Z9/37. zasedání Zastupitelstva města Brna
konané dne 15.9.2026

9. Návrh aktualizace Informační strategie města Brna na období 2026 - 2030

Anotace

Informační strategie rozpracovává cíl strategie pro Brno, rozvíjení informačního systému v rámci Magistrátu města Brna a městských částí, do systému 11 vzájemně provázaných strategických cílů. 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.

Návrh usnesení

Zastupitelstvo města Brna

1. schvaluje aktualizaci Informační strategie města Brna na období 2026 - 2030, která tvoří přílohu č. … tohoto zápisu

2. ukládá Radě města Brna

- naplňovat jednotlivé cíle obsažené v Informační strategii města Brna na období 2026 - 2030
T: průběžně

- předkládat Zastupitelstvu města Brna ke schválení aktualizace Informační strategie města Brna na období 2026 - 2030
T: jedenkrát za dva roky

Stanoviska

Rada města Brna projednala materiál na své schůzi R9/187 konané dne 29. 7. 2026
a **doporučila** ZMB ke schválení.

Podpis zpracovatele pro archivaci

Zpracovatel

Elektronicky podepsáno

Ing. David Menšík

vedoucí odboru - Odbor městské informatiky

20.8.2026 v 13:34

Garance správnosti, zákonnosti materiálu

Spolupodepisovatel

Elektronicky podepsáno

Bc. Tomáš Aberl

člen RMB - Člen Rady města Brna - předkladatel/ka

17.8.2026 v 08:03

Obsah materiálu

Důvodová zpráva:

Rada města Brna předkládá Zastupitelstvu města Brna aktualizovaný dokument „Informační strategie města Brna na období 2026 – 2030“ verze 7.0. Tento dokument je výstupem činnosti pracovní skupiny pro aktualizaci informační strategie, jmenované RMB, složené ze zástupců politického vedení města, pracovníků Magistrátu města Brna a Technických sítí Brno akciová společnost. Informační strategie města Brna byla zpracována pro období let 2026 – 2030 jako strategický dokument, který je návrhem postupu k dosažení cílového stavu informatiky města Brna do horizontu konce roku 2030.

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

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

Následující tabulka uvádí souhrn strategických cílů (viz. tabulka 1 z dokumentu „Informační strategie města Brna na období 2026 – 2030“).

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	Komunikovat nabídku a poskytovat jednotné 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 ICT služeb SMB
Procesy	Umožnit technologiemi elektronické služby	Využívat workflow služeb s optimalizovanými interními procesy 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 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 Navázat úzkou spolupráci OMI-ORGO Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a kybernetické odolnosti Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace

Pro každý z cílů je stanovena metrika a jeho rozpad do stavu dosaženého v jednotlivých letech 2026 – 2030. Naplnění strategických cílů je plánováno realizovat 7 strategickými ICT projekty (resp. programy, pokud se budou dále realizačně členit) rozloženými do let 2026 až 2030. 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. Stanovením strategických cílů jsou nastaveny dlouhodobé priority směrem ke chtěnému plánovanému stavu.

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

Rada města Brna projednala materiál na své schůzi R9/187 konané dne 29. 7. 2026 a doporučila ZMB ke schválení.

Schváleno jednomyslně **9 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
pro	pro	pro	pro	pro	pro	pro	-	pro	pro	-

Komise pro informační technologie RMB na svém 42. jednání dne 21. 7. 2026 projednala a doporučila RMB přijmout usnesení.

Hlasování:
pro-proti-zdržel se-nehlasoval: **7-0-1-0/8**

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

Materiál nepodléhá projednání ve výborech RMB.

Analýza současného stavu (SWOT)

Strategické cíle (na období 2026 až 2030)

Strategická mapa (Balanced Scorecard schéma)

Implementace strategie (strategické projekty)

Informační strategie města Brna

Na období 2026 - 2030

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
7.00	11.6.2026	Per Partes	Aktualizace strategie na období 2026 až 2030	260611 Informacni strategie (SMB) v7_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 lednu 2026 až červnu 2026. 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 2030. 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 2025.

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 2030. 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	Komunikovat nabídku a poskytovat jednotné 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 ICT služeb SMB
Procesy	Umožnit technologiemi elektronické služby	Využívat workflow služeb s optimalizovanými interními procesy 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 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 Navázat úzkou spolupráci OMI-ORGO Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a kybernetické odolnosti 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 7 strategickými ICT projekty (resp. programy, pokud se budou dále realizačně členit) rozloženými do let 2026 až 2030. 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	2026	2027	2028	2029	2030
Jednotná aplikace města Brna / JAMB (Webová a mobilní platforma města Brna)					
Digitální služby města Brna (přes JAMB)					
Systematizace řízení kybernetické bezpečnosti					
Zavedení dohledových a reaktivních technologií (včetně visibility služeb)					
Centrální služby a aplikace (katalog ICT služeb SMB)					
Architektura a koordinace					
Technologický standard SMB					

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	Nejméně 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	

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	vedoucí referátu Projektového řízení, Odbor městské informatiky
Barbora Raputová	manažer projektu AISMB, Odbor městské informatiky
František Sedláček	koordinátor KB, Kancelář kybernetické bezpečnosti
Kristýna Bukalová	architekt kybernetické bezpečnosti, Kancelář kybernetické bezpečnosti
Eva Chaloupková	vedoucí Organizačního odboru
Jaroslav Petrák	Odbor strategického rozvoje a spolupráce
Michal Jukl	ředitel ICT, TSB
Roman Veselý	manažer kybernetické bezpečnosti, TSB
Jan Zachoval	podniková architektura, Aricoma Systems, a. s.
Lukáš Vlček	podniková architektura, Aricoma Systems, a. s.
Jiří Michálek	solution manager, Aricoma Systems, a. s.
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	Solkind s.r.o., advokátní kancelář
Stanislav Mozgva	Solkind s.r.o., advokátní kancelář

Předmět:	Předmětem aktualizace informační strategie je informatika města Brna v letech 2026 až 2030. 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 2026 - 2030. 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, pátá aktualizace 12.3.2025 a šestá aktualizace 11.6.2026. 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 2030 • 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. Uvedený přehled není vyčerpávající a má orientační povahu; s ohledem na dynamický vývoj právní úpravy v oblasti informačních a komunikačních technologií je nezbytné při naplňování Informační strategie města Brna vždy vycházet z aktuálního znění příslušných právních předpisů a zohlednit i předpisy, které do tohoto přehledu nebyly zařazeny.

Právní předpisy ČR:

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

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

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

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

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

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

- Zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů
- Zákon č. 240/2000 Sb., o krizovém řízení, ve znění pozdějších předpisů
- **Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů**

  Zákon **o informačních systémech veřejné správy**[1] stanovuje práva a povinnosti osob, jež souvisejí s vytvářením, správou, provozem a rozvojem určitých informačních systémů veřejné správy (např. Portál veřejné správy), jakož i z toho vyplývajících informačních systémů (např. Czech POINT). Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností. Tato data jsou potřebná jednak pro jiné informační systémy, jednak pro zajištění správních činností příslušných orgánů. Z působnosti zákona jsou naopak vyňaty informační systémy veřejné správy spravované buďto pro potřeby nakládání s utajovanými informacemi, zpravodajskými službami, Národním bezpečnostním úřadem a Národním úřadem pro kybernetickou a informační bezpečnost.
- Zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů – *bude zrušeno k 1. 1. 2027 a nahrazeno zákonem č. 231/2025 Sb.*
- **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

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.

podmínky podnikání a výkon státní správy, včetně regulace trhu, v oblasti elektronických komunikací. Právní úprava zde obsažená reguluje především přenos informací prostřednictvím sítí elektronických komunikací a rozhlasového a televizního vysílání. Z věcné působnosti zákona je naopak vyňat obsah rozhlasového či televizního vysílání, jakož i obsah sdílený prostřednictvím internetu.

- **Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů**

  Zákon o ochraně utajovaných informací upravuje podmínky pro ochranu utajovaných informací, včetně personální, administrativní, fyzické a informační bezpečnosti a bezpečnosti informačních a komunikačních systémů, a dále podmínky bezpečnostní způsobilosti k výkonu tzv. citlivých činností. Pro Statutární město Brno je zákon relevantní zejména v návaznosti na zákon č. 266/2025 Sb., o kritické infrastruktuře, podle něhož je výkon funkce manažera kritické infrastruktury citlivou činností podmíněnou způsobilostí podle tohoto zákona, a dále při provozu informačních systémů, v nichž by byly zpracovávány utajované informace.

- **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

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

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

- Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
- Zákon č. 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. 222/2016 Sb., o Sbírce zákonů a mezinárodních smluv a o tvorbě právních předpisů vyhlašovaných ve Sbírce zákonů a mezinárodních smluv (zákon o Sbírce zákonů a mezinárodních smluv), ve znění pozdějších předpisů**

  Zákon zavádí elektronickou Sbírku zákonů a mezinárodních smluv (e-Sbírka) a elektronický legislativní proces (eSEL) a upravuje tvorbu, vyhlašování a zpřístupňování právních předpisů v digitální podobě; účinnosti nabyl k 1. 1. 2024. Třebaže se zákon primárně vztahuje na celostátní právní předpisy, pro Statutární město Brno je relevantní jako součást širšího rámce elektronizace a zpřístupňování práva (ve vazbě na zákon č. 35/2021 Sb., o Sbírce právních předpisů územních samosprávných celků) a při napojení informačních systémů města na centrální služby eGovernmentu.

- **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

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.

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.

též působnost Ministerstva vnitra a Správy základních registrů na úseku elektronické identifikace. Zahrnuta byla též právní úprava přestupků na úseku elektronické identifikace.

- **Zákon č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů**

  Zákon **o zpracování osobních údajů** transponuje a v určitých směrech doplňuje nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

- **Zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů**

  Zákon o přístupnosti transponuje do českého právního řádu směrnici (EU) 2016/2102 a ukládá povinným subjektům, včetně územních samosprávných celků, zajistit přístupnost svých internetových stránek a mobilních aplikací. Stanoví mimo jiné povinnost zveřejňovat prohlášení o přístupnosti a dodržovat příslušné technické standardy (harmonizované normy). Pro Statutární město Brno jde o přímo relevantní úpravu ve vazbě na strategický projekt jednotné aplikace města Brna (webová a mobilní platforma) a na poskytování digitálních služeb prostřednictvím těchto kanálů.

  Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů

  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. 35/2021 Sb., o Sbírce právních předpisů územních samosprávných celků a některých správních úřadů, ve znění pozdějších předpisů**

  Zákon zavádí elektronickou Sbírku právních předpisů územních samosprávných celků a některých správních úřadů a stanoví pravidla pro vyhlašování a zpřístupňování právních předpisů obcí (zejména obecně závazných vyhlášek a nařízení) prostřednictvím jednotného informačního systému. Pro Statutární město Brno jako původce vlastních právních předpisů z něj plynou povinnosti při jejich elektronickém vyhlašování a publikaci, které je třeba zohlednit při rozvoji informačních systémů města.

- Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci
- Zákon č. 231/2025 Sb., o řízení a kontrole veřejných financí – *bude účinný od 1. 1. 2027*
- **Zákon č. 264/2025 Sb., o kybernetické bezpečnosti**

  Zákon o kybernetické bezpečnosti je klíčový právní předpis, který upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zákon plně transponuje evropskou směrnici NIS 2 (EU) 2022/2555 do českého právního řádu a s účinností od 1. 11. 2025 nahrazuje dosavadní zákon č.

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.

181/2014 Sb. Vymezuje mimo jiné působnost Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) a dalších orgánů při zajišťování bezpečnosti informačních systémů, sítí a služeb důležitých pro fungování společnosti a státu. Cílem této právní úpravy je zásadním způsobem zvýšit odolnost vůči kybernetickým hrozbám, harmonizovat požadavky na zabezpečení sítí a systémů a posílit důvěru uživatelů v digitální infrastrukturu. Zákon významně rozšiřuje okruh regulovaných subjektů a služeb (včetně veřejné správy, zdravotnictví, energetiky či IT služeb) a pro tyto účely zavádí dva bezpečnostní režimy podle významu provozované služby: režim vyšších a režim nižších povinností. Nová regulace klade důraz na zavedení konkrétních organizačních a technických bezpečnostních opatření, která zahrnují řízení rizik, procesní kroky zabezpečení, kontrolu, audit a efektivní detekci a řešení kybernetických bezpečnostních incidentů.

- Zákon č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti
- Zákon č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře)
- Zákon o kritické infrastruktuře nabyl účinnosti dne 19. 8. 2025 a do českého právního řádu transponuje směrnici CER (EU) 2022/2557. Problematiku kritické infrastruktury vyčleňuje z dosavadního krizového zákona (zákon č. 240/2000 Sb.) a zavádí samostatnou úpravu odolnosti kritických subjektů. Namísto dřívějšího modelu založeného na jednotlivých prvcích kritické infrastruktury zavádí přístup zaměřený na subjekty poskytující tzv. základní služby (např. v odvětvích energetiky, dopravy, bankovnictví, zdravotnictví, dodávek vody, digitální infrastruktury či veřejné správy). Dotčeným subjektům ukládá zejména povinnost provádět posouzení rizik, zpracovat plán odolnosti, ověřovat spolehlivost pracovníků a hlásit závažné incidenty; současně zavádí funkci manažera kritické infrastruktury jako citlivou činnost. Zákon o kritické infrastruktuře a zákon o kybernetické bezpečnosti tvoří provázaný systém ochrany základních služeb a digitální bezpečnosti, který se vyhýbá duplicitám.
- Zákon č. 60/2026 Sb., o správě dat, o řízeném přístupu k datům a o změně některých souvisejících zákonů (zákon o správě dat a o řízeném přístupu k datům) – *bude účinný od 1. 1. 2028 a částečně od 1. 1. 2029*

Související podzákonné právní předpisy ČR:

- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, 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. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy
- Vyhláška č. 334/2025 Sb., o Portálu Národního úřadu pro kybernetickou a informační bezpečnost a požadavcích na některé úkony
- Vyhláška č. 408/2025 Sb., o regulovaných službách
- Vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
- Vyhláška č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností
- Vyhláška č. 411/2025 Sb., o bezpečnostních úrovních informačních systémů veřejné správy
- Vyhláška č. 412/2025 Sb., o bezpečnostních pravidlech pro orgány veřejné správy

využívající služby poskytovatelů cloud computingu

- Vyhláška č. 505/2025 Sb., o některých požadavcích pro zápis do katalogu cloud computingu

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 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) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu (eIDAS 2.0)**

  Revize nařízení eIDAS (tzv. eIDAS 2.0), účinná od 20. 5. 2024, zásadním způsobem rozšiřuje stávající rámec pro elektronickou identifikaci a služby vytvářející důvěru. Jejím těžištěm je zřízení evropského rámce pro digitální identitu a zavedení tzv. Evropské peněženky digitální identity (EU Digital Identity Wallet), kterou jsou členské státy povinny zpřístupnit občanům, rezidentům i právnickým osobám. Peněženka má sloužit jako bezpečný a standardizovaný prostředek pro uchovávání a selektivní sdílení ověřených údajů a elektronických potvrzení (atributů) napříč EU, a to vůči orgánům veřejné moci i soukromým subjektům.

- **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

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).

osobních údajů právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a kontaktních údajů právnické osoby.

- **Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV**

  Tzv. trestněprávní směrnice (Law Enforcement Directive, LED) upravuje zpracování osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů a výkonu trestů, tedy oblast, která je vyňata z působnosti GDPR. Do českého právního řádu je adaptována v hlavě třetí zákona č. 110/2019 Sb., o zpracování osobních údajů. Pro Statutární město Brno je relevantní zejména ve vazbě na činnost obecní (městské) policie a na provoz souvisejících informačních systémů a kamerových systémů využívaných při plnění úkolů v oblasti veřejného pořádku.

- **Směrnice Evropského parlamentu a Rady (EU) 2016/2102 ze dne 26. října 2016 o přístupnosti internetových stránek a mobilních aplikací subjektů veřejného sektoru**

  Směrnice o přístupnosti ukládá subjektům veřejného sektoru povinnost zajistit, aby jejich internetové stránky a mobilní aplikace byly přístupné, tj. vnímatelné, ovladatelné, srozumitelné a stabilní pro všechny uživatele, zejména osoby se zdravotním postižením. Do českého právního řádu je směrnice transponována zákonem č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací. Pro Statutární město Brno jde o přímo relevantní úpravu ve vazbě na strategický projekt jednotné aplikace města Brna (webová a mobilní platforma) a na poskytování digitálních služeb prostřednictvím těchto kanálů.

- **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.

- **Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích)**

  Tzv. směrnice ePrivacy upravuje ochranu soukromí a osobních údajů v odvětví elektronických komunikací, včetně pravidel pro ukládání informací a přístup k informacím v koncových zařízeních uživatelů (typicky tzv. cookies a obdobné sledovací technologie) a důvěrnosti sdělení. Do českého právního řádu je transponována zejména zákonem č. 127/2005 Sb., o elektronických komunikacích. Pro Statutární město Brno je relevantní při provozu internetových stránek a mobilní aplikace města, zejména při nasazování cookies, analýze návštěvnosti a dalších sledovacích technologií, kde je třeba řešit náležitosti souhlasu uživatele.

- Nařízení Evropského parlamentu a Rady (EU) č. 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii.

- **Nařízení Evropského parlamentu a Rady (EU) 2018/1724 ze dne 2. října 2018, kterým se zřizuje jednotná digitální brána pro poskytování přístupu k informacím, postupům**

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.

a k službám podpory a pro řešení problémů a kterým se mění nařízení (EU) č. 1024/2012 (nařízení o jednotné digitální bráně).

Nařízení o jednotné digitální bráně (Single Digital Gateway) zřizuje jednotné kontaktní místo, jehož prostřednictvím mají občané a podniky získat snadný online přístup k informacím, správním postupům a službám podpory napříč členskými státy EU. Klíčovým prvkem je tzv. zásada „pouze jednou“ (once-only), podle níž by orgány veřejné moci neměly opakovaně vyžadovat údaje, které již má veřejná správa k dispozici. Pro Statutární město Brno je nařízení relevantní zejména ve vazbě na strategický projekt jednotné aplikace města a digitálních služeb, neboť určuje standardy dostupnosti, srozumitelnosti a online dokončitelnosti vybraných postupů poskytovaných prostřednictvím elektronických kanálů.

- 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
- **Směrnice Evropského parlamentu a Rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru**

  Směrnice o otevřených datech (tzv. Open Data Directive) stanoví pravidla pro opakované použití informací veřejného sektoru a podporuje jejich zpřístupňování v otevřených a strojově čitelných formátech, včetně tzv. dynamických dat a datových souborů s vysokou hodnotou. Do českého právního řádu je transponována zejména zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění novely provedené zákonem č. 241/2022 Sb. (účinné od 1. 9. 2022), která zavedla institut otevřených dat a Národní katalog otevřených dat. Pro Statutární město Brno je směrnice relevantní při publikaci otevřených dat města a při provozu souvisejících informačních systémů a datových sad.
- Nařízení Evropského parlamentu a Rady (EU) 2019/1150 ze dne 20. června 2019 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) 2023/2854 ze dne 13. prosince 2023 o** harmonizovaných **pravidlech pro spravedlivý přístup k datům a jejich využívání a o**

změně nařízení (EU) 2017/2394 a směrnice (EU) 2020/1828 (akt o datech)

Akt o datech, účinný ode dne 12. září 2025, doplňuje akt o správě dat (nařízení (EU) 2022/868) a vytváří právní rámec pro spravedlivý přístup k datům generovaným připojenými výrobky a souvisejícími službami (zejména průmyslovým a IoT datem) a pro jejich sdílení. Stanoví pravidla pro přístup uživatelů k datům, která svým užíváním generují, pro jejich předávání třetím stranám, pro zpřístupňování dat subjektům veřejného sektoru za výjimečných okolností a pro usnadnění přechodu mezi poskytovateli služeb zpracování dat (cloudových služeb). Pro Statutární město Brno je nařízení relevantní zejména v kontextu řešení Smart City a zpracování dat z chytrých zařízení a senzorů (např. chytré parkování, měření kvality ovzduší), a to jak v pozici uživatele těchto dat, tak v pozici subjektu veřejného sektoru.

- **Nařízení Evropského parlamentu a Rady (EU) 2024/903 ze dne 13. března 2024, kterým se stanoví opatření pro vysokou úroveň interoperability veřejného sektoru v celé Unii (nařízení o interoperabilní Evropě)**

  Nařízení o interoperabilní Evropě (Interoperable Europe Act), použitelné ode dne 12. července 2024, stanoví opatření na podporu přeshraniční interoperability transevropských digitálních veřejných služeb a rámec pro jejich správu. Zavádí mimo jiné povinné posouzení interoperability před přijetím či výraznou změnou informačních systémů podporujících tyto služby, sdílení a opakované používání řešení interoperability a strukturovanou spolupráci veřejné správy, na níž se podle nařízení mohou podílet i regiony a města. Pro Statutární město Brno je nařízení relevantní při koordinaci, standardizaci a architektonickém řízení ICT města a při napojování městských systémů na centrální a transevropské digitální veřejné služby; úzce navazuje na nařízení o jednotné digitální bráně, akt o správě dat a akt o datech.

- 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**)
  - *Kapitoly I a II a kapitola III oddíl 4, kapitola V, kapitola VII a kapitola XII a článek 78 se použijí od 2. 8. 2025, s výjimkou článku 101.*
- 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)**
  - *Článek 14 se použije ode dne 11. 9. 2026 a kapitola IV (články 35 až 51) se použije ode dne 11. 6. 2026.*
- 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**)
  - *Článek 6 odst. 1 a odpovídající povinnosti stanovené v tomto nařízení se použijí ode dne 2. 8. 2027.*

- 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)**
  - *Nařízení se použije ode dne 11. 12. 2027. Výjimkou je článek 14, který se použije ode dne 11. 9. 2026 a kapitola IV (články 35 až 51), která se použije ode dne 11. 6. 2026.*

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.

Artificial Intelligence (AI) je umělá inteligence, tedy soubor metod a algoritmů, které umožňují systémům interpretovat data, učit se z nich a adaptivně vykonávat úkoly bez explicitního naprogramování každého kroku.

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.

Kancelář kybernetické bezpečnosti (KKB) je útvar Magistrátu města Brna, který zajišťuje a řídí kybernetickou bezpečnost města.

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

Kybernetický bezpečnostní incident (KBI) je událost nebo soubor událostí, které vedou nebo mohou vést k narušení důvěrnosti, integrity nebo dostupnosti informačních nebo komunikačních systémů či dat.

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.

Registr práv a povinností (RPP) je jeden ze základních registrů českého eGovernmentu.

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

1. Vytvořit mobilní aplikaci a webový portál služeb

Katalog služeb pro občany a návštěvníky města je připraven.

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

Probíhá veřejná zakázka „Jednotná aplikace města Brna“ formou jednacího řízení s uveřejněním s předpokládanou realizací první fáze v průběhu let 2026 a 2027.

Probíhá implementace webového portálu s moderními technologickými a bezpečnostními

standardy. Předpokládaná publikace veřejnosti v 2.Q 2026.

Byla vytvořena první verze návrhu plánu rozvoje webového portálu.

Předpokládané spuštění mobilní aplikace v první produkční verzi je v 2027. Je vytvořen plán rozvoje mobilní aplikace.

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

Konsolidace domén AD (Active Directory) probíhá s předpokladem dokončení v roce 2026.

Integrace služeb IDM do informačních systémů v rozsahu SŘBI je dokončována s předpokladem dokončení Q2 2026, zbývá realizovat aktivity v návaznosti s konsolidací AD (Active Directory). Cílovým stavem bude sjednocení přístupů do aplikací a zvýšení zabezpečení.

Autentizační brána je připravena k nasazení, je otestována a jsou promítnuty požadavky na změny – požadavky NZoKB.

Pro zajištění zvýšené odolnosti proti kybernetickým útokům je nutný upgrade technologické platformy - termín 2Q 2026.

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

Je licencován doplněk Microsoft 365 E5 Security add-on a aktivně provozována správa zranitelností Microsoft Defender XDR. Zbývá doladit procesní vrstvu sledování zranitelností tak, aby byla plně integrovaná do stávajícího bezpečnostního prostředí a architektury.

Byl pořízen systém pro visibilitu služeb ALTWORX, který umožnuje získávat aktuální informace o poskytovaných službách města v rozsahu regulované služby jak pro sledování provozních, tak security parametrů.

Proběhla konsolidace provozního prostředí Active Directory, která umožnila nasazení pokročilých trustů a bezpečnostních technologií odpovídajících aktuálním standardům a trendům. Tato konsolidace také umožní vystavení dalších prvků moderního bezpečnosntího ekosystému od infrastrukturní vrstvy přes aplikační, až po aplikaci moderních prvků pro uživatelskou správu bezpečnosti (VPN, MFA, ...)

Je nasazován systém prevence úniku dat (Data Loss Prevention systém), byla zvýšena ochrana některých dalších systémů jejich zařazením do log managementu a probíhá debata o integraci jednotlivých částí bezpečnostního ekosystému do komplexní technologické platformy, která by umožnila sledování a korelaci údajů z jednotlivých nástrojů pro získání lepšího vhledu do stavu prostředí jako celku.

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

TSB provozuje a poskytuje dvě geograficky oddělená a redundantní datová centra s dostatečnou kapacitou pro další rozvoj, a to jak poskytování vlastních služeb (viz níže), tak pro umístění infrastruktury SMB, případně dalších organizací či městských firem. Potenciál moderních datových center není nyní využíván v míře a rozsahu, v jaké by být využívám mohl.

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 typu Flowmon, které mají jako součást své výbavy moduly IDS a díky bezpečnému kanálu z dozorového centra (SOC) jsou schopny proaktivního zásahu v režimu 24/7.

Centrum MSB je zakončeno na MN3.

TSB poskytuje a rozvíjí digitální služby (IaaS, PaaS, SaaS) s využitím svých dvou datových center a v roce 2025 významně modernizovaného datového úložiště, a to především pro MČ, příspěvkové organizace. Základem jsou MSP/MSSP platformy, které umožňují kromě základní infrastruktury nabídnout služby provozního i bezpečnostního monitoringu, správy aktualizací, zálohování, identifikace zranitelností, detekce škodlivého kódu EDR/XDR, eIDAS služby (HSM) etc.

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

Vznikl nový Referát projektového řízení na OMI, který byl obsazen dvěma stávajícími funkčními místy a jedním novým funkčním místem.

Byly identifikovány okruhy činností rolí pro technickou podporu ÚMČ ze strany OMI.

Co se týče referátu KB, v uplynulém roce byla vytknuta nedostatečná personální kapacita referátu s ohledem na nutnost řešit právní a projektové záležitosti, hlavně s ohledem na vzrůstající komplexitu a propojenost regulatorních požadavků a požadavků vůči ÚMČ a koncernovým společnostem. Řešení problému se zatím hledá. Jinak je útvar personálně stabilní a má dostatek kapacit na všechny úkoly.

6. Využívat workflow služeb přes jednotné prezentační rozhraní

Optimalizace WF pro využití v mobilní aplikaci byla zpracována do zadávací dokumentace VZ pro vytvoření mobilní aplikace.

Pro webový portál služeb byla vybrána agenda poplatků za psa v působnosti 29 MČ.

7. Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby

Standard připojování MČ do LOG managementu je v přípravě, k posunutí termínu došlo kvůli odložení legislativy ze strany NÚKIBu, předpokládané dokončení do půlky roku 2026. Standard pro koncernové společnosti zaveden ve formě standardu připojení do systému řízení vizibility služeb od fy Altworx, jednotlivé bezpečnostní aspekty si společnosti mají zájem i nadále řídit samy.

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

Katalog ICT služeb OMI je dokončen a byl rozšířen o služby podle požadavků eIDAS (IDM, přístup do NIA).

TSB disponuje katalogem ICT a KB služeb, které jsou nabízeny a poskytovány ÚMČ, příspěvkovým organizacím SMB a koncernovým společnostem.

Je připraven návrh projektového záměru 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

Řízení metodami EA (Enterprise Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy.

V rámci Řídícího orgánu ICT pro řízení ICT SMB je využívána EA kancelář MMB k posouzení a koordinaci projektových záměrů SMB.

Byla vytvořena směrnice pro zadávání architektonických prvků do centrální evidence. Pracovní postup bude upraven s ohledem na rozložení centrální evidence pro aplikační část a infrastrukturní část v průběhu roku 2026.

Kancelář podnikové architektury se kromě aktualizace modelu ICT prostředí podle metodiky

TOGAF podílí i na mapování služeb a vazeb na požadavky výkonu agend z RPP. To se děje v souvislosti s požadavky novelizované legislativy pro oblast ISVS (zejména vyhlášky 360/2023 Sb. O dlouhodobém řízení ISVS).

10. Koordinovat rozvoj ICT města řízením projektového portfolia

Metodický pokyn Metodika Řízení projektů OMI byl doplněn o šablony dokumentů a projektovou knihovnu.

Řídící orgán ICT pro řízení ICT SMB standardně posuzuje projektové záměry v perimetru SMB.

Nové významné projekty SMB 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 je smluvně zajištěna u ČS v rámci pilotního nasazení.

Návrh řešení nasazení vybraných služeb byl zpracován do zadávací dokumentace VZ pro vytvoření mobilní aplikace.

Pro webový portál služeb byla vybrána agenda poplatků za psa v působnosti 29 MČ.

12. Systematizovat řízení kybernetické bezpečnosti přes bezpečnostní architekturu a odolnost

Legislativa nabyla platnosti 4. 8. 2025 a účinnosti až 1. 11. 2025 (Zákon č. 264/2025 Sb. o kybernetické bezpečnosti a Zákon č. 265/2025 Sb. kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti) jeho prováděcí předpisy jsou v účinnosti taktéž 1. 11. 2025.

Je vytvořená metodika slovního popisu bezpečnostní dokumentace, společný soubor bezpečnostních požadavků a plněných opatření, a šablony jednotlivých systémů. Tato metodika je částečně aplikovaná na AIS a ISVS ve správě OMI, je třeba ji dokončit a ověřit.

Po ověření bude dále zpracována do architektury a z její analýzy bude možné navrhnout další opatření.

Některé agendy jsou řešeny přes centrálně poskytované AIS/ISVS mimo správu OMI MMB. U těchto systémů se řeší způsob a podmínky nastavení bezpečného provozu. Některé budou například v blízké době vyžadovat vlastní MFA vynucené jejich dodavatelem, nebo budou potřebovat jiný technologický zásah, vynucený centrálně řízenou úrovní bezpečnosti.

13. Podporovat využívání služeb městského cloudu organizacemi SMB

V současné době se sjednocuje katalog ICT služeb SMB. Bude vytvořen portál ICT služeb SMB.

14. Rozšířit využívání centrálních aplikací podle závazných standardů

Centrální aplikace jsou poskytovány z prostředí MMB.

Byl dohodnut a nastaven výměnný formát mezi GPC a EA, započal proces kontroly jednotlivých systémů.

Pokračování tvorby technologického standardu je realizováno po personálním posílení OMI v oblasti dokumentování ICT prostředí SMB. Rozsah potřebných prací na standardech je značný a bude nutné vytvořenou dokumentaci průběžně udržovat. Cílovým stavem bude dokumentace v takové formě, aby bylo možné ji udržovat aktuální podle požadavků legislativy a zároveň byly

efektivně využívány omezené kapacity. Zároveň jsou využívány v maximální míře existující popisy a dokumentace i vazby na centrální zdroje informací (např. RPP, RAZR atp.). Dokumentace je aktualizována průběžně podle požadavků nové legislativy.

15. Zavést dlouhodobou správu služeb

Je v realizaci Katalog služeb externím subjektům, který má za cíl propojit služby, agendy a aplikace, aby mohl sloužit jako podklad pro strategické řízení ICT.

16. Digitalizovat služby města

Návrh řešení nasazení vybraných služeb byl zpracován do zadávací dokumentace VZ pro vytvoření mobilní aplikace.

Pro webový portál služeb byla vybrána agenda poplatků za psa v působnosti 29 MČ. Pilotní ověření vybrané služby proběhne v rámci implementace webového portálu.

Probíhá implementace webového portálu s moderními technologickými a bezpečnostními standardy. Předpokládaná publikace veřejnosti v 2.Q 2026.

17. Vytvořit moderní, společné, bezpečné a efektivní ICT města

Podniková architektura (Enterprise Architecture) je vytvářena podle metodiky TOGAF a je základním informačním zdrojem jak pro popisy ICT komponent, tak i pro celkový obraz ICT prostředí včetně vazeb a je průběžně rozvíjena. Vzhledem k požadavkům legislativy a projektům jako je katalog služeb, je rozvíjen popis v oblasti business vrstvy ve vazbě na agendy, vykonávané úřadem.

Technický soulad aktiv je v tuto chvíli ověřován pomocí mapování bezpečnostní architektury, existujících propojení mezi jednotlivými AIS/ISVS a bezpečnostními opatřeními a dalšími nástroji, které slouží k evidenci a dokumentaci stavu bezpečnosti provozovaných systémů.

V současné době je aktualizována bezpečnostní dokumentace v rozsahu SŘBI města. Současně je aktualizován minimální bezpečnostní standard ÚMČ tak, aby veškerá dokumentace vyhovovala požadavkům NZoKB a jeho prováděcím předpisům.

18. Centrálně řídit ICT města

Řídící orgán ICT pro řízení ICT SMB standardně posuzuje projektové záměry v perimetru SMB.

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

19. Dosahovat soulad s digitální legislativou (compliance)

V roce 2024 proběhlo šetření týkající se připravenosti na soulad s tehdejším návrhem nové legislativy. Výstupem šetření bylo patnáct doporučení, které se týkaly jednotlivých oblastí podle návrhu legislativy. Výstupy šetření byly předloženy RMB včetně plánu nápravných opatření, v tuto chvíli zbývají k dořešení 2 a předpoklad splnění je v Q2 2026. Některá řešení spočívala v pořízení vybraných technologií a zajištění procesních postupů k nim, například v nasazení systému správy zranitelností nebo systému visibility strategických služeb. Tyto systémy již běží a nastavují se do plného fungování. Další části souladu, související s organizačními nastaveními, jsou v přípravě a budou nastaveny v souladu s akčním plánem do 9. 2. 2027, kdy uplyne přesně rok od určení města do nižšího režimu v regulované službě Výkon svěřených pravomocí.

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)
4,2	Oblast informační bezpečnosti je řízena koordinátorem kybernetické bezpečnosti SMB.
4,1	Jistota prostředků na kalendářní rok v rámci schváleného rozpočtu.
4,1	Kvalifikovaní správci aplikací a ICT infrastruktury v oblasti, kterou mají ve své pracovní náplni.
4,1	Projektová kancelář OMI řídí IT projektové portfolio MMB, včetně projektů kybernetické bezpečnosti (KB).
3,9	Existence webové platformy města Brna.
3,9	Vznikl řídící orgán ICT ke koordinaci ICT v rámci perimetru SMB (MMB, městské části, městské firmy a příspěvkové organizace města).
3,8	Zvyšující se bezpečnostní povědomí mezi pracovníky OMI a rovněž pracovníky MMB.
3,7	Dosažené zkušenosti s implementací informačních systémů.
3,6	Vysoká znalost technologických trendů a jejich zavádění.
3,1	Vznikla pracovní skupina pro využití AI v rámci MMB.

	Opportunities (vnější příležitosti)
4,2	Dlouhodobá partnerská spolupráce s NÚKIB, DIA a MV ČR.
4,1	Využití AI pro chod úřadu i komunikaci s občany.
4,1	Využití analýzy procesů z ORGO.
3,8	Aktivovat systém hodnocení dodavatelů.
3,7	Využití potenciálu odborníků v rámci města ve formě poradenského orgánu.
3,7	Maximalizovat využití čerpání prostředků z fondů EU.
3,0	Zapojení vysokých škol do rozvoje informatiky města Brna včetně aktivní spolupráce města při výuce studentů.
2,9	V Brně na trhu práce existují vzdělaní a kompetentní pracovníci v oblasti ICT.

	Weaknesses (vnitřní slabé stránky)
4,3	Nedostatek vnitřních odborných kapacit vzhledem k rostoucímu významu a rozvoji informatiky vede ke zvýšenému nákupu externích služeb.
4,1	Ne všichni klíčoví uživatelé (garanti) mají dostatečné znalosti, aby definovali požadavky na informatiku

	(formulace toho, co chtějí). OMI nemůže suplovat metodické role uživatelů.
3,9	Odměňovací systém neumožňuje získávat nové a udržet stávající pracovníky IT.
3,8	Technologické roztříštění webových stránek města.
3,6	Neochota úředníků k využití ICT potenciálu a změn.
3,6	Nedostatečné personální zajištění obsahu a obsluhy webové platformy.
3,4	Klíčové uživatele je obtížné motivovat pro spolupráci v projektových týmech týkajících se informatiky z důvodu střetu liniových a projektových struktur.
3,0	Nedostatečné povědomí klíčových uživatelů o plánovaní kapacit zdrojů OMI na pokrytí požadavků.
	Threats (vnější hrozby)
4,3	Masivní vývoj kybernetických útoků a jejich forem.
4,3	Se změnou politické reprezentace může dojít k zásadním změnám ve směrování a financování ICT.
4,2	Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.
4,1	Nárůst požadavků na dokumentaci v ICT dnes zejména v oblasti informační a kybernetické bezpečnosti.
4,0	Rozšiřování projektů v ICT mimo gesci OMI.
4,0	Masivní nárůst legislativních požadavků a jejich dopady v oblasti ICT a kybernetické bezpečnosti.
3,9	Dlouhá doba od vytvoření záměru do jeho realizace způsobená interními předpisy nebo platnou legislativou.
3,9	Absence aktuálního procesního modelu činností při zpracování agend neumožňující orchestraci při řízení ICT a při řízení kybernetické bezpečnosti (včetně rozvoje).
3,6	Obtížné vysvětlení a porozumění komplexní problematice řešené v IT neodborníkům na IT napříč SMB (MMB + MČ) včetně politického vedení.
3,6	Přeceňování a nedostatek schopností správně používat umělou inteligenci (fabulace a halucinace).
3,5	Ze zadávacích řízení podle ZZVZ mohou vzejít neadekvátní dodavatelé nebo mohou zadávací řízení trvat nepredikovatelnou dobu.
3,4	Vzrůstající komplexita a regulace požadovaných technických opatření v ICT.
3,4	Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT.
3,3	Přidělení finančních prostředků z rozpočtu je vždy jen na rok (rozpočtování je jen roční), v IT není zavedeno víceleté financování.
3,1	Hrozby spojené s užíváním zařízení umístěných mimo perimetr.
2,9	Narůstající význam regulace v oblasti AI (umělé inteligence).
2,4	Narůstající význam IoT a Scada prvků zvyšující míru rizik v rámci SMB.
2,4	Zneužití práva na informace (zákon 106/1999 Sb.) ke zjišťování neveřejných informací.
2,3	Uživatelé pracující vzdáleně (mimo kancelář) se obracejí s lokálními ICT problémy na servisní podporu OMI mimo jeho gesci.

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)
4,4	Kvalitní komunikační infrastruktura připojení ÚMČ.
4,4	Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ).
4,4	Architektura pro integrace aplikací - integrační platforma (s využitím principů ESB a ETL).
4,3	Jsou k dispozici opakovatelně použitelné architektonické stavební bloky pro využití aplikacemi SMB (např. NIA Proxy, ISZR Proxy).
4,2	Je zřízena samostatná role bezpečnostního architekta a solution architekta. Bezpečnostní architektura je

	provázána na EA MMB.
4,1	Validní informace o EA MMB jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.
4,1	Efektivní licencování pro základní části městského AIS a office SW.
4,0	Rada města Brna vydala minimální standard kybernetické bezpečnosti pro MČ, jehož dodržování je závazné.
3,7	Rozšíření služeb provozovaných z městského cloudu pro všechny městské subjekty SMB.
3,7	V rámci SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) se zajištěnou ochranou proti jejich ztrátě.
3,6	Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy.
3,6	Kvalitní prostory a technologické zázemí pro umístění uzlových ICT prvků (datové centrum).
	Opportunities (vnější příležitosti)
4,9	On-line řešení a služby jsou koncepčně pojaty jako jeden celek (mobilní aplikace, portál brňáka, webová platforma).
4,5	Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.
4,4	Využití shodných datových zdrojů pro různé aplikace města.
4,4	Nasazení systému pro sledování visibility strategických služeb poskytovaných SMB.
4,4	Vydání IT směrnic závazných pro SMB.
4,4	Vytvoření a správa katalogu služeb ICT SMB.
4,1	Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu.
4,0	Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy).
3,9	Popsání definice vazeb mezi projekty a sesouladění postupů – road-mapa na období několika let s pravidelnou aktualizací.
3,9	Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).
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	Metodická pomoc kompetenčního centra uživatelům z ÚMČ a organizací města.
3,6	Vytvoření jednotné platformy pro využívání AI MMB a MČ.
3,6	Propojení konfiguračních databází udržovaných MMB a samostatně dodavateli/správci částí infrastruktury.
3,4	Vytvoření prioritizace cca 350 aplikací a odstupňovaný přístup k nim podle jejich priorit.
3,4	Vytvoření centrálního přístupového bodu pro řízený přístup uživatelů do IS města a k aplikacím z různých platforem.
3,2	Je k dispozici prostředí (framework) pro tvorbu jednoduché podpory procesů a workflow v nich (MOSS - MS Office SharePoint Services) s komunitou uživatelů.
3,1	Využití externích kapacit výzkumu a vývoje pro oponenturu rozvojových koncepčních plánů a projektů (CERIT, NUKIB, Útvar hlavního architekta eGov, DIA ...).
2,9	Zvyšující se zájem stakeholderů o přístup k informacím z EA modelu.
2,9	Využití Národního architektonického plánu s návrhovými vzory vybraných oblastí.
2,9	Vytvořit prostředí pro drobné aplikace odborných útvarů SMB.
	Weaknesses (vnitřní slabé stránky)
4,5	Chybí vazba na business vrstvu zpracovávanou ORGO v BPMN diagramech.
4,4	Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti.
4,4	Řada aplikací nemá dokumentaci.

4,1	Neexistuje provozní konfigurační management na datové a aplikační vrstvě.
3,9	Nedostatečná aplikace principů procesního řízení.
3,9	Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).
3,9	IDM nemá zadefinované role z business vrstvy (není propojení až do procesní business vrstvy a její rozpracování na role).
3,7	Používání legacy aplikací neintegrovatelných či vyžadujících výjimky z koncepce pro integraci systémů.
3,6	Model EA zahrnuje jen MMB a absentují organizace SMB.
3,6	Ne všechna data jsou ukládána do datových úložišť ve strukturované podobě, která umožní řízení přístupu dle oprávnění.
3,5	Není využívána geograficky oddělená záložní infrastruktura (nejsou přestěhovány do záložního centra servery clusterů).
3,4	Platformová technologická roztříštěnost (např. různé db stroje).
3,3	Závislost rozvoje ICT architektury na přidělených prostředcích (rozpočtu).
3,2	Městské firmy si spravují vlastní podružná menší datová centra i aplikace bez vazby na EA.
3,1	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).
3,0	Plánování a využití kapacit všech zdrojů v souladu s požadavky vykonávaných procesů.
	Threats (vnější hrozby)
4,1	Legislativní změny vyžadující podrobnější popis systémů (procesy, architektura, bezpečnost, ...).
4,0	Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.
3,9	Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24.
3,8	Odpovědnost za agendy svěřené městským společnostem (výkon svěřených pravomocí), které je mohou dále outsourcovat svým dodavatelům, bez reálné možnosti jejich kontroly.
3,8	Nedostatečná pozornost ze strany tvůrců prvků celostátního eGovernment, věnovaná specifickým potřebám statutárních měst.
3,6	Neexistence plánu a pevných milníků pro nasazení nových centrálních IS s dopadem na činnosti OVM, což znamená negativní dopady na plánování zdrojů OVM, zejména při našem rozsahu správního obvodu (např. aplikace CRR, CRV, digitalizace dokumentů pro centrální agendy, rušení místní příslušnosti ...).
3,6	Licenční a technologická závislost na dodavateli (vendor lock-in).
3,3	Konfliktní požadavky změn legislativy s dopadem do informačních systémů.
3,2	Vynucená koordinace s podřízenými organizacemi z hlediska regulovaných služeb poskytovaných ve sdílené infrastruktuře ve formě podpůrných aktiv.
3,1	EA model obsahuje koncentrované informace a při neoprávněném přístupu k nim jde o bezpečnostní riziko.
3,0	Organizační změny posilující přístup k aplikacím z vnějšího prostředí vyvolají problémy s licencemi a technologiemi.
2,8	Nedostatečnost kapacity komunikační infrastruktury pro nové služby nabízené z internetu (např. video streaming, práce s 3D modely).

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)
4,6	Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.
4,5	Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb.
4,4	Člen RMB pro oblast informatiky.

4,2	Poskytování vybraných veřejných služeb přes internet.
4,2	Sjednocené a vybudované prostředí pro výkon veřejné správy.
4,0	Digitalizace vnitřních procesů řízení města (eMMB).
4,0	Dlouhodobé strategické řízení informatiky.
3,9	Koordinace ICT projektů městských subjektů (Řídící orgán ICT).
3,9	Geografický informační systém přístupný pro občany, organizace, úřady SMB.
3,9	SMB má statut a může v rámci něj prosadit cíle v IT jak na MMB, tak i na ÚMČ (čl. 39 a 40).
3,7	Vysoká úroveň řízení kybernetické bezpečnosti.
3,7	Spolupráce se státní správou v oblasti kybernetické bezpečnosti.
3,3	Jsou vytvořeny specializované subjekty města k poskytování specifických ICT služeb (TSB, BKOM, DPMB, ...).
3,2	Poskytování služeb založených společností a zřízených organizací městem přes internet.
3,2	Řízené zpřístupňování dat interním i externím uživatelům.

Opportunities (vnější příležitosti)

4,4	Sjednocení komunikace nabízených služeb SMB občanům přes centrální aplikaci.
4,2	Naplnění webové platformy města.
4,0	Aplikace nového Zákona o kybernetické bezpečnosti s dopadem nejen na bezpečnost (systematizace, procesy, ...).
3,7	Využití potenciálu umělé inteligence pro zefektivnění interních i externích procesů.
3,7	Využití možností spolufinancování nových služeb z externích zdrojů.
3,6	Definice zákazníka ICT služeb a jeho potřeb.
3,4	Zapojení Odboru strategického rozvoje a spolupráce do tvorby strategických vizí pro ICT.
3,4	Spolupráce s jinými městy v ČR a EU.
2,9	Využívání standardizovaných IT produktů poskytovaných na celostátní úrovni.
2,8	Využití aktivit v rámci externích subjektů ke standardizaci požadavků na výstupy z IS OVM.
2,7	Zintenzivnění spolupráce se středními a vysokými školami (využití jejich potenciálu).

Weaknesses (vnitřní slabé stránky)

4,5	Existuje prostor pro realizaci ICT projektů bez projednání s OMI.
4,4	Nedostatečná komunikace v rámci SMB, městských společností a organizací.
4,2	Dlouhá doba od převedení vize do projektů.
4,1	Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu.
3,9	Nízká míra využití potenciálu zavedených technologií.
3,9	Pro občana nejsou v dostatečné míře přístupné všechny agendy přes internet. Portál občana (prezentační portál) umožňující sledování procesu není dokončen.
3,4	Nízké povědomí o důležitosti výdajů do IT.
3,4	Neexistence ICT technologického standardu města.
3,3	Není definován katalog elektronicky poskytovaných služeb SMB.
3,3	Nedostatečné zapojení Odboru strategického rozvoje a spolupráce do tvorby strategických vizí pro ICT.
3,3	Nemožnost řešit projekty/úkoly v informatice v době, kdy vznikají (legislativní a procesní omezení).
2,1	Omezený přístup k demografickým údajům na MČ.

Threats (vnější hrozby)

4,6	Kybernetické hrozby a hrozby prostředí ohrožující fungování ICT.
4,2	Nárůst požadavků na informatiku při zachování stávajícího objemu finančních a lidských zdrojů.
4,1	Obtížná koordinace specializovaných subjektů města k poskytování specifických ICT služeb (TSB, BKOM, DPMB, Veletrhy Brno, ...).

3,9	Daná lhůta na implementaci všech opatření vyplývajících ze Zákona o kybernetické bezpečnosti.
3,9	Vzrůstající nároky na dostupnost a důvěrnost poskytovaných služeb.
3,9	Vznikají požadavky na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.
3,8	Neochota ke změnám u vnitřních uživatelů ICT na MMB i ÚMČ.
3,7	Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.
3,4	Obtížnost standardizace při potřebě specifických ICT řešení na ÚMČ.
3,4	Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.
3,2	Zapojení AI do přípravy útoků na ICT prostředí (např. sběr dat z registru smluv).

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)
4,3	Neomezenost počtu interních uživatelů v klíčových aplikacích z pohledu přístupu na informační systémy.
4,2	Město poskytuje digitální služby pro komunikaci s občany.
3,8	Zavedený systém visibility kritických služeb (zvýšení dostupnosti služeb).
3,8	Průběžná obnova techniky (koncových zařízení).
3,4	Zavedená podpora uživatelů SMB pomocí service-desku.
3,4	Pravidelná školení na způsob práce s aplikacemi.
3,3	Pokročilá aplikační podpora uživatelů (interních i externích).
3,2	Technologické umožnění práce na dálku.
3,2	Dostupnost aktualizovaných manuálů na intranetu.
3,1	Poskytnutí prostředků uživatelům pro přístup k informacím i z domova.
3,0	Poskytnutí dočasného přístupu k wi-fi návštěvníkům MMB a trvalého připojení zaměstnancům MMB.

	Opportunities (vnější příležitosti)
4,6	Vytvoření a rozvoj komunikačních aplikací pro občana - portál občana Brna, mobilní aplikace, Brno ID, ...
4,3	Zlepšení bezpečnostního povědomí uživatelů.
3,7	Podpora uživatelů prostřednictvím nástrojů AI.
3,6	Využití drobných specializovaných aplikací používaných v jiných městech.
3,4	Zavést hodnocení kvality vyřešení požadavků zadaných v service-desku uživatelem.
2,8	Pokrytí wi-fi připojení do všech prostorů (dnes ve vybraných prostorách - kanceláře vedoucích a zasedací místnosti).
2,4	Využití možností prvků "mikro ICT" (princip Internetu věcí) a spolupráce s mobilním HW pro zpřístupnění služeb ICT občanům.

	Weaknesses (vnitřní slabé stránky)
4,4	Uživatelé nejsou dostatečně seznámeni s riziky používání nových (mobilních) zařízení.
4,2	Neznalost uživatele, jak požádat a specifikovat novou funkcionalitu.
4,1	Uživatelé nemají povědomí o reálných možnostech řešení jejich požadavků (času, schopnosti řešit požadavek, finanční náročnosti). Nedostatečně objektivní požadavky uživatelů.
4,0	Roztříštěná komunikace města Brna s občany z hlediska informačních systémů.
3,9	Klíčoví uživatelé z jednotlivých odborů MMB nemají uvolněnou kapacitu na poskytování součinnosti v IT při řešení požadavků týkajících se jejich odborné problematiky.
3,9	Bezpečnostní povědomí uživatelů je nedostatečné pro kybernetické útoky.

3,5	Dosud nezavedená elektronická podpora některých vnitřních schvalovacích procesů úřadu.
3,4	Nedůvěra uživatelů k používání service-desku.
3,1	Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.
3,1	Uživatelé s přístupem k elektronickým materiálům vyžadují rovněž jejich tištěnou podobu, která pro jejich činnost není nutná.
3,0	Nejednotný přístup uživatelů k realizaci svých požadavků (formulace, spolupráce na řešení).
2,1	Snížená uživatelská podpora v období mimo pracovní dobu.

	Threats (vnější hrozby)
4,6	Výpadek metropolitní sítě a internetu (včetně KIVS) znamená nefunkčnost významných agend SMB.
4,6	Napadení výpočetní techniky uživatele s omezením dostupnosti dat na ní uložených (např. ransomware).
4,4	Závislost na správném fungování centrálních aplikací při poskytování služeb.
4,2	Důvěra v možnosti umělé inteligence bez posouzení správnosti výsledků.
3,9	Přílišná důvěřivost uživatelů k neznámým zdrojům (připojování se k neznámým WiFi).
3,0	Vzrůstající komplexita a závislost na digitálně poskytovaných službách.
2,9	Mylný pohled na možnosti úřadu při řešení "životních situací" bez vnímání omezení (legislativa, zdroje..).
2,9	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)	
4,6	Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.	Přínosy
4,5	Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb.	Přínosy
4,4	Kvalitní komunikační infrastruktura připojení ÚMČ.	Architektura
4,4	Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ).	Architektura
4,4	Architektura pro integrace aplikací - integrační platforma (s využitím principů ESB a ETL).	Architektura
4,4	Člen RMB pro oblast informatiky.	Přínosy
4,3	Jsou k dispozici opakovatelně použitelné architektonické stavební bloky pro využití aplikacemi SMB (např. NIA Proxy, ISZR Proxy).	Architektura
4,3	Neomezenost počtu interních uživatelů v klíčových aplikacích z pohledu přístupu na informační systémy.	Uživatelé
4,2	Město poskytuje digitální služby pro komunikaci s občany.	Uživatelé
4,2	Poskytování vybraných veřejných služeb přes internet.	Přínosy
4,2	Sjednocené a vybudované prostředí pro výkon veřejné správy.	Přínosy
4,2	Je zřízena samostatná role bezpečnostního architekta a solution architekta. Bezpečnostní architektura je provázána na EA MMB.	Architektura
4,2	Oblast informační bezpečnosti je řízena koordinátorem kybernetické bezpečnosti SMB.	Organizace
4,1	Validní informace o EA MMB jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.	Architektura
4,1	Jistota prostředků na kalendářní rok v rámci schváleného rozpočtu.	Organizace
4,1	Kvalifikovaní správci aplikací a ICT infrastruktury v oblasti, kterou mají ve své pracovní náplni.	Organizace
4,1	Efektivní licencování pro základní části městského AIS a office SW.	Architektura
4,1	Projektová kancelář OMI řídí IT projektové portfolio MMB, včetně projektů kybernetické bezpečnosti (KB).	Organizace

4,0	Digitalizace vnitřních procesů řízení města (eMMB).	Přínosy
4,0	Dlouhodobé strategické řízení informatiky.	Přínosy
4,0	Rada města Brna vydala minimální standard kybernetické bezpečnosti pro MČ, jehož dodržování je závazné.	Architektura
3,9	Koordinace ICT projektů městských subjektů (Řídící orgán ICT).	Přínosy
3,9	Existence webové platformy města Brna.	Organizace
3,9	Geografický informační systém přístupný pro občany, organizace, úřady SMB.	Přínosy
3,9	SMB má statut a může v rámci něj prosadit cíle v IT jak na MMB, tak i na ÚMČ (čl. 39 a 40).	Přínosy
3,9	Vznikl řídící orgán ICT ke koordinaci ICT v rámci perimetru SMB (MMB, městské části, městské firmy a příspěvkové organizace města).	Organizace
3,8	Zavedený systém visibility kritických služeb (zvýšení dostupnosti služeb).	Uživatelé
3,8	Průběžná obnova techniky (koncových zařízení).	Uživatelé
3,8	Zvyšující se bezpečnostní povědomí mezi pracovníky OMI a rovněž pracovníky MMB.	Organizace
3,7	Vysoká úroveň řízení kybernetické bezpečnosti.	Přínosy
3,7	Rozšíření služeb provozovaných z městského cloudu pro všechny městské subjekty SMB.	Architektura
3,7	Dosažené zkušenosti s implementací informačních systémů.	Organizace
3,7	Spolupráce se státní správou v oblasti kybernetické bezpečnosti.	Přínosy
3,7	V rámci SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) se zajištěnou ochranou proti jejich ztrátě.	Architektura
3,6	Vysoká znalost technologických trendů a jejich zavádění.	Organizace
3,6	Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy.	Architektura
3,6	Kvalitní prostory a technologické zázemí pro umístění uzlových ICT prvků (datové centrum).	Architektura
3,4	Zavedená podpora uživatelů SMB pomocí service-desku.	Uživatelé
3,4	Pravidelná školení na způsob práce s aplikacemi.	Uživatelé
3,3	Jsou vytvořeny specializované subjekty města k poskytování specifických ICT služeb (TSB, BKOM, DPMB, ...).	Přínosy
3,3	Pokročilá aplikační podpora uživatelů (interních i externích).	Uživatelé
3,2	Technologické umožnění práce na dálku.	Uživatelé
3,2	Dostupnost aktualizovaných manuálů na intranetu.	Uživatelé
3,2	Poskytování služeb založených společností a zřízených organizací městem přes internet.	Přínosy
3,2	Řízené zpřístupňování dat interním i externím uživatelům.	Přínosy
3,1	Vznikla pracovní skupina pro využití AI v rámci MMB.	Organizace
3,1	Poskytnutí prostředků uživatelům pro přístup k informacím i z domova.	Uživatelé
3,0	Poskytnutí dočasného přístupu k wi-fi návštěvníkům MMB a trvalého připojení zaměstnancům MMB.	Uživatelé

Opportunities (vnější příležitosti)

4,9	On-line řešení a služby jsou koncepčně pojaty jako jeden celek (mobilní aplikace, portál brňáka, webová platforma).	Architektura
4,6	Vytvoření a rozvoj komunikačních aplikací pro občana - portál občana Brna, mobilní aplikace, Brno ID, ...	Uživatelé
4,5	Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.	Architektura
4,4	Sjednocení komunikace nabízených služeb SMB občanům přes centrální aplikaci.	Přínosy
4,4	Využití shodných datových zdrojů pro různé aplikace města.	Architektura
4,4	Nasazení systému pro sledování visibility strategických služeb poskytovaných SMB.	Architektura

4,4	Vydání IT směrnic závazných pro SMB.	Architektura
4,4	Vytvoření a správa katalogu služeb ICT SMB.	Architektura
4,3	Zlepšení bezpečnostního povědomí uživatelů.	Uživatelé
4,2	Naplnění webové platformy města.	Přínosy
4,2	Dlouhodobá partnerská spolupráce s NÚKIB, DIA a MV ČR.	Organizace
4,1	Využití AI pro chod úřadu i komunikaci s občany.	Organizace
4,1	Využití analýzy procesů z ORGO.	Organizace
4,1	Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu.	Architektura
4,0	Aplikace nového Zákona o kybernetické bezpečnosti s dopadem nejen na bezpečnost (systematizace, procesy, ...).	Přínosy
4,0	Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy).	Architektura
3,9	Popsání definice vazeb mezi projekty a sesouladění postupů – road-mapa na období několika let s pravidelnou aktualizací.	Architektura
3,9	Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).	Architektura
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	Aktivovat systém hodnocení dodavatelů.	Organizace
3,7	Podpora uživatelů prostřednictvím nástrojů AI.	Uživatelé
3,7	Metodická pomoc kompetenčního centra uživatelům z ÚMČ a organizací města.	Architektura
3,7	Využití potenciálu umělé inteligence pro zefektivnění interních i externích procesů.	Přínosy
3,7	Využití možností spolufinancování nových služeb z externích zdrojů.	Přínosy
3,7	Využití potenciálu odborníků v rámci města ve formě poradenského orgánu.	Organizace
3,7	Maximalizovat využití čerpání prostředků z fondů EU.	Organizace
3,6	Využití drobných specializovaných aplikací používaných v jiných městech.	Uživatelé
3,6	Vytvoření jednotné platformy pro využívání AI MMB a MČ.	Architektura
3,6	Propojení konfiguračních databází udržovaných MMB a samostatně dodavateli/správci částí infrastruktury.	Architektura
3,6	Definice zákazníka ICT služeb a jeho potřeb.	Přínosy
3,4	Zapojení Odboru strategického rozvoje a spolupráce do tvorby strategických vizí pro ICT.	Přínosy
3,4	Vytvoření prioritizace cca 350 aplikací a odstupňovaný přístup k nim podle jejich priorit.	Architektura
3,4	Vytvoření centrálního přístupového bodu pro řízený přístup uživatelů do IS města a k aplikacím z různých platforem.	Architektura
3,4	Spolupráce s jinými městy v ČR a EU.	Přínosy
3,4	Zavést hodnocení kvality vyřešení požadavků zadaných v service-desku uživatelem.	Uživatelé
3,2	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 externích kapacit výzkumu a vývoje pro oponenturu rozvojových koncepčních plánů a projektů (CERIT, NUKIB, Útvar hlavního architekta eGov, DIA ...).	Architektura
3,0	Zapojení vysokých škol do rozvoje informatiky města Brna včetně aktivní spolupráce města při výuce studentů.	Organizace
2,9	Zvyšující se zájem stakeholderů o přístup k informacím z EA modelu.	Architektura
2,9	Využívání standardizovaných IT produktů poskytovaných na celostátní úrovni.	Přínosy

2,9	Využití Národního architektonického plánu s návrhovými vzory vybraných oblastí.	Architektura
2,9	V Brně na trhu práce existují vzdělaní a kompetentní pracovníci v oblasti ICT.	Organizace
2,9	Vytvořit prostředí pro drobné aplikace odborných útvarů SMB.	Architektura
2,8	Využití aktivit v rámci externích subjektů ke standardizaci požadavků na výstupy z IS OVM.	Přínosy
2,8	Pokrytí wi-fi připojení do všech prostorů (dnes ve vybraných prostorách - kanceláře vedoucích a zasedací místnosti).	Uživatelé
2,7	Zintenzivnění spolupráce se středními a vysokými školami (využití jejich potenciálu).	Přínosy
2,4	Využití možností prvků "mikro ICT" (princip Internetu věcí) a spolupráce s mobilním HW pro zpřístupnění služeb ICT občanům.	Uživatelé

Weaknesses (vnitřní slabé stránky)

4,5	Chybí vazba na business vrstvu zpracovávanou ORGO v BPMN diagramech.	Architektura
4,5	Existuje prostor pro realizaci ICT projektů bez projednání s OMI.	Přínosy
4,4	Uživatelé nejsou dostatečně seznámeni s riziky používání nových (mobilních) zařízení.	Uživatelé
4,4	Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti.	Architektura
4,4	Nedostatečná komunikace v rámci SMB, městských společností a organizací.	Přínosy
4,4	Řada aplikací nemá dokumentaci.	Architektura
4,3	Nedostatek vnitřních odborných kapacit vzhledem k rostoucímu významu a rozvoji informatiky vede ke zvýšenému nákupu externích služeb.	Organizace
4,2	Neznalost uživatele, jak požádat a specifikovat novou funkcionalitu.	Uživatelé
4,2	Dlouhá doba od převedení vize do projektů.	Přínosy
4,1	Neexistuje provozní konfigurační management na datové a aplikační vrstvě.	Architektura
4,1	Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu.	Přínosy
4,1	Uživatelé nemají povědomí o reálných možnostech řešení jejich požadavků (času, schopnosti řešit požadavek, finanční náročnosti). Nedostatečně objektivní požadavky uživatelů.	Uživatelé
4,1	Ne všichni klíčoví uživatelé (garanti) mají dostatečné znalosti, aby definovali požadavky na informatiku (formulace toho, co chtějí). OMI nemůže suplovat metodické role uživatelů.	Organizace
4,0	Roztříštěná komunikace města Brna s občany z hlediska informačních systémů.	Uživatelé
3,9	Nedostatečná aplikace principů procesního řízení.	Architektura
3,9	Klíčoví uživatelé z jednotlivých odborů MMB nemají uvolněnou kapacitu na poskytování součinnosti v IT při řešení požadavků týkajících se jejich odborné problematiky.	Uživatelé
3,9	Odměňovací systém neumožňuje získávat nové a udržet stávající pracovníky IT.	Organizace
3,9	Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).	Architektura
3,9	IDM nemá zadefinované role z business vrstvy (není propojení až do procesní business vrstvy a její rozpracování na role).	Architektura
3,9	Nízká míra využití potenciálu zavedených technologií.	Přínosy
3,9	Pro občana nejsou v dostatečné míře přístupné všechny agendy přes internet. Portál občana (prezentační portál) umožňující sledování procesu není dokončen.	Přínosy
3,9	Bezpečnostní povědomí uživatelů je nedostatečné pro kybernetické útoky.	Uživatelé
3,8	Technologické roztříštění webových stránek města.	Organizace
3,7	Používání legacy aplikací neintegrovatelných či vyžadujících výjimky z koncepce pro integraci systémů.	Architektura
3,6	Model EA zahrnuje jen MMB a absentují organizace SMB.	Architektura
3,6	Ne všechna data jsou ukládána do datových úložišť ve strukturované podobě, která umožní řízení	Architektura

	přístupu dle oprávnění.	
3,6	Neochota úředníků k využití ICT potenciálu a změn.	Organizace
3,6	Nedostatečné personální zajištění obsahu a obsluhy webové platformy.	Organizace
3,5	Není využívána geograficky oddělená záložní infrastruktura (nejsou přestěhovány do záložního centra servery clusterů).	Architektura
3,5	Dosud nezavedená elektronická podpora některých vnitřních schvalovacích procesů úřadu.	Uživatelé
3,4	Klíčové uživatele je obtížné motivovat pro spolupráci v projektových týmech týkajících se informatiky z důvodu střetu liniových a projektových struktur.	Organizace
3,4	Platformová technologická roztříštěnost (např. různé db stroje).	Architektura
3,4	Nedůvěra uživatelů k používání service-desku.	Uživatelé
3,4	Nízké povědomí o důležitosti výdajů do IT.	Přínosy
3,4	Neexistence ICT technologického standardu města.	Přínosy
3,3	Není definován katalog elektronicky poskytovaných služeb SMB.	Přínosy
3,3	Nedostatečné zapojení Odboru strategického rozvoje a spolupráce do tvorby strategických vizí pro ICT.	Přínosy
3,3	Nemožnost řešit projekty/úkoly v informatice v době, kdy vznikají (legislativní a procesní omezení).	Přínosy
3,3	Závislost rozvoje ICT architektury na přidělených prostředcích (rozpočtu).	Architektura
3,2	Městské firmy si spravují vlastní podružná menší datová centra i aplikace bez vazby na EA.	Architektura
3,1	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
3,1	Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.	Uživatelé
3,1	Uživatelé s přístupem k elektronickým materiálům vyžadují rovněž jejich tištěnou podobu, která pro jejich činnost není nutná.	Uživatelé
3,0	Nedostatečné povědomí klíčových uživatelů o plánovaní kapacit zdrojů OMI na pokrytí požadavků.	Organizace
3,0	Plánování a využití kapacit všech zdrojů v souladu s požadavky vykonávaných procesů.	Architektura
3,0	Nejednotný přístup uživatelů k realizaci svých požadavků (formulace, spolupráce na řešení).	Uživatelé
2,1	Snížená uživatelská podpora v období mimo pracovní dobu.	Uživatelé
2,1	Omezený přístup k demografickým údajům na MČ.	Přínosy

Threats (vnější hrozby)

4,6	Výpadek metropolitní sítě a internetu (včetně KIVS) znamená nefunkčnost významných agend SMB.	Uživatelé
4,6	Napadení výpočetní techniky uživatele s omezením dostupnosti dat na ní uložených (např. ransomware).	Uživatelé
4,6	Kybernetické hrozby a hrozby prostředí ohrožující fungování ICT.	Přínosy
4,4	Závislost na správném fungování centrálních aplikací při poskytování služeb.	Uživatelé
4,3	Masivní vývoj kybernetických útoků a jejich forem.	Organizace
4,3	Se změnou politické reprezentace může dojít k zásadním změnám ve směrování a financování ICT.	Organizace
4,2	Nárůst požadavků na informatiku při zachování stávajícího objemu finančních a lidských zdrojů.	Přínosy
4,2	Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.	Organizace
4,2	Důvěra v možnosti umělé inteligence bez posouzení správnosti výsledků.	Uživatelé
4,1	Legislativní změny vyžadující podrobnější popis systémů (procesy, architektura, bezpečnost, ...).	Architektura
4,1	Nárůst požadavků na dokumentaci v ICT dnes zejména v oblasti informační a kybernetické bezpečnosti.	Organizace
4,1	Obtížná koordinace specializovaných subjektů města k poskytování specifických ICT služeb (TSB, BKOM, DPMB, Veletrhy Brno, ...).	Přínosy

4,0	Rozšiřování projektů v ICT mimo gesci OMI.	Organizace
4,0	Masivní nárůst legislativních požadavků a jejich dopady v oblasti ICT a kybernetické bezpečnosti.	Organizace
4,0	Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.	Architektura
3,9	Daná lhůta na implementaci všech opatření vyplývajících ze Zákona o kybernetické bezpečnosti.	Přínosy
3,9	Přílišná důvěřivost uživatelů k neznámým zdrojům (připojování se k neznámým WiFi).	Uživatelé
3,9	Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24.	Architektura
3,9	Vzrůstající nároky na dostupnost a důvěrnost poskytovaných služeb.	Přínosy
3,9	Vznikají požadavky na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.	Přínosy
3,9	Dlouhá doba od vytvoření záměru do jeho realizace způsobená interními předpisy nebo platnou legislativou.	Organizace
3,9	Absence aktuálního procesního modelu činností při zpracování agend neumožňující orchestraci při řízení ICT a při řízení kybernetické bezpečnosti (včetně rozvoje).	Organizace
3,8	Odpovědnost za agendy svěřené městským společnostem (výkon svěřených pravomocí), které je mohou dále outsourcovat svým dodavatelům, bez reálné možnosti jejich kontroly.	Architektura
3,8	Neochota ke změnám u vnitřních uživatelů ICT na MMB i ÚMČ.	Přínosy
3,8	Nedostatečná pozornost ze strany tvůrců prvků celostátního eGovernment, věnovaná specifickým potřebám statutárních měst.	Architektura
3,7	Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.	Přínosy
3,6	Obtížné vysvětlení a porozumění komplexní problematice řešené v IT neodborníkům na IT napříč SMB (MMB + MČ) včetně politického vedení.	Organizace
3,6	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
3,6	Licenční a technologická závislost na dodavateli (vendor lock-in).	Architektura
3,6	Přeceňování a nedostatek schopností správně používat umělou inteligenci (fabulace a halucinace).	Organizace
3,5	Ze zadávacích řízení podle ZZVZ mohou vzejít neadekvátní dodavatelé nebo mohou zadávací řízení trvat nepredikovatelnou dobu.	Organizace
3,4	Obtížnost standardizace při potřebě specifických ICT řešení na ÚMČ.	Přínosy
3,4	Vzrůstající komplexita a regulace požadovaných technických opatření v ICT.	Organizace
3,4	Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT.	Organizace
3,4	Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.	Přínosy
3,3	Konfliktní požadavky změn legislativy s dopadem do informačních systémů.	Architektura
3,3	Přidělení finančních prostředků z rozpočtu je vždy jen na rok (rozpočtování je jen roční), v IT není zavedeno víceleté financování.	Organizace
3,2	Zapojení AI do přípravy útoků na ICT prostředí (např. sběr dat z registru smluv).	Přínosy
3,2	Vynucená koordinace s podřízenými organizacemi z hlediska regulovaných služeb poskytovaných ve sdílené infrastruktuře ve formě podpůrných aktiv.	Architektura
3,1	Hrozby spojené s užíváním zařízení umístěných mimo perimetr.	Organizace
3,1	EA model obsahuje koncentrované informace a při neoprávněném přístupu k nim jde o bezpečnostní riziko.	Architektura
3,0	Vzrůstající komplexita a závislost na digitálně poskytovaných službách.	Uživatelé
3,0	Organizační změny posilující přístup k aplikacím z vnějšího prostředí vyvolají problémy s licencemi a technologiemi.	Architektura

2,9	Mylný pohled na možnosti úřadu při řešení "životních situací" bez vnímání omezení (legislativa, zdroje..).	Uživatelé
2,9	Narůstající význam regulace v oblasti AI (umělé inteligence).	Organizace
2,9	Legislativní omezení ICT služeb pro externí subjekty (občan, právnické osoby ..).	Uživatelé
2,8	Nedostatečnost kapacity komunikační infrastruktury pro nové služby nabízené z internetu (např. video streaming, práce s 3D modely).	Architektura
2,4	Narůstající význam IoT a Scada prvků zvyšující míru rizik v rámci SMB.	Organizace
2,4	Zneužití práva na informace (zákon 106/1999 Sb.) ke zjišťování neveřejných informací.	Organizace
2,3	Uživatelé pracující vzdáleně (mimo kancelář) se obracejí s lokálními ICT problémy na servisní podporu OMI mimo jeho gesci.	Organizace

2.3. Variantní strategické možnosti vycházející z analýzy kvadrantů SWOT

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

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

[SO1] Využití vnitřní silné stránky

Architektura pro integrace aplikací - integrační platforma (s využitím principů ESB a ETL).
Jsou k dispozici opakovatelně použitelné architektonické stavební bloky pro využití aplikacemi SMB (např. NIA Proxy, ISZR Proxy).
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.
Validní informace o EA MMB jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.
Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.

k vnější příležitosti

On-line řešení a služby jsou koncepčně pojaty jako jeden celek (mobilní aplikace, portál brňáka, webová platforma).

[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.

[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).

[SO4] Využití vnitřní silné stránky

Člen RMB pro oblast informatiky.

Dlouhodobé strategické řízení informatiky.

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

Město poskytuje digitální služby pro komunikaci s občany.

Poskytování vybraných veřejných služeb přes internet.

Sjednocené a vybudované prostředí pro výkon veřejné správy.

k vnější příležitosti

Vytvoření a rozvoj komunikačních aplikací pro občana - portál občana Brna, mobilní aplikace, Brno ID, ...

[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 webové platformy města.

[SO7] Využití vnitřní silné stránky

Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.

k vnější příležitosti

Využití shodných datových zdrojů pro různé aplikace města.

[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

Oblast informační bezpečnosti je řízena koordinátorem kybernetické bezpečnosti SMB.

Je zřízena samostatná role bezpečnostního architekta a solution architekta. Bezpečnostní architektura je provázána na EA MMB.

k vnější příležitosti

Zlepšení bezpečnostního povědomí uživatelů.

Aplikace nového Zákona o kybernetické bezpečnosti s dopadem nejen na bezpečnost (systematizace, procesy, ...).

[SO10] Využití vnitřní silné stránky

Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ).

Validní informace o EA MMB jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.

k vnější příležitosti

Využití AI pro chod úřadu i komunikaci s občany.

Podpora uživatelů prostřednictvím nástrojů AI.

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.

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

Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb.

Kvalitní komunikační infrastruktura připojení ÚMČ.

k zamezení vnější hrozby

Výpadek metropolitní sítě a internetu (včetně KIVS) 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

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

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

Vznikla pracovní skupina pro využití AI v rámci MMB.

k zamezení vnější hrozby

Důvěra v možnosti umělé inteligence bez posouzení správnosti výsledků.

[ST7] Využití vnitřní silné stránky

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.

[ST8] Využití vnitřní silné stránky

Člen RMB pro oblast informatiky.

Projektová kancelář OMI řídí IT projekt

ové portfolio MMB, včetně projektů kybernetické bezpečnosti (KB).

k zamezení vnější hrozby

Nárůst požadavků na informatiku při zachování stávajícího objemu finančních a lidských zdrojů.

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.

[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

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.

[ST12] Využití vnitřní silné stránky

Člen RMB pro oblast informatiky.

Dlouhodobé strategické řízení informatiky.

k zamezení vnější hrozby

Se změnou politické reprezentace může dojít k zásadním změnám ve směrování a financování ICT.

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).

[WO2] Překonání vnitřní slabosti

Uživatelé nejsou dostatečně seznámeni s riziky používání nových (mobilních) zařízení.

využitím vnější příležitosti

Zlepšení bezpečnostního povědomí uživatelů.

[WO3] Překonání vnitřní slabosti

Pro občana nejsou v dostatečné míře přístupné všechny agendy přes internet. Portál občana (prezentační portál) umožňující sledování procesu není dokončen.

využitím vnější příležitosti

Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).

On-line řešení a služby jsou koncepčně pojaty jako jeden celek (mobilní aplikace, portál brňáka, webová platforma).Vytvoření a rozvoj komunikačních aplikací pro občana - portál občana Brna, mobilní aplikace, Brno ID, ...

[WO4] Překonání vnitřní slabosti

Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).

využitím vnější příležitosti

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

Chybí vazba na business vrstvu zpracovávanou ORGO v BPMN diagramech.

využitím vnější příležitosti

Využití potenciálu umělé inteligence pro zefektivnění interních i externích procesů.

[WO7] Překonání vnitřní slabosti

Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).

využitím vnější příležitosti

Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu.

Využití možností spolufinancování nových služeb z externích zdrojů.

[WO8] 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).

[WO9] 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.

[WO10] Překonání vnitřní slabosti

Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti.

využitím vnější příležitosti

Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.

Aplikace nového Zákona o kybernetické bezpečnosti s dopadem nejen na bezpečnost (systematizace, procesy, ...).

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

[WT1] Preventivní obrana proti skloubení vnitřní slabosti

Neexistuje provozní konfigurační management na datové a aplikační vrstvě.

Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti.

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 bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti.

s vnější hrozbou

Kybernetické hrozby a hrozby prostředí ohrožující fungování ICT.

Masivní vývoj kybernetických útoků a jejich forem.

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

[WT3] Preventivní obrana proti skloubení vnitřní slabosti

Odměňovací 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.

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.

[WT5] Preventivní obrana proti skloubení vnitřní slabosti

Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).

s vnější hrozbou

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.

s vnější hrozbou

Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24.

[WT8] Preventivní obrana proti skloubení vnitřní slabosti

Uživatelé nemají povědomí o reálných možnostech řešení jejich požadavků (času, schopnosti řešit požadavek, finanční náročnosti). Nedostatečně objektivní požadavky uživatelů.

s vnější hrozbou

Důvěra v možnosti umělé inteligence bez posouzení správnosti výsledků.

2.4. Strategické záměry vycházející z variantních strategických možností

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

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

	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
4,71	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. 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. Rada města Brna vydala minimální standard kybernetické bezpečnosti pro MČ, jehož dodržování je závazné.	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. Napadení výpočetní techniky uživatele s omezením dostupnosti dat na ní uložených (např. ransomware).	Aplikace nového Zákona o kybernetické bezpečnosti s dopadem nejen na bezpečnost (systematizace, procesy, ...). Chránit bezpečnost dat bez ohledu na jejich uložení. Vybudování systému visibility kritických služeb.

	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
4,67	S-O	Architektura pro integrace aplikací - integrační platforma (s využitím principů ESB a ETL). Jsou k dispozici opakovatelně použitelné architektonické stavební bloky pro využití aplikacemi SMB (např. NIA Proxy, ISZR Proxy). 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. Validní informace o EA MMB jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu. Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.	On-line řešení a služby jsou koncepčně pojaty jako jeden celek (mobilní aplikace, portál brňáka, webová platforma). Vytvoření a rozvoj komunikačních aplikací pro občana - portál občana Brna, mobilní aplikace, Brno ID, ...	Jednotná koncepce aplikací komunikujících s občany města.

	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
4,58	S-O	Validní informace o EA MMB jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu. 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.
	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
4,46	W-O	Pro občana nejsou v dostatečné míře přístupné všechny agendy přes internet. Portál občana (prezentační portál) umožňující sledování procesu není dokončen. Není definován katalog elektronicky poskytovaných služeb 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). Vytvoření a rozvoj komunikačních aplikací pro občana - portál občana Brna, mobilní aplikace, Brno ID, ...	Umožnit přístup občanům k agendám přes velkou městskou aplikaci (mobilní aplikace) a portál občana (web).
	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
4,42	W-T	Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti. Výpadek metropolitní sítě a internetu (včetně KIVS) znamená nefunkčnost významných agend SMB.	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.	Řídit bezpečnostní architekturu napříč SMB a dohlížet na implementaci bezpečnostních standardů v SMB podle nového ZKB (řídí kancelář kybernetické bezpečnosti). Zvýšit míru organizace informační bezpečnosti a schopnosti reakce a obnovy po útoku s ohledem na požadavky vyplývající z business continuity.
	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
4,17	W-O	Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti. Výpadek metropolitní sítě a internetu (včetně KIVS) znamená nefunkčnost významných agend SMB.	Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti. Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové	Řídit bezpečnostní architekturu napříč SMB a dohlížet na implementaci bezpečnostních standardů v SMB podle nového ZKB (řídí kancelář kybernetické

			stavy). Vytvoření kompetenčního modelu v rámci týmu včasné reakce SŘBI pro případy havarijních a krizových stavů.	bezpečnosti).
	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
4,17	S-T	Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb. Kvalitní komunikační infrastruktura připojení ÚMČ.	Výpadek metropolitní sítě a internetu (včetně KIVS) 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. Vybudování systému visibility kritických služeb.
	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,92	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
3,71	W-O	Chybí vazba na business vrstvu zpracovávanou ORGO v BPMN diagramech. Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu. Ne všichni klíčoví uživatelé (garanti) mají dostatečné znalosti, aby definovali požadavky na informatiku (formulace toho, co chtějí). OMI nemůže suplovat metodické role uživatelů.	Využití potenciálu umělé inteligence pro zefektivnění interních i externích procesů. Využití AI pro chod úřadu i komunikaci s občany. Využití analýzy procesů z ORGO. Vydání IT směrnic závazných pro SMB.	Navázat úzkou spolupráci OMI-ORGO zaměřenou na optimalizaci procesů a snížení jejich administrativy využitím potenciálu AI.
	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
3,67	W-O	Dlouhá doba od převedení vize do projektů. Nedostatečná komunikace v rámci SMB, městských společností a organizací.	Popsání definice vazeb mezi projekty a sesouladění postupů – road-mapa na období několika let s pravidelnou aktualizací. Koordinace ICT projektů městských subjektů (Řídící orgán ICT). Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy).	Pomocí Řídícího orgánu ICT propojení strategického (Informační strategie), architektonického (EA, bezpečnostní architektura) a projektového (portfolio ICT projektů) řízení. Koordinace portfolia ICT projektů v rámci SMB.

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
3,67	W-O	Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu. Chybí vazba na business vrstvu zpracovávanou ORGO v BPMN diagramech. Uživatelé nemají povědomí o reálných možnostech řešení jejich požadavků (času, schopnosti řešit požadavek, finanční náročnosti). Nedostatečně objektivní požadavky uživatelů. Neznalost uživatele, jak požádat a specifikovat novou funkcionalitu. Ne všichni klíčoví uživatelé (garanti) mají dostatečné znalosti, aby definovali požadavky na informatiku (formulace toho, co chtějí). OMI nemůže suplovat metodické role uživatelů.	Využití potenciálu umělé inteligence pro zefektivnění interních i externích procesů. Využití AI pro chod úřadu i komunikaci s občany. Využití analýzy procesů z ORGO. Vydání IT směrnic závazných pro SMB. Vytvoření a správa katalogu služeb ICT. Vydání IT směrnic závazných pro SMB.	Navázat úzkou spolupráci OMI-ORGO zaměřenou na optimalizaci procesů a snížení jejich administrativy využitím potenciálu AI. Maximálně propojit IT pracovníky s klíčovými pracovníky odborů do rozvoje a využívání IS.
	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
3,54	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.

	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
3,50	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. Přílišná důvěřivost uživatelů k neznámým zdrojům (připojování se k neznámým WiFi).	Systematické vzdělávání uživatelů v oblasti informační bezpečnosti a reakce na kybernetické hrozby. Zavedení bezpečnostních technologií umožňujících včasnou detekci a reakci na koncových zařízeních.

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,46	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. Nárůst požadavků na dokumentaci v ICT dnes zejména v oblasti informační a kybernetické bezpečnosti. Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.	Dlouhodobé plánování zdrojů podle projektů v ICT a bezpečnosti.

	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,46	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	Kvalifikovaní správci aplikací a ICT infrastruktury v oblasti, kterou mají ve své pracovní náplni. Dosažené zkušenosti s implementací informačních systémů. Člen RMB pro oblast informatiky.	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
3,21	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, ...). Odpovědnost za agendy svěřené městským společnostem (výkon svěřených pravomocí), které je mohou dále outsourcovat svým dodavatelům, bez reálné možnosti jejich kontroly. Licenční a technologická závislost na dodavateli (vendor lock-in). Ze zadávacích řízení podle ZZVZ mohou vzejít neadekvátní dodavatelé nebo mohou zadávací řízení trvat nepredikovatelnou dobu.	Aktivní zjišťování plánů rozvoje centrálních IS s cílem získat dostatečný čas na přípravu souvisejících změn. Zavést hodnocení a řízení dodavatelů/dodavatelských řetězců s přihlédnutím k metodice dle nového ZKB.
	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
2,75	S-O	Zavedená podpora uživatelů pomocí service-desku.	Zavést hodnocení kvality vyřešení požadavků zadaných v Help Desku uživatelem. 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.

3. Návrh cílového stavu

Cílový stav je popsán v systému 17 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).

Cíle jsou očíslovány v souladu s předchozí verzí IT strategie. Pokud bylo některého cíle dosaženo a nebyl nahrazen cílem novým, je číslo tohoto cíle z důvodu zachování kontinuity vynecháno.

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	Navázat úzkou spolupráci OMI-ORGO	Spoluprací OMI-ORGO dojde k vytvoření vazby na business vrstvu zpracovávanou ORGO v BPMN diagramech.
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.
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 s optimalizovanými interními procesy 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. Pro optimalizaci procesů a snížení jejich administrativy se využije potenciál AI.
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	Jednotný katalog ICT služeb umožňuje využívat infrastrukturní, platformové, bezpečnostní a aplikační služby poskytované pro SMB centrálně jednotným způsobem (zahrnuje SMB, městské organizace a městské firmy).

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.
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 ICT zákazníků

číslo	strategický cíl	popis
11	Komunikovat nabídku a poskytovat jednotné 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 na základě jejich optimalizace. Zvýšení kontextové informovanosti a transparentnosti (kroky proběhlé a příští).
13	Podporovat využívání služeb městského cloudu organizacemi SMB	Městské cloudové služby uvedené v jednotném katalogu ICT služeb na portálu SMB (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 (aplikační ICT služby, např. GINIS, eSPIS) 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 ICT služeb SMB	Všechny služby uvedené v katalogu ICT služeb SMB, 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 Řídícím orgánem ICT.
19	Dosahovat soulad s digitální legislativou (compliance)	Služby města poskytované digitalizovaně jsou plně v souladu s legislativními požadavky.

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.

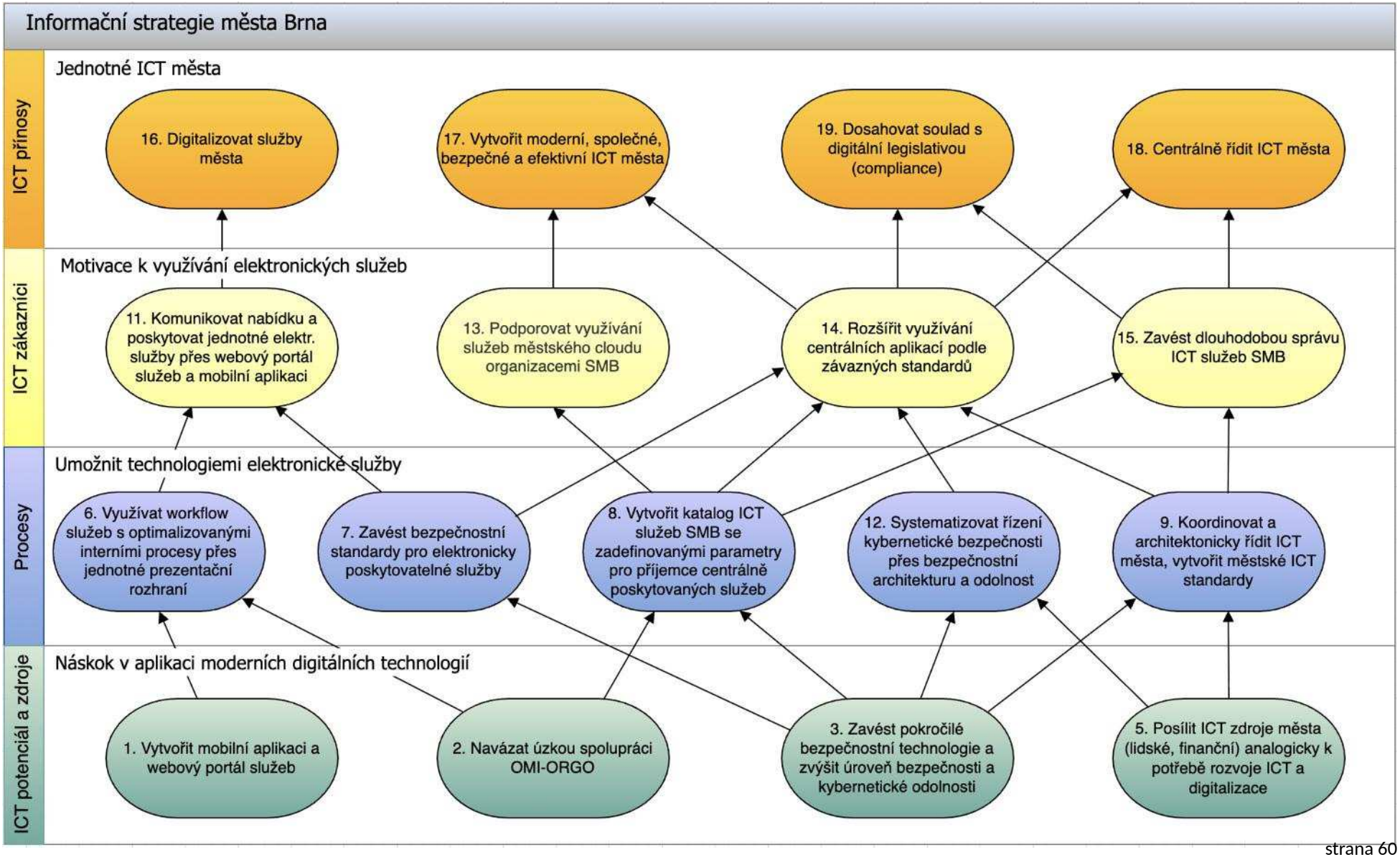
Ve strategické mapě (schéma Balanced Scorecard) jsou kauzální vazby znázorněny šipkami, kdy ve směru šipky je uvažován vztah příčina vyvolávající následek. Zaměření na strategicky významné vztahy, bez ambice na analýzu všech myslitelných vazeb mezi cíli, je jednou z hlavních předností použité metody 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;
- 5 cílů v perspektivě Procesy;
- 4 cíle 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 čtveřice 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. *Navázat úzkou spolupráci OMI-ORGO;*
3. *Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a kybernetické odolnosti;*
6. *Využívat workflow služeb s optimalizovanými interními procesy přes jednotné prezentační rozhraní;*
7. *Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby;*
11. *Komunikovat nabídku a poskytovat jednotné 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:

2. Navázat úzkou spolupráci OMI-ORGO;

3. Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a kybernetické odolnosti;

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, 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 legislativou* kauzálně propojuje deset cílů směřujících k zajištění souladu ICT SMB s požadavky legislativy:

2. Navázat úzkou spolupráci OMI-ORGO;

3. Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a kybernetické odolnosti;

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;

15. Zavést dlouhodobou správu ICT služeb SMB;

19. Dosahovat soulad s digitální legislativou (compliance).

Soulad s digitální legislativou je založen na uplatnění pokročilých bezpečnostních technologií a na nasazení odpovídajících zdrojů včetně spolupráce specializovaných útvarů MMB (zejména OMI a ORGO), 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:

2. Navázat úzkou spolupráci OMI-ORGO;

3. Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a kybernetické odolnosti;

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;

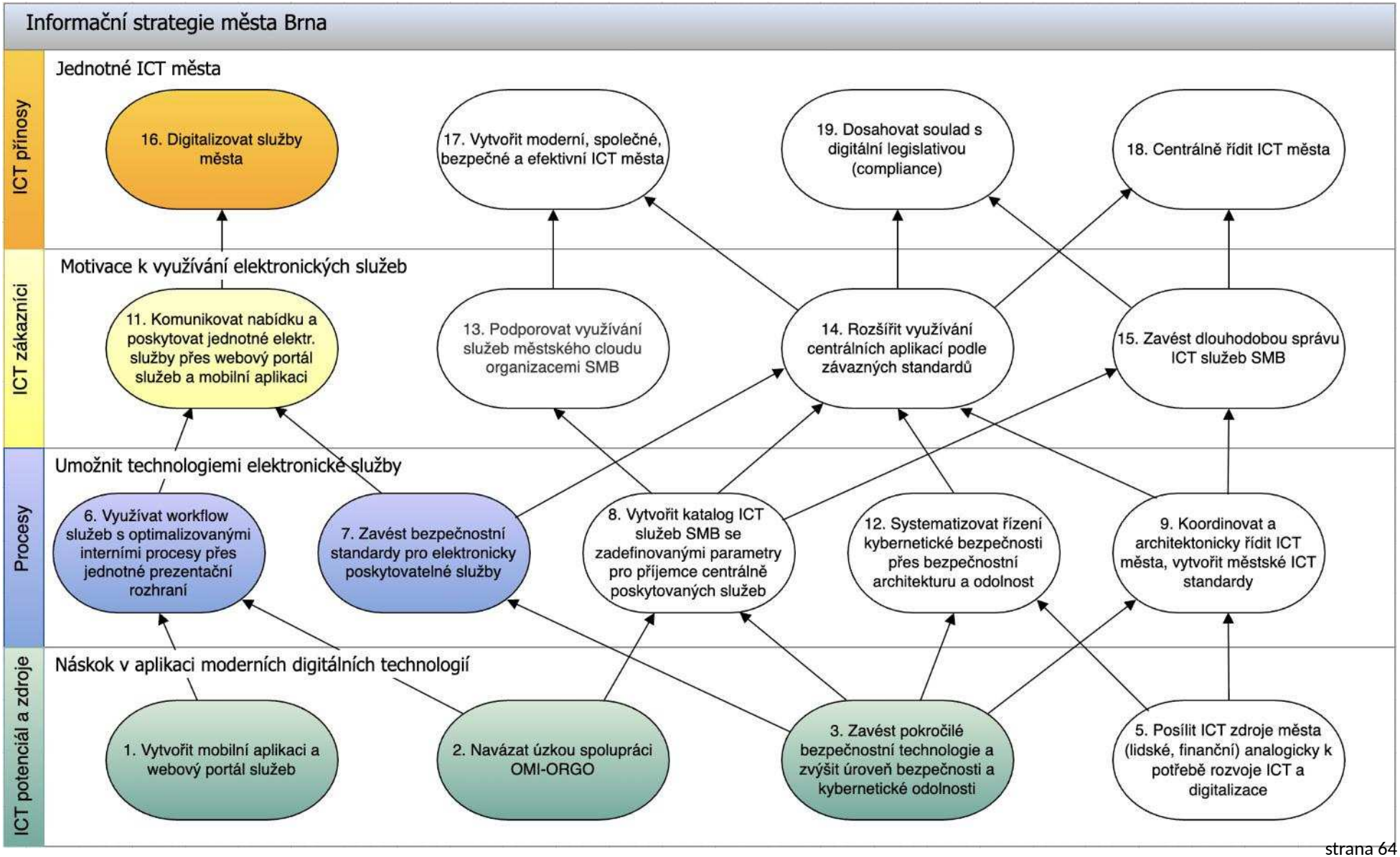
14. Rozšířit využívání centrálních aplikací podle závazných standardů;

15. Zavést dlouhodobou správu ICT služeb SMB;

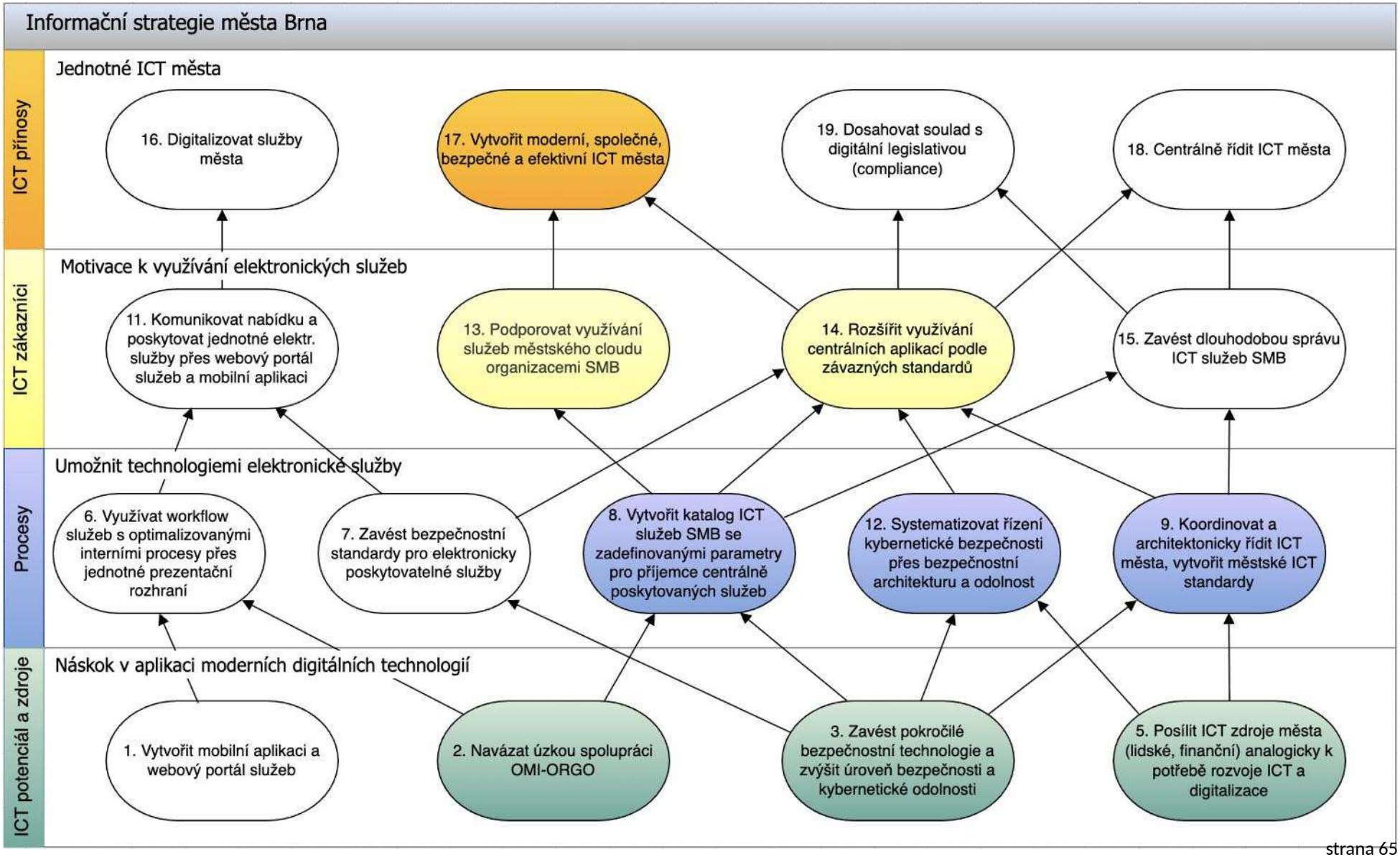
18. Centrálně řídit ICT města.

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.

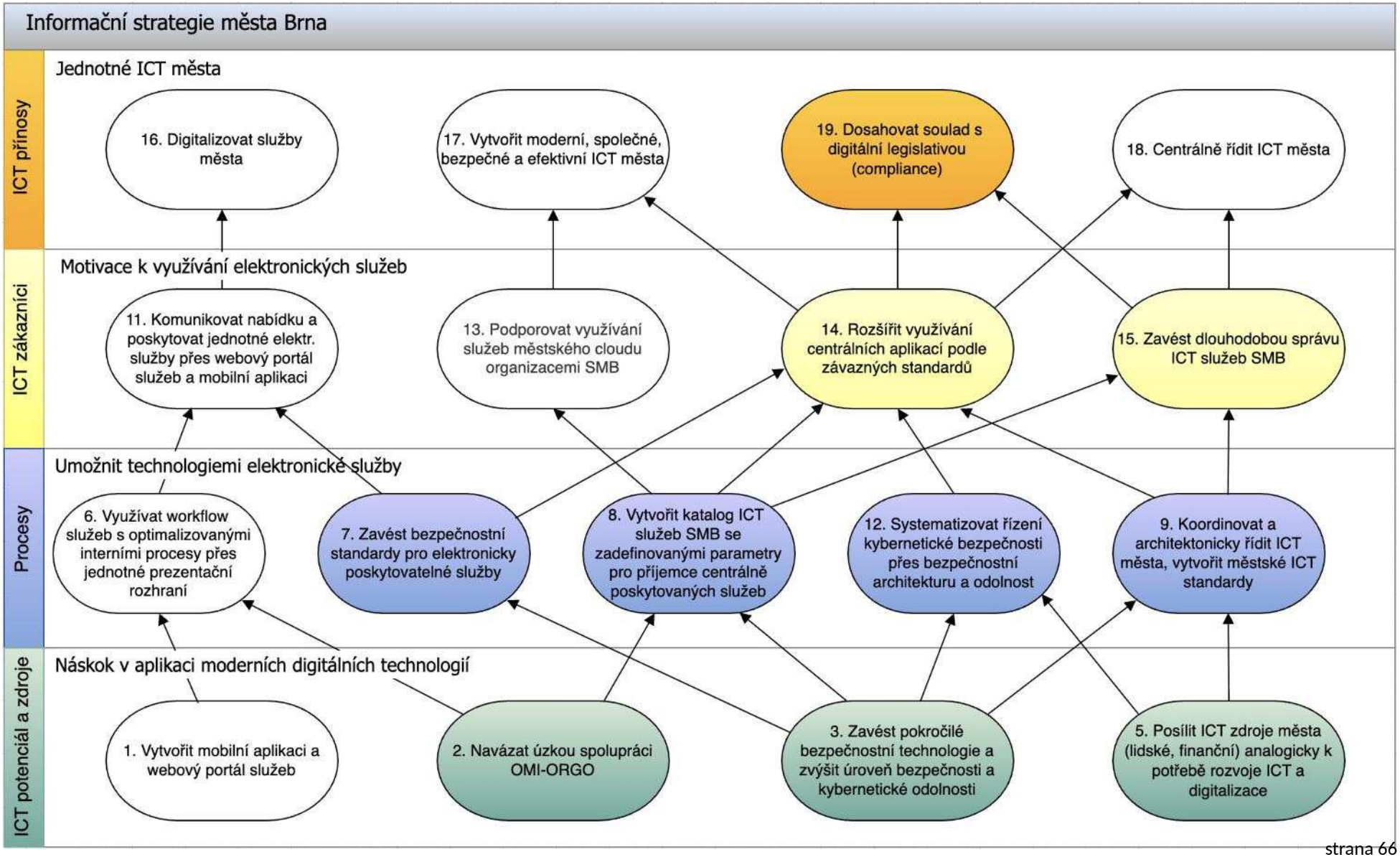
3.3.2. Řetězec digitalizace služeb



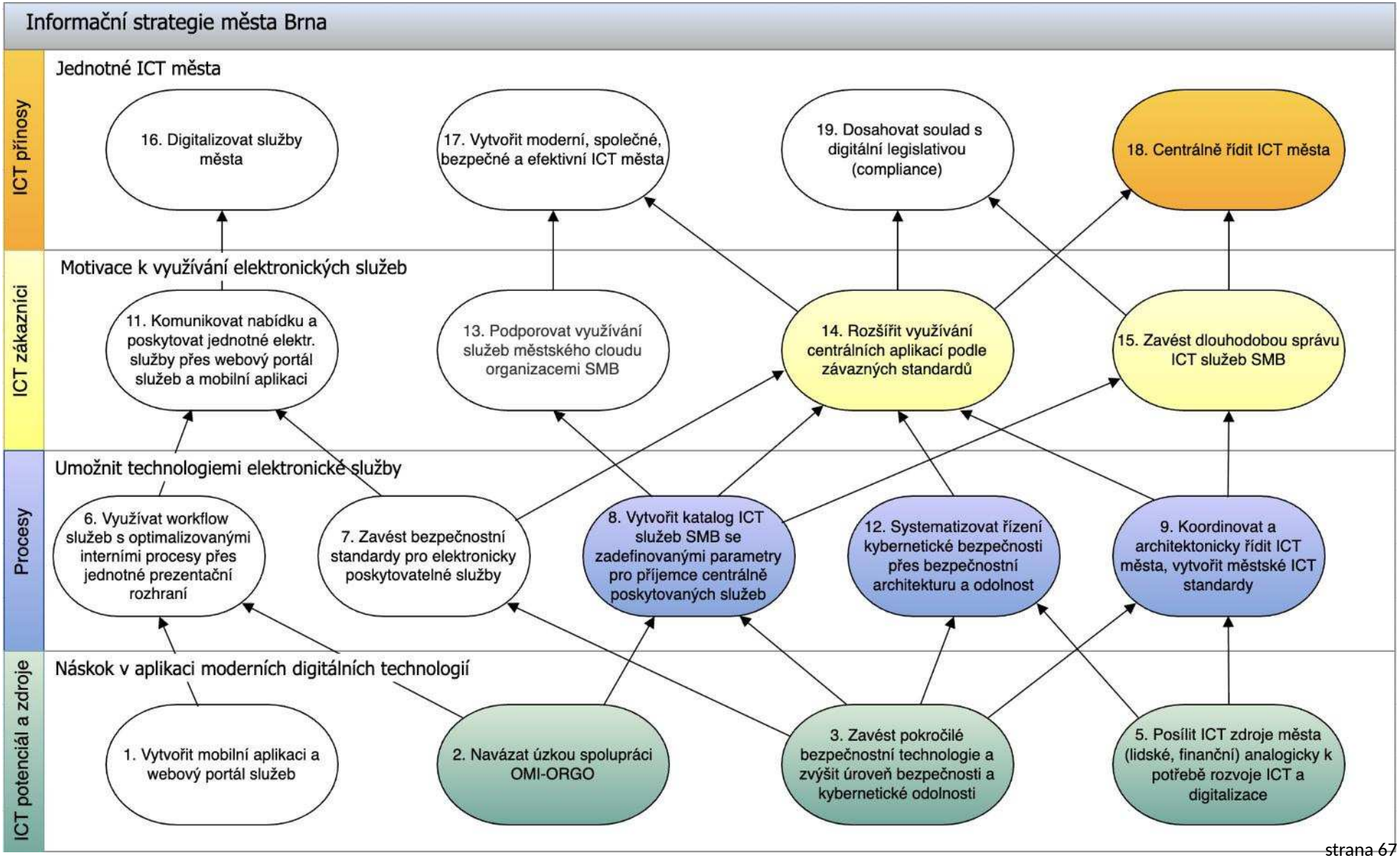
3.3.3. Řetězec tvorby ICT města



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 2026, 2027, 2028, 2029 a 2030.

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	2026	Připraven katalog služeb pro občany a návštěvníky města. Vytvořen koncept integrace aplikací do mobilní aplikace. Město provozuje webový portál služeb v souladu s moderními technologickými a bezpečnostními standardy. Je vytvořen plán rozvoje webového portálu služeb.
			2027	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.
			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.
			2030	Rozvoj mobilní aplikace o nové služby podle plánu. Rozvoj webového portálu služeb podle plánu.
2	Navázat úzkou spolupráci OMI-ORGO	Popsána business vrstva v BPMN diagramech	2026	Model spolupráce ORGO-OMI je formálně dohodnut, včetně zakotvení spolupráce do Organizačního řádu. Je vytipován soubor pilotních procesů určených k optimalizaci.
			2027	Spolupráce ORGO-OMI je připravena, vybrané pilotní procesy jsou optimalizovány a připraveny pro implementaci. Je provedeno vyhodnocení mechanismu spolupráce pro metodický popis postupů společné pracovní platformy.
			2028	Spolupráce ORGO-OMI je standardní součástí projektového řízení pro relevantní projekty a je cíleně využívána automatizace a AI tam, kde to dává smysl. Je provedeno vyhodnocení přínosů optimalizovaných procesů a využity výstupy spolupráce jako podklad pro dlouhodobé plánování další digitalizace.
3	Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti a	Vyspělost bezpečnostního modelu města	2026	V rozsahu SMB je realizován systém visibility stavu kritických služeb. Zjištěn zájem ÚMČ, příspěvkových organizací a městských firem (organizace SMB) využívat centrální služby pro detekci zranitelností v jejich sítích.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
	kybernetické odolnosti		2027	Zavedeno vícefaktorové ověřování uživatelů a zařízení včetně pokročilých funkcí správy identit. Vytvořen a provozován centrální systém automatizované reakce na detekované a kategorizované KBI. Rozvoj systému visibility stavu kritických služeb v SMB o další služby. Rozvoj odebíraných služeb dohledového a dozorového bezpečnostního centra. Je nasazena a aktivně provozována technologie prevence úniku dat, která zahrnuje běžné komunikační kanály napříč MMB.
			2028	Metropolitní síť města Brna je provozována na základě jasné bezpečnostní architektury, jednotlivé provozované technologie jsou propojeny a tvoří synergizující celky, umožňující procesní řízení v klidu i v případě krizových scénářů. Jsou zavedeny a zdokumentovány propoje v rámci jednotlivých technologií, vedoucí k zajištění požadavků procesního modelu.
			2029	Provozovaná bezpečnostní architektura umožňuje na základě vnitřní robustnosti rozvoj a podporuje uživatelskou bezpečnost v rámci aplikace procesního modelu ORGO při dodržení platných procesů, technologie dohlížejí na případná porušení některých pracovních postupů a informují o nich příslušné osoby.
			2030	Provozované bezpečnostní technologie zajišťují soulad s legislativními požadavky, technologická základna se podle potřeby udržuje a obměňuje v reakci na nové požadavky.
5	Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace	Obsazení rolí	2026	Vznik pracoviště technické podpory ÚMČ (dvě pozice). Rozšíření KKB o 2 funkční místa. Změna organizace KKB na víceúrovňově řízený útvar.
			2027	Vydefinovány role analytiků potřeb uživatelů pro zjišťování potřeb uživatelů a jejich realizovatelnost v ICT prostředí.
			2028	Vznik pracoviště pro analýzu potřeb uživatelů s 2 novými funkčními místy.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
6	Využívat workflow služeb s optimalizovanými interními procesy přes jednotné prezentační rozhraní	Zavedeno workflow služeb na portálu i městské aplikaci	2026 2027 2028 2029	Vysoutěženo jednotné prezentační rozhraní pro mobilní aplikaci. Vytvořen zastřešující rozcestník pro služby města Brna poskytované přes web. Workflow u aplikací poskytujících služby úřadu je navrženo ve spolupráci s garanty procesů a ORGO. Vytvořeno jednotné prezentační rozhraní pro mobilní aplikaci a pro služby poskytované přes web. Dokončena mobilní aplikace. Vyhodnocení zkušeností z nasazování služeb a plán rozvoje na další rok. Rozvoj aplikací podle schváleného plánu rozvoje.
7	Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby	Bezpečnostní standardy zavedeny	2026 2027 2028 2029 2030	Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro městské akciové společnosti a pro významné příspěvkové organizace. Standard připojování MČ a městských organizací do LOG managementu. Jsou stanovena závazná pravidla pro používání vybraných forem umělé inteligence provozovaných na městské platformě a využívání agentních systémů ležících mimo ni. 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. Existují otestované typové scénáře, krizové a havarijní plány pro krizové řízení v doméně kybernetické bezpečnosti standardizované podle principů krizového řízení města a principů řízení služeb SMB. Typové scénáře pro doménu kybernetické bezpečnosti jsou provázány s ostatními doménami a krizové řízení bezpečnosti služeb je založeno na testovatelných scénářích opírajících se o platné standardy. Bezpečnostní standardy pro elektronicky poskytované služby, založené na řízené bezpečnostní architektuře, jsou pravidelně testovány a využívány jako podklad pro oblast krizového a havarijního řízení.
8	Vytvořit katalog ICT služeb SMB se zadefinovanými parametry pro příjemce centrálně poskytovaných	Katalog ICT služeb vytvořen	2026 2027	Katalog ICT služeb SMB je dokončen (první vydání), včetně návrhu souvisejících procesů správy katalogu. Katalog ICT služeb SMB umožňuje využívat sdílené aplikační, infrastrukturní, platformové a bezpečnostní služby (včetně cloudu) jednotným způsobem, a to pro SMB a zřizované organizace

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
	služeb			města (městské firmy).
			2028	Optimalizovaná verze katalogu ICT služeb SMB (aktualizované vydání) umožňuje 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	2026	Napojení centrální evidence infrastrukturních služeb (GPC) do EA modelu a s tím spojená aktualizace EA modelu, bude sloužit jako podklad pro visibilitu kritických služeb. Nalezení způsobu provázání bezpečnostní architektury a Enterprise Architecture.
			2027	Vydána směrnice a pracovní postup pro zadávání architektonických prvků a integraci dílčích agendových systémů do EA modelu. Systémy centrálně poskytované v rámci SMB jsou zavedeny v EA modelu. Řízení metodami EA (Enterprise Architecture) je aplikováno v rámci SMB na centrálně poskytované systémy.
			2028	Vybrané služby dané legislativou (RPP) jsou provázány na EA ve vhodné míře detailu.
			2029	Doplněny další služby z RPP provázané na EA.
			2030	Doplněna business vrstva do EA modelu ve spolupráci s ORGO.
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	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.
			2030	Jsou udržovány a podle potřeby aktualizovány procesy pro krizové řízení a řešení incidentů napříč SMB bez ohledu na jejich rozsah využívající možnosti sdílené architektury.
11	Komunikovat nabídku a poskytovat jednotné elektr.	Životní situace řešeny elektronicky přes portál	2026	Platební brána je implementována pro služby vyžadující platby. Pilotní prověření vybraných služeb přes webový portál služeb.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
	služby přes webový portál služeb a mobilní aplikaci	služeb či mobilní aplikaci		Nasazení zvolených služeb přes webový portál služeb.
			2027	Nasazení zvolených služeb přes mobilní aplikaci.
			2028	Vytvoření datové analytiky pro zrychlení a optimalizaci průběhu procesu. Rozvoj služeb přes mobilní aplikaci a webový portál služeb.
			2029	Rozvoj služeb přes mobilní aplikaci a webový portál služeb.
			2030	Rozvoj služeb přes mobilní aplikaci a webový portál služeb.
13	Podporovat využívání služeb městského cloudu organizacemi SMB	Městské cloudové služby využívány městskými firmami	2026	Zahájen design městského cloudu a portálu ICT služeb.
			2027	Dokončen design městského cloudu a portálu ICT služeb, které bude poskytovat. Portál umožňuje objednávání ICT služeb městského cloudu (objednávkový portál cloudových služeb).
			2028	Přístup k ICT službám městského cloudu je zajištěn pro všechny organizace SMB.
			2029	Rozvoj portfolia ICT služeb.
14	Rozšířit využívání centrálních aplikací podle závazných standardů	ICT služby poskytované SMB standardizovány	2026	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 ...). Navržena struktura technologického standardu (jako základní technologický rámec s možností jeho využití ve výběrových řízeních) s vazbou na architektonické principy.
			2027	Navržen technologický standard v 1. verzi.
			2028	Zpřesnění technologického standardu. Centrálně poskytované aplikace (aplikační ICT služby, např. GINIS, eSPIS) 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 ...).
			2029	Jsou využívány a udržovány technologické, architektonické a bezpečnostní standardy ICT SMB.
15	Zavést dlouhodobou správu ICT služeb SMB	Spolupracující subjekty	2026	Každá ICT služba, která je definována v katalogu ICT služeb, má svého garanta.
			2027	Hlavní garant ICT služby je stanoven u všech služeb uvedených v katalogu ICT služeb, na kterých se podílí více garantů.
			2028	Správa služeb bude optimalizována.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
16	Digitalizovat služby města	Očekávané přínosy z elektronizace služeb dosaženy	2026 2027 až 2030	Město disponuje elektronicky poskytovanými službami pro zvolené služby (1. etapa). Vyhodnoceny přínosy z digitalizovaných služeb. Doplněny další služby.
17	Vytvořit moderní, společné, bezpečné a efektivní ICT města	ICT města sdíleno	2028 2029 2030	Městská ICT infrastruktura je v souladu s technologickými ICT standardy a KB standardy. Technická aktiva MMB jsou v souladu s technologickými 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	2026 až 2030	ICT města je centrálně řízeno Řídícím orgánem ICT SMB. ICT služby jsou dlouhodobě koordinovány určenými garanty.
19	Dosahovat soulad s digitální legislativou (compliance)	Legislativní požadavky jsou naplňovány v plném rozsahu na celém území SMB	2026 až 2030	Návrh a implementace nových opatření plynoucích z aktuálních legislativních změn. Zajištění souladu městských standardů a interních normativních aktů s legislativním prostředím v oblasti ICT včetně mechanismů periodického přezkoumávání. 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 17 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. Systematizace řízení kybernetické bezpečnosti
4. Zavedení dohledových a reaktivních technologií (včetně visibility služeb)
5. Centrální služby a aplikace (katalog ICT služeb SMB)
6. Architektura a koordinace
7. Technologický standard SMB

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	2026	Připraven katalog služeb pro občany a návštěvníky města. Vytvořen koncept integrace aplikací do mobilní aplikace. Město provozuje webový portál služeb v souladu s moderními technologickými a bezpečnostními standardy. Je vytvořen plán rozvoje webového portálu služeb.
		2027	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.
		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.
		2030	Rozvoj mobilní aplikace o nové služby podle plánu. Rozvoj webového portálu služeb podle plánu.

4.2.2. Digitální služby města Brna (přes JAMB)

Účel strategického projektu:

Přínosový cíl 16. *Digitalizovat služby města*.

Cíle strategického projektu:

2	Navázat úzkou spolupráci OMI-ORGO	2026	Model spolupráce ORGO-OMI je formálně dohodnut, včetně zakotvení spolupráce do Organizačního řádu. Je vytipován soubor pilotních procesů určených k optimalizaci.
		2027	Spolupráce ORGO-OMI je připravena, vybrané pilotní procesy jsou optimalizovány a připraveny pro implementaci. Je provedeno vyhodnocení mechanismu spolupráce pro metodický

			popis postupů společné pracovní platformy.
		2028	Spolupráce ORGO-OMI je standardní součástí projektového řízení pro relevantní projekty a je cíleně využívána automatizace a AI tam, kde to dává smysl. Je provedeno vyhodnocení přínosů optimalizovaných procesů a využity výstupy spolupráce jako podklad pro dlouhodobé plánování další digitalizace.
5	Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace	2027	Vydefinovány role analytiků potřeb uživatelů pro zjišťování potřeb uživatelů a jejich realizovatelnost v ICT prostředí.
		2028	Vznik pracoviště pro analýzu potřeb uživatelů s 2 novými funkčními místy.
6	Využívat workflow služeb s optimalizovanými interními procesy přes jednotné prezentační rozhraní	2026	Vysoutěženo jednotné prezentační rozhraní pro mobilní aplikaci.
		2027	Vytvořen zastřešující rozcestník pro služby města Brna poskytované přes web. Workflow u aplikací poskytujících služby úřadu je navrženo ve spolupráci s garanty procesů a ORGO. Vytvořeno jednotné prezentační rozhraní pro mobilní aplikaci a pro služby poskytované přes web. Dokončena mobilní aplikace.
		2028	Vyhodnocení zkušeností z nasazování služeb a plán rozvoje na další rok.
		2029	Rozvoj aplikací podle schváleného plánu rozvoje.
11	Poskytovat elektr. služby přes webový portál služeb a mobilní aplikaci	2026	Platební brána je implementována pro služby vyžadující platby. Pilotní prověření vybraných služeb přes webový portál služeb. Nasazení zvolených služeb přes webový portál služeb.
		2027	Nasazení zvolených služeb přes mobilní aplikaci.
		2028	Vytvoření datové analytiky pro zrychlení a optimalizaci průběhu procesu. Rozvoj služeb přes mobilní aplikaci a webový portál služeb.
		2029	Rozvoj služeb přes mobilní aplikaci a webový portál služeb.
		2030	Rozvoj služeb přes mobilní aplikaci a webový portál služeb.

4.2.3. Systematizace řízení kybernetické bezpečnosti

Účel strategického projektu:

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

Cíle strategického projektu:

5	Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace	2026	Rozšíření KKB o 2 funkční místa. Změna organizace KKB na víceúrovňově řízený útvar.
7	Zavést bezpečnostní standardy pro elektronicky	2026	Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro městské akciové společnosti a pro významné příspěvkové organizace. Standard připojování MČ a městských organizací do LOG

	poskytovatelné služby		managementu. Jsou stanovena závazná pravidla pro používání vybraných forem umělé inteligence provozovaných na městské platformě a využívání agentních systémů ležících mimo ni.
		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.
		2028	Existují otestované typové scénáře, krizové a havarijní plány pro krizové řízení v doméně kybernetické bezpečnosti standardizované podle principů krizového řízení města a principů řízení služeb SMB.
		2029	Typové scénáře pro doménu kybernetické bezpečnosti jsou provázány s ostatními doménami a krizové řízení bezpečnosti služeb je založeno na testovatelných scénářích opírajících se o platné standardy.
		2030	Bezpečnostní standardy pro elektronicky poskytované služby, založené na řízené bezpečnostní architektuře, jsou pravidelně testovány a využívány jako podklad pro oblast krizového a havarijního řízení.
12	Systematizovat řízení kybernetické bezpečnosti přes bezpečnostní architekturu a odolnost	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.
		2030	Jsou udržovány a podle potřeby aktualizovány procesy pro krizové řízení a řešení incidentů napříč SMB bez ohledu na jejich rozsah využívající možnosti sdílené architektury.

4.2.4. Zavedení dohledových a reaktivních technologií (včetně visibility služeb)

Účel strategického projektu:

Přínosový cíl 17. *Vytvořit moderní, společné, bezpečné a efektivní 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	2026	V rozsahu SMB je realizován systém visibility stavu kritických služeb. Zjištěn zájem ÚMČ, příspěvkových organizací a městských firem (organizace SMB) využívat centrální služby pro detekci zranitelností v jejich sítích.
		2027	Zavedeno vícefaktorové ověřování uživatelů a zařízení včetně pokročilých funkcí správy identit. Vytvořen a provozován centrální systém automatizované reakce na detekované a kategorizované KBI.

			Rozvoj systému visibility stavu kritických služeb v SMB o další služby. Rozvoj odebíraných služeb dohledového a dozorového bezpečnostního centra. Je nasazena a aktivně provozována technologie prevence úniku dat, která zahrnuje běžné komunikační kanály napříč MMB.
		2028	Metropolitní síť města Brna je provozována na základě jasné bezpečnostní architektury, jednotlivé provozované technologie jsou propojeny a tvoří synergizující celky, umožňující procesní řízení v klidu i v případě krizových scénářů. Jsou zavedeny a zdokumentovány propoje v rámci jednotlivých technologií, vedoucí k zajištění požadavků procesního modelu.
		2029	Provozovaná bezpečnostní architektura umožňuje na základě vnitřní robustnosti rozvoj a podporuje uživatelskou bezpečnost v rámci aplikace procesního modelu ORGO při dodržení platných procesů, technologie dohlížejí na případná porušení některých pracovních postupů a informují o nich příslušné osoby.
		2030	Provozované bezpečnostní technologie zajišťují soulad s legislativními požadavky, technologická základna se podle potřeby udržuje a obměňuje v reakci na nové požadavky.

4.2.5. Centrální služby a aplikace (katalog ICT služeb SMB)

Účel strategického projektu:

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

Cíle strategického projektu:

8	Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb	2026	Katalog ICT služeb SMB je dokončen (první vydání), včetně návrhu souvisejících procesů správy katalogu.
		2027	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).
		2028	Optimalizovaná verze katalogu ICT služeb SMB (aktualizované vydání) umožňuje 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	Zahájen design městského cloudu a portálu ICT služeb.
		2027	Dokončen design městského cloudu a portálu ICT služeb, které bude poskytovat. Portál umožňuje objednávání ICT služeb městského cloudu (objednávkový portál cloudových služeb).
		2028	Přístup k ICT službám městského cloudu je zajištěn pro všechny organizace SMB.
		2029	Rozvoj portfolia ICT služeb.
15	Zavést dlouhodobou správu ICT služeb SMB	2026	Každá ICT služba, která je definována v katalogu ICT služeb, má svého garanta.
		2027	Hlavní garant ICT služby je stanoven u všech služeb uvedených v katalogu ICT služeb, na kterých se podílí více garantů.
		2028	Správa služeb bude optimalizována.

4.2.6. Architektura a koordinace

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	2026	Vznik pracoviště technické podpory ÚMČ (dvě pozice).
9	Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy	2026	Napojení centrální evidence infrastrukturních služeb (GPC) do EA modelu a s tím spojená aktualizace EA modelu, bude sloužit jako podklad pro visibilitu kritických služeb. Nalezení způsobu provázání bezpečnostní architektury a Enterprise Architecture.
		2027	Vydána směrnice a pracovní postup pro zadávání architektonických prvků a integraci dílčích agendových systémů do EA modelu. Systémy centrálně poskytované v rámci SMB jsou zavedeny v EA modelu. Řízení metodami EA (Enterprise Architecture) je aplikováno v rámci SMB na centrálně poskytované systémy.
		2028	Vybrané služby dané legislativou (RPP) jsou provázány na EA ve vhodné míře detailu.
		2029	Doplněny další služby z RPP provázané na EA.
		2030	Doplněna business vrstva do EA modelu ve spolupráci s ORGO.
14	Rozšířit využívání centrálních aplikací podle závazných standardů	2026	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 …).
		2028	Centrálně poskytované aplikace (aplikační ICT služby, např. GINIS, eSPIS) 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 …).
		2029	Jsou využívány a udržovány technologické, architektonické a bezpečnostní standardy ICT SMB.
15	Zavést dlouhodobou správu ICT služeb SMB	2026	Každá ICT služba, která je definována v katalogu ICT služeb, má svého garanta.
		2027	Hlavní garant ICT služby je stanoven u všech služeb uvedených v katalogu ICT služeb, na kterých se podílí více garantů.
		2028	Správa služeb bude optimalizována.

4.2.7. Technologický standard SMB

Účel strategického projektu:

Přínosový cíl 18. *Centrálně řídit ICT města*.

Cíle strategického projektu:

14	Rozšířit využívání centrálních aplikací podle závazných standardů	2026	Navržena struktura technologického standardu (jako základní technologický rámec s možností jeho využití ve výběrových řízeních) s vazbou na architektonické principy.
		2027	Navržen technologický standard v 1. verzi.
		2028	Zpřesnění technologického standardu.
		2029	Jsou využívány a udržovány technologické, architektonické a bezpečnostní standardy ICT 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		2026	2027	2028	2029	2030
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 mobilní aplikace.					
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.					
Cíl	**Digitální služby města Brna (přes JAMB)**					
2	Model spolupráce ORGO-OMI je formálně dohodnut, včetně zakotvení spolupráce do Organizačního řádu. Je vytipován soubor pilotních procesů určených k optimalizaci.					
2	Spolupráce ORGO-OMI je připravena, vybrané pilotní procesy jsou optimalizovány a připraveny pro implementaci. Je provedeno vyhodnocení mechanismu spolupráce pro metodický popis postupů společné pracovní platformy.					
2	Spolupráce ORGO-OMI je standardní součástí projektového řízení pro relevantní projekty a je cíleně využívána automatizace a AI tam, kde to dává smysl.					
2	Je provedeno vyhodnocení přínosů optimalizovaných procesů a využity výstupy spolupráce jako podklad pro dlouhodobé plánování další digitalizace.					
5	Vydefinovány role analytiků potřeb uživatelů pro zjišťování potřeb uživatelů a jejich realizovatelnost v ICT prostředí.					
5	Vznik pracoviště pro analýzu potřeb uživatelů s 2 novými funkčními místy.					
6	Vysoutěženo jednotné prezentační rozhraní pro mobilní aplikaci.					

Strategické projekty		2026	2027	2028	2029	2030
6	Vytvořen zastřešující rozcestník pro služby města Brna poskytované přes web.					
6	Workflow u aplikací poskytujících služby úřadu je navrženo ve spolupráci s garanty procesů a ORGO.					
6	Vytvořeno jednotné prezentační rozhraní pro mobilní aplikaci a pro služby poskytované přes web.					
6.	Dokončena mobilní aplikace.					
6.	Vyhodnocení zkušeností z nasazování služeb a plán rozvoje na další rok.					
6.	Rozvoj aplikací podle schváleného plánu rozvoje.					
11	Platební brána je implementována pro služby vyžadující platby.					
11	Pilotní prověření vybraných služeb přes webový portál služeb.					
11	Nasazení zvolených služeb přes webový portál služeb.					
11	Nasazení zvolených služeb přes mobilní aplikaci.					
11	Vytvoření datové analytiky pro zrychlení a optimalizaci průběhu procesu.					
11	Rozvoj služeb přes mobilní aplikaci a webový portál služeb.					
Cíl	**Systematizace řízení kybernetické bezpečnosti**					
5	Rozšíření KKB o 2 funkční místa.					
5	Změna organizace Kanceláře kybernetické bezpečnosti na víceúrovňově řízený útvar.					
7	Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro městské akciové společnosti a pro významné příspěvkové organizace.					
7	Standard připojování MČ a městských organizací do LOG managementu.					
7	Jsou stanovena závazná pravidla pro používání vybraných forem umělé inteligence provozovaných na městské platformě a využívání agentních systémů ležících mimo ni.					

Strategické projekty		2026	2027	2028	2029	2030
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.					
7	Existují otestované typové scénáře, krizové a havarijní plány pro krizové řízení v doméně kybernetické bezpečnosti standardizované podle principů krizového řízení města a principů řízení služeb SMB.					
7	Typové scénáře pro doménu kybernetické bezpečnosti jsou provázány s ostatními doménami a krizové řízení bezpečnosti služeb je založeno na testovatelných scénářích opírajících se o platné standardy.					
7	Bezpečnostní standardy pro elektronicky poskytované služby, založené na řízené bezpečnostní architektuře, jsou pravidelně testovány a využívány jako podklad pro oblast krizového a havarijního řízení.					
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.					
12	Jsou udržovány a podle potřeby aktualizovány procesy pro krizové řízení a řešení incidentů napříč SMB bez ohledu na jejich rozsah využívající možnosti sdílené architektury.					
Cíl	**Zavedení dohledových a reaktivních technologií (včetně visibility služeb)**					
3	V rozsahu SMB je realizován systém visibility stavu kritických služeb.					
3	Zjištěn zájem ÚMČ, příspěvkových organizací a městských firem (organizace SMB) využívat centrální služby pro detekci zranitelností v jejich sítích.					
3	Zavedeno vícefaktorové ověřování uživatelů a zařízení včetně pokročilých funkcí správy identit.					
3	Vytvořen a provozován centrální systém automatizované reakce na detekované a kategorizované KBI.					
3	Rozvoj systému visibility stavu kritických služeb v SMB o další služby.					

Strategické projekty		2026	2027	2028	2029	2030
3	Rozvoj odebíraných služeb dohledového a dozorového bezpečnostního centra.		■			
3	Je nasazena a aktivně provozována technologie prevence úniku dat, která zahrnuje běžné komunikační kanály napříč MMB.		■			
3	Metropolitní síť města Brna je provozována na základě jasné bezpečnostní architektury, jednotlivé provozované technologie jsou propojeny a tvoří synergizující celky, umožňující procesní řízení v klidu i v případě krizových scénářů.			■		
3	Jsou zavedeny a zdokumentovány propoje v rámci jednotlivých technologií, vedoucí k zajištění požadavků procesního modelu.			■		
3	Provozovaná bezpečnostní architektura umožňuje na základě vnitřní robustnosti rozvoj a podporuje uživatelskou bezpečnost v rámci aplikace procesního modelu ORGO při dodržení platných procesů, technologie dohlížejí na případná porušení některých pracovních postupů a informují o nich příslušné osoby.				■	
3	Provozované bezpečnostní technologie zajišťují soulad s legislativními požadavky, technologická základna se podle potřeby udržuje a obměňuje v reakci na nové požadavky.					■
Cíl	**Centrální služby a aplikace (katalog ICT služeb SMB)**					
8	Katalog ICT služeb SMB je dokončen (první vydání), včetně návrhu souvisejících procesů správy katalogu.	■				
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).		■			
8	Optimalizovaná verze katalogu ICT služeb SMB (aktualizované vydání) umožňuje využívat sdílené aplikační, infrastrukturní, platformové a bezpečnostní služby (včetně cloudu) jednotným způsobem, a to pro SMB a zřizované organizace města (městské firmy).			■		
13	Zahájen design městského cloudu a portálu ICT služeb.	■				
13	Dokončen design městského cloudu a portálu ICT služeb, které bude poskytovat.		■			
13	Portál umožňuje objednávání ICT služeb městského cloudu (objednávkový portál cloudových služeb).		■			
13	Přístup k ICT službám městského cloudu je zajištěn pro všechny organizace SMB.			■		
13	Rozvoj portfolia ICT služeb.				■	
15	Každá ICT služba, která je definována v katalogu ICT služeb, má svého garanta.	■				

Strategické projekty		2026	2027	2028	2029	2030
15	Hlavní garant ICT služby je stanoven u všech služeb uvedených v katalogu ICT služeb, na kterých se podílí více garantů.		■			
15	Správa služeb bude optimalizována.			■		
Cíl	**Architektura a koordinace**					
5	Vznik pracoviště technické podpory ÚMČ (dvě pozice).	■				
9	Napojení centrální evidence infrastrukturních služeb (GPC) do EA modelu a s tím spojená aktualizace EA modelu, bude sloužit jako podklad pro visibilitu kritických služeb.	■				
9	Nalezení způsobu provázání bezpečnostní architektury a Enterprise Architecture.	■				
9	Vydána směrnice a pracovní postup pro zadávání architektonických prvků a integraci dílčích agendových systémů do EA modelu.		■			
9	Systémy centrálně poskytované v rámci SMB jsou zavedeny v EA modelu.		■			
9	Řízení metodami EA (Enterprise Architecture) je aplikováno v rámci SMB na centrálně poskytované systémy.		■			
9	Vybrané služby dané legislativou (RPP) jsou provázány na EA ve vhodné míře detailu.			■		
9	Doplněny další služby z RPP provázané na EA.				■	
9	Doplněna business vrstva do EA modelu ve spolupráci s ORGO.					■
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	Centrálně poskytované aplikace (aplikační ICT služby, např. GINIS, eSPIS) 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	Každá ICT služba, která je definována v katalogu ICT služeb, má svého garanta.	■				
15	Hlavní garant ICT služby je stanoven u všech služeb uvedených v katalogu ICT služeb, na kterých se podílí více garantů.		■			

	Strategické projekty	2026	2027	2028	2029	2030
15	Správa služeb bude optimalizována.					
Cíl	**Technologický standard SMB**					
14	Navržena struktura technologického standardu (jako základní technologický rámec s možností jeho využití ve výběrových řízeních) s vazbou na architektonické principy.					
14	Navržen technologický standard v 1. verzi.					
14	Zpřesnění technologického standardu.					
14	Jsou využívány a udržovány technologické, architektonické a bezpečnostní standardy ICT 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	nejméně 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	