B R N O

Datum 1.10.2020
Počet stran 71
Verze 3.00

Analýza současného stavu (SWOT)

Strategické cíle (na období 2020 až 2024)

Strategická mapa (Balanced Scorecard schéma)

Implementace strategie (strategické projekty)

Aktualizace Informační strategie města Brna

Na období 2020 - 2024

Změnové řízení dokumentu

Verze	Datum	Autor	Popis či komentář změny	Elektronický soubor
1.00	28.11.2011	Per Partes	Uvolněná verze po přezkoumání	111128 Informacni strategie (MMB) v1_00
1.01	6.12.2011	Per Partes	Formální úprava textu	111206 Informacni strategie (MMB) v1_01
2.00	11.5.2015	Per Partes	Aktualizace strategie na období 2015 až 2018	150511 Informacni strategie (MMB) v2_00
3.00	1.10.2020	Per Partes	Aktualizace strategie na období 2020 až 2024	201001 Informacni strategie (MMB) v3_00

Obsah

Úvodní shrnutí

Informační strategie je základním dokumentem pro strategické řízení v oblasti informatiky města Brna.

Předkládaný dokument „Aktualizace informační strategie města Brna“ byl vyhotoven strategickým týmem (uvedeným v kap. 1. *Základní identifikace a klíčové pojmy*) v rámci pracovních setkání konaných v měsících lednu až září 2020. Odráží názor tohoto týmu na strategický rozvoj informatiky města Brna a jsou v něm formulovány strategické cíle a k nim příslušné realizační projekty do konce roku 2024. Plánování je zde dovedeno až do určení portfolia konkrétních strategických projektů. Samotná informační strategie je pak sladěna se strategií *Vize a Strategie #brno 2050* a vizí informatiky města dosahuje na tento dlouhodobý horizont. Dokument aktualizuje předchozí informační strategii města Brna vytvořenou na roky 2015 až 2018.

Město Brno

Město Brno je ve smyslu čl. 99 zákona č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů, ve spojení s § 3 zákona č. 128/2000 Sb., o obcích, ve znění pozdějších předpisů (dále jen "zákon o obcích"), základním územně samosprávným celkem, tj obcí. Obec je dle § 2 zákona o obcích veřejnoprávní korporací s vlastním majetkem, pečující o všestranný rozvoj svého území a o potřeby svých občanů, a při plnění svých úkolů chrání též veřejný zájem. Za účelem naplnění těchto svých úkolů město Brno, kromě jiného, zřizuje příspěvkové organizace, organizační složky města a obchodní korporace (dále společně také jen "dotčené subjekty").

Město Brno je zároveň dle § 4 zákona o obcích statutárním městem. Území města Brna je v souladu se Statutem města Brna členěno na 29 městských částí, které jsou organizačními jednotkami města Brna.

V rámci péče o všestranný rozvoj svého území a o potřeby svých občanů město Brno zpracovává tento dokument "Aktualizace informační strategie města Brna", upravující strategický rozvoj informatiky města Brna, kterým město Brno formuluje strategické cíle a k nim navrhuje zpracovat příslušné realizační projekty v oblasti informatiky s výhledem do konce roku 2024. Město Brno, jeho městské části, jakož i dotčené subjekty jsou povinny, v rámci péče o všestranný rozvoj svého území a o potřeby svých občanů, a v rámci jim svěřených pravomocí, cíle stanovené dokumentem "Aktualizace informační strategie města Brna" zohledňovat při plnění svých úkolů.

Strategické cíle

Při zpracování informační strategie byla aplikována metoda Balanced Scorecard. Základem informační strategie je strategická mapa dávající do souvislosti vytyčené strategické cíle z hlediska jejich vzájemných kauzálních vazeb (viz kap. 3.3.1. *Strategická mapa*). Cíle byly v souladu s touto metodou zasazeny do čtyř strategických perspektiv. Podrobně jsou cíle rozebrány v kap. 3. *Návrh cílového stavu.* Následující tabulka udává souhrn strategických cílů, přičemž horní perspektiva ICT přínosů formuluje přínosy dosažené touto informační strategii pro nadřazenou strategii *Vize a Strategie #brno 2050*.

Perspektiva	Motto	Cíle
ICT přínosy	Moderní ICT města	Elektronizace služeb veřejné správy (elektronická radnice) Vytvořit moderní, společné a bezpečné ICT města Otevření městských dat veřejnosti
ICT zákazníci	Motivace k využívání elektronických služeb	Poskytovat elektronické služby přes internetovou přepážku v uživatelsky intuitivní a jednotné podobě Podporovat využívání cloudových služeb městskými firmami Rozšířit využívání aplikací v městském cloudu podle závazných standardů Posilovat důvěru ve sdílení dat a propagovat otevřená data a jejich využití
Procesy	Umožnit technologiemi elektronické služby	Podpořit technologiemi workflow pro elektronicky poskytovatelné služby Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce v cloudu Architektonicky řídit ICT města a vytvořit městské ICT standardy Poskytovat z informačních systémů data klasifikovaná jako veřejná
ICT potenciál a zdroje	Náskok v aplikaci moderních digitálních technologií	Vytvořit platformu pro moderní portál města Zavést eIDAS (elektronická identita a důvěryhodné el. dokumenty) Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách Vytvořit sdílený městský cloud postavený na odolné infrastruktuře vč. datových úložišť Posílit datovou integraci přes integrační platformu

Tab.1: Přehled strategických cílů

Strategické projekty

Pro každý cíl je zpracováno měřítko jeho dosažení a stanoveny hodnoty, kterých má být v rámci strategie dosaženo. Naplnění strategických cílů je plánováno realizovat 11 strategickými projekty rozloženými do let 2020 až 2024. V kapitole 4. *Plán implementace strategie* jsou projekty rozpracovány do časové osy a podrobně rozebrány ve vazbě na strategické cíle a plánované hodnoty v jednotlivých letech.

Projekt		2021	2022	2023	2024
POR	Portál města Brna				
WT	Workflow technologie				
ESL	Elektronické služby				
eIDAS	eIDAS				
BST	Bezpečnostní standardy				
SOC	Městské dohledové provozní a bezpečnostní centrum				
MC	Městský cloud				
APPMC	Aplikace v cloudu				
ARCH	Architektonické řízení městské informatiky				
OD	Otevřená data				
INT	Integrační platforma				

Tab.2: Přehled strategických projektů

Aktualizace strategie

Stanovením strategických cílů je nastavena dlouhodobá prioritizace směrem ke chtěnému plánovanému stavu. Strategické řízení však nebude účinné, pokud nedojde k neustálému zlepšování strategie na základě vnějších a vnitřních podnětů. Aktualizace tohoto dokumentu by měla být prováděna v souladu s těmto zásadami:

Zaměření na	Přezkoumání s aktualizací	Výstup
Systém strategických cílů	1 x ročně Při změně nadřazené Vize a Strategie #brno 2050	Aktualizovaný dokument Informační strategie
Portfolio strategických projektů	1 x kvartálně Při vzniku výjimečné situace na některém ze strategických projektů	Hlášení o stavu portfolia strategických projektů

Tab.3: Principy aktualizace strategie

1. Základní identifikace a klíčové pojmy

Základní identifikace

Zpracovatelé:

Tým pro provedení aktualizace informační strategie byl složen z následujících dvou skupin:

1. Tým města Brna
Skupina zástupců vedení města stanovujících dlouhodobé směrování města v oblasti informatiky. Složení skupiny:

- Ondřej Kotas (zastupitel pro informatiku)
- Michal Jukl (ředitel ICT, TSB)
- Jiří Kučera (vedoucí Úseku 2. náměstka primátora)
- Vladimír Halm (vedoucí odd. správy inf. systému, Odbor městské informatiky)
- Dušan Hájek (vedoucí odd. systémové a tech. podpory, Odbor městské informatiky)
- David Menšík (vedoucí Odboru městské informatiky)
- Lukáš Boula (člen Komise informačních technologií)
- Robert Schindler (TSB, architekt kybernetické bezpečnosti)
- Jan Holeček (vedoucí odd. strategického plánování, Odbor strategického rozvoje a spolupráce)
- Rostislav Obrlík (vedoucí Úseku tajemníka).

2. Tým externí podpory
Skupina expertů na strategické řízení a informatiku doplňující zdroje města o expertní podporu danou vedením pracovních schůzek (workshopů) a zpracováním závěrů z workshopů do aktualizované informační strategie města aplikací metody Balanced Scorecard. Složení skupiny:

- Petr Hujňák (Per Partes Consulting, s.r.o.)
- Jaroslav Hujňák (Per Partes Consulting, s.r.o.)
- Milan Šebesta (MT Legal s.r.o.)
- Petr Pernica (MT Legal s.r.o.).

Předmět:

Předmětem informační strategie je informatika města Brna v letech 2020 až 2024.
Účelem projektu aktualizace informační strategie bylo stanovit základní strategické cíle rozvoje informatiky města Brna tak, aby informatika podporovala dosahování strategických záměrů vytyčených vedením města Brna zejména v oblasti:

- Strategická a Programová část strategie #brno2050
- Strategické cíle kybernetické bezpečnosti
- Otevřená data
- Smart city

se zohledněním existence:

- Enterprise architecture
- Městské infrastruktury SMB.

Cílem projektu bylo aktualizovat dokument Informační strategie města Brna na období 2020 - 2024. Původní dokument Informační

	strategie byl vydán dne 6.12.2011 a jeho první aktualizace proběhla dne 7.5.2015. Informační strategie z roku 2015 je dostupná na www.brno.cz/brno-aktualne/tiskovy-servis/tiskove-zpravy/a/informacni-strategie-mesta-brna/.
Provedené úkony:	V rámci aktualizace informační strategie byly provedeny následující workshopy strategického týmu: • Analýza současného stavu – SWOT analýzy • Analýza současného stavu – analýza kvadrantů SWOT • Návrh cílového stavu – strategické cíle k roku 2024 a s výhledem k roku 2030 • Návrh cílového stavu – strategická mapa a kauzální řetězce • Implementační plán přechodu – měřítka plnění cílů • Implementační plán přechodu – strategické projekty • Závěrečné přezkoumání strategie (dokument Informační strategie) - přezkoumání a prezentace celkového dokumentu.

Legislativní rámec ČR a EU

Legislativní rámec podává stručný přehled zákonů, nařízení vlády, vyhlášek a nařízení Evropského parlamentu (dále také jen „právní předpisy“) dopadajících na oblast informačních a komunikační technologií, jež mohou pro konkrétní případy stanovovat práva a povinnosti dotčených osob, která bude nutné při naplňování *Informační strategie města Brna* respektovat.

Níže uvedený přehled právních předpisů (řazeno chronologicky) s obecným popisem obsahu vybraných právních předpisů s důrazem na oblast informačních technologií slouží k základní orientaci při zvažování podmínek a způsobů naplňování *Informační strategie města Brna*.

Právní předpisy ČR:

- **Zákon č. 123/1998 Sb., o právu na informace o životním prostředí, ve znění pozdějších předpisů**

  Zákon **o právu na informace o životním prostředí**, kromě toho, že je právní normou upravující podmínky výkonu práva na včasné a úplné informace o životním prostředí, stanoví také pravidla pro zřízení infrastruktury pro prostorová data pro účely politik životního prostředí a politik nebo činností, které mohou mít vliv na životní prostředí a zpřístupňování prostorových dat prostřednictvím síťových služeb na Národním geoportálu INSPIRE (dále jen „geoportál“). Tento zákon je tak právním předpisem, jež upravuje, kromě jiného, zpřístupňování a předávání prostorových dat a metadat na geoportál z vlastního internetového rozhraní s využitím služeb založených na prostorových datech a technické požadavky na geoportál.

- **Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů**

  Zákon **o svobodném přístupu k informacím** je obecnou právní normou, která zajišťuje právo veřejnosti na informace, které mají k dispozici státní orgány, orgány územní samosprávy, jakož i další subjekty, které rozhodují na základě zákona o právech a povinnostech občanů a právnických osob. Tyto povinné subjekty jsou tímto zákonem zavázány především k tomu, aby zveřejňovaly základní a standardní informace o své činnosti automaticky tak, aby byly všeobecně přístupné. Ostatní informace, které mají k dispozici, jsou povinné subjekty povinny poskytnout na požádání žadatele, tj. každé fyzické nebo právnické osoby. Vyňaty jsou informace, jejichž poskytnutí zákon výslovně vylučuje nebo v nutné míře omezuje. Jde zejména o informace, které jsou na základě zákona prohlášeny za utajované, nebo informace, které by porušily ochranu osobnosti a soukromí osob. Zákon také stanovuje náležitosti žádosti o poskytnutí informace, postup při jejím podávání a vyřizování, zakotvuje možnost odvolání proti rozhodnutí o odmítnutí

žádosti, včetně přezkumu tohoto rozhodnutí správním soudem, a upravuje hrazení nákladů spojených s poskytnutím informace povinným subjektem.

- **Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů**

  Autorský zákon představuje komplexní úpravu práva autorského a práv souvisejících s právem autorským. Zákon, kromě jiného, upravuje vztahy mezi uživateli a tvůrci autorských děl, mezi které patří také počítačové programy (např. v podobě SW, webových stránek a aplikací), databáze nebo kartografická díla (např. v podobě digitálních map). Právní úprava zde obsažená reguluje osobnostní a majetková práva autorů autorských děl, tj. zejména právo autora osobovat si autorství, právo na nedotknutelnost díla, nebo právo na rozmnožování díla, právo na rozšiřování originálu nebo rozmnoženiny díla apod.
- Zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů
- Zákon č. 240/2000 Sb., o krizovém řízení, ve znění pozdějších předpisů
- **Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů**

  Zákon **o informačních systémech veřejné správy**[1] stanovuje práva a povinnosti osob, jež souvisejí s vytvářením, správou, provozem a rozvojem určitých informačních systémů veřejné správy (např. Portál veřejné správy), jakož i z toho vyplývajících informačních systémů (např. Czech POINT). Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností. Tato data jsou potřebná jednak pro jiné informační systémy, jednak pro zajištění správních činností příslušných orgánů. Z působnosti zákona jsou naopak vyňaty informační systémy veřejné správy spravované buďto pro potřeby nakládání s utajovanými informacemi, zpravodajskými službami, Národním bezpečnostním úřadem a Národním úřadem pro kybernetickou a informační bezpečnost.
- Zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů
- **Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů**

  Zákon **o některých službách informační společnosti**[2] je normou transponující příslušný předpis Evropské unie. Účelem právní úpravy zde obsažené tak je zapracovat do českého právního řádu některé instituty související s rozvojem informační společnosti (tj. společnosti, která se opírá o shromažďování, využívání a šíření informací) a elektronického obchodu, dále pak stanovit odpovědnost, práva a povinnosti poskytovatelů služeb informační společnosti (např. operátorů elektronických komunikací, poskytovatelů hostingových služeb či provozovatelů diskusních serverů), jakož i osob šířících obchodní sdělení[3] v jednom zákonném celku.
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů

---

1 **Informační systém veřejné správy** je funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy. Každý informační systém veřejné správy zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále nástroje umožňující výkon informačních činností.

2 **Služba informační společnosti** je jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu; služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat.

3 Za **obchodní sdělení** se považují všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb. nebo image určitého podniku.

- Zákon č. 500/2004 Sb., správní řád ve znění pozdějších předpisů, ve znění pozdějších předpisů
- **Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů**

  Zákon **o elektronických komunikacích**[4] upravuje na základě práva Evropské unie podmínky podnikání a výkon státní správy, včetně regulace trhu, v oblasti elektronických komunikací. Právní úprava zde obsažená reguluje především přenos informací prostřednictvím sítí elektronických komunikací a rozhlasového a televizního vysílání. Z věcné působnosti zákona je naopak vyňat obsah rozhlasového či televizního vysílání, jakož i obsah sdílený prostřednictvím internetu.
- **Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů**

  Zákon **o elektronických úkonech a autorizované konverzi dokumentů** obsahuje právní úpravu elektronických úkonů orgánů veřejné moci vůči fyzickým osobám a právnickým osobám, jakož i elektronických úkonů fyzických osob a právnických osob vůči orgánům veřejné moci a elektronických úkonů mezi orgány veřejné moci navzájem prostřednictvím datových schránek.[5] Účelem zavedení institutu datových schránek pro doručování je přiblížení orgánu veřejné moci občanovi prostřednictvím elektronických nástrojů, zefektivnění komunikace mezi občanem a orgánem veřejné moci a komunikace mezi orgány veřejné moci. K zajištění správného fungování datových schránek směřuje též zavedení a sjednocení systému jednoznačné identifikace fyzických osob (na základě osobního čísla, které je této osobě přiděleno), jakož i právnických osob a orgánů veřejné moci při elektronické komunikaci. V neposlední řadě zákon upravuje též autorizovanou konverzi dokumentů.[6]
- **Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů**

  Zákon **o základních registrech** je právním předpisem upravujícím, kromě jiného, obsah základních registrů[7], informačního systému základních registrů[8] a informačního systému územní identifikace a stanoví práva a povinnosti, které souvisejí s jejich vytvářením, užíváním a provozem. Smyslem a účelem právní úpravy je zakotvení základních registrů, jakožto unikátních zdrojů nejčastěji využívaných údajů při výkonu veřejné správy (referenční údaje) a zefektivnění jejich využití. Prostřednictvím informačního systému základních registrů má být zajištěno, mimo jiné, provedení identifikace a autentizace a následně i autorizace uživatelů. Informační systém základních registrů také uchovává záznamy o událostech spojených s poskytovanými službami a údaji ze základních registrů.
- Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
- **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů**

---

4 **Elektronickými komunikacemi** se rozumí technologie (satelitní sítě, mobilní sítě apod.) pro přepravu, přenos, nebo směrování signálů (obraz, data, telefonie) v elektronické podobě.

5 **Datovou schránkou** se v pojetí zákona rozumí elektronické úložiště určené k doručování elektronických dokumentů mezi orgány veřejné moci na straně jedné a fyzickými a právnickými osobami na straně druhé.

6 **Konverzí** se rozumí úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo datovém souboru způsobem zajišťujícím shodu obsahu těchto dokumentů a připojení doložky o provedení konverze, nebo úplné převedení dokumentu obsaženého v datové zprávě do dokumentu v listinné podobě způsobem zajišťujícím shodu obsahu těchto dokumentů a připojení doložky. Výstupnímu dokumentu se pak přiznávají stejné právní účinky jako ověřené kopii.

7 **Základním registrem** se rozumí informační systém veřejné správy, tj. registr obyvatel, registr osob registr územní identifikace registr práv a povinností.

8 **Informačním systémem základních registrů** se rozumí informační systém veřejné správy, jehož prostřednictvím je zajišťováno sdílení dat mezi jednotlivými základními registry navzájem, základními registry a agendovými informačními systémy a agendovými informačními systémy navzájem, správa oprávnění přístupu k datům a další činnosti.

Zákon **o kybernetické bezpečnosti** upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti, jakož i zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů, přičemž zapracovává příslušné předpisy Evropské unie. Účel zákona pak tkví v zajištění právní ochrany specifických informačních a komunikačních systémů před kybernetickými bezpečnostními incidenty, jež spočívají buďto v narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. Pro tyto účely zákon rozlišuje dvojí bezpečnostní opatření, a totiž opatření organizační, jež zahrnují povinnost pořizovat plány (jímž bude např. bezpečnostní politika) a aplikovat řídící, organizační a kontrolní postupy (zde pak např. kontrola a audit), a opatření technická, jež specifikují jednotlivé okruhy technických řešení týkajících se zabezpečení informačních a komunikačních systémů včetně detekce, vyhodnocování a řešení kybernetických bezpečnostních událostí a incidentů (dle zákona např. fyzická bezpečnost, nástroj pro detekci kybernetických bezpečnostních událostí, aplikační bezpečnost apod.).

- Zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů
- Zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů
- **Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů**
- Zákon **o službách vytvářejících důvěru pro elektronické transakce** v návaznosti na příslušný předpis Evropské unie[9] upravuje zejména požadavky na podepisování dokumentů v závislosti na podepisující osobě a osobě, vůči níž je právně jednáno. Zákon dále vymezuje též postupy kvalifikovaných poskytovatelů služeb vytvářejících důvěru, které vydávají certifikáty ověřující identitu podepisujících osob, a také vymezuje působnost Ministerstva vnitra v této oblasti, jakož i stanovuje sankce, které může tento orgán v rámci svého dohledu uložit. Ústředním pojmem, se kterým zákon pracuje, je pojem elektronického podpisu.[10] Právní úprava zde obsažená velkou měrou přispívá k rozšiřování elektronizace právního styku a tím i k jeho značnému usnadnění.
- **Zákon č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů**

  Zákon **o elektronické identifikaci**[11] představuje právní základ pro prokazování totožnosti s využitím elektronické identifikace, pakliže právní předpis, nebo výkon působnosti vyžaduje prokázání totožnosti. Zákonná úprava zavádí obecné principy institutu elektronické identifikace, čímž umožňuje fyzickým osobám při přístupu k příslušným on-line službám nebo jiným činnostem použití systémů elektronické identifikace zaručujících bezpečnou a důvěryhodnou elektronickou identifikaci fyzických osob. Zákon v návaznosti na přímo použitelný předpis Evropské unie upravuje kromě využití elektronické identifikace též působnost Ministerstva vnitra a Správy základních registrů na úseku elektronické identifikace. Zahrnuta byla též právní úprava přestupků na úseku elektronické identifikace.
- **Zákon č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů**

  Zákon **o zpracování osobních údajů** transponuje a v určitých směrech doplňuje nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.
- **Zákon č. 12/2020 Sb. o právu na digitální služby a o změně některých zákonů**

9 Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

10 **Elektronickým podpisem** se rozumí data v elektronické podobě, která podepisující osoba používá k podepsání.

11 **Elektronickou identifikací** se rozumí postup používání osobních identifikačních údajů v elektronické podobě, které jednoznačně identifikují určitou osobu, a to za pomocí číselného údaje.

Zákon **o právu na digitální služby**[12] **a o změně některých zákonů** je obecný právní předpis, který upravuje právo fyzických a právnických osob na poskytnutí digitálních služeb orgány veřejné moci a právo fyzických a právnických osob činit digitální úkony na straně jedné. Zákon dále stanovuje povinnost orgánů veřejné moci poskytovat digitální služby a přijímat digitální úkony a některá další práva a povinnosti související s poskytováním digitálních služeb na straně druhé. Cílem této právní úpravy tak je zásadním způsobem posílit práva fyzických a právnických osob v pozici uživatelů služeb, tj. *de facto „*klientů orgánů veřejné moci“, na poskytnutí služeb orgánů veřejné moci elektronicky, tj. právě formou digitální služby.

Související podzákonné právní předpisy ČR:

- Vyhláška č. 442/2006 Sb., kterou se stanoví struktura informací zveřejňovaných o povinném subjektu způsobem umožňujícím dálkový přístup, ve znění pozdějších předpisů
- Vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy), ve znění pozdějších předpisů
- Vyhláška č. 53/2007 Sb., o technických a funkčních náležitostech uskutečňování vazeb mezi informačními systémy veřejné správy prostřednictvím referenčního rozhraní (vyhláška o referenčním rozhraní), ve znění pozdějších předpisů
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů
- Vyhlášky 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů
- Nařízení vlády č. 425/2016 Sb. o seznamu informací zveřejňovaných jako otevřená data, ve znění pozdějších předpisů
- Vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, ve znění pozdějších předpisů
- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů

Právní předpisy EU:

- **Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES**

  Nařízení Evropského parlamentu a Rady (EU) **č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu** (zkráceně eIDAS) je právním aktem Evropské unie v oblasti služeb vytvářejících důvěru, přičemž jej doplňuje již platný zákon č. 297/2016 Sb. a doprovodný zákon č. 298/2016 Sb., jakož i zákon č. 250/2017 Sb. Nařízení stanovuje podmínky, za nichž členské státy uznávají prostředky pro elektronickou identifikaci fyzických a právnických osob,[13] které spadají do oznámeného systému elektronické identifikace[14] jiného členského státu. Dále stanovuje pravidla pro služby vytvářející důvěru[15], zejména u elektronických transakcí a právní rámec

12 **Digitální službou** se zde rozumí úkon vykonávaný orgánem veřejné moci vůči uživateli služby (např. konverze podkladů a dokumentů). Naproti tomu **digitálním úkonem** je úkon vykonávaný uživatelem služby vůči orgánu veřejné moci (např. elektronické podání).

13 Jako typický příklad zde lze uvést prostředky pro vytváření bezpečných elektronických podpisů.

14 Oznámení systému elektronické identifikace zahrnuje mj. jeho popis, včetně úrovní záruky a vydavatele či vydavatelů prostředků pro elektronickou identifikaci v rámci tohoto systému.

15 **Službou vytvářející důvěru** se rozumí elektronická služba, která je zpravidla poskytována za úplatu a spočívá ve

pro elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování a certifikační služby pro autentizaci internetových stránek. Tím vytváří právní prostředí pro veškeré důležité aspekty elektronických transakcí.

- **Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)**

  Právní úprava v **obecném nařízení o ochraně osobních údajů** stanovuje práva a povinnosti v oblasti zpracování osobních údajů[16] fyzických osob – subjektů údajů, a to bez ohledu na jejich státní příslušnost nebo bydliště. Tím má být zajištěna jednotná úroveň ochrany fyzických osob v celé Unii a zamezeno rozdílům bránícím volnému pohybu osobních údajů v rámci vnitřního trhu. Toto nařízení se naopak nevztahuje na zpracování osobních údajů právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a kontaktních údajů právnické osoby.

- Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“)

  Právní úprava **aktu o kybernetické bezpečnosti**, kromě jiného, upravuje rámec pro zavedení evropského systému certifikace kybernetické bezpečnosti[17], jehož účelem je zajistit odpovídající úroveň kybernetické bezpečnosti produktů, služeb a procesů informačních a komunikačních technologií v Unii a zabránit roztříštění vnitřního trhu, pokud jde o systémy certifikace.

- Nařízení Evropského parlamentu a Rady (EU) č. 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii
- Směrnice Evropského parlamentu a Rady 2007/2/ES ze dne 14. března 2007 o zřízení Infrastruktury pro prostorové informace v Evropském společenství (INSPIRE)
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii

Shora uvedené právní předpisy jsou platné a účinné ke dni vydání Informační strategie.

vytváření, ověřování shody a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami nebo ve vytváření, ověřování shody a ověřování platnosti certifikátů pro autentizaci internetových stránek nebo v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami. Jako příklad lze uvést LongTermDocs od Software 602.

16 **Osobním údajem** jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Za osobní údaj jsou též považovány síťové identifikátory (např. IP adresa).

17 Systém certifikace je ucelený soubor pravidel, technických požadavků, norem a procesů sjednaný na evropské úrovni, jímž se posuzují kyberneticko-bezpečnostní vlastnosti konkrétního produktu, služby či procesu.

Klíčové pojmy a zkratky

Agenda je regulací uložený ucelený souhrn vzájemně souvisejících procesů vykonávaných úřadem jako výkon státní správy nebo samosprávy v souvislosti s poskytováním veřejné služby. Jde o souhrn prací, především administrativních, souvisejících s vykonáváním úřadu nebo funkce (pozice).

Aplikace (Aplikační software, ASW) je programové vybavení (tj. software), které je určeno pro přímou interakci s uživatelem. Účelem aplikace je zpracování a řešení konkrétního problému uživatele při výkonu státní správy nebo samosprávy v rámci vykonávání procesů v agendě. Agenda může být podporována jednou či více aplikacemi, případně může jedna aplikace sloužit pro podporu více agend.

Balanced Scorecard (BSC) je metoda vytvořená Robert S. Kaplanem a David P. Nortonem, která je určena pro strategické plánování a řízení. BSC měří výkonnost organizace pomocí čtyř perspektiv:

- finanční,
- zákaznické,
- interních podnikových procesů,
- učení se a růstu.

Pro měření výkonnosti informatiky byly perspektivy upraveny na:

- ICT přínosy,
- ICT zákazníci,
- procesy,
- ICT potenciál a zdroje.

Základní myšlenkou je soustředit organizaci na ty cíle a měřítka, která hrají důležitou roli při naplňování strategie a dosahování strategických cílů.

Business Process Management (BPM) jsou metodiky a postupy pro procesní řízení v organizacích.

eGovernment cloud (eGC) zahrnuje tři hlavní kategorie cloudových služeb poskytovaných Ministersvem vnitra České republiky v rámci cloud computingu: IaaS (Infrastructure as a Service - služby na úrovni datových center, sítí a HW), PaaS (Platform as a Service - služby na úrovni standardních SW platforem, jako jsou databáze, webové servery) a SaaS (Software as a Service - kompletní funkcionalita standardních nebo standardizovatelných aplikací poskytovaná jako služba, např. e-mail, ekonomický systém, spisová služba apod.).

Electronic Identification, Authentication and Trust Services (eIDAS), služby vytvářející důvěru a elektronická identifikace podle nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu.

Enterprise Architecture (podniková architektura, architektura organizace) obsahuje popis cílů organizace, způsobů, jak jsou tyto cíle dosahovány pomocí procesů a způsobů, jak mohou tyto procesy být podpořeny technologiemi. Zahrnuje tedy všechny zásadní aspekty organizace – business (strategie, procesy), informace (metadata, datové modely), software (aplikační software, rozhraní, jejich propojení) i technologie (hardware, aplikační a databázové servery, sítě).

Gestor je pracovník úřadu vykonávající pro určitou agendu metodickou činnost, tj. konkretizuje a optimalizuje postupy procesů (činností) vykonávaných v rámci agendy úřadem. Z pohledu informatiky je gestor představitelem klíčových uživatelů aplikace podporující danou agendu. Z pohledu organizační struktury je gestorem liniový vedoucí skupiny klíčových uživatelů, zpravidla jde o vedoucího oddělení nebo odboru.

IT as a service (ITaaS) je model poskytování informačních technologií formou řízených služeb s definovaným katalogem poskytovaných IT služeb. V tomto modelu je klíčové rozpoznávání potřeb příjemců služeb a agilní přizpůsobování IT služeb těmto potřebám. Příjemcem IT služeb

mohou být občané, podnikatelé či návštěvníci města. IT služby jsou poskytovány stejnou formou i dovnitř města a pro městské subjekty.
Model ITaaS vyžaduje standardizaci a zjednodušení produktů dodávaných IT, zvýšenou finanční transparentnost a přímější přidružení cen k položkám katalogu služeb a spotřebě služeb včetně zvýšené provozní efektivnosti IT.

ICT je obecně zaužívaná zkratka pro informační a komunikační technologie.

ICT infrastruktura zahrnuje zejména servery, disková pole a fibre channel switche. Obecně ji lze definovat jako souhrn hardwarových a softwarových komponent a služeb, které slouží k zajištění bezproblémového fungování IT.

Integrační datová platforma (middleware, IDP) je nástroj pro centrální správu komunikace a kooperace mezi programy. Vytváří jednotné a centrálně spravované prostředí pro propojení původně nezávislých dílčích řešení či aplikací do provázaného systému.

Internet věcí (Internet of Things, IoT) je označení pro síť fyzických zařízení, která jsou vybavena elektronikou, softwarem, senzory, pohyblivými částmi a síťovou konektivitou umožňující těmto zařízením se propojit a vyměňovat si data.

Klíčový uživatel je pracovník úřadu se znalostí agendy nebo její části. Jedná se o vlastníka jednoho či více procesů (činností) podporovaných aplikací.

Kybernetická bezpečnost (KB) je souhrn právních, organizačních, technických a vzdělávacích prostředků k zajištění ochrany kybernetického prostoru.

Managed security service provider (MSSP) je poskytovatel spravovaných bezpečnostních služeb monitorování a správy bezpečnostních zařízení a systémů, jako je spravovaný firewall, detekce narušení, virtuální privátní síť, skenování zranitelností a antivirové služby.

Perspektiva je v metodě Balanced Scorecard specifická oblast, ve které se určují strategické cíle. K jednotlivým strategickým cílům jsou přiřazeny klíčové ukazatele výkonnosti.

Portál národního bodu pro identifikaci a autentizaci (NIA) je nástroj, který slouží pro bezpečné a zaručené ověření totožnosti uživatele on-line služeb poskytovaných zejména veřejnou správou.

Schéma Balanced Scorecard (strategická mapa) je grafické znázornění strategických cílů ve čtyřech perspektivách s vyznačením jejich provázanosti. Strategická mapa je tedy vizualizací strategických (kauzálních) řetězců příčin a následků v rámci perspektiv metody Balanced Scorecard.

Security Operation Center (SOC), též dohledové provozní a bezpečnostní operační centrum, je centrum, které zajišťuje komplexní centralizaci řízení bezpečnostních událostí a incidentů v jednom bodě s cílem minimalizovat reakční doby na incident a škody z něj plynoucí.

Systém pro řízení privilegovaných účtů (PIM/PAM) je bezpečnostní technologie sloužící pro zvýšení zabezpečení technických aktiv při všech aktivitách administrátorů, infrastrukturních aplikačních správců, uživatelů nebo externích dodavatelů a smluvních partnerů, kteří využívají privilegovaných účtů. PIM (Privileged Identity Management) je systém pro monitorování a ochranu účtů superuživatelů v IT prostředí organizace. PAM (Privileged Access Management) je řešení, které slouží k zabezpečení, řízení, správě a monitorování privilegovaných přístupů k citlivým aktivům – servery, databáze, aplikace, bezpečnostní nástroje, síťové prvky apod.

Systém řízení bezpečnosti informací (SŘBI) vymezuje programové a technické prostředky zahrnuté do kybernetického prostoru ve správě SMB. Dokument SŘBI obsahuje seznam do SŘBI začleněných informačních a komunikačních systémů.

Strategický řetězec tvoří spojení cílů napříč perspektivami Balanced Scorecard a to na základě vztahu příčin a následků. V BSC se vždy vyskytuje několik základních strategických řetězců, které se vyznačují ve strategické mapě (schématu Balanced Scorecard).

Strategický tým je složen je složen z týmu města Brna stanovujícího dlouhodobé směrování města v oblasti informatiky a z týmu externí podpory, který doplňuje zdroje města o expertní podporu.

SWOT analýza (SWOT) je metoda, jejíž pomocí je možno identifikovat silné (Strengths) a slabé (Weaknesses) stránky, příležitosti (Opportunities) a hrozby (Threats), spojené s určitými oblastmi zájmu, jako např. organizací informatiky, procesy, architekturou informačního systému, dosahování očekávaných přínosů nebo spokojeností zákazníků / uživatelů. Základ metody spočívá v klasifikaci a ohodnocení jednotlivých faktorů, které jsou rozděleny do 4 výše uvedených základních skupin. Vzájemnou interakcí faktorů silných a slabých stránek na jedné straně vůči příležitostem a hrozbám na straně druhé lze získat nové kvalitativní informace, které charakterizují a hodnotí úroveň jejich vzájemného střetu.

TOGAF je mezinárodně uznávaný rámec pro řízení tvorby Enterprise Architecture ve společnostech využívajících prostředků informačních a komunikačních technologií.

2. Analýza současného stavu

Analýza současného stavu informatiky byla provedena pomocí SWOT analýz pro oblasti:

- Organizace informatiky a informatické procesy;
- Podniková architektura (Enterprise Architecture);
- Přínosy informatiky;
- Spokojenost uživatelů.

V každé z uvedených oblastí byly zjištěny její:

- Vnitřní silné stránky (**S**trengths);
- Vnitřní slabé stránky (**W**eaknesses);
- Vnější příležitosti (**O**pportunities);
- Vnější hrozby (**T**hreats).

Výroky ve SWOT analýzách byly ohodnoceny strategickým týmem (bez týmu externí podpory) z hlediska jejich významnosti (síly výroku) a seřazeny do výsledné sumarizační SWOT tabulky. Následně byly rozebrány variantní zaměření strategie na základě analýzy kvadrantů sumarizační SWOT podle variantních možností vycházejících ze současně dosaženého stavu a potenciálu rozvoje.

Strategie	Opportunities (příležitosti)	Threats (hrozby)
Strengths (silné stránky)	Strategie S-O „VYUŽITÍ“ *Využití vnitřních silných stránek a vnějších příležitostí*	Strategie S-T „KONFRONTACE“ *Využití vnitřní síly k zamezení vnějších hrozeb*
Weaknesses (slabé stránky)	Strategie W-O „HLEDÁNÍ“ *Překonání vnitřních slabostí k využití vnějších příležitostí*	Strategie W-T „VYHÝBÁNÍ“ *Preventivní obrana proti skloubení vnitřních slabostí s vnějšími hrozbami*

Tab.4: Variantní zaměření strategie na základě analýzy kvadrantů SWOT

2.1. Výchozí stav

Kapitola obsahuje shrnutí dosaženého stavu informatiky města, který vstupuje jako východisko do přípravy této informační strategie.

2.1.1. Splnění strategických cílů z předchozí strategie

V této podkapitole je shrnut stav splnění strategických cílů stanovených v Informační strategii města Brna z roku 2015. Informační strategie z roku 2015 je dostupná na: www.brno.cz/brno-aktualne/tiskovy-servis/tiskove-zpravy/a/informacni-strategie-mesta-brna/.

1. Vytvořit moderní portál města

Předmětem aktuálně vypsané Veřejné zakázky je vytvoření a rozvoj Platformy pro weby města Brna, na které bude možné dále stavět nové webové projekty dle aktuální potřeby. Na Platformě bude v rámci předmětu Veřejné zakázky jako první projekt spuštěn a provozován nový web www.brno.cz. Součástí předmětu Veřejné zakázky je Podpora a Údržba, jakož i Customizace Platformy.

2. Vybudovat úložiště dat (DWH - datový sklad, UNED - úložiště nestrukturovaných dat, DES - digitální spisovna)

DWH – projekt datového skladu je od r. 2015 realizován jako jeden z modulů AIS GINIS. Slouží jako zdroj informací pro subprojekty „ROZKLIKÁVACÍ ROZPOČET“ „EPM“ a další, dále je též k dispozici pro otevřená data

UNED – v závěru roku 2015 a počátkem roku 2016 byla zpracována analýza jako podklad pro pokračování realizace formou VZ. Studie identifikuje v té době známé zdroje dat, které tvoří „digitální stopu“ činnosti úřadu a momentálně existují v různých typech dat. Zabývá se i možnými návrhy využití – z pohledu sledování trendů je například velmi zajímavý vývoj v čase, patrný z dostupných dat. Projekt zatím nepokročil pro nenaplánování financí.

DESA – projekt na Důvěryhodnou Elektronickou Spisovnu vychází z požadavků legislativy na řízení životního cyklu dokumentů produkovaných především spisovou službou, ale i jinými AIS. Je to specifický typ úložiště, který musí být napojen na ESS, a zároveň musí mít implementovány procesy pro udržení důvěryhodnosti dokumentů a souborů (obnova časových značek, certifikátů atd.).

3. Obnovit ICT infrastrukturu a odstranit kritická místa infrastruktury

Podkladem pro návrhy obnovy infrastruktury byla částečně zpracovaná Enterprise Architektura ICT SMB (koresponduje s cílem IS č. 6) a dalším podkladem byly dílčí analýzy stavu a predikce dalšího rozvoje ICT města.

Výsledkem byla podklady a posléze realizace VZ na vytvoření záložního DC a obnovu datového úložiště. Zprovozněno záložní centrum, migrace do nového datového úložiště se rozbíhá v rámci komplexního projektu.

Bylo realizováno redundantní internetové připojení v roce 2017 včetně změny providera a byla provedena obnova aktivních prvku metropolitní sítě.

4. Trvale zvyšovat úroveň kvalifikace a znalostí pracovníků informatiky SMB

V roce 2017 byl nastartován projekt s názvem „Zvýšení odborných znalostí zaměstnanců MMB", registrační číslo CZ.03.4.74/0.0/0.0/]6_033/0002908, který byl spolufinancován Evropskou unií prostřednictvím Operačního programu Zaměstnanost.

V roce 2018 proběhla v rámci výše uvedeného projektu školení zaměstnanců Odboru městské informatiky v následujících kurzech:

- TOGAF® 9.1 L1 Foundation (CZ),
- Enterprise architektura,
- Řízení požadavků a změn,
- Základní školení principů servisu a zabezpečení ICT dle ISO 20000 a zásady bezpečnosti ICT dle požadavků ISO 27000,
- Řízení kvality při správě ICT,
- ITIL® Foundation.

5. Vybudovat metodické a znalostní centrum informatiky SMB

Jsou vybudovány neformální kontakty na klíčové instituce v oblasti ICT – FI Masarykovy university, FIT VUT Brno, NSMC, NUKIB, NBU, MV ČR OHA, ISZR, Microsoft ČR. Při hledání možných řešení se snažíme v rámci těchto kontaktů nalézat možné varianty a také je oponovat s cílem najít optimální variantu. SMB má zástupce v KISMO a účastní se aktivně práce komise na různých dílčích projektech v oblasti rozvoje e-governmentu. Dále spolupracujeme RVIS a s pracovními skupinami, které ustavil digitální zmocněnec úřadu vlády ČR.

6. Zavést architektonické řízení a pravidla pro poskytování dat

V rámci přípravy informační strategie v roce 2015 došla pracovní skupina k poznání, že městské ICT je rozsáhlý a komplexní systém a nelze jej spravovat a rozvíjet jen formou ad-hoc požadavků. Proto byl stanoven tento strategický okruh, jehož cílem bylo popsat stav, a navrhnout postup pro realizaci rozvojových projektů se zahrnutím vazeb na celé ICT prostředí a s optimálním využitím komponent a návrhem řešení, které splní požadavky na otevřenost ve smyslu komunikace s jinými ICT prvky a bude integrováno s již existujícími komponentami.

Byla zpracována Enterprise Architektura ICT SMB v základní úrovni dekompozice podle metodiky TOGAFF – v souladu s požadavky a doporučeními metodiky MV ČR, útvaru OHA, který vyžaduje popisy ve formě EA pro schvalování ISMS. Architektura je zatím jen v základní úrovni dekompozice a identifikace procesů zejména v prvé, business úrovni, do většího detailu až na úroveň popis nejnižší technologické vrstvy a provázání přes bezpečnostní aspekty celé ICT města se vzhledem k pozastavení projektu nepokračovalo. Součástí projektu je tedy zatím popis As-Is stavu a základní návrhy parentů pro některá uvažovaná budoucí řešení pro To-Be stav.

Pokud by se pokračovalo do detailní úrovně, byly by k dispozici jednak podklady pro efektivní řízení a rozvoj celého městského ICT, a navíc by byla k dispozici velmi podrobná mapa procesů a zdroj informací také pro plnění požadavků, které vyplývají z GDPR a ZoKB.

Nezbytnou je také spolupráce enterprise architekta se security architektem – nové komponenty by měly kromě jiného splnit požadavky na otevřenost rozhraní včetně designu dle zásad „security by default“ atd.

7. Poskytovat ICT infrastrukturu jako cloudovou službu (PaaS) v modelu kapacity na vyžádání (UC)

Podkladem pro tento strategický okruh byly návrhy členů pracovní skupiny, kde byla identifikována potřeba dynamického zpřístupnění městského ICT podle požadavků městských organizací. Koresponduje se strategickým cílem obnovy infrastruktury. Smyslem bylo vytvoření privátního cloudu, který by umožnil škálování výkonu a prostoru pro realizaci procesů podle požadavků města a jeho organizací. Částečně je zahrnuto do projektu obnovy datového centra a migrace do nového datového úložiště.

8. Zavést proces motivace pracovníků informatiky

Odbor městské informatiky se při odměňování pracovníků musí řídit platnými a zavedenými postupy. Možnosti motivace finančními prostředky jsou proto v podmínkách úřadu značně omezeny. Také z tohoto důvodu se začíná objevovat problém, kdy zájem o uvolněné pracovní pozice je téměř nulový. Proces motivace pracovníků se soustředí tedy spíše na metody nehmotné povahy. Zejména dobré pracovní podmínky, dobré pracovní vztahy, preference vlastních zaměstnanců při postupech, kompletní delegování úkolů, pravomoci a odpovědnosti apod.

9. Zavést řízení projektového portfolia s autorizací projektů a roadmapu portfolia

V roce 2010 v rámci projektu „Optimalizace řízení informatiky MMB, CZ.1.04/4.1.01/53.00085“, který byl spolufinancován z operačního programu Lidské zdroje a zaměstnanost realizováno školení zaměstnanců OMI „Principy a postupy projektového řízení“. Současně byla vypracována metodika „Řízení a koordinace projektů informatiky“ včetně portfolia vzorů dokumentů, materiál je aktuálně používán. V současné době bude zahájeno zpracování nové projektové metodiky Odboru městské informatiky.

10. Prosadit městské standardy

Prosazování standardů je podpořeno přijetím Bezpečnostní politiky informací a zavedením Systém řízení informační bezpečnosti ve shodě s normou ČSN ISO 27001 spolu se Systémem řízení kvality dle normy ČSN ISO 9001. Standardy prozatím nejsou stanoveny, předpokládá se jejich

definice v souvislosti se zaváděním Systému řízení bezpečnosti informací pro prvek kritické informační infrastruktury Statutárního města Brna.

11. Poskytovat otevřená data (Open Data)

Tento cíl je provázán se vznikem zdrojů dat, zejména UNED. První část byla naplněna projektem „rozklikávací rozpočet“, proběhl pilotní projekt pro poskytování dat z městských IS nad daty GIS MB.

Pro další rozvoj poskytování dat z různých systémů je k dispozici výkonná integrační platforma na bázi produktu Clover ETL, která může kromě jiného zprostředkovat data i ve formě vystavených služeb na servis-bus (obdoba eGSB v centrálních AIS) a tím zjednodušit možné využití dat i s případnými funkcionalitami kontroly kvality dat, řízením přístupů a auditními službami.

12. Poskytovat služby přes portál úředníka a občana

Současný vývoj této oblasti se soustředí na využití nově spuštěného Portálu občana spravovaného resortem ministerstva vnitra, který byl spuštěn 8. července tohoto roku. Myšlenkou portálu veřejné správy je obdobně jako v jiných státech EU nad digitálními službami státu postavit jednu zastřešující službu, přes kterou by se mohli přihlašovat občané a řešit různé životní situace. Výhodou je zejména přístup s jedněmi přihlašovacími údaji a nové možnosti elektronické identifikace (hlavně díky novým eOP a novému NIA portálu).

13. Dosáhnout vzájemně prospěšných dlouhodobých vztahů s kvalifikovanými dodavateli

Hodnocení dodavatelů bylo zavedeno periodicky od roku 2017 jako součást Systému řízení informační bezpečnosti (ISMS) na Odboru městské informatiky. U všech servisních smluv jsou definovány požadavky na úroveň poskytované služby formou SLA parametrů.

14. Plánovat dlouhodobý transparentní rozvoj informatiky města

Koresponduje se strategickým cílem 6. a je v korelaci se všemi rozvojovými projekty. Nové ICT prvky by měly vždy projít posouzení z pohledu dopadů do celkové architektury ICT, v maximální míře využívat možných synergií s již implementovanými nebo plánovanými prvky a mít definovaný business case a též posouzení nákladů dle TCO.

15. Společně sdílet centrálně instalované aplikace (MMB, MČ)

Cíl je naplňován postupným rozvojem základních AISů města a zpřístupňováním dalším služeb centrálně provozovaných AIS a zprostředkováním dat z různých zdrojů.

Zatím není rozpracována myšlenka vytvoření frameworku pro miniaplikace, které by mohly využívat nebo případně samy vytvářet městské části podle jednotných standardů. Též zatím není využito uvažované možnosti třeba ve spolupráci s vysokými školami vytvořit platformu s definovanými standarty pro mobilní aplikace (obdoba prostředí GOOGLE Play nebo APPSTORE)

16. Zvýšit transparentnost a otevřenost radnice

Spolupráce na některých projektech se spolkem Otevřená města. Jedná se o spolek měst, která prosazují otevřené fungování místní samosprávy, zejména: zveřejňování informací a Open Data, otevřené zadávání veřejných zakázek, zapojování veřejnosti do rozhodování, open source a otevřené technologie.

Koresponduje s výše uvedenými strategickými cíli 11. a 12.

17. Zvýšit elektronizaci služeb veřejné správy

Tento cíl koresponduje se strategickým cílem 1. a je podmíněn v oblasti přenesené působnosti

legislativními možnostmi. V oblasti samosprávy jsou již k dispozici některé služby na portále ESHOP DPMB. Další vývoj elektronizace některých procesů probíhá u přípravy a oběhu dokumentů pro jednání RMB.

18. Disponovat vhodně dimenzovanou, provozně hospodárnou a bezpečnou infrastrukturou

Koresponduje se strategickými cíli 3. a 6. Obnova infrastruktury by měla vycházet z posouzení Enterprise architektem jak z pohledu plnění požadavků business vrstvy, tak provázání se stávajícími komponentami městského ICT, tak i z pohledu security architekta. Nezbytným je zahrnutí požadavků řešení podle principů nejen technických ale i ze ZoKB a GDPR (security by default, otevřená rozhraní, PAAS, SOA, využití služeb přes service-bus atd.). Cílem musí být také sjednocení infrastruktury v optimální podobě pro udržení přiměřených nákladů na správu technologií – opět nutno posuzovat minimálně dle metodiky TCO. Využití cloudových služeb realizováno pro vhodné aplikace (AZURE – eDeska). Zakomponováno využití dalších modulů v IDM pro prostředí emailů (účty LDAP). Realizováno otestování infrastruktury pomocí penetračních testů.

19. Dosahovat vysoké efektivnosti informatiky města

Koresponduje s celou Informační strategií města Brna z roku 2015 – je to zastřešující cíl.

2.1.2. Současný stav ICT města

ICT Statutárního města Brna je tvořeno komplexem HW, SW a komunikačních komponent.

Ve stručném výčtu jde o:

1. Metropolitní síť na optické bázi, včetně aktivních prvků – zajištění propojení a komunikace mezi objekty MMB, všech 29 úřadů městských částí a městské policie.
2. HW prvky – servery a aktivní komponenty ICT infrastruktury (např. firewally a další prvky). Jde řádově o několik desítek fyzických HW komponent, zejména serverů a řádově několik stovek virtuálních strojů se specializovanými funkcemi.
3. SW prvky – zde se jedná o IS, kterými jsou podporován aktivity úřadu jak v oblasti procesů přenesené působnosti (výkon státní správy), tak ve výkonu samostatné působnosti (samospráva). Součástí jsou hlavní AISy, které jsou provozovány a spravovány centrálně OMI MMB pro městské organizace a to:
    - e-spis a e-spis Lite – elektronická spisová služba, centrálně provozováno pro MMB, ÚMČ, MPB a příspěvkové organizace
    - GINIS – ekonomické, rozpočtové, majetkové, přestupkové a další agendy, centrálně provozováno pro MMB, ÚMČ a MPB
    - MATRIKA – centrálně provozováno pro 9 ÚMČ
    - VITA Stavební úřad – centrálně provozováno pro ÚMČ se stavebním úřadem a pro MMB (odbor OÚSŘ)
    - GISMB – geografický informační systém, centrálně provozováno pro MMB, ÚMČ, MPB a příspěvkové organizace.

V oblasti aplikací je dohromady okolo 400 aplikací, které jsou většinou vzájemně provázány a využívají datové zdroje jak interní, tak externí.

Klíčovými externími zdroji jsou centrální registry, které jsou využívány v rozsahu, definovaném legislativními požadavky k získávání referenčních údajů (ISZR) i dalších údajů pro výkon činností úřadu (registry řidičů, RSV – registr silničních vozidel …).

Všechny výše skupiny hlavních komponent městského ICT tvoří vzájemně provázaný, komplexní

systém, pro jeho rozvoj je nutné stanovení strategických cílů pro další rozvoj i správu. Strategie musí vzhledem ke komplexitě tohoto ICT prostředí respektovat pravidla pro otevřená řešení a spolupráci mezi jednotlivými komponentami jak interními, tak externími. Dalším požadavkem je nutnost akceptace jen takových řešení, které zapadají do konceptu „security by default“.

To vše musí nejen respektovat požadavky platné legislativy, ale korespondovat i s celkovou strategií města i celostátní strategií „Digitální Česko“. Samozřejmostí musí být i prostor pro reagování na aktuální i budoucí technologické trendy.

2.2. SWOT analýzy

Současná praxe řízení rozvoje informatiky je postavena kolem liniové odpovědnosti a pravomoci. Odbor městské informatiky je začleněn do Úseku 2. náměstka primátorky. V souladu s požadavky projektového řízení jsou všechny strategické rozvojové projekty schvalovány Radou města Brna po jejich předchozím schválení v Komisi informatiky.

SWOT analýzy byly provedeny strategickým týmem bez týmu externí podpory (viz kapitola 1. *Základní identifikace a klíčové pojmy*) v následujících oblastech:

- Organizace informatiky a informatické procesy (ICT procesy, lidé, finance);
- Podnikové architektury (business procesy, informační toky, aplikace, infrastruktura);
- Vedení města (přínosy pro umožnění lepšího a efektivnějšího fungování města);
- Uživatele (podpora koncového uživatele, řešení rozvojových požadavků, dodávka aplikačních služeb, uživatelská přívětivost).

Jednotlivé výroky ve SWOT byly ohodnoceny v pětibodové stupnici, kde 5 značí mimořádně silný prvek a 1 slabý prvek. Hodnota uvedená u výroku je dána jako průměr hodnocení všech členů strategického týmu (bez týmu externí podpory).

2.2.1. SWOT Organizace informatiky a informatické procesy

Výroky uvedené ve SWOT tabulce vychází z úhlu pohledu strategického týmu na organizaci a řízení informatiky.

	Strengths (vnitřní silné stránky)
4,6	Kvalifikovaní správci aplikací a ICT infrastruktury v oblasti, kterou mají ve své pracovní náplni.
4,3	Jistota prostředků na kalendářní rok v rámci schváleného rozpočtu.
4,0	Dosažené zkušenosti s implementací informačních systémů.
4,0	Vysoká znalost technologických trendů a jejich zavádění.
3,9	Průběžně aktualizovaný a doplňovaný popis procesů MMB.
3,8	Zvyšující se bezpečnostní povědomí mezi pracovníky OMI a rovněž pracovníky MMB.
3,6	Certifikace OMI na informační bezpečnost (procesy řízení a realizace projektů v oblasti ICT, poskytování služeb uživatelům ICT) podle ISO 27001.
3,4	Systém povinného vzdělávání úředníků.

	Opportunities (vnější příležitosti)
4,1	Disponibilní vzdělaní a kompetentní pracovníci v ICT v Brně.
3,9	Zapojení vysokých škol do rozvoje informatiky města Brna včetně aktivní spolupráce města při výuce studentů.
3,4	Maximální možné čerpání prostředků z fondů EU.
3,4	Využití potenciálu odborníků v rámci města ve formě poradenského orgánu.
3,1	Transformace služeb informatiky do samostatného ekonomického subjektu ovládaného městem Brnem.

	Weaknesses (vnitřní slabé stránky)
4,5	Motivační systém neumožňuje získávat nové a udržet stávající pracovníky IT.
3,8	Samostatný vzájemně málo koordinovaný postup MČ při rozvoji IS.
3,8	Ne všichni klíčoví uživatelé (garanti) mají dostatečné znalosti, aby definovali požadavky na informatiku (formulace toho, co chtějí). OMI nemůže suplovat metodické role uživatelů.
3,8	Nedostatek vnitřních odborných kapacit vzhledem k rostoucímu významu informatiky vede ke zvýšenému nákupu externích služeb.
3,3	Nedostatečné povědomí klíčových uživatelů o plánovaní kapacit zdrojů OMI na pokrytí požadavků.
3,1	Klíčové uživatele je obtížné motivovat pro práci týkající se informatiky z důvodu střetu liniových a projektových struktur.

	Threats (vnější hrozby)
5,0	Masivní vývoj kybernetických útoků a jejich forem.
4,0	Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT.
3,9	Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.
3,6	Z výběrových řízení podle ZVZ mohou vzejít neadekvátní dodavatelé nebo mohou výběrová řízení trvat nepredikovatelnou dobu.
3,3	Dlouhá doba od vytvoření záměru do jeho realizace způsobená interními předpisy nebo platnou legislativou.
2,8	Přidělení finančních prostředků z rozpočtu je vždy jen na rok (rozpočtování je jen roční), v IT není zavedeno víceleté financování.

2.2.2. SWOT Podniková architektura

Výroky uvedené ve SWOT tabulce vychází z úhlu pohledu strategického týmu na informatiku města.

	Strengths (vnitřní silné stránky)
4,9	Validní informace o EA jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.
4,7	V rámci TSB je prováděno technologicky moderní ukládání dat se zajištěnou ochranou proti jejich ztrátě.
4,7	Kvalitní prostory a technologické zázemí pro umístění uzlových ICT prvků (datové centrum).
4,4	Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ).
4,4	Kvalitní komunikační infrastruktura připojení ÚMČ.
4,3	Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy.
4,2	Efektivní licencování pro základní části městského AIS a office SW.
4,0	Architektura pro integrace aplikací – integrační platforma (s využitím principů ESB a ETL).
3,7	Je k dispozici prostředí (framework) pro tvorbu jednoduché podpory procesů a workflow v nich (MOSS – MS Office SharePoint Services) s komunitou uživatelů.

	Opportunities (vnější příležitosti)
4,7	Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.
4,6	Vytvoření a správa katalogu služeb ICT.
4,4	Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy).
4,4	Propojení GPC konfiguračních databází udržovaných MMB a samostatně dodavateli/správci částí infrastruktury.
4,4	Řízení optimalizace licencí ve vazbě na skutečnou potřebu.

	Opportunities (vnější příležitosti)
4,3	Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu.
4,3	Vytvoření centrálního přístupového bodu pro řízený přístup uživatelů do IS města a k aplikacím z různých platforem.
4,2	Větší využití ETL Clover pro datovou integraci systémů.
4,1	Vytvoření samostatného útvaru řešícího informatiku SMB.
4,0	Vydání IT směrnic závazných pro SMB.
4,0	Vytvořit prostředí pro drobné aplikace odborných útvarů SMB.
4,0	Vytvoření prioritizace cca 350 aplikací a odstupňovaný přístup k nim podle jejich priorit.
4,0	Využití Národního architektonického plánu s návrhovými vzory vybraných oblastí.
3,9	Využití externích kapacit výzkumu a vývoje pro oponenturu rozvojových koncepčních plánu a projektů (CERIT, NUKIB, Útvar hlavního architekta eGov…).
3,9	Metodická pomoc kompetenčního centra uživatelům z ÚMČ a organizací města.
3,9	Popsání definice vazeb mezi projekty a sesouladění postupů – road-mapa na období několika let s pravidelnou aktualizací.
3,1	Zvyšující se zájem stakeholderů o přístup k informacím z EA modelu.

	Weaknesses (vnitřní slabé stránky)
4,3	Neexistuje provozní aplikační a datový monitoring a konfigurační management na aplikační vrstvě.
4,3	Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).
4,1	Chybí vazba na business vrstvu zpracovávanou ORGO v BPMN diagramech.
4,0	Chybí standardizovaný Business CASE propojený na EA.
4,0	Data nejsou ukládána do datových úložišť ve strukturované podobě, která umožní řízení přístupu dle oprávnění.
4,0	Neexistence geograficky oddělené záložní infrastruktury.
3,9	Model EA zahrnuje jen MMB a absentují organizace SMB.
3,9	Nevytvořený katalog datových prvků a inventarizace dat jak z provozních IS, tak s využitím plánovaného budování úložišť dat (DWH – datový sklad, UNED – úložiště nestrukturovaných dat, DES - digitální spisovna).
3,9	Zastaralá HW infrastruktura.
3,7	Městské firmy si spravují vlastní podružná menší datová centra i aplikace bez vazby na EA.
3,7	Nedostatečná aplikace principů procesního řízení.
3,6	Neexistence záložních tras propojení uzlových bodů metropolitní sítě.
3,4	Nedostatečně rozvinutá integrační platforma (middleware).
3,3	IDM nemá zadefinované role z business vrstvy (není propojení EA až do procesní business vrstvy a její rozpracování na role).
3,3	Závislost rozvoje architektury na přidělených prostředcích (rozpočtu).
3,2	Není záloha Internetového připojení – při výpadku dojde k ohrožení činností úřadu. Neexistence paralelního (náhradního) internetového připojení.
3,1	Omezený a složitý přístup k aplikacím z vnějšího prostředí – restriktivní řešení bezpečnostních rizik.
3,0	Řada aplikací nemá dokumentaci.
2,9	Platformová technologická roztříštěnost (např. různé db stroje).
2,6	Plánování a využití kapacit všech zdrojů v souladu s požadavky vykonávaných procesů.

	Threats (vnější hrozby)
4,6	Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.
4,0	EA model obsahuje koncentrované informace a při neoprávněném přístupu k nim jde bezpečnostní riziko.

	Threats (vnější hrozby)
3,8	Neexistence plánu a pevných milníků pro nasazení nových centrálních IS s dopadem na činnosti OVM (orgán veřejné moci), což znamená negativní dopady na plánování zdrojů OVM, zejména při našem rozsahu správního obvodu (např. aplikace CRR, CRV, digitalizace dokumentů pro centrální agendy, rušení místní příslušnosti …).
3,6	Konfliktní požadavky změn legislativy s dopadem do informačních systémů.
3,6	Nedostatečná pozornost ze strany tvůrců prvků celostátního eGovernment, věnovaná specifickým potřebám statutárních měst.
3,4	Hrozba výpadku veřejného internetového připojení u MMB.

2.2.3. SWOT Přínosy informatiky pro SMB

Výroky uvedené ve SWOT tabulce vychází z úhlu pohledu strategického týmu na přínosy informatiky pro SMB.

	Strengths (vnitřní silné stránky)
4,9	Zpřístupňování dat interním i externím uživatelům.
4,6	Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.
4,4	Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb.
4,4	Poskytování vybraných veřejných služeb přes internet.
4,3	Poskytování služeb založených společností a zřízených organizací městem přes internet.
4,1	Sjednocené a vybudované prostředí pro výkon veřejné správy.
4,1	Uvolněný zastupitel pro oblast informatiky.
4,0	SMB má statut a může v rámci něj prosadit cíle v IT jak na MMB, tak i na ÚMČ (čl. 39 a 40).
3,6	Vytvořené prostředí pro zapojení občanů do dění města Brna.
3,4	Jsou vytvořeny specializované subjekty města k poskytování specifických ICT služeb.
2,3	Vybudovány pilotní lokality s poskytnutou konektivitou pro bezplatný přístup do internetu.

	Opportunities (vnější příležitosti)
4,7	Definice zákazníka ICT služeb a jeho potřeb.
4,3	Standardizace IT produktů na celostátní úrovni.
4,3	Rozšiřování zdrojů pro Open Data.
4,1	Koordinace ICT projektů městských subjektů.
3,9	Zintenzivnění spolupráce se středními a vysokými školami (využití jejich potenciálu).
3,9	Využití aktivit v rámci externích subjektů ke standardizaci požadavků na výstupy z IS OVM.
3,7	Spolupráce s jinými městy v ČR a EU.
3,6	Využití přínosů Smart City.
3,4	Využití možností spolufinancování nových služeb z externích zdrojů.

	Weaknesses (vnitřní slabé stránky)
4,6	Neexistence ICT technologického standardu města.
4,4	Nemožnost řešit problémy v informatice v době, kdy vznikají.
4,4	Pro občana nejsou přístupné agendy přes internet. Neexistuje superpodatelna (prezentační portál) umožňující sledování procesu.
4,3	Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu.
4,3	Není definován katalog elektronicky poskytovaných služeb.
4,1	Nízká míra využití potenciálu zavedených technologií.
4,1	Nízká srozumitelnost výdajů do IT. Důvodové zprávy zdůvodňují výdaje příliš technicky. Neexistují jednotná kritéria (metriky).

	Weaknesses (vnitřní slabé stránky)
3,9	Zastaralé a nepřehledné webové stránky města.

	Threats (vnější hrozby)
4,1	Požadavek na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.
4,1	Legislativa omezuje možnosti cílené komunikace s občanem např. v oblasti osobních údajů.
4,0	Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.
4,0	Realizace Open Data bez existujících pravidel.
4,0	Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.
3,9	Obtížnost standardizace při potřebě specifických ICT řešení na ÚMČ.

2.2.4. SWOT Spokojenost uživatelů

Výroky uvedené ve SWOT tabulce vychází z úhlu pohledu strategického týmu na spokojenost uživatelů informačních systémů.

	Strengths (vnitřní silné stránky)
5,0	Neomezenost počtu uživatelů v klíčových aplikacích z pohledu přístupu na informační systémy.
4,7	Zavedená helpdesková podpora uživatelů.
4,4	Průběžná obnova techniky (koncových zařízení).
3,7	Pravidelné školení na způsob práce s aplikacemi.
3,4	Dostupnost aktualizovaných manuálů na intranetu.

	Opportunities (vnější příležitosti)
4,6	Poskytnutí prostředků uživatelům pro přístup k informacím i z domova.
4,4	Poskytnutí dočasného přístupu k wi-fi návštěvníkům a zaměstnancům MMB.
4,1	Vytvoření "internetové přepážky".
4,0	Využití drobných specializovaných aplikací používaných v jiných městech.
3,9	Rozšíření IT na externí uživatele.
3,5	Postupy pro zpřístupnění a zpracování informací získaných cestou non-IT se zpětnou reakcí do IS přes vhodné prostředí.
3,3	Využití možností prvků "mikro ICT" (princip "Internetu věcí") a spolupráce s mobilním HW pro zpřístupnění služeb ICT občanům.

	Weaknesses (vnitřní slabé stránky)
4,6	Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.
4,4	Dosud nezavedená elektronická podpora některých vnitřních schvalovacích procesů úřadu (např. cestovních příkazů).
4,3	Uživatelé nemají povědomí o reálných možnostech řešení jejich požadavků (času, schopnosti řešit požadavek, finanční náročnosti). Nedostatečně objektivní požadavky uživatelů.
4,0	Klíčoví uživatelé z jednotlivých odborů MMB nemají uvolněnou kapacitu na poskytování součinnosti v IT při řešení požadavků týkajících se jejich odborné problematiky.
4,0	Uživatelé s přístupem k elektronickým materiálům vyžadují rovněž jejich tištěnou podobu, která pro jejich činnost není nutná.
3,7	Nejednotný přístup uživatelů k realizaci svých požadavků (formulace, spolupráce na řešení).

	Threats (vnější hrozby)
5,0	Výpadek metropolitní sítě a internetu znamená nefunkčnost významných agend SMB.

	Threats (vnější hrozby)
4,4	Závislost na správném fungování centrálních aplikací při poskytování služeb.
3,9	Legislativní omezení ICT služeb pro externí subjekty (občan, právnické osoby ...) ve formě využití inteligentních formulářů.
3,7	Mylný pohled na možnosti úřadu při řešení "životních situací" bez vnímání omezení (legislativa, zdroje ...).
3,4	Dodavatelé nemají dostatečnou znalost postupů ve veřejné správě a jsou závislí na znalostech uživatelů.

2.2.5. Sumarizační SWOT

Sumarizační SWOT tabulka obsahuje všechny výroky z předchozích SWOT analýz seřazené podle jejich síly od nejsilnějšího k nejslabšímu.

	Strengths (vnitřní silné stránky)	
5,0	Neomezenost počtu uživatelů v klíčových aplikacích z pohledu přístupu na informační systémy.	Uživatelé
4,9	Validní informace o EA jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.	Architektura
4,9	Zpřístupňování dat interním i externím uživatelům.	Přínosy
4,7	V rámci TSB je prováděno technologicky moderní ukládání dat se zajištěnou ochranou proti jejich ztrátě.	Architektura
4,7	Zavedená helpdesková podpora uživatelů.	Uživatelé
4,7	Kvalitní prostory a technologické zázemí pro umístění uzlových ICT prvků (datové centrum).	Architektura
4,6	Kvalifikovaní správci aplikací a ICT infrastruktury v oblasti, kterou mají ve své pracovní náplni.	Organizace
4,6	Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.	Přínosy
4,4	Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ).	Architektura
4,4	Kvalitní komunikační infrastruktura připojení ÚMČ.	Architektura
4,4	Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb.	Přínosy
4,4	Poskytování vybraných veřejných služeb přes internet.	Přínosy
4,4	Průběžná obnova techniky (koncových zařízení).	Uživatelé
4,3	Jistota prostředků na kalendářní rok v rámci schváleného rozpočtu.	Organizace
4,3	Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy.	Architektura
4,3	Poskytování služeb založených společností a zřízených organizací městem přes internet.	Přínosy
4,2	Efektivní licencování pro základní části městského AIS a office SW.	Architektura
4,1	Sjednocené a vybudované prostředí pro výkon veřejné správy.	Přínosy
4,1	Uvolněný zastupitel pro oblast informatiky.	Přínosy
4,0	Dosažené zkušenosti s implementací informačních systémů.	Organizace
4,0	Vysoká znalost technologických trendů a jejich zavádění.	Organizace
4,0	Architektura pro integrace aplikací – integrační platforma (s využitím principů ESB a ETL).	Architektura
4,0	SMB má statut a může v rámci něj prosadit cíle v IT jak na MMB, tak i na ÚMČ (čl. 39 a 40).	Přínosy
3,9	Průběžně aktualizovaný a doplňovaný popis procesů MMB.	Organizace
3,8	Zvyšující se bezpečnostní povědomí mezi pracovníky OMI a rovněž pracovníky MMB.	Organizace
3,7	Pravidelné školení na způsob práce s aplikacemi.	Uživatelé
3,7	Je k dispozici prostředí (framework) pro tvorbu jednoduché podpory procesů a workflow v nich (MOSS – MS Office Share Point Services) s komunitou uživatelů.	Architektura
3,6	Certifikace OMI na informační bezpečnost (procesy řízení a realizace projektů v oblasti ICT, poskytování služeb uživatelům ICT) podle ISO 27001.	Organizace
3,6	Vytvořené prostředí pro zapojení občanů do dění města Brna.	Přínosy

	Strengths (vnitřní silné stránky)	
3,4	Jsou vytvořeny specializované subjekty města k poskytování specifických ICT služeb.	Přínosy
3,4	Dostupnost aktualizovaných manuálů na intranetu.	Uživatelé
3,4	Systém povinného vzdělávání úředníků.	Organizace
2,3	Vybudovány pilotní lokality s poskytnutou konektivitou pro bezplatný přístup do internetu.	Přínosy

	Opportunities (vnější příležitosti)	
4,7	Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.	Architektura
4,7	Definice zákazníka ICT služeb a jeho potřeb.	Přínosy
4,6	Vytvoření a správa katalogu služeb ICT.	Architektura
4,6	Poskytnutí prostředků uživatelům pro přístup k informacím i z domova.	Uživatelé
4,4	Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy).	Architektura
4,4	Propojení GPC konfiguračních databází udržovaných MMB a samostatně dodavateli/správci částí infrastruktury.	Architektura
4,4	Řízení optimalizace licencí ve vazbě na skutečnou potřebu.	Architektura
4,4	Poskytnutí dočasného přístupu k wi-fi návštěvníkům a zaměstnancům MMB.	Uživatelé
4,3	Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu.	Architektura
4,3	Vytvoření centrálního přístupového bodu pro řízený přístup uživatelů do IS města a k aplikacím z různých platforem.	Architektura
4,3	Standardizace IT produktů na celostátní úrovni.	Přínosy
4,3	Rozšiřování zdrojů pro Open Data.	Přínosy
4,2	Větší využití ETL Clover pro datovou integraci systémů.	Architektura
4,1	Vytvoření samostatného útvaru řešícího informatiku SMB.	Architektura
4,1	Koordinace ICT projektů městských subjektů.	Přínosy
4,1	Vytvoření "internetové přepážky".	Uživatelé
4,1	Disponibilní vzdělaní a kompetentní pracovníci v ICT v Brně.	Organizace
4,0	Vydání IT směrnic závazných pro SMB.	Architektura
4,0	Vytvořit prostředí pro drobné aplikace odborných útvarů SMB.	Architektura
4,0	Vytvoření prioritizace cca 350 aplikací a odstupňovaný přístup k nim podle jejich priorit.	Architektura
4,0	Využití Národního architektonického plánu s návrhovými vzory vybraných oblastí.	Architektura
4,0	Využití drobných specializovaných aplikací používaných v jiných městech.	Uživatelé
3,9	Zapojení vysokých škol do rozvoje informatiky města Brna včetně aktivní spolupráce města při výuce studentů.	Organizace
3,9	Využití externích kapacit výzkumu a vývoje pro oponenturu rozvojových koncepčních plánu a projektů (CERIT, NUKIB, Útvar hlavního architekta eGov…).	Architektura
3,9	Metodická pomoc kompetenčního centra uživatelům z ÚMČ a organizací města.	Architektura
3,9	Popsání definice vazeb mezi projekty a sesouladění postupů – road-mapa na období několika let s pravidelnou aktualizací.	Architektura
3,9	Zintenzivnění spolupráce se středními a vysokými školami (využití jejich potenciálu).	Přínosy
3,9	Využití aktivit v rámci externích subjektů ke standardizaci požadavků na výstupy z IS OVM.	Přínosy
3,9	Rozšíření IT na externí uživatele.	Uživatelé
3,7	Spolupráce s jinými městy v ČR a EU.	Přínosy
3,6	Využití přínosů Smart City.	Přínosy
3,5	Postupy pro zpřístupnění a zpracování informací získaných cestou non-IT se zpětnou reakcí do IS přes vhodné prostředí.	Uživatelé

	Opportunities (vnější příležitosti)	
3,4	Využití možností spolufinancování nových služeb z externích zdrojů.	Přínosy
3,4	Maximální možné čerpání prostředků z fondů EU.	Organizace
3,4	Využití potenciálu odborníků v rámci města ve formě poradenského orgánu.	Organizace
3,3	Využití možností prvků "mikro ICT" (princip "Internetu věcí") a spolupráce s mobilním HW pro zpřístupnění služeb ICT občanům.	Uživatelé
3,1	Zvyšující se zájem stakeholderů o přístup k informacím z EA modelu.	Architektura
3,1	Transformace služeb informatiky do samostatného ekonomického subjektu ovládaného městem Brnem.	Organizace

	Weaknesses (vnitřní slabé stránky)	
4,6	Neexistence ICT technologického standardu města.	Přínosy
4,6	Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.	Uživatelé
4,5	Motivační systém neumožňuje získávat nové a udržet stávající pracovníky IT.	Organizace
4,4	Nemožnost řešit problémy v informatice v době, kdy vznikají.	Přínosy
4,4	Pro občana nejsou přístupné agendy přes internet. Neexistuje superpodatelna (prezentační portál) umožňující sledování procesu.	Přínosy
4,4	Dosud nezavedená elektronická podpora některých vnitřních schvalovacích procesů úřadu (např. cestovních příkazů).	Uživatelé
4,3	Neexistuje provozní aplikační a datový monitoring a konfigurační management na aplikační vrstvě.	Architektura
4,3	Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).	Architektura
4,3	Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu.	Přínosy
4,3	Není definován katalog elektronicky poskytovaných služeb.	Přínosy
4,3	Uživatelé nemají povědomí o reálných možnostech řešení jejich požadavků (času, schopnosti řešit požadavek, finanční náročnosti). Nedostatečně objektivní požadavky uživatelů.	Uživatelé
4,1	Chybí vazba na business vrstvu zpracovávanou ORGO v BPMN diagramech.	Architektura
4,1	Nízká míra využití potenciálu zavedených technologií.	Přínosy
4,1	Nízká srozumitelnost výdajů do IT. Důvodové zprávy zdůvodňují výdaje příliš technicky. Neexistují jednotná kritéria (metriky).	Přínosy
4,0	Chybí standardizovaný Business CASE propojený na EA.	Architektura
4,0	Data nejsou ukládána do datových úložišť ve strukturované podobě, která umožní řízení přístupu dle oprávnění.	Architektura
4,0	Neexistence geograficky oddělené záložní infrastruktury.	Architektura
4,0	Klíčoví uživatelé z jednotlivých odborů MMB nemají uvolněnou kapacitu na poskytování součinnosti v IT při řešení požadavků týkajících se jejich odborné problematiky.	Uživatelé
4,0	Uživatelé s přístupem k elektronickým materiálům vyžadují rovněž jejich tištěnou podobu, která pro jejich činnost není nutná.	Uživatelé
3,9	Model EA zahrnuje jen MMB a absentují organizace SMB.	Architektura
3,9	Nevytvořený katalog datových prvků a inventarizace dat jak z provozních IS, tak s využitím plánovaného budování úložišť dat (DWH – datový sklad, UNED - úložiště nestrukturovaných dat, DES - digitální spisovna).	Architektura
3,9	Zastaralá HW infrastruktura.	Architektura
3,9	Zastaralé a nepřehledné webové stránky města.	Přínosy
3,8	Samostatný vzájemně málo koordinovaný postup MČ při rozvoji IS.	Organizace
3,8	Ne všichni klíčoví uživatelé (garanti) mají dostatečné znalosti, aby definovali požadavky na informatiku (formulace toho, co chtějí). OMI nemůže suplovat metodické role uživatelů.	Organizace

	Weaknesses (vnitřní slabé stránky)	
3,8	Nedostatek vnitřních odborných kapacit vzhledem k rostoucímu významu informatiky vede ke zvýšenému nákupu externích služeb.	Organizace
3,7	Městské firmy si spravují vlastní podružná menší datová centra i aplikace bez vazby na EA.	Architektura
3,7	Nedostatečná aplikace principů procesního řízení.	Architektura
3,7	Nejednotný přístup uživatelů k realizaci svých požadavků (formulace, spolupráce na řešení).	Uživatelé
3,6	Neexistence záložních tras propojení uzlových bodů metropolitní sítě.	Architektura
3,4	Nedostatečně rozvinutá integrační platforma (middleware).	Architektura
3,3	IDM nemá zadefinované role z business vrstvy (není propojení EA až do procesní business vrstvy a její rozpracování na role).	Architektura
3,3	Závislost rozvoje architektury na přidělených prostředcích (rozpočtu).	Architektura
3,3	Nedostatečné povědomí klíčových uživatelů o plánovaní kapacit zdrojů OMI na pokrytí požadavků.	Organizace
3,2	Není záloha Internetového připojení – při výpadku dojde k ohrožení činností úřadu. Neexistence paralelního (náhradního) internetového připojení.	Architektura
3,1	Omezený a složitý přístup k aplikacím z vnějšího prostředí – restriktivní řešení bezpečnostních rizik.	Architektura
3,1	Klíčové uživatele je obtížné motivovat pro práci týkající se informatiky z důvodu střetu liniových a projektových struktur.	Organizace
3,0	Řada aplikací nemá dokumentaci.	Architektura
2,9	Platformová technologická roztříštěnost (např. různé db stroje).	Architektura
2,6	Plánování a využití kapacit všech zdrojů v souladu s požadavky vykonávaných procesů.	Architektura

	Threats (vnější hrozby)	
5,0	Masivní vývoj kybernetických útoků a jejich forem.	Organizace
5,0	Výpadek metropolitní sítě a internetu znamená nefunkčnost významných agend SMB.	Uživatelé
4,6	Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.	Architektura
4,4	Závislost na správném fungování centrálních aplikací při poskytování služeb.	Uživatelé
4,1	Požadavek na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.	Přínosy
4,1	Legislativa omezuje možnosti cílené komunikace s občanem např. v oblasti osobních údajů.	Přínosy
4,0	Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT.	Organizace
4,0	EA model obsahuje koncentrované informace a při neoprávněném přístupu k nim jde bezpečnostní riziko.	Architektura
4,0	Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.	Přínosy
4,0	Realizace Open Data bez existujících pravidel.	Přínosy
4,0	Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.	Přínosy
3,9	Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.	Organizace
3,9	Obtížnost standardizace při potřebě specifických ICT řešení na ÚMČ.	Přínosy
3,9	Legislativní omezení ICT služeb pro externí subjekty (občan, právnické osoby ..) ve formě využití inteligentních formulářů.	Uživatelé
3,8	Neexistence plánu a pevných milníků pro nasazení nových centrálních IS s dopadem na činnosti OVM, což znamená negativní dopady na plánování zdrojů OVM, zejména při našem rozsahu správního obvodu (např. aplikace CRR, CRV, digitalizace dokumentů pro centrální agendy, rušení místní příslušnosti …).	Architektura
3,7	Mylný pohled na možnosti úřadu při řešení "životních situací" bez vnímání omezení (legislativa, zdroje ...).	Uživatelé

	Threats (vnější hrozby)	
3,6	Z výběrových řízení podle ZVZ mohou vzejít neadekvátní dodavatelé nebo mohou výběrová řízení trvat nepredikovatelnou dobu.	Organizace
3,6	Konfliktní požadavky změn legislativy s dopadem do informačních systémů.	Architektura
3,6	Nedostatečná pozornost ze strany tvůrců prvků celostátního eGovernment, věnovaná specifickým potřebám statutárních měst.	Architektura
3,4	Hrozba výpadku veřejného internetového připojení u MMB.	Architektura
3,4	Dodavatelé nemají dostatečnou znalost postupů ve veřejné správě a jsou závislí na znalostech uživatelů.	Uživatelé
3,3	Dlouhá doba od vytvoření záměru do jeho realizace způsobená interními předpisy nebo platnou legislativou.	Organizace
2,8	Přidělení finančních prostředků z rozpočtu je vždy jen na rok (rozpočtování je jen roční), v IT není zavedeno víceleté financování.	Organizace

2.3. Variantní strategické možnosti vycházející z analýzy kvadrantů SWOT

Výsledky SWOT analýz ukazují na následující variantní strategické možnosti pro další rozvoj informatiky. Jde o možnosti generované z analýzy kvadrantů SWOT analýz, nejde zde tedy ještě o strategické záměry nebo cíle.

Strategie S-O „VYUŽITÍ“ (využití vnitřních silných stránek a vnějších příležitostí)

[SO1] Využití vnitřní silné stránky
Zpřístupňování dat interním i externím uživatelům.
k vnější příležitosti
Definice zákazníka ICT služeb a jeho potřeb.
Vytvoření a správa katalogu služeb ICT.
Poskytnutí prostředků uživatelům pro přístup k informacím i z domova.

[SO2] Využití vnitřní silné stránky
Neomezenost počtu uživatelů v klíčových aplikacích z pohledu přístupu na informační systémy.
k vnější příležitosti
Definice zákazníka ICT služeb a jeho potřeb.

[SO3] Využití vnitřní silné stránky
Validní informace o EA jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.
k vnější příležitosti
Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.
Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy).

[SO4] Využití vnitřní silné stránky
V rámci TSB je prováděno technologicky moderní ukládání dat se zajištěnou ochranou proti jejich ztrátě.
k vnější příležitosti
Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu.

[SO5] Využití vnitřní silné stránky
Efektivní licencování pro základní části městského AIS a office SW.
Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ).
k vnější příležitosti
Řízení optimalizace licencí ve vazbě na skutečnou potřebu.

[SO6] Využití vnitřní silné stránky
Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ).
k vnější příležitosti
Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu.

[SO7] Využití vnitřní silné stránky
Poskytování služeb založených společností a zřízených organizací městem přes internet.
k vnější příležitosti
Vytvoření centrálního přístupového bodu pro řízený přístup uživatelů do IS města a k aplikacím z různých platforem.

[SO8] Využití vnitřní silné stránky
Kvalitní prostory a technologické zázemí pro umístění uzlových ICT prvků (datové centrum).
k vnější příležitosti
Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.
Standardizace IT produktů na celostátní úrovni.
Vydání IT směrnic závazných pro SMB.

[SO9] Využití vnitřní silné stránky
Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb.
k vnější příležitosti
Definice zákazníka ICT služeb a jeho potřeb.
Vytvoření a správa katalogu služeb ICT.

[SO10] Využití vnitřní silné stránky
Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy.
k vnější příležitosti
Standardizace IT produktů na celostátní úrovni.
Vytvoření samostatného útvaru řešícího informatiku SMB.

Strategie S-T „KONFRONTACE“ (využití vnitřní síly k zamezení vnějších hrozeb)

[ST1] Využití vnitřní silné stránky
V rámci TSB je prováděno technologicky moderní ukládání dat se zajištěnou ochranou proti jejich ztrátě.
k zamezení vnější hrozby
Masivní vývoj kybernetických útoků a jejich forem.
Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.

[ST2] Využití vnitřní silné stránky
Kvalitní prostory a technologické zázemí pro umístění uzlových ICT prvků (datové centrum).
Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb.
Kvalitní komunikační infrastruktura připojení ÚMČ.
k zamezení vnější hrozby
Výpadek metropolitní sítě a internetu znamená nefunkčnost významných agend SMB.

[ST3] Využití vnitřní silné stránky
Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.
k zamezení vnější hrozby
Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.

[ST4] Využití vnitřní silné stránky
Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy.
k zamezení vnější hrozby
Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.

[ST5] Využití vnitřní silné stránky
Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy.
k zamezení vnější hrozby
Požadavek na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.

[ST6] Využití vnitřní silné stránky
Uvolněný zastupitel pro oblast informatiky.
k zamezení vnější hrozby
Neexistence plánu a pevných milníků pro nasazení nových centrálních IS s dopadem na činnosti OVM, což znamená negativní dopady na plánování zdrojů OVM, zejména při našem rozsahu správního obvodu (např. aplikace CRR, CRV, digitalizace dokumentů pro centrální agendy, rušení místní příslušnosti …).
Realizace Open Data bez existujících pravidel.

[ST7] Využití vnitřní silné stránky
Dosažené zkušenosti s implementací informačních systémů.
k zamezení vnější hrozby
Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.

Strategie W-O „HLEDÁNÍ“ (překonání vnitřních slabostí využitím vnějších příležitostí)

[WO1] Překonání vnitřní slabosti
Neexistuje provozní aplikační a datový monitoring a konfigurační management na aplikační vrstvě.
využitím vnější příležitosti
Zintenzivnění spolupráce se středními a vysokými školami (využití jejich potenciálu).

[WO2] Překonání vnitřní slabosti
Neexistence ICT technologického standardu města.
využitím vnější příležitosti
Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.

[WO3] Překonání vnitřní slabosti
Pro občana nejsou přístupné agendy přes internet. Neexistuje superpodatelna (prezentační portál) umožňující sledování procesu.
využitím vnější příležitosti
Vytvoření centrálního přístupového bodu pro řízený přístup uživatelů do IS města a k aplikacím z různých platforem.
Vytvoření "internetové přepážky".

[WO4] Překonání vnitřní slabosti
Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.
využitím vnější příležitosti
Disponibilní vzdělaní a kompetentní pracovníci v ICT v Brně.

[WO5] Překonání vnitřní slabosti
Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu.
využitím vnější příležitosti
Vytvoření a správa katalogu služeb ICT.
Vydání IT směrnic závazných pro SMB.

[WO6] Překonání vnitřní slabosti
Nízká míra využití potenciálu zavedených technologií.
využitím vnější příležitosti
Definice zákazníka ICT služeb a jeho potřeb.
Využití aktivit v rámci externích subjektů ke standardizaci požadavků na výstupy z IS OVM.

[WO7] Překonání vnitřní slabosti
Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).
využitím vnější příležitosti
Využití externích kapacit výzkumu a vývoje pro oponenturu rozvojových koncepčních plánu a projektů (CERIT, NUKIB, Útvar hlavního architekta eGov …).
Zintenzivnění spolupráce se středními a vysokými školami (využití jejich potenciálu).
Využití aktivit v rámci externích subjektů ke standardizaci požadavků na výstupy z IS OVM.

[WO8] Překonání vnitřní slabosti
Není definován katalog elektronicky poskytovaných služeb.
využitím vnější příležitosti
Vytvoření a správa katalogu služeb ICT.

Strategie W-T „VYHÝBÁNÍ“ (preventivní obrana proti skloubení vnitřních slabostí s vnějšími hrozbami)

[WT1] Preventivní obrana proti skloubení vnitřní slabosti
Neexistuje provozní aplikační a datový monitoring a konfigurační management na aplikační vrstvě.
Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.
s vnější hrozbou
Masivní vývoj kybernetických útoků a jejich forem.
Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.

[WT2] Preventivní obrana proti skloubení vnitřní slabosti
Neexistence ICT technologického standardu města.
s vnější hrozbou
Obtížnost standardizace při potřebě specifických ICT řešení na ÚMČ.

[WT3] Preventivní obrana proti skloubení vnitřní slabosti
Motivační systém neumožňuje získávat nové a udržet stávající pracovníky IT.
s vnější hrozbou
Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT.

[WT4] Preventivní obrana proti skloubení vnitřní slabosti
Data nejsou ukládána do datových úložišť ve strukturované podobě, která umožní řízení přístupu dle oprávnění.
s vnější hrozbou
Realizace Open Data bez existujících pravidel.

[WT5] Preventivní obrana proti skloubení vnitřní slabosti
Uživatelé nemají povědomí o reálných možnostech řešení jejich požadavků (času, schopnosti řešit požadavek, finanční náročnosti). Nedostatečně objektivní požadavky uživatelů.

s vnější hrozbou
Legislativa omezuje možnosti cílené komunikace s občanem např. v oblasti osobních údajů.
Požadavek na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.

[WT6] Preventivní obrana proti skloubení vnitřní slabosti
Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).
s vnější hrozbou
Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.
Neexistence plánu a pevných milníků pro nasazení nových centrálních IS s dopadem na činnosti OVM, což znamená negativní dopady na plánování zdrojů OVM, zejména při našem rozsahu správního obvodu (např. aplikace CRR, CRV, digitalizace dokumentů pro centrální agendy, rušení místní příslušnosti …).

[WT7] Preventivní obrana proti skloubení vnitřní slabosti
Nízká srozumitelnost výdajů do IT. Důvodové zprávy zdůvodňují výdaje příliš technicky. Neexistují jednotná kritéria (metriky).
s vnější hrozbou
Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.

[WT8] Preventivní obrana proti skloubení vnitřní slabosti
Pro občana nejsou přístupné agendy přes internet. Neexistuje superpodatelna (prezentační portál) umožňující sledování procesu.
s vnější hrozbou
Legislativa omezuje možnosti cílené komunikace s občanem např. v oblasti osobních údajů.

[WT9] Preventivní obrana proti skloubení vnitřní slabosti
Nemožnost řešit problémy v informatice v době, kdy vznikají.
s vnější hrozbou
Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.

[WT10] Preventivní obrana proti skloubení vnitřní slabosti
Neexistence geograficky oddělené záložní infrastruktury.
s vnější hrozbou
Výpadek metropolitní sítě a internetu znamená nefunkčnost významných agend SMB.
Závislost na správném fungování centrálních aplikací při poskytování služeb.

2.4. Strategické záměry vycházející z variantních strategických možností

Z variantních strategických možností získaných porovnáním kvadrantů SWOT analýz byly následně jejich seskupením na základě podobného zaměření vytvořeny možné strategické záměry, které ukazují na nejlépe využitelné strategické možnosti vyplývající ze současného stavu.

Strategické záměry byly ohodnoceny v pětibodové stupnici, kde 5 značí mimořádně silný záměr a 1 slabý záměr. Hodnota uvedená u záměru je dána jako průměr hodnocení všech členů strategického týmu (bez týmu externí podpory). Strategické záměry jsou seřazeny od nejvýše hodnocených směrem ke klesajícímu ohodnocení.

	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
4,9	S-O	SMB má statut a může v rámci něj prosadit cíle v IT jak na MMB, tak i na ÚMČ (čl. 39 a 40). Neomezenost počtu uživatelů v klíčových aplikacích z pohledu přístupu na informační systémy. Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ). Poskytování služeb založených společností a zřízených organizací městem přes internet. Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb. V rámci TSB je prováděno technologicky moderní ukládání dat se zajištěnou ochranou proti jejich ztrátě. Kvalitní prostory a technologické zázemí pro umístění uzlových ICT prvků (datové centrum).	Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu. Vydání IT směrnic závazných pro SMB.	Rozšířit využívání aplikací v městském cloudu podle závazně dohodnutých pravidel.

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
4,6	W-O	Pro občana nejsou přístupné agendy přes internet. Neexistuje superpodatelna (prezentační portál) umožňující sledování procesu. Není definován katalog elektronicky poskytovaných služeb.	Vytvoření centrálního přístupového bodu pro řízený přístup uživatelů do IS města a k aplikacím z různých platforem. Vytvoření "internetové přepážky". Vytvoření a správa katalogu služeb ICT.	Umožnit přístup k agendám přes internet pomocí internetové přepážky nabízející služby dle katalogu služeb ICT.

	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
4,5	S-O	Validní informace o EA jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu. Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy. Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.	Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti. Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy).	Vytvořit technologický standard SMB (nikoliv jen MMB). Dlouhodobě plánovat architektonický rozvoj na všech úrovních EA.

	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
4,4	S-T	V rámci TSB je prováděno technologicky moderní ukládání dat se zajištěnou ochranou proti jejich ztrátě. Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.	Masivní vývoj kybernetických útoků a jejich forem. Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.	Chránit bezpečnost dat (integrita, dostupnost, důvěrnost)..

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
4,3	W-T	Neexistuje provozní aplikační a datový monitoring a konfigurační management na aplikační vrstvě. Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.	Masivní vývoj kybernetických útoků a jejich forem. Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.	Zvýšení úrovně informační bezpečnosti na všech vrstvách (tj. včetně datové).

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
4,3	W-T	Neexistence geograficky oddělené záložní infrastruktury.	Výpadek metropolitní sítě a internetu znamená nefunkčnost významných agend SMB. Závislost na správném fungování centrálních aplikací při poskytování služeb.	Dosáhnout odolnosti infrastruktury proti výpadku jednotlivých prvků vč. internetového připojení.

	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
4,1	S-T	Kvalitní prostory a technologické zázemí pro umístění uzlových ICT prvků (datové centrum). Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb. Kvalitní komunikační infrastruktura připojení ÚMČ.	Výpadek metropolitní sítě a internetu znamená nefunkčnost významných agend SMB.	Dosáhnout odolnosti infrastruktury proti výpadku jednotlivých prvků vč. internetového připojení.

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
4,0	W-O	Neexistence ICT technologického standardu města.	Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.	Vytvořit technologický standard SMB (nikoliv jen MMB).

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
4,0	W-O	Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu. Nízká míra využití potenciálu zavedených technologií. Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi. Dosud nezavedená elektronická podpora některých vnitřních schvalovacích procesů úřadu (např. cestovních příkazů).	Vytvoření a správa katalogu služeb ICT. Vydání IT směrnic závazných pro SMB.	Maximálně propojit IT pracovníky a garanty do rozvoje a využívání IS.

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
4,0	W-T	Data nejsou ukládána do datových úložišť ve strukturované podobě, která umožní řízení přístupu dle oprávnění.	Realizace Open Data bez existujících pravidel.	Zvýšení úrovně informační bezpečnosti na všech vrstvách (tj. včetně datové).

	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
3,9	S-O	Zpřístupňování dat interním i externím uživatelům. Zavedená helpdesková podpora uživatelů.	Definice zákazníka ICT služeb a jeho potřeb. Vytvoření a správa katalogu služeb ICT. Poskytnutí prostředků uživatelům pro přístup k informacím i z domova.	Poskytovat profesionálně zadefinované ICT služby za nastavených SLA/OLA parametrů pro interní a externí uživatele.

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
3,9	W-O	Neexistuje provozní aplikační a datový monitoring a konfigurační management na aplikační vrstvě.	Zintenzivnění spolupráce se středními a vysokými školami (využití jejich potenciálu).	Aktivní monitoring na aplikační a datové vrstvě zavést s využitím potenciálu středních škol a univerzit.

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,8	W-T	Motivační systém neumožňuje získávat nové a udržet stávající pracovníky IT.	Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT.	Vytvořit motivační systém pro pracovníky v IT. který bude pro určité skupiny pracovníků dostatečně atraktivní.

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,8	W-T	Nemožnost řešit problémy v informatice v době, kdy vznikají.	Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.	Aktivní zjišťování plánů rozvoje centrálních IS s cílem získat dostatečný čas na přípravu souvisejících změn. Zavést pravidla pro rychlé schvalování projektů na základě shody s informační strategií, architekturou s jejich zdůvodněním formou Business Case.

	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
3,6	S-T	Uvolněný zastupitel pro oblast informatiky. Dosažené zkušenosti s implementací informačních systémů.	Neexistence plánu a pevných milníků pro nasazení nových centrálních IS s dopadem na činnosti OVM, což znamená negativní dopady na plánování zdrojů OVM, zejména při našem rozsahu správního obvodu (např. aplikace CRR, CRV, digitalizace dokumentů pro centrální agendy, rušení místní příslušnosti …). Závislost na správném fungování centrálních aplikací při poskytování služeb. Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.	Aktivní zjišťování plánů rozvoje centrálních IS s cílem získat dostatečný čas na přípravu souvisejících změn.

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
3,6	W-O	Motivační systém neumožňuje získávat nové a udržet stávající pracovníky IT.	Disponibilní vzdělaní a kompetentní pracovníci v ICT v Brně.	Vytvořit motivační systém pro pracovníky v IT. který bude pro určité skupiny pracovníků dostatečně atraktivní.

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
3,6	W-O	Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).	Využití externích kapacit výzkumu a vývoje pro oponenturu rozvojových koncepčních plánu a projektů (CERIT, NUKIB, Útvar hlavního architekta eGov…). Zintenzivnění spolupráce se středními a vysokými školami (využití jejich potenciálu). Využití aktivit v rámci externích subjektů ke standardizaci požadavků na výstupy z IS OVM.	Zintenzivnit spolupráci s externími zdroji.

	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
3,5	S-T	Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy. Validní informace o EA jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.	Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.	Realizovat dlouhodobé rozvojové projekty přesahující volební období.

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,5	W-T	Neexistence ICT technologického standardu města.	Obtížnost standardizace při potřebě specifických ICT řešení na ÚMČ.	Technologický standard SMB musí umožňovat realizaci specifických ICT řešení za definovaných podmínek.

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,5	W-T	Nízká srozumitelnost výdajů do IT. Důvodové zprávy zdůvodňují výdaje příliš technicky. Neexistují jednotná kritéria (metriky).	Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.	Zavést pravidla pro rychlé schvalování projektů na základě shody s informační strategií, architekturou s jejich zdůvodněním formou Business Case.

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,3	W-T	Uživatelé nemají povědomí o reálných možnostech řešení jejich požadavků (času, schopnosti řešit požadavek, finanční náročnosti). Nedostatečně objektivní požadavky uživatelů.	Požadavek na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení. Legislativa omezuje možnosti cílené komunikace s občanem např. v oblasti osobních údajů.	Maximálně propojit IT pracovníky a garanty do rozvoje a využívání IS.

3. Návrh cílového stavu

Cílový stav je popsán v systému 19 strategických cílů zařazených ve čtyřech perspektivách metody Balanced Scorecard, přičemž cíle slouží k dosažení vize a mise informatiky města Brna. Strategické cíle jsou vzájemně provázané a vytvářejí strategické řetězce, které ukazují na příčinu a následek v systému strategických cílů.

3.1. Vize & mise informatiky města Brna

3.1.1. Vize města[18]

Brno v roce 2050 je v mezinárodních srovnáních synonymem atraktivního a zároveň udržitelného města.

Brňané oceňují vysokou kvalitu života ve městě, které jim nabízí uplatnění v práci i podnikání, zábavě i odpočinku. Propojují se zde plody výzkumu a inovací s ekonomickou prosperitou jednotlivců i firem. Městská krajina se snoubí s okolní přírodou. Brno je město bez bariér a poskytuje Brňanům kvalitní veřejný prostor. Otevřenost i soudržnost na jedné straně a zdravé a odolné prostředí na straně druhé zde vytvářejí domov a bezpečné zázemí pro půl milionu lidí.

Brňané si uvědomují vzácnost a omezenost přírodních zdrojů, podporují jejich efektivní využití, tak aby město mělo stále dostatek vody, energie i prostředků pro svůj rozvoj. Chtějí město zanechat budoucím generacím ve stejném nebo lepším stavu.

Brňané vnímají, že město je spravováno energicky, moderně a efektivně. Jeho správa a rozvoj jsou založeny na kultivované veřejné debatě a dlouhodobé spolupráci všech partnerů. Město dýchá pro své obyvatele a ti mohou být na své město hrdi.

Brno je město spravované dobře a s láskou. **Systém správy města je jednoduchý, srozumitelný a vstřícný k obyvatelům města**. Brňané se dlouhodobě zajímají o rozvoj města a aktivně se na něm podílejí. Už dávno se však nejedná jen o samotné Brno: město se svým zázemím funguje jako jeden propojený celek – Brněnská metropolitní oblast.

Brno v roce 2050 hovoří jazykem srozumitelným občanům města i jeho návštěvníkům. Kromě českého jazyka je možné komunikovat s orgány města bez jakýkoliv omezení minimálně ještě dalším jedním světovým jazykem – anglicky. **Informace jsou jednoduše dohledatelné a srozumitelné všem.** Jsou vždy aktuální, důvěryhodné, poučné, nestranné, jednoduché na pochopení, užitečné a přesné. Brno vytváří taková místa, která zjednodušují občanům dohledatelnost libovolných informací týkajících se města i přístup ke službám, které město poskytuje. Informační systém měst a jeho organizací je integrován do systému e-Governmentu, úkony i komunikace ze strany města i občanů probíhá převážně elektronicky. Napříč celým systémem **je zajištěna kybernetická bezpečnost**.

Díky jednotnému informačnímu portálu, ve kterém budou přehledně, srozumitelně a strukturovaně prezentovány připravované i realizované záměry města, **bude zajištěna informovanost** veřejnosti i vstupní prostor pro zapojení do participačních aktivit. Koordinovaným zapojením odborníků z univerzit, praxe i zahraničí a vytvořením prostoru pro odborný dialog bude zajištěno zvýšení kvality výstupů veřejné správy města. Zmíněné změny povedou ke zvýšení kvality života ve městě i spokojenosti obyvatel.

Otevřená data jsou v roce 2050 obnovitelným palivem digitální ekonomiky, jehož těžba město nestojí takřka nic. **Brno dává k dispozici všechna data s výjimkou zákonných omezení**, která mají před otevřeností přednost. Uvědomuje si, že bez kontextu může být nesnadné otevřená data interpretovat, proto zveřejňuje nejen surová data, ale i jejich popis, včetně popisu základních souvislostí, které mezi jednotlivými datovými sadami panují.

18 Vize a Strategie **#brno 2050** (https://brno2050.cz/pdf/Strategie_BRNO_2050_strategicka_cast_FINAL_web_12_12_2017.pdf)

3.1.2. Vize informatiky města Brna

Informatika města Brna vytváří pomocí moderních informačních a komunikačních technologií trvalé podmínky pro efektivní správu města a zajišťuje jednoduchou a srozumitelnou komunikaci a sdílení informací mezi městem, občany a společnostmi v brněnské metropoli.

3.1.3. Mise informatiky města Brna

Informatika města Brna bude postavena na městském cloudu poskytujícím služby v modelu IT jako služba (IT as a service - ITaaS).

3.2. Strategické cíle

Na základě SWOT analýzy současného stavu byly stanoveny strategické cíle ve čtyřech perspektivách metody Balanced Scorecard:

- ICT přínosy;
- ICT zákazníci;
- Procesy;
- ICT potenciál a zdroje.

Pro každou perspektivu bylo stanoveno motto, které souhrnně vyjadřuje strategické směřování informatiky pro danou perspektivu.

Název perspektivy a v ní pokládaná stěžejní otázka pro stanovení strategických cílů	**Motto perspektivy**
Perspektiva ICT přínosů Jaké přínosy bude mít zadávající organizace (město Brno)?	Moderní ICT města
Perspektiva ICT zákazníků Co získají zákazníci (uživatelé, občané)?	Motivace k využívání elektronických služeb
Perspektiva procesů Jaké procesy a funkcionalita informačních systémů umožní dosáhnout hodnot pro uživatele?	Umožnit technologiemi elektronické služby
Perspektiva ICT potenciálu a zdrojů Jaký je potenciál a zdroje pro strategický rozvoj informatiky města?	Náskok v aplikaci moderních digitálních technologií

Při formulování strategických cílů byly zohledněny zásady metodiky Balanced Scorecard (Horváth & Partners: Balanced Scorecard v praxi, Profess Consulting s.r.o., 2002):

- Omezující funkce: BSC vede k omezení nadbytku údajů plynoucích z operativních činností (na základě definice služeb a ukazatelů) na ty, které mají strategický význam a identifikují důležité změny (v rámci perspektiv).
- Funkce zaměření: BSC koncentruje pozornost politického vedení příp. orgánů veřejné správy na ujednané a významné perspektivy.
- Spojovací funkce: BSC je spojovacím článkem mezi strategií a přidělováním finančních prostředků.
- Integrační funkce: BSC zohledňuje rovnoměrně jak finanční, tak nefinanční charakteristiky. Tím BSC vyrovnává převahu čistě monetárních aspektů, jejichž převažující vliv lze často objevit i v nových modelech řízení státní a veřejné správy.
- Argumentační funkce: BSC zohledňuje různé úhly pohledu (perspektivy), které musí každá organizace obsahově naplnit (cíli a měřítky výkonnosti).

3.2.1. Cíle v perspektivě ICT potenciál a zdroje

číslo	strategický cíl	popis
1	Vytvořit platformu pro moderní portál města	Jsou implementovány technologie pro centrální technologické řešení portálu města umožňující poskytovat zejména elektronické služby: • úřední pro občany / úředníky • turisticko / informační • otevřená data • geoportál. Součástí portálu města Brna je řešení jeho kybernetické bezpečnosti.
2	Zavést eIDAS (elektronická identita a důvěryhodné el. dokumenty)	Plné zajištění shody s požadavky eIDAS umožňující poskytovat důvěryhodné elektronické služby Úřadu.
3	Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách	Provozování městského dohledového provozního a bezpečnostního centra (SOC - Security Operation Center) integrujícího všechny bezpečnostní technologie.
4	Vytvořit sdílený městský cloud postavený na odolné infrastruktuře vč. datových úložišť	Sdílený městský cloud je vybaven geograficky oddělenými redundantními datovými centry s plnou datovou a infrastrukturní redundancí.
5	Posílit datovou integraci přes integrační platformu	Všechny významné datové a transformační vazby na MMB (vnitromagistrátní informační systémy) jsou realizovány přes integrační platformu.

3.2.2. Cíle v perspektivě procesů

číslo	strategický cíl	popis
6	Podpořit technologiemi workflow pro elektronicky poskytovatelné služby	Portál má zavedeny pokročilé workflow technologie (nastavování procesů) umožňující poskytovat elektronické služby.
7	Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby	Standardy zajišťují neustálou bezpečnost (důvěrnost, integritu a dostupnost) a důvěryhodnost elektronicky poskytovatelných služeb.
8	Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce v cloudu	Katalog ICT služeb umožňuje využívat infrastrukturní, platformové a bezpečnostní služby cloudu jednotným způsobem, a to pro SMB a zřizované organizace města.
9	Architektonicky řídit ICT města a vytvořit městské ICT standardy	Řízení EA (Enterprice Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy. Architektura podporuje vzdálený bezpečný přístup do systémů.
10	Poskytovat z informačních systémů data klasifikovaná jako veřejná	Otevřená data jsou zveřejňována ve standardních otevřených formátech dle MV ČR v souladu s jejich klasifikací prostřednictvím integrační platformy.

3.2.3. Cíle v perspektivě zákazníků

číslo	strategický cíl	popis
11	Poskytovat elektr. služby přes internetovou přepážku v uživatelsky intuitivní a jednotné podobě	Zvolené životní situace jsou poskytovány elektronicky (na základě vyhodnocení pilotního procesu). Možnost sledování průběhu procesu vyřizování životní situace občanem. Zrychlení průběhu procesů. Zvýšení kontextové informovanosti o procesu (kroky proběhlé a příští) a jeho transparentnosti.
12	Podporovat využívání cloudových služeb městskými firmami	Městské cloudové služby (zálohování, úložiště, bezpečnost) jsou poskytovány za výhodných ekonomických podmínek z pozice jednotlivých městských firem obtížně dosažitelných a na profesionální úrovni.
13	Rozšířit využívání aplikací v městském cloudu podle závazných standardů	Městský cloud bude ve shodě s eGC ČR a město bude mít zavedeny standardy pro oblast informatiky v souladu s požadavky e-governmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...).
14	Posilovat důvěru ve sdílení dat a propagovat otevřená data a jejich využití	Poskytovaná otevřená data jsou zabezpečena, tj. zejména je zaručenost jejich důvěryhodnost ve smyslu jejich pravosti (znalost zdroje) a jejich integrity (nejsou neautorizovaně modifikována nežádoucím způsobem). Příprava poskytování otevřených dat z informačních systémů města, jeho MČ a společností.

3.2.4. Cíle v perspektivě ICT přínosů

číslo	strategický cíl	popis
15	Elektronizace služeb veřejné správy (elektronická radnice)	Je vytvořena technologická platforma s uživatelsky přívětivým rozhraním pro elektronickou formu komunikace a participace občanů s úředníky.
16	Vytvořit moderní, společné a bezpečné ICT města	Město disponuje moderní modulární a stále se rozvíjející ICT infrastrukturou, která je sdílena v rámci MMB, MČ a městských firem. Infrastruktura poskytuje maximálně efektivní elektronické služby a její bezpečnost je zajištěna na profesionální úrovni.
17	Otevření městských dat veřejnosti	Veřejnost má přístup k dobře interpretovatelným otevřeným datům, čímž se zvyšuje transparentnost radnice a zájem občanů o spolupráci s ní.

3.3. Provázání strategických cílů do systému

Strategické cíle nejsou navzájem oddělené a na sobě nezávislé, ale jsou vzájemně propojeny a navzájem se ovlivňují. Vztahy příčin a následků mezi strategickými cíli odrážejí logičnost strategických úvah. Implicitní předpoklady nabývají na základě strategických vztahů příčin a následků explicitní podobu. Úspěch strategie závisí na společném působení všech strategických cílů v rámci jednoho vzájemně provázaného a uceleného systému.

Strategické cíle jsou vzájemně provázané a vytvářejí strategické řetězce, které ukazují na příčinu a následek v systému strategických cílů. Kauzální řetězce příčin a následků jednotlivých strategických cílů ukazují souvislosti a závislosti mezi strategickými cíli. Vazby mezi cíli ukazují, jak musí jednotlivé oblasti spolupůsobit, aby bylo možné realizovat strategii jako celek. Ukazují na vstupní cíle a na vrcholové cíle, k jejichž dosažení musí být předchozí cíle rovněž naplněny.

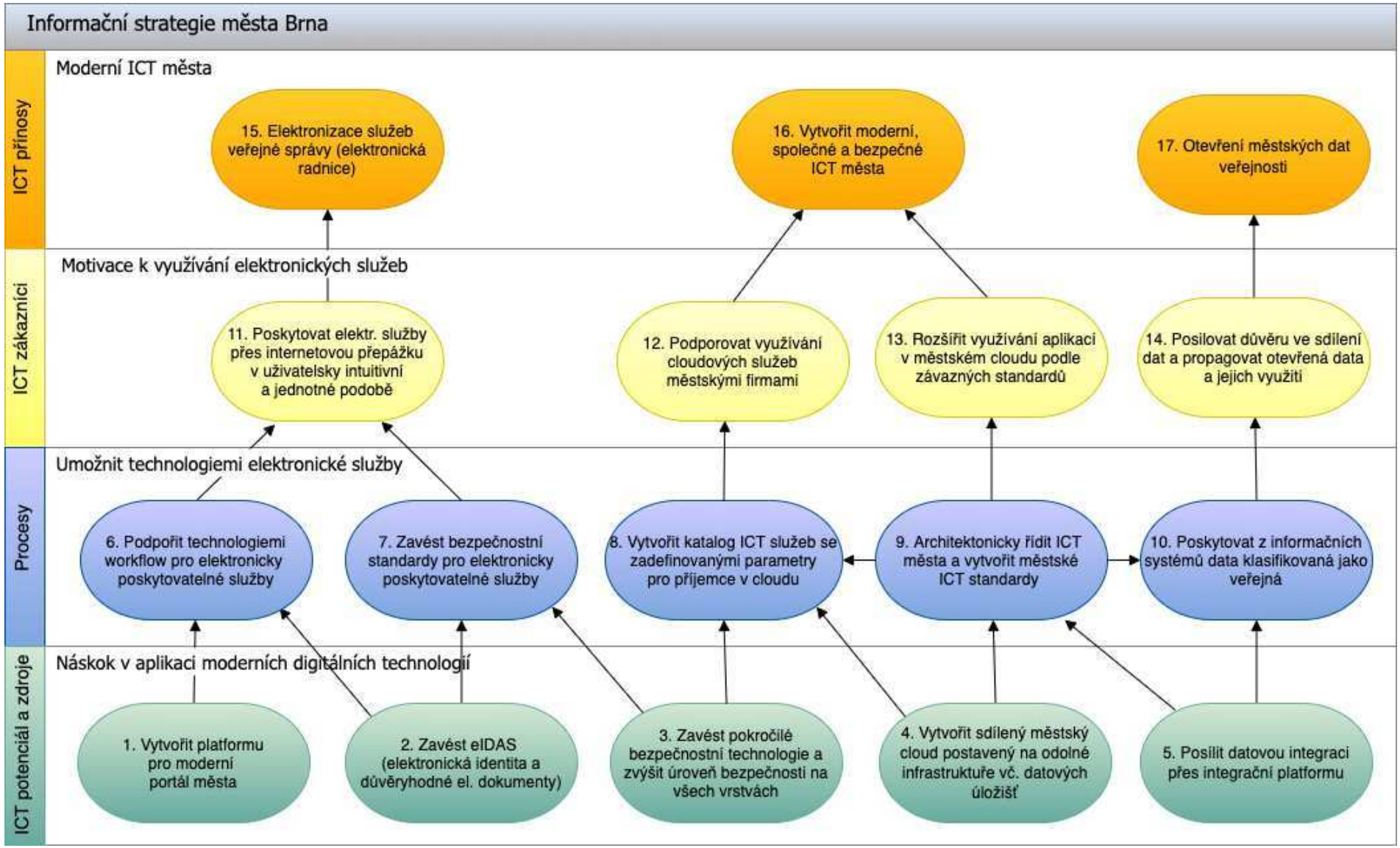
Ve strategické mapě (schéma Balanced Scorecard) jsou kauzální vazby znázorněny šipkami, kdy ve směru šipky je uvažován vztah příčina vyvolávající následek. Zaměření na strategicky významné vztahy, bez ambice na analýzu všech myslitelných vazeb mezi cíli, je jednou z hlavních předností použité metody Balanced Scorecard.

Strategická mapa (schéma Balanced Scorecard) uvedená na následující straně představuje souhrnné znázornění systému strategických cílů a jejich kauzálních vazeb. Obsahuje:

- 3 cíle v perspektivě ICT přínosy;
- 4 cíle v perspektivě ICT zákazníci;
- 5 cílů v perspektivě Procesy;
- 5 cílů v perspektivě ICT potenciál a zdroje.

Mapa integruje systém strategických cílů do jednoho schématu a ukazuje na podmíněnost cílů zařazených do jednotlivých perspektiv.

3.3.1. Strategická mapa (schéma Balanced Scorecard)



Informační strategie města Brna je postavena na základně perspektivy *ICT potenciál a zdroje*. Strategickým záměrem cílů v této perspektivě je umožnit dosažení cílů v navazujících perspektivách, zejména v perspektivě *Procesy*. Nebude-li dosaženo cílů v perspektivě *ICT potenciál a zdroje*, bude nemožné dosáhnout cílů v perspektivě *Procesy*.

Strategické cíle v perspektivě *Procesy* mají podmiňující charakter pro cíle v perspektivě *ICT zákazníci*. Dosažení cílů, díky jimž uživatelé informačního systému města Brna získají nové hodnoty oproti stávajícímu stavu, není možné bez zvládnutých procesů v oblastech zdůrazněných strategickými cíli této perspektivy.

Logika strategie vychází z toho, že dosažení strategických cílů pro zákazníka, tj. uživatele informačního systému a další zainteresované strany, se odrazí v přínosech pro město Brno. Proto je ve strategii perspektiva *ICT přínosy* podmíněna dosažením cílů perspektivy *ICT zákazníci*. Přínosy jsou v informační strategii očekávány v těchto oblastech:

- Elektronizace služeb veřejné správy (elektronická radnice);
- Vytvořit moderní, společné a bezpečné ICT města;
- Otevření městských dat veřejnosti.

Zaměření strategie na dosažení koncového efektu jako nosného přínosu její realizace je formulováno pomocí trojice strategických cílů uskupených v perspektivě *ICT přínosy*. Ostatní cíle jsou směrovány k dosažení cílů této perspektivy, jak je zřejmé ze strategické mapy.

Ve strategické mapě jsou čitelné dominantní řetězce kauzálně souvisejících cílů. Byly identifikovány tři dominantní strategické řetězce:

- Řetězec elektronizace služeb;
- Řetězec ICT města;
- Řetězec otevřenosti dat.

Řetězec elektronizace služeb

Strategický řetězec **elektronizace služeb** je uskupen kolem sedmi cílů vertikálně směřujících k dosažení podpory elektronické komunikace s občany a systémy veřejné správy:

1. *Vytvořit platformu pro moderní portál města;*
2. *Zavést eIDAS (elektronická identita a důvěryhodné el. dokumenty);*
3. *Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách;*
6. *Podpořit technologiemi workflow pro elektronicky poskytovatelné služby;*
7. *Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby;*
11. *Poskytovat elektr. služby přes internetovou přepážku v uživatelsky intuitivní a jednotné podobě;*
15. *Elektronizace služeb veřejné správy (elektronická radnice).*

Jedná se o skupinu cílů směřující ke zvýšení transparentnosti a otevřenosti radnice a k elektronizaci služeb veřejné správy. Strategie vychází z toho, že dosažení těchto vrcholových přínosů je třeba postavit od základů vzniklých z vytvoření moderního portálu města. Pro to, aby bylo dosaženo elektronická komunikace a participace občanů s úředníky, je třeba zajistit důvěryhodnost elektronických služeb poskytovaných Úřadem, bezpečný přístup občanů k dokumentům zprostředkovaných portálem a poskytovat elektronické služby v předem známých na sebe navazujících krocích (workflow) v souladu s bezpečnostními standardy zajišťujícími důvěrnost, integritu a dostupnost elektronicky poskytovaných služeb. Tím bude občanům umožněno vyřizovat své životní situace elektronicky přes internetovou přepážku v uživatelsky

intuitivní a jednotné podobě. Konečným důsledkem realizace těchto postupových cílů je elektronizace služeb veřejné správy.

Řetězec ICT města

Strategický řetězec **ICT města** kauzálně propojuje osm cílů směřujících k dosažení moderní ICT infrastruktury sdílené v rámci MMB, MČ a městskými firmami:

3. Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách;
4. Vytvořit sdílený městský cloud postavený na odolné infrastruktuře vč. datových úložišť;
5. Posílit datovou integraci přes integrační platformu;
8. Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce v cloudu;
9. Architektonicky řídit ICT města a vytvořit městské ICT standardy;
12. Podporovat využívání cloudových služeb městskými firmami;
13. Rozšířit využívání aplikací v městském cloudu podle závazných standardů;
16. Vytvořit moderní, společné a bezpečné ICT města.

ICT infrastruktura města je základním předpokladem pro poskytování elektronických služeb. Aby mohla úspěšně plnit svou roli, musí být dostatečně bezpečná, odolná proti výpadkům a schopná poskytovat požadovaná data. Jednotnost využívání služeb ICT města je dána službami popsanými v katalogu služeb poskytovaných ICT infrastrukturou, které vycházejí z možností centrálně řízené architektury systémů a zohledňují městské ICT standardy. Tím je umožněno městským firmám využívat za výhodných ekonomických podmínek cloudové služby v souladu s požadavky e-govermentu ČR. Vrcholovým cílem tohoto řetězce je dosažení modulární ICT infrastruktury, která poskytuje maximálně efektivní elektronické služby s bezpečností zajištěnou na profesionální úrovni.

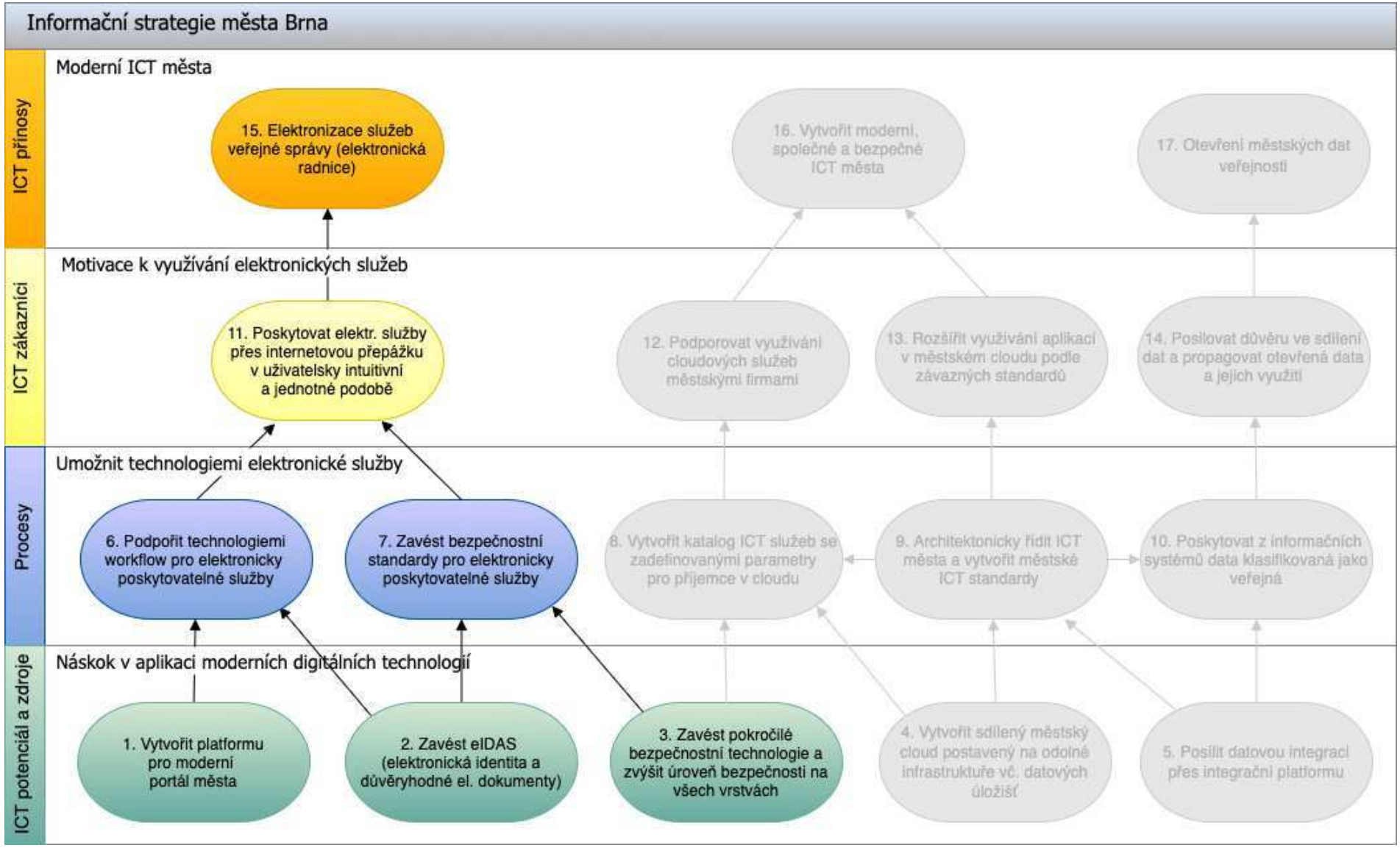
Řetězec otevřenosti dat

Strategický řetězec **otevřenosti dat** kauzálně propojuje šest cílů směřujících k otevření městských dat veřejnosti:

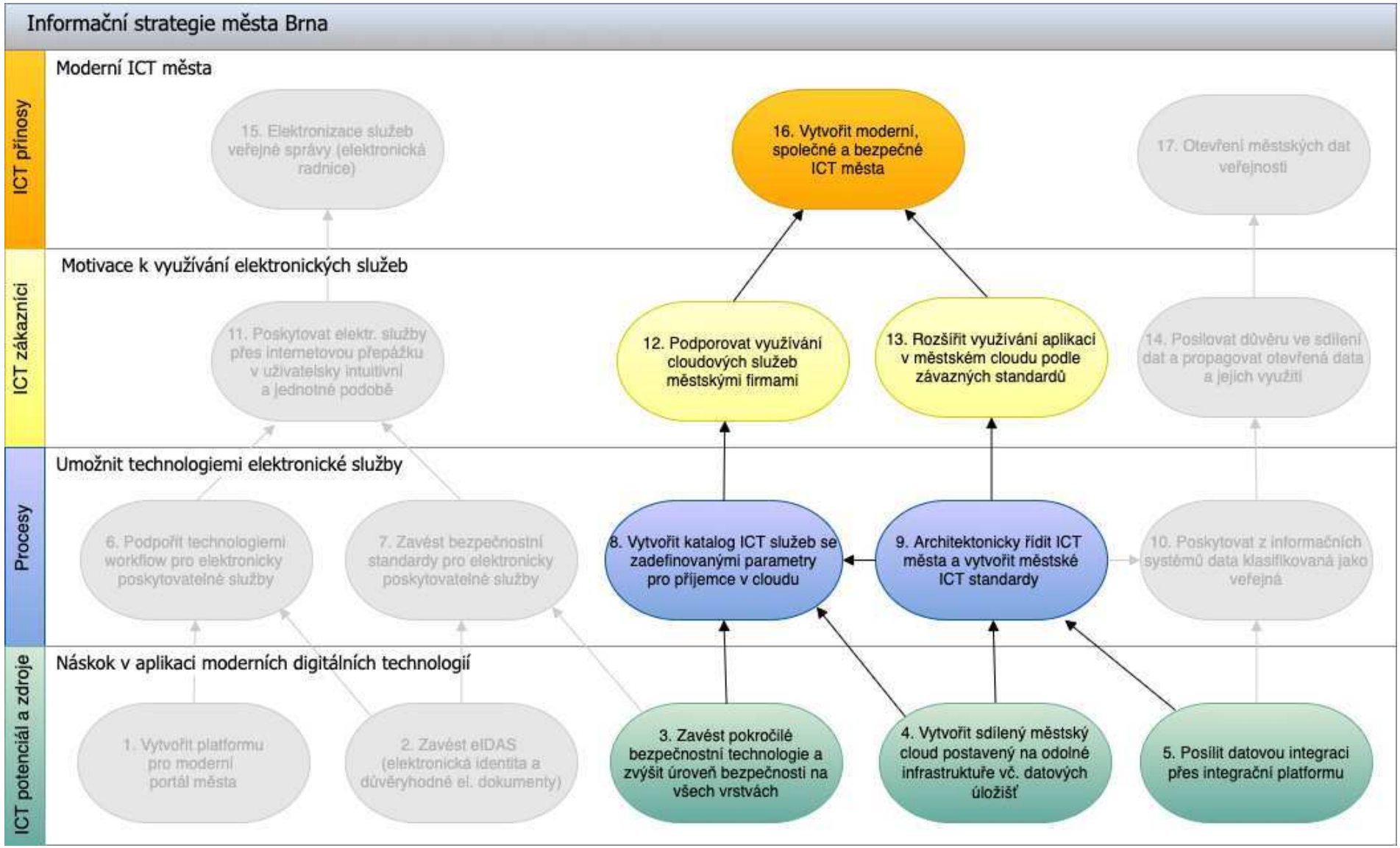
4. Vytvořit sdílený městský cloud postavený na odolné infrastruktuře vč. datových úložišť;
5. Posílit datovou integraci přes integrační platformu;
9. Architektonicky řídit ICT města a vytvořit městské ICT standardy;
10. Poskytovat z informačních systémů data klasifikovaná jako veřejná;
14. Posilovat důvěru ve sdílení dat a propagovat otevřená data a jejich využití;
17. Otevření městských dat veřejnosti.

Poskytování otevřených dat je založeno na městském cloudu s datovými centry s redundantně uloženými daty. Začlenění systémů do celku je architektonicky řízeno, přičemž otevřená data jsou na základě jejich klasifikace zveřejňována prostřednictvím integrační platformy. Otevřená data jsou zabezpečena (je zaručena jejich důvěryhodnost a integrita) a zpřístupněna veřejnosti.

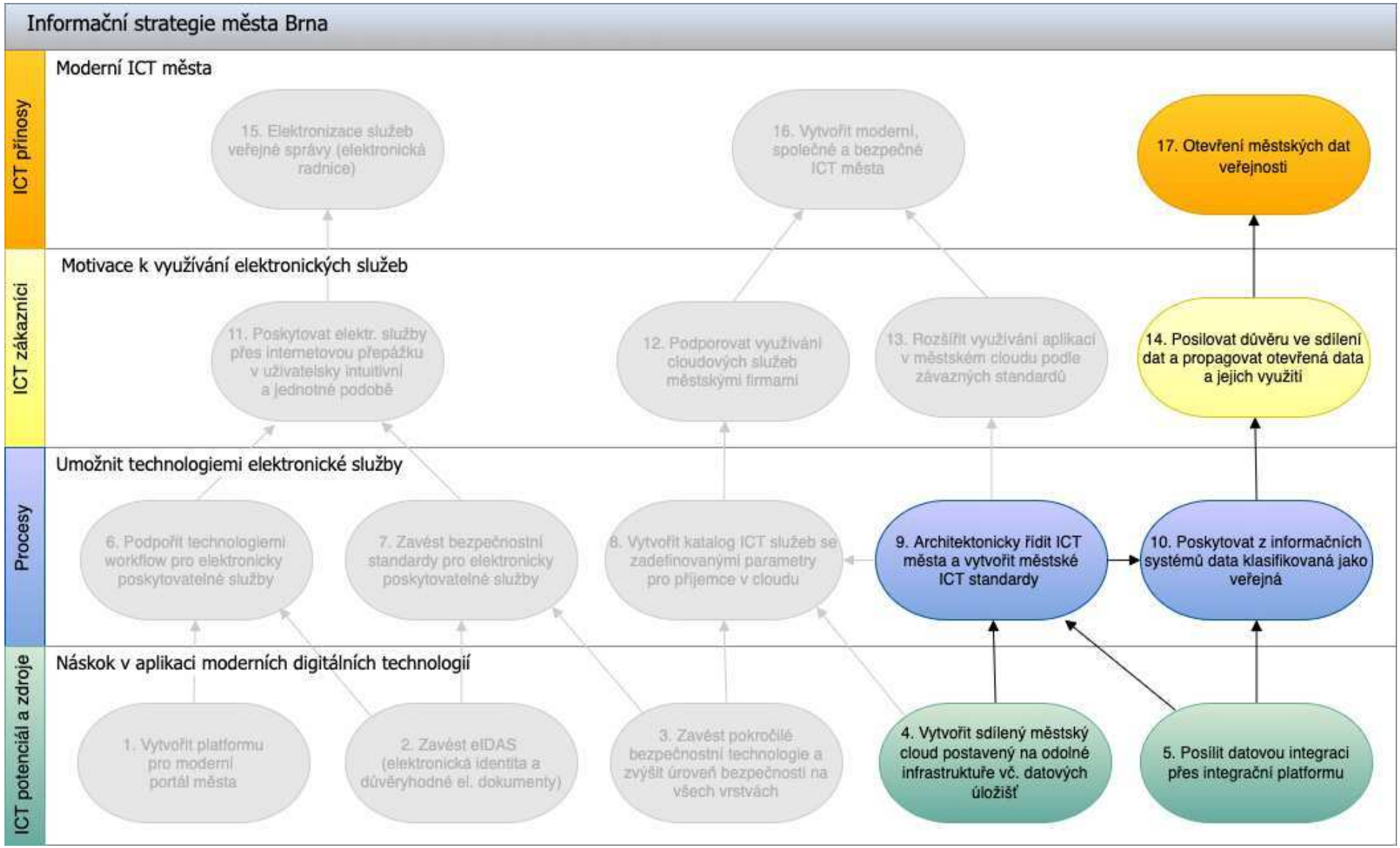
3.3.2. Řetězec elektronizace služeb



3.3.3. Řetězec ICT města



3.3.4. Řetězec otevřenosti dat



4. Plán implementace strategie

Metoda Balanced Scorecard dává rámec pro vytvoření systému cílů a jejich implementaci jako balancovaného celku. Identifikovaná příčina a následek mezi cíli umožňuje naplánovat, jak se vzájemně ovlivňují stanovené cíle a jak postupovat při realizaci portfolia strategických projektů. Jednotlivé strategické projekty naplňují strategické cíle a v souladu s tím, jak jsou vzájemně provázány strategické cíle, jsou provázány rovněž strategické projekty směřující k jejich dosažení. Úspěšné naplňování strategie je tedy přímo závislé na úspěšné realizaci strategických projektů.

4.1. Měřítka (metriky) plnění cílů

Pro každý strategický cíl uvedený ve strategické mapě bylo stanoveno:

- měřítko realizace;
- cílové hodnoty pro roky 2021, 2022, 2023 a 2024.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
1	Vytvořit platformu pro moderní portál města	Technologie portálu	2021 2022	Zvolena technologie portálu a provedena pilotní implementace v části informačního portálu (www.brno.cz). Autentizační brána Brno ID pro občany integrována s NIA v rámci portálu města. Integrovány workflow technologie do portálu. Jsou implementovány technologie pro centrální technologické řešení portálu města. Součástí portálu města Brna je řešení jeho kybernetické bezpečnosti.
2	Zavést eIDAS (elektronická identita a důvěryhodné el. dokumenty)	Shoda s eIDAS	2021 2022	Dokončena autentizační brána pro vnitřní IDM města (SMB). Integrace systémů v rozsahu SŘBI. Pilotně zavedeny technologie pro důvěryhodný oběh dokumentů. Federování identit s městskými organizacemi. Ověřeny a poskytovány technologie pro důvěryhodný oběh dokumentů. Plné zajištění shody s požadavky eIDAS umožňující poskytovat důvěryhodné elektronické služby Úřadu.
3	Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách	Služby SOC	2021 2022 2023 2024	Naimplementován centrální LOG management. Spuštěny služby SOC pro systémy začleněné do centrálního LOG managementu. Naimplementován systém PIM/PAM. Integrace velkých městských organizací do SOC. Provozování městského dohledového provozního a bezpečnostního centra SOC integrujícího všechny bezpečnostní technologie.
4	Vytvořit sdílený městský cloud postavený na odolné infrastruktuře vč. datových úložišť	Plná datová a infrastrukturní redundance	2021 2022	Uvedení do plného provozu redundantní DC včetně redundantních datových linek napojených na SMB. Poskytování alternativního internetového připojení pro SMB a jeho organizace. Poskytování zabezpečeného vzdáleného přístupu do SMB infrastruktury organizacím SMB. Zahájení poskytování služeb ve formě MSSP (managed security service provider). Rozšiřování služeb městského cloudu o služby pro eIDAS.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
5	Posílit datovou integraci přes integrační platformu	Datové a integrační vazby MMB přes integrační platformu	2021 2022 2023 2024	Definován a nastaven Service Bus integrační platformy. Spisová služba a GIS komunikuje přes integrační platformu. Využití Service Bus pro elektronické služby městského portálu občana. Integrace dílčích agendových systémů podle posouzení jejich priorit. Všechny významné datové a transformační vazby na MMB jsou realizovány přes integrační platformu.
6	Podpořit technologiemi workflow pro elektronicky poskytovatelné služby	Zavedeno workflow na portálu	2021 2022 2023	Odzkoušení technologií workflow nad portálem. Vytvoření studie proveditelnosti pro využívání workflow. Do portálu naimplementovány základní komponenty identifikované v rámci studie proveditelnosti. Implementace doplňkových komponent. Portál má zavedeny pokročilé workflow technologie (nastavování procesů) umožňující poskytovat elektronické služby.
7	Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby	Bezpečnostní standardy zavedeny	2021 2022 2023	Standard připojování MČ a městských organizací do LOG managementu. Závazné bezpečnostní standardy pro MČ. Standardy pro přidělování oprávnění / přístupů do PIM/PAM. Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro MČ, městské akciové a příspěvkové organizace s vazbou na SOC. Standardy zajišťují neustálou bezpečnost (důvěrnost, integritu a dostupnost) a důvěryhodnost elektronicky poskytovatelných služeb.
8	Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce v cloudu	Katalog ICT služeb vytvořen	2021 2022 2023	Vytvoření pilotního katalogu ICT služeb. Registrace služeb městského cloudu v eGC (egovernment cloud). Katalog ICT služeb je dokončen a rozšířen o služby pro eIDAS. Katalog ICT služeb umožňuje využívat infrastrukturní, platformové a bezpečnostní služby cloudu jednotným způsobem, a to pro SMB a zřizované organizace města (městské firmy).

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
9	Architektonicky řídit ICT města a vytvořit městské ICT standardy	EA aplikována v SMB a zřizovaných organizacích města	2021 2022 2023 2024	Stanoveny základní architektonické principy ICT města. Vytvořena směrnice a pracovní postup pro zadávání architektonických prvků do centrální evidence. Vytvořené ICT standardy vycházející z Metodiky pro evidenci služeb veřejné správy. Vytvořené KB standardy vycházející z doporučení daných zákonem o kybernetické bezpečnosti. Vytvořena směrnice a pracovní postup pro zpracování projektových záměrů. Vytvořena směrnice a pracovní postup pro integraci dílčích agendových systémů. Centrální evidence obsahuje aktuální stav všech významných architektonických prvků MMB. U všech nových ICT projektů je zpracován projektový záměr tak, aby splňoval architektonické principy. Požadavky z ICT projektů s dopadem na architekturu jsou evidovány, analyzovány a schvalovány architektonickou komisí města pro ICT. Systémy centrálně poskytované v rámci SMB jsou zavedeny v centrální evidenci. Řízení metodami EA (Enterprice Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy.
10	Poskytovat z informačních systémů data klasifikovaná jako veřejná	Zveřejňování otevřených dat umožněno přes městský portál	2021 2022 2023	Data jsou klasifikována. Otevřená data jsou zpřístupněna přes elektronické služby městského portálu prostřednictvím integrační platformy (Service Bus). Otevřená data jsou zveřejňována ve standardních otevřených formátech dle MV ČR v souladu s jejich klasifikací. Jsou zpřístupněna otevřená data z agendových systémů napojených na integrační platformu.
11	Poskytovat elektr. služby přes internetovou přepážku v uživatelsky intuitivní a jednotné podobě	Životní situace řešeny elektronicky přes portál města	2021 2022 2023 2024	Pilotní prověření vyřizování životní situace platby poplatků v GINIS (proof of concept). Pilotní prověření vyřizování vybrané životní situace na portálu města. Nasazení služeb pro vyřizování zvolených životních situací na portál města. Možnost sledování průběhu procesu vyřizování životní situace občanem. Zvýšení kontextové informovanosti o procesu (kroky proběhlé a příští) a jeho transparentnosti.
12	Podporovat využívání cloudových služeb městskými firmami	Městské cloudové služby využívány městskými firmami	2021 2022 2023 2024	Na městském cloudu jsou poskytovány vybrané služby KB (kybernetické bezpečnosti). Městské cloudové služby (zálohování, úložiště, bezpečnost) jsou poskytovány za výhodných ekonomických podmínek z pozice jednotlivých městských firem obtížně dosažitelných a na profesionální úrovni. Portál umožňuje objednávání služeb městského cloudu. Přístup ke službám městského cloudu je zajištěn pro všechny organizace SMB.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
13	Rozšířit využívání aplikací v městském cloudu podle závazných standardů	Městský cloud standardizován	2021 2022 2023 2024	Vytvořen standard týkající se bezpečnosti technických aktiv. Aktualizace provozních řádů centrálních informačních systémů. Navržena struktura technologického standardu (jako základní technologický rámec s možností jeho využití ve výběrových řízeních) s vazbou na architektonické principy. Propojení architektonického řízení s konfiguračním managementem (GPC databáze). Naplnění struktury technologického standardu v prioritních částech. Úplné dokončení technologického standardu. Městský cloud je ve shodě s eGC ČR a jsou zavedeny standardy pro oblast informatiky v souladu s požadavky e-governmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...).
14	Posilovat důvěru ve sdílení dat a propagovat otevřená data a jejich využití	Otevřená data certifikována	2021 2022 2023	 Všechna otevřená data poskytovaná elektronicky přes městský portál jsou zabezpečena a nesou informaci o jejich důvěryhodnosti, tj. zejména je zaručena jejich důvěryhodnost ve smyslu jejich pravosti (znalost zdroje) a jejich integrity (nejsou neautorizovaně modifikována nežádoucím způsobem). Je podporováno využití otevřených dat z agendových systémů přístupných v reálném čase.
15	Elektronizace služeb veřejné správy (elektronická radnice)	Očekávané přínosy z elektronizace služeb dosaženy	2021 2022 2024	Vytvořena koncepce portálu města s očekávanými přínosy zejména z pohledu elektronizace radnice. Rozpracován způsob začlenění životních situací do portálu města a zvolena životní situace pro pilotní ověření. Vyhodnoceny přínosy z pilotního ověření vybrané životní situace poskytované přes portál města se stanovením začlenění dalších životních situací do portálu. Vyhodnoceny přínosy z životních situací poskytovaných přes portál. Město disponuje elektronicky poskytovanými službami pro všechny zvolené životní situace.
16	Vytvořit moderní, společné a bezpečné ICT města	ICT města sdíleno	2021 2022 2023 2024	Technická aktiva v cloudu mají stanoveny požadavky na zajištění kybernetické bezpečnosti. Technická aktiva MMB jsou v souladu s technologickými standardy. Městská ICT infrastruktura je v souladu s technologickými ICT standardy a KB standardy. Město disponuje moderní modulární a stále se rozvíjející ICT infrastrukturou, která je sdílena v rámci MMB, MČ a městských organizací. Infrastruktura poskytuje maximálně efektivní elektronické služby a její bezpečnost je zajištěna na profesionální úrovni.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
17	Otevření městských dat veřejnosti	Přístup veřejnosti k datům umožněn	2021 2022 2023 2024	Pilotní zveřejňování otevřených dat ze systému GINIS. Zahájení procesu zveřejňování otevřených dat z agendových systémů MMB. Všechna otevřená data poskytovaná z MMB přes portál města jsou poskytována automatizovaně, u MČ a městských organizací v maximální dosažitelné míře. Veřejnost má přístup k dobře interpretovatelným otevřeným datům, čímž se zvyšuje transparentnost radnice a zájem občanů o spolupráci s ní.

4.2. Strategické projekty

Na pokrytí 17 strategických cílů byly navrženy následující strategické projekty:

1.	POR	Portál města Brna
2.	WT	Workflow technologie
3.	ESL	Elektronické služby
4.	eIDAS	eIDAS
5.	BST	Bezpečnostní standardy
6.	SOC	Městské dohledové provozní a bezpečnostní centrum
7.	MC	Městský cloud
8.	APPMC	Aplikace v cloudu
9.	ARCH	Architektonické řízení městské informatiky
10.	OD	Otevřená data
11.	INT	Integrační platforma

U každého projektu jsou uvedeny naplánované dílčí projektové cíle, které jsou odvozeny z postupových hodnot strategických cílů zahrnutých do projektu. Složitější projektové cíle může být vhodné realizovat jako podprojekty, zejména pokud budou realizovány dodavatelsky.

4.2.1. Portál města Brna

Účel projektu:

Přínosový cíl 15. *Elektronizace služeb veřejné správy (elektronická radnice)*.

Cíle projektu:

1	Technologie portálu	2021 2022	Zvolena technologie portálu a provedena pilotní implementace v části informačního portálu (www.brno.cz). Autentizační brána Brno ID pro občany integrována s NIA v rámci portálu města. Integrovány workflow technologie do portálu. Jsou implementovány technologie pro centrální technologické řešení portálu města. Součástí portálu města Brna je řešení jeho kybernetické bezpečnosti.

4.2.2. Workflow technologie

Účel projektu:

Přínosový cíl 15. *Elektronizace služeb veřejné správy (elektronická radnice)*.

Cíle projektu:

6	Podpořit technologiemi workflow pro elektronicky poskytovatelné služby	2021 2022 2023	Odzkoušení technologií workflow nad portálem. Vytvoření studie proveditelnosti pro využívání workflow. Do portálu naimplementovány základní komponenty identifikované v rámci studie proveditelnosti. Implementace doplňkových komponent. Portál má zavedeny pokročilé workflow technologie (nastavování procesů) umožňující poskytovat elektronické služby.

4.2.3. Elektronické služby

Účel projektu:

Přínosový cíl 15. *Elektronizace služeb veřejné správy (elektronická radnice)*.

Cíle projektu:

11	Životní situace řešeny elektronicky přes portál města	2021 2022 2023 2024	Pilotní prověření vyřizování životní situace platby poplatků v GINIS (proof of concept). Pilotní prověření vyřizování vybrané životní situace na portálu města. Nasazení služeb pro vyřizování zvolených životních situací na portál města. Možnost sledování průběhu procesu vyřizování životní situace občanem. Zvýšení kontextové informovanosti o procesu (kroky proběhlé a příští) a jeho transparentnosti.
15	Očekávané přínosy z elektronizace služeb dosaženy	2021 2022 2024	Vytvořena koncepce portálu města s očekávanými přínosy zejména z pohledu elektronizace radnice. Rozpracován způsob začlenění životních situací do portálu města a zvolena životní situace pro pilotní ověření. Vyhodnoceny přínosy z pilotního ověření vybrané životní situace poskytované přes portál města se stanovením začlenění dalších životních situací do portálu. Vyhodnoceny přínosy z životních situací poskytovaných přes portál. Město disponuje elektronicky poskytovanými službami pro všechny zvolené životní situace.

4.2.4. eIDAS

Účel projektu:

Přínosový cíl 15. *Elektronizace služeb veřejné správy (elektronická radnice)*.

Cíle projektu:

2	Shoda s eIDAS	2021 2022	Dokončena autentizační brána pro vnitřní IDM města (SMB). Integrace systémů v rozsahu SŘBI. Pilotně zavedeny technologie pro důvěryhodný oběh dokumentů. Federování identit s městskými organizacemi. Ověřeny a poskytovány technologie pro důvěryhodný oběh dokumentů. Plné zajištění shody s požadavky eIDAS umožňující poskytovat důvěryhodné elektronické služby Úřadu.

4.2.5. Bezpečnostní standardy

Účel projektu:

Přínosový cíl 15. *Elektronizace služeb veřejné správy (elektronická radnice)*.
Přínosový cíl 16. *Vytvořit moderní, společné a bezpečné ICT města*.

Cíle projektu:

7	Bezpečnostní standardy zavedeny	2021 2022 2023	Standard připojování MČ a městských organizací do LOG managementu. Závazné bezpečnostní standardy pro MČ. Standardy pro přidělování oprávnění / přístupů do PIM/PAM. Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro MČ, městské akciové a příspěvkové organizace s vazbou na SOC. Standardy zajišťují neustálou bezpečnost (důvěrnost, integritu a dostupnost) a důvěryhodnost elektronicky poskytovatelných služeb.

4.2.6. Městské dohledové provozní a bezpečnostní centrum

Účel projektu:

Přínosový cíl 16. *Vytvořit moderní, společné a bezpečné ICT města*.

Cíle projektu:

3	Služby SOC	2021 2022 2023 2024	Naimplementován centrální LOG management. Spuštěny služby SOC pro systémy začleněné do centrálního LOG managementu. Naimplementován systém PIM/PAM. Integrace velkých městských organizací do SOC. Provozování městského dohledového provozního a bezpečnostního centra SOC integrujícího všechny bezpečnostní technologie.

4.2.7. Městský cloud

Účel projektu:

Přínosový cíl 16. *Vytvořit moderní, společné a bezpečné ICT města*.

Cíle projektu:

4	Plná datová a infrastrukturní redundance	2021 2022	Uvedení do plného provozu redundantní DC včetně redundantních datových linek napojených na SMB. Poskytování alternativního internetového připojení pro SMB a jeho organizace. Poskytování zabezpečeného vzdáleného přístupu do SMB infrastruktury organizacím SMB. Zahájení poskytování služeb ve formě MSSP (managed security service provider). Rozšiřování služeb městského cloudu o služby pro eIDAS.
8	Katalog ICT služeb vytvořen	2021 2022 2023	Vytvoření pilotního katalogu ICT služeb. Registrace služeb městského cloudu v eGC (egovernment cloud). Katalog ICT služeb je dokončen a rozšířen o služby pro eIDAS. Katalog ICT služeb umožňuje využívat infrastrukturní, platformové a bezpečnostní služby cloudu jednotným způsobem, a to pro SMB a zřizované organizace města (městské firmy).

12	Městské cloudové služby využívány městskými firmami	2021 2022 2023 2024	Na městském cloudu jsou poskytovány vybrané služby KB (kybernetické bezpečnosti). Městské cloudové služby (zálohování, úložiště, bezpečnost) jsou poskytovány za výhodných ekonomických podmínek z pozice jednotlivých městských firem obtížně dosažitelných a na profesionální úrovni. Portál umožňuje objednávání služeb městského cloudu. Přístup ke službám městského cloudu je zajištěn pro všechny organizace SMB.

4.2.8. Aplikace v cloudu

Účel projektu:

Přínosový cíl 16. *Vytvořit moderní, společné a bezpečné ICT města*.

Cíle projektu:

13	Městský cloud standardizován	2021 2022 2023 2024	Vytvořen standard týkající se bezpečnosti technických aktiv. Aktualizace provozních řádů centrálních informačních systémů. Navržena struktura technologického standardu (jako základní technologický rámec s možností jeho využití ve výběrových řízeních) s vazbou na architektonické principy. Propojení architektonického řízení s konfiguračním managementem (GPC databáze). Naplnění struktury technologického standardu v prioritních částech. Úplné dokončení technologického standardu. Městský cloud je ve shodě s eGC ČR a jsou zavedeny standardy pro oblast informatiky v souladu s požadavky e-govermentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...).
16	ICT města sdíleno	2021 2022 2023 2024	Technická aktiva v cloudu mají stanoveny požadavky na zajištění kybernetické bezpečnosti. Technická aktiva MMB jsou v souladu s technologickými standardy. Městská ICT infrastruktura je v souladu s technologickými ICT standardy a KB standardy. Město disponuje moderní modulární a stále se rozvíjející ICT infrastrukturou, která je sdílena v rámci MMB, MČ a městských organizací. Infrastruktura poskytuje maximálně efektivní elektronické služby a její bezpečnost je zajištěna na profesionální úrovni.

4.2.9. Architektonické řízení městské informatiky

Účel projektu:

Přínosový cíl 16. *Vytvořit moderní, společné a bezpečné ICT města*.

Cíle projektu:

9	EA aplikována v SMB a zřizovaných organizacích města	2021 2022 2023 2024	Stanoveny základní architektonické principy ICT města. Vytvořena směrnice a pracovní postup pro zadávání architektonických prvků do centrální evidence. Vytvořené ICT standardy vycházející z Metodiky pro evidenci služeb veřejné správy. Vytvořené KB standardy vycházející z doporučení daných zákonem o kybernetické bezpečnosti. Vytvořena směrnice a pracovní postup pro zpracování projektových záměrů. Vytvořena směrnice a pracovní postup pro integraci dílčích agendových systémů. Centrální evidence obsahuje aktuální stav všech významných architektonických prvků MMB. U všech nových ICT projektů je zpracován projektový záměr tak, aby splňoval architektonické principy. Požadavky z ICT projektů s dopadem na architekturu jsou evidovány, analyzovány a schvalovány architektonickou komisí města pro ICT. Systémy centrálně poskytované v rámci SMB jsou zavedeny v centrální evidenci. Řízení metodami EA (Enterprice Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy.
13	Městský cloud standardizován	2021 2022 2023 2024	Vytvořen standard týkající se bezpečnosti technických aktiv. Aktualizace provozních řádů centrálních informačních systémů. Navržena struktura technologického standardu (jako základní technologický rámec s možností jeho využití ve výběrových řízeních) s vazbou na architektonické principy. Propojení architektonického řízení s konfiguračním managementem (GPC databáze). Naplnění struktury technologického standardu v prioritních částech. Úplné dokončení technologického standardu. Městský cloud je ve shodě s eGC ČR a jsou zavedeny standardy pro oblast informatiky v souladu s požadavky e-govermentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...).

4.2.10. Otevřená data

Účel projektu:

Přínosový cíl 17. *Otevření městských dat veřejnosti*.

Cíle projektu:

10	Zveřejňování otevřených dat umožněno přes městský portál	2021 2022 2023	Data jsou klasifikována. Otevřená data jsou zpřístupněna přes elektronické služby městského portálu prostřednictvím integrační platformy (Service Bus). Otevřená data jsou zveřejňována ve standardních otevřených formátech dle MV ČR v souladu s jejich klasifikací. Jsou zpřístupněna otevřená data z agendových systémů napojených na integrační platformu.

14	Otevřená data certifikována	2021 2022 2023	Všechna otevřená data poskytovaná elektronicky přes městský portál jsou zabezpečena a nesou informaci o jejich důvěryhodnosti, tj. zejména je zaručena jejich důvěryhodnost ve smyslu jejich pravosti (znalost zdroje) a jejich integrity (nejsou neautorizovaně modifikována nežádoucím způsobem). Je podporováno využití otevřených dat z agendových systémů přístupných v reálném čase.
17	Přístup veřejnosti k datům umožněn	2021 2022 2023 2024	Pilotní zveřejňování otevřených dat ze systému GINIS. Zahájení procesu zveřejňování otevřených dat z agendových systémů MMB. Všechna otevřená data poskytovaná z MMB přes portál města jsou poskytována automatizovaně, u MČ a městských organizací v maximální dosažitelné míře. Veřejnost má přístup k dobře interpretovatelným otevřeným datům, čímž se zvyšuje transparentnost radnice a zájem občanů o spolupráci s ní.

4.2.11. Integrační platforma

Účel projektu:

Přínosový cíl 16. *Vytvořit moderní, společné a bezpečné ICT města*.
Přínosový cíl 17. *Otevření městských dat veřejnosti*.

Cíle projektu:

5	Datové a integrační vazby MMB přes integrační platformu	2021 2022 2023 2024	Definován a nastaven Service Bus integrační platformy. Spisová služba a GIS komunikuje přes integrační platformu. Využití Service Bus pro elektronické služby městského portálu občana. Integrace dílčích agendových systémů podle posouzení jejich priorit. Všechny významné datové a transformační vazby na MMB jsou realizovány přes integrační platformu.

4.3. Harmonogram strategických projektů

Na následující straně je uveden harmonogram strategických projektů znázorňující časový postup realizace strategických cílů. Pro každý projekt jsou uvedeny číslem strategické cíle (viz kapitola 3.3.1. *Strategická mapa (schéma Balanced Scorecard)*), které naplňuje.

Strategické projekty		2021	2022	2023	2024
Cíl	**Portál města Brna**				
1	Zvolena technologie portálu a provedena pilotní implementace v části informačního portálu (www.brno.cz).				
1	Autentizační brána Brno ID pro občany integrována s NIA v rámci portálu města.				
1	Integrovány workflow technologie do portálu.				
1	Jsou implementovány technologie pro centrální technologické řešení portálu města. Součástí portálu města Brna je řešení jeho kybernetické bezpečnosti.				
Cíl	**Workflow technologie**				
6	Odzkoušení technologií workflow nad portálem. Vytvoření studie proveditelnosti pro využívání workflow.				
6	Do portálu naimplementovány základní komponenty identifikované v rámci studie proveditelnosti.				
6	Implementace doplňkových komponent.				
6	Portál má zavedeny pokročilé workflow technologie (nastavování procesů) umožňující poskytovat elektronické služby.				
Cíl	**Elektronické služby**				
11	Pilotní prověření vyřizování životní situace platby poplatků v GINIS (proof of concept).				
11	Pilotní prověření vyřizování vybrané životní situace na portálu města.				
11	Nasazení služeb pro vyřizování zvolených životních situací na portál města.				
11	Možnost sledování průběhu procesu vyřizování životní situace občanem. Zvýšení kontextové informovanosti o procesu (kroky proběhlé a příští) a jeho transparentnosti.				
15	Vytvořena koncepce portálu města s očekávanými přínosy zejména z pohledu elektronizace radnice.				
15	Rozpracován způsob začlenění životních situací do portálu města a zvolena životní situace pro pilotní ověření.				
15	Vyhodnoceny přínosy z pilotního ověření vybrané životní situace poskytované přes portál města se stanovením začlenění dalších životních situací do portálu.				
15	Vyhodnoceny přínosy z životních situací poskytovaných přes portál.				

Strategické projekty		2021	2022	2023	2024
15	Město disponuje elektronicky poskytovanými službami pro všechny zvolené životní situace.				
Cíl	**eIDAS**				
2	Dokončena autentizační brána pro vnitřní IDM města (SMB).				
2	Integrace systémů v rozsahu SŘBI.				
2	Pilotně zavedeny technologie pro důvěryhodný oběh dokumentů.				
2	Federování identit s městskými organizacemi.				
2	Ověřeny a poskytovány technologie pro důvěryhodný oběh dokumentů.				
2	Plné zajištění shody s požadavky eIDAS umožňující poskytovat důvěryhodné elektronické služby Úřadu.				
Cíl	**Bezpečnostní standardy**				
7	Standard připojování MČ a městských organizací do LOG managementu.				
7	Závazné bezpečnostní standardy pro MČ.				
7	Standardy pro přidělování oprávnění / přístupů do PIM/PAM.				
7	Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro MČ, městské akciové a příspěvkové organizace s vazbou na SOC.				
7	Standardy zajišťují neustálou bezpečnost (důvěrnost, integritu a dostupnost) a důvěryhodnost elektronicky poskytovatelných služeb.				
Cíl	**Městské dohledové provozní a bezpečnostní centrum**				
3	Naimplementován centrální LOG management.				
3	Spuštěny služby SOC pro systémy začleněné do centrálního LOG managementu.				
3	Naimplementován systém PIM/PAM.				
3	Integrace velkých městských organizací do SOC.				

Strategické projekty		2021	2022	2023	2024
3	Provozování městského dohledového provozního a bezpečnostního centra SOC integrujícího všechny bezpečnostní technologie.				
Cíl	**Městský cloud**				
4	Uvedení do plného provozu redundantní DC včetně redundantních datových linek napojených na SMB.				
4	Poskytování alternativního internetového připojení pro SMB a jeho organizace.				
4	Poskytování zabezpečeného vzdáleného přístupu do SMB infrastruktury organizacím SMB.				
4	Zahájení poskytování služeb ve formě MSSP (managed security service provider).				
4	Rozšiřování služeb městského cloudu o služby pro eIDAS.				
8	Vytvoření pilotního katalogu ICT služeb.				
8	Registrace služeb městského cloudu v eGC (egovernment cloud).				
8	Katalog ICT služeb je dokončen a rozšířen o služby pro eIDAS.				
8	Katalog ICT služeb umožňuje využívat infrastrukturní, platformové a bezpečnostní služby cloudu jednotným způsobem, a to pro SMB a zřizované organizace města (městské firmy).				
12	Na městském cloudu jsou poskytovány vybrané služby KB (kybernetické bezpečnosti).				
12	Městské cloudové služby (zálohování, úložiště, bezpečnost) jsou poskytovány za výhodných ekonomických podmínek z pozice jednotlivých městských firem obtížně dosažitelných a na profesionální úrovni.				
12	Portál umožňuje objednávání služeb městského cloudu.				
12	Přístup ke službám městského cloudu je zajištěn pro všechny organizace SMB.				
Cíl	**Aplikace v cloudu**				
13	Vytvořen standard týkající se bezpečnosti technických aktiv.				
13	Navržena struktura technologického standardu (jako základní technologický rámec s možností jeho využití ve výběrových řízeních) s vazbou na architektonické principy.				
13	Propojení architektonického řízení s konfiguračním managementem (GPC databáze).				

Strategické projekty		2021	2022	2023	2024
13	Naplnění struktury technologického standardu v prioritních částech.				
13	Úplné dokončení technologického standardu.				
13	Městský cloud je ve shodě s eGC ČR a jsou zavedeny standardy pro oblast informatiky v souladu s požadavky e-govermentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...).				
16	Technická aktiva v cloudu mají stanoveny požadavky na zajištění kybernetické bezpečnosti.				
16	Technická aktiva MMB jsou v souladu s technologickými standardy.				
16	Městská ICT infrastruktura je v souladu s technologickými ICT standardy a KB standardy.				
16	Město disponuje moderní modulární a stále se rozvíjející ICT infrastrukturou, která je sdílena v rámci MMB, MČ a městských organizací. Infrastruktura poskytuje maximálně efektivní elektronické služby a její bezpečnost je zajištěna na profesionální úrovni.				
Cíl	**Architektonické řízení městské informatiky**				
9	Stanoveny základní architektonické principy ICT města.				
9	Vytvořena směrnice a pracovní postup pro zadávání architektonických prvků do centrální evidence.				
9	Vytvořené ICT standardy vycházející z Metodiky pro evidenci služeb veřejné správy.				
9	Vytvořené KB standardy vycházející z doporučení daných zákonem o kybernetické bezpečnosti.				
9	Vytvořena směrnice a pracovní postup pro zpracování projektových záměrů.				
9	Vytvořena směrnice a pracovní postup pro integraci dílčích agendových systémů.				
9	Centrální evidence obsahuje aktuální stav všech významných architektonických prvků MMB.				
9	U všech nových ICT projektů je zpracován projektový záměr tak, aby splňoval architektonické principy.				
9	Požadavky z ICT projektů s dopadem na architekturu jsou evidovány, analyzovány a schvalovány architektonickou komisí města pro ICT.				
9	Systémy centrálně poskytované v rámci SMB jsou zavedeny v centrální evidenci.				

Strategické projekty		2021	2022	2023	2024
9	Řízení metodami EA (Enterprice Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy.				
13	Vytvořen standard týkající se bezpečnosti technických aktiv.				
13	Aktualizace provozních řádů centrálních informačních systémů.				
13	Navržena struktura technologického standardu (jako základní technologický rámec s možností jeho využití ve výběrových řízeních) s vazbou na architektonické principy.				
13	Propojení architektonického řízení s konfiguračním managementem (GPC databáze).				
13	Naplnění struktury technologického standardu v prioritních částech.				
13	Úplné dokončení technologického standardu.				
13	Městský cloud je ve shodě s eGC ČR a jsou zavedeny standardy pro oblast informatiky v souladu s požadavky e-govermentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...).				
Cíl	**Otevřená data**				
10	Data jsou klasifikována.				
10	Otevřená data jsou zpřístupněna přes elektronické služby městského portálu prostřednictvím integrační platformy (Service Bus). Otevřená data jsou zveřejňována ve standardních otevřených formátech dle MV ČR v souladu s jejich klasifikací.				
10	Jsou zpřístupněna otevřená data z agendových systémů napojených na integrační platformu.				
14	Všechna otevřená data poskytovaná elektronicky přes městský portál jsou zabezpečena a nesou informaci o jejich důvěryhodnosti, tj. zejména je zaručena jejich důvěryhodnost ve smyslu jejich pravosti (znalost zdroje) a jejich integrity (nejsou neautorizovaně modifikována nežádoucím způsobem).				
14	Je podporováno využití otevřených dat z agendových systémů přístupných v reálném čase				
17	Pilotní zveřejňování otevřených dat ze systému GINIS.				
17	Zahájení procesu zveřejňování otevřených dat z agendových systémů MMB.				
17	Všechna otevřená data poskytovaná z MMB přes portál města jsou poskytována automatizovaně, u MČ a městských organizací v maximální dosažitelné míře.				

Strategické projekty		2021	2022	2023	2024
17	Veřejnost má přístup k dobře interpretovatelným otevřeným datům, čímž se zvyšuje transparentnost radnice a zájem občanů o spolupráci s ní.				

Cíl	**Integrační platforma**				
5	Definován a nastaven Service Bus integrační platformy.				
5	Spisová služba a GIS komunikuje přes integrační platformu.				
5	Využití Service Bus pro elektronické služby městského portálu občana.				
5	Integrace dílčích agendových systémů podle posouzení jejich priorit.				
5	Všechny významné datové a transformační vazby na MMB jsou realizovány přes integrační platformu.				

Závěr

Informační strategie je v souladu s principy metody Balanced Scorecard navržena jako ambiciózní a vychází z představ o disponibilních zdrojích na její realizaci v době jejího vytvoření. Strategie je živým dokumentem a předpokládá se, že v toku času může dojít ke změnám cílů, zdrojů a podmínek nutných pro její realizaci. Z těchto důvodů je nezbytné přistoupit ke sledování jejího naplňování. Pro usnadnění sledování plnění strategie ve smyslu naplňování strategických cílů je strategie rozpracována až do prováděcí úrovně dané strategickými projekty, přičemž každý projekt má přímou vazbu na realizaci konkrétních strategických cílů. Řízení portfolia strategických projektů se tak stává základním nástrojem pro sledování plnění informační strategie.

Portfolio strategických projektů není neměnné a bude se vyvíjet v čase. Musí proto docházet k vyhodnocování projektů a aktualizaci portfolia strategických projektů, která může mít dopad až do nadřazených strategických cílů. Při změně portfolia se proto doporučuje přezkoumat a balancovat informační strategii jako celek. Přitom nejde o negativní jev, ale o situaci, která je metodou Balanced Scorecard očekávána s tím, že považuje přezkoumání dosahování strategie za zpětnovazebný zdroj učení se a růstu. Smyslem přezkoumání a aktualizace strategie je trvalé dosahování souladu mezi strategickými cíli a možnostmi organizace z hlediska disponibility zdrojů na její realizaci. V případě nedosahování cílů se má za to, že není k dispozici dostatek zdrojů na jejich realizaci a je potřeba proto opětovně vybalancovat soulad mezi cíli a zdroji.

Strategické řízení nebude účinné, pokud nedojde k neustálému zlepšování strategie na základě vnějších a vnitřních podnětů. Aktualizace informační strategie by měla být prováděna v souladu s těmto zásadami:

Zaměření na	Přezkoumání s aktualizací	Výstup
Systém strategických cílů	1 x ročně Při změně nadřazené Vize a Strategie #brno 2050	Aktualizovaný dokument Informační strategie
Portfolio strategických projektů	1 x kvartálně Při vzniku výjimečné situace na některém ze strategických projektů	Hlášení o stavu portfolia strategických projektů