Z9/27. zasedání Zastupitelstva města Brna
konané dne 10.6.2025

16. Návrh aktualizace Informační strategie města Brna na období 2025 - 2029

Anotace

Informační strategie města Brna byla zpracována pro období let 2025 – 2029 jako strategický dokument, který je návrhem postupu k dosažení cílového stavu informatiky města Brna do horizontu konce roku 2029. Informační strategie rozpracovává cíl strategie pro Brno, rozvíjení informačního systému v rámci Magistrátu města Brna a městských částí, do systému 19 vzájemně provázaných strategických cílů.

Návrh usnesení

Zastupitelstvo města Brna

1. schvaluje aktualizaci Informační strategie města Brna na období 2025 - 2029, která tvoří přílohu č. … tohoto zápisu

2. ukládá Radě města Brna

- naplňovat jednotlivé cíle obsažené v Informační strategii města Brna na období 2025 - 2029
T: průběžně

- předkládat Zastupitelstvu města Brna ke schválení aktualizace Informační strategie města Brna na období 2025 - 2029
T: jedenkrát za dva roky

Stanoviska

Rada města Brna projednala na své schůzi R9/128 konané dne 23. 4. 2025 a **doporučila** ZMB ke schválení.

Podpis zpracovatele pro archivaci

Zpracovatel

Elektronicky podepsáno
Ing. David Menšík
vedoucí odboru - Odbor městské informatiky
2.5.2025 v 07:01
Garance správnosti, zákonnosti materiálu

Spolupodepisovatel

Elektronicky podepsáno

Mgr. Radek Řeřicha

vedoucí úseku - 4. úsek

2.5.2025 v 07:27

Obsah materiálu

Důvodová zpráva:

Rada města Brna předkládá Zastupitelstvu města Brna dokument Aktualizace Informační strategie města Brna na období 2025 - 2029. 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 2025 – 2029 jako strategický dokument, který je návrhem postupu k dosažení cílového stavu informatiky města Brna do horizontu konce roku 2029.

Informační strategie rozpracovává cíl strategie pro Brno, rozvíjení informačního systému v rámci Magistrátu města Brna a městských částí, do systému 19 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 (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 města Vytvořit moderní, společné, bezpečné a efektivní ICT města Centrálně řídit ICT města Dosahovat soulad s digitální legislativou (compliance)
ICT zákazníci	Motivace k využívání elektronických služeb	Poskytovat elektr. služby přes webový portál služeb a mobilní aplikaci Podporovat využívání služeb městského cloudu organizacemi SMB Rozšířit využívání centrálních aplikací podle závazných standardů Zavést dlouhodobou správu služeb
Procesy	Umožnit technologiemi elektronické služby	Využívat workflow služeb přes jednotné prezentační rozhraní Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby Vytvořit katalog ICT služeb SMB se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy Koordinovat rozvoj ICT města řízením projektového portfolia Systematizovat řízení kybernetické bezpečnosti přes bezpečnostní architekturu a odolnost
ICT potenciál a zdroje	Náskok v aplikaci moderních digitálních technologií	Vytvořit mobilní aplikaci a webový portál služeb Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty) Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a kybernetické odolnosti Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace

Tab.1: Přehled strategických cílů

Podrobně jsou uvedené strategické cíle upřesněny a detailněji popsány v kapitole dokumentu číslo *3. Návrh cílového stavu*. Pro každý z cílů je stanovena metrika a jeho rozpad do stavu dosaženého v jednotlivých letech 2025 – 2029. Na tuto strukturu jsou přímo navázány návrhy strategických projektů, pomocí kterých budou cíle naplněny. V kapitole *4. Plán implementace strategie* jsou projekty rozpracovány do aktualizované 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 jedenkrát za dva roky, případně při změně nadřazené Strategie pro Brno.

Rada města Brna projednala materiál na své schůzi R9/128 konané dne 23. 4. 2025 a doporučila ZMB ke schválení.

Schváleno jednomyslně **8 členy**.

JUDr. Vaňková	Mgr. Černý	RNDr. Chvátal Ph.D.	JUDr. Kerndl	Ing. Podivinská	Bc. Aberl	Ing. arch. Bořecký	Petr Bořecký	Ing. Kratochvíl	JUDr. Matonohová	JUDr. Oliva
----	nepř.	pro	nepř.	pro	pro	pro	pro	pro	pro	pro

Komise pro informační technologie RMB na svém 31. jednání dne 15. 4. 2025 projednala a doporučila RMB přijmout usnesení.

Hlasování:
pro-proti-zdržel se-nehlasoval: **9-0-2-0/11**

Mgr. Krásný	Slavíček	BcA. Berg	Černý	Ing. Hlaváček	Bc. Kment	Ing. Machů	Mgr. Pokorná	Mgr. Šimíček	MVDr. Trojan	Mgr. Zemek	Ing. Mejzlík	Valeš
pro	pro	pro	pro	zdržel se	xxx	pro	xxx	pro	pro	zdržel se	pro	pro

Analýza současného stavu (SWOT)

Strategické cíle (na období 2025 až 2029)

Strategická mapa (Balanced Scorecard schéma)

Implementace strategie (strategické projekty)

Informační strategie města Brna

Na období 2025 - 2029

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
5.00	27.7.2023	Per Partes	Aktualizace strategie na období 2023 až 2027	230727 Informacni strategie (SMB) v5_00
6.00	12.3.2025	Per Partes	Aktualizace strategie na období 2025 až 2029	250312 Informacni strategie (SMB) v6_00

Obsah

Úvodní shrnutí

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

Předkládaný dokument „Informační strategie města Brna“ byl vyhotoven strategickým týmem (uvedeným v kap. 1. *Základní identifikace a klíčové pojmy*) v rámci pracovních setkání konaných v měsících říjnu 2024 až březnu 2025. 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 2029. 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 v roce 2022.

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 "Informační strategie města Brna", upravující strategický rozvoj informatiky města Brna, kterým město formuluje strategické cíle a k nim navrhuje zpracovat příslušné realizační projekty v oblasti informatiky s výhledem do konce roku 2029. 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 "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 města Vytvořit moderní, společné, bezpečné a efektivní ICT města Centrálně řídit ICT města Dosahovat soulad s digitální legislativou (compliance)

Perspektiva	Motto	Cíle
ICT zákazníci	Motivace k využívání elektronických služeb	Poskytovat elektr. služby přes webový portál služeb a mobilní aplikaci Podporovat využívání služeb městského cloudu organizacemi SMB Rozšířit využívání centrálních aplikací podle závazných standardů Zavést dlouhodobou správu služeb
Procesy	Umožnit technologiemi elektronické služby	Využívat workflow služeb přes jednotné prezentační rozhraní Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby Vytvořit katalog ICT služeb SMB se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy Koordinovat rozvoj ICT města řízením projektového portfolia Systematizovat řízení kybernetické bezpečnosti přes bezpečnostní architekturu a odolnost
ICT potenciál a zdroje	Náskok v aplikaci moderních digitálních technologií	Vytvořit mobilní aplikaci a webový portál služeb Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty) Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a kybernetické odolnosti Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace

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 2025 až 2029. 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	2025	2026	2027	2028	2029
Jednotná aplikace města Brna / JAMB (Webová a mobilní platforma města Brna)	■	■	■	■	■
Digitální služby města Brna (přes JAMB)	■	■	■	■	■
Služby autentikace podle eIDAS	■	■			
Systematizace řízení kybernetické bezpečnosti	■	■	■	■	■
Zajištění odolnosti	■				
Zavedení dohledových a reaktivních technologií	■	■	■		
Centrální služby a aplikace, služby a aplikace v cloudu	■	■	■		
Koordinace, standardizace a architektura	■	■	■		
Systém řízení projektového portfolia	■	■	■		

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 za 2 roky 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:

Tomáš Aberl	radní pro informatiku a sport
Vladan Krásný	předseda Komise informačních technologií
David Slavíček	člen Komise informačních technologií
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 KB, Kancelář kybernetické bezpečnosti
Kristýna Bukalová	architekt kybernetické bezpečnosti, Kancelář kybernetické bezpečnosti
Rostislav Obrlík	vedoucí Úseku tajemníka
Iveta Štarhová	Odbor strategického rozvoje a spolupráce
Michal Jukl	ředitel ICT, TSB
Jan Zachoval	podniková architektura, Aricoma Systems, a. s.
Jiří Michálek	solution manager, EPD s. r. o.
Aleš Mejzlík	zástupce za odbornou veřejnost, Komise informačních technologií

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.

Právní podpora:

David Mareš	MT Legal s.r.o.
Stanislav Mozgva	MT Legal s.r.o.

Předmět:

Předmětem aktualizace informační strategie je informatika města Brna v letech 2025 až 2029.

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
- Smart city

se zohledněním existence:

- Enterprise architecture
- Městské infrastruktury SMB.

Cílem projektu bylo aktualizovat dokument Informační strategie města Brna na období 2025 - 2029. Původní dokument Informační strategie byl vydán dne 6.12.2011, jeho první aktualizace proběhla dne 7.5.2015, druhá aktualizace 1.10.2020, třetí aktualizace 23.6.2022, čtvrtá aktualizace 27.7.2023 a pátá aktualizace 12.3.2025. 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 2029
- 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.

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

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

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

  Autorský zákon představuje komplexní úpravu práva autorského a práv souvisejících s právem autorským. Zákon, kromě jiného, upravuje vztahy mezi uživateli a tvůrci autorských děl, mezi které patří také počítačové programy (např. v podobě SW, webových stránek a aplikací), databáze nebo kartografická díla (např. v podobě digitálních map). Právní úprava zde obsažená reguluje osobnostní a majetková práva autorů autorských děl, tj. zejména právo autora osobovat si autorství, právo na nedotknutelnost díla, nebo právo na rozmnožování díla, právo na rozšiřování originálu nebo rozmnoženiny díla apod.

- Zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů
- Zákon č. 240/2000 Sb., o krizovém řízení, ve znění pozdějších předpisů

- **Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů**

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

- Zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů

- **Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů**

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

- Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů

- 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,

1 **Informační systém veřejné správy** je funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy nebo plnění jiných funkcí státu anebo dalších veřejnoprávních korporací. Každý informační systém veřejné správy zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále technické a programové prostředky, případně jiné nástroje umožňující výkon informačních činností.

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

3 Za **obchodní sdělení** se považují všechny formy sdělení, včetně reklamy a vybízení k návštěvě internetových stránek, určeného k přímé či nepřímé podpoře zboží či služeb. nebo image určitého podniku osoby, která je podnikatelem nebo vykonává regulovanou činnost.

4 **Elektronickými komunikacemi** se rozumí technologie (satelitní sítě, mobilní sítě apod.) pro přepravu, přenos, nebo směrování signálů (obraz, data, telefonie) v elektronické podobě.
Elektronickým komunikačním zařízením se rozumí technické zařízení pro vysílání, přenos, směrování, spojování nebo příjem signálů prostřednictvím elektromagnetických vln.

jakož i obsah sdílený prostřednictvím internetu.

- **Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů**

  Zákoník práce je základním právním předpisem na úseku pracovního práva, který upravuje především právní vztahy mezi zaměstnavateli a zaměstnanci při výkonu závislé práce nebo v souvislosti s ním. Stanoví tedy primárně soubor základních práv a povinností smluvních stran základních pracovněprávních vztahů, kterými jsou pracovní poměr a právní vztahy založené dohodami o pracích konaných mimo pracovní poměr (dohoda o provedení práce a dohoda o pracovní činnosti). Ve vazbě na oblast informačních technologií zákoník práce mj. vymezuje rámec pro výkon práce na dálku (tzv. home office).

- **Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů**

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

- **Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů**

  Zákon **o základních registrech** je právním předpisem upravujícím, kromě jiného, obsah základních registrů[7], informačního systému základních registrů[8] a informačního systému územní identifikace a stanoví práva a povinnosti, které souvisejí s jejich vytvářením, užíváním a provozem. Smyslem a účelem právní úpravy je zakotvení základních registrů, jakožto unikátních zdrojů nejčastěji využívaných údajů při výkonu veřejné správy (referenční údaje) a zefektivnění jejich využití. Prostřednictvím informačního systému základních registrů má být zajištěno, mimo jiné, provedení identifikace a autentizace a následně i autorizace uživatelů. Informační systém základních registrů také uchovává záznamy o událostech spojených s poskytovanými službami a údaji ze základních registrů.

- Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

5 **Datovou schránkou** se v pojetí zákona rozumí elektronické úložiště, které je určeno k doručování orgány veřejné moci, provádění úkonů vůči orgánům veřejné moci a dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob.

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, který je součástí referenčního, sdíleného a bezpečného rozhraní informačních systémů veřejné správy a jehož prostřednictvím je zajišťováno sdílení údajů mezi základními registry navzájem, základními registry a agendovými informačními systémy, základními registry a soukromoprávními systémy pro využívání údajů, agendovými informačními systémy, jejichž prostřednictvím se zapisují údaje do základních registrů, a jinými agendovými informačními systémy a mezi agendovými informačními systémy, jejichž prostřednictvím se zapisují údaje do základních registrů, a soukromoprávními systémy pro využívání údajů, správa oprávnění přístupu k údajům a další činnosti podle tohoto zákona.

- **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 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

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 jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání.

11 **Elektronickou identifikací** se rozumí postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu.

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.

- Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci

Související podzákonné právní předpisy ČR:

- 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
- 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. 515/2020 Sb., o struktuře informací zveřejňovaných o povinném subjektu a o osnově popisu úkonů vykonávaných v rámci agendy
- 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
- Vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu
- Vyhláška č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy

Právní předpisy EU (platné a účinné):

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

  Nařízení Evropského parlamentu a Rady (EU) **č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu** (zkráceně eIDAS) je právním aktem Evropské unie v oblasti služeb vytvářejících důvěru, přičemž jej doplňuje již platný zákon č. 297/2016 Sb. a doprovodný zákon č. 298/2016 Sb., jakož i

12 **Digitální službou** se zde rozumí úkon vy konávaný orgánem veřejné moci vůči uživateli služby v rámci agendy a vedený v katalogu služeb jako úkon v elektronické podobě; za digitální službu se považuje i úkon vykonávaný vůči uživateli služby kontaktním místem veřejné správy v rámci agendy. Naproti tomu **digitálním úkonem** je úkon vykonávaný uživatelem služby vůči orgánu veřejné moci v rámci agendy a vedený v katalogu služeb jako úkon v elektronické podobě.

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) 2019/790 ze dne 17.dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES
- Nařízení Evropského parlamentu a Rady (EU) 2019/1150 ze dne 20. června 2019

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.

o podpoře spravedlnosti a transparentnosti pro podnikatelské uživatele online zprostředkovatelských služeb

- Směrnice Evropského parlamentu a Rady (EU) 2019/1152 ze dne 20. června 2019 o transparentních a předvídatelných pracovních podmínkách v Evropské unii
- Směrnice Evropského parlamentu a Rady (EU) 2019/1158 ze dne 20. června 2019 o rovnováze mezi pracovním a soukromým životem rodičů a pečujících osob a o zrušení směrnice Rady 2010/18/EU
- Nařízení Evropského parlamentu a Rady (EU) č. 2022/868 ze dne 30. května 2022 o evropské správě dat a o změně nařízení (EU) 2018/1724 (**akt o správě dat**)
- Nařízení Evropského parlamentu a Rady (EU) č. 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (**nařízení o digitálních službách**)
- Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice rady 2008/114/ES (**směrnice CER**)
- Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnici (EU) 2018/1972 a o zrušení 2016/1148 (**směrnice NIS 2**)
- Nařízení Evropského parlamentu a Rady (EU) 2025/38 ze dne ze dne 19. prosince 2024, kterým se stanovují opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických hrozeb a incidentů a pro připravenost a reakci na ně a mění nařízení (EU) 2021/694 (**nařízení o kybernetické solidaritě**)

Právní předpisy EU (platné, doposud neúčinné či vyžadující další transpozici):

- Nařízení Evropského parlamentu a Rady (EU) Č. 2024/1689 ze dne 13.6.2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (**akt o umělé inteligenci**)
- Nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 **(akt o kybernetické odolnosti)**

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.

Architekt kybernetické bezpečnosti (AKB) navrhuje bezpečnostní architektury informačních systémů, jejich jednotlivé komponenty, vzájemné vazby a dohlíží na soulad implementace architektury informačních systémů se systémem řízení bezpečnosti informací.

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).

Enterprise Service Bus (ESB) je centrální softwarová komponenta, která provádí integraci mezi aplikacemi.

Extract-Transform-Load (ETL) označuje proces extrakce, transformace a nahrání dat z jednoho či více zdrojů do datového skladu.

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.

Magistrát města Brna (MMB) je označení městského úřadu statutárního města Brna.

Managed service provider (poskytovatel řízené služby, MSP) je poskytovatel služeb souvisejících s instalací, správou, provozem nebo údržbou technických aktiv, a to prostřednictvím asistence nebo aktivní správy, které jsou prováděny v prostorách zákazníků nebo na dálku.

Managed security service provider (poskytovatel řízené bezpečnostní služby, 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.

Organizační odbor (ORGO) je odbor, který mj. zabezpečuje oblast organizace a řízení MMB a vzájemnou informovanost mezi MMB a úřady městských částí a ochranu informací a osobních údajů v rámci MMB (GDPR).

Orgán veřejné moci (OVM) je státní orgán, územní samosprávný celek a fyzická nebo právnická osoba, byla-li jí svěřena působnost v oblasti veřejné správy.

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.

Statutární město Brno (SMB) je město Brno, jehož vnitřní poměry ve věci správy města jsou upraveny statutem.

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.

Supervisory Control And Data Acquisition (SCADA) je systém, který z centrálního pracoviště monitoruje technická zařízení a procesy a umožňuje jejich parametrizaci.

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 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 aktivum je technický nebo programový prostředek anebo vybavení.

Technické sítě Brno (TSB) je městská 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.

Úřad městské části (ÚMČ) je úřad nejmenší správní a samosprávné jednotky SMB. Statutární město Brno je územně členěným statutárním městem a člení se na 29 městských částí (MČ).

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 2023 a 2024 v Informační strategii města Brna aktualizované v roce 2025 (verze 6.00).

1. Vytvořit mobilní aplikaci a webový portál služeb

V rámci veřejné zakázky „Tvorba a provoz webové platformy města Brna“ je provozována Webová platforma města Brna, na které je implementováno a plně v provozu 12 webů včetně webů MČ Medlánky a Bystrc, u 9 webů na produkčním prostředí je nasazován obsah a 5 webů je v testovacím prostředí. V rozpracovanosti jsou dva miniweby.

Webová Platforma má smluvně zajištěn nejen provoz, podporu, údržbu a servis, ale i rozvoj. Umožňuje ověřování identit NIA, ISDS, Brno ID, při ověřeném řešení kybernetické bezpečnosti a přístupnosti.

Byl vytvořen koncept integrace jak do webového portálu služeb, tak i do mobilní aplikace. Součástí konceptu je i řešení kybernetické bezpečnosti.

V průběhu tvorby konceptu byl iniciován strategický projekt „Jednotná aplikace města Brna“, přičemž bylo rozhodnuto, že se bude v tomto projektu řešit pouze mobilní aplikace. V současné době probíhá veřejná zakázka s předpokládanou realizací v průběhu let 2025 a 2026.

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

Integrace služeb IDM do informačních systémů v rozsahu SŘBI je rozpracována s předpokladem dokončení Q2 2025, zbývá 1 z 13-ti systémů.

Autentizační brána je připravena k nasazení, je třeba otestovat a případně upravit podle požadovaných změn – předpokládané dokončení Q2 2025, nutno harmonizovat podle požadavků nového zákona o kybernetické bezpečnosti (NZoKB). Pro zajištění zvýšené odolnosti proti kybernetickým útokům je nutný upgrade technologické platformy.

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

Byl naimplementován centrální „LOG management“, který zajišťuje jak shromažďování logů pro další technologie bezpečnostního dohledu, tak i provozní monitoring.

Součástí bezpečnostní technologie je současně sada komponent Flowmon (výkonný nástroj pro síťový monitoring, analýzu a zabezpečení) prostřednictví níž je poskytován trvalý dohled a hlášení událostí zajištěný připojením do vzdáleného Secure Operation Centra (SOC).

Nasazení a provozování centrální technologie automatizovaných detekcí zranitelností bylo odloženo na Q2 2025.

Byl implementován a nakonfigurován systém PIM/PAM.

4. Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť

TSB vytvořilo a poskytuje služby MSP/MSSP (dohled nad metropolitní sítí, služba zálohování, služba skenování zranitelností, správa antivirových řešení etc.).

Infrastrukturní prostředí smluvně spravované TSB, tedy datová centra a MSB, je trvale dosledováno bezpečnostním týmem TSB.

Obě datová centra jsou redundantně propojená včetně konektivity do internetu.

Infrastrukturní prostřední MMB včetně MSB, sestávající z více redundantních datových center, je hlídána robustním systémem sond, které mají jako součást své výbavy moduly IDS (Intrusion Detection System) a díky bezpečnému kanálu z dozorového centra (SOC) jsou schopny proaktivního zásahu v režimu 24/7.

5. Posílit zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace ICT

Referát KB vznikl jako součást odboru 4. Úseku v roce 2023, v současné době má 5 funkčních míst a je schopný zastávat všechny úkoly definované v návrhu nového zákona o kybernetické bezpečnosti (NZoKB).

Do stávajícího funkčního místa pro projektové řízení na OMI MMB byla přijata nová kolegyně.

Jedno pracovní místo pro vývoj aplikací bylo obsazeno novým kolegou, který se věnuje projektu „Jednotná aplikace města Brna“ (JAMB). Druhé pracovní místo zatím obsazeno není.

Pracovní místo pro servisní podporu infrastruktury bylo obsazeno novým kolegou.

Obsazení role Solution achitect bylo vyřešeno smluvně.

Zajištění zastupitelnosti rolí splněno přijetím a zaškolením osoby v roli bezpečnostního analytika, která má dostatečné znalosti akcí kanceláře KB, aby mohla zastupovat manažera. Role architekta KB momentálně má částečnou zastupitelnost vzhledem k propojení informací mezi architektem kybernetické bezpečnosti a enterprise architektem.

6. Využívat workflow služeb přes jednotné prezentační rozhraní

Jako pilotní služba MMB byla vybrána agenda poplatků za odvoz a likvidaci komunálního odpadu. Na optimalizaci WF pro využití v mobilní aplikaci se pracuje.

7. Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby

Byly realizovány standardy pro přidělování oprávnění, přístupů do PIM/PAM.

Připravuje se standard připojování MČ a městských organizací do LOG managementu.

Během roku 2024 byla rozhodnutím Koncernového výboru zřízena Pracovní skupina pro ICT a KB Koncernu. Byl zřízen Orgán pro architektonické řízení ICT projektů, působící na úrovni koncernu; navázána spolupráce s příspěvkovými organizacemi v oblasti KB.

Byl zaveden systém řízení kybernetické bezpečnosti dle nového zákona o kybernetické bezpečnosti, respektive direktivy NIS2 (aktualizovaná verze evropské směrnice Network and Information Security o kybernetické bezpečnosti z roku 2016). Splnění bylo potvrzeno metodickým auditem NÚKIB podle NZoKB.

8. Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb

Ve spolupráci s technickými správci byla provedena inventarizace poskytovaných ICT služeb OMI MMB a naplněn katalog ICT služeb údaji o poskytovaných ICT službách OMI MMB. Prozatím je katalog ICT služeb v podobě tabulky. V řešení je vytvoření databáze v prostředí ServiceDesku, tak aby existoval jeden zdroj informací o poskytovaných ICT službách.

Byl vytvořen a je k dispozici katalog ICT služeb poskytovaných TSB, a to ve formě tabulky a katalogových listů.

Katalog ICT služeb je dokončen a bude rozšířen o služby podle požadavků eIDAS (modul autentizační brána IDM).

TSB využívá service deskovou aplikaci a nyní dochází k implementaci interního katalogu do tohoto systému (cíl Q2/2025). V návrhu je možné nyní zohlednit požadavky SMB na strukturu a obsah katalogu.

Připravuje se zadání pro projekt jednotného katalogu ICT služeb v rozsahu SMB, městských organizací a městských firem.

9. Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy

Byla vytvořena směrnice a pracovní postup pro zadávání architektonických prvků do centrální evidence.

Byl vytvořen pracovní postup pro integraci dílčích agendových systémů vycházející z architektonického principu definovaného v rámci podnikové architektury (EA).

Systémy centrálně poskytované v rámci SMB jsou zavedeny v centrální evidenci.

Byl ustanoven Řídící orgán ICT pro řízení architektury SMB. Požadavky z ICT projektů SMB s dopadem na architekturu jsou evidovány, analyzovány a schvalovány Řídícím orgánem ICT.

Řízení metodami EA 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).

Významné ICT projekty SMB jsou evidovány a schvalovány Řídícím orgánem ICT a to s vazbou na řízení projektového portfolia.

10. Koordinovat rozvoj ICT města řízením projektového portfolia

Směrnice a pracovní postup pro zpracování projektových záměrů MMB v oblasti ICT je v realizaci.

Byl ustanoven Řídící orgán ICT pro řízení ICT SMB.

U všech nových ICT projektů MMB je zpracováván projektový záměr.

Pravidla pro klasifikaci významnosti projektů v rámci projektového portfolia města (ve fázi projektového záměru) jsou ukotvena ve statutu Řídícího orgánu ICT, v Koncernovém pokynu a v Pokynu příspěvkovým organizacím.

Nové významné projekty jsou ve fázi projektového záměru autorizovány Řídícím orgánem ICT.

11. Poskytovat elektr. služby přes webový portál služeb a mobilní aplikaci

V rámci zajišťování podkladů pro zadávací dokumentaci VZ na platební bránu byl proveden průzkum využití na jednotlivých odborech MMB. Platební brána implementována není.

Jako pilotní služba MMB byla vybrána agenda poplatků za odvoz a likvidaci komunálního odpadu. Probíhají jednání se zástupci OŽP k pilotnímu nasazení této služby.

12. Umožnit interním uživatelům práci z prostředí domova

Byly nasazeny, otestovány a jsou provozovány technologie, umožňující bezpečný vzdálený přístup včetně vícefaktorového ověření. Zkušeností z provozu se vzdáleným přístupem byly vyhodnoceny a na jejich základě byly provedeny úpravy technologií.

Bylo realizováno posílení bezpečnostních prvků pro vzdálený přístup.

13. Podporovat využívání služeb městského cloudu organizacemi SMB

TSB připravilo a již poskytuje vybrané služby KB.

Primárně jsou ICT a KB služby využívány městskými částmi a příspěvkovými organizacemi a tyto služby jsou plně ekonomicky konkurenceschopné a/nebo v konečném důsledku výhodnější.

Tyto služby jsou popsány „katalogovými listy TSB“ a v případě vytvoření objednávkového portálu MMB/SMB je TSB připraveno vložit své popsané služby do tohoto portálu.

Připravuje se zadání pro projekt jednotného katalogu ICT služeb v rozsahu SMB, městských organizací a městských firem.

14. Rozšířit využívání centrálních aplikací podle závazných standardů

Propojení architektonického řízení s konfiguračním managementem (GPC databáze) je v realizaci, probíhá kontrola dat.

Své cloudové služby TSB neregistrovalo do eGC, protože je ovládanou společností SMB, své služby nenabízí mimo struktury SMB, a tudíž je v postavení interního provozovatele. Cíl vznikl v době, kdy nebylo zcela zřejmé, jestli bude registrace nutná. V případě požadavku jsou TSB připraveny provést registraci svých služeb, ale nyní to není shledáno jako účelné.

Pokračování tvorby technologického standardu bude realizováno po personálním posílení OMI

v oblasti dokumentování ICT prostředí SMB.

15. Prohloubit spolupráci pracovníků SMB v oblasti ICT projektů a architektury

Pravidla pro klasifikaci významnosti projektů v rámci projektového portfolia města (ve fázi projektového záměru) jsou ukotvena ve statutu Řídícího orgánu ICT, v Koncernovém pokynu a v Pokynu příspěvkovým organizacím.

16. Digitalizovat služby města

Koncepčně bylo rozhodnuto, že v rámci projektu JAMB se bude řešit pouze mobilní část městské aplikace a webový portál služeb bude řešen samostatně. Proběhlo začlenění životních situací do mobilní aplikace a byla zvolena služba pro pilotní ověření.

Jako pilotní služba MMB byla vybrána agenda poplatků za odvoz a likvidaci komunálního odpadu. Pilotní ověření vybrané služby zatím neproběhlo.

17. Vytvořit moderní, společné a bezpečné ICT města

Enterprise architektura je průběžně vyvíjená záležitost, která se neváže na standardy, vznik standardů se řeší paralelně na základě hlavně legislativních požadavků.

Řeší se uplatnitelnost standardů ze strany města vůči dalším subjektům i v rámci výběrových řízení, které město vypisuje samo pro sebe.

Pro účely kybernetické bezpečnosti existuje minimální standard pro ÚMČ a bezpečnostní standardy v podobě SŘBI a interních normativních aktů, které jsou průběžně revidovány.

18. Centrálně řídit ICT města

Byl ustanoven Řídící orgán ICT pro řízení ICT SMB.

Pravidla pro klasifikaci významnosti projektů v rámci projektového portfolia města (ve fázi projektového záměru) jsou ukotvena ve statutu Řídícího orgánu ICT, v Koncernovém pokynu a v Pokynu příspěvkovým organizacím.

Nové významné projekty jsou ve fázi projektového záměru autorizovány Řídícím orgánem ICT.

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)	
4,8	Projektová kancelář OMI řídí IT projektové portfolio MMB, včetně projektů kybernetické bezpečnosti (KB).
4,7	Vznikl řídící orgán ICT ke koordinaci ICT v rámci perimetru SMB (MMB, městské části, městské firmy a příspěvkové organizace města).
4,6	Kvalifikovaní správci aplikací a ICT infrastruktury v oblasti, kterou mají ve své pracovní náplni.
4,6	Oblast informační bezpečnosti je řízena koordinátorem kybernetické bezpečnosti SMB.
4,5	Jistota prostředků na kalendářní rok v rámci schváleného rozpočtu.
4,3	Existence webové platformy města Brna.
3,9	Vysoká znalost technologických trendů a jejich zavádění.
3,8	Zvyšující se bezpečnostní povědomí mezi pracovníky OMI a rovněž pracovníky MMB.
3,7	Dosažené zkušenosti s implementací informačních systémů.
3,4	Rozdělení rozpočtových prostředků na provoz ICT a kybernetickou bezpečnost.
2,3	TSB je pověřeno koncernovým pokynem ke koordinaci ICT a KB v rámci koncernu (obchodních společností města).
Opportunities (vnější příležitosti)	
4	Maximalizovat využití čerpání prostředků z fondů EU.
4	Využití popisu procesů MMB v procesních modelech (ORGO).
4	Dlouhodobá partnerská spolupráce s NÚKIB, DIA a MV ČR.
3,8	Využití potenciálu odborníků v rámci města ve formě poradenského orgánu.
3,7	V Brně na trhu práce existují vzdělaní a kompetentní pracovníci v oblasti ICT.
3	Zapojení vysokých škol do rozvoje informatiky města Brna včetně aktivní spolupráce města při výuce studentů.
Weaknesses (vnitřní slabé stránky)	
4,7	Odměňovací systém neumožňuje získávat nové a udržet stávající pracovníky IT.
4,2	Ne všichni klíčoví uživatelé (garanti) mají dostatečné znalosti, aby definovali požadavky na informatiku (formulace toho, co chtějí). OMI nemůže suplovat metodické role uživatelů.
4	Nedostatek vnitřních odborných kapacit vzhledem k rostoucímu významu a rozvoji informatiky vede ke zvýšenému nákupu externích služeb.
3,6	Klíčové uživatele je obtížné motivovat pro spolupráci v projektových týmech týkajících se informatiky z důvodu střetu liniových a projektových struktur.
3,5	Nedostatečné povědomí klíčových uživatelů o plánovaní kapacit zdrojů OMI na pokrytí požadavků.
3,3	Neochota úředníků k využití ICT potenciálu a změn.
3,3	Nedostatečné personální zajištění obsahu a obsluhy webové platformy.
Threats (vnější hrozby)	
4,4	Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT.
4,3	Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.
4,3	Rozšiřování projektů v ICT mimo gesci OMI.
4,2	Se změnou politické reprezentace může dojít k zásadním změnám ve směrování a financování ICT.
4,1	Masivní vývoj kybernetických útoků a jejich forem.
3,8	Nárůst požadavků na dokumentaci v ICT dnes zejména v oblasti informační a kybernetické bezpečnosti.

3,7	Masivní nárůst legislativních požadavků a jejich dopady v oblasti ICT a kybernetické bezpečnosti.
3,7	Dlouhá doba od vytvoření záměru do jeho realizace způsobená interními předpisy nebo platnou legislativou.
3,5	Hrozby spojené s užíváním zařízení umístěných mimo perimetr.
3,5	Ze zadávacích řízení podle ZZVZ mohou vzejít neadekvátní dodavatelé nebo mohou zadávací řízení trvat nepredikovatelnou dobu.
3,2	Vzrůstající komplexita a regulace požadovaných technických opatření v ICT.
3,1	Narůstající význam regulace v oblasti AI (umělé inteligence).
2,9	Uživatelé pracující vzdáleně (mimo kancelář) se obracejí s lokálními ICT problémy na servisní podporu OMI mimo jeho gesci.
2,8	Narůstající význam IoT a Scada prvků zvyšující míru rizik v rámci SMB.
2,7	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)	
4,8	Je zřízena samostatná role bezpečnostního architekta a solution architekta. Bezpečnostní architektura je provázána na EA MMB.
4,7	Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ).
4,7	Validní informace o EA MMB jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.
4,5	Architektura pro integrace aplikací - integrační platforma (s využitím principů ESB a ETL).
4,5	Rada města Brna vydala minimální standard kybernetické bezpečnosti pro MČ, jehož dodržování je závazné.
4,4	Efektivní licencování pro základní části městského AIS a office SW.
4,4	Kvalitní komunikační infrastruktura připojení ÚMČ.
4,4	V rámci SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) se zajištěnou ochranou proti jejich ztrátě.
3,9	Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy.
3,9	Rozšíření služeb provozovaných z městského cloudu pro všechny městské subjekty SMB.
3,8	Jsou k dispozici opakovatelně použitelné architektonické stavební bloky pro využití aplikacemi SMB (např. NIA Proxy, ISZR Proxy).
3,8	Kvalitní prostory a technologické zázemí pro umístění uzlových ICT prvků (datové centrum).
Opportunities (vnější příležitosti)	
4,7	Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.
4,6	Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).
4,3	Vytvoření a správa katalogu služeb ICT SMB.
4,2	Nasazení systému pro sledování visibility strategických služeb poskytovaných SMB.
4,1	Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy).
4,1	Vydání IT směrnic závazných pro SMB.

3,8	Větší využití ETL Clover pro datovou integraci systémů.
3,8	Vytvoření kompetenčního modelu v rámci týmu včasné reakce SŘBI pro případy havarijních a krizových stavů.
3,7	Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu.
3,7	Propojení konfiguračních databází udržovaných MMB a samostatně dodavateli/správci částí infrastruktury.
3,7	Vytvoření prioritizace cca 350 aplikací a odstupňovaný přístup k nim podle jejich priorit.
3,6	Metodická pomoc kompetenčního centra uživatelům z ÚMČ a organizací města.
3,5	Popsání definice vazeb mezi projekty a sesouladění postupů – road-mapa na období několika let s pravidelnou aktualizací.
3,3	Vytvoření centrálního přístupového bodu pro řízený přístup uživatelů do IS města a k aplikacím z různých platforem.
3,1	Je k dispozici prostředí (framework) pro tvorbu jednoduché podpory procesů a workflow v nich (MOSS - MS Office SharePoint Services) s komunitou uživatelů.
3	Vytvořit prostředí pro drobné aplikace odborných útvarů SMB.
3	Zvyšující se zájem stakeholderů o přístup k informacím z EA modelu.
2,9	Využití Národního architektonického plánu s návrhovými vzory vybraných oblastí.
2,7	Využití externích kapacit výzkumu a vývoje pro oponenturu rozvojových koncepčních plánů a projektů (CERIT, NUKIB, Útvar hlavního architekta eGov, DIA ...).
Weaknesses (vnitřní slabé stránky)	
4,4	Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti.
4,3	Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).
4,3	Řada aplikací nemá dokumentaci.
4	Neexistuje provozní konfigurační management na datové a aplikační vrstvě.
3,9	Chybí vazba na business vrstvu zpracovávanou ORGO v BPMN diagramech.
3,8	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).
3,8	IDM nemá zadefinované role z business vrstvy (není propojení až do procesní business vrstvy a její rozpracování na role).
3,7	Model EA zahrnuje jen MMB a absentují organizace SMB.
3,7	Platformová technologická roztříštěnost (např. různé db stroje).
3,7	Nedobudována geograficky oddělená záložní infrastruktura.
3,6	Používání zastaralých aplikací neintegrovatelných či vyžadujících výjimky z koncepce pro integraci systémů.
3,6	Nedostatečná aplikace principů procesního řízení.
3,4	Ne všechna data jsou ukládána do datových úložišť ve strukturované podobě, která umožní řízení přístupu dle oprávnění.
3,2	Závislost rozvoje ICT architektury na přidělených prostředcích (rozpočtu).
2,9	Městské firmy si spravují vlastní podružná menší datová centra i aplikace bez vazby na EA.
2,5	Plánování a využití kapacit všech zdrojů v souladu s požadavky vykonávaných procesů.
Threats (vnější hrozby)	
4,6	Legislativní změny vyžadující podrobnější popis systémů (procesy, architektura, bezpečnost, ...).
4,3	Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24.
4,2	Konfliktní požadavky změn legislativy s dopadem do informačních systémů.
4,1	Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.

3,7	Organizační změny posilující přístup k aplikacím z vnějšího prostředí vyvolají problémy s licencemi a technologiemi.
3,6	EA model obsahuje koncentrované informace a při neoprávněném přístupu k nim jde o bezpečnostní riziko.
3,5	Nedostatečná pozornost ze strany tvůrců prvků celostátního eGovernment, věnovaná specifickým potřebám statutárních měst.
3,2	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	Nedostatečnost kapacity komunikační infrastruktury pro nové služby nabízené z internetu (např. video streaming, práce s 3D modely).
2,8	Licenční a technologická závislost na dodavateli (vendor lock-in).
2,6	Vynucená koordinace s podřízenými organizacemi z hlediska regulovaných služeb poskytovaných ve sdílené infrastruktuře ve formě podpůrných aktiv.

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)	
4,8	Koordinace ICT projektů městských subjektů (Řídící orgán ICT).
4,8	Dlouhodobé strategické řízení informatiky.
4,7	Člen RMB pro oblast informatiky.
4,5	SMB má statut a může v rámci něj prosadit cíle v IT jak na MMB, tak i na ÚMČ (čl. 39 a 40).
4,4	Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.
4,3	Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb.
4,3	Vysoká úroveň řízení kybernetické bezpečnosti.
4,1	Geografický informační systém přístupný pro občany, organizace, úřady SMB.
4	Poskytování vybraných veřejných služeb přes internet.
4	Sjednocené a vybudované prostředí pro výkon veřejné správy.
4	Digitalizace vnitřních procesů řízení města (eMMB).
3,8	Řízené zpřístupňování dat interním i externím uživatelům.
3,7	Spolupráce se státní správou v oblasti kybernetické bezpečnosti.
3,2	Poskytování služeb založených společností a zřízených organizací městem přes internet.
3,1	Jsou vytvořeny specializované subjekty města k poskytování specifických ICT služeb.
Opportunities (vnější příležitosti)	
4,6	Sjednocení komunikace nabízených služeb SMB občanům přes centrální aplikaci.
4,6	Naplnění nové webové platformy města.
4	Využívání standardizovaných IT produktů poskytovaných na celostátní úrovni.
4	Spolupráce s jinými městy v ČR a EU.
3,9	Využití možností spolufinancování nových služeb z externích zdrojů.
3,7	Definice zákazníka ICT služeb a jeho potřeb.
3,6	Využití potenciálu umělé inteligence pro zefektivnění interních i externích procesů.
3,3	Zintenzivnění spolupráce se středními a vysokými školami (využití jejich potenciálu).

3,1	Využití aktivit v rámci externích subjektů ke standardizaci požadavků na výstupy z IS OVM.
Weaknesses (vnitřní slabé stránky)	
4,7	Existuje prostor pro realizaci ICT projektů bez projednání s OMI.
4,4	Dlouhá doba od převedení vize do projektů.
4,4	Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu.
4,1	Neexistence ICT technologického standardu města.
4,1	Nedostatečná komunikace v rámci SMB.
4,1	Pro občana nejsou v dostatečné míře přístupné všechny agendy přes internet. Neexistuje portál občana (prezentační portál) umožňující sledování procesu.
4	Nedostatečné zapojení Odboru strategického rozvoje a spolupráce do tvorby strategických vizí pro ICT.
3,6	Nízké povědomí o důležitosti výdajů do IT.
3,4	Nízká míra využití potenciálu zavedených technologií.
3,3	Není definován katalog elektronicky poskytovaných služeb.
3,1	Nemožnost řešit problémy v informatice v době, kdy vznikají (legislativní a procesní omezení).
2,7	Omezený přístup k demografickým údajům na MČ.
Threats (vnější hrozby)	
4,4	Nárůst požadavků na informatiku při zachování stávajícího objemu finančních a lidských zdrojů.
4,3	Kybernetické hrozby a hrozby prostředí ohrožující fungování ICT.
4,2	Neochota ke změnám u vnitřních uživatelů ICT na MMB i ÚMČ.
4	Vznikají požadavky na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.
4	Vzrůstající nároky na dostupnost a důvěrnost poskytovaných služeb.
3,6	Obtížnost standardizace při potřebě specifických ICT řešení na ÚMČ.
3,6	Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.
3,6	Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.

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)	
4,1	Zavedená podpora uživatelů pomocí service-desku.
4	Průběžná obnova techniky (koncových zařízení).
4	Technologické umožnění práce na dálku.
4	Dostupnost aktualizovaných manuálů na intranetu.
3,9	Neomezenost počtu interních uživatelů v klíčových aplikacích z pohledu přístupu na informační systémy.
3,9	Poskytnutí dočasného přístupu k wi-fi návštěvníkům MMB a trvalého připojení zaměstnancům MMB.
3,7	Pravidelná školení na způsob práce s aplikacemi.
3,5	Pokročilá aplikační podpora uživatelů (interních i externích).
Opportunities (vnější příležitosti)	
4,6	Vytvoření komunikačních aplikací pro občana - internetová přepážka (portál občana Brna), mobilní aplikace.
3,8	Využití drobných specializovaných aplikací používaných v jiných městech.
3,7	Podpora uživatelů prostřednictvím chatbot a voicebot.

3,4	Poskytnutí prostředků uživatelům pro přístup k informacím i z domova.
3,4	Poskytnutí možnosti využívat umělou inteligenci pro zjednodušení práce uživatelů.
3,2	Zavést hodnocení kvality vyřešení požadavků zadaných v service-desku uživatelem.
2,9	Pokrytí wi-fi připojení do všech prostorů (dnes ve vybraných prostorách - kanceláře vedoucích a zasedací místnosti).
2,6	Využití možností prvků "mikro ICT" (princip Internetu věcí) a spolupráce s mobilním HW pro zpřístupnění služeb ICT občanům.
Weaknesses (vnitřní slabé stránky)	
4,3	Uživatelé nemají povědomí o reálných možnostech řešení jejich požadavků (času, schopnosti řešit požadavek, finanční náročnosti). Nedostatečně objektivní požadavky uživatelů.
4,1	Klíčoví uživatelé z jednotlivých odborů MMB nemají uvolněnou kapacitu na poskytování součinnosti v IT při řešení požadavků týkajících se jejich odborné problematiky.
3,9	Neznalost uživatele, jak požádat o novou funkcionalitu.
3,8	Nedůvěra uživatelů k používání service-desku.
3,8	Uživatelé s přístupem k elektronickým materiálům vyžadují rovněž jejich tištěnou podobu, která pro jejich činnost není nutná.
3,6	Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.
3,4	Dosud nezavedená elektronická podpora některých vnitřních schvalovacích procesů úřadu (např. cestovních příkazů).
2,4	Nejednotný přístup uživatelů k realizaci svých požadavků (formulace, spolupráce na řešení).
2,3	Snížená uživatelská podpora v období mimo pracovní dobu.
Threats (vnější hrozby)	
4,4	Napadení výpočetní techniky uživatele s omezením dostupnosti dat na ní uložených (např. ransomware).
4,3	Výpadek metropolitní sítě a internetu znamená nefunkčnost významných agend SMB.
4,3	Závislost na správném fungování centrálních aplikací při poskytování služeb.
3,8	Důvěra v možnosti umělé inteligence bez posouzení správnosti výsledků.
3,6	Vzrůstající komplexita a míra digitalizace poskytovaných služeb.
2,8	Mylný pohled na možnosti úřadu při řešení "životních situací" bez vnímání omezení (legislativa, zdroje..).
2,5	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)		
4,8	Projektová kancelář OMI řídí IT projektové portfolio MMB, včetně projektů kybernetické bezpečnosti (KB).	Organizace
4,8	Je zřízena samostatná role bezpečnostního architekta a solution architekta. Bezpečnostní architektura je provázána na EA MMB.	Architektura
4,8	Koordinace ICT projektů městských subjektů (Řídící orgán ICT).	Přínosy
4,8	Dlouhodobé strategické řízení informatiky.	Přínosy
4,7	Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ).	Architektura
4,7	Vznikl řídící orgán ICT ke koordinaci ICT v rámci perimetru SMB (MMB, městské části, městské firmy a příspěvkové organizace města).	Organizace

4,7	Validní informace o EA MMB jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.	Architektura
4,7	Člen RMB pro oblast informatiky.	Přínosy
4,6	Kvalifikovaní správci aplikací a ICT infrastruktury v oblasti, kterou mají ve své pracovní náplni.	Organizace
4,6	Oblast informační bezpečnosti je řízena koordinátorem kybernetické bezpečnosti SMB.	Organizace
4,5	Jistota prostředků na kalendářní rok v rámci schváleného rozpočtu.	Organizace
4,5	Architektura pro integrace aplikací - integrační platforma (s využitím principů ESB a ETL).	Architektura
4,5	Rada města Brna vydala minimální standard kybernetické bezpečnosti pro MČ, jehož dodržování je závazné.	Architektura
4,5	SMB má statut a může v rámci něj prosadit cíle v IT jak na MMB, tak i na ÚMČ (čl. 39 a 40).	Přínosy
4,4	V rámci SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) se zajištěnou ochranou proti jejich ztrátě.	Architektura
4,4	Kvalitní komunikační infrastruktura připojení ÚMČ.	Architektura
4,4	Efektivní licencování pro základní části městského AIS a office SW.	Architektura
4,4	Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.	Přínosy
4,3	Existence webové platformy města Brna.	Organizace
4,3	Vysoká úroveň řízení kybernetické bezpečnosti.	Přínosy
4,3	Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb.	Přínosy
4,1	Geografický informační systém přístupný pro občany, organizace, úřady SMB.	Přínosy
4,1	Zavedená podpora uživatelů pomocí service-desku.	Uživatelé
4	Dostupnost aktualizovaných manuálů na intranetu.	Uživatelé
4	Digitalizace vnitřních procesů řízení města (eMMB).	Přínosy
4	Sjednocené a vybudované prostředí pro výkon veřejné správy.	Přínosy
4	Průběžná obnova techniky (koncových zařízení).	Uživatelé
4	Technologické umožnění práce na dálku.	Uživatelé
4	Poskytování vybraných veřejných služeb přes internet.	Přínosy
3,9	Neomezenost počtu interních uživatelů v klíčových aplikacích z pohledu přístupu na informační systémy.	Uživatelé
3,9	Vysoká znalost technologických trendů a jejich zavádění.	Organizace
3,9	Rozšíření služeb provozovaných z městského cloudu pro všechny městské subjekty SMB.	Architektura
3,9	Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy.	Architektura
3,9	Poskytnutí dočasného přístupu k wi-fi návštěvníkům MMB a trvalého připojení zaměstnancům MMB.	Uživatelé
3,8	Zvyšující se bezpečnostní povědomí mezi pracovníky OMI a rovněž pracovníky MMB.	Organizace
3,8	Řízené zpřístupňování dat interním i externím uživatelům.	Přínosy
3,8	Kvalitní prostory a technologické zázemí pro umístění uzlových ICT prvků (datové centrum).	Architektura
3,8	Jsou k dispozici opakovatelně použitelné architektonické stavební bloky pro využití aplikacemi SMB (např. NIA Proxy, ISZR Proxy).	Architektura
3,7	Spolupráce se státní správou v oblasti kybernetické bezpečnosti.	Přínosy
3,7	Pravidelná školení na způsob práce s aplikacemi.	Uživatelé
3,7	Dosažené zkušenosti s implementací informačních systémů.	Organizace
3,5	Pokročilá aplikační podpora uživatelů (interních i externích)	Uživatelé

3,4	Rozdělení rozpočtových prostředků na provoz ICT a kybernetickou bezpečnost.	Organizace
3,2	Poskytování služeb založených společností a zřízených organizací městem přes internet.	Přínosy
3,1	Jsou vytvořeny specializované subjekty města k poskytování specifických ICT služeb.	Přínosy
2,3	TSB je pověřeno koncernovým pokynem ke koordinaci ICT a KB v rámci koncernu (obchodních společností města).	Organizace
Opportunities (vnější příležitosti)		
4,7	Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.	Architektura
4,6	Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).	Architektura
4,6	Sjednocení komunikace nabízených služeb SMB občanům přes centrální aplikaci.	Přínosy
4,6	Naplnění nové webové platformy města.	Přínosy
4,6	Vytvoření komunikačních aplikací pro občana - internetová přepážka (portál občana Brna), mobilní aplikace.	Uživatelé
4,3	Vytvoření a správa katalogu služeb ICT SMB.	Architektura
4,2	Nasazení systému pro sledování visibility strategických služeb poskytovaných SMB.	Architektura
4,1	Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy).	Architektura
4,1	Vydání IT směrnic závazných pro SMB.	Architektura
4	Maximalizovat využití čerpání prostředků z fondů EU.	Organizace
4	Využívání standardizovaných IT produktů poskytovaných na celostátní úrovni.	Přínosy
4	Dlouhodobá partnerská spolupráce s NÚKIB, DIA a MV ČR.	Organizace
4	Spolupráce s jinými městy v ČR a EU.	Přínosy
4	Využití popisu procesů MMB v procesních modelech (ORGO).	Organizace
3,9	Využití možností spolufinancování nových služeb z externích zdrojů.	Přínosy
3,8	Využití drobných specializovaných aplikací používaných v jiných městech.	Uživatelé
3,8	Větší využití ETL Clover pro datovou integraci systémů.	Architektura
3,8	Vytvoření kompetenčního modelu v rámci týmu včasné reakce SŘBI pro případy havarijních a krizových stavů.	Architektura
3,8	Využití potenciálu odborníků v rámci města ve formě poradenského orgánu.	Organizace
3,7	Definice zákazníka ICT služeb a jeho potřeb.	Přínosy
3,7	Vytvoření prioritizace cca 350 aplikací a odstupňovaný přístup k nim podle jejich priorit.	Architektura
3,7	Propojení konfiguračních databází udržovaných MMB a samostatně dodavateli/správci částí infrastruktury.	Architektura
3,7	V Brně na trhu práce existují vzdělaní a kompetentní pracovníci v oblasti ICT.	Organizace
3,7	Podpora uživatelů prostřednictvím chatbot a voicebot.	Uživatelé
3,7	Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu.	Architektura
3,6	Metodická pomoc kompetenčního centra uživatelům z ÚMČ a organizací města.	Architektura
3,6	Využití potenciálu umělé inteligence pro zefektivnění interních i externích procesů.	Přínosy
3,5	Popsání definice vazeb mezi projekty a sesouladění postupů – road-mapa na období několika let s pravidelnou aktualizací.	Architektura
3,4	Poskytnutí prostředků uživatelům pro přístup k informacím i z domova.	Uživatelé
3,4	Poskytnutí možnosti využívat umělou inteligenci pro zjednodušení práce uživatelů.	Uživatelé

3,3	Zintenzivnění spolupráce se středními a vysokými školami (využití jejich potenciálu).	Přínosy
3,3	Vytvoření centrálního přístupového bodu pro řízený přístup uživatelů do IS města a k aplikacím z různých platforem.	Architektura
3,2	Zavést hodnocení kvality vyřešení požadavků zadaných v service-desku uživatelem.	Uživatelé
3,1	Je k dispozici prostředí (framework) pro tvorbu jednoduché podpory procesů a workflow v nich (MOSS - MS Office SharePoint Services) s komunitou uživatelů.	Architektura
3,1	Využití aktivit v rámci externích subjektů ke standardizaci požadavků na výstupy z IS OVM.	Přínosy
3	Zapojení vysokých škol do rozvoje informatiky města Brna včetně aktivní spolupráce města při výuce studentů.	Organizace
3	Vytvořit prostředí pro drobné aplikace odborných útvarů SMB.	Architektura
3	Zvyšující se zájem stakeholderů o přístup k informacím z EA modelu.	Architektura
2,9	Využití Národního architektonického plánu s návrhovými vzory vybraných oblastí.	Architektura
2,9	Pokrytí wi-fi připojení do všech prostorů (dnes ve vybraných prostorách - kanceláře vedoucích a zasedací místnosti).	Uživatelé
2,7	Využití externích kapacit výzkumu a vývoje pro oponenturu rozvojových koncepčních plánů a projektů (CERIT, NUKIB, Útvar hlavního architekta eGov, DIA ...).	Architektura
2,6	Využití možností prvků "mikro ICT" (princip Internetu věcí) a spolupráce s mobilním HW pro zpřístupnění služeb ICT občanům.	Uživatelé
Weaknesses (vnitřní slabé stránky)		
4,7	Odměňovací systém neumožňuje získávat nové a udržet stávající pracovníky IT.	Organizace
4,7	Existuje prostor pro realizaci ICT projektů bez projednání s OMI.	Přínosy
4,4	Dlouhá doba od převedení vize do projektů.	Přínosy
4,4	Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti.	Architektura
4,4	Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu.	Přínosy
4,3	Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).	Architektura
4,3	Uživatelé nemají povědomí o reálných možnostech řešení jejich požadavků (času, schopnosti řešit požadavek, finanční náročnosti). Nedostatečně objektivní požadavky uživatelů.	Uživatelé
4,3	Řada aplikací nemá dokumentaci.	Architektura
4,2	Ne všichni klíčoví uživatelé (garanti) mají dostatečné znalosti, aby definovali požadavky na informatiku (formulace toho, co chtějí). OMI nemůže suplovat metodické role uživatelů.	Organizace
4,1	Neexistence ICT technologického standardu města.	Přínosy
4,1	Nedostatečná komunikace v rámci SMB.	Přínosy
4,1	Pro občana nejsou v dostatečné míře přístupné všechny agendy přes internet. Neexistuje portál občana (prezentační portál) umožňující sledování procesu.	Přínosy
4,1	Klíčoví uživatelé z jednotlivých odborů MMB nemají uvolněnou kapacitu na poskytování součinnosti v IT při řešení požadavků týkajících se jejich odborné problematiky.	Uživatelé
4	Nedostatek vnitřních odborných kapacit vzhledem k rostoucímu významu a rozvoji informatiky vede ke zvýšenému nákupu externích služeb.	Organizace
4	Neexistuje provozní konfigurační management na datové a aplikační vrstvě.	Architektura
4	Nedostatečné zapojení Odboru strategického rozvoje a spolupráce do tvorby strategických vizí pro ICT.	Přínosy
3,9	Neznalost uživatele, jak požádat o novou funkcionalitu.	Uživatelé

3,9	Chybí vazba na business vrstvu zpracovávanou ORGO v BPMN diagramech.	Architektura
3,8	IDM nemá zadefinované role z business vrstvy (není propojení až do procesní business vrstvy a její rozpracování na role).	Architektura
3,8	Nedůvěra uživatelů k používání service-desku.	Uživatelé
3,8	Uživatelé s přístupem k elektronickým materiálům vyžadují rovněž jejich tištěnou podobu, která pro jejich činnost není nutná.	Uživatelé
3,8	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
3,7	Model EA zahrnuje jen MMB a absentují organizace SMB.	Architektura
3,7	Platformová technologická roztříštěnost (např. různé db stroje).	Architektura
3,7	Nedobudována geograficky oddělená záložní infrastruktura.	Architektura
3,6	Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.	Uživatelé
3,6	Nedostatečná aplikace principů procesního řízení.	Architektura
3,6	Klíčové uživatele je obtížné motivovat pro spolupráci v projektových týmech týkajících se informatiky z důvodu střetu liniových a projektových struktur.	Organizace
3,6	Nízké povědomí o důležitosti výdajů do IT.	Přínosy
3,6	Používání zastaralých aplikací neintegrovatelných či vyžadujících výjimky z koncepce pro integraci systémů.	Architektura
3,5	Nedostatečné povědomí klíčových uživatelů o plánovaní kapacit zdrojů OMI na pokrytí požadavků.	Organizace
3,4	Nízká míra využití potenciálu zavedených technologií.	Přínosy
3,4	Ne všechna data jsou ukládána do datových úložišť ve strukturované podobě, která umožní řízení přístupu dle oprávnění.	Architektura
3,4	Dosud nezavedená elektronická podpora některých vnitřních schvalovacích procesů úřadu (např. cestovních příkazů).	Uživatelé
3,3	Nedostatečné personální zajištění obsahu a obsluhy webové platformy.	Organizace
3,3	Není definován katalog elektronicky poskytovaných služeb.	Přínosy
3,3	Neochota úředníků k využití ICT potenciálu a změn.	Organizace
3,2	Závislost rozvoje ICT architektury na přidělených prostředcích (rozpočtu).	Architektura
3,1	Nemožnost řešit problémy v informatice v době, kdy vznikají (legislativní a procesní omezení).	Přínosy
2,9	Městské firmy si spravují vlastní podružná menší datová centra i aplikace bez vazby na EA.	Architektura
2,7	Omezený přístup k demografickým údajům na MČ.	Přínosy
2,5	Plánování a využití kapacit všech zdrojů v souladu s požadavky vykonávaných procesů.	Architektura
2,4	Nejednotný přístup uživatelů k realizaci svých požadavků (formulace, spolupráce na řešení).	Uživatelé
2,3	Snížená uživatelská podpora v období mimo pracovní dobu.	Uživatelé
Threats (vnější hrozby)		
4,6	Legislativní změny vyžadující podrobnější popis systémů (procesy, architektura, bezpečnost, ...).	Architektura
4,4	Napadení výpočetní techniky uživatele s omezením dostupnosti dat na ní uložených (např. ransomware).	Uživatelé
4,4	Nárůst požadavků na informatiku při zachování stávajícího objemu finančních a lidských zdrojů.	Přínosy
4,4	Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT.	Organizace
4,3	Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24.	Architektura
4,3	Závislost na správném fungování centrálních aplikací při poskytování služeb.	Uživatelé

4,3	Kybernetické hrozby a hrozby prostředí ohrožující fungování ICT.	Přínosy
4,3	Výpadek metropolitní sítě a internetu znamená nefunkčnost významných agend SMB.	Uživatelé
4,3	Rozšiřování projektů v ICT mimo gesci OMI.	Organizace
4,3	Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.	Organizace
4,2	Neochota ke změnám u vnitřních uživatelů ICT na MMB i ÚMČ.	Přínosy
4,2	Se změnou politické reprezentace může dojít k zásadním změnám ve směrování a financování ICT.	Organizace
4,2	Konfliktní požadavky změn legislativy s dopadem do informačních systémů.	Architektura
4,1	Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.	Architektura
4,1	Masivní vývoj kybernetických útoků a jejich forem.	Organizace
4	Vznikají požadavky na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.	Přínosy
4	Vzrůstající nároky na dostupnost a důvěrnost poskytovaných služeb.	Přínosy
3,8	Nárůst požadavků na dokumentaci v ICT dnes zejména v oblasti informační a kybernetické bezpečnosti.	Organizace
3,8	Důvěra v možnosti umělé inteligence bez posouzení správnosti výsledků.	Uživatelé
3,7	Dlouhá doba od vytvoření záměru do jeho realizace způsobená interními předpisy nebo platnou legislativou.	Organizace
3,7	Organizační změny posilující přístup k aplikacím z vnějšího prostředí vyvolají problémy s licencemi a technologiemi.	Architektura
3,7	Masivní nárůst legislativních požadavků a jejich dopady v oblasti ICT a kybernetické bezpečnosti.	Organizace
3,6	Vzrůstající komplexita a míra digitalizace poskytovaných služeb.	Uživatelé
3,6	Obtížnost standardizace při potřebě specifických ICT řešení na ÚMČ.	Přínosy
3,6	Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.	Přínosy
3,6	EA model obsahuje koncentrované informace a při neoprávněném přístupu k nim jde o bezpečnostní riziko.	Architektura
3,6	Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.	Přínosy
3,5	Nedostatečná pozornost ze strany tvůrců prvků celostátního eGovernment, věnovaná specifickým potřebám statutárních měst.	Architektura
3,5	Hrozby spojené s užíváním zařízení umístěných mimo perimetr.	Organizace
3,5	Ze zadávacích řízení podle ZZVZ mohou vzejít neadekvátní dodavatelé nebo mohou zadávací řízení trvat nepredikovatelnou dobu.	Organizace
3,2	Vzrůstající komplexita a regulace požadovaných technických opatření v ICT.	Organizace
3,2	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
3,1	Narůstající význam regulace v oblasti AI (umělé inteligence).	Organizace
3	Nedostatečnost kapacity komunikační infrastruktury pro nové služby nabízené z internetu (např. video streaming, práce s 3D modely).	Architektura
2,9	Uživatelé pracující vzdáleně (mimo kancelář) se obracejí s lokálními ICT problémy na servisní podporu OMI mimo jeho gesci.	Organizace

2,8	Narůstající význam IoT a Scada prvků zvyšující míru rizik v rámci SMB.	Organizace
2,8	Licenční a technologická závislost na dodavateli (vendor lock-in).	Architektura
2,8	Mylný pohled na možnosti úřadu při řešení "životních situací" bez vnímání omezení (legislativa, zdroje..).	Uživatelé
2,7	Přidělení finančních prostředků z rozpočtu je vždy jen na rok (rozpočtování je jen roční), v IT není zavedeno víceleté financování.	Organizace
2,6	Vynucená koordinace s podřízenými organizacemi z hlediska regulovaných služeb poskytovaných ve sdílené infrastruktuře ve formě podpůrných aktiv.	Architektura
2,5	Legislativní omezení ICT služeb pro externí subjekty (občan, právnické osoby ..).	Uživatelé

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
Koordinace ICT projektů městských subjektů (Řídící orgán ICT).
Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ).
Zavedená podpora uživatelů pomocí service-desku.
Kvalifikovaní správci aplikací a ICT infrastruktury v oblasti, kterou mají ve své pracovní náplni.
k vnější příležitosti
Definice zákazníka ICT služeb a jeho potřeb.

[SO2] Využití vnitřní silné stránky
Neomezenost počtu interních uživatelů v klíčových aplikacích z pohledu přístupu na informační systémy.
Efektivní licencování pro základní části městského AIS a office SW.
k vnější příležitosti
Vytvoření a správa katalogu služeb ICT SMB.
Definice zákazníka ICT služeb a jeho potřeb.

[SO3] Využití vnitřní silné stránky
Validní informace o EA MMB jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.
Je zřízena samostatná role bezpečnostního architekta a solution architekta. Bezpečnostní architektura je provázána na EA MMB.
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).
Definice zákazníka ICT služeb a jeho potřeb.

[SO4] Využití vnitřní silné stránky
Člen RMB pro oblast informatiky.
Dlouhodobé strategické řízení informatiky.
Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy.
Projektová kancelář OMI řídí IT projektové portfolio MMB, včetně projektů kybernetické bezpečnosti (KB).
Koordinace ICT projektů městských subjektů (Řídící orgán ICT).
Vznikl řídící orgán ICT ke koordinaci ICT v rámci perimetru SMB (MMB, městské části, městské firmy a příspěvkové organizace města).
Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ).

k vnější příležitosti
Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).
Sjednocení komunikace nabízených služeb SMB občanům přes centrální aplikaci.
Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu.
Nasazení systému pro sledování visibility strategických služeb poskytovaných SMB.

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

[SO6] Využití vnitřní silné stránky
Člen RMB pro oblast informatiky.
Projektová kancelář OMI řídí IT projektové portfolio MMB, včetně projektů kybernetické bezpečnosti (KB).
Poskytování vybraných veřejných služeb přes internet.
Poskytování služeb založených společností a zřízených organizací městem přes internet.
k vnější příležitosti
Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).
Naplnění nové webové platformy města.

[SO7] 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.

[SO8] Využití vnitřní silné stránky
Projektová kancelář OMI řídí IT projektové portfolio MMB, včetně projektů kybernetické bezpečnosti (KB).
Validní informace o EA MMB jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.
Je zřízena samostatná role bezpečnostního architekta a solution architekta. Bezpečnostní architektura je provázána na EA MMB.
Oblast informační bezpečnosti je řízena koordinátorem kybernetické bezpečnosti SMB.
k vnější příležitosti
Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.

[SO9] Využití vnitřní silné stránky
Zavedená servis-desková podpora uživatelů.
k vnější příležitosti
Zavést hodnocení kvality vyřešení požadavků zadaných v Help Desku uživatelem.
Podpora uživatelů prostřednictvím chatbot a voicebot.

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

[ST1] Využití vnitřní silné stránky
Je zřízena samostatná role bezpečnostního architekta a solution architekta. Bezpečnostní architektura je provázána na EA MMB.
Oblast informační bezpečnosti je řízena koordinátorem kybernetické bezpečnosti SMB.
V rámci SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) se zajištěnou ochranou proti jejich ztrátě.
Rada města Brna vydala minimální standard kybernetické bezpečnosti pro MČ, jehož dodržování je závazné.
k zamezení vnější hrozby
Masivní vývoj kybernetických útoků a jejich forem.
Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24.
Napadení výpočetní techniky uživatele s omezením dostupnosti dat na ní uložených (např. ransomware).

Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.

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

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

[ST4] Využití vnitřní silné stránky
Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy.
Koordinace ICT projektů městských subjektů (Řídící orgán ICT).
Dlouhodobé strategické řízení informatiky.
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.
Koordinace ICT projektů městských subjektů (Řídící orgán ICT).
Dlouhodobé strategické řízení informatiky.
k zamezení vnější hrozby
Vznikají požadavky na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.
Neochota ke změnám u vnitřních uživatelů ICT na MMB i ÚMČ.

[ST6] Využití vnitřní silné stránky
Člen RMB 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 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.
Kvalifikovaní správci aplikací a ICT infrastruktury v oblasti, kterou mají ve své pracovní náplni.
k zamezení vnější hrozby
Závislost na správném fungování centrálních aplikací při poskytování služeb.
Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.

[ST8] Využití vnitřní silné stránky
Člen RMB pro oblast informatiky.
Projektová kancelář OMI řídí IT projektové portfolio MMB, včetně projektů kybernetické bezpečnosti (KB).
k zamezení vnější hrozby
Nárůst požadavků na informatiku při zachování stávajícího objemu finančních a lidských zdrojů.
Vzrůstající komplexita a míra digitalizace poskytovaných služeb.
Vzrůstající nároky na dostupnost a důvěrnost poskytovaných služeb.

[ST9] Využití vnitřní silné stránky
Člen RMB pro oblast informatiky.
k zamezení vnější hrozby
Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.
Odměňovací systém neumožňuje získávat nové a udržet stávající pracovníky IT.

[ST10] Využití vnitřní silné stránky
Kvalifikovaní správci aplikací a ICT infrastruktury v oblasti, kterou mají ve své pracovní náplni.
k zamezení vnější hrozby
Legislativní změny vyžadující podrobnější popis systémů (procesy, architektura, bezpečnost, ...).
Závislost na správném fungování centrálních aplikací při poskytování služeb.

[ST11] Využití vnitřní silné stránky
Oblast informační bezpečnosti je řízena koordinátorem kybernetické bezpečnosti SMB.
Je zřízena samostatná role bezpečnostního architekta. Bezpečnostní architektura je provázána na EA.
k zamezení vnější hrozby
Hrozby spojené s užíváním zařízení umístěných mimo perimetr.
Napadení výpočetní techniky uživatele s omezením dostupnosti dat na ní uložených (např. ransomware).
Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24 (je dnes zajištěno na úrovni infrastruktury).

[ST12] 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.

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

[WO1] Překonání vnitřní slabosti
Dlouhá doba od převedení vize do projektů.
využitím vnější příležitosti
Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy).
Definice zákazníka ICT služeb a jeho potřeb.

[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 jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).
Vytvoření komunikačních aplikací pro občana - internetová přepážka (portál občana Brna), mobilní aplikace.
Sjednocení komunikace nabízených služeb SMB občanům přes centrální aplikaci.

[WO4] Překonání vnitřní slabosti
Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).
využitím vnější příležitosti
Vytvoření prioritizace cca 350 aplikací a odstupňovaný přístup k nim podle jejich priorit.
Maximalizovat využití čerpání prostředků z fondů EU.
Popsání definice vazeb mezi projekty a sesouladění postupů – road-mapa na období několika let s pravidelnou aktualizací.

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

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

[WO7] Překonání vnitřní slabosti
Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).
využitím vnější příležitosti
Využívání standardizovaných IT produktů poskytovaných na celostátní úrovni.
Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu.
Využití možností spolufinancování nových služeb z externích zdrojů.
Využití potenciálu odborníků v rámci města ve formě poradenského orgánu.
Využití externích kapacit výzkumu a vývoje pro oponenturu rozvojových koncepčních plánů a projektů (CERIT, NUKIB, Útvar hlavního architekta eGov, DIA ...).
Spolupráce s jinými městy v ČR a EU.

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

[WO9] Překonání vnitřní slabosti
Existuje prostor pro realizaci ICT projektů bez projednání s OMI.
využitím vnější příležitosti
Vytvoření a správa katalogu služeb ICT SMB
Sjednocení komunikace nabízených služeb SMB občanům přes centrální aplikaci.
Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).

[WO10] Překonání vnitřní slabosti
Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu.
využitím vnější příležitosti
Definice zákazníka ICT služeb a jeho potřeb.
Vytvoření a správa katalogu služeb ICT.

[WO11] Překonání vnitřní slabosti
Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti.
využitím vnější příležitosti
Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.

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.
Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti.
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.
Kybernetické hrozby a hrozby prostředí ohrožující fungování ICT.

[WT2] Preventivní obrana proti skloubení vnitřní slabosti
Neexistence ICT technologického standardu města.
Existuje prostor pro realizaci ICT projektů bez projednání s OMI.
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.
Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).
s vnější hrozbou
Nárůst požadavků na informatiku při zachování stávajícího objemu finančních a lidských zdrojů.
Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT.
Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.

[WT4] 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 rozsahu správního obvodu (např. aplikace CRR, CRV, digitalizace dokumentů pro centrální agendy, rušení místní příslušnosti ...).

[WT5] Preventivní obrana proti skloubení vnitřní slabosti
Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).
s vnější hrozbou
Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.
Nedostatečná pozornost ze strany tvůrců prvků celostátního eGovernment, věnovaná specifickým potřebám statutárních měst.
Legislativní změny vyžadující podrobnější popis systémů (procesy, architektura, bezpečnost, ...).
Vznikají požadavky na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.

[WT6] Preventivní obrana proti skloubení vnitřní slabosti
Existuje prostor pro realizaci ICT projektů bez projednání s OMI.
s vnější hrozbou
Vznikají požadavky na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.

[WT7] 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.
Není definován katalog elektronicky poskytovaných služeb.
s vnější hrozbou
Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24.

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
4,58	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.	Sjednocení komunikace nabízených služeb SMB občanům přes centrální aplikaci. Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).	Umožnit přístup občanům k agendám přes velkou městskou aplikaci (mobilní aplikace) a portál občana (web).
	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
4,42	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 bez ohledu na jejich uložení.
	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
4,33	S-T	Dlouhodobé strategické řízení informatiky. Koordinace ICT projektů městských subjektů (Řídící orgán ICT). Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy. Validní informace o EA MMB jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.	Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.	Koordinace portfolia ICT projektů v rámci SMB. Plánovat zdroje dlouhodobě s vazbou na rozvojové projekty realizující požadavky v ICT města.

	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
4,33	S-O	Validní informace o EA MMB 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. Člen RMB pro oblast informatiky. Dlouhodobé strategické řízení informatiky.	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
4,25	W-T	Existuje prostor pro realizaci ICT projektů bez projednání s OMI.	Vznikají požadavky na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.	Standardizovat postupy pro vznik nových rozvojových požadavků s dopadem do ICT vznášených věcnými útvary MMB.
	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
4,08	W-O	Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).	Popsání definice vazeb mezi projekty a sesouladění postupů – road-mapa na období několika let s pravidelnou aktualizací. Koordinace ICT projektů městských subjektů. Vytvoření prioritizace cca 350 aplikací a odstupňovaný přístup k nim podle jejich priorit. Maximalizovat využití čerpání prostředků z fondů EU.	Koordinace portfolia ICT projektů v rámci SMB. Plánovat zdroje dlouhodobě s vazbou na rozvojové projekty realizující požadavky v ICT města.

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
4,00	W-O	Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti.	Vydání IT směrnic závazných pro SMB. Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti. Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy) Vytvoření kompetenčního modelu v rámci týmu včasné reakce SŘBI pro případy havarijních a krizových stavů.	Řídit bezpečnostní architekturu napříč SMB a dohlížet na implementaci bezpečnostních standardů v SMB (řídí kancelář kybernetické bezpečnosti).
	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,83	W-T	Motivační systém neumožňuje získávat nové a udržet stávající pracovníky IT. Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).	Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT. Nárůst požadavků na informatiku při zachování stávajícího objemu finančních a lidských zdrojů. Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.	S nárůstem pracovní náplně vzrůstající s digitalizací všech činností města zvýšit finanční zdroje a analogicky počet pracovníků OMI. Vytvořit motivační systém pro pracovníky v IT. který bude dostatečně atraktivní pro stávající i nové pracovníky.
	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
3,83	W-O	Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu. Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.	Vytvoření a správa katalogu služeb ICT. Vydání IT směrnic závazných pro SMB.	Maximálně propojit IT pracovníky s klíčovými pracovníky odborů do rozvoje a využívání IS.

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,83	W-T	Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti. 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. Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24. Kybernetické hrozby a hrozby prostředí ohrožující fungování ICT.	Zvýšit míru organizace informační bezpečnosti a schopnosti reakce a obnovy po útoku s ohledem na požadavky vyplývající z business continuity.
	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
3,83	S-T	Oblast informační bezpečnosti je řízena koordinátorem kybernetické bezpečnosti SMB. 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). Kybernetické hrozby a hrozby prostředí ohrožující fungování ICT.	Zajistit bezpečnost uživatelů pracujících vně chráněného městského perimetru.
	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
3,67	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. Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24 (je dnes zajištěno na úrovni infrastruktury).	Zvýšit odolnost poskytovaných služeb proti jejich výpadku.
	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
3,67	S-O	Poskytování vybraných veřejných služeb přes internet. Zavedená podpora uživatelů pomocí service-desku.	Definice zákazníka ICT služeb a jeho potřeb. Vytvoření a správa katalogu služeb ICT.	Poskytovat profesionálně zadefinované ICT služby za nastavených SLA/OLA parametrů pro interní uživatele a externí uživatele.

	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
3,58	S-O	Zavedená servis-desková podpora uživatelů.	Zavést hodnocení kvality vyřešení požadavků zadaných v Help Desku uživatelem. Nasazení systému pro sledování visibility strategických služeb poskytovaných SMB. Podpora uživatelů prostřednictvím chatbot a voicebot.	Zvýšení orientace na podporu uživatelů s posílením service-deskových funkcí. Standardizovat postupy pro poskytování servisních služeb, rozdělení na katalogové služby a projekty.
	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,50	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. Legislativní změny vyžadující podrobnější popis systémů (procesy, architektura, bezpečnost, ...).	Maximálně propojit IT pracovníky s klíčovými pracovníky odborů do rozvoje a využívání IS.
	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
3,42	S-T	Člen RMB 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 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. Zavést pravidla a procesy pro nasazení bezpečnostních opatření a projektů v režimu krizového řízení.

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,33	W-T	Nedostatek vnitřních odborných kapacit vzhledem k rostoucímu významu a rozvoji informatiky vede ke zvýšenému nákupu externích služeb. Nárůst požadavků na informatiku při zachování stávajícího objemu finančních a lidských zdrojů.	Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni. Vzrůstající komplexita a míra digitalizace poskytovaných služeb. Legislativní změny vyžadující podrobnější popis systémů (procesy, architektura, bezpečnost, ...).	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 a architekturou s jejich zdůvodněním formou projektového záměru.
	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
3,17	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 interních 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 aplikací v městském cloudu podle závazně dohodnutých pravidel.

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
2,67	W-O	Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).	Využití externích kapacit výzkumu a vývoje pro oponenturu rozvojových koncepčních plánů a projektů (CERIT, NUKIB, Útvar hlavního architekta eGov, DIA …). Zintenzivnění spolupráce se středními a vysokými školami (využití jejich potenciálu). Využití aktivit v rámci externích subjektů ke standardizaci požadavků na výstupy z IS OVM (orgánů veřejné moci).	Zintenzivnit spolupráci s externími zdroji.

3. Návrh cílového stavu

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

3.1. Vize & mise informatiky města Brna

3.1.1. Vize města[18]

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

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

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

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

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

Brno v roce 2050 hovoří jazykem srozumitelným občanům města i jeho návštěvníkům. Kromě českého jazyka je možné komunikovat s orgány města bez jakýkoliv omezení minimálně ještě dalším jedním světovým jazykem – anglicky. **Informace jsou jednoduše dohledatelné a srozumitelné všem.** Jsou vždy aktuální, důvěryhodné, poučné, nestranné, jednoduché na pochopení, užitečné a přesné. Brno vytváří taková místa, která zjednodušují občanům dohledatelnost libovolných informací týkajících se města i přístup ke službám, které město poskytuje. Informační systém měst a jeho organizací je integrován do systému 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 k tomu zřízeným orgánem Rady města na projektové a architektonické úrovni za účelem zajištění potřeb statutárního města Brna a příjemců jeho služeb.

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 mobilní aplikaci a webový portál služeb	Mobilní aplikace a webový portál služeb jsou naplněny službami: • úřední pro občany / úředníky • turisticko / informační • otevřená data • geoportál. Součástí řešení je zajištění 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 a kybernetické odolnosti	Stav poskytovaných služeb a jejich klíčových systémů je kontinuálně monitorován s pružnou a rychlou reakcí na identifikované anomálie.
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 ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace	ICT zdroje jsou zajištěny a vybalancovány v takové výši, aby byly realizovatelné cíle směřující k rozvoji ICT a digitalizaci v rámci SMB. Plánovat zdroje dlouhodobě s vazbou na rozvojové projekty realizující požadavky v ICT města. Maximálně propojit IT pracovníky s klíčovými pracovníky odborů do rozvoje a využívání IS.

3.2.2. Cíle v perspektivě procesů

číslo	strategický cíl	popis
6	Využívat workflow služeb přes jednotné prezentační rozhraní	Aplikace jsou zpřístupněny na portálu pro poskytování elektronických služeb a přes jednotnou aplikaci města Brna (JAMB). 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 SMB se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb	Katalog ICT služeb umožňuje využívat infrastrukturní, platformové a bezpečnostní služby poskytované pro SMB centrálně jednotným způsobem.

číslo	strategický cíl	popis
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. Postupy pro vznik nových rozvojových požadavků s dopadem do ICT vznášených věcnými útvary MMB jsou standardizovány. ICT města je řízeno v souladu s technologickým standardem SMB. Interním a externím uživatelům jsou poskytovány profesionálně zadefinované ICT služby podle nastavených SLA/OLA parametrů.
10	Koordinovat rozvoj ICT města řízením projektového portfolia	Projektové portfolio zahrnuje významné projekty z hlediska rozvoje ICT města a umožňuje jejich koordinované řízení v rámci SMB.
12	Systematizovat řízení kybernetické bezpečnosti přes bezpečnostní architekturu a odolnost	Bezpečnostní architektura je řízena napříč SMB. Bezpečnostní standardy v SMB jsou implementovány. Je dosaženo schopnosti reakce a obnovy po útoku s ohledem na požadavky vyplývající z business continuity. Jsou zavedena pravidla a procesy pro nasazení bezpečnostních opatření a projektů v režimu krizového řízení.

3.2.3. Cíle v perspektivě zákazníků

číslo	strategický cíl	popis
11	Poskytovat elektr. služby přes webový portál služeb a mobilní aplikaci	Zvolené životní situace a služby města jsou poskytovány elektronicky. Možnost sledování průběhu procesů občanem. Zrychlení průběhu procesů. Zvýšení kontextové informovanosti a transparentnosti (kroky proběhlé a příští).
13	Podporovat využívání služeb městského cloudu organizacemi SMB	Městské cloudové služby (zálohování, úložiště, bezpečnost) jsou poskytovány v souladu s legislativou za výhodných ekonomických podmínek obtížně dosažitelných z pozice jednotlivých městských organizací.
14	Rozšířit využívání centrálních aplikací podle závazných standardů	Centrálně poskytované aplikace budou ve shodě s Informační koncepcí ČR a město bude mít zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...). Je vytvořen a udržován technologický standard SMB.
15	Zavést dlouhodobou správu služeb	Všechny služby uvedené v katalogu služeb, na kterých se podílí více garantů, mají stanoveného správce služeb (koordinátora). Správce služeb dlouhodobě spravuje služby tak, aby odpovídaly požadavkům konzumentů těchto služeb.

3.2.4. Cíle v perspektivě ICT přínosů

číslo	strategický cíl	popis
16	Digitalizovat služby města	Je vytvořena technologická platforma s uživatelsky přívětivým rozhraním pro elektronickou formu komunikace občanů s úředníky a poskytování informací a služeb obyvatelům a návštěvníkům města.
17	Vytvořit moderní, společné, bezpečné a efektivní 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	Centrálně řídit ICT města	Řízení ICT města je prováděno centralizovaně na projektové, architektonické a bezpečnostní úrovni orgánem zřízeným Radou města.
19	Dosahovat soulad s digitální legislativou (compliance)	ICT a data jsou chráněna bez ohledu na jejich uložení proti všem formám kybernetických útoků v souladu s požadavky legislativy.

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.

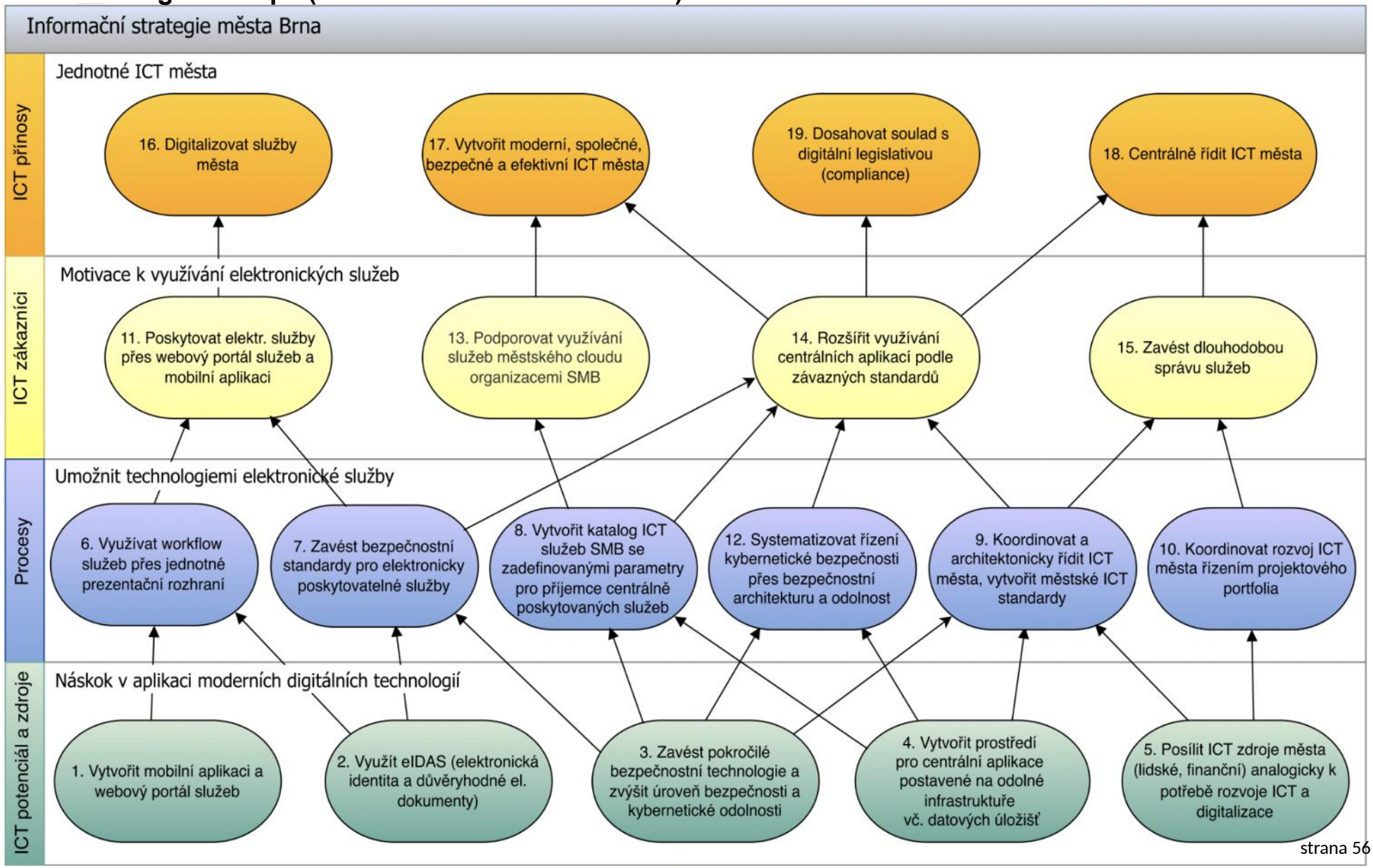
Ve strategické mapě (schéma Balanced Scorecard) jsou kauzální vazby znázorněny šipkami, kdy ve směru šipky je uvažován vztah příčina vyvolávající následek. Zaměření na strategicky významné vztahy, bez ambice na analýzu všech myslitelných vazeb mezi cíli, je jednou z hlavních předností použité metody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

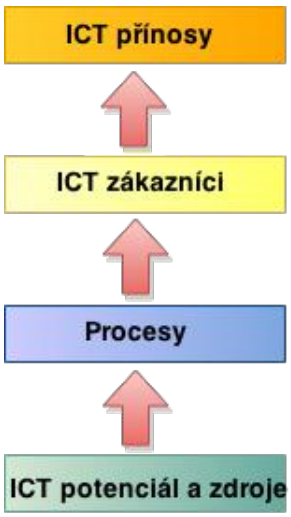
Strategická mapa (schéma Balanced Scorecard) uvedená na následující straně představuje souhrnné znázornění systému strategických cílů a jejich kauzálních vazeb. Obsahuje:

- 4 cíle v perspektivě ICT přínosy;
- 4 cíle v perspektivě ICT zákazníci;
- 6 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 (městská mobilní aplikace, portál služeb);
- Vytvoření moderního, společného, bezpečného a efektivního 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 čtyři dominantní strategické řetězce:

- Řetězec digitalizace služeb;
- Řetězec tvorby ICT města;
- Řetězec souladu s digitální legislativou;
- Řetězec řízení ICT města.

Řetězec digitalizace služeb

Strategický řetězec ***digitalizace služeb*** je uskupen kolem sedmi cílů vertikálně směřujících k dosažení digitální komunikace s občany prostřednictvím mobilní aplikace a webového portálu služeb:

1. *Vytvořit mobilní aplikaci a webový portál služeb;*
2. *Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty);*
3. *Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a kybernetické odolnosti;*

6. *Využívat workflow služeb přes jednotné prezentační rozhraní;*
7. *Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby;*
11. *Poskytovat elektr. služby přes webový portál služeb a mobilní aplikaci;*
16. *Digitalizovat služby města.*

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 a jednotné mobilní aplikace města. Proto, aby bylo dosaženo digitální komunikace při spolupráci občanů s úředníky, je třeba zajistit důvěryhodnost elektronických služeb poskytovaných Úřadem, bezpečný přístup občanů k dokumentům zprostředkovaných městským portálem občana a jednotnou aplikací 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 tvorby ICT města

Strategický řetězec ***tvorby ICT města*** kauzálně propojuje devět cílů směřujících k vytvoření moderního, společného a bezpečného ICT umožňujícího interním uživatelům ICT služeb SMB využívat aplikace vzdáleným přístupem, poskytovat služby organizacím SMB prostřednictvím cloudových služeb a v neposlední řadě využívat na MMB, MČ a městských firmách centrální sdílené aplikace:

3. *Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a kybernetické odolnosti;*
4. *Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť;*
5. *Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace;*
8. *Vytvořit katalog ICT služeb SMB se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb;*
9. *Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy;*
12. *Systematizovat řízení kybernetické bezpečnosti přes bezpečnostní architekturu a odolnost;*
13. *Podporovat využívání služeb městského cloudu organizacemi SMB;*
14. *Rozšířit využívání centrálních aplikací podle závazných standardů;*
17. *Vytvořit moderní, společné a bezpečné a efektivní ICT města.*

Vysoká úroveň bezpečnosti ICT je základním předpokladem pro poskytování digitálních služeb uživatelům ICT. Jednotnost využívání služeb ICT města je dána službami popsanými v katalogu ICT služeb, které vycházejí z možností centrálně řízené architektury systémů a zohledňují městské ICT standardy. Tím je umožněno příjemcům ICT služeb využívat za výhodných ekonomických podmínek cloudové služby a centrální aplikace v souladu s požadavky eGovernmentu ČR.

Řetězec souladu s digitální legislativou

Strategický řetězec ***souladu s digitální legislativou*** vznikl jako odpověď na nárůst legislativních požadavků na bezpečnost a odolnost informačních systémů veřejné správy. Strategický řetězec *souladu s digitální infrastrukturou* kauzálně propojuje devět cílů směřujících k zajištění souladu ICT SMB s požadavky legislativy:

3. *Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a kybernetické odolnosti;*
4. *Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť;*
5. *Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace;*
7. *Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby;*
8. *Vytvořit katalog ICT služeb SMB se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb;*
9. *Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy;*
12. *Systematizovat řízení kybernetické bezpečnosti přes bezpečnostní architekturu a odolnost;*
14. *Rozšířit využívání centrálních aplikací podle závazných standardů;*
19. *Dosahovat soulad s digitální legislativou (compliance).*

Soulad s digitální legislativou je založen na uplatnění pokročilých bezpečnostních technologií a na vytvoření bezpečného a odolného infrastrukturního prostředí, obojí je nezbytné pro centrální poskytovaní ICT služeb. Vzhledem k závislosti města na ICT a digitalizaci služeb je třeba architektonicky řídit ICT města podle závazných standardů a zohlednit při řízení legislativní požadavky a to zejména ty, které se týkají kybernetické bezpečnosti a odolnosti ICT města.

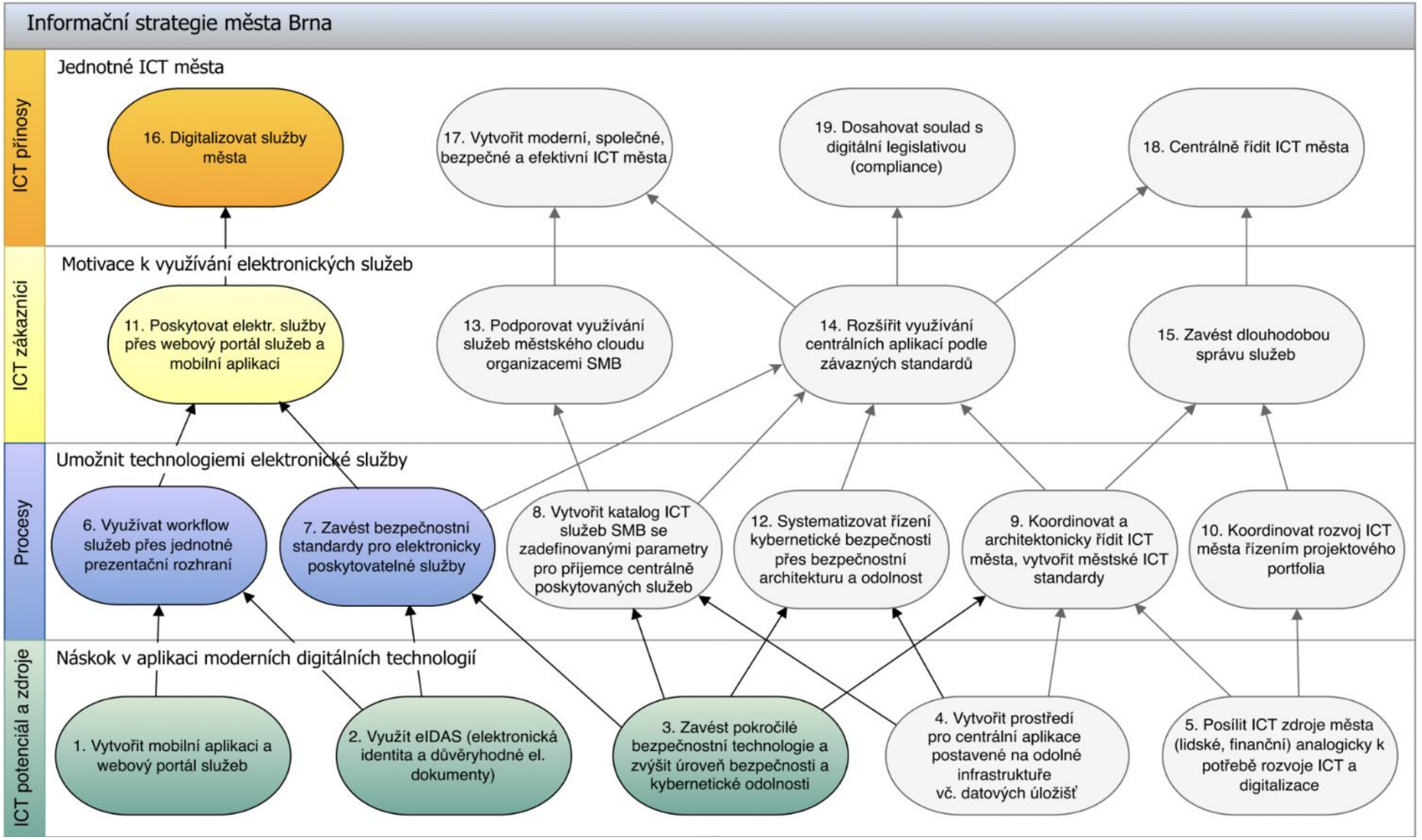
Řetězec řízení ICT města

Strategický řetězec ***řízení ICT města*** zohledňuje nárůst požadavků na digitalizaci veřejné správy. Strategický řetězec *řízení ICT města* kauzálně propojuje devět cílů směřujících k centrálnímu řízení rozvoje ICT SMB:

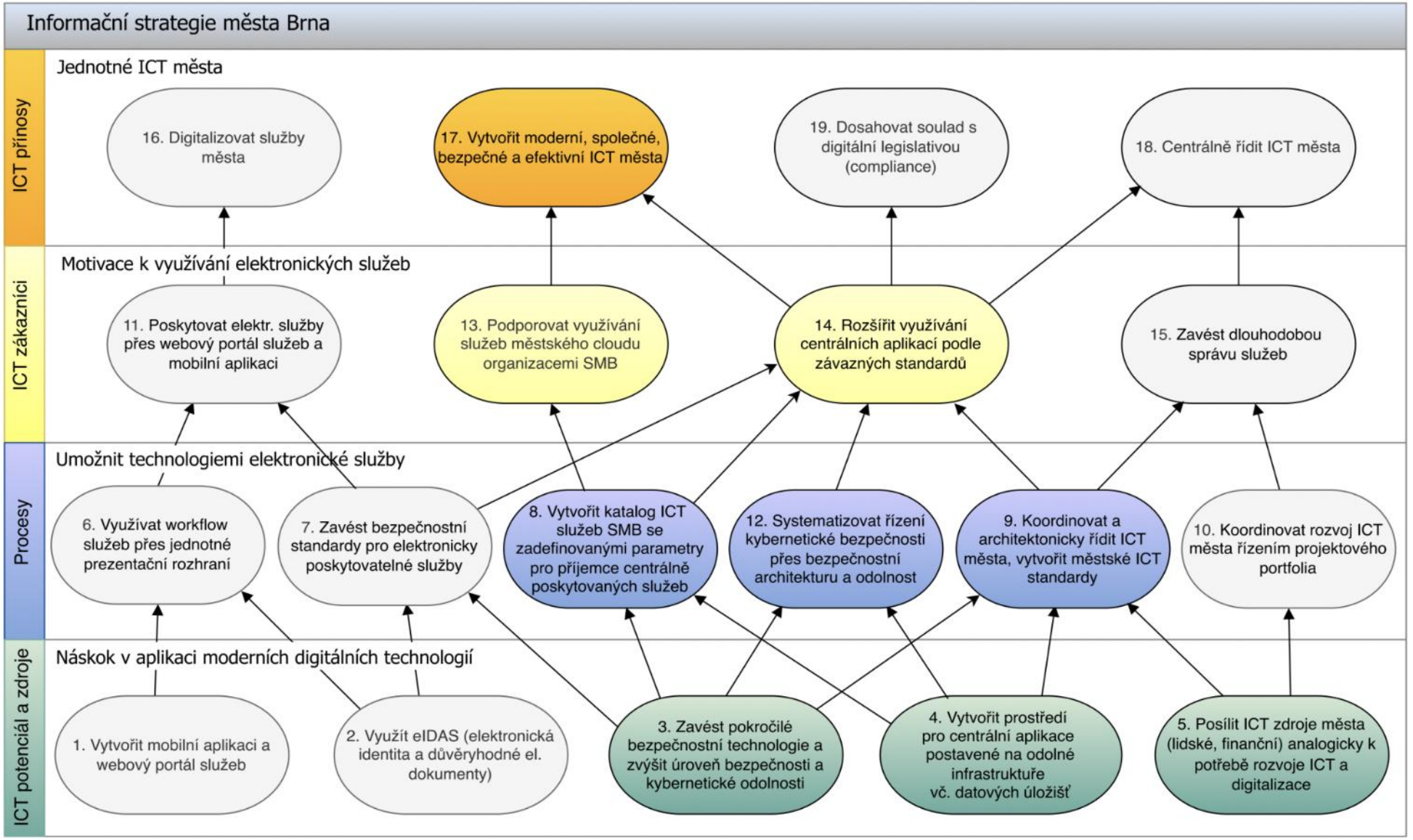
3. *Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a kybernetické odolnosti;*
4. *Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť;*
5. *Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace;*
9. *Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy;*
10. *Koordinovat rozvoj ICT města řízením projektového portfolia;*
12. *Systematizovat řízení kybernetické bezpečnosti přes bezpečnostní architekturu a odolnost;*
14. *Rozšířit využívání centrálních aplikací podle závazných standardů;*
15. *Zavést dlouhodobou správu služeb;*
18. *Centrálně řídit ICT města.*

Centrální řízení ICT města je založeno na uplatnění pokročilých bezpečnostních technologií a na vytvoření bezpečného a odolného infrastrukturního prostředí, obojí je nezbytné pro centrální poskytovaní ICT služeb. Pro narůstající závislost města na ICT a digitalizaci služeb je třeba k současnému trendu přerodu města na tzv. „IT-intenzivní organizaci“, tj. organizaci, která již de facto nemůže fungovat ve všech základních aspektech bez ICT a digitálních technologií, posílit analogicky ICT zdroje. Aby bylo se zdroji efektivně a hospodárně vynakládáno z perspektivy celého města a zdroje mohly být sdíleny, je strategický řetězec řízení ICT města zacílen na posílení centrálního architektonického řízení, městské standardy, rozšiřování využívání centrálních aplikací a centrální spolupráci pracovníků SMB při řízení ICT projektů významných pro celé město.

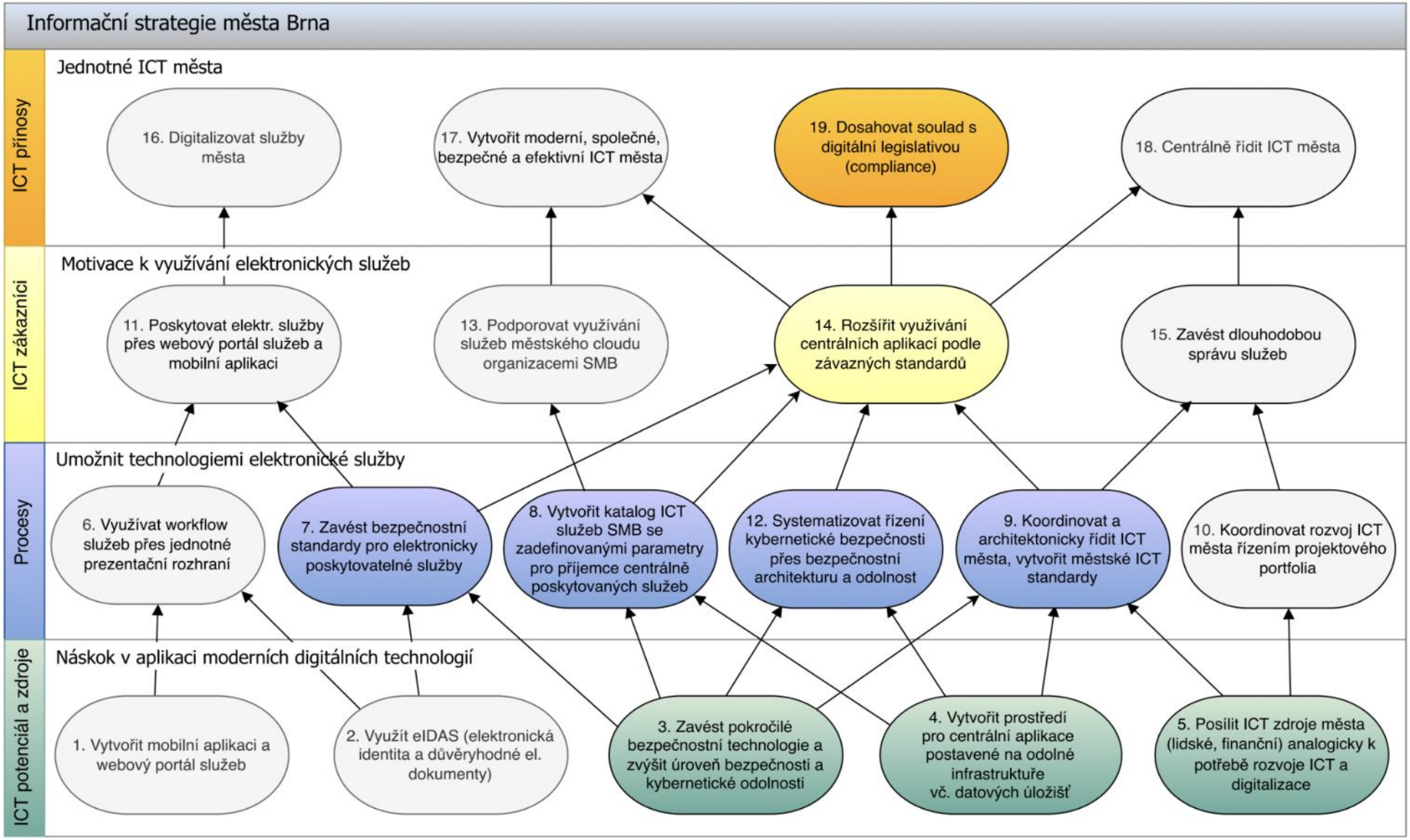
3.3.2. Řetězec digitalizace služeb



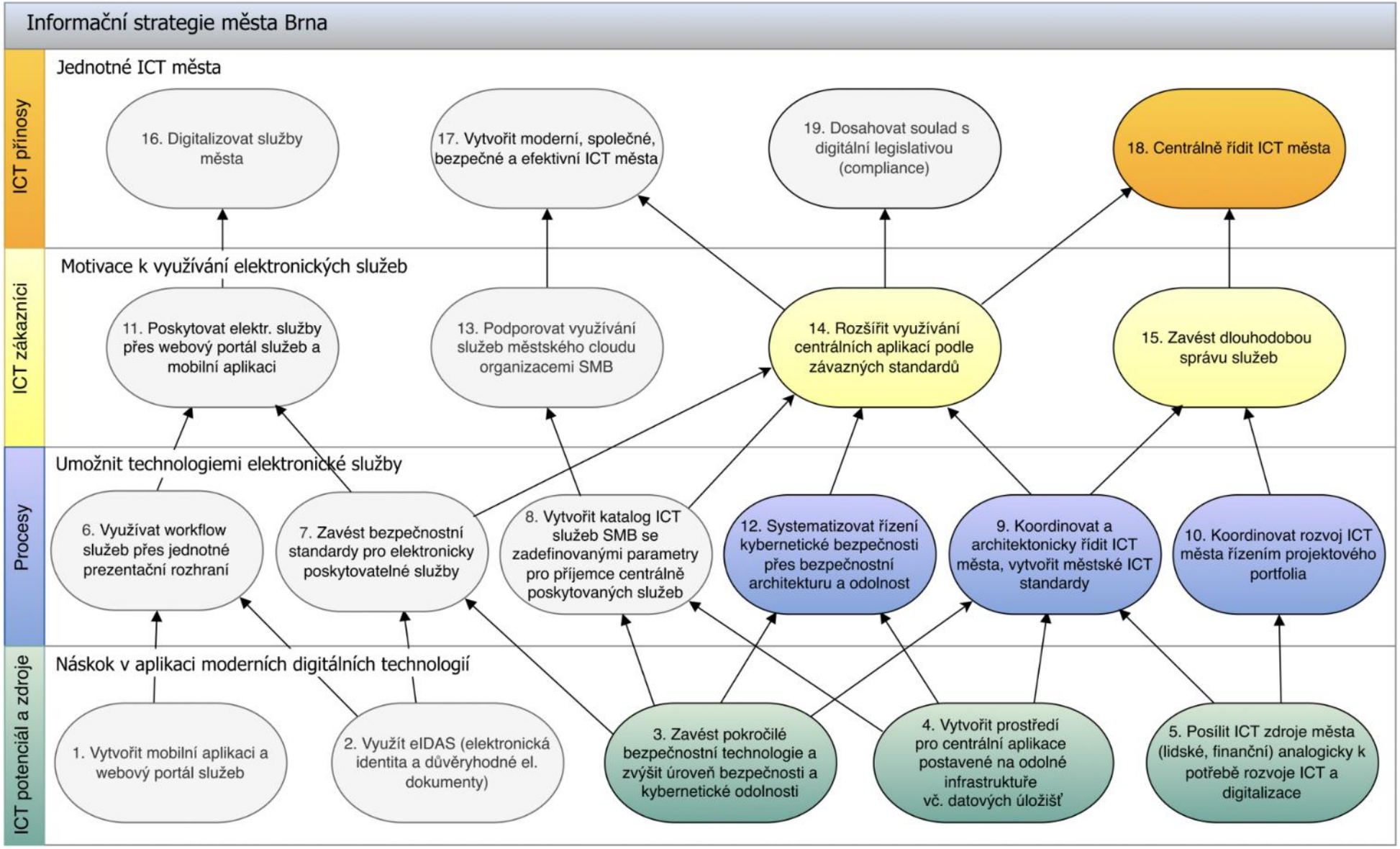
3.3.3. Řetězec tvorby ICT města



3.3.4. Řetězec souladu s digitální legislativou



3.3.5. Řetězec řízení ICT města



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 2025, 2026, 2027, 2028 a 2029.

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 mobilní aplikaci a webový portál služeb	Technologie a bezpečnost portálu	2025	Připraven katalog služeb pro občany a návštěvníky města. Vytvořen koncept integrace aplikací do webového portálu služeb. Vytvořen koncept integrace aplikací do mobilní aplikace. Součástí webového portálu služeb je řešení jeho kybernetické bezpečnosti. Město provozuje webový portál služeb v souladu s moderními technologickými a bezpečnostními standardy. Je vytvořen plán rozvoje webového portálu služeb.
			2026	Město provozuje mobilní aplikaci v souladu s moderními technologickými a bezpečnostními standardy v 1. produkční verzi. Je vytvořen plán rozvoje mobilní aplikace. Rozvoj webového portálu služeb podle plánu.
			2027	Rozvoj mobilní aplikace o nové služby podle plánu. Rozvoj webového portálu služeb podle plánu.
			2028	Rozvoj mobilní aplikace o nové služby podle plánu. Rozvoj webového portálu služeb podle plánu.
			2029	Rozvoj mobilní aplikace o nové služby podle plánu. Rozvoj webového portálu služeb podle plánu.
2	Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty)	Shoda s eIDAS	2025	Konsolidace domén a AD (Active Directory).
			2026	Autentizační brána IDM je využívána pro potřeby aplikací/služeb města (SMB). Vytvoření propojených identit (federace) pro účely využívání služeb MMB městskými organizacemi.
3	Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a kybernetické odolnosti	Vyspělost bezpečnostního modelu města	2025	Je nasazena a provozována centrální technologie automatizovaných detekcí zranitelností v rámci sítě MMB. V rozsahu MMB je realizován systém vizualizace stavu kritických služeb.
			2026	Vytvořen a provozován centrální systém automatizované reakce na detekované a kategorizované KBI. V rozsahu SMB je realizován systém vizualizace stavu kritických služeb. Zavedení vícefaktorového ověřování uživatelů a zařízení včetně pokročilých funkcí správy identit. Zjištěn zájem ÚMČ, příspěvkových organizací a městských firem (organizace SMB) využívat centrální služby pro detekci zranitelností v jejich sítích.
			2027	Rozvoj systému vizualizace stavu kritických služeb v SMB o další služby.

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	2025	Dosažení plné redundance systémů v rámci dvou geograficky oddělených center.
5	Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace	Obsazení rolí	2025 2026 2027	Vydefinovat role analytiků potřeb uživatelů pro zjišťování potřeb uživatelů a jejich realizovatelnost v ICT prostředí. Vydefinovat role pro technickou podporu ÚMČ. Vznik pracoviště pro analýzu potřeb uživatelů s novými funkčními místy. Rozvoj pracoviště pro analýzu potřeb uživatelů.
6	Využívat workflow služeb přes jednotné prezentační rozhraní	Zavedeno workflow služeb na portálu i městské aplikaci	2025 2026	Výběr pilotních služeb a návrh jejich workflow. Optimalizace workflow pilotních služeb pro cílový stav k využití ve webovém portálu služeb a v městské aplikaci. Workflow u aplikací poskytujících služby úřadu přes portál i městskou aplikaci je navrženo ve spolupráci s garanty procesů a ORGO. Vyhodnocení zkušeností z nasazování služeb v roce 2025 a plán rozvoje na další rok.
7	Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby	Bezpečnostní standardy zavedeny	2025 2026 2027	Standard připojování MČ a městských organizací do LOG managementu. Zaveden systém řízení kybernetické bezpečnosti dle nového zákona o kybernetické bezpečnosti / direktivy NIS2. 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. Zaveden procesní model pro detekované KBI s možným dopadem nebo přesahem přes více než jednu součást SMB.
8	Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb	Katalog ICT služeb vytvořen	2025 2026	Katalog ICT služeb SMB je dokončen a rozšířen o služby pro eIDAS. Katalog ICT služeb SMB umožňuje využívat sdílené aplikační, infrastrukturní, platformové a bezpečnostní služby (včetně cloudu) jednotným způsobem, a to pro SMB a zřizované organizace města (městské firmy) v první verzi.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
			2027	Optimalizovaná verze katalogu ICT služeb SMB umožňující využívat sdílené aplikační, infrastrukturní, platformové a bezpečnostní služby (včetně 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	2025	Řízení metodami EA (Enterprise Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy. Vytvořena směrnice a pracovní postup pro zadávání architektonických prvků do centrální evidence.
			2026	Vytvořena směrnice a pracovní postup pro integraci dílčích agendových systémů. Systémy centrálně poskytované v rámci SMB jsou zavedeny v centrální evidenci.
			2027	Vybrané služby dané legislativou (RPP) jsou provázány na EA ve vhodné míře detailu. Nalezení způsobu provázání bezpečnostní architektury a Enterprise Architecture. Doplněny další služby z RPP provázané na EA.
10	Koordinovat rozvoj ICT města řízením projektového portfolia	Oblasti koordinace v projektovém porfoliu	2025	Projektové portfolio zahrnuje významné projekty z hlediska rozvoje ICT města a umožňuje jejich koordinované řízení v rámci OMI.
			2026	Koordinované řízení projektů je zavedeno na MMB.
			2027	Koordinované řízení projektů je zavedeno v rámci SMB.
12	Systematizovat řízení kybernetické bezpečnosti přes bezpečnostní architekturu a odolnost	Existuje bezpečnostní architektura SMB, která posiluje celkovou bezpečnost SMB a umožňuje včasnou a pohotovou reakci na incidenty	2025	Zpracování podkladů ke stávající situaci dle požadavků platné legislativy.
			2026	Vytvoření bezpečnostní architektury na základě nového systému řízení a informací o technologické vrstvě ICT. Je navržena technologická koncepce propojených bezpečnostních opatření vedoucích k jednotnému řízení architektury KB SMB.
			2027	Implementace bezpečnostních standardů v rozsahu MMB a zavedení procesů jejich kontroly.
			2028	Vytvoření závazných pravidel pro subjekty SMB s účelem dosažení jednotné bezpečnostní architektury poskytovaných služeb.
			2029	Jsou zavedeny procesy pro krizové řízení a řešení incidentů napříč SMB bez ohledu na jejich rozsah využívající možnosti sdílené architektury.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
11	Poskytovat elektr. služby přes webový portál služeb a mobilní aplikaci	Životní situace řešeny elektronicky přes portál služeb či mobilní aplikaci	2025 2026 2027 2028 2029	Platební brána je implementována pro služby vyžadující platby. Pilotní prověření vybrané služby přes webový portál služeb a mobilní aplikaci. Nasazení zvolených služeb přes webový portál služeb a mobilní aplikaci. Vytvoření datové analytiky pro zrychlení a optimalizaci průběhu procesu. Rozvoj služeb přes mobilní aplikaci a webový portál služeb. Rozvoj služeb přes mobilní aplikaci a webový portál služeb. Rozvoj služeb přes mobilní aplikaci a webový portál služeb.
13	Podporovat využívání služeb městského cloudu organizacemi SMB	Městské cloudové služby využívány městskými firmami	2026 2027 2028	Portál umožňuje objednávání služeb městského cloudu (objednávkový portál cloudových služeb). Přístup ke službám městského cloudu je zajištěn pro všechny organizace SMB. Rozvoj portfolia služeb.
14	Rozšířit využívání centrálních aplikací podle závazných standardů	ICT služby poskytované SMB standardizovány	2025 2026 2027	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). Městský cloud je ve shodě s uveřejněnými podmínkami 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 podmínkami 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.
15	Zavést dlouhodobou správu služeb	Spolupracující subjekty	2025 2026	V případě více garantů u významných ICT projektů bude určen správce služeb (koordinátor). Správce služeb (koordinátor) je stanoven u všech služeb uvedených v katalogu služeb, na kterých se podílí více garantů.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
16	Digitalizovat služby města	Očekávané přínosy z elektronizace služeb dosaženy	2026 2027 až 2029	Město disponuje elektronicky poskytovanými službami pro všechny zvolené služby (1. etapa). Vyhodnoceny přínosy z digitalizovaných služeb. Doplněny nové služby (2. etapa).
17	Vytvořit moderní, společné a bezpečné ICT města	ICT města sdíleno	2026 2027 2028	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	Centrálně řídit ICT města	Centralizace řízení ICT	2025 2026	Řízení ICT města je prováděno centralizovaně na projektové a architektonické úrovni orgánem zřízeným Radou města (tj. Řídícím orgánem ICT SMB). ICT služby jsou dlouhodobě koordinovány určenými správci služeb.
19	Dosahovat soulad s digitální legislativou (compliance)	Legislativní požadavky jsou naplňovány v plném rozsahu na celém území SMB	2025 2026 2028 2029	Návrh a implementace nových opatření plynoucích z aktuálních legislativních změn. Zajištění souladu městských standardů a interních normativních aktů s legislativním prostředím v oblasti IT včetně mechanismů periodického přezkoumávání. Revize interních normativů a rozšíření platných standardů na celé SMB. Poskytované služby a jejich podpůrné systémy jsou v souladu s platnou legislativou a tento soulad je pravidelně ověřován na základě standardů.

4.2. Strategické ICT projekty

Na pokrytí 19 strategických cílů byly navrženy následující strategické ICT projekty:

1. Jednotná aplikace města Brna / JAMB (Webová a mobilní platforma města Brna)
2. Digitální služby města Brna (přes JAMB)
3. Služby autentikace podle eIDAS
4. Systematizace řízení kybernetické bezpečnosti
5. Zajištění odolnosti
6. Zavedení dohledových a reaktivních technologií
7. Centrální služby a aplikace, služby a aplikace v cloudu
8. Koordinace, standardizace a architektura
9. Systém řízení projektového portfolia

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. Jednotná aplikace města Brna / JAMB (Webová a mobilní platforma města Brna)

Účel strategického projektu:

Přínosový cíl 16. *Digitalizovat služby města*.

Cíle strategického projektu:

1	Vytvořit mobilní aplikaci a webový portál služeb	2025	Připraven katalog služeb pro občany a návštěvníky města. Vytvořen koncept integrace aplikací do webového portálu služeb. Vytvořen koncept integrace aplikací do mobilní aplikace. Součástí webového portálu služeb je řešení jeho kybernetické bezpečnosti. Město provozuje webový portál služeb v souladu s moderními technologickými a bezpečnostními standardy. Je vytvořen plán rozvoje webového portálu služeb.
		2026	Město provozuje mobilní aplikaci v souladu s moderními technologickými a bezpečnostními standardy v 1. produkční verzi. Je vytvořen plán rozvoje mobilní aplikace. Rozvoj webového portálu služeb podle plánu.
		2027	Rozvoj mobilní aplikace o nové služby podle plánu. Rozvoj webového portálu služeb podle plánu.
		2028	Rozvoj mobilní aplikace o nové služby podle plánu. Rozvoj webového portálu služeb podle plánu.
		2029	Rozvoj mobilní aplikace o nové služby podle plánu. Rozvoj webového portálu služeb podle plánu.
5	Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace	2025	Vydefinovat role analytiků potřeb uživatelů pro zjišťování potřeb uživatelů a jejich realizovatelnost v ICT prostředí. Vydefinovat role pro technickou podporu ÚMČ.
		2026	Vznik pracoviště pro analýzu potřeb uživatelů s novými funkčními místy (pro rozvoj mobilní aplikace a webového portálu služeb).
		2027	Rozvoj pracoviště pro analýzu potřeb uživatelů.

4.2.2. Digitální služby města Brna (přes JAMB)

Účel strategického projektu:

Přínosový cíl 16. *Digitalizovat služby města*.

Cíle strategického projektu:

6	Využívat workflow služeb přes jednotné prezentační rozhraní	2025	Výběr pilotních služeb a návrh jejich workflow. Optimalizace workflow pilotních služeb pro cílový stav k využití ve webovém portálu služeb a v městské aplikaci. Workflow u aplikací poskytujících služby úřadu přes portál i městskou aplikaci je navrženo ve spolupráci s garanty procesů a ORGO.
		2026	Vyhodnocení zkušeností z nasazování služeb v roce 2025 a plán rozvoje na další rok.
11	Poskytovat elektr. služby přes webový portál služeb a mobilní aplikaci	2025	Platební brána je implementována pro služby vyžadující platby. Pilotní prověření vybrané služby přes webový portál služeb a mobilní aplikaci.
		2026	Nasazení zvolených služeb přes webový portál služeb a mobilní aplikaci.
		2027	Vytvoření datové analytiky pro zrychlení a optimalizaci průběhu procesu. Rozvoj služeb přes mobilní aplikaci a webový portál služeb.
		2028	Rozvoj služeb přes mobilní aplikaci a webový portál služeb.
		2029	Rozvoj služeb přes mobilní aplikaci a webový portál služeb.

4.2.3. Služby autentikace podle eIDAS

Účel strategického projektu:

Přínosový cíl 16. *Digitalizovat služby města*.
Přínosový cíl 17. *Vytvořit moderní, společné a bezpečné ICT města.*

Cíle strategického projektu:

2	Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty)	2025	Konsolidace domén a AD (Active Directory).
		2026	Autentizační brána IDM je využívána pro potřeby aplikací/služeb města (SMB). Vytvoření propojených identit (federace) pro účely využívání služeb MMB městskými organizacemi.

4.2.4. Systematizace řízení kybernetické bezpečnosti

Účel strategického projektu:

Přínosový cíl 19. *Dosahovat soulad s digitální legislativou (compliance).*
Přínosový cíl 17. *Vytvořit moderní, společné a bezpečné ICT města.*

Cíle strategického projektu:

7	Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby	2025	Standard připojování MČ a městských organizací do LOG managementu. Zaveden systém řízení kybernetické bezpečnosti dle nového zákona o kybernetické bezpečnosti / direktivy NIS2. Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro městské akciové společnosti a pro významné příspěvkové organizace.

		2026 2027	Úroveň bezpečnosti a důvěryhodnosti elektronicky poskytovaných služeb je periodicky hodnocena a prokazována na základě jasných metodik vyplývajících z přijatých standardů. Zaveden procesní model pro detekované KBI s možným dopadem nebo přesahem přes více než jednu součást SMB.
12	Systematizovat řízení kybernetické bezpečnosti přes bezpečnostní architekturu a odolnost	2025 2026 2027 2028 2029	Zpracování podkladů ke stávající situaci dle požadavků platné legislativy. Vytvoření bezpečnostní architektury na základě nového systému řízení a informací o technologické vrstvě ICT. Je navržena technologická koncepce propojených bezpečnostních opatření vedoucích k jednotnému řízení architektury KB SMB. Implementace bezpečnostních standardů v rozsahu MMB a zavedení procesů jejich kontroly. Vytvoření závazných pravidel pro subjekty SMB s účelem dosažení jednotné bezpečnostní architektury poskytovaných služeb. Jsou zavedeny procesy pro krizové řízení a řešení incidentů napříč SMB bez ohledu na jejich rozsah využívající možnosti sdílené architektury.

4.2.5. 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	2025	Dosažení plné redundance systémů v rámci dvou geograficky oddělených center.

4.2.6. Zavedení dohledových a reaktivních technologií

Účel strategického projektu:

Přínosový cíl 17. *Vytvořit moderní, společné a bezpečné ICT města*.
Přínosový cíl 19. *Dosahovat soulad s digitální legislativou (compliance).*

Cíle strategického projektu:

3	Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a kybernetické odolnosti	2025 2026	Je nasazena a provozována centrální technologie automatizovaných detekcí zranitelností v rámci sítě MMB. V rozsahu MMB je realizován systém vizualizace stavu kritických služeb. Vytvořen a provozován centrální systém automatizované reakce na detekované a kategorizované KBI. V rozsahu SMB je realizován systém vizualizace stavu kritických služeb. Zavedení vícefaktorového ověřování uživatelů a zařízení včetně pokročilých funkcí správy identit. Zjištěn zájem ÚMČ, příspěvkových organizací a městských firem (organizace SMB) využívat centrální služby pro detekci zranitelností v jejich sítích.

		2027	Rozvoj systému vizualizace stavu kritických služeb v SMB o další služby.

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:

8	Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb	2025 2026 2027	Katalog ICT služeb SMB je dokončen a rozšířen o služby pro eIDAS. Katalog ICT služeb SMB umožňuje využívat sdílené aplikační, infrastrukturní, platformové a bezpečnostní služby (včetně cloudu) jednotným způsobem, a to pro SMB a zřizované organizace města (městské firmy) v první verzi. Optimalizovaná verze katalogu ICT služeb SMB umožňující využívat sdílené aplikační, infrastrukturní, platformové a bezpečnostní služby (včetně cloudu) jednotným způsobem, a to pro SMB a zřizované organizace města (městské firmy).
13	Podporovat využívání služeb městského cloudu organizacemi SMB	2026 2027 2028	Portál umožňuje objednávání služeb městského cloudu (objednávkový portál cloudových služeb). Přístup ke službám městského cloudu je zajištěn pro všechny organizace SMB. Rozvoj portfolia služeb.

4.2.8. Koordinace, standardizace a architektura

Účel strategického projektu:

Přínosový cíl 18. *Centrálně řídit ICT města*.

Cíle strategického projektu:

5	Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace	2025 2026 2027	Vydefinovat role analytiků potřeb uživatelů pro zjišťování potřeb uživatelů a jejich realizovatelnost v ICT prostředí. Vydefinovat role pro technickou podporu ÚMČ. Vznik pracoviště pro analýzu potřeb uživatelů s novými funkčními místy. Rozvoj pracoviště pro analýzu potřeb uživatelů.
9	Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy	2025 2026 2027	Řízení metodami EA (Enterprise Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy. Vytvořena směrnice a pracovní postup pro zadávání architektonických prvků do centrální evidence. Vytvořena směrnice a pracovní postup pro integraci dílčích agendových systémů. Systémy centrálně poskytované v rámci SMB jsou zavedeny v centrální evidenci. Vybrané služby dané legislativou (RPP) jsou provázány na EA ve vhodné míře detailu. Nalezení způsobu provázání bezpečnostní architektury a Enterprise Architecture. Doplněny další služby z RPP provázané na EA.

14	Rozšířit využívání centrálních aplikací podle závazných standardů	2025 2026 2027	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). Městský cloud je ve shodě s uveřejněnými podmínkami 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 podmínkami 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.
15	Zavést dlouhodobou správu služeb	2025 2026	V případě více garantů u významných ICT projektů bude určen správce služeb (koordinátor). Správce služeb (koordinátor) je stanoven u všech služeb uvedených v katalogu služeb, na kterých se podílí více garantů.

4.2.9. Systém řízení projektového portfolia

Účel strategického projektu:

Přínosový cíl 18. *Centrálně řídit ICT města*.

Cíle strategického projektu:

10	Koordinovat rozvoj ICT města řízením projektového portfolia	2025 2026 2027	Projektové portfolio zahrnuje významné projekty z hlediska rozvoje ICT města a umožňuje jejich koordinované řízení v rámci OMI. Koordinované řízení projektů je zavedeno na MMB. Koordinované řízení projektů je zavedeno v rámci SMB.

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		2025	2026	2027	2028	2029
Cíl	**Jednotná aplikace města Brna / JAMB (Webová a mobilní platforma města Brna)**					
1	Připraven katalog služeb pro občany a návštěvníky města.					
1	Vytvořen koncept integrace aplikací do webového portálu služeb.					
1	Vytvořen koncept integrace aplikací do mobilní aplikace.					
1	Součástí webového portálu služeb je řešení jeho kybernetické bezpečnosti.					
1	Město provozuje webový portál služeb v souladu s moderními technologickými a bezpečnostními standardy.					
1	Je vytvořen plán rozvoje webového portálu služeb.					
1	Město provozuje mobilní aplikaci v souladu s moderními technologickými a bezpečnostními standardy v 1. produkční verzi.					
1	Je vytvořen plán rozvoje mobilní aplikace.					
1	Rozvoj webového portálu služeb podle plánu.					
1	Rozvoj mobilní aplikace o nové služby podle plánu.					
1	Rozvoj webového portálu služeb podle plánu.					
1	Rozvoj mobilní aplikace o nové služby podle plánu.					
1	Rozvoj webového portálu služeb podle plánu.					
1	Rozvoj mobilní aplikace o nové služby podle plánu.					
1	Rozvoj webového portálu služeb podle plánu.					
5	Vznik pracoviště pro analýzu potřeb uživatelů s novými funkčními místy (pro rozvoj mobilní aplikace a webového portálu služeb).					

Strategické projekty		2025	2026	2027	2028	2029
Cíl	**Digitální služby města Brna (přes JAMB)**					
6	Výběr pilotních služeb a návrh jejich workflow. Optimalizace workflow pilotních služeb pro cílový stav k využití ve webovém portálu služeb a v městské aplikaci.					
6	Workflow u aplikací poskytujících služby úřadu přes portál i městskou aplikaci je navrženo ve spolupráci s garanty procesů a ORGO.					
6	Vyhodnocení zkušeností z nasazování služeb v roce 2025 a plán rozvoje na další rok.					
11	Platební brána je implementována pro služby vyžadující platby.					
11	Pilotní prověření vybrané služby přes webový portál služeb a mobilní aplikaci.					
11	Nasazení zvolených služeb přes webový portál služeb a mobilní aplikaci.					
11	Vytvoření datové analytiky pro zrychlení a optimalizaci průběhu procesu.					
11	Rozvoj služeb přes mobilní aplikaci a webový portál služeb.					
11	Rozvoj služeb přes mobilní aplikaci a webový portál služeb.					
11	Rozvoj služeb přes mobilní aplikaci a webový portál služeb.					
Cíl	**Služby autentikace podle eIDAS**					
2	Konsolidace domén a AD (Active Directory).					
2	Autentizační brána IDM je využívána pro potřeby aplikací/služeb města (SMB).					
2	Vytvoření propojených identit (federace) pro účely využívání služeb MMB městskými organizacemi.					
Cíl	**Systematizace řízení kybernetické bezpečnosti**					
7	Standard připojování MČ a městských organizací do LOG managementu.					
7	Zaveden systém řízení kybernetické bezpečnosti dle nového zákona o kybernetické bezpečnosti / direktivy NIS2.					

Strategické projekty		2025	2026	2027	2028	2029
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.					
7	Zaveden procesní model pro detekované KBI s možným dopadem nebo přesahem přes více než jednu součást SMB.					
12	Zpracování podkladů ke stávající situaci dle požadavků platné legislativy.					
12	Vytvoření bezpečnostní architektury na základě nového systému řízení a informací o technologické vrstvě ICT.					
12	Je navržena technologická koncepce propojených bezpečnostních opatření vedoucích k jednotnému řízení architektury KB SMB.					
12	Implementace bezpečnostních standardů v rozsahu MMB a zavedení procesů jejich kontroly.					
12	Vytvoření závazných pravidel pro subjekty SMB s účelem dosažení jednotné bezpečnostní architektury poskytovaných služeb.					
12	Jsou zavedeny procesy pro krizové řízení a řešení incidentů napříč SMB bez ohledu na jejich rozsah využívající možnosti sdílené architektury.					
Cíl	**Zajištění odolnosti**					
4	Dosažení plné redundance systémů v rámci dvou geograficky oddělených center.					
Cíl	**Zavedení dohledových a reaktivních technologií**					
3	V rozsahu metropolitní sítě Brno (MSB) a na vybraných veřejných bodech MSB je nasazena a provozována centrální technologie automatizovaných detekcí zranitelností.					
3	V rozsahu MMB je realizován systém vizualizace stavu kritických služeb.					
3	Vytvořen a provozován centrální systém automatizované reakce na detekované a kategorizované KBI.					
3	V rozsahu SMB je realizován systém vizualizace stavu kritických služeb.					
3	Zavedení vícefaktorového ověřování uživatelů a zařízení včetně pokročilých funkcí správy identit.					

	Strategické projekty	2025	2026	2027	2028	2029
3	Zjištěn zájem ÚMČ, příspěvkových organizací a městských firem (organizace SMB) využívat centrální služby pro detekci zranitelností v jejich sítích.					
3	Rozvoj systému vizualizace stavu kritických služeb v SMB o další služby.					
Cíl	**Centrální služby a aplikace, služby a aplikace v cloudu**					
8	Katalog ICT služeb SMB je dokončen a rozšířen o služby pro eIDAS.					
8	Katalog ICT služeb SMB umožňuje využívat sdílené aplikační, infrastrukturní, platformové a bezpečnostní služby (včetně cloudu) jednotným způsobem, a to pro SMB a zřizované organizace města (městské firmy) v první verzi.					
8	Optimalizovaná verze katalogu ICT služeb SMB umožňující využívat sdílené aplikační, infrastrukturní, platformové a bezpečnostní služby (včetně cloudu) jednotným způsobem, a to pro SMB a zřizované organizace města (městské firmy).					
13	Portál umožňuje objednávání služeb městského cloudu (objednávkový portál cloudových služeb).					
13	Přístup ke službám městského cloudu je zajištěn pro všechny organizace SMB.					
13	Rozvoj portfolia služeb.					
Cíl	**Koordinace, standardizace a architektura**					
5	Vydefinovat role analytiků potřeb uživatelů pro zjišťování potřeb uživatelů a jejich realizovatelnost v ICT prostředí.					
5	Vydefinovat role pro technickou podporu ÚMČ.					
5	Vznik pracoviště pro analýzu potřeb uživatelů s novými funkčními místy.					
5	Rozvoj pracoviště pro analýzu potřeb uživatelů.					
9	Řízení metodami EA (Enterprise Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy.					
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	Systémy centrálně poskytované v rámci SMB jsou zavedeny v centrální evidenci.					

Strategické projekty		2025	2026	2027	2028	2029
9	Vybrané služby dané legislativou (RPP) jsou provázány na EA ve vhodné míře detailu.					
9	Nalezení způsobu provázání bezpečnostní architektury a Enterprise Architecture.					
9	Doplněny další služby z RPP provázané na EA.					
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	Městský cloud je ve shodě s uveřejněnými podmínkami 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.					
14	Centrálně poskytované aplikace budou ve shodě s podmínkami 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 ...).					
14	Jsou využívány a udržovány technologické, architektonické a bezpečnostní standardy ICT SMB.					
15	V případě více garantů u významných ICT projektů bude určen správce služeb (koordinátor).					
15	Správce služeb (koordinátor) je stanoven u všech služeb uvedených v katalogu služeb, na kterých se podílí více garantů.					
Cíl	**Systém řízení projektového portfolia**					
10	Projektové portfolio zahrnuje významné projekty z hlediska rozvoje ICT města a umožňuje jejich koordinované řízení v rámci OMI.					
10	Koordinované řízení projektů je zavedeno na MMB.					
10	Koordinované řízení projektů je zavedeno v rámci SMB.					

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 za 2 roky	Aktualizovaný dokument Informační strategie
	Při změně nadřazené Vize a Strategie #brno 2050	
Portfolio strategických ICT projektů	1 x kvartálně	Hlášení o stavu portfolia strategických ICT projektů
	Při vzniku výjimečné situace na některém ze strategických projektů	