B R N O

Datum 27.07.2023
Počet stran 76
Verze 5.00

Analýza současného stavu (SWOT)

Strategické cíle (na období 2023 až 2027)

Strategická mapa (Balanced Scorecard schéma)

Implementace strategie (strategické projekty)

Informační strategie města Brna

Na období 2023 - 2027

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

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 březnu až červenci 2023 jako aktualizace předchozí Informační strategie. 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 2027. Plánování je zde dovedeno až do určení portfolia konkrétních strategických projektů. Samotná informační strategie je pak sladěna se strategií *Vize a Strategie #brno 2050* a vizí informatiky města dosahuje na tento dlouhodobý horizont. Dokument aktualizuje předchozí verzi informační strategii města Brna vytvořenou v roce 2022.

Město Brno

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

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

V rámci péče o všestranný rozvoj svého území a o potřeby svých občanů město Brno zpracovává tento dokument "Aktualizace informační strategie města Brna", upravující strategický rozvoj informatiky města Brna, kterým město Brno formuluje strategické cíle a k nim navrhuje zpracovat příslušné realizační projekty v oblasti informatiky s výhledem do konce roku 2027. Město Brno, jeho městské části, jakož i dotčené subjekty jsou povinny, v rámci péče o všestranný rozvoj svého území a o potřeby svých občanů, a v rámci jim svěřených pravomocí, cíle stanovené dokumentem "Aktualizace informační strategie města Brna" zohledňovat při plnění svých úkolů.

Strategické cíle

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

Perspektiva	Motto	Cíle
ICT přínosy	Jednotné ICT města	Digitalizovat služby města Vytvořit moderní, společné a bezpečné ICT města Centrálně řídit ICT města
ICT zákazníci	Motivace k využívání elektronických služeb	Poskytovat elektr. služby přes webový portál služeb a mobilní aplikaci Umožnit interním uživatelům práci z prostředí domova Podporovat využívání služeb městského cloudu organizacemi SMB Rozšířit využívání centrálních aplikací podle závazných standardů Prohloubit spolupráci pracovníků SMB v oblasti ICT projektů a architektury
Procesy	Umožnit technologiemi elektronické služby	Využívat workflow služeb přes jednotné prezentační rozhraní Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy Koordinovat rozvoj ICT města řízením projektového portfolia
ICT potenciál a zdroje	Náskok v aplikaci moderních digitálních technologií	Vytvořit mobilní aplikaci a webový portál služeb Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty) Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace

Tab.1: Přehled strategických cílů

Strategické ICT projekty

Pro každý cíl je zpracováno měřítko jeho dosažení a stanoveny hodnoty, kterých má být v rámci strategie dosaženo. Naplnění strategických cílů je plánováno realizovat 10 strategickými ICT projekty (resp. programy, pokud se budou dále realizačně členit) rozloženými do let 2023 až 2027. 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	2023	2024	2025	2026	2027
Webová a mobilní platforma města Brna	■	■	■		
Digitální služby města Brna (přes webový portál služeb a městskou mobilní aplikaci)	■	■	■	■	■
Služby autentikace podle eIDAS	■	■	■		
Systematizace řízení kybernetické bezpečnosti	■	■	■	■	■
Zajištění odolnosti		■			
Zavedení dohledových a reaktivních technologií	■	■	■	■	■
Městský cloud	■	■		■	
Centrální služby a aplikace, služby a aplikace v cloudu	■	■	■		
Koordinace, standardizace a architektura	■	■	■		
Systém řízení projektového portfolia	■	■	■		

Tab.2: Přehled strategických projektů

Aktualizace strategie

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

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

Tab.3: Principy aktualizace strategie

1. Základní identifikace a klíčové pojmy

Základní identifikace

Zpracovatelé:

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

1. Tým města Brna

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

Tomáš Aberl	(radní pro informatiku a sport)
Vladan Krásný	(předseda Komise informačních technologií)
David Slavíček	(člen Komise informačních technologií)
David Menšík	(vedoucí Odboru městské informatiky)
Vladimír Halm	(vedoucí Odd. správy inf. systému, Odbor městské informatiky)
Dušan Hájek	(vedoucí odd. systémové a tech. podpory, Odbor městské informatiky)
Jan Kotas	(manažer projektu AISMB, Odbor městské informatiky)
František Sedláček	(koordinátor KB, Kancelář kybernetické bezpečnosti)
Rostislav Obrlík	(vedoucí Úseku tajemníka)
Jaroslav Mikuš	(Referát právně-ekonomický, Oddělení strategického plánování, Odbor strategického rozvoje a spolupráce)
Michal Jukl	(ředitel ICT, TSB)
Robert Schindler	(architekt kybernetické bezpečnosti, TSB)
Aleš Mejzlík	(zástupce za odbornou veřejnost, Komise informačních technologií)
Jan Zachoval	(podniková architektura, AUTOCONT a. s.)
Lukáš Vlček	(podniková architektura, AUTOCONT a. s.).

2. Tým externí podpory

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

Petr Hujňák	(Per Partes Consulting, s. r. o.)
Jaroslav Hujňák	(Per Partes Consulting, s. r. o.)

Právní podpora:

Milan Šebesta	(MT Legal)
David Mareš	(MT Legal).

Předmět:

Předmětem aktualizace informační strategie je informatika města Brna v letech 2023 až 2027.

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 2023 - 2027. 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 byla zpracována ke dni 23.6.2022 a čtvrtá aktualizace 27.7.2023. 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 2027
- Návrh cílového stavu – strategická mapa a kauzální řetězce
- Plán implementace strategie – měřítka plnění cílů
- Implementační plán přechodu – strategické ICT projekty
- Závěrečné přezkoumání strategie - přezkoumání celkového dokumentu.

Legislativní rámec ČR a EU

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

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

Právní předpisy ČR:

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

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

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

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

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

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

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

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

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

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

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

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

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

- Zákon č. 500/2004 Sb., správní řád ve znění pozdějších předpisů, ve znění pozdějších předpisů

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

  Zákon **o elektronických komunikacích**[4] upravuje na základě práva Evropské unie podmínky podnikání a výkon státní správy, včetně regulace trhu, v oblasti elektronických komunikací. Právní úprava zde obsažená reguluje především přenos informací prostřednictvím sítí elektronických komunikací a rozhlasového a televizního vysílání. Z věcné působnosti zákona je naopak vyňat obsah rozhlasového či televizního vysílání,

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

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

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

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

jakož i obsah sdílený prostřednictvím internetu.

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

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

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

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

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

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

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

- **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů**

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

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

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

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

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

- Zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů
- Zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů
- **Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů**

  Zákon **o službách vytvářejících důvěru pro elektronické transakce** v návaznosti na příslušný předpis Evropské unie[9] upravuje zejména požadavky na podepisování dokumentů v závislosti na podepisující osobě a osobě, vůči níž je právně jednáno. Zákon dále vymezuje též postupy kvalifikovaných poskytovatelů služeb vytvářejících důvěru, které vydávají certifikáty ověřující identitu podepisujících osob, a také vymezuje působnost Ministerstva vnitra v této oblasti, jakož i stanovuje sankce, které může tento orgán v rámci svého dohledu uložit. Ústředním pojmem, se kterým zákon pracuje, je pojem elektronického podpisu.[10] Právní úprava zde obsažená velkou měrou přispívá k rozšiřování elektronizace právního styku a tím i k jeho značnému usnadnění.

- **Zákon č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů**

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

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

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

- **Zákon č. 12/2020 Sb. o právu na digitální služby a o změně některých zákonů**

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

10 **Elektronickým podpisem** se rozumí data v elektronické podobě, která 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.

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

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

Související podzákonné právní předpisy ČR:

- Vyhláška č. 515/2020 Sb., o struktuře informací zveřejňovaných o povinném subjektu a o osnově popisu úkonů vykonávaných v rámci agendy
- Vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy), ve znění pozdějších předpisů
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů
- Vyhlášky 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů
- Vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, ve znění pozdějších předpisů
- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů
- Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, ve znění pozdějších předpisů
- Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu

Právní předpisy EU (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

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.

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

oznámeného systému elektronické identifikace[14] jiného členského státu. Dále stanovuje pravidla pro služby vytvářející důvěru[15], zejména u elektronických transakcí a právní rámec pro elektronické podpisy, elektronické pečetě, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování a certifikační služby pro autentizaci internetových stránek. Tím vytváří právní prostředí pro veškeré důležité aspekty elektronických transakcí.

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

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

- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii

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

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

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

- Směrnice Evropského parlamentu a Rady 2007/2/ES ze dne 14. března 2007 o zřízení Infrastruktury pro prostorové informace v Evropském společenství (INSPIRE)

- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii

- Nařízení Evropského parlamentu a Rady (EU) 2019/1150 ze dne 20. června 2019

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

15 **Službou vytvářející důvěru** se rozumí elektronická služba, která je zpravidla poskytována za úplatu a spočívá ve vytváření, ověřování shody a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami nebo ve vytváření, ověřování shody a ověřování platnosti certifikátů pro autentizaci internetových stránek nebo v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami. Jako příklad lze uvést LongTermDocs od Software 602.

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

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

o podpoře spravedlnosti a transparentnosti pro podnikatelské uživatele online zprostředkovatelských služeb

- Směrnice Evropského parlamentu a Rady (EU) 2019/1152 ze dne 20. června 2019 o transparentních a předvídatelných pracovních podmínkách v Evropské unii
- Směrnice Evropského parlamentu a Rady (EU) 2019/1158 ze dne 20. června 2019 o rovnováze mezi pracovním a soukromým životem rodičů a pečujících osob a o zrušení směrnice Rady 2010/18/EU

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

- 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) 2022/2555 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**)
- 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

Klíčové pojmy a zkratky

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

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

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

Autentikace (autentizace) je proces ověření proklamované identity subjektu.

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

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

Pro měření výkonnosti informatiky byly perspektivy upraveny na:

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

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

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

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

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

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

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

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

Gestor je pracovník úřadu vykonávající pro určitou agendu metodickou činnost, tj. konkretizuje a

optimalizuje postupy procesů (činností) vykonávaných v rámci agendy úřadem. Z pohledu informatiky je gestor představitelem klíčových uživatelů aplikace podporující danou agendu. Z pohledu organizační struktury je gestorem liniový vedoucí skupiny klíčových uživatelů, zpravidla jde o vedoucího oddělení nebo odboru.

IT as a service (ITaaS) je model poskytování informačních technologií formou řízených služeb s definovaným katalogem poskytovaných IT služeb. V tomto modelu je klíčové rozpoznávání potřeb příjemců služeb a agilní přizpůsobování IT služeb těmto potřebám. Příjemcem IT služeb mohou být občané, podnikatelé či návštěvníci města. IT služby jsou poskytovány stejnou formou i dovnitř města a pro městské subjekty.
Model ITaaS vyžaduje standardizaci a zjednodušení produktů dodávaných IT, zvýšenou finanční transparentnost a přímější přidružení cen k položkám katalogu služeb a spotřebě služeb včetně zvýšené provozní efektivnosti IT.

ICT je obecně zaužívaná zkratka pro informační a komunikační technologie.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Technické sítě Brno (TSB) je 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 v Informační strategii města Brna aktualizované v roce 2022 (verze 4.00).

1. Vytvořit moderní portál města

V rámci veřejné zakázky „Tvorba a provoz webové platformy města Brna“ byla vytvořena Platforma pro weby města Brna, na které jsou implementovány a plně v provozu weby: brno.cz, en.brno.cz (anglická verze webu brno.cz), onstage.cz, cosedeje.brno.cz, návrhy.damenavas.cz bezpecnejsi.brno.cz. Momentálně se dokončuje web archiv.brno.cz. Dále se aktuálně řeší weby městských částí Kohoutovice, Bystrc, Medlánky a Starý Lískovec. Následně bude možné dále stavět nové webové projekty dle aktuální potřeby. Také je smluvně zajištěna Podpora a Údržba, jakož i Customizace Platformy.

Webová platforma umožňuje ověřování identit NIA, ISDS, Brno ID. Součástí je i řešení kybernetické bezpečnosti. Z hlediska měřítka strategického cíle je tato provozovaná platforma technologicky i bezpečnostně základem pro vybudování Portálu města.

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

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

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

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

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

Probíhá veřejná zakázka „LOG management“ - implementace plánována v roce 2023. V cílovém stavu bude zajišťovat jak shromažďování logů pro další technologie bezpečnostního dohledu, tak i provozní monitoring. Vybraný systém též umožní automatizovat upozornění na anomální jevy a podporu pro obsluhu ICT prostředí.

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

Došlo k systematizaci nových procesů pro evidenci, ověřování a předávání KB incidentů z různých zdrojů, připravují se automatizované sondy s moduly detekce anomálií (částečně splněno).

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

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

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

Datové linky jsou vybudovány. Datové propojení obou datových center je těsně před dokončením. Veškeré potřebné aktivní prvky byly již dodány a probíhá jejich zapojení a konfigurace. Rozdělení technologií proběhne do konce letošního roku. Zdržení způsobila nedostupnost klíčových aktivních prvků na globálním trhu související s nedostupností čipů.

TSB DC (B5, S29) jsou plně redundantní včetně internetové konektivity.

Centrum metropolitní sítě je zakončeno na MN3 v tuto chvíli představuje SPOF.

5. Posílit datovou integraci přes integrační platformu

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

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

Je definován a nastaven Service Bus integrační platformy, Service Bus je využíván pro elektronické služby městského portálu.

6. Využívat workflow aplikací přes jednotné prezentační rozhraní

Webový portál je připraven jako FrontEnd jednotlivých systémů, zajišťujících jednotlivé služby.

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

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

Výběr aplikace a návrh workflow na základě BPMN diagramů vytvořených na ORGO bude začleněn do projektu Městského portálu občana.

7. Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby

Standardy jsou postupně připravovány a je aplikována jak legislativa pro oblast kyberbezpečnosti, tak i doporučení směrnic (NIS 2, …) a metodické podklady NÚKIB.

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

Závazná pravidla kybernetické bezpečnosti pro ÚMČ existují a jsou zmíněny ve Statutu města, standardy pro PIM/PAM doposud stanoveny nejsou, čeká se na dokončení implementace IDM pro SŘBI.

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

Byly zahájeny práce na pilotním zpracování Katalogu ICT služeb města Brna, jehož součástí budou i služby městského cloudu. V současné době katalog není dokončen. Katalog bude průběžně doplňován podle kapacitních možností.

Byly analyzovány požadavky na ICT služby (pro aplikace) a požadavky ve formě atributů byly doplněny do EA modelu.

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

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

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

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

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

Byla navržena směrnice a pracovní postup pro zadávání architektonických prvků do centrální evidence. Byla navržena směrnice a pracovní postup pro integraci dílčích agendových systémů. Centrální evidence obsahuje aktuální stav všech významných architektonických prvků MMB. Systémy centrálně poskytované v rámci SMB jsou zavedeny v centrální evidenci.

10. Poskytovat z informačních systémů data klasifikovaná jako veřejná

Otevřená data jsou zveřejňována ve standartních otevřených formátech dle MV ČR (nyní už dle Digitální informační agentury). Z informačních systému města je vytěžen GIS a pokračuje rozšiřování otevřených dat z úředních desek MČ.

11. Poskytovat elektr. služby přes portál města v uživatelsky intuitivní a jednotně publikované podobě

V rámci veřejné zakázky „Tvorba a provoz webové platformy města Brna“ byla vytvořena webová platforma pro weby města Brna, na které je již plně funkční web brno.cz. Webová platforma je vybavena funkcionalitami pro možnost ověření identity prostřednictvím NIA, ISDS a Brno ID.

Bylo provedeno Proof-of-Concept testování vyřizování životní situace platby místního poplatku za komunální odpad prostřednictvím AIS GINIS. Bylo ověřeno v aplikaci POSOH (pohledy na osobní účty poplatníků za KO, řešení umožnilo poplatky právnických osob). Další převod agendy do GINISu pozastaven pro změnu požadavků OŽP.

12. Umožnit interním uživatelům práci z prostředí domova

V rámci veřejné zakázky byl realizován projekt „Rozšíření systému VDI VMware Horizon. Stávající implementace kapacitně obslouží 100 připojení vzdálených uživatelů současně. Pro interní uživatele ICT služeb SMB je tedy umožněno využívat aplikace vzdáleným přístupem podle nastavených SLA/OLA parametrů. Postupový cíl pro rok 2022 byl splněn.

13. Podporovat využívání služeb městského cloudu organizacemi SMB

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

Provozní řád byl aktualizován s ohledem na současný stav technologií a procesů OMI MMB. Existují architektonické zásady a metodiky, které jsou aplikovatelné pro další práci na technologickém standardu.

TSB provozují cloudové služby, virtuální servery (VPS) - IaaS/PaaS, zálohování, pronájem diskového prostoru, poskytování aplikací jako služby (spisová služba, ERP) _(SaaS), bezpečnostní dohled etc.

14. Rozšířit využívání centrálních aplikací podle závazných standardů

V roce 2022 byl vytvořen standard týkající se bezpečnosti technických aktiv. Standard má v tuto chvíli dvě části – Systém řízení bezpečnosti informací, který byl vytvořen v roce 2016 a aktualizován s provazbou na procesy města v 6/2022, a dále Minimální standard kybernetické bezpečnosti pro úřady městských částí, který byl schválen RMB v 6/2022 a jehož dodržování je od H1/2022 ukotveno jako povinnost pro městské části ve Statutu města Brna.

TSB poskytují (nyní již) zpoplatněnou službu Posouzení stavu kybernetické bezpečnosti (PSKB), prostřednictvím které je možné plnění standardů ověřit.

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

Brněnská otevřená data jsou publikována dle definovaného procesu, nebyl zaznamenán žádný bezpečnostní incident. Data jsou publikována vždy v souladu s primárním poskytovatelem dat i koncovými uživateli.

Nejnáročnějším procesem je pak zajištění aktuálnosti dat a kontrola funkčnosti zdrojových služeb.

16. Digitalizovat služby veřejné správy (městský portál občana)

V rámci veřejné zakázky „Tvorba a provoz webové platformy města Brna“ byla vytvořena webová platforma pro weby města Brna, na které je již plně funkční web brno.cz.

Web brno.cz sice lze považovat za portál města s koncepčně uspořádanými informacemi o službách, ovšem z hlediska očekávaných přínosů z pohledu elektronizace radnice, k výraznému pokroku nedošlo. Způsob začlenění životních situací do portálu rozpracován sice byl, ovšem (až na objednávání na přepážky) bez digitální komunikace.

17. Vytvořit moderní, společné a bezpečné ICT města

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

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

18. Otevřít městská data veřejnosti

Probíhá rozšiřování nabídky otevřených dat na portálu data.Brno, dle ohlasů veřejnosti jsou stále více využívaná. Cílem je dále nabídku rozšiřovat a zkvalitňovat. Prospěšné je i pořádání akcí typu hackathon, kde dochází k vysoké interakci mezi poskytovatelem dat a koncovými uživateli, na základě jejichž připomínek může být datový katalog dále rozvíjen.

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)	
4,3	Kvalifikovaní správci aplikací a ICT infrastruktury v oblasti, kterou mají ve své pracovní náplni.
4,3	Projektová kancelář OMI řídí IT projektové portfolio MMB, včetně projektů kybernetické bezpečnosti (KB).
4,1	Oblast informační bezpečnosti je řízena koordinátorem kybernetické bezpečnosti SMB.
4,0	Existence webové platformy města Brna.
3,9	Jistota prostředků na kalendářní rok v rámci schváleného rozpočtu.
3,9	Vysoká znalost technologických trendů a jejich zavádění.
3,5	Dosažené zkušenosti s implementací informačních systémů.
3,1	Zvyšující se bezpečnostní povědomí mezi pracovníky OMI a rovněž pracovníky MMB.
2,5	TSB je pověřeno koncernovým pokynem ke koordinaci ICT a KB v rámci koncernu (obchodních společností města).
Opportunities (vnější příležitosti)	
3,9	Maximalizovat využití čerpání prostředků z fondů EU.
3,4	Využití potenciálu odborníků v rámci města ve formě poradenského orgánu.
3,1	V Brně na trhu práce existují vzdělaní a kompetentní pracovníci v oblasti ICT.
2,8	Využití popisu procesů MMB (ORGO).
2,6	Zapojení vysokých škol do rozvoje informatiky města Brna včetně aktivní spolupráce města při výuce studentů.
2,4	Převedení vybraných služeb informatiky do samostatného ekonomického subjektu ovládaného městem Brnem za koordinace OMI.
Weaknesses (vnitřní slabé stránky)	
4,7	Odměňovací systém neumožňuje získávat nové a udržet stávající pracovníky IT.
4,4	Nedostatek vnitřních odborných kapacit vzhledem k rostoucímu významu a rozvoji informatiky vede ke zvýšenému nákupu externích služeb.
4,4	Ne všichni klíčoví uživatelé (garanti) mají dostatečné znalosti, aby definovali požadavky na informatiku (formulace toho, co chtějí). OMI nemůže suplovat metodické role uživatelů.
4,1	Nedostatečná koordinace ICT v rámci SMB.
3,9	Neochota úředníků k využití ICT potenciálu a změn.
3,9	Nedostatečné povědomí klíčových uživatelů o plánovaní kapacit zdrojů OMI na pokrytí požadavků.
3,6	Klíčové uživatele je obtížné motivovat pro spolupráci v projektových týmech týkajících se informatiky z důvodu střetu liniových a projektových struktur.
2,9	Nedostatečné personální zajištění obsahu a obsluhy webové platformy.
Threats (vnější hrozby)	
4,4	Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.
4,1	Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT.
4,1	Masivní vývoj kybernetických útoků a jejich forem.
3,9	Hrozby spojené s užíváním zařízení umístěných mimo perimetr.
3,9	Z výběrových řízení podle ZZVZ mohou vzejít neadekvátní dodavatelé nebo mohou výběrová řízení trvat nepredikovatelnou dobu.
3,7	Uživatelé pracující vzdáleně (mimo kancelář) se obracejí s lokálními ICT problémy na servisní podporu OMI mimo jeho gesci.
3,6	Překotný vývoj legislativních požadavků a jejich dopady v oblasti ICT a kybernetické bezpečnosti.
3,5	Se změnou politické reprezentace může dojít k zásadním změnám ve směrování a financování ICT.
3,4	Vzrůstající komplexita a regulace požadovaných technických opatření v ICT.
3,2	Dlouhá doba od vytvoření záměru do jeho realizace způsobená interními předpisy nebo platnou legislativou.

3,1	Přidělení finančních prostředků z rozpočtu je vždy jen na rok (rozpočtování je jen roční), v IT není zavedeno víceleté financování.
2,1	Narůstající význam IoT a Scada prvků zvyšující míru rizik v rámci SMB.

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)	
4,5	Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ).
4,4	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 kancelářský software.
3,9	Architektura pro integrace aplikací - integrační platforma (s využitím principů ESB a ETL).
3,8	Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy.
3,7	Je zřízena samostatná role bezpečnostního architekta. Bezpečnostní architektura je provázána na EA MMB.
3,7	Kvalitní komunikační infrastruktura připojení ÚMČ.
3,6	Jsou k dispozici opakovatelně použitelné architektonické stavební bloky pro využití aplikacemi SMB (např. NIA Proxy, ISZR Proxy)
3,1	Je k dispozici prostředí (framework) pro tvorbu jednoduché podpory procesů a workflow v nich (MOSS - MS Office SharePoint Services) s komunitou uživatelů.
3,1	Kvalitní prostory a technologické zázemí pro umístění uzlových ICT prvků (datové centrum).
3,0	V rámci SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) se zajištěnou ochranou proti jejich ztrátě.
2,8	Rozšíření služeb provozovaných z městského cloudu pro všechny městské subjekty SMB.
Opportunities (vnější příležitosti)	
4,5	Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.
4,4	Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).
4,2	Vytvoření a správa katalogu služeb ICT.
4,1	Popsání definice vazeb mezi projekty a sesouladění postupů – road-mapa na období několika let s pravidelnou aktualizací.
3,9	Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy).
3,7	Vydání IT směrnic závazných pro SMB.
3,6	Větší využití ETL Clover pro datovou integraci systémů.
3,6	Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu.
3,4	Propojení konfiguračních databází udržovaných MMB a samostatně dodavateli/správci částí infrastruktury.
3,3	Vytvořit prostředí pro drobné aplikace odborných útvarů SMB.
3,2	Metodická pomoc kompetenčního centra uživatelům z ÚMČ a organizací města.
3,2	Zvyšující se zájem stakeholderů o přístup k informacím z EA modelu.
3,1	Vytvoření prioritizace cca 350 aplikací a odstupňovaný přístup k nim podle jejich priorit.
3,1	Využití Národního architektonického plánu s návrhovými vzory vybraných oblastí.
3,0	Vytvoření centrálního přístupového bodu pro řízený přístup uživatelů do IS města a k aplikacím z různých platforem.
3,0	Využití externích kapacit výzkumu a vývoje pro oponenturu rozvojových koncepčních plánů a projektů (CERIT, NUKIB, Útvar hlavního architekta eGov, DIA …).

Weaknesses (vnitřní slabé stránky)	
4,7	Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).
4,2	Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti.
4,1	Neexistuje provozní aplikační a datový monitoring a konfigurační management na aplikační vrstvě.
4,1	Používání zastaralých aplikací neintegrovatelných či vyžadujících výjimky z koncepce pro integraci systémů.
3,9	Chybí standardizovaný Projektový záměr včetně pohledu EA (principy EA, analýzy přínosů a nákladů apod.).
3,9	Řada aplikací nemá dokumentaci.
3,7	Závislost rozvoje ICT architektury na přidělených prostředcích (rozpočtu).
3,6	Model EA zahrnuje jen MMB a absentují organizace SMB.
3,5	Nedostatečná aplikace principů procesního řízení.
3,5	Plánování a využití kapacit všech zdrojů v souladu s požadavky vykonávaných procesů.
3,4	Chybí vazba na business vrstvu zpracovávanou ORGO v BPMN diagramech.
3,4	Ne všechna data jsou ukládána do datových úložišť ve strukturované podobě, která umožní řízení přístupu dle oprávnění.
3,4	Platformová technologická roztříštěnost (např. různé db stroje).
3,3	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).
3,1	Nedobudována geograficky oddělená záložní infrastruktura.
3,1	Městské firmy si spravují vlastní podružná menší datová centra i aplikace bez vazby na EA.
2,7	IDM nemá zadefinované role z business vrstvy (není propojení až do procesní business vrstvy a její rozpracování na role).
Threats (vnější hrozby)	
4,1	Legislativní změny vyžadující podrobnější popis systémů (procesy, architektura, bezpečnost, ...).
4,1	Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24.
4,0	Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.
3,6	EA model obsahuje koncentrované informace a při neoprávněném přístupu k nim jde o bezpečnostní riziko.
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 …).
3,5	Centralizace administrace technických map (do správy kraje).
3,5	Nedostatečnost kapacity komunikační infrastruktury pro nové služby nabízené z internetu (např. video streaming, práce s 3D modely).
3,4	Konfliktní požadavky změn legislativy s dopadem do informačních systémů.
3,4	Licenční a technologická závislost na dodavateli (vendor lock-in).
3,4	Nedostatečná pozornost ze strany tvůrců prvků celostátního eGovernment, věnovaná specifickým potřebám statutárních měst.
3,2	Vynucená koordinace s podřízenými organizacemi z hlediska regulovaných služeb poskytovaných ve sdílené infrastruktuře ve formě podpůrných aktiv.
3,1	Organizační změny posilující přístup k aplikacím z vnějšího prostředí vyvolají problémy s licencemi a technologiemi.

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)	
4,7	Člen RMB pro oblast informatiky.
4,5	Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.
4,3	Poskytování vybraných veřejných služeb přes internet.
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).
3,6	Sjednocené a vybudované prostředí pro výkon veřejné správy.
3,5	Poskytování služeb založených společností a zřízených organizací městem přes internet.
3,4	Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb.
3,3	Zpřístupňování dat interním i externím uživatelům.
2,4	Jsou vytvořeny specializované subjekty města k poskytování specifických ICT služeb.
2,1	Vybudovány pilotní lokality s poskytnutou konektivitou pro bezplatný přístup do internetu.
Opportunities (vnější příležitosti)	
4,5	Koordinace ICT projektů městských subjektů.
4,5	Sjednocení komunikace nabízených služeb SMB občanům přes centrální aplikaci.
4,4	Naplnění nové webové platformy města.
4,2	Definice zákazníka ICT služeb a jeho potřeb.
3,9	Využívání standardizovaných IT produktů poskytovaných na celostátní úrovni.
3,7	Využití možností spolufinancování nových služeb z externích zdrojů.
2,9	Spolupráce s jinými městy v ČR a EU.
2,7	Zintenzivnění spolupráce se středními a vysokými školami (využití jejich potenciálu).
2,7	Využití aktivit v rámci externích subjektů ke standardizaci požadavků na výstupy z IS OVM.
Weaknesses (vnitřní slabé stránky)	
4,7	Neexistence ICT technologického standardu města.
4,7	Nedostatečná koordinace ICT projektů v rámci SMB.
4,3	Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu.
4,1	Není definován katalog elektronicky poskytovaných služeb.
4,1	Nízké povědomí o důležitosti výdajů do IT.
3,9	Pro občana nejsou v dostatečné míře přístupné všechny agendy přes internet. Neexistuje portál občana (prezentační portál) umožňující sledování procesu.
3,6	Omezený přístup k demografickým údajům na MČ.
3,5	Nemožnost řešit problémy v informatice v době, kdy vznikají (legislativní a procesní omezení).
3,5	Nízká míra využití potenciálu zavedených technologií.
Threats (vnější hrozby)	
4,7	Nárůst požadavků na informatiku při zachování stávajícího objemu finančních a lidských zdrojů.
4,2	Vznikají požadavky na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.
4,1	Vzrůstající nároky na dostupnost a důvěrnost poskytovaných služeb.
3,8	Obtížnost standardizace při potřebě specifických ICT řešení na ÚMČ.
3,7	Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.
3,6	Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.

2.2.4. SWOT Spokojenost uživatelů

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

Strengths (vnitřní silné stránky)	
4,3	Zavedená podpora uživatelů pomocí service-desku.
4,1	Neomezenost počtu interních uživatelů v klíčových aplikacích z pohledu přístupu na informační systémy.
3,9	Průběžná obnova techniky (koncových zařízení).
3,4	Pravidelné školení na způsob práce s aplikacemi.
3,4	Dostupnost aktualizovaných manuálů na intranetu.
Opportunities (vnější příležitosti)	
4,3	Vytvoření komunikačních aplikací pro občana - internetová přepážka (portál občana Brna), mobilní aplikace.
3,2	Poskytnutí dočasného přístupu k wi-fi návštěvníkům a zaměstnancům MMB.
3,1	Poskytnutí prostředků uživatelům pro přístup k informacím i z domova.
3,0	Podpora uživatelů prostřednictvím chatbot a voicebot.
2,9	Využití drobných specializovaných aplikací používaných v jiných městech.
2,9	Zavést hodnocení kvality vyřešení požadavků zadaných v service-desku uživatelem.
2,5	Využití možností prvků "mikro ICT" (princip Internetu věcí) a spolupráce s mobilním HW pro zpřístupnění služeb ICT občanům.
Weaknesses (vnitřní slabé stránky)	
4,7	Infrastruktura není připravena na masivní přístup interních uživatelů z vnějšího prostředí (práce z domova).
4,3	Nedůvěra uživatelů k používání service-desku.
4,2	Uživatelé nemají povědomí o reálných možnostech řešení jejich požadavků (času, schopnosti řešit požadavek, finanční náročnosti). Nedostatečně objektivní požadavky uživatelů.
4,0	Klíčoví uživatelé z jednotlivých odborů MMB nemají uvolněnou kapacitu na poskytování součinnosti v IT při řešení požadavků týkajících se jejich odborné problematiky.
3,7	Dosud nezavedená elektronická podpora některých vnitřních schvalovacích procesů úřadu (např. cestovních příkazů).
3,5	Uživatelé s přístupem k elektronickým materiálům vyžadují rovněž jejich tištěnou podobu, která pro jejich činnost není nutná.
3,3	Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.
3,2	Neexistující bezdrátové připojení interních uživatelů do vnitřní sítě.
3,1	Nejednotný přístup uživatelů k realizaci svých požadavků (formulace, spolupráce na řešení).
3,1	Snížená uživatelská podpora v období mimo pracovní dobu.
Threats (vnější hrozby)	
4,2	Napadení výpočetní techniky uživatele s omezením dostupnosti dat na ní uložených (např. ransomware).
4,1	Výpadek metropolitní sítě a internetu znamená nefunkčnost významných agend SMB.
4,1	Závislost na správném fungování centrálních aplikací při poskytování služeb.
4,0	Vzrůstající komplexita a míra digitalizace poskytovaných služeb.
3,2	Mylný pohled na možnosti úřadu při řešení "životních situací" bez vnímání omezení (legislativa, zdroje..).
3,1	Dodavatelé nemají dostatečnou znalost postupů ve veřejné správě a jsou závislí na znalostech uživatelů.
3,1	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)		
4,7	Člen RMB pro oblast informatiky.	Přínosy
4,5	Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ).	Architektura
4,5	Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.	Přínosy
4,4	Validní informace o EA MMB jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.	Architektura
4,3	Kvalifikovaní správci aplikací a ICT infrastruktury v oblasti, kterou mají ve své pracovní náplni.	Organizace
4,3	Projektová kancelář OMI řídí IT projektové portfolio MMB, včetně projektů kybernetické bezpečnosti (KB).	Organizace
4,3	Poskytování vybraných veřejných služeb přes internet.	Přínosy
4,3	Zavedená podpora uživatelů pomocí service-desku.	Uživatelé
4,1	Oblast informační bezpečnosti je řízena koordinátorem kybernetické bezpečnosti SMB.	Organizace
4,1	Efektivní licencování pro základní části městského AIS a kancelářský software.	Architektura
4,1	Neomezenost počtu interních uživatelů v klíčových aplikacích z pohledu přístupu na informační systémy.	Uživatelé
4,0	Existence webové platformy města Brna.	Organizace
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	Architektura pro integrace aplikací - integrační platforma (s využitím principů ESB a ETL).	Architektura
3,9	Průběžná obnova techniky (koncových zařízení).	Uživatelé
3,9	Jistota prostředků na kalendářní rok v rámci schváleného rozpočtu.	Organizace
3,9	Vysoká znalost technologických trendů a jejich zavádění.	Organizace
3,8	Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy.	Architektura
3,7	Je zřízena samostatná role bezpečnostního architekta. Bezpečnostní architektura je provázána na EA MMB.	Architektura
3,7	Kvalitní komunikační infrastruktura připojení ÚMČ.	Architektura
3,6	Jsou k dispozici opakovatelně použitelné architektonické stavební bloky pro využití aplikacemi SMB (např. NIA Proxy, ISZR Proxy)	Architektura
3,6	Sjednocené a vybudované prostředí pro výkon veřejné správy.	Přínosy
3,5	Dosažené zkušenosti s implementací informačních systémů.	Organizace
3,5	Poskytování služeb založených společností a zřízených organizací městem přes internet.	Přínosy
3,4	Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb.	Přínosy
3,4	Pravidelné školení na způsob práce s aplikacemi.	Uživatelé
3,4	Dostupnost aktualizovaných manuálů na intranetu.	Uživatelé
3,3	Zpřístupňování dat interním i externím uživatelům.	Přínosy
3,1	Zvyšující se bezpečnostní povědomí mezi pracovníky OMI a rovněž pracovníky MMB.	Organizace
3,1	Je k dispozici prostředí (framework) pro tvorbu jednoduché podpory procesů a workflow v nich (MOSS - MS Office SharePoint Services) s komunitou uživatelů.	Architektura
3,1	Kvalitní prostory a technologické zázemí pro umístění uzlových ICT prvků (datové centrum).	Architektura
3,0	V rámci SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) se zajištěnou ochranou proti jejich ztrátě.	Architektura
2,8	Rozšíření služeb provozovaných z městského cloudu pro všechny městské subjekty SMB.	Architektura

2,5	TSB je pověřeno koncernovým pokynem ke koordinaci ICT a KB v rámci koncernu (obchodních společností města).	Organizace
2,4	Jsou vytvořeny specializované subjekty města k poskytování specifických ICT služeb.	Přínosy
2,1	Vybudovány pilotní lokality s poskytnutou konektivitou pro bezplatný přístup do internetu.	Přínosy
Opportunities (vnější příležitosti)		
4,5	Koordinace ICT projektů městských subjektů.	Přínosy
4,5	Sjednocení komunikace nabízených služeb SMB občanům přes centrální aplikaci.	Přínosy
4,5	Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.	Architektura
4,4	Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).	Architektura
4,4	Naplnění nové webové platformy města.	Přínosy
4,3	Vytvoření komunikačních aplikací pro občana - internetová přepážka (portál občana Brna), mobilní aplikace.	Uživatelé
4,2	Vytvoření a správa katalogu služeb ICT.	Architektura
4,2	Definice zákazníka ICT služeb a jeho potřeb.	Přínosy
4,1	Popsání definice vazeb mezi projekty a sesouladění postupů – road-mapa na období několika let s pravidelnou aktualizací.	Architektura
3,9	Maximalizovat využití čerpání prostředků z fondů EU.	Organizace
3,9	Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy).	Architektura
3,9	Využívání standardizovaných IT produktů poskytovaných na celostátní úrovni.	Přínosy
3,7	Využití možností spolufinancování nových služeb z externích zdrojů.	Přínosy
3,7	Vydání IT směrnic závazných pro SMB.	Architektura
3,6	Větší využití ETL Clover pro datovou integraci systémů.	Architektura
3,6	Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu.	Architektura
3,4	Využití potenciálu odborníků v rámci města ve formě poradenského orgánu.	Organizace
3,4	Propojení konfiguračních databází udržovaných MMB a samostatně dodavateli/správci částí infrastruktury.	Architektura
3,3	Vytvořit prostředí pro drobné aplikace odborných útvarů SMB.	Architektura
3,2	Metodická pomoc kompetenčního centra uživatelům z ÚMČ a organizací města.	Architektura
3,2	Zvyšující se zájem stakeholderů o přístup k informacím z EA modelu.	Architektura
3,2	Poskytnutí dočasného přístupu k wi-fi návštěvníkům a zaměstnancům MMB.	Uživatelé
3,1	V Brně na trhu práce existují vzdělaní a kompetentní pracovníci v oblasti ICT.	Organizace
3,1	Vytvoření prioritizace cca 350 aplikací a odstupňovaný přístup k nim podle jejich priorit.	Architektura
3,1	Poskytnutí prostředků uživatelům pro přístup k informacím i z domova.	Uživatelé
3,1	Využití Národního architektonického plánu s návrhovými vzory vybraných oblastí.	Architektura
3,0	Vytvoření centrálního přístupového bodu pro řízený přístup uživatelů do IS města a k aplikacím z různých platforem.	Architektura
3,0	Využití externích kapacit výzkumu a vývoje pro oponenturu rozvojových koncepčních plánů a projektů (CERIT, NUKIB, Útvar hlavního architekta eGov, DIA …).	Architektura
3,0	Podpora uživatelů prostřednictvím chatbot a voicebot.	Uživatelé
2,9	Využití drobných specializovaných aplikací používaných v jiných městech.	Uživatelé
2,9	Spolupráce s jinými městy v ČR a EU.	Přínosy
2,9	Zavést hodnocení kvality vyřešení požadavků zadaných v service-desku uživatelem.	Uživatelé

2,8	Využití popisu procesů MMB (ORGO).	Organizace
2,7	Zintenzivnění spolupráce se středními a vysokými školami (využití jejich potenciálu).	Přínosy
2,7	Využití aktivit v rámci externích subjektů ke standardizaci požadavků na výstupy z IS OVM.	Přínosy
2,6	Zapojení vysokých škol do rozvoje informatiky města Brna včetně aktivní spolupráce města při výuce studentů.	Organizace
2,5	Využití možností prvků "mikro ICT" (princip Internetu věcí) a spolupráce s mobilním HW pro zpřístupnění služeb ICT občanům.	Uživatelé
2,4	Převedení vybraných služeb informatiky do samostatného ekonomického subjektu ovládaného městem Brnem za koordinace OMI.	Organizace
Weaknesses (vnitřní slabé stránky)		
4,7	Odměňovací systém neumožňuje získávat nové a udržet stávající pracovníky IT.	Organizace
4,7	Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).	Architektura
4,7	Neexistence ICT technologického standardu města.	Přínosy
4,7	Nedostatečná koordinace ICT projektů v rámci SMB.	Přínosy
4,7	Infrastruktura není připravena na masivní přístup interních uživatelů z vnějšího prostředí (práce z domova).	Uživatelé
4,4	Nedostatek vnitřních odborných kapacit vzhledem k rostoucímu významu a rozvoji informatiky vede ke zvýšenému nákupu externích služeb.	Organizace
4,4	Ne všichni klíčoví uživatelé (garanti) mají dostatečné znalosti, aby definovali požadavky na informatiku (formulace toho, co chtějí). OMI nemůže suplovat metodické role uživatelů.	Organizace
4,3	Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu.	Přínosy
4,3	Nedůvěra uživatelů k používání service-desku.	Uživatelé
4,2	Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti.	Architektura
4,2	Uživatelé nemají povědomí o reálných možnostech řešení jejich požadavků (času, schopnosti řešit požadavek, finanční náročnosti). Nedostatečně objektivní požadavky uživatelů.	Uživatelé
4,1	Není definován katalog elektronicky poskytovaných služeb.	Přínosy
4,1	Nedostatečná koordinace ICT v rámci SMB.	Organizace
4,1	Neexistuje provozní aplikační a datový monitoring a konfigurační management na aplikační vrstvě.	Architektura
4,1	Používání zastaralých aplikací neintegrovatelných či vyžadujících výjimky z koncepce pro integraci systémů.	Architektura
4,1	Nízké povědomí o důležitosti výdajů do IT.	Přínosy
4,0	Klíčoví uživatelé z jednotlivých odborů MMB nemají uvolněnou kapacitu na poskytování součinnosti v IT při řešení požadavků týkajících se jejich odborné problematiky.	Uživatelé
3,9	Pro občana nejsou v dostatečné míře přístupné všechny agendy přes internet. Neexistuje portál občana (prezentační portál) umožňující sledování procesu.	Přínosy
3,9	Neochota úředníků k využití ICT potenciálu a změn.	Organizace
3,9	Nedostatečné povědomí klíčových uživatelů o plánovaní kapacit zdrojů OMI na pokrytí požadavků.	Organizace
3,9	Chybí standardizovaný Projektový záměr včetně pohledu EA (principy EA, analýzy přínosů a nákladů apod.).	Architektura
3,9	Řada aplikací nemá dokumentaci.	Architektura
3,7	Dosud nezavedená elektronická podpora některých vnitřních schvalovacích procesů úřadu (např. cestovních příkazů).	Uživatelé
3,7	Závislost rozvoje ICT architektury na přidělených prostředcích (rozpočtu).	Architektura

3,6	Klíčové uživatele je obtížné motivovat pro spolupráci v projektových týmech týkajících se informatiky z důvodu střetu liniových a projektových struktur.	Organizace
3,6	Omezený přístup k demografickým údajům na MČ.	Přínosy
3,6	Model EA zahrnuje jen MMB a absentují organizace SMB.	Architektura
3,5	Nemožnost řešit problémy v informatice v době, kdy vznikají (legislativní a procesní omezení).	Přínosy
3,5	Uživatelé s přístupem k elektronickým materiálům vyžadují rovněž jejich tištěnou podobu, která pro jejich činnost není nutná.	Uživatelé
3,5	Nedostatečná aplikace principů procesního řízení.	Architektura
3,5	Plánování a využití kapacit všech zdrojů v souladu s požadavky vykonávaných procesů.	Architektura
3,5	Nízká míra využití potenciálu zavedených technologií.	Přínosy
3,4	Chybí vazba na business vrstvu zpracovávanou ORGO v BPMN diagramech.	Architektura
3,4	Ne všechna data jsou ukládána do datových úložišť ve strukturované podobě, která umožní řízení přístupu dle oprávnění.	Architektura
3,4	Platformová technologická roztříštěnost (např. různé db stroje).	Architektura
3,3	Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.	Uživatelé
3,3	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
3,2	Neexistující bezdrátové připojení interních uživatelů do vnitřní sítě.	Uživatelé
3,1	Nedobudována geograficky oddělená záložní infrastruktura.	Architektura
3,1	Městské firmy si spravují vlastní podružná menší datová centra i aplikace bez vazby na EA.	Architektura
3,1	Nejednotný přístup uživatelů k realizaci svých požadavků (formulace, spolupráce na řešení).	Uživatelé
3,1	Snížená uživatelská podpora v období mimo pracovní dobu.	Uživatelé
2,9	Nedostatečné personální zajištění obsahu a obsluhy webové platformy.	Organizace
2,7	IDM nemá zadefinované role z business vrstvy (není propojení až do procesní business vrstvy a její rozpracování na role).	Architektura
Threats (vnější hrozby)		
4,7	Nárůst požadavků na informatiku při zachování stávajícího objemu finančních a lidských zdrojů.	Přínosy
4,4	Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.	Organizace
4,2	Vznikají požadavky na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení.	Přínosy
4,2	Napadení výpočetní techniky uživatele s omezením dostupnosti dat na ní uložených (např. ransomware).	Uživatelé
4,1	Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT.	Organizace
4,1	Výpadek metropolitní sítě a internetu znamená nefunkčnost významných agend SMB.	Uživatelé
4,1	Masivní vývoj kybernetických útoků a jejich forem.	Organizace
4,1	Legislativní změny vyžadující podrobnější popis systémů (procesy, architektura, bezpečnost, ...).	Architektura
4,1	Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24.	Architektura
4,1	Vzrůstající nároky na dostupnost a důvěrnost poskytovaných služeb.	Přínosy
4,1	Závislost na správném fungování centrálních aplikací při poskytování služeb.	Uživatelé
4,0	Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.	Architektura
4,0	Vzrůstající komplexita a míra digitalizace poskytovaných služeb.	Uživatelé

3,9	Hrozby spojené s užíváním zařízení umístěných mimo perimetr.	Organizace
3,9	Z výběrových řízení podle ZZVZ mohou vzejít neadekvátní dodavatelé nebo mohou výběrová řízení trvat nepredikovatelnou dobu.	Organizace
3,8	Obtížnost standardizace při potřebě specifických ICT řešení na ÚMČ.	Přínosy
3,7	Uživatelé pracující vzdáleně (mimo kancelář) se obracejí s lokálními ICT problémy na servisní podporu OMI mimo jeho gesci.	Organizace
3,7	Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.	Přínosy
3,6	Překotný vývoj legislativních požadavků a jejich dopady v oblasti ICT a kybernetické bezpečnosti.	Organizace
3,6	EA model obsahuje koncentrované informace a při neoprávněném přístupu k nim jde o bezpečnostní riziko.	Architektura
3,6	Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.	Přínosy
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
3,5	Se změnou politické reprezentace může dojít k zásadním změnám ve směrování a financování ICT.	Organizace
3,5	Centralizace administrace technických map (do správy kraje).	Architektura
3,5	Nedostatečnost kapacity komunikační infrastruktury pro nové služby nabízené z internetu (např. video streaming, práce s 3D modely).	Architektura
3,4	Konfliktní požadavky změn legislativy s dopadem do informačních systémů.	Architektura
3,4	Licenční a technologická závislost na dodavateli (vendor lock-in).	Architektura
3,4	Vzrůstající komplexita a regulace požadovaných technických opatření v ICT.	Organizace
3,4	Nedostatečná pozornost ze strany tvůrců prvků celostátního eGovernment, věnovaná specifickým potřebám statutárních měst.	Architektura
3,2	Mylný pohled na možnosti úřadu při řešení "životních situací" bez vnímání omezení (legislativa, zdroje..).	Uživatelé
3,2	Dlouhá doba od vytvoření záměru do jeho realizace způsobená interními předpisy nebo platnou legislativou.	Organizace
3,2	Vynucená koordinace s podřízenými organizacemi z hlediska regulovaných služeb poskytovaných ve sdílené infrastruktuře ve formě podpůrných aktiv.	Architektura
3,1	Organizační změny posilující přístup k aplikacím z vnějšího prostředí vyvolají problémy s licencemi a technologiemi.	Architektura
3,1	Přidělení finančních prostředků z rozpočtu je vždy jen na rok (rozpočtování je jen roční), v IT není zavedeno víceleté financování.	Organizace
3,1	Dodavatelé nemají dostatečnou znalost postupů ve veřejné správě a jsou závislí na znalostech uživatelů.	Uživatelé
3,1	Legislativní omezení ICT služeb pro externí subjekty (občan, právnické osoby ..).	Uživatelé
2,1	Narůstající význam IoT a Scada prvků zvyšující míru rizik v rámci SMB.	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
Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ).
Zavedená podpora uživatelů pomocí service-desku.
k vnější příležitosti
Definice zákazníka ICT služeb a jeho potřeb.
Vytvoření a správa katalogu služeb ICT.

[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
Definice zákazníka ICT služeb a jeho potřeb.

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

[SO4] Využití vnitřní silné stránky
Člen RMB pro oblast informatiky.
Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy.
k vnější příležitosti
Koordinace ICT projektů městských subjektů.
Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu.

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

[SO6] Využití vnitřní silné stránky
Poskytování vybraných veřejných služeb přes internet.
Poskytování služeb založených společností a zřízených organizací městem přes internet.
k vnější příležitosti
Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).
Naplnění nové webové platformy města.

[SO7] Využití vnitřní silné stránky
Člen RMB pro oblast informatiky.
k vnější příležitosti
Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).

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

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

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

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

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

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

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

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

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

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

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

[ST9] Využití vnitřní silné stránky
Člen RMB pro oblast informatiky.
k zamezení vnější hrozby
Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.
Legislativní změny vyžadující podrobnější popis systémů (procesy, architektura, bezpečnost, ...).
Odměňovací systém neumožňuje získávat nové a udržet stávající pracovníky IT.

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

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

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

[WO3] Překonání vnitřní slabosti
Pro občana nejsou v dostatečné míře přístupné všechny agendy přes internet. Neexistuje portál občana (prezentační portál) umožňující sledování procesu.
využitím vnější příležitosti
Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).
Vytvoření komunikačních aplikací pro občana - internetová přepážka (portál občana Brna), mobilní aplikace.
Sjednocení komunikace nabízených služeb SMB občanům přes centrální aplikaci.

[WO4] Překonání vnitřní slabosti

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

využitím vnější příležitosti

Vytvoření prioritizace cca 350 aplikací a odstupňovaný přístup k nim podle jejich priorit.

Koordinace ICT projektů městských subjektů.

Maximalizovat využití čerpání prostředků z fondů EU.

Popsání definice vazeb mezi projekty a sesouladění postupů – road-mapa na období několika let s pravidelnou aktualizací.

[WO5] Překonání vnitřní slabosti

Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu.

využitím vnější příležitosti

Vytvoření a správa katalogu služeb ICT.

Vydání IT směrnic závazných pro SMB.

[WO6] Překonání vnitřní slabosti

Nízká míra využití potenciálu zavedených technologií.

využitím vnější příležitosti

Definice zákazníka ICT služeb a jeho potřeb.

Využití aktivit v rámci externích subjektů ke standardizaci požadavků na výstupy z IS OVM.

[WO7] Překonání vnitřní slabosti

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

využitím vnější příležitosti

Využívání standardizovaných IT produktů poskytovaných na celostátní úrovni.

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

Využití možností spolufinancování nových služeb z externích zdrojů.

Využití potenciálu odborníků v rámci města ve formě poradenského orgánu.

Využití externích kapacit výzkumu a vývoje pro oponenturu rozvojových koncepčních plánů a projektů (CERIT, NUKIB, Útvar hlavního architekta eGov, DIA …).

Spolupráce s jinými městy v ČR a EU.

[WO8] Překonání vnitřní slabosti

Není definován katalog elektronicky poskytovaných služeb.

využitím vnější příležitosti

Vytvoření a správa katalogu služeb ICT.

[WO9] Překonání vnitřní slabosti

Nedostatečná koordinace ICT v rámci SMB.

Nedostatečná koordinace ICT projektů v rámci SMB.

využitím vnější příležitosti

Koordinace ICT projektů městských subjektů.

Propojení Informační strategie s EA tak, aby se mohly definovat segmenty rozvoje architektury (přechodové stavy).

[W10] Překonání vnitřní slabosti
Infrastruktura není připravena na masivní přístup interních uživatelů z vnějšího prostředí (práce z domova).
využitím vnější příležitosti
Definice zákazníka ICT služeb a jeho potřeb.
Vytvoření a správa katalogu služeb ICT.

[W11] Překonání vnitřní slabosti
Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti.
využitím vnější příležitosti
Koordinace ICT projektů městských subjektů.
Vydání IT směrnic závazných pro SMB.
Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.

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

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

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

[WT3] Preventivní obrana proti skloubení vnitřní slabosti
Motivační systém neumožňuje získávat nové a udržet stávající pracovníky IT.
Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).
s vnější hrozbou
Nárůst požadavků na informatiku při zachování stávajícího objemu finančních a lidských zdrojů.
Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT.

[WT4] Preventivní obrana proti skloubení vnitřní slabosti
Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).
s vnější hrozbou
Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.
Neexistence plánu a pevných milníků pro nasazení nových centrálních IS s dopadem na činnosti OVM, což znamená negativní dopady na plánování zdrojů OVM, zejména při rozsahu správního obvodu (např. aplikace CRR, CRV, digitalizace dokumentů pro centrální agendy, rušení místní příslušnosti ...).

[WT5] Preventivní obrana proti skloubení vnitřní slabosti
Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).
s vnější hrozbou
Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.

[WT6] Preventivní obrana proti skloubení vnitřní slabosti
Infrastruktura není připravena na masivní přístup interních uživatelů z vnějšího prostředí (práce z domova).
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
Infrastruktura není připravena na masivní přístup interních uživatelů z vnějšího prostředí (práce z domova).
Není definován katalog elektronicky poskytovaných služeb.
s vnější hrozbou
Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24.

2.4. Strategické záměry vycházející z variantních strategických možností

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

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

	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
5,0	S-O	Validní informace o EA MMB jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu. Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy. Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB. Člen RMB pro oblast informatiky.	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. Zavést roli odpovědnou za koncepci rozvoje architektury systémů v rámci SMB (solution architekt). Solution architekt bude pracovat v týmu s ostatními architekty SMB. Koncepci rozvoje mu bude schvalovat člen RMB pro oblast informatiky. *Předpokládaná hierarchie:* *- Rada města (+Komise informatiky jako poradní orgán)* *- Člen RMB pro oblast informatiky* *- Rada pro řízení ICT SMB* *- Solution architekt SMB a Rada pro řízení ICT architektury SMB* *- Zástupci subjektů SMB odpovědných za ICT architekturu*

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
4,6	W-O	Neexistence bezpečnostní architektury zohledňující potřeby města v oblasti kybernetické bezpečnosti.	Koordinace ICT projektů městských subjektů. Vydání IT směrnic závazných pro SMB. Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.	Vytvořit a udržovat technologický standard SMB (nikoliv jen MMB). Dlouhodobě plánovat architektonický rozvoj na všech úrovních EA. Řídit bezpečnostní architekturu napříč SMB a dohlížet na implementaci bezpečnostních standardů v SMB (řídí kancelář kybernetické bezpečnosti). *Předpokládaná hierarchie:* *- Rada města (+ Komise informatiky jako poradní orgán)* *- Člen RMB pro oblast informatiky* *- Rada pro řízení ICT SMB* *- Výbor kybernetické bezpečnosti SMB (v kooperaci s Radou pro řízení ICT architektury SMB)* *- Koordinátor kybernetické bezpečnosti SMB* *- Zástupci subjektů SMB odpovědní za kybernetickou bezpečnost*
	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
4,3	W-O	Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).	Popsání definice vazeb mezi projekty a sesouladění postupů – road-mapa na období několika let s pravidelnou aktualizací. Koordinace ICT projektů městských subjektů. Vytvoření prioritizace cca 350 aplikací a odstupňovaný přístup k nim podle jejich priorit. Maximalizovat využití čerpání prostředků z fondů EU.	Koordinace portfolia ICT projektů v rámci SMB. Plánovat zdroje dlouhodobě s vazbou na rozvojové projekty realizující požadavky v ICT města. *Předpokládaná hierarchie:* *- Rada města (+Komise informatiky jako poradní orgán)* *- Člen RMB pro oblast informatiky* *- Rada pro řízení ICT SMB* *- Projektová kancelář pro řízení portfolia ICT projektů SMB* *- Manažeři projektů SMB*

	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
4,3	S-T	Řízený rozvoj aplikací – stanoveny prioritní oblasti rozvoje aplikačních platforem, definovány základní aplikační okruhy. Validní informace o EA MMB jsou shromážděny v jednom centrálně udržovaném modelu vč. postupu pro správu modelu.	Obtížná realizace dlouhodobých projektů s mnoha vzájemnými vazbami s přesahem volebního období.	Koordinace portfolia ICT projektů v rámci SMB. Plánovat zdroje dlouhodobě s vazbou na rozvojové projekty realizující požadavky v ICT města.
	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
4,2	W-O	Neexistence ICT technologického standardu města.	Definování technologického standardu SMB zabraňujícího technologické roztříštěnosti.	Vytvořit technologický standard SMB (tj. vč. městských společností a organizací).
	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
4,1	W-O	Pro občana nejsou v dostatečné míře přístupné všechny agendy přes internet. Neexistuje portál občana (prezentační portál) umožňující sledování procesu. Není definován katalog elektronicky poskytovaných služeb.	Sjednocení komunikace nabízených služeb SMB občanům přes centrální aplikaci. Vytvoření jednotné mobilní aplikace pro poskytování služeb SMB (včetně jeho akciových společností a vybraných příspěvkových organizací).	Umožnit přístup občanům k agendám přes velkou městskou aplikaci (mobilní aplikace) a portál občana (web).
	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
4,1	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).	Zajistit bezpečnost uživatelů pracujících vně chráněného městského perimetru.
	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
4,1	W-T	Infrastruktura není připravena na masivní přístup interních uživatelů z vnějšího prostředí (práce z domova). Neexistuje provozní aplikační a datový monitoring a konfigurační management na aplikační vrstvě. Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.	Masivní vývoj kybernetických útoků a jejich forem. Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům. Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24.	Zvýšit úrovně informační bezpečnosti na všech vrstvách (včetně zajištění dohledu a reakce na incidenty).

	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
4,1	W-O	Nedostatečná komunikace ostatních odborů MMB s OMI při definování řešení vyžadujících aktivní IT podporu. Nízká míra využití potenciálu zavedených technologií. Není stanovena minimální úroveň IT znalostí pro práci s informačními technologiemi.	Vytvoření a správa katalogu služeb ICT. Vydání IT směrnic závazných pro SMB.	Maximálně propojit IT pracovníky s klíčovými pracovníky odborů do rozvoje a využívání IS.
	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
4,0	S-T	V rámci SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) se zajištěnou ochranou proti jejich ztrátě. Existence integrační platformy umožňující efektivní a řízený přístup k datům v AIS SMB.	Masivní vývoj kybernetických útoků a jejich forem. Důvěrné informace mohou být s ohledem na charakter organizace nedostatečně chráněny proti útokům.	Chránit bezpečnost dat v datových centrech.
	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
4,0	W-T	Motivační systém neumožňuje získávat nové a udržet stávající pracovníky IT. Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).	Odchody kvalifikovaných pracovníků vyškolených na MMB v problematice IT. Nárůst požadavků na informatiku při zachování stávajícího objemu finančních a lidských zdrojů. Stálý počet pracovníků OMI oproti nárůstu počtu agend, u kterých poskytují první úroveň podpory.	S nárůstem pracovní náplně vzrůstající s digitalizací všech činností města zvýšit finanční zdroje a analogicky počet pracovníků OMI. Vytvořit motivační systém pro pracovníky v IT. který bude dostatečně atraktivní pro stávající i nové pracovníky.
	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
3,9	S-O	Poskytování vybraných veřejných služeb přes internet. Zavedená podpora uživatelů pomocí service-desku.	Definice zákazníka ICT služeb a jeho potřeb. Vytvoření a správa katalogu služeb ICT. Poskytnutí prostředků uživatelům pro přístup k informacím i z domova.	Poskytovat profesionálně zadefinované ICT služby za nastavených SLA/OLA parametrů pro interní uživatele a externí uživatele.
	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,7	W-T	Uživatelé nemají povědomí o reálných možnostech řešení jejich požadavků (času, schopnosti řešit požadavek, finanční náročnosti). Nedostatečně objektivní požadavky uživatelů.	Požadavek na funkce městského ICT prostředí bez ohledu na současná legislativní a procesní omezení. Legislativa omezuje možnosti cílené komunikace s občanem např. v oblasti osobních údajů.	Maximálně propojit IT pracovníky s klíčovými pracovníky odborů do rozvoje a využívání IS.

	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
3,6	S-T	Člen RMB pro oblast informatiky. Dosažené zkušenosti s implementací informačních systémů.	Neexistence plánu a pevných milníků pro nasazení nových centrálních IS s dopadem na činnosti OVM, což znamená negativní dopady na plánování zdrojů OVM, zejména při rozsahu správního obvodu (např. aplikace CRR, CRV, digitalizace dokumentů pro centrální agendy, rušení místní příslušnosti ...). Závislost na správném fungování centrálních aplikací při poskytování služeb. Krátký čas na řešení problémů v IT, které vznikly změnou řešení na celostátní úrovni.	Aktivní zjišťování plánů rozvoje centrálních IS s cílem získat dostatečný čas na přípravu souvisejících změn.
	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,5	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.	Aktivní zjišťování plánů rozvoje centrálních IS s cílem získat dostatečný čas na přípravu souvisejících změn. Zavést pravidla pro rychlé schvalování projektů na základě shody s informační strategií a architekturou s jejich zdůvodněním formou projektového záměru.
	Prevence	proti skloubení vnitřní slabosti	s vnější hrozbou	dosažením záměru
3,5	W-T	Neexistence ICT technologického standardu města.	Obtížnost standardizace při potřebě specifických ICT řešení na ÚMČ.	Technologický standard SMB musí umožňovat realizaci specifických ICT řešení za definovaných podmínek.
	Využití	vnitřní silné stránky	k zamezení vnější hrozby	dosažením záměru
3,4	S-T	Kvalitní prostory a technologické zázemí pro umístění uzlových ICT prvků (datové centrum). Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb. Kvalitní komunikační infrastruktura připojení ÚMČ.	Výpadek metropolitní sítě a internetu znamená nefunkčnost významných agend SMB. Nárůst požadavků na dodržení garantované úrovně bezpečnosti a provozu služeb v režimu 7x24 (je dnes zajištěno na úrovni infrastruktury).	Zvýšit odolnost poskytovaných služeb proti jejich výpadku.

	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
3,3	S-O	Zavedená servis-desková podpora uživatelů.	Zavést hodnocení kvality vyřešení požadavků zadaných v Help Desku uživatelem. Podpora uživatelů prostřednictvím chatbot a voicebot.	Zvýšení orientace na podporu uživatelů s posílením service-deskových funkcí.
	Využití	vnitřní silné stránky	k realizaci vnější příležitosti	dosažením záměru
3,2	S-O	SMB má statut a může v rámci něj prosadit cíle v IT jak na MMB, tak i na ÚMČ (čl. 39 a 40). Neomezenost počtu interních uživatelů v klíčových aplikacích z pohledu přístupu na informační systémy. Společné využívání centrálně instalovaných aplikací (MMB, ÚMČ). Poskytování služeb založených společností a zřízených organizací městem přes internet. Město vlastní dostatečně výkonnou metropolitní infrastrukturu pro rozšiřování služeb. V rámci SMB je prováděno technologicky moderní ukládání dat v datových centrech (TSB) se zajištěnou ochranou proti jejich ztrátě. Kvalitní prostory a technologické zázemí pro umístění uzlových ICT prvků (datové centrum).	Rozšíření společného využívání centrálně instalovaných aplikací do organizací města s využitím městského cloudu. Vydání IT směrnic závazných pro SMB.	Rozšířit využívání aplikací v městském cloudu podle závazně dohodnutých pravidel.
	Překonání	vnitřní slabosti	využitím vnější příležitosti	dosažením záměru
3,0	W-O	Požadavky kladené na útvar informatiky převyšují možnosti zdrojů (několikanásobné přetížení zdrojů).	Využití externích kapacit výzkumu a vývoje pro oponenturu rozvojových koncepčních plánu a projektů (CERIT, NUKIB, Útvar hlavního architekta eGov…). Zintenzivnění spolupráce se středními a vysokými školami (využití jejich potenciálu). Využití aktivit v rámci externích subjektů ke standardizaci požadavků na výstupy z IS OVM (orgánů veřejné moci).	Zintenzivnit spolupráci s externími zdroji.

3. Návrh cílového stavu

Cílový stav je popsán v systému 18 strategických cílů zařazených ve čtyřech perspektivách metody Balanced Scorecard, přičemž cíle slouží k dosažení vize a mise informatiky města Brna. Strategické cíle jsou vzájemně provázané a vytvářejí strategické řetězce, které ukazují na příčinu a následek v systému strategických cílů.

3.1. Vize & mise informatiky města Brna

3.1.1. Vize města[18]

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

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

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

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

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

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

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

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

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

souvislostí, které mezi jednotlivými datovými sadami panují.

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.

3.2. Strategické cíle

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

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

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

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

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

- Omezující funkce: BSC vede k omezení nadbytku údajů plynoucích z operativních činností (na základě definice služeb a ukazatelů) na ty, které mají strategický význam a identifikují důležité změny (v rámci perspektiv).
- Funkce zaměření: BSC koncentruje pozornost politického vedení příp. orgánů veřejné

správy na ujednané a významné perspektivy.

- Spojovací funkce: BSC je spojovacím článkem mezi strategií a přidělováním finančních prostředků.
- Integrační funkce: BSC zohledňuje rovnoměrně jak finanční, tak nefinanční charakteristiky. Tím BSC vyrovnává převahu čistě monetárních aspektů, jejichž převažující vliv lze často objevit i v nových modelech řízení státní a veřejné správy.
- Argumentační funkce: BSC zohledňuje různé úhly pohledu (perspektivy), které musí každá organizace obsahově naplnit (cíli a měřítky výkonnosti).

3.2.1. Cíle v perspektivě ICT potenciál a zdroje

číslo	strategický cíl	popis
1	Vytvořit mobilní aplikaci a webový portál služeb	Mobilní aplikace a webový portál služeb jsou naplněny službami: • úřední pro občany / úředníky • turisticko / informační • otevřená data • geoportál. Součástí řešení je zajištění kybernetické bezpečnosti.
2	Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty)	Důvěryhodné elektronické služby jsou provázány do aplikací města.
3	Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách	Provozování městského dohledového provozního a bezpečnostního centra SMB (SOC - Security Operation Center) integrujícího všechny bezpečnostní technologie.
4	Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť	Infrastrukturní prostředí je trvale dozorováno (provozní a bezpečnostní monitoring) a vybaveno geograficky oddělenými redundantními datovými centry s plnou datovou a infrastrukturní redundancí.
5	Posílit 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.

3.2.2. Cíle v perspektivě procesů

číslo	strategický cíl	popis
6	Využívat workflow služeb přes jednotné prezentační rozhraní	Aplikace jsou zpřístupněny na portálu pro poskytování elektronických služeb. Workflow u aplikací poskytujících služby úřadu přes portál je navrženo ve spolupráci s procesním modelováním BPMN diagramů na ORGO.
7	Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby	Standardy zajišťují bezpečnost (důvěrnost, integritu a dostupnost) a důvěryhodnost elektronicky poskytovatelných služeb.
8	Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb	Katalog ICT služeb umožňuje využívat infrastrukturní, platformové a bezpečnostní služby poskytované pro SMB centrálně jednotným způsobem.
9	Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy	Řízení EA (Enterprise Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy. Architektura podporuje vzdálený bezpečný přístup do systémů.
10	Koordinovat rozvoj ICT města řízením projektového portfolia	Projektové portfolio zahrnuje významné projekty z hlediska rozvoje ICT města a umožňuje jejich koordinované řízení v rámci SMB.

3.2.3. Cíle v perspektivě zákazníků

číslo	strategický cíl	popis
11	Poskytovat elektr. služby přes webový portál služeb a mobilní aplikaci	Zvolené životní situace a služby města jsou poskytovány elektronicky. Možnost sledování průběhu procesů občanem. Zrychlení průběhu procesů. Zvýšení kontextové informovanosti a transparentnosti (kroky proběhlé a příští).
12	Umožnit interním uživatelům práci z prostředí domova	Určeným/schváleným interním uživatelům ICT služeb SMB je umožněno využívat aplikace vzdáleným přístupem podle nastavených SLA/OLA parametrů.
13	Podporovat využívání služeb městského cloudu organizacemi SMB	Městské cloudové služby (zálohování, úložiště, bezpečnost) jsou poskytovány za výhodných ekonomických podmínek obtížně dosažitelných z pozice jednotlivých městských organizací.
14	Rozšířit využívání centrálních aplikací podle závazných standardů	Centrálně poskytované aplikace budou ve shodě s Informační koncepcí ČR a město bude mít zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...). Bude vytvořen a udržován technologický standard SMB.
15	Prohloubit spolupráci pracovníků SMB v oblasti ICT projektů a architektury	Řízení ICT projektů a EA (Enterprise Architecture) je prováděno ve spolupráci ICT pracovníků a dalších odborných pracovníků/garantů v rámci SMB.

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.
17	Vytvořit moderní, společné a bezpečné ICT města	Město disponuje moderní modulární a stále se rozvíjející ICT infrastrukturou, která je sdílena v rámci MMB, MČ, městských firem a organizací. Infrastruktura poskytuje maximálně efektivní elektronické služby a její bezpečnost je zajištěna na profesionální úrovni.
18	Centrálně řídit ICT města	Řízení ICT města je prováděno centralizovaně na projektové a architektonické úrovni orgánem zřízeným Radou města.

3.3. Provázání strategických cílů do systému

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

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

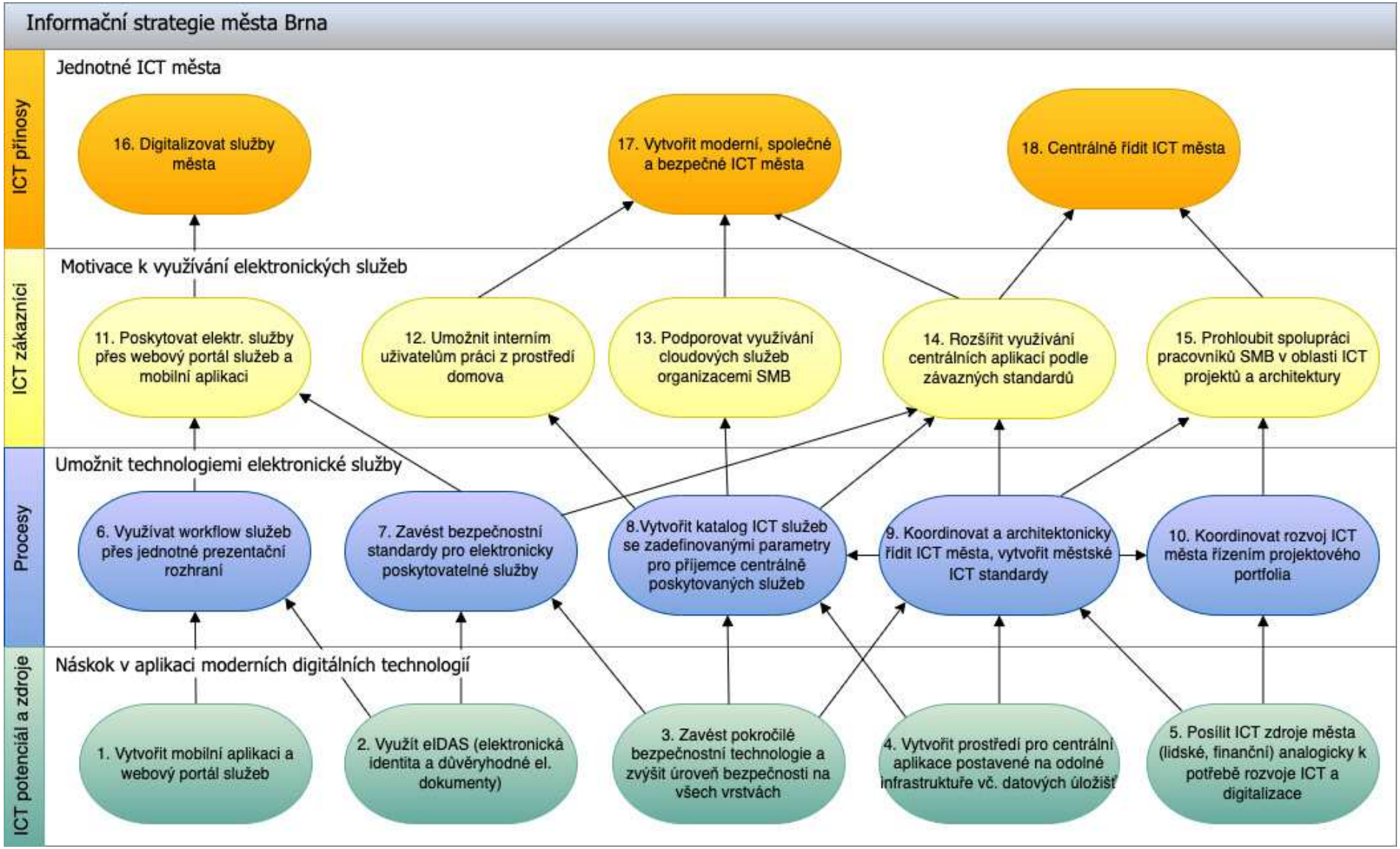
Ve strategické mapě (schéma Balanced Scorecard) jsou kauzální vazby znázorněny šipkami, kdy ve směru šipky je uvažován vztah příčina vyvolávající následek. Zaměření na strategicky významné vztahy, bez ambice na analýzu všech myslitelných vazeb mezi cíli, je jednou z hlavních předností použité metody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

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

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

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

3.3.1. Strategická mapa (schéma Balanced Scorecard)



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

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

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

Přínosy jsou v informační strategii očekávány v těchto oblastech:

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

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

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

- Řetězec digitalizace služeb;
- Řetězec tvorby ICT města;
- Řetězec řízení ICT města.

Řetězec digitalizace služeb

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

1. *Vytvořit mobilní aplikaci a webový portál služeb;*
2. *Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty);*
3. *Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách;*
6. *Využívat workflow služeb přes jednotné prezentační rozhraní;*
7. *Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby;*
11. *Poskytovat elektr. služby přes webový portál služeb a mobilní aplikaci;*
16. *Digitalizovat služby města.*

Jedná se o skupinu cílů směřující ke zvýšení transparentnosti a otevřenosti radnice a k digitalizaci služeb veřejné správy. Strategie vychází z toho, že dosažení těchto vrcholových přínosů je třeba postavit od základů vzniklých z vytvoření moderního portálu města. Pro to, 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 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 cíle směřující 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. Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty);

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

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

5. Posílit 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 se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb;

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

12. Umožnit interním uživatelům práci z prostředí domova;

13. Podporovat využívání cloudových služeb organizacemi SMB;

14. Rozšířit využívání centrálních aplikací podle závazných standardů;

17. Vytvořit moderní, společné a bezpečné 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 řízení ICT města

Strategický řetězec ***řízení ICT města*** vznikl jako odpověď na vzrůstající požadavky na digitalizaci veřejné správy. Tento řetězec nahrazuje strategický řetězec otevřenosti městských dat, jehož strategicky sledované cíle byly již dosaženy nebo převedeny do provozních cílů a proto není nutné cíle týkající se otevřenosti městských dat dále sledovat v rámci informační strategie. Strategický řetězec *řízení ICT města* kauzálně propojuje jedenáct cílů směřujících k centrálnímu řízení rozvoje ICT SMB:

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

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

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

5. Posílit 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 se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb;

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

10. Koordinovat rozvoj ICT města řízením projektového portfolia;

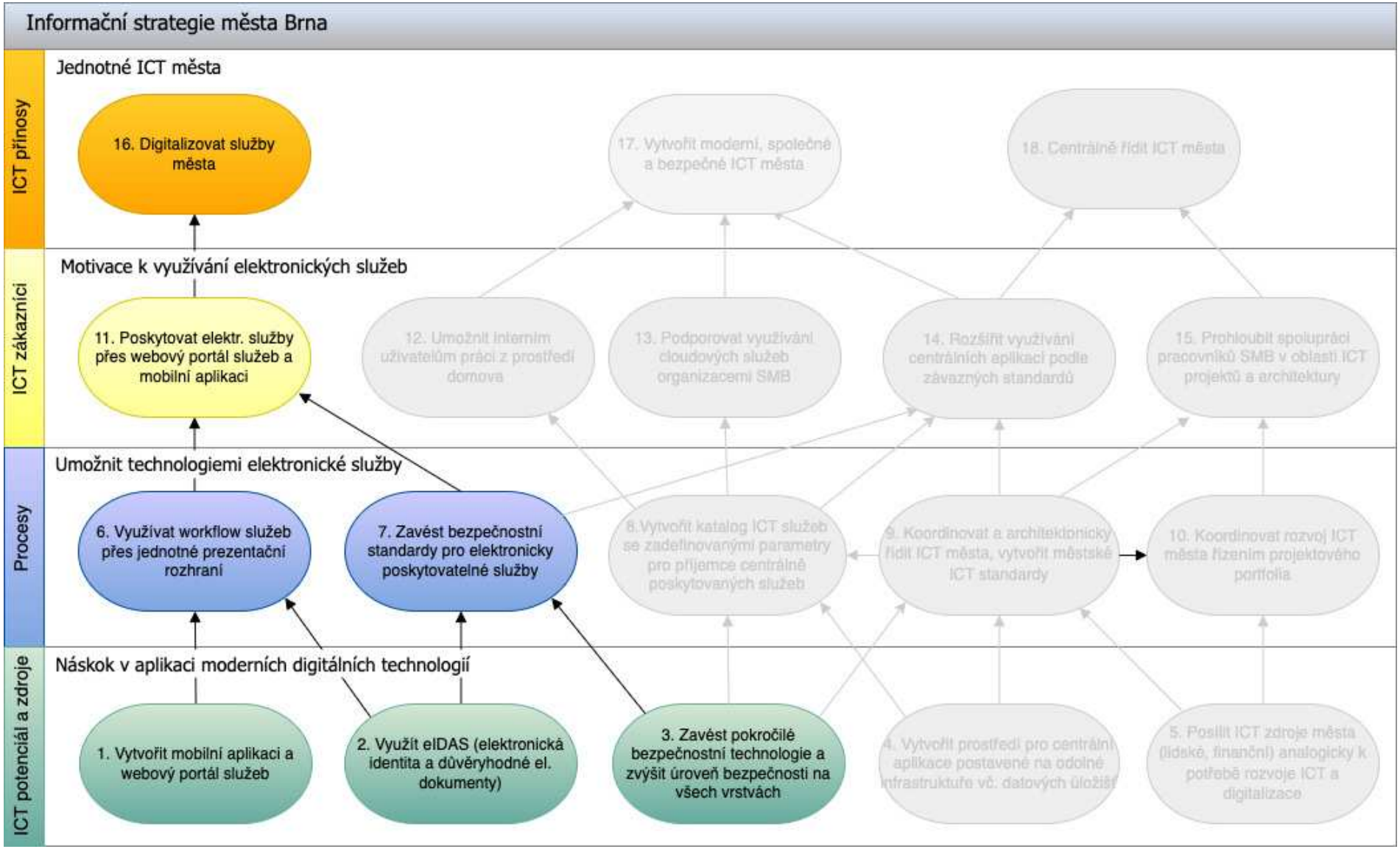
14. Rozšířit využívání centrálních aplikací podle závazných standardů;

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

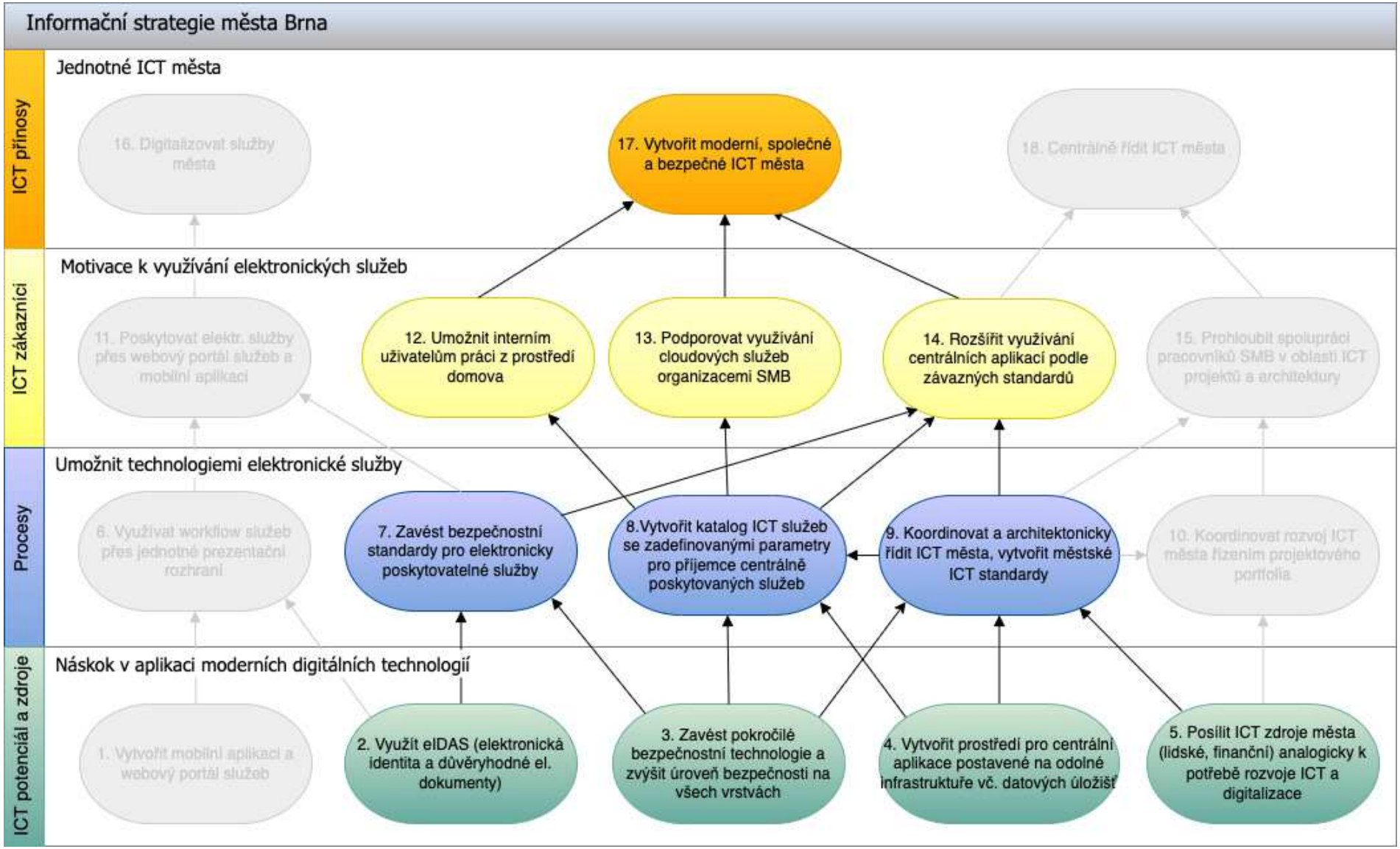
18. Centrálně řídit ICT města.

Centrální řízení ICT města je založeno na uplatnění pokročilých bezpečnostních technologií a na vytvoření 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. Pro realizaci této strategie je posílení ICT zdrojů podmínkou nutnou pro dosažení strategických cílů překračujících jinak možnosti současných zdrojů. 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.

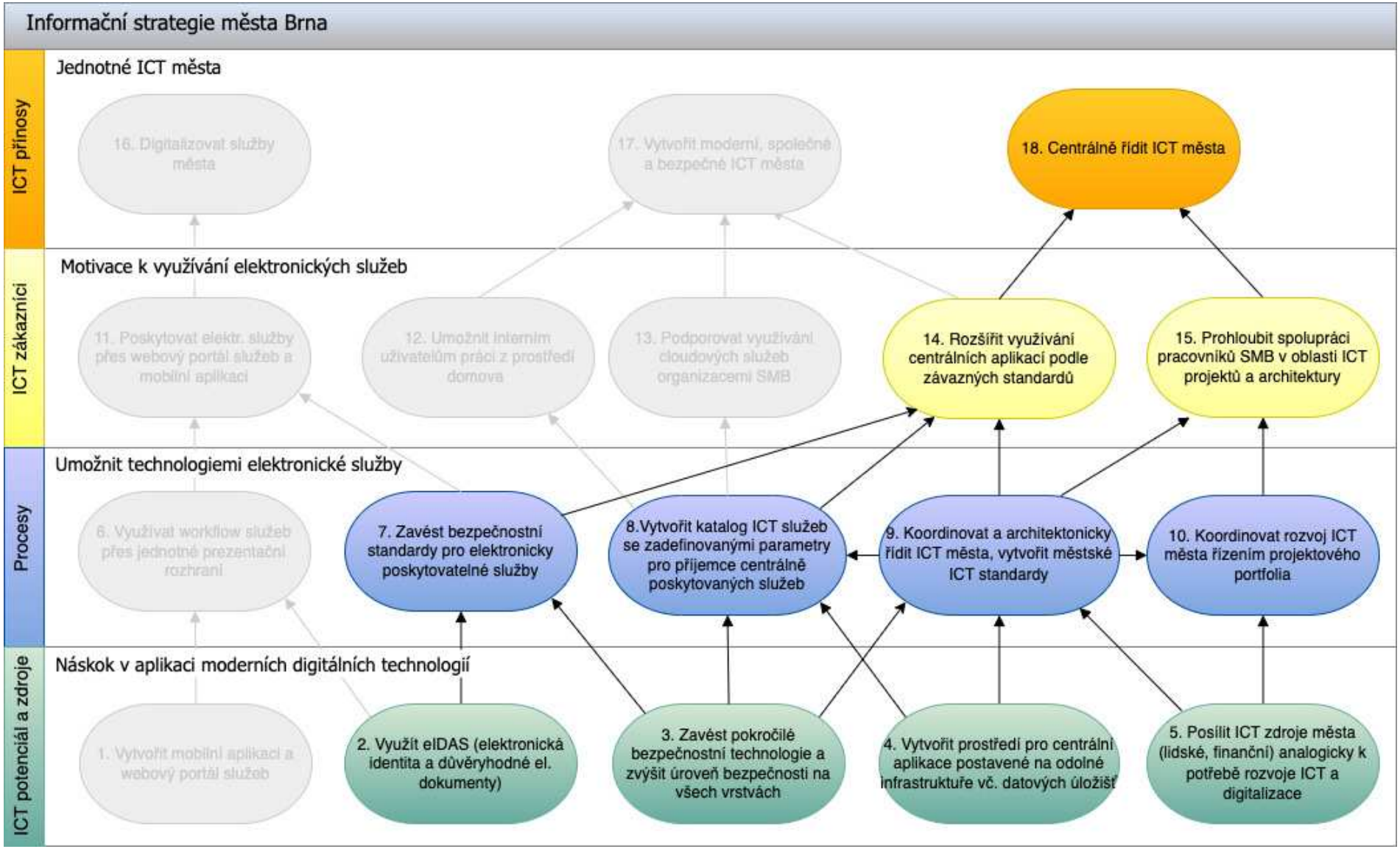
3.3.2. Řetězec digitalizace služeb



3.3.3. Řetězec tvorby ICT města



3.3.4. Řetězec 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 2023, 2024, 2025, 2026 a 2027.

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	2023 2024 2025	Webová platforma, na které bude provozován webový portál služeb, umožňuje ověření identit, včetně NIA. Vytvořen koncept integrace aplikací do webového portálu služeb. Vytvořen koncept integrace aplikací do mobilní aplikace. Součástí webového portálu služeb je řešení jeho kybernetické bezpečnosti. Portál je připraven pro naplnění službami. Realizace mobilní aplikace. Integrovány vybrané aplikační služby do webového portálu služeb a mobilní aplikace. Město provozuje webový portál služeb v souladu s moderními technologickými a bezpečnostními standardy. Město provozuje mobilní aplikaci v souladu s moderními technologickými a bezpečnostními standardy.
2	Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty)	Shoda s eIDAS	2023 2024 2025	Dokončena integrace služeb IDM do informačních systémů v rozsahu SŘBI. Jsou nasazeny technologie pro důvěryhodný oběh dokumentů. Autentizační brána IDM je připravena pro potřeby aplikací/služeb města (SMB). Plné zajištění shody s požadavky eIDAS umožňující poskytovat důvěryhodné elektronické služby Úřadu. Autentizační brána IDM je využívána pro potřeby aplikací/služeb města (SMB). Vytvoření propojených identit (federace) pro účely využívání služeb MMB městskými organizacemi.
3	Zavést pokročilé bezpečnostní technologie a zvýšit úroveň bezpečnosti na všech vrstvách	Vyspělost bezpečnostního modelu města	2023 2024 2025 2026	Naimplementován centrální LOG management SMB. V rozsahu MSB a na vybraných veřejných bodech SMB je nasazena a provozována centrální technologie automatizovaných detekcí zranitelností. Nakonfigurován systém PIM/PAM. V rozsahu MSB včetně přípojných bodů je realizován systém sdružených dozorových bezpečnostních sond, poskytujících automatizované detekce KBU/KBI zahrnující varování reakčního týmu. Vytvořen a provozován centrální systém sběru, analýzy a interpretace událostí z různých zdrojů MSB za účelem detekce anomálií a KBI. Vytvořen a provozován centrální systém automatizované reakce na detekované a kategorizované KBI. Provozování dohledového provozního a bezpečnostního centra SOC integrujícího všechny

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
				bezpečnostní technologie SMB.
4	Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť	Plná datová a infrastrukturní redundance	2023 2024	Zahájení poskytování služeb ve formě MSSP (managed security service provider). Rozšiřování služeb městského cloudu o služby pro eIDAS. Infrastrukturní prostředí je trvale dozorováno (provozní a bezpečnostní monitoring) a vybaveno geograficky oddělenými redundantními datovými centry s plnou datovou a infrastrukturní redundancí.
5	Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace	Obsazení rolí	2023 2024 2025	Dokončení vzniku samostatného referátu Kanceláře kybernetické bezpečnosti včetně personálního obsazení. Nábor pracovníka do stávajícího funkčního místa pro projektové řízení na OMI MMB. Dvě pracovní místa pro vývoj aplikací města. Zajistit funkční místo pro servisní podporu infrastruktury na OMI MMB (nárůst servisních požadavků v souvislosti se vzdáleným přístupem, home office, videokonferencemi). Obsazení role Solution Architect. Zajištění zastupitelnosti rolí podle požadavků NIS2 resp. nového zákona o kybernetické bezpečnosti. ICT zdroje jsou zajištěny a vybalancovány v takové výši, aby byly realizovatelné cíle směřující k rozvoji ICT a digitalizaci v rámci SMB.
6	Využívat workflow služeb přes jednotné prezentační rozhraní	Zavedeno workflow služby na portálu i městské aplikaci	2023 2024 2025	Výběr pilotní služby a návrh jejího workflow. Optimalizace workflow pilotní služby pro cílový stav k využití ve webovém portálu služeb a v městské aplikaci. Workflow u aplikací poskytujících služby úřadu přes portál i městskou aplikaci je navrženo ve spolupráci s garanty procesů a ORGO.
7	Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby	Bezpečnostní standardy zavedeny	2024 2025 2026	Standardy pro přidělování oprávnění / přístupů do PIM/PAM. Standard připojování MČ a městských organizací do LOG managementu. Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro městské akciové společnosti a pro významné příspěvkové organizace. Zaveden systém řízení kybernetické bezpečnosti dle nového zákona o kybernetické bezpečnosti / direktivy NIS2. Úroveň bezpečnosti a důvěryhodnosti elektronicky poskytovaných služeb je periodicky hodnocena a prokazována na základě jasných metodik vyplývajících z přijatých standardů.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
8	Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb	Katalog ICT služeb vytvořen	2023 2024 2025	Naplnění vytvořeného pilotního katalogu ICT služeb. Registrace služeb městského cloudu v eGC (eGovernment cloud). Katalog ICT služeb je dokončen a rozšířen o služby pro eIDAS. Katalog ICT služeb umožňuje využívat infrastrukturní, platformové a bezpečnostní služby cloudu jednotným způsobem, a to pro SMB a zřizované organizace města (městské firmy).
9	Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy	EA aplikována v SMB a zřizovaných organizacích města	2023 2024	Vytvořena směrnice a pracovní postup pro zadávání architektonických prvků do centrální evidence. Vytvořena směrnice a pracovní postup pro integraci dílčích agendových systémů. Systémy centrálně poskytované v rámci SMB jsou zavedeny v centrální evidenci. Ustanovení Rady pro řízení ICT architektury SMB. Požadavky z ICT projektů MMB s dopadem na architekturu jsou evidovány, analyzovány a schvalovány Radou pro řízení ICT architektury SMB. Vytvořené ICT standardy vycházející z Metodiky pro evidenci služeb veřejné správy. Řízení metodami EA (Enterprise Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy. Architektura podporuje proaktivní bezpečnostní přístup v celém životním cyklu systému (od záměru až po vyřazení). Významné ICT projekty SMB (vazba na řízení projektového portfolia) jsou evidovány a schvalovány Radou pro řízení ICT architektury SMB.
10	Koordinovat rozvoj ICT města řízením projektového portfolia	Oblasti koordinace v projektovém porfoliu	2023 2024 2025	Vytvořena směrnice a pracovní postup pro zpracování projektových záměrů MMB v oblasti ICT. Ustanovení Rady pro řízení ICT SMB. U všech nových ICT projektů MMB je zpracován projektový záměr. Stanovení hranic/pravidel pro klasifikaci významnosti projektů v rámci projektového portfolia města (ve fázi projektového záměru). Autorizace významných nových ICT projektů města (ve fázi projektového záměru). Projektové portfolio zahrnuje významné projekty z hlediska rozvoje ICT města a umožňuje jejich koordinované řízení v rámci SMB.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
11	Poskytovat elektr. služby přes webový portál služeb a mobilní aplikaci	Životní situace řešeny elektronicky přes portál služeb či mobilní aplikaci	2023 2024 2025 2026	Platební brána je implementována pro služby vyžadující platby. Pilotní prověření vybrané služby přes webový portál služeb a mobilní aplikaci. Nasazení zvolených služeb přes webový portál služeb a mobilní aplikaci. Vytvoření datové analytiky pro zrychlení a optimalizaci průběhu procesu.
12	Umožnit interním uživatelům práci z prostředí domova	Interním uživatelům je umožněn vzdálený přístup do aplikací SMB	2023 2024	Vyhodnocení zkušeností z provozu se vzdáleným přístupem a na základě toho případné dopady do technologií. Posílení bezpečnostních prvků pro vzdálený přístup.
13	Podporovat využívání služeb městského cloudu organizacemi SMB	Městské cloudové služby využívány městskými firmami	2023 2024 2026	Městské cloudové služby (zálohování, úložiště, bezpečnost) jsou poskytovány za výhodných ekonomických podmínek z pozice jednotlivých městských firem obtížně dosažitelných a na profesionální úrovni. Portál umožňuje objednávání služeb městského cloudu (objednávkový portál cloudových služeb). Přístup ke službám městského cloudu je zajištěn pro všechny organizace SMB.
14	Rozšířit využívání centrálních aplikací podle závazných standardů	ICT služby poskytované SMB standardizovány	2023 2024 2025	Navržena struktura technologického standardu (jako základní technologický rámec s možností jeho využití ve výběrových řízeních) s vazbou na architektonické principy. Propojení architektonického řízení s konfiguračním managementem (GPC databáze). Městský cloud je ve shodě s uveřejněnými podmínkami eGC ČR a jsou zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...). Úplné dokončení technologického standardu. Centrálně poskytované aplikace budou ve shodě s podmínkami eGC ČR a město bude mít zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...). Jsou využívány a udržovány technologické, architektonické a bezpečnostní standardy ICT SMB.
15	Prohloubit spolupráci pracovníků SMB v oblasti ICT projektů a architektury	Spolupracující subjekty	2024 2025	Projednání a zveřejnění hranic/pravidel pro klasifikaci významnosti projektů v rámci projektového portfolia města (ve fázi projektového záměru). Zahájení autorizace významných nových ICT projektů města (ve fázi projektového záměru). Řízení ICT projektů a EA (Enterprise Architecture) je prováděno ve spolupráci ICT pracovníků a dalších odborných pracovníků/garantů v rámci SMB.

Číslo	Strategický cíl	Měřítko	Rok	Popis dosaženého stavu v jednotlivých letech
16	Digitalizovat služby města	Očekávané přínosy z elektronizace služeb dosaženy	2023 2024 2026 2027	Vytvořena koncepce webového portálu služeb a městské aplikace s očekávanými přínosy. Rozpracován způsob začlenění životních situací do webového portálu služeb a městské aplikace a zvolena životní situace pro pilotní ověření. Vyhodnoceny přínosy z pilotního ověření vybrané životní situace poskytované přes portál a městskou aplikaci města se stanovením začlenění vybraných služeb. Město disponuje elektronicky poskytovanými službami pro všechny zvolené služby. Vyhodnoceny přínosy z digitalizovaných služeb.
17	Vytvořit moderní, společné a bezpečné ICT města	ICT města sdíleno	2024 2025 2026	Technická aktiva MMB jsou v souladu s technologickými standardy. Městská ICT infrastruktura je v souladu s technologickými ICT standardy a KB standardy. Město disponuje moderní modulární a stále se rozvíjející ICT infrastrukturou, která je sdílena v rámci MMB, MČ, městských firem a organizací. Infrastruktura poskytuje maximálně efektivní elektronické služby a její bezpečnost je zajištěna na pokročilé úrovni. Celá infrastruktura je dozorována na více úrovních za účelem zajišťování vysoké důvěryhodnosti.
18	Centrálně řídit ICT města	Centralizace řízení ICT	2024 2025	Významné projekty města jsou centrálně řízeny Radou pro řízení ICT SMB. Směřování městského ICT v provozní i bezpečnostní rovině je centrálně řízeno. Řízení ICT města je prováděno centralizovaně na projektové a architektonické úrovni orgánem zřízeným Radou města (tj. Radou pro řízení ICT SMB).

4.2. Strategické ICT projekty

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

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

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

4.2.1. 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	2023 2024 2025	Webová platforma, na které bude provozován webový portál služeb, umožňuje ověření identit, včetně NIA. Vytvořen koncept integrace aplikací do webového portálu služeb. Vytvořen koncept integrace aplikací do mobilní aplikace. Součástí webového portálu služeb je řešení jeho kybernetické bezpečnosti. Portál je připraven pro naplnění službami. Realizace mobilní aplikace. Integrovány vybrané aplikační služby do webového portálu služeb a mobilní aplikace. Město provozuje webový portál služeb v souladu s moderními technologickými a bezpečnostními standardy. Město provozuje mobilní aplikaci v souladu s moderními technologickými a bezpečnostními standardy.
5	Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace	2023	Dvě pracovní místa pro vývoj aplikací města.

4.2.2. Digitální služby města Brna (přes webový portál služeb a městskou mobilní aplikaci)

Účel strategického projektu:

Přínosový cíl 16. *Digitalizovat služby města*.

Cíle strategického projektu:

6	Využívat workflow služeb přes jednotné prezentační rozhraní	2023 2024 2025	Výběr pilotní služby a návrh jejího workflow. Optimalizace workflow pilotní služby pro cílový stav k využití ve webovém portálu služeb a v městské aplikaci. Workflow u aplikací poskytujících služby úřadu přes portál i městskou aplikaci je navrženo ve spolupráci s garanty procesů a ORGO.
11	Poskytovat elektr. služby přes webový portál služeb a mobilní aplikaci	2023 2024 2025 2026	Platební brána je implementována pro služby vyžadující platby. Pilotní prověření vybrané služby přes webový portál služeb a mobilní aplikaci. Nasazení zvolených služeb přes webový portál služeb a mobilní aplikaci. Vytvoření datové analytiky pro zrychlení a optimalizaci průběhu procesu.

4.2.3. Služby autentikace podle eIDAS

Účel strategického projektu:

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

Cíle strategického projektu:

2	Využít eIDAS (elektronická identita a důvěryhodné el. dokumenty)	2023 2024 2025	Dokončena integrace služeb IDM do informačních systémů v rozsahu SŘBI. Jsou nasazeny technologie pro důvěryhodný oběh dokumentů. Autentizační brána IDM je připravena pro potřeby aplikací/služeb města (SMB). Plné zajištění shody s požadavky eIDAS umožňující poskytovat důvěryhodné elektronické služby Úřadu. Autentizační brána IDM je využívána pro potřeby aplikací/služeb města (SMB). Vytvoření propojených identit (federace) pro účely využívání služeb MMB městskými organizacemi.

4.2.4. Systematizace řízení kybernetické bezpečnosti

Účel strategického projektu:

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

Cíle strategického projektu:

5	Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace	2023 2024	Dokončení vzniku samostatného referátu Kanceláře kybernetické bezpečnosti včetně personálního obsazení. Zajištění zastupitelnosti rolí podle požadavků NIS2 resp. nového zákona o kybernetické bezpečnosti.
7	Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby	2024 2025 2026	Standard připojování MČ a městských organizací do LOG managementu. Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro městské akciové společnosti a pro významné příspěvkové organizace. Zaveden systém řízení kybernetické bezpečnosti dle nového zákona o kybernetické bezpečnosti / direktivy NIS2. Úroveň bezpečnosti a důvěryhodnosti elektronicky

			poskytovaných služeb je periodicky hodnocena a prokazována na základě jasných metodik vyplývajících z přijatých standardů.

4.2.5. Zajištění odolnosti

Účel strategického projektu:

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

Cíle strategického projektu:

4	Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť	2024	Infrastrukturní prostředí je trvale dozorováno (provozní a bezpečnostní monitoring) a vybaveno geograficky oddělenými redundantními datovými centry s plnou datovou a infrastrukturní redundancí.
5	Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace	2023	Zajistit funkční místo pro servisní podporu infrastruktury na OMI MMB (nárůst servisních požadavků v souvislosti se vzdáleným přístupem, home office, videokonferencemi).
7	Zavést bezpečnostní standardy pro elektronicky poskytovatelné služby	2024	Standardy pro přidělování oprávnění / přístupů do PIM/PAM.

4.2.6. Zavedení dohledových a reaktivních technologií

Účel strategického projektu:

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

Cíle strategického projektu:

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

4.2.7. Městský cloud

Účel strategického projektu:

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

Cíle strategického projektu:

4	Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť	2023	Rozšiřování služeb městského cloudu o služby pro eIDAS.
8	Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb	2024	Registrace služeb městského cloudu v eGC (eGovernment cloud).
13	Podporovat využívání služeb městského cloudu organizacemi SMB	2023 2024 2026	Městské cloudové služby (zálohování, úložiště, bezpečnost) jsou poskytovány za výhodných ekonomických podmínek z pozice jednotlivých městských firem obtížně dosažitelných a na profesionální úrovni. Portál umožňuje objednávání služeb městského cloudu (objednávkový portál cloudových služeb). Přístup ke službám městského cloudu je zajištěn pro všechny organizace SMB.

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

Účel strategického projektu:

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

Cíle strategického projektu:

4	Vytvořit prostředí pro centrální aplikace postavené na odolné infrastruktuře vč. datových úložišť	2023	Zahájení poskytování služeb ve formě MSSP (managed security service provider).
8	Vytvořit katalog ICT služeb se zadefinovanými parametry pro příjemce centrálně poskytovaných služeb	2023 2024 2025	Naplnění vytvořeného pilotního katalogu ICT služeb. Katalog ICT služeb je dokončen a rozšířen o služby pro eIDAS. Katalog ICT služeb umožňuje využívat infrastrukturní, platformové a bezpečnostní služby cloudu jednotným způsobem, a to pro SMB a zřizované organizace města (městské firmy).
12	Umožnit interním uživatelům práci z prostředí domova	2023 2024	Vyhodnocení zkušeností z provozu se vzdáleným přístupem a na základě toho případné dopady do technologií. Posílení bezpečnostních prvků pro vzdálený přístup.

4.2.9. Koordinace, standardizace a architektura

Účel strategického projektu:

Přínosový cíl 18. *Centrálně řídit ICT města*.

Cíle strategického projektu:

5	Posílit ICT zdroje města (lidské, finanční) analogicky k potřebě rozvoje ICT a digitalizace	2023 2025	Obsazení role Solution Architect. ICT zdroje jsou zajištěny a vybalancovány v takové výši, aby byly realizovatelné cíle směřující k rozvoji ICT a digitalizaci v rámci SMB (pro architektonické řízení).
9	Koordinovat a architektonicky řídit ICT města, vytvořit městské ICT standardy	2023 2024	Vytvořena směrnice a pracovní postup pro zadávání architektonických prvků do centrální evidence. Vytvořena směrnice a pracovní postup pro integraci dílčích agendových systémů. Systémy centrálně poskytované v rámci SMB jsou zavedeny v centrální evidenci. Ustanovení Rady pro řízení ICT architektury SMB. Požadavky z ICT projektů MMB s dopadem na architekturu jsou evidovány, analyzovány a schvalovány Radou pro řízení ICT architektury SMB. Vytvořené ICT standardy vycházející z Metodiky pro evidenci služeb veřejné správy. Řízení metodami EA (Enterprise Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy. Architektura podporuje proaktivní bezpečnostní přístup v celém životním cyklu systému (od záměru až po vyřazení). Významné ICT projekty SMB (vazba na řízení projektového portfolia) jsou evidovány a schvalovány Radou pro řízení ICT architektury SMB.
14	Rozšířit využívání centrálních aplikací podle závazných standardů	2023 2024 2025	Navržena struktura technologického standardu (jako základní technologický rámec s možností jeho využití ve výběrových řízeních) s vazbou na architektonické principy. Propojení architektonického řízení s konfiguračním managementem (GPC databáze). Naplnění struktury technologického standardu v prioritních částech. Městský cloud je ve shodě s eGC ČR a jsou zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...). Úplné dokončení technologického standardu. Centrálně poskytované aplikace budou ve shodě s eGC ČR a město bude mít zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...). Jsou využívány a udržovány technologické, architektonické a bezpečnostní standardy ICT SMB.
15	Prohloubit spolupráci pracovníků SMB v oblasti ICT projektů a architektury	2025	Řízení ICT projektů a EA (Enterprise Architecture) je prováděno ve spolupráci ICT pracovníků a dalších odborných pracovníků/garantů v rámci SMB.

4.2.10. Systém řízení projektového portfolia

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	2023 2025	Nábor pracovníka do stávajícího funkčního místa pro projektové řízení na OMI MMB. ICT zdroje jsou zajištěny a vybalancovány v takové výši, aby byly realizovatelné cíle směřující k rozvoji ICT a digitalizaci v rámci SMB (pro projektové řízení).
10	Koordinovat rozvoj ICT města řízením projektového portfolia	2023 2024 2025	Vytvořena směrnice a pracovní postup pro zpracování projektových záměrů MMB v oblasti ICT. Ustanovení Rady pro řízení ICT SMB. U všech nových ICT projektů MMB je zpracován projektový záměr. Stanovení hranic/pravidel pro klasifikaci významnosti projektů v rámci projektového portfolia města (ve fázi projektového záměru). Autorizace významných nových ICT projektů města (ve fázi projektového záměru). Projektové portfolio zahrnuje významné projekty z hlediska rozvoje ICT města a umožňuje jejich koordinované řízení v rámci SMB.
15	Prohloubit spolupráci pracovníků SMB v oblasti ICT projektů a architektury	2024 2025	Projednání a zveřejnění hranic/pravidel pro klasifikaci významnosti projektů v rámci projektového portfolia města (ve fázi projektového záměru). Zahájení autorizace významných nových ICT projektů města (ve fázi projektového záměru). Řízení ICT projektů a EA (Enterprise Architecture) je prováděno ve spolupráci ICT pracovníků a dalších odborných pracovníků/garantů v rámci SMB.

4.3. Harmonogram strategických projektů

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

Strategické projekty		2023	2024	2025	2026	2027
Cíl	**Webová a mobilní platforma města Brna**					
1	Webová platforma, na které bude provozován webový portál služeb, umožňuje ověření identit, včetně NIA.					
1	Vytvořen koncept integrace aplikací do webového portálu služeb.					
1	Vytvořen koncept integrace aplikací do mobilní aplikace.					
1	Součástí webového portálu služeb je řešení jeho kybernetické bezpečnosti.					
1	Portál je připraven pro naplnění službami.					
1	Realizace mobilní aplikace.					
1	Integrovány vybrané aplikační služby do webového portálu služeb a mobilní aplikace.					
1	Město provozuje webový portál služeb v souladu s moderními technologickými a bezpečnostními standardy.					
1	Město provozuje mobilní aplikaci v souladu s moderními technologickými a bezpečnostními standardy.					
5	Dvě pracovní místa pro vývoj aplikací města.					
Cíl	**Digitální služby města Brna (přes webový portál služeb a městskou mobilní aplikaci)**					
6	Výběr pilotní služby a návrh jejího workflow.					
6	Optimalizace workflow pilotní služby pro cílový stav k využití ve webovém portálu služeb a v městské aplikaci.					
6	Workflow u aplikací poskytujících služby úřadu přes portál i městskou aplikaci je navrženo ve spolupráci s garanty procesů a ORGO.					
11	Platební brána je implementována pro služby vyžadující platby.					
11	Pilotní prověření vybrané služby přes webový portál služeb a mobilní aplikaci.					
11	Nasazení zvolených služeb přes webový portál služeb a mobilní aplikaci.					
11	Vytvoření datové analytiky pro zrychlení a optimalizaci průběhu procesu.					

Strategické projekty		2023	2024	2025	2026	2027
Cíl	**Služby autentikace podle eIDAS**					
2	Dokončena integrace služeb IDM do informačních systémů v rozsahu SŘBI.					
2	Jsou nasazeny technologie pro důvěryhodný oběh dokumentů.					
2	Autentizační brána IDM je připravena pro potřeby aplikací/služeb města (SMB).					
2	Plné zajištění shody s požadavky eIDAS umožňující poskytovat důvěryhodné elektronické služby Úřadu.					
2	Autentizační brána IDM je využívána pro potřeby aplikací/služeb města (SMB).					
2	Vytvoření propojených identit (federace) pro účely využívání služeb MMB městskými organizacemi.					
Cíl	**Systematizace řízení kybernetické bezpečnosti**					
5	Dokončení vzniku samostatného referátu Kanceláře kybernetické bezpečnosti včetně personálního obsazení.					
5	Zajištění zastupitelnosti rolí podle požadavků NIS2 resp. nového zákona o kybernetické bezpečnosti.					
7	Standard připojování MČ a městských organizací do LOG managementu.					
7	Závazná strategie a pravidla kybernetické bezpečnosti stanovena pro městské akciové společnosti a pro významné příspěvkové organizace.					
7	Zaveden systém řízení kybernetické bezpečnosti dle nového zákona o kybernetické bezpečnosti / direktivy NIS2.					
7	Úroveň bezpečnosti a důvěryhodnosti elektronicky poskytovaných služeb je periodicky hodnocena a prokazována na základě jasných metodik vyplývajících z přijatých standardů.					
Cíl	**Zajištění odolnosti**					
4	Infrastrukturní prostředí je trvale dozorováno (provozní a bezpečnostní monitoring) a vybaveno geograficky oddělenými redundantními datovými centry s plnou datovou a infrastrukturní redundancí.					
5	Zajistit funkční místo pro servisní podporu infrastruktury na OMI MMB (nárůst servisních požadavků v souvislosti se vzdáleným přístupem, home office, videokonferencemi).					
7	Standardy pro přidělování oprávnění / přístupů do PIM/PAM.					

Strategické projekty		2023	2024	2025	2026	2027
Cíl	**Zavedení dohledových a reaktivních technologií**					
3	Naimplementován centrální LOG management SMB.					
3	V rozsahu MSB a na vybraných veřejných bodech SMB je nasazena a provozována centrální technologie automatizovaných detekcí zranitelností.					
3	Nakonfigurován systém PIM/PAM.					
3	V rozsahu MSB včetně přípojných bodů je realizován systém sdružených dozorových bezpečnostních sond, poskytujících automatizované detekce KBU/KBI zahrnující varování reakčního týmu.					
3	Vytvořen a provozován centrální systém sběru, analýzy a interpretace událostí z různých zdrojů MSB za účelem detekce anomálií a KBI.					
3	Vytvořen a provozován centrální systém automatizované reakce na detekované a kategorizované KBI.					
3	Provozování dohledového provozního a bezpečnostního centra SOC integrujícího všechny bezpečnostní technologie SMB.					
Cíl	**Městský cloud**					
4	Rozšiřování služeb městského cloudu o služby pro eIDAS.					
8	Registrace služeb městského cloudu v eGC (eGovernment cloud).					
13	Městské cloudové služby (zálohování, úložiště, bezpečnost) jsou poskytovány za výhodných ekonomických podmínek z pozice jednotlivých městských firem obtížně dosažitelných a na profesionální úrovni.					
13	Portál umožňuje objednávání služeb městského cloudu (objednávkový portál cloudových služeb).					
13	Přístup ke službám městského cloudu je zajištěn pro všechny organizace SMB.					
Cíl	**Centrální služby a aplikace, služby a aplikace v cloudu**					
4	Zahájení poskytování služeb ve formě MSSP (managed security service provider).					
8	Naplnění vytvořeného pilotního katalogu ICT služeb.					
8	Katalog ICT služeb je dokončen a rozšířen o služby pro eIDAS.					
8	Katalog ICT služeb umožňuje využívat infrastrukturní, platformové a bezpečnostní služby cloudu jednotným způsobem, a to pro SMB a zřizované organizace města (městské firmy).					

	Strategické projekty	2023	2024	2025	2026	2027
12	Vyhodnocení zkušeností z provozu se vzdáleným přístupem a na základě toho případné dopady do technologií.					
12	Posílení bezpečnostních prvků pro vzdálený přístup.					
Cíl	**Koordinace, standardizace a architektura**					
5	Obsazení role Solution Architect.					
5	ICT zdroje jsou zajištěny a vybalancovány v takové výši, aby byly realizovatelné cíle směřující k rozvoji ICT a digitalizaci v rámci SMB. - pro architektonické řízení					
9	Vytvořena směrnice a pracovní postup pro zadávání architektonických prvků do centrální evidence.					
9	Vytvořena směrnice a pracovní postup pro integraci dílčích agendových systémů.					
9	Systémy centrálně poskytované v rámci SMB jsou zavedeny v centrální evidenci. Ustanovení Rady pro řízení ICT architektury SMB.					
9	Požadavky z ICT projektů MMB s dopadem na architekturu jsou evidovány, analyzovány a schvalovány Radou pro řízení ICT architektury SMB.					
9	Vytvořené ICT standardy vycházející z Metodiky pro evidenci služeb veřejné správy.					
9	Řízení metodami EA (Enterprise Architecture) je aplikováno na všechny systémy MMB a v rámci SMB na centrálně poskytované systémy.					
9	Architektura podporuje proaktivní bezpečnostní přístup v celém životním cyklu systému (od záměru až po vyřazení).					
9	Významné ICT projekty SMB (vazba na řízení projektového portfolia) jsou evidovány a schvalovány Radou pro řízení ICT architektury SMB.					
14	Navržena struktura technologického standardu (jako základní technologický rámec s možností jeho využití ve výběrových řízeních) s vazbou na architektonické principy.					
14	Propojení architektonického řízení s konfiguračním managementem (GPC databáze).					
14	Naplnění struktury technologického standardu v prioritních částech.					
14	Městský cloud je ve shodě s eGC ČR a jsou zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...).					
14	Úplné dokončení technologického standardu.					

	Strategické projekty	2023	2024	2025	2026	2027
14	Centrálně poskytované aplikace budou ve shodě s eGC ČR a město bude mít zavedeny standardy pro oblast informatiky v souladu s požadavky eGovernmentu ČR (např. bezpečnost, technologie, vzdálený přístup, otevřená data, aplikace ...).					
14	Jsou využívány a udržovány technologické, architektonické a bezpečnostní standardy ICT SMB.					
15	Řízení ICT projektů a EA (Enterprise Architecture) je prováděno ve spolupráci ICT pracovníků a dalších odborných pracovníků/garantů v rámci SMB.					
Cíl	**Systém řízení projektového portfolia**					
5	Nábor pracovníka do stávajícího funkčního místa pro projektové řízení na OMI MMB.					
5	ICT zdroje jsou zajištěny a vybalancovány v takové výši, aby byly realizovatelné cíle směřující k rozvoji ICT a digitalizaci v rámci SMB. - pro projektové řízení					
10	Vytvořena směrnice a pracovní postup pro zpracování projektových záměrů MMB v oblasti ICT.					
10	Ustanovení Rady pro řízení ICT SMB.					
10	U všech nových ICT projektů MMB je zpracován projektový záměr.					
10	Stanovení hranic/pravidel pro klasifikaci významnosti projektů v rámci projektového portfolia města (ve fázi projektového záměru).					
10	Autorizace významných nových ICT projektů města (ve fázi projektového záměru).					
10	Projektové portfolio zahrnuje významné projekty z hlediska rozvoje ICT města a umožňuje jejich koordinované řízení v rámci SMB.					
15	Projednání a zveřejnění hranic/pravidel pro klasifikaci významnosti projektů v rámci projektového portfolia města (ve fázi projektového záměru).					
15	Zahájení autorizace významných nových ICT projektů města (ve fázi projektového záměru).					

Závěr

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

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

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

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