DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

Metody řízení ICT veřejné správy ČR

Úvod

Součástí a zároveň klíčovým předpokladem splnění cílů Informační koncepce České republiky[1)] (také jako “IKČR” nebo "Informační koncepce ČR") je zavedení efektivní centrální koordinace řízení ICT a jeho podpory transformačních iniciativ směrem k digitalizaci VS a plnému eGovernmentu. To bude možné pouze díky koordinovanému úsilí o uvedení lokálních IK jednotlivých OVS do souladu s cíli, principy a zásadami IKČR[2)]. Dokument „Metody řízení ICT veřejné správy ČR“ (také jako „MŘICT“) upravuje rámec pravidel pro centrální koordinované řízení ICT podpory eGovernmentu, řízení jeho legislativních změn, budování a provozování ICT kapacit a kompetencí státních podniků a agentur, řízení útvarů informatiky v jednotlivých OVS i řízení životního cyklu jednotlivých ISVS a dalších IS ve veřejné správě. Rozpracovává a navazuje na zásady řízení ICT uvedené v IKČR, jejíž je nedílnou obsahovou součástí.

Pro usnadnění využití je dokument maximálně zestručněn, podrobnější rozpracování jednotlivých témat je obsaženo v jeho dodatcích a přílohách, publikovaných prostřednictvím tzv. Znalostní báze[3)].

Na dokument MŘICT bude dále navazovat řada legislativních a metodických dokumentů, týkajících se jednotlivých disciplín řízení ICT, například řízení změn, projektového řízení, řízení hospodárnosti zdrojů a vyhodnocování TCO v IT apod.

Vznik MŘICT je dán usnesením vlády ze dne 3. října 2018 č. 629, jako následný dokument ke schválené IKČR[4)], která je součástí programu „Digitální Česko“. Mezi další následné dokumenty Informační koncepce ČR patří také: Slovník pojmů eGovernmentu, Národní architektonický rámec a Národní architektonický plán.

Tento dokument je zároveň výstupem záměru č. 488[5)] v rámci dílčího cíle IKČR 5.01 schváleného[6)] implementačního plánu hlavního cíle č. 5 Informační koncepce ČR „Efektivní a centrálně koordinované ICT veřejné správy“ pro rok 2019 programu „Digitální Česko“.

Účel dokumentu

Komu je dokument určen. Cílovou skupinou MŘICT jsou **řídící pracovníci jednotlivých orgánů veřejné správy** (OVS, viz níže)**, zodpovědní za řízení ICT útvarů jejich úřadů (CIO ICT).**

Co jsou hlavní přínosy dokumentu. MŘICT jako takový definuje celkový přístup k systému řízení ICT ve veřejné správě ČR. Současně svou navazující Znalostní bází (de-facto jako prováděcím manuálem IKČR) stanovuje konkrétní, přímo aplikovatelné kroky, které jsou nutné pro plnění principů a zásad obsažených v IKČR. Tyto kroky prezentuje:

- **s respektem ke specifikům daným charakterem úřadu**, tzn., zohledňuje, zda jde o úřad státní správy nebo samosprávy[7)],
- **včetně odkazů na aktuálně platná legislativní omezení** těchto kroků.

Jaké je zmocnění k dokumentu. IKČR, vydaná 3. října 2018, definuje základní požadavky na řízení a rozvoj orgánů veřejné správy a jejich útvarů informatiky tak, aby byly schopny naplňovat cíle rozvoje služeb informačních systémů veřejné správy, řídit jejich životní cyklus a zlepšovat se, a zároveň jim ukládá povinnost vytvářet svou informační koncepci podle IKČR a jejích příloh, když stanovuje:

- **cíle České republiky** v oblasti informačních systémů veřejné správy (také jako "ISVS") **a**
- **obecné principy** pořizování, vytváření, správy a provozování informačních systémů veřejné správy v České republice.

Proč dokument přečíst. Dokument je formulován jako komplexní rukověť (kompendium), tj. obsahuje nejen konkrétní recepty, ale i žádoucí rámcové předpoklady: např. organizační uspořádání, technologické vybavení a personální složení, ale i potřebné nastavení kompetenčního rozhraní vůči vedení úřadu, svým klientům = útvarům zajišťujícím výkon agend VS, i vůči ostatním podpůrným útvarům. Ale zejména:

- poskytuje argumentaci pro získání potřebné podpory ze strany vedení,
- obsahuje přehled klíčových rizik role CIO ICT, včetně doporučení, jak tato rizika eliminovat,
- obsahuje ucelený, navzájem provázaný přehled nejlepších, osvědčených postupů a praxí řízení ICT VS,
- nabízí řadu připravených formulářů a pomůcek, například pro efektivní sběr požadavků, nebo pro tvorbu nejčastějších dokumentů a reportů,
- umožní při využití metodiky a jejích následných příloh uvnitř organizace v rámci spravovaného útvaru zajistit lepší koordinaci vůči ostatním úřadům, především při sdílení služeb.

Jak je doporučeno s dokumentem pracovat. Je doporučeno se v dokumentu nejprve zorientovat, pochopit a přijmout zde navrhovanou strukturu systému řízení ICT úřadu a seznámit se s přehledem nabízených metod řízení. Následně má být postupováno současně cestou implementace systému řízení do organizace, viz postup a plán realizace změn, a současně dokument slouží, společně se Znalostní bází, jako zásobárna znalostí a pomůcek pro situace, kdy bude potřebné jich využít.

Působnost MŘICT

IKČR je závazná pro všechny státní orgány a orgány územních samosprávných celků (také jako „úřady“[8]) – ty, včetně veřejnoprávních korporací, tvořených vedle nich samotných i jimi zřizovanými příspěvkovými a obchodními organizacemi, dle § 1 odst. 1 zákona o ISVS souhrnně označuje pojmem orgány veřejné správy (také jako „OVS“). MŘICT jsou návazným dokumentem IKČR, který rozvíjí principy, zásady a cíle v ní vedené a **pro úřady je závazný** v míře dodržování principů, zásad a cílů IKČR.

Zároveň ale, protože pro oblast samosprávy platí některé odlišnosti dané definicí samosprávy[9], je odlišné i uplatnění dokumentu **MŘICT** v orgánech územně samosprávných celků. Tomu bude postupně přizpůsobován jak obsah dalších vydání MŘICT, tak zejména detailní materiály ve Znalostní bázi.

Pro ostatní orgány veřejné moci (také jako „OVM“), které nejsou OVS (například školy nebo nemocnice) sice IKČR (a tedy ani její přílohy včetně MŘICT) závazné nejsou, ale i jim může jejich využívání přinést řadu výhod, tzn. je jim využití doporučeno.

V organizacích veřejné správy je MŘICT doporučený pro řízení veškeré ICT podpory činností úřadu, nikoli jenom pro tu část, která je formálně svěřena IT útvaru. Jinými slovy, v souladu s tímto dokumentem musí tyto organizace řídit i správu IT řešení, kompletně spravovaných externími dodavateli a také IT (HW, SW) prvků, nacházející se a spravovaných kdekoli v OVS, typicky v odborných nebo provozních útvarech (tzv. „stínové“, nebo „šedé[10]“ IT).

Podstatné je, že veškeré řízení dodávek ICT služeb na podporu všech funkcí OVS musí být svěřeno pod jednu nedělitelnou a z pohledu OVS centrální zodpovědnost a kontrolu, která bude ICT úřadu spravovat v souladu s MŘICT.

Struktura dokumentu

1. Kapitola "Úvod" představuje východiska pro formulování v koncepci dále uvedených pravidel.
2. Kapitola "Současný a cílový stav řízení ICT" shrnuje stručnou charakteristiku stávajícího stavu informatiky ve veřejné správě ČR, motivaci ke změnám, hlavní očekávané změny a způsob popisu cílového stavu.
3. Kapitola "Předpoklady a východiska řízení ICT" shrnuje klíčové předpoklady a východiska, za který se řízení ICT úřadu odehrává.
4. Kapitola "Řízení jednotlivých ICT řešení" popisuje nezbytné minimální postupy a schopnosti úřadů a jejich

útvarů informatiky při návrhu, budování, provozu a rozvoji nebo ukončení jednotlivých IS.
5. Kapitola "Řízení na úrovni útvaru ICT" se zaměřuje na klíčové činnosti a kompetence útvaru ICT pro zabezpečení rozvoje jednotlivých IS v celém jejich životním cyklu v souladu s architekturou úřadu a architekturou eGovernmentu ČR.
6. Kapitola "Spolupráce s ostatními útvary úřadu a eGovernmentu" představuje klíčové přesahy řízení informatiky a ostatních manažerských disciplín úřadu, zde zejména odkazy a základní pravidla z oblasti řízení bezpečnosti úřadu a ochrany informací a provozních útvarů úřadu.
7. Kapitola "Postup a plán realizace změn" obsahuje přehled úkolů, které musí být splněny, aby se MŘICT naplnily, analýzu klíčových implementačních rizik koncepce, návrh způsobu monitoringu postupu plnění úkolů koncepce a zásady vyhodnocování a aktualizace této IKČR.
8. Kapitola "Přehledy klíčových povinností řízení ICT" obsahuje přehledy klíčových povinností při řízení ICT úřadu.
9. Kapitola "Přehled a rejstřík metod řízení ICT" obsahuje přehledy a rejstříky popisovaných metod řízení ICT.

Periodicita a aktualizace dokumentu MŘICT

Vzhledem k trvale dynamickému rozvoji nejen ICT, ale i veřejné správy jako takové, v době, kdy progresivně roste podíl centrálně zajišťovaných sdílených služeb ICT VS atd., je o to nezbytnější trvalá a průběžná aktualizace řídících dokumentů ICT. Ta bude respektovat veškerá, navzájem velmi provázaná legislativní opatření a zároveň vytvářet východisko pro zachování nezbytné stability a konzistence řízení všech úrovní ICT VS, při současné potřebě udržení souladu s IK ČR.

Proto také dokument MŘICT, stejně jako ostatní navazující dokumenty IKČR a jejich rozšiřující Znalostní báze budou po projednání s digitálními zmocněnci a ICT manažery jednotlivých resortů a s odbornou veřejnosti v rámci příslušného pracovního výboru RVIS aktualizovány průběžně.

Ukotvení MŘICT v rámci OVS a její legislativní opora

Obsahově metodika vychází zejména ze zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů (dále také jako "zákon č. 365/2000 Sb."), který stanovuje pravomoci a povinnosti které souvisejí s vytvářením, správou, provozem, užíváním a rozvojem informačních systémů veřejné správy spravovaných státními orgány nebo orgány územních samosprávných celků (také jako "orgán veřejné správy" nebo „OVS“). Na základě tohoto zákona je dle § 5a odst. 1 vytvářena Informační koncepce ČR, stanovující cíle České republiky v oblasti informačních systémů veřejné správy (také jako "ISVS") a obecné principy pořizování, vytváření, správy a provozování informačních systémů veřejné správy v České republice na období 5 let. Aktuální Informační koncepce ČR byla vládou schválena ke dni 3. října 2018.[11)]

Orgány veřejné správy podle IKČR a jejích následných a navazujících dokumentů vytvářejí svou informační koncepci[12)] a další dokumenty[13)].

Dle výše uvedených skutečností je možné dovodit a interpretovat, že Metodika jako jeden z navazujících dokumentů IKČR, která je výslovně předpokládána zákonem č. 365/2000 Sb., je pro všechny orgány veřejné správy závazná, ovšem tento striktní výklad je potřeba brát s rezervou vzhledem k rozpracovanosti i dalším faktorům MŘICT a proto se **tento dokument pro OVS bere jako doporučený**. Již dnes je však jasné, a jeví se jako vhodné, využít a přebírat budoucí prostředí Metod (tedy Metody samotné a jeho přílohy, standardy, metodiky, předlohy apod.) do svých vlastních interních aktů (soubor interních směrnic a nařízení). K tomuto účelu lze využít stávající platnou legislativu, která umožňuje vytvářet formou interních aktů sadu závazných norem, které mohou vycházet z Metod. Metodika bude vymezovat jednotlivé oblasti působnosti, které následně může vydat odpovědná osoba (představený) se všemi dílčími odlišnostmi a unikátnosti svého úřadu, a to právě formou interního aktu (směrnice, nařízení apod.).

Podle § 11 odst. 4 zákona č. 234/2014 Sb., o státní službě ve znění pozdějších předpisů (dále také jako "zákon č.

234/2014 Sb.") **náměstek pro státní službu, vedoucí služebního úřadu, státní tajemník nebo personální ředitel sekce pro státní službu** může vydat služební předpis, který je závazný pro všechny státní zaměstnance, zaměstnance v pracovním poměru vykonávající činnosti podle §5 odst. 1, písmeno e) ve služebním úřadu a podřízených složkách a kterým se implementuje tato metodika formou již zmíněných interních aktů.

Metodiku a tvorbu interních aktů a standardů má vytvářet představený s nejvyšší odpovědností za ICT na úřadě (tedy nejvýše postavený představený se splněným oborem služby Informační a komunikační technologie[14)] dle zákona č. 234/2014 Sb. Ten v §5, písmeno e) ustavuje jako jednu z činností státní služby: *vytváření a správu informačních systémů veřejné správy podle jiného zákona, s výjimkou provozních informačních systémů.*

Stejným způsobem může zavázat metodiky a garanty z jiných útvarů (tzn. jiných organizačních jednotek) k plnění interních aktů vycházející z MŘICT tak, že každý, kdo se věcně podílí na tvorbě a změnách služeb ICT musí mít obor služby Informační a komunikační technologie[15)] (v případě služebních míst) a v náplni práce takové činnosti splňující de facto oborem služby Informační a komunikační technologie[16)]. Všichni s oborem služby Informační a komunikační technologie[17)] a doplněné náplně práce pak budou těmito akty přímo interně vázáni.

Tímto způsobem může dojít k nastavení maticového (horizontálního) řízení v rámci životního cyklu ISVS v daném OVS a jeho rezortu na základě zákonných postupů.

Dalším zásadním přínosem tohoto přístupu je možnost interním aktem zavázat rezortní organizace k plnění cílů Metod (MŘICT) viz výše.

Řízení ICT jako cíl IKČR

Efektivní a centrálně koordinované ICT veřejné správy představuje hlavní cíl číslo 5 IKČR. MŘICT je jedním z prostředků, jak tohoto cíle dosáhnout. Metody řízení ICT VS ČR ale nemohou být pouze dokumentem, nýbrž musí představovat sdílenou kompetenci OVS, spravovanou, šířenou a konzultačně podporovanou z opravdového znalostního centra státu.

Za tím účelem obsahuje IKČR i dílčí cíl č. 5.2, který konkrétně ukládá: „**Vybudování centrální odborné kompetence a kapacity k metodickému řízení procesů řízení ICT v OVS.** Pro podporu efektivního řízení útvarů informatiky OVS a celého životního cyklu jejich IS je potřeba vybudovat institucionální centrální odbornou kompetenci pro tyto procesy (ITIL, CoBIT, IT4IT), která bude autoritou a metodickou záštitou pro OVS.“

Naplnění cíle 5.2 je na základě kompetenčního zákona plně v pravomoci Ministerstva vnitra. Zde by tedy měl vzniknout útvar s celostátní působností, obsahující ty nejlepší specialisty na metody řízení ICT. Pracovně jej pro účely MŘICT nazývejme Odbor řízení informatiky (OŘI). Tento útvar přirozeně doplní zodpovědnost Odboru eGovernmentu (také jako "OeG") za koordinaci toho **„Jak transformovat VS na eGovernment?“** a zodpovědnost Odboru hlavního architekta eGovernmentu (také jako "OHA") za koordinaci toho **„Co stavět?“** svou vlastní zodpovědností za to **„Jak se o ICT starat?“.**

Tento útvar by měl být tím, kdo bude aktualizovat MŘICT, bude plnit odpovídající část Znalostní báze detailními dokumenty a akcelerátory a bude vydávat potřebné ICT standardy, viz také dílčí cíl IKČR 5.6.

Bude velmi praktické, pokud na základě řady ustanovení zákona č. 365/2000 Sb., a navazujících předpisů bude ohlášena agenda „Řízení informačních a komunikačních technologií veřejné správy“. Toto ohlášení podléhá pravidlům zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů (dále také jako "zákon č. 111/2009 Sb."), konkrétně § 53. Současně by se OŘI měl stát věcným správcem několika IS podporujících tuto agendu. Takovými systémy jsou například rejstřík informačních systémů veřejné správy, provozovaný v AIS Působnostním (součást RPP) dle § 52c zákona č. 111/2009 Sb., budoucí IS pro Katalog ICT služeb veřejné správy a IS pro řízení změnových záměrů (nyní dočasně a částečně v rámci Digitálního Česka a jeho katalogu záměrů). Tyto systémy by dále měly být integrovány nebo být součástí nástroje pro i Katalog (digitálních) služeb VS ČR a IS Programové a projektové kanceláře eGovernmentu ČR, viz dále.

Kompetenci existujících odborů OeG, OHA a výše plánovaného OŘI musí pro účely koordinace úspěšného naplňování cílů IKČR (včetně NAP a MŘICT), doplnit ještě útvar představující na MV kompetenci a celostátní působnost v oblasti řízení programů digitální transformace veřejné správy a portfolií transformačních projektů, tedy celostátní Programová a projektová kancelář VS. Pracovně bude tento útvar nazýván PPK, respektive O3P[18)].

Ostatní navazující dokumenty IKČR

Kromě na MŘICT, jako na navazující dokument č. 1, odkazuje IKČR ještě na další tři navazující dokumenty, a to:

- navazující dokument č. 2 - Slovník pojmů eGovernmentu (také jako „SPeG“),
- navazující dokument č. 3 - Národní architektonický rámec VS ČR (také jako „NAR“) a
- navazující dokument č. 4 - Národní architektonický plán VS ČR (také jako „NAP“).

Spojujícím prvkem navazujících dokumentů č. 3 a č. 4 je existence tzv. Národní architektury veřejné správy ČR, které je proto níže vysvětlena.

Slovník pojmů eGovernmentu

Protože jednoznačnost výkladu v jakémkoliv dokumentu používaných pojmů je základním předpokladem jeho shodného chápání, bylo vytvoření Slovníku pojmů eGovernmentu (také jako “SPeG”), jako samostatného dokumentu uloženo Usnesením Vlády ČR č. 629 z 3. 10. 2018 - k programu „Digitální Česko“ a návrhu změn Statutu Rady[19)].

SPeG zavádí jednotný výklad pojmů a jejich případných synonym z platné legislativy, potřebných jako jeden z nástrojů koordinovaného budování eGovernmentu podle NAP a pro koordinované řízení informatiky veřejné správy. Tento slovník společně vysvětluje zejména pojmy používané v IKČR a všech jejích navazujících dokumentech. MŘICT ve slovníku aktualizuje a o nové pojmy rozšiřuje pojmosloví specifikované: Slovníkem pojmů Národní architektury veřejné správy ČR a Slovníkem nejčastěji používaných pojmů ve veřejné správě[20)], tak aby výklad byl v souladu s aktuálním zněním mezinárodních manažerských (ITIL, Řízení výkonnosti - 3E) a architektonických metodik (TOGAF a ArchiMate).

Pro vyšší srozumitelnost je dokument MŘICT maximálně kompaktní a stručný. U pojmů, jejichž zavedení, nebo podrobnější výklad je obsahem samostatných dokumentů, je na tyto konkrétní dokumenty uveden odkaz.

Národní architektura veřejné správy ČR

Veřejná správa ČR, stejně jako každý jednotlivý úřad, je socio-ekonomicko-technický systém, který má architekturu, tj. obsahuje soubor prvků, které tvoří strukturu systému, jejich vzájemných vazeb, jejich chování (fungování) a principů a pravidel jejich vzniku a vývoje v průběhu času.

Národní architektura ICT veřejné správy ČR (také jako „NAČR“) je tedy souhrn architektur a popisů architektur všech jednotlivých úřadů veřejné správy, včetně všech centrálních sdílených prvků eGovernmentu. Je uplatněním metod a myšlení podnikové architektury na veřejnou správu na vyšší, republikové úrovni. Jejím cílem je zejména:

- zavést jednotný strukturovaný popis a komunikaci služeb veřejné správy a jejich ICT podpory, jako jeden z předpokladů dosažení cílů IKČR,
- maximálně ochránit investice do sdílených prvků technologické a datové infrastruktury českého eGovernmentu a urychlit jeho další rozvoj.

Užitek z NAČR budou mít všechny zájmové skupiny (Stakeholders), zejména ale:

- Centrální architekti eGovernmentu (OHA a OEG)
- Ředitelé projektů
- Ředitelé informatiky OVS
- Hlavní architekti OVS a korporací
- Auditoři NKÚ a dalších kontrolních orgánů
- Řídící orgány strukturálních fondů
- Správci rozpočtu a další role,

a to zejména díky možnosti, využívat společný a sdílený strukturovaný popis ICT ve veřejné správě.

Nezastupitelnou roli v řízení ICT VS mají útvary architektury jednotlivých OVS. Architekti na úrovni úřadu mají realizovat nejméně těchto pět rozdílných, ale vzájemně se doplňujících a podmiňujících funkcí:

- Přirozený vzor a leader (metodik) tvorby Enterprise architektur a architektur řešení v jednotlivých OVS v resortu (úřadu), 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, …)
- Enterprise Architekt a architekt řešení architektur (byznys, aplikačních, datových i technologických) centrálních sdílených (nebo jednotných) služeb a centrálních sdílených (nebo standardizovaných) systémů eGovernmentu na úrovni resortu (úřadu).
- Lokální (interní) Enterprise Architekt úřadu a těch organizací úřadu (resortu), které jej o to požádají a kde nepostačí předchozí role rádce.
- Kontrolní orgán (jako stavební úřad) předběžně kontrolující vybrané vlastnosti v rámci resortu (úřadu) předkládaných IT projektů vůči zásadám NAP (vůči územnímu plánu) a vůči vyhlášeným standardům architektury řešení (jako ve stavebnictví vůči tzv. regulačnímu plánu).
- Auditní orgán stanovující požadovanou úroveň architektonické zralosti jednotlivých organizací resortu (úřadu), jejich architektonického oddělení a jeho procesů a governance a orgán kontrolující dosažení této úrovně v požadovaném čase a její zachování.

Národní architektonický plán

Národní architektonický plán VS ČR (také jako “NAP”) slouží jako základní nástroj pro formulaci způsobu realizace cílů a principů Informační koncepce ČR a informačních koncepcí jednotlivých orgánů veřejné správy.

Jednotnost tvorby a užívání NAP je zajištěna dodržování pravidel Národního architektonického rámce, viz dále.

Orgánům veřejné správy – správcům informačních systémů, poskytuje jasnou (názornou) a konkrétní představu toho, jak bude vypadat informatika VS ČR ve stanoveném horizontu 5 let, které prvky informatizace veřejné správy budou centrální a sdílené, které lokální prvky musí být jednotné podle předložených vzorů a které mohou být libovolné, jejich vzájemné vazby a návaznosti při současném dodržení stanovených architektonických principů.

Podmínkou udržení a rozvoje NAP, který je z podstaty znalostní disciplínou, je trvalé udržování dostatečných kapacit s dostatečnou kompetencí pro NAČR. K tomu je – stejně jako v jiných odborných oblastech, potřeba vypracovat a zavést koncepci vzdělávání, certifikace znalostí a akreditace vzdělávacích a certifikačních institucí.

Nedílnou součástí prostředí NAP jsou tzv. Nástroje NAP, sada prostředků převážně z oblasti informačních technologií, pro podporu modelování, vyhodnocování a vzájemného sdílení obsahu znalostí o architekturách, realizované jako kombinace centrálního architektonického nástroje a úložiště NAP, případných lokálních nástrojů orgánů veřejné správy a integrace na další centrální prvky eGovernmentu, jako Základní registry a Datové schránky.

Každé řešení, zachycené v NAP, bude procházet životním cyklem a bude muset být řízeno s využitím metod uvedených v MŘICT.

Národní architektonický rámec

Národní architektonický rámec VS ČR (také jako “NAR”) zavádí závaznou metodiku modelování, udržování a používání a prostředky popisu architektury orgánů veřejné správy a architektury informačních systémů veřejné správy.

NAR obsahuje zejména metodiku pro:

- **Popis architektury** - tj. návrh prostředků, jakými zachytit jednotlivé obrazy architektury podle potřeb zainteresovaných skupin.
- **Postup tvorby architektury** - tj. návrh postupu tvorby, údržby a užití architektury úřadů, v jejím životním cyklu, rozdělený do fází a organizovaný podle domén architektury.
- **Organizaci architektonického týmu** - tj. doporučení, jaká má být struktura týmu, jeho dovednosti, znalosti, způsob řízení a kontroly a místo v celkovém řízení úřadu.

Architektonické procesy a nezbytné schopnosti, rozvíjené podrobněji v NAR, jsou v MŘICT jako součást metody Architektura úřadu[21)] uváděny do kontextu ostatních metod, užívaných v rámci životního cyklu ICT řešení.

Další navazující dokumenty k MŘICT

IKČR a stejně tak tato metodika předpokládá, že bude na tuto metodiku dále navazovat řada legislativních a metodických dokumentů a pomůcek, týkajících se jednotlivých disciplín řízení ICT, například řízení změn, projektového řízení, řízení hospodárnosti zdrojů a vyhodnocování TCO v IT apod.

Všechny navazující dokumenty s podrobnějšími pravidly, znalostmi, návody a pomůckami pro praktické použití, tzv. akcelerátory budou tvořit souhrnnou Znalostní bázi metod řízení ICT VS ČR, publikovanou společně s dalšími znalostmi k IKČR a jejím navazujícím dokumentům NAP, NAR a Slovník pojmů eGovernmentu.

Vztah MŘICT k vybraným legislativním předpisům

Chod každého úřadu, včetně jeho útvaru informatiky, je řízen řadou právních předpisů, ze kterých vycházejí rozmanité povinnosti. Proto je důležité, aby všichni zodpovědní představení u věcných i technických správců (a ostatních klíčových rolí) měli k dispozici takový aktuální seznam povinností s odkazy na zdrojové předpisy, včetně již avizovaných očekávaných změn. Pro usnadnění této potřeby připravuje MV do Znalostní báze jako akcelerátor přehled povinností a časový harmonogram („Kalendář CIO“), viz také Přehledy klíčových povinností řízení ICT.

Seznam těch nejdůležitějších a pro manažery informatiky nejvíce relevantních předpisů bude průběžně aktualizován jako součást Znalostní báze. Zde jsou dále uvedeny pouze vybrané, aktuálně platné a účinné legislativní zdroje určující kompetence, procesní role, omezení, aj., podstatné pro MŘICT. Jsou to zákony:

- č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů
  - určuje základní kompetence a vymezuje působnost jednotlivých ústředních orgánů státní správy
  - stanovuje zásady činnosti ústředních orgánů státní správy
- č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
  - definuje roli Správce národního katalogu otevřených dat [§4c/2]
- č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů:
  - definuje klíčové role včetně např.: Správce ISVS, Provozovatel ISVS a Uživatel ISVS
  - definuje klíčové pojmy: ISVS a provozní informační systém, služba ISVS, referenční rozhraní a vazba mezi ISVS, Portál veřejné správy a Centrální místo služeb,
  - vymezuje základní instituty zejm.: vytváření ISVS, sdílení dat

    - specifikuje povinnosti Vlády, Ministerstva a OVS spojené s ISVS, tj. zejm.: ohlašovací povinnost a povinnost mít atestovanou informační koncepci,
- č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a vyhláška 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):
    - definuje role správců, provozovatelů, garantů aktiv a nově i Výboru pro řízení kybernetické bezpečnosti a role Manažera, Architekta a Auditora kybernetické bezpečnosti,
    - definuje základní instituty a vymezuje klíčové pojmy včetně zejména pojmů: Kritická informační infrastruktura (KII), Významný informační systém (VIS), Základní služba, Digitální služba, Hrozba, Zranitelnost, Akceptovatelné riziko, Podpůrné aktivum a Primární aktivum,
    - definuje činnosti Řízení aktiv a Řízení dodavatelů.
- č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů
- č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů
- č. 234/2014 Sb., o státní službě, ve znění pozdějších předpisů, ve znění pozdějších předpisů
- č. 110/2019 Sb., o zpracování osobních údajů
    - stanovující rozsah ochrany osobních údajů, který je nutné zohlednit při tvorbě informačních systémů a při návrhu systémů pro práci s dokumenty.
- č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění zákona č. 183/2017 Sb.
- č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů
- a další

Současný a cílový stav řízení ICT

Celý dokument MŘICT je formulován tak, aby maximálně motivoval cílovou skupinu jeho primárních příjemců k tomu, aby ho četli, vnímali a aktivně užívali v něm obsažená doporučení. Klíčové předpoklady a záměry, ze kterých při tom vychází, jsou:

- eliminovat obavy:
    - z rozsahu cílů a úkolů, plynoucích pro ně z IKČR a z probíhající digitální transformace veřejné správy,
    - z rizik, spojovaných zejména v poslední dekádě s investicemi do rozvoje informatizace
- podpořit chuť vedoucích ICT útvarů úřadů využít příležitost a:
    - dále rozvíjet a zlepšovat v rámci vlastní zodpovědnosti informatiků “svého” úřadu ale i rezortu
    - vystoupit ze stávajícího stínu IT a získat podstatný podíl na celkové digitální transformaci “svého” úřadu a celé veřejné správy.

Každý z čtenářů může mít jenom některé z těchto motivací nebo i zcela jiné, ale doporučení MŘICT by každopádně měla být nápomocná pro zmírnění či eliminaci ostatních obav a rizik a pro posílení či naplnění nadějí a příležitostí budoucího, lepšího stavu informatiky úřadů a její role v rámci digitální transformace.

Zjednodušená charakteristika současné ICT VS ČR

Hlavní pozitiva

Veřejná správa ČR má tisíce pracovníků. Někteří pracují v útvarech zajišťujících ICT podporu a jsou mezi nimi i vysoce odborní specialisté. Všichni jsou připraveni se podílet na digitální transformaci svých úřadů. Elektronizace však představuje změnu chodu úřadu, zde tedy pracovníci v ICT útvarech mohou přispět svou odborností, nikoli tvorbou a samotnou volbou přístupu nebo strategie.

ICT je jednou z mála oblastí, kde centrální řešení pro pečlivě vybrané aktivity velice rychle a účinně zvyšuje kvalitu a snižuje pracnost.

ICT VS ČR a jí podporovaný eGovernment ČR má aktuálně:

- vybudovány:
  - bezpečnou a spolehlivou společnou komunikační základnu – KIVS,
  - jeden společný propojovací uzel veřejného Internetu a datových sítí jednotlivých OVS, který zároveň plní funkci bezpečnostního a dohledového centra - CMS,
  - společné přístupové body – samoobslužný Portál veřejné správy a asistovaný Czech POINT,
- centralizována klíčová referenční data (Základní registry)
- vydánu řadu:
  - legislativních dokumentů (např.: Zákon č. 365/2000 Sb., …),
  - závazných standardů (např. eGon Service Bus)
- v provozu řadu digitálních služeb využívaných jak úředníky VS, tak občany, např.:
  - Czech POINT,
  - Datové schránky,
  - Národní identitní autorita.

Klíčové nedostatky

Na základě provedeného ICT Benchmarku veřejné správy (Digitální Česko, 2018), mezinárodních srovnání i vlastních šetření autorského týmu MŘICT se ukazuje, že úroveň ICT ve veřejné správě ČR a jeho podpora rozvoji eGovernmentu a digitální transformace veřejné správy zdaleka nedosahuje úrovně běžné v jiných odvětvích společenského života ČR. Zpoždění oproti úrovni, oprávněně očekávané klienty veřejné správy ve srovnání například s elektronizací bankovnictví, pojišťovnictví či telekomunikacemi na území ČR či s veřejnou správou vyspělých zemí (severské země EU, Korea, USA, Nový Zéland a další) dosahuje 10 a více let.

Rychlého pokroku je možné dosáhnout prostým uplatněním nejlepších praxí z těchto oborů a zemí. Příčiny jsou známé, hlavními faktory opožďování a neefektivity dosavadních ICT investic jsou:

1. nejednoznačnost a nekonzistence kompetencí (zodpovědností) jednotlivých aktérů při řízení jak celého ICT VS, tak jednotlivých služeb a systémů, zejména současné nastavení:
   - o vzájemných kompetencí zákonného (průběžného) liniového řízení veřejné správy ČR a programového řízení digitální transformace úřadů,
   - o rozdílů v samostatnosti různých druhů orgánů VS, tzn. rozdílů jejich právního statutu a z něho plynoucích odlišných práv a povinností,
2. podceňování informatiků a informatiky jako profese a oboru služby vzhledem k jejich zodpovědnosti za chod nezbytných podmínek výkonu služeb veřejné správy a k nevyužitému vysokému potenciálu při digitální transformaci právních předpisů, služeb a úřadů samotných,
3. vysoká rizikovost řízení ICT investic,
4. časté přeskupování a reorganizování ICT útvarů, které v důsledku také vede k několikaměsíční paralýze a nečinnosti, resp. neplnění rozvojových (investičních) úkolů a k pouze základní údržbě ICT služeb,
5. časté změny a neadekvátní tlak na ICT útvary, který vede zejména vysoce odborné a motivované pracovníky k odchodům, nebo ke ztrátě motivace a vyhoření, obecně dochází k defenzivním aktivitám vedení ICT a ztrátě schopnosti vést, koncepčně rozvíjet a inovovat, velmi často pak dochází k zástupným důvodům k odvolání daného vedoucího pracovníka či představeného,
6. v rámci personální politiky se velmi často nevyužívají veškeré dostupné mechanismy zvyšující motivační faktory daného pracovníka[22)], z hlediska vzdělávání se pohlíží na školení pro pracovníky ICT jako na drahé a tudíž nerealizovatelné, druhotně tak daný pracovník odborně neroste a snižuje se jeho motivace,
7. v oblasti rozpočtu se díky nedůvěře a zmiňované rizikovosti ICT služeb, nahlíží na služby ICT jako na zbytné a nákladově vysoké. Pravidelně tak dochází ke kritickým škrtům primárně v provozních - tedy mandatorních výdajích (kde jsou ve většině závazky delší než 1 rok) investiční výdaje nevyjímaje, děje se tak ve většině bez negociace s představeným ICT, který nedisponuje jakýmkoli nástrojem obrany svého rozpočtu. Dochází tak k poddimenzování služeb a jejich zastarávání, které v důsledku znamená

nespolehlivost pro klienta a porušování bezpečnosti např. ve formě bezpečnostních zranitelností, na jejichž odstranění strana zadavatele nemá dostatečné finanční prostředky.

8. v oblasti krácení investičních prostředků dochází k nenaplňování vize a úkolů politického vedení úřadu (nerealizují se nové IS ani změny těch stávajících), druhotně pak k prohlubující se nedůvěře k ICT jako takovému. Mnohdy dochází i k nemožnosti realizovat zákonné změny, nebo k chybám při zadávání, kdy je zadavatel nucen pracovat s jiným, sníženým, rozpočtem a tudíž nejsou, a nemohou být obslouženy všechny původní požadavky interního zadavatele.
9. v oblasti snižování rozpočtu dochází většinou k ochuzení a zanedbání vzhledu rozhraní (UI/UX) pro uživatele a pro klienta digitálních služeb VS (příjemné a intuitivní prostředí je klíčové pro spokojenost klienta VS). Tyto efekty následně mohou vést k nespokojenosti klienta VS s danou službou, tlaku na vedení úřadu a následné nespokojenosti s vedením ICT.
10. nedostatečná vymahatelnost plnění i platných povinností v oblasti řízení ICT a rozvoje eGovernmentu,
11. neschopnost veřejné správy fungovat v rovnoprávném a vyváženém partnerství s dodavateli ICT řešení a služeb, zejména:
    - nedostatek kompetentních lidských zdrojů a informací na straně OVS, a to zejména:
        - pro plánování a řízení rozvoje jednotlivých řešení (architektura) a
        - pro plánování a řízení dodávky rozsáhlých změn řešení (projektové řízení)
        - pro plánování a řízení provozu jednotlivých řešení (řízení služeb apod.)
    - zcela nevyvážené smluvní a licenční vztahy,
12. neexistence provázanosti čerpání státního rozpočtu na velikosti přínosu a míře aktivity zapojení se do plnění státní strategie eGovernmentu,
13. neschopnost vedení a členů ICT útvarů lidsky formulovat a propagovat svoje úspěchy a přínosy danému OVS a jeho rezortu,
14. neexistence centrálního katalogu ICT služeb ke sdílení (též sdílitelných služeb). Částečně bude vyřešeno katalogem služeb dle č. zákona č. 12/2020 Sb., ale katalog služeb veřejné správy nenahradí katalog ICT služeb, což může způsobit:
    - omezené využívání a pomalý přechod OVS k využívání již centrálně poskytovaných sdílitelných ICT služeb veřejné správy,
    - centrálně nekoordinovaného vynakládání prostředků ze státního rozpočtu na ICT VS a tím výrazně nižší než možnou úroveň synergie ICT projektů jednotlivých OVS,
15. absence:
    - jednotně uplatňované metodiky posuzování potřebnosti a přínosů ICT záměrů[23)] pro plnění strategických cílů ČR, jako podkladu pro centrálně koordinované:
        - rozhodování o prioritizaci čerpání finančních prostředků ze státního rozpočtu,
        - objektivní vyhodnocování přínosu ICT projektů / akcí[24)],
    - vymezení odpovědností a práv klíčových rolí (věcný správce, technický správce, provozovatel) v legislativě,
16. nedostatečné kompetenční vymezení práv a zodpovědností mezi jednotlivými úrovněmi řízení VS a i navzájem mezi jednotlivými útvary VS, a to zejména:
    - útvary zajišťujícími:
        - strategický rozvoj VS na národní úrovni / za rozvoj eGovernmentu,
        - metodické řízení a výkon konkrétních agend VS (role věcného správce),
    - útvary odpovědnými za poskytování informační podpory těmto agendám (role technického správce),
17. nedostatečná úroveň specializace a motivace ICT pracovníků VS,
18. problematické:
    - obsazování pracovních pozic s vyšší kvalifikační náročností v oboru ICT a udržitelnost pracovníků na těchto pozicích.
    - může existovat řešení, které je jedinečné, ale zároveň pro potřeby úřadu nejlepší. V takovém případě je potřeba zvažovat veškeré výhody i nevýhody plynoucí z nejlepšího řešení, ale možného vendor lock-in, ale i povinností nediskriminovat danou § 6 zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů,
    - dlouhodobé podfinancování – jak investiční, tak i provozní, ICT VS,
    - vyvazování se z historických, pro úřady VS nevýhodných smluv (vendor-lock).

MŘICT zavádí / uplatňuje v první fázi **výlučně opatření k řešení nejpalčivějších z uvedených příčin, a**

to tak, aby byla ihned aplikovatelná na základě platných strategických dokumentů schválených vládou ČR, tzn. taková, u kterých vyžadovat jejich uplatňování není podmíněno realizací žádných legislativních změn.

Definice, poslání a vize informatizace úřadů VS ČR

Definice:

Informační služby[25)] nebo také služby informačních systémů a informačních/komunikačních technologií jsou služby těch útvarů a organizací veřejné správy (a jejich externích dodavatelů), které takovými technologiemi disponují, těm útvarům nebo organizacím, které informační podporu pro efektivní výkon veřejných služeb potřebují.

Rozvoj informační podpory výkonu veřejné správy, zkráceně také informatiky, se nazývá informatizací veřejné správy. Informatizace je klíčovým předpokladem a nedílnou součástí digitální transformace veřejné správy a realizace IKČR. MŘICT je jedním z nástrojů vytvářející prostředí („ekosystém“) pro sdílení informací, standardizaci a růstu ICT útvarů v rámci VS ČR.

Poslání:

Posláním ICT útvarů ve veřejné správě ČR je podporovat služby veřejné správy pomocí bezpečných, hospodárných, inovativních, sdílených a kvalitních technologií.

Vize:

Profesionálové informačních a komunikačních technologií ve veřejné správě ČR jsou důvěryhodnými a uznávanými strategickými partnery vedení svých organizací, informujícími je o inovativních možnostech ICT a poskytujícími jim koncepční, kvalitní a bezpečné ICT služby, podporující jak lepší služby veřejné správy občanům a firmám, tak zefektivňující interní procesy veřejné správy.

Své znalosti a přístupy mezi sebou efektivně sdílí prostřednictvím prostředí, které vytváří a udržuje MŘICT.

Zásady řízení ICT z IKČR

Informační koncepce ČR ve svém textu přináší vedle cílů a architektonických principů budování eGovernmentu také „Obecné principy pořizování, vytváření, správy a provozování informačních systémů veřejné správy“ alias základní zásady řízení útvarů informatiky OVS a životního cyklu ISVS. Uvedené zásady představují minimální povinné předpoklady pro zajištění koordinovaného rozvoje a úspěšné realizace změn služeb ICT jednotlivých

OVS a eGovernmentu, navrhovaných podle uvedených principů IKČR a naplňujících její cíle.

Tabulka obecné principy pořizování, vytváření, správy a provozování informačních systémů veřejné správy dle dokumentu IKČR

ID	Název zásady řízení ICT
Z 1	Na prvním místě je klient
Z 2	Standardy plánování a řízení ICT
Z 3	Strategické řízení pomocí IK OVS
Z 4	Řízení architektury
Z 5	Řízení požadavků a změn
Z 6	Řízení výkonnosti a kvality
Z 7	Řízení zodpovědnosti za služby a systémy
Z 8	Řízení katalogu služeb
Z 9	Udržení interních kompetencí
Z 10	Procesní řízení
Z 11	Řízení přínosů a hodnoty
Z 12	Řízení kapacit zdrojů
Z 13	Nezávislost návrhu, řízení a kontroly kvality
Z 14	Vztah informatiky a legislativy
Z 15	Řízení financování ICT
Z 16	Využívání otevřeného software a standardů
Z 17	Podpora vyváženého partnerství s dodavateli

Uvedené zásady je tak třeba respektovat jako klíčové východisko pro řízení celého životního cyklu ICT úřadu, od stanovení kritérií pro inventuru aktuálního stavu ICT úřadu, včetně vyhodnocení změn oproti předchozímu roku (blíže viz Postup a plán realizace změn), přes zadávání projektů a řízení změn, až po hodnocení jejich výsledků, a to na všech úrovních řízení.

Zároveň MŘICT obsahuje základní informace o podstatné části manažerských metod potřebných pro implementaci uvedených zásad v kontextu řízení nejen celkových schopností úřadu a jeho útvaru informatiky, ale i řízení životního cyklu jednotlivých ISVS spravovaných úřadem. Popisy jednotlivých metod se budou dále prohlubovat v následujících vydáních MŘICT a zejména průběžně zdokonalovat v přílohách a dodatcích publikovaných průběžně prostřednictvím Znalostní báze.

Detailní popis jednotlivých principů ve struktuře obdobné popisu architektonických principů dle NAR, plus kontrolní seznamy s pomocnými otázkami a další akcelerátory, včetně zpětného mapování toho, jak jednotlivé metody přispívají k naplňování cílů a zásad IKČR, budou také součástí Znalostní báze.

Na prvním místě je klient

Z1 - Rozhodování v IT je na prvním místě zaměřeno na dodávku efektivních služeb, představujících zřetelnou hodnotu pro externí i interní klienty, příjemce a uživatele těchto ICT služeb na podporu výkonu služeb veřejné správy. Tzn. mimo jiné, že nově budované informační systémy nemají být pouhou evidencí (kartotékou) zákonem uložených údajů, ale mají být prostředkem efektivní podpory procesů výkonu služeb agend veřejné správy. A to, jak podporou práce úředníka, tak podporou samoobslužného procesu na straně klienta veřejné správy.

Tento obecný princip má dvě složky, jedna směřuje na vlastní řízení ICT na bázi vyváženého vztahu mezi věcnými a technickými správci řešení, kde věcný správce je klientem ICT a reprezentuje koncové klienty úřadu (úředníky i občany/organizace).

Druhá složka má přesah do architektonických principů ve vrstvách byznys a aplikační architektury a mění účel a způsob podpory výkonu služeb veřejné správy a provozu úřadů aplikačními službami IS.

Nejčastější vhodné metody pro naplnění zásady:

- Řízení vztahůu se zákazníkye (externími i interními)m
- Architektura úřadu (EA)Enterprise Architecture
- Řízení IT služeb ITIL/ITSM - řízení IT služeb (část)
- Řízení procesů (BPM - Business Process Management)

Standardy plánování a řízení ICT

Z2 - Rozvoj služeb je řízen pomocí zavedeného systému Enterprise architektury a dalších návazných standardů. Standardizované postupy vyhovují specifikaci metodických standardů a doporučení vydávaných Ministerstvem vnitra, zejména Národního architektonického rámce s možností využití dalších návazných mezinárodních standardů (TOGAF, ArchiMate, COBIT, ITIL, IT4IT, UML...) pro řízení EA a ICT procesů a služeb.

Tento obecný princip říká, že procesy a postupy plánování a řízení ICT úřadu nejsou na libovůli úřadu a IT manažera, ale že mají být do předpisů i praxe úřadu vedle MŘICT a NAR, respektive jako jejich rozšíření, zavedeny odpovídající části mezinárodních standardů.

Nejčastější metody, v nichž se zásada uplatní:

- Řízení IT služeb ITIL/ITSM, IT4IT
- Řízení výkonnosti (Cobit)
- Řízení rizik (CoSO)
- Řízení architektury (TOGAF, ArchiMate, UML)
- Řízení projektů (PRINCE2, PMI)
- a další

Strategické řízení pomocí IK OVS

Z3 - Rozvoj IS OVS je řízen dlouhodobým plánem – Informační koncepcí daného OVS. Ta zahrnuje jak strategické změny, tak potřeby procesní optimalizace, tak potřeby vyplývající ze stavu ICT. IK OVS stanovuje cíle orientované na zlepšování služeb externím klientům (veřejnost) a interním klientům (zlepšování subjektu). Třetí doporučená skupina tvoří cíle orientované na zlepšování IT (řízení služeb).

Informační koncepce OVS musí podporovat realizaci cílů koncepce/strategie subjektu, pokud jsou stanoveny, musí podporovat realizaci cílů infomační koncepce ČR a musí reflektovat principy a zásady, které tato stanovuje.

Cíle musí splňovat specifikaci „SMART“, tj. specifičnost/konkrétnost, měřitelnost, dosažitelnost (musí existovat alokace finančních a lidských zdrojů pro realizaci cíle), relevantnost a časového vymezení.

Tento obecný princip podtrhuje podstatnou změnu spočívající v tom, že:

- řízení ICT OVM nesmí být reaktivní, ale plánované
- dokument IK OVM není „papír do šuplíku“, ale je základním nástrojem řízení.

Informační koncepce je dokumentem zachycujícím plán řízení prostřednictvím metody Enterprise Architecture.

Navazuje na cíle stanovené zejména interní „Strategii rozvoje úřadu“ a „na ICT strategii úřadu“ (pokud je vypracovávána samostatně), dále na cíle IKČR, vládní programové prohlášení a sektorové strategie rezortu a úřadu. Cíle, stanovené v těchto strategiích (zejména rozvoje úřadu a ICT) musí být SMART, tj. dle metody Strategického řízení, případně vč. Balanced ScoreCard.

Nejčastější vhodné metody pro naplnění zásady:

- Architektura úřadu (EA)Enterprise Architecture
- Strategické řízení + BSC (Balanced ScoreCard)

Řízení architektury

Z4 - Architektura jednotlivých ICT řešení musí být navržena podle byznys architektury agendy, v kontextu k architektuře celého OVS a celého eGovernmentu. Zejména musí být zohledněny sdílené služby OVS a eGovernmentu a potenciál dalšího sdílení.

Každý subjekt je povinen udržovat svůj model EA v aktuálním stavu, úrovni detailu dle své velikosti a v konzistentním stavu s povinným obsahem stanoveným Ministerstvem vnitra, který reprezentuje společné sdílené služby a prvky architektury a zároveň v konzistentním stavu s obsahem své Informační koncepce.

Architektura je čtyřvrstvá, tj. ke každému procesu/agendě existuje vazba na příslušné aplikace ISVS (a/nebo provozní systémy), které proces podporují, dále vazba na příslušnou technologickou a komunikační infrastrukturu, ve které jsou systémy realizovány a provozovány.

Do EA modelu OVS musí být zapracovány části národního modelu (NAP), specifikující architekturu sdílených služeb. Pokud OVS poskytuje nějakou sdílenou službu, musí její EA model publikovat přes MV/OHA.

Tento obecný princip upřesňuje předchozí princip Z3. Nejčastější vhodné metody pro naplnění zásady:

- Architektura úřadu (EA)Enterprise Architecture

Řízení požadavků a změn

Z5 - Vyhodnocování zpětné vazby, incidentů a požadavků na služby. Funkční proces řízení životního cyklu požadavků (na nové funkce, změny, opatření eliminující rizika) je z hlediska řízení informačních služeb a řízení změn architektury klíčový. Požadavky musí být průběžně evidovány, vyhodnocovány a zapracovány do aktualizací informační koncepce subjektu, do programových dokumentů, investičních záměrů, projektů nebo plánů drobných změn.

Tento obecný princip vyžaduje zavedení několika procesů z metod řízení dodávky ICT služeb (ITIL/ITSM).

Současně je jeho součástí vzájemně se doplňující řízení malých změn (v rámci podpory provozu) a velkých změn (v režimu projektového řízení) v návaznosti na Roadmapu IK OVS.

Nejčastější vhodné metody pro naplnění zásady:

- Řízení požadavků v rámci řízení ICT služeb ITIL/ITSM
- Architektura úřadu (EA)Enterprise Architecture
- Programové a projektové řízení

Řízení výkonnosti a kvality

Z6 - Vyhodnocování výkonnosti a kvality, minimálně principy měřitelnosti a zpětné vazby, budou zavedeny do všech procesů/postupů, stejně jako role, pozice manažera kvality (nezávislost výkonnosti a kvality IT na řízení rozvoje a provozu IT).

Kvalita, výkonnost a zodpovědnost v oblasti řízení ICT OVS bude pravidelně ověřována formou auditu a benchmarku.

Tento obecný princip zdůrazňuje několik klíčových aspektů řízení výkonnosti a kvality služeb IT a výkonnosti služeb veřejné správy a provozu, podporovaných službami IT.

Nejčastější vhodné metody pro naplnění zásady:

- Řízení kvality
- Řízení výkonnosti
- Řízení vztahů se zákazníky
- Enterprise ArchitectureArchitektura úřadu (EA)
- Audit IT
- Benchmark

Řízení zodpovědnosti za služby a systémy

Z7 - Každá agenda/proces a jeho služba musí mít svého vlastníka (osobu), který určuje strukturu a způsob výkonu procesu/agendy a je odpovědný za zlepšování, napříč všemi podpůrnými IS.

Každý ISVS (nebo provozní systém) má definovaného garanta/správce (věcného a technického) a provozovatele, napříč všemi podporovanými agendami a službami.

Tento obecný princip nově stanovuje jednoznačnou povinnost úřadu mít definované externí i interní procesy a služby výkonu veřejné správy i služby provozu. A dále povinnost, mít pro každý identifikovaný proces a pro každou jeho službu jednu osobu zodpovědnou za jejich kvalitu a trvalé zlepšování.

Současně tento princip zhmotňuje řešení tradičního problému vztahu mezi odbornými a IT útvary povinností úřadu mít ke každému informačnímu systému dvojici znalých a zodpovědných osob, věcného správce a technického správce.

Nejčastější vhodné metody pro naplnění zásady:

- Řízení kvality
- Řízení vztahů se zákazníky (interními i externími)
- Řízení služeb
- Řízení IT služeb (ITIL/ITSM)
- Řízení procesů (BPM)
- Architektura úřadu (EA)

Řízení katalogu služeb

Z8 - IT podpora OVS je řízena pomocí katalogu ICT služeb (převážně aplikačních, ale i technologických a

infrastrukturních), kterými jsou podporovány procesy výkonu interních i externích služeb veřejné správy úřadu (tradičních i digitálních). Každý subjekt aktualizuje, publikuje a propaguje na internetu svůj katalog elektronických/digitálních služeb orientovaných na veřejnost a v intranetu obdobný katalog interních digitálních služeb.

Externí katalog digitálních služeb je svázaný s příslušnými životními/podnikatelskými událostmi/situacemi. Tento katalog je následně konsolidován a publikován Ministerstvem vnitra na portálu veřejné správy. Místní samospráva využívá v rámci přenesené působnosti část katalogu s předlohami vytvořenými Ministerstvem vnitra.

Katalog interních ICT služeb OVS obsahuje i služby dostupné pro něj jako sdílené služby z různých úrovní veřejné správy.

Tento obecný princip se doplňuje s předchozím principem (o zodpovědnostech) a nastavuje povinnost úřadu mít aktuální a při řízení úřadu využívat jak katalog (byznys) služeb úřadu (výkonu VS i provozu), tak specificky katalog služeb ICT útvaru a jeho externích pod-dodavatelů. Katalog ICT služeb je podmnožinou a nedílnou součástí katalogu interních (provozních) služeb úřadu, společně se službami správy nemovitostí, účetnictví, personalistiky, nákupu, administrace, právního oddělení a dalších).

Katalog slouží jak pro řízení kvality a výkonnosti dodávky těchto služeb, tak pro řízení jejich rozvoje, ale také jako prostředek jejich užití (konzumace) v intranetu úřadu.

Nejčastější vhodné metody pro naplnění zásady:

- Řízení kvality
- Řízení vztahů se zákazníky (interními i externími)
- Řízení služeb
- Řízení IT služeb (ITIL/ITSM)
- Řízení procesů (BPM)
- Architektura úřadu (EA)

Udržení interních kompetencí

Z9 - Pro všechny klíčové role řízení služeb eGovernmentu a řízení informatiky má OVS vytvořeny interní pozice. To je nezbytné pro udržení nezávislosti na dodavatelích, kontinuity a celostního pohledu, a zejména zodpovědnosti. Pracovníci v těchto rolích si udržují kompetence aktivním zapojením do všech činností spojených s dodavateli a přebírají jejich dovednosti (Learning by doing).

Tento obecný princip vede úřad ke splnění jednoho z mnoha předpokladů schopnosti se transformovat a pružně rozvíjet bez závislosti na externích dodavatelích, v tomto případě bez závislosti na jejich kapacitách a jejich znalostech.

Princip zdůrazňuje, že úřad musí zajistit jak dostatek kapacit (obsazených pozic), tak dostatek kompetencí, získaných praxí. To prakticky znamená, že pracovníci, kteří mají být nositeli určitých znalostí, musí být značnou částí svých úvazků uvolněni pro aktivní práci v projektech s externími dodavateli, a o celou dobu působení v projektu je vedle úspěšného dokončení projektu jejich hlavním cílem převzetí, zdokumentování a interní sdílení maxima znalostí dodavatele.

Nejčastější vhodné metody pro naplnění zásady:

- Řízení projektů a portfolií (část - řízení kapacit)
- Řízení znalostí (KM - Knowledge Management)

- Řízení lidských zdrojů (HR)

Procesní řízení

Z10 - Bude zavedeno procesní řízení nejen v IT, ale ve všech agendách/procesech. To mj. znamená, že každý proces má vlastníka/garanta a definované výstupy (služby, produkty). Dále pak definované nástroje (ISVS u agend) a role, které je využívají a vykonávají jednotlivé činnosti procesu/agendy. Role není organizační pozice. Hierarchie organizační struktury nadřízený/podřízený není procesní přístup a má řešit jen mimořádné stavy, které nejsou součástí standardních postupů.

Tento obecný princip dále prohlubuje princip Z7 (Zodpovědnosti) tím, že podporuje v úřadech zavedení skutečného procesního řízení, nezávislého na rigidní organizační hierarchii (liniového řízení). Přechodně se tomu dá napomoci změnou organizační na tzv. procesně orientovanou, tj. takovou, ve které hierarchie zodpovědností kopíruje hierarchii procesní dekompozice.

Obecný princip očekává, že útvar ICT bude v zavádění procesního řízení (jako předpokladu řízení dodávky služeb) průkopníkem v celém úřadu a že současně model řízení v ICT bude v souladu s konceptem budoucího procesního a servisního řízení celého úřadu (spoludefinuje jej).

Nejčastější vhodné metody pro naplnění zásady:

- Řízení ICT služeb (ITIL/ITSM)
- Organizační management (část HR)
- Řízení procesů (BPM)
- Architektura úřadu (EA)
- Řízení kvality

Řízení přínosů a hodnoty

Z11 - Všechno rozhodování se řídí pravidly „řádného hospodáře“ a „Value for Money“. Všechny projekty ISVS musí (spolu s formulářem OHA) disponovat zpracovaným investičním záměrem typu „business case“ s jasně identifikovaným přínosem pro veřejnost a/nebo úřad. Pro tvorbu „business case“ projektu se využije metodika OHA MV ČR, obohacená o osvědčené prvky metodik jiných resortů, jako např. metody logického rámce z metodiky MPSV a ESF ČR.

Tento obecný princip zavádí do úřadu schopnost, posuzovat každý záměr na změnu (a většinou i na výdaje) na základě poctivého finančního a nefinančního porovnání hodnoty přínosů (výstupů, výsledků, ale zejména dopadů - „ k čemu je to dobré“) a potřeby zdrojů (kapacit, znalostí, financí), s přihlédnutím k eliminaci rizik.

Nejčastější vhodné metody pro naplnění zásady:

- Investiční záměr (Business Case)
- Logický rámec (FogFrame)
- Řízení výkonnosti a řízení nákladů - ukazatele TCO, ROI, PublicROI
- IT Controlling

Řízení kapacit zdrojů

Z12 - OVS průběžně připravuje zajištění dostatečného množství a kvality interních kapacit vlastníků procesů/agend, garantů/správců systémů, projektových manažerů a architektů, odpovídající jejich předpokládanému uvolnění do programů a projektů realizace transformačních změn.

Projekty pak musí mít zajištěnu dostatečnou kapacitu klíčových pracovníků zadavatele (OVS), kteří drží know-how výkonu jednotlivých procesů, využití stávajících (návazných a/nebo nahrazovaných) systémů a provozních/ bezpečnostních standardů zadavatele. Tyto kapacity musí být reálně alokovány (převedeny) do projektu úměrně svým rolím a fázím projektu. Tím bude, mimo jiné zajištěn potřebný přenos znalostí z projektu a od dodavatele do liniových struktur OVS.

Tento obecný princip navazuje Z9 (... získávání znalostí od dodavatele ...), ale z pohledu zajištění interních kapacit a interních znalostí, čímž jej doplňuje.

Princip zavazuje úřad, aby se nepouštěl do transformačních a do ICT projektů, dokud nebude mít dostatečnou kapacitu dostatečně znalých zaměstnanců, které bude dostatečnou měrou schopen uvolnit do projektu realizace změn. Princip akcentuje dlouhodobost a průběžnost přípravy takových kapacit a kompetencí jako investice do změny a tak ve shodě s cílem 4.6 Informační koncepce ČR.

Nejčastější vhodné metody pro naplnění zásady:

- Řízení projektů a portfolií (část - řízení kapacit)
- Řízení znalostí (KM - Knowledge Management)
- Řízení lidských zdrojů (HR)
- Organizační management (část HR)

Nezávislost návrhu, řízení a kontroly kvality

Z13 - Projekt musí být řízen dle standardní projektové metodiky interním PM s dostatečnou alokovanou kapacitou a kvalifikací po celou dobu návrhu, implementace a předávání ISVS do provozu, nebo externím PM (z kompetenčního centra). Pouze v případě nedostupnosti interních zdrojů a zdrojů kompetenčního centra je možné zadat PM roli externímu subjektu soutěží. Vybraný uchazeč nesmí mít vztah s dodavatelem ani provozovatelem.

Stejně tak je účelné mít v projektech prvek nezávislé kontroly kvality, a to jak kvality projektového řízení, tak kvality návrhu a dodávaného řešení.

V projektu musí být odděleny klíčové role. V případě komponentizace musí být vzájemně na sobě nezávislí systémový integrátor, dodavatelé komponent a provozovatel(-é). Přebírající a provozující subjekt nesmí mít vztah s externím subjektem zajišťujícím návrh, nebo implementaci. Přebírající a provozující subjekt musí být povinně zahrnut do akceptačního řízení implementace.

Tento obecný princip zdůrazňuje nezastupitelnou roli projektového manažera na straně zadavatele. Současně přináší prvek nezávislého dozoru a kontroly kvality na straně zadavatele.

Přitom princip zdůrazňuje nutnost právní, smluvní i faktické nezávislosti některých rolí při dodávkách řešení a služeb. Nejčastější vhodné metody pro naplnění zásady:

- Řízení projektů a portfolií (část - řízení kapacit)
- Řízení nákupu a smluv
- Řízení dodávky ICT služeb (ITIL/ITSM)

Vztah informatiky a legislativy

Z14 - Návrhy možností informační podpory legislativních úprav je nutno vypracovávat společně s návrhy přijímání právních předpisů či jejich změn tak, aby se vzájemně ovlivňovaly směrem ke vzniku moderních a proveditelných ustanovení.

Informační podporu legislativních úprav je nutné připravovat a ověřovat již v průběhu legislativního procesu, nikoli až v okamžiku platnosti či dokonce účinnosti zákona.

Tento obecný princip zdůrazňuje novou roli ICT odborníků při zajištění vysoké pravděpodobnosti proveditelnosti právních úprav, z nichž většina v současné fázi vývoje lidské společnosti a státní správy potřebuje nějakou míru ICT podpory.

Nejčastější vhodné metody pro naplnění zásady:

- Řízení ICT služeb (ITIL/ITSM)
- Řízení legislativního procesu
- Řízení projektů
- Organizační management (část HR)
- Řízení procesů (BPM)
- Architektura úřadu (EA)
- Architektura úřadu (SA)
- Řízení vývoje SW - zde část prototypování, ověřování konceptu (PoC - Proof of Concept, SandBox)

Řízení financování ICT

Z15 - Dlouhodobé profesionální řízení finančních zdrojů a využívání fondů EU je integrálním principem pro všechny OVS. Je třeba pracovat s metodikou finančních kalkulací na bázi indexu rentability/CBA (analýza přínosů a celkových nákladů) a TCO (celkových nákladů na vlastnictví ICT), včetně budování kompetence ekonomicky kalkulovat optimální efektivitu a výkonnost agendy (procesu) s různou úrovní poměru personálních nákladů na její výkon a nákladů na její IT podporu. Je třeba zlepšit nejen oblast řízení investic, ale neméně dlouhodobé finanční plánování obnov infrastruktury a provozní podpory systémů

.

Tento obecný princip navazuje na zásadu Z11 (řízení přínosů a hodnoty) a přidává povinnost úřadu disponovat kapacitou a kompetencí pro řízení ICT investic a jejich financování.

Nejčastější vhodné metody pro naplnění zásady:

- Řízení plánování a financování investic
- Investiční záměr (Business Case)
- Logický rámec (FogFrame)
- Řízení výkonnosti a řízení nákladů - ukazatele TCO, ROI, PublicROI
- IT Controlling

Využívání otevřeného software a standardů

Z16 - Stát k zamezení vysokým dlouhodobým nákladům a rizikům používá otevřený software a otevřené

standardy. Proto správce ISVS využije stávajících otevřených projektů nebo nechá nový zdrojový kód otevřený a znovu využitelný, publikuje ho pod příslušnými licencemi anebo pro konkrétní část kódu poskytne přesvědčivé vysvětlení, pro to nelze provést. Pokud využití otevřeného kódu není pro realizaci ISVS možné či vhodné, pak pro taková řešení postupuje podle zásady Z17 o vyváženém partnerství s dodavateli.

Tento obecný princip pro ústřední koordinační orgány eGovernmentu a ICT povinnost vytvářet, shromažďovat a publikovat sdílitelné části řešení a aplikovatelné standardy.

Pro ostatní úřady představuje povinnost a) při návrhu řešení takové zdroje znát a aplikovat a b) po úspěšném vývoji vlastních řešení poskytnout zdroje a zkušenosti centrální autoritě.

Nejčastější vhodné metody pro naplnění zásady:

- Řízení ICT služeb (ITIL/ITSM)
- Řízení projektů
- Řízení vývoje SW
- Řízení znalostí

Podpora vyváženého partnerství s dodavateli

Z17 - Správce ISVS musí zajistit, aby vždy disponoval zdrojovými kódy ISVS, detailní dokumentací k ISVS, licenčními právy k ISVS (právy k užívání autorského díla) a vlastní způsobilostí rozhodovat o ISVS tak, aby bylo možné upravovat a spravovat systém i prostřednictvím třetích osob, nezávislých na původním dodavateli či správci ISVS.

Tento obecný princip navazuje na zásady Z9 (interní kompetence) a Z13 (nezávislé role) a zdůrazňuje ostatní nezbytné náležitosti pro dosažení smluvních vztahů a reálných projektů a dodávky služby v situaci vyváženého partnerství s dodavateli.

Princip v manažerské oblasti doplňuje (spolu ještě s Z16 a dalšími) architektonické principy P9, P10, P16 a zejména P17 Informační koncepce ČR.

Nejčastější vhodné metody pro naplnění zásady:

- Řízení projektů a portfolií (část - řízení kapacit)
- Řízení nákupu a smluv
- Řízení dodávky ICT služeb (ITIL/ITSM)
- Řízení znalostní (KM)

Předpoklady úspěšné digitální transformace veřejné správy

Evropská komise ve svém materiálu „Akční plán EU pro „eGovernment“ na období 2016–2020“ uvádí že: „Je třeba, aby moderní a efektivně fungující orgány veřejné správy zaručovaly rychlé a vysoce kvalitní služby pro občany a vstřícné prostředí pro podniky, jak to uznávají nedávné roční analýzy růstu. Orgány veřejné správy musejí transformovat své zázemí, znovu zvážit a přetvořit stávající postupy a služby a zpřístupnit svá data a služby jiným správním orgánům a pokud možno také podnikům a občanské společnosti.“[26)]

Ke zmiňovanému urychlení a zlepšení může dojít i beze změn aktuálně platné legislativy.

K realizaci uvedeného předpokladu je třeba realizovat zejména tyto změny:

- zavést koncepční a strategické plánování a řízení rozvoje ICT služeb OVS podle potřeb klientů z jejich odborných útvarů, a to bez výjimek pro celé OVS, a to v dlouhodobém výhledu tzn.:
  - celková architektura úřadu, centrální architektonické kancelář, hlavní architekt OVS a jeho rezortu
  - IT architektura jednotlivých řešení,
  - správa portfolií procesů, aplikací i technologií,
  - to vše řízeno informační koncepcí OVS,
- zavést důsledné programové a projektové řízení plánování a realizace změn ICT služeb, a to jak na straně rozsahu a zdrojů, tak na straně přínosů, to především znamená:
  - celkové jednotné řízení všech (IT i ne-IT) projektů a programů úřadu,
  - centrální programová a projektová kancelář,
  - profesionální projektoví manažeři, spravující portfolia projektů, i napříč úřadem,
- zajistit možnost vzájemné, objektivní a snadné srovnatelnosti ICT projektů VS, tzn. zejména vytvořit jednoduchá, jednotná pravidla pro předkládání a schvalování ICT projektů jednotlivých úřadů VS a zajistit jejich důsledné dodržování. Pravidla musí obsahovat zejména:
  - jasné vodítko co schvalovat,
  - kdo (na jaké úrovni veřejné správy) bude projekt schvalovat, nebo připomínkovat,
  - jasné vymezení projektu, a to zejména
  - věcného cíle projektu, včetně dobře měřitelných kritérií, přičemž věcným cílem nemá být bezúčelné pořízení technologií, ale vždy má sloužit k dosažení konkrétních efektů buď pro uživatele VS, nebo klienty služeb VS, může se jednat o:
    - zajištění veřejného zájmu
    - splnění zákonného požadavku,
    - zvýšení dostupnosti,
    - snížení zátěže,
    - zvýšení kvality pro klienta VS
    - zvýšení bezpečnosti služby
    - Věcný cíl má obsahovat zejména:
      - stručnou specifikaci přínosu pro plnění národních (republikových) a EU strategických cílů, například cílů programu Digitální Česko apod., a cílů OVS,
      - analýzu nebo jiný kvalifikovaný odhad ekonomického nebo jiného pozitivního efektu v časovém horizontu 5 nebo 7 let.
- zavést centrální, jednotnou prioritizaci projektů rozvoje na národní úrovni na základě jejich přínosů pro plnění celonárodních (republikových) strategických cílů,
- zprovoznit klíčové řídící katalogy, zejména pak:
  - Katalog digitálních služeb, respektive centrálně poskytovaných sdílitelných služeb ICT VS,
  - Katalog ICT a transformačních záměrů / projektů VS obsahující uvedení:
    - účelu a hlavních cílů záměru / projektu včetně toho, k jakému (dílčímu) cíli Digitálního Česka má přispět,
    - jakých ICT služeb / jakého ISVS se daný záměr / projekt týká, a to včetně uvedení jejich věcného správce,
    - v jakém je záměr / projekt aktuálně stavu,
    - jakou výši zdrojů záměr / projekt vyžaduje, má alokováno nebo již spotřeboval.
- generálně uvolnit rozpočtová pravidla natolik, aby jednotlivé OVS získaly větší míru kompetence k flexibilním změnám financování. Na základě důsledného a objektivního posuzování efektivnosti interně a externě zajišťovaných ICT služeb, pak mohou flexibilněji reagovat na měnící se potřeby a rychleji a efektivněji uspokojovat klienty a uživatele, jde zejména o:
  - možnost odůvodněně navyšovat podíl outsourcovaných služeb (tzn. netrvat na dodržení ve finančních plánech uvedených podílů investic a provozních výdajů),
  - odůvodněně přesouvat přidělené zdroje mezi schválenými projekty.

Struktura popisu žádoucího budoucího stavu

Jako dokument primárně určený vedoucím (manažerům) ICT útvarů úřadů VS jsou MŘICT orientovány na praxi, a proto nejprve uvádí podstatné informace k tomu, jak řídit a jak přitom užívat jednotlivé metody, a to ve dvou

oblastech, úrovních řízení:

- při řízení v rámci životního cyklu jednotlivých ISVS,
- při řízení aktiv, projektů, procesů a schopností informatiky úřadu jako celku,

Následně jsou uvedeny informace o potřebných ostatních schopnostech úřadu, o něž se manažer útvaru informatiky může a musí opřít a přirozeně na ně navazovat (ekonomika, personalistika, bezpečnost, nemovitosti, nákup apod.). Tyto schopnosti informatika čerpá jako službu ostatních provozních útvarů úřadu, viz Spolupráce s ostatními útvary úřadu a eGovernmentu.

Všechny následující informace jsou de facto popisem cílového (žádoucího, optimalizovaného) budoucího stavu řízení ICT VS ČR, jehož je možno dosáhnout právě realizací těchto doporučení v jednotlivých OVS i vytvořením centrálních předpokladů v MV a dalších institucích.

Teoretická východiska navrženého systému řízení ICT, klíčové informace o jeho postavení v hierarchii řízení veřejné správy ČR a ostatní detailní a doplňkové informace, ze kterých MŘICT vycházejí, jsou uvedena samostatně ve Znalostní bázi.

Od přístího vydání, na základě obdržené odezvy odborné veřejnosti, bude do MŘICT postupně doplňována ještě jedna úroveň detailu řízení, a to postupy řízení životního cyklu jednotlivých dílčích aplikačních služeb / služeb informačních systémů. Stávající vydání MŘICT se zaměřuje vždy společně na všechny měněné služby jednoho IS, podle jeho životního cyklu.

Předpoklady a východiska řízení ICT

Tato kapitola shrnuje vybrané klíčové předpoklady a východiska úspěšného a efektivního řízení ICT na úrovni úřadu i jeho jednotlivých řešení. Proto je tato kapitola východiskem pro kapitoly navazující, zabývající se jednotlivými úrovněmi a postupy řízení ICT v OVS.

Aby ICT útvar mohl plnit účel své existence (poskytovat ICT podporu) efektivně, musí k tomu mít zajištěny (poskytnuty) následující předpoklady, které jsou na všech úrovních veřejné správy shodné, liší se jen šíře záběru a hloubka detailu:

- kompetence, myšleno pravomoci a odpovědnosti, a s nimi spojený respekt a vliv,
- motivace - tj. cíle, principy, pravidla, měřítka kvality a úspěchu
- instituce, způsob organizace, funkce, procesy a služby
- zdroje (technologické, finanční, personální, vědomostní),
- metody a nástroje pro řízení zdrojů a služeb
- organizační stabilitu a kontinuitu
- možnosti a nástroje interní propagace výsledků a nabídky práce svého útvaru
- partnery,
    - klienty uvnitř OVS (objednatele ICT služeb)
    - vedení a orgány úřadu
    - centrální řídící a nadřízené koordinační orgány
    - dodavatele a provozovatele řešení a služeb
    - odborné organizace a komunity a další.

Pro zajištění hladkého výkonu funkce ICT OVS, případně jeho rezortu nebo veřejné korporace, je nutné zajistit následující základní východiska:

1. **Klíčové role a kompetence –** jednoznačně nastavit pravomoci a povinnosti ICT útvaru, resp. jeho vedoucích a řadových pracovníků. Zejména je třeba se zaměřit na klíčový vztah poskytovatele ICT služeb a jeho zákazníka, resp. interního objednatele (věcného garanta). Řídící úroveň ICT OVS (ministerstva, korporace) musí disponovat takovými nástroji řízení, aby mohla aktivně koordinovat ICT služby na svojí a

rezortní úrovni, vydávat řídící akty, metodiky a rámce, které napomáhají řízení a koordinaci.

2. **Úrovně řízení (koordinace) a zodpovědností – management** ICT s lokální zodpovědností vůči vedení svého úřadu (na příslušné úrovni hierarchie veřejné správy) musí být účelně a účinně podpořen centrální koordinací z korporátních (rezortních) a z ústředních orgánů. Technický správce **jednoho** ISVS musí být podpořen vedoucím ICT útvaru úřadu.
3. **Měřítka výkonnosti ICT a kvality jeho řízení** – pro transparentní hodnocení výkonu a kvality řízení ICT vůči vedení OVM musí být nastaveny a využívány jednoznačné a měřitelné, transparentní a srozumitelné ukazatele úspěšnosti změn a výkonnosti řízeného ICT a nastaveny nástroje a způsob jejich prezentace.
4. **Vrstvy architektury** – při řízení ICT úřadu musí být respektován životní cyklus ISVS (funkčního celku) na všech jeho vrstvách, jak byznys služeb, aplikačních ICT služeb, tak služeb sdílené technologické a komunikační infrastruktury OVS a státu,
5. **Celostní přístup – při** řízení každé jednotlivé změny nebo požadavku (informačního systému nebo **jeho** služby) pro konkrétního objednatele je vždy nutné vnímat souvislosti a potřeby celku, tj. zejména vlastního úřadu a všech jeho součástí, případného zřizovatele a celé veřejné správy, případně EU, a vytvořit prostředí umožňující rychle a správně rozhodovat s přihlédnutím k těmto skutečnostem (dopadová analýza).
6. **Odpovídající zdroje –** je nezbytné chápat ICT jako nezbytnou a povinnou podporu, bez které by výkon agend veřejných služeb nebyl možný, a pro jejichž zlepšování a zlevňování je nutné do služeb ICT odpovídajícím způsobem (adekvátně) investovat a přínosy ICT využívat a pravidelně a objektivně vyhodnocovat.

Legislativní a společenská východiska

Systémový dohled nad architekturou

Stejně jako ve stavebnictví, kde mají všechna větší města kromě stavebního úřadu i úřad hlavního architekta, který dohlíží na respektování územního plánu města, i eGovernment ČR má svého Hlavního architekta, který dohlíží na rozvoj a prosazování NAČR a na dodržování NAP. Stejně, jako pro stavbu budov platí řada jednotných oborových předpisů upravujících např. statiku, požární bezpečnost, sanitární vybavenost, splnění hygienických parametrů, elektrické rozvody apod. staveb, i pro eGovernment platí jednotné předpisy, standardy a architektonické vzory.

Stejně jako územní plán jasně geograficky vymezuje, kde budou obytné zóny, kde průmyslové či naopak oddechové, kudy povedou jaké komunikace a definuje pro ně závazné architektonické zásady (sklony střech, orientaci hřebenů, počet pater atd.), i NAP vymezuje takové architektonické zásady pro národní eGovernment. A stejně jako při kolaudaci staveb je ověřováno dodržení schváleného projektu, i u akceptace ICT rozvojových akcí je třeba ověřovat dodržení řešení, které bylo schváleno.

Rozvoj NAP i dohled nad dodržováním v něm obsažených pravidel a soulad s aktuální IKČR zajišťuje OHA. Ten posuzuje a vydává stanoviska ke všem ICT záměrům a projektům subjektům povinným dle zák. č. 365/2000 Sb. nebo dle Usnesení vlády ČR č. 899/2015 Sb.

Systémový dohled nad řízením ICT

Také pořizování, vytváření, správy a provozování informačních systémů veřejné správy v České republice musí mít svůj odpovídající systémový dohled. Obdobně jako u dohledu na architekturu je i systémový dohled nad řízením ICT VS je plně v kompetenci MV ČR.

Tato koordinace a dohledy dosud nebyly na MV ČR v odpovídajícím odboru institucionalizovány (na rozdíl od OHA v případě architektury), viz také Úvod. Proto byl tento dohled po dobu a pro účely digitální transformace veřejné správy ČR a odpovídající ICT podpory částečně substituován na základě Usnesení vlády ze dne 15. 04. 2019 č. 259 k Implementačním plánům programu „Digitální Česko“, kterým byli v rámci jednotlivých resortů nově ustaveni Digitální zmocněnci ústředního správního úřadu. Ti jsou kromě příslušného ministra spoluřízeni a

reportují Vládnímu zmocněnci pro digitalizaci a IT.

Konkrétní pravomoci a povinnosti Digitálního zmocněnce jsou specifikovány dokumentem, který byl vydán RVIS a je součástí Znalostní báze.

Z dlouhodobého hlediska je potřebná kombinace koordinace od obou institucí:

- Liniové řízení kontinuity služeb, znalostí, metod a standardů, kvality a výkonnosti útvarem Řízení ICT MV (OŘI) a
- Programové řízení zásadních (strategických) transformačních změn útvarem Vládního zmocněnce pro digitalizaci a IT, podpořeným odborem eGovernmentu (OeG), odborem hlavního architekta (OHA) a útvarem řízení programů a portfolií projektů (O3P[27]), aktuálně chybějícím, ale potřebným na podporu programu Digitální Česko.

Ekonomické souvislosti

Od rozvoje ICT podpory veřejné správy a obecně od digitální transformace VS se vedle hodnot pro koncové klienty služeb VS (občany a podnikatele), jako je zvýšení atraktivity služeb, zkrácení lhůt, snížení nákladů na straně klientů apod., očekávají přínosy pro veřejnou správu ve dvou zásadních oblastech:

- snížení jednotkových IT nákladů, tj. zlepšení poměru cena/výkon, respektive mnohem rychlejší nárůst rozsahu, kvality a bezpečnosti IT služeb než nárůst rozpočtových výdajů na ně, zejména odstraněním duplicit a přechodem na efektivnější, sdílené služby (například eGovernment Cloud) a
- razantní snížení nákladů na vlastní výkon služeb veřejné správy díky jeho elektronizaci, tj. snížení spotřeby lidských i materiálních zdrojů nebo jejich přesunutí do oblastí veřejné správy, která nebyla vykonávána dostatečně, jejichž potřeba roste nebo se nově objevuje.

Stále rostoucí požadavky na rozsah IT služeb, na jejich kvalitu a bezpečnost znamenají, že se náklady na IT služby celkově nebudou (nemohou) snižovat. Přitom je nutné respektovat, že dosahování všech uvedených přínosů je investicí, tj. nejprve se výdaj musí zvýšit o cenu realizovaných opatření, aby následně mohl o to více poklesnout (v případě investice do úspor).

Součástí řízení ICT musí být uvědomění si těchto cílů a ovládání metod řízení a prostředků k jejich dosažení, včetně metod nákladového řízení ICT a metod měření přínosů změn.

Programové financování – finanční zdroje mimo státní rozpočet

MŘICT na více místech dokumentu zmiňuje využití tzv. programů a projektů pro potřeby programového financování a současně uvádí, že pro řízení zavedení změn (jakéhokoli rozsahu) musí být všechny programy a projekty sladěné, tj. jedná se v obou pohledech stále o jedny a tytéž programy změn.

Finančními zdroji mimo státní rozpočet jsou ve většině rozvojové fondy a technické fondy pomoci. Těmito fondy jsou ve většině Strukturální fondy EU. Tyto fondy slouží k financování cílů regionální a strukturální politiky EU čili hlavně ke zvyšování hospodářské vyspělosti evropských regionů. Finanční podpora z fondů je rozdělována prostřednictvím tzv. operačních programů, které určují zaměření podpory pro daný region, nebo sektor (např. dopravu, zemědělství, digitální transformace a ICT atd.). Metodami a přístupem jak žádat a programově řídit se velice detailně zabývají metodiky zpracované jednotlivými gestory, kteří v souladu s politikami EU tyto vytváří. Je nepraktické a nemožné, aby se MŘICT detailně zaobíralo mimorozpočtovým financováním.

Harmonogram (finančního) plánování

Pro čerpání prostředků ze státního rozpočtu je třeba respektovat termíny sestavení a schvalování státního rozpočtu, tzn. nároky do plánu uplatňovat nejen v potřebné struktuře, ale i ve stanovených termínech.

V termínech je třeba nastavit finanční reporting tak, aby docházelo v maximální možné míře k včasné predikci s problémy v čerpání (nedočerpání/přečerpání).

Zákon o veřejných zakázkách

Veřejná zakázka na pořízení či úpravu informačního systému z pohledu CIO obsahuje obvykle několik částí spojených se samotným pořízením resp. modifikací informačního systému, zajištěním služeb spojených s podporou provozu a údržby daného informačního systému a jeho rozvoje, případně dalších druhů podpor, jako je například uživatelská podpora. Při přípravě příslušné veřejné zakázky je tedy nezbytně nutné mít vyjasněno, zda mají být tyto požadované potřeby zahrnuty do společného rámce jednoho zadávacího řízení či jsou zahrnuty v rámci souběhu s jiným zadávacím řízením nebo jsou pokryty již existujícím platným kontraktem.

Pokud informační systém vyžaduje pořízení dílčích části např. HW či jiné technologické komponenty, které jsou nezbytné pro řádný běh, důrazně se doporučuje, soutěžit je společně s informačním systémem. Pokud tomu tak není, může dojít k nepříjemné situaci, kdy se nepodaří řádně či včas vysoutěžit a zadat veškeré části potřebné pro provoz samotného informačního systému. V situaci, kdy nelze soutěžit veškeré komponenty v celku, nebo jsou využívány sdílené technologické komponenty, které budou pořízeny v rámci jiné veřejné zakázky, je pak doporučeno s útvary připravujícími a realizujícími veřejné zakázky daná rizika omezit, především zajištěním návazností či souběhem jednotlivých veřejných zakázek - o takové spolupráci také v Spolupráce s ostatními útvary úřadu a eGovenrmentu.

S ohledem na druh a režim veřejné zakázky [28)], a tím i finanční limit, je nezbytně nutné dbát obezřetnosti a již v přípravě zakázky předvídat požadavky na rozvoj či podporu, které mohou mít vliv na možnosti budoucího čerpání finančních prostředků, plynoucí ze zadané veřejné zakázky (skutečně vysoutěženého předmětu).

Pro potřeby dalšího rozvoje a úprav, především pak s ohledem na problematiku Vendor Lock-in, je nezbytné zakomponovat do podmínek zadávacího řízení kvalitativní hodnotící kritéria (technologická neutralita, dodavatelská segmentace, nabývací práva ke kódu, diverzifikace vývojových a provozních platforem, ...) příslušná opatření, která neznemožní v budoucnu takové požadavky řádně a komponentově izolovaně soutěžit. Požadavky vyžadující úpravy v jiných informačních systémech je nutné zohlednit při přípravě zadávacího řízení a konzultovat takové požadavky s příslušnými útvary, zda jsou pokryty v rámci jiných již zadaných veřejných zakázek, nebo zda musí být řešeny v rámci této veřejné zakázky.

Komplikace spojené s veřejnými zakázkami, které mohou nastat:

- Doba trvání především otevřeného nadlimitního řízení na dodávky či služby (zvýšená náročnost na procesní úkony)
- Komplikace v průběhu zadávacího řízení (možný nízký počet nabídek či námitky uchazečů)
- Žádná nabídka, nebo žádný vítěz a nezbytné opakování dané části

Zvládnutí procesů nákupu investic a služeb v souladu s ustanoveními zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále také jako "ZoZVZ") je pro jeho komplikovanost a nutnost přesoutěžení zhotovitelů po uplynutí 4 leté doby plnění jedním ze základních omezení a obtíží řízení ICT.

V dalších vydáních MŘICT budou vydána základní doporučení k aplikaci ZoZVZ v ICT a ve Znalostní bázi budou průběžně aktualizovány informace o nejlepší praxi, návody a pomůcky pro tuto oblast.

Řídící kontrola a další působení kontrolních orgánů

Řídící kontrola je spolu s interním auditem součástí vnitřního kontrolního systému dané organizace, který je podmnožinou finanční kontroly, upravené zákonem č. 320/2001 Sb., oo finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů (dále také jako "zákon č. 320/2001 Sb.") a jeho prováděcí vyhláškou č. 416/2004 Sb., kterou se provádí zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění zákona č. 309/2002 Sb., zákona č.

320/2002 Sb. a zákona č. 123/2003 Sb. (dále také jako "vyhláška č. 416/2004 Sb.")

Řídící kontrola je dle § 3 odst. 4 písm. a) zákona č. 320/2001 Sb., kontrolou „zajišťovanou odpovědnými vedoucími zaměstnanci jako součást vnitřního řízení orgánu veřejné správy při přípravě operací před jejich schválením, při průběžném sledování uskutečňovaných operací až do jejich konečného vypořádání a vyúčtování a následném prověření vybraných operací v rámci hodnocení dosažených výsledků a správnosti hospodaření“[29]. Kontrola má tedy následující čtyři fáze:

- předběžnou kontrolu před vznikem závazku nebo nároku,
- předběžnou kontrolu po vzniku závazku nebo nároku,
- kontrolu průběžnou a
- kontrolu následnou.

Výkon předběžné kontroly zajišťují v různých fázích:

- příkazce operace,
- správce rozpočtu a
- hlavní účetní.

Kontrolu průběžnou a následnou pak mohou provádět tytéž nebo jiné k tomu pověřené osoby.

Při výkonu řídící kontroly by měly být uplatňovány (jsou blíže popsány v příslušné vyhlášce[30] a které specifikují skutečnosti, jež je třeba v dané fázi kontroly prověřit):

- schvalovací,
- operační,
- hodnotící a
- revizní postupy.

Je zcela běžné, že v otázce řídící kontroly se mnohdy ze strany ICT útvarů argumentuje, že jejich posláním je provozní, technická a rozvojová činnost ICT, za jejichž účelem byly tyto útvary zřízeny a provádění řídící kontroly je pro ně pouze a jenom administrativní zátěží, která nepřináší nic užitečného a jako taková je tato činnost upozaďována a marginalizována. Řídící kontrola je však zákonnou povinností a nelze ji v žádném případě opomíjet, ba naopak je nutné tyto kontroly integrálně vtělit do útvaru tak, aby byla jeho přirozenou a jednou z nejdůležitějších činností. Níže jsou uvedené některé často se opakující nedostatky, výčet však není vyčerpávající a má spíše navést k zavedení řídící kontroly a vyhnout se tak nepříjemnostem a kritickým chybám v oblasti finančního řízení.

Jde tedy o následující chyby a nedostatky :

- nedostatečná úprava řídicí kontroly,
- nejednoznačné vymezení pravomocí a odpovědností při výkonu řídicí kontroly,
- realizace výdajů bez provedení řídicí kontroly,
- schválení finanční operace neoprávněnou osobou,
- nedostatečné provádění následné kontroly,
- opožděné předkládání vyúčtování a úhrad,
- nesprávné zadávání veřejných zakázek,
- nedostatečné pořizování průkazných záznamů o všech provedených operacích a kontrolách,
- nedostatečné předávání informací o významných rizicích, závažných nedostatcích a přijímaných opatřeních k jejich nápravě.

Vzhledem k cenám ICT by otázka jejich smysluplnosti, dosažení deklarovaných cílů a splnění principů 3E[31] měla být zpětně pečlivě prověřována.

Další věcná a odborná doplnění budou obsažena v následujících vydáních po projednání s odbornou veřejnosti.

Klíčové role v ICT a eGovernmentu

Stejně tak, jako metodické řízení jednotlivých agend VS spadá pod věcně příslušné ministerstvo a řízení a poskytování platformových služeb eGovernmentu spadá pod Ministerstvo vnitra, i uvnitř jednotlivých OVS musí výkon agend VS spadat pod agendově příslušné útvary úřadu.

Naproti tomu předmětem činnosti ICT útvarů úřadů musí být pouze proaktivní poskytování informační podpory pro správný, bezpečný a kvalitní výkon agend VS. Z výše uvedeného vyplývá, že ICT útvary jsou jedním z tzv. provozních či podpůrných útvarů úřadu, poskytujících služby na základě obdržených požadavků. Z toho dále vyplývá, že:

- agendově věcně příslušné útvary úřadu jsou v roli klientů ICT, jsou věcnými správci aplikace ISVS a poskytují ICT útvaru jako technickému správci věcné zadání[32)] a potřebnou součinnost při realizaci a provozu řešení, včetně zpětné vazby od uživatelů, protože mají detailní procesní znalost dané agendy, související legislativy, vazeb a konsekvencí,
- ICT útvar – se v roli poskytovatele ICT služeb a technického správce řešení ISVS dělí minimálně na tři základní nezaměnitelné celky, (řízení ICT, provoz ICT a rozvoj ICT), které si vzájemně poskytují služby, které však nesou společnou odpovědnost vůči zadavateli (věcnému správci), tedy musí mít jednoho hlavního představeného a jeho „štáb“. Tyto základní celky se ještě jemněji člení nejméně na následující specializované role:
  - **Provoz** – pořizování a správa komodit, komunikace, administrativa, provozní a business monitoring, SLM a SLA negociace, OLM a OLA, správa UC, provozní procesy a nástroje.
  - **Kybernetická bezpečnost** – dohled, monitoring, Zák. o KB, CLOUD, SIEM, IDM, PIM/PAM, zranitelnosti, rizika a další.
  - **Rozvoj a vývoj** – vztah s klienty, digitální služby, projekty, elektronizace, idea management, strategie a její změny – údržba akčního plánu atd.
  - **Architektura a standardizace** – tvorba a údržba architektury a koncepce, tvorba a údržba standardů (vyjma bezpečnostních) ve spolupráci s ostatními ICT útvary, spolu-gestor strategií a akčních plánů (vlastník je CIO), spolu-gestor idea managementu, nositel inovace.
  - **Metodická, aplikační a procesní podpora agend a systémů** – analytici AIS/IS se znalostí metod a procesů, klíčoví uživatelé, znalci legislativy se schopností právní algoritmizace a definice požadavků na zákony z pozice ICT. Tito mohou být v praxi s výhodou zařazeni do struktury odborných útvarů.
  - **Koordinace rezortu** – v případě, že má ICT představený mandát ke koordinaci rezortu může disponovat (a je více než vhodné) zvláštním útvarem pro tuto činnost.
  - **Podpora CIO** - organizační, administrativní, ekonomická, právní a další podpora hlavního představeného útvaru ICT (tedy CIO).
  - **Informační podpora** - útvar ICT služeb poskytuje informační podporu digitálním službám VS / výkonu agend VS, tzn., provozuje a rozvíjí „jejich“ agendové informační systémy (také jako „AIS“), nebo interní provozní informační systémy úřadu podle potřeb a pokynů odborného útvaru.

Je žádoucí, aby došlo ke změnám ve finančním řízení, tj. aby se odborný útvar stal držitelem rozpočtu a příkazcem operace pro výdaje ICT řešení, podporující „jeho“ agendy, tj. podle úsloví „kdo objednává, ten platí“.

ICT útvar nemusí nutně vykonávat tyto funkce svými kmenovými zaměstnanci, může mu v tomto pomáhat k tomu zřízená organizace - ve veřejné správě např. státní podniky (NAKIT, CENDIS, SPCSS,...). Vždy však za tuto službu vůči věcnému správci odpovídá útvar ICT, který ji u organizace objednává.

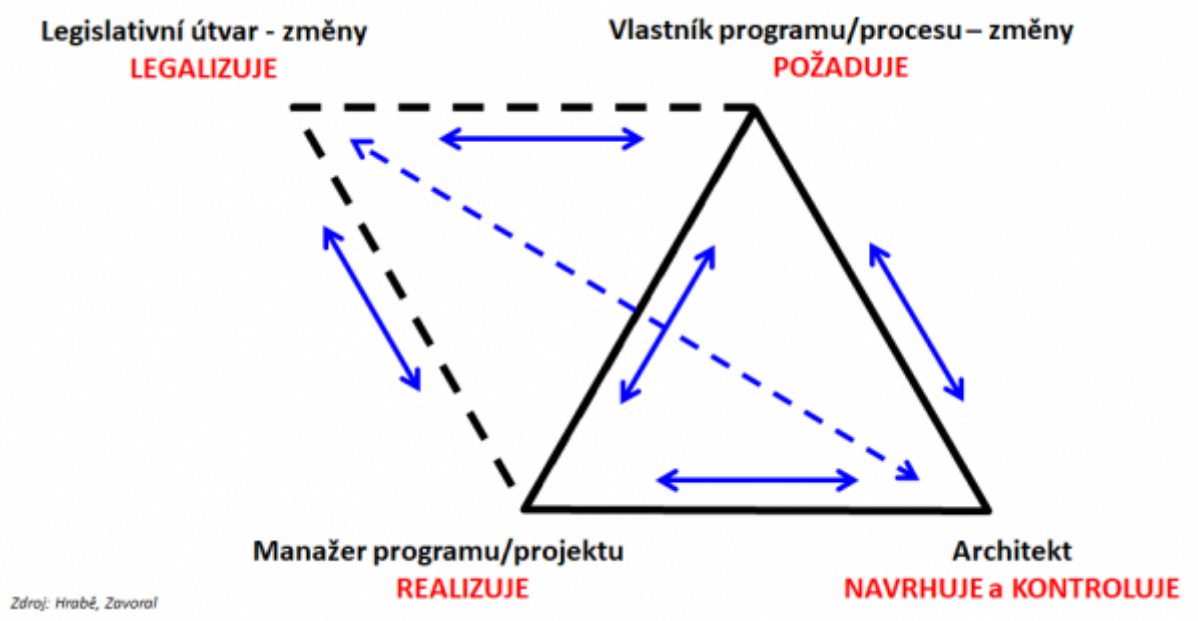
Nejjednodušším způsobem, jak v úřadu realizovat účinné rozdělení povinností a práv pro účely zajišťování informační podpory výkonu agend veřejné správy, je ustavit níže uvedené klíčové role správy ISVS nebo provozního systému.

Podrobný popis povinností a práv těchto a dalších identifikovaných rolí v procesech řízení vývoje a dodávky ICT služeb bude po projednání s odbornou veřejnosti obsažen v následujících vydáních a ve Znalostní bázi. Jsou to zejména role:

- **Věcný správce (služeb) ISVS** – OVS (jeho útvar), který je často jako tzv. gestor agendy zmocněn (kompetenčním zákonem, uvnitř úřadu organizačním řádem) zajišťovat výkon agendy veřejné správy nebo interní provozní funkci/službu, a to včetně její adekvátní podpory službami informačních a komunikačních technologií.
- **Technický správce (služeb) ISVS** – úřad nebo útvar, pověřený uspokojováním požadavků odborného útvaru (věcného správce ISVS) na ICT podporu jeho agendy službami odpovídajícího ISVS nebo provozního IS.
- **Provozovatel (služeb) ISVS** – úřad nebo útvar, de-facto (reálně, skutečně) provozující ISVS nebo provozní systém, který dané ICT služby pro agendu pro provozní funkci poskytuje.

Klíčové čtyři doplňkové role k výše uvedeným, uplatňující se zejména při plánování a realizaci změn informačních systémů jsou, viz následující obrázek čtyřúhelníku:

- **Procesní vlastník**, vlastník změny – nejčastěji roli přebírá věcný správce či garant.
- **Enterprise architekt** a **architekt řešení**
- **Manažer projektu**
- **Legislativní útvar** - útvar, který má znalost v oblasti legislativy, která se změnou upravuje. Slouží také ke správně napsanému znění dle legislativních pravidel



Je důležité podotknout, že legislativní útvar může legalizovat jen ty změny, která má daný úřad v gesci.

Za optimálních cílových podmínek jsou všechny výše uvedené role (a jejich pozice) součástí (velkého) útvaru věcného správce, anebo jsou součástí „štábu“ vedení úřadu a sdílenou službou pro (menšího) věcného správce IS. Role architekt řešení se může dále rozdělit na:

- **Byznys architekt řešení** (analytik) je (měl by být) součástí útvaru věcného správce,
- **IT architekt řešení** je (měl by být) v ICT útvaru.

Na základě rozsáhlosti agendy úřadu, centrální rezortní koordinace architektury, je přípustné (doporučené) členit architektonické role detailněji. Principy a příklady členění viz NAR a Znalostní báze.

ICT kompetenční matice

Řídit ICT úřadu znamená rozdělit nejen kompetence uvnitř ICT útvaru, ale i stanovit jeho kompetenční rozhraní s ostatními provozními / podpůrnými útvary OVS. K tomu je nutný řídící akt na vyšší úrovni řízení, než má vedoucí ICT útvaru. Optimálně by toto rozhraní mělo být vydáno vedením úřadu formou, interního aktu řízení,

který by obsahoval i ICT kompetenční matici a byl v souladu s byznys vrstvou Enterprise architektury úřadu. Smyslem kompetenční matice je (nejen pro oblast ICT) eliminovat možné kolize kompetencí rolí a útvarů, které vycházejí z různých zdrojů (od závazné legislativy po interní akty řízení úřadu).

ICT kompetenční matice úřadu by měla obsahovat, kromě v předchozí kapitole uvedených rolí a útvarů, které jsou ICT útvaru nadřízené, také nadřízené a podřízené externí instituce, zejména však tyto interní útvary OVS:

- **útvar bezpečnostní** – zejména Manažer kybernetické bezpečnosti, je-li ustaven mimo ICT útvar a útvar zajišťující fyzickou bezpečnost OVS ev. další útvary bezpečnosti v rámci OVS,
- **útvar právní a legislativní** – zejm. z pohledu vhodných právních formulací v rámci zadávání veřejných zakázek a smluv, včetně smluv na outsourcované ICT služby, autorského (licenčního) práva, zadávání znaleckých a právních posudků, v oblasti legislativy pak zcela jistě součinnost v oblasti návrhů a novel zákonů tak, aby docházelo k přísnému souladu mezi technickými možnostmi a právními formulacemi zákonů a podzákonných norem. Vzájemná symbióza při realizaci právních deklarací a technických algoritmizací v IS/AIS a službách ICT, přináší sekundárně hospodárnost a včasnost realizace legislativního opatření formou ICT řešení,
- **útvar veřejných zakázek** – jedná se o metodickou, věcnou ev. právní a výkladovou podporu ve vztahu k ZoZVZ a zastupování vně úřadu ve vztahu k dozorovým a dalším orgánům ve věci VZ (ÚOHS, NKÚ, MMR, MF, kontrolní výbor PS ev. další vládní skupiny a výbory)
- **útvary finanční a majetkové** – jedná se primárně o plánování, financování a hospodaření s majetkem, a to jak z pohledu věcného, zákonného, tak termínového,
- **útvary personální a mzdový** – primárně v oblasti vzdělávání, motivace a stabilizace interních pracovníků,
- **útvar architektury úřadu** – Enterprise architekti, centrální procesní analytici,
- **útvary kyberbezpečnosti** - architekt kybernetické bezpečnosti a auditor kybernetické bezpečnosti,
- **útvar interního auditu** a
- **útvar propagace a komunikace** + **tiskový mluvčí**.

Více o spolupráci útvaru ICT s ostatními útvary také v Spoulpráce s ostatními útvary úřadu a eGovernmentu.

Jako podklad pro návrh detailní kompetenční matice úřadu bude možné využít vzorové ICT kompetenční matice obsažené jako jedna z pomůcek ve Znalostní bázi.

Další věcná a odborná doplnění budou obsažena v následujících vydáních po projednání s odbornou veřejnosti.

Úrovně řízení a zodpovědností ve veřejné správě

Postupy řízení ICT v OVS musí respektovat aktuálně platné kompetence jednotlivých aktérů řízení. To konkrétně znamená řídící procesy realizovat přizpůsobené:

- charakteru úřadu – odlišný postup mají úřady státní správy, úřady samosprávy, ostatní orgány veřejné moci,
- dle organizační úrovně úřadu v hierarchii veřejné správy,
- v závislosti na charakteru změny a závažnosti jejích dopadů jak na infrastrukturu VS, tak na digitální služby VS a na data.

Správné je pouze takové nastavení kompetencí, které respektuje zařazení OVS současně do:

- úrovně podle finančního řízení a uplatňování práv zřizovatele a
- organizační hierarchické úrovně řízení jednotlivých agend veřejné správy a jejich ICT podpory.

Vedle toho je důležité správné vnímání a zohlednění koordinační role ústředních orgánů, které z kompetenčního zákona a dle rozhodnutí vlády ČR zodpovídající za centrální řízení a koordinaci rozvoje ICT na podporu eGovernmentu, tj. zejména Ministerstva vnitra ČR, Rady vlády pro informační společnost a Zmocněnce vlády pro digitalizaci a informační technologie.

Bližší popis vlastností a model výše uvedených úrovní řízení a popis jejich pro řízení ICT významných faktorů přináší Znalostní báze řízení ICT VS ČR.

Funkční a procesní model ICT OVS

Útvar ICT OVS, jako jeho velmi významná provozní schopnost, má svou architekturu ve všech jejích horizontálních vrstvách i vertikálních motivačních doménách, viz doménový model architektury v NAR.

Pro popis a pochopení požadovaných schopností ICT a jejich zajištění je potřebné znát a využívat modely současného a budoucího stavu architektury ICT oddělení. Přitom je velmi účelné vycházet z mezinárodních knihoven nejlepších praxí (standardů) a referenčních modelů pro útvary ICT VS ČR, které budou postupně publikovány ve Znalostní bázi.

Byznys architektura informatické schopnosti OVS

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a aktualizováno průběžně ve Znalostní bázi.

Aplikační architektura informatické schopnosti OVS

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a aktualizováno průběžně ve Znalostní bázi.

Ukazatele hodnocení úspěšnosti řízení ICT

Tak, jako ve všech oborech, i v ICT VS je nezbytným předpokladem správného řízení znalost a publikování deklarovaných ukazatelů (kritérií), podle kterých jsou výsledky, tzn. úspěšnost řízení posuzovány.

Ukazatele pro hodnocení ICT VS jsou jak národní – obsažené ve strategických dokumentech eGovernmentu, a tak mezinárodní, a to jak průřezové ukazatele nejlepších praxí (jako COBIT), tak odvětvové ukazatele pro informatizaci veřejné správy a celé společnosti.

Důležité národní ukazatele výkonnosti ICT

- metriky k cílům IKČR
- ICT Benchmark, jako součást benchmarku provozních profesí (správa nemovitostí, účetnictví, nákup a další).

Mezinárodní ukazatele výkonnosti ICT

- COBIT

Mezinárodní ukazatele výkonnosti (indexy) eGovernmentu

- DESI - EU index,
- OSN index a
- OECD index.

Více informací o jednotlivých dostupných a doporučených systémech ukazatelů, včetně pomůcek pro jejich praktické uplatnění bude průběžně udržováno ve Znalostní bázi.

Čtyři vrstvy architektury

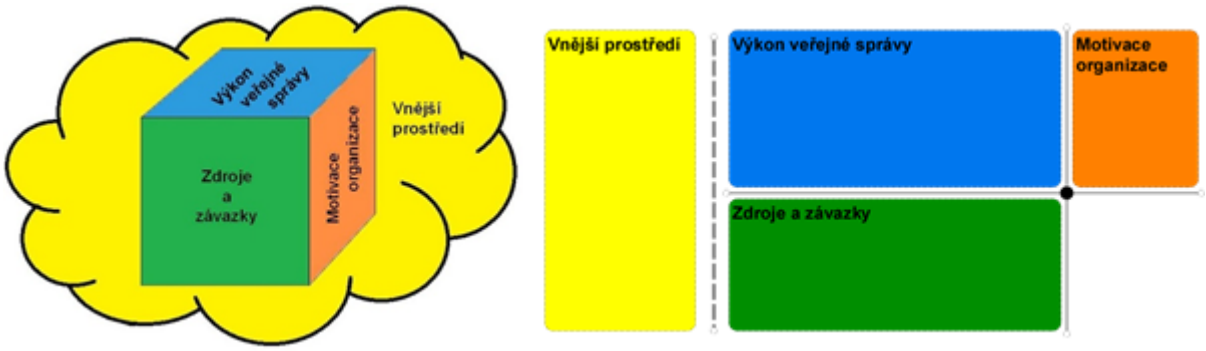
Veškeré řízení ICT služeb pro výkon služeb veřejné správy a provozu úřadu probíhá na čtyřech vrstvách architektury a zodpovědnosti za služby, v pořadí shora:

- byznys vrstva výkonu služeb veřejné správy úřadu a výkonu interních provozních služeb úřadu,
- vrstva služeb informačních systémů, zvaná také aplikační a datová, poskytující aplikační služby přímé informatické podpory výkonu byznys služeb,
- vrstva IT technologické infrastruktury, poskytující zejména platformové technologické služby výpočetního výkonu a úložného prostoru pro aplikace,
- vrstva komunikační a fyzické infrastruktury, poskytující služby umístění technologických prvků a jejich propojení s vnější sítí eGovernmentu a internetu.

Tato struktura je odrazem rozdílné manažerské a právní zodpovědnosti za dodávku služeb na jednotlivých vrstvách a je maticově kolmá k zodpovědnosti úřadu jako celku za každý jeden ISVS, který je jako logický informační systém a funkční celek rozložen právě přes tyto čtyři vrstvy vzájemně se podmiňujících služeb.

Jednoznačná průřezová odpovědnost za služby jednotlivých vrstev se v úřadu musí promítnout do příslušných pozic a rolí, jejichž náplní jsou zejména činnosti a postupy popsané v Řízení na úrovni útvaru ICT OVS a Spolupráce s ostatními útvary úřadu a eGovernmentu.

Pohled na úřad jako celek



Každý IS a každá ICT služba je součástí OVS, jehož celkový kontext je potřeba vždy vzít při rozhodování v úvahu. Celek OVS je možné, stejně jako celou veřejnou správu, nebo naopak jakoukoli její nejmenší část, třeba jeden ICT útvar, nejjednodušeji popsat takto:

Model jednotného pohledu na všechny prvky veřejné správy a každé její součásti.

Na obrázku je vyobrazení jednotného modelu a jeho celkového popisu v rámci veřejné správy a každé její součásti, kdy nejvyšší úroveň je zobrazena v symbolické podobě krychle jako rozvinutý model.

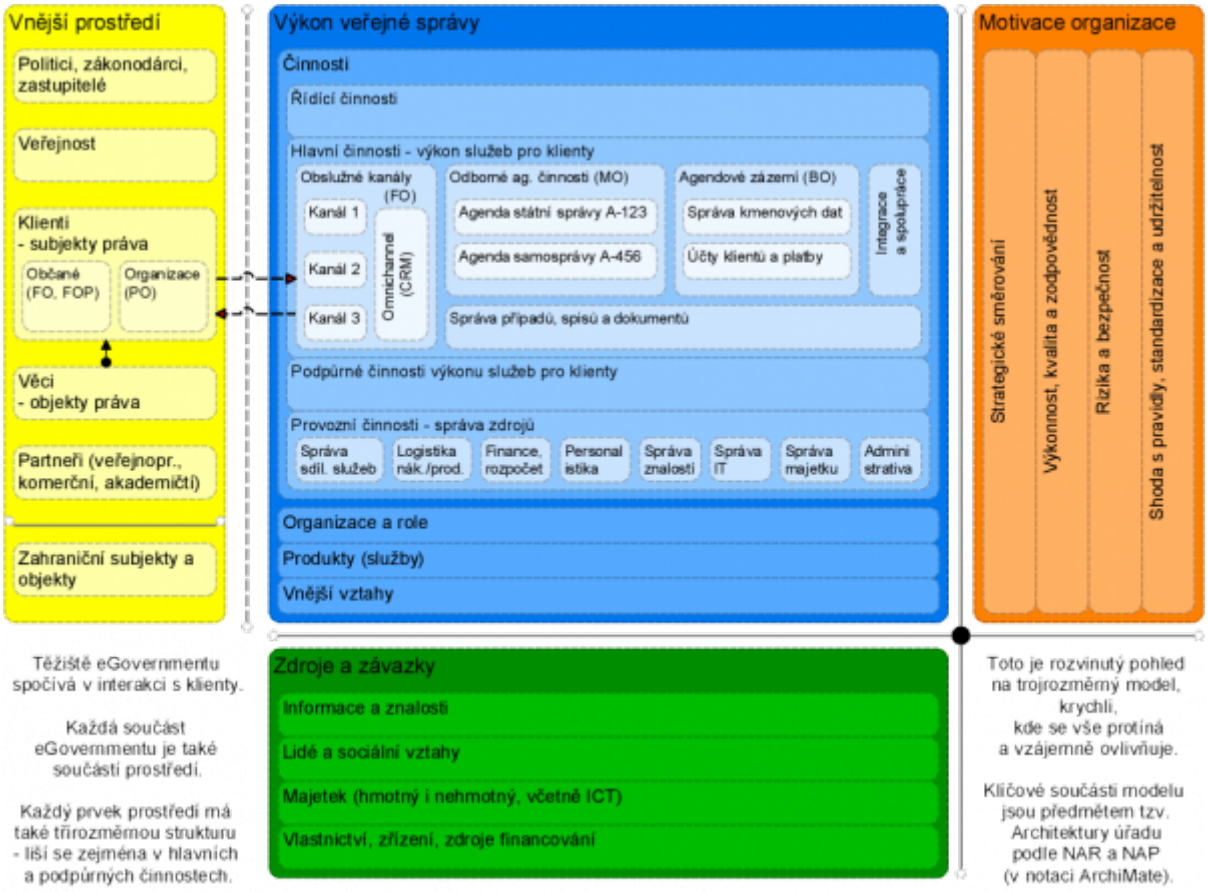
Všechny interní a externí činnosti OVS (modrý rozměr úřadu) mají za úkol poskytovat služby veřejné správy do okolního prostředí (žlutý oblak) přes definované „úřední“ rozhraní komunikace mezi soukromoprávním a veřejnoprávním prostředím. K tomuto přístupu potřebuje OVS jasnou motivaci, proč služby poskytovat právě v určitém rozsahu a určitým způsobem (oranžový rozměr). K zajištění pak potřebuje veškeré zdroje, kterými jsou lidé, znalosti, majetek, institucionální (právní) a finanční zajištění (zelený rozměr).

Součástí výše uvedeného je přirozeně i IT útvar samotný, včetně jeho procesů a ICT služeb v modré, jeho lidé, data, HW a SW, rozpočet v zelené a jeho pravidla, předpisy a koncepce v oranžové části obrázku.

Za důležitý aspekt je považován i čas, ten však není do modelu zahrnut. Čas jako takový plyne objektivně a

nezávisle, nelze si ho přidělit ani přivlastnit. Správná práce s časem je ale nedílnou součástí procesů plánování a řízení, a je nedílnou součástí manažerských rozhodnutí a v mnohém ovlivňuje (pozitivně i negativně) priority všech realizovaných i budoucích změn.

Detailnější pohled na celkový model úřadu ukazuje následující Obrázek. Kompletní informace o celkovém modelu je publikována a udržována v rámci NAP ve Znalostní bázi



Cílům a přínosům odpovídající zdroje

V souladu s výše uvedeným modelem platí[33], že základním a nezbytným zdrojem VS obecně, tedy i ICT služeb a eGovernmentu jsou lidé. Lidé, kteří mají znalosti, informace a dovednosti. Aby je ale mohli uplatnit, musí mít k dispozici: odpovídající technologie a nástroje, majetek, zajištěné financování a zastávanému místu / pozici odpovídající kompetence a motivaci.

Stejně tak formování činnosti úřadu (co, jak, proč a jak dobře dělá) je výslednicí 4 vzájemně propojených motivačních aspektů:

- strategie (středně a dlouhodobé strategické směrování a řízení),
- výkonnost a kvalita (řízení pomocí měřitelných a předem definovaných ukazatelů),
- bezpečnost (řízení opatření na zmírnění rizik a zranitelností),
- soulad s předpisy (právo (včetně komunitárního), vnitřní předpisy (interní řídící akty), pravidla udržitelnosti a 3E).

Součástí výkonu veřejných služeb je i jeho průřezová řídící schopnost, obsahující zejména dílčí schopnosti odpovídající každé ze složek motivace. Ty lze z jiného úhlu pohledu rozdělit na:

- řízení (management) a
- dohled a kontrolu (governance)[34], [35].

Všechny výše uvedené aspekty tvoří jeden logický funkční celek, v případě výpadku nebo absence jediného, je eGovernment pouze částečně funkční, geometrickou řadou nefunkčních aspektů se pak může stát zcela nefunkční.

Kromě technologií, dat a personálu musí útvar OVS poskytující ICT služby (bez rozdílu zda externě či interně) disponovat dostatečnými finančními zdroji z rozpočtu OVS.

Z důvodu vyšší efektivity by klienti IT útvarů (věcní správci, metodici, legislativa apod.) měli ve svých požadavcích a zadáních respektovat časový faktor – tj. dodávat požadavky v dostatečném předstihu a pro finální termín realizace změny respektovat termíny, vycházející z reálných a dosažitelných rozsahů předložených odbornými ICT útvary.

Souhrnně lze také říci, že v dnešní velmi dynamicky se měnící a elektronizované společnosti je právě útvar informatiky nositelem a realizátorem očekávaných změn a přínosů, jeho úlohu nelze nadále snižovat a jeho rozpočet redukovat. Zcela přirozené a organické navyšování ICT rozpočtu a dalších odpovídajících ICT zdrojů je třeba **vnímat jako investici** do získání těchto přínosů, ať do získání nových kvalit služeb veřejné správy, dosažení úspor nákladů při výkonu těchto služeb nebo do úspor **jednotkových** nákladů při výkonu ICT služeb, viz také Předpoklady a východiska řízení ICT.

Proto je nutné přistupovat k řadě činností v plánování a řízení ICT s tímto vědomím investice do přínosů a úměrně tomu používat zejména **metod ex-ante** (efektivního posuzování investice před provedením výdajů), na něž je v tomto dokumentu kladen velký důraz.

Řízení jednotlivých ICT řešení

Zákon č. 365/2000 Sb. předpokládá, že v rámci Informační koncepce ČR bude blíže řešena i problematika řízení informačních systémů veřejné správy. Doporučení MŘICT je vhodné použít v nezměněné podobě a tedy k uplatnění v plném rozsahu ICT portfolia (IT architektury) OVS. Přizpůsobení konkrétním situacím je však jako u jakékoliv jiné metodiky více než vhodné.

Řízení jednotlivých IS je možné popsat a návody a akcelerátory k němu ve Znalostní bázi poskytnout buď se zaměřením na detail fáze a aktivity v etapě životního cyklu IS nebo se zaměřením na typické činnosti a metody, které se sice obvykle vyskytují v určitých fázích, ale mohou se i opakovat a překrývat (např. výběr dodavatele, řízení projektu, zmírnění závislosti na dodavateli apod.).

Tato kapitola přináší a kombinuje oba pohledy. Detailní informace a akcelerátory, zejména k výstupům a metodám podle životního cyklu IS přináší připravovaná znalostní báze.

Všechny činnosti při řízení jednotlivých IS musí být vykonávány v kontextu celého úřadu a eGovernmentu ČR a EU, v rámci činností a postupů popsaných dále v Řízení na úrovni útvaru ICT OVS a Spolupráce s ostatními útvary úřadu a eGovernmentu.

Řízení informačních systémů podle etap a fází jejich životního cyklu

Bez respektování životních cyklů změn nelze efektivně zajišťovat schopnost ICT služeb (informačních systémů a ICT infrastruktury) pro účely bezpečného a kvalitního výkonu služeb veřejné správy. Toto konstatování platí jak z hlediska životnosti technických komponent, platnosti smluvní podpory poskytovatelů, tak zejména z pohledu změn potřeb jednotlivých interních útvarů úřadu a očekávání klientů veřejné správy.

V posledních letech došlo postupně k zásadním změnám v počtu a rozsahu ICT služeb úřadů, tento nárůst vyžaduje kvalitnější nastavení správy a řízení ICT a zvyšuje nároky na jejich obsluhu. Mezi zásadní milníky patří

práce v elektronické spisové službě, využití základních registrů, povinnosti při správě dat (bezpečnost), povinnosti při správě osobních údajů (GDPR), možnost přenesení vybraných částí mimo úřad (Cloud) či posilování zájmu o digitální služby veřejné správy. Nelze odhlédnout od nových trendů a inovací v technologické části ICT, kde je primární zátěž na lidské zdroje v různých formách inovačních upgradů a postupném zařazování zcela odlišných technologických přístupů než před deseti lety. Nové systémy v mnoha případech díky jisté zastaralosti musí brát v úvahu staré frameworky a technologie při architektonických návrzích, což zadavatele stojí zvýšené úsilí, a ve většině kdy není vyhnutí i vyšší finanční nároky.

Každý informační systém prochází postupnými etapami svého rozvoje, jejichž zlomovým okamžikem je vždy uvedení do produktivního provozu nové (nebo výrazně obměněné) sady služeb, přinášejících pro zadavatele nové byznys hodnoty. Tento okamžik přináší dokončením díla (změny) tzv. přechodovou architekturu, resp. pro danou úroveň poznání a zadání v daném čase na nějaký čas cílovou architekturu systému a celého úřadu.

Období, činnosti a stavy mezi každými dvěma takovými okamžiky spuštění služeb s přidanou hodnotou nazýváme jednou etapou života systému. Etapa se tak rovná jednomu průchodu všemi fázemi životního, nebo také vývojového [36)] cyklu informačního systému, respektive jeho celého funkčního celku. Vývoj života každého IS se tak pohybuje po jakési trvale vzestupné spirále, v případě poklesu zájmu o systém a postupného odebírání funkcí i po následné sestupné spirále, tvořené etapami.

Stejně tak, jako ISVS mají oproti komerčním informačním systémům svá specifika, má je nutně i jejich životní cyklus, tzn. při řízení životního cyklu systémů / služeb ICT VS je nutné postupovat odlišně a respektovat jiné zákonné povinnosti a jiné časové termíny.

Pro zajištění potřebné adresnosti (kdo odpovídá) lze při současném respektování logiky věcné podstaty činností v životním cyklu ICT služby / informačního / komunikačního systému veřejné správy můžeme průběh každé etapy rozlišovat do těchto fází [37)]:

1. STRATEGIE
2. PLÁNOVÁNÍ A PŘÍPRAVA (včetně závěrečného návrhu realizace)
3. REALIZACE
4. PRODUKČNÍ PROVOZ (včetně řízených změn)
5. VYHODNOCENÍ
6. UKONČENÍ SLUŽBY

Grafické vyjádření logické návaznosti těchto fází v etapě života IS znázorňuje následující Obrázek:

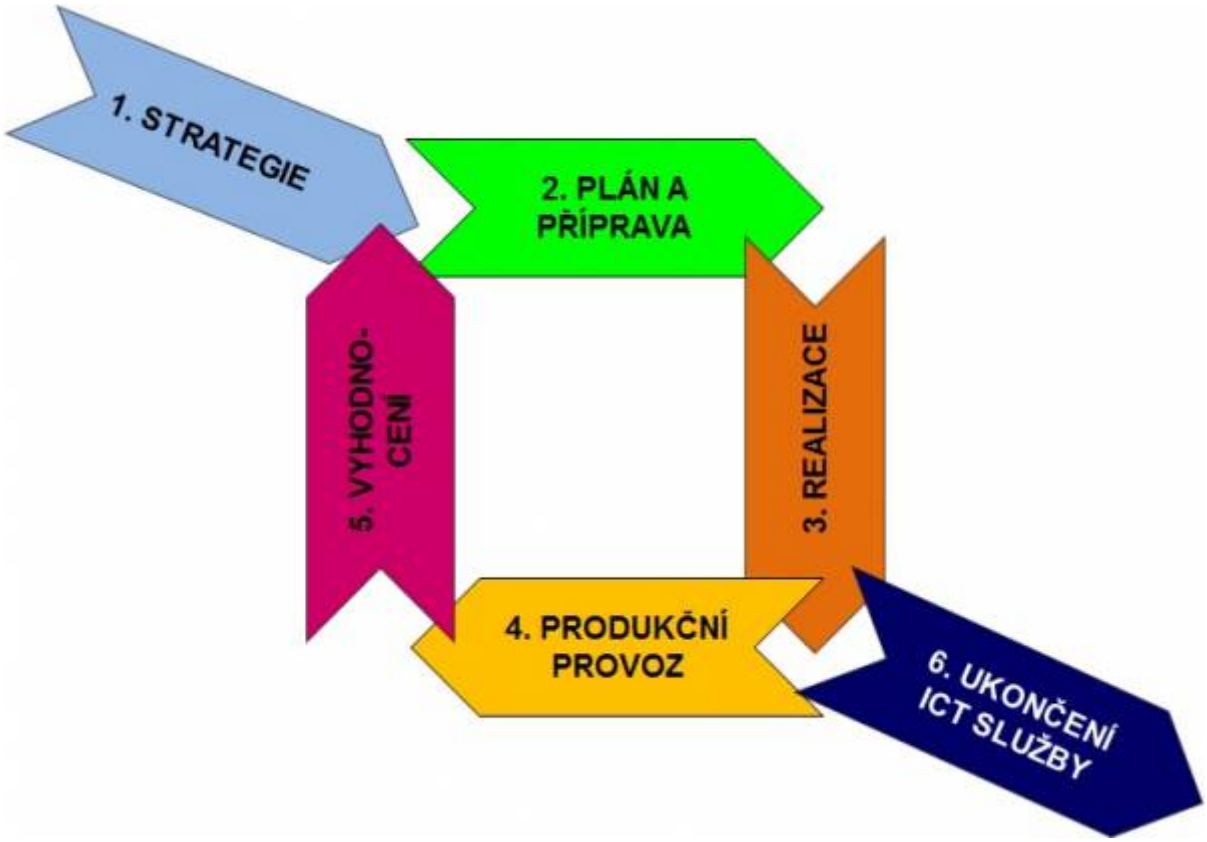
Výsadní postavení mezi životními etapami informačního systému má první a poslední průchod jednotlivými fázemi etapy jeho životního cyklu. První etapa života IS konstituuje jeho existenci, dává mu smysl, účel a zmocnění, formuje dlouhodobě jeho architekturu a platformu. Proto jsou v tomto cyklu akcentovány vnější strategické impulsy a chybí vnitřní vyhodnocení.

Poslední životní etapa IS začíná strategickým rozhodnutím o ukončení poskytování služby / existence systému, a končí fyzickou likvidací informačního systému, avšak to celé je také plánovaný a řízený implementační (archivační a likvidační) projekt, procházející fázemi plánování, přípravy a realizace.

Všechny ostatní etapy rozvoje IS představují postupné doplňování funkcí informačního systému na základě zhodnocení jeho stavu a potřeb a/nebo na základě vnějšího impulsu - strategické a legislativní změny, nebo jeho technologické a platformové povýšení (upgrade).

Etapám života a fázím životního cyklu IS odpovídá i struktura plánování a vyhodnocování nákladů na ně, viz metodika TCO.

Pojem „fáze“ znamená určité období podobných nebo spolu úzce souvisejících činností, někdy i velmi dlouhé, neměnné - například fáze produkčního provozu. Vedle toho pojem „etapa“ znamená část cesty od počátku do konce, v tomto případě od jednoho rozsahu produktivních služeb k novému rozsahu a hodnotě produktivních služeb. Etapa se tedy skládá z fází.



Rozpad těchto jednotlivých životních etap do struktury: „etapa“ (cyklus) – „fáze“ – „krok“ – „činnost“ – „úkon“, potřebný pro konkretizaci jednotlivých aktivit řízení vychází z Metodické příručky pro potřeby projektového řízení v organizacích ústřední státní správy vydané MV ČR[38)], je zpracován v tabulce: „Scénář aktivit životního cyklu ICT služby VS ČR“ a je součástí Znalostní báze**.**

Scénář aktivit životního cyklu ICT služby VS ČR (také jako „scénář“), kromě výše uvedené hierarchie aktivit, obsahuje i jednotlivé procesní kroky, konkrétní dokumenty (jak je definuje Pokyn ministra vnitra[39)]), standardně nezbytné (inicializační) vstupy a výstupy, a dále i vzájemné návazností (podmíněnost zahájení) a klíčové na aktivitě zúčastněné role.

Popisy jednotlivých výše uvedených fází každé životní etapy IS jsou pro snazší srozumitelnost všechny shodně členěny na tyto části:

1. Rámcová charakteristika fáze.
2. Principy fáze – hlavní rysy a požadavky, principy, jejichž dodržování je pro správné řízení aktivit této fáze určující.
3. Doporučené metody – metody, jejichž využití je pro danou fázi doporučeno.
4. Legislativní zakotvení – výběr legislativních dokumentů, které je při výkonu aktivit této fáze každé etapy nutné respektovat.
5. Dotčené role – výběr rolí, které by se měly na výkonu aktivit této fáze životní etapy aktivně podílet.
6. Vstupy, a zdroje, výstupy:
    - nutné vstupy – iniciátory fáze – přehled úkonů a rozhodnutí (dokumentů), které jsou nutným předpokladem = iniciují zahájení výkonu aktivit této fáze,
    - zdroje potřebné pro efektivnost aktivit v dané fázi – zdroje (informace, technické prostředky, organizační opatření, personální zdroje atd.), bez nichž nelze výkon aktivit této fáze realizovat efektivně,
    - výstupy jednotlivých fází slouží jednak k dokumentaci, že konkrétní úkon (např. rozhodnutí nebo jmenování) proběhl a jednak jako vstup následujícího úkonu / kroku / fáze.
7. Dílčí fáze a kroky – stručný popis konkrétních aktivit zařazených do této fáze životní etapy IS, plus doporučené metody, jejich hlavní milníky (výstupy a nejen termíny, ale i výstupy) a účastníci (role).
8. Postup a způsoby řízení - posloupnost dílčích fází, kroků a výstupů dané fáze, pokud je předepsána. Spolu s tím pravidla pro společné nebo jinak vzájemně související řízení v rámci fáze, projektové a liniové.

V tomto úvodním vydání MŘICT jsou pro přehlednost a srozumitelnost uvedeny u každé fáze pouze podkapitoly Rámcová charakteristika, Principy fáze a případně Dílčí fáze a kroky. Zbylé části popisu a všechny rozšiřující přílohy, obsahující výše uvedené Scénáře a další potřebné akcelerátory k jednotlivým fázím budou postupně doplňovány do odpovídajících částí Znalostní báze.

Různé části každé fáze jedné etapy životního cyklu IS mají také různé formy řízení - liniové a programové/projektové. Zatímco podstatná část plánování, přípravy a realizace radikální změny IS, případně ukončení jeho služby, se řídí jako program a projekt, s využitím projektových rolí, tak část strategických příprav, veškerý provoz, vyhodnocování a průběžné zlepšování se dějí v běžném liniovém řízení útvarů a rolí věcného a technického správce systému.

Fázím 1, 2 a 3 životního cyklu, vedoucím ke službám s novou hodnotou, odpovídá obvykle jeden rozvojový program, tvořený jedním nebo více dílčími projekty, jejichž sladěnou realizací vzniknou programem očekávané přínosy.

Každý projekt realizace podstatné změny IS, tj. vývojový a implementační projekt, bez ohledu na obsah nebo velikost, obsahuje v různém rozsahu zastoupené, ale vždy přítomné následující „projektové fáze“:

- **Identifikace, iniciace a koncepce projektu** - je naplánována budoucí existence projektu (již např. v architektonické Roadmapě IK OVS) a projekt je nahrubo definován, koncipován. Jsou stanoveny jeho cíle a základní podmínky. To se odehrává ve fázi ŽC IS č. 1-Strategie.
- **Plánování a příprava projektu**, po jeho schválení a zahájení, včetně ustavení projektových struktur a jeho materiálního a personálního zajištění ve fázi č. 2-Plánování a příprava.
- **Realizace projektu**, typicky po výběru dodavatele, zahrnující ustavení společných projektových struktur s dodavatelem, cílový koncept řešení a dodávku (vývoj, implementace) řešení v míře odpovídající zvolenému způsobu realizace (vodopád, agilní, kombinace, ...), včetně testování.
- **Příprava produktivního provozu**, zahrnující přípravu včetně školení, migrací dat, okamžik zahájení užívání a počáteční rozšířenou podporu dodavatele, oba body ve fázi č. 3-Realizace.
- **Uzavření projektu**, zahrnující závěrečnou akceptaci výstupů a předání řešení do trvalé podpory, na počátku fáze č. 4-Provoz.
- **Průběžné plánování, monitoring a řízení projektu**, ve všech fázích projektu a v odpovídajících fázích 1, 2, 3 a 4 etapy životního cyklu.

Fáze životního cyklu IS	**Fáze realizačního projektu**	**Klíčové výstupy a milníky**
STRATEGIE	* Identifikace, iniciace a koncepce	* Strategické zadání. * Informační koncepce OVS, obsahující projekt. * Enterprise architektura projektu. * Stanovisko OHA
PLÁN A PŘÍPRAVA	* Plánování a příprava projektu	* Definice projektu[40)], Projektový záměr. * Architektura řešení projektu. * Funkční a ne-funkční specifikace. * Rozhodnutí o (ne)realizaci projektu * Investiční záměr * Registrace projektu na MF. * Rozpočtové opatření úřadu vč. určení příkazce * Zadávací dokumentace VZ. * Výběr dodavatele / Smlouva s dodavatelem.
REALIZACE	* Realizace projektu * Příprava produktivního provozu	* Blueprint[41)] * Vývojové zadání * Testovací scénáře a protokoly * ... a mnoho dalších.
PRODUKČNÍ PROVOZ	* Uzavření projektu	* Akceptační protokol. * Dokumentace skutečného provedení. * Vyhodnocení projektu = Zpráva o průběhu projektu.

Fáze životního cyklu IS	Fáze realizačního projektu	Klíčové výstupy a milníky
Průběžně - přes 1, 2, 3 a 4	* Plánování, monitoring a řízení projektu.	* Plán řízení projektu, včetně * Plán zdrojů * Registr rizik a dalších

Vztah fází životního cyklu IS a fází typického realizačního projektu.

Další výstupy a milníky fází realizačního projektu jsou popsány v detailních materiálech Znalostní báze k jednotlivým fázím etapy životního cyklu a k metodice řízení projektů.

Překrývání etap životního cyklu. Etapy životního cyklu jednoho IS se mohou vzájemně překrývat s fázovým posunem. Tedy současně jsou některé služby IS rutinně provozovány, některé služby z dřívějších etap již jsou utlumovány a likvidovány a nové služby z další etapy rozvoje systému jsou plánovány nebo realizovány.

Překrývání fází jedné etapy. Stejně tak fáze jedné etapy se ve svých činnostech mohou překrývat či předbíhat. Například ještě nejsou provedeny všechny činnosti uzavření realizačního projektu a finální předání řešení do produktivního provozu, přesto již jsou služby jako výstupy projektu produktivně užívány.

Manažeři věcného i technického správce, provozovatele i dodavatele se musí v jednotlivých etapách a fázích orientovat a jejich souběhy a překryvy vědomě zvládat.

Fáze 1 - STRATEGIE

Rámcová charakteristika strategie

Fáze strategie obsahuje aktivity uskutečňované při formulování strategií rozvoje veřejné správy, OVS (jeho rezortu) a jeho IT útvaru a v odpovídajících změnách právních předpisů, z nichž vyplynou požadavky na nové nebo změněné služby ICT podpory výkonu veřejné správy. Do strategické fáze byly – vzhledem k životnímu cyklu jedné ICT služby / jednotlivého systému VS, zařazeny i kroky strategického plánování prováděné společně za všechny ICT služby a systémy úřadu, konkrétně vytvoření a aktualizace Informační koncepce OVS, se současnou aktualizací jeho architektury úřadu (EA).

Fáze strategie zahrnuje aktivity související s formulováním strategií rozvoje veřejné správy, strategií OVS a jejich IT útvarů a v odpovídajících změnách právních předpisů, z nichž vyplynou požadavky na nové nebo změněné služby ICT podpory výkonu veřejné správy. To platí zejména v případě ústředních správních úřadů, v jejichž odborné gesci jsou jednotlivé právní předpisy a u nichž je možné a potřebné se na tvorbě celostátních strategií a právních předpisů z pozice informatiků podílet.

U ostatních úřadů, zejména pak u úřadů územních samospráv je třeba přizpůsobovat vlastní strategie v závislosti na změnách právních předpisů a požadavcích na fungování veřejné správy ze strany občanů.

Součástí fáze strategie jsou tyto činnosti:

- Podíl na tvorbě strategických dokumentů vlády, nebo spolupráce formou poskytnutí vstupů a zpětné vazby.
- Podíl na tvorbě nebo změně právních předpisů, a/nebo studium existujících a připravovaných právních norem a předpisů, včetně norem a nařízení EU a analýza jejich vlivu na ICT prostředí OVS.
- Podíl na tvorbě vlastních strategických dokumentů OVS, včetně vypracování ICT strategie OVS, pokud ji OVS vytváří, ev. rezortu, je-li taková strategie vytvářena.
- Analýza potřeb zainteresovaných stran, tj. zejména vedení úřadu a potřeb odborných oddělení na základě komunikace s věcnými garanty jednotlivých odborných agend.
- Identifikace s cíli a plány OVS a rezortu, s cíli a plány na národní úrovni (IKČR a další), s cíli a plány na úrovni EU a vytvořit vlastní cíle ICT.
- Vypracování a aktualizace dlouhodobé architektonické vize a celkové architektury úřadu (EA) OVS.

- Vypracování analýzy obsahující stav nyní (As-Is) v následujících obdobích nebo při změnách pak **vždy** vytvořit analýzu rozdílovou s vyhodnocením rozdílu formou samostatného, manažerského shrnutí (toto shrnutí je možné připojit jako přílohu dané rozdílové analýzy).
- Zajištění ostatních potřebných vstupů pro navazující fázi přípravy a strategické a projektové plánování
- Vypracování a aktualizace Informační koncepce OVS, respektive dalších na ni navazujících střednědobých a dlouhodobých plánů rozvoje ICT prostředí OVS.
- Prioritizace identifikovaných záměrů a příprava střednědobých výhledů a dlouhodobých finančních plánů pro naplnění plánů rozvoje ICT, umožňujících přesné plánovaní a čerpání rozpočtu, nejlépe formou ročních akčních plánů pro implementaci cílů a adaptaci na ně.

Fáze 1 – Strategie je sice nedílnou součástí každé životní etapy jednotlivého IS, ale plnou měrou se u ní uplatní a převažují metody a prostředky strategického řízení a plánování ICT na úrovni celého útvaru a úřadu, v kontextu eGovernmentu ČR a EU, viz Řízení na úrovni útvaru ICT.

Pro usnadnění a podporu procesů fáze řízení strategie budou do Znalostní báze NA VS ČR postupně doplněny zejména:

1. Zásady, postupy a příklady na podporu tvorby tzv. Digitálně přívětivé legislativy.
2. Referenční model, architektonické vzory, tabulkové šablony a detailní pokyny pro tvorbu a údržbu architektury úřadu a její vize.
3. Kontrolní seznamy potřebných vstupů pro tvorbu architektury a plánování projektů.
4. Vzorová šablona a další pomůcky pro tvorbu Informační koncepce OVS, zejména kontrolní seznamy pro ověřování shody s IK ČR.
5. Pomůcky a postupy pro prioritizaci záměrů před a po schválení rozpočtu.
6. Pomůcky a postupy na podporu přípravy a vyjednávání o rozpočtu.
7. Pomůcky, návody a zdroje pro definici cílů.
8. Předlohy podob akčních plánů.

Principy a pravidla utváření strategie

- **Zásady strategického plánování ISVS v kontextu architektury úřadu.** Pro každý ISVS úřadu musí být ve společné Informační koncepci úřadu (také jako "IK" nebo "IK OVS") stanoveno, jaký je žádoucí cílový stav ISVS na konci plánovacího horizontu IK a proč a jakými projekty, případně programy budou potřebné změny IS realizovány a v jakém časovém horizontu.
- **Návaznost na celkovou (věcnou, byznys) strategii a IT strategii úřadu, vycházející ze strategie eGovernmentu.** Dlouhodobé řízení informačních systémů veřejné správy se musí opírat o strategické cíle úřadu v oblasti výkonu veřejné správy a jeho informační podpory, v kontextu strategických cílů nadřazených struktur úřadu. Není přípustné vytvářet v IK úřadu dlouhodobý plán ISVS bez doložitelného a srozumitelného odkazu na plány rozvoje a změn agend, které ISVS podporuje, a bez kontextu plánovaných změn úřadu a eGovernmentu jako celku. Není možné vytvořit nebo aktualizovat IK OVS bez předchozí aktualizace jejích strategických vstupů (agendové strategie, strategie úřadu a IT strategie) a naopak, po každé změně těchto vstupů se musí zkontrolovat platnost IK OVS a případně ji aktualizovat.
- **Architektura ISVS.** Každý věcný správce ISVS a věcný správce centrálního prvku eGovernmentu je povinen pro tento systém udržovat model stávající, cílové a případně přechodné architektury na úrovni architektury úřadu (EA) a architektury řešení (SA), souladu s metodikou Národního architektonického rámce. Pro potřebu žádosti o stanovisko OHA k programu, investičnímu záměru a projektu je dostatečný model požadovaného stavu architektury ISVS na úrovni podrobnosti architektury úřadu (PSA)[42)]. Po získání kladného stanoviska OHA, je-li toto z hlediska objemu projektu relevantní, je zapotřebí rozpracovat architekturu ISVS, nebo její změny, pro účely výběru řešení a dodavatele řešení do formy tzv. architektury řešení[43)]. Z té se následně sestavuje seznam požadavků funkční a tzv. ne-funkční (myšleno ostatní než funkční) specifikace[44)] pro účely zadávací dokumentace výběrového řízení dle ZoZVZ.
- **Kombinace všech požadavků.** Součástí strategického naplánování každého ISVS na počátku nové etapy jeho rozvoje musí být kombinace strategických požadavků na změny s mandatorními požadavky například na bezpečnost (GDPR), na elektronickou identifikaci a dokumenty (eIDAS) nebo cíle a standardy eGovernmentu (IKČR). U již existujících IS musí být tyto externí požadavky kombinovány s interními

požadavky, plynoucími z vyhodnocení stávajícího stavu IS (fáze 5).

- **Periody řízení.** Činnosti a výstupy ve fázi 1 – Strategie jsou řízeny v průběžném, periodickém a Ad-Hoc režimu:
  - **Průběžně** je aktualizována celková (enterprise) architektura OVS, vždy po dokončení implementace jakékoli změny, ale také po změně strategie a v rámci realizace změnového řízení.
  - **Periodicky**, nejméně jedenkrát za 2 roky, ale také vždy při změně strategických vstupů, je aktualizována Informační koncepce OVS.
  - **Periodicky - každoročně**, v období před zahájením přípravy rozpočtu, je aktualizován plán projektů z IK OVS (Roadmapa).
  - **Ad-hoc**, když nastanou a jsou identifikovány nové požadavky a zásadní podněty (volby, změna vedení, nová legislativa apod.).

Fáze 2 - PLÁN A PŘÍPRAVA

Rámcová charakteristika plánování a přípravy

Fáze obsahující kroky a aktivity navazující na v předchozí fázi stanovené strategické směrování jednotlivého informačního systému, toto směrování rozpracovává do návrhu jednotlivých potřebných změn, jejich vzájemných souvislostí a časového plánu. Součástí fáze jsou i všechna nezbytná připomínkování, posouzení a schvalování zvoleného způsobu řešení, tj. záměru rozvoje ICT úřadu, jako podmínky zahájení souvisejících výdajů ze státního rozpočtu

Projekty změn služeb veřejné správy se stále více opírají o podporu informatiky. Všechny projekty v úřadu navíc sdílí omezené množství pro projekty vhodných lidských zdrojů. Z těchto důvodů musí být všechny projekty v oblasti informatiky prokazatelně koordinovány se všemi běžícími i plánovanými projekty celého úřadu, ať již společně tvoří těsně provázané rozvojové programy nebo budou řízeny jenom volněji jako portfolia projektů.

Důležitá je komunikace s útvarem účetnictví o účetní povaze pořizovaných aktiv a dalších plnění. Ne vše, co se odborníkovi na ICT může jeví jako dlouhodobý majetek jím z účetního pohledu skutečně je. Při opomenutí mohou nastat závažná rizika porušení rozpočtové kázně a dalších sankcí.

Metody a postupy fáze 2 – Plánování a příprava představují naplnění Zásad a postupů pro pořizování a vytváření informačních systémů veřejné správy - část I, a podklad pro aktualizaci a doplnění těchto zásad dle Vyhlášky č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy), o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy) v okruhu otázek: jak nalézt správné řešení pro naplnění byznys potřeb poskytování veřejných služeb (a jejich změn).

Popis fáze uvádí, kromě jiného, základní povinnosti, jak postupovat z pozice útvaru ICT při hledání nejvhodnějších ICT řešení pro optimální naplnění byznys potřeb úřadu při dodávce jeho veřejných služeb.

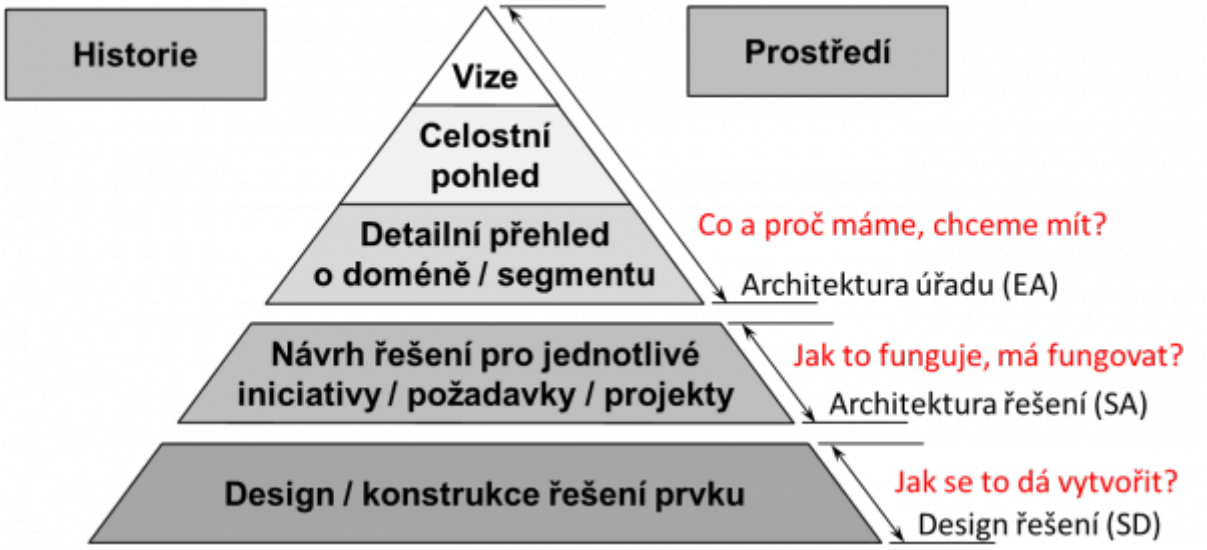
Ve fázi Plánování a přípravy v čase jdou vedle sebe, doplňují se a prolínají 3 pracovní proudy, podrobněji viz Tabulka 3:

- věcný, obsahové plánování – co má být předmětem cílového řešení (architektura)
- plánování zdrojů, zejména lidských a finančních (projektové plánování)
- zajištění legitimity změn – legislativní příprava

Míra poznání / Proud	Legislativa záměru	Architektura záměru	Zdroje záměru
Úvodní představa	Návrh záměru zákona	Enterprise Architektura záměru	Nárok na rozpočet a pracovníky
Zpřesněná představa	Schválený zákon ve finálním znění	Architektura řešení záměru	Alokované zdroje
Proveditelné zadání	Vydány vyhlášky a Interní akty řízení	Design řešení	Vydané zdroje na řešení

Přehled vztahů souběžných pracovních proudů fáze Plánování a přípravy.

Věcné plánování, tedy architektonická příprava, se odehrává v krocích postupně se zvyšujícího detailu poznání, vyjádřeného v grafických modelech a seznamech požadovaných komponent a jejich vlastností; ve shodě s tím, jak tyto úrovně definuje NAR, viz následující Obrázek:



Na základní modely cílové architektury úřadu, vytvořené v rámci předchozí fáze 1-Strategie pro celý úřad a využité pro vydání Informační koncepce OVS, navazuje tzv. „architektura před startem projektu“ (PSA[45]). Tato architektura poskytuje model budoucího řešení a jeho nejbližšího kontextu na úrovni detailu EA a obsahuje spolu se základním projektovým záměrem dostatek údajů pro sestavení Žádosti o stanovisko OHA.

Následuje nalezení tzv. architektury řešení, která se zaměřuje na otázku, jak má hledané řešení fungovat a je vedle grafických diagramů vyjádřena tzv. funkční a ne-funkční specifikací. Nezbytnou součástí je rozhodnutí o variantě řešení. Společně s upřesněným projektovým záměrem, obsahujícím rozhodnutí o strategii implementace, o způsobu zajištění vlastních, odsouhlasení CBA a rozhodnutí o pokračování procesu směrem k pořízení řešení (nákupem, vývojem nebo kombinací), je architektura řešení a specifikace základem zadávací dokumentace veřejné zakázky.

Předpokladem pro věcné plánování a přípravu je podíl ICT specialistů na tvorbě věcného záměru příslušného právního předpisu spojeného se změnou, a to zejména a plnou měrou, pokud se jedná o OVS, v jehož gesci je předmětná právní úprava a jež bude správcem příslušného IS. Úlohou ICT v této oblasti je zejména:

- poskytnout legislativnímu týmu potřebnou schopnost systémového myšlení a širokého kontextu celého úřadu a eGovernmentu ČR a EU,
- přispět k DPL - digitální přívětivosti zákona znalostmi zejména aktuálních technologických možností a uživatelských zvyklostí a očekávání,
- poskytnout logickou kontrolu a včasné ověření reálné proveditelnosti dopadů zákona do realizace v ICT,
- včas získávat informace pro další plánovací činnosti v ICT

Proto je úloha ICT nejvýraznější již ve fázi prvních idejí a formulování věcného záměru změny předpisu, ale přetrvává až do definitivního schválení předpisu a jeho prováděcích předpisů.

V projektovém plánování zdrojů je nezbytné včas a s dobrou znalostí připravované legislativy, potřebného rozsahu změn a prací a jejich termínování žádat a zajišťovat všechny druhy zdrojů k tomu existujícími úkony a dokumenty (programové financování, projektový záměr, …). Důležitou součástí přípravy zdrojů je získání externích zdrojů, tj. výběr dodavatele úspěšným procesem veřejné zakázky a uzavřením smlouvy, finálně v sobě spojující výstupy všech tří souběžných plánovacích a přípravných proudů.

Úspěch a efektivita fáze Plánování a přípravy závisí velkou měrou na tom, jak se podaří načasovat práce ve

všech třech proudech a jak se podaří vzájemně využívat poznání a výstupů z jednotlivých činností a vyhnout se duplicitním pracím a dokumentům.

Důležitým předpokladem úspěchu celého životního cyklu je již ve fázi Plánování a příprav zahrnout do rozsahu a záměru, zadání a smluv také:

- Zohlednění všech mandatorních potřeb a pravidel, nesvázaných s příslušným agendovým nebo provozním předpisem (eIDAS, bezpečnost, GDPR, e-Identita, principy eGovernmentu z IKČR apod.).
- Vytvoření předpokladů pro následné efektivní řízení kvality a výkonnosti služeb (SLA).
- Vytvoření předpokladů pro převzetí znalostí od dodavatelů a zmírnění závislosti na nich.
- Vytvoření předpokladů pro vybudování a zajištění schopnosti úřadu provozovat (nebo ovládat provoz) řešení a další předpoklady.
- Vytvoření předpokladů pro vyhodnocení měřitelných parametrů projektů, řešení i dodavatelů ve fázi 6.

Optimalizace tohoto souběhu plánovacích proudů, zajištění uvedených předpokladů a usnadnění všech činností bude předmětem dokumentů a pomůcek, které budou součástí dalšího vydání MŘICT a Znalostní báze.

Principy a pravidla plánování

- Plánování a příprava jednotlivého programu či projektu se musí dít v souladu a s využitím metod a nástrojů plánování programů, projektů a portfolií na úrovni celého úřadu a v kontextu celého eGovernmentu.
- Souběh a soulad tří plánovacích a přípravných proudů (legislativní, architektonický a zdrojový).
- Podíl informatiků na tvorbě právních předpisů záměru (pokud je to pro OVS relevantní).
    - spolupráce při zadání a identifikaci potřeb,
    - konzultace a potvrzení z hlediska věcné správnosti,
    - revize a schválení výsledného znění z hlediska věcné správnosti.
- Postupné plánování cílového stavu se záměrem spojeného funkčního celku přes všechny 4 vrstvy architektury.
- Včasné plánování a alokování všech potřebných zdrojů (finančních, lidských, technických i znalostních).
- Zohlednění všech mandatorních požadavků.
- Komunikace s útvarem účetnictví o účetní povaze pořizovaných aktiv a dalších plnění
- Vytvoření předpokladů pro následující fáze.
- Využití principu ex-ante kontroly a nástrojů PoC (Proof of Concept), viz další kapitoly.
- V EA modelech pomocí dekompozice služeb vytvářet předpoklady, motivátory a rozhraní pro měření KPI a následné vyhodnocování SLA a OLA a řízení (SLM).
- Při dekompozici vždy uplatňovat a plánovat, co bude outsourcováno a co insourcováno, a provést analýzu dopadů na rozpočet OVS (v případě požadavků na UC) a na interní zdroje a jejich kapacitu (v případě požadavků na interní OLA).
- V případě využití sdílených služeb brát při sestavování úrovně služby (% dostupnosti) všechny SLA včetně sdílených a až dle těchto ukazatelů navrhovat SLA s garanty a navrhnout monitoring.
- Do definice SLA vždy zařadit požadavky všech aktérů a klíčových uživatelů.
- Vždy pečlivě plánovat kapacity pro realizaci a následný provoz nejlépe formou dopadové analýzy, a to na zdroje:
    - Finanční
    - Technické (včetně nástrojů pro podporu projektů (PPM) a provozu (ServiceDesk)
    - Lidské (včetně operátorů HelpDesku a zdrojů potřebných na součinnosti)
- Vždy vypracovat matici rizik změn jako přílohu pro dokumentaci v rámci realizace, o rizicích musí být informováno minimálně vedení útvaru ICT, věcný garant a sponzor projektu.
- Určit mandatorní smluvní požadavky zejména pak:
    - autorská práva,
    - sankce a slevy,
    - katalogové SLA listy,
    - definice součinností,
    - exitové strategie a povinností, atd.

Fáze 3 – REALIZACE

Rámcová charakteristika realizace

Fáze realizace plánovaných změn informačního systému představuje jádro vývojového a implementačního projektu, naplánovaného, spuštěného a koncepčně rozpracovaného v předchozí fázi této etapy životního cyklu řešení. Realizace uskutečňuje vlastní dodávku standardního aplikačního SW vybavení, jeho parametrizaci a programové přizpůsobení a/nebo vývoj SW na míru a/nebo pořízení SW jako služby. Pro obě formy pořízení SW tzv. „On-premise“ představuje realizace také dodávku platforem a infrastruktury, vybudování všech potřebných běhových prostředí [46)], a to minimálně třístupňového (vývojové, testovací a produkční), optimálně u rozsáhlých systémů čtyřstupňového (vývojové, testovací, preprodukční a produkční) ve výjimečných odůvodněných případech je přípustné dvoustupňové (nekritické systémy bez kritických dat a integrací např. BI) a ustavení schopnosti úřadu provozovat a podporovat řešení.

Metody a postupy fáze realizace nahrazují a rozvíjejí tzv. Zásady a postupy pro pořizování a vytváření informačních systémů veřejné správy – část II (implementace nakoupeného řešení a pořízení řešení vývojem, nebo kombinace obou). Půjde o podstatné doplnění zásad dle Vyhlášky č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy) v okruhu otázek: jak vybrané řešení úspěšně zavést a uvést do produktivního provozu. Tedy podstatné a celostátně plošně platné standardy k požadavkům vyhlášky (po její předpokládané novele).

Řízení projektů realizace jednotlivých IS musí být prováděno v kontextu řízení změn na úrovni celého útvaru ICT a změn celého úřadu, viz zejména Řízení na úrovni útvaru ICT. To znamená zejména:

- společné řízení dílčích projektů v rámci celkového řízení portfolií a programů
- společné řízení IT a ne-IT změn
- společné řízení velkých (např. projektových) a malých (např. liniových, průběžných) změn – sdílenými postupy, nástroji a zdroji.

Pro usnadnění a podporu procesů fáze řízení realizace budou do Znalostní báze postupně doplněny zejména:

1. Doporučené postupy a metodiky pro tvorbu a záznam analytických modelů na úrovni architektury řešení (SA) a designu řešení (SD)
    1. Datové modely
    2. Procesní modely
    3. Dekompoziční modely
    4. Use-Case a stavové modely
2. Doporučené normy a metodiky pro projektové řízení realizačních projektů (včetně případného vývoje)
3. Interní vývojové normy

Principy a pravidla realizace

- Změny od určité velikosti, rozsahu či charakteru musí být řízeny jako projekt.
- Akceptaci řešení provádí vždy klient (zadavatel, věcný správce) ve spolupráci s dalšími zúčastněnými stranami (integrované OVS, SZR, ...).
- Struktura kroků, výstupů a metod projektu musí odpovídat zvolenému typu zaváděného řešení (hotový SW, vlastní vývoj, SW jako služba), implementační strategii (Big-Beng, Pilot-Roll/out) a vývojové strategii (Waterfall/Agile) a jejich případným kombinacím.
- Projekty s vyššími nároky na přizpůsobení uživatelů musí obsahovat adaptační aktivity dle metodiky OCM, které bude doplněno do Znalostní báze.
- Činnosti fáze realizace jednoho IS musí být vždy vykonávány v souladu s metodami řízení realizace na úrovni celého útvaru/úřadu a s využitím společných metod a nástrojů.
- V případě realizace velkého projektu dodavatelem s globální osvědčenou metodikou řízení projektů a vývoje je možné použít tuto metodiku, pokud bude v souladu ustanoveními tohoto dokumentu a jeho

příloh a pokud se ji podaří provázat s povinnými (minimálními) kroky a výstupy řízení projektů VS ČR, až budou vydány.

Dílčí etapy / kroky realizace

Realizace projektově řízené změny IS ve fázi 3. jeho životního cyklu, typicky po výběru dodavatele, představuje uskutečnění následujících projektových fází realizačního projektu dle metodiky projektového řízení:

- **Ustavení projektových struktur**, společných týmů s dodavatelem, vyčlenění prostor, sjednání projektového kalendáře, zprovoznění platformy sdílení znalostí a dokumentů, apod.
- **Prováděcí projekt** (alias Blueprint, cílový koncept, analýza a návrh řešení, apod.), a to nejméně:
  - Byznys koncept - jak se bude řešení používat (funkce, procesy, služby, role, výstupy-produkty, apod.)
  - IT koncept - jak bude řešení zhotoveno, parametrizováno či vyvinuto, aby naplnilo byznys koncept, včetně
  - Koncept bezpečnosti a ochrany osobních údajů - jak budou zapracovány mandatorní požadavky
  - Koncept zajištění všech IT prostředí, včetně provozní infrastruktury
  - Koncept testování a ověřování
  - Koncept rolí a oprávnění
  - Koncept migrace dat a uvedení do produktivního provozu
  - Aktualizace architektury řešení (přes všechny vrstvy), případně změna EA, pokud na ni vede změnové řízení.
- **Vývoj a implementace řešení**, tj. vytvoření vývojového a testovacího IT prostředí včetně OS, platforem a databází, instalace, parametrizace a přizpůsobení hotových řešení a vývoj SW řešení na míru, včetně všech forem ověřování požadované funkčnosti - testování, ověření konceptu (PoC[47)]) a dokumentace vývoje a nastavení.
- **Příprava produktivního provozu**, zahrnující vytvoření produkčního IT prostředí, včetně zajištění služeb třetích stran, přípravu uživatelů včetně školení, migrací dat, okamžik zahájení užívání, ustavení vlastní schopnosti úřadu provozovat a podporovat řešení (včetně monitorovacích nástrojů dostupnosti a odezvy služeb) a počáteční rozšířenou podporu dodavatele.
- **Uzavření projektu**, závěrečnou akceptaci výstupů a předání řešení do trvalé podpory, včetně kompletní vývojové, provozní a uživatelské dokumentace skutečného provedení řešení.
- **Průběžné plánování, monitoring a řízení projektu** - probíhá ve všech fázích projektu.

Jednotlivým projektovým fázím je podřazena celá řada dílčích činností, milníků a výstupů, viz podrobné dílčí kapitoly ve Znalostní bázi.

Důležitou projektovou činností na počátku realizace je ustavení projektových struktur a mobilizace jeho interních lidských a materiálních zdrojů.

Od okamžiku produktivního spuštění prvních služeb, zařazených do rozsahu realizačního projektu, začíná tento naplňovat současně i obsah fáze životního cyklu č. 4 - Provoz a osoby a týmy, zodpovědné na straně zákazníka a případně outsourcovaného provozovatele, se musí aktivně na těchto projektových fázích podílet, počínaje přípravou produkčního prostředí a produktivního provozu.

Fáze 4 - PRODUKČNÍ PROVOZ

Rámcová charakteristika provozu

Fáze produktivního provozu je charakteristická potřebou zajistit dodávku služeb, uvedených do provozu k předchozímu milníku, při zachování parametrů kvantity, kvality i bezpečnosti služby a pokud možno při rostoucí hospodárnosti a efektivitě dodávky služby, umožněné prohlubování zkušeností i průběžným zlepšováním provozu beze změny služby. Stručně řečeno jde o zajištění dohodnutých úrovní služeb (SLA ev.

OLA).

Druhou klíčovou charakteristikou fáze produktivního provozu je, že se během ní realizují převážně průběžným, liniovým řízení útvaru ICT a/nebo smluvního partnera drobné změny rozsahu nebo kvality služeb, které pro své uskutečnění nevyžadují aktivity fází 2 - příprava a plánování a 3 - realizace změny. Stručně řečeno jde o nepřetržitou identifikaci, kvalifikaci, plánování a realizaci drobných změn, tedy sběr požadavků a změnové řízení.

Je důležité identifikované změny klasifikovat z hlediska jejich velikosti, způsobu řízení jejich realizace a hlediska jejich priorit. Základní prioritou technického správce a provozovatele je předcházení nedostupnosti služeb systému a splnění termínu realizace změn služeb (zejména legislativních). Ostatní změny s nízkou prioritou je účelné sdružovat do balíků práce k termínům nových verzí předmětného řešení. Do této skupiny patří i změny zaměřené na měřitelná zlepšení efektivnosti, tedy změny přinášející významnou úsporu zdrojů (finančních, technických nebo organizačních). Na posledním místě z hlediska provozu jsou změny, které nenaplňují ani jednu z výše uvedených kategorií, ale například zvyšují kvalitu služby a komfort pro uživatele.

Výše uvedené musí odrážet vztah mezi řídící osobou, zodpovědnou za dodávku služeb informačního systému, a interním útvarem nebo externím dodavatelem. Tento smluvní vztah a obecně schopnost úřadu (technického správce) zajistit efektivní provoz je nutno zahrnout již do fází přípravy, plánování a realizace vzniku nového systému nebo jeho zásadní změny. Zodpovědná osoba musí být oprávněná a kompetentní k rozhodování o správě a provozu systému a o čerpání zdrojů, včetně garantovaných tzv. mandatorních zdrojů (rozpočtu provozních nákladů, povinných interních rolí, materiálně-technického zabezpečení).

Provozem se myslí i zajištění chodu infrastruktury nezbytné pro dodávku aplikačních služeb. Pořízení a obměna infrastruktury se řídí podle pravidel fází 2 a 3, případně 1 životního cyklu řešení.

Důležitou podmínkou a součástí řízení provozu je udržování aktuální produktové (vývojové), provozní a uživatelské dokumentace informačních systémů, tj. funkčních celků ve všech vrstvách jejich architektury. Majetek je v této fázi již ve stavu způsobilém k užívání a může být tedy účetně zařazen do majetku a má mu být stanoven odpisového plánu (doby odpisování). Při opomenutí odpisového plánu je zde riziko neprůkaznosti účetnictví.

Pro podporu obou aspektů provozu (kontinuální dodávky služeb i identifikace a realizace změn) je klíčové poskytování uživatelské i technické podpory.

Více o klíčových metodách používaných při řízení provozu na úrovni každého IS se nachází v Řízení jednotlivých ICT řešení.

Vedle činností pro zajištění provozu služeb jednotlivých informačních systémů je nutné vybudovat a užívat schopnosti provozního řízení centralizovaně, napříč jednotlivými IS, ať již je to například:

- celková správa datových center a virtualizované infrastruktury
- celková správa klíčových aplikačních platforem
- celková péče o uživatele
- celkové řízení konfigurace řešení
- celkové plánování a řízení změna a verzí
- celkové plánování a řízení zdrojů pro provoz

Více v kapitolách o metodách provozního řízení na úrovni ICT útvaru, Řízení na úrovni útvaru ICT.

Pro usnadnění a podporu procesů fáze řízení provozu budou do Znalostní báze postupně doplněny zejména následující akcelerátory:

1. Obecné návrhy na monitoring dostupnosti a odezev
2. Vzorové procesy HelpDesku
3. Odpovědnost klíčových rolí a jejich kompetence (jako součást celkové matice RACI)
4. Odkazy na dokumenty, které jsou pro tuto fázi nezbytné / doporučené
5. Popis strategie a realizace zálohování, včetně ověření, zda procesy obnovy jsou funkční.

Principy a pravidla provozu

- Zajistit chod nezměněné služby
- Zajistit realizaci změn pro udržení kvality služby a pro její průběžný rozvoj
- Zajistit realizaci změn pro zvýšení efektivity služby
- Realizovat pouze „malé“ změny, nepředstavující projekty ve fázích 2 a 3 životních etap informačního systému
- Vytvořit a řídit Katalog ICT služeb (aktuálně provozovaných)[48)].
- K údržbě a rozvoji ICT služeb (systémů) VS, za jejichž flexibilní legislativní rozvoj jako věcný správce OVS odpovídá, mít vlastní útvar, nebo ovládané středisko kompetence (útvar podpory služeb, kompetenční centrum).
- Všechny poskytované služby jsou monitorovány min. na úrovní End2End (business strojové scénáře a skripty) monitoringu.
- Provoz jednotlivého IS se vždy řídí v kontextu a vykonává prostředky řízení provozu celého úřadu.
- Všechny potřeby vzniklé samotným provozem dílčího celku se musí sdružovat jednom místě a u jedné odpovědné osoby.
- Všechny služby musí být obsluhovány jednotně pomocí jednotlivých ITSM managementů.
- Musí probíhat řízení kvality služeb za pomocí SLM, pravidelné SLA negociace, a to jak na úrovni pracovních týmů, tak řídících výborů.
- Stanovení odpisového plánu (doby odpisování) pro majetek.
- Nutnost reakce na bezpečnostní incidenty spojené s osobními údaji.

Dílčí etapy / kroky provozu

Kroky řízení provozu lze seskupit do čtyř oblastí:

- Zajištění provozního (běhového) prostředí (typicky projektově již jako součást fáze realizace) a převzetí zodpovědnosti za dodávku služeb pořízených řešení.
- Zajištění zachování požadované úrovně služeb
  - Úkony provozní bezpečnosti – dle Disaster Recovery plánu
  - Monitoring dosahované úrovně služeb včetně bezpečnostního monitoringu
  - Zajištění správy identit a přístupu privilegovaných uživatelů v oblasti bezpečnosti a provozu.
  - Prevence a profylaxe
  - Údržba HW a SW
- Podpora uživatelů
  - HelpDesk / ServiceDesk s procesy obsluhy a správy incidentů, správy problémů a iniciace procesů správy změn
- Průběžný rozvoj řešení – řízení realizace změn s kroky:
  - identifikace a klasifikace incidentů a požadavků na změnu
  - posouzení a prioritizace změnových požadavků
  - plánování změn a řízení verzí
  - realizace a dokumentace změn
  - Informování o změnách a rozdílová školení.

Fáze 5 - VYHODNOCENÍ provozu a služeb IS

Rámcová charakteristika vyhodnocení

Součástí fáze Vyhodnocení provozu a služeb je několik podstatných typů vyhodnocení, zejména vyhodnocení:

- zda realizační projekt dosáhl plánovaných hodnot (rozsahu, času, potřeby zdrojů) a očekávané kvality výstupů,
- zda se daří dodávat ICT služby v očekávané úrovni (SLA) - interním nebo externím provozovatelem,

- jaké problémy a požadavky na změny lze dovodit z nahlášených incidentů (neshod),
- zda se s podporou těchto ICT služeb daří dosáhnout očekávaných byznys benefitů, tj. zda se naplnily parametry a přínosy ICT investice,
- zda kombinace přetrvávající byznys potřeby ICT služeb a jejich udržitelné kvality dává i nadále důvod pro zachování nebo rozvoj řešení, resp. naopak pro ukončení poskytování služeb tohoto systému,
- jaká rizika a opatření pro jejich zmírnění se pojí s projektem změny nebo s provozem ICT služeb systému.
- zda dodavatelé naplňují smluvní očekávání kvalitní a vyvážené spolupráce nebo je třeba je z další spolupráce vyřadit.

Důležitým významem vyhodnocení realizačního projektu je, pokud jeho závěry mohou být použity nejen pro lepší nastavení vnitřních pravidel řízení, ale také pro závěry směrem k dodavatelům. V tuto chvíli již je již taková konstrukce možná. Zákon o kybernetické bezpečnosti se v politice řízení dodavatelů zcela jasně vymezuje vzhledem ke kvalitě dodávaného řešení. Zákon o zadávání veřejných zakázek se zcela jasně vymezuje vzhledem k porušení bezpečnosti. Souladem těchto zcela již dnes identických podmínek jsme schopni definovat kvalitu uchazeče /dodavatele a v případě špatných zkušeností vyřadit uchazeče z výběrového řízení, pokud jsou neshody za definovanou hranicí.

Pro vyhodnocení bude vytvořena samostatná část (sada údajů) v katalogu ICT, která se bude orientovat na kvalitu dodaného řešení. Především se bude hodnotit kvalita odevzdaného výsledku oproti zadání, ale také se bude hodnotit kvalita spokojenosti klienta s odevzdaným výsledkem. Jedná se zároveň o kvalitu dodavatele i útvaru ICT.

Principy a pravidla vyhodnocení

- Povinnou součástí všech předchozích fází etapy životního cyklu (a fází projektů) musí být vytváření a naplňování předpokladů (například měřitelných cílů) pro vyhodnocování projektů, provozu i dodavatelů.
- Povinnou součástí změnových projektů i provozu musí být vyhodnocování splnění dosažených cílů a parametrů, nebo zmírnění identifikovaných rizik a jejich interpretace do požadavků a potřeb vůči malým změnám nebo velkým změnám a s nimi spojené nové etapě životního cyklu.
- Vedle konkrétních (věcných, agendových) cílů a požadavků musí být předmětem vyhodnocení i naplňování mandatorních požadavků (jako je bezpečnost, ochrana osobních údajů, apod.).
- Součástí vyhodnocování rizik a dopadů je i posuzování potřeby tzv. mandatorních (nepodkročitelných) zdrojů, nezbytných pro zachování stávajícího rozsahu a úrovně služeb informačního systému.

Dílčí etapy / kroky vyhodnocení

Vyhodnocení projektu - (ne)dosažení cílů projektu

- Věcný gestor agendy spolu s Technickým správcem a Manažerem kybernetické bezpečnosti vyhodnotí míru naplnění:

- dílčích cílů projektu
- SLA klíčových parametrů ICT služby / systému,

Vyhodnocení investiční akce

- Věcný gestor agendy spolu s Technickým správcem vyhodnotí:

- dosažení cílů a plánovaných přínosů
- splnění harmonogramu
- dodržení rozpočtu,

Analýza provozních dat / plnění znalostní databáze (Best Practice)

- Provozovatel na základě reportů dohledového centra (HelpDesk):

- zpracuje a vedení OVS předloží výroční zprávu,
- průběžně doplňuje / aktualizuje ICT znalostní databázi úřadu

Formulace doporučení od změn nastavení po další rozvoj / ukončení provozu

- Věcný gestor agendy spolu s Technickým správcem a Manažerem kybernetické bezpečnosti (průběžně) posuzují:

- návrhy a doporučení změn (funkcionalit i SLA parametrů) zaslaná Uživateli i Provozovatelem (Dodavatelem)
- možnosti optimalizace a
- perspektivnost dalšího rozvoje,

- Technický správce naformuluje a Věcnému správci předloží:

- návrhy optimalizačních operativních opatření a rozvoje služby,
- připomínky a požadavky změn

Rozhodnutí o ukončení poskytování služby / provozu systému

- Na základě výroční zprávy **Věcný gestor agendy** rozhodne, zda poskytování ICT služby / provoz informačního či komunikačního systému ukončit nebo ne.

Fáze 6 - UKONČENÍ ICT SLUŽBY

Rámcová charakteristika ukončení služby

Ukončení života systému a jeho případná náhrada jiným je strategickým rozhodnutím, které musí být podpořeno architektonickými a ekonomickými podklady a musí být dlouhodobě připravováno v IK OVS. Součástí ukončení služby je plnění exit plánu dohodnutého s dodavatelem či provozovatelem.

S ukončením provozu je tedy nutno počítat již při formulaci zadání na výběr dodavatele, uzavření smlouvy[49)] a při průběhu implementace[50)]. Pro potřebu ukončení provozu ISVS a přechodu na jiný ISVS musí mít úřad zasmluvněnu povinnost stávajícího dodavatele ISVS poskytnout veškerou potřebnou součinnost, práva, data, dokumentaci a informace, účastnit se jednání s úřadem a popřípadě s třetími stranami za účelem plynulého a řádného převedení všech činností spojených s poskytováním služeb na úřad a/nebo nového poskytovatele, exporty veškerých dat s vyčerpávajícími popisy, včetně vytvoření základních datových zdrojů jednotlivých agend a modulů, které umožní na základě požadavků úřadu vytvořit dostatečně strukturovaná data, které bude moci importovat jiný ISVS bez hluboké znalosti databázové struktury stávajícího ISVS. Na základě datových zdrojů bude možné naplnit exitový plán pro přechod na jiný systém.

Stejně tak musí být ukončení zohledňováno v architektuře, tzn., architekturu řešení je třeba navrhovat již s vědomím nutnosti podpory efektivního ukončení životního cyklu ISVS.

Je žádoucí, aby věcně zodpovědné osoby za koncová informační a komunikační zařízení zvážily v souladu s principy 3E a dalšími právními předpisy v závěru životního cyklu ICT zařízení jejich vyřazení z účetní evidence bez provedení fyzické likvidace pro následné efektivní využívání koncových zařízení v rámci úřadu, až do doby úplného opotřebování.

Principy ukončení služby

- Na fakt, že služba bude ukončována, je třeba myslet již v prvních fázích návrhu služby a to:
  - Technicky.
  - Smluvně.
  - Provozně.

    - Datově/migračně.
- Ukončení služby může mít důvody:
    - Finanční náročnosti údržby a rozvoje služby (nástroje TCO).
    - Morální zastaralost a nedostatečnost.
    - Smluvní.
    - Agenda již není vykonávána, nebo byla novelizována natolik, že změna znamená porušení 3E principu

Dílčí etapy / kroky

Plán náhrady ukončovaného řešení novým (novou generací, jiným systémem)

Ověření využitelnosti komponent:

- Technický správce zpracuje a Věcnému správci agendy předloží ke schválení:
- analýzu využitelnosti komponent ve vlastnictví OVS (včetně SW licencí) s návrhem na majetková opatření (převod na jinou ICT službu / útvar, resp. odprodej / likvidace nevyužitelných),
- analýzu možných rizik a dopadů,
- kvalifikovaný odhad nákladů na likvidaci,
- reálný harmonogram likvidace,
- Věcný gestor agendy:
- posoudí návrh Technického správce, který buď schválí, nebo vrátí s požadavkem konkrétních požadavků jeho změn,
- určí, která data (včetně provozní dokumentace) a jak archivovat, a která a jak zlikvidovat.

Administrativní opatření:

- Technický správce zpracuje a Provozovateli předá k realizaci:
- projekt ukončení poskytování ICT služby / provozu ICT systému,

Technická opatření:

- Provozovatel ve spolupráci s Dodavatelem:
- odinstaluje zařízení a určená odveze je k likvidaci,
- migruje / archivuje / likviduje data,
- zpracuje kompletní dokumentaci likvidace

Zásady strategického plánování ISVS v kontextu architektury úřadu

Přístup ex-ante k plánování a řízení změn a jejich přínosů

Způsoby promítání realizace strategických cílů do změn struktury a chování úřadu, tj. do změn jeho architektury, a naplánování vzájemně souvisejících proveditelných balíčků práce (programů, projektů) pro realizaci těchto změn a jejich IT podpory jsou úlohou manažerské metody EA-architektura úřadu, která je základním prostředkem tvorby Informační koncepce orgánu veřejné správy.

Řešení v ICT mají mít dlouhodobý charakter, a to lze pouze při plánování. Plánování znamená znalost závazků vzniklých potřeb před jejich zavedením, tedy tzv. **ex-ante kontrola** vynaložených zdrojů na změnu prostředí. Je velice neefektivní realizovat zadání povrchně a nekoncepčně (např. vylepšovat nasazení po akceptaci a

nasazení na produkci). Tento přístup je dlouhodobě neudržitelný, a především velmi nákladný a obtížně spravovatelný.

V případě přístupu ex-ante, kdy programově hodnotíme dopady změny na začátku při návrhu, můžete zavedení změny podle jednotlivých dopadů pozitivně ovlivnit, primárně v oblasti nákladů (investičních i provozních, kvality a architektury).

Nejefektivnějším možným a zároveň nejprůkaznějším nástrojem potvrzení či ověření vhodnosti vybraného způsobu řešení v rámci ex-ante kontroly je realizace ověřovacího projektu (PoC – Proof of Concept) na podmnožině funkcionalit a případů užití dostatečně reprezentujících koncept řešení předmětné problematiky. Za účelem minimalizace nákladů na realizaci PoC je vhodné využít dostupné otevřené (Open source) technologie. Tyto pak lze v případě potřeby v rámci produkčního implementačního projektu zaměnit za technologie komerční s garantovanou komerční podporou. Nemalým přínosem takového postupu je dále ověření a upřesnění požadavků na jednotlivé produkty na otevřených technologiích a následné přesnější cílení na produkční funkcionality vyžadované od komerčních produktů.

Dalším důvodem pro realizaci PoC projektů je komunikace připravovaných služeb, funkcionalit a jejich podoby a formy směrem ke koncovým uživatelům. Jedním z hlavních architektonických principů na úrovni eGovernmentu ČR je princip „Použitelnosti“ budovaných aplikací. Dle tohoto principu musí být služby veřejné správy navrhovány vždy s ohledem na potřeby klienta – občana tak, aby mohl za všech okolností vyřídit svoji životní situaci v úplnosti elektronickou službou. Zároveň by měli být klienti – občané dle principu „Transparentnosti“ pořízení, provozu a rozvoje služeb veřejné správy informováni o záměrech a cílech budování on-line veřejných služeb tak, aby byli schopni využít všech dostupných prostředků k ovlivnění jejich směřování na základě jejich zákonných práv a demokratických principů.

Pro naplnění výše uvedených principů se jako vhodný postup implementace nových služeb veřejné správy jeví právě ověření konceptů, technologií a jejich funkcionalit v takzvaném ověřovacím PoC projektu (Proof of Concept) před samotným návrhem a výstavbou cílových řešení. Tento postup poskytne uživatelům možnost otestovat služby a funkcionality již v době jejich návrhu, a tedy i možnost vyjadřovat se k podobě návrhu, případně zasílat náměty na změnu, rozšíření, či optimalizace navrhovaných služeb. Tak lze zajistit, že služby budou navrženy s ohledem na očekávání klientů – občanů a všechny případné nesrovnalosti, rozpory či dodatečné požadavky/očekávání klientů – občanů podchytit již v začátku a zapracovat do koncepce řešení nově připravované služby.

U informačních systémů je ex-ante kontrola spojená nejčastěji s vypršením smlouvy na dobu určitou, kde další veřejná soutěž sebou nese např. změnové požadavky, které nebylo možné ze smlouvy plnit. V takovém okamžiku je zcela nezbytné zahrnout do ex-ante kontroly komplexní revizi výhradních a nevýhradních licencí daného řešení ve vztahu k vendor-lock efektům, možnosti využití cloudu a další možnosti sdílení.

Ex-ante přístup se tedy může v nejbližším období stát jednoduchým nástrojem pro zmírnění rizik pro všechny ISVS. Pro každý jednotlivý a souhrnně pro všechny ISVS úřadu pak bude v Informační koncepci OVS stanoveno, jaký je žádoucí cílový stav ISVS na konci plánovacího horizontu IS včetně důvodu proč tomu tak je. Tedy z jakých důvodů vyplývajících z vlastních vlastností ISVS, z požadavků jím podporovaných procesů a služeb veřejné správy úřadu ev. z jakých externích příčin, dále jakými činnostmi budou potřebné změny IS realizovány a do kdy.

Návaznost na byznys a IT strategii úřadu, korporace a eGovernmentu

Dlouhodobé řízení informačních systémů veřejné správy musí být opřeno o strategické cíle úřadu v oblasti výkonu veřejné správy a jeho informační podpory, v kontextu strategických cílů nadřazených struktur úřadu, tj. veřejnoprávní korporace svého zřizovatele (má-li takovou a takového), eGovernmentu ČR a EU.

Není přípustné vytvářet v IK úřadu dlouhodobý plán ISVS bez doložitelného a srozumitelného odkazu na plány rozvoje a změn agend, které ISVS podporuje, a bez kontextu plánovaných změn úřadu a eGovernmentu jako celku.

Bez zvláštního zdůvodnění (flexibilní reakce na neočekávané změny vnějšího nebo vnitřního prostředí) není přípustné plánovat, připravovat a realizovat záměry, které nebyly předem identifikovány v IK OVS. Řádným způsobem vyřešení nenadálé potřeby zásadní změny IS je provést nejprve aktualizaci IK OVS, a tak zachytit do plánování veškerý potřebný kontext úřadu a eGovernmentu, teprve poté zahájit plánování a přípravu projektového záměru.

Enterprise architektura ISVS a jeho architektura řešení

Každý věcný správce ISVS a věcný správce centrálního prvku eGovernmentu povinen pro tento systém udržovat model stávající, cílové a případně přechodné architektury na úrovni podrobnosti architektury úřadu (EA) a model architektury jeho řešení v souladu s metodikou Národního architektonického rámce.

Modely cílové architektury ISVS, na všech jejich vrstvách a doménách, vycházejí z celkové architektury úřadu, kterou všechny společně tvoří.

Model určitého požadovaného stavu architektury ISVS na úrovni podrobnosti architektury úřadu se označuje mezinárodní zkratkou PSA[51)] a odpovídá souboru změn, které mají být na ISVS realizovány rozvojovým programem nebo projektem.

Tato úroveň modelu je odpovídající pro potřeby IK úřadu a pro potřebu žádosti o stanovisko OHA k programu, investičnímu záměru a projektu.

Po získání kladného stanoviska OHA, je-li toto z hlediska objemu projektu relevantní, je vhodné přikročit k rozpracování podrobnější architektury ISVS, nebo jeho změn, pro účely výběru řešení a dodavatele řešení, tzv. architektury řešení[52)]. Z té se následně sestavuje seznam požadavků funkční a tzv. ne-funkční (myšleno ostatní než funkční) specifikace[53)] pro účely zadávací dokumentace výběrového řízení dle ZVZ.

Jak je uvedeno na jiném místě tohoto dokumentu, architektura řešení a její modely musí být nedílnou součástí návrhu provozních parametrů a její vizuální model dopomáhá k dekompozici (stávající i nové systémy) a přesnému návrhu rozhraní pro měření a řízení kvality služeb (SLA/SLM).

ISVS v Informační koncepci orgánu veřejné správy

Pro každý a pro všechny ISVS úřadu musí být ve společné Informační koncepci úřadu stanoveno, jaký je žádoucí cílový stav ISVS na konci plánovacího horizontu IK a proč, tedy z jakých důvodů vyplývajících z vlastních vlastností ISVS, z požadavků jím podporovaných procesů a služeb veřejné správy úřadu a z externích příčin, dále jakými proveditelnými balíčky práce (programy a projekty) budou potřebné změny IS realizovány a do kdy.

V IK OVS se kombinují dva „kolmé“ pohledy na ISVS:

- Jednotlivý pohled na logický ISVS (funkční celek) ve všech čtyřech vrstvách a čtyřech vertikálních doménách jeho architektury
- Celkový pohled na každou horizontální a vertikální architektonickou doménu tak, že zřetelně ukazuje kontext každého jednotlivého ISVS.

Řízení služeb informačního systému

Základním pravidlem a doporučením MŘICT pro ICT útvary OVS je přejít na řízení vztahu poskytovatelů a odběratelů funkcí podpory informačních systémů pomocí služeb, pokud se tak u nich již nestalo dříve

Příští vydání dokumentu MŘICT a průběžné přírůstky Znalostní báze rozvinou informace, doporučení a pomůcky v této oblasti řízení ICT, například o:

- správě Servisního katalogu resortní a jednotlivé organizace, eventuálně Servisního katalog na úrovni eGovernment
- převodu funkcí jednoho IS do podoby služeb a jak tyto služby plánovat, řídit a měřit na úrovni jednoho IS a jak je zapojit do centrálního řízení služeb.

Pravidla plánování rozvoje ISVS

V této kapitole budou vydána praktická doporučení, jak při řízení rozvoje jednoho IS účelně zkombinovat vstupy ze strategického plánování, mandatorních požadavků a výstupů ze správy byznys a uživatelských požadavků.

Doplněny budou také odkazy na odpovídající kapitoly mezinárodních standardů, například ITIL.

Nedílnou součástí budou doporučení a praktické návody pomůcky pro plánování požadavků na pro rozvoj IS nezbytné dodatečné zdroje, tedy finanční a personální plánování na úrovni jednoho IS v kontextu útvaru a úřadu.

Podstatné je, že řízení rozvoje jednoho IS musí vždy a plně využívat metody a nástroje řízení rozvoje IT aktiv celého úřadu, tj. portfolií aktiv po jednotlivých vrstvách, například plány rozvoje klíčových platforem, více v Řízení na úrovni útvaru ICT.

Pravidla ukončení provozu ISVS a přechodu na jiný

Ukončení života systému a jeho případná náhrada jiným je dalším strategickým rozhodnutím, které musí být podpořeno architektonickými a ekonomickými podklady a musí být dlouhodobě připravováno v IK OVS.

S ukončením provozu je nutno počítat již od jeho spuštění, architekturu PSA a architekturu řešení je třeba navrhovat s vědomím nutnosti podpory efektivního ukončení životního cyklu ISVS. Ukončení provozu se věnují i další kapitoly tohoto dokumentu. Další věcná a odborná doplnění budou obsažena v následujících vydáních po projednání s odbornou veřejností.

Zásady pro výběr a pořízení informačních systémů veřejné správy

Tato kapitola je první částí rozpracování požadavků: „Zásady a postupy pro pořizování a vytváření informačních systémů veřejné správy“ dle Vyhlášky č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy) v okruhu otázek: jak nalézt správné řešení pro naplnění byznys potřeb poskytování veřejných služeb (a jejich změn).

Pravidla pro financování pořízení IT řešení

Pravidla jednoty programového řízení rozvoje informatizace

MŘICT stanovuje, že využití tzv. programů pro potřeby programového financování a současně pro řízení zavedení změn musí být sladěné, tj. jedná se v obou pohledech stále o jedny a tytéž programy změn.

Je možné žádat o programové financování rozvoje informatiky úřadu pouze ve shodě s tím, jak byly programy změn pro jednotlivé ISVS identifikovány v cestovní mapě (Roadmap) architektury úřadu a v jeho informační koncepci.

Z toho plyne, že není správné a možné používat prostředky a nástroje programového financování pro potřeby provozu a údržby ICT řešení, přestože přitom půjde o investiční prostředky a zhodnocení majetku, pokud se

nejedná o změny realizované jako projekty v rámci rozvojových programů, viz dále.

Naopak to možné je, tj. i v případě, že některá provozní úloha (provozně financovaná) přesahuje možnosti liniového útvaru, využije pro koordinaci interních a externích zdrojů metody projektového řízení a pro koordinaci změn nástroje programového řízení. Tj. i tyto úlohy mohou být přiřazeny do rozvojových programů a věcně společně řízeny.

Bude stanoveno jaké je nejlepší praxe programového financování vzhledem k jednomu ISVS tak, aby současně vázala financování na očekávané benefity, ale současně ponechávala dostatečnou manažerskou flexibilitu, zejména u malých ISVS.

Pravidla pro ekonomiku a financování změn IT řešení

Ministerstvo vnitra s případnou revizí Ministerstva financí stanoví závazná pravidla průběžného udržitelného a řiditelného financování provozu ICT ve střednědobém horizontu, založeném na povinném vyhodnocování pětiletých Celkových nákladů na vlastnictví (angl. Total Cost of Ownership).

To mimo jiné předpokládá přinejmenším v oblasti řízení ekonomiky informatizace zavedení druhého okruhu účetnictví a evidenci spotřeby zdrojů úřadu (lidí, majetku, energií, znalostí, ...) v peněžním vyjádření jako tzv. náklady podle jednotlivých nositelů nákladů. Tj. zejména dynamických nositelů nákladů, kterými jsou programy, projekty a zakázky a statických nositelů nákladů, kterými jsou střediska útvaru ICT, jednotlivé součásti ICT řešení, fáze životního cyklu tohoto řešení a jednotlivé poskytované služby.

Dále to předpokládá aktualizaci skladby rozpočtové struktury a rozpočtových pravidel.

Tím se přejde od řízení finančních výdajů k řízení efektivity ICT prostřednictvím porovnávání a řízení spotřeby zdrojů, viz také ICT Benchmarking.

Pravidla pro řízení financování sdílených ICT služeb

Aktuálně jediným zákonným postupem pro financování zřízení, provozování a poskytování sdílené ICT služby je právním předpisem pověřit konkrétní OVS takovým úkolem při současném přidělení odpovídající rozpočtové položky. Výsledná sdílená služba je následně poskytována ostatním, v předpisu uvedeným OVS (nebo i OVM) zdarma, jako například služby ISDS, ISZR apod.

Návrhy, aby sdílené ICT služby byly hrazeny z kapitoly Všeobecná pokladní správa nebyly zatím akceptovány, namísto toho došlo k dohodě, že v závazných ukazatelích jednotlivých kapitol státního rozpočtu budou stanoveny specifické výdajové ukazatele, které budou zahrnovat výdaje spojené se správou, provozem a rozvojem klíčových informačních systémů veřejné správy, tj. základních registrů, informačního systému základních registrů, informačního systému sdílené služby, centrálního místa služeb, portálu veřejné správy, informačního systému, jehož prostřednictvím je zajišťován výkon působnosti kontaktních míst veřejné správy, a národního bodu pro identifikaci a autentizaci.

Pravidla rozhodování o způsobu realizace řešení ICT

Každý nový IS úřadu a jeho služby je možné pořídit několika způsoby. A to z pohledu způsobu technické realizace aplikačního SW vybavení, tedy jako:

- ASW pořízené vývojem na míru
- Typové ASW (TASW[54)])
- jako aplikační službu (SaaS[55)])
- nebo kombinací všech tří přístupů

Řešení může být také realizováno v různé granularitě aplikačních komponent zahrnutých do logického ISVS**, a to jako:**

- **velké monolitické řešení,**
- **procesně orientované komponentové řešení (jednotky komponent)**
- **orchestrace mikroslužeb (App-Store)**
- **kombinací všech třech způsobů v různých částech řešení.**

Každá dílčí část z celkového **řešení informačního** systému **může být pořízena v různém modelu zajištění zodpovědnosti za jeho dodávku, provoz a správu, a to:**

- **vlastními kmenovými zaměstnanci**
- insourcingem **(doplněním chybějících kapacit od externího dodavatele při zachování interní zodpovědnosti za službu**,
- outsourcingem **nebo tzv. cloudem (smluvním přenesením zodpovědnosti za službu dodavateli)**
- nebo hybridním řešením**.**

Pokud není způsob pořízení a realizace [56)] ICT služeb předepsán OVS zákonem nebo jiným právním předpisem, musí tento o způsobu pořízení (například nákupem řešení do vlastní správy, vývojem řešení vlastními silami nebo pořízením jako sdílené služby) rozhodovat se zodpovědností dobrého hospodáře, tzn. na základě komplexního posouzení reálně možných variant s přihlédnutím k hlediskům ekonomickým – zejména k již vlastněným existujícím podpůrným aktivům včetně etapy jejich životnosti, tak i k celkovým nákladům na vlastnictví [57)] a dalším, pro danou ICT službu relevantním požadavkům, např. bezpečnostním, termínovým atd.

Při tomto rozhodování musí správce ISVS a vedení úřadu vzít v úvahu nejenom dosavadní možnosti realizace, ale i možnosti veřejnou správou připravované. Těmi jsou zejména strategicky podporované formy sdílených služeb a služeb eGovernment cloudu.

G-cloud jsou sdílené ICT služby nabízené a provozované pro subjekty veřejné správy buď modelem *vládního cloudu* nebo modelem *komerčního cloudu*. Vládní cloud tvoří sdílené služby provozované státními datovými centry na jejich infrastruktuře. Komerční cloud jsou sdílené služby provozované komerčními subjekty na komerční infrastruktuře. Oba modely mají své katalogy nabízených služeb a související e-shop.

Katalog sdílitelných certifikovaných služeb publikuje formou veřejného portálu ty nabízené ICT služby, které mohou organizace veřejné správy využívat jako sdílitelnou službu, a publikuje také finanční a další podmínky jejich využití. Jedná se o obdobu amerického (**http://cloud.cio.gov**) nebo britského (http://govstore.service.gov.uk/cloudstore) katalogu.

Kritéria využití služeb eGovernment cloudu

Rozhodnutí, zda využít cloud či nikoli, přichází buď ve chvíli návrhu nového ISVS, nebo jeho obměně, upgrade apod. Znamená to, že technický správce musí znát a do plánu rozvoje každého ISVS vždy zvážit využití sdílených služeb eGC – infrastrukturních, platformových, softwarových i procesních, tak jak budou věcně i legálně dostupné a pro správce ISVS povinné nebo ekonomicky výhodné.

V podmínkách daného OVS a jeho rezortu je v rámci přípravy ISVS pro eventuální využití služeb eGC nutné provést zejména následující procesní kroky:

- Věcní správci ISVS s pomocí metodik eGC zhodnotí pro svůj ISVS závažnost bezpečnostních dopadů, a pro celý ISVS nebo pro jeho jednotlivé funkční části stanoví úroveň bezpečnostních dopadů 1-4 (Nízká, Střední, Vysoká, Kritická),
- Věcní správci identifikují další služby (datové centra, monitoring, ServiceDesk, penetrační testy, dočasné datové úložiště, služby mobilního sdílení dat, služby osobní produktivity, služby správy koncových uživatelských zařízení, služby portálu jako end user interface, provozní personál, konzultační služby atd.…), které k provozu a rozvoji ISVS potřebují,
- Techničtí správci stanoví odpovídající architekturu implementace ISVS s využitím služeb eGC

- Věcní správci s pomocí technických správců a TCO metodik eGC určí části ISVS, pro jejichž provoz by bylo ekonomické využít služeb eGC,
- Věcní správci uloží do IS o ISVS (tj. do katalogu aktuálně provozovaných ISVS) informace o svém ISVS v požadované struktuře, včetně případného požadavku na využití služeb eGC.

Kritéria pro využití služeb eGovernment Cloudu, představující kombinaci rozhodování podle hodnocení bezpečnostních dopadů a určení požadované bezpečnostní úrovně a na základě ekonomické výhodnosti budou aktualizována příslušnými právními předpisy a publikována s podrobnými návody a pomůckami jako součást Znalostní báze.

Pravidla pro lepší nákup ICT řešení

Obstarávání ICT nákupem podle povahy konkrétního záměru se ve veřejné správě řídí požadavky právních předpisu upravujících nakládaní s veřejnými prostředky, zejména předpisy upravujícími zadávání veřejných zakázek.

Všem zástupcům veřejné správy, účastnícím se v různých rolích procesu nákupu ICT, ukládá MŘICT povinnost vyhodnocovat, zda a jaké překážky při naplňování této koncepce způsobuje regulace nakládání s veřejnými prostředky a navrhovat MMR podněty k legislativním úpravám tak, aby byly naplno zachovány principy této regulace, přitom však, aby bylo umožněno jednotlivými nákupy naplňovat koncepční řízení informatiky VS ČR podle IKČR a podle informačních koncepcí jednotlivých orgánů veřejné správy.

Základními problémy dobrého nákupu ICT řešení jsou zejména:

- rozpor mezi přehnaně striktními opatřeními ZoZVZ, spojenými s nediskriminační soutěží jednoho ISVS nebo jeho dílčí komponenty a potřebou OVS jako dobrého hospodáře využít sdílené platformy eGovernmentu, úřadu nebo sdílené platformy společné pro více komponent jednoho ISVS
- rozpor mezi běžným právním výkladem ZoZVZ ve smyslu nutnosti každé 4 roky „přesoutěžit“ dodavatele ISVS a mezi reálnou morální a technologickou udržitelnosti přinejmenším ASW/TASW v trvání 10-15 let.
- rozpor mezi až „panickou“ obavou ze závislosti na dodavateli na jedné straně, a naopak přehlížením potenciálu dodavatele na druhé straně, aniž by se dařilo dosáhnout výhodného vyváženého dlouhodobého partnerství s dodavateli ISVS nebo jejich komponent.

Jako dobrou praxi lze doporučit základní přístupy pro OVS a jejich rezorty. Do budoucna měly zejména využívat následující nástroje pro zvýšení transparentnosti přípravy a realizace zakázek na dodávky informačních systémů:

- **Marketingový průzkum trhu** – představuje veřejnosti záměry organizace a umožňuje se vyjádřit k požadavkům a poptávanému konceptu řešení.
- **Předběžná (individuální) tržní konzultace** – z historické zkušenosti vyplývá, že vhodným způsobem realizace tržní konzultace je individuální komunikace s podnikatelskými subjekty či veřejností. V průběhu v minulosti realizovaných tržních konzultací se totiž mnohdy ukázalo, že konzultace realizované za účasti více účastníků a zejména podnikatelských subjektů brání otevřenému dialogu. Každá ze stran v případě takové tržní konzultace intenzivně brání své know-how před potenciální konkurencí. Doporučenou formou jsou tedy individuální tržní konzultace spolu s řádnou dokumentací jejich průběhu a výstupů.
- **Ověřovací projekt (PoC)** – bylo popsáno v rámci přístupu ex-ante kontroly v předcházejících kapitolách.

Další věcná a odborná doplnění budou obsažena v následujících vydáních po projednání s odbornou veřejností.

Základní opatření proti závislosti na dodavatelích v návrhu a nákupu

Základní podstata jevu závislosti na dodavateli (také Vendor-Lock-In) vyplývá zejména ze čtyř faktorů, a to:

- z neschopnosti úřadu rozvíjet ISVS, protože sám při jeho implementaci a následné údržbě nevybudoval

takovou kompetenci, tj. dostatek kvalifikovaných lidských zdrojů a dostatek znalostí, informací a dovedností;
- z nemožnosti si takové zdroje obstarat, protože na zpravidla základě pro úřad nevhodného nastavení práv a povinností vůči dodavateli k tomu úřad není původním dodavatelem smluvně oprávněn;
- z nemožnosti vysoutěžit z více dodavatelů služeb k produktu z důvodu unikátnosti vývojového či provozního prostředí, nebo neexistence více dodavatelů služeb k produktu na trhu;
- z vlastností produktu, který je dodán bez vývojového prostředí (pouze zkompilovaný, spustitelný), bez zdrojových kódů, modelu a dokumentace, takže jej ani při nejlepší vůli nelze měnit.

Z toho pro přípravu, implementaci a rozvoj ISVS vyplývají následující pravidla:

1. Úřad nesmí uzavřít takovou smlouvu, spojenou s informačním systémem, která by neobsahovala licenční ujednání, opravňující úřad poskytnout veškeré, v rámci smluvního plnění získané výstupy (zdrojový kód, vývojové prostředí, datový model, dokumentaci díla, školící podklady, uživatelské příručky apod.) libovolnému subjektu třetí strany dle své vlastní volby k podpoře, údržbě rozvoji nebo ukončení provozu a náhradě informačního systému.
2. Úřad není oprávněn uzavírat smlouvy, které by byly jednostranně nevýhodné, ať již pro něj nebo pro dodavatele. I podstatná nevýhodnost smluv vůči dodavateli se nakonec obrátí proti zadavateli, například zvýšenými riziky, zejména spojenými s neschopností dodavatele dostát neúměrným závazkům.
3. Úřad nesmí uzavřít smlouvu, spojenou s informačním systémem, který je natolik unikátní, že neexistuje více dodavatelů/poskytovatelů služeb, kteří jsou schopni takový systém rozvíjet, upravovat či provozovat.
4. V případě aplikačního SW těch řešení IS, která nepředpokládají a neumožňují žádné modifikace (datového modelu, programového kódu) ani přidávání Ad-on modulů, tj. dodávají se pouze ve spustitelném, zkompilovaném tvaru, bez zdrojových kódů a bez vývojového prostředí (například Antivirus nebo části Office) také musí platit, že veškeré výstupy spojené s dílem, dodané s ním nebo vzniklé v projektu musí být smluvně dostupné pro libovolné třetí strany, resp. veřejné, vyjma vlastního práva užívat řešení.

Ostatní standardní (krabicový, COTS, TASW) aplikační SW pro řešení, u kterých OVS naopak předpokládá, že je bude potřebovat upravit na míru, a to nejen v rozsahu parametrických změn (např. uživatelské číselníky), ale i změn datového modelu a programových funkcí a veškerý SW vyvinutý na míru:

- musí být smluvně i fyzicky dodán v podobě, umožňující úřadu dílo libovolně vlastními silami nebo s pomocí třetích stran udržovat a dále rozvíjet,
- nikdy nesmějí být dodána pouze již zkompilovaná do spustitelného prostředí (Run-Time), ale musí obsahovat i plnou podporu fáze změn (Design-Time), tj. vývojové prostředí se všemi modely, knihovnami, zdrojovým kódem, vývojovou dokumentací apod.

Dále veškerý aplikační i provozní SW, vyvinutý na požadavek a za prostředky úřadu veřejné správy ČR, nebo EU, musí být dodán s otevřenou licencí, umožňující jeho využití, nebo využití jeho částí, kterýmkoli orgánem veřejné moci ČR – Open Source a licence EUPL.

Další detailní informace o Anti Vendor-Lock-In jsou uvedeny zde, a budou dále doplňovány a průběžně aktualizovány ve Znalostní bázi.

Dlouhodobě se jedná o zajištění přidané hodnoty v oblasti provozu informačních systémů a aplikací prostřednictvím optimalizace uspořádání vazeb mezi jednotlivými systémy či aplikacemi a využití sdílených aplikačních funkcí. V užším technickém pojetí se jedná o integraci různých technických částí informačního systému (i různé vyzrálosti a morální zastaralosti), tedy systémů či aplikací do jednoho celku převážně pomocí integračních a orchestračních nástrojů.

Cílem je výstavba takové architektury informačních systémů, která efektivně podporuje procesy a agendy v rámci OVS a jeho rezortu. Dále tento přístup umožňuje razantní zvýšení interoperability, flexibility a zároveň snižuje riziko závislosti na konkrétním dodavateli (tzv. vendor lock-in). Toho bude dosaženo zejména vytvářením aplikačních komponent, které poskytují služby, sdílené více aplikacemi.

Naplněním tohoto cíle dojde k výraznému zjednodušení stávající architektury a snížení nákladů na modifikaci stávajících systémů a aplikací. Vedle snížení nákladů na implementaci a integraci nových systémů a aplikací

dojde k větší automatizaci procesů, což přinese snížení nákladů a větší rychlost zpracování dat. V neposlední řadě bude umožněna snadnější integrace se systémy externích subjektů.

Pro úspěšné dosažení představeného přístupu by měla být realizována následující opatření:

- Přechod na servisně orientovanou a orchestrovanou architekturu – výstavba ESB/BPM platformy
- Postupný přechod jednotlivých aplikací (systémů) na servisně orientovanou architekturu
- Vedení dokumentace IS a služeb ICT v modelech, které jsou v souladu se standardy TOGAF a ArchiMate.

Další věcná a odborná doplnění budou po projednání s odbornou veřejností obsažena v následujících vydáních a ve Znalostní bázi.

Dosahování dlouhodobého vyváženého partnerství s dodavateli (zabránění Vendor-Lock-In)

MŘICT a Znalostní báze budou napomáhat vzniku a udržení dlouhodobého vyváženého partnerství útvarů ICT s jejich dodavateli publikováním řady návodů a pomůcek, například vzorů smluv a zadávacích dokumentací či standardů a návodů (how-to). Zvážen bude také model, kdy se budou dílčí smlouvy jednotlivých OVS odkazovat na všeobecné obchodní podmínky veřejné správy, vydané po dohodě MV nebo MMR.

Každému OVS by stále zůstávala volba nebo modifikace, ale v obchodních podmínkách již by byla vyvážená práva obou stran. Může se jednat o samostatnou přílohu, která bude reflektovat jak směrnici o majetku státu, tak zajištění znalostí k informačním systémům.

Další věcná a odborná doplnění budou obsažena v následujících vydáních po projednání s odbornou veřejností.

Zásady pořizování programového vybavení jako Open Source

Open Source software a free software (OSS&FS) je nedílnou součástí ICT již mnoho let. Z bezpečnostního hlediska je již dávno prokázáno, že jsou tyto produkty bezpečné. Bohužel již mnoho produktů se historicky změnilo z OSS na placenou verzi. Dále se mnoho produktů přestalo podporovat a téměř u všech OSS projektů platí, že změny si musíme zařídit sami.

Pořízení OSS je tedy rozhodně rizikové, pokud nezvážíme všechny dopady. V každém případě použitím OSS nám nevzniká řízení a správa bezúplatně. Dlouhodobá udržitelnost informačních celků není závislá na krátkodobém řešení. Primárním pohledem musí být život informačního celku během 5 a více let jeho životnosti, s jasnou strategií, jak k s ním i po základních 5 letech (relevantních pro TCO) dále pracovat.

Pro užití a vhodnost integrace jednotlivých OSS produktů vznikne samostatná metodika. Bude zaměřena nejen na integraci OSS prvků do informačních celků, ale i na možnost sdílení úspěšných produktů jako je spisovka nebo anonymizér. Více o tématu bude publikováno ve Znalostní bázi.

Pravidla pro oceňování vývoje nebo úprav IS

Pro lepší stanovení maximální ceny díla nebo pro porovnatelnost variant řešení s různou mírou programového přizpůsobení je nutné v ICT VS ČR používat jednotnou metodiku oceňování vývoje (nebo úprav) programového vybavení pro OVS, založenou např. na metodě funkčních bodů podle ČSN ISO/IEC 20926.

Tato metodika by měla být vypracována a vydána jako další ze standardů útvaru OŘI MV, viz Úvod, a publikována ve Znalostní bázi.

Smluvní zabezpečení

Vedoucí pracovníci útvarů ICT se musí v praxi potýkat s celou řadou typů smluvních vztahů (vývoj, provoz, podpora, licence,...), aniž by při tom měli k dispozici adekvátní podporu.

Důležitým krokem je sjednotit typy smluv podle obsahu, délky, rozsahu apod., tj. přinést jednotu a řád do smluvního systému v řízení vztahů ICT s dodavateli. Dále je potřebné sebrat zkušenosti a přeměnit je na vyjádření nejlepší praxe v podobě garantovaných šablon smluv, včetně jejich případné kombinace s všeobecnými obchodními podmínkami, viz výše.

Jedním z cílů dalšího vydání MŘICT a průběžné aktualizace Znalostní báze je přinést další informace, dokumenty a pomůcky na podporu bezpečného a efektivního uzavíraní smluvních vztahů v ICT veřejné správy.

Koncepce řízení úspěšné realizace projektů navržených ICT změn

Tato kapitola je druhou částí rozpracování požadavků: „Zásady a postupy pro pořizování a vytváření informačních systémů veřejné správy“ dle Vyhlášky č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy) v okruhu otázek: jak vybrané řešení úspěšně zavést a uvést do produktivního provozu. Obsahuje podstatné a celostátně plošně platné standardy k požadavkům vyhlášky (po její předpokládané novele).

Pravidla řízení programů a projektů jednotlivých ISVS

Informatika v úřadu slouží svým interním klientům, informatické projekty mají přispívat k naplnění cílů celého úřadu, projekty změn veřejných služeb se stále více opírají o podporu informatiky. Všechny projekty v úřadu navíc sdílí omezené množství pro projekty vhodných lidských zdrojů. Proto musí být všechny jednotlivé projekty ISVS vzájemně koordinovány v rámci útvaru ICT, potom šířeji v rámci všech projektů celého úřadu a do budoucna i eGovernmentu ČR.

Koordinace projektů, jejich provazování do programů a správa portfolií projektů je službou Projektové kanceláře úřadu (také jako "PK"[58)]). Navazuje na práci strategických útvarů a je znalostně podpořena službami útvaru celkové architektury úřadu, architektonické kanceláře (také jako "AK"). Více o společném řízení projektů a programů na úrovni úřadu v Řízení na úrovni útvaru ICT.

Řízení programu rozvoje ISVS

Všechny projekty, které vzájemně spolu souvisí v časové věcné či jiné návaznosti musí být řízeny jako program, aby bylo zajištěno, že společně dodají větší hodnotu a s větší jistotou, než kdyby byly řízeny každý samostatně.

Zatímco řízení projektů je zaměřeno primárně na dosažení plánovaných výstupů při dodržení spotřeby plánovaných zdrojů, je řízení programu zaměřeno zejména na splnění strategických cílů a dosažení očekávaných přínosů. Z tohoto pohledu je doporučeno, aby i každý samostatný projekt byl řízen nejenom s využitím projektových, ale i programových principů. Více o řízení programů Řízení na úrovni útvaru ICT.

Řízení projektů ISVS jako součást portfolia

Velmi často je v útvaru ICT a v celém úřadu současně řízeno velké množství projektů. Zodpovědnost za jejich řízení je rozdělena mezi několik projektových ředitelů s podporou projektových manažerů. Skupině projektů se společnou zodpovědností jednoho ředitele nebo projektového manažera, nebo naopak skupině projektů, podobných si obsahem, funkčním celkem, dodavatelem, sdílenými zdroji či jiným kritériem, se říká portfolio.

Základním rysem portfolia je, že za něj někdo konkrétní zodpovídá a vývoj všech projektů ve svém portfoliu někomu reportuje.

Pro každý jednotlivý projekt ISVS z toho plyne, že musí být jednoznačně přidělen jednomu řediteli nebo manažeru a stát se tak součástí jeho portfolia, jeho zodpovědnosti a jeho výkaznictví vůči PK a vedení úřadu.

Více o technikách řízení portfolia projektů v Řízení na úrovni útvaru ICT.

Pravidla řízení jednotlivých realizačních projektů ISVS

Pro každou činnost v oblasti informatiky, která splňuje definici projektu či podle rozsahu jejích důsledků, je IKČR stanoveno, aby od samého začátku byla důsledně řízena jako projekt, tj. s využitím metod, zodpovědností a nástrojů projektového řízení.

Několik definic projektu, které se vzájemně mírně liší, ale všechny vyjadřují tutéž podstatu:

- Projektem je časově, nákladově a zdrojově omezený soubor aktivit vedoucí k prosazení rozvojových strategických cílů, změn a inovací (kromě provozu, ale včetně rozsáhlých případů údržby, oprav, obnovy a nákupu služeb nebo hmotného i nehmotného majetku).
- Projekt je časově omezené úsilí podniknuté za účelem vytvoření jedinečného produktu, služby nebo výsledku. To znamená, že projekt má definovaný začátek a konec. Jeho výsledkem je vytvořený jedinečný produkt či schopnost poskytovat službu, což je rozdíl od provozních činností, které jsou opakující se a bez definovaného konce.
- Podle jiné definice je projektem *„jedinečný časově, nákladově a zdrojově omezený proces realizovaný za účelem vytvoření definovaných výstupů co do kvality, standardů a požadavků“*.
- Projekt přináší jednorázovou (skokovou) změnu kvality svého předmětu, v tomto případě primárně změnu vlastností ISVS, kvalitativní změnu ICT infrastruktury, nebo změnu schopností útvaru informatiky, má pevný cíl, tj. rozsah změny, která musí být uskutečněna ve stanoveném čase a s využitím naplánovaného rozsahu zdrojů (finančních, lidských, materiálních,...).

Povinnost uplatnit projektové řízení je stanovena pro projekty (alespoň jedno z toho):

- jejichž hodnota výdajů je větší než 10% rozvojové a inovativní části ročního IT rozpočtu úřadu (nikoli provozní části rozpočtu),
- u kterých míra zapojení lidských zdrojů (interních a externích, IT a odborných dohromady) přesahuje 10% vlastní roční interní kapacity IT útvaru úřadu - kritérium kapacit,
- příprava a realizace změny trvá více než 3 měsíce - kritérium času,

při kterých změny ICT řešení či infrastruktury mohou mít dopady na její odolnost proti kybernetickým rizikům nebo na schopnost dodávat služby veřejné správy - kritérium rizik.

Po zkušenosti z praktické aplikace těchto pravidel je možné v dalším vydání dokumentu hranice projektového řízení ještě nějak omezit a vyjít tak vstříc malým úřadům, zejména samosprávám.

Pro každý projekt, splňující výše uvedené podmínky, je úřad povinen zařadit do týmu projektu již před zahájením projektu odpovídající množství interních zaměstnanců tak, aby zajistil, že v projektu uplatněné či vytvořené Know-how zůstane jako znalost a dovednost (nikoli jenom dokumentace) nadále k dispozici v úřadu. Toto je jedním z několika nezbytných předpokladů obrany proti nežádoucí míře závislosti na dodavatelích (Vendor Lock-In). V této souvislosti je třeba zajistit, aby:

- zaměstnanci úřadu, jejichž zařazení do projektu přesahuje 10% pracovní doby (4 hodiny týdně), byli pro projekt uvolněni[59)] a odpovídající část jejich běžné práce a zodpovědnosti byla (formálně i fakticky) převedena na ostatní zaměstnance úřadu.
- zaměstnanci v rozsahu svého začlenění do projektu podléhali personálně vedení projektu, tzn., že jejich přímým nadřízeným je vedoucí řešitelského týmu, který mj. schvaluje výkazy práce zaměstnance a přiznává mu odměny za práci na projektu. Eskalačními úrovněmi jsou projektový manažer a řídící výbor.

To je možné řešit formou pověřovacích dekretů, viz níže.
- v případě účasti externího dodavatele byly v zadávací dokumentaci a smlouvě jako nedílné součástí plnění požadovány činnosti, výstupy a způsob práce (přístup), vedoucí k efektivnímu předání znalostí a aktivních dovedností (například: nastavení systému nebo naplňování číselníků v systému neprovádí externí poradce, nýbrž interní zaměstnanec pod vedením poradce, ...).

V části MŘICT o přístupu k řízení útvarů informatiky je popsáno, jakými rolemi a pozicemi musí úřad a útvar IT minimálně disponovat (In/Out), aby mohl plnit výše uvedené požadavky. Pro kvalitní a bezpečné řízení projektů ICT změn je nutné přinejmenším přiřadit konkrétní lidské zdroje (jmenovitě) k následujícím rolím:

- Sponzor projektu – statutární člen vedení úřadu[60])
- Ředitel projektu – příkazce operace, (u nadresortních projektů je nezbytné jmenování vládou)
- Projektový manažer – odborník na projektové řízení
- Architekt řešení (doménový i platformový)
- Analytik – interní konzultant, schopný parametrizovat a rozvíjet řešení
- Manažer skupiny IT služeb („obchodník“ s IT službami pro interní klienty – odborné útvary)
- Manažer provozu ICT
- Nákupčí externích služeb
- Ekonom IT (správce rozpočtu projektu) - schopný controllingu útvaru, projektů i komponent
- Auditor IT – poskytujícího vedení ICT i ostatním složkám úřadu funkce IT governance
- a další

Ve Znalostní bázi bude připravena tabulka očekávaných pracovních a služebních pozic pro jednotlivé projektové role.

Jmenování musí proběhnout písemně, prostřednictvím pověřovacího dekretu s podpisem jmenovaného a představeného / vedoucího pracovníka. Přitom je zjevné, že úřad může pro realizaci těchto rolí využít externích dodavatelů služeb, tím se ale nezbavuje povinnosti mít rolím přiděleny interní zaměstnance, „stínující“ - kontrolující externisty, s jasně definovanými zodpovědnostmi. Role sponzor projektu, ředitel projektu a ekonom IT (správce rozpočtu projektu) není možné zajistit externě.

Každý projekt musí mít uvedené role uspořádány v organizační struktuře, obsahující v hierarchii pravomocí a zodpovědností:

- Řídící výbor projektu (také jako "ŘVP"), vedený jeho předsedou a zahrnující přinejmenším sponzora projektu a ředitele projektu a statutárního zástupce úřadu, pokud jím není sponzor ani ředitel projektu.
- Hlavní tým projektu (také jako "HTP"), vedený ředitelem projektu, zahrnující přinejmenším projektového manažera, manažera projektu za dodavatele, projektového administrátora, Hlavního architekta projektu a vedoucí řešitelských týmů. Součástí hlavního týmu projektu jsou dle potřeby podpůrné role pro ředitele projektu, jako například technický a věcný gestor projektu, právník, ekonom (správce rozpočtu projektu), manažer kvality a manažer publicity projektu.
- Řešitelské týmy projektu (také jako "TP"), vedené vedoucími řešitelských týmů a zahrnující přinejmenším členy týmu ze strany úřadu, případně členy týmu za dodavatele.

U velmi malých projektů[61] je možné role a zodpovědnosti v plánu řízení projektu odpovídajícím způsobem redukovat, například tak, že část role a zodpovědností řídícího výboru přebírá samostatný ředitel projektu (který nesmí nikdy chybět), zbylou část zodpovědností ŘVP přebírá vedení úřadu jako celek, část rolí a zodpovědností hlavního týmu přebírá projektový manažer a zbylou část rolí HTP a všechny role řešitelských týmů přebírá jeden společný tým projektu. Redukce je na rozhodnutí projektové kanceláře nebo vedení úřadu, tam, kde ještě PK není.

Každý ICT projekt bez ohledu na obsah nebo velikost obsahuje metodikou stanovenou minimální sadu fází svého životního cyklu s pevně stanovenými termíny.

Bez ohledu na použitou metodiku projektového řízení (Prince2, PMI, atd.) musí projekt projít nejméně povinnou, metodikou stanovenou minimální sadou kontrolních milníků či průběžných aktivit, sladěných jak s potřebou dodávky kvalitních ICT řešení, tak s požadavky procesů finanční kontroly a veřejných zakázek.

Z povinné a rozšířené sady milníků, průběžných činností a výstupů projektu se zdůvodněným způsobem při iniciálním plánování projektu vyberou milníky, činnosti a výstupy relevantní pro konkrétní projekt. Ne výběr, vynechání povinného milníku, činnosti nebo výstupu je nutné v projektové dokumentaci zřetelně zdůvodnit.

Projekt, řízený ve shodě s těmito pravidly IKČR musí vytvořit a užívat přinejmenším metodikou stanovenou minimální sadu výstupů / pracovních dokumentů. Každý projekt musí mít v rámci projektové přípravy zpracován minimálně projektový záměr, v průběhu realizace plán řízení projektu a při ukončení zprávu o průběhu projektu.

Součástí mechanismu řízení projektu musí být povinný reporting vedení úřadu, například prostřednictvím projektové kanceláře, či řídícího výboru projektu jedenkrát měsíčně, obsahující metodikou stanovenou minimální sadu údajů.

Součástí řízení projektu musí být aktivní práce s klíčovými zainteresovanými stranami, jejich oprávněnými potřebami a očekáváními.

Součástí řízení projektu musí být průběžné a závěrečné vyhodnocení dosažených výsledků a přínosů, řízené poučení se z nabytých zkušeností[62)].

Více informací a pravidel k řízení ICT projektů a jejich portfolií, včetně vazeb na řízení lidských zdrojů vydá MV ČR ve formě aktualizace Metodiky řízení IT projektů, kterou bude publikovat také jako součást Znalostní báze.

Řízení rizik a bezpečnosti v realizačních projektech

Důležitou a neopominutelnou součástí řízení projektu je, vedle řízení rozsahu, času a zdrojů projektu (rozpočet, lidé a technika/aktiva), také řízení rizik a přijímání přiměřených opatření pro jejich snížení.

Součástí řízení rizik a bezpečnosti projektu je řízení kybernetických rizik a bezpečnosti v souladu s metodami jejich řízení a pomocí nástrojů na úrovni celého ICT útvaru a úřadu, Řízení na úrovni útvaru ICT.. Jako optimální metoda řízení rizik slouží kombinace postupů ze standardních metod projektového řízení, z rámce TOGAF a z vydaných doporučení NÚKIB. Je plánováno vydat ve Znalostní bázi sadu akcelerátorů na podporu nejlepší praxe v této oblasti.

V projektu se musí uplatnit i další principy jako „Security by design“ a metody jako bezpečný vývoj SW.

Schvalování projektů Odborem HA MV ČR

Proces je řízen v souladu průběžně vydávanými Metodickými pokyny OHA a jim odpovídajícími formuláři, viz web OHA, které společně s dalšími návody a pomůckami budou průběžně aktualizovány ve Znalostní bázi.

Zásady dokumentace skutečného provedení IT řešení

Znalost aktuálního stavu konfiguračních položek ICT aplikační a technologické architektury je nezbytným předpokladem jejího efektivního řízení. Součástí této znalosti ale často není aktuální dokumentace ICT systémů, resp. akceptovaná dokumentace skutečného provedení požadované změny (např. nastavení přístupových práv jednotlivých uživatelských rolí) nebo nové ICT služby, a to včetně znalosti o aktuální smluvní podpoře (maintenance), resp. o smluvních SLA (jaká jsou, do kdy trvají, …).

Odpovědnost za promítnutí akceptovaných změn do aktuální dokumentace by vždy měla být pro jednotlivé ICT systémy jednoznačně určena.

Optimální je tuto činnost zařadit jako nedílnou součást do akceptačních procesů a odpovědností za ně pověřit organizačně příslušného Technického správce.

Standardy, vzory a typové příklady takové dokumentace budou postupně aktualizovány ve Znalostní bázi.

Dokumentace programových modifikací

V posledních dvou letech se významně posunula správa programového vybavení díky možnosti vlastního nasazení portálu Gitlab, který nejen spravuje všechny verze programového vybavení, ale především je možné nastavit u tohoto způsobu nasazování i strojové kontroly. Dále je možné se vracet mezi verzemi a také kontrolovat popsaný zdrojový kód. V komerčním světě velice rychle došlo ke změně nasazování systémů přes Gitlab, protože takové nasazení nevyžaduje lidskou součinnost a zároveň je zde úplná auditní stopa provedených změn.

Aktualizace architektury řešení a architektury úřadu

Aktualizace architektury by měla mít nastavený milník jednou ročně nebo maximálně dvouletý cyklus v případě malých v liniovém řízení realizovaných změn. V případě projektově realizovaných změn musí být v rámci akceptace výstupů projektu, s dokumentací skutečného provedení společně dokončena a předána i aktualizace modelů architektury předmětného řešení na všech úrovních podrobnosti (EA-PSA, SA i SD[63)]).

Katalogové listy musí mít v sobě i záznam o všech změnách a následně v daném milníku dojde k propagaci všech změn z katalogových listů do modelů architektury.

Zásady akceptace výstupů projektu a přechodu do produktivního provozu

Pečlivá akceptace výsledků realizace změn a ověření úspěšného přechodu nových služeb IS do produktivního provozu je jedním z klíčových okamžiků projektu i milníkem životního cyklu informačního systému.

Řádná akceptace výstupů souvisí přímo také s tzv. Ex-ante přístupem k plánování a řízení změn (viz Řízení jednolitých ICT řešení), neboť umožňuje ověřit dosažení plánovaných ukazatelů vybraného způsobu řešení.

Záměrem MŘICT je v návaznosti na typy uzavřených smluv (Řízení jednolitých ICT řešení), různé způsoby realizace řešení realizovaných změny (Řízení jednolitých ICT řešení), Metodiku řízení IT projektů (Řízení jednolitých ICT řešení) a další aspekty pořizovaného řešení, připravit a ve Znalostní bázi aktualizovat sadu návodů a akcelerátorů pro snazší a důslednější provedení řádné akceptace dodávky realizovaných změn.

Pravidla efektivního řízení provozu a dodávky služeb, nákupu služeb a průběžného zlepšování

Odpovídá procesům dle ITIL: částečně Service Design, částečně Service Transition, plně Service Operation a Continual Service Improvement a dále procesům dle COBIT 5: Deliver, Service and Support

Budeme diskutovat s dalšími partnery a výsledek bude doplněn.

Budování a údržba kompetencí k provozu a rozvoji IT řešení

Budování monitoringu, definice monitoringu a budování oddělení pro podporu a rozvoj ICT služeb, včetně mechanismů návazností na katalogové listy a SLA.

Budeme diskutovat s dalšími partnery a výsledek bude doplněn.

Příklad pravidla: Úřad je povinen již v průběhu implementace nového řešení nebo po účinnosti této IKČR k řešením, u nichž tak v minulosti neučinil, vybudovat vlastní středisko kompetence (kompetenční centrum) k údržbě a rozvoji IS, za jejichž flexibilní legislativní rozvoj jako věcný správce odpovídá. Vlastní kompetenční středisko může nahradit zajištěním takové kompetence od jiného subjektu veřejné správy nebo státem vlastněného subjektu, smluvně nebo ze zákona, musí se však jednak o kompetentní kapacity, nezávislé na původním dodavateli, s nimiž může úřad disponovat, jakoby šlo o vlastní zaměstnance.

Kompetenční středisko je nutné udržovat pro řešení a platformy těchto řešení.

Zásady a postupy pro provozování informačních systémů veřejné správy

Budeme diskutovat s dalšími partnery a výsledek bude doplněn.

Zásady péče o klienty a uživatele služeb informačních systémů

Dílčí doporučení vážící se ke znalostní bázi ServiceDesku: Vypořádání každé životní situace ve světě ICT musí být měřitelné, protože 90 % všech životních situací se opakuje a díky znalostní bázi se ve všech případech zrychluje systém řízení obsluhy. Každý incident se poprvé řeší dny, na podruhé hodiny a při dalším stejném případu se vyřeší ve stejný den.

Pokud používáte informační systém, centralizujete všechny požadavky do jednoho místa a máte na jejich vypořádání zodpovědný tým, potom následná klasifikace těchto požadavků zrychlí zcela přirozeně jejich vypořádání.

Další metody péče o klienty ISVS budou po projednání s odbornou veřejnosti obsaženy v následujících vydáních MŘICT a aktualizovány ve Znalostní bázi.

Pravidla nepřímého řízení (governance) ISVS

Metody nepřímého řízení (governance) ISVS budou po projednání s odbornou veřejnosti obsaženy v následujících vydáních MŘICT a aktualizovány ve Znalostní bázi.

Řízení na úrovni útvaru ICT

Systém řízení ICT úřadu jako jeho průřezové provozní schopnosti zahrnuje dvě klíčové oblasti procesů či funkcí. Nejdůležitější je společné a jednotné řízení rozvoje informačních systémů a jejich služeb pro klienty. Důležité je ale také efektivní řízení a správa vlastních zdrojů a neustále zlepšování řídících procesů v IT.

Tato kapitola pokrývá obojí, ale zejména shrnuje vybrané klíčové úlohy, postupy a metody pro řízení ICT OVS jako jednotného celku a současně vyzdvihuje opakující se metody a postupy z životních cyklů jednotlivých IS, které vyžadují jednotný a centrální přístup (z pohledu OVS i státu).

Tyto centrální činnosti na úrovni úřadu a státu odpovídají i identifikovaným fázím životního cyklu jednotlivých ICT aktiv (IS, řešení, funkčních celků), více v Řízení jednotlivých ICT řešení a jsou předpokladem toho, aby se individuální činnosti správy jednotlivých aktiv odehrávaly koordinovaně, v souvislostech a s respektem k celkovým zájmům OVS a VS ČR.

Klíčové principy řízení ICT v úřadu

Pravidla v této kapitole představují základní společné standardy pro liniové i projektové řízení informatiky napříč ostatními oblastmi (strategického, taktického a provozního) řízení.

Přes posílení prvků sdílení a celostátní koordinace zůstává zásadní řízení informatiky a informatizace na úrovni jednotlivých OVS. Model řízení ICT (managementu) a dohledu na ICT (governance) na úrovni OVS musí být postaven zejména na následujících klíčových principech:

- Organizace má platnou, správnou a srozumitelnou Informační koncepci OVS.
- Organizace má funkční organizační strukturu, kapacity a dovednosti pro řízení zavedení změn, formulovaných v IK OVS.
- Organizace rozvíjí a oceňuje kompetence kvalifikovaných pracovníků, na nichž leží tíže implementace IK OVS
- Organizace je schopna vlastními silami provozovat nebo řídit provoz implementovaných řešení a průběžně je operativně zlepšovat
- Organizace respektuje mezinárodní standardy a nejlepší praxe a je schopna jim přizpůsobit svoje vnitřní předpisy a procesy

Každý OVS, zodpovědný za řízení informačních technologií ve vlastní správě, musí být schopen efektivně a správně vykonávat funkce pro řízení životního cyklu ICT:

1. Tvorba strategií a koncepcí ICT, včetně:
    1. podílu na tvorbě legislativy úřadu a ICT a eGovernment legislativy
    2. správy architektury úřadu
2. Plánování a organizace řízení ICT, včetně:
    1. řízení ICT zdrojů - lidských, znalostních, materiálních
    2. řízení portfolií ICT aktiv - informačních, aplikačních a technologických komponent
3. Pořizování ICT a realizace změn ICT, včetně:
    1. správy architektury a dokumentace ICT řešení
    2. řízení nákupu
    3. řízení programů a projektů
4. Provoz, údržba ICT a podpora klientů a uživatelů
5. Monitoring a vyhodnocování služeb ICT (jako prostředek governance, tj. dohledu a kontroly)
6. Archivace, útlum, konzervace a ukončování řešení, s případnou migrací do nových (Exit strategie)

Přístup k organizaci a managementu informatiky

Vnitřní výstavba útvarů informatiky musí odpovídat struktuře požadovaných rolí a jejich kompetencí podle této metodiky, tj. strategické plánování a řízení, pořízení a implementace změn, řízení provozu a dodávky služeb, ICT governance.

Spolu s rozvíjející se specializací informačních technologií roste i nutnost rozvoje struktury útvaru ICT. V té by měly působit také útvary týkající se architektury a vazby architektury na další výše popsané a zmíněné činnosti v rámci celého úřadu. Jen tak lze zajistit, že ICT, jako klíčový provozní útvar úřadu, bude bráno jako partner již při formulování legislativních změn, tj. na legislativní úrovni, a ne až při realizaci legislativy na technické úrovni.

Také do každého ICT útvaru úřadu VS je třeba doplnit nebo zlepšit jak roli ICT architekta (architektonické kanceláře, AK ICT), tak roli profesionálních projektových manažerů ICT projektů (projektové kanceláře, PK ICT), které obě společně pracují pro CIO úřadu.

V rámci Strategického řízení informatiky a ICT Governance je nutné implementovat vazbu ICT útvaru do celkové struktury úřadu. To předpokládá mimo jiné, že:

1. vedoucí útvaru (CIO) ICT musí být součástí nejvyššího vedení úřadu – na ministerstvech náměstek, aby mohl inspirovat rozvoj jeho veřejných služeb a
2. musí dojít k zásadní změně vztahu útvaru ICT s ostatními útvary úřadu ve smyslu Klient – Dodavatel,
3. v úřadu musí existovat architektonická kancelář úřadu (AK OVS) a projektová kancelář úřadu, (PK OVS), které navrhují obsah strategických změn architektury úřadu a koordinují programy jejich zavedení, včetně jejich ICT částí (projektů).

Budeme diskutovat s dalšími partnery a výsledek bude doplněn v dalším vydání.

Vlastní architektura útvaru ICT

Každý útvar ICT v rámci zajištění své průřezové provozní schopnosti má (má mít) udržovanou svou vlastní architekturu úřadu (EA), a to ve všech doménách podle NAR.

To znamená, že i útvar ICT musí mít a aktivně užívat model dekompozice schopností či byznys funkcí (procesů a služeb) v podobě tabulky a grafické mapy. Tyto by měl užívat k analýze a komunikaci silných a slabých stránek svých schopností a plánování jejich zlepšování.

Obdobně musí mít útvar ICT k dispozici mapu portfolia aplikačních komponent, používaných na podporu ICT procesů, stejně tak mapu dedikované technologické, fyzické a komunikační infrastruktury pro tyto vlastní aplikace.

Útvar ICT má mít udržovanou i relevantní část motivační architektury ve všech čtyřech vertikálních doménách, aby mohl sdílet v týmu i se zbytkem úřadu porozumění své motivaci a poslání, své výkonnosti, bezpečnosti i svým regulacím a omezením.

Lze předpokládat, že aktivitou pilotních úřadů při adopci těchto Metod řízení vzniknou a budou zobecněny ověřené modely jednotlivých domén architektury ICT schopnosti a budou publikovány v NAP a ve Znalostní bázi jako referenční modely a akcelerátory modelování OVS.

Personální politika a rozvoj lidských zdrojů ve vztahu k ICT VS

Budování lidských zdrojů je jedním z nejdůležitějších předpokladů k dosažení cílů informatizace. Koncepční i operativní záměry se do praxe dostanou, pouze pokud budou realizovány motivovanou, zručnou a kompetentní pracovní silou IT zaměstnanců ve veřejné správě.

Podle IKČR převezme MV ČR jako jeden z prostředků koordinace informatizace VS ČR dle zákona č. 365/200 Sb. také koncepční, metodickou a koordinační zodpovědnost za budování lidských zdrojů v informatice VS, viz hlavní cíl č. 4. Bude také iniciátorem a koordinátorem rozvojových programů v této oblasti.

Přesto i nadále zůstává plná zodpovědnost za plánování a řízení získání, udržení a rozvoje kvalifikovaných IT kapacit na vedení jednotlivých orgánů veřejné správy.

MV ČR vydá pro tuto oblast řízení ICT Metodiku (nebo koncepci) řízení lidských zdrojů a bude publikovat další informace a pomůcky ve Znalostní bázi.

Přístup k rozvoji lidských zdrojů informatizace

Základními trendy řešení lidských zdrojů v informatice VS jsou in-sourcing špičkových (IT strategie, architektura a management) a rutinních, generických IT disciplín (jako třeba HelpDesk, provozní operátoři), využívání expertů od dodavatelů (platformoví specialisté) a především úsilí získat a udržet vlastní zaměstnance pro řízení ICT a pěstování vztahů s klienty, věcnými správci IS.

Doplňkovým trendem je budování expertních, rychle dostupných kapacit pro specifické konzultační úlohy (architektura úřadu, tvorba IK, výpočet TCO, podpora při žádosti na OHA, podpora zadávací dokumentace apod.) ve sdílených kompetenčních centrech VS ČR.

Každý ICT útvar hledá hranici pro vypořádání potřeb vlastními silami nebo dodavatelem. Samotná správa a řízení by mělo být ve vlastních rukách, ale vlastní tvorba řešení již není dnes vyžadována z několika důvodů. Jedním důvodem je riziko pro dlouhodobou udržitelnost, kdy ztrátou vlastních lidských zdrojů přijde OVS o možnost řešení změn IS. Druhým je samotný princip 3E, kdy při zadání nemám konkurenceschopnost danou trhem. In-house tvorba je vhodná pro vybrané oblasti, kdy se jedná o jednoduchou službu, která nebude znamenat v budoucnu re-inženýring nebo naopak službu, kde zadání je zcela unikátní.

In-sourcing má však v ICT stále své silné působiště, a to nejen v obsazení ServisDesku, ale pro kontroling všech systémů.

Musí zde být zastoupení provozu, bezpečnosti a rozvoje. Každý útvar má na starosti různé aktivity, které však mají společné hranice a není možné je od sebe oddělit. Mezi bezpečností a provozem v posledních letech vznikala bariéra přijetím politik, ale nakonec se opět spojili a dnes spíše fungují díky společné hranici jako možnost výjimečného zastoupení. Rozvoj a vývoj systémů nikdy provozem a bezpečností nezastoupíte, ale zároveň odtržení je zcela nemožné, protože polovina procesů je sdílená. Outsourcing vždy představoval alternativní řešení zajištění potřeb, ale již před 15 lety se jasně ukázalo, že dává ekonomický smysl pouze outsourcing hybridní, tedy takový, který lze dobře zkontrolovat.

Vliv na personální strategie a profilaci zaměstnanců ICT bude mít nepochybně případný nástup volného využívání kapacit Národních datových center, respektive státní části eGovernment Cloudu, jakmile to bude možné.

Rozvoj a udržení znalostí a kompetencí

Informatika je znalostní disciplínou, závislou na udržování aktuálních přehledových i detailních znalostech v oboru. Provedený ICT Benchmark zjistil, že některé OVS mají pro každého zaměstnance ICT útvaru v rozpočtu na vzdělávání vyhrazenu mizivou částku, odpovídající 1 hodině až 1 dni komerčního školení ročně.

Aktivní zapojení ICT do digitální transformace a dobře napsaná IK úřadu musí argumentačně podpořit vyjednávání informatiků o rozpočtu. Vedle toho je ale úlohou útvaru Řízení ICT na MV (OŘI) zajistit dostupnější školení pracovníků VS podílejících se na řízení a provozu ICT služeb, ať využitím výše uvedených kompetenčních center VS nebo pro tento účel úzce spolupracovat s univerzitními pracovišti.

Podmínkou rozvíjení kompetencí je ale vůbec vlastní pracovníky získat a udržet. Proto je nutné změnit odměňování pracovníků, řídících ICT ve státní správě tak, aby se blížilo svojí úrovní srovnatelným profesím v soukromém sektoru a aby bylo závislé na dosahování jasně stanovených osobních cílů. To odpovídá hlavnímu cíli č. 4 IKČR a musí realizovat opatřeními centrálními i místními, například větším využitím institutu „Klíčového zaměstnance“.

S ohledem na obtížnost prosazení této změny by změna mohla probíhat postupně od klíčových rolí k rolím méně významným. Klíčovými rolemi jsou v této fázi role, které budou vytvářet novou koncepci řízení ICT ve VS, navrhovat architekturu služeb VS a ICT služeb, formulovat sourcingovou strategii, formulovat poptávky na externí dodávky, vybírat nejvhodnější nabídky a kontrolovat stav dodávek.

Vztah profese ICT a státní služby

Základem poctivého řízení je věci neskrývat a nazývat je pravými jmény. Pokud tedy podle IKČR a MŘICT jsou v ICT VS potřební odborníci například pro role z oblasti strategického plánování a řízení transformačních změn, tedy zejména role architektů úřadu nebo programových a projektových manažerů, pak je potřeba urychleně rozšířit obory státní služby o tyto role. Tato změna je v souladu s dílčím cílem 4.1 IKČR.

Současně platí, že profese podílející se na řízení ICT, eGovernmentu a strategických změnách musí být schopné čerpat a přenášet do veřejné správy zkušenosti z mnoha dalších odvětví. Musejí být proto velmi flexibilní na pracovním trhu, přičemž díky své expertíze ani nestojí o ochrannou ruku služebního poměru, naopak.

Pro takové případy by mělo být možné zaměstnávat experty jak ve služebním, tak v zaměstnaneckém poměru, a bez ohledu na to je odměnit stejně jako na trhu práce, odkud je potřeba je do VS získat a zde udržet.

Ekonomické a finanční řízení ICT

Sestavování rozpočtu, rozpočtová opatření

Rozpočet jako takový je klíčový pro fungování všech ICT služeb dané organizace a ve většině se skládá z mnoha položek. Je na každém představeném, jak a jakými nástroji bude provádět, nebo provádí faktické sestavování a následné reportování rozpočtu. Rozpočet na nejvyšší úrovni tvoří povinné (obligatorní[64)]) a nepovinné (fakultativní) výdaje. Rozdělení lze definovat též jako provozní (OPEX) a investiční (CAPEX), toto označení se využívá převážně v soukromoprávních organizacích, ale významově je lze vztáhnout i na oblast veřejné správy.

Při sestavování rozpočtu je třeba si uvědomit několik souvislostí:

- ICT má ve správě majetek, o který je třeba dlouhodobě pečovat s péčí dobrého hospodáře – to znamená, že na každou položku je třeba počítat s položkou podpory a správně se rozhodnout, zda je nebo není nutné podporu pořizovat (velkou nápomoc k tomuto má dlouhodobá vize a strategie)
- V čase může docházet ke snižování cen u IT komodit, tudíž je třeba sledovat a plánovat jejich snižování např. přesoutěžením dle ZoZVZ[65)] apod.
- Morální zastarávání informačních systémů počínaje sedmým rokem IS prodražuje systém (mandatorní výdaje jsou progresivní), desátým rokem pak může dojít k markantnímu nárůstu. Z tohoto důvodu je třeba systém inovovat, nebo začít plánovat jeho obměnu.
- Mnoho komodit lze využívat jako službu.
- Interní zdroje nejsou ty nejlevnější, naopak jsou nejvzácnější a mnohdy jedinečné – proto je neefektivní nasazovat tyto zdroje na plnění závazků, o kterých si myslíme, že je zvládne každý – zde ušetříme na nákladech minimum a o tento lidský zdroj ve většině po nějaké době přijdeme a jeho nahrazení stojí organizaci vysoké finanční prostředky a vždy odliv znalostí k externímu dodavateli.
- Nové projekty a požadavky nevznikají většinou ze dne na den, vedení organizace by mělo mít ve své kultuře zakořeněno, že každý nový požadavek je komunikován na všechny aktéry včetně ICT útvaru. Je více než vhodné oslovit při sestavování rozpočtu své věcné garanty, a zavést systém sběru požadavku (bude zmíněno dále v dokumentu).

Sestavování rozpočtu pak nemá být jednostranný akt. Požadavků a nároků, které ICT útvar předkládá, se může zdát příliš, ale je třeba si uvědomit, že tento útvar představuje podpůrnou jednotku mnoha interních služeb a služeb klientům VS. Proto je nutné rozpočet ekonomickému představenému interpretovat a vzájemně ho vyjednat v takové míře, že je všem aktérům jasné, co jaká položka znamená a jaký účel podporuje. Závěrem musí dojít k předakceptaci rozpočtu.

K finální akceptaci pak dojde po potvrzení rozpočtu vládou a parlamentem. V případě požadavku na **snížení rozpočtu** může docházet **pouze ke snižování fakultativních výdajů**. Představený ICT v tomto případě připraví dopadovou analýzu, na které části služeb ICT bude mít toto snížení dopad včetně definice rizik a upozorní písemnou formou vedení úřadu.

Ke snižování výdajů obligatorních (provozních) položek pak může zákonitě docházet pouze v programovém financování, tedy středně a dlouhodobém výhledu. Důvodem jsou hrozby a vysoká bezpečnostní rizika související se snižováním dlouhodobých závazků a s nimi spojeným poklesem rozsahu, kvality dostupnosti nebo bezpečnosti služeb. Tomuto snižování musí předcházet důkladná dopadová analýza a schválení jejích závěrů vedením úřadu. Ve většině případů musí být dlouhodobé snížení spojeno s předchozí jednorázovou investicí do opatření, která snížení umožní a/nebo rizika zmírní.

Na tomto místě je třeba upozornit, že jakýmkoli neplánovaným zásahem do mandatorních výdajů (resp. jejich finančního krytí) v rámci ročního rozpočtu může dojít k porušení zákonných povinností (ZoKB, ZoFK atd.). Jakoukoli odpovědnost za případnou škodu má následně ten představený, který mandatorní výdaje bez analýzy a schválení ICT představeného uskutečnil, eventuálně schválil, nebo nařídil.

Reporting a kontrola rozpočtu

Každý představený musí kontrolovat čerpání rozpočtu zejména z těchto důvodů:

- Předběžná řídící kontrola dle zákona.
- Kontrola plnění smluvních závazků.
- Naplňování rozpočtu, jde zde zejména o položky nově pořízené – zde může být zajímavá rozdílová položka plán-skutečnost.
- Porovnání plnění 3-5 let v hlavních kategoriích, tedy mandatorní a fakultativní výdaje.
- Sledování nákladů na všechny služby ICT – zde se sledují položky interních personálních výdajů (včetně školení) a výdajů na provoz a rozvoj služeb ev. nákladů na pořízení nových ICT služeb

Detailnost rozpočtu je závislá na požadavcích představeného a stylu jeho řízení ev. na požadavcích jeho nadřízeného. Je vhodné sestavovat vlastní reporty a v koordinaci se svým nadřízeným reporty pro nadřízeného.

Tvar a podoba reportu je závislá na možnostech útvaru ICT. Doporučeným postupem může být vedení v podobě tabulky přístupné pod heslem na sdíleném disku. Nejhodnějším způsobem se však jeví on-line reportovací nástroj s pokročilou vizuální stránkou ev. portálovým přístupem na základě rolí a identity.

Jak již bylo zmíněno výše, rozpočet ICT útvaru se skládá z několika částí, tedy z:

- provozních prostředků určených na služby a nákupy do 40 tisíc Kč.
- investičních prostředků, které vychází z programového financování a reprodukce majetku.
- dotačních titulů, které sice navyšují v daném čase rozpočet na schválenou investici, ale zároveň zamkne tento titul kofinancovanou částku, tedy je nutné snížit rozpočet ostatních nákladů.
- nadpožadavků, které mohou být někdy schváleny, ale jejich čerpání pak musí být zahrnuto v aktuálním rozpočtu a případné nevyčerpání se nakonec objeví v nespotřebovaných nárocích, které uměle navyšují rozpočet pro daný rok.
- krátkodobých nebo dlouhodobých rozpočtových opatření, které vychází z aktuálních potřeb čerpání.

Všechny výše uvedené části jsou realizovány samostatně a je nutné z nich vytvořit reálné možnosti pro optimalizaci nákladů. Základním východiskem je znalost všech závazků a precizní nastavení pevných plateb mimo rámec legislativních změn (tyto si žijí vlastním životem a i v případě schválení navýšení rozpočtu jsou tyto prostředky k dispozici až v dalším roce).

Problematice rozpočtování a finančního řízení bude věnována samostatná metodika vycházející z praxe a z přirozeného chování ICT.

Koncepce řízení ekonomiky ICT ve veřejné správě

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Řízení smluv a závazků vůči dodavatelům

Nedílnou součástí řízení ICT je správa smluvních vztahů s dodavateli, a to zejména z těchto klíčových hledisek:

- udržování přehledu o smluvních závazcích a plánování cash-flow výdajů

- udržování přehledu o termínech ukončení smluv a plánování jejich obnovy

Součástí řízení smluv je i úsilí o konsolidaci portfolia vztahů do řiditelného množství dlouhodobých partnerů a snaha o narovnání chybně uzavřených, obvykle nevyvážených smluvních vztahů.

Samostatným tématem je správy portfolia licencí a licenčních smluv, viz následující kapitola.

Útvar ICT musí, často ve spolupráci s ekonomickým útvarem, disponovat bezchybnou, nejlépe elektronickou evidencí údajů o smlouvách a ze smluv tak, aby s pomocí těchto nástrojů mohl plnit potřeby z výše uvedených hledisek. Přitom je důležité vzít v potaz ještě následující:

- Obnovení smlouvy (například na údržbu) může v procesu tvorby zadání a výběru dodavatele dle ZoZVZ trvat až dva roky, proto je potřebné jej zahájit s dostatečným předstihem.
- IS pro evidenci a řízení smluv s dodavateli je transakční systém, nemůže být nahrazen jenom spisovou službou, nýbrž na ni musí být integrován.
- IS smluv musí být propojen na správu portfolií (katalogů) ICT aktiv a umožnit řízení i z jejich pohledu.
- Součástí řízení smluv je i vazba na řízení rizik, spojených s výpadkem smluv a na řízení rozpočtů, pro zajištění závazků ze smluv.

Více praktických doporučení a pomůcek k řízení smluv s dodavateli bude postupně vydáno ve Znalostní bázi.

Komplexní správa licencí

Řízení licencí je dnes zcela samostatná oblast ICT, která musí mít pozici pro roli “licenčního manažera” alespoň na centrální úrovni (míněno jeden člověk za každý rezort, jinou korporaci nebo velký OVS) nebo dílčí roli u pozice manažera ICT v menším OVS. Součástí aktivit licenčních manažerů je stanovit pravidla a mít vlastní licenční politiku. Právě v těchto pravidlech může licenční manažer potvrdit platformu jednotlivých rezortů, korporací a OVS.

Mezi primární aktivity této role patří správa licencí Microsoft, IBM, Oracle, WMvare, antiviru, Adobe a dalších, které se užívají v různých oblastech ICT. Mezi sekundární aktivity potom patří zpřehlednění a správa všech dalších licencí každého OVS.

U každé licence je nejdůležitější její rozsah, čas a náklady. Dále je důležité, k jakému objektu se vztahuje (jak se počítá) - uživatelé, procesory, apod. Podstatné je však, jaká jsou s licencí spojené práva, například přenositelnost pro osoby třetích stran.

Pokud se úřad rozhodne pro OSS/FS licenci, potom musí zajistit její alternativní řešení v případě ztráty podpory (pro názornost uvádíme, že v případě užití Open Office stačí konstatovat v případě ztráty podpory nutnost pořízení Microsoft Office nebo jiného podobného produktu).

Evidence licencí v ICT musí být na jedné straně provázána na majetkovou evidenci v ekonomickém útvaru, dále na správu portfolií aktiv (Katalogy), na správu uživatelů a oprávnění, správu znalostí a kompetencí (Anti-Vendor-Lock-In opatření) apod.

Součástí místní nebo korporátní správy licencí musí být vazba na centrální nákupy licencí státu a maximální využití nabízených centrálních licencí, viz SPolupráce s ostatními útvary úřadu a eGovernmentu.

OpenSource Software a Free Software

Součástí zodpovědnosti role Licenčního manažera OVS je i koordinovat a podporovat rozhodování o použití OpenSource Software a Free Software (také jako "OSS/FS") jako způsobu realizace jednotlivých IS, viz kapitola Řízení jednolitých ICT řešení.

Na úrovni útvaru ICT, případně korporace a státu, je potřeba přijmout politiky a opatření, která umožní na jedné

straně převzít zodpovědnost a vybudovat kapacity pro podporu a údržbu OSS/FS, zejména pokud bude mít podobu sdíleného programového kódu veřejné správy a na druhé straně budou představovat exit strategii odchodu od OSS/FS v případě ztráty jeho podpory.

Součástí kompetence licenčního manažera je také disponovat nezbytnými znalostmi, podklady a pomůckami pro úspěšné zacházení s OSS/FS v průběhu životního cyklu IS (návrh řešení, zadávací dokumentace, smluvní ustanovení, správa kódu, dokumentace, sdílení apod.).

Další věcná a odborná doplnění budou po projednání s odbornou veřejnosti obsažena v následujících vydáních MŘICT a aktualizována ve Znalostní bázi.

Správa vlastních informačních systémů ICT

Útvar ICT je případě dodávky služeb ICT podpory pro své vlastní procesy ve dvojí roli klienta i dodavatele těchto služeb. Proto je třeba, aby útvar ICT:

- pro dílčí řízení těchto systémů důsledně rozdělil role Věcného správce a Technického správce mezi dva zaměstnance, přičemž na úrovni CIO jde o zdvojení zodpovědnosti,
- pro celkové řízení portfolií a služeb postupoval stejně, jako při správě aplikací pro všechny ostatní věcné správce.

V důsledku toho musí být i aplikace potřebné pro řízení ICT a dodávku ICT služeb plnohodnotně viditelné v celkových modelech architektury úřadu, viz také Předpoklady a východiska řízení ICT.

Další věcná a odborná doplnění, týkající se jednotlivých klíčových typů informačních systémů, užívaných útvarem ICT pro vnitřní řízení a poskytování svých služeb (CMDB[66)], ServiceDesk, apod.), budou po projednání s odbornou veřejnosti obsažena v následujících vydáních MŘICT a aktualizována ve Znalostní bázi.

Strategické plánování a řízení ICT OVS

Zásadní změnou v řízení ICT OVS, zdůrazňovanou v MŘICT, je samo zavedení a důsledné využívání pro-aktivního strategického plánování ICT, v kontrastu s dosud povětšinou reaktivním přístupem k zavádění změn a k řízení provozu řešení pro ISVS a další systémy.

Další podstatnou změnou je úsilí o plánování a řízení s poznáním a porozuměním úřadu v jako celku a v kontextu eGovernmentu ČR a EU a v kontextu reálných potřeb a možností klientů úřadu čerpat jeho zejména digitální služby.

Součástí a podporou pro tento změněný přístup je nově, v souladu s cíli IKČR, využití architektury úřadu jako manažerské metody na podporu řízení ICT a digitální transformace úřadu.

Přístup ke strategickému řízení informatiky prostřednictvím architektury úřadu

V běžném managementu transformujících se organizací, a pro veřejnou správu to platí obzvláště, je velká mezera mezi kreativním stanovením strategických směrů a cílů a nalezením proveditelných zadání realizačních projektů akčního plánu. Většina strategických změn musí současně obsahovat podstatnou změnu ICT podpory a vede na ICT projekty výstavby nebo zásadní změny ICT řešení.

Zcela oprávněnou potřebou útvaru ICT v roli technického správce je dostávat od strategických a odborných útvarů (věcný správce) smysluplné, správné, srozumitelné a proveditelné zadání, viz také přístup ex-ante Řízení jednolitých ICT řešení.

Prostředkem, jak překlenout propast mezi zvoleným strategickým směrováním a proveditelným zadáním projektu je právě využití architektury úřadu, zejména vypracování architektonické vize a kompletní individuální architektury úřadu a jejich uplatnění při tvorbě Informační koncepce OVS a při návrhu řešení jednotlivých změnových záměrů.

Pravidla tvorby architektonické vize a architektury úřadu

Každý orgán veřejné správy je povinen jako předpoklad, východisko a součást své Informační koncepce vytvořit a udržovat individuální model cílového stavu a plánovaných přechodových stavů architektury svého úřadu v souladu s pravidly Národního architektonického rámce a IKČR.

Úřady na vrcholové a gesční úrovni (viz Kap 4.1.3) veřejné správy jsou povinny udržovat model architektury úřadu v rozsahu odpovídajícím tomu, jak je daný úřad povinen, oprávněn či schopen přímo nebo nepřímo ovlivňovat podřízené organizace, tvořící spolu s ním veřejnoprávní korporaci, ať již rozpočtově, metodicky, spádově, přirozenou autoritou.

Metodika NAR předepisuje úřadům vytvářet individuální modely své architektury ve třech stupních rozsahu, jako modely strategické, segmentové a schopnostní architektury úřadu.

Tvorba a údržba celkových konzistentních modelů architektury úřadu je trvalý a iterativní proces, realizující změny v architektuře jednotlivými konkrétními zadáními (úlohami), architektonickými angažmá[67)]. Typickými architektonickými angažmá tedy budou:

- architektonická vize úřadu
- architektura pro aktualizaci Informační koncepce úřadu,
- architektura projektu pro žádost na OHA,
- architektura pro posouzení proveditelnosti legislativní změny, apod.

Každé architektonické angažmá úspěšně končí schválením jeho výstupů architektonickou radou úřadu a jejich akceptací zadavatelem (sponzorem).

Kompletní pravidla pro tvorbu architektonické vize a kompletní individuální architektury OVS přináší dokument Národní architektonický rámec (NAR). Další detaily a pomůcky, zejména k jednotlivým typům architektonických angažmá jsou průběžně aktualizovány ve Znalostní bázi.

Role, procesy a obory v rámci architektonických změn úřadu

Schopnost tvorby údržby a užití architektury úřadu a její organizace, by měla být v každém OVS zajištěna nejméně dvoustupňově, s případnou vazbou na architektonické orgány a role nadřízené korporace a eGovernmentu ČR.

Prakticky půjde zejména o rozdělení kompetencí mezi architektonickou kancelář úřadu (AK), která spolu s projektovou kanceláří úřadu bude součástí „štábu“ vedení úřadu a mezi útvar architektury ICT, začleněný do útvaru ICT úřadu.

Architektonická kancelář úřadu s rolemi Hlavního architekta a doménových Enterprise architektů zajišťuje zejména celkový pohled na architekturu úřadu na úrovni detailu „enterprise“, prvotní rozpracování strategického směrování a podporu Informační koncepce OVS.

Útvar architektury ICT má naproti tomu zejména zodpovědnost za detailnější úrovně proveditelné architektury jednotlivých řešení na úrovni „Solution“ a „Design“.

Ve „štábní“ AK jsou více potřebné role byznys architektů, podporujících věcné správce jednotlivých segmentů úřadu a jejich agend ve tvorbě byznys zadání, kdežto v útvaru IT architektury jsou více potřební aplikační, datoví a technologičtí architekti jednotlivých platforem a řešení.

Tato doporučená pravidla samozřejmě mohou mít své výjimky, dočasně například útvar ICT může suplovat i kompetence Hlavního a Doménových enterprise architektů.

Za účelem zajištění výkonu řízení architektury by měly být definovány zejména tyto procesy:

- Řízení architektonických změn,
- Poskytování konzultací a metodické podpory,
- Řízení architektonických standardů,
- Řízení dokumentace architektury,
- Správa úložiště architektonických modelů.

Za účelem rozdělení odpovědností za jednotlivé složky architektury má být architektura dané organizace ve smyslu návrhu, rozvoje a údržby rozdělena do několika oborů, zejména odpovídajících doménám metamodelu NAR, tedy na:

- motivační architektury, zejména strategická architektura a bezpečnostní architektura,
- vertikální architektury jednotlivých segmentů, agend a schopností a jejich informačních systémů, přes všechny vrstvy
- horizontální architektury úřadu: byznys architektura, aplikační architektura, datová architektura, technologická architektura a síťová architektura
- průřezové architektury - celková Enterprise architektura a její vize.

Obor architektury jako takový představuje podmnožinu architektury, vyžadující od odpovědných architektů podobnou specifickou kvalifikaci a znalosti. Za návrh, správu a rozvoj architektur v jednotlivých oborech je odpovědná role hlavního architekta pro daný obor. Odpovědnosti a úkoly těchto rolí budou detailně dopracovány v dalších přílohách MŘICT ve Znalostní bázi.

Principy, vzory a referenční architektury – standardy pro architektonické změny

V rámci výše uvedených a popisovaných změn na architektonické úrovni je nutné definovat standardy, v podobě tzv. architektonických principů a architektonických vzorů[68)] a přístup k referenčním architekturám, které zavazují jednotlivé role a vytváří tak účinný nástroj k centrální jednotné koordinaci architektonických změn.

Obecně lze nahlížet na problematiku principů, vzorů a referenčních modelů následovně:

- Architektonické principy definují základní pravidla pro návrh architektury v jednotlivých oborech.
- Architektonické vzory deklarativně vyjmenovávají seznam standardních a povolených technologií, jejich kombinací a způsobů použití, metodik a přístupů k budování řešení zaměřených na specifické oblasti a problémy. Architektonické vzory jsou povinnou předlohou příslušných částí architektur úřadu nebo jednotlivých řešení. Vzory jsou referencí (odkazem) architektonického obsahu.
- Referenční modely architektury představují jednotnou klasifikaci v modelu a topologii (umístění) prvků určité domény nebo segmentu v diagramu. Referenční modely jsou referencí (odkazem) řádu a formy.

Útvary architektury mají povinnost přebírat celostátní architektonické principy, vzory a referenční modely z NAP a NAR a uplatňovat je ve vlastních individuálních modelech. Mají právo vytvářet vlastní dílčí principy, vzory a referenční modely na úrovni celého úřadu nebo dokonce veřejnoprávní korporace (rezortu, kraje nebo obce), pokud nejsou v rozporu s celostátními.

Je žádoucí, aby se oboje (státní i vlastní) principy, vzory a referenční modely plně uplatnily v celém životním cyklu jednotlivých ISVS a promítly se do standardizace a sjednocování architektur celého úřadu, včetně například prosazování jednotlivých standardizovaných platforem v zadávacích dokumentacích pro výběr dodavatele dle ZoZVZ.

Další věcná a odborná doplnění, týkající se architektonických principů, vzorů a referenčních modelů, budou po projednání s odbornou veřejnosti obsažena v následujících vydáních NAR a NAP a aktualizována ve Znalostní

bázi.

Návrh ICT služeb souborem nástrojů architektur řešení a řízení služeb

Pro návrh a následnou podporu služeb ICT a vlastně služeb jako takových lze využít kombinací systematických pohledů ITIL v5 a NAR (resp. TOGAF[69)]), respektive kombinaci jejich metod.

ITIL je dnes faktickým standardem pro implementaci řízení IT služeb a sbírka nejlepších zkušeností („best practice“) z oblasti řízení služeb IT a z nich vyplývajících doporučení. Za pomoci jednotlivých managementů nabízí systematický přístup k nalézání, plánování, dodávce a podpoře IT služeb (klient VS, interní zadavatel/klíčový uživatel). Svými oblastmi pokrývá celý životní cyklus služeb v částech Service Strategy, Service Design, Service Transition, Service Operation a Continual Service Improvement. Řídit služby dle ITIL tedy znamená zejména nastavit procesy a připravit systémovou podporu. Efektivní řízení ICT služeb dle ITIL (SLM) a vyhodnocování jejich SLA vyžaduje existenci tzv. runtime model služby neboli servisní strom služby.

Naproti tomu pomocí Enterprise architektury realizujeme formální popis architektury organizace a jejích klíčových prvků a vazeb. TOGAF resp. ADM [70)] pak zavádí systematický přístup k řízení architektury služby jako takové včetně jejích změn. V rámci návrhu a životního cyklu služby se EA model vytváří dříve než servisní strom a model tedy může sloužit jako podklad pro návrh servisního stromu.

Aktuálně je problém návrhu služby ve vztahu k jejímu řízení tristní, tedy, že dochází ve většině k úplné absenci a zanedbání, resp. zadavatel si není vůbec vědom, že SLA nebo OLA bude v budoucnu definovat. Právě stručně popsaný vizuální model (architektura) služby může rychle a efektivně celou věc návrhu služby zkvalitnit a pokrýt budoucí rizika spojená s návrhem měření a podpory jako takové. Pro funkční model návrhu služby a ve vztahu k jejímu provozu jsou nezbytné následující předpoklady:

- EA model je uložen v architektonickém repositáři organizace
- v EA modelu je na aplikační vrstvě každá aplikace a služba prezentována jednou entitou, tedy jedná se o jakýsi prototyp aplikace
- na technologické vrstvě jsou modelovány již všechny instance v souladu se servisním stromem

Kombinací metod ITIL a Enterprise architektury lze pak využít pro:

- návrh a implementaci služeb dle ITIL v organizaci,
- popis dané služby vizuálním architektonickým modelem,
- účely dekompozice a definice klíčových rozhraní služby a definic indikátorů a měření,
- nástroj rychlé dopadové analýzy v případě jakékoli změny v rámci služby, změny v rámci celé organizace tzn. jaký dopad má tvorba nové služby na celý ekosystém ICT.

Sjednotitelem a hybatelem je jak v ITIL, tak NAR změna. Přitom se z hlediska volby dalšího postupu musí rozlišovat tzv. velké a malé změny. Velké změny jsou takové, jdou nad rámec stávající schválené architektury úřadu, představují vznik nových objektů, komponent a služeb a vyžadují zapojení procesu aktualizace architektury úřadu (EA), případně její IK OVS. Naproti tomu za malé změny se považují takové, které nezakládají existenci ničeho nového, nevyžadují změnu architektury úřadu, ale přinášejí nějakou novou kvalitu služeb. Proto je vhodnější změny rozdělovat na změnu stávající ICT služby a tvorbu ICT služby nové.

Centrální úložiště modelů architektur OVS a práce s ním

Architektonické úložiště může být velice účinný nástroj pro koncepční práci v rámci všech změn služeb ICT. Architektonické úložiště, stejně jako třeba úložiště programových kódů, plní archivační a operační funkce. Je to podpůrný informační systém sloužící pro popis, centrální evidenci, řízení a sdílení architektury. Na úrovni OVS (a/nebo jeho korporace - rezortu, kraje, obce) je vytvořeno za účelem zajištění konzistentních, vzájemně kompatibilních a propojitelných popisů a modelů architektury.

Předpokladem je vytvořená a udržována závazná metodika návrhu a dokumentace architektury, která vychází primárně z metodiky NAR a principů a standardů IT architektury z NAP. Následnou práci s úložištěm provádí jakákoli role Architekt (externí/interní). Architekt před zahájením tvorby návrhu architektury vždy ověří existenci standardů - principů, vzorů a referenčních architektur upravujících návrh architektury v řešené oblasti v systému resortního úložiště modelů. Pokud Architekt nemá přímý přístup k úložišti, vyžádá si od správce úložiště export architektonických vzorů, principů a referenčních architektur vztahujících se k dané problematice.

Úložiště má nejenom ukládat jednotlivé modely, ale zejména disponovat nadstavbou pro rychlou dopadovou a rozdílovou analýzu při změnách velkého i malého rozsahu. Tato nadstavba má jednoduše (nejlépe ve stromové struktuře) a pomocí dotazů a výrazů najít potřebné vztahy a informace o uložených objektech. Objekty v úložišti nemusí mít pouze charakter architektonický, je zde možné uložit nebo integrovat informace z jiných zdrojů jako je HR (org. struktura), ERP (finanční a majetkové informace), PPM (informace o portfoliích projektů a projektech samotných), CMDB a servisního katalogu (informace o službách a položkách infrastruktury) apod. Úložiště musí umožňovat rozdělit právy pohledy na celý resort a úřad (hlavní architekt a další role) od pohledů na řešení a služby (jejich správci a dodavatelé).

Architektura OVS, případně jeho rezortu musí být v rozsahu stanoveném NAR předávána do centrálního architektonického úložiště, spravovaného OHA MV. Předpokladem správné funkce je správně definované integrační rozhraní a jeho konfigurace, s povinným využitím mezinárodního standardu modelů ArchiMate TOGAMEFF[71)]. Dalším důležitým předpokladem je metodika tvorby architektury daného OVS a jeho rezortu, které musí úplně adaptovat standardy a principy NAR.

Informační koncepce OVS

Povinnost zpracovávat informační koncepci je uložena zákonem č. 365/2000 Sb. všem OVS, které spravují ISVS. Uvedený zákon a jeho „prováděcí“ vyhláška 529/2006 Sb. specifikují jak obsahovou strukturu informační koncepce OVS, tak i procesy s ní spojené.

Metodickým a znalostním základem IK OVS je individuální model stávající a cílové architektury úřadu. Informační koncepce OVS je oficiálním (tzv. dodatelným) dokumentem pro výsledky práce architektura úřadu.

Další věcná a odborná doplnění, týkající se tvorby Informační koncepce OVS, budou po projednání s odbornou veřejnosti obsažena v následujících vydáních NAR a NAP, vydána jako metodické pokyny OHA a aktualizována ve Znalostní bázi.

Další metody strategického řízení ICT

Další metody strategického plánování a řízení ICT útvaru, vedle architektury úřadu a IK OVS, budou po projednání s odbornou veřejnosti obsaženy v následujících vydáních MŘICT a aktualizovány ve Znalostní bázi.

Plán realizace změn (Roadmapa)

Plán nezbytných balíčků práce (námětů, záměrů, projektů, programů) vedoucích k realizaci rozdílů mezi stávající a cílovou architekturou úřadu, zejména v oblasti ICT podpory všech jeho činností je výsledkem architektonické práce a projektového plánování.

Formálně je tento plán součástí povinné Informační koncepce OVS a základem řízení transformačních změn OVS v jeho projektové kanceláři. Vedle toho je ale předmětem sdílení a centrální koordinace s (budoucí) projektovou kanceláří eGovernmentu.

Řízení identifikace a realizace změn ICT OVS

Pro správný chod služeb ICT a útvaru ICT je řízení změn klíčové. Změna je velkým hybatelem, který ovlivňuje celé ICT prostředí a organizaci samotnou. Základem je řízení očekávání resp. požadavků. Ve velké většině mohou být právě požadavky realizovány formou změny. Jak již bylo výše naznačeno, změna sjednocuje metodiku ITIL, který řídí spíše provoz a rozvoj stávajících služeb a TOGAF, který se soustřeďuje na nové služby, resp. je i vhodné ho využívat v kombinaci s ITIL přístupem na velké změny v rámci stávajících služeb.

Všechny výše uvedené postupy je třeba jednotně definovat, včetně rolí a odpovědností. Dobré praxe a rozpracované metody přístupu kombinace ITIL a TOGAF budou součástí detailní metodiky, která toto téma rozpracuje detailněji včetně předloh a schémat ve Znalostní bázi.

Dále třeba uvést definičně a ideově do kontextu RFC a IT architekturu. Zkratka RFC, pocházející z anglického názvu „Request for change“, reprezentuje v prostředí úřadu požadavek na změnu. RFC v kontextu řízení architektury je požadavek na změnu mající dopad do jednoho nebo více architektonických oborů.

Change management proces reprezentuje v prostředí dané organizace standardní proces zajišťující příjem, zpracování, implementaci a nasazení požadavků na změnu. Change management proces v kontextu řízení architektury je proces řízení změny mající dopad do architektury anebo vyžadující architektonické vstupy.

Sběr a vyhodnocování požadavků na změny, jejich řízení a klasifikace

Požadavek je základ provozu a rozvoje služeb ICT. Standardní a jednotné řízení zajišťuje službu ICT kvalitní a inovativní. Požadavky mohou vznikat v těchto kategoriích:

- Běžným provozem (infrastruktura, koncový uživatel, klíčový uživatel apod.)
- Jako výstup procesů ITIL zejména však Incident (včetně Security In.), Problem, Continuity a Availability management
- SLM – řídící výbory a SLA negociační schůzky
- Obsluha klientů (call centrum, dotazník spokojenosti apod.)

Jako inovativní proces vstupující svými požadavky je třeba zmínit Idea management.

Ve veřejné správě je třeba brát v mnohých případech do úvahy další zdroje požadavků:

- Legislativa (zákony a podzákony, komunitární právo EU)
- Političtí představitelé (Vláda ČR a její program, ministr a politické vedení OVS, program strany)
- Zápisy z porad jednotlivých odborných sekcí a porad daného OVS

Co se týče kanálů, je třeba omezit počet kanálů, které zadávají požadavky na minimum a mít je, pokud je to možné, pod kontrolou jednoho konkrétního organizačního útvaru.

Nejběžnější variantou obsluhy požadavků je ServiceDesk. Snahou ICT útvaru by mělo být všemi dostupnými nástroji donutit aktéry a procesy zadávat své požadavky právě zde. Organizačně a zdrojově je to nejméně náročný způsob obsluhy požadavků. Jak již bylo uvedeno výše, je dobrá úroveň obsluhy požadavků základem vzrůstající kvality ICT služeb a spokojenosti jejich klientů a uživatelů.

Další logickou částí je obsluha požadavku. Obecně se dá konstatovat, že obsluhu a koordinaci většiny požadavků zvládá, ze své podstaty, ServiceDesk (také jako „SD“) resp. funkce HelpDesk a obsluhující role SD. V rámci těchto aktivit lze plně využít jak technické nástroje SD tak best-practices ITILu. Pro požadavky projektové může sloužit nástroj PPM (Project Portfolio Management) a metodicky pak best-practices oboru jako PRINCE 2 apod.

Pro zvýšení transparentnosti přípravy nových služeb OVS a jeho rezortu a za účelem zefektivnění výsledných řešení je vhodné pří budování nových služeb využívat pilotních projektů s možností zapojení odborné veřejnosti

do návrhu a testování konceptů řešení, a tak ověřovat potřebnost, vhodnost, funkcionality a další aspekty navrhovaných řešení. Tento postup poskytuje uživatelům možnost otestovat služby a funkcionality již v době jejich návrhu, a zároveň možnost vyjadřovat se k podobě návrhu, případně zasílat náměty na změnu, rozšíření, či optimalizace navrhovaných služeb. Tak lze zajistit, že služby budou navrženy s ohledem na očekávání klientů – občanů a všechny případné nesrovnalosti, rozpory či dodatečné požadavky/očekávání klientů VS podchytit již v počátku a zapracovat do koncepce řešení nově připravované služby. Další nesporným přínosem realizace ověřovacích projektů je upřesnění požadavků na cílové řešení a očekávané funkcionality. V rámci případných veřejných zakázek na dodávku celých anebo částí služeb již lze poptávat přesnou množinu jasně definovaných funkcionalit. Minimalizuje se tak riziko, že budou neefektivně požadovány v budoucnu nevyužívané funkcionality a riziko vznesení velkého počtu změnových požadavků na optimalizace či přizpůsobení využívaných služeb.

Podrobnější informace, návody, postupy a pomůcky budou po projednání s odbornou veřejností vydány jako samostatný metodický dokument a jako průběžně aktualizovaná součást Znalostní báze.

Řízení projektů a programů úřadu

Informatika úřadu veřejné správy slouží jak jeho interním uživatelům pro výkon agend veřejné správy, tak externím klientům.

Ani na úrovni lokální samosprávy by žádné ICT projekty veřejné správy, tzn. ani podpůrných služeb (např. projekt elektronické spisové služby, nebo evidence docházky) proto neměly být čistě jednoúčelové, ale mají přispívat k naplnění cílů celého úřadu jako součásti celého eGovernmentu.

Všechny projekty úřadu, včetně informatických, musí být koordinovány vedle rozpočtového plánování a čerpání, přinejmenším v těchto aspektech:

- přínos projektu k naplňování cílů úřadu - musí existovat přehled, které projekty naplňují, které cíle a obráceně, které cíle jsou naplňovány jakými projekty,
- společné změny v architektuře úřadu - časově i funkčně sladěné realizace změn jednotlivých komponent architektury, se zřetelnou preferencí ke sjednocování a využívání společných řešení,
- koordinovaná spotřeba zdrojů jednotlivými projekty, zejména lidských - musí existovat centrální přehled úřadu o zaměstnancích, přidělených částí svého úvazku k jednotlivým projektům, ať již z pohledu projektů či z pohledu kapacit jednotlivých zaměstnanců.
- koordinované využití ostatních materiálních a majetkových zdrojů úřadu, jako jsou společné prostory, výpočetní kapacity, dostupný čas pro odstávky a výpadky apod.

Koordinace projektů, jejich provazování do programů a správa portfolií projektů je službou Projektové kanceláře úřadu (také jako "PK"[72)]). Navazuje na práci strategických útvarů a je znalostně podpořena službami útvaru celkové architektury úřadu, architektonické kanceláře (také jako "AK"). Oba tvary společně by měly být přednostně součástí tzv. „štábu“ vedení úřadu.

V druhé, nižší úrovni, již výhradně pro ICT projekty probíhá tato koordinace a řízení v útvarech řízení projektů, strategie a IT architektury uvnitř útvaru ICT úřadu.

Další věcná a odborná doplnění k celé problematice řízení projektů a programů budou po projednání s odbornou veřejnosti obsažena v následujících vydáních MŘICT a aktualizována ve Znalostní bázi.

Kategorizace programů a projektů

Pro snazší orientaci a aplikaci metod řízení programů a projektů by ty měly být děleny do více kategorií podle různých faktorů:

Podle pozice a zodpovědnosti investora, zejména podle jeho místa v hierarchii veřejné správy:

- celostátní projekty, svěřené vládou jednomu úřadu (dodá ředitele)

Podle velikosti či významu projektu

- strategický
- normální
- malý

Podle dopadu a způsobu jeho realizace

- Individuální (centrální nebo lokální), vždy v jediném úřadu
- Vějířovité (centrum → území)
- Postupné (Pilot / Roll-Out) šíření téhož (typové)
- Kombinované

Řízení programů

Všechny projekty, které vzájemně spolu souvisí v časové věcné či jiné návaznosti musí být řízeny jako program, aby bylo zajištěno, že společně dodají větší hodnotu a s větší jistotou, než kdyby byly řízeny každý samostatně.

Programy změn je možné identifikovat jak uvnitř jednotlivého OVS, tak napříč více organizacemi VS. V takovém případě musí být v definici programu jednoznačně stanoveno, které OVS bude program řídit.

Zatímco řízení projektů je zaměřeno primárně na dosažení plánovaných výstupů při dodržení spotřeby plánovaných zdrojů, je řízení programu zaměřeno zejména na splnění strategických cílů a dosažení očekávaných přínosů. Z tohoto pohledu je doporučeno, aby i každý samostatný projekt byl řízen nejenom s využitím projektových, ale i programových principů.

Základními sedmi principy programového řízení[73)] je:

- Být v souladu se strategií úřadu a s nadresortními strategiemi
- Být vůdcem změny
- Komunikovat žádoucí lepší budoucí stav úřadu
- Soustředit se na přínosy a možná ohrožení
- Přinášet měřitelnou hodnotu změny
- Navrhnout a vybudovat soudržné (coherent) schopnosti úřadu
- Trvale se učit ze zkušeností.

Programy změn je možné identifikovat jak uvnitř jednotlivého OVS, tak napříč více organizacemi VS. V takovém případě musí být v definici programu jednoznačně stanoveno, které OVS bude program řídit.

Všechny budoucí programy změn, nějak spojené s IT, musí být identifikovány v aktualizované IK OVS. Všechny finanční programy v rámci programového financování musí mít svůj předobraz v příslušném, v IKČR uvedeném věcném programu změn, pouze formální vytváření programů jen za účelem financování není podle IKČR přípustné. Přitom ale musí být pravidly rozpočtového financování zachován dostatečný prostor pro flexibilní manažerské rozhodování o realokaci přidělených finančních prostředků podle měnících se podmínek úřadu a eGovernmentu (re-prioritizace).

Všechny OVS, u nichž lze identifikovat projekty (viz následující kapitoly), které spolu vzájemně souvisí a společně se podílejí na dosahování přínosů, musí zavést procesy řízení programů, byť v praktickém minimálním rozsahu.

Pro nadresortní programy je nezbytné ustavení organizační struktury vládou ČR, včetně jmenovitého určení konkrétních osob manažersky odpovědných za řízení programu (ředitel programu) a oprávněných k přímému zadávání a vyžadování plnění úkolů ze strany zainteresovaných subjektů z jiných resortů.

Více informací a pravidel k řízení IT rozvojových programů, včetně vazeb na programové financování, vydá MV

ČR ve spolupráci s MF ČR ve formě Metodiky řízení IT rozvojových programů, ve které bude i základní struktura programu.

Řízení portfolia projektů

Aktivní správa jednoho či více portfolií projektů úřadu je prostředkem efektivního rozhodování o těchto projektech ve vzájemných souvislostech a ve vztahu k cílům úřadu a dostupným zdrojům úřadu. Obzvláště důležité je to v prostředí IT veřejné správy, kde zdánlivě či dokonce skutečně řada projektů spotřebovává množství zdrojů, aniž by přinesly očekávané přínosy.

V oblasti řízení projektových lidských zdrojů musí úřad vést plán rozvoje vybraných zaměstnanců tak, aby se z nich staly zdroje pro projekty, tj. aby byli schopni převzít zodpovědnost za vedení projektu (včetně projektových manažerů na straně objednatele), za specifické role ve štábu projektu, jako je architekt projektu, za vedení řešitelských týmů a za „stínování“ klíčových specialistů dodavatele, tj. za samostatnou práci na projektu pod vedením dodavatele a za převzetí know-how v rámci projektu. Toto určení musí být nezbytně zohledněno v charakteristikách služebních míst předmětných zaměstnanců.

Projekt, který by si z dostupných volných úvazků kmene kvalifikovaných zaměstnanců úřadu, představujících možné zdroje projektů, nedokázal sestavit projektové týmy a naplnit odhadovanou potřebnou kapacitu interních projektových pracovníků (viz povinně interní obsazování projektových rolí), nesmí být zahájen, dokud nebudou příslušně kvalifikované zdroje opět k dispozici. Takový projekt by si již od počátku nesl nepřípustně vysoké riziko neúspěchu. Projektové zdroje úřadu na druhou stranu nesmí být přetěžovány nad zákonné limity Služebního zákona a Zákoníku práce, nuceny k práci ve volném čase. To vedle rizik chybovosti vede z dlouhodobého hlediska k trvalé ztrátě těchto zdrojů úřadu.

V situaci, kdy plánované změny v úřadu a v jeho ICT vedou na více programů a projektů, než jaké jsou dostupné finanční, lidské a materiální zdroje úřadu, musí být prokazatelně uplatněn proces tzv. prioritizace projektů. A to nejméně jednou ročně, v souvislosti s plánováním rozpočtu, nebo kdykoli, kdy souběžně spuštěné nebo plánované projekty narazí na limity zdrojů úřadu. Proces prioritizace spočívá v rozdělení dostupných zdrojů a jejich přidělení pouze projektům, představujícím nejvyšší příspěvek k naplnění cílů úřadu nebo nezbytným dle legislativních změn. Projekty, které díky své aktuálně nižší prioritě nedosáhnou na zdroje úřadu, nebudou spuštěny nebo budou zastaveny do doby, dokud se nezvýší jejich priority nebo se nezvýší dostupné projektové zdroje úřadu. Popsaný proces je v gesci projektové kanceláře úřadu. Projektová kancelář musí být informována o všech projektech od okamžiku zahájení předprojektové přípravy.

Více informací a pravidel k řízení portfolií IT projektů, včetně vazeb na řízení lidských zdrojů, vydá MV ČR ve formě aktualizace Metodiky řízení IT projektů a rozmanitých akcelerátorů ve Znalostní bázi.

Řízení jednotlivých IT projektů

Řízení jednotlivých projektů ICT, podrobněji viz Řízení jednolitých ICT řešení, musí být centrálně koordinováno jak z pohledu „malé“ projektové kanceláře útvaru ICT, tak PK úřadu a nakonec i z pohledu budoucí centrální PK státu, resp. eGovernmentu, jakmile bude zřízena.

Realizace malých změn - průběžné zlepšování

V mnohých případech se to děje, ale není doporučeno, aby realizaci drobných, resp. malých změn řídil Change Manager. V případě malých změn je vhodnější tzv. koordinace, kdy exekuci provádí Koordinátor změny. V případě prosté koordinace nemá daná řídící role změny tolik formálních povinností v oblasti dokumentace a řízení jako role projektového vedoucího, a ve většině koordinuje i více změn a reportuje ve většině stručněji na úrovni operačního řízení provozu v jistých případech to bývá i úroveň projektově-rozvojová.

Řízení změn bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Řízení provozu IS a dodávky služeb

Řízení podpory klientů a uživatelů ICT služeb

Řízení podpory klientů a uživatelů ICT služeb bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Řízení provozu výpočetních a komunikačních technologií

Součástí každého útvaru provozu služeb OVS a jeho rezortu by měly být definovány požadované provozní parametry poptávaných systémů a služeb. Provozní parametry zahrnují především ukazatele dostupnosti služeb či systémů pro koncové uživatele a ukazatele doby odezvy. Oba typy parametrů by měly být navrhovány s ohledem na význam poskytovaných služeb a rozhraní, prostřednictvím kterých jsou služby poskytovány. Hodnoty provozních parametrů by pak měly být zohledněny v návrhu architektury cílových řešení, zejména v části zajištění kontinuity a výkonu řešení, a smluvně podchyceny ve smlouvách na provoz služeb a informačních systémů (SLA).

V prostředí OVS a jeho rezortu by měl být postupně zaveden přístup k definici smluvních parametrů služeb v tzv. katalogových listech služeb. Základní myšlenkou přístupu je, že služby jsou poskytovány prostřednictvím jednoho či více rozhraní a každé rozhraní je klasifikováno významem dle kategorií „Gold“, „Silver“ a „Bronz“. Pro jednotlivé kategorie služeb pak lze vytvořit sdílené katalogové listy a aplikačně specifické služby řešit v případě potřeby v rámci stručných specializovaných katalogových listů. Tento přístup lze aplikovat při přípravě libovolných zakázek s charakterem dodávek služeb provozu a podpory.

Řízení provozu výpočetních a komunikačních technologií na úrovni celého úřadu bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Monitoring provozu a služeb ICT

Každý systém, aplikace či služby musí být navrženy a implementovány tak, aby je bylo možné začlenit do dohledového systému OVS a dané rezortní organizace. Monitoring systém musí pokrývat metriky, jež jsou v provozních smlouvách (SLA) označeny jako automaticky monitorované a monitorovat tyto metriky v souladu s postupy a parametry v provozních smlouvách definovanými. Mimo takto označených metrik musí monitoring sledovat a vyhodnocovat další metriky obvyklé pro daný typ systému či aplikace.

Detailní metodiky a technický návrh týkající se nástrojů monitoringu budou doplněny po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Řízení rizik a bezpečnosti v ICT útvaru

Hlavním cílem při organizaci a řízení bezpečnosti v úřadu a v jeho útvaru informatiky je vytvoření a využívání řídících procesů pro efektivní prosazování a kontrolu bezpečnosti informačních systémů a technologií.

Pro řízení Kybernetické bezpečnosti a rizik se doporučuje využívat ustanovení zákona č. 181/2014 Sb. o Kybernetické bezpečnosti (včetně vyhlášky) nejen pro systémy spadající do gesce tohoto zákona, ale i pro ostatní informační systémy, neboť tento předpis stanovuje vhodné metody řízení kybernetické bezpečnosti.

Řízení rizik v ICT útvaru

Jakmile útvar ICT dostane úkol přesahující čerpání stávajících zdrojů, měl by alespoň před zahájením jeho plnění provést analýzu rizik a vytvořit mapu rizik, která – když je správně vyplněná – slouží pro celé řízení jako kontrolní prvek.

Mapa rizik by měla mimo oblast působnosti zohledňovat i rizika z jiných oblastí, která mohou způsobit pozastavení nebo zrušení úkolu. Mezi hlavní rizikové oblasti lze řadit:

- oblast kybernetické bezpečnosti
- oblast finanční
- oblast organizační
- oblast politickou (zohlednění případných politických rozhodnutí ovlivňujících splnění úkolu)
- oblast legislativní (zohlednění případné změny právních předpisů a jejich výkladu ovlivňujících splnění úkolu)

Jednotlivá rizika je nutné pojmenovat a odůvodnit jejich relevanci k danému úkolu. Následně musí být provedeno jejich zhodnocení za účelem stanovení způsobu jejich mitigace v rámci procesu řízení rizik.

Každé riziko má svého vlastníka, tedy osobu nebo entitu s odpovědností a pravomocí riziko řídit a opatření, která lze přijmout za účelem jeho zmírnění či úplného zrušení. Úroveň opatření přijatých za účelem mitigace rizik by měla být v souladu s výsledkem hodnocení rizik. V tomto ohledu je nutné si však uvědomit, že dosažení 100% eliminace veškerých rizik není možné ani při neomezených zdrojích. Je tak věcí vedení organizace, aby stanovilo přijatelnou úroveň rizika a zajistilo prostředky (nejen finanční, ale i personální, kompetenční atd.) nutné pro její dosažení.

Pro optimální účinnost potlačování rizik je vhodná kombinace technických a organizačních opatření. Na většinu rizik je přitom nutné pamatovat již před samotnou realizací daného úkolu či v rámci přípravy smluvní dokumentace s dodavateli.

Vedle řízení rizik na úrovni jednotlivých IS, jejich návrhu, vývoje a provozu, viz také Řízení jednolitých ICT řešení, spočívá těžiště řízení rizik a bezpečnosti v činnostech na úrovni celého úřadu, realizovaných útvarem informatiky ve spolupráci s dalšími bezpečnostními strukturami úřadu, jako jsou fyzická bezpečnost, Pověřenec pro GDPR, BOZP apod., viz Spolupráce s ostatními útvary úřadu a eGovernmentu.

Pro hodnocení rizik z oblasti kybernetické bezpečnosti lze využít metodiku vydanou NÚKIB, tvořenou hlavními aktivitami:

- Mapování a evidence aktiv
- Analýza rizik
- Proces řízení rizik
- Plán zvládání rizik,
- Hodnocení rizik
- Kontroly a audity

Tuto metodiku bude dobré provázat s metodami řízení rizik z projektových standardů (PMI, Prince2) a rámce TOGAF, společně s řízení finančních rizik apod. tak, aby mohly všechny společně přispívat do jednotného registru a procesů řízení všech rizik na úrovni úřadu. MŘICT podporuje při snížení či eliminaci rizik doporučení a metodické materiály tvořené NÚKIB:

- Minimální bezpečnostní standard
- Bezpečnostní standard pro videokonference
- Vodítka pro hodnocení dopadů

Přílohy typu mapy rizik včetně legendy, podpůrných otázek a měření dopadů a další věcná a odborná doplnění budou publikována po projednání s odbornou veřejností v následujících vydáních MŘICT a ve Znalostní bázi.

Řízení ICT bezpečnosti

Nezbytnou součástí dlouhodobě udržitelného provozu a rozvoje ICT daného OVS je prosazení kybernetické (informační) bezpečnosti. Za tímto účelem musí každý OVS implementovat stabilizovaný systém řízení bezpečnosti informací dle ZoKB a standardu ČSN ISO/IEC 27001:2013. V rámci tohoto systému nadále pokračuje zajištění bezpečnosti IS zařazených do ISVS prostřednictvím provozu a zlepšování systému řízení bezpečnosti informací. Dále by měl být kladen důraz na vyšší zapojení organizačních celků OVS do bezpečnostních činností, zefektivnění dohledových a monitorovacích činností a prohloubení zajištění bezpečnosti IS daného OVS.

Provoz a bezpečnost jsou propojeny díky několika aspektům. Je to primárně dostupnost, kdy bezpečnost stejně jako provoz zajímá dostupnost systému. V mnoha ohledech lze vzájemně využívat informace z monitoringových nástrojů.

Velice vhodné se jeví propojení Katalogu služeb a bezpečnostních aktiv, kdy lze díky propojení na další ITSM nástroj tedy Konfigurační databázi promítnout na jednotlivé položky rizika a tím velice rychle vidět dopady např. výpadků na aktiva organizace. Propojení se může dít jak na úrovni služby – jako její další atribut, nebo konkrétní konfigurační položky znovu na úrovni atributu.

Nabízí se zde i nástroj spojení Incidentů v rámci jednoho nástroje ITSM, tedy ServiceDesku. V tomto případě dochází k symbiotickým efektům obsluhy jednoho incidentu, kdy v případě Incidentu bezpečnostního dochází pouze ke změně kategorie, kdy tato změna automaticky přiřadí řešení Incidentu jiné skupině řešitelů. Je zde na místě provést opatření pro zajištění vyšší bezpečnosti informací, týkající se jak daného Incidentu, tak jednotlivých informací vznikající v rámci řešení. Těmito opatřeními jsou technická omezení viditelnosti těchto informací v rámci nástroje (konkrétní role bezpečnostním oddělení vidí vše, ostatní např. pouze parametry SLA a řešitel).

Další průnikovou problematikou je změna a její obsluha. Kupříkladu bezpečnost konzumuje institut standardní a emergency změny. Standardní též tzv. předschválená změna podstatně zkracuje řešení bezpečnostních Incidentů, resp. jejich remediaci přesně v dikci Incidentu, tedy řešení s nejvyšší prioritou vedoucí k rychlému odstranění, nebo eliminaci možného negativního dopadu Incidentu (porušení integrity, dostupnosti, důvěrnosti). Je třeba uvést, že bezpečnostním Incidentem se rozumí jakákoliv událost, která vede nebo může vést k narušení důvěrnosti, dostupnosti nebo integrity informací v rámci OVS a jeho rezortu. Bezpečnostním incidentem je jakékoli porušení obecných povinností uvedených v bezpečnostních směrnicích daného OVS, pro které nebyla udělena výjimka. Události, které mohou být bezpečnostním incidentem a které ovlivňují bezpečnost informací, mohou nastat v souvislosti s personální, administrativní, technickou i fyzickou bezpečností.

Pro zajištění vyšší operability a akceschopnosti je nasazován v OVS technologie bezpečnostního monitoringu tzv. SIEM. OVS by měly disponovat nejenom systémem pro ukládání a normalizaci bezpečnostních logů, ale i pokročilou funkcionalitou tedy korelací logů. Tento systém má disponovat nejenom událostmi ze síťových prvků a sítě, ale hlavně událostmi z aplikací a služeb.

V rámci práce s monitoringem se nabízí vystavění obdoby servisních stromů (pojem ITSM) v rámci bezpečnostního monitoringu. Reálně se pak takové stromy staví obdobně (konfigurační databáze = databáze aktiv (nebo CMDB s bezpečnostními informacemi) nad bezpečnostními informacemi. Oba monitoring systémy (operační a bezpečnostní) pak mohou vzájemně eskalovat svoje kritické události (provozní = faultové, bezpečnostní kritické bezpečnostní události). Poslední oblastí bezpečnostního monitoringu ve vztahu k provozu IT je přístup privilegovaných uživatelů na aktiva resp. technické nody (zařízení) v prostředí dané organizace. Tento přístup je kritický a jeho monitoring musí být oblast jedinečná a uzavřená pro bezpečnostní oddělení OVS. Přístupy privilegovaných uživatelů musí být eskalovány do bezpečnostního monitoringu OVS a pravidelně reportovány, nesmí existovat nezdůvodněný privilegovaný přístup na síťové zařízení.

Zařazení bezpečnosti OVS do útvaru ICT není škodlivé v případě, že jsou kritická a riziková aktiva plně pod auditním a metodickým dohledem představeného útvaru KB. Výhodou společného organizačního zařazení jsou:

- Společně řízení změn a projektů ev. činností snižující rizika na bezpečnostních aktivech.
- Společný rozpočet.

- Sdílení analytických zdrojů.
- Sdílení projektových a koordinačních zdrojů.
- Další věcná a odborná doplnění budou obsažena v následujících vydáních po projednání s odbornou veřejností.

Správa a řízení IT aktiv

Správa celkového portfolia služeb

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Správa aplikačního portfolia

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Správa technologického portfolia

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Správa datových fondů OVS

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Odlišný přístup k pořizování a správě ICT komodit

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Přístup k nepřímému řízení a dohledu na informatizaci (governance)

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Zavedení řízení kvality služeb

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Reporting pro management a governance ICT

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

ICT Controlling a benchmarking

Pro hodnocení projektových záměrů, pro porovnání různých variant řešení ICT projektů mezi sebou, pro sledování a řízení nákladů služeb aktuálně provozovaných ICT řešení a pro další manažerské účely ve veřejné správě ČR je vytvořena metodika výpočtu *celkových nákladů vlastnictví (TCO)*, resp. u externě provozovaných ICT služeb metodika de facto *celkových nákladů užití* ICT služby.

Absolutní výše nákladů vlastnictví (TCO) i odvozené vztažené (relativní) ukazatele patří mezi tzv. klíčové ukazatele výkonnosti (Key Performance Indicators, KPI), nebo tvoří součást výpočtu (hodnotového stromu, Value Tree) některých souhrnných KPI.

Ukazatele TCO jsou aktuálně v rámci VS ČR pro podporu řízení ICT již uplatňovány nebo alespoň k užití doporučeny v následujících oblastech řízení:

1. Analýza a porovnání nákladů na stávající informační systémy napříč centrální státní správou, tj. **benchmarking** mezi kapitolami a ústředními správními úřady.
2. Zjišťování **efektivity investice** více variant řešení u nově plánovaných ICT projektů.
3. **Ekonomická náročnost** v Žádosti o stanovisko OHA k ICT projektu.
4. Porovnání nákladů stávajícího řešení ICT služby s náklady řešení ICT služby prostřednictvím **eGovernment cloudu**.
5. Rozvoj **controllingu** ICT služeb veřejné správy.

Další informace o controllingu a benchmarkingu ICT budou po projednání s odbornou veřejností a publikovány v následujících vydáních MŘICT a ve Znalostní bázi.

Standardizace v řízení ICT

Rozsáhlá a náročná kapitola o standardizaci v ICT bude doplněna po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Spolupráce s ostatními útvary úřadu a eGovernmentu

neboli **Vazby na navazující manažerské disciplíny a regulace.**

Všechny útvary OVS (včetně ICT samotného) jsou stávajícími nebo potenciálními klienty dodávky služeb ICT útvaru. Spolupráce s nimi, jako s klienty, je nejdůležitější formou vzájemných vztahů, ta je ale popsána průběžně ve všech ostatních kapitolách dokumentu, nikoli v této.

Tato kapitola se zabývá ostatními klíčovými vzájemnými vztahy útvaru ICT s odbornými a provozními útvary, ve kterých:

1. IT proces se dá úspěšně vykonat jenom ve spolupráci s těmito útvary (ekonomika, bezpečnost a ochrana soukromí, správa majetku, právní, personalistika apod.), nebo

2. odborníci ICT mají (nebo mají mít) důležitý podíl na výkonu procesů těchto útvarů (legislativa, strategie, transformace - digitální zmocněnec, bezpečnost apod.).

Všude tam, kde kterákoli dovednost řízení ICT má překryv s jinými disciplínami řízení úřadu, je nutné se vůči těmto disciplínám vymezit a stanovit jejich styčné plochy a kontaktní body s řízením ICT.

Stejně tak všude, kde je třeba průřezově přes celý úřad nebo korporaci zareagovat na nějakou novou regulaci nebo novou potřebu, sehraje informatika významnou roli, byť manažerská oblast nebo iniciativa nejsou primárně informatické.

Některé oblasti řízení a spolupráce již jsou takto upraveny v samostatných kapitolách (projektové řízení, řízení ekonomiky ICT, řízení kvality ICT, řízení personálních zdrojů ICT apod.). Jiné jsou uvedeny zde, a to stručným obecným obsahem, případně odkazem na samostatné materiály, shrnutím těchto materiálů nebo plným obsahem.

Primárně toto ve vztahu k ICT platí pro disciplíny:

- spolupráce na péči o klienty úřadu
- spolupráce na tvorbě strategií a legislativy
- spolupráce s digitálním zmocněncem OVS
- řízení ICT bezpečnosti, kde jde o spolupráci a kompetenční rozhraní zejména s:
    - Manažerem kybernetické bezpečnosti (dle ZoKB) a
    - Pověřencem pro ochranu osobních údajů (dle GDPR),
- správa byznys architektury, modelování a řízení interních procesů úřadu, tzn. aktivní spolupráce s útvarem úřadu, do jehož kompetence patří nejen řízení interních procesů úřadu, ale i např. sdílení dat,
- plánování a financování rozvoje ICT (nejen technologií = infrastruktury, ale i personálního zabezpečení a informačních procesů), tzn. spolupráce s:
    - finančním oddělením,
    - oddělením správy majetku a
    - personálním útvarem,
- realizaci veřejných zakázek, a to jak při pořizování technologií do majetku, tak při nákupu externích služeb[74)]. To kromě administrativních úkonů vyžaduje i dobrou znalost práva - zejména licenčního.

Do této kapitoly je zařazena i spolupráce útvaru ICT s odpovídajícími útvary a orgány veřejnoprávní korporace, pokud je její součástí, a s centrálními koordinačními orgány, tj. s Ministerstvem vnitra a Zmocněncem vlády pro IT a digitalizaci.

Podpora útvarů péče o klienty služeb úřadu

Informatika bude poskytovat stále rostoucí podporu procesům výkonu služeb veřejné správy pro její klienty, zejména v podobě rostoucího podílu digitálních služeb. Již nyní jsou to právě útvary ICT, které klientům digitálních služeb poskytují podporu.

V rámci digitální transformace úřadů by v nich ale měly vznikat nové útvary, které převezmou zodpovědnost za společnou problematiku obsluhy klientů a péče o ně, napříč agendami OVS a napříč obslužnými kanály, s rostoucím podílem univerzálních obslužných kanálů (CzechPOINT a PVS - Portál občana, případně celostátní call-centrum). Takové útvary se procesně nazývají anglickými výrazy Front-End nebo Front-Office.

Součástí jejich zodpovědnosti je jednotně definovat, evidovat, publikovat a propagovat služby úřadu, zejména ty digitální. Dále koordinovat dodávku těchto služeb odbornými útvary a jednotně zadávat a přejímat služby ICT podpory obsluhy klientů a vyhodnocovat jejich kvalitu.

Úkolem útvaru ICT je navázat spolupráci se vznikajícím útvarem Služeb (a péče) pro klienty a nalézt první hmatatelné společné body v jejich vztahu jako věcný a technický správce Front-Office řešení pro dodávku služeb úřadu. Jedněmi z prvních praktických společných úloh jsou:

- správa katalogu služeb ve všech kanálech obsluhy
- správa znalostí a poskytování podpory ve všech kanálech obsluhy apod.

Integrovaný externí ServiceDesk pro digitální služby

Příkladem praktické spolupráce s útvarem péče o klienty je společný, sdílený ServiceDesk pro digitální i tradiční obslužné kanály. Podstata spolupráce spočívá v tom, že klienti služeb úřadu, ve všech obslužných kanálech, obvykle potřebují podporu zejména ve dvou oblastech:

- obsahové - kde a jak hledat správné služby pro životní situace, co a jak vyplňovat do podání, jaké a jak dokládat přílohy apod.
- ICT - jak správně aplikace samoobslužných kanálů instalovat a užívat, jak se vyrovnat s chybami či neznalostmi.

Nejlepší praxe ukazuje, že úřad má mít přinejmenším pro své samoobslužné klienty jednotný ServiceDesk, zajišťující jak znalostní bází, tak personálním obsazením podporu v obou výše uvedených okruzích problémů. To vyžaduje společné koordinované řízení z obou útvarů.

Specifické je, že útvar ICT zde vystupuje jak v roli technického správce sdíleného řešení, tak jako dodavatel znalostí a kapacit podpory uživatelů v technických aspektech služeb.

Přístup k legislativní podpoře informatizace VS

Další rozvoj informatizace VS ČR vyžaduje zejména tvorbu nových právních předpisů a změny předpisů stávajících tak, aby předpokládaly, umožňovaly a vynucovaly naplnění architektonických principů eGovernmentu, uvedených v IKČR, tj. byly tzv. digitálně přívětivé.

Vzhledem k tomu, že valná většina legislativních změn zahrnuje nebo vyvolává i změny IT podpory výkonu veřejné správy, měli by být IT analytici a architekti úřadů přizváni do procesu tvorby úprav agendové legislativy již na úrovni přípravy legislativního záměru. Změny legislativy musí ve svém znění i v doprovodných dokumentech zohledňovat logiku, algoritmizovatelnost a parametrizovatelnost zákonných regulací a proveditelnost jejich IT podpory, a to zejména formulováním přesného byznys zadání odpovídající IT podpory a dostatečné nebo postupně časované doby pro její realizaci - implementační lhůty.

Jedním z nezastupitelných úkolů architektury úřadu (veřejné správy) je být podkladem pro optimalizaci veřejné správy a pro optimalizaci legislativy. Architekti a analytici musejí být zapojeni do procesu přípravy tezí i konkrétní legislativy, a naopak do procesu realizace nové legislativy v úřadu. Více souvislostí k zapojení do tvorby legislativy ve fázi 2-Palánování a příprava etapy životního cyklu jednoho ISVS také v Řízení jednolitých ICT řešení.

Podstatné pro další rozvoj informatizace VS ČR bude také odblokování překážek vystavěných dosavadní legislativou v oblasti eGovernmentu, nákupu ICT a ve správě ICT zdrojů, zejména lidských, viz také vztah řízení lidských zdrojů a Státní služba.

Důležité pro implementaci IKČR je, aby všechny nové nebo významněji měněné právní předpisy byly adaptovány tak, že budou reálně naplňovat principy IKČR podle měřítek a kontrolních otázek Digitálně přívětivé legislativy[75)].

Digitálně přívětivá legislativa

IKČR se svými architektonickými principy a z nich plynoucími pravidly již je harmonicky sladěna se Zásadami pro tvorbu Digitálně přívětivé legislativy.

Z toho plyne, že důsledné uplatnění těchto Zásad při tvorbě legislativy, včetně její kontroly ověřovacími otázkami k naplnění zásad, podstatně napomůže k implementaci IKČR do praxe VS ČR.

Proto IKČR a MŘICT vede útvary informatiky, tj. Technické správce ISVS těch úřadů, které zodpovídají jak za přípravu nebo připomínkování legislativy, tak za následnou implementaci její ICT podpory, k tomu, aby:

- se účastnili přípravy věcného záměru zákona nebo jeho změny
- prosazovali architektonické a systémové myšlení jako logický základ proveditelných předpisů
- požadovali jako součást zadání pro budování IT podpory změny legislativy od svého příslušného Věcného správce již od prvotních záměrů odpovědi na kontrolní otázky dle DPL.

Jedním z konkrétních cílů (DC 4.2) IKČR je zavést nutnost naplnění DPL jako novou povinnost a nedílnou součást legislativního procesu.

IT bezpečnost a ochrana údajů v kontextu úřadu

Informatika jako systémová a celostní disciplína v úřadu je přirozeným partnerem podobných a příbuzných disciplín, jako je bezpečnost úřadu, ochrana údajů, dodržování pravidel, řízení kvality, výkonnosti a zodpovědnosti.

Je například v praxi ověřeno, že téměř všechny prvky architektury úřadu, jsou současně předmětem ochrany, ale současně také prostředkem ochrany a často i rizikovým faktorem (informace, technologie, zaměstnanci, budovy, činnosti apod.). To platí významnou měrou pro prvky architektury úřadu, které jsou ve správě útvaru ICT, tedy primární a podpůrná aktiva.

Proto informatika a pro její strategické plánování a řízení v MŘICT vyžadovaná metoda architektury úřadu mohou být výše uvedeným disciplínám v úřadu velmi užitečné. Architektura úřadu totiž postupně objevuje, pojmenovává a popisuje všechny podstatné součásti struktury a chování úřadu a tato znalost je klíčových východiskem práce ostatních disciplín. A obráceně, práce specializovaných disciplín ověřuje a doplňuje poznání architektury úřadu a je proto přinejmenším velmi užitečnou zpětnou vazbou.

Útvar ICT je povinen navázat s útvary zodpovědnými za výše uvedené disciplíny vzájemně výhodnou otevřenou spolupráci. Některé příklady spolupráce jsou uvedeny v následujících kapitolách, další věcná a odborná doplnění budou po projednání s odbornou veřejností obsažena v následujících vydáních MŘICT a ve Znalostní bázi.

Podíl IT na celkové bezpečnosti úřadu

Řízení kybernetických rizik a bezpečnosti jednotlivých IS a celé informatiky úřadu musí být vykonáváno v souladu s celkovým řízením rizik a bezpečnosti úřadu tak, aby identifikovaná rizika a přijímaná opatření byla součástí jednotných a celkových procesů a registrů rizik na úrovni celého úřadu a dle své závažnosti se i IT / kybernetická rizika stala součástí rozhodování a řízení celého úřadu.

Přijetím zákona o kybernetické bezpečnosti se vytvořilo ideální prostředí pro rozvoj procesů v ICT. Právě procesy řešené přes ICT deklarují měřitelnou úsporu, bezespornost, nezvratnost a mnoho dalších přirozených vlastností ze světa ICT.

Bohužel tyto procesy nejsou řešeny komplexně a každý úřad má procesy s kvalitní auditní stopou a procesy, které jsou beze stopy. Důraz na odpovědnost za jednotlivé oblasti působnosti v rámci stanovených rolí podle zákona má za následek kvalitní postupný rozvoj. Tento rozvoj však obvykle nemá svou finanční ani organizační změnu. Každý útvar ICT respektuje nová pravidla, ale zároveň se snaží postupně jednotlivé milníky oddálit, protože čeká na finanční úspory nebo personální navýšení pro realizaci změn. To má napravit i naplňování pravidel MŘICT, kde jsou již všechny tyto souvislosti vzaty v úvahu.

Podíl IT na ochraně údajů a GDPR

V oblasti řízení ochrany soukromí a osobních údajů musí všechny vrstvy architektury úřadu a IT dovednosti být uvedeny do souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 z 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, také jako „GDPR“) a stávajícím zákonem č. 110/2019 Sb., o zpracování osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, stanovujícími rozsah ochrany osobních údajů, který je nutné zohlednit při tvorbě informačních systémů a při návrhu systémů pro práci s dokumenty.

Přestože primární zodpovědnost za naplnění povinností z těchto předpisů leží na vedení úřadu, pověřenci (DPO) a věcných správcích, hraje útvar ICT významnou roli v analýze stavu a potřeb ochrany osobních údajů, v implementaci IT opatření, zajištění vstupních a výstupních bodů a v respektování jednotlivých rolí dle GDPR a jejich smluvních vztahů.

Z nařízení GDPR vyplývá, že zpracování osobních údajů musí být v rozsahu nezbytně nutném a přiměřeném pro zajištění bezpečnosti sítě a informací, to jest schopnosti sítě nebo informačního systému odolávat na dané úrovni spolehlivosti, náhodným událostem nebo protiprávnímu či zlovolnému jednání ohrožujícímu dostupnost, pravost, správnost a důvěrnost uložených či předávaných osobních údajů a bezpečnost souvisejících služeb poskytovaných či přístupných prostřednictvím těchto sítí a systémů. Vlastní zodpovědností ICT je tedy plnění těchto daných požadavků.

Obdobně jako ve vztahu mezi zodpovědnostmi za dlouhodobé řízení ICT a zodpovědnostmi za kybernetickou bezpečnost i ve vztahu k GDPR a ochraně osobních údajů je nutné na sebe vzájemně mapovat klíčové role a sladit jejich povinnosti na jedné straně a klíčové potřebné schopnosti a dovednosti na druhé straně. Jde zejména o tyto role:

- správce, společní správci,
- zpracovatel,
- **pověřenec,**
- příjemce,
- třetí strana apod.

Těmto rolím musí IT poskytnout nebo od dodavatelů zprostředkovat nezbytné IT znalosti, současně prostřednictvím IT útvarem uzavíraných smluv přenést na své dodavatele odpovídající část povinností, spojených se zpřísněnou ochranou osobních údajů.

Úlohou IT útvaru jako technického správce je implementovat do všech dotčených informačních systémů opatření zajišťující tzv. mandatorní požadavky výše uvedených předpisů. Za formulaci konkrétních přesných požadavků/zadání implementace pro jednotlivé IS odpovídají jejich věcní správci ve spolupráci s odbornými rolemi GDPR.

Informační systémy, v rámci kterých uživatelé nakládají s osobními údaji fyzických osob, musí zajišťovat důslednou ochranu těchto dat před zneužitím. Za minimální bezpečnostní opatření lze považovat důsledné oddělení uživatelských účtů v systému, správu hesel, logování přístupů, možnost reagovat na personální změny v řadách uživatelů, nastavení přístupových práv apod. Opatření musí zahrnovat:

- Logování k přístupu k osobním údajům
- Šifrování osobních údajů
- Pseudonymizace osobních údajů
- Anonymizace osobních údajů
- Funkce pro realizaci práv subjektů práva
- Vyhledávání osobních údajů ve struktuře databází a hypertextem.

Požadavky vedoucí na tato opatření, převzatá primárně z evropské legislativy[76)], vyvolávají potřebu „nastartování“ nové etapy vývoje dotčených IS s fázemi 1, 2 a 3. Obdobně je tomu automaticky při výstavbě

nového řešení, kde musí být tyto mandatorní požadavky zohledněny a příslušná opatření zahrnuta do rozsahu, návrhu a plánu řešení, viz také architektonický princip P7 Důvěryhodnost a bezpečnost a v něm zahrnuté zásady „Privacy by Default“ a „Privacy by Design“.

Role útvaru ICT je klíčovou ve všech fázích životního cyklu přípravy, výstavby, modifikaci a provozu nových či stávajících řešení. Osobní údaje jsou tak bezpečné, jak bezpečné je prostředí, ve kterých se osobní údaje zpracovávají. Proto je nezbytné z pohledu IT dostatečně zabezpečit následující oblasti, které mají primární vliv na prostředí, ve kterém se zpracovávají osobní údaje:

- Technické zabezpečení:
  - ICT technologie, kde dochází ke zpracování osobních údajů (Samotné řešení ve kterém dochází ke zpracování osobních údajů, včetně všech možnosti kde dochází vstupně výstupním operacím)
  - Podpůrné, globální či sdílené ICT, které jsou využívány pro zabezpečení provozu samotného řešení (Backend, Frontend)
  - Prostředky a techniky, kterými jsou osobní údaje přenášeny mimo primární ICT či mimo ICT zcela
  - Datové nosiče pro ukládání dat
- Smluvní zabezpečení
  - Smluvní vztahy se všemi poskytovateli produktů a služeb, kteří se dostávají do kontaktu s daným prostředím uvedeným v části Technické zabezpečení
- Procesy:
  - Vývoj
  - Změnová řízení
  - Provoz

Ideální způsob zabezpečení z pohledu GDPR je kombinace technicko-organizačních a smluvních opatření. Je nezbytné si uvědomit, že jeden druh ochrany není dostatečný.

Spolupráce s ostatními provozními útvary

Ačkoli je útvar informatiky svými schopnostmi a přínosy pro úřad v mnohém výjimečný, svou podstatou je to provozní servisní útvar, obdobný a příbuzný všem ostatním (personalistice, správě nemovitostí, ekonomice, správě znalostí, nákupu, případně dalším).

Při přechodu na řízení úřadu pomocí služeb je na útvaru ICT, aby porozuměl tomu, jaké služby těmto útvarům poskytuje a jaké od nich odebírá. Je důležité vyjasnit hranice spolupráce, na níž k této výměně vzájemných služeb dochází. Manažer a pracovníci útvaru informatiky si mají být dobře vědomi, jaké služby jsou oprávněni v těchto provozních oblastech od „sesterských“ útvarů žádat.

Současně by si všechny provozní útvary měly uvědomit, že jejich společnými a jedinými klienty jsou všichni zaměstnanci úřadu. Proto by tyto útvary měly napřít síly, analyzovat, co již mají společného a jak se mohou dále sblížit a sjednotit, aby své služby zaměstnancům poskytovaly jednotným, přívětivým a efektivním způsobem, včetně zaměstnaneckých samoobsluh, viz Spolupráce s ostatními útvary úřadu a eGovernmentu o zapojení provozních útvarů do společného centra sdílených služeb pro zaměstnance.

Praktické příklady nejlepší praxe, návody, vzory a další akcelerátory pro oblasti spolupráce ICT s provozními útvary, zmíněné v následujících kapitolách, budou doplněny po projednání s odbornou veřejností a publikovány v následujících vydáních MŘICT a ve Znalostní bázi.

Spolupráce s ekonomickými útvary

Podstatou spolupráce CIO s útvary ekonomiky je, že manažer informatiky je sice zodpovědný za plánování rozpočtu, za platby smluvních závazků, za nákladový controlling projektů a jednotlivých řešení a za další ekonomické operace, ale není a ani nemá být expertem v této oblasti.

Část těchto úloh, zejména ve větších ICT útvarech, zajistí svým ekonomicky vzdělaným personálem v rolích ekonoma/-ky, kontroléra/-ky apod., přesto je oprávněn žádat adekvátní podporu službami ekonomických profesionálů z příslušných útvarů.

Příkladem obtíží ve spolupráci je proces financování rozvojových záměrů. Základním problémem tohoto procesu je čas, který proběhne mezi věcným záměrem a podpisem smlouvy. U nového zákona nebo jeho obsáhlé novely se jedná se o roky práce, které nemají dopad do rozpočtu, ale často se právě tyto finance v rozpočtu objeví. Naopak někdy RIA nemá finanční zatížení, protože se změna děje na jiném úřadě. Principem dobrého nastavení je disponibilita finančních prostředků, které jsou nutné pro řízení změn. ICT útvar by neměl řešit po kolaudaci svého ICT disponibilitu finančních prostředků na jeho provoz. Ekonomický útvar musí mít správné podklady od ICT útvaru, aby mohl disponibilitu řešit na úrovni celého rozpočtu, a útvar ICT musí pravidelně informovat o příslušných změnách.

Spolupráce s personálními útvary

Podstatou spolupráce CIO s personálními útvary je jeho potřeba získávat, udržovat a intenzivně vzdělávat svůj odborný personál.

Personální práce je přirozenou součástí práce každého manažera, ale ani ICT manažer na ni nemá být takovým odborníkem. Má plné právo žádat od personálních útvarů podporu při náboru nových zaměstnanců, přípravě zaměstnaneckých benefitů a pobídek, přípravě a realizaci vzdělávacích programů, při hodnocení zaměstnanců a plánování jejich dalšího růstu apod. Oprávněně očekává, že se mu dostane zejména služeb personálního a personálně-právního poradenství vzhledem ke služebnímu zákonu, zákoníku práce a dalším předpisům.

Spolupráce na veřejných zakázkách

Podstatou spolupráce CIO s útvarem právním a útvarem veřejných zakázek jsou jeho oprávněné potřeby bezpečně, tj. legálně zvládnout proces výběru dodavatele pod ZoZVZ bez rezignace na věcnou, odbornou podstatu zakázky.

Každá veřejná zakázka má nejméně dva hlavní aspekty. Prvním je potřeba toho, kdo nakupuje - musí tzv. „vědět, co chce“. Je úkolem útvaru ICT jako technického správce, obstarávajícího řešení pro věcného správce, aby do zakázky dodal správné a srozumitelné zadání, tj. architekturu řešení, jeho funkční a ne-funkční specifikaci, včetně SLA, část smluvních požadavků a další atributy spojené s jeho obvyklou rolí příkazce operace.

Oprávněně očekává službu od odborníků na právo a nákup, že do zakázky vloží bezchybnou procesní znalost a druhou část smluvních podmínek, které pro CIO následně zajistí smluvní vztah s dodavatelem, představující vyvážené partnerství[77)].

Běžným příkladem obtíží je nedostatek vzájemných znalostí a stále se měnící prostředí. Stejně jako garant aktiva potřebuje praxi pro svou roli, tak i odpovědné osoby za zakázky potřebují praxi a především dodržování protikorupčních pravidel. Únik informací před vypsáním veřejné zakázky lze významně omezit předběžnými tržními konzultacemi a samotný průběh zakázky lze často vyřešit jednacím řízením s uveřejněním, které umožňuje přístup všech dodavatelů a minimalizuje množství dodatečných informací.

Dalším obrovským dopadem výkladu ZoZVZ z let minulých jsou služby provozu na 4 roky, kde již minulý rok mnoho právních kanceláří vyzvalo ICT útvary k delším časům. Pokud zadavatel zachová vlastnictví zdrojových kódů u sebe a soutěží rozvoj, potom nic nebrání dlouhodobé údržbě. Možnost definovat delší časy v rámci veřejných zakázek tak, aby to odráželo standardní praxi, kdy například běžné doby na údržbu SW/HW (Maintenance) bývá nabízena na 3, 5, popřípadě 10 let by měla být diskutována při dalších revizích zákona.

Spolupráce se správou nemovitostí

Podstata spolupráce se správou a údržbou nemovitostí je dvojí:

1. Potřeba útvaru ICT využívat specifické prostory a s nimi spojené služby
2. Významná podobnost procesů poskytování služeb pro zaměstnance při péči o koncová ICT zařízení a při péči o ostatní pracovní vybavení, navíc často s potřebou časové synchronizace služeb, obojí mnohdy napojeno na personální služby (nástup, stěhování, odchod zaměstnance).

První bod spolupráce by měl vést k poskytování služeb správy nemovitostí s SLA obdobnými, jako jsou SLA, spojené s dodávkou služeb klientům útvaru ICT.

Druhý bod spolupráce by měl vést na společnou koordinaci poskytovaných služeb, sdílné metod, postupů, nástrojů i dispečerského personálu pro obě kategorie služeb, s možností rozšíření až do podoby centra sdílených provozních služeb, viz dále.

Společné zapojení v centru sdílených služeb pro zaměstnance

Společnými klienty provozních útvarů jsou zaměstnanci a manažeři úřadu, kteří všichni mají právě z těchto svých univerzálních rolí potřebu čerpat sady provozních služeb pro zaměstnance a někteří k tomu ještě sadu služeb pro manažery.

Jejich společnou potřebou je čerpat tyto služby snadno, jednotně, obslužným kanálem podle své volby, tj. osobně, v portálu úředníka nebo v call-centru dispečinku služeb.

Útvar ICT bude v takovém centru sdílených služeb hrát významnou roli, proto by měl ověřit takovou potřebu ve svém úřadu a potom napomoci procesní a digitální transformaci úřadu v provozní oblasti iniciováním a vybudováním takového centra sdílených služeb.

Dlouhodobým trendem je pro veřejnou správu ČR federativní uspořádání takových center s možností kombinace lokálních služeb se službami sdílenými na korporátní (resortní, krajské nebo obecní) úrovni a sdílenými provozními službami na celostátní úrovni (například eLearnig).

Centrální koordinace řízení ICT státu

Protože centralizace řízení VS ČR je stanovena zákonem[78)], musí být i eGovernment, který je vlastně VS vykonávanou v digitálním (kybernetickém) prostředí, řízen centrálně. To pro ICT útvary úřadů znamená povinnost se nejen při provozu, ale již i při projektování rozvoje jimi pro výkon služeb VS zajišťovaných podpůrných ICT služeb (jak interní, tak externí) řídit a dodržovat centrálně vydávané dokumenty pro oblast ICT VS.

Že nutnost vybudování centrálních kompetencí vnímá i vláda ČR, dokládá i hlavní cíl č. 5 programu DČ, pilíře IKČR – Efektivní a centrálně koordinované ICT veřejné správy, konkrétně dílčí cíl č. 5.2 - Alokace adekvátních lidských a finančních zdrojů pro realizaci IK ČR.

V následujících kapitolách bude po projednání s odbornou veřejností v dalších vydáních MŘICT uvedena sada praktických doporučení pro manažery útvarů ICT, jak realizovat úspěšně spolupráci s centrálními koordinačními orgány.

Podrobnější informace, návody a další pomůcky budou průběžně aktualizovány ve Znalostní bázi.

Ekonomická koordinace

V situaci obtížné až faktické nevymahatelnosti i zákonných povinností, je jediným účinným nástrojem řízení centrální kontrola čerpání státního rozpočtu, a to již od fáze tvorby finančních plánů a odsouhlasování položek na kapitolu ICT jednak dle potřebnosti pro zajištění provozu a jednak dle souladu s IKČR a přínosů jednotlivých akcí / projektů pro naplňování státem prioritizovaných strategických cílů.

Programové financování

Více informací a potřebné akcelerátory k centrální koordinaci programového financování ICT bude po projednání s odbornou veřejností publikováno v následujících vydáních MŘICT, podrobnější informace, návody a další pomůcky bude obsahovat Znalostní báze.

Metodika logického rámce

Logický rámec (LR, LogFrame, logická rámcová matice – LRM) slouží jako pomůcka při stanovování základních parametrů projektu. Je součástí metodiky návrhu a řízení projektu označované jako „Logical Framwork Approach (LFA)“, která uceleně řeší přípravu, návrh, realizaci i vyhodnocení projektu.

Metodika logického rámce[79)], zpracovaná MPSV pro čerpání z Evropského sociálního fondu v rámci Operačního programu zaměstnanost, je osvědčeným nástrojem pro přípravu žádosti o registraci akce a získání příspěvku z EU a na základě zkušeností pozitivních zkušeností MPSV bude vhodné ji využívat pro všechny projekty v rámci eGovernmentu ve fázích 1 a 2 jejich životního cyklu.

V rámci logického rámce se identifikují cíle, přínosy a výstupy příslušného projektu, ale i vazby mezi nimi. Zároveň logický rámec obsahuje i objektivně ověřitelné ukazatele a zdroje k jejich ověření, která umožní stanovit míru dosažení cílů a přínosů projektu.

Více informací a potřebné akcelerátory k LRM bude obsahovat Znalostní báze.

Investiční záměr, CBA a Studie proveditelnosti

Klíčovým dokumentem pro čerpání státního rozpočtu je dle platných postupů Investiční záměr. Ten na základě schváleného rozpočtu a v kapitolním sešitě úřadu přidělených finančních prostředků, zpracovává a k registraci na Ministerstvu financí předkládá úřad.

Součástí požadavků na financování ICT projektů VS by vždy mělo být prokázání, že zvolena byla varianta:

- proveditelná,
- s nejlepším poměrem přínosů a nákladů, a to z pohledů:

- kybernetické bezpečnosti,
- uživatelské přívětivosti – jak pro občanskou veřejnost a komerční subjekty, tak pro úředníky VS,
- využitelnosti jak stávající ICT infrastruktury, tak znalostí a schopností interních pracovníků,
- dlouhodobé udržitelnosti.

Více informací a potřebné akcelerátory k Investičním záměrům, CBA a Studiím proveditelnosti bude obsahovat Znalostní báze.

Koordinace realizace změn a dosahování přínosů

Implementace změn probíhá formou projektů případně programů, pro jejichž řízení existuje celá řada vhodných metodik. Z hlediska projektů eGovernmentu se jeví jako zásadní jejich vzájemná koordinace, návaznost na strategii eGovernmentu a v neposlední řadě měření úspěchu implementace příslušné změny (projektu/programu).

Pro tento účel je nejvhodnější metodika logického rámce popsaná výše, která jednak definuje cíle a přínosy implementovaných změn a zejména stanovení míry jejich dosažení. Logický rámec projektů by se měl stát povinnou součástí Centrálního katalogu záměrů a projektů zmíněného v následující kapitole a měl by se stát i součástí závěrečného hodnocení projektu nebo programu. Kromě míry dosažení cílů a přínosu projektu by součástí závěrečného hodnocení měla být i analýza pozitivních zkušeností, a zejména, pokud projekt nedosáhl stanovených cílů, analýza příčin neúspěchu.

Poznatky ze závěrečné analýzy by měly být k dispozici ostatním OVS, které je využijí pro optimalizaci svých projektů, ale zejména centrální kanceláři pro řízení projektů, programů a portfolia (P3O), která bude tyto poznatky využívat k dalšímu zkvalitnění procesů přípravy a řízení projektů, programů a portfolia.

Centrální řízení bude vhodné implementovat právě i v rámci řízení programů a portfolia, přičemž je zřejmé, že zejména v oblasti řízení programů a portfolia je nutná spolupráce různých subjektů VS, a to jak jejich IT organizací, tak i odborných složek. Pro koordinaci a řízení programů a portfolia projektů bude nutné implementovat centrální kancelář pro řízení projektů, programů a portfolia využívající metodiku P3O (Project, Programme, Portfolio Office vycházející z metodik PRINCE 2, MSP a MoP), pravděpodobně jako součást MVČR. Tato kancelář musí disponovat odborníky s příslušnými certifikáty, vybavenými dostatečnými pravomocemi pro jednání s různými subjekty VS a jejich organizačními jednotkami na všech úrovních řízení.

Centrální katalog záměrů a projektů

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Řízení licencí a OSS/FS

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Postup a plán realizace změn

Základním cílem je dosáhnout řízeného ICT, tedy měřitelné schopnosti reakce na příchozí změny. Takový stav může nastartovat teprve v okamžiku, kdy víme, kde jsme. Tím však nemáme na mysli pouze ICT útvar, ale dodržení této metodiky pro zjištění současného stavu celého úřadu.

Tato kapitola obsahuje dva pohledy na věcný a časový akční plán (Roadmap), a to:

- přehled souvisejících nezbytných aktivit a změn na úrovni státu a eGovernmentu
- přehled prvních kroků adaptace útvaru ICT úřadu na pravidla MŘICT

Podrobnější a aktualizované informace v obou oblastech budou doplněny po projednání s odbornou veřejností a publikovány v následujících vydáních MŘICT a ve Znalostní bázi.

Prioritizace změnových opatření státu a OVS

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT.

Doporučený postup realizace žádoucího stavu v OVS

Teprve po stabilizaci úřadu do stavu známých provozních změn je možné se začít věnovat změnám v samotných informačních systémech.

Vzhledem k tomu, že aktuálně je ICT VS ČR v tzv. transformačním období, a tedy ještě řada prostředků a nástrojů není vytvořena, a protože stav ICT na jednotlivých úřadech je velice různorodý, nelze pro dosažení žádoucího stavu stanovit dostatečně podrobný postup, který by platil univerzálně.

Aby byl dostatečně obecný, lze doporučit pouze následující, podle závažnosti dopadů seřazený, seznam:

1. provést rámcovou katalogizaci:
    - kompetencí ICT útvaru vůči jeho okolí, tzn. jak ostatním útvarům úřadu, tak vůči externím subjektům,
    - skutečného souladu a platnými / aktuálními povinnostmi danými:
        - zákonnými povinnostmi (včetně IKČR),
        - interními akty řízení úřadu,
        - úkoly uloženými vedením úřadu,
    - vyřízení požadavků obdržených:
        - od provozního útvaru ICT – zejména jde o požadavky založené na reportech HelpDesku a požadavcích plynoucích z provozuschopnosti technologií,
        - od klientů, tzn. ostatních útvarů úřadu, kterým ICT útvar poskytuje podporu pro jejich činnost,
        - od interních pracovníků útvaru, tj. jak náměty na zlepšení, tak např. rekvalifikační a mzdové požadavky.
    - disponibilních zdrojů ve smyslu výhledu na nejbližší 3 roky, zejména:
        - technologických, tzn. ne jen kapacitních rezerv, ale i blížící se životnosti, úrovně odolnosti proti bezpečnostním rizikům,
        - personálním z pohledu zejm. zajištění potřebné úrovně odbornosti a časové kapacity,
        - finančních, tzn. jak výše a struktura přiděleného rozpočtu, tak i ve finančním plánu úřadu zahrnutých položek,
        - objektových – ne jen z hlediska vhodnosti stávajících prostor, ale i včetně jejich komunikačního a napěťového připojení, atp.
2. provést reálné vyhodnocení zjištěných nedostatků, opět v časovém horizontu 3 let (optimálně kvantifikovatelně prioritizované dle možných důsledků),
    - Pro případ, že některé z nedostatků budou klasifikovány jak potenciálně rizikové, pro ně zpracovat akční plán minimalizace dopadů včetně předpokládaných požadavků na zdroje a urychleně ho předložit vedení úřadu,
3. zpracovat a vedení úřadu předložit novou informační koncepci úřadu, která kromě návrhu nové (cílové) Enterprise architektury úřadu bude obsahovat i časový a věcný plán jak nové architektury (v rámci ICT transformace úřadu) dosáhnout, a to včetně změn v personální oblasti, změn procesů zadávání a vyřizování požadavků na ICT podporu a změn ve financování. Vzhledem k reálnému stavu rozpočtů OVS je doporučeno rovnou v tomto dokumentu zpracovat plán minimálně ve dvou variantách, a to tak, aby byl zřejmý jejich rozdíl, konkrétně:
    - minimalistická varianta, která bude de-facto shodná s akčním plánem minimalizace rizik,
    - optimální varianta – návrh, jak by si počínal dobrý hospodář s výhledem alespoň na 5 let.
4. na základě odezvy vedení úřadu na předloženou novou informační koncepci úřadu, zpracovat návrhy:
    - rozpočtových opatření ke změně plánu finančního rozpočtu ICT útvaru,
    - personálního rozvoje útvaru ICT, tj. zejména:

- návrh org. změny, kterou v rámci ICT vytvoří nové role, a to včetně rámcového popisu pracovní náplně těchto rolí a s ní souvisejících práv a povinností a kvalifikačních předpokladů,
- návrh personálních opatření, kterým nově vytvořené role obsadí,
- návrh zajištění minimálního obsazení rolí pro vypořádání potřeb,
- plán rekvalifikace,

Nastartování změn

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT.

Přehled a plán změn (akční plán)

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT.

Vytvoření Znalostní báze Metod řízení ICT VS ČR

Vytvoření odborného útvaru MV pro Metody a standardy řízení ICT

Zapojení odborných komunit

Vyhodnocování pilotních projektů (adaptovaných informačních koncepcí)

Aktivní publikování a řízení znalostí v bázi a další

Nutné organizační a kompetenční změny

Analýza rizik a strategie jejich zmírnění

Informační koncepce ČR a její navazující dokumenty jsou implementovány do praxe prostřednictvím uvedením jednotlivých Informačních koncepcí OVS do souladu s nimi a implementací těchto místních koncepcí.

Je potřebné dopředu dobře chápat známá rizika implementace principů tohoto dokumentu, která se nemusí uplatnit u každého úřadu stejnou měrou a připravit opatření pro jejich zmírnění. Riziky jsou zejména:

Tabulka Přehled vybraných zásadních rizik implementace IK ČR a MŘICT prostřednictvím IK OVS.

Č.	Riziko	Opatření
1.	Neprovázanost IT a odborných (zejména legislativních) útvarů	Zavedení pravidel v organizačních řádek, které zapojují IT odborníky z řad věcných správců (odborných útvarů) i technického správce (ICT útvaru) do tvorby strategií úřadu a sektoru a legislativy.
2.	Nedostatek fundovaných IT odborníků na straně VS	Využívání všech aktuálně dostupných nástrojů (jako je institut klíčového zaměstnance) pro získání a udržení těchto zaměstnanců.
3.	Špatná kvalita stávajících dat	Zavedení čištění dat jako průběžného procesu úřadu, včetně jeho institucionalizace v odpovídajících pracovních pozicích, předpisech a nástrojích.

Č.	Riziko	Opatření
4.	Meziresortní překážky spolupráce a nedostatečné nadresortní koordinační kapacity	Posílení kapacit koordinačních odborů MV a koordinace strategického rámce Digitální Česko. Zapojení rezortních odborníků a digitálních zmocněnců, využívání společných zdrojů Kompetenčních center a další
5.	Stávající smluvní a nesmluvní (znalostní, kapacitní) závislosti	Postupné odbourávání všech příčin závislosti na dodavatelích jako je vybudování interní kompetence, změna smluv u stávajících nebo nových VZ, převzetí správy dokumentace, převzetí zdrojových kódů, migrace řešení na otevřené platformy s širokou partnerskou sítí v ČR apod.
6.	Rezistence vůči změnám z těchto pravidel	Motivace vedení úřadu i zaměstnanců k osvojení si cílů digitální transformace VS ČR. Posílení a změna organizačních struktur úřadu o pozice, které mohou a dokáží být tahouny změny. (Dočasné) posílení kapacit zaměstnanců tak, aby vedle každodenní rutiny měli prostor i pro realizaci změn. Přirozená výměna zaměstnanců ve prospěch těch lépe přijímacích digitalizační změny, apod.
7.	Nedostatečné finanční zdroje	Včasná příprava ICT záměrů (a jejich potřeb zdrojů), jejich evidence v IK OVM a registru záměrů Digitálního Česka, připravenost argumentů pro vyjednávání o rozpočtu, připravenost akceptovat financování ze zdrojů EU a další.

Jaká jsou další rizika a jakými opatřeními rizika zmírnit, bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT.

Monitoring postupu

Jakým způsobem a jakými prostředky se bude monitorovat implementace koncepce, bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT.

Aktualizace koncepce a akčního plánu

Jaký bude proces vyhodnocování, aktualizace a předkládání MŘICT, bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT.

Přehledy klíčových povinností při řízení ICT

Provázanost legislativních povinností útvarů ICT

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT.

Kalendář aktivit v řízení ICT

Přehled životních cyklů všech úrovní řízení ICT:

- Jeden konkrétní informační systém - sekvence fází ve spirále na sebe navazujících etap života řešení.
  - Jedna etapa trvá několik let, při dobrém řízení se mohou i časově překrývat
  - Důležitou roli hraje délka veřejných výběrových řízení
  - Důležitými milníky jsou doba záruky a délka smlouvy na podporu, fyzická trvanlivost platformy a doby povinného upgrade, délka podpory produktu výrobcem apod.
- celý útvar informatiky - základní cyklus je dán plánováním ročního rozpočtu a pětiletého rozpočtového

výhledu
    - ovlivněno cyklem organizačních změn (systemizací, 2x ročně)
    - 5 let je i délka informační koncepce, s aktualizací každé dva roky nejméně.
- celý úřad OVS - období mezi zásadními změnami strategie, v důsledku
    - změny politického vedení (volební cyklus)
    - změny klíčového managementu,
    - podstatné legislativní změny
- eGovernment ČR a EU
    - dlouhodobé strategie (10 let)
    - dotační období 7+2 roky

Nejkratší, roční, cyklus určuje rozvržení prací na správě IT aktiv a dalších zdrojů tak, aby prokazatelně zjištěná změněná potřeba (správa portfolií, inventury, architektura a roadmapa úřadu) se mohla promítnout do vyjednávání o odpovídajícím rozpočtu.

Obdobně potřeba lidských zdrojů musí být identifikována do června tak, aby v červenci byla schválena systematizace od ledna příštího roku.

Z toho plyne, že první pololetí je zejména obdobím nezbytných koncepčních prací, kdežto druhé pololetí je zejména obdobím dokončování projektů, aby se stihly spotřebovat přidělené finanční prostředky.

Měsíční kalendář činností v ICT

Na základě výše uvedených řídících cyklů, nejvíce podle ročního a 5 letého rozpočtového cyklu bude podle nejlepší praxe a povinností z právních předpisů navržen a ve Znalostní bázi ICT udržován vzorový kalendář typických periodických ICT zodpovědností a činností, doplněný o kontextové odkazy na detailní návody a další akcelerátory.

Přehled a Rejstřík metod řízení ICT

Přehled metod pro řízení ICT VS ČR

- 3E (Economy, Efficiency, Expediency) - efektivnost, hospodárnost, účelnost
- ABC (Activity Based Costing) - procesní řízení nákladů
- Analýza rizik (Risk Management)
- Benchmarking
- BPM (Business Proces Management) – procesní řízení
- BSC (Balanced Scorecard) - systém vyvážených ukazatelů výkonnosti podniku
- Byznys analýzy a plánování
- Capability Based Planning (metodika The OpenGroup)
- CBA (Cost Benefit Analýza) – hodnocení nákladů a přínosů
- DPL – digitální přívětivá legislativa
- Finanční plánování
- Kompetenční matice (RASCI)
- Logický rámec - strukturovaná koncentrace (na jedné stránce) všeho podstatného o projektu umožňující každému rychle pochopit, proč se projekt realizuje a čeho se má dosáhnout. Slouží ke koordinaci lidí a řízení změn, v maximální míře aplikuje SMART přístup.
- Měření výkonnosti (PM - performance measurement)
- Metodiky určení TCO pro pořízení a provoz ICT služeb v rámci Government Cloudu (Příloha č. 3. Souhrnné analytické zprávy Projekt Příprava vybudování eGovernment cloudu TCO)
- Personální rozvoj

- Programové řízení
- Projektové řízení,
- PoC (Proof of Concept) – ověření konceptu (nejen funkční, ale i ekonomické, náročnost a předpoklady implementace, ..)
- RASCI matice – viz Kompetenční matice
- RCA (Root Cause Analysis) - Analýza primární příčiny
- RIA (Regulatory Impact Assessment) - hodnocení dopadů regulace
- Roadmap - podrobný plán/postup/harmonogram
- ROI (Return On Investments) - Návratnost investic
- Řízení kvality (Quality Management)
- Řízení nákladů (Cost Controlling)
- Řízení portfolia (služeb) (Mop – Portfolio Management)
- Řízení potřeb / požadavků
- Řízení rizik (MoR – Management of Risk)
- Řízení vztahů se zákazníky
- Řízení zdrojů
- Řízení změn (včetně řízení programů a projektů, viz samostatné metody).
- Řízení životního cyklu
- Řízení podle odchylek
- Řízení údržby dle spolehlivosti (Reliability maintenance)
- SMART přístup - cíle by vždy měly být: Specifikované, Měřitelné, Akceptovatelné, Reálné a Termínované
- Standardizace
- Strategické plánování:
  - Tvorba ICT strategie
  - Enterprise Architektura
- Studie mezinárodního srovnání
- Studie proveditelnosti,
- SWOT analýza
- TCO (Total Cost of Ownership) – celkové náklady na vlastnictví
- Věcný rámec

Rejstřík metod řízení ICT

Bude doplněn v dalším vydání MŘICT.

1)
na základě zmocnění podle § 5a odst. 1 zákona č. 365/2000 Sb.
2)
Právě to, společně se strukturami a procesy centrální koordinace implementace IKČR, je předmětem cíle DC 5.01
3)
Kompletní wikipedie společné Znalostní báze Metod řízení ICT a Národní architektury VS ČR je aktuálně na odkazu: https://archi.gov.cz/znalostni-baze:znalostni_baze
4)
Informační koncepce ČR dle § 5a odst. 1 zákona č. 365/2000 Sb., stanoví cíle České republiky v oblasti informačních systémů veřejné správy a obecné principy pořizování, vytváření, správy a provozování informačních systémů veřejné správy v České republice na období 5 let, kterou Ministerstvo vnitra v rámci dlouhodobého řízení informačních systémů veřejné správy vytváří a předkládá vládě ke schválení.
5)
Příloha č. 2 - Úplný jmenovitý seznam záměrů, ve všech klasifikacích (ABCDE), vázaných na pilíř, hlavní a dílčí cíl (Shrnutí implementačních plánů pro 2019)
6)
Usnesení vlády ze dne 15. dubna 2019 č. 255, k Implementačním plánům programu „Digitální Česko“
7)
Převážně v podobě akcelerátorů, návodů či předloh na míru těmto úřadům.
8)

V užším slova smyslu je úřad institucionální složkou samosprávných celků, na rozdíl od nich samých však jejich úřad nemá právní subjektivitu a jedná jménem celé samosprávného celku (obce či kraje).
9)

Jedná se zejména o tyto faktory:

- každá obec či kraj jsou samostatné subjekty a je jim možno ukládat povinnosti pouze zákony,
- rozhodování obce je kolektivní (rozhoduje zastupitelstvo),
- obec může vykonávat mimo samosprávných činností i státní správu v přenesené působnost a správu majetku obce.

10)

Z angl. Shadow IT
11)

Usnesení vlády ČR ze dne 3. října 2018 č. 629 k programu „Digitální Česko“ a návrhu změn Statutu Rady vlády pro informační společnost
12)

OVS dle § 5a odst. 2 zákona o ISVS vytvářejí a vydávají informační koncepci orgánu veřejné správy, uplatňují ji v praxi a vyhodnocují její dodržování. V informační koncepci orgánu veřejné správy orgány veřejné správy stanoví své dlouhodobé cíle v oblasti řízení kvality a bezpečnosti spravovaných informačních systémů veřejné správy a vymezí obecné principy pořizování, vytváření, správy a provozování svých informačních systémů veřejné správy.
13)

OVS dle § 5a odst. 3 zákona o ISVS v souladu s vlastní vydanou informační koncepcí vytvářejí a vydávají provozní dokumentaci k jednotlivým informačním systémům veřejné správy, uplatňují ji v praxi a vyhodnocují její dodržování.
14) , 15) , 16) , 17)

Obor služby dle nařízení vlády 1/2019 Sb. https://www.zakonyprolidi.cz/cs/2019-1/
18)

Koresponduje s mezinárodní zkratkou P3O, z angl. Programme, Portfolio & Project Office, ale představuje zkratku pro Odbor programů, portfolií a projektů, tedy 3P.
19)

Konkrétně na základě úkolu ministra vnitra (bod II., odst. 1., písm. e), a od září 2019 je publikován na internetových stránkách Ministerstva vnitra
20)

Viz odkaz http://svs.institutpraha.cz/
21)

Z angl. Enterprise Architecture
22)

například institut klíčového zaměstnance, viz analýza RVIS.
23)

Namísto využívání mezinárodně uznávaných, jednoznačně kvantifikovatelných kvalitativních indikátorů, jsou běžně užívány nepodstatné množstevní ukazatele.
24)

Aktuálně nejčastější je vyhodnocování pouze dle splnění plánovaného čerpání finančních prostředků.
25)

Vychází z následující definice služby: „Služba je funkce úřadu/útvaru, poskytnutá konkrétním poskytovatelem konkrétnímu příjemci služby podle předem dané formální dohody (zákon, vyhláška, dohoda o úrovni služby - SLA) tak, že přináší příjemci vnímanou hodnotu, za kterou by byl ochoten zaplatit přiměřenou cenu.
26)

Dostupné z: EUR-LEX
27)

Pracovní zkratka, viz Úvod
28)

hlava III zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů
29)

ČESKO. § 3 odst. 4 písm. a) zákona č. 320/2001 Sb.. In: Zákony pro lidi.cz [online]. © AION CS 2010-2019. Dostupné z: https://www.zakonyprolidi.cz/cs/2001-320#p3-4-a
30)

Vyhláška č. 416/2004 Sb., kterou se provádí zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění zákona č. 309/2002 Sb., zákona č. 320/2002 Sb. a

zákona č. 123/2003 Sb.
31)

§ 2 zákona č. 320/2001 Sb., oo finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů
32)

Zadání musí být v souladu se zákonným zmocněním a se specifikací agendy v Registru práv a povinností.
33)

Převzato upraveno ze zápisu jednání VV pro IKČR ze dne 21.06.2019.
34)

Governance je zejména pro ty, kdož se přímého řízení nezúčastňují, jako např. vlastníci, akcionáři, správci, politici, komerční partneři, akademičtí partneři a zahraničí (sběrný box – zahraniční klienti, subjekty, klienti, partneři aj.).
35)

Jiný výklad pojmu Governance: Stanovení politik a průběžné sledování jejich řádného provádění členy řídícího orgánu organizace. Další informace: https://dictionary.cambridge.org/dictionary/english/governance
36)

Odpovídá angl. zkratce SDLC - Software Development Life Cycle
37)

Jiní autoři také užívají výrazů: kroků, stupňů nebo etap, ale tyto pojmy jsou ponechány pro jiné účely.
38)

https://www.zakazky.mvcr.cz/document_audit_26145/MV_CEPR_-_Metodicka_prirucka.pdf
39)

Pokyn ministra vnitra č. 5/2017 ze dne 25. ledna 2017, kterým se zřizuje projektová kancelář a upravuje řízení projektů v oboru působnosti Ministerstva vnitra
40)

Z angl. Project Charter
41)

Z původního významu „modrotiskového plánu, výkresu konstrukce zařízení“, více: https:%%//%%cs.wikipedia.org/wiki/Diazotypie, nyní detailní prováděcí návrh řešení.
42)

Z angl. Project Start Architecture, model systému pro budoucí projekt na úrovni Enterprise Architecture.
43)

angl. Solution Architecture.
44)

Z angl. Functional & Non-functional Specification.
45)

Z angl. Project Start Architecture
46)

Angl. také „Landscape“.
47)

Z angl. Proof of Concept.
48)

Jak dokládají publikované zkušenosti např. z USA a Velké Británie, je katalog jedním z klíčových nástrojů řízení ICT ve veřejné správě. Navazuje na katalog služeb veřejné správy a eviduje veškeré ICT služby (SaaS, DaaS, PaaS, IaaS), které jsou aktuálně provozovány jak pro interní potřebu úřadů, tak nabízeny jako e-služby občanům a firmám.
49)

Smlouva by se měla vyvarovat nevýhodných ustanovení (Vendor-Lock-In), viz:
. https://archi.gov.cz/znalostni_baze:vendorlock.
50)

Také se používá pojem „exit plán“ nebo „exit strategie“.
51)

Z angl. Project Start Architecture, (raději než české PAS - projektová architektura systému nebo SAP - systémová architektura projektu)
52)

Z angl. Solution Architecture.
53)

Z angl. Functional & Non-functional Specification.
54)

Angl. zkratka je COTS (Commercial off-the-shelf).
55)

Z angl. Software-as-a-Service
56)

Z angl. deployment - nasazení, rozvinutí
57)

Viz metodika TCO: Metodika TCO ICT služeb VS
58)

V angl. Project Management Office - PMO.
59)

Je třeba umožnit, aby zaměstnanec byl pro projekt uvolněn i bez svého souhlasu a bez souhlasu svého přímého představeného, například s využitím §47 Služebního zákona, č. 234/2014 Sb. o přeložení. Bylo by užitečné prosadit legislativní úpravu nejdelší doby přeložení bez souhlasu zaměstnance na 120 dnů v kalendářním roce a se souhlasem zaměstnance až na dobu trvání projektu.
60)

pokud jím není Ředitel projektu nebo Věcný gestor změny (agendy
61)

Definice malého projektu a velmi malého projektu budou ještě hledány.
62)

Z angl. Lessons Learned
63)

Enterprise architektura, architektura řešení i návrh (design) řešení.
64)

zde také někde uváděné jako součást tzv. mandatorních zdrojů.
65)

Zákon č 134/2016 Sb. o zadávání veřejných zakázek.
66)

databáze konfigurací, z angl.. Configuration Management DataBase
67)

Z angl. engagement - bohužel není vhodný ustálený překlad.
68)

Z angl. Pattern.
69)

Národní architektonický rámec (NAR) byl vytvořen na základě kombinace TOGAF 9.2 a ArchiMate 3.1.
70)

Z angl. Architecture Development Method.
71)

Z angl. The OpenGroup ArchiMate Model Exchange File Format.
72)

V angličtině Project Management Office - PMO.
73)

Dle metodiky MSP (Managing Successful Programmes), například (Williams, 2004).
74)

V širším smyslu ICT služby, tzn. ne jen „pouhé“ podpory / maintenace (např.: update SW), ale i DaaS, cloudových služeb (zejm.: SaaS, IaaS, PaaS, DPaaS) apod.
75)

Z angl. Digital proper legislation (DPL), například na ria.vlada.cz
76)

GDPR
77)

Anglicky by se řeklo Win/win, tzn. přibližně, že obě strany jsou vítězi.
78)

Zákon č. 2/1969 Sb. - Zákon České národní rady o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky
79)

https:%%//%%www.esfcr.cz/documents/21802/782328/02_Metodika_logickeho_ramce.pdf/b840b4ad-5d37-44c4-ade4-70f663f8047f