Z8/40. zasedání Zastupitelstva města Brna
konané dne 6.9.2022

Návrh aktualizace Informační strategie města Brna na období 2022 - 2026

Anotace

Aktualizace Informační strategie města Brna byla zpracována pro období let 2022 - 2026 jako strategický dokument, který je návrhem postupu k dosažení cílového stavu informatiky města Brna do horizontu konce roku 2026.

Návrh usnesení

Zastupitelstvo města Brna

1. schvaluje aktualizaci Informační strategie města Brna na období 2022 - 2026, která tvoří přílohu č. ... tohoto zápisu

2. ukládá Radě města Brna naplňovat jednotlivé cíle obsažené v Informační strategii města Brna na období 2022 - 2026
T: průběžně

Radě města Brna předkládat Zastupitelstvu města Brna ke schválení aktualizace Informační strategie města Brna
T: jedenkrát ročně

Stanoviska

Rada města Brna projednala na své schůzi R8/228 konané dne 20. 7. 2022 a **doporučila** ZMB ke schválení.

Podpis zpracovatele pro archivaci

Zpracovatel

Elektronicky podepsáno
Ing. David Menšík
vedoucí odboru - Odbor městské informatiky
8.8.2022 v 12:00
Garance správnosti, zákonnosti materiálu

Spolupodepisovatel

Elektronicky podepsáno

Mgr. Jiří Kučera

vedoucí úseku - Úsek 2. náměstka primátorky

8.8.2022 v 13:05

Obsah materiálu

Důvodová zpráva:

Rada města Brna předkládá Zastupitelstvu města Brna dokument Aktualizace Informační strategie města Brna na období 2022 - 2026. Tento dokument vytvořila pracovní skupina jmenovaná RMB, složená ze zástupců politického vedení města, pracovníků Magistrátu města Brna a Technických sítí Brno akciová společnost. Informační strategie města Brna byla zpracována pro období let 2022 – 2026 jako strategický dokument, který je návrhem postupu k dosažení cílového stavu informatiky města Brna do horizontu konce roku 2026.

Informační strategie rozpracovává cíl strategie pro Brno, rozvíjení informačního systému v rámci Magistrátu města Brna a městských částí, do systému 18 vzájemně provázaných strategických cílů. Vychází zejména ze strategického skeletu image města Brna, kde vnitřní i vnější vztahy jsou budovány s vizí oboustranné a pozitivní komunikace města, občanů a městských částí.

Při zpracování informační strategie byly identifikovány dále uvedené hlavní strategické cíle. Při jejich identifikaci a definici priorit byla aplikována metoda Balanced Scorecard. Základem informační strategie je strategická mapa dávající do souvislosti vytyčené strategické cíle z hlediska jejich vzájemných kauzálních vazeb. Cíle byly v souladu s touto metodou zasazeny do čtyř strategických perspektiv. Podrobně jsou cíle rozebrány v dokumentu v kapitole 3. Návrh cílového stavu.

Pro každý z cílů je stanovena metrika a jeho rozpad do stavu dosaženého v jednotlivých letech 2022 – 2026. Na tuto strukturu je přímo navázáno 9 strategických projektů, pomocí kterých budou cíle naplněny. V kapitole 4. Plán implementace strategie jsou projekty rozpracovány do časové osy po letech a podrobně rozebrány ve vazbě na strategické cíle, měřítka cílů a plánované hodnoty.

Stanovením strategických cílů jsou nastaveny dlouhodobé priority směrem ke chtěnému plánovanému stavu. Strategické řízení však nebude účinné, pokud nedojde k neustálému zlepšování strategie na základě vnějších a vnitřních podnětů. Toho je třeba dosáhnout formou aktualizace podle reálného stavu vývoje ICT a požadavků na splnění jednotlivých cílů jak z oblasti legislativy, platné pro orgány veřejné moci, tak z vyhodnocení provozních parametrů komponent, ze kterých se skládají IS města Brna. Aktualizace tohoto dokumentu by měla být prováděna nejméně 1 x ročně, případně při změně nadřazené Strategie pro Brno.

Rada města Brna na jednání R8/228 dne 20. 7. 2022 projednala a doporučila materiál Zastupitelstvu města Brna ke schválení, a to jednomyslně 10 členy.

JUDr. Vaňková	Mgr. Hladík	Bc. Koláčný	JUDr. Oliva	JUDr. Kerndl	Róbert Čuma	Ing. Fišer	Ing. Grund	RNDr. Chvátal	Ing. Kratochvíl	Mgr. Suchý
pro	pro	pro	pro	pro	pro	pro	-----	pro	pro	pro

Komise pro informační technologie RMB na svém 36. jednání dne 18. 7. 2022 projednala a doporučila RMB přijmout usnesení.

Hlasování dne 18. 7. 2022:
pro-proti-zdržel se-nehlasoval: **8-0-0-0/8**

PRO: 8 (Ondřej Kotas, Ing. Jan Grmela, Ing. Jindřich Zechmeister, Lukáš Boula, Ondřej Valeš, Ing. Zdeněk Machů, Mgr. Martin Lažnovský, Bc. Jiří Kment)
PROTI: 0
ZDRŽEL SE: 0
NEHLASOVAL:0

Analýza současného stavu (SWOT)

Strategické cíle (na období 2022 až 2026)

Strategická mapa (Balanced Scorecard schéma)

Implementace strategie (strategické projekty)

Aktualizace Informační strategie města Brna

Na období 2022 - 2026

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
4.00	23.6.2022	Per Partes	Aktualizace strategie na období 2022 až 2026	220623 Informacni strategie (MMB) v4_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 únoru až květnu 2022. Odráží názor tohoto týmu na strategický rozvoj informatiky města Brna a jsou v něm formulovány strategické cíle a k nim příslušné strategické ICT projekty do konce roku 2026. 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 verzi informační strategii města Brna vytvořenou na roky 2021 až 2024.

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 2026. 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 strategií pro nadřazenou strategii *Vize a Strategie #brno 2050*.

Perspektiva	Motto	Cíle
ICT přínosy	Jednotné ICT města	Digitalizovat služby veřejné správy (městský portál občana) Vytvořit moderní, společné a bezpečné ICT města Otevřít městská data veřejnosti
ICT zákazníci	Motivace k využívání elektronických služeb	Poskytovat elektr. služby přes portál města v uživatelsky intuitivní a jednotně publikované podobě Umožnit interním uživatelům práci z prostředí domova Podporovat využívání služeb městského cloudu organizacemi SMB Rozšířit využívání centrálních aplikací podle závazných standardů Posilovat důvěru ve sdílení dat a propagovat otevřená data a jejich využití
Procesy	Umožnit technologiemi elektronické služby	Využívat workflow aplikací přes jednotné prezentační rozhraní Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy Poskytovat z informačních systémů data klasifikovaná jako veřejná
ICT potenciál a zdroje	Náskok v aplikaci moderních digitálních technologií	Vytvořit moderní portál města Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty) Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť Posílit datovou integraci přes integrační platformu

Tab.1: Přehled strategických cílů

Strategické ICT 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 9 strategickými ICT projekty (resp. programy, pokud se budou dále realizačně členit) rozloženými do let 2022 až 2026. 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	2022	2023	2024	2025	2026
Webová platforma města Brna					
Portál občana Brna					
Služby autentikace podle eIDAS					
Zajištění odolnosti					
Zavedení dohledových a reaktivních technologií					
Městský cloud					
Centrální služby a aplikace, služby a aplikace v cloudu					
Koordinace, standardizace a architektura					
Otevřená data					

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 následujícími 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 ICT projektů	1 x kvartálně Při vzniku výjimečné situace na některém ze strategických projektů	Hlášení o stavu portfolia strategických ICT 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)
- Jiří Kučera (vedoucí Úseku 2. náměstka primátora)
- David Menšík (vedoucí Odboru městské informatiky)
- Vladimír Halm (vedoucí odd. správy inf. systému, Odbor městské informatiky)
- Dušan Hájek (vedoucí odd. systémové a tech. podpory, Odbor městské informatiky)
- Jan Kotas (manažer projektu AISMB, Odbor městské informatiky)
- František Sedláček (koordinátor kybernetické bezpečnosti, Kancelář kybernetické bezpečnosti)
- Rostislav Obrlík (vedoucí Úseku tajemníka)
- Martina Pacasová (manažer strategie města, oddělení strategického plánování, Odbor strategického rozvoje a spolupráce)
- Lukáš Boula (člen Komise informačních technologií)
- Michal Jukl (ředitel ICT, TSB)
- Robert Schindler (architekt kybernetické bezpečnosti, TSB)
- Jan Zachoval (Enterprise Architecture Consultant, AUTOCONT a. s.)
- Lukáš Vlček (Enterprise Architecture Consultant, AUTOCONT a. s.).

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.).

Předmět:

Předmětem aktualizace informační strategie je informatika města Brna v letech 2022 až 2026.

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 2022 - 2026. Původní dokument Informační strategie byl vydán dne 6.12.2011, jeho první aktualizace proběhla dne 7.5.2015, druhá aktualizace 1.10.2020 a třetí aktualizace byla zpracována ke dni 23.6.2022. Informační strategie je publikována na webu města Brna (www.brno.cz).
Provedené úkony:	V rámci aktualizace informační strategie byly provedeny následující workshopy strategického týmu: • Analýza současného stavu – SWOT analýzy • Analýza současného stavu – analýza kvadrantů SWOT, strategické záměry • Návrh cílového stavu – strategické cíle s výhledem do roku 2026 • Návrh cílového stavu – strategická mapa a kauzální řetězce • Plán implementace strategie – měřítka plnění cílů • Implementační plán přechodu – strategické ICT projekty • Závěrečné přezkoumání strategie - přezkoumání 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

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.

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
- 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

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

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.

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**

  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

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.

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**

  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
- Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, ve znění pozdějších předpisů
- Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu

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

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).

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 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.

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 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).

Agendový informační systém (AIS) je informační systém zpracovávající příslušnou agendu.

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.

Autentikace (autentizace) je proces ověření proklamované identity subjektu.

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 Ministerstvem 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 (EA) (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.

Identity management (IDM) představuje systém pro centralizovanou správu identit.

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.

Metropolitní síť Brno (MSB) je komunikační infrastruktura, která umožňuje vzájemné datové propojení důležitých uzlových bodů města.

Odbor městské informatiky (OMI) je odbor zodpovědný za zabezpečení provozu a rozvoje ICT SMB. Jeho další rolí je koordinace a řízení informatiky města Brna.

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.

Strategický ICT projekt je koordinované úsilí v oblasti informatiky realizující přínos pro organizaci stanovený v její strategii. Projekt se dále realizačně může členit anebo může být chápán jako program složený z dílčích projektů.

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.

Technické sítě Brno (TSB) je městká společnost poskytující služby pro SMB v oblastech inženýrských sítí a ICT.

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;
- Architektura ICT města;
- Přínosy informatiky pro SMB;
- 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 verze strategie

V této podkapitole je shrnut stav splnění strategických cílů stanovených pro rok 2021 v Informační strategii města Brna aktualizované v roce 2020 (verze 3.00).

1. Vytvořit platformu pro moderní portál města

Předmětem aktuálně realizované 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 byl v předstihu již implementován pilotní web „OnStage“. Následně bude v rámci předmětu Veřejné zakázky spuštěn a provozován nový web www.brno.cz. Součástí předmětu Veřejné zakázky je Podpora a Údržba, jakož i Customizace Platformy.

2. Zavést eIDAS (elektronická identita a důvěryhodné el. dokumenty)

Autentikační brána je dokončena a napojena na vnitřní IDM SMB. Finálním cílem je využívat bránu pro napojování jednotlivých identitních systémů a splnit cíl federování identit. Dalším využitím je zprostředkování ověřené identity v požadované úrovni dle legislativních požadavků. Postupně probíhá napojování aplikačních IS tam, kde dává napojení smysl, u ostatních je v IDM vedena evidence oprávnění. Rovněž je v modulu IDM Asset evidováno základní rozdělení licencí a dalších ICT prvků, včetně certifikátů se sledováním jejich platnosti. Dalším krokem může být federování identit s městskými organizacemi, realizované pomocí autentikační brány, která již nyní umožňuje federování identit s městskými organizacemi - technologie je již nyní připravena.

Integrace systémů v rozsahu určeném SŘBI není zatím u všech daných systémů v plném rozsahu.

Technologie pro interní důvěryhodný oběh dokumentů zatím není nasazena ani vybrána, základní požadavky splňuje oběh v elektronické spisové službě, která ale v současné implementaci nepodporuje workflow.

3. Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti ve všech vrstvách

Probíhá veřejná zakázka „LOG management“ - implementace plánována v roce 2022. V cílovém stavu bude zajišťovat jak shromažďování logů pro další technologie bezpečnostního dohledu, tak i provozní monitoring. Vybraný systém též umožní automatizovat upozornění na anomální jevy a podporu pro obsluhu ICT prostředí.

Systém PIM/PAM je naimplementován jako integrovaný modul v IDM a nyní je v ověřovacím provozu. Bude umožňovat správu privilegovaných účtů včetně auditních logů.

4. Vytvořit sdílený městský cloud postavený na odolné infrastruktuře vč. datových úložišť

Existují dvě datová centra v objektech TSB, která jsou plně redundantně propojena. Diskové úložiště je rozděleno do dvou geograficky oddělených lokalit.

Je vybudována robustní síťová infrastruktura. Jsou poskytovány dílčí cloudové služby pro vybrané městské subjekty.

5. Posílit datovou integraci přes integrační platformu

Byl definován a nastaven Service Bus integrační platformy. Prostřednictvím Service Bus se postupně řeší další integrace. Probíhá implementace využití Service Bus pro on-line služby webové platformy.

Integrace AIS pomocí zvolené technologie Clover ETL je podporována i v rámci koncepce podnikové architektury MMB. Pokročilé možnosti při integraci různých AISů ukazují v dlouhodobém pohledu významný přínos ke stabilitě provozu.

6. Podpořit technologiemi workflow pro elektronicky poskytovatelné služby

Webový portál bude sloužit jako FrontEnd jednotlivých systémů, zajišťujících jednotlivé služby.

Bylo přijato rozhodnutí, že portál nebude za účelem provozování služeb poskytovat vlastní workflow, ale umožní nasměrování k příslušným službám s podporou workflow.

Integrace on-line služeb do portálu bude umožněna díky možnostem zvoleného prostředí WEBové platformy, i zapojení integrační datové platformy.

7. Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby

Standardy jsou postupně připravovány a je aplikována jak legislativa pro oblast kyberbezpečnosti,

tak i doporučení směrnic (NIS 2, …) a metodické podklady NÚKIB.

Je prováděno vyhodnocování stavu bezpečnosti prostředí IS ÚMČ s cílem identifikace nejčastějších slabých míst. Na základě vyhodnocování je upravován bezpečnostní standard a jsou připravovány projekty pro nápravu nejzávažnějších zjištění.

8. Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce v cloudu

Byly zahájeny práce na pilotním zpracování Katalogu ICT služeb města Brna, jehož součástí budou i služby městského cloudu. V současné době katalog není dokončen.

9. Architektonicky řídit ICT města a vytvořit městské ICT standardy

Byly stanoveny základní architektonické principy ICT města v dokumentu „Zásady_EA_v_prostředí MMB_v1.1.“. Tento materiál je souhrnem doporučení pro definici požadavků na nový či změněný ICT prvek v rámci ICT prostředí SMB. Obsahem jsou postupy jak pro definici požadavků, tak i pro posouzení dopadů a upřesnění business zadání.

Stávající verze modelu podnikové architektury obsahuje centrální evidenci architektonických prvků = repositář EA. Nejsou obsaženy aktuální informace z oblasti infrastruktury, zde bude klíčovým zdrojem v současnosti implementovaná konfigurační báze.

Postup další aktualizace modelu je popsán v dokumentu "Metodika_rizeni_EA_v_ prostredi_MMB_v1.3". Dalším navazujícím krokem bude vytvoření ICT standardů, vycházejících z doporučení Odboru hlavního architekta eGovernmentu ČR pro evidenci služeb veřejné správy.

U všech nových ICT projektů bude zpracován projektový záměr tak, aby splňoval architektonické principy podle metodiky TOGAF.

10. Poskytovat z informačních systémů data klasifikovaná jako veřejná

Data z informačních systémů města, která mají potenciál pro publikaci jako otevřená data, jsou zatím analyzována. Prvními typy dat jsou tak data o hlasování brněnského zastupitelstva nebo metadata z úřední desky města Brna a některých MČ.

11. Poskytovat elektr. služby přes internetovou přepážku v uživatelsky intuitivní a jednotné podobě

Předmětem aktuálně realizované Veřejné zakázky „Tvorba a provoz webové platformy města Brna“ je nejen vytvoření a rozvoj Platformy pro weby města Brna, ale i implementace Portálu občana Brna.

Bylo provedeno Proof-of-Concept testování vyřizování životní situace platby místního poplatku za komunální odpad prostřednictvím AIS GINIS.

12. Podporovat využívání cloudových služeb městskými firmami

Na městském cloudu jsou poskytovány vybrané služby 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.

Existuje nabídka cloudových služeb pro subjekty města. Tyto jsou nabízeny k využití a některé subjekty již tyto služby využívají.

13. Rozšířit využívání aplikací v městském cloudu podle závazných standardů

Na městském cloudu jsou poskytovány vybrané služby KB (kybernetické bezpečnosti). Standardy bezpečnosti pro technická aktiva jsou součástí SŘBI a další relevantní dokumentace.

Provozní řád byl aktualizován s ohledem na současný stav technologií a procesů OMI MMB.

Existují architektonické zásady a metodiky, které jsou aplikovatelné pro další práci na technologickém standardu.

14. Posilovat důvěru ve sdílení dat a propagovat otevřená data a jejich využití

V roce 2021 se podařilo publikovat mnoho otevřených datových sad, které mají vysoký potenciál pro další využití. Datové sady jsou v maximální míře aktuální s kvalitním popisem, což vede i k jejich zvýšenému využití v aplikacích třetích stran. To samo o sobě posiluje důvěru a jejich další využívání, velmi pečlivě je i sbírána zpětná vazba od uživatelů pro další vylepšování služby.

V roce 2022 je plánováno nastavené tempo otevírání dat udržet. Výraznou propagační akcí pak byl 1. městský hackathon, kde došlo k velkému využití brněnských otevřených dat.

15. Elektronizace služeb veřejné správy (elektronická radnice)

Předmětem aktuálně realizované Veřejné zakázky „Tvorba a provoz webové platformy města Brna“ je nejen vytvoření a rozvoj Webové platformy pro weby města Brna, ale i implementace Portálu občana města Brna.

16. Vytvořit moderní, společné a bezpečné ICT města

Řízení kybernetické a informační bezpečnosti bylo systematizováno a v jeho rámci jsou popsány a aplikovány bezpečnostní role, procesy a odpovědnosti. Řízení bezpečnosti bylo svěřeno samostatnému útvaru s celoměstskou koordinační a normotvornou působností.

Systém řízení bezpečnosti informací vznikl v podobě řízené bezpečnostní dokumentace, platné v rámci vybraných systémů OMI MMB a dalších součástí města. Probíhá vytvoření minimálního společného standardu pro kybernetickou bezpečnost úřadů městských částí a jsou realizovány postupy a procesy pro řízení bezpečnosti od technické úrovně přes organizační až po strategickou. V rámci Systému řízení bezpečnosti informací jsou řešeny minimální standardy a požadavky pro provoz kritických systémů města.

17. Otevření městských dat veřejnosti

V roce 2021 bylo publikováno mnoho otevřených dat zejména z prostředí městského GIS.

Od roku 2021 je datový portál města data.Brno postaven na technologii ArcgisHUB, což umožnuje mít data ve vyšší kvalitě i aktuálnosti než v předchozím řešení založeném na technologii CKAN. Publikována jsou data statická i senzorická (skrze řešení Geoevent server od ESRI).

V roce 2022 je plánováno zaměřit se na publikaci otevřených dat od městských společností.

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);
- Architektura ICT města (business procesy, informační toky, aplikace, infrastruktura);
- Přínosy informatiky pro SMB (přínosy pro umožnění lepšího a efektivnějšího fungování města);
- Spokojenost uživatelů (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.
4,1	Oblast informační bezpečnosti je řízena vlastním specializovaným útvarem Kanceláří kybernetické bezpečnosti na úrovni úseku.
4,0	Dosažené zkušenosti s implementací informačních systémů.
4,0	Vysoká znalost technologických trendů a jejich zavádění.
3,8	Zvyšující se bezpečnostní povědomí mezi pracovníky OMI a rovněž pracovníky MMB.
3,4	Systém povinného vzdělávání úředníků.

Opportunities (vnější příležitosti)	
4,1	Disponibilní vzdělaní a kompetentní pracovníci v ICT v Brně.
4,0	Využití popisu procesů MMB (ORGO).
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	Převedení vybraných služeb informatiky do samostatného ekonomického subjektu ovládaného městem Brnem za koordinace OMI.

Weaknesses (vnitřní slabé stránky)	
4,5	Motivační systém neumožňuje získávat nové a udržet stávající pracovníky IT.
4,2	Nedostatek vnitřních odborných kapacit vzhledem k rostoucímu významu a rozvoji informatiky vede ke zvýšenému nákupu externích služeb.
4,0	Klíčové uživatele je obtížné motivovat pro spolupráci v projektových týmech týkajících se informatiky z důvodu střetu liniových a projektových struktur.
4,0	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	Samostatný vzájemně málo koordinovaný postup MČ při rozvoji IS.
3,3	Nedostatečné povědomí klíčových uživatelů o plánovaní kapacit zdrojů OMI na pokrytí požadavků.

Threats (vnější hrozby)	
5,0	Masivní vývoj kybernetických útoků a jejich forem.
4,1	Hrozby spojené s užíváním zařízení umístěných mimo perimetr.
4,0	Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT.
4,0	Překotný vývoj legislativních požadavků v oblasti digitalizace a kybernetické bezpečnosti.
3,9	Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.
3,9	Uživatelé pracující vzdáleně (mimo kancelář) se obracejí s lokálními ICT problémy na servisní podporu OMI mimo jeho gesci.
3,6	Z výběrových řízení podle ZZVZ 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.

Threats (vnější hrozby)	
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 Architektura ICT města

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 SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) 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).
3,8	Je zřízena samostatná role bezpečnostního architekta. Bezpečnostní architektura je provázána na EA.
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 konfiguračních databází udržovaných MMB a samostatně dodavateli/správci částí infrastruktury.
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 ÚMČ a městských společností a organizací.
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 plánů 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.
3,8	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).
4,2	Komplikovanost přistupovat k aplikacím z vnějšího prostředí - restriktivní řešení bezpečnostních rizik.
4,1	Chybí vazba na business vrstvu zpracovávanou ORGO v BPMN diagramech.
4,0	Chybí standardizovaný Projektový záměr včetně pohledu EA (principy EA, analýzy přínosů a nákladů apod.).
4,0	Ne všechna data jsou ukládána do datových úložišť ve strukturované podobě, která umožní řízení přístupu dle oprávnění.
4,0	Nedobudována geograficky oddělená záložní infrastruktura.
4,0	Závislost rozvoje ICT architektury na přidělených prostředcích (rozpočtu).
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).
3,7	Městské firmy si spravují vlastní podružná menší datová centra i aplikace bez vazby na EA.
3,7	Nedostatečná aplikace principů procesního řízení.
3,3	IDM nemá zadefinované role z business vrstvy (není propojení až do procesní business vrstvy a její rozpracování na role).
3,0	Řada aplikací nemá dokumentaci.
2,9	Platformová technologická roztříštěnost (např. různé databázové 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 o bezpečnostní riziko.
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 …).
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.

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.

Strengths (vnitřní silné stránky)	
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.
3,4	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 (legislativní a procesní omezení).
4,4	Pro občana nejsou v dostatečné míře přístupné všechny agendy přes internet. Neexistuje portál občana (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).
3,9	Zastaralé a nepřehledné webové stránky města.

Threats (vnější hrozby)	
4,1	Vznikají požadavky 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. Některé procesy nebude možno řešit s očekávanou on-line přívětivostí.
4,0	Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.
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.

Opportunities (vnější příležitosti)	
4,4	Poskytnutí dočasného přístupu k wi-fi návštěvníkům a zaměstnancům MMB.
4,1	Vytvoření portálu občana - "internetové přepážky".
4,0	Využití drobných specializovaných aplikací používaných v jiných městech.
3,9	Podpora uživatelů prostřednictvím chatbot a voicebot.
3,9	Zavést hodnocení kvality vyřešení požadavků zadaných v Help Desku uživatelem.
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).
4,4	Nedůvěra uživatelů k používání Help Desku.
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)	
4,9	Napadení výpočetní techniky uživatele s omezením dostupnosti dat na ní uložených (např. ransomware).
4,9	Výpadek metropolitní sítě a internetu znamená nefunkčnost významných agend SMB.
4,4	Závislost na správném fungování centrálních aplikací při poskytování služeb.
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.
3,2	Legislativní omezení ICT služeb pro externí subjekty (občan, právnické osoby …).

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	Zavedená helpdesková podpora uživatelů.	Uživatelé
4,7	V rámci SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) se zajištěnou ochranou proti jejich ztrátě.	Architektura
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

Strengths (vnitřní silné stránky)		
4,4	Průběžná obnova techniky (koncových zařízení).	Uživatelé
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
4,3	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
4,1	Oblast informační bezpečnosti je řízena vlastním specializovaným útvarem Kanceláří kybernetické bezpečnosti na úrovni úseku.	Organizace
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
3,8	Je zřízena samostatná role bezpečnostního architekta. Bezpečnostní architektura je provázána na EA.	Architektura
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 SharePoint Services) s komunitou uživatelů.	Architektura
3,6	Vytvořené prostředí pro zapojení občanů do dění města Brna.	Přínosy
3,4	Dostupnost aktualizovaných manuálů na intranetu.	Uživatelé
3,4	Jsou vytvořeny specializované subjekty města k poskytování specifických ICT služeb.	Přínosy
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	Poskytnutí prostředků uživatelům pro přístup k informacím i z domova.	Uživatelé
4,6	Vytvoření a správa katalogu služeb ICT.	Architektura
4,4	Poskytnutí dočasného přístupu k wi-fi návštěvníkům a zaměstnancům MMB.	Uživatelé
4,4	Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy).	Architektura
4,4	Propojení konfiguračních databází udržovaných MMB a samostatně dodavateli/správci částí infrastruktury.	Architektura
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

Opportunities (vnější příležitosti)		
4,1	Vytvoření portálu občana - "internetové přepážky".	Uživatelé
4,1	Vytvoření samostatného útvaru řešícího informatiku ÚMČ a městských společností a organizací.	Architektura
4,1	Koordinace ICT projektů městských subjektů.	Přínosy
4,1	Disponibilní vzdělaní a kompetentní pracovníci v ICT v Brně.	Organizace
4,0	Využití drobných specializovaných aplikací používaných v jiných městech.	Uživatelé
4,0	Využití popisu procesů MMB (ORGO).	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
3,9	Podpora uživatelů prostřednictvím chatbot a voicebot.	Uživatelé
3,9	Zavést hodnocení kvality vyřešení požadavků zadaných v Help Desku uživatelem.	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 plánů 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
3,8	Zvyšující se zájem stakeholderů o přístup k informacím z EA modelu.	Architektura
3,7	Spolupráce s jinými městy v ČR a EU.	Přínosy
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	Převedení vybraných služeb informatiky do samostatného ekonomického subjektu ovládaného městem Brnem za koordinace OMI.	Organizace

Weaknesses (vnitřní slabé stránky)		
4,6	Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.	Uživatelé
4,6	Neexistence ICT technologického standardu města.	Přínosy
4,5	Motivační systém neumožňuje získávat nové a udržet stávající pracovníky IT.	Organizace
4,4	Dosud nezavedená elektronická podpora některých vnitřních schvalovacích procesů úřadu (např. cestovních příkazů).	Uživatelé
4,4	Nemožnost řešit problémy v informatice v době, kdy vznikají (legislativní a procesní omezení).	Přínosy
4,4	Pro občana nejsou v dostatečné míře přístupné všechny agendy přes internet. Neexistuje portál občana (prezentační portál) umožňující sledování procesu.	Přínosy
4,4	Nedůvěra uživatelů k používání Help Desku.	Uživatelé
4,3	Uživatelé nemají povědomí o reálných možnostech řešení jejich požadavků (času, schopnosti řešit požadavek, finanční náročnosti). Nedostatečně objektivní požadavky uživatelů.	Uživatelé
4,3	Neexistuje provozní aplikační a datový monitoring a konfigurační management na aplikační vrstvě.	Architektura

Weaknesses (vnitřní slabé stránky)		
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
4,2	Nedostatek vnitřních odborných kapacit vzhledem k rostoucímu významu a rozvoji informatiky vede ke zvýšenému nákupu externích služeb.	Organizace
4,2	Komplikovanost přistupovat k aplikacím z vnějšího prostředí - restriktivní řešení bezpečnostních rizik.	Architektura
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	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
4,0	Klíčové uživatele je obtížné motivovat pro spolupráci v projektových týmech týkajících se informatiky z důvodu střetu liniových a projektových struktur.	Organizace
4,0	Ne všichni klíčoví uživatelé (garanti) mají dostatečné znalosti, aby definovali požadavky na informatiku (formulace toho, co chtějí). OMI nemůže suplovat metodické role uživatelů.	Organizace
4,0	Chybí standardizovaný Projektový záměr včetně pohledu EA (principy EA, analýzy přínosů a nákladů apod.).	Architektura
4,0	Ne všechna data jsou ukládána do datových úložišť ve strukturované podobě, která umožní řízení přístupu dle oprávnění.	Architektura
4,0	Nedobudována geograficky oddělená záložní infrastruktura.	Architektura
4,0	Závislost rozvoje ICT architektury na přidělených prostředcích (rozpočtu).	Architektura
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	Zastaralé a nepřehledné webové stránky města.	Přínosy
3,8	Samostatný vzájemně málo koordinovaný postup MČ při rozvoji IS.	Organizace
3,7	Nejednotný přístup uživatelů k realizaci svých požadavků (formulace, spolupráce na řešení).	Uživatelé
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
3,3	IDM nemá zadefinované role z business vrstvy (není propojení až do procesní business vrstvy a její rozpracování na role).	Architektura
3,3	Nedostatečné povědomí klíčových uživatelů o plánovaní kapacit zdrojů OMI na pokrytí požadavků.	Organizace
3,0	Řada aplikací nemá dokumentaci.	Architektura
2,9	Platformová technologická roztříštěnost (např. různé databázovéstroje).	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
4,9	Napadení výpočetní techniky uživatele s omezením dostupnosti dat na ní uložených (např. ransomware).	Uživatelé

Threats (vnější hrozby)		
4,9	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	Vznikají požadavky 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. Některé procesy nebude možno řešit s očekávanou on-line přívětivostí.	Přínosy
4,1	Hrozby spojené s užíváním zařízení umístěných mimo perimetr.	Organizace
4,0	Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT.	Organizace
4,0	Překotný vývoj legislativních požadavků v oblasti digitalizace a kybernetické bezpečnosti.	Organizace
4,0	EA model obsahuje koncentrované informace a při neoprávněném přístupu k nim jde o bezpečnostní riziko.	Architektura
4,0	Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.	Přínosy
4,0	Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.	Přínosy
3,9	Uživatelé pracující vzdáleně (mimo kancelář) se obracejí s lokálními ICT problémy na servisní podporu OMI mimo jeho gesci.	Organizace
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
3,8	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
3,6	Z výběrových řízení podle ZZVZ 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	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
3,2	Legislativní omezení ICT služeb pro externí subjekty (občan, právnické osoby …).	Uživatelé
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 SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) 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
Zavedená helpdesková podpora uživatelů.
k vnější příležitosti
Zavést hodnocení kvality vyřešení požadavků zadaných v Help Desku uživatelem.
Podpora uživatelů prostřednictvím chatbot a voicebot.

[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 SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) 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.
Legislativní omezení ICT služeb pro externí subjekty (občan, právnické osoby …).

[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
Vznikají požadavky 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 …).

[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.

[ST8] Využití vnitřní silné stránky
Oblast informační bezpečnosti je řízena vlastním specializovaným útvarem Kanceláří kybernetické bezpečnosti na úrovni úseku.
Je zřízena samostatná role bezpečnostního architekta. Bezpečnostní architektura je provázána na EA.
k zamezení vnější hrozby
Napadení výpočetní techniky uživatele s omezením dostupnosti dat na ní uložených (např. ransomware).
Hrozby spojené s užíváním zařízení umístěných mimo perimetr.

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 v dostatečné míře přístupné všechny agendy přes internet. Neexistuje portál občana (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 portálu občana - "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.
Nedůvěra uživatelů k používání Help Desku.
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.
Hrozby spojené s užíváním zařízení umístěných mimo perimetr.

[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
Komplikovanost přistupovat k aplikacím z vnějšího prostředí - restriktivní řešení bezpečnostních rizik.
s vnější hrozbou
Hrozby spojené s užíváním zařízení umístěných mimo perimetr.
Uživatelé pracující vzdáleně (mimo kancelář) se obracejí s lokálními ICT problémy na servisní podporu OMI mimo jeho gesci.

[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. Některé procesy nebude možno řešit s očekávanou on-line přívětivostí.
Vznikají požadavky na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.
Překotný vývoj legislativních požadavků v oblasti digitalizace a kybernetické bezpečnosti.

[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 v dostatečné míře přístupné všechny agendy přes internet. Neexistuje portál občana (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 (legislativní a procesní omezení).
Nedostatek vnitřních odborných kapacit vzhledem k rostoucímu významu a rozvoji informatiky vede ke zvýšenému nákupu externích služeb.
s vnější hrozbou
Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.

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.

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
4,7	W-O	Pro občana nejsou v dostatečné míře přístupné všechny agendy přes internet. Neexistuje portál občana (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 portálu občana - "internetové přepážky". Vytvoření a správa katalogu služeb ICT.	Umožnit přístup k agendám přes internet pomocí portálu občana. Informatika města má umožňující roli pro digitalizaci služeb a nabízí podporu odborných útvarů pomocí katalogu služeb ICT.
	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
4,7	S-T	V rámci SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) 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 v datových centrech vč. městského cloudu.
	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
4,6	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 a udržovat technologický standard SMB (nikoliv jen MMB). Dlouhodobě plánovat architektonický rozvoj na všech úrovních EA.

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
4,4	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.

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
4,4	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.

	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
4,0	S-T	Oblast informační bezpečnosti je řízena vlastním specializovaným útvarem Kanceláří kybernetické bezpečnosti na úrovni úseku. Je zřízena samostatná role bezpečnostního architekta. Bezpečnostní architektura je provázána na EA.	Hrozby spojené s užíváním zařízení umístěných mimo perimetr. Napadení výpočetní techniky uživatele s omezením dostupnosti dat na ní uložených (např. ransomware).	Zajištění bezpečnosti uživatelů pracujících vně chráněného městského perimetru.

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
4,0	W-O	Motivační systém neumožňuje získávat nové a udržet stávající pracovníky IT.	Disponibilní vzdělaní a kompetentní pracovníci v ICT v Brně. Zintenzivnění spolupráce se středními a vysokými školami.	Vytvořit motivační systém pro pracovníky v IT. který bude pro určité skupiny pracovníků dostatečně atraktivní.

	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
3,9	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 SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) 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 centrálně instalovaných aplikací města podle závazně dohodnutých pravidel.

	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
3,9	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.	Zvýšit odolnost infrastruktury proti výpadku jednotlivých prvků.

	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
3,9	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 využitím EA.

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,9	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 a jednotné schvalování projektů na základě shody s informační strategií, EA s jejich zdůvodněním formou projektového záměru.
	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
3,7	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
3,7	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 v oblasti SMB.
	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
3,7	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.
	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,3	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.

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
3,1	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
3,1	W-T	Nemožnost řešit problémy v informatice v době, kdy vznikají(legislativní a procesní omezení). Nedostatek vnitřních odborných kapacit vzhledem k rostoucímu významu a rozvoji informatiky vede ke zvýšenému nákupu externích služeb.	Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni. Překotný vývoj legislativních požadavků v oblasti digitalizace a kybernetické bezpečnosti.	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 projektového záměru.

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
3,1	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.

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,1	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. Aktivně zjišťovat plány rozvoje legislativy.

	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
3,0	S-O	Zavedená helpdesková podpora uživatelů.	Zavést hodnocení kvality vyřešení požadavků zadaných v Help Desku uživatelem. Podpora uživatelů prostřednictvím chatbot a voicebot.	Zvýšení orientace na podporu uživatelů s posílením helpdeskových funkcí.

	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
2,9	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.

3. Návrh cílového stavu

Cílový stav je popsán v systému 18 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 eGovernmentu, 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 poskytuje centralizované a integrované ICT služby koordinované Odborem městské informatiky za účelem zajištění potřeb statutárního města Brna v souladu s městským statutem.

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)?	Jednotné 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 moderní portál města	Portál města je naplněn službami: • úřední pro občany / úředníky • turisticko / informační • otevřená data • geoportál. Součástí portálu města Brna je řešení jeho kybernetické bezpečnosti.
2	Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty)	Důvěryhodné elektronické služby jsou provázány do aplikací města.
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 prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť	Infrastrukturní prostředí je trvale dozorováno (provozní a bezpečnostní monitoring) a vybaveno 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	Využívat workflow aplikací přes jednotné prezentační rozhraní	Aplikace jsou zpřístupněny na portálu pro poskytování elektronických služeb. Workflow u aplikací poskytujících služby úřadu přes portál je navrženo ve spolupráci s procesním modelováním BPMN diagramů na ORGO.
7	Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby	Standardy zajišťují bezpečnost (důvěrnost, integritu a dostupnost) a důvěryhodnost elektronicky poskytovatelných služeb.
8	Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb	Katalog ICT služeb umožňuje využívat infrastrukturní, platformové a bezpečnostní služby poskytované centrálně jednotným způsobem, a to pro SMB a zřizované organizace města.
9	Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy	Řízení EA (Enterprise 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 centrálního publikačního bodu. Existují jednoznačné procesy pro deklasifikaci, anonymizaci a kontrolu zveřejňovaných dat.

3.2.3. Cíle v perspektivě zákazníků

číslo	strategický cíl	popis
11	Poskytovat elektr. služby přes portál města v uživatelsky intuitivní a jednotně publikované 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	Umožnit interním uživatelům práci z prostředí domova	Pro interní uživatele ICT služeb SMB je umožněno využívat aplikace vzdáleným přístupem podle nastavených SLA/OLA parametrů.
13	Podporovat využívání služeb městského cloudu organizacemi SMB	Městské cloudové služby (zálohování, úložiště, bezpečnost) jsou poskytovány za výhodných ekonomických podmínek z pozice jednotlivých městských organizací obtížně dosažitelných a na profesionální úrovni.
14	Rozšířit využívání centrálních aplikací podle závazných standardů	Centrálně poskytované aplikace budou ve shodě s eGC ČR a město bude mít zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...). Bude vytvořen a udržován technologický standard SMB.
15	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
16	Digitalizovat služby veřejné správy (městský portál občana)	Je vytvořena technologická platforma s uživatelsky přívětivým rozhraním pro elektronickou formu komunikace a participace občanů s úředníky.
17	Vytvořit moderní, společné a bezpečné ICT města	Město disponuje moderní modulární a stále se rozvíjející ICT infrastrukturou, která je sdílena v rámci MMB, MČ, městských firem a organizací. Infrastruktura poskytuje maximálně efektivní elektronické služby a její bezpečnost je zajištěna na profesionální úrovni.
18	Otevřít městská data 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.

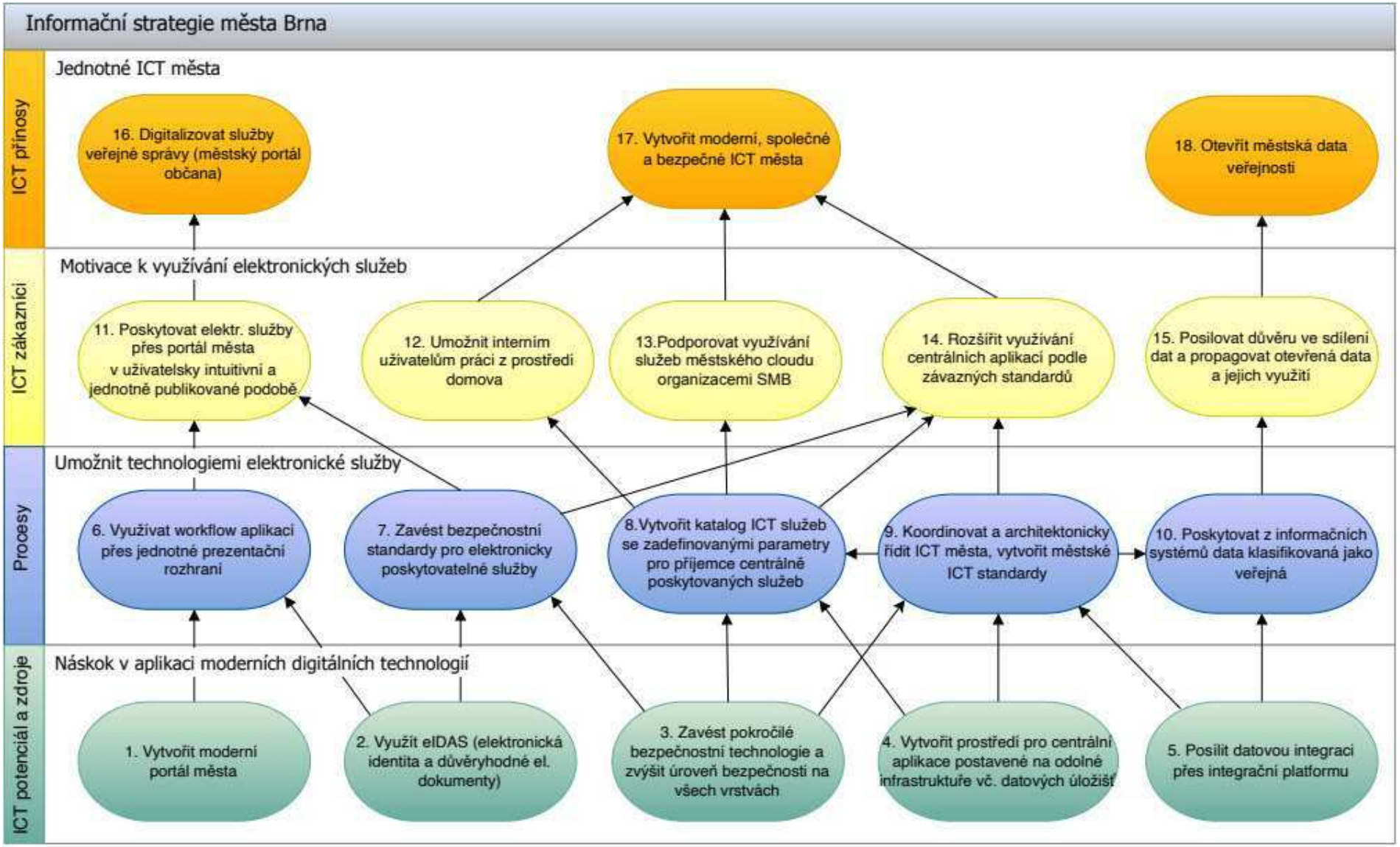
Ve strategické mapě (schéma Balanced Scorecard) jsou kauzální vazby znázorněny šipkami, kdy ve směru šipky je uvažován vztah příčina vyvolávající následek. Zaměření na strategicky významné vztahy, bez ambice na analýzu všech myslitelných vazeb mezi cíli, je jednou z hlavních předností použité metody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

- Digitalizace služeb veřejné správy (městský portál občana);
- Vytvoření moderního, společného a bezpečného 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 digitalizace služeb;
- Řetězec ICT města;
- Řetězec otevřenosti městských dat.

Řetězec digitalizace služeb

Strategický řetězec ***digitalizace* služeb** je uskupen kolem sedmi cílů vertikálně směřujících k dosažení digitální komunikace s občany prostřednictvím městského portálu občana:

1. *Vytvořit moderní portál města;*
2. *Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty);*
3. *Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách;*
6. *Využívat workflow aplikací přes jednotné prezentační rozhraní;*
7. *Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby;*
11. *Poskytovat elektr. služby přes portál města v uživatelsky intuitivní a jednotně publikované podobě;*
16. *Digitalizovat služby veřejné správy (městský portál občana).*

Jedná se o skupinu cílů směřující ke zvýšení transparentnosti a otevřenosti radnice a k digitalizaci 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 digitální komunikace a participace občanů s úředníky, je třeba zajistit důvěryhodnost elektronických služeb poskytovaných Úřadem, bezpečný přístup občanů k dokumentům zprostředkovaných městským portálem občana 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 v uživatelsky intuitivní podobě. Konečným důsledkem realizace

těchto postupových cílů je digitalizace služeb veřejné správy.

Řetězec ICT města

Strategický řetězec **ICT města** kauzálně propojuje cíle směřující k dosažení moderního, společného a bezpečného ICT umožňujícího interním uživatelům ICT služeb SMB využívat aplikace vzdáleným přístupem, poskytovat služby organizacím SMB prostřednictvím městského cloudu a v neposlední řadě využívat na MMB, MČ a městských firmách centrální sdílené aplikace:

2. *Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty);*
3. *Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách;*
4. *Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť;*
5. *Posílit datovou integraci přes integrační platformu;*
7. *Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby;*
8. *Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb;*
9. *Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy;*
12. *Umožnit interním uživatelům práci z prostředí domova;*
13. *Podporovat využívání služeb městského cloudu organizacemi SMB;*
14. *Rozšířit využívání centrálních aplikací podle závazných standardů;*
17. *Vytvořit moderní, společné a bezpečné ICT města.*

ICT infrastruktura města je základním předpokladem pro poskytování digitálních služeb interním uživatelům ICT služeb SMB. Aby mohla úspěšně plnit svou roli, musí být dostatečně bezpečná, odolná proti výpadkům a schopná poskytovat požadovaná data interním uživatelům ICT služeb SMB vzdáleným přístupem do aplikací podle nastavených SLA/OLA parametrů.
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 organizacím SMB využívat za výhodných ekonomických podmínek cloudové služby a centrální aplikace v souladu s požadavky eGovernmentu ČR.

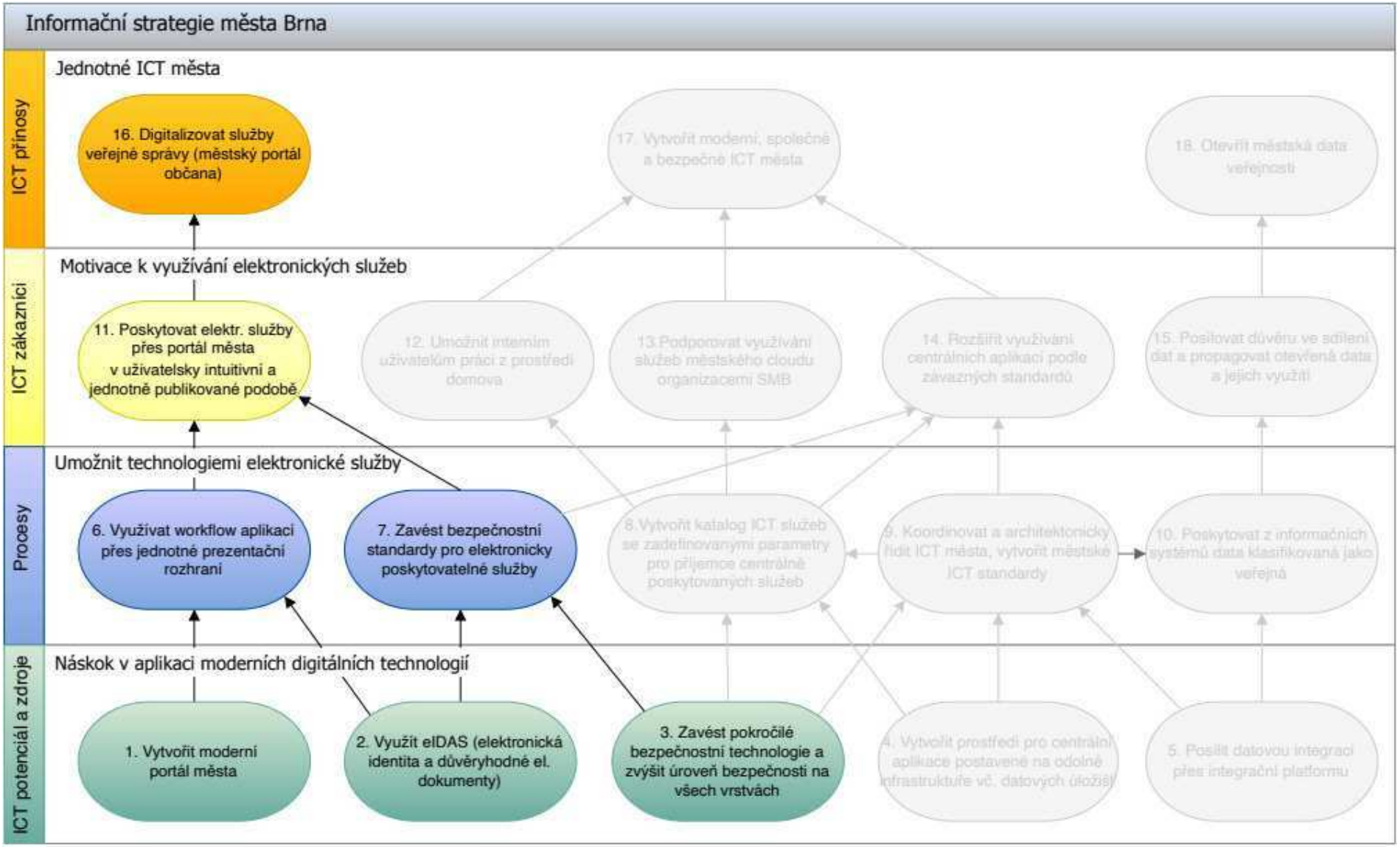
Řetězec otevřenosti městských dat

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

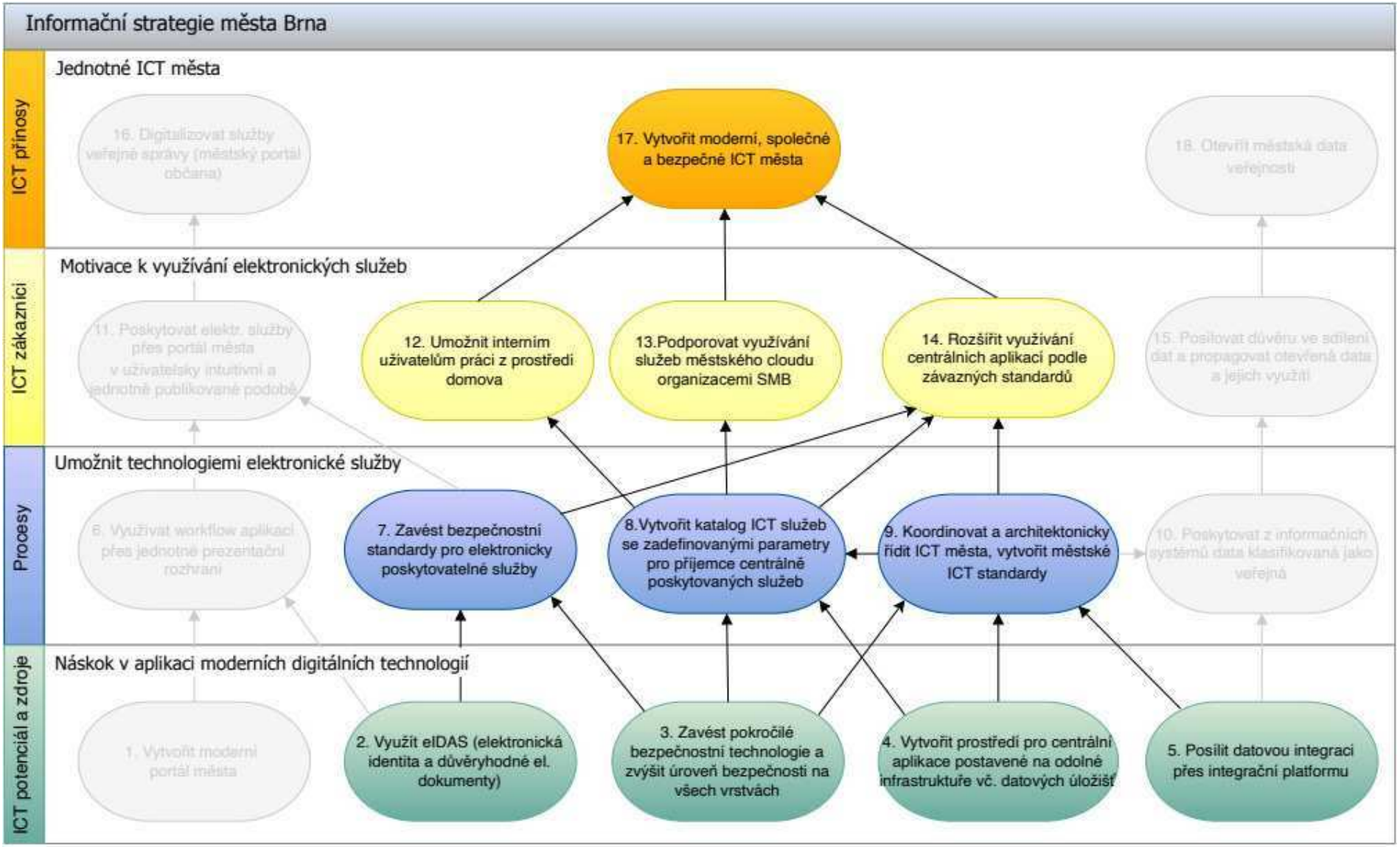
3. *Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách;*
4. *Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť;*
5. *Posílit datovou integraci přes integrační platformu;*
9. *Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy;*
10. *Poskytovat z informačních systémů data klasifikovaná jako veřejná;*
15. *Posilovat důvěru ve sdílení dat a propagovat otevřená data a jejich využití;*
18. *Otevřít městská data veřejnosti.*

Poskytování otevřených dat je založeno na uplatnění bezpečnostních technologií pro jejich poskytování z informačních systémů. 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.

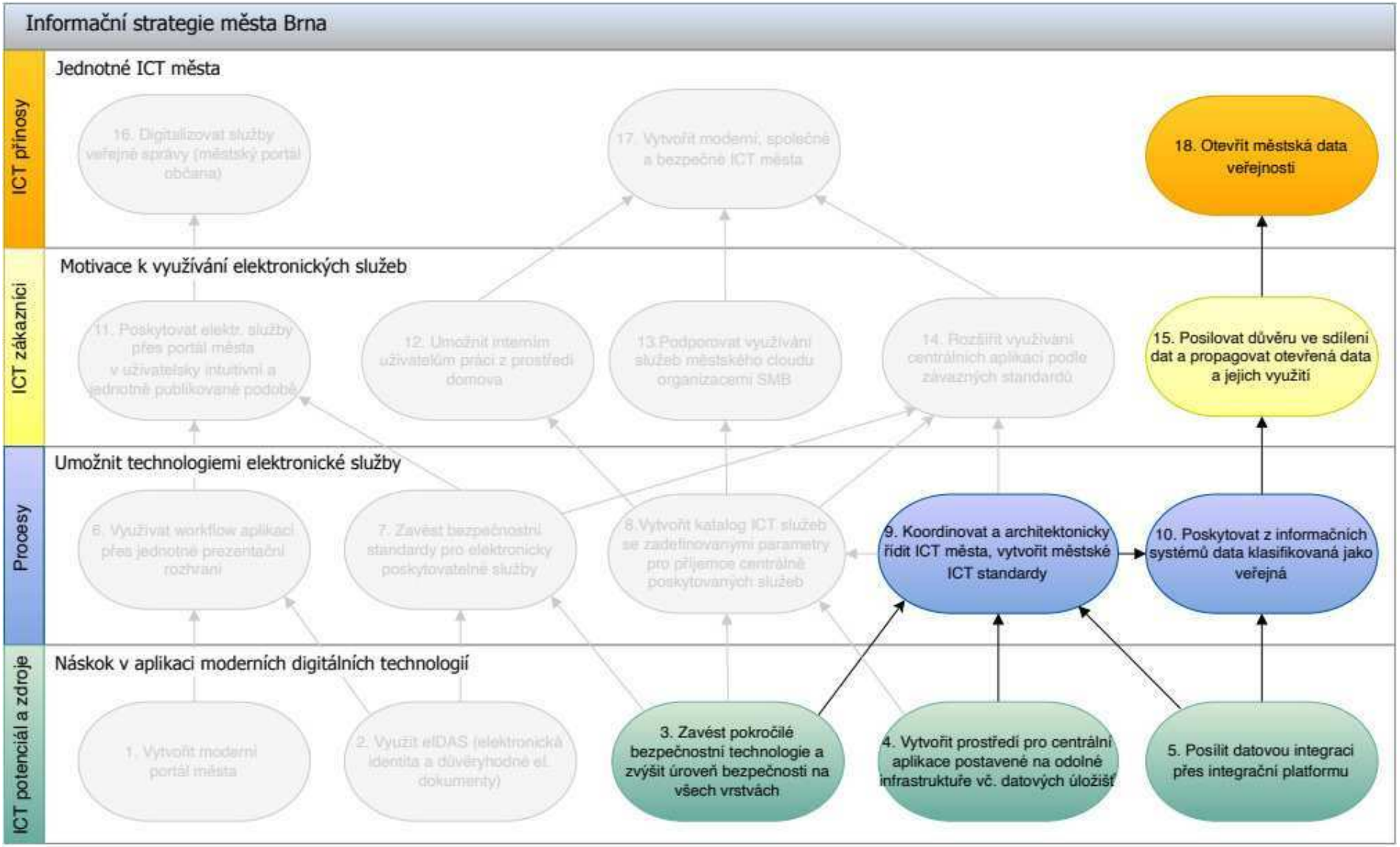
3.3.2. Řetězec digitalizace služeb



3.3.3. Řetězec ICT města



3.3.4. Řetězec otevřenosti městských 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 ICT 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 2022, 2023, 2024, 2025 a 2026.

Na dosažení vytčených strategických cílů lze tak usuzovat jak aplikací měřítka, tak přesněji také z dosažení předem stanovených cílových hodnot pro jednotlivé roky.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
1	Vytvořit moderní portál města	Technologie a bezpečnost portálu	2023 2024	Portál města má integrován centrální bod (autentizační brána IDM) pro ověření identit a jejich poskytovatelů, včetně NIA. Integrovány aplikační služby do portálu města. Součástí portálu města Brna je řešení jeho kybernetické bezpečnosti. Portál je připraven pro naplnění službami. Integrace webů MČ do webové platformy města Brna (analýza od roku 2022). Město provozuje vlastní portál v souladu s moderními technologickými a bezpečnostními standardy.
2	Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty)	Shoda s eIDAS	2022 2023	Integrace služeb IDM do informačních systémů v rozsahu SŘBI. Jsou připraveny technologie pro důvěryhodný oběh dokumentů. Vytvoření propojených identit (federace) pro účely využívání služeb MMB městskými organizacemi. Autentizační brána IDM je využívána pro potřeby aplikací/služeb města (SMB). Plné zajištění shody s požadavky eIDAS umožňující poskytovat důvěryhodné elektronické služby Úřadu.
3	Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách	Vyspělost bezpečnostního modelu města	2022 2023 2024 2025 2026	Naimplementován systém PIM/PAM. Naimplementován centrální LOG management SMB. V rozsahu MSB a na vybraných veřejných bodech SMB je nasazena a provozována centrální technologie automatizovaných detekcí zranitelností. V rozsahu MSB včetně přípojných bodů je realizován systém sdružených dozorových bezpečnostních sond, poskytujících automatizované detekce KBU/KBI zahrnující varování reakčního týmu. Vytvořen a provozován centrální systém sběru, analýzy a interpretace událostí z různých zdrojů MSB za účelem detekce anomálií a KBI. Vytvořen a provozován centrální systém automatizované reakce na detekované a kategorizované KBI. Provozování dohledového provozního a bezpečnostního centra SOC integrujícího všechny bezpečnostní technologie SMB.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
4	Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť	Plná datová a infrastrukturní redundance	2022 2023 2024	Uvedení do plného provozu redundantní DC včetně redundantních datových linek napojených na SMB. 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. Infrastrukturní prostředí je trvale dozorováno (provozní a bezpečnostní monitoring) a vybaveno geograficky oddělenými redundantními datovými centry s plnou datovou a infrastrukturní redundancí.
5	Posílit datovou integraci přes integrační platformu	Datové a integrační vazby MMB přes integrační platformu	2022 2024 2025	Definován a nastaven Service Bus integrační platformy. Využití Service Bus pro elektronické služby městského portálu občana. Integrace dílčích aplikací podle posouzení jejich priorit. Všechny významné datové a transformační vazby na MMB jsou realizovány přes integrační platformu.
6	Využívat workflow aplikací přes jednotné prezentační rozhraní	Zavedeno workflow na portálu	2022 2023 2024	Výběr aplikace a návrh workflow na základě BPMN diagramů vytvořených na ORGO. Optimalizace workflow pilotní aplikace pro cílový stav k využití v městském portálu občana. Workflow u aplikací poskytujících služby úřadu přes portál je navrženo ve spolupráci s procesním modelováním BPMN diagramů na ORGO.
7	Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby	Bezpečnostní standardy zavedeny	2023 2024 2026	Závazné bezpečnostní standardy pro MČ. Standardy pro přidělování oprávnění / přístupů do PIM/PAM. Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro MČ. Standard připojování MČ a městských organizací do LOG managementu. Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro městské akciové společnosti a pro významné příspěvkové organizace. Úroveň bezpečnosti a důvěryhodnosti elektronicky poskytovaných služeb je periodicky hodnocena a prokazována na základě jasných metodik vyplývajících z přijatých standardů.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
8	Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb	Katalog ICT služeb vytvořen	2022 2023 2024 2025	Analyzovány požadavky na ICT služby (pro aplikace) a požadavky ve formě atributů doplněny do EA modelu. 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).
9	Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy	EA aplikována v SMB a zřizovaných organizacích města	2022 2023 2024 2026	Vytvořena směrnice a pracovní postup pro zadávání architektonických prvků do centrální evidence. Vytvořena směrnice a pracovní postup pro integraci dílčích agendových systémů. Centrální evidence obsahuje aktuální stav všech významných architektonických prvků MMB. Systémy centrálně poskytované v rámci SMB jsou zavedeny v centrální evidenci. 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. U všech nových ICT projektů je zpracován projektový záměr tak, aby splňoval architektonické principy. Požadavky z ICT projektů MMB s dopadem na architekturu jsou evidovány, analyzovány a schvalovány architektonickou komisí města pro ICT. Řízení metodami EA (Enterprise Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy. Architektura podporuje proaktivní bezpečnostní přístup v celém životním cyklu systému (od záměru až po vyřazení). Požadavky z ICT projektů SMB s dopadem na architekturu jsou evidovány, analyzovány a schvalovány architektonickou komisí města pro ICT.
10	Poskytovat z informačních systémů data klasifikovaná jako veřejná	Zveřejňování otevřených dat umožněno přes městský portál	2022 2023 2025	Otevřená data jsou zveřejňována ve standardních otevřených formátech dle MV ČR v souladu s jejich klasifikací. Zveřejňování otevřených dat z městských společností (např. polohy vozidel SAKO, obsazenost sportovišť STAREZ, BRNO ID a pípni a jeď). Jsou zpřístupněna otevřená data z agendových systémů SMB. Zdrojová data se dostávají do centrálního publikačního bodu přes integrační platformu. Publikována otevřená data od komerčních subjektů.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
11	Poskytovat elektr. služby přes portál města v uživatelsky intuitivní a jednotně publikované podobě	Životní situace řešeny elektronicky přes portál města	2022 2023 až 2025 2026	Pilotní prověření vyřizování vybrané životní situace na portálu města. Nasazení služeb pro vyřizování zvolených životních situací na portál města, vybrané aplikace jsou zpřístupněny v městském portálu občana. Možnost sledování průběhu procesu vyřizování životní situace občanem. Vytvoření datové analytiky pro zrychlení průběhu procesů a zvýšení kontextové informovanosti o procesu a jeho transparentnosti.
12	Umožnit interním uživatelům práci z prostředí domova	Interním uživatelům je umožněn vzdálený přístup do aplikací SMB	2022 2023	Pro interní uživatele ICT služeb SMB je umožněno využívat aplikace vzdáleným přístupem podle nastavených SLA/OLA parametrů. Vyhodnocení zkušeností z provozu se vzdáleným přístupem a na základě toho případné dopady do technologií.
13	Podporovat využívání služeb městského cloudu organizacemi SMB	Městské cloudové služby využívány městskými firmami	2022 2024 2026	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 (objednávkový portál cloudových služeb). Přístup ke službám městského cloudu je zajištěn pro všechny organizace SMB.
14	Rozšířit využívání centrálních aplikací podle závazných standardů	ICT služby poskytované SMB standardizovány	2022 2023 2024 2025	Vytvořen standard týkající se bezpečnosti technických aktiv. 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. Městský cloud je ve shodě s eGC ČR a jsou zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...). Úplné dokončení technologického standardu. Centrálně poskytované aplikace budou ve shodě s eGC ČR a město bude mít zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...). Jsou využívány a udržovány technologické, architektonické a bezpečnostní standardy ICT SMB.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
15	Posilovat důvěru ve sdílení dat a propagovat otevřená data a jejich využití	Otevřená data certifikována	2022 2023 2025	Je vytvořen systém (definován proces) pro prokazování důvěryhodnosti dat. Všechna otevřená data poskytovaná elektronicky přes městský datový portál jsou zabezpečena a nesou informaci o jejich důvěryhodnosti v souladu se systémem prokazování důvěryhodnosti dat. Je podporováno využití otevřených dat z agendových systémů přístupných v pseudoreálném čase.
16	Digitalizovat služby veřejné správy (městský portál občana)	Očekávané přínosy z elektronizace služeb dosaženy	2022 2023 2025 2026	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. Město disponuje elektronicky poskytovanými službami pro všechny zvolené životní situace. Vyhodnoceny přínosy z digitalizovaných služeb řešících životní situace občanů.
17	Vytvořit moderní, společné a bezpečné ICT města	ICT města sdíleno	2024 2025 2026	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, městských firem a organizací. Infrastruktura poskytuje maximálně efektivní elektronické služby a její bezpečnost je zajištěna na pokročilé úrovni. Celá infrastruktura je dozorována na více úrovních za účelem zajišťování vysoké důvěryhodnosti.
18	Otevřít městská data veřejnosti	Přístup veřejnosti k datům umožněn	2022 2023 2024 2025 2026	Jsou uplatňovány postupy pro zjišťování potřeb veřejnosti z hlediska otevřených dat. Provedena analýza potřeb poskytování otevřených dat z agendových systémů. Analýza zahrnuje bezpečnostní, procesní a systémovou perspektivu, které poskytují komplexní náhled na problematiku zveřejnitelnosti konkrétních kategorií městských dat. Senzorické data z městských společností jsou automaticky publikována jako open data. Zahájení procesu zveřejňování otevřených dat z agendových systémů MMB. Všechna otevřená data poskytovaná z MMB přes datový 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 ICT projekty

Na pokrytí 18 strategických cílů byly navrženy následující strategické ICT projekty:

1.	Webová platforma města Brna
2.	Portál občana Brna
3.	Služby autentikace podle eIDAS
4.	Zajištění odolnosti
5.	Zavedení dohledových a reaktivních technologií
6.	Městský cloud
7.	Centrální služby a aplikace, služby a aplikace v cloudu
8.	Koordinace, standardizace a architektura
9.	Otevřená data

U každého strategického 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 samostatné projekty či jejich podprojekty, zejména pokud budou realizovány dodavatelsky.

4.2.1. Webová platforma města Brna

Účel strategického projektu:

Přínosový cíl 16. *Digitalizovat služby veřejné správy (městský portál občana)*.

Cíle strategického projektu:

1	Vytvořit moderní portál města	2023 2024	Portál města má integrován centrální bod (autentizační brána IDM) pro ověření identit a jejich poskytovatelů, včetně NIA. Integrovány aplikační služby do portálu města. Součástí portálu města Brna je řešení jeho kybernetické bezpečnosti. Portál je připraven pro naplnění službami. Integrace webů MČ do webové platformy města Brna (analýza od roku 2022). Město provozuje vlastní portál v souladu s moderními technologickými a bezpečnostními standardy.

4.2.2. Portál občana Brna

Účel strategického projektu:

Přínosový cíl 16. *Digitalizovat služby veřejné správy (městský portál občana)*.

Cíle strategického projektu:

5	Posílit datovou integraci přes integrační platformu	2022	Využití Service Bus pro elektronické služby městského portálu občana.
6	Využívat workflow aplikací přes jednotné prezentační rozhraní	2022 2023 2024	Výběr aplikace a návrh workflow na základě BPMN diagramů vytvořených na ORGO. Optimalizace workflow pilotní aplikace pro cílový stav k využití v městském portálu občana. Workflow u aplikací poskytujících služby úřadu přes portál je navrženo ve spolupráci s procesním modelováním BPMN diagramů na ORGO.

11	Poskytovat elektr. služby přes portál města v uživatelsky intuitivní a jednotně publikované podobě	2022 2023 až 2025 2026	Pilotní prověření vyřizování vybrané životní situace na portálu města. Nasazení služeb pro vyřizování zvolených životních situací na portál města, vybrané aplikace jsou zpřístupněny v městském portálu občana. Možnost sledování průběhu procesu vyřizování životní situace občanem. Vytvoření datové analytiky pro zrychlení průběhu procesů a zvýšení kontextové informovanosti o procesu a jeho transparentnosti.

4.2.3. Služby autentikace podle eIDAS

Účel strategického projektu:

Přínosový cíl 16. *Digitalizovat služby veřejné správy (městský portál občana)*.
Přínosový cíl 17. *Vytvořit moderní, společné a bezpečné ICT města.*

Cíle strategického projektu:

2	Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty)	2022 2023	Integrace služeb IDM do informačních systémů v rozsahu SŘBI. Jsou připraveny technologie pro důvěryhodný oběh dokumentů. Vytvoření propojených identit (federace) pro účely využívání služeb MMB městskými organizacemi. Autentizační brána IDM je využívána pro potřeby aplikací/služeb města (SMB). Plné zajištění shody s požadavky eIDAS umožňující poskytovat důvěryhodné elektronické služby Úřadu.

4.2.4. Zajištění odolnosti

Účel strategického projektu:

Přínosový cíl 17. *Vytvořit moderní, společné a bezpečné ICT města.*

Cíle strategického projektu:

4	Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť	2022 2023 2024	Uvedení do plného provozu redundantní DC včetně redundantních datových linek napojených na SMB. Zahájení poskytování služeb ve formě MSSP (managed security service provider). Infrastrukturní prostředí je trvale dozorováno (provozní a bezpečnostní monitoring) a vybaveno geograficky oddělenými redundantními datovými centry s plnou datovou a infrastrukturní redundancí.
7	Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby	2023 2024 2026	Závazné bezpečnostní standardy pro MČ. Standardy pro přidělování oprávnění / přístupů do PIM/PAM. Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro MČ. Standard připojování MČ a městských organizací do LOG managementu. Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro městské akciové společnosti a pro významné příspěvkové organizace. Úroveň bezpečnosti a důvěryhodnosti elektronicky poskytovaných služeb je periodicky hodnocena a

			prokazována na základě jasných metodik vyplývajících z přijatých standardů.

4.2.5. Zavedení dohledových a reaktivních technologií

Účel strategického projektu:

Přínosový cíl 16. *Digitalizovat služby veřejné správy (městský portál občana)*.
Přínosový cíl 17. *Vytvořit moderní, společné a bezpečné ICT města.*

Cíle strategického projektu:

3	Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách	2022 2023 2024 2025 2026	Naimplementován systém PIM/PAM. Naimplementován centrální LOG management SMB. V rozsahu MSB a na vybraných veřejných bodech SMB je nasazena a provozována centrální technologie automatizovaných detekcí zranitelností. V rozsahu MSB včetně přípojných bodů je realizován systém sdružených dozorových bezpečnostních sond, poskytujících automatizované detekce KBU/KBI zahrnující varování reakčního týmu. Vytvořen a provozován centrální systém sběru, analýzy a interpretace událostí z různých zdrojů MSB za účelem detekce anomálií a KBI. Vytvořen a provozován centrální systém automatizované reakce na detekované a kategorizované KBI. Provozování dohledového provozního a bezpečnostního centra SOC integrujícího všechny bezpečnostní technologie SMB.

4.2.6. Městský cloud

Účel strategického projektu:

Přínosový cíl 17. *Vytvořit moderní, společné a bezpečné ICT města*.

Cíle strategického projektu:

4	Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť	2023	Rozšiřování služeb městského cloudu o služby pro eIDAS.
8	Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb	2023	Registrace služeb městského cloudu v eGC (eGovernment cloud).
13	Podporovat využívání služeb městského cloudu organizacemi SMB	2022 2024 2026	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 (objednávkový portál cloudových služeb). Přístup ke službám městského cloudu je zajištěn pro všechny organizace SMB.

4.2.7. Centrální služby a aplikace, služby a aplikace v cloudu

Účel strategického projektu:

Přínosový cíl 17. *Vytvořit moderní, společné a bezpečné ICT města*.

Cíle strategického projektu:

4	Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť	2022	Poskytování zabezpečeného vzdáleného přístupu do SMB infrastruktury organizacím SMB.
8	Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb	2022 2023 2024 2025	Analyzovány požadavky na ICT služby (pro aplikace) a požadavky ve formě atributů doplněny do EA modelu. Vytvoření pilotního katalogu ICT služeb. 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	Umožnit interním uživatelům práci z prostředí domova	2022 2023	Pro interní uživatele ICT služeb SMB je umožněno využívat aplikace vzdáleným přístupem podle nastavených SLA/OLA parametrů. Vyhodnocení zkušeností z provozu se vzdáleným přístupem a na základě toho případné dopady do technologií.

4.2.8. Koordinace, standardizace a architektura

Účel strategického projektu:

Přínosový cíl 17. *Vytvořit moderní, společné a bezpečné ICT města*.
Přínosový cíl 18. *Otevřít městská data veřejnosti*.

Cíle strategického projektu:

5	Posílit datovou integraci přes integrační platformu	2022 2024 2025	Definován a nastaven Service Bus integrační platformy. Integrace dílčích aplikací podle posouzení jejich priorit. Všechny významné datové a transformační vazby na MMB jsou realizovány přes integrační platformu.
9	Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy	2022 2023	Vytvořena směrnice a pracovní postup pro zadávání architektonických prvků do centrální evidence. Vytvořena směrnice a pracovní postup pro integraci dílčích agendových systémů. Centrální evidence obsahuje aktuální stav všech významných architektonických prvků MMB. Systémy centrálně poskytované v rámci SMB jsou zavedeny v centrální evidenci. 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. U všech nových ICT projektů je zpracován projektový záměr tak, aby splňoval architektonické principy.

		2024 2026	Požadavky z ICT projektů MMB s dopadem na architekturu jsou evidovány, analyzovány a schvalovány architektonickou komisí města pro ICT. Řízení metodami EA (Enterprise Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy. Architektura podporuje proaktivní bezpečnostní přístup v celém životním cyklu systému (od záměru až po vyřazení). Požadavky z ICT projektů SMB s dopadem na architekturu jsou evidovány, analyzovány a schvalovány architektonickou komisí města pro ICT.
14	Rozšířit využívání centrálních aplikací podle závazných standardů	2022 2023 2024 2025	Vytvořen standard týkající se bezpečnosti technických aktiv. 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. Městský cloud je ve shodě s eGC ČR a jsou zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...). Úplné dokončení technologického standardu. Centrálně poskytované aplikace budou ve shodě s eGC ČR a město bude mít zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...). Jsou využívány a udržovány technologické, architektonické a bezpečnostní standardy ICT SMB.

4.2.9. Otevřená data

Účel strategického projektu:

Přínosový cíl 18. *Otevřít městská data veřejnosti*.

Cíle strategického projektu:

10	Poskytovat z informačních systémů data klasifikovaná jako veřejná	2022 2023 2025	Otevřená data jsou zveřejňována ve standardních otevřených formátech dle MV ČR v souladu s jejich klasifikací. Zveřejňování otevřených dat z městských společností (např. polohy vozidel SAKO, obsazenost sportovišť STAREZ, BRNO ID a pípni a jeď). Jsou zpřístupněna otevřená data z agendových systémů SMB. Zdrojová data se dostávají do centrálního publikačního bodu přes integrační platformu. Publikována otevřená data od komerčních subjektů.

15	Posilovat důvěru ve sdílení dat a propagovat otevřená data a jejich využití	2022 2023 2025	Je vytvořen systém (definován proces) pro prokazování důvěryhodnosti dat. Všechna otevřená data poskytovaná elektronicky přes městský datový portál jsou zabezpečena a nesou informaci o jejich důvěryhodnosti v souladu se systémem prokazování důvěryhodnosti dat. Je podporováno využití otevřených dat z agendových systémů přístupných v pseudoreálném čase.

4.3. Harmonogram strategických projektů

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

Strategické projekty		2022	2023	2024	2025	2026
Cíl	**Webová platforma města Brna**					
1	Portál města má integrován centrální bod (autentizační brána IDM) pro ověření identit a jejich poskytovatelů, včetně NIA.					
1	Integrovány aplikační služby do portálu města.					
1	Součástí portálu města Brna je řešení jeho kybernetické bezpečnosti.					
1	Portál je připraven pro naplnění službami.					
1	Integrace webů MČ do webové platformy města Brna (analýza od roku 2022).					
1	Město provozuje vlastní portál v souladu s moderními technologickými a bezpečnostními standardy.					
Cíl	**Portál občana Brna**					
5	Využití Service Bus pro elektronické služby městského portálu občana.					
6	Výběr aplikace a návrh workflow na základě BPMN diagramů vytvořených na ORGO.					
6	Optimalizace workflow pilotní aplikace pro cílový stav k využití v městském portálu občana.					
6	Workflow u aplikací poskytujících služby úřadu přes portál je navrženo ve spolupráci s procesním modelováním BPMN diagramů na ORGO.					
11	Pilotní prověření vyřizování vybrané životní situace na portálu města.					
11	Nasazení služeb pro vyřizování zvolených životních situací na portál města, vybrané aplikace jsou zpřístupněny v městském portálu občana.					
11	Možnost sledování průběhu procesu vyřizování životní situace občanem.					
11	Vytvoření datové analytiky pro zrychlení průběhu procesů a zvýšení kontextové informovanosti o procesu a jeho transparentnosti.					
Cíl	**Služby autentikace podle eIDAS**					
2	Integrace služeb IDM do informačních systémů v rozsahu SŘBI.					
2	Jsou připraveny technologie pro důvěryhodný oběh dokumentů.					

Strategické projekty		2022	2023	2024	2025	2026
2	Vytvoření propojených identit (federace) pro účely využívání služeb MMB městskými organizacemi.					
2	Autentizační brána IDM je využívána pro potřeby aplikací/služeb města (SMB).					
2	Plné zajištění shody s požadavky eIDAS umožňující poskytovat důvěryhodné elektronické služby Úřadu.					
Cíl	**Zajištění odolnosti**					
4	Uvedení do plného provozu redundantní DC včetně redundantních datových linek napojených na SMB.					
4	Zahájení poskytování služeb ve formě MSSP (managed security service provider).					
4	Infrastrukturní prostředí je trvale dozorováno (provozní a bezpečnostní monitoring) a vybaveno geograficky oddělenými redundantními datovými centry s plnou datovou a infrastrukturní redundancí.					
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.					
7	Standard připojování MČ a městských organizací do LOG managementu.					
7	Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro městské akciové společnosti a pro významné příspěvkové organizace.					
7	Úroveň bezpečnosti a důvěryhodnosti elektronicky poskytovaných služeb je periodicky hodnocena a prokazována na základě jasných metodik vyplývajících z přijatých standardů.					
Cíl	**Zavedení dohledových a reaktivních technologií**					
3	Naimplementován systém PIM/PAM.					
3	Naimplementován centrální LOG management SMB.					
3	V rozsahu MSB a na vybraných veřejných bodech SMB je nasazena a provozována centrální technologie automatizovaných detekcí zranitelností.					
3	V rozsahu MSB včetně přípojných bodů je realizován systém sdružených dozorových bezpečnostních sond, poskytujících automatizované detekce KBU/KBI zahrnující varování reakčního týmu.					
3	Vytvořen a provozován centrální systém sběru, analýzy a interpretace událostí z různých zdrojů MSB za účelem detekce anomálií a KBI.					

Strategické projekty		2022	2023	2024	2025	2026
3	Vytvořen a provozován centrální systém automatizované reakce na detekované a kategorizované KBI.					
3	Provozování dohledového provozního a bezpečnostního centra SOC integrujícího všechny bezpečnostní technologie SMB.					
Cíl	**Městský cloud**					
4	Rozšiřování služeb městského cloudu o služby pro eIDAS.					
8	Registrace služeb městského cloudu v eGC (eGovernment cloud).					
13	Městské cloudové služby (zálohování, úložiště, bezpečnost) jsou poskytovány za výhodných ekonomických podmínek z pozice jednotlivých městských firem obtížně dosažitelných a na profesionální úrovni.					
13	Portál umožňuje objednávání služeb městského cloudu (objednávkový portál cloudových služeb).					
13	Přístup ke službám městského cloudu je zajištěn pro všechny organizace SMB.					
Cíl	**Centrální služby a aplikace, služby a aplikace v cloudu**					
4	Poskytování zabezpečeného vzdáleného přístupu do SMB infrastruktury organizacím SMB.					
8	Analyzovány požadavky na ICT služby (pro aplikace) a požadavky ve formě atributů doplněny do EA modelu.					
8	Vytvoření pilotního katalogu ICT služeb.					
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	Pro interní uživatele ICT služeb SMB je umožněno využívat aplikace vzdáleným přístupem podle nastavených SLA/ OLA parametrů.					
12	Vyhodnocení zkušeností z provozu se vzdáleným přístupem a na základě toho případné dopady do technologií.					
Cíl	**Koordinace, standardizace a architektura**					
5	Definován a nastaven Service Bus integrační platformy.					
5	Integrace dílčích aplikací podle posouzení jejich priorit.					

Strategické projekty		2022	2023	2024	2025	2026
5	Všechny významné datové a transformační vazby na MMB jsou realizovány přes integrační platformu.				■	
9	Vytvořena směrnice a pracovní postup pro zadávání architektonických prvků do centrální evidence.	■				
9	Vytvořena směrnice a pracovní postup pro integraci dílčích agendových systémů.	■				
9	Centrální evidence obsahuje aktuální stav všech významných architektonických prvků MMB.	■				
9	Systémy centrálně poskytované v rámci SMB jsou zavedeny v centrální evidenci.	■				
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	U všech nových ICT projektů je zpracován projektový záměr tak, aby splňoval architektonické principy.		■			
9	Požadavky z ICT projektů MMB s dopadem na architekturu jsou evidovány, analyzovány a schvalovány architektonickou komisí města pro ICT.		■			
9	Řízení metodami EA (Enterprise Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy.		■			
9	Architektura podporuje proaktivní bezpečnostní přístup v celém životním cyklu systému (od záměru až po vyřazení).			■		
9	Požadavky z ICT projektů SMB s dopadem na architekturu jsou evidovány, analyzovány a schvalovány architektonickou komisí města pro ICT.					■
14	Vytvořen standard týkající se bezpečnosti technických aktiv.	■				
14	Navržena struktura technologického standardu (jako základní technologický rámec s možností jeho využití ve výběrových řízeních) s vazbou na architektonické principy.		■			
14	Propojení architektonického řízení s konfiguračním managementem (GPC databáze).		■			
14	Naplnění struktury technologického standardu v prioritních částech.		■			
14	Městský cloud je ve shodě s eGC ČR a jsou zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...).		■			
14	Úplné dokončení technologického standardu.			■		

Strategické projekty		2022	2023	2024	2025	2026
14	Centrálně poskytované aplikace budou ve shodě s eGC ČR a město bude mít zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...). Jsou využívány a udržovány technologické, architektonické a bezpečnostní standardy ICT SMB.					
Cíl	**Otevřená data**					
10	Otevřená data jsou zveřejňována ve standardních otevřených formátech dle MV ČR v souladu s jejich klasifikací.					
10	Zveřejňování otevřených dat z městských společností (např. polohy vozidel SAKO, obsazenost sportovišť STAREZ, BRNO ID a pípni a jeď).					
10	Jsou zpřístupněna otevřená data z agendových systémů SMB. Zdrojová data se dostávají do centrálního publikačního bodu přes integrační platformu.					
10	Publikována otevřená data od komerčních subjektů.					
15	Je vytvořen systém (definován proces) pro prokazování důvěryhodnosti dat.					
15	Všechna otevřená data poskytovaná elektronicky přes městský datový portál jsou zabezpečena a nesou informaci o jejich důvěryhodnosti v souladu se systémem prokazování důvěryhodnosti dat.					
15	Je podporováno využití otevřených dat z agendových systémů přístupných v pseudoreálném čase.					

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 ICT projektů se tak stává základním nástrojem pro sledování plnění informační strategie.

Portfolio strategických ICT 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 ICT projektů	1 x kvartálně Při vzniku výjimečné situace na některém ze strategických projektů	Hlášení o stavu portfolia strategických ICT projektů