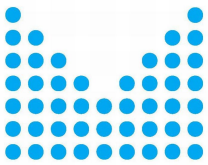
Materiál Ministerstva vnitra



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Export z Národní architektury eGovernmentu ČR

Obsah

Řízení na úrovni útvaru ICT OVS

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[1)]) 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[2)] 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[3)], 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[4)]. 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[5)] 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[6]), 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 [7] 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[8)]. 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"[9)]). 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[10)] 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.

1) zde také někde uváděné jako součást tzv. mandatorních zdrojů.
2) Zákon č 134/2016 Sb. o zadávání veřejných zakázek.
3) databáze konfigurací, z angl.. Configuration Management DataBase
4) Z angl. engagement - bohužel není vhodný ustálený překlad.
5) Z angl. Pattern.
6) Národní architektonický rámec (NAR) byl vytvořen na základě kombinace TOGAF 9.2 a ArchiMate 3.1.
7) Z angl. Architecture Development Method.
8) Z angl. The OpenGroup ArchiMate Model Exchange File Format.
9) V angličtině Project Management Office - PMO.
10) Dle metodiky MSP (Managing Successful Programmes), například (Williams, 2004).