FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

# ZADÁNÍ DIPLOMOVÉ PRÁCE

| | |
|---|---|
| **Název:** | Analýza a návrh procesů Technologické agentury ČR v souvislosti s bezpečností informací |
| **Student:** | Bc. Marian-Daniel Rolník |
| **Vedoucí:** | Ing. Petra Pavlíčková, Ph.D. |
| **Studijní program:** | Informatika |
| **Studijní obor:** | Webové a softwarové inženýrství |
| **Katedra:** | Katedra softwarového inženýrství |
| **Platnost zadání:** | Do konce letního semestru 2020/21 |

## Pokyny pro vypracování

Cílem diplomové práce je analyzovat procesy Technologické agentury České republiky (TA ČR) v souvislosti s bezpečností informací, poskytováním IT služeb a vytvořit návrh integrovaného procesního rámce řízení IT služeb a bezpečnosti informací.
1. Nastudujte a analyzujte potřebné informace k problematice bezpečnosti informací, řízení IT služeb a standardizované požadavky na systémy managementu.
2. Nastudujte a analyzujte nástroje pro modelování procesů v TA ČR (SW ARPO).
3. Porovnejte a vyberte metodiku řízení systému bezpečnosti informací a poskytování služeb IT pro její aplikaci v návrhu řešení.
4. Zanalyzujte aktuální business procesy v TA ČR v souvislosti s bezpečností informací a managementem rizik.
5. Navrhněte řešení pro redesign procesů a politik v TA ČR za účelem certifikace ISO 27 000 a ISO 20 000.
6. Zhodnoťte navržené řešení a přínos pro TA ČR a další možný rozvoj.

## Seznam odborné literatury

Dodá vedoucí práce.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 11. prosince 2019

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Diplomová práce

# Analýza a návrh procesů Technologické agentury ČR v souvislosti s bezpečností informací

***Bc. Marian-Daniel Rolník***

Katedra softwarového inženýrství
Vedoucí práce: Ing. Petra Pavlíčková, Ph.D.

28. května 2020

# Poděkování

Tímto bych chtěl poděkovat vedoucí diplomové práce paní Ing. Petře Pavlíčkové, Ph.D. za přínosné konzultace k této práci. Dále bych jí chtěl poděkovat za všechny informace, které jsem si odnesl z předmětů, které vedla.

Další poděkování patří Technologické agentuře ČR za to, že mi bylo umožněno diplomovou práci vytvořit v rámci jejího rozvoje. Zejména chci poděkovat Vítězslavu Vlasákovi a Radovanu Luptákovi, za trpělivost a konzultace, které mi s prací významně pomohly. Děkuji i všem zaměstnancům TA ČR, kteří mi poskytli svůj čas pro sdělení informací, které jsou uvedeny v této práci.

Děkuji svojí rodině za dlouhodobou podporu ve studiu a za pomoc, kterou mi poskytovali během posledních let.

Děkuji za podporu svojí přítelkyni, za poskytnutí nesčetných připomínek a za její výdrž v období psaní této diplomové práce.

# Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo"), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 28. května 2020 ……

### Odkaz na tuto práci

Rolník, Marian-Daniel. *Analýza a návrh procesů Technologické agentury ČR v souvislosti s bezpečností informací.* Diplomová práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2020.

# Abstrakt

Práce se věnuje návrhu procesů a politik Technologické agentury ČR. Před návrhy byla vytvořena analýza procesů Technologické agentury ČR v souvislosti s bezpečností informací. Na základě této analýzy je vytvořen návrh procesů a politik. Navržené procesy jsou vytvořeny dle metodiky ARIS s použitím nástroje SW ARPO. Návrhy procesů a politik byly vytvořeny na základě série norem ISO/IEC 20000 a ISO/IEC 27000 s cílem certifikace na tyto normy.

**Klíčová slova** procesní řízení, bezpečnost informací, podnikové procesy, ISO/IEC 20000, ISO/IEC 27000, ARIS, SW ARPO, Release and Deployment management, Incident management, bezpečnostní politika

# Abstract

This thesis is devoted to the design of processes and policies of the Technology Agency of the Czech Republic. Prior to designing processes and policies, an analysis of the processes of the Technology Agency of the Czech Republic in connection with information security was created. Based on this analysis, a design of processes and policies is proposed. The proposed processes are implemented according to the ARIS methodology with ARPO SW tools. The design of processes and policies have been established on the basis of ISO/IEC 20000 and ISO/IEC 27000 standards with regard to certificates for these standards.

**Keywords** process management, information security, business processes, ISO/IEC 20000, ISO/IEC 27000, ARIS, SW ARPO, Release and Deployment management, Incident management, security policy

# Obsah

# Seznam obrázků

# Seznam tabulek

# Úvod

Současná doba je dobou informačních technologií a neustálého a rychlého vývoje. Se vzrůstající digitalizací využíváme pro sběr, sdílení a evidenci dat nejrůznější informační systémy a aplikace, kterým bezpodmínečně důvěřujeme. Aplikace a informační systémy ale nemusí být tak dobře zabezpečeny, jak si myslíme. Příkladem může být v současné době často diskutovaná kauza Benešovské nemocnice, ve které došlo k napadení interních systémů hackerem. Během tohoto útoku došlo k vyřazení určitých systémů, které byly pro chod nemocnice kritické. Tato událost je jen jednou z mnoha událostí, které se dnes dějí, ale vzhledem k tomu, že měla přímý dopad na pacienty nemocnice, bylo jí veřejností dopřáno velké pozornosti. Snahou hackerů nemusí být pouze vyřazení systémů z provozu, ale i odcizení důležitých dat, která jsou v systémech organizací uchovávána.

Nejen samotná existence napadnutelných chyb v softwaru může zapříčinit únik nebo ztrátu dat, ale i nesprávné používání těchto systémů. Správná organizace práce je nedílnou součástí při snaze zabránit těmto útokům. Pro efektivní organizaci práce se v dnešní době využívají různé systémy řízení procesů. Řízení procesů a jejich úprava významně zasahují do chodu organizace a je nutné je řídit s ohledem na provoz informačních systémů a s ohledem na strategické směřování organizace. Důležitou součástí organizace práce nejsou pouze procesy, ale i pravidla, podle kterých se musí zaměstnanci řídit.

Přes několik let už jsem v kanceláři Technologické agentury České republiky (TA ČR) zaměstnán jako administrátor Informačního systému Technologické agentury. Tento informační systém je používán TA ČR pro podporu většiny klíčových procesů. Systém nepoužívají pouze zaměstnanci TA ČR, ale systém je využíván dalšími uživateli z prostředí výzkumu a vývoje. Vzhledem k tomu, že se jedná o jeden z nejdůležitějších systémů TA ČR, jsou v něm tedy uchována i data, která jsou citlivá nejen pro TA ČR, ale i pro uživatele systému.

Díky absolvování několika předmětů na ČVUT, které se zabývají bezpeč-

ností softwaru a procesním řízením, jsem si vědom nebezpečí, která plynou z nedostatečného zabezpečení nebo z nesprávného nastavení procesů v organizaci.

Proto jsem se rozhodl v této práci analyzovat procesy Technologické agentury ČR v souvislosti s bezpečností informací. Analýza plyne z účastí na schůzích TA ČR, stínování manažerů, studování zápisů schůzí, rozhovorů s klíčovými osobami, vlastní pracovní zkušenosti v TA ČR a ze schůzí s externími subjekty. Na základě této analýzy je vytvořen návrh úpravy procesů a politik, které slouží jako první kroky k certifikaci podle norem ISO/IEC 20000-1 a ISO/IEC 27001. Normy jsou mezinárodně uznávanými standardy a i z toho důvodu byly pro řešení mé práce zvoleny. Vytvořené návrhy by měly přispět ke zvýšení bezpečnosti TA ČR.

Kapitola 1

# Cíl práce

Cílem této diplomové práce je vytvoření návrhu úpravy procesů Technologické agentury České republiky. Tomuto návrhu předchází nastudování metodik řízení systému bezpečnosti informací a poskytování služeb IT a analýza procesů TA ČR za použití těchto metodik (ITIL, série norem ISO/IEC).

Dalším cílem je, aby tento návrh byl v souladu s normami uvedenými výše a následná možnost certifikace podle normy ISO/IEC 27001, která se zabývá systémem řízení bezpečnosti informací. Cílem je také možnost certifikace podle normy ISO/IEC 20000-1, která se zabývá integrovaným procesním rámcem organizace.

Vzhledem k tomu, že Technologická agentura ČR používá pro popis svých interních procesů nástroj SW ARPO, je nutné tento nástroj nastudovat a modely v něm vytvořit.

Cílem práce není obsáhnout a navrhnout všechny procesy a politiky pro soulad s normami výše uvedenými, ale poskytnout úpravu vybraných procesů a politik, které budou sloužit jako know-how organizaci při vytváření nových podnikových procesů nebo úpravě stávajících procesů, jelikož normy určují rámec, ale neposkytují konkrétní opatření „šitá na míru“ organizaci.

Technologická agentura ČR je organizační složkou státu, která se musí řídit konkrétními zákony. Důležitým požadavkem je nastudování těchto zákonů.

Na závěr bude zhodnoceno navržené řešení a jeho přínos pro TA ČR společně s dalším možným rozvojem.

Kapitola 2

# Procesy a procesní řízení

Všechny organizace fungují na základě činností, které vykonávají lidé, kteří pro ně pracují. Procesní řízení přináší systém a nástroje, jak tyto činnosti uspořádat, propojit a řídit tak, aby byly vysoce efektivní a přinášely užitek pro zákazníky, majitele a zaměstnance organizace. [1]

Procesní řízení je alternativou k funkčnímu řízení, v němž je podnik rozdělen na provozy, úseky, odbory, oddělení a každý útvar má svoji agendu a svoje odpovědnosti. V modelu funkčního řízení mají útvary tendenci vytvářet kolem sebe bariéry (zejména komunikační a informační), čímž trpí kvalita činností, které jsou důležité pro prosperitu podniku. [2]

Procesní řízení jako prioritu definuje proces, tj. sekvenci činností, které je třeba udělat a to bez ohledu na organizační uspořádání (např. proces vyřízení objednávky). Teprve následně se stanoví, kdo jednotlivé činnosti provádí a jak jsou pracovníci organizováni. Výsledkem je opět vnitřní struktura podniku, ale přizpůsobená tomu, aby co nejvíce podporovala podnikové procesy. [3]

## 2.1 Podnikový proces

Pod pojmem podnikový proces zpravidla rozumíme objektivně přirozenou posloupnost činností, konaných s úmyslem dosažení daného cíle v objektivně daných podmínkách. [3]

U procesů hraje základní roli čas. Je hovořeno o posloupnosti činností, tedy i časové posloupnosti. Pokud popisujeme proces, je popisována posloupnost, ne struktura. Popisujeme procesně, nikoliv objektově. [3]

K podnikovému procesu tedy patří tyto aspekty:

1. cíl,
2. úmysl,
3. objektivní přirozenost postupu,

4. objektivně dané podmínky.

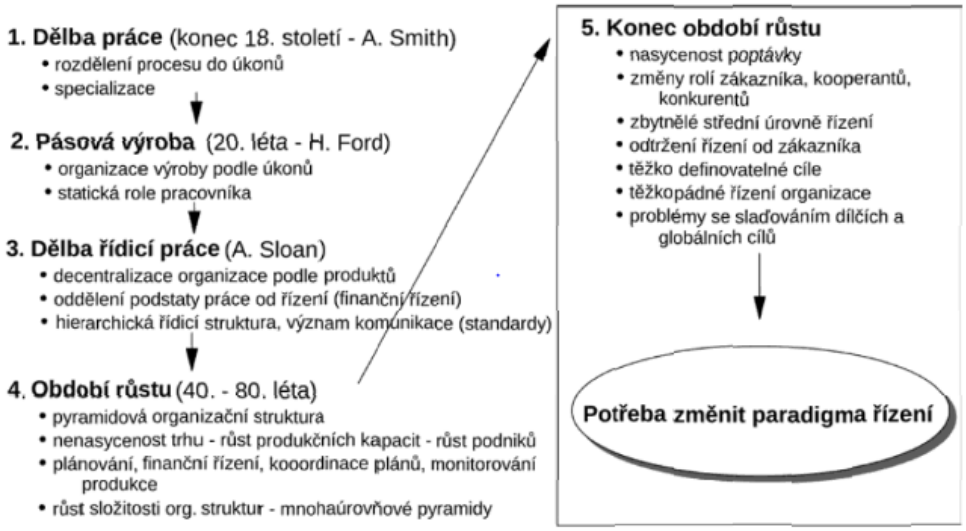
## 2.2 Procesně řízená organizace

Procesním řízením se rozumí řízení organizace takovým způsobem, v němž podnikové procesy hrají klíčovou roli. [3]

### 2.2.1 Historie procesního řízení

Přístup k pracovnímu stylu a organizačním principům se od časů vzniku firem značně změnil. Postupy, které byly platné v 18. století se postupně stávají starými, ztrácejí platnost nebo jsou byly postupně nahrazovány. [3]

Obrázek 2.1 ilustruje základní mezníky v historii vývoje řízení podniků podle Hammera a Champyho.




Obrázek 2.1: Historie vývoje řízení podniků [3]

Prvním milníkem v historii byla dělba práce. Práce byla rozdělena na úkony, které umožňovaly úzkou specializaci, což vedlo k prudkému růstu kvalifikace. Toto rozdělení mělo dalekosáhlé důsledky ve vnitřním uspořádání organizace a následně i uspořádání trhu.

Dalším milníkem je rozdělení práce podle H. Forda, který vynalezl pohyblivý pás, místo pohyblivých lidí. Dříve museli dělníci táhnout součástky ke statickým automobilům. Henry Ford a jeho pás umožnil, aby staticky stáli dělníci a součástky jezdily k dělníkům. [4]

Dělba práce, kdy dělník dělá pouze zlomek z celého produktu a práce k němu sama přijede přispěla až k tisícinásobnému růstu produktivity oproti přístupu, kdy celý výrobek dělal jeden člověk sám. [3]

Dalším milníkem byla decentralizace podle produktů, dělba práce a hierarchická struktura. Toto rozdělení zvyšuje efektivitu, ale na druhou stranu může mít zničující efekt z hlediska celé společnosti. Cíle jednotlivých divizí mohou být v rozporu a mohou ztrácet na efektivnosti. V dané době ale nebyly tyto problémy kritickými. [3]

Celá poválečná doba je nazvaná dobou růstu. Zlepšování organizace a práce a z toho plynoucí růst efektivnosti umožnilo růst průmyslu, k čemuž pomohly i obě světové války. Vývoj technologie a její používání měl za následek změny ve fungování, zejména v komunikaci. Informace proudí rychleji, trh se stává nasyceným. [3]

Podle [5] jsou 3 síly, které vytvořily nový svět pro byznys. Jsou to:

- Customers - zákazníci,
- Competition - konkurence,
- Change - změna.

Zákazník se stává pánem a jelikož je trh nasycený a zákazníci si mohou vybírat z nepřeberného množství produktů, zvyšuje se i konkurence a potřeba flexibility a rychlé reakce na změny stavu trhu.

V současném prostředí je více kvalifikovaných odborníků a odpadá problém rozdělovat úkoly na nejmenší možné části, aby práci zvládli i nekvalifikovaní pracovníci, jak tomu bylo v dřívějších dobách. [3]

### 2.2.2 Orientace na procesy

Základní podstata fungování se změnila a organizaci nelze řídit na základě pevně definované organizační struktury, kde má každý zaměstnanec předem určené místo, definovanou odpovědnost a k tomu příslušné pravomoci. Takové řízení předpokládá předem definované neměnné posloupnosti činností. Taková organizace nemůže být pružná a flexibilní vůči změnám. [3]

Organizace by se měla přeorientovat na přístup, kde je představa podnikových procesů jako „soubor činností, který vyžaduje jeden nebo více vstupů a tvoří výstup, jenž představuje hodnotu pro zákazníka“. [5]

Aby mohla organizace naplňovat svou primární funkci, musí konat. Obecnou abstrakcí konání organizace je soustava jejích podnikových procesů. Souvislosti procesů a uvědomění si jich v souvislosti organizace je esencí fungování organizace. Nikoliv organizační struktura ani informační systém. Podnikové procesy tvoří základní obsahovou strukturu fungování organizace. [3]

## 2.3 Dělení procesů

Podle [6] je možné dělit různými způsoby a každá organizace si může vybrat způsob, který je jí nejbližší a vyhovuje jejím potřebám.

Procesy je možné dělit na:

- vnitropodnikové procesy a procesy jdoucí za hranici firmy;
- procesy zaměřené na externího zákazníka a interního zákazníka (procesy zajišťující realizaci produktu);
- procesy zajišťující krátkodobou prosperitu a procesy zajišťující dlouhodobou prosperitu;
- technologické (například výroba) a informační (výzkum, vývoj a strategie);
- materiální, informační a procesy závazků a vztahů;
- jednoduché, středně složité a složité;
- procesy řídící, procesy přípravy zdrojů, procesy realizace produktu, procesy dalšího rozvoje (rozdělení je z normy EN ISO 9001:2000, což už neplatí v nové aktualizované verzi EN ISO 9001:2015 [7];
- hlavní a podpůrné, přičemž podpůrné se dále dělí na pomocné a obslužné;
- transakční, vývojové, podpůrné, infrastrukturní, řídící a mezipodnikové;
- hlavní, řídící a podpůrné.

Dle [6] je doporučeno používat poslední rozdělení - hlavní, řídící a podpůrné procesy. Je často používáno v praxi, jelikož je jednoduché, přehledné a poskytuje důležité informace o procesu a napovídá, jak má být řízen. Je jasně ukázáno, jaký význam jednotlivé procesy mají a tím napomáhá stanovit priority procesů, které mají projít reengineeringem. Tabulka 2.1 uvádí základní charakteristiku hlavních, řídících a podpůrných procesů.

Hlavní jsou takové procesy, které přímo přispívají k naplnění poslání organizace. Řídící procesy mají za úkol vytvořit jednotný a maximálně funkční systém řízení. Podpůrné procesy jsou zaměřeny na poskytování produktů a služeb zákazníkům nebo klíčovým procesům, které mohou být zajišťovány externě subdodavatelsky.

## 2.4 Řízení podniku

V této kapitole jsou rozebrány způsoby řízení podniku. Zejména je rozebráno procesní řízení a funkční řízení. Tato dvě řízení jsou porovnána.

Tabulka 2.1: Typy, způsob řízení a všeobecná charakteristika podnikových procesů [6]

| **Typ procesu** | **Způsob, jakým má být řízen** | **Charakteristika procesu** | | | |
|---|---|---|---|---|---|
| | | **Přidává hodnotu?** | **Probíhá napříč organizací?** | **Má externí zákazníky?** | **Generuje tržby (zisk)?** |
| hlavní | výkonově | ANO | ANO | ANO | ANO |
| řídící | nákladově | NE | ANO | NE | NE |
| podpůrný | výkonově, možnost outsourcingu | ANO | NE | NE | NE |

### 2.4.1 Procesní řízení

V procesním řízení je hlavní prioritou proces. Proces má vstupy a výstupy a generuje pro organizaci přidanou hodnotu. V procesu je důležitý jak zákazník procesu, tak jeho vlastník. Zákazník procesu může být interní i externí. Pokud proces nepřináší zisk nebo hodnotu jiným procesům, měl by být odstraněn a neměl by existovat. [8]

Jak je vidět na obrázku 2.2, procesní řízení probíhá nezávisle na organizační struktuře organizace. Tím se stává flexibilnějším a skrz procesní řízení lze rychleji reagovat na změny oproti funkčnímu řízení.

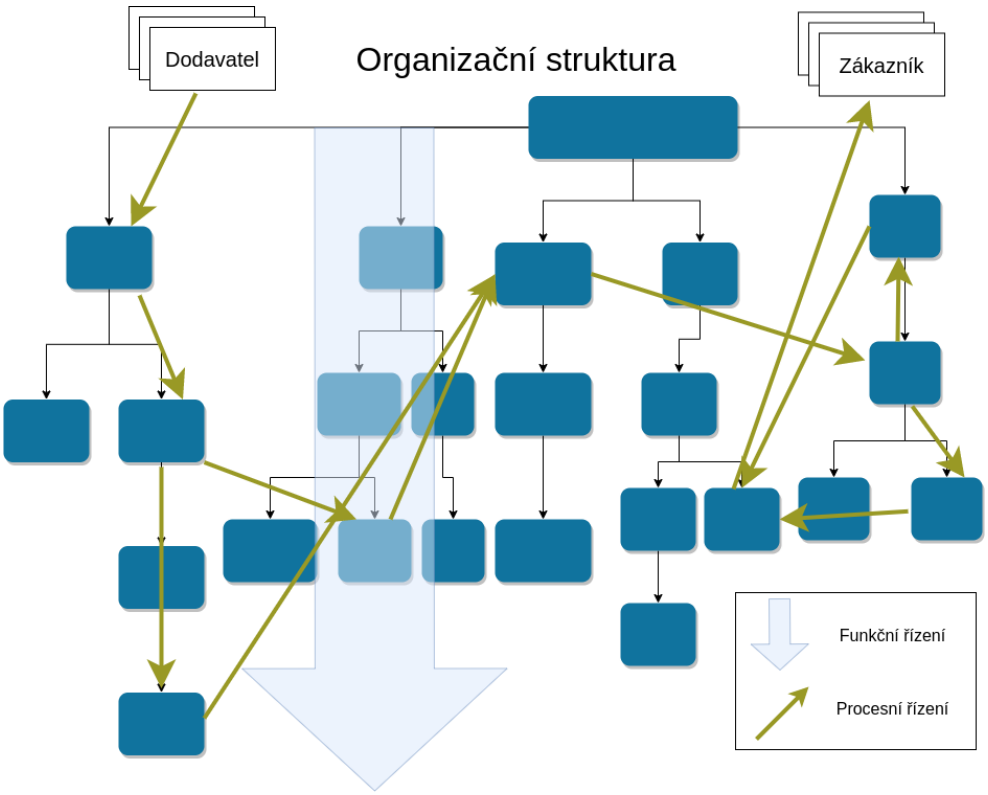
### 2.4.2 Funkční řízení

Funkčním řízením je nazýván přístup k řízení, který je založen na pevném vymezení funkční, v rámci hierarchie, organizační struktury. Pracovní postupy jsou založeny na vertikálních vztazích nadřízený-podřízený. Přímá horizontální spolupráce bývá minimální. [9]

Tento postup řízení byl definován již v roce 1776 Adamem Smithem a vychází z tradiční dělby práce podle specializace a je založen na rozložení práce na nejjednodušší úkony tak, aby byly jednoduše proveditelné i nekvalifikovanými pracovníky, více v kapitole 2.2.1. Toto rozdělení vede k rozdělení práce mezi organizační jednotky, které jsou rozdělené na základě odborností (funkcí). [10]

### 2.4.3 Rozdíl mezi funkčním a procesním řízením

Základním rozdílem mezi procesním a funkčním řízením je stanovení jednotky řízení, k níž se vztahuje odpovědnost, rozpočet a data. V procesním řízením je touto jednotkou proces. Naproti tomu ve funkčním řízením je touto jednotkou organizační útvar. [11]




Obrázek 2.2: Procesní vs. Funkční řízení procesů

Procesní přístup k řízení je orientován nejen na výsledek práce (produkt), ale i na postup jeho dosažení. Práce není vykonávána separátně v oddělených funkčních jednotkách, ale naopak jimi „protéká“. Při procesním přístupu k řízení dochází ke zlepšení obvykle formou optimalizace a zjednodušení celého toku práce. Zatímco jsou organizační jednotky známé a přesně definované, procesy a jejich průběh při využití funkčního přístupu zmapovány a definovány nejsou. Toto prakticky znamená, že procesy v organizaci odpovídají jejím přirozeným činnostem, ale jsou často rozdrobeny a zamlženy organizačními strukturami. Pracovníci uvažují o jednotlivých činnostech a ne o procesu jako celku. Procesy také zůstávají neřízeny, jelikož manažeři jsou pověřeni vedením útvarů nebo pracovních jednotek, ale žádný z nich nemá zodpovědnost za celý úkol, tj. proces. [12]

Na obrázku 2.2 můžeme vidět rozdělení na procesní řízení a funkční řízení podniku. Jak je vidět, organizace je rozdělena hierarchicky a ve funkčním řízení se soustředí každá organizační jednotka na svůj úkol, bez ohledu na ostatní jednotky. Nedívají se na proces jako na celek, ale sledují například pouze svoji část procesu, kterou mají na starosti. Odpovědnosti vedou shora dolů a celkový proces nemá svého vlastníka, který by za výsledek (produkt) a

cestu k němu měl zodpovědnost.

Naproti tomu je z obrázku 2.2 vidět, že procesní řízení a samotný proces je rozdělen horizontálně, napříč organizací a jednotlivé úkony jsou prováděny s ohledem na celkový proces a každý pracovník má zodpovědnost za svoji část procesu.

V tabulce 2.2 jsou vidět rozdíly přístupů v takových organizacích. Celkově je patrné, že v každé ze sedmi dimenzí jsou uvedeny charakteristiky obou srovnávaných typů organizace.

| | Tradiční organizace | Procesně řízená organizace |
|---|---|---|
| Organizační struktura | • Hierarchická struktura<br>• Příkaz a kontrola (rozděl a panuj) | • Necentrická, síťová struktura<br>• Pružná a měnitelná struktura |
| Velení | • Zaměřeno donvnitř<br>• Top-down na základě hierarchie | • Zaměřené interně i externě<br>• Distribuované |
| Vůdcovství | • Vedoucí pracovníci jsou vybíráni mezi „hvězdami“ v hierarchické struktuře<br>• Vedoucí pracovníci nastavují agendu<br>• Vedoucí pracovníci vyvolávají změny | • Vedoucím je kdokoliv, podle aktuální potřeby procesu<br>• Vedoucí pracovníci vytvářejí prostředí pro úspěch<br>• Vedoucí pracovníci vytvářejí kapacity pro změnu |
| Lidé a kultura | • Dlouhodobé odměňování<br>• Vertikální rozhodování<br>• Odměňování jednotlivců a malých týmů | • „Vlastním svou vlastní kariéru“<br>• Pravomoci jsou delegovány<br>• Očekávaná spolupráce je následně odměňována |
| Znalosti | • Zaměřené na vnitřní procesy<br>• Individuálními vlastnostmi pracovníků | • Zaměřené na zákazníky<br>• Institucionální vlastnost organizace |
| Soudržnost | • „Natvrdo“ zadrátovaná v procesech<br>• Interní důležitost | • Vize organizace vložené do jednotlivců<br>• Dopady promítnuty mimo organizaci |
| Spojenectví | • Doplňuje/zvýrazňuje současné mezery<br>• Spojování se vzdálenými partnery | • Vytváření nové hodnoty a vytěsňování slabých služeb<br>• Spojování s konkurenty, zákazníky a dodavateli |

Tabulka 2.2: Rozdíly mezi tradičním (funkčním) řízením a procesním řízením organizace - upraveno dle [13]

Kapitola 3

# Technologická agentura České republiky

Technologická agentura ČR je organizační složkou státu a byla zřízena v roce 2009 zákonem č. 130/2002 Sb. o podpoře výzkumu, experimentálního vývoje a inovací. Programy Technologické agentury ČR mají za cíl zajistit podporu výzkumu, vývoje a inovací. Technologická agentura ČR centralizuje státní podporu aplikovaného výzkumu a vývoje, která byla do té doby roztříštěna mezi velký počet poskytovatelů. [14]

## 3.1 Popis organizace

Technologická agentura byla zřízena zákonem č. 130/2002 a vykonává všechny činnosti pro které byla zřízena. [15] Technologická agentura České republiky dle zákona č. 130/2002 zabezpečuje:

- přípravu a realizaci programů aplikovaného výzkumu, vývoje a inovací včetně programů pro potřeby státní správy;
- výběr návrhů programových projektů a jejich hodnocení;
- poskytování účelové podpory na řešení programových projektů;
- kontrolu plnění smluv o poskytnutí podpory nebo rozhodnutí o poskytnutí podpory a čerpání účelové podpory;
- hodnocení a kontrolu průběhu řešení programových projektů, jejich cílů a kontrolu výsledků dosažených programovými projekty;
- zpracování návrhu výdajů Technologické agentury ČR a zpráv o její činnosti;

- poradenství řešitelům projektů a uživatelům výsledků aplikovaného výzkumu, vývoje a inovací;
- podporu komunikace mezi výzkumnými organizacemi a soukromým sektorem a podílové financování programových projektů;
- jednání s příslušnými orgány České republiky nebo Evropské unie o slučitelnosti poskytování podpory se současným trhem;
- spolupráci s obdobnými zahraničními agenturami.

[14]

### 3.1.1 Organizační struktura TA ČR

Technologická agentura ČR je zřízená státem a je v čele zastoupena předsedou. Dalšími úředními orgány jsou výzkumná a kontrolní rada. Organizační a administrativní činnost TA ČR zajišťuje Kancelář TA ČR. Podrobná organizační struktura je vyobrazena schématem na obrázku A.2. [16]

#### 3.1.1.1 Výzkumná rada

Výzkumná rada především určuje směrování TA ČR. Vytváří strategické plány na následující období, zaměření nově připravovaných programů. Navrhuje nominace do poradních orgánů TA ČR a vyhodnocuje výsledky programů, jež TA ČR realizuje. [16]

#### 3.1.1.2 Kontrolní rada

Kontrolní rada zejména kontroluje rozdělování finančních prostředků TA ČR. Kontrolní rada projednává stížnosti a předkládá stanoviska a doporučení předsednictvu. [16]

#### 3.1.1.3 Předsednictvo

Předsednictvo TA ČR je výkonným orgánem agentury. Věnuje se strategickým činnostem, které plynou z výzkumné rady. Taktéž se věnuje doporučením a podnětům, které plynou z kontrolní rady a vykonává operativní činnosti vyplývající z chodu Kanceláře TA ČR. Vykonává taktéž úkoly dané usnesením vlády. [16]

#### 3.1.1.4 Kancelář TA ČR

Kancelář TA ČR se dělí na:

1. Sekce kabinetu,
2. Sekce rozvoje a řízení programů,

3. Sekce implementace programů,
4. Sekce provozní
5. Sekce realizace resortních potřeb,
6. Sekce projektové podpory.

[16]

### 3.1.2 Programy TA ČR

Technologická agentura České republiky vytváří jednotlivé programy a určuje jejich zaměření. Tato zaměření vytváří Výzkumná rada TA ČR a provozně jsou realizovány Kanceláří TA ČR. Pro každý program jsou definovány parametry, které musí jednotlivé projekty programu splňovat. Mezi tyto parametry patří například:

- doba trvání programu,
- doba trvání projektu,
- maximální intenzita podpory poskytovaná státem,
- typy uchazečů o podporu atd.

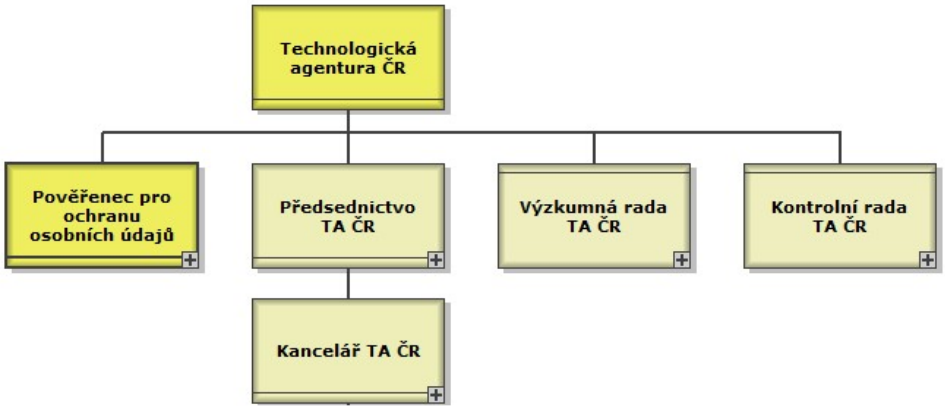
Jednotlivé programy TA ČR jsou pojmenovávány podle řecké abecedy a mezi programy patří i takové, které poskytují spolupráci se zahraničními resorty a podporují mezinárodní výzkum a vývoj. [16]

## 3.2 Technologická agentura České republiky jako procesně řízená organizace

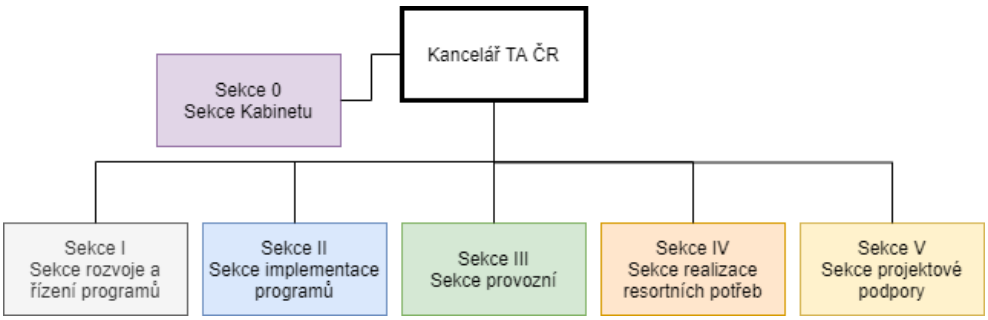
Technologická agentura České republiky má dle zákona č. 130/2002 Sb. jasně danou organizační strukturu. Struktura je hierarchická a pevná a rozdělení podle zákona je vidět na obrázku 3.1 a 3.2 . Kancelář TA ČR se dále dělí na menší celky, jak je vidět na obrázku 3.2. Každá sekce má svoje poslání a jasný cíl.

Toto rozdělení vede ke klasickému funkčnímu řízení, kde je vertikální rozdělení vztahů mezi nadřízeným a podřízeným. Již od roku 2014 TA ČR přešla na procesní řízení, kde se zodpovědnosti a data vztahují k procesu podle kapitoly 2.4.3.

Pokud se zohlední specifické potřeby a požadavky veřejné správy může toto řízení segmentu veřejné správy také výrazně prospět. Metodiku procesního řízení je nutné pro potřeby veřejné správy upravit, zohlednit specifické potřeby úřadů a dalších institucí a také podmínky, za nichž vedoucí úřadů a jiných organizací svou funkci vykonávají. [17]




Obrázek 3.1: Organizační struktura [18]




Obrázek 3.2: Organizační struktura - Kancelář TA ČR [18]

### 3.2.1 Procesní model a procesy Technologické agentury ČR

TA ČR disponuje komplexním procesním modelem, který poskytuje základní definici workflow jednotlivých procesů agentury a dokumentů, resp. formulářů představující klíčové produkty realizačních procesů. Základní konstrukt workflow se promítá do konfigurace a nastavení postupů/formulářů/funkcionalit podpůrného informačního systému ISTA. [19]

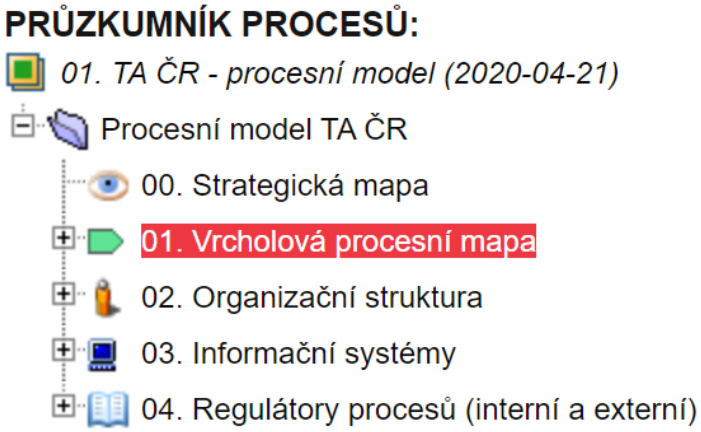
TA ČR pro modelování procesů používá modelovací a analytický nástroj ARPO BPMN++ Modeler a derivát modelovací notace ARIS Method. V procesním modelu TA ČR jsou zastoupeny následující typy modelů:

- Vrcholová procesní mapa (1. úroveň),
- Diagram struktury procesu - VAC,
- Diagram aktivit - rozšířený EPC,
- Diagram alokace procesu - SIPOC,
- Model informačních systémů,

- Model organizační struktury,
- Model struktury informací.

Technologická agentura ČR je procesně řízenou organizací. Procesní model TA ČR poskytuje strukturovaný pohled na klíčové procesy, jejichž konstrukt vychází zejména z požadavků zákona č. 130/2002 Sb., o podpoře výzkumu a vývoje ve znění pozdějších předpisů. Procesní rámec TA ČR je také základní definicí požadavků pro podpůrné informační systémy ISTA a ISŘB. V procesním modelu je evidováno celkem 18 různě rozsáhlých klíčových a 20 podpůrných procesů, které se dále rozpadají do cca 800 samostatných procesních diagramů. Jednotlivé činnosti jsou kontextově svázány s procesními rolemi a vstupy/výstupy ve formě formulářů. [20]

Procesní model TA ČR obsahuje 4 vrstvy, jak je vidět na obrázku 3.3, které by dle [21] měly být vždy součástí procesního modelu. Ostatní vrstvy lze dopracovat v rámci dalšího rozvoje a upřesňování a precizovaní obsahu procesního modelu.



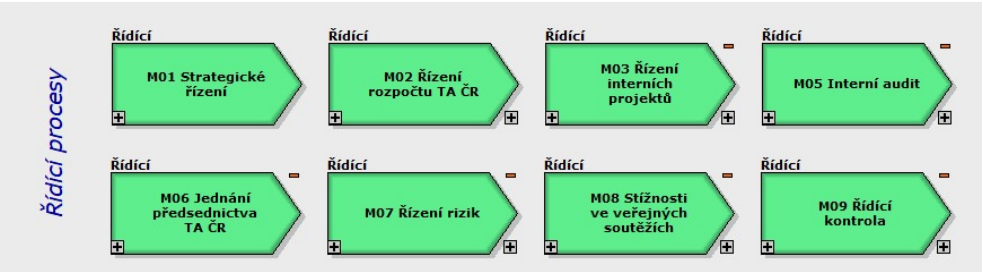

Obrázek 3.3: Vrstvy procesního modelu [18]

Procesní model je neustále revidován a upravován tak, aby odpovídal aktuálnímu stavu řízení procesů v TA ČR. Je rozdělen na 3 typy procesů - řídící, klíčové a podpůrné procesy, jak popisuje kapitola 2.3

#### 3.2.1.1 Řídící procesy

Řídící procesy nevytvářejí hodnotu pro zákazníka, ale jsou nastaveny tak, aby vytvořily maximálně funkční systém řízení. Jsou to aktivity, které koordinují, řídí, organizují a plánují vše ostatní. Slouží k efektivnímu fungování hlavních i podpůrných procesů a tím organizace jako celku.

Mezi řídící procesy v Technologické agentuře patří, jak je na obrázku 3.4:




Obrázek 3.4: Procesní model TA ČR - Řídící procesy [18]

- Strategické řízení,
- Řízení rozpočtu,
- Řízení interních projektů,
- Interní audity,
- Jednání předsednictva TA ČR,
- Řízení rizik,
- Stížnosti ve veřejných soutěžích,
- Řídící kontrola.

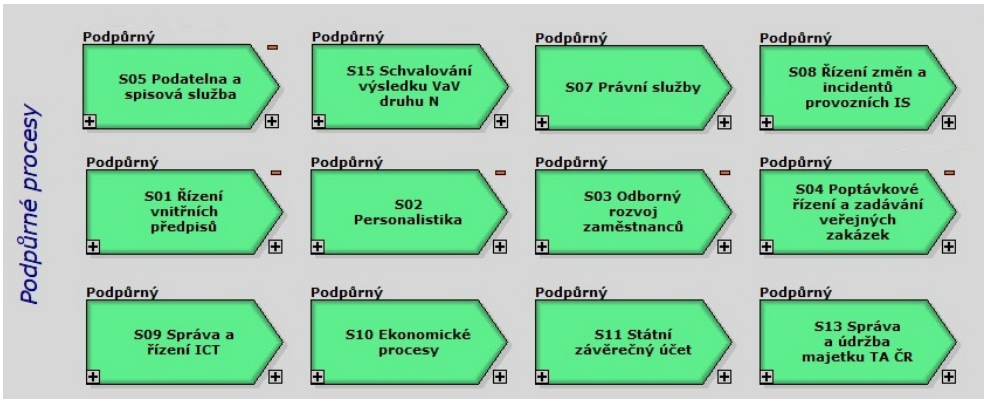
#### 3.2.1.2 Podpůrné procesy

Cílem podpůrných procesů je zajistit chod klíčových neboli hlavních procesů a zajistit chod organizace. Jejich jediným účelem je podpora hlavních procesů a poskytují produkty a služby zákazníkům nebo klíčovým procesům.

#### 3.2.1.3 Klíčové procesy

Klíčové nebo také hlavní procesy jsou takové, které přispívají k naplnění poslání organizace. Jedná se o hlavní agendu TA ČR, určenou zákonem č. 130/2002 Sb., o podpoře výzkumu a vývoje z veřejných prostředků. Jak je popsáno na obrázku 3.6, jsou zde uvedeny všechny procesy, které se týkají veřejné soutěže a projektů, kterým TA ČR poskytuje finanční podporu, pokud jsou schváleny a vybrány pro podporu. Mezi klíčové procesy patří, mimo ty, které jsou uvedeny na obrázku 3.6, i:

- Řízení programů,
- Správa hodnotitelů,




Obrázek 3.5: Procesní model TA ČR - Podpůrné procesy [18]

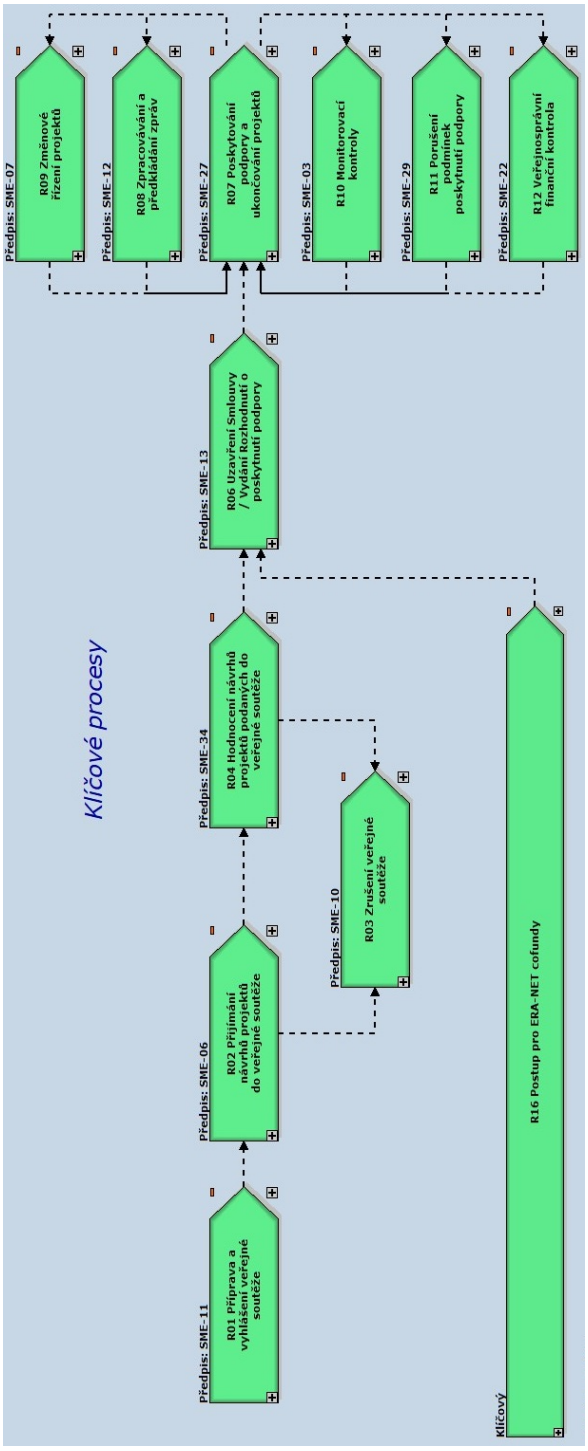
- Zajištění hodnocení návrhů projektů a projektů v realizaci,
- Helpdesk pro uchazeče a příjemce podpory.

## 3.3 Systém ISTA

Pro uvedení do kontextu je důležité zmínit, že Technologická agentura České republiky provozuje informační systém ISTA, který byl pro TA ČR vytvořen firmou AHASWARE s.r.o. [22]

Informační systém ISTA podporuje některé z klíčových procesů TA ČR. Prostřednictvím systému ISTA se mimo jiné přijímají návrhy projektů, podávají zprávy z průběhu projektu, uzavírají smlouvy s hodnotiteli projektů. Všechny tyto akce jsou popsané v procesním modelu a systém je infrastrukturou reálného systému organizace. Pouze informační systém integrovaný prostřednictvím jednotného modelu podnikových procesů může být dostatečnou informační infrastrukturou procesně řízené firmy na všechny její požadavky na pružnost chování. [3]

Podnikové procesy se tedy zabývají fungováním organizace a informační systém poskytuje pouze infrastrukturu pro integraci procesního řízení. Automatizace procesů v systému nezaručuje flexibilitu a zakotvení procesu do informačního systému naopak flexibilitu procesu snižuje. [3]




Obrázek 3.6: Procesní model TA ČR - Klíčové procesy [18]

Kapitola 4

# Metodika, notace modelování procesů a nástroje pro modelování

Práce obsahuje analýzu a návrh procesů Technologické agentury ČR, je nutné se tedy zabývat nástroji a notacemi modelování procesů. Technologická agentura používá pro modelování procesů nástroj ARPO SW a již existuje procesní model TA ČR, ve kterém je evidováno 18 různě rozsáhlých klíčových a 20 podpůrných procesů, které se dále rozpadají do cca 800 samostatných procesních diagramů. [20]

V procesním modelu TA ČR je použita metodika ARIS a nástroj ARPO SW. Tato metodika i tento nástroj jsou dále využity v další práci a v modelování procesů. Je nezbytné je popsat a pro TA ČR je esenciální využití tohoto nástroje a metodiky.

## 4.1 Náležitosti modelování

Základními prvky v modelování procesů jsou:

- proces,
- činnost,
- podnět,
- vazba–návaznost.

Proces je vždy modelován jako posloupnost vzájemně navazujících činností. Činnosti mohou nebo nemusí být popsány jako proces. Závisí to na použitém nástroji, stylu autora, omezení velikosti, tedy nezávisí na obsahu procesu samotného. [3]

Jednotlivé činnosti jsou na sebe navázány a tvoří strukturu. Návaznosti jsou tvořeny pomocí vazeb. Vazbami jsou definována různá uspořádání v procesu. Vazby se mohou křížit a jsou definovány základní typy - ARIS je nazývá logickými operandy. [3]

## 4.2 Metodika ARIS

Metodika ARIS byla vyvinuta prof. Dr. Augustem-Wilhelmem Scheerem. Tato metodika nedefinuje žádný přesný postup, ale poskytuje řadu pohledů k modelování jednotlivých aspektů organizace, včetně procesů, aby mohl být vytvořen návrh a analýza systému podniku. [3]

Metodika ARIS poskytuje pět základních pohledů na podnik (viz obr 4.1):

1. Organizační pohled - popisuje pracovníky, organizační jednotky a vztah mezi nimi;

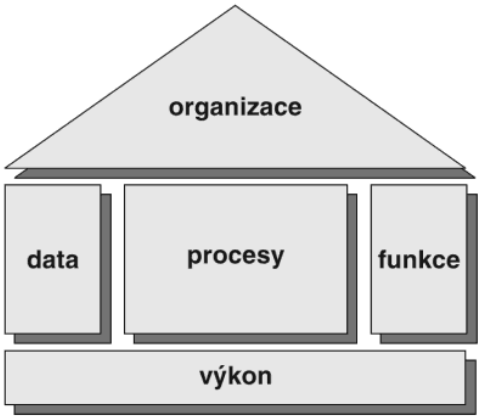
2. Datový pohled - je tvořen stavy a událostmi, stavy jsou měněny událostmi;

3. Funkční pohled - funkce systému a jejich vzájemné vztahy;

4. Procesní pohled - zachycuje vztahy mezi jednotlivými pohledy skrz podnikové procesy, které jsou centrální integrující prvek podniku;

5. Výkonový pohled - nástroj realizace průběžného zlepšování procesů.

[3]




Obrázek 4.1: Pět základních pohledů ARIS [3]

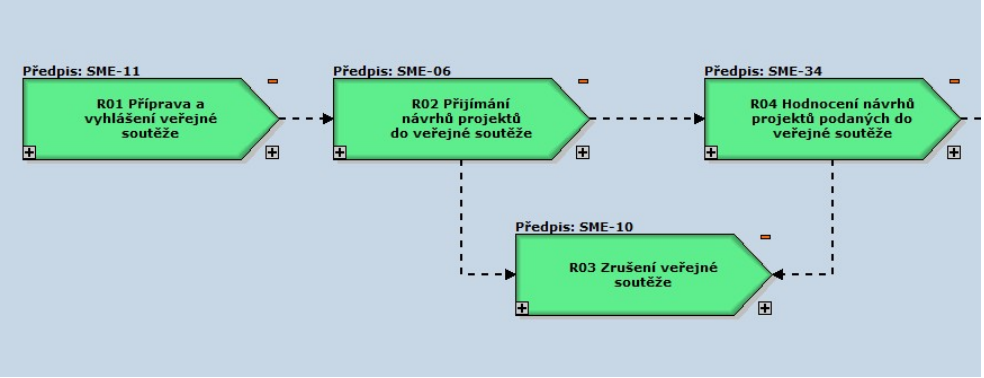
### 4.2.1 Modelování procesů pomocí metody ARIS

Základem všech modelů jsou procesní modely. Procesní model je soustavou všech modelů a obsahuje úrovně:

- přehledová úroveň - hlavní proud a vzájemné návaznosti procesů na sebe;
- úroveň procesu - kontext všech procesů v souvislosti s objekty;
- úroveň podprocesu - základní řazení podprocesů, do nichž se proces rozkládá;
- úroveň činností - detailně modelovány procesy jako struktura činností, stavů a souvisejících objektů a aspektů.

K modelování procesů metodou ARIS se používají následující specializované diagramy:

- diagram Value Added Chain (VAC) pro přehledovou úroveň a řazení procesů (viz příklad na obrázku 4.2);
- diagram hierarchické struktury procesů pro přehledovou úroveň;
- diagram procesu EPC pro kontextovou úroveň popisu;
- diagram eEPC pro úroveň činností (viz obrázek 4.3);
- doplňkový diagram ERM pro popis struktury informací.



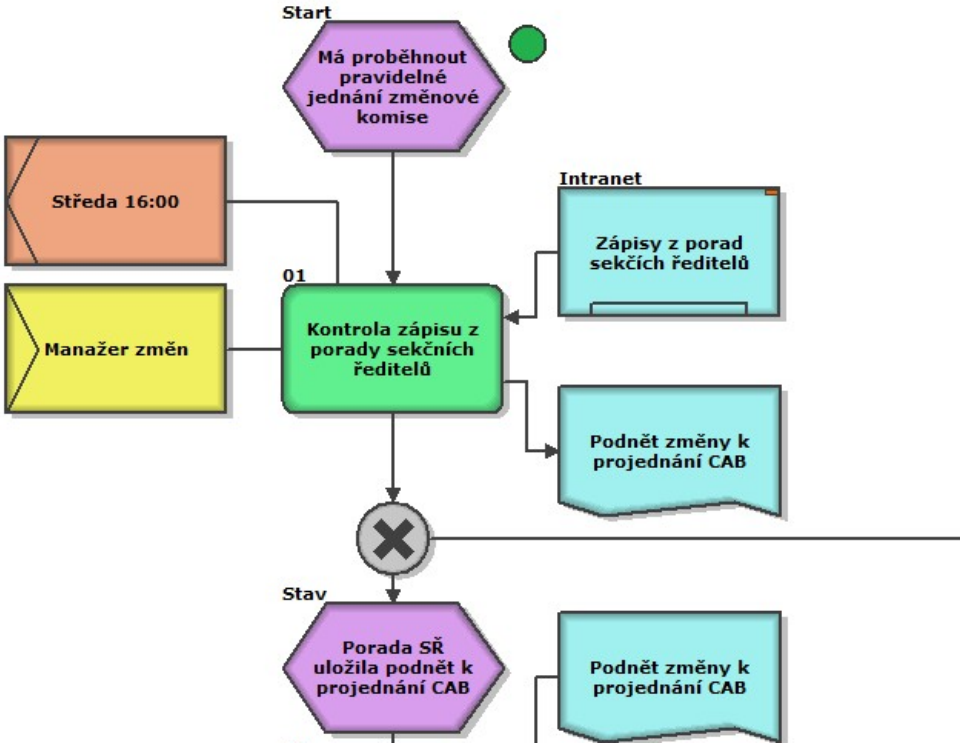

Obrázek 4.2: Příklad VAC diagramu [18]

K popisu procesu používá metoda ARIS základní komponenty:

- událost (event),
- funkce (function),

- data (data),
- zaměstnanec (employee),
- organizační jednotka (organizational unit),
- produkt/služba (product/service).

[3]




Obrázek 4.3: Příklad eEPC diagramu [18]

Modelování a skládání výsledného procesu se řídí následovně:

1. události spouštějí akce, funkce generují události;
2. data jsou zpracovávána ve funkcích;
3. zaměstnanci jsou odpovědní za funkce;
4. zaměstnanci náleží do organizačních jednotek;
5. funkce tvoří výstupy a zpracovávají vstupy.

Modely procesů popisují časově logický vztah funkcí a obsahují zejména tyto prvky: události, funkce, logické operátory (OR, XOR, AND apod.). Událost popisuje vzniklý stav objektu organizace, který dále ovlivňuje nebo řídí průběh podnikového procesu organizace. [3]

### 4.2.2 Procesní landscape

Procesní landscape slouží k určení procesů, které jsou zapojeny do tvoření hodnot pro zákazníky. Jsou to procesy, které jsou spolu spojené a určitým způsobem spolu souvisí. V procesním landscape může být vytvořena hierarchie, která určuje další rozdělení procesů na menší části.

Procesní landscape umožňuje určit procesy, které vytváří pro zákazníka hodnotu a umožňuje určit jejich závislosti. [23]

### 4.2.3 Shrnutí ARIS

Metoda ARIS je velmi ambiciózní, jelikož se snaží o zachycení všech aspektů procesu modelem. Poskytuje nejen pohled na proces, ale i jeho kontextové zařazení a jednotlivé pohledy jsou vzájemně důmyslně propojeny.

ARIS patří dlouhodobě k nejvýznamnějším hráčům na poli modelování a řízení podnikových procesů, a to také díky propracovanosti svého metodického základu. [3] ARIS má dlouhodobou a kvalitativně silnou vazbu na praxi. Procesy podle ARIS nelze popisovat izolovaně, naopak vytváří složité vrstvy a vazby.

## 4.3 SW ARPO

SW ARPO je CASE nástroj s centrálním repository, který je vyvíjen od roku 2006 společností KLUG Solutions. Odvětví CASE nástrojů se rozvíjí v souladu s potřebami procesně řízených organizací. Procesy se stávají explicitními a nejsou závislé na informačních systémech, které procesy pouze podporují. ARPO (Advanced Repository of Process Oriented information) umožňuje modelovat procesy organizace s využitím řady notací. Je v něm umožněno vytvářet kontextové vazby podnikových procesů na jejich okolí, analyzovat procesy, vytvářet sestavy reportů a publikovat model do nejrůznějších formátů. [21]

### 4.3.1 Použité modely

V této kapitole budou popsány dva modely, které budou použity v následujících částech práce. . Těmito modely jsou eEPC (extended Event-drive Process Chain) a VAC (Value Added Chain). V následujících kapitolách je popsáno, k čemu jednotlivé modely slouží a jaké typy objektů se v tomto modelu používají.

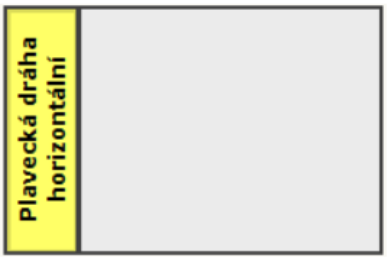
#### 4.3.1.1 Model VAC

Diagram struktury procesů - VAC se obvykle využívá k zaznamenání struktury subprocesů nebo k detailní analýze jednoho procesu. K jednotlivým subprocesům mohou být navázány další modely (v této práci bude využíván eEPC diagram). Analýza nahlíží na proces jako na hodnotový řetězec, nikoliv pouze

jako na objekt. Předmětem zájmu je zde vždy jediný proces. Cílem dekompozice procesu je objevit všechny subprocesy a zařadit je do hodnotového řetězce podle jejich vzájemného uspořádání. [21]

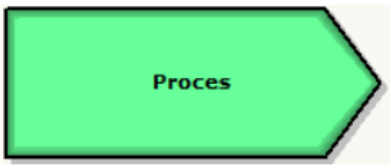
Konstrukce procesního diagramu VAC nahlíží na strukturu jednoho konkrétního procesu a v modelu jsou použity určité typy objektů. Jsou zde uvedeny ty objekty, které jsou použity ve VAC modelech této práce.

**Plavecká dráha**
Plavecké dráhy se používají ke kategorizaci a organizaci aktivit na základě organizačních jednotek nebo procesních rolí. V případě procesního diagramu VAC jsou plavecké dráhy obvykle využívány k zachycení struktury subprocesů jdoucích napříč organizační strukturou.




Obrázek 4.4: VAC - Plavecká dráha [21]

**Proces**
V procesním modelu VAC je jeden dílčí subproces představován objektem. Výchozí filtr metody modelování umožňuje objekt dále hierarchizovat na modely typů VAC, eEPC, BPMN a SIPOC.




Obrázek 4.5: VAC - Proces [21]

#### 4.3.1.2 Model eEPC

Účelem tohoto modelu je zachytit průběh procesu v celé jeho šíři. Rozšířený EPC představuje nejkomplexnější definici podnikového procesu. Takto detailní model může být na druhou stranu kontraproduktivní, neboť se uživatel, s ohledem na velký počet objektů, může v rozsáhlém modelu ztratit. Model eEPC

popisuje dynamickou stránku jediného (sub)procesu a tvoří postup pro vykonavatele procesů.

Objekty, které jsou zde uvedené jsou použité v samotných modelech v další části práce.

**Aktivita**
Aktivita je základním stavebním kamenem eEPC diagramu a vyjadřuje, co má být v rámci toku procesu vykonáno. Jedná se o nejobecnější zápis kroku procesu.


Obrázek 4.6: eEPC - Aktivita [21]

**Událost**
Událost popisuje stav před nebo po vykonání aktivity. Mezi aktivitou a událostí je vazba typu „vytváří“. Událost je výstupem aktivity a vstupní podmínkou následující aktivity. Událost je spojena aktivační vazbou na aktivitu. V modelovací notaci ARPO se rozlišují tři typy událostí:

- spouštěcí,
- stavové a
- koncové.

Každý proces v eEPC musí začínat a končit událostí.


Obrázek 4.7: eEPC - Událost [21]

**Logické operandy AND, OR, XOR**
Logické spojky mají v popisu procesu dvojí význam. Mohou rozdělovat nebo spojovat tok činností. V prvním případě má spojka jeden vstup a minimálně

dva výstupy. V druhém případě má spojka nejméně 2 vstupy a právě jeden výstup.

AND-split má právě jeden vstup a minimálně dva výstupy a rozděluje tok procesu na paralelně probíhající cesty. AND-join tyto rozdělené cesty zase spojuje v jednu.

Obrázek 4.8: eEPC - Logický operand AND [21]

OR-split rozpojuje tok procesu do jedné z možných cest. Cesty mohou být vybrány všechny a OR-join tyto cesty opět spojuje v jednu.

Obrázek 4.9: eEPC - Logický operand OR [21]

XOR-split rozpojuje tok procesu do jedné z možných cest a analogicky XOR-join tyto vzájemně se vylučující prvky spojuje zpět do jednoho toku.

Obrázek 4.10: eEPC - Logický operand XOR [21]

**Procesní role**

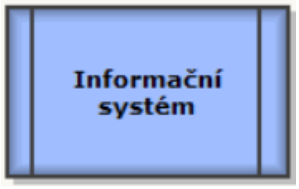
Procesní role je charakterizována schopností porozumění části procesu a jeho vykonávání. V diagramu eEPC se používá k zaznamenání odpovědnosti za realizaci kroku procesu, případně popisu dalších logických vazeb aktivity.


Obrázek 4.11: eEPC - Procesní role [21]

**Dokument**
Objekt, který lze využít k zaznamenání elektronických/fyzických dokumentů a dalších entit v podobě vstupů/výstupů. Slouží k zachycení kontextové vazby.


Obrázek 4.12: eEPC - Dokument [21]

**Informační systém**
K zaznamenání aplikačního pokrytí popisovaného kroku procesu může být použit objekt Informační systém.




Obrázek 4.13: eEPC - Informační systém [21]

**Software**
Slouží k zachycení kontextové vazby, aktivity jsou podporovány konkrétní aplikací.


Obrázek 4.14: eEPC - Software [21]

**Rozhraní procesu**
Tvoří přechodové spojky mezi jednotlivými procesy a je důležitou vlastností procesního modelu. V ideálním světě jsou rozhraní procesů popisována pomocí SLA.


Obrázek 4.15: eEPC - Rozhraní procesu [21]

Kapitola 5

# Regulatorní požadavky

Technologická agentura České republiky se jako každá jiná organizace musí řídit legislativou ČR a nesmí tedy porušovat zákon. V této kapitole budou uvedeny zákony a jejich dopad pro TA ČR. Legislativa a zákony, které se přímo týkají TA ČR byly konzultovány s právním oddělením, a zákony, které se týkají bezpečnosti informací byly konzultovány s bezpečnostním ředitelem TA ČR.

Zákony vytvářejí hranice, které TA ČR musí dodržovat a v dalších kapitolách této práce jsou popsány postupy a opatření, která s těmito zákony nesmí být v rozporu.

Požadavky, které jsou uvedeny Zákonem č. 181/2004 Sb., o kybernetické bezpečnosti a Vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti musí být naplněny a jsou shrnuty v této kapitole.

Jelikož se tato práce zabývá procesním řízením a úpravou procesů s ohledem na bezpečnost informací, byly vybrány tyto zákony, kterými je nezbytně nutné se zabývat při nastavování procesů a bezpečnosti informací:

- Nařízení Evropského parlamentu a Rady (EU) 2016/679. - General Data Protection Regulation (GDPR);
  - Zákon č. 110/2019 Sb. - Zákon o zpracování osobních údajů.
- Zákon č. 130/2002 Sb. - Zákon o podpoře výzkumu a vývoje z veřejných prostředků;
- Zákon č. 134/2002 Sb. - Zákon o zadávání veřejných zakázek;
- Zákon č. 159/2006 Sb. - Zákon o střetu zájmů;
- Zákon č. 181/2014 Sb. - Zákon o kybernetické bezpečnosti;
  - Vyhláška č. 82/2018 Sb. - Vyhláška o kybernetické bezpečnosti.
- Zákon č. 219/2000 Sb. - Zákon o majetku České republiky;

- Zákon č. 300/2008 Sb. - Zákon o elektronických úkonech a autorizované konverzi dokumentů;

## 5.1 Nařízení Evropského parlamentu a Rady (EU) 2016/679. - General Data Protection Regulation GDPR

Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES neboli zkráceně GDPR představuje právní ochranu občanů proti neoprávněnému zacházení s jejich daty a osobními údaji. [24]

### 5.1.1 Správce osobních údajů

Správce určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá. Správce zpracovává osobní údaje pro účely vyplývající z jeho činnosti. [24]

### 5.1.2 Zpracovatel osobních údajů

Zpracovatel je pověřen správcem, aby pro něj prováděl s osobními údaji zpracovatelské operace. Zpracovatel se od správce liší, že s údaji provádí jen takové operace, kterými jej správce pověřil. [24]

### 5.1.3 Zpracování údajů a související části nařízení

Osobní údaje, i když jsou dobrovolně subjektem zveřejněné, nelze zpracovávat. Veřejnost údajů nikdy neznamená, že je možné tyto údaje dále bezmezně zpracovávat. [24]

Subjekty mají právo být zapomenuty, tedy právo na výmaz z databáze správce, pokud je splněna alespoň jedna z následujících podmínek:

- osobní údaje nejsou již potřebné pro účely, pro které byly shromážděny;
- subjekt údajů odvolá souhlas se zpracováním a neexistuje další důvod pro zpracování;
- subjekt vznese námitku proti zpracování a neexistují jiné převládající oprávněné důvody pro zpracování;
- protiprávní zpracování údajů.

[24]

Správce musí být schopen doložit, že zpracování osobních údajů je v souladu s Obecným nařízením. Každý správce je tak povinen přijmout adekvátní bezpečnostní opatření.

### 5.1.4 Příprava na GDPR

Nařízení GDPR se týká každého, kdo zpracovává v jakékoliv formě osobní data subjektů údajů. Nerozlišují se nosiče, na kterých jsou data uložena. GDPR se vztahuje jak na elektronické, tak na fyzické nosiče dat.

Při zavádění opatření se musí správce zamyslet nad následujícími body a zavést taková opatření, aby splňoval požadavky následujících bodů:

- spravedlivé získání souhlasu se zpracováním osobních údajů;
- specifikace účelu;
- používání a zvěřejňování informací;
- bezpečnost;
- přiměřenost, relevantnost a nezbytný obsah;
- přesnost a aktuálnost;
- doba uchovávání;
- právo na přístup;
- registrace;
- školení a vzdělávání;
- koordinace a shoda;

### 5.1.5 Zásady a principy GDPR

Základní principy GDPR jsou uvedeny v následujících šesti bodech:

- zákonnost, korektnost a transparentnost;
- účelové omezení (omezení účelem);
- minimalizace údajů (minimalizace dat);
- přesnost;
- omezení uložení (omezení uchovávání);
- integrita a důvěrnost.

### 5.1.6 Vztah GDPR a ISO normy 27001

Norma ISO 27001 je rámcovou normou pro ochranu a bezpečnost dat. GDPR hovoří o osobních datech jako o kritické informaci a všechny organizace mají povinnost je chránit. ISO 27001 nepokrývá všechny požadavky GDPR, nicméně implementace normy ISO 27001 zahrnuje většinu požadavků vyplývajících z GDPR. Některá opatření by ale měla být upravena tak, aby obsahovala osobní údaje v rámci systému řízení bezpečnosti informací (ISMS). Implementace ISMS v souladu s normou ISO 27001 může být chápána jako jistý krok vedoucí k dosažení souladu s GDPR. [24]

## 5.2 Zákon č. 110/2019 Sb., o zpracování osobních údajů

V této kapitole jsou uvedeny informace dle [25].

Účinností tohoto zákona od 24. 4. 2019 došlo ke zrušení předešlého zákona 101/2000 Sb., o ochraně osobních údajů. Adaptačním zákonem k GDPR se rozumí právě tento zákon vydaný českými zákonodárci.

Tento zákon rozvádí nebo upřesňuje již zavedená ustanovení GDPR. Zákonodárce ale využil i možnost odchýlit se od GDPR a stanovuje určité výjimky. Jedním z příkladů je stanovení hranice pro způsobilost dítěte se zpracováním osobních údajů, která je stanovena na 15 let. [26, 27]

Zákon musí být dodržen v plné míře, ale pro účely zavádění procesů s ohledem na bezpečnost informací byly vybrány nejdůležitější paragrafy zákona, na které se nesmí zapomenout při plánování a implementaci opatření, která budou podporovat bezpečnost informací.

Podle § 14 musí být jmenován pověřenec pro ochranu osobních údajů. Tento pověřenec je v Technologické agentuře jmenován. Jeho funkce musí být specifikována a musí být určeny jeho odpovědnosti a povinnosti.

Pokud jsou sbírány data pro statistické účely, musí být, podle § 16, splněny určité podmínky, aby bylo zákonu vyhověno. Je nutné, aby byly uchovávány záznamy o tom, kdo s daty pracuje. Při práci s osobními údaji pro statistické účely musí být zavedena určitá opatření s ohledem na povahu těchto dat. Některá z opatření mohou být:

- pseudonymizace dat,
- šifrování dat,
- princip CIA,
- zvláštní omezení přenosu dat do třetí země atd.

Podle § 25 smí být data, která umožňují identifikaci osoby, uchovávána pouze na dobu takovou, která je nezbytná k dosažení účelů jejich zpracování.

Tento účel musí být stanoven správcem údajů. § 32 Zákona pojednává o povinnostech spravujícího orgánu o osobních datech. Má povinnost:

- chránit osobní údaje,
- omezit nepřiměřené zpracování osobních údajů,
- nezveřejňovat automaticky údaje,
- vést dokumentaci o opatřeních o ochraně osobních údajů,
- vést přehledy, které obsahují:
  - název a kontaktní údaje správce,
  - účel zpracování údajů,
  - kategorie příjemců,
  - přenos údajů do třetích zemí,
  - lhůty pro výmaz nebo přezkum potřebnosti údajů,
  - obecný popis zabezpečení údajů.

Pokud spravující orgán provádí automatizované pořizování záznamů, musí podle § 36 Zákona uchovávat záznamy o vložení, úpravě, kombinování, sdělení údajů apod. Tyto záznamy musí uchovávat po dobu tří let.

Měl by být posouzen vliv na ochranu osobních údajů tak, jak ukládá § 37 Zákona. Pokud některé údaje mohou vést k vysokému riziku neoprávněného zásahu do práv a svobod, musí spravující orgán vypracovat popis, jak bude s údaji naloženo. Musí se posoudit riziko a musí být vypracována opatření ke zmenšení tohoto rizika.

Zákon stanovuje podle § 40 požadavek na zabezpečení osobních údajů. Toto zabezpečení zahrnuje omezení přístupů, přenosu a změny. Musí být zajištěna obnovitelnost osobních údajů a bezpečnost a spolehlivost informačního systému. Pokud se vyskytnou chyby, musí být hlášeny.

Pokud dojde k porušení zabezpečení osobních údajů, měl by se tento fakt oznamovat Národnímu úřadu pro kybernetickou a informační bezpečnost podle § 41 Zákona. Toto platí, pokud je velké riziko zásahu do práv a svobod subjektu údajů.

## 5.3 Zákon č. 130/2002 Sb., o podpoře výzkumu a vývoje z veřejných prostředků

V této kapitole jsou uvedeny informace dle [28].

Zákonem o podpoře výzkumu a vývoje z veřejných prostředků bylo ustanovené založení Technologické agentury České republiky. Zákon se zabývá, jak

už z názvu plyne, podporou výzkumu z veřejných prostředků. Jsou zde uvedeny obecné informace, jak mají žadatelé o podporu žádat o finance a jakým způsobem musí být vyhlašovány veřejné soutěže o podporu. Z toho zákona byly vybrány důležité paragrafy, které se dotýkají bezpečnosti informací a souvisí s procesním rámcem organizace.

Poskytování podpory nemůže být dle § 7 poskytnuto osobě, která byla pravomocně odsouzena pro trestný čin, jehož skutková podstata souvisí s předmětem jejího podnikání, nebo pro trestný čin hospodářský nebo trestný čin proti majetku. Dále nesmí být poskytnuta podpora podniku v obtížích. Nemůže se podporovat příjemce, kterému byl vystaven inkasní příkaz.

Dle § 12 může být podpora poskytnuta příjemci pouze na základě poskytnutí pravdivých informací. § 12 souvisí s ochranou osobních údajů, jak je uvedeno v kapitole 5.1.

§ 13 uvádí požadavky, které je nutné plnit. Tyto požadavky souvisí s bezpečností informací a procesy, jelikož je nutné, aby data byla sbírána za účelem k tomu určenému. TA ČR má povinnost provádět kontrolu cílů projektu. Pokud je trvání projektu, pro který se podpora žádá, delší než 2 roky, je uložena povinnost tento projekt kontrolovat ještě jednou v průběhu řešení projektu. Je uložena povinnost provádět kontrolu u příjemců nejméně u 5 % objemu poskytnuté podpory v daném roce. Projekt musí být na závěr vyhodnocen. Musí být vyhodnoceno plnění cílů. Musí být vyhodnocen vztah cílů a výsledků a tato skutečnost musí být dále postoupena do Informačního systému Výzkumu, Vývoje a Inovací (IS VaVai).

Dle § 24 může být zrušena vyhlášena veřejná soutěž. Je tedy nutné z pohledu TA ČR se na takovou skutečnost připravit a řešit v rámci procesního řízení, jak se s takovou situací vypořádat.

## 5.4 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Informace uvedené v této kapitole jsou dle [29].

Zákon o kybernetické bezpečnosti je jedním z hlavních zákonů, které musí organizace řešit, aby měla správně vyřešenou informační bezpečnost.

Důležité je určit, do jaké kategorie správce nebo poskytovatel služby spadá, od toho se dále odvíjí povinnosti uvedené v dalších paragrafech. Jednotlivé kategorie jsou uvedeny v § 3 Zákona. V tomto paragrafu se také píše, kterým osobám se ukládají povinnosti v oblasti kybernetické bezpečnosti.

Dle § 4 Zákona jsou subjekty povinny zavést a provádět bezpečnostní opatření s ohledem na § 3. Musí zohledňovat bezpečnostní požadavky ve smlouvách s dodavateli. Požadavkem zákona je zavést opatření, která zohledňují zajištění bezpečnosti sítě komunikace, řízení kontinuity činností, monitorování, audity, testování a soulad s mezinárodními předpisy.

Dle § 8 má subjekt podle § 3 povinnost bezodkladně hlásit kybernetické incidenty příslušnému úřadu. Činnost vládního CERT, na který se kybernetické incidenty hlásí, zajišťuje Národní centrum kybernetické bezpečnosti (NCKB), které je výkonnou sekcí Národního úřadu pro kybernetickou a informační bezpečnost(NÚKIB). [30]

Dle § 11 mají subjekty povinnost vytvářet opatření. Těmito opatřeními se rozumí úkony, jichž je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu.

Dle § 23 Úřad vykonává kontrolu v oblasti kybernetické bezpečnosti. Pokud existuje důvodné podezření, že subjekt neplní svoje povinnosti stanovené tímto zákone, provede na něj Úřad kontrolu.

Dle § 24 může Úřad zakázat provoz systému subjektu, pokud se zjistí pochybení. Zákaz může trvat po dobu, než je problém opraven.

Zákon byl dále v roce 2018 rozšířen o vyhlášku č. 82/2018 Sb., o kybernetické bezpečnosti.

### 5.4.1 Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti

Tato kapitola vychází z [31].

Vyhláška č. 82/2018 Sb. významně ovlivňuje a rozšiřuje povinnosti osob a orgánů v některých oblastech kybernetické bezpečnosti.

Konkrétně se jedná o:

- obsah a strukturu bezpečnostní dokumentace;
- management rizik, včetně řízení aktiv;
- obsah a rozsah bezpečnostních opatření;
- management kybernetických bezpečnostních incidentů atd.

Vyhláška o kybernetické bezpečnosti dle [32] byla uváděna jako vycházející ze standardu ISO/IEC 27001. Toto tvrzení je zavádějící a je podstatný rozdíl mezi vyhláškou a normou ISO. Norma ISO/IEC 27001 je univerzální a je aplikovatelná na jakoukoliv organizaci. Dle [32] je rozdíl v tom, že je na organizaci samotné, jak opatření z normy ISO/IEC 27001 aplikuje, naproti tomu vyhláška není obecným doporučením, ale závazným předpisem, který ukládá, jak má organizace příslušná aktiva chránit.

Pokud by autoři Zákonu o kybernetické bezpečnosti učinili ISO/IEC 27001 závaznou jejím uvedením v zákoně, mohli by způsobit řadu problémů, které vychází z volnosti normy, nejednoznačnosti doporučení a z autorských práv a nutnosti pořízení normy. [32]

Systém ISTA, který TAČR spravuje a poskytuje jako službu je systémem, který v současnosti není kritickým informačním systémem ani významným informačním systémem. [33] Informační systém ISTA je veden jako ISVS. [34]

Do budoucna je ale možné, že s přibývajícím počtem poskytovaných služeb a zvyšujícím počtem vedených osob v systému ISTA bude tento systém jako významný informační systém uváděn. Z hlediska legislativy je nutné připravit se na tuto skutečnost.

#### 5.4.1.1 Pojmy k následující kapitole

**Information System Management System**
ISMS neboli systém řízení bezpečnosti informací se sestává z politik, postupů, směrnic a příslušných zdrojů a činností, aby zajistila ochranu informačních aktiv. ISMS představuje systematický přístup k ustavení, implementaci, provozování, monitorování, přezkoumávání, udržování a zlepšování bezpečnosti informací organizace tak, aby byly dosaženy její cíle. [35]

**Princip CIA**
Princip CIA je tvořen třemi základními prvky:

- Confidentiality - Pouze autorizovaní uživatelé a autorizované procesy by měly mít přístup k zobrazení nebo úpravě dat;
- Integrity - Data by měla být úplná a správná. Musí být zabráněná úmyslná nebo neúmyslná manipulace s daty;
- Availability - Oprávnění lidé k manipulaci s daty by k nim měli mít přístup, kdy potřebují.

Tyto tři body tvoří tzv. CIA triádu. Tento model může být organizací využit k bezpečné správě dat. [36]

**Service Continuity Management**
IT Service Continuity Management řídí rizika, která by mohla vážně ohrozit chod IT služeb. SCM zajišťuje, aby poskytovatel služeb byl vždy schopen zajistit minimální domluvenou úroveň služby snižováním rizik hrozby a plánováním obnovení poskytovaných služeb, pokud služba vypadne. [37]

#### 5.4.1.2 Požadavky Vyhlášky č. 82/2018 Sb.

Dle § 3 je nutné stanovit rozsah, jehož se bezpečnost informací týká. Poté se jedná o samotné zavedení systému řízení bezpečnosti informací (ISMS - Information Security Management System).

§ 4 vyhlášky určuje nutnost řízení aktiv. Musí být stanoveny metodiky, které se týkají řízení aktiv. Na základě principu CIA se musí určit primární

aktiva. Jak se aktiva ohodnotí je uvedeno v příloze č. 1 vyhlášky. Dále je v § 4 uvedeno, jakým způsobem se s aktivy nakládá.

Podle § 5 vyhlášky je nutné řízení rizik. Řízení rizik musí mít stanovenou metodiku, jakým způsobem se rizika mají řídit. Musí být identifikovány hrozby a zranitelnosti. Rizika se musí pravidelně hodnotit, posuzovat a upravovat dle potřeb. Musí se zohledňovat významné změny v systémech. Pokud riziko nastane, musí se dokumentovat, jak k němu došlo a jak s ním dále naložit.

Dle § 6 vyhlášky musí být zajištěna organizační bezpečnost. V organizaci musí být zajištěna komunikace povinností v souladu s bezpečností. Musí být zajištěna podpora ISMS a jeho neustálý rozvoj napříč celou organizací.

§ 7 vyhlášky určuje povinnost bezpečnostních rolí v organizaci. Jedná se o manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti, garanta aktiva a auditora kybernetické bezpečnosti. Zavedení těchto rolí v organizaci se řídí dle § 6 vyhlášky odst. 3-7.

§ 8 určuje povinnost řídit dodavatele. Musí se stanovit významní dodavatelé a musí být vedena jejich evidence v rámci organizace. § 8 stanovuje nutnost řízení rizik spojených s dodavateli, zavádění bezpečnostních opatření a jejich kontrolu.

Dle § 9 musí být pro lidské zdroje v organizaci vytvořeny plány rozvoje bezpečnostního povědomí. Taktéž musí být zavedena pravidelná školení pro všechny osoby v organizaci. § 9 zahrnuje kontrolu dodržování bezpečnostní politiky a určuje pravidla při jejím porušení.

§ 10 vyhlášky určuje povinnost řízení provozu a komunikace. Jsou stanoveny pravidla pro zajištění bezpečného provozu informačního systému. Povinná osoba tyto pravidla aktualizuje v souvislosti s plánovanými změnami. Musí být odděleno testovací, vývojové a produkční prostředí.

§ 11 stanovuje povinnost řízení bezpečnosti pro změny. Změny musí být přezkoumávány a dokumentovány. Musí být dokumentována rizika a dále případně aktualizována bezpečnostní politika a dokumentace.

§ 12 zahrnuje pravidla pro řízení přístupů. Přístupy musí být řízeny na základě politiky vedené organizací. Řízení přístupů zahrnuje:

- opatření pro přístup a ochranu údajů,
- identifikátory a přístupová práva,
- opatření pro bezpečné používání zařízení,
- odebírání a přidělování přístupových opatření atd.

Dle § 13 jsou řízena rizika, významné změny, vývoj, údržba. Je zde uvedena bezpečnost testovacího prostředí a bezpečnost použitých dat. Musí být prováděny bezpečnostní testy před uvedením změny do produkčního prostředí.

§ 14 určuje povinnost zaznamenávat bezpečnostní incidenty a události. Musí být vytvořeny postupy pro vyhodnocování událostí a zvládání incidentů.

Stejně tak musí být vytvořeny postupy pro sběr, získání a uchování dat o událostech. Taktéž musí být zajištěno vytváření opatření na základě incidentů.

Dle § 15 musí být zajištěn Service Continuity Management (BCM). Musí být stanovena politika pro BCM, havarijní plány, testování a analýza.

§ 16 určuje povinnost provádění auditu kybernetické bezpečnosti. Perioda provádění auditu se liší dle rozdělení podle § 3 Zákona č. 181/2014 Sb.

§ 17 stanovuje povinnost fyzické bezpečnosti, jež se týká omezení přístupu do budovy a oblastí, ve kterých jsou uchovávány a zpracovávány informace.

Dle § 18 se musí zajistit bezpečnost komunikačních sítí v rámci organizace. Jsou zde uvedena pravidla pro zajištění ochrany komunikační sítě.

§ 19 určuje pravidla pro správu a ověřování identit. Zahrnuje ověřování, řízení počtu přístupů, odolnost proti odcizení.

Dle § 20 povinná osoba řídí přístupová oprávnění do systému v centralizovaném nástroji.

Musí být využíváno nástrojů pro automatickou ochranu stanic, telefonů, serverů, datových úložišť apod. jak ukládá § 21. Tato ochrana je proti škodlivému kódu.

Dle § 22 musí být zaznamenávány události v informačních systémech. Jedná se o všechny přístupy do systému, připojení nových zařízení do komunikační sítě, všechny změny provedené v informačních systémech a uživatelů, kteří tyto změny provádí.

§ 23 udává povinnost detekce kybernetických bezpečnostních událostí. Zejména se jedná o ověřování a kontrolu přenášených dat a blokování nežádoucí komunikace.

Dle § 24 musí být aplikace bezpečná. Před uvedením do provozu musí být provedeny penetrační testy. Aplikace musí být zajištěna před neoprávněnou činností a poptřením provedených činností.

§ 26 udává povinnost používání aktuálních kryptografických prostředků, algoritmů a klíčů. Je zde uvedeno i používání systému správy klíčů a certifikátů.

§ 27 hovoří o zajišťování úrovně dostupnosti informací, což se týká Service availability managementu.

§ 29 udává, že na poskytovatele digitální služby podle § 3 písmena h) Zákona č. 181/2014 Sb. se ustanovení § 3 až § 28 vyhlášky nepoužijí. Proto je důležité určit, do jaké kategorie systém spadá.

§ 30 stanovuje zavedení bezpečnostní politiky a dokumentace. Tato musí být pravidelně přezkoumávána a aktualizována. Politika musí být komunikována, řízena, chráněna a musí být přehledná a úplná.

§ 31 hovoří o bezpečnostním incidentu a o jeho kategorizaci.

Dle § 32 se musí bezpečnostní incidenty hlásit národnímu CERT, jehož činnost zajišťuje Národní centrum kybernetické bezpečnosti (NCKB). [30] Hlášení bezpečnostního incidentu musí mít náležitosti, které specifikuje § 32.

V příloze Vyhlášky 82/2018 Sb. jsou uvedeny parametry nastavení jednotlivých paragrafů vyhlášky. Je zde uvedeno:

- hodnocení aktiv;
- hodnocení rizik;
- zranitelnosti a hrozby;
- likvidace dat;
- obsah bezpečnostní politiky;
- bezpečnostní role;
- bezpečnostní opatření pro smluvní vztahy s dodavateli.

## 5.5 Zákon č. 219/2000 Sb., o majetku České republiky

Tato kapitola vychází z [38].

Zákon o majetku České republiky a jejím vystupování v právních vztazích určuje, jak s majetkem ČR nakládat. Jelikož je Technologická agentura České republiky organizační složkou státu [14] a aktivum je pojem, který označuje majetek, je nutné se zabývat bezpečností majetku. V zákoně je uvedena povinnost inventarizace majetku a jeho účelné využívání. Položky majetku jsou aktivy a je nutné s nimi nakládat jako s každým jiným aktivem.

## 5.6 Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

Zákon o elektronických úkonech a autorizované konverzi dokumentů pojednává zejména o způsobu využití datových schránek. V TA ČR jsou některé právní úkony konány prostřednictvím datové schránky.

V rámci bezpečnosti § 8 pojednává o oprávněných osobách k přístupu do datové schránky. Pokud hrozí nebezpečí zneužití datové schránky, musí se neprodleně uvědomit ministerstvo. Taktéž je se zde uvádí pokyny k využívání datové schránky. Ta se musí využívat tak, aby neohrožovala informační systém datových schránek.

## 5.7 Shrnutí regulatorních požadavků

Při vytváření a úpravě procesů se musí nejprve označit požadavky zákona, které se daného procesu týkají. Tyto požadavky musí být splněny a na tomto základě se může proces stavět. Vyhláška o kybernetické bezpečnosti určuje jasné meze a jasná pravidla, jak se mají požadavky na kybernetickou bezpečnost splnit. Každá organizace je ale jedinečná a neexistuje unifikovaná „kuchařka“, jež by udávala jasný postup, jak dosáhnout souladu se zákonem.

Hlavní pilíře, o které se opírám při tvorbě a úpravě procesů v souvislosti s bezpečností informací jsou:

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti;
- Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti;
- GDPR.

Kapitola 6

# Řízení služeb informačních technologií a bezpečnosti informací

Ve světě zcela založeném na informačních technologiích je schopnost efektivně dosahovat cílů založena na fungování informačních a komunikačních technologií a efektivnosti řízení služeb informačních technologií při akceptovatelných nákladech a rychlosti zavádění těchto služeb. [39]

Zároveň k řízení služeb informačních technologií neodmyslitelně patří i bezpečnost informací. Jelikož jsou informační technologie pro většinu organizací naprosto neodmyslitelnou složkou a informace a know-how bývá v organizaci tím nejcennějším, vybavuje se nám pojem informační bezpečnost. Chceme mít informace, které potřebujeme, ve stavu, aby se s nimi dalo pracovat a chráněné, aby se nedostaly k někomu, kdo je nemá vidět. [40, 41]

Dnes je k dispozici mnoho obranných a ochranných nástrojů. Existuje řada standardů, které se zabývají problematikou bezpečnosti informací. K nejčastějším příčinám úniku dat patří lidský faktor, tzn. ztráta pracovního zařízení (telefony, počítače), nedbalost, špatné zacházení se zařízení, útoky při home-office atd. [42]

Aby se těmto únikům efektivně zabránilo, je možné vytvořit si sadu pravidel, podle vlastního uvážení, a tyto pravidla dodržovat. Lepším řešením je ale následovat standardy, které vycházejí z best-practices a tyto upravit a aplikovat na svoji organizaci. [40]

Mezi tyto standary a best-practices patří i tři následující. Jsou jimi ITIL (IT Infrastructure Library), norma ISO/IEC 20000 a ISO/IEC 27000.

## 6.1 ITIL

Služby se od rozvoje informačních technologií stále více rozvíjí a ITIL je nejrozšířenějším přístupem k IT Service Management (ITSM). ITIL poskytuje ucelenou sadu osvědčených postupů, které pochází jak od veřejnosti, tak i z privátního sektoru. [43]

ITIL se v praxi využívá právě pro nastavení a řízení IT procesů. ITIL je některými nazýván standard. ITIL není standardem, ale frameworkem. [44] Organizace nejsou povinny implementovat každý proces podle ITIL nebo ITIL perfektně následovat. ITIL organizacím poskytuje pomoc při implementaci ITSM. [44]

Nynější verze ITIL v4 je vylepšená verze ITIL v3 a obsahuje vylepšené strategické elementy, které poskytují lepší soulad řízení IT služeb s požadavky byznysu. Procesy ITIL v3 jsou nyní v novější verzi nazývány praktikami. [45]

Z důvodu přístupu pouze ke starší verzi jsem se rozhodl použít ITIL v3. ITIL v3 je stále popisován jako relevantní a je vyžadován globálně tisícovkami provozovatelů IT služeb. [45]

ITIL v3 zahrnuje pět klíčových knih, které pokrývají všechny fáze životního cyklu IT služeb (viz obrázek 6.1):

- Strategie služeb (Service strategy),
- Provoz služeb (Service operation),
- Přechod služeb (Service transition),
- Návrh služeb (Service design),
- Neustálé zlepšování služeb (Continual service improvement).

[46]

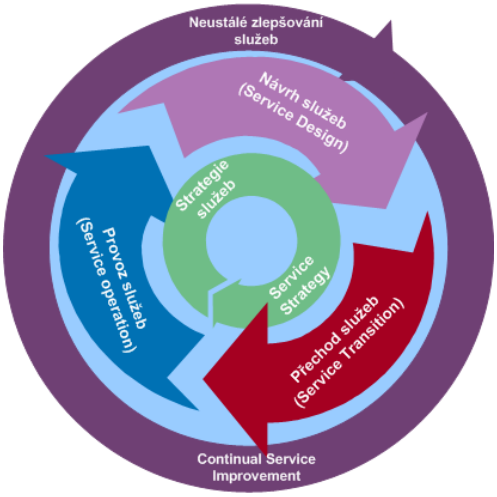
### 6.1.1 Service strategy (Strategie služeb)

Strategie služeb je prvním krokem v cyklu služeb ITIL. Jak je vidět na obrázku 6.1, Strategie služeb zaujímá centrální poizici v základním schématu ITIL. [47]

Strategie služeb je plán, který je vytvořen organizací, aby dosáhla svých cílů. Základním principem je určení konkurence na trhu a zavedení základních pravidel a postupů, jak poskytovat lepší služby než ostatní. Organizace musí poskytovat zákazníkům co nejlepší hodnotu. [48]

Strategie služeb se zabývá věcmi, které jsou zabjímavé pro CIO (Chief Information Officer). Zaměřuje se na:

- rozvoj trhu služeb,
- typy poskytovatelů služeb,




Obrázek 6.1: Fáze životního cyklu IT služeb podle ITIL v3 [46]

- portfolio služeb,
- finance v řízení služeb,
- vztahy s byznysem.

Strategie říká organizaci, jak se zaměřit na organizaci z pohledu shora a jak vnímat služby z pohledu nákladů, rizik a výkonnosti.

Strategie služeb říká *„proč“*, ne *„jak“*. [48]

### 6.1.2 Service operation (Provoz služeb)

Provoz služeb se série ITIL v3 poskytuje best-practices, jak udržovat stabilitu při poskytování IT služeb a jak dosáhnout požadované úrovně poskytovaných služeb. Základními cíli provozu služeb jsou:

- minimalizovat nedostupnost služeb při každodenních aktivitách;
- zajistit, že služby jsou poskytovány podle sjednaných pravidel;
- přijmout opatření a zavést best-practices, aby organizace neztrácela na uzavřených smlouvách;
- redukovat incidenty a problémy organizace;
- podpora uživatelům v užívání služby.

[49]

#### 6.1.2.1 Procesy provozu služeb

Do procesů provozu a služeb podle ITIL patří pět následujících:

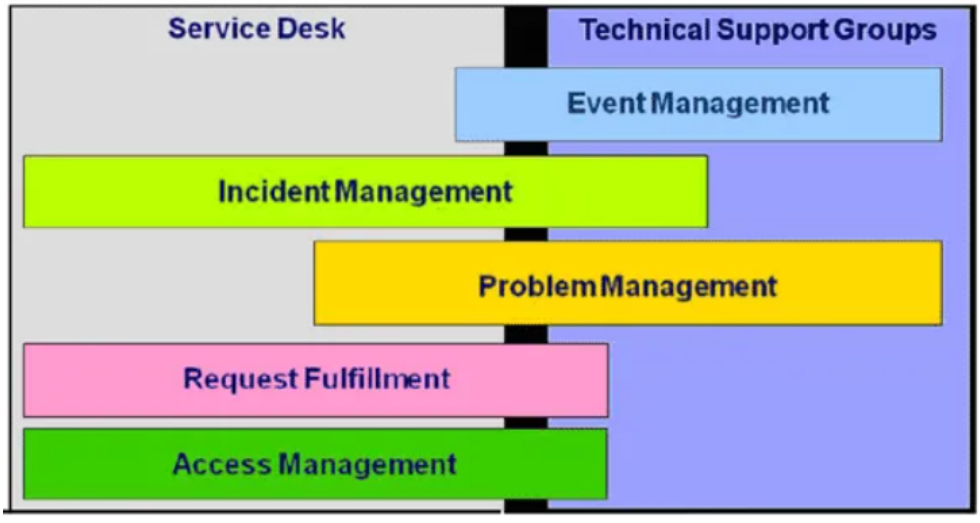
- Event Management (Správa událostí) - neustálé sledování služeb, událostí a navrhování kroků dalšího postupu;
- Incident Management (Řízení incidentů) - proces, který je odpovědný za co nejrychlejší obnovení provozu IT služby;
- Request Fullfillment (Plnění požadavků) - proces, který je odpovědný za potvrzování a zpracování požadavků od zákazníků;
- Problem Management (Řešení problémů) - proces, který se zabývá nalezením příčin problémů.
- Access Management (Řízení přístupů) - proces, který slouží k udělení oprávnění uživatelům užívat službu.

[49]

#### 6.1.2.2 Zodpovědnost funkčních skupin vůči procesům

Zodpovědnosti za jednotlivé procesy provozu služeb jsou přiřazovány dvěma funkčním skupinám. Jednou z nich je Service Desk a druhou z nich je skupina technické podpory, která zahrnuje technické, aplikační a operativní řízení.

Na obrázku 6.2 je znázorněno, jaký proces patří do jaké funkční skupiny, aby mohl být efektivně řízen.




Obrázek 6.2: Zodpovědnosti funkčních skupin za procesy provozu služeb [49]

### 6.1.3 Service transition (Přechod služeb)

Tato část ITIL v3 poskytuje postupy a best-practices jak doručit nové nebo upravené služby požadované byznysem, do živého/produkčního prostředí. Přechod služeb poskytuje typicky spíše řízení IT projektu, než Business as Usual (BAU).

Přechod služeb řídí přechod nových nebo změněných služeb z fáze Service design (návrhu služeb) do Service operation (provozu služeb). [50]

#### 6.1.3.1 Cíle a účel ITIL Service transition

Hlavními cíli jsou:

- řízení přechodu nových a změněných služeb do živého/produkčního prostředí;
- vylepšení schopnosti poskytovatele služeb nakládat s velkým množstvím změn a vydáním nových nebo změněných služeb;
- řízení změn, jako změny dodavatelů, změny možností služeb apod.;
- vytvoření postupů při opakujících se akcích v organizaci tak, aby bylo pro organizaci jednoduché a efektivní vydávání nových a změněných služeb do živého/produkčního nebo testovacího prostředí.

[50]

#### 6.1.3.2 Procesy přechodu služeb

Mezi procesy přechodu služeb patří sedm procesů:

- Project Management (řízení projektů) - proces, který se zabývá plánováním a koordinováním zdrojů pro nasazení v rámci předem definovaných nákladů, času a kvality;
- Change Management (řízení změn) - proces, který se zabývá životním cyklem všech změn. Umožňuje organizaci zavedení přínosných změn a předcházení změnám, které nejsou autorizované;
- Change Evaluation (vyhodnocení změn) - proces, který se využívá k evaluaci velkých změn a je volán procesem řízení změn, aby schválil požadovanou velkou změnu;
- Service asset a Configuration Management (Aktiva služby a řízení konfigurace) - proces, který se zabývá vztahem konfiguračních jednotek, které jsou potřeba pro poskytování IT služeb;

- Release a Deployment Management (řízení vydání a nasazení) - proces, který slouží k řízení vydání a nasazení na testovací a živá/produkční prostředí. Primárním účelem je zajištění integrity a ochraně prostředí a nasazení správných komponent;
- Service validation a Testing (ověření a testování služeb) - proces, který je zodpovědný za takové ověřování a testování, aby byly uspokojeny potřeby zákazníků;
- Knowledge Management (řízení znalostí) - proces, zodpovědný za sbírání, analýzu, uchovávání a sdílení znalostí napříč organizací.

[50]

### 6.1.4 Service design (Návrh služeb)

ITIL Service design poskytuje best-practices v souvislosti s návrhem nových IT služeb, procesů a jiných aspektů ITSM. Návrh služeb definuje, jak na sebe vzájemně působí plánované řešení služeb s technickým prostředím a byznysem.

Primární úlohou tohoto procesu je návrh nových IT služeb, procesů a dalších aspektů ITSM. Cíli tohoto procesu jsou:

- zlepšení kvality poskytovaných služeb,
- zjednodušit implementaci nových nebo změněných služeb,
- zlepšit soulad služeb a požadavků byznysu,
- vytvářet a zefektivňovat řízení IT.

[51]

#### 6.1.4.1 Procesy návrhu služeb

ITIL definuje 11 procesů, které patří do návrhu služeb:

- Design coordination (koordinace návrhu) - proces, který zajišťuje koordinaci mezi všemi procesy, aktivitami a zdroji procesů návrhu služeb;
- Service catalogue Management (řízení katalogu služeb) - proces, který zajišťuje udržování katalogu služeb, jeho pravidelnou revizi a přesné informace v něm;
- Service level Management (řízení úrovně služeb) - proces, který je zodpovědný za vyjednávání podmínek SLA (Service Level Agreement) se zákazníkem, a za poskytování služeb sjednaných se zákazníkem;
- Capacity Management (řízení kapacit) - proces, který zařizuje, aby byla IT infrastruktura adekvátní k zasmluvněným podmínkám;

- Availability Management (řízení dostupnosti) - definuje, plánuje, řídí, měří a vylepšuje všechny aspekty dostupnosti IT služeb;
- IT Service continuity Management (řízení kontinuity IT služeb) - zařizuje přes management rizik, aby byla za jakýchkoliv podmínek dostupná minimální sjednaná úroveň služeb;
- Information security Management (řízení bezpečnosti informací) - zajišťuje, aby byla zajištěna dostupnost, integrita a důvěrnost informací;
- Supplier management (řízení dodavatelů) - zajišťuje, aby byly smlouvy s dodavateli v souladu s požadavky byznysu a zajišťuje plnění požadavků dodavateli podle sjednaných podmínek;
- Risk management (řízení rizik) - proces, který zajišťuje řízení rizik, identifikaci hrozeb u aktiv a vyhodnocování zranitelností aktiv;
- Compliance Management (řízení souladu) - zajišťuje dodržování organizačních politik a požadavků uložených zákony;
- Architecture Management (řízení architektury) - zajišťuje rámec budoucího vývoje a technologie a bere v potaz strategii služeb a nové technologie.

[51]

### 6.1.5 Continual service improvement (Neustálé zlepšování služeb)

Neustále zlepšování služeb má za cíl vytvoření metrik k vylepšování kvality služeb skrz učení se z úspěchů nebo neúspěchů v minulosti. K tomu využívá podobného přístupu jako Demingův cyklus (PDCA cyklus).

Mezi cíli neustálého zlepšování služeb patří:

- revize a analýza příležitostí ke zlepšení,
- analýza a vyhodnocování dosažených úspěchů,
- zlepšení efektivity rozdělování zdrojů poskytovaných služeb,
- soulad s řízením kvality za účelem podpory aktivit ke zlepšování kvality služeb.

#### 6.1.5.1 Proces zlepšování v 7 krocích

Neustálé zlepšování služeb definuje proces zlepšování, který obsahuje 7 kroků (7-Step improvement process):

1. identifikace a definování strategie ke zlepšení,
2. definování, co se má měřit,
3. sběr dat,
4. zpracování dat,
5. analýza nasbíraných dat,
6. prezentace a použití informací,
7. implementace zlepšení.

[52]

## 6.2 ISO/IEC 20000

Série norem ISO/IEC 20000 je prvním standardem, který byl vytvořen pro řízení IT služeb. Standard je vytvořen mezinárodní organizací pro standardizaci (International Organization for Standardization - ISO) a je založen na znalostech a zkušenostech expertů, kteří se v oboru pohybují. [53] ISO/IEC 20000 byl vytvořen technickou comisí ISO/IEC JTC 1/SC 7, *Software and system engineering*, a je založen na BS 15000, který byl vytvořen BSI technickou komisí BDD/3 *Information services management*. [53]

Série norem ISO/IEC 20000 obsahuje více částí.

Norma ISO/IEC 20000-1 je první z nich a definuje požadavky, jak kvalitativně provozovat systém a služby. Norma zavádí integrovaný procesní rámec a její první část vymezuje požadavky na systém managementu služeb.

Norma ISO/IEC 20000-2 určuje pokyny pro použití systému managementu služeb.

Třetí část ISO/IEC 20000-3 určuje pokyny pro vymezení rozsahu a použitelnosti ISO/IEC 20000-1.

Další části normy se zabývají například integracemi s dalšími normami nebo jinými dokumenty pro systém managementu služeb.

### 6.2.1 Klíčové přínosy implementace série norem ISO/IEC 20000

Mezi klíčové přínosy implementace série norem ISO/IEC 20000 patří:

- standardizace procesů a zefektivnění činnosti poskytování IT služeb;

- získání přehledů o nákladech IT služeb;
- řízení služeb shora, přes strategie, až po operativní řízení;
- získání konkurenční výhody přes ostatními poskytovateli IT služeb;
- optimalizace procesů poskytování IT služeb.

[54]

### 6.2.2 ISO/IEC 20000-1

Norma ISO/IEC 20000-1 stanovuje požadavky na vytvoření, zavedení a udržování systému managementu služeb (SMS). Norma je vytvořena tak, aby bylo možné ji integrovat s jinými systémy, například systémem managementu kvality založeném na ISO 9001 nebo se systémem řízení bezpečnosti informací založeném na normě ISO/IEC 27001. [55]

Na obrázku 6.3 jsou uvedeny jednotlivé kapitoly ISO/IEC 20000-1. Tento obrázek není přesnou reprezentací SMS v organizaci. Poskytuje pouze rámec, který může organizace využít. Jednotlivé pojmy nejsou směrodatné a mohou být organizací nahrazeny podle vykonávané činnosti.

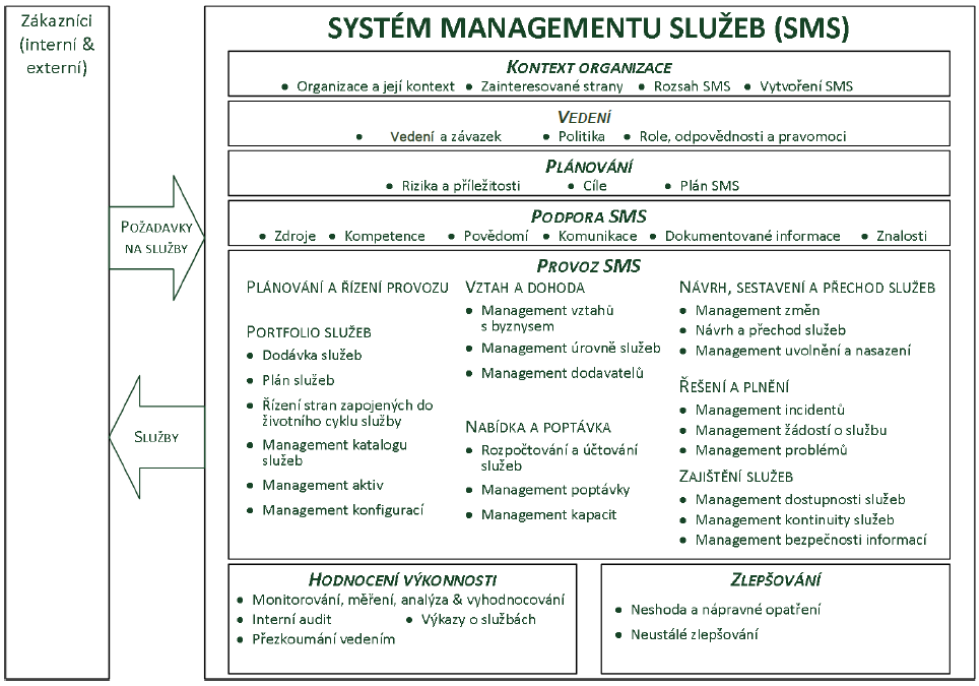
Norma neposkytuje model, který může být slepě následován, ale spíše ucelenou prezentaci požadavků, které může organizace pro svoji potřebu využít. Pro zavedení SMS však organizace nesmí vyloučit žádný z uvedených požadavků, které jsou v normě uvedeny. [55]

Všechny požadavky uvedené v normě jsou obecné a jsou použitelné pro jakoukoliv organizaci bez ohledu na velikost nebo typ organizace a na povahu poskytovaných služeb.

Tato norma v první řadě poukazuje na určení rozsahu systému managementu služeb. Je nutné, aby si organizace určila, do jaké míry bude SMS postihovat organizaci a musí určit, kam až budou opatření a nové procesy zasahovat. [55]

Dále jsou zde určeny povinnosti vedení. Pokud se organizace rozhodne systém managementu služeb zavádět, vedení organizace musí tento krok podpořit. Mimo jiné musí být vedením zajištěno, že:

- politika managementu služeb a cíle jsou stanoveny se strategickými cíli organizace;
- je zaveden a udržován plán managementu služeb tak, aby byla podpořena politika managementu služeb;
- jsou k dispozici zdroje pro systém managementu služeb;
- je komunikována důležitost tohoto systému;
- SMS bude dosahovat zamýšlených výsledků.




Obrázek 6.3: Systém managementu služeb [55]

[55]

Na vedení organizace je v tomto ohledu kladen velký důraz a pokud vedení není v souladu s těmito ustanoveními, je zavedení SMS a dosáhnutí požadovaného cíle velmi problematické.

Musí být vytvořena politika managementu služeb, která je úplná, přesná a obsahuje stanovené požadavky normou.

Systém managementu služeb musí být po celý jeho životní cyklus podporován. Organizace musí vyčlenit technické, informační, lidské a finanční zdroje potřebné pro vytvoření, zavedení, udržování a neustálé zlepšování SMS.

Důležitost SMS musí být komunikována a všechny osoby, kterých se SMS týká musí být uvědoměno o existenci politik managementu služeb a jiných potřebných dokumentů. [55]

#### 6.2.2.1 Provoz systému managementu služeb

Mezi požadavky systému managementu služeb patří zavedení řízení v různých oblastech podniku, které souvisí s poskytováním služeb jak interním, tak externím zákazníkům. Těmito řízeními (managementy) jsou:

I. Service portfolio (portfolio služeb),

   i. Service delivery (dodávka služeb) - organizace provádí činnosti pro poskytování služeb;

ii. Plan the services (plánování služeb) - organizace musí plánovat a řídit služby podle zavedených politik;

iii. Control of parties involved in the service lifecycle (řízení stran zapojených do životního cyklu služby) - musí být řízeny odpovědnosti za požadavky podle normy a organizace musí brát zodpovědnost za služby bez ohledu na to, která strana je zapojena do činností podporující životní cyklus služby;

iv. Service catalogue management (management katalogu služeb) - musí být vytvořen a spravován katalog služeb;

v. Asset management (management aktiv) - organizace zajišťuje, aby byla aktiva v souladu se závazky;

vi. Configuration management (management konfigurací) - musí být zajištěny konfigurační jednotky a tyto musí být i řízeny

II. Relationship and agreement (vztah a dohoda),

i. Business relationship management (management vztahů s byznysem) - proces, který určuje, že musí být udržovány vztahy se zákazníky;

ii. Service level management (management úrovně služeb) - proces, který zastřešuje dodávání služeb a dohody mezi zákazníkem a organizací;

iii. Supplier management (management dodavatelů) - proces zajišťující vztah a smlouvy s externími nebo interními dodavateli;

III. Supply and demand (nabídka a poptávka),

i. Budgeting and accounting for services (rozpočtování a účtování služeb) - organizace musí řídit rozpočtování;

ii. Demand management (management poptávky) - proces monitorování poptávky;

iii. Capacity management (management kapacit) - proces, který řídí kapacity tak, aby byly naplněny závazky;

IV. Service design, build and transition (návrh, sestavení a přechod služeb),

i. Change management (management změn) - proces, který zajišťuje, aby byly řízeny změny, a aby bylo zabráněno změnám, které nejsou schváleny;

ii. Service design and transition (Návrh a přechod služeb) - procesy, které zahrnují, aby byly nové nebo změněné služby správně plánovány a navrhovány;

iii. Release and deployment management (management uvolnění a nasazení) - proces, který plánuje a řídí release. Zahrnuje i napojení na management změn a musí být monitorován a zlepšován;

V. Resolution and fullfilment (řešení a plnění)

i. Incident management (management incidentů) - proces, který řídí incidenty, jejich klasifikaci, eskalaci a poučení se z již proběhlých incidentů;

ii. Service request management (management žádostí o službu) - proces, který se zabývá žádostmi o službu, kdy každá žádost musí být zaznamenávána, prioritizována, vypořádána a ukončena;

iii. Problem management (management problémů) - proces, který se zabývá daty z incidentů a snaží se předejít novým incidentům nebo jejich opakování;

VI. Service assurance (Zajištění služeb)

i. Service availability management (management dostupnosti služeb) - proces, který se zabývá riziky zajištění služeb. Požadavky by měly splňovat uzavřená SLA;

ii. Service continuity management (management kontinuity služeb) - proces, který zajišťuje kontinuitu služby a v případě výpadku služby zajišťuje napravení podle stanovených pravidel;

iii. Information security management (management bezpečnosti informací) - určuje zajištění politiky bezpečnosti informací a pravidelné přezkoumávání a řízení informační bezpečnosti. Také je nutné sbírat bezpečnostní incidenty, prioritizovat je, vyřizovat a uzavírat.

[55]

### 6.2.3 Certifikace ISO/IEC 20000-1

Na soulad s normou ISO/IEC 20000-1 je možné se certifikovat. Cílem certifikace je deklarovat:

- plnění požadavků mezinárodní normy ISO/IEC 20000-1;
- zavedení systematického přístupu v oblasti systému řízení služeb;
- zvýšení standardu a kvality poskytovaných služeb.

[56]

## 6.3 ISO/IEC 27000

ISO (International Organization for Standardization) rezervovala sérii ISO 27000 pro normy z oblasti bezpečnosti informací.

Norma ISO/IEC 27000 obsahuje přehled, termíny a definice, které budou v této rešerši používány. Bezpečnosti informací rozvíjí komplexní terminologickou síť. Z tohoto důvodu byly přesně definovány termíny a definice, aby nedocházelo k informačnímu šumu. [57]

Tento model obsahuje rysy, u kterých experti v daném oboru dosáhli shody, pokud jde o poslední stav mezinárodního vývoje. Z těchto expertů je vytvořena komise, která se věnuje vývoji mezinárodních norem systémů řízení bezpečnosti informací, nazývaných také řada norem Systém řízení bezpečnosti informací - Information Security Management System (ISMS). [57]

### 6.3.1 Information Security Management System – ISMS

ISMS sestává z politik, postupů, směrnic a příslušných zdrojů a činností, které organizace řídí, aby zajistila ochranu informačních aktiv. ISMS představuje systematický přístup k ustanovování, implementování, provozování vylepšování bezpečnosti informací. K úspěšné implementaci ISMS přispívá dobrá analýza požadavků na ochranu informačních aktiv a aplikace těchto požadavků s cílem ochrany informací podle těchto požadavků. ISMS je založen na posuzování rizik a tvorbě opatření nebo přijímání těchto rizik tak, aby byly dosaženy cíle společnosti. [57]

#### 6.3.1.1 Principy úspěšné implementace ISMS

- Povědomí o potřebě bezpečnosti informací;
- Určení odpovědnosti za bezpečnosti informací;
- Začlenění závazku vedení a zájmů zúčastněných stran;
- Zvýšení společenských hodnot;
- Posouzení rizika, na základě kterého budou stanovena příslušná opatření, aby bylo dosaženo přijatelných úrovní rizika;
- Bezpečnost začleněná jako základní prvek do informačních sítí a systémů;
- Aktivní prevence a detekce incidentů bezpečnosti informací;
- Zajištění komplexního přístupu k řízení bezpečnosti informací;
- Neustálé opakované posuzování bezpečnosti informací a provádění modifikací dle potřeby.

### 6.3.2 Bezpečnost informací

Pro zajištění úspěchu v činnosti organizace, kontinuitu této činnosti a minimalizace dopadů incidentů bezpečnosti informací, vyžaduje bezpečnost informací použití a řízení vhodných opatření.

Tohoto se dosáhne implementací sady opatření, vybraných a řízených pomocí ISMS. Tato opatření je nutné specifikovat, implementovat, monitorovat, přezkoumávat a zlepšovat tam, kde je to nezbytné, aby se zajistilo splnění specifických cílů bezpečnosti informací a podnikatelských cílů organizace. Příslušná opatření by měla být uceleně začleněna do procesů činnosti organizace. [57]

### 6.3.3 Důležitost ISMS

Je potřeba se zabývat riziky spojenými s informačními aktivy organizace. Je nutné, aby návrh a provoz ISMS odrážel zájmy a požadavky na bezpečnost informací všech zúčastněných stran včetně zákazníků, dodavatelů, obchodních partnerů, akcionářů a dalších relevantních třetích stran.

Organizace a jejich systémy čelí bezpečnostním hrozbám ze širokého okruhu zdrojů, zahrnující podvody, špionáže, sabotáže, vandalismus aj. Poškození informačních systémů a sítí způsobená škodlivým programem, počítačovým hackingem apod. se stávají stále běžnějšími a stále sofistikovanějšími.

Bezpečnost informací často není při vývoji systému brána v úvahu. Často je také považována pouze za technické řešení. Tato bezpečnost omezená pouze na technické řešení může být neúčinná, není-li podporována příslušným řízením a postupy v kontextu ISMS. Začlenění bezpečnosti do informačního systému, je-li již vytvořený, může být obtížné a nákladné.

Například řízení přístupu, která mohou být technická, fyzická, administrativní nebo kombinovaná, poskytují prostředky, zajišťující, že přístup k informačním aktivům je oprávněný a omezený, a že vychází z požadavků činnosti organizace a bezpečnostních požadavků. [57]

Úspěšné zavedení ISMS umožňuje:

- Dosáhnout větší záruky, že informační aktiva jsou neustále chráněna před hrozbami;
- Udržovat strukturovaný a komplexní rámec pro identifikování a posuzování rizik bezpečnosti informací;
- Zlepšování prostředí, ve kterém se řízení uskutečňuje;
- Efektivně docílit souladu s právními normami a předpisy.

### 6.3.4 ISO/IEC 27001

Tato mezinárodní norma specifikuje požadavky na ustavení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací. Termíny a definice pro použití této normy jsou specifikované v ISO 27000. [35]

#### 6.3.4.1 Politika bezpečnosti informací

Je nutné, aby vrcholové vedení stanovilo bezpečnostní politiku. Bezpečnostní politika je dokument a měla by dle normy obsahovat cíle bezpečnosti informací organizace nebo by měla poskytovat rámec pro nastavení cílů bezpečnosti informací. Bezpečnostní politika zahrnuje i závazek k neustálému zlepšování.

Musí být dostupná jako dokumentovaná informace a komunikována v rámci organizace. Zainteresované strany by ji měly mít k dispozici. [35]

#### 6.3.4.2 Rizika

Organizace musí mít zajištěno řízení rizik. Rizika musí být posuzována podle pravidel, která jsou určená organizací. Rizika musí být identifikována, klasifikována, hodnocena, řešena a evaluována. Musí být zavedena opatření, která snižují rizika a řeší je. Tato opatření jsou uvedena v příloze normy ISO/IEC 27001 a opatření musí odpovídat vyhodnoceným rizikům. [35]

#### 6.3.4.3 Opatření podle ISO/IEC 27001

Příloha A normy ISO/IEC 27001 obsahuje jednotlivé skupiny opatření a způsob, jakým se mají aplikovat. Opatření jsou formulována obecně a je na organizaci, jak bude tato opatření implementovat a řešit. Opatření by měla být zavedena v dokumentované podobě a komunikována. Pro informaci zde uvádím některá ze skupin opatření:

- Bezpečnost lidských zdrojů,
- Řízení aktiv,
- Řízení přístupů,
- Kryptografie atd.

Jednotlivé skupiny obsahují výčet opatření. Tato opatření jsou dále rozvedeny v normě ISO/IEC 27002 a v též normě jsou uvedeny pokyny k implementaci. Není zde explicitně uvedeno, jak by se měla opatření aplikovat, jen je popsáno, jakým způsobem. Konkrétní implementace je závislá na organizaci. Pokud chce být ale organizace v souladu s normou ISO/IEC 27001, nesmí vynechat ani jedno opatření. [35]

## 6.4 Zhodnocení

Standard ISO/IEC 20000-1 spolu s frameworkem ITIL mohou být zavedeny společně a skvěle spolupracují. Oba zajišťují poskytování konzistentních, efektivních a spolehlivých IT služeb. [58]

Ve standardu ISO/IEC 20000-1 je také uvedena kapitola o informační bezpečnosti a o managementu informační bezpečnosti, jak je uvedeno v kapitole 6.2.2.1. ITIL má informační bezpečnost zahrnutou oproti normě ISO/IEC 20000-1 v kapitole Service design (návrh služeb), jak je uvedeno v kapitole 6.1.4.1. Je vidět, že obě tyto metodiky na informační bezpečnost myslí, a že je důležitá.

Dle statistik, jak je uvedeno v tabulce 6.1, je vidět, že celkový počet certifikátů ISO/IEC 20000-1 každým rokem stoupá. [59]

| **Rok** | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|
| **Počet** | 2778 | 4537 | 5005 | 5327 |

Tabulka 6.1: Celkový počet vydaných certifikátů ISO/IEC 20000-1 celosvětově [60]

Stejně tak, jak je vidět v tabulce 6.2, celkový počet certifikátů na soulad s normou ISO/IEC 27001 také každým rokem stoupá.

| **Rok** | 2013 | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|---|
| **Počet** | 21604 | 23005 | 27536 | 33290 | 39501 |

Tabulka 6.2: Celkový počet vydaných certifikátů ISO/IEC 27001 celosvětově [60]

Certifikace se stává běžnější a organizace je používají, aby zajistily lepší poskytování služeb nebo lepší bezpečnost informací, jelikož informace jsou v dnešním světě informačních technologií velmi důležité.

Na normy ISO/IEC 20000-1 a ISO/IEC 27001 se může nechat organizace certifikovat. Organizace se nemůže certifikovat na ITIL. Certifikace ITIL je v podobě kurzu a certifikátu pro osoby. [58]

Pokud se organizace rozhodne certifikovat na některou z norem ISO, činí to z vlastní vůle a certifikát je platný 3 roky. Poté se musí organizace pro udržení certifikace certifikovat znovu. [61]

Podle kapitoly 6.1 bylo zjištěno, že ITIL je velmi rozsáhlý a poskytuje ucelené informace o zavedení řízení systému IT služeb. Jednotlivé kapitoly obsahují mnoho informací a pro organizaci může být složité implementovat doporučení ITIL správným způsobem.

Oproti tomu normy ISO jsou v porovnání s doporučeními ITIL krátké. Poskytují striktní požadavky a návody k implementaci těchto požadavků. Již

ale není specificky popsáno, co se v jaké organizaci používá, a kde je dobré začít. Neposkytují ani best-practices, jak je tomu v ITIL.

Jak je vidět na obrázku 6.4, je zde rozděleno, co všechno ITIL pokrývá a jak se procesy do jednotlivých fází rozdělují.


Obrázek 6.4: Fáze a procesy ITIL [62]

ITIL se zaměřuje na služby, které jsou poskytovány skrz IT. Oproti tomu uvedené série norem jsou použitelné v jakékoliv organizaci, nezávisle na zaměření. ITIL může být ale použit i v organizaci, která se primárně IT nezabývá. Téměř každá organizace ke svému fungování používá nějaký informační systém a nějakým způsobem je s IT spojena.

Série norem ISO/IEC 20000 původně vznikla z ITIL v2 a od té doby nenabyla na objemu, ale požadavky normy se staly značně realističtější. [62]

Pro zavedení ITSM procesů může organizace použít ITIL a poté ověřit, zda jsou požadavky splněny skrz certifikaci na normu ISO. Problémem je, že organizace může implementovat doporučení z ITIL nějakým způsobem a potom narazit, když by vedení požadovalo ISO certifikaci, jelikož norma má striktní požadavky, zatímco doporučení požadavky nejsou.

Z důvodu, že TA ČR není primárně IT organizací, ale zabývá se poskytováním služeb a informací a informační systém ISTA podporuje většinu klíčových procesů, byly zvoleny všechny 3 metodiky a práce s nimi. Primárně jsou použity normy ISO, ale jak již bylo zmíněno, normy poskytují mantinely a požadavky, co se má dělat a jen krátký návod k implementaci. ITIL je použit pouze jako podpora, o kterou se dá opřít, pokud jsou požadavky v normě nejasné.

ISO/IEC 20000 poskytuje požadavky na procesy a systémy managementu, ITIL poskytuje návod a vedení. Norma ISO/IEC 20000 požaduje 13 procesů bez přesného životního cyklu, oproti tomu ITIL popisuje 5 fází životního cyklu.

Série norem ISO/IEC 27000 podobně jako série ISO/IEC 20000 má požadavky na dokumentaci a přesné znění pravidel a jak plyne ze statistik na tabulce 6.2, je stále více používaná a vede organizaci k lepšímu zabezpečení informací.

Kapitola 7

# Analýza aktuálních procesů TA ČR

V této kapitole je uvedena analýza aktuálních procesů TA ČR v souvislosti s bezpečností informací a managementem rizik. Management rizik a bezpečnost informací spolu značně souvisí a vytváří pro nastavení procesů v organizaci základ, kolem kterého by měla organizace svoje procesy utvářet a měnit, aby nedošlo ke ztrátě dat nebo jiným incidentům.

V této kapitole jsou analyzovány procesy podle ISO/IEC 20000 a jejich návaznost na bezpečnost informací podle ISO/IEC 27000.

Tato analýza je jedním z nejdůležitějších bodů této diplomové práce a zabývá se spojením dvou oblastí - ISMS (Information Security Management System) a SMS (Service Management System).

## 7.1 Procesní landscape dle ISO/IEC 20000-1

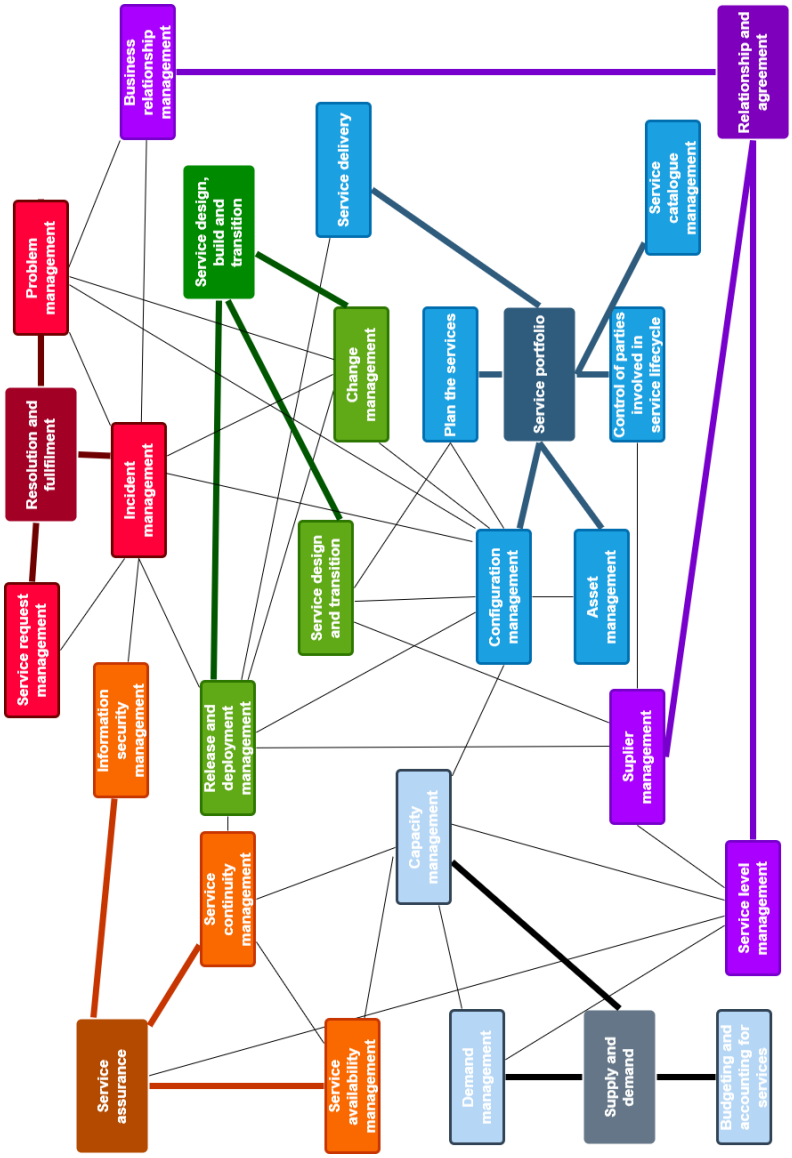
Procesní ladscape podle kapitoly 4.2.2 umožňuje určit související procesy a jejich návaznosti a dává celkový přehled o procesech při jejich dalším používání a vytváření.

Zákazníky procesů dle ISO/IEC 20000 jsou podle kapitoly 6.2 interní i externí zákazníci, podle toho, komu je služba určena a pro koho vytváří hodnotu.

Z analýzy procesů podle série norem ISO/IEC 20000 byl vytvořen model, který je na obrázku 7.1. V tomto modelu jsou specifikovány jednotlivé oblasti procesního řízení podle kapitoly 6.2.2.1. Jednotlivé celky jsou barevně odlišeny.

Každá skupina je označena jinou barvou. V této skupině je jeden nadřazený prvek, který je označen tmavší barvou. Tlusté čáry znamenají příslušnost k jedné skupině.

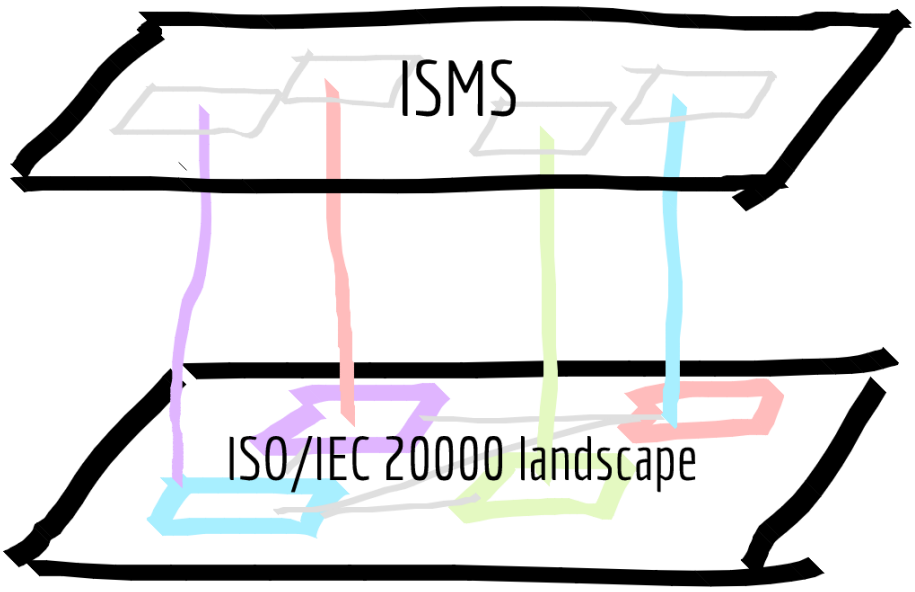
Tenké čáry reprezentují vztah mezi jednotlivými řízeními. Znamená to, že pokud se v organizaci zavádí některé z řízení, musí být bráno v úvahu i další




Obrázek 7.1: Procesní landscape dle ISO/IEC 20000-1 - vlastní zpracování

napojené řízení. Pomocí tohoto modelu byly jednotlivé procesy analyzovány a popsány.

Souvislost s bezpečností informací a systémem řízení bezpečnosti informací je znázorněna na obrázku 7.2. Dolní část obrázku reprezentuje model z obrázku 7.1 a nad ním je zobrazen Information Security Management System. ISMS zavádí určitá opatření a pravidla podle normy ISO/IEC 27001 a ty jsou připojena k jednotlivým řízením (v obrázku znázorněno barevnými obdélníky). Tato řízení musí respektovat vytvořená opatření (v obrázku znázorněno šedými obdélníky), aby jak SSM, tak ISMS splňovaly požadavky norem.




Obrázek 7.2: Znázornění procesního landscape ve spojení s ISMS - vlastní zpracování

## 7.2 Průběh analýzy

Analýza byla prováděna s cílem srovnat aktuální stav na TA ČR s požadavky normy ISO/IEC 20000 a ISO/IEC 27000. Tato analýza probíhala v období třech měsíců a poznatky, které byly analýzou zjištěny, jsou shrnuty v další kapitole.

Technologická agentura má přes 120 zaměstnanců, více než 10 dodavatelů pro různé oblasti agendy TA ČR a přes 25 systémů. [63, 64] Je poskytovatelem služby a poskytovatelem finanční podpory pro výzkum a vývoj v ČR.

Výsledků analýz bylo dosaženo následovně:

- Dotazy a požadavky na helpdesk TA ČR;

  Osobní zkušenost s prací v aplikaci helpdesk, kterou TA ČR poskytuje k řešení dotazů nebo požadavků uživatelů, kteří využívají služby TA ČR. Tato práce přinesla vhled do první a druhé úrovně podpory a přímý kontakt s uživateli aplikace ISTA.

- Stínování provozního manažera;

  Provozní manažer má v TA ČR na starosti zajištění provozu. Stínováním provozního manažera bylo dosaženo přehledu o tom, s kým jednotlivá oddělení komunikují a jakým způsobem komunikují. Dále bylo zjištěno, s jakými problémy se provozní manažer potýká. Hlavně řeší vztah byz-

nysu a ICT oddělení. Provozní manažer se zabývá okrajově i smlouvami s dodavateli.

- Účast na schůzích CAB;

  CAB neboli Change Advisory Board je hlavním prvkem Change managementu, kde se projednávají veškeré změny, které se v TA ČR dějí. Na těchto schůzích byla zjištěna různá rizika a problémy, se kterými se TA ČR vypořádává pomocí řízení změn.

- Rozhovory s klíčovými osobami na TA ČR;

  Byly prováděny rozhovory o fungování procesů na TA ČR a zajišťování chodu klíčových procesů. Rozhovory probíhaly s vedoucími pracovníky jednotlivých oddělení, aby se zajistilo, že informace pochází z více zdrojů a z různých kontextů TA ČR. Bezpečnost informací byla konzultována s bezpečnostním ředitelem TA ČR.

- Schůze a rozhovory mimo TA ČR;

  Proběhla schůze s NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost) ohledně bezpečnosti informací a certifikace dle ISO/IEC 27001. Dále proběhla schůze s externím konzultantem ze společnosti RELSIE spol. s r. o., která poskytuje nezávislé audity a certifikaci dle ISO/IEC 27001.

- Studování zápisů z řídících orgánů TA ČR;

  Zápisy schůze řídícího výboru TA ČR obsahují řešení různých problémů TA ČR a poskytují vhled do strategického řízení celé organizace. Tyto zápisy poskytly ucelený pohled shora na celou organizaci a spojení dílčích částí procesů organizace.

Informace z výše uvedených zdrojů byly zpracovány v analýzy a v následující kapitole jsou uvedeny pouze některé důležité nebo zajímavé části, jelikož celý popis analýz by byl nad rámec diplomové práce.

## 7.3 Analýza procesů

Bezpečnost informací zasahuje do procesního rámce napříč. Nelze vypreparovat jednotlivé oblasti, které by se bezpečnosti informací týkaly nebo netýkaly. Ať se děje v organizaci cokoliv, zahrnuje tato činnost práci s informacemi nebo fyzickou bezpečnost nebo další aspekty bezpečnosti. S tím jsou spojená i rizika, která se snaží systém bezpečnosti informací zmírnit nebo zcela vyloučit.

V této kapitole jsou popsány jednotlivé procesy podle normy ISO/IEC 20000-1 a jejich vztah k bezpečnosti informací.

V této kapitole nejsou rozebrány klíčové procesy Technologické agentury ČR, jelikož klíčové procesy jsou podporovány podpůrnými procesy, které nevytvářejí hodnotu pro externího zákazníka, ale v rámci organizace na nich klíčové procesy stojí. Pokud dojde k bezpečnostnímu incidentu, dojde k němu v průběhu klíčového procesu, ale z důvodu špatného nastavení podpůrných procesů nebo z důvodu nedodržení bezpečnostních politik zavedených organizací. Podpůrné procesy popisují činnosti, které se vyskytují napříč klíčovými procesy. Například management problémů popisuje obecně jak s problémy nakládat nezávisle na tom v jakém klíčovém procesu se problém vyskytl.

K vyhodnocení byly použity metriky náročnosti implementace a příznivého dopadu po implementaci. Výsledek se spočítá jako součin těchto dvou metrik. Nejvyšší výsledné číslo indikuje nejlepší poměr náročnosti a dopadu.

Byla použita stupnice od 1 do 5 následovně:

a) Dopad

   1. Žádný nebo minimální dopad - 1,
   2. Nízký dopad - 2,
   3. Střední dopad - 3,
   4. Vyšší dopad - 4,
   5. Maximální dopad - 5.

b) Náročnost

   1. Maximální náročnost - 1,
   2. Vyšší náročnost - 2,
   3. Střední náročnost - 3,
   4. Nízká náročnost - 4,
   5. Žádná nebo minimální náročnost - 5.

Vzhledem k počtu a rozsáhlosti analýz jsou v této práci popisy výsledků zkráceny na minimální možný rozsah, dostatečný k pochopení jednotlivých kapitol. Následující kapitoly jsou vypracovány s použitím zdrojů uvedených v předchozí kapitole a na základě norem ISO/IEC 20000-1 a ISO/IEC 27001 [35, 55].

### 7.3.1 Asset management - management aktiv

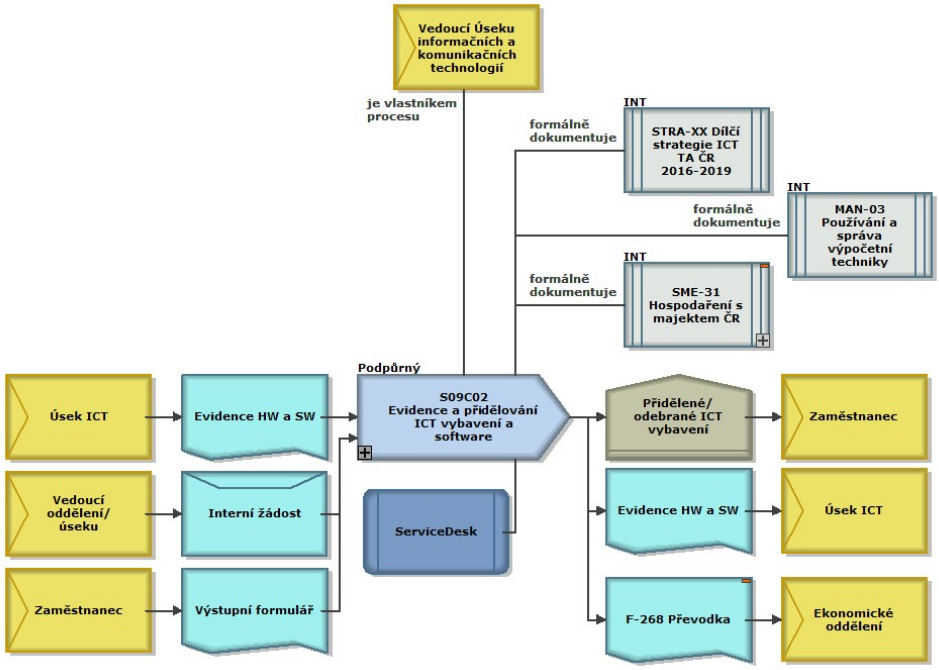
Aktiva mají být řízena tak, aby odpovídala plánování SMS. K plánování SMS neodmyslitelně patří i řízení dodávky služeb a vytváření hodnot pro zákazníka. Aktiva musí být řízena tímto stylem. Organizace si musí určit i konfigurační položky, jelikož management aktiv souvisí s konfiguračním managementem.

V Technologické agentuře ČR jsou řízena hmotná aktiva v interním systému pro evidenci majetku. Jsou zde evidovány vlastníci aktiv, provádějí se revize těchto aktiv.

Nehmotná aktiva jsou uvedena pouze v katalogu rizik, kde se s nimi hlavně pracuje.

#### 7.3.1.1 Asset management v souvislosti s bezpečností informací a managementem rizik

V souvislosti s bezpečností informací existují předpisy, které se zaměřují na používání a správu výpočetní techniky. Zde jsou uvedena bezpečnostní opatření, která se mají dodržovat. Model Evidence je uveden na obrázku 7.3.




Obrázek 7.3: Evidence a přidělování ICT vybavení a software [18]

Pro potřeby bezpečnosti informací a procesního rámce jsou aktiva nedostatečně popsána a proces, který zajišťuje práci s novými aktivy a jejich bezpečností není plně nastaven a popsán.

Management rizik s riziky spojenými s aktivy aktuálně pracuje. TA ČR ví, která aktiva jsou nejdůležitější a od nich se také odvíjí rizika.

#### 7.3.1.2 Dopad a náročnost zavedení/upravení Asset managementu

a) Náročnost - 2 vyšší. Postihuje aktiva v celé organizaci;

b) Dopad - 4 vyšší. S ohodnocenými a správně vedenými aktivy se dá dále dobře pracovat.

### 7.3.2 Configuration management - management konfigurací

Dle normy ISO/IEC 20000-1 musí být identifikovány, zaznamenávány, kontrolovány a verifikovány konfigurační jednotky. Přístup ke konfiguračním jednotkám musí být řízen a vztahy jednotlivých konfiguračních jednotek musí být zaznamenány. Všechny konfigurační jednotky musí být dohledatelné a auditovatelné.

V Technologické agentuře ČR není zaveden proces konfiguračního managementu. Některé prvky konfiguračního managementu jsou prováděny, nejedná se ale o formalizovaný proces, který by byl řízen.

Jelikož jsou v budově Technologické agentury umístěny některé servery a existují aplikace, které na nich běží, je nezbytné mít do budoucna tyto procesy nastavené a sepsané.

Technologická agentura ČR využívá aplikace Racktables, která popisuje lokální serverovnu a všechny běžící aplikace na lokálních serverech.

Formálně nejsou zavedeny konfigurační jednotky a nejsou popsány vztahy mezi nimi, což ovlivňuje i chod ostatních procesů a kvalitu dodávání služeb. Proces souvisí s Change managementem, který je popsán v kapitole 7.3.7.

#### 7.3.2.1 Configuration management v souvislosti s bezpečností informací a managementem rizik

Norma ISO/IEC 27001 se přímo na management konfigurací neodkazuje. V kapitolách normy jsou ale uvedené některé požadavky, na které by se rozhodně mělo brát ohled při nastavování procesu managementu konfigurací.

Jsou to kapitoly:

- Řízení aktiv - odpovědnosti za aktiva, klasifikace informací a manipulace s médii;
- Řízení přístupů - řízení přístupu k systémům a nastavení oprávnění;
- Kryptografie - kryptografická opatření;
- Fyzická bezpečnost - správa a řízení technických zařízení, zabezpečení oblastí.

Tyto kapitoly normy ISO/IEC 27001 přímo souvisí s managementem konfigurací. Pokud existují nějaké konfigurační jednotky, jsou jistě i aktivy a mělo by se s nimi jako s aktivy zacházet.

Přístupy do různých systémů musí být řízeny a to platí i pro management konfigurací, který bude v budoucnu s rozvojem organizace stěžejní.

V budově jsou servery, na kterých běží aplikace, které podporují chod organizace. Musí být tedy řízeny přístupy a oprávnění vstupovat do těchto prostor.

Kryptografické zabezpečení je nutností, kterou norma také vyžaduje.

Management rizik s managementem konfigurací aktivně nepracuje, jelikož nejsou nastavené konfigurační jednotky a jejich vztahy. Jakmile bude tento problém vyřešen, rizika se budou na management konfigurací odkazovat.

#### 7.3.2.2 Dopad a náročnost zavedení/upravení Configuration managementu

a) Náročnost - 1 maximální. Určení konfiguračních jednotek a vztahů je jednou z nejtěžších disciplín;

b) Dopad - 5 maximální. Celkový přehled o konfiguračních jednotkách a jejich vztazích.

### 7.3.3 Business relationship management - management vztahů s byznysem

Jedná se o podporu komunikace se zákazníkem. Je nutné přezkoumávat výkonnosti a výsledky poskytovaných služeb. Zabývá se řešením stížností a řešením zpětné vazby.

V systému ISTA je možnost podat zpětnou vazbu, která se uchovává, ale není s ní aktuálně nijak nakládáno. Proces sběru tohoto informací a nakládání s nimi je podobný Incident managementu.

Zpětná vazba od uživatelů je jednou z nejdůležitějších forem pro zlepšování kvality dodávaných služeb.

#### 7.3.3.1 Business relationship management v souvislosti s bezpečností informací a managementem rizik

Problém, který může nastat je sběr informací od uživatelů a různé možnosti úniku informací. Bezpečnost informací podle normy ISO/IEC 27001 řídí i bezpečnost komunikací a zálohování. Informace, které jsou přijaty od uživatelů by měly být zálohovány a pokud se sbírají i osobní data, mělo by s nimi být naloženo i podle zákona GDPR.

Rizika spojená s únikem informací jsou v katalogu rizik uvedena.

#### 7.3.3.2 Dopad a náročnost zavedení/upravení Business relationship managementu

a) Náročnost - 3 střední. Zavedení procesu není náročné, vyžaduje zdroje a nastavení přímočarého procesu;

b) Dopad - 1 minimální. Bez jiných procesů, které by správně pracovaly s tímto je dopad minimální.

### 7.3.4 Service level management - management úrovně služeb

Do tohoto managementu spadají dohody mezi zákazníkem a organizací (SLA - Service Level Agreement). Cílem je, aby byly správně nastaveny a bylo v nich obsaženo vše, co je potřeba. V normě ISO/IEC 20000-2 je uvedeno, jaké části by SLA mělo mít.

Procesy uzavírání SLA nejsou formálně popsány, ale jsou dodržována jistá pravidla, která jsou uvedená v interních směrnících TA ČR. Technologická agentura ČR má v organizační struktuře i právní oddělení, které se smlouvami zabývá.

Se svými zákazníky, kterým poskytuje službu, má TA ČR uzavřené SLA a jsou dohledatelné na portálu smlouvy.gov.cz.

#### 7.3.4.1 Service level management v souvislosti s bezpečností informací a managementem rizik

Bezpečnost informací podle normy ISO/IEC 27001 se na úroveň poskytovaných služeb příliš neodkazuje. Nicméně norma říká, že smlouvy mají být uzavírány s ohledem na bezpečnost informací. Znamená to tedy, že pokud je poskytována služba, mělo by být zajištěno její bezpečné používání a smluvně zavedeny požadavky na bezpečnost informací.

Rizika spojená s poskytováním služeb a smlouvami uzavíranými se zákazníky jsou vedena.

#### 7.3.4.2 Dopad a náročnost zavedení/upravení Service level managementu

a) Náročnost - 2 vyšší. Revize všech SLA a nastavení procesu musí být v souladu s ostatními procesy;

b) Dopad - 1 minimální. Nastavení SLA je aktuálně v pořádku, nejsou evidovány problémy.

### 7.3.5 Supplier management - management dodavatelů

Na TA ČR jsou zavedené postupy, jakým způsobem se řídí dodavatelé. Role, které jsou na TA ČR odpovědné za řízení vztahů, výkonnosti a smluv s dodavateli jsou provozní manažer a vedoucí pracovníci, kteří mají na starosti různé systémy TA ČR.

S dodavateli není udržováno vyhodnocování a zlepšování. Tyto dva aspekty nejsou řízené, jelikož nejsou popsané metriky, podle kterých by se měly řídit. Samozřejmě ve smlouvách s dodavateli existují sankce a plnění, pokud nedodrží

smluvní podmínky, ale formalizovaný proces, který by se zabýval pravidelným vyhodnocováním a zlepšováním neexistuje.

#### 7.3.5.1 Supplier management v souvislosti s bezpečností informací a managementem rizik

Dle normy ISO/IEC 27001 by měly by být dokumentovány požadavky v oblasti bezpečnosti informací na zmírnění rizik spojených s přístupem dodavatele k aktivům organizace. Tyto požadavky jsou uvedeny ve smlouvách a v některých interních dokumentech TA ČR.

Výměna informací s dodavatelem a postupy pro tento proces nejsou stanoveny. Odpovědnosti a povinnosti ve vztahu dodavatele a zákazníka jsou stanoveny smluvně.

Ve smlouvách by měly být uvedeny požadavky na bezpečnost informací, aby nenastala nedorozumění, jak se budou požadavky obou stran plnit.

Technologická agentura ČR se zabývá pouze nejdůležitějšími věcmi, které plynou z plnění závazků dodavatelem. Řízení dodavatelů z pohledu bezpečnosti není na takové úrovni, kteoru norma ISO/IEC 27001 požaduje.

Management rizik na samotného dodavatele jako riziko nehledí a zabývá se pouze vztahem produktu dodavatele a TA ČR.

#### 7.3.5.2 Dopad a náročnost zavedení/upravení Supplier managementu

a) Náročnost - 4 nižší. Nastavení procesu pro jednoho dodavatele, který dodává systém má nižší náročnost;

b) Dopad - 1 minimální. Udržování vztahů s dodavateli je na dobré úrovni.

### 7.3.6 Capacity management - management kapacit

Dle normy ISO/IEC 20000-1 musí být řízen lidské, technické, informační a finanční zdroje. Musí být stanoveno plánování zdrojů do budoucna na základě poptávky.

Technologická agentura ČR se snaží centralizovat výzkum v ČR, do budoucna je tedy počítáno s navyšováním počtů zaměstnanců a je uzavřena rámcová smlouva s více dodavateli informačních systémů, aby bylo podpořeno dodávání služby, kterou TA ČR poskytuje.

Formálně se proces řízení kapacit není zaveden.

#### 7.3.6.1 Capacity management v souvislosti s bezpečností informací a managementem rizik

Série norem ISO/IEC 27000 tento problém řeší v kapitole bezpečnosti lidských zdrojů a řízení aktiv. Pokud se navyšují stavy lidských zdrojů, musí být

zajištěna určitá opatření před vznikem pracovního poměru, při vzniku pracovního poměru a při ukončení nebo změně pracovního poměru. Bezpečnostní požadavky jsou zasmluvněné, není ale procesně zajištěn proces adaptace. Management rizik na adaptační proces myslí a je uveden v katalogu rizik.

#### 7.3.6.2 Dopad a náročnost zavedení/upravení Capacity managementu

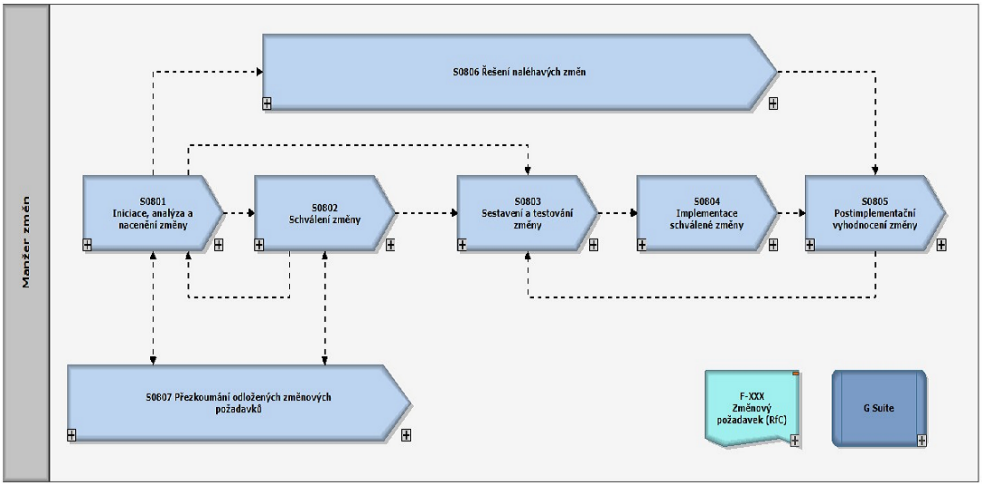
a) Náročnost - 4 nižší. Souvisí pouze s poptávkou služeb, neváže se na mnoho jiných managementů;

b) Dopad - 1 minimální. Na TA ČR nebyl zjištěn zásadní problém v této oblasti.

### 7.3.7 Change management - management změn

V Technologické agentuře ČR je zaveden proces managementu změn. Změny jsou řízené a je formálně popsán proces řízení změn, který se dodržuje. Je ustanoven CAB (Change Advisory Board), který má na starosti změny a je zavedena role manažera změn, který má určitá práva a povinnosti.

Na modelu, který je zobrazen na obrázku 7.4 je zobrazen proces managementu změn.




Obrázek 7.4: Proces managementu změn [18]

Management změn souvisí s dalšími oblastmi řízení v organizaci. Je s ním spojen například management incidentů nebo management uvolnění a nasazení. Při implementaci tohoto managementu bylo myšleno na případné další implementace nových procesů nebo jejich vylepšování a je možná integrace těchto procesů do již vytvořeného procesu managementu změn.

#### 7.3.7.1 Change management v souvislosti s bezpečností informací a managementem rizik

Jelikož se management změn týká většího množství procesů a souvisí s dalšími řízeními, bezpečnost informací zde hraje velkou roli. Musí být zajištěno, že informace, které jsou komunikovány v tomto procesu jsou úplné a pravdivé. Musí být zajištěna bezpečnost provozu a provozní postupy.

Management rizik spolupracuje s managementem změn, jelikož některé změny vytvářejí rizika. Rizika jsou vedena u jednotlivých změnových požadavků a je s nimi nakládáno podle pravidel určených managementem změn.

#### 7.3.7.2 Dopad a náročnost zavedení/upravení Change managementu

a) Náročnost - 1 maximální. Proces je již zaveden a procesně ho měnit nebo upravovat vyžaduje maximální úsilí;

b) Dopad - 1 minimální. Proces managementu změn je funkční, změna by nepřinesla užitek.

### 7.3.8 Release and deployment management - management uvolnění a nasazení

Nezáleží na tom, jak je nasazení urgentní, musí proběhnout přes Release management. Pravidelné release nové verze systému se provádí jednou za dva týdny pro hlavní systém TA ČR, kterým je ISTA. Proces není formálně popsán a na tomto procesu závisí většina činností TA ČR. Jelikož se provádí velmi často, mohou nastávat chyby, které chce TA ČR minimalizovat.

Některé změny a nasazení probíhají mimo Release management, jelikož jsou urgentní. Nasazení proběhne v pořádku, ale na produkčním prostředí se vyskytne chyba. Tato chyba potom dále spadá do Incident managementu.

#### 7.3.8.1 Release and deplyment management v souvislosti s bezpečností informací a managementem rizik

Řízení aktiv a jejich bezpečnost je prioritou. Pokud se do živého/produkčního prostředí zanese chyba, nastává problém, který může vést až k bezpečnostnímu incidentu. Bezpečnostní incidenty se musí hlásit na pověřený úřad podle zákona v kapitole 5.

Chyby v nasazení mohou vést až k porušení nařízení GDPR o osobních údajích nebo se může dojít k úniku citlivých dat jednotlivých příjemců finanční podpory na výzkum.

Spojitost s managementem rizik je zde vysoká. Každé nasazení s sebou nese riziko úniku dat nebo zanesení chyby do produkčního prostředí.

Například za poslední 2 měsíce proběhlo 17 nasazení mimo pravidelný release.

#### 7.3.8.2 Dopad a náročnost zavedení/upravení Release and deployment managementu

a) Náročnost - 2 vyšší. Jsou zavedeny určité procesy, které jsou v nesouladu s ISO/IEC 20000.

b) Dopad - 5 maximální. Vztahuje se na samotné fungování organizace a řeší rizika s vysokou prioritou.

### 7.3.9 Incident management - management incidentů

Řešení incidentů a jejich management není na TA ČR formálně zaveden. Velké incidenty (Major incidents) jsou eskalovány a existuje proces řešení těchto incidentů, je ale nutné, aby byly řešeny všechny incidenty. Pokud nastane únik dat nebo se v rámci Release managementu dostane chyba do produkce, je nutné, aby se tyto incidenty řídily.

Incidenty musí být klasifikovány. Klasifikace incidentů probíhá, ale oddělují se pouze velké (major) incidenty od běžných. Není zaveden log incidentů a učení se z již proběhlých incidentů.

#### 7.3.9.1 Incident management v souvislosti s bezpečností informací a managementem rizik

Bezpečnost informací se zabývá bezpečnostními incidenty. Únik dat nebo porušení nařízení GDPR nebo další incidenty se považují za velký problém v oblasti řízení bezpečnosti informací a musí s takovými incidenty být nakládáno podle pravidel. Bezpečnostním incidentem není pouze únik dat, ale například chyba v integritě informací nebo lidské chyby nebo prolomení opatření fyzické bezpečnosti.

Management rizik musí s incidenty počítat a považovat bezpečnostní incidenty jako možná rizika.

#### 7.3.9.2 Dopad a náročnost zavedení/upravení Incident managementu

a) Náročnost - 3 střední. Proces je přímočarý a navazuje na Change management a Release management;

b) Dopad - 3 střední. Logování incidentů, poučení se z nich spolu s dovedností vypořádávat efektivně incidenty posouvá dopad na střední úroveň.

### 7.3.10 Service request management - management žádostí o službu

Je realizován podobným procesem jako incident management. Požadavky na službu jsou standardními požadavky. Spadá do procesu Incident managementu

a je procesem Incident managementu spouštěn. V TA ČR není formálně zaveden, ale používá se na denní bázi. Existují úrovně podpory, které tento management řeší.

#### 7.3.10.1 Service request management v souvislosti s bezpečností informací a managementem rizik

Jsou zde rizika, která Service request management zavádí. Nejnebezpečnější je v tomto managementu výměna informací. Jsou zavedené některé postupy, které by si zasloužily revizi, jelikož pro komunikaci některých osobních údajů využívají komunikace, která není považována za bezpečnou.

Systém bezpečnosti informací musí zavést komunikační postupy pro různé typy dat.

#### 7.3.10.2 Dopad a náročnost zavedení/upravení Incident managementu

a) Náročnost - 4 nižší. Zavedení procesu je nutné formalizovat;

b) Dopad - 1 minimální. Proces již funguje a nejsou identifikovány zásadní problémy.

### 7.3.11 Problem management - management problémů

Souvisí s managementem incidentů. Incidenty musí být logovány a posuzovány. Z trendů incidentů se poté identifikuje problém. Na TA ČR není formálně zaveden. Není rozlišováno mezi problémem a incidentem. Z incidentu aktuálně vyplývá, že existuje problém a ten se řeší.

Procesně se problémy aktuálně řeší přes Change management.

#### 7.3.11.1 Problem management v souvislosti s bezpečností informací a managementem rizik

Jelikož nejsou řešeny incidenty a problémy jsou identifikovány podle neformálních postupů, může docházet z hlediska bezpečnosti k většímu počtu incidentů.

Z hlediska managementu rizik jsou problémy zaměňovány s incidenty a rizika s nimi spojená taktéž.

#### 7.3.11.2 Dopad a náročnost zavedení/upravení Problem managementu

a) Náročnost - 1 maximální. Nejprve se musí zavést formalizovaný proces incident managementu;

b) Dopad - 4 vyšší. Problémy jsou zaměňovány s incidenty a jejich řešení by mohlo významně organizaci prospět.

### 7.3.12 Service availability management - management dostupnosti služeb

Management dostupnosti služeb je v TA ČR prováděn. Není formálně zaveden, ale jsou jisté postupy, které jsou dodržovány. Systém je neustále monitorován a při kritických událostech je zvýšená dostupnost na 99,9 %. Systém je dostupný dle smluv každodenně na 16 hodin (7x16).

Nedostupnost systému je řešena komunikací s dodavatelem a přes incident management, který není formálně zaveden.

#### 7.3.12.1 Service availability management v souvislosti s bezpečností informací a managementem rizik

Bezpečnost informací dbá na dostupnost informací a na bezpečnost provozu. Všechny události v systému musí být zaznamenávány pro případ, kdy by došlo k nedostupnosti služby.

Riziko nedostupnosti služby je vedeno a konkrétním opatření pro toto riziko je zavedení zvýšené podpory dodavatelem v kritických časech poskytování služeb.

#### 7.3.12.2 Dopad a náročnost zavedení/upravení Service availability managementu

a) Náročnost - 4 nižší. Je nutné formalizování procesu;

b) Dopad - 1 minimální. Proces již funguje a nejsou identifikovány zásadní problémy.

### 7.3.13 Service continuity management - management kontinuity služeb

Je nutné vytvořit a udržovat plány kontinuity služeb. Pokud služba vypadne, není jasné, jak se má TA ČR zachovat pro zachování služby. Pokud služba vypadla nebo nebyla dostupná, vyřešil se problém pomocí incident managementu.

Plány pro zajištění kontinuity služby by měly být uloženy na bezpečném místě a měly by být pravidelně testovány a revidovány.

#### 7.3.13.1 Service continuity management v souvislosti s bezpečností informací a managementem rizik

Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací jsou řešeny opatřeními v normě ISO/IEC 27001. Opět platí, že všechny události musí být zaznamenávány a zkoumány z hlediska bezpečnosti informací. Pokud dojde k výpadku, musí být zajištěna dostupnost a integrita informací.

Management rizik se odkazuje na řízení kontinuity služeb z hlediska poskytování služeb dalším resortům.

#### 7.3.13.2 Dopad a náročnost zavedení/upravení Service continuity managementu

a) Náročnost - 3 střední. Je nutné formalizování procesu, vytvoření plánů kontinuity činností;

b) Dopad - 2 nižší. TA ČR by byla lépe připravena na události výpadku služby. Aktuálně nejsou evidovány větší problémy.

### 7.3.14 Information security management - management bezpečnosti informací

Managementem bezpečnosti informací se zabývá celá série norem ISO/IEC 27000. Jsou zavedené některé postupy, jak se chovat k určitým datům v určité situaci. Jsou popsány postupy, jak nakládat s hmotnými aktivy.

Informace, které jsou k dispozici nejsou vedeny jako řízený dokument, který by popisoval celou problematiku bezpečnosti informací. Série norem ISO/IEC 27000 ukládá vytvoření a udržování politiky bezpečnosti informací. Systém bezpečnosti informací kromě politiky a dokumentovaných informací vyžaduje implementaci přes 150 opatření, aby mohla být organizace certifikována na normu ISO/IEC 27001.

ISMS funguje na principu PDCA (Plan-Do-Check-Act) neboli Demingově cyklu. Je nutné neustálé zlepšování systému řízení bezpečnosti informací.

#### 7.3.14.1 Dopad a náročnost zavedení/upravení Information security managementu

a) Náročnost - 2 vyšší. Je nutné formalizování procesu, vytvoření politiky bezpečnosti informací a zavedení jednotlivých opatření;

b) Dopad - 5 maximální. Zavedení opatření dle ISO/IEC 27001 zajistí formalizované řízení bezpečnosti informací v době, kdy informace patří mezi nejdůležitější aktiva organizace.

### 7.3.15 Zhodnocení analýzy procesů v TA ČR

Provedená analýza slouží k tomu, aby bylo zjištěno, kde tkví největší problém a za účelem určení procesů, které v nejbližší době budou mít největší dopad na chod organizace.

V tabulce 7.1 jsou uvedeny jednotlivé managementy a přehledně zobrazeny jejich náročnosti a dopady. Poslední sloupec indikuje, které z managementů vycházejí nejlépe v poměru užitečnosti a náročnosti implementace.

Podle posledního sloupce je v nejbližší budoucnosti nejvýhodnější implementovat procesy Release and deployment managementu a Incident managementu. Procesy systému řízení bezpečnosti informací jsou zde také zahrnuty.

Na základě této analýzy budou v následujících kapitolách rozebrán a navržen proces Release and deployment managementu a proces Incident managementu dle ISO/IEC 20000 a ITIL. Pro zavedení systému řízení bezpečnosti informací budou uvedena opatření, která by se měla implementovat nejdříve, na základě managementu rizik a problémů, se kterými má Technologická agentura ČR dlouhodobější problémy.

| Management | Náročnost | Dopad | Výsledek |
|---|---|---|---|
| Asset management | 2 | 4 | 8 |
| Configuration management | 1 | 5 | 5 |
| Business relationship management | 3 | 1 | 3 |
| Service level management | 2 | 1 | 2 |
| Supplier management | 4 | 1 | 4 |
| Capacity management | 4 | 1 | 4 |
| Change management | 1 | 1 | 1 |
| **Release and deployment management** | 2 | 5 | **10** |
| **Incident management** | 3 | 3 | **9** |
| Service request management | 4 | 1 | 4 |
| Problem management | 1 | 4 | 4 |
| Service availability management | 4 | 1 | 1 |
| Service continuity management | 3 | 2 | 6 |
| **Information security management** | 2 | 5 | **10** |

Tabulka 7.1: Tabulka s přehledem náročnosti a dopadu

### 7.3.16 Zhodnocení analýzy z pohledu bezpečnosti informací

V provedené analýze byly zjištěny určité oblasti problémů bezpečnosti informací. Release and deployment management a Incident management byly vyhodnoceny jako nejvýhodnější pro návrh a implementaci. S těmito dvěma procesy souvisí i oblasti bezpečnosti informací, které by měly být řízeny.

Těmito oblastmi jsou:

- bezpečnost a řízení osobních údajů,
- bezpečnost výměny informací,
- bezpečnost v procesech vývoje,
- bezpečnost aktiv,

- bezpečnostní incidenty,
- řízení přístupů.

Tyto oblasti budou dále probrány a k určitým z nich navržena opatření a politiky tak, aby témata Release and deploy managementu a Incident managementu byla navržena jak z pohledu řízení, tak z pohledu bezpečnosti. Pro účely této diplomové práce jsem pro detailní rozbor vybral pouze dvě oblasti, neboť návrh řešení pro všechny výše zmíněné oblasti by byl nad rámec této diplomové práce. Těmito oblastmi jsou:

- bezpečnost výměny informací,
- bezpečnost v procesech vývoje.

Tyto oblasti jsou úzce spjaty s Release and deployment managementem a Incident managementem a vytvoření pravidel, podle kterých procesy budou řídit je v tomto případě nejlepší.

Kapitola 8

# Redesign procesů TA ČR

V této kapitole jsou probrány návrhy úpravy procesů Release and deployment managementu a Incident managementu. Byly vybrány na základě předchozí analýzy a budou navrženy s cílem certifikace na normu ISO/IEC 20000-1. Jsou pokryty hlavně tyto 2 procesy, jelikož návrhy a úprava dalších procesů jsou nad rámec diplomové práce. Cílem je zajistit postupnou implementaci procesů tak, aby v budoucnosti byla certifikace možná.

Integrace procesního rámce do organizace není jednoduchou disciplínou a implementace návrhů se musí dělat iterativně, jelikož prostředí organizace je organické a mění se.

Návrhy procesů byly vytvořen v systému SW ARPO popsaném v kapitole 4.3. Byly použity modely VAC a eEPC, které jsou popsány v kapitole 4.3.1. Soulad návrhů a navržených politik musí být také udržen s legislativními požadavky, které jsou uvedeny v kapitole 5.

## 8.1 Release and Deployment management

Release and deployment management má vytvořený v Technologické agentuře základ, na kterém je možné stavět. Jsou zavedeny jisté postupy, které splňují požadavky Release and deployment managementu podle ISO/IEC 20000-1, ale nejsou formálně zavedené, jako předpis, který se má ve všech případech dodržovat.

### 8.1.1 Požadavky na Release and deployment management podle ISO/IEC 20000-1

Hlavním cílem a účelem tohoto managementu je zajistit, aby všechna nasazení do živého/produkčního prostředí byla řízena a kontrolována za účelem splnění požadavků.

Součástí tohoto procesu je i návaznost na management konfigurací a aktiv. Nasazení služeb, aktiv nebo konfiguračních jednotek do živého prostředí je řízeno tímto procesem.

Release and deployment management úzce spolupracuje s Change managementem tam, kde je to možné. Nasazení se může skládat z jedné nebo více změn. Mohou být definovány různé typy nasazení jako například:

- standardní,
- nouzový,
- selektivní,
- rozdělený na fáze aj.

Tyto typy nasazení jsou definovány frekvencí nasazení a způsobem, jakým jsou řízeny.

Nasazení nových nebo změněných služeb do živého prostředí musí být plánováno. Případná nedostupnost služby musí být komunikována se zákazníkem.

Při každém plánování nasazení musí být určena kritéria akceptace nasazení. Pokud tato kritéria nejsou naplněna, je určeno, jak dále postupovat. Může se postupovat tak, že nasazení bude kompletně zrušeno nebo se provedou změny, které budou akceptační kritéria splňovat.

Musí být zajištěna integrita služeb. To znamená, že pokud by mohla být ohrožena, jsou vytvořeny tzv. rollback postupy, které jsou aplikovány v případě, že je potřeba zachovat službu při špatném nasazení.

Všechna nasazení musí být monitorována a zaznamenávána. Na základě těchto dat se poté určuje, jakým způsobem se může Release and deployment management vylepšovat. Se špatným nasazením jsou spojeny i incidenty, které se objeví ihned po nasazení. Tyto incidenty jsou analyzovány a vedou k neustálému vylepšování procesu.

Pokud například neproběhne nasazení úspěšně, může Change management revidovat změny, které byly provedeny a incident management může zajistit workaround, který je potřebný k zajištění poskytování služby.

Nasazení, která jsou komplexnější musí být dokumentována v detailním plánu nasazení. Plán nasazení musí obsahovat datum nasazení a další dokumentované informace, jako nově nasazené nebo změněné služby, navázaná aktiva nebo konfigurační jednotky.

### 8.1.2 Aktuální stav

V kapitole 7.3.8 je uvedena pouze krátká analýza, ale návrh procesů vyžaduje větší analýzu, která je uvedena v této kapitole.

V Technologické agentuře ČR je zavedena role Release manažera. Release manažer je prostředníkem mezi dodavatelem systému a byznysem, a koordinuje proces a čas nasazení.

Release systému ISTA probíhá aktuálně jednou za dva týdny. Každým nasazením se do systému přidá více než 10 změn. Každé dva týdny tedy vznikají nové verze systému a hrozí zde riziko, že se do systému dříve nebo později zavede fatální chyba.

Systém ISTA má 3 prostředí:

- prostředí TEST - testovací a vývojové prostředí, kde se vyvíjí a testují všechny požadavky;
- prostředí EDU - školící prostředí, které je kopií konfigurace produkčního prostředí, obsahující testovací data;
- prostředí PROD - živé/produkční prostředí.

Release manažer vždy před nasazením rozešle e-mail klíčovým stranám byznysu, kteří jsou zadavateli požadavků, aby určili, které požadavky byly implementovány a otestovány na prostředí TEST a mohly se přidat do balíku nasazení. Školící prostředí zde nehraje žádnou roli.

Požadavky jsou testovány samotnými implementátory požadavků nebo zadavateli a neexistují žádné testovací scénáře nebo uživatelské akceptační testy.

Testování balíku nasazení provádí pouze dodavatel, v TA ČR není zaveden proces, který by zajišťoval kontrolu a neprovádí se testování vydání.

Pokud se po nasazení objevují chyby, řeší se ad-hoc incident managementem a nebo klasickým požadavkem na nasazení, který poté opravuje chybu.

Existují také požadavky, které se nasazují mimo pravidelné nasazení a nejsou součástí balíku nasazení. Tyto požadavky nejsou vedeny separátně, ale jsou vedeny jako klasické požadavky. Jedná se většinou o rychlé opravení chyby.

Proces není formálně popsaný, vše je řízeno Release managerem a dodavatelem, kteří si vytvořili postupy, které dodržují.

Proces by měl aktivně spolupracovat s Change managementem, který je v TA ČR zavedený. Pokud se vytvoří změna, jsou na ni navázané požadavky pro změny v systému ISTA. Zpětna komunikace zde ale není, což je problém. Pokud je požadavek zaveden, není nastaveno, jak má být Change management informován o nasazení.

Problém také nastává v operaci s daty musí se podrobně popsat práce s daty a aktivy, které Release and deployment management postihuje, což ale není předmětem normy ISO/IEC 20000-1.

### 8.1.3 Vlastní návrh

Vlastní návrh tohoto procesu je založen na požadavcích normy ISO/IEC 20000-1 a opírá se z části o ITIL. Návrh je vytvořen, aby byl v souladu se sérií norem ISO/IEC 20000, která je popsána v kapitole 6.2. Základním kamenem pro vytvoření modelu procesu Release and deployment managementu je cyklus, který je zobrazen na obrázku 8.1.


Obrázek 8.1: Životní cyklus Release and deployment managementu [65]

Všechny aktivity zobrazené na obrázku 8.1 jsou pro Release and deployment management esenciální a podporují požadavky ISO/IEC 20000-1.

ITIL popisuje komplexní procoes Release and deployment management v následujících krocích:

- Plánování release a nasazení (release and deployment planning),
- Vývoj a testování release (release build and test),
- Nasazení (deployment),
- Vyhodnocení a uzavření (review and close).

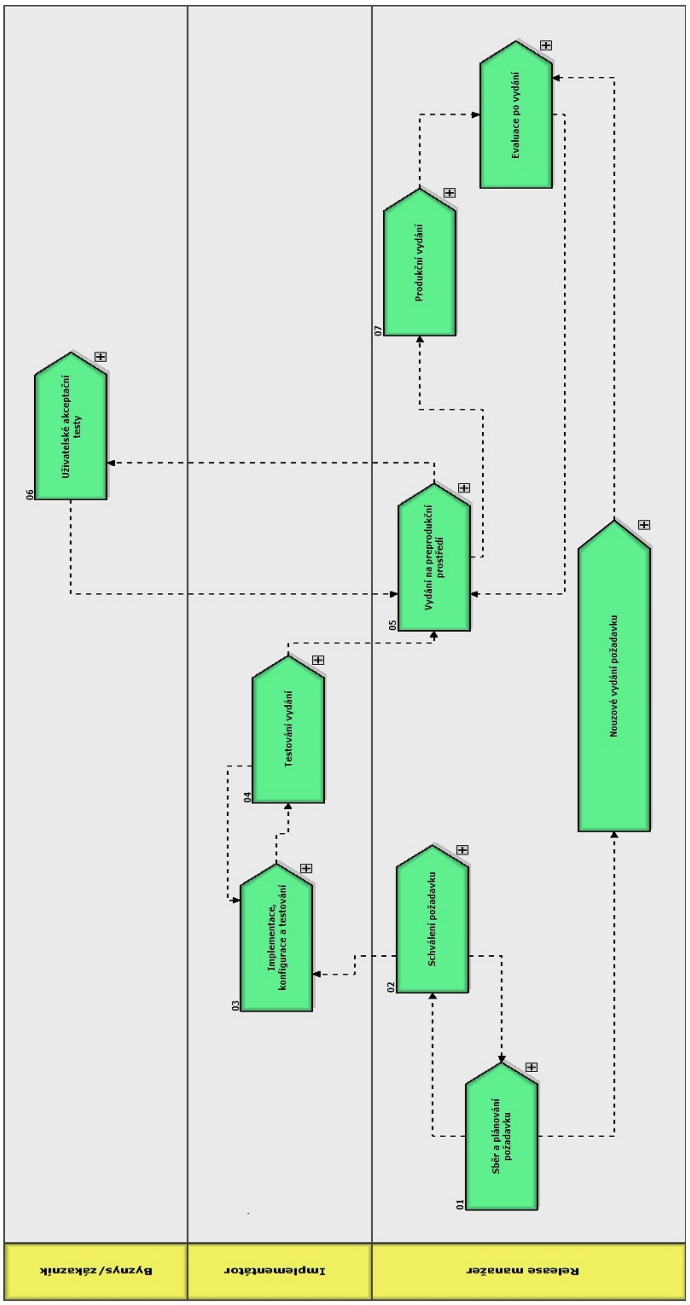
[66]

#### 8.1.3.1 Model subprocesů procesu Release and deployment managementu

Na obrázku 8.2 je zobrazen vymodelovaný proces Release and deployment managementu pomocí VAC (Value Added Chain) a v každý ze subprocesů odkazuje na podrobný eEPC model, který reprezentuje další závislosti a kontext procesu. Jsou dodržena všechna kritéria, která požaduje norma ISO/IEC 20000-1. Návrh modelu je připravený k postupné implementaci.

Proces se skládá z následujících částí, které jsou podrobněji rozebrány v dalších kapitolách:

- Sběr a plánování požadavků;




Obrázek 8.2: VAC model Release and deployment managementu - vlastní zpracování

- Schválení požadavků;
- Implementace, konfigurace, testování;
- Testování vydání;
- Vydání na preprodukční prostředí;
- Uživatelské akceptační testy;
- Produkční vydání;
- Evaluace po vydání;
- Nouzové vydání požadavku.

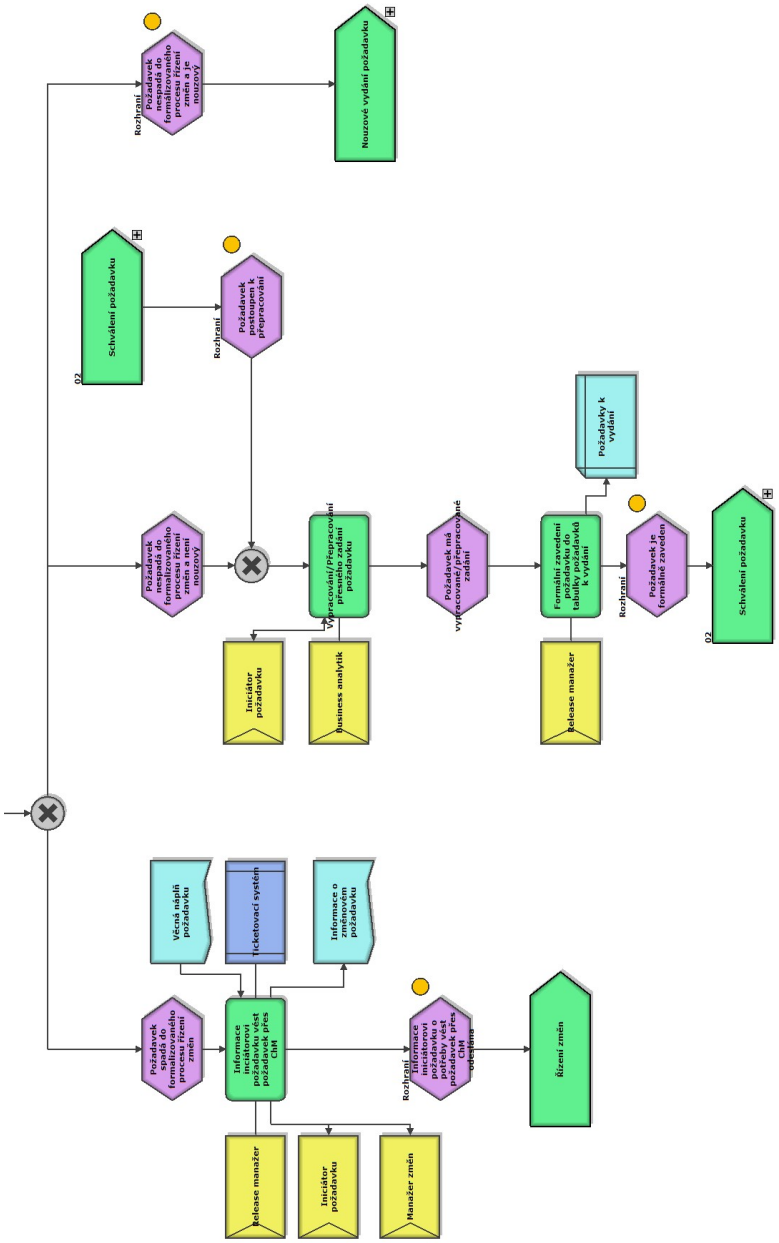
#### 8.1.3.2 Sběr a plánování požadavků

V tomto procesu jsou sbírány požadavky z různých zdrojů. Je nezbytné, aby požadavky byly posouzeny a vyhodnoceny, zda spadají do release managementu a zda je nutné se jimi zabývat. V tomto subprocesu probíhá rozhodnutí, zda je požadavek relevantní nebo ne. Pokud se na základě prvotní analýzy zjistí, že požadavek není relevantní, je zamítnut a subproces končí. Pokud je požadavek schválen a postoupen k nasazení, musí být nejprve posouzeno, jakým způsobem se bude požadavek k nasazení řešit. Pokud je požadavek naléhavý a řeší zásadní chybu, vstupuje se do subprocesu Nouzového nasazení požadavku, popsaného v kapitole 8.1.3.10. Tento subproces se odkazuje i na Change management. Některé požadavky jsou navázány ke změnovému požadavku a v procesu Release and Deployment managementu jsou nasazeny. Release manažer v tomto subprocesu musí zavést požadavek do tabulky požadavků a specifikovat kritéria akceptace nasazení tohoto požadavku. Je nezbytné, aby byl každý požadavek zaznamenán pro budoucí zhodnocení nebo revizi.

Na obrázku 8.3 je zobrazeno, do jakých procesů požadavek vstupuje a je zde znázorněno, kdy se formálně požadavek Release manažerem zavádí. V modelech jsou také navrženy odpovědnosti, systémy, vstupy a výstupy procesu.

#### 8.1.3.3 Schválení požadavků

V tomto subprocesu je zavedeno pravidelné setkání Release Board. Release Borad je role, ve které jsou zastoupeni někteří z členů CAB, release manažer a další osoby, které se podílí na Release and deployment managementu. Schůze tohoto útvaru je navržena, aby probíhala pravidelně a měly by zde být řešeny formálně zavedené požadavky v seznamu požadavků k nasazení. V tomto subprocesu jsou požadavky schvalovány, odkládány, zamítány nebo přeloženy k přepracování. Mohou se zde objevit požadavky, které přichází z Change managementu a jsou připraveny k implementaci.




Obrázek 8.3: Výřez z eEPC modelu subprocesu Sběr a plánování požadavků - vlastní zpracování

#### 8.1.3.4 Implementace, konfigurace, testování

Součástí tohoto subprocesu je implementace, konfigurace a testování požadavků. Požadavky jsou implementovány a testovány, poté jsou předloženy jako vyřešené a vstupují do procesu Testování vydání v kapitole 8.1.3.5. Technologická agentura ČR má dodavatele systému, ale zaměstnává i vlastní vývojáře, kteří systém ISTA programují/konfigurují.

#### 8.1.3.5 Testování vydání

V tomto subprocesu se provádí testování vůči závislostem na jiné požadavky, jak je popsáno v zadání. Pokud požadavek požaduje rollback postup, je toto znázorněno také v požadavku a v této fázi jsou požadavky na rollback implementovány. Tyto postupy jsou i na rollback postup otestovány a takto otestované vydání požadavku je poté postoupeno k vydání na preprodukční prostředí.

#### 8.1.3.6 Vydání na preprodukční prostředí

V tomto subprocesu je řešeno vytvoření balíku požadavků k nasazení. Tento balík se musí otestovat a pokud vyžaduje některý požadavek uživatelské akceptační testování, je požadavek směrován na subproces, uvedený v kapitole 8.1.3.7. Dokud nejsou všechny požadavky uživatelsky otestované a není upraven balík k nasazení takovým způsobem, který odpovídá akceptačním kritériím, nemůže se přejít do nasazení balíku na produkční prostředí. V opačném případě se do procesu produkčního prostředí přejde. Jako preprodukční prostředí je využito prostředí EDU, které se aktuálně pro Release and deployment management nevyužívá.

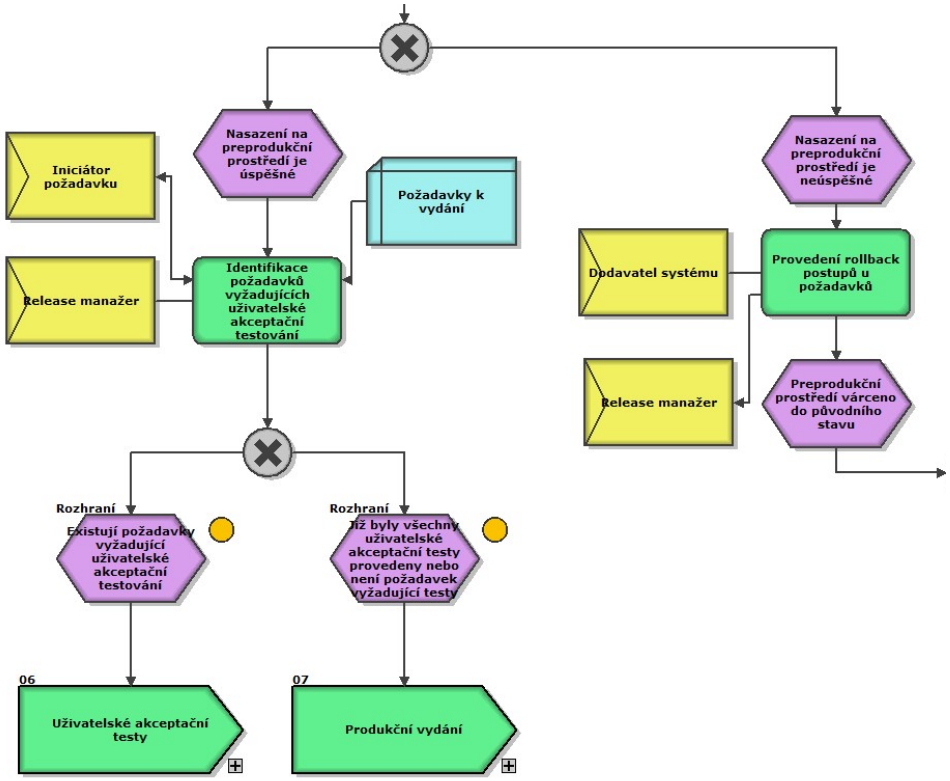
Na výřezu modelu na obrázku 8.4 je znázorněno rozdělení, pokud existují požadavky, u kterých je stále nutné uživatelské akceptační testování. Pokud již takové nejsou, následuje subproces Produkční vydání.

#### 8.1.3.7 Uživatelské akceptační testy

Subproces Uživatelského akceptačního testování je navržen jednoduše. Požadavky, které do tohoto procesu vstupují mají definovány akceptační testování. Toto testování je provedeno a subproces dále vstupuje do Vydání na preprodukční prostředí.

#### 8.1.3.8 Produkční vydání

Během tohoto subprocesu je provedeno vydání na produkční prostředí a jsou informovány klíčové role, které by měly o vydání nové verze vědět. Zároveň má Release manažer povinnost vytvořit Release notes (poznámky k vydání) a rozeslat je určeným rolím. Pokud nasazení neproběhne úspěšně, vyřeší se rollback postupy a nastane-li incident, směruje proces do Incident managementu.




Obrázek 8.4: Výřez modelu eEPC subprocesu Vydání na preprodukční prostředí - vlastní zpracování

Frekvence nasazení by se měla rozšířit ze dvou týdnů na minimálně 4 týdny. Jelikož režie tohoto procesu je náročnější a vyžaduje pro správně řízení více času. Dalším důvodem je, aby se zamezilo vydání neotestovaných požadavků. Rizikem je, že pokud se sníží frekvence nasazení, bude přibývat více požadavků k nasazení mimo pravidelný čas Release managementu.

#### 8.1.3.9 Evaluace po vydání

V evaluaci po vydání na produkční prostředí je zhodnoceno, jakým způsobem bylo provedeno nasazení. Jsou vedeny statistiky o jednotlivých nasazeních a je zde rozhodnuto, zda by se měly aplikovat praktiky lessons learned pro příští vydání. Neustálé zlepšování tohoto procesu je také jedním z bodů požadavků normy ISO/IEC 20000-1. Každý plán nasazení je zde evaluován.

#### 8.1.3.10 Nouzové vydání požadavku

Tento subproces je zaveden z důvodu nutnosti zavedení nápravných nebo nouzových vydání a zabývá se celým procesem od schválení požadavku, přes nasa-

zení na preprodukční prostředí až po nasazení na produkční prostředí. Tento proces může probíhat mimo plánované nasazení, ale jsou zde vedeny informace o balíku nasazení a další náležitosti, které jsou specifikované u požadavku. I přestože je vydání požadavku naléhavé a nutné, nesmí se vynechat žádné testování a ani se nepřeskakuje vydání na preprodukční prostředí. Celý proces probíhá podobně jako hlavní proces Deployment a release managementu.

### 8.1.4 Přínos navrženého řešení

Hlavním přínosem je, že se na produkční prostředí nebudou dostávat neotestované požadavky a funkce Release and deployment managementu bude poskytovat framework pro zlepšování kvality poskytovaných služeb.

Nové řešení integrace Release and deployment managementu je zlepšení spolupráce s Change managementem a propojení těchto dvou řízení v celek, který spolu funguje.

Oproti aktuálnímu řešení přináší pravidelné a otestované nasazení snížení rizika vnesení chyby do produkčního prostředí. Toto riziko má každá organizace, ale implementací tohoto procesu se významně snižuje.

Navržené řešení snižuje frekvenci nasazení ze dvou týdnů na minimálně čtyři týdny.

Tento návrh a implementace návrhu poskytuje soulad s normou ISO/IEC 20000-1 pro budoucí certifikaci na tuto normu.

## 8.2 Incident management

Incident management není v Technologické agentuře formálně zaveden. Některé incidenty se podle určitých postupů řeší, jiné se nechávají být. Složitá je také identifikace incidentů. Není jasné dáno, co incidentem je, a co incidentem není. Incident management má návaznosti i na Release and deployment management.

### 8.2.1 Požadavky na Incident management podle ISO/IEC 20000-1

Hlavním cílem a účelem Incident managementu je obnovit postižené služby co nejdříve je to možné na úroveň sjednaných služeb. Aktivity Incident managementu mohou minimalizovat dopad incidentů na kvalitu poskytovaných služeb. Všechny incidenty musí být zaznamenávána a klasifikována. Klasifikace je určena organizací, ale musí být provedena. Jednotlivé metriky, podle kterých se může incident klasifikovat jsou například typ, váha, naléhavost, postižené konfigurační jednotky apod. Na základě této klasifikace musí být incidenty řešeny.

Vyskytují se i incidenty, které jsou stejného původu nebo vycházejí ze stejné oblasti problému. Tyto incidenty musí být identifikovány a jejich zá-

znamy jsou potom použity k lepšímu vyhodnocení situace a k rychlejšímu vyřešení problému.

Pokud nemohou být incidenty vyřešeny v požadovaném čase, je nutná eskalace incidentů a jejich převedení na vyšší instance organizace.

Všechny incidenty musí být zaznamenávány pro statistiky a účely auditu. Organizace může zaznamenávat různé aspekty incidentu, od doby řešení až po nalezení, kterých SLA se incident týká apod.

Musí být zavedeny role, které souvisí s vypořádáváním incidentů.

Musí být řešeny velké (major) incidenty, o kterých musí být záznamy. Tyto záznamy jsou pravidelně poskytovány vyššímu managementu. Velké (major) incidenty jsou přiřazeny speciálnímu personálu, který je řeší.

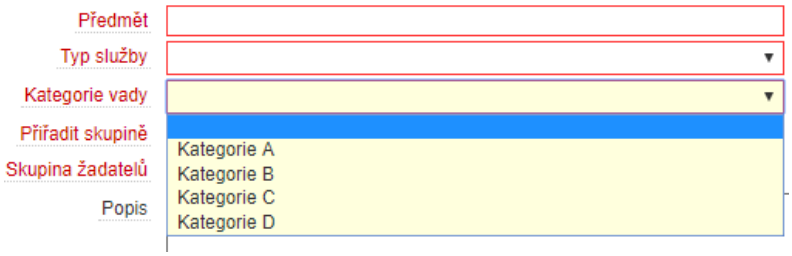
### 8.2.2 Aktuální stav

V kapitole 7.3.9.1 je uvedena pouze krátká analýza, ale návrh procesů vyžaduje větší analýzu, která je uvedena v této kapitole.

Technologická agentura ČR má zavedeny termíny, které se používají pro ohodnocení vyhodnocení požadavku. Jedná se o:

- Požadavek na změnu,
- Požadavek na informaci,
- Chyba,
- Incident.

Tyto jednotlivé termíny jsou používány podle subjektivního pocitu zadavatele do ticketovacího systému. Vyskytne-li se chyba v systému, vznikne nový požadavek, který je většinou označen jako chyba. Tento požadavek se dostane na provozního manažera, který požadavek vyřeší nebo eskaluje tak, že v systému založí nový požadavek, který označí jako incident (viz obrázek 8.5) a předá jej na doavatele systému.




Obrázek 8.5: Založení incidentu v ISTA [67]

S dodavatelem systému ISTA je zasmluvněno řešení těchto incidentů. Každý incident má kategorii a oblast, které části systému se týká. Kategorie jsou čle-

něny podle toho, na kolik uživatelů má incident vliv a kategoriemi je také ovlivněna reakční doba na incident ze strany dodavatele.

Za incidenty se v Technologické agentuře ČR označují jen takové incidenty, které jsou eskalovány na dodavatele systému ISTA, tedy na nejvyšší úroveň podpory.

TA ČR nevede souhrnný seznam všech incidentů, pouze, jak je výše uvedeno, takových, které jsou eskalovány na dodavatele systému ISTA.

Dle smlouvy dodavatel ISTA provozuje podpůrné centrum s možností telefonického kontaktu v případě nedostupnosti systému.

Velké (major) incidenty se řeší zavedenými postupy, ale záznamy s problémem, postupem řešení apod. nejsou vedeny.

Problém je tedy s termíny, které jsou používané a v nejasnosti těchto termínů. Jelikož je ISTA poskytována jako služba, je nutné aby všechny incidenty byly zaznamenávány a podle toho i řešeny.

### 8.2.3 Vlastní návrh

Incident management je z hlediska náročnosti o stupeň jednodušší k implementaci, než Release and deployment management. Model tohoto procesu je tedy přímočařejší, ale naplňuje všechny požadavky normy ISO/IEC 20000-1.

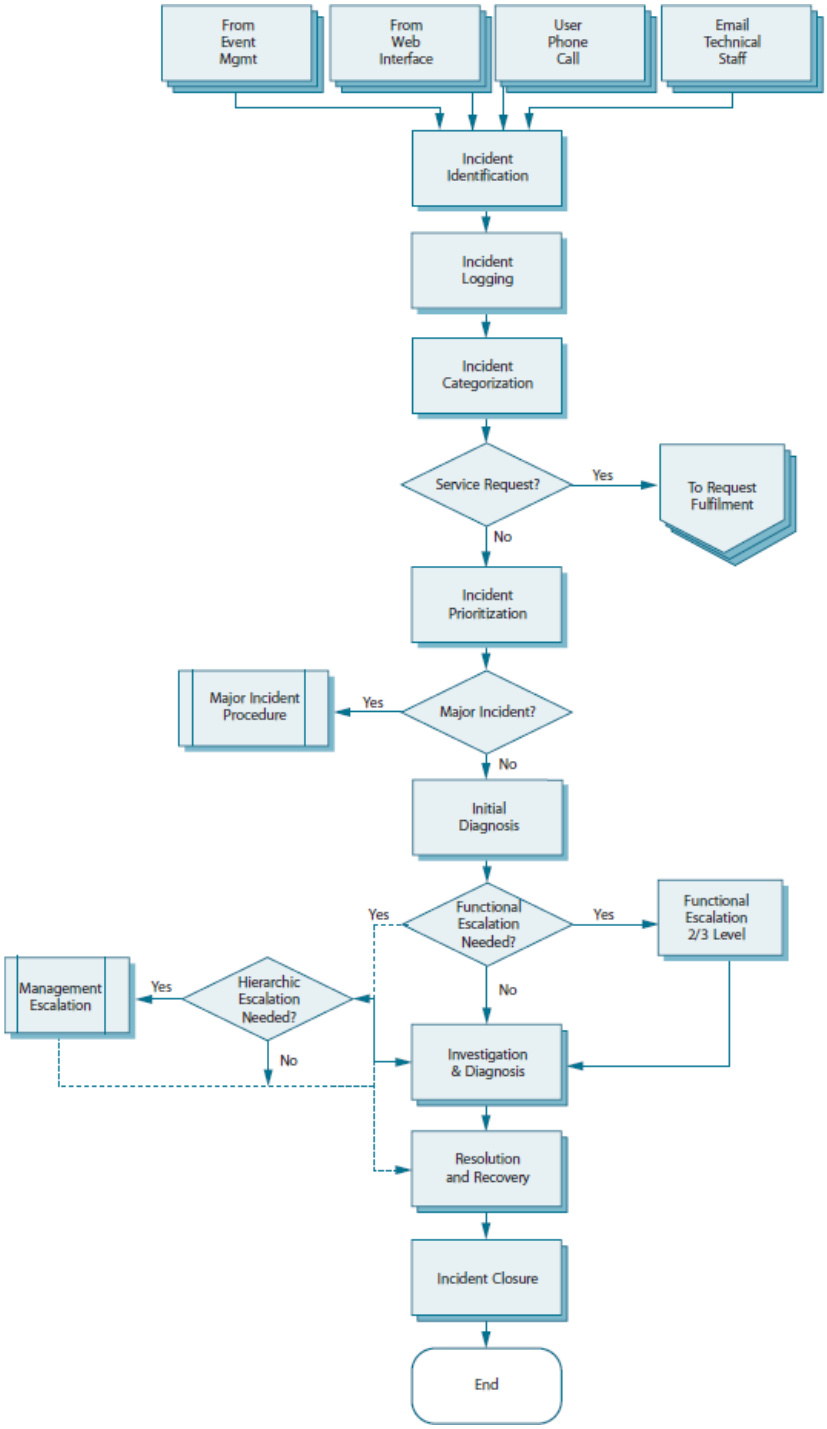
ITIL poskytuje základní model procesu Incident managementu (viz obrázek 8.6, který je možné využít. Tento model byl využit i při návrhu vlastního procesu, ale je nutné přizpůsobit proces organizaci, pro kterou se proces modeluje.

#### 8.2.3.1 Model subprocesů procesu Incident managementu

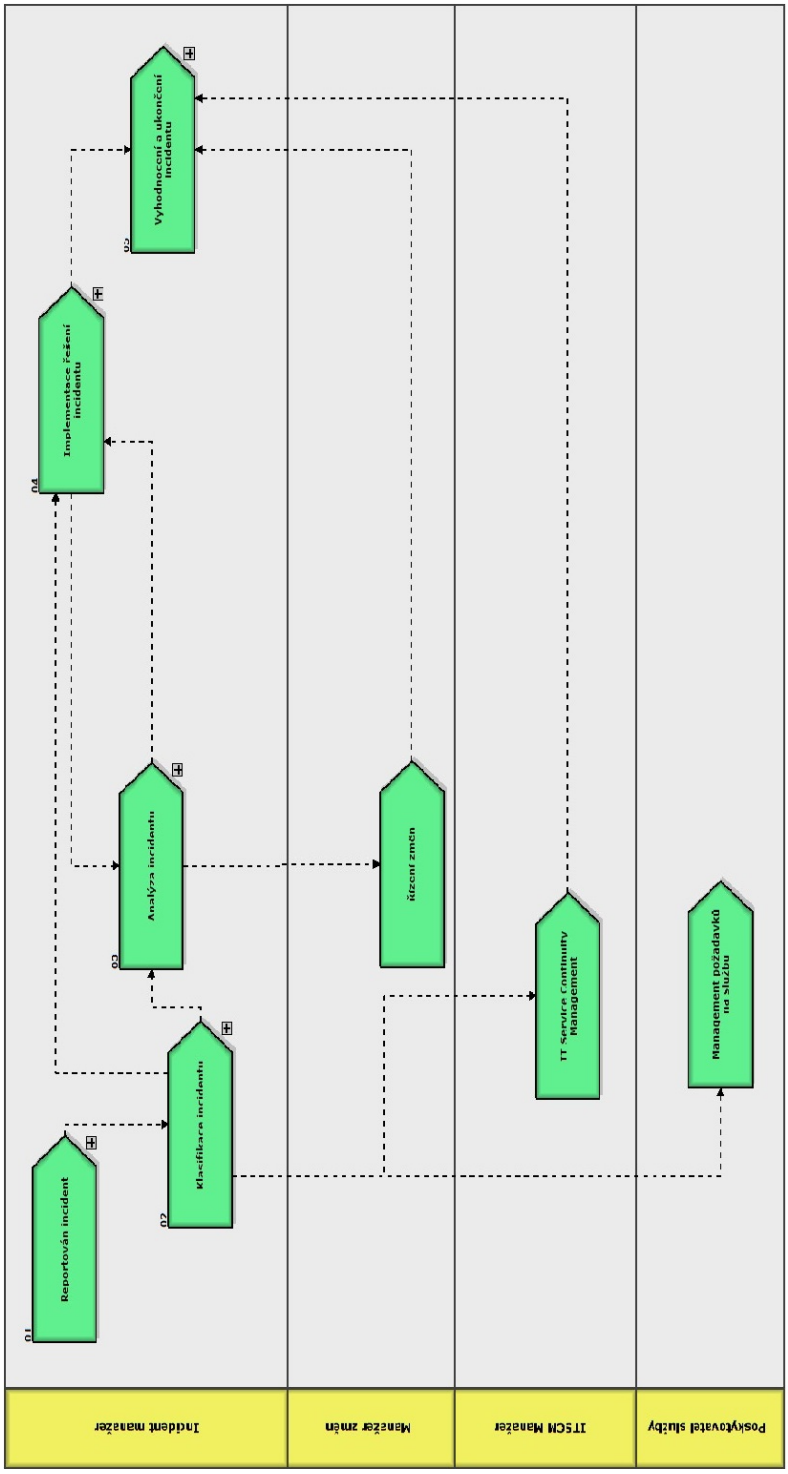
Na obrázku 8.7 je zobrazen vymodelovaný proces Incident managementu pomocí VAC (Value Added Chain) a každý ze subprocesů odkazuje na podrobný eEPC model, který reprezentuje další závislosti a kontext procesu. Kritéria určená ISO/IEC 20000-1 jsou dodržena a návrh modelu je připraven k implementaci.

Proces se skládá z následujících částí, které jsou popsány v dalších kapitolách:

- Reportování incidentu,
- Klasifikace incidentu,
- Analýza incidentu,
- Implementace řešení incidentu,
- Vyhodnocení a ukončení incidentu.




Obrázek 8.6: Incident management procesní flow [68]




Obrázek 8.7: VAC model Incident managementu - vlastní zpracování

#### 8.2.3.2 Reportování incidentu

V subprocesu reportování incidentu je zaveden stav, kdy je reportován incident a je vyřešeno zaznamenávání incidentu a jeho zařazení do logu incidentů. Subproces dále navazuje do subprocesu Klasifikace incidentu.

#### 8.2.3.3 Klasifikace incidentu

V tomto subprocesu je rozhodnuto, zda je zavedený incident pouze požadavkem na službu a podle toho je dále řešen jiným procesem a rolemi. Pokud se skutečně o incident jedná, je prozkoumán již zavedený log incidentů, zda se zde nenachází korespondující incident. Tyto incidenty se k sobě sváží a řeší se společně. V tomto kroku se také odlišují klasické incidenty od incidentů velkých. Velké incidenty jsou poté přesměrovány na řešení pomocí Business Continuity Managementu, který se bude touto problematikou zabývat společně s incident managementem. Ostatní incidenty se vyhodnotí a pokud je známé řešení, může se hned vyřešit na prvním stupni podpory. Pokud řešení známo není, postupuje se dále do analýzy incidentů. Toto rozdělení je zobrazeno na výřezu z modelu na obrázku 8.8.

#### 8.2.3.4 Analýza incidentu

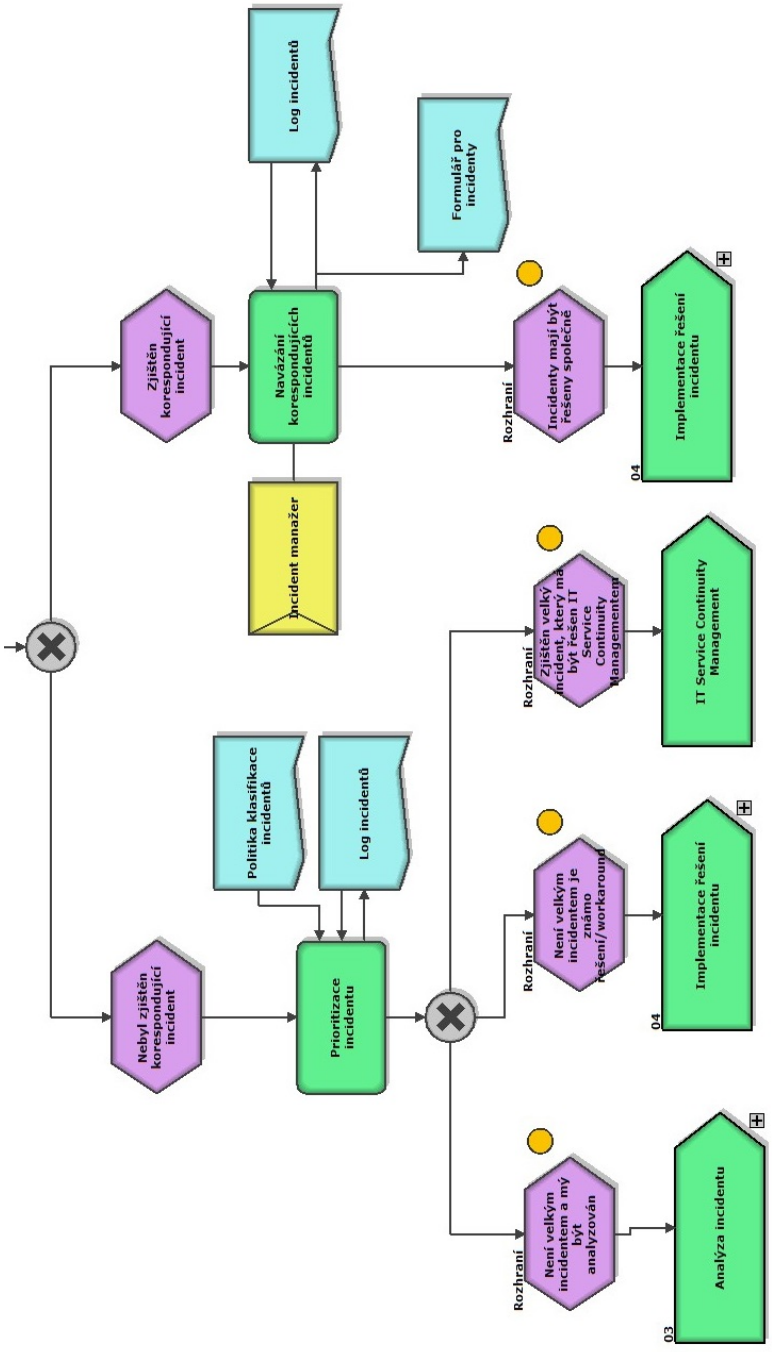
V tomto subprocesu dochází k samotnému nalezení řešení nebo přenesení na vyšší instanci. Vyšší instancí je zde zvolen CAB, který se zabývá většími změnami a formalizovaný proces změn je zaveden. Bylo rozhodnuto, že větší incidenty a jejich řešení musí být vyhodnocována a vytvářena Change managementem. Pokud analýza incidentu nevede do Change managementu, nalezne se řešení nebo workaround na nižší vrstvě podpory. Toto řešení následně směruje do Implementace řešení incidentu.

#### 8.2.3.5 Implementace řešení incidentu

Subproces Implementace řešení incidendu, jak název napovídá, určuje, že musí být provedena implementace analyzovaného řešení. Pokud toto řešení není schváleno a není úspěšné, vrací se incident zpět do analýzy incidentu. Incident management je navržen tak, že incident nemůže být uzavřen, dokud není vyřešen permanentním řešením nebo určitým workaroundem.

#### 8.2.3.6 Vyhodnocení a ukončení incidentu

Je-li implementace řešení incidentu úspěšná, zkontrolují se ještě navázané incidenty. Tyto incidenty jsou potom uzavřeny a je zachována jejich stopa, pro další analýzy a statistiky.




Obrázek 8.8: Výřez modelu eEPC subprocesu Klasifikace incidentu - vlastní zpracování

### 8.2.4 Přínos navrženého řešení

Přínosem tohoto procesu je vyjasnění termínů, které se v Incident management používají.

Návrh procesu upravuje proces Incident managementu a vztahuje řešení i na Change management, který je do procesu zapojen.

Všechny incidenty budou správně vedeny a pokud se objeví incident, který je podobný již vyřešenému incidentu, je možné řešení znovu zanalyzovat a upravit.

V neposlední řadě je přínosem soulad s normou ISO/IEC 20000-1 a připravenost oblasti Incident managementu na certifikaci podle ISO/IEC 20000-1.

## 8.3 Zhodnocení navrženého řešení pro certifikaci ISO/IEC 20000-1

Organizace se může rozhodnout pokud chce certifikaci na určitou normu. Toto rozhodnutí je dobrovolné a potvrzuje soulad zavedených opatření/procesů s požadavky normy. Předchozí dva procesy byly navrženy a namodelovány tak, aby tyto požadavky splňovaly.

Požadavkem normy ISO/IEC 20000-1 je, aby procesy v prostředí organizace byl řízeny a dokumentovány. Nejtěžším krokem je tedy formální zavedení. Namyšlené a namodelované procesy dle best-practices a normy slouží jako základ pro další procesy, které budou v TA ČR navrhovány. Je určen postup, jak tyto procesy navrhovat a čím se řídit.

Implementaci podle ISO/IEC 20000 nelze udělat naráz. Je zde důležitý princip PDCA, který určuje, jak se má implementace navrženého procesu vytvářet.

Na základě těchto dvou procesů a procesu Change managementu, který je již formálně zavedený a implementovaný, se budou postupně skládat nové procesy, které mohou tyto navržené procesy mírně upravovat.

Oblast procesního řízení není statická a vyžaduje flexibilitu. Proto je nutné, aby byly zavedené procesy připraveny pro návrh a implementaci dalších požadavků, které norma ISO/IEC 20000-1 vyžaduje.

Byly navrženy procesy Release and deployment managementu a Incident managementu. Návrhy jsou v souladu s ISO/IEC 20000-1 a podporují řešení problémů popsaných v kapitolách aktuálního stavu.

Navržený Incident management se nebude zabývat jen incidenty, které souvisí se systémem ISTA, ale všemi incidenty, které se v TA ČR vyskytnou.

Kapitola 9

# Návrh politik a opatření TA ČR v souvislosti s ISO/IEC 27000

V této kapitole jsou navrženy některé politiky, tedy pravidla, která slouží k tomu, aby se Technologická agentura ČR v budoucnosti mohla nechat certifikovat na soulad s normou ISO/IEC 27001.

Důležitý pro TA ČR je soulad s regulatorními požadavky, které jsou uvedeny v kapitole 5. Série norem ISO/IEC 27000 pojednává, jak je uvedeno v kapitole 6.3 o ochraně dat a o systému bezpečnosti informací. Norma slouží jako podklad pro vytvoření a aplikaci určitých politik a pravidel, tak aby byla zajištěna ochrana informací..

Norma se zabývá aktivy a riziky spojenými s aktivy. Všechna data, která jako organizace uchováváme, jsou aktiva. Všechen majetek, který Technologická agentura má, je aktivem. Na základě ohodnocení těchto aktiv se poté tvoří opatření, která s těmito aktivy pracují.

Cílem této práce není ohodnotit aktiva, ani vytvořit metodiku hodnocení aktiv, ale navržení určitých opatření a pravidel, které budou sloužit jako první krok k certifikaci ISO/IEC 27001.

V následujících kapitolách budou rozebrány oblasti bezpečnosti, které vyplynuly z analýzy v kapitole 7.3.16. Z těchto oblastí byly vybrány dvě, ke kterým se budou vázat navržené politiky a navržená opatření v souvislosti s certifikací ISO/IEC 27001.

## 9.1 Bezpečnost obecně

Zavedená opatření a politiky postrádají smysl, pokud nejsou lidmi dodržovány. Jak je uvedeno v kapitole 6, jedním z nejčastějších důvodů selhání bezpečnosti je lidský faktor. Je tedy nutné, aby byla zavedena taková politika, která řídí komunikaci bezpečnosti k pracovníkům organizace.

Jelikož Technologická agentura ČR využívá jako prostředek ke sdílení určitých informací platformu Google Suite a Google Drive od spoelčnosti Google, návrhem je:

- aby byla vytvořena sdílená složka bezpečnosti informací, která bude obsahovat řízené dokumenty a politiky, jež budou přístupné všem zaměstnancům;
- pravidelné proškolování zaměstnanců (může být formou e-learningu) o bezpečnostních rizikách a předpisech a opatřeních, které TA ČR předepisuje.

G Suite je certifikovaný na normu ISO/IEC 27001 a je tedy zajištěno certifikací mezinárodního standardu, že jsou informace zabezpečené. [69]

## 9.2 Bezpečnost výměny informací

Informace jsou stěžejním aktivem, kterým se systém řízení bezpečnosti informací zabývá. Způsoby, kterými se informace přenášejí jsou často sporné a měly by být pravidelně revidovány a kontrolovány.

Lidská chyba je rizikem. Tohoto rizika se nelze zbavit, ale jeho pravděpodobnost lze značně snížit. I když je G Suite certifikovanou platformou a údaje na Google Drive jsou zabezpečené, nejsou zabezpečené proti lidské chybě sdílení s nepovolanými osobami.

Lidské pochybení může nastat buď vědomě nebo nevědomě. Zabránit vědomým pochybením je složité, opatření tedy budou sloužit k zabránění nevědomé chyby vytvořením postupů výměny a sdílení informací.

### 9.2.1 Problémy TA ČR související s výměnou informací

V této kapitole jsou uvedeny některé problémy s výměnou informací, které má Technologická agentura ČR a mohou souviset s Release and deployment managementem a Incident managementem.

1) Helpdesk

   Technologická agentura ČR pracuje s osobními údaji uživatelů, kteří používají systém ISTA. Jednou z věcí je problém, kdy přes uživatelský helpdesk probíhá výměna osobních informací, které uživatelé posílají za účelem například vložení do systému. Pokud tyto údaje slouží k

2) E-mail

   Dalším problémem je přenášení informací e-mailem, což u některých kritických informací není žádoucí forma komunikace. Příkladem je například exportování údajů do IS VaVaI, kdy pro zpracovávání je exportní

dávka uživatelem zasílána e-mailem na oddělení TA ČR, kde se data upraví a až poté se do IS VaVaI nahrají.

3) Telefon

Výměna informací telefonickou komunikací není žádoucí, jelikož není žádná auditní stopa o tom, co bylo v telefonátu probíráno. Pokud jsou informace uživatelům sděleny správně, ale uživatel je nenásleduje, může dojít ke sporu a například uživatel nemusí stihnout podání návrhu projektu do ISTA a přijde tak o finanční podporu.

4) Výměna informací při práci z domova

Při práci z domova hrozí riziko napadení sítě uživatele, který z domova využívá připojení k síti prostřednictvím vlastních zařízení. Pokud organizace používá pro připojení do sítě VPN (Virtual Private Network) a zařízení je odcizeno, potom může útočník využít uložených přihlašovacích údajů a organizaci takto napadnout. V období pandemie koronaviru je tento problém ještě více zaznamenatelný.

5) Fyzická média

S používáním fyzických médií nastává problém tehdy, pokud na nich jsou uloženy údaje, které mohou při odcizení tohoto média způsobit určité škody. Pokud jsou bezpečnější způsoby, jak data přenést, neměla by se fyzická média (např. USB Flash Disk vůbec používat). Data uložená na úložišti počítače také nejsou chráněna, pokud není například zavedeno šifrování disků.

### 9.2.2 Návrh řešení problémů souvisejících s výměnou informací

Norma ISO/IEC 27001, stejně tak, jako vyhláška uvedená v kapitole 5.4.1 udávají, že musí být zajištěny postupy a pravidla pro přenos informací. Cílem je zachovat bezpečnost informací přenášených v rámci organizace s jakýmkoli externím subjektem.

Pro řešení výše uvedených problémů je nutné vytvořit pravidla, která budou v organizaci veřejné přístupná a budou komunikována tak, aby v rámci organizace nedošlo k problému, že zaměstnanec není s informační bezpečností obeznámen.

Opatření pro řešení výše uvedených problémů jsou následující:

1) Helpdesk

Opatření:

1. Výměna informací přes helpdesk není chybou. Musí být ale zajištěno:

- šifrovaná komunikace,
- zaznamenávání veškeré komunikace,
- ochrana důvěrnosti,
- nezanechávání důvěrných údajů v komunikaci nebo zajištění jejich vymazání.

2. Při komunikaci upozornit uživatele, aby neposílal svoje osobní údaje nebo údaje někoho jiného, aby nedošlo k porušení osobních práv. Pokud jsou informace přece odeslány, správce musí tyto údaje vymazat, pokud vedou k identifikaci osoby.
3. Při nutnosti výměny osobních informací nebo jiných citlivých informací přesměrovat uživatele na jiný zavedený systém přenosu citlivých informací, ve kterém probíhá řízené uchovávání údajů a jejich pravidelný výmaz.
4. Upgrade nebo přechod na jinou aplikaci helpdesk, která podporuje pravidla zavedená organizací.

2) E-mail

Opatření:

1. Nepoužívat e-mail pro komunikaci jakýchkoliv citlivých údajů, souborů nebo jakýchkoliv dat. E-mail je nebezpečný a snadno napadnutelný prostředek komunikace. Je možné využívat jiné, bezpečnější prostředky komunikace.

3) Telefon

Opatření:

1. Pro komunikaci důležitých informací a postupů nepoužívat telefon jako komunikační prostředek.
2. Pro všechny telefonické hovory používat nahrávání telefonátu a informovat o tom účastníky telefonátu. Nahrávání telefonátu je z důvodu auditní stopy.

4) Výměna informací při práci z domova

Opatření:

1. Zakázání práce z domova z pohledu bezpečnosti.
2. Vytvoření pravidel, která budou platit pro všechny zaměstnance, kteří pracují z domova. Některá pravidla na zařízeních jsou technicky vynutitelná. (Nemožnost připojení k určitým sítím apod.)

5) Fyzická média

Opatření:

1. Zákaz používání fyzických médií pro výměnu informací.
2. Povolení používání šifrovaných fyzických médií.

Opatření uvedená výše byla rozdělena dle typu média. Opatření se dají kategorizovat do jednotlivých politik. Dílčí problémy je tedy možné obecně popsat nezávisle na jednotlivém médiu. Z opatření jsou vytvořena obecná pravidla. Tato pravidla jsou uspořádána v politikách a netýkají se jednotlivých bezpečnostních problémů, ale bezpečnosti obecně. V následujících kapitolách jsou uvedeny návrhy určitých politik, které musí být vytvořeny pro soulad s normou ISO/IEC 27001 a týkají se výše uvedených problémů a opatření.

**Politika pro použití komunikačních zařízení**

Tato politika určuje pravidla pro zaměstnance organizace, kteří používají zařízení poskytnutá organizací. Obsah politiky:

1) datum platnosti politiky,
2) datum poslední revize,
3) popis rolí, na které se tato politika vztahuje;
   - odpovědnosti,
   - povinnosti.
4) popis komunikačních zařízení, na které se tato politika vztahuje;
5) pravidla:
   - pravidla pro získání komunikačních zařízení,
   - pravidla pro používání komunikačních zařízení,
   - pravidla pro vrácení komunikačních zařízení.

**Politika přenosu informací**

Tato politika se týká předpisů přenosu informací. Obsah politiky:

1) datum platnosti politiky,
2) datum poslední revize,
3) popis rolí, na které se tato politika vztahuje;
   - odpovědnosti,
   - povinnosti.
4) klasifikace informací:

- A
- B
- C
- ...

5) pravidla komunikace pro určitou klasifikaci:
   - A
   - B
   - C
   - ...
6) pravidla a postupy pro ochranu před odposloucháváním, kopírováním, pozměněním;
7) postupy pro detekci a ochranu před malwarem;
8) postupy pro likvidaci veškeré podnikové korespondence;
9) postupy pro práci se záznamníky a jinými nahrávacími zařízeními.

Klasifikace informací bude obsahovat i pravidla, která se týkají problematiky GDPR. Pravidla, která budou zavedena musí být v souladu s požadavky GDPR (kapitola 5.1).

## 9.3 Bezpečnost v procesech vývoje

Jelikož se Release and deployment management zabývá zároveň i vývojem, je podle normy ISO/IEC 27001 nutné, aby požadavky, které jsou zahrnuty do vylepšení informačního systému nebo do nového informačního systému, byly vyvozeny z politik a předpisů organizace. Výsledky identifikace těchto požadavků by měly být poté přezkoumány všemi zúčastněnými stranami [35].

### 9.3.1 Problémy TA ČR související s bezpečností v procesech vývoje

V této kapitole jsou uvedeny určité problémy, které má TA ČR v souvislosti s bezpečností procesů vývoje a souvisí s Incident managementem a Release and deployment managementem.

1) Riziko vnesení chyby do produkčního prostředí

   S vysokou frekvencí nasazování nových verzi aplikace je v TA ČR pravděpodobnost zanesení chyby do produkce velmi vysoká. S tím souvisí i bezpečnost aplikace a riziko úniku dat nebo neoprávněných přístupů. Neprovádí se akceptační testy a v požadavcích na nasazení nejsou akceptační kritéria uváděna.

2) Součinnost bezpečnosti s řízením změn

   Pokud existuje změna, která zasahuje do větší části systému nebo postihuje více oblastí systému, nejsou zavedeny bezpečnostní požadavky, které by zajistily ochranu a testování těchto navázaných oblastí. Ve změnových požadavcích jsou uvedeny všechny oblasti, které změna může postihnout, ale nejsou uvedeny z hlediska bezpečnosti. Změnové požadavky se již odkazují na GDPR.

   Součinnost Release and deployment managementu s Change managementem není formálně nastavena. Change management se na vydané změnové požadavky musí doptávat a může zde vzniknout problém, kdy je nasazena nějaká změna nebo zásah do systému, o kterém Change management neví.

3) Problémy vývojového prostředí

   Prostředí TEST se využívá jako vývojové prostředí. Vývojáři na TA ČR využívají prostředí TEST přímo k vývoji, přímo na tomto prostředí se dají upravovat části systému a ovlivňovat tak chod tohoto prostředí. To má za následek, že v případě neřízené úpravy může změna ovlivnit určité části systému, ve kterých se vyskytne chyba.

4) Testování bezpečnosti systému

   Při akceptaci systému po vývoji byly provedeny nezávislé penetrační testy dle OWASP Top 10. Od té doby dodavatel garantuje aktuálnost použitých softwarových komponent a opravuje známé bezpečnostní chyby. Pokud se o nějakém problému ví, je možné chybu napravit nebo počítat s rizikem, že problém nastane. Pokud problém ani není znám, je to horší, jelikož nevíme, co můžeme od systému čekat. Testování bezpečnosti se provádí, ale ne na takové úrovni, jakou vyžaduje norma.

### 9.3.2 Návrh řešení problémů souvisejících s bezpečností v procesech vývoje

Norma ISO/IEC 27001 i s vyhláškou o kybernetické bezpečnosti v kapitole 5.4.1 udávají, že musí být zajištěna bezpečnost informací při vývoji. Vývoj se týká i implementace změn. Vyhláška přímo říká, že musí být zajištěno řízení bezpečnosti pro změny, řízení bezpečnosti vývojového prostředí.

Opatření pro řešení výše uvedených problémů jsou následující:

1) Riziko vnesení chyby do produkčního prostředí;

   Opatření:

   1. Zajištění bezpečnosti formálního procesu Release and deployment managementu, což zajišťují bezpečnostní požadavky ve fázi návrhu požadavku a bezpečnostní kontrolní body ve fázích implementace.

Získání záruky od dodavatele systému, pokud není vývoj prováděn organizací interně. Vývoj aplikace ISTA probíhá jak dodavateli, tak interními vývojáři. Je tedy nutné zajistit bezpečnost z obou dvou zdrojů.

2. Zajištění řízení verzí, které už je z části řízeno, ale není formálně popsáno v dokumentu.
3. Proškolování vývojářů ohledně bezpečnosti informací a zajištění kurzů v souvislosti s bezpečným vývojem.

2) Součinnost bezpečnosti s řízením změn

Opatření:

1. Doplnění odkazu na bezpečnostní požadavky do formulářů změnového požadavku.
2. Doplnění role bezpečnostního manažera jako klíčové osoby ve změnovém požadavku.
3. Zapojení bezpečnostního manažera do procesu řízení změn, aby vnesl pohled ze strany bezpečnosti informací.
4. Implementace Release and deployment managementu a provázání řízení změn s nasazováním nových změn.

3) Problémy vývojového prostředí

Opatření:

1. Formální vytvoření postupů pro konfiguraci systému a postupy pro nakládání s informacemi ve vývojovém prostředí, jelikož neformálně jsou postupy zavedeny.
2. Měly by být formálně zavedeny postupy verzování dat a postupy pro jejich zálohování.

4) Testování bezpečnosti systému

Opatření:

1. Zavedení pravidelného testování aplikace proti kybernetickým útokům;
2. Zavedení pravidelného bezpečnostního interního auditu.

Tato opatření lze opět shrnout obecně do pravidel a politik, které se týkají systému řízení bezpečnosti informací.

#### Úprava politiky řízení změn

K již vytvořeným postupům a zavedenému formálnímu řízení změn přibude součinnost s Release and deployment managementem a řízením bezpečnosti. Ucelí se tak pohled na celý průběh změny a nasazení nových změn. Bezpečnosti informací propojení těchto dvou procesů pomůže, jelikož se dobrou součinností těchto dvou procesů zamezí komunikačnímu šumu.

#### Politika bezpečného vývoje

Tato politika by měla být stanovena a pravidla, která z ní plynou, by měla být uplatněna pro vývoj softwaru a systémů. Bezpečný vývoj lze popsat jako požadavek na vytváření bezpečných služeb, architektury, softwaru a systému. Obsah politiky je následující:

1) datum platnosti politiky,
2) datum poslední revize,
3) popis rolí, na které se tato politika vztahuje;
    - odpovědnosti,
    - povinnosti.
4) opatření bezpečnosti vývojového prostředí,
5) postupy bezpečného vývoje:
    - bezpečnost v metodologii vývoje,
    - směrnice bezpečného programování,
6) bezpečnost verzování.

Vytvoření politiky pro bezpečný je pouze prvním krokem ke zlepšení. Při zavedení tohoto návrhu se musí politika vynutit, aby byla zaměstnanci Technologické agentury dodržována. Vývoj na TA ČR probíhá i externě, musí se tedy získat záruka od dodavatelů, že vývoj probíhá bezpečně. Ve smlouvách mezi TA ČR a třetí stranou jsou obsaženy i požadavky na bezpečnost.

## 9.4 Bezpečnostní politika

Vytvořené politiky nemohou obsahovat všechna pravidla a opatření. V politikách bude obsažen pouze základní rámec a pravidla. Politiky se budou odkazovat na tyto provozní postupy.

Všechny zavedené politiky, postupy a zavedená opatření jsou zastřešena hlavním dokumentem bezpečnosti informací, kterým je bezpečnostní politika.

Bezpečnostní politika musí být schválená managementem a stanovuje přístup organizace k řízení cílů bezpečnosti informací. Bezpečnostní politika Technologické agentury ČR je v současné době revidována (k datu 20. 5. 2020).

Po vytvoření výše uvedených návrhů politik bude bezpečnostní politika těmito vytvořenými politikami podporována. Bezpečnostní politika se na dílčí politiky bude odkazovat. Politiky jsou strukturované tak, aby pokrývaly určité oblasti bezpečnosti informací organizace podle potřeby organizace.

## 9.5 Neustálé zlepšování

Předpisy a zavedené politiky se mohou upravovat a měnit. Je zde důležitý cyklus Plan-Do-Check-Act. Tyto dokumenty se nejdříve naplánují, poté se implementují, dále se zkontroluje, zda jsou nastaveny správně a nakonec se jedná s výsledky, které jsou vstupem pro další cyklus PDCA. Neustálé zlepšování je jedním z požadavků normy ISO/IEC 27001 a neustálé zlepšování je uvedeno také v regulatorních požadavcích v kapitole 5.4.1.

## 9.6 Přínos navrženého řešení pro TA ČR

Technologická agentura ČR v oblasti řízení bezpečnosti má zavedeny jisté směrnice, které se zabývají uričtými tématy, která jsou uvedená výše. Pro certifikaci podle ISO/IEC 27001 se musí politiky vytvořit a pravidelně revidovat. Politika se musí udržovat jako řízený dokument s daty vytvoření, revize nebo ukončení platnosti dokumentu.

Vytvoření těchto politik a zavedení pravidel by přineslo TA ČR výhodu jednotného způsobu vyměňování informací. Jelikož se Technologická agentura ČR spoléhá na uvědomělost svých zaměstnanců, nejsou formálně zavedena pravidla pro výměnu informací. Některé směrnice na toto téma odkazují, ale neexistuje jeden nebo více ucelených dokumentů k dispozici na jednom místě. Zavedení těchto politik by vedlo k větším povědomí o bezpečnosti informací. Musí být zajištěny nejenom politiky, ale i jejich neustálá komunikace a školení pro zaměstnance, aby se Technologická agentura v budoucnu mohla certifikovat na ISO/IEC 27001.

Zavedením politik bezpečného řízení vývoje a jejich vynucováním se zajistí ochrana informací, které zasahují do celého cyklu vývoje informačního systému.

Bezpečnostní politika se bude na nové implementované politiky odkazovat s cílem zajištění vyšší bezpečnosti informací v celém cyklu poskytování služeb.

Technologická agentura ČR bude zavedením návrhů nových bezpečnostních politik blíže k certifikaci podle ISO/IEC 27001, jelikož tyto politiky pokrývají část požadavků normy ISO/IEC 27001.

Kapitola 10

# Zhodnocení řešení a další možný rozvoj

Navržená řešení procesů a bezpečnostních politik slouží jako část práce, která bude použita k budoucí certifikaci Technologické agentury ČR na normy ISO/IEC 20000-1 a ISO/IEC 27001. Témata systém řízení bezpečnosti informací a systém managementu služeb jsou velice rozsáhlá. Z těchto témat byly vybrány na základě analýzy nejdůležitější části, které v poměru cena/výkon vytváří největší přidanou hodnotu pro aktuální stav v Technologické agentuře ČR. Vytvoření procesů a politik, které zcela pokrývají obě normy je nad rámec diplomové práce.

Nový proces Release and deployment managementu poskytne Technologické agentuře ČR větší kontrolu nad změnami, které se vnášejí do systému. Poskytne i kontrolu nad dílčími částmi systému, které mohou být nasazením nové verze aplikace ovlivněné. Proces se může dále aplikovat nejen na systém ISTA, ale i na jiné systémy, které TA ČR v budoucnu může používat. Proces Release and deployment management byl navrhnut podle požadavků ISO/IEC 20000-1.

Proces Incident managementu poskytne přehled o událostech, které ovlivňují poskytování služeb. Nastavení nového procesu Incident managementu umožní Technologické agentuře ČR na incidenty lépe reagovat a potažmo bude sloužit i k vyvarování se již nastalých incidentů nebo předcházení nových incidentů. Incident management byl navrhnut podle nejlepších praktik a podle požadavků uvedených v ISO/IEC 20000-1.

Implementace návrhů procesů je vytvořena v nástroji ARPO BPMN++ Modeler, který podporuje metodiku ARIS a provázání jednotlivých procesů. V přiloženém médiu této práce je HTML stránka s interaktivním modelem, kterým je možné ukázat vzájemné propojení jednotlivých procesů. Vytvořené modely budou postupně vkládány do procesního modelu TA ČR, který je popsaný v kapitole 3.2.1.

Implementace návrhů politik umožní Technologické agentuře ČR integraci procesního rámce do prostředí, které je bezpečné. Návrhy politik a jejich strukturování umožní Technologické agentuře ČR pohled shora na celou problematiku bezpečnosti informací.

Návrh politik je na základě požadavků ISO/IEC 27001 a poskytuje bezpečnostní rámec pro integraci procesů Release and deployment managementu a Incident managementu.

## 10.1 Další rozvoj

Části z diplomové práce budou použity do revize bezpečnostní politiky. Jelikož součástí diplomové práce není zpracování všech politik a procesů uvedených v použitých normách, dalším rozvojem této práce bude postupná integrace dalších procesů a politik, za účelem certifikace ISO/IEC 27001 a ISO/IEC 20000-1.

Rozvoj bude také probíhat během implementace těchto návrhů. Tyto návrhy se budou implementovat pomocí změnového řízení TA ČR a některé požadavky jsou již zavedeny ve změnovém řízení. Konkrétně probíhá iniciace změny - Zavedení Release notes. Tímto se dále i ověří zavedený proces změnového řízení. Každý proces bude zaváděn postupně, malými dílčími kroky, které se budou revidovat a upravovat, až do té doby, než vznikne finální produkt, který bude připraven na certifikaci.

Stejným způsobem se budou zavádět i politiky a postupy pro systém bezpečnosti informací. Navržené politiky se vytvoří a postupnými kroky se bude provádět implementace za účelem certifikace ISO/IEC 27001.

# Závěr

Cílem této diplomové práce bylo nastudovat informace problematiky bezpečnosti informací, řízení IT služeb a regulatorních požadavků, a využít nastudované informace k analýze procesů TA ČR v souvislosti s bezpečností informací. Dalším cílem bylo vytvořit na základě této analýzy návrh úprav procesů a politik za účelem certifikace ISO/IEC 20000-1 a ISO/IEC 27001. Na závěr bylo cílem zhodnotit navržené řešení a přínos pro TA ČR.

Pro uvedení práce do kontextu procesního řízení byla nejprve nastudována problematika procesního a funkčního řízení organizace. Dále byly nastudovány metodiky pro procesní řízení IT služeb a řízení bezpečnosti informací. Jedná se o ITIL, a série norem ISO/IEC 20000 a ISO/IEC 27000.

Dále byl nastudován nástroj SW ARPO, který Technologická agentura ČR využívá pro modelování svých procesů a bylo nutné jej tedy v této práci využít. Byly nastudovány jednotlivé notace a modely, které se pro modelování procesů v TA ČR využívají.

Pro účely analýzy a návrh samotného řešení úpravy procesů a politik v TA ČR byly vybrány metodiky pro řízení IT služeb a bezpečnosti informací. Analýza procesů TA ČR probíhala na základě požadavků série norem ISO/IEC 20000 ISO/IEC 27000 a byl porovnán aktuální stav procesů TA ČR s těmito normami.

Na základě analýzy byly dále vybrány dva procesy, které byly na základě metriky cena/výkon určeny k návrhu a úpravě. Těmito procesy jsou Release and Deployment Management a Incident Management. Tyto procesy byly navrženy a namodelovány v softwaru SW ARPO. Procesy byly navrženy tak, aby splňovaly požadavky, které určuje norma ISO/IEC 20000-1 a přispěly k možnosti certifikace ISO/IEC 20000-1.

Jako první byl navržen proces Release and Deployment Management. Aktuálně probíhá na základě určených postupů a pravidel, která nejsou formálně popsána. Hlavní změnou oproti aktuálnímu stavu je formální zavedení procesu, využití všech dostupných aplikačních prostředí, zavedení určitých rolí, pro které byly stanoveny odpovědnosti a povinnosti.

Dále byl navržen Incident Management, který je nyní využíván v rámci systémových chyb ISTA. Nové řešení poskytuje obecný pohled na řízení incidentů napříč celou agenturou. Návrh nového řešení určuje chod procesu od vzniku incidentu, přes klasifikaci, analýzu, řešení incidentu, až po uzavření a vyhodnocení incidentu. Evidence všech incidentů napříč celou agenturou vede k efektivnějšímu řešení incidentů a vyvozování závěrů, které budou sloužit ke vzniku preventivních opatření proti novým incidentům.

Na základě normy ISO/IEC 27001 byly navrženy určité politiky, které souvisí s bezpečností informací a vybranými procesy Release and Deployment Managementu a Incident Managementu. Jedná se o politiku bezpečného vývoje, politiku pro použití komunikačních zařízení a politiku přenosu informací.

Na závěr byly jednotlivé návrhy zhodnoceny. Byl zhodnocen přínos návrhů pro TA ČR a byl popsán další možný rozvoj této práce.

Tato práce slouží jako první krok k získání certifikace ISO/IEC 20000-1 a ISO/IEC 27001. Do budoucna může práce také sloužit jako know-how Technologické agentury ČR při vytváření nových podnikových procesů, úpravě stávajících procesů a vytváření pravidel bezpečnosti informací.

# Bibliografie


1. FIŠER, Roman. *Procesní řízení, řízení procesů* [online] [cit. 2020-03-10]. Dostupné z: `https://www.attis.cz/procesni-rizeni-rizeni-procesu`.
2. URBAN, Jan. *PROCESNÍ ŘÍZENÍ* [online]. 2017 [cit. 2020-03-03]. Dostupné z: `https://news.cafin.cz/clanek/procesni-rizeni`.
3. ŘEPA, Václav. *Podnikové procesy: Procesní řízení a modelování, 2., aktualizované a rozšířené vydání.* Grada Publishing a.s. ISBN 9788024767222.
4. SWAN, Tony. *Ford's Assembly Line Turns 100: How It Really Put the World on Wheels* [online]. 2013 [cit. 2020-04-10]. Dostupné z: `https://www.caranddriver.com/features/a15115930/fords-assembly-line-turns-100-how-it-really-put-the-world-on-wheels-feature/`.
5. VERKERK, Maarten. *Trust and Power on the Shop Floor: An Ethnographical, Ethical and Philosophical Study on Responsible Behaviour in Industrial Organisations.* Eburon Uitgeverij B.V. ISBN 9059720334.
6. ŠMÍDA, Filip. *Zavádění a rozvoj procesního řízení ve firmě.* Grada Publishing a.s. ISBN 8024716798.
7. *ČSN EN ISO 9001 Systémy managementu kvality - Požadavky.* Biskupský dvůr 1148/5, Praha 1, Česká republika, 2015-09. Dostupné také z: `https://www.iso.org/standard/62085.html`. Česká technická norma (ČSN). Česká agentura pro standardizaci.
8. MANAGEMENTMANIA.COM. *Procesní řízení (Process-based management).* [online]. 2019 [cit. 2020-02-27]. Dostupné z: `https://managementmania.com/cs/procesni-rizeni`.
9. ATTIS SOFTWARE S.R.O. *FUNKČNÍ ŘÍZENÍ* [online] [cit. 2020-05-11]. Dostupné z: `https://www.attis.cz/organizacni-struktura-podniku/funkcni-rizeni`.

10. MANAGEMENTMANIA.COM. *Řízení procesů (Process Management).* [online]. 2016 [cit. 2020-05-11]. Dostupné z: https://managementmania.com/cs/rizeni-procesu.

11. BM SERVIS. *Procesní versus funkční řízení podniku* [online] [cit. 2020-05-11]. Dostupné z: http://www.bmservis.cz/blog-informacni-systemy/procesni-versus-funkcni-rizeni-podniku/.

12. POKORNÁ, Olga. *SROVNÁNÍ FUNKČNÍHO A PROCESNÍHO PŘÍSTUPU K ŘÍZENÍ ORGANIZACE* [online]. 2008 [cit. 2020-05-11]. Dostupné z: https://adoc.tips/srovnani-funkniho-a-procesniho-pistupu-k-izeni-organizace.html.

13. ŘEPA, Václav. *Procesně řízená organizace*. Grada Publishing a.s. ISBN 9788024778662.

14. TA ČR. *O nás* [online]. 2020 [cit. 2020-05-11]. Dostupné z: https://www.tacr.cz/o-nas/.

15. TA ČR. *AUDIT ČINNOSTI TA ČR* [online]. 2020 [cit. 2020-02-27]. Dostupné z: https://www.tacr.cz/dokums_raw/urednideska/CSProject_Audit%20%C4%8Dinnost%C3%AD%20TA%20%C4%8CR.pdf.

16. TA ČR. *O nás* [online] [cit. 2020-05-11]. Dostupné z: https://www.tacr.cz/wp-content/uploads/documents/2019/10/03/1570108321_Brozura_TACR.pdf.

17. SLUŽBY PRO MĚSTA A OBCE. *Procesní řízení* [online] [cit. 2020-05-12]. Dostupné z: https://spmo.cz/sluzby-pro-mesta-a-obce/procesni-rizeni/.

18. TECHNOLOGICKÁ AGENTURA ČR. *Procesní model TA ČR* [online]. 2020 [cit. 2020-05-12]. Dostupné z: https://procesnimodel.tacr.cz/.

19. TECHNOLOGICKÁ AGENTURA ČR. *Slovní popis procesního modelu* [online]. 2019 [cit. 2020-05-12]. Dostupné z: https://docs.google.com/document/d/1gJe6T9EDyfzX1lCgvl6Q7cMJoN9zlsiuKatEHUQ2rgQ/edit.

20. VLASÁK, Vítězslav. *Informační schůzka o procesním modelu TA ČR* [rozhovor]. Evropská 1692, 160 00 Praha 6, 2020.

21. KLUG SOLUTIONS. *Uživatelská dokumentace k SW ARPO* [online]. 2019 [cit. 2020-04-25]. Dostupné z: https://www.klugsolutions.cz/znalostni-baze/index.htm.

22. AHASWARE S.R.O. *AHASWARE s.r.o.* [online]. 2020 [cit. 2020-05-15]. Dostupné z: http://ahasware.cz/.

23. SOFTWARE AG. *Process landscape* [online]. 2020 [cit. 2020-04-13]. Dostupné z: https://www.ariscommunity.com/process-landscape.

24. NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Grada Publishing, 2017. ISBN 978-80-271-0668-4.

25. ČESKO. *Zákon č. 110/2019 Sb.* [online] [cit. 2020-04-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110.

26. CETKOVSKÁ, Barbora; MÁLEK, Jakub. *Adaptační zákon k GDPR byl konečně přijat* [online]. 2019 [cit. 2020-04-25]. Dostupné z: https://www.epravo.cz/top/clanky/adaptacni-zakon-k-gdpr-byl-konecne-prijat-109122.html.

27. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Základní příručka k ochraně údajů* [online]. 2019 [cit. 2020-04-25]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-ochrane-udaju/ds-4744/p1=4744.

28. ČESKO. *Zákon č. 130/2002 Sb.* [online] [cit. 2020-04-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2002-130.

29. ČESKO. *Zákon č. 181/2014 Sb.* [online] [cit. 2020-04-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181.

30. NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI. *CO JE NCKB* [online]. 2020 [cit. 2020-03-13]. Dostupné z: https://www.govcert.cz/.

31. ČESKO. *Vyhláška č. 82/2018 Sb.* [online] [cit. 2020-04-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82.

32. GOLL, Jan. *Zákon o kybernetické bezpečnosti versus ISO 27001* [online]. 2019 [cit. 2020-05-20]. Dostupné z: http://m.systemonline.cz/sprava-it/zakon-o-kyberneticke-bezpecnosti-versus-iso-27001.htm.

33. TA ČR. *Dílčí strategie ICT TA ČR.* 2019.

34. MINISTERSTVO VNITRA ČR. *AIS RPP Působnostní* [online]. 2019 [cit. 2020-03-13]. Dostupné z: https://rpp-ais.egon.gov.cz/AISP/verejne/isvs/zobrazeni-isvs/18134%20.

35. *ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.* Biskupský dvůr 1148/5, Praha 1, Česká republika, 2014-09. Dostupné také z: https://www.iso.org/standard/54534.html. Česká technická norma (ČSN). Česká agentura pro standardizaci.

36. FRUHLINGER, Josh. *The CIA triad: Definition, components and examples* [online]. 2020 [cit. 2020-03-13]. Dostupné z: https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html.

37. UNIVERSITY OF CALIFORNIA, SAN FRANCISCO. *IT Service Continuity Management* [online] [cit. 2020-03-13]. Dostupné z: https://itsm.ucsf.edu/it-service-continuity-management.

38. ČESKO. *Zákon č. 219/2000 Sb.* [online] [cit. 2020-04-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-219.

39. BDO. *Řízení IT služeb* [online]. 2014 [cit. 2020-03-13]. Dostupné z: http://bdo-it.cz/cz/rizeni-ict-projektu.

40. GITY, A.S. *Zavedení systému řízení bezpečnosti* [online] [cit. 2020-03-13]. Dostupné z: http://www.chrantesidata.cz/cs/art/472-isms-serial-o-rizeni-bezpecnosti.

41. SEIGE, Viktor. *Informační bezpečnost? Proč ne!* [online]. 2020 [cit. 2020-03-13]. Dostupné z: https://www.systemonline.cz/clanky/informacni-bezpecnost-proc-ne.htm?mobilelayout=false.

42. EZDRAV.CZ. *Pochybení zaměstnanců patří mezi nejčastější příčiny úniku dat i v Česku* [online]. 2020 [cit. 2020-03-13]. Dostupné z: http://ezdrav.cz/pochybeni-zamestnancu-patri-mezi-nejcastejsi-priciny-uniku-dat-i-v-cesku/.

43. AXELOS. *WELCOME TO THE OFFICIAL ITIL® WEBSITE* [online]. 2020 [cit. 2020-04-15]. Dostupné z: https://web.archive.org/web/20141022043004/http://www.itil-officialsite.com/home/home.asp.

44. GREENE, Jarod. *The Essential Guide to ITIL Framework and Processes* [online]. 2020 [cit. 2020-04-15]. Dostupné z: https://www.cherwell.com/library/essential-guides/essential-guide-to-itil-framework-and-processes/.

45. AXELOS. *ITIL® Update* [online]. 2020 [cit. 2020-04-15]. Dostupné z: https://www.axelos.com/itil-update.

46. DCIT, A.S. *Procesní řízení IT* [online]. 2020 [cit. 2020-04-15]. Dostupné z: https://www.dcit.cz/cs/konzultace/procesni-rizeni-IT.

47. TUTORIALSPOINT. *ITIL - Service Strategy Overview* [online]. 2020 [cit. 2020-04-15]. Dostupné z: https://www.tutorialspoint.com/itil/service_strategy_overview.htm.

48. TOPALOVIC, Drago. *ITIL Service Strategy: What and Why of ITSM* [online]. 2020 [cit. 2020-04-15]. Dostupné z: https://advisera.com/20000academy/knowledgebase/itil-service-strategy-itsm/.

49. BRAHMACHARY, Ayan. *ITIL Service Operation Processes Explained | ITIL Foundation | ITSM* [online]. 2018 [cit. 2020-04-15]. Dostupné z: https://www.certguidance.com/itil-service-operation-explained-itsm/.

50. BRAHMACHARY, Ayan. *ITIL Service Transition Processes Explained | ITIL Foundation | ITSM* [online]. 2018 [cit. 2020-04-15]. Dostupné z: https://www.certguidance.com/itil-service-transition-explained-brief/.

51. BRAHMACHARY, Ayan. *ITIL Service Design Processes Explained | ITIL Foundation | ITSM* [online]. 2019 [cit. 2020-04-15]. Dostupné z: https://www.certguidance.com/itil-service-design-explained-brief/.

52. BRAHMACHARY, Ayan. *ITIL Continual Service Improvement | ITIL Foundation | ITSM* [online]. 2018 [cit. 2020-04-15]. Dostupné z: https://www.certguidance.com/continual-service-improvement-itil-itsm/.

53. DUGMORE, Jenny; LACY, Shirley. *The Differences Between Bs 15000 and Iso/Iec 20000*. BSI British Standards Institution. ISBN 9780580473487.

54. A-KOMPLEX. *MANAGEMENT SLUŽEB IT - ISO/IEC 20000-1* [online]. 2020 [cit. 2020-04-20]. Dostupné z: https://www.akomplex.eu/poradenstvi/iso-iec-20000-1/.

55. *ČSN ISO/IEC 20000-1 Informační technologie - Management služeb - Část 1: Požadavky na systém managementu služeb*. Biskupský dvůr 1148/5, Praha 1, Česká republika, 2019-10. Dostupné také z: https://www.iso.org/standard/70636.html. Česká technická norma (ČSN). Česká agentura pro standardizaci.

56. CERTIFIKACE MANAŽERSKÝCH SYSTÉMŮ. *Certifikace systému managementu služeb podle normy ISO / IEC 20000-1* [online]. 2020 [cit. 2020-04-25]. Dostupné z: https://www.cems-cz.com/produkt/68-certifikace-systemu-managementu-sluzeb-podle-normy-iso-iec-20000-1.

57. *ČSN EN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. Biskupský dvůr 1148/5, Praha 1, Česká republika, 2020-06. Dostupné také z: https://www.iso.org/news/ref2266.html. Česká technická norma (ČSN). Česká agentura pro standardizaci.

58. ZITEK, Neven. *ISO 20000 and ITIL – How are they related?* [online] [cit. 2020-04-30]. Dostupné z: https://advisera.com/20000academy/knowledgebase/iso-20000-and-itil-how-are-they-related/.

59. CHARLET, Laurent. *THE ISO SURVEY* [online]. 2018 [cit. 2020-04-30]. Dostupné z: https://www.iso.org/the-iso-survey.html.

60. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO Survey of certifications to management system standards - Full results* [online]. 2018 [cit. 2020-04-30]. Dostupné z: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1.

61. BSI. *Certification to ISO/IEC 20000-1 Service Management* [online]. 2018 [cit. 2020-04-30]. Dostupné z: https://www.bsigroup.com/en-IN/ISOIEC-20000-IT-Service-Management/Certification-for-ISO-20000/.

62. VALENTIC, Branimir. *ITIL and ISO 20000: A Comparison* [online] [cit. 2020-04-30]. Dostupné z: https://advisera.com/20000academy/knowledgebase/itil-iso-20000-comparison/.

63. LUPTÁK, Radovan. *Informační schůzka o provozu TA ČR* [rozhovor]. Evropská 1692, 160 00 Praha 6, 2020.

64. KUBÍČEK, Vladimír. *Informační schůzka o infrastruktuře TA ČR* [rozhovor]. Evropská 1692, 160 00 Praha 6, 2020.

65. COMPUTER CAREERS. *Software Release Management: What You Need To Know* [online]. 2019 [cit. 2020-05-15]. Dostupné z: https://www.computercareers.org/software-release-management-what-you-need-to-know/.

66. OFFICE OF GOVERNMENT COMMERCE. *ITIL Service Transition*. TSO (The Stationery Office). ISBN 978 0 11 331048 7.

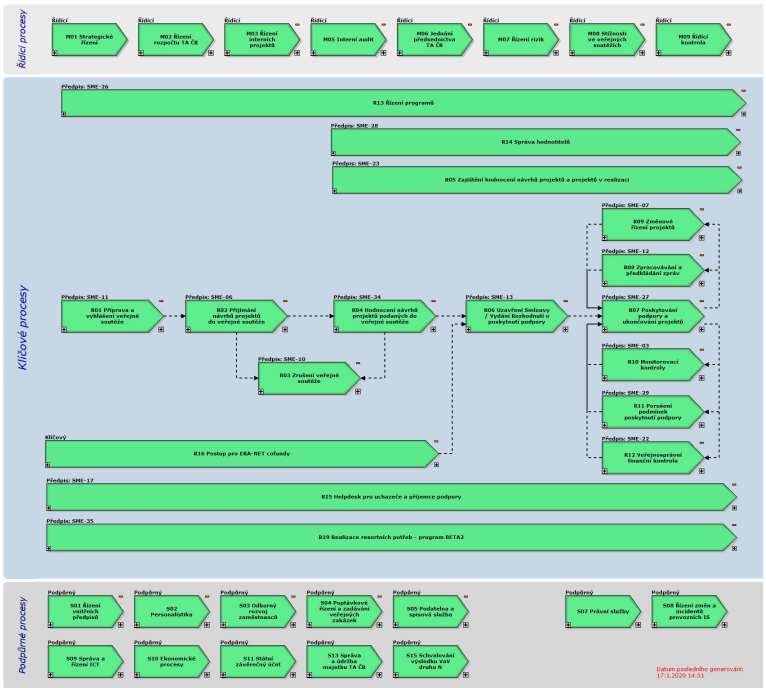
67. TECHNOLOGICKÁ AGENTURA ČR. *ISTA* [online] [cit. 2020-05-15]. Dostupné z: https://ista.tacr.cz/.

68. OFFICE OF GOVERNMENT COMMERCE. *ITIL Service Operation*. TSO (The Stationery Office). ISBN 978 0 11 331046 3.

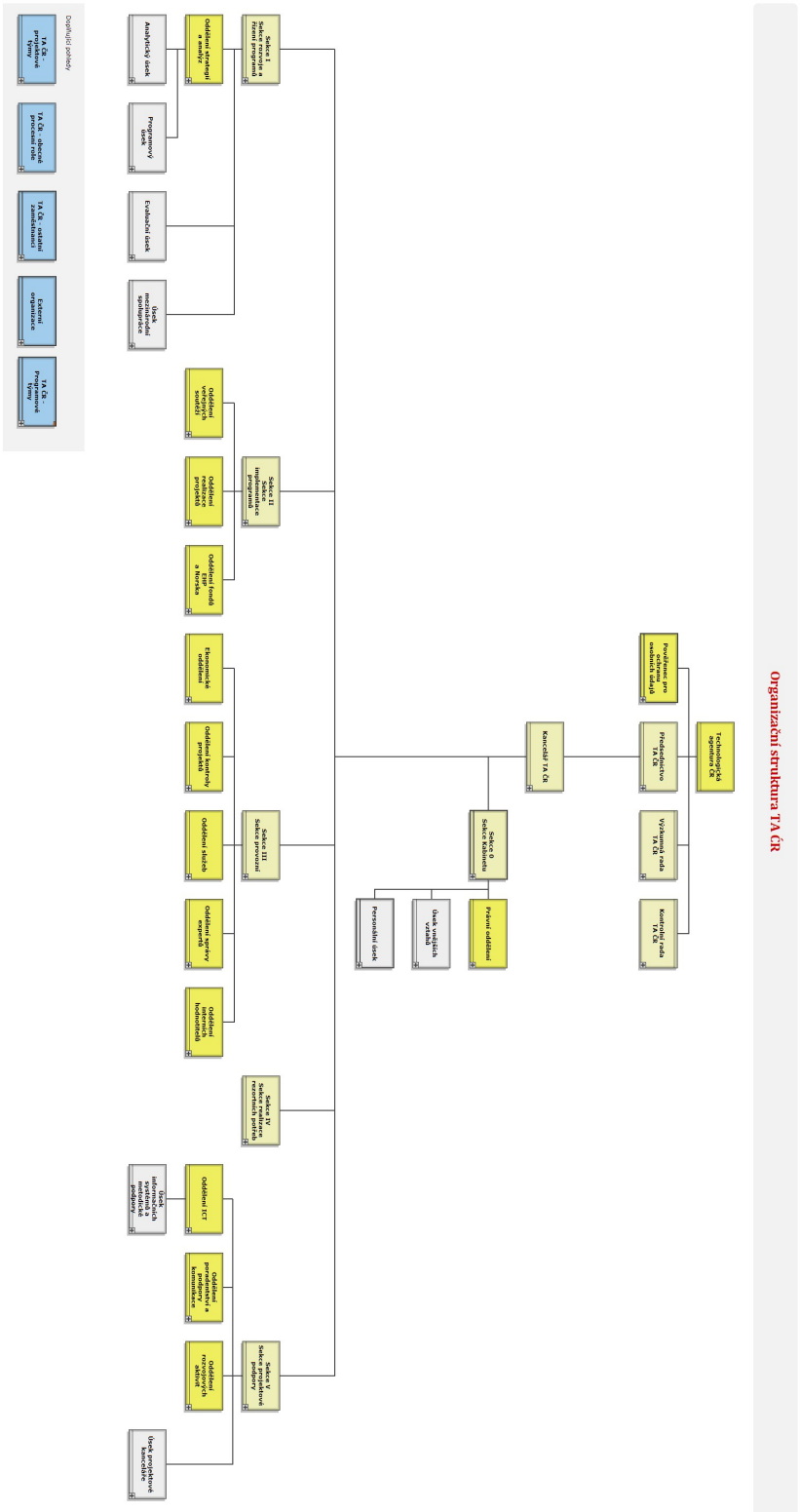
69. GOOGLE. *ISO/IEC 27001* [online] [cit. 2020-05-10]. Dostupné z: https://cloud.google.com/security/compliance/iso-27001.

Dodatek A

# Obrázky a modely




Obrázek A.1: Procesní model TA ČR




Obrázek A.2: Organizační struktura TA ČR

Dodatek **B**

# Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `src`
  - `thesis` ..... adresář se zdrojovou formou práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF