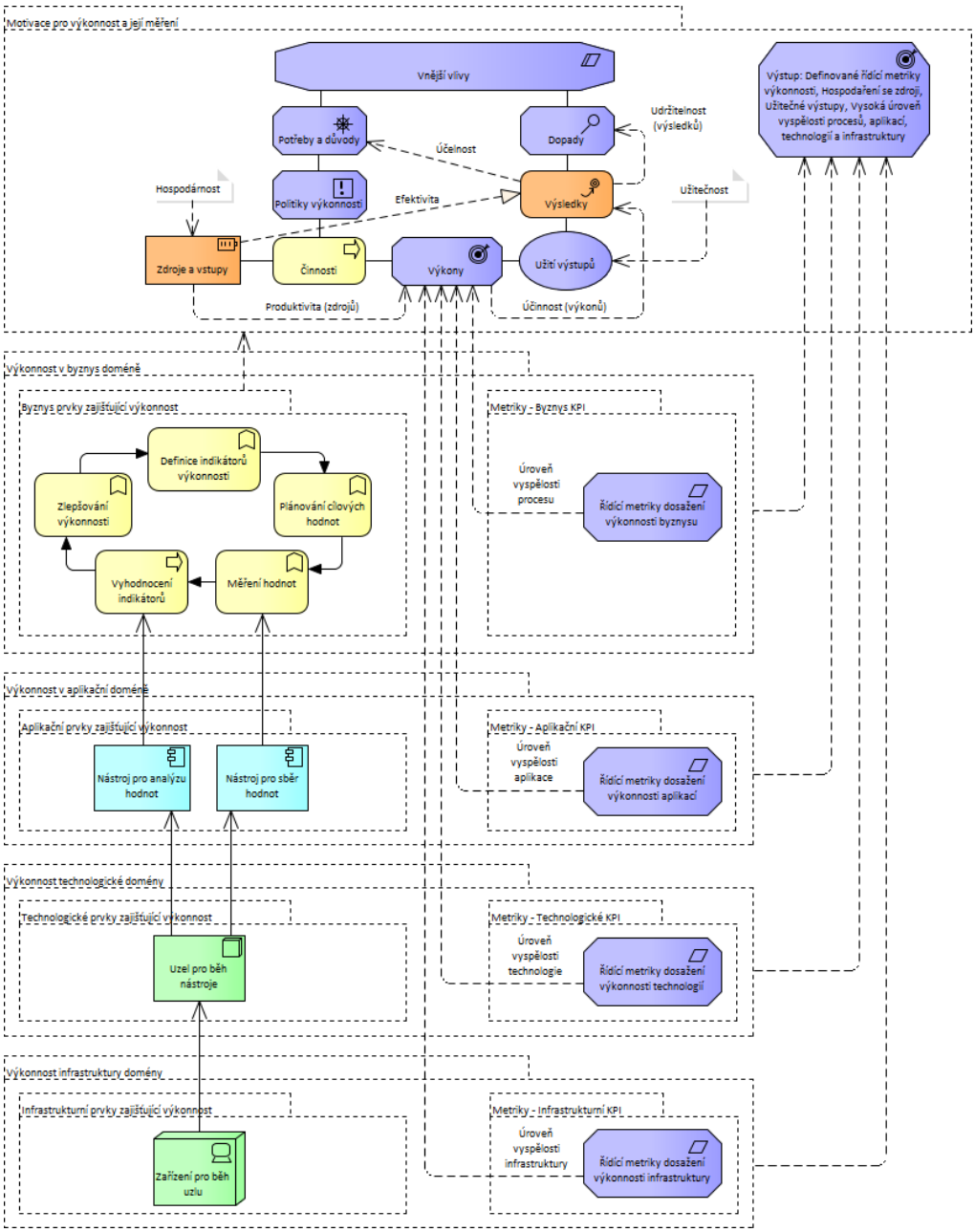
Obrázek 43 Vzor pro budoucí metamodel architektury strategie a směřování (DSS), Zdroj: Asseco CE, a.s.,

6.3.12.2 Vzor pro budoucí metamodel architektury výkonnosti a kvality (DVK)

Tento návrhový vzor si klade otázky: Jak řídíme zdroje, činnosti a výkony? Jaká je produktivita našich zdrojů? Jaká je účinnost našich výkonů? Jaká je udržitelnost našich výsledků? Které řídící metriky výkonnosti máme definovány? Jak je měřena úroveň vyspělosti procesů, aplikací, technologií a

infrastruktury? Jaké prvky byly navrženy pro zajišťování výkonnosti? A to vše ve všech doménách architektury.

Návrh obsahuje definice pro řídící metriky výkonnosti, hospodaření se zdroji, soupis potřeb, politik, dopadů a využitelných výstupů, změřitelnou úroveň vyspělosti procesů, aplikací, technologií a infrastruktury tvořící výkonné služby v resortu zdravotnictví.



Obrázek 44 Vzor pro budoucí metamodel architektury výkonnosti a kvality (DVK), Zdroj: Asseco CE, a.s.,