Architecture Description

Common Capabilities to Support Northern Ireland Citizen Service Delivery

Prepared for

Digital Shared Services (DSS), Department of Finance, Northern Ireland

Prepared by

Microsoft Services, Digital Advisory and Architectural Services

Date: 21/12/2018

Version: 1.0 Final

Executive Summary

In 2017 both Digital Shared Services (DSS) and Microsoft agreed to expand their working relationship from a purely tactical and reactive relationship to include a strategic dimension with initial quarterly "Roundtable" Meetings started in November of that year. From these meetings a longer-term program of work was defined by DSS and Microsoft.

With the NI Direct Strategic Partnership nearing the end of its first framework tenure, the program of work identified a priority focussing on Digital Transformation and the acceleration of onboarding and improvement of delivery of Northern Ireland (NI) Citizen Services. Key objectives of this priority focussed upon identifying and enhancing digital capabilities, whilst identifying efficiencies in order to benefit the services and improve the end-user experience for the citizen. An initial workshop delivered by a Microsoft Government Industry Architect specialising in Citizen Services identified areas for further discussion, assessment and review. It is these key areas that shaped the objectives of the current engagement with DSS which started in September 2018 and completed in December 2018 with the presentation of this document to DSS. The agreed objectives of this engagement were:

1. **Deliver an initial Conceptual Architecture, IT Service Map & enhancement roadmap to support DSS business change, focusing primarily on citizen facing services**
    - Refer to sections 3, 3.1-3.6, 4.1.1 and 4.3.1 for these deliverables
2. **Provide insight to DSS into Developing a Digital Enterprise Architecture (EA) Function to enable the delivery of repeatable and continuous change**
    - Refer to sections 3.7.4, 4.1.2 and 4.3.2 for these deliverables
3. **Refine the vision & objectives for the DSS Enterprise Architecture function**
    - Refer to section 0, 3.7.1-3.7.4 for these deliverables

A Microsoft Services project team working very closely with DSS and members of the Technical Design Group (TDG) ran a large number of workshops from September 2018 – November 2018 focussing on establishing an understanding of the current DSS EA and Citizen Services delivery working practices. These workshops covered the following areas:

- Scenario Planning
- Capability Modelling
- Architecture Definition
- EA Practice Development
- IT Service Map
- Roadmap Definition

During the workshops and subsequent analysis, there were a number of key observations noted:

- A portfolio of projects for citizen services have been successfully delivered. However, **the approaches were often siloed and inconsistent, with opportunities for re-use missed**. This resulted in some duplication of effort and un-necessary additional costs. This type of approach in the longer term often leads to increased costs, supportability issues and a poor, inconsistent citizen experience;
- Some of the **citizen services capabilities providing broadly available functionality could have been delivered utilising already available COTS and/or Public Cloud services**, rather than being

created and developed from new. Developing from new in the longer term often leads to more complex solutions, security issues, upgrade paths and increased time to introduce new features and functionality;

- There is currently **no Enterprise Architecture function (as described in this document) operating across NICS**. There are pockets of EA, but this is not consistent in approach and often siloed;
- Enterprise Architecture involvement **through application & portfolio review and assessment is absent or often considered too late in the process;**
- There was evidence that representatives from across the **participating departments were unaware of similar initiatives happening in other parts of NICS**. In the longer term this can create issues with end user relationships and engagement, generation of relevant pipeline initiatives and subsequent prioritisation;
- Whilst it is recognised that work is on-going in order to determine an overall view of the required capabilities for Citizen Services in the medium to longer term, it must be noted that this information was not available during this engagement.

Given the strategic focus of NI government and DSS specifically on improving citizen services while ensuring a sustained, planned implementation and a drive for reuse, MS believes that DSS has a good foundation to achieve the next level of capabilities in citizen service delivery. MS believes future citizen services work should be focused around three main themes:

- **connected citizens, businesses** and initially the most important – **connected government**;
- **delivering pro-active services**, thus driving the personalization of the experience for citizens and business representatives, enabling significant rethinking of delivery approach for some of the existing services;
- achieve **sustainability of citizen services IT environment** through reuse of data and common platform elements, unification of dev and ops approaches, insights into platform use.

The most important aspects to accelerate the implementation of this next level of citizen services delivery in NI are:

- **coordination of business and IT efforts, management of service dependencies**, aligning roadmaps, key stakeholders and timelines across DSS and broader government;
- set of solid **reusable services and reusable or modular platforms** owned by DSS to accelerate implementation, at the same time providing better experience for citizens and deep insights for government leaders;
- **unifying data exchange in government** through APIs, data sets and event publishing, supported by appropriate policies for data reuse within government (and beyond), information architecture focus;
- **infusing rich citizen identity into all government systems** while relying on different trusted identity providers (e.g. banks, gov.uk, NIDA) and social identity providers to drive personalization and ease of adoption;
- introducing more **modern IT service implementation and management practices** leveraging elements of DevSecOps and public cloud, leveraging platforms more than basic infrastructure.

Considering the vision for Enterprise Architecture, Citizen Services technical capabilities and architecture as detailed within this document, Microsoft would recommend and encourage the DSS leadership team to support:

- The **establishment of an Enterprise wide architecture function** within DSS as a key priority and a required enabler for the continued and future success of DSS to enable it to deliver on its strategic goals. The remit of the EA function should be beyond DSS in order to provide greater value for NICS;
- Taking into account any additional information on future Citizen Services pipeline and architectural information that was not available during the engagement timeline, **task the EA function on agreeing the core capabilities required for Citizen Services; confirming the architectural blueprint, platforms and infrastructure to deliver these capabilities and develop a plan to implement**. It is noted that DSS, the NICS Departments and their partners will need to continue delivering those citizen services already in use;
- **Embedding the EA function into the NICS governance model, allowing for their inclusion in early discussions across DSS and the other NICS Departments** in order to ensure they have visibility of pipeline and initiatives so that they can maintain and plan for future changes to the core capabilities, platforms and architecture. This will also allow for a focus on appropriate re-use of already available capabilities and data sources, driving reduction in complexity, standardisation, cost avoidance and reducing the time to on-board new services. It will also encourage and build upon the relationships with NICS;
- Ensuring that DSS have **a sustainable Target Operating model for the EA function;**
- If DSS and NICS decide to make more use of the Public Cloud to deliver Citizen Services, there will also be a need for the development of **a sustainable and efficient model for delivering and maintaining a hybrid (On-Premise and Public Cloud) operating model** in order to support the EA function and core capabilities required. This can also be extended then to support the other NICS departments in the delivery of those services that they will be responsible for;
- With Public Cloud capabilities developing at faster and faster rates, and with its growing acceptance and proliferation to host more and more public services, ensure **the EA function has capacity to remain current with the new capabilities and technologies to support the digital capabilities** required for Citizen Services.

Acknowledgments

The MS Services project team wish to thank DSS for funding this engagement, their professional approach and for making their staff available over the course of the 14 weeks. This open, honest, transparent approach and enthusiastic participation by all, allowed for the objectives of the engagement to be met within the planned schedule and budget. It was clearly evident that DSS and TDG are passionate about the delivery of NI Citizen Services and continuing to build upon the success to date. The MS project team would also like to thank DSS for hosting many of the workshops in Dundonald House.

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change Reference
19/10/2018	Mark Loughran, Aldis Vilums	0.9 Draft	Initial content on positioning, goals, scenarios and capabilities required for citizen service delivery
03/12/2018	Microsoft team	1.0 Draft	Initial full scope version as draft for review with customer
21/12/2018	TDG and Microsoft Team	1.0 Final	Updates to document based on feedback, additional content. Document prepared for release.

Reviewers

Name	Version Approved	Position	Date
Paul Farnan	1.0 Final	Delivery Manager, Digital Advisory Services	20/12/2018
Steven McIvor	1.0 Final	Account Delivery Executive, Microsoft Services	21/12/2018
Gerry Thompson	1.0 Final	Head of Service Planning	06/12/2018
Stephen Patterson	1.0 Final	Head of Digital Development	06/12/2018
Lee Goudie	1.0 Final	Digital Development	06/12/2018
Steven McGaughey	1.0 Final	Land & Property Services	06/12/2018
Alan Ross	1.0 Final	Service Planning	06/12/2018

Table of contents

Executive Summary ii

1. Introduction 8

1.1. Context 8

1.2. Goals 9

1.3. Key Stakeholders 9

1.4. References 10

1.5. Document Organization 12

1.6. Intended Audience 12

2. Needs 13

2.1. Strategic Context 13

2.2. Business View 16

2.3. Ethical Principles 19

2.4. Architectural Principles 20

2.5. Architectural Constraints 24

2.6. Quality Attribute View 26

3. Architecture 31

3.1. Capabilities View 31

3.2. Application Architecture View 49

3.3. Information View 57

3.4. Development, Security & Operations Lifecycle View 58

3.5. Infrastructure View 63

3.6. Security View 67

3.7. Governance View – Enterprise Architecture 70

4. Roadmap 76

4.1. Initiatives 76

4.2. Benefit Dependency Map 82

4.3. Initial Plan 84

5. Appendices 92

5.1. Glossary of Key Terms 92

5.2. Inflight and Planned Projects 94

5.3. EA Capability Model – Capability Definitions 97
5.4. Mandatory Service Documentation 101
5.5. Technical Initiatives 103
5.6. Solution Architecture Details 108

1. Introduction

This section introduces the context of the work performed by Microsoft (MS, MSFT) together with Digital Shared Services (DSS) Department of Finance (Northern Ireland) in revisiting/assessing the citizen services delivery capabilities, approach, defining future vision and initiatives required to achieve better services delivery aligned with digital strategy of government or Northern Ireland.

1.1. Context

Northern Ireland government has been on the journey of providing citizen services with support of IT solutions for some time and have achieved good recognition for the services implemented so far. Given that this has been a period of fast growth, some of the approaches leveraged (although intended) were not necessarily unified across various government departments and systems.

Now planning implementation of the new digital strategy for Northern Ireland government Digital Shared Services team is reassessing the approaches based on the learnings of previous projects to come up with an approach that will meet the next set of goals outlined under the constraints that are given, while ensuring sustainable service management practices going forward.

As part of this effort in 2017 both Digital Shared Services and Microsoft agreed to expand their working relationship from tactical to strategic with quarterly "Roundtable" Meetings initiated in November 2017.

A long-term program of work was defined by Digital Shared Services and Microsoft.

The priority agreed was “Digital NI” with a set of workshops to be delivered by a Microsoft Government Industry Architect and Microsoft Consulting Services.

Microsoft have a unique combination of internal and external systems knowledge and global experience in delivering Digital Transformation activities for other Governments world-wide.

Digital Shared Services are looking at ways to accelerate Digital Transformation in the future, with a focus on innovation and enhanced digital capabilities that will benefit citizens.

A key enabler identified for “Digital NI” during DSS and Microsoft workshops was the development of Enterprise Architecture Blueprint for DSS that would enable:

- A unified map of common capabilities to be used in planning – assessing gaps against future vision, defining priorities and supporting initiatives;
- Identification of efficiency gains by identifying elements for reuse;
- Stronger technology infrastructure through modern application lifecycle management approaches and platforms;
- Solid foundation for onboarding new customers and citizen solutions to drive consistency for citizens and operational gains for government.

This document represents the summary of the results of the work on enterprise architecture blueprint specifically for citizen services engagement and IT services involved in supporting this engagement.

1.2. Goals

Given that enterprise architecture is continuous, the goal here is to draft an initial blueprint of required capabilities, understand the gaps in these capabilities that exist and create an overall plan of common services and initiatives to support them going forward.

This initial blueprint only goes into details of solutions for the priority areas and common services provided by DSS. It stops at a detailed level of logical architecture that should support initiative planning and prioritization but does not prescribe any specific technical solutions or approaches.

Specific areas/objectives for the Microsoft's engagement on helping to kick-start the process are:

1. Deliver an initial Conceptual Architecture, IT Service Map & enhancement roadmap to support DSS business change;
2. Provide insight to Digital Shared Services (DSS) into developing a Digital Enterprise Architecture function to enable the delivery of repeatable and continuous change;
3. Refine the vision & objectives for the DSS Enterprise Architecture function.

1.3. Key Stakeholders

Table 1 details the key stakeholders engaged during this engagement. It also lists stakeholders that will be affected by the implementation of this work, given position of DSS as provider of shared services in government of Northern Ireland.

Table 1: Key stakeholders

Stakeholder / Group	Position / Description
Caron Alexander	Director, Digital Shared Services (Executive Sponsor)
Trevor Steenson	Head of Digital Transformation Service
Damian Martin	Chief Operating Officer
Ignatius O'Doherty	Chief Strategy Officer
Seamus McLean	Head of Enterprise Digital Development
Stephen Patterson	Head of Digital Development
Gerry Thompson	Head of Service Planning
Lee Goudie	Digital Development
Steve Ravey	Digital Transformation Service
Jonathan Smith	Public Sector Shared Services Programme
Alan Ross	Service Planning

Stakeholder / Group	Position / Description
Gina McConville	Head of Customer Services
Steven McCaughey	Land and Property Services
Sharon Muir	Account Manager (DAERA and DFI)
Aidan McMichael	Digital Transformation Service
Owen Murray	Digital Transformation Service
Information Governance and Innovation Board (IGIB)	Provides strategic governance for Information Technology, Information Assurance and Information Management,
Strategic Design Authority (SDA)	Sets standards, technical direction and approves technical design of ICT services.
Technical Design Group (TDG)	Provides technical advice, guidance and support to the SDA.

1.4. References

Table 2 details the other sources of information that is useful to understand the context of this document and overall goals of the digital services investments made so far and planned in Northern Ireland government.

Table 2: References

Reference	Title	Description	Author	Version	Date
1	System assessment information	Questionnaire based information on various systems that are used currently in government to deliver citizen services	Departments of Northern Ireland government, DSS	N/A	02/10/2018
2	Making Lives Better - A Strategy for Digital Transformation of Public Services 2017-2021	This Strategy sets out a Vision for transforming how NI Government works, which means that: ▪ People and businesses will be enabled to digitally engage with Government at a time	Department of Finance	N/A	2017

Reference	Title	Description	Author	Version	Date
		and place that suits them. - Government operations are digitally transformed to deliver effective and efficient public services; and - Government aspires to embrace digital in everyday public services to deliver better outcomes.			
3	ICT Strategy 2017-2021. Delivering better public services through Technology	This strategy sets a number of principles which include making best use of economies of scale and Shared Services; value for money procurement and flexible contract options; innovative training to lower identified staff skills gaps and the inclusion of security and assurance as part of ICT solutions	Department of Finance	N/A	2017
4	Cyber Security	A Strategic Framework for Action 2017-2021	Department of Finance		
5	National Cyber Security Strategy 2016-2021	National Cyber Security Strategy sets out plan to make UK confident, capable and resilient in a fast-moving digital world	HM Government		
6	Outcomes delivery plan 2018-19	Improving wellbeing for all by tackling disadvantage and driving economic growth	NICS		
7	Technology Code of Practice, Guidance	Guidance on set of practices to be followed	Government Digital Service	N/A	26/02/2018

Reference	Title	Description	Author	Version	Date
		when implementing digital service in government			
8	Digital Service Standard	The Digital Service Standard is a set of 18 criteria to help government create and run good digital services	Government Digital Service	N/A	Version available on 17/10/2018

1.5. Document Organization

This document is organized into multiple top-level sections and covers these topics:

- Introduction – provides context and positioning of the work associated with architectural blueprints, stakeholders involved and affected;
- Needs – defines the context of the work, defining strategic inputs, typical scenarios to be supported, defining architectural principles and constraints that are to be adhered to when implementing any citizen services, including common technical components provided by DSS;
- Architecture – this section of the document outlines the future set of capabilities required, assessment of the existing situation against the capabilities and future needs, identification of shared capabilities to be provided/owned by DSS, and priorities and initial architecture for top priority shared capabilities;
- Roadmap – outlines the initiatives needed to cover gaps in capabilities identified in architecture against the future state, defines proposed roadmap of implementation considering priorities, dependencies and alignment to work that is currently being done or being planned;
- Appendices – provides additional supporting materials for the readers of the document.

Given the continuous nature of enterprise architecture as a function, this document should also be considered a live document that is updated whenever needs or architectural approaches change. The roadmap should also be adjusted as initiatives are implemented or priorities change.

1.6. Intended Audience

Given the specifics of the document, it is intended primarily for:

- Enterprise architecture team and Solutions Architects in DSS to revisit and adjust the enterprise architecture of citizen services related shared services going forward, plan new initiatives and document their priorities;
- Enterprise and Solutions architects in other teams to learn:
  - about the principles and constraints of building department specific service and
  - how to leverage common services provided by DSS and roadmap of those services being provided;
- Vendors and delivery teams that are working on the implementation of the initiatives documented so that they have the context on how the capability supports broader citizen engagement and what are the architectural practices and constraints to follow.

2. Needs

This section details the identified needs for citizen engagement linked to strategic goals and technical and implementation principles to achieve both citizen visible functionality, but also ensure it is implemented in a sustained way promoting reuse and further enhancement. Specifically, topics covered are:

- Strategic context of citizen engagement defining "**why**" the changes required and future state;
- Current State Analysis – reviews of NI Citizens Service provision to date;
- Ethical principles and constraints to be followed to define stance on privacy and security elements of solutions;
- Architectural principles driving the vision of "**how**" solutions should be implemented and what they should be promoting technically and citizen engagement-wise;
- Architectural constraints defining the limits/restrictions that exist in the current environment;
- Business view documenting the summary of department needs and extracting common capabilities that are the primary subject of this architecture work;
- Quality attribute view to define important solution quality attributes solutions need to adhere.

2.1. Strategic Context

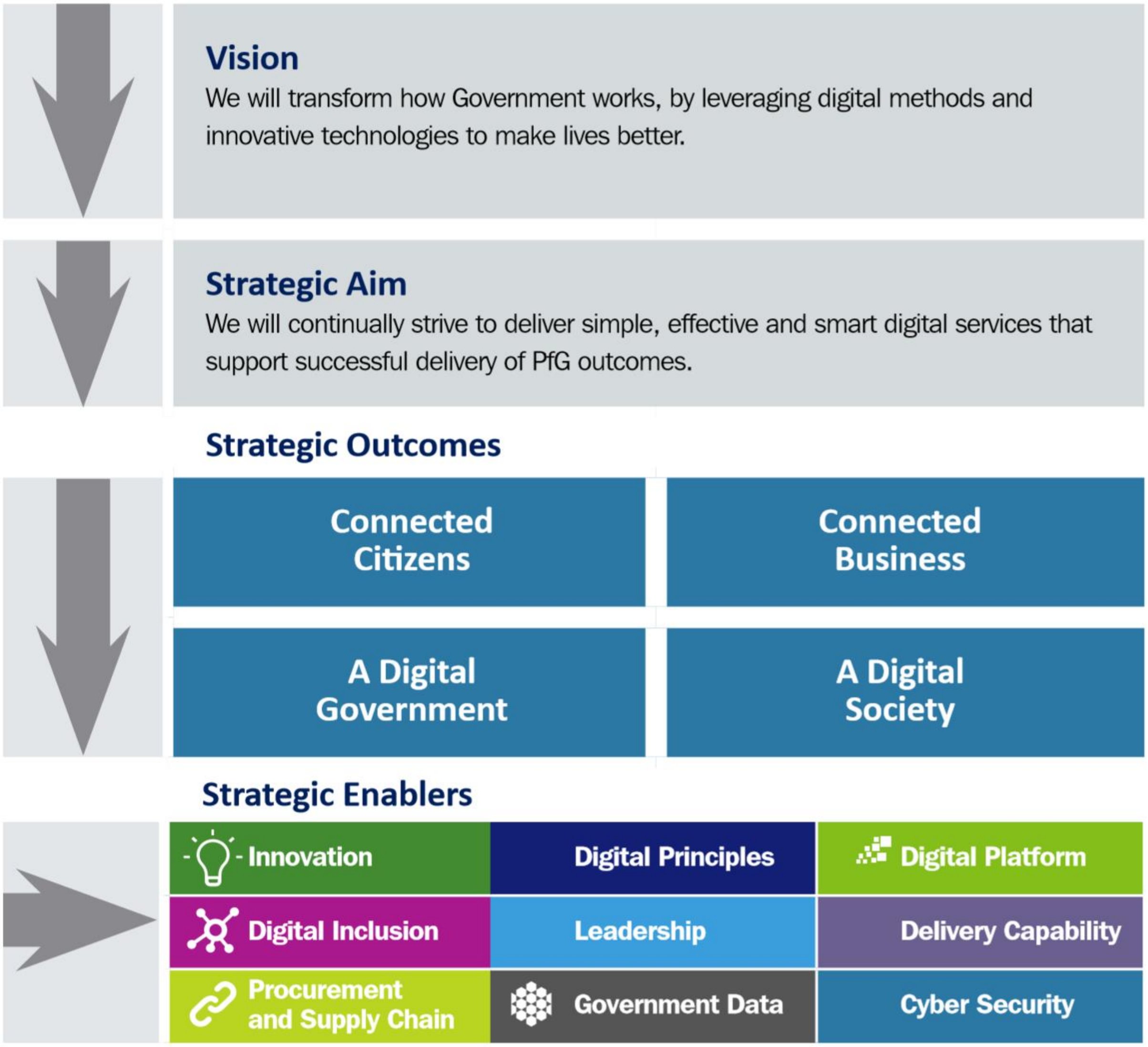
"Making Lives Better - A Strategy for Digital Transformation of Public Services 2017-2021" outlines the vision, strategic aim, strategic outcomes and enablers to digitally transform Northern Ireland (NI) Government (see Figure 1).

Drivers for ongoing transformation in NI referenced include:

- Rising citizen expectations;
- Delivery of Programme for Government outcomes;
- Technology Trends;
- State of Public Finances.

The work on enterprise architecture of citizen service enabling IT services (especially the shared services) described in this document supports all strategic outcomes by:

- covering the capabilities that are required in shared digital platform to help achieve the outcomes;
- defining architectural and security principles and constraints for all government IT investments related to citizen engagement;
- proposing a model for delivery of IT services going forward, adopting industry leading Application Lifecycle Management (ALM) and partner engagement models, driving more involvement and therefore full ownership of services within DSS teams throughout the IT service lifecycle.



Vision
We will transform how Government works, by leveraging digital methods and innovative technologies to make lives better.

Strategic Aim
We will continually strive to deliver simple, effective and smart digital services that support successful delivery of PfG outcomes.

Strategic Outcomes

Connected Citizens	Connected Business
A Digital Government	A Digital Society

Strategic Enablers

Innovation	Digital Principles	Digital Platform
Digital Inclusion	Leadership	Delivery Capability
Procurement and Supply Chain	Government Data	Cyber Security

Figure 1: Digital Transformation Strategy vision, aim, outcomes and enablers[1]

[1] See strategy document [2] for details

The "Northern Ireland Civil Service ICT Strategy 2017-2021 - Delivering Better Public Services through Technology" (see Figure 2 for strategy overview) has been developed to support the enablement of modern public citizen and business services through better use of technology, work processes and investment in staff. The strategy establishes several important drivers which have been identified as essential to delivering future change:

- Digital transformation agenda;
- Changing data and privacy compliance requirements;
- Changing Business Needs;
- Investing in infrastructure & Shared Services;
- Cyber Security;
- Collaboration working;
- Working within budgetary constraints;
- Programme for Government priorities.

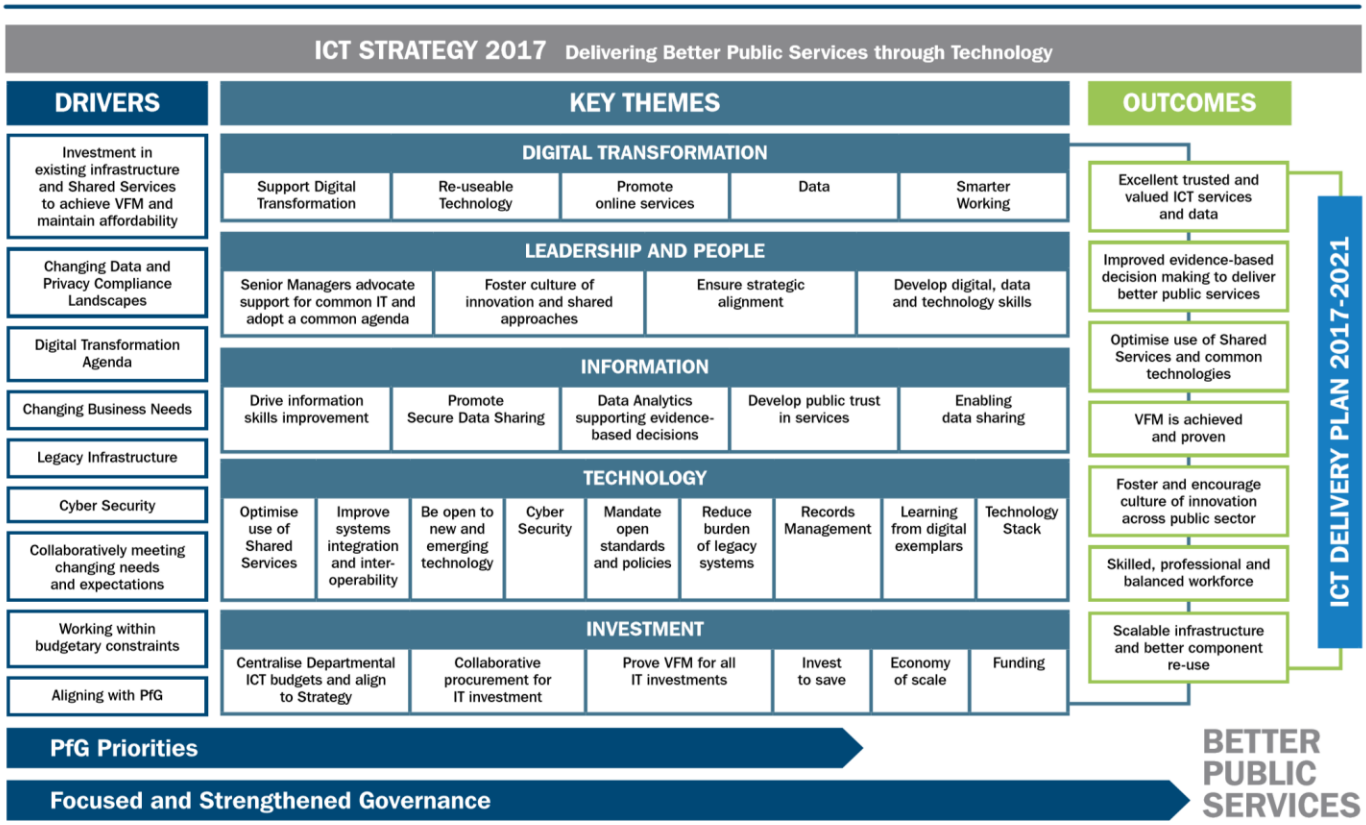

ICT STRATEGY 2017 Delivering Better Public Services through Technology
DRIVERS
Investment in existing infrastructure and Shared Services to achieve VFM and maintain affordability
Changing Data and Privacy Compliance Landscapes
Digital Transformation Agenda
Changing Business Needs
Legacy Infrastructure
Cyber Security
Collaboratively meeting changing needs and expectations
Working within budgetary constraints
Aligning with PfG
KEY THEMES
DIGITAL TRANSFORMATION
Support Digital Transformation
Re-useable Technology
Promote online services
Data
Smarter Working
LEADERSHIP AND PEOPLE
Senior Managers advocate support for common IT and adopt a common agenda
Foster culture of innovation and shared approaches
Ensure strategic alignment
Develop digital, data and technology skills
INFORMATION
Drive information skills improvement
Promote Secure Data Sharing
Data Analytics supporting evidence-based decisions
Develop public trust in services
Enabling data sharing
TECHNOLOGY
Optimise use of Shared Services
Improve systems integration and inter-operability
Be open to new and emerging technology
Cyber Security
Mandate open standards and policies
Reduce burden of legacy systems
Records Management
Learning from digital exemplars
Technology Stack
INVESTMENT
Centralise Departmental ICT budgets and align to Strategy
Collaborative procurement for IT investment
Prove VFM for all IT investments
Invest to save
Economy of scale
Funding
OUTCOMES
Excellent trusted and valued ICT services and data
Improved evidence-based decision making to deliver better public services
Optimise use of Shared Services and common technologies
VFM is achieved and proven
Foster and encourage culture of innovation across public sector
Skilled, professional and balanced workforce
Scalable infrastructure and better component re-use
ICT DELIVERY PLAN 2017-2021
PfG Priorities
Focused and Strengthened Governance
BETTER PUBLIC SERVICES

Figure 2 ICT Strategy 2017-2021 Overview

As part of the ICT strategy, cyber security has been identified as a key driver. Today's world reflects a new reality: technology is ever-present, and with easy access to digital services. The frequency and sophistication of cybersecurity attacks are increasing.

As outlined in the "Cyber Security – A Strategic Framework for Action 2017-2021" citizens, businesses and government all have their responsibilities to protect online services. The NI Executive has a commitment to deliver services with a high level of security and confidence for users of public sector citizens services and systems.

Security needs to be the forefront when considering the future infrastructure and development architecture for citizen services. It is also something that will continue to evolve and require ongoing review due to the emerging techniques being used.

2.2. Business View

The purpose of the NICS Digital Transformation programme is to provide higher quality public services in Northern Ireland. The Digital Transformation strategy will enable the further development of public sector digital citizen services to deliver Programme for Government outcomes through the increased usage of online channels to access public services.

2.2.1. Key Personas

Key personas involved in end-to-end citizen service delivery, the assessment of current solutions and needs for the future to achieve the citizen services and ICT strategic goals are defined in Table 3. Assessment of future needs is a synthesis of strategic outcomes and identified scenarios.

Table 3: Key personas, assessment of the current level of IT support for the service delivery

Persona	Description	Assessment of future needs
Citizen	Citizens are the primary consumers of the government services requesting information and tasks to be performed by government. Examples are services related person and family, e.g. birth registration, marriage details, education related services, property and vehicle related services.	▪ one government view ▪ access to unified and well-structured services information ▪ access to services over multiple channels ▪ providing feedback about service delivery ▪ personalized experience ▪ moving away from interactions over phone, in-person and using paper submissions, e.g., submitting and receiving digital documents in a secure way ▪ unified identity over all government systems to enable government to government cross-checks of information and implement only once (tell us once) principle ▪ accessing "my information" managed by the government to help in data quality and ensure citizens can view digital information on them ▪ accessing digital licenses/permits/certs to verify licenses/permits/certs issued to

Persona	Description	Assessment of future needs
		other (business) to introduce more self-service checks and to move to more digital overall environment
Business representative	Business representatives request/receive services from government related to the businesses and non-governmental organisations (NGOs) they represent. Examples include dealing with properties of the business, requesting various licenses and permits.	▪ one government view ▪ access to unified and well-structured services information for businesses and NGOs ▪ unification of interactions with government to reuse profile, delegation information, channels ▪ reduction of administrative burden via further simplification of processes via digitalization ▪ personalization (tailoring business experience)
Government Employee	Employees of departments, agencies and related organisations that are involved in providing services to citizens. Example interactions would include processing request cases, preparing the resulting changes in registries or documentation requested, communicating with citizens.	▪ designing and building services with citizen needs at the centre ▪ leveraging technologies to most of their potential in government processes ▪ culture of innovation and collaboration throughout organisations ▪ planning incentives to encourage citizens in society to take advantage of leading-edge digital services
Government Employee: Executive	Leads government teams, agencies/departments that plan evolution of their citizen services, prioritize investments into citizen service improvements, oversee the process of providing citizen services.	▪ being able to target resources on digital transformation initiatives that would make significant difference ▪ eliminate waste through efficient use of technologies, enable faster change
Non-resident	Citizens of foreign countries requesting and receiving services in Norther Ireland, e.g. EU citizens.	Not prioritized at present. The approach to be revisited after Brexit and also when aligned with Tourism NI.
Internal developers building government systems	Internal and contracted developers building IT systems to provide citizen services electronically or support providing	▪ more agility in building out new services and improving existing ones ▪ better time to market for citizen services leveraging latest platforms and approaches

Persona	Description	Assessment of future needs
	citizen services through automating business processes.	
External third-party developers	External developers that are building third party systems for citizens or businesses that might need to interact with government or use data published by government.	▪ access to government shared data sets to reuse in own solutions ▪ access to government APIs enabling integration of government functionality into own solutions, e.g., ERPs.

2.2.2. Scenarios – Inflight and Planned

At the time of writing, a full pipeline of citizen related projects across all departments was unavailable. DSS were working on developing a list from information requested from various departments and other public sector bodies.

MS completed an assessment of the available inflight and planned citizens services during workshops to establish an initial understanding of the common themes across services. A list of the available inflight or planned services is provided in Appendix 5.2

2.2.3. Current State Analysis

During the initial scenario discovery workshops DSS and MSFT reviewed the delivery of the initial NI Citizen services (known as '16x16') plus in-flight/planning projects. Stakeholders shared what they considered worked well and could be improved on from an architectural perspective.

The following are some of the key observations:

- A portfolio of projects for citizen services have been delivered successfully but the approaches were often siloed and inconsistent. This often resulted in duplication and lack of re-use was evident;
- Much of the delivery of Citizen services was by external suppliers – minimal skills development for internal resources;
- Future pipeline of work from across government departments is unclear (information requested from departments is being collated by DSS); many departments have their own digital strategy;
- There is currently no Enterprise Architecture function (as described in this document) across NICS;
- The current DSS architecture function is mostly reactive in terms of engagement with business;
- Broadly, architectural engagement is fragmented across departments;
- Architecture involvement through application & portfolio assessment is absent or often considered too late in the process;
- Whilst currently lacking a strong architecture function, there is a clear appetite from stakeholders across the business to establish a performing Enterprise Architecture function;
- The establishment of an Enterprise Architecture function will require senior stakeholder support and investment.

2.2.4. Common Themes Across Scenarios

The following are some of the common themes extracted from inflight and planned citizen services.

- Data sharing within government and with 3rd parties;
- Enabling omni-channel access;
- End-to-end digital information exchange;
- Secure messaging with the citizen;
- Identity requirements are evolving;
- Notifications;
- Case management;
- Move towards a personalized citizen experience;
- Analytics, insights.

2.3. Ethical Principles

An important aspect to achieve digital inclusion is to ensure that all citizens benefit from the digital transformation of service delivery regardless of the preferred way they access government services or interact with government.

This subsection defines principles to follow when planning and implementing platforms and e-services solutions to ensure accessibility of services and overall inclusion. Each new solution/service needs to be evaluated against the categories defined in the list below.

Categories and specific ethical principles to follow for any systems providing citizen services are:

- Fairness
  - When implementing automatic classification algorithms, decision support systems, algorithms implemented should be tested for potential bias (commonly known as a problem in machine learning based evaluation algorithms for loan application, social security applications etc.);
- Inclusion
  - Citizen service implementation should consider providing various engagement channels, including support for non-digital engagement to ensure all categories of citizens are supported;
  - Pricing of services provided online vs. in-person should not have a different price for the base service; additional pricing can be required for additional value-add services, e.g., delivery results via courier delivery warrants additional cost regardless of in-person or electronic service request submission;
- Transparency
  - Automated decisions made in the system need appropriate reasoning (trail of evidence) preserved and exposed to users as well;
- Accountability
  - Each service should have an owner through its entire lifecycle – someone in a department responsible for the initial delivery and ongoing enhancement of the service, through to de-commissioning;

All the DSS owned IT services and platforms supporting public servants delivering citizen services should be promoting/supporting general NICS Code of Ethics:

- ‘integrity’ is putting the obligations of public service above your own personal interests;
- ‘honesty’ is being truthful and open;
- ‘objectivity’ is basing your advice and decisions on rigorous analysis of the evidence; and
- ‘impartiality’ is acting solely according to the merits of the case and serving equally well Governments of different political persuasions.

2.4. Architectural Principles

Architectural Principles are long-lasting and rarely changing statements and guidelines that govern the design, implementation and operation of the solutions. They are derived from the specific needs and priorities of the stakeholders and provide a decision-making framework for the architecture that govern its construction.

A list of architectural principles defined in this section are the ones to drive architectural decisions for any citizen facing e-service or service delivery supporting platform implementation in Northern Ireland government. Architectural principles can cover approaches at various levels of “depth” – some of them relate to the design process/approach, some to deployment platforms to be targeted, some are technical principles that drive implementation of the solution in a certain way, i.e., using certain patterns.

Architectural principles for Northern Ireland have two sections:

- General principles that are derivation of technology code of practices (see [6] in Section 1.4) and digital service standards (see [7] in Section 1.4) of gov.uk;
- Northern Ireland specific additions to the list of principles, going into more specific details or requirements related to shared service use provided by DSS.

Table 4 details the Architectural Principles that govern implementation of citizen facing service delivery systems and elements of back-office systems that participate in service delivery.

Table 4: NI specific general architectural principles

#	Architectural Principle	Rationale/Source	Implication
AP1	Maintain your service catalogue	It is important to provide unified structured service catalogue regardless of the department providing the actual service so that citizens or business representatives get unified experience of finding and launching the services they want to consume from government.	Leverage common service catalogue management whenever there are new services or changes to services delivered to citizens or business representatives
AP2	Leverage public cloud capabilities (where appropriate)	To modernize approach of building and hosting government solutions, gain benefits of on-demand infrastructure provisioning and scalability, ready-made platform as a service component, public	When architecting and designing solutions to support citizen services delivery, public cloud technologies and hosting

#	Architectural Principle	Rationale/Source	Implication
		cloud hosting should be assessed as default choice.	approach should be considered as default. This also means that hybrid solutions leveraging new public cloud capabilities while accessing existing private cloud and on-premises systems/services should be default end-to-end model for the service implementation.
AP3	Manage IT service documentation and configuration centrally	Having documentation and configuration maintained in a shared repository enables better understanding of services to be maintained, also allows for more openness when services need to be extended in future. Also, this approach ensures that there is a responsible party for maintaining all documentation and it does not get lost. For guidance on structure of what content needs to be maintained for any system/service, see Appendix (5.2).	Leverage DSS maintained shared configuration and document repository
AP4	Track and expose usage information	Important element in evolving services, learning what is working, what is not, is tracking usage of the services, user behaviour patterns, platforms used to access the service (e.g., mobile vs. desktop use). Therefore, each service needs to track the usage both by anonymous as well as logged in users, expose this usage information in reports/dashboards for service owners.	Leverage common service for tracking service/platform usage related events
AP5	Track service delivery status	Citizen centric service delivery means that citizens get information on status of their service delivery, they and call centre employees can see the history of previous service requests. To accomplish this, each service delivery process needs	Leverage common service delivery history service

#	Architectural Principle	Rationale/Source	Implication
		to track and share centrally information about progress of service delivery.	
AP6	Expose APIs, queue messages	One of the biggest challenges in citizen service delivery is standardized exchange of information to ensure that the same approach is used by a single service to get functionality or data from systems in different departments.	When building systems, or new services, expose any public functionality via APIs or queues and communicate with other services using message queues (where possible) or API calls (where sync exchange of data required)
AP7	Use centralized identity/federation providers	Good user experience requires users not to be prompted for user credentials multiple times and for sure not to require different credentials and accounts to access different services of the same government. This is true for both citizens accessing services and government employees accessing systems to provide those services.	All citizens and business representatives should have a single identity hub securing access to all non-anonymous services provided by government. All government internal systems accessed by government employees or other government systems should leverage single identity hub (single identity or federated).
AP8	Follow UX guidance	As per more high-level principles understanding the user needs is key to defining well thought out approach for providing a service. General UX guidance and specific UX trained resources can help in ensuring unified citizen experience even when set of services are built separately by different teams.	Follow the UX guidance provided by DSS team, reuse visual assets and guidance, involve DSS UX architects in defining the approach.
AP9	Follow secure development guidelines	Many of today's attacks on services exposed on internet are happening via application not infrastructure layers of the overall solution. Following secure development process ensures risks are minimized.	Follow existing secure development and IT service delivery guidance defined in UK, specific additions defined in NI.

#	Architectural Principle	Rationale/Source	Implication
AP10	Leverage feature flags	Often IT platforms, especially those hosting multiple services often have additions. Adopting always on and always running approach for running a service requires these services to be added over time to a limited set of beta testers first and then to be opened. Feature flags ensure this approach.	Leverage common feature flags service provided when implementing own solutions that will evolve over time and will have features arriving as they are adopted by back office teams.

Platform specific Architectural Principles that need to be adhered to when building reusable platforms intended for other development teams are defined in Table 5.

Table 5: NI shared platform specific architectural principles

#	Architectural Principle	Rationale/Source	Implication
AP11	Ensure multi-tenancy support	Platforms are systems that are used by multiple user groups, e.g., different department teams, each providing a specific scenario while reusing horizontal functionality. Given different teams from different departments are using those solutions, platforms need to ensure proper segregation for clarity but also data security purposes. E.g., case management platform supporting many case management solutions should support different teams working with them and not interfering with each other, and not seeing each other's data.	Platform testing should include test cases showing how multiple separate teams can leverage platform without interfering.
AP12	Ensure citizen multi-channel support	Given that citizen interaction needs to be often provided over multiple interaction channels (e.g., portal, mobile), platforms need to be designed with this approach in mind and that the platform is disconnected from citizen channel used.	Platform implementation should expose citizen facing functionality via APIs and queues, not specific UI.
AP13	Expose functionality for departments as APIs	Automation of entire processes (including backend) is an important driver of service delivery efficiency. It helps with the reuse of existing functionality in existing department systems.	Any platform implemented should expose specific government functionality as APIs.

#	Architectural Principle	Rationale/Source	Implication
			For example, platform service of sending notifications should expose APIs for other government systems to send notifications to citizens and get updates on the status of notifications sent.
AP14	Document for developers extensively	Platforms are used by other developer teams building their systems and reusing platform capabilities. Having a well-documented platform is the key for its adoption.	When implementing platform consider extensive documentation targeted at developers as a priority. Consider hackathons and training sessions. Implementing COTS platforms should be considered a priority where possible as they have documentation for developers maintained by ISVs providing the platform.
AP15	Ensure multiple development teams can add new “scenarios”	Platforms are not only used by multiple government teams, but their configuration should be possible by multiple development teams to keep the implementation free of vendor lock-ins.	Ensure part of platform acceptance includes checks for other developer teams using the platform – starting with documentation and ending with test environments.

2.5. Architectural Constraints

The Architectural Constraints are derived from specific stakeholder dictates and govern its construction by defining items with which it must comply or otherwise consider.

Architectural constraints are more precise than the architectural principles. These are things where there is no option to interpret them.

Table 6 details the Architectural Constraints that govern the citizen services enabling solutions.

Table 6: Architectural Constraints

#	Architectural Constraint	Rationale/Source	Implication
AC1	Employee identity management source is Active Directory exposing OpenID Connect and SAML-P endpoints	At present NI government is leveraging Active Directory as the source identity management solution for government employees. Active Directory Federation Services is used to federate-in partner employees requiring access to government systems.	Active Directory and solutions depending on its data should be used as the employee identity source going forward as well. SAML-P to be used as most prominent protocol for authentication in enterprises – all employee facing solutions exposing UI should be leveraging SAML-P or OpenID Connect as authentication protocols.
AC2	REST based APIs exchanging JSON documents are the message/document exchange approach	Both public solutions as well as solutions within organisations are nowadays leveraging REST based APIs that leverage JSON data objects as it is a lightweight approach well suited for a mobile-first world. They technically and semantically support well defined API taxonomy of the data/functionality provided by the government.	Solutions exposing APIs should do so leveraging REST and JSON.
AC3	Citizen (external) identity management is based on OAuth/OpenID Connect	To enable a lightweight and mobile first environment, enable integration with public identity providers like Google, Facebook and Microsoft modern identity protocols should be leveraged.	OAuth/Open ID Connect to be used as the most prominent authentication protocol for citizen facing services.
AC4	Centralized content management platform is Drupal	NI Government has significant skills and technology investments in Drupal for managing public and internal content management sites and their existing service catalogue.	Any solution component requiring content or service catalogue-based functionality should be built using Drupal. Functionality should be front-end with custom APIs to reduce risk of lock-in.

#	Architectural Constraint	Rationale/Source	Implication
AC5	DSS manages custom-built services	Outsourcing custom tailored solutions to external providers causes a risk of lock-in and limited amount of innovation by having multiple teams working on the solution over longer lifespan of the service.	DSS should be managing and supporting custom built, tailored solutions, they should not be outsourced as managed services. External managed services can be those that are ready-made community services not requiring customization, only configuration.
AC6	Solution security should adhere to government-wide standards	Information security is critical in the digital age. Therefore, all citizen facing solutions need to adhere to appropriate government policies related to IT security.	GOV.UK ▪ Security Policy Framework ▪ Security by design NCSC ▪ NCSC guidance ▪ NCSC Guidance on Making services hard to compromise General ▪ OWASP Top 10 Most Critical Web Application Security Risks ▪ ISO27001 and ISO27002
AC7	Monitoring/management should leverage a common hybrid solution	Running a distributed, hybrid IT environment introduces challenges of it being managed efficiently. Adherence to the same monitoring/management approach by all solutions is therefore critical to ensure uninterrupted services.	When building new systems to support citizen services, they should be leveraging a common hybrid monitoring and management approach defined by DSS

2.6. Quality Attribute View

Quality Attributes refer to cross cutting concerns that affect many elements of the solution and addresses:

- Usability and Accessibility;
- Security and Compliance;
- Availability and Reliability;
- Extensibility;

- Manageability, Maintainability and Supportability.

In the context of this document and describing the enterprise architecture of the citizen facing components/solutions/services, this section focuses on the general rules to enforce a consistent implementation of common quality attributes. The intention of this section is not to describe specific requirements for each of the solutions/components involved in providing citizen services.

2.6.1. Usability and Accessibility

Usability and accessibility cover multiple aspects that make sure solutions are more approachable by their users. Each of these aspects together with relevant guidance are described in this list:

- Accessibility
  - The Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018
  - GDS Guidance
- Assisted digital
  - Assisted digital guidance
  - Additional GDS guidance: assisted digital support introduction
  - Additional GDS guidance: designing assisted digital
- Usability
  - NIDirect UXM
  - NIDirect principles
- Personalization
  - each citizen should manage their main contact information and personal details that are common across all departments and agencies of the government in a single profile; there should be no need for multiple credentials, multiple places to enter and validate e-mail addresses etc.

2.6.2. Security and Compliance

Quality Attributes for Security and Compliance and common guidance for citizen facing systems and platforms are:

- Confidentiality: each of the common platforms developed should ensure data access is walled by institution (government department) and provided only based on users belonging to the institution and a clear and well defined legitimate need to access the data;
- Privacy:
  - solutions providing citizen services should be explicit about any personal data that is used and should explain how that data will be used and stored;
  - access to citizen data should be granted only to citizens themselves or their delegates and to institutions (e.g., government departments and their agencies) serving a citizen request;
  - handling of personally identifiable Information (PII) should follow local and international standards (e.g., GDPR that applies for all EU users of the solution, e.g., potential investors using solutions as business representatives)
- Integrity: data integrity and prevention of data manipulation should be achieved by system components performing auditing of all critical data changes in the system;

- Legitimate use: legitimate use of functionality should be enforced by solutions providing citizen services through access control based on identity of the government employees and their security roles granting access to limited functionality only;
- Accountability: accountability and tracking of actions to users that performed them should be achieved in the citizen facing solutions by auditing important activities performed by citizens or government employees, or systems of departments.

2.6.3. Availability and Resilience

There are three types of services that are often participating in the delivery of citizen services:

- common platforms hosting other services, e.g., a citizen portal platform that is integrated and hosts multiple forms of specific services;
- common services that are used by many other services as part of service delivery, e.g., notification service or citizen profile service;
- specific services that provide specialized functionality or workflow management and is leveraged only in a specific service.

When designing one of the above new service types, availability and resilience requirements should be defined individually. However due to the impact of reused services and platforms, a general rule is to have higher availability and resilience targets for reused services because they impact downstream availability of the services using them.

Specific principles to be considered by default and to follow when implementing common platforms and services to achieve high availability and resilience are:

- design loose coupling of services, prioritize interfaces that are asynchronous, leverage processing queues;
- host solutions in locally highly available hosting environments (e.g., two datacentres distributed in the same geo-area – less than 100 km apart) ideally in an active-active configuration to sustain single data centre failure;
- implement event tracking integrated with hybrid monitoring solution;
- leverage front-end gateways/components that can support limits to throttle access to services.

2.6.4. Performance and Scalability

Citizen facing solutions are intended to be used by residents of the Northern Ireland and visitors/investors. Therefore, citizen facing solutions from an overall data and load scale guidance perspective should target a maximum of 2 million users. Note that each service due to its specifics and applicable audience (e.g., exposed only to business representatives) should appropriately adjust scale targets both for load (simultaneous and peak load) as well as for data amounts (depend also on retention policies for data that component operates with).

Specific principles to be considered by default when implementing services leveraging IaaS and PaaS hosting environments (does not apply to SaaS where external provider should ensure scalability) are:

- enable and test scale-up of the solution (handling more load increasing size of the hosting infrastructure);

- enable and test scale-out for all components of the solution (handling increased loads by adding additional resources of the same type, scaling down when loads decrease);
- implement scale-out using scale units defining specific baseline load that each scale unit can handle;
- run performance tests, measure end-user load times assuming different access channels used by citizens (3G, 4G, broadband);
- trace performance related metrics for insights into service load and analysis of load patterns.

2.6.5. Extensibility

Citizen services are provided by multiple departments and agencies of the government. These services often have the same process elements (browsing service catalogue, request, getting status updates, processing workflow, getting results). To optimize the investments and to ensure a better user experience, an overall approach for citizen services should rely on common capabilities reused across the service landscape.

There are two levels of reuse:

- reuse of common ready-made services, e.g., using the service delivery status tracking so that citizens get updates in a unified way through portal/mobile and notifications;
- reuse of common platforms to build out new services (services elements) easier/faster, e.g., using e-forms engine to develop and host e-forms in a portal without custom coding and call backend APIs based on metadata defined in service catalogue.

Details on how extensibility therefore is achieved depends on those two different reuse types:

- extensibility of ready-made services is achieved through registering any new client application which uses them and ensuring re-use of those services when building an overall solution;
- platform extensibility is allowing:
    - multiple different institutions to use the solution for their needs (e.g., case management solution used by different institutions to handle their specific cases) without affecting each other;
    - multiple development teams to build new solution elements following common developer guidance (e.g., publishing APIs for data and functionality sharing, creating new custom workflows for processing citizen requests).

See Table 5 for details on what platforms should support to drive platform extensibility and prevent lock-in.

2.6.6. Manageability, Maintainability and Supportability

Given that investments in service delivery supporting IT are long-term investments, solution approaches should ensure that the configuration/customisation elements of the solutions, including documentation, are maintained well and are easy to access and change in a controlled manner. Given recent DevSecOps developments, this should be supported with automated processes for testing and deployment as much as possible.

To enable good day to day management of the solution and enable planning service improvements, any service or platform should follow this general guidance:

- track technical solution related events, especially ones related to warnings and errors affecting the health of the solution/service;
- leverage hybrid monitoring solutions provided by DSS to strive for a single pane of glass monitoring approach;
- track business events providing insights into how a solution is used, when and by who;
- prioritize the use of platforms and technologies that provide automated management capabilities (management APIs) and implement service specific management APIs so that management tasks can be automated.

3. Architecture

This section details the enterprise architecture of the common elements and approach for supporting citizen services delivery and makes use of these architectural views:

- Capabilities describes:
  - all technical capabilities that are required for providing citizen services, describing their expected future state given the needs identified in section 2;
  - subset of common capabilities that are core for a unified citizen experience and for driving more IT reuse, therefore a focus for DSS;
  - assessment of the capability current state against the functional and non-functional (approach) requirements/vision;
- Application Architecture View:
  - defines the services to support the common capabilities and platforms to support the easier development of new e-services in a consistent way;
  - identifies services exposed to external partners building their own service delivery solutions, yet wanting to leverage solutions and components of others to provide a better citizen experience and more digital processing of internal workflows;
- Information View defines information assets ownership with a focus on those information assets that would be of particular interest to other departments across government or to citizens directly, with the goal of improving citizen services or information availability to citizens;
- Development & Operations Lifecycle View defines the suggested approach for sustainable development, management, maintenance and evolution of solutions;
- Infrastructure View outlines the main infrastructure and solution hosting elements/approaches that need to be introduced for modern solution development and hosting, ensuring public cloud environments can be leveraged efficiently for the benefit of faster service implementation and scalability;
- Security View defines security approaches to use when implementing the overall solution and specifically common capabilities across the infrastructure solution proposed;
- Governance View defines a proposed enterprise architecture function that is required to proceed with the work of controlled and sustained implementation, maintenance and evolution of citizen facing solutions in Northern Ireland government.

3.1. Capabilities View

This subsection provides an overall list of citizen services delivery capabilities and the planned future state based on outcomes of DSS and MS workshops and envisioning sessions, as well as an analysis of strategic goals and needs arising from current approach of managing the citizen services platforms.

It then identifies the common capabilities that DSS already provide as shared services/platforms and the ones that need to be provided by DSS to optimize and speed up delivering e-services in a citizen focused way across the government. The implementation gap against the required future state is provided as well.

3.1.1. Citizen Service Delivery Capabilities

The list of capabilities that are already used in NI government across various departments and the ones that are required to provide services based on the needs identified as part of assessment, also based on similar solutions in other countries is schematically shown in Figure 3.

Figure 3 uses colour coding to depict the capabilities that are considered more core (green and light blue) that are used/needed in almost any e-service and capabilities that are more optional (dark blue). As with any capability map, some of the capabilities are more enablers and used by government internally, whilst some are the ones directly leveraged by citizens and residents consuming the services.

Each of the capabilities mentioned represents potentially multiple services working together to provide the capability to employees or citizens. Details on each capability and the value it provides in the overall citizen service delivery environment for citizens or government employees is described in Table 7.

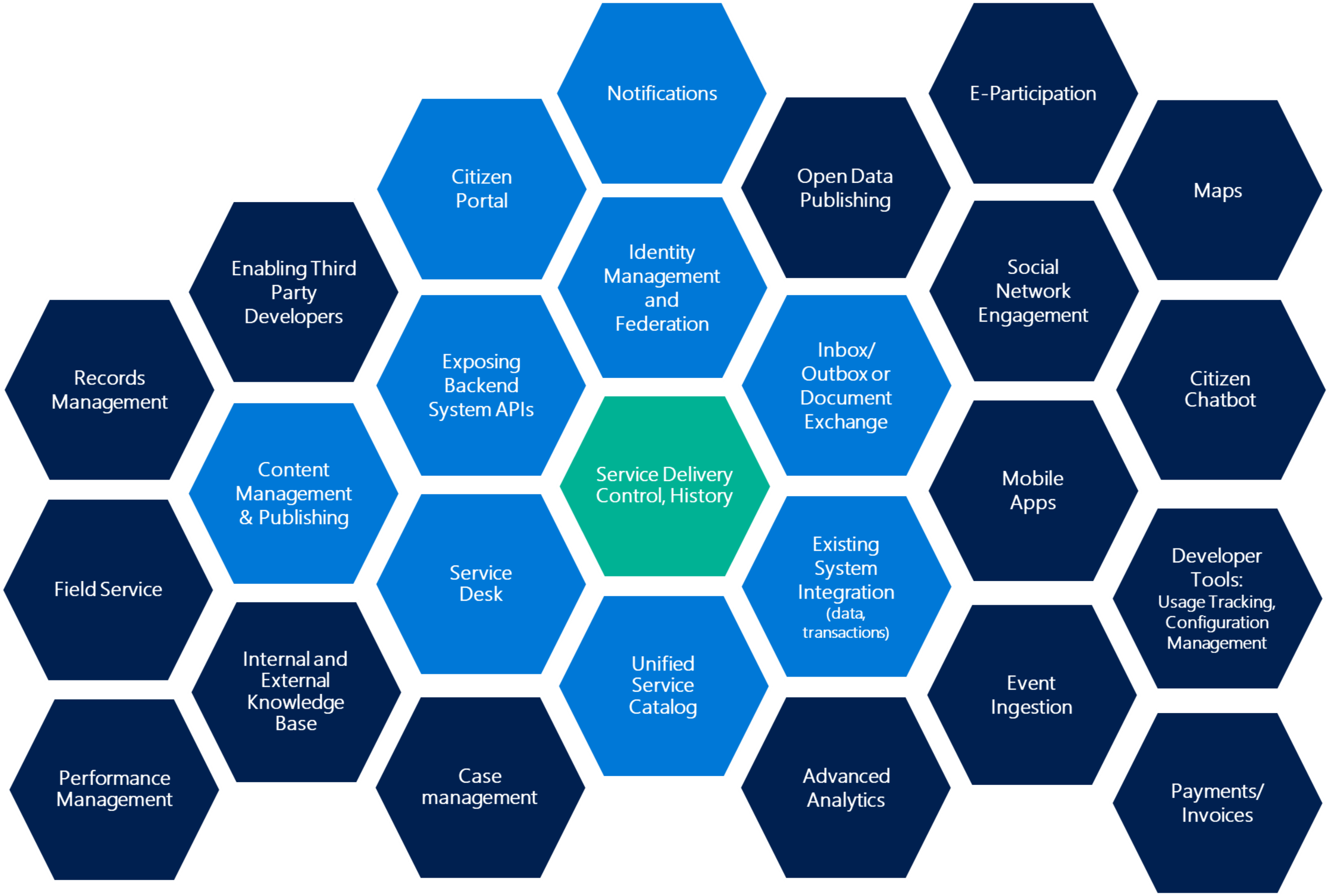

Notifications
E-Participation
Citizen Portal
Open Data Publishing
Maps
Enabling Third Party Developers
Identity Management and Federation
Social Network Engagement
Records Management
Exposing Backend System APIs
Inbox/ Outbox or Document Exchange
Citizen Chatbot
Content Management & Publishing
Service Delivery Control, History
Mobile Apps
Field Service
Service Desk
Existing System Integration (data, transactions)
Developer Tools: Usage Tracking, Configuration Management
Internal and External Knowledge Base
Unified Service Catalog
Event Ingestion
Performance Management
Case management
Advanced Analytics
Payments/ Invoices

Figure 3: Citizen service delivery main capabilities

A description of capabilities and their future envisioned state based on strategic guidance and workshop results is provided in Table 7. Future state is envisioned to have achievable goals, but not focused on a specific end date. The roadmap of achieving some of the future state requirements is presented in section 4. Note that some of the capabilities that are closely related are described in this table together. Also please note that the future state could match the current status achieved already for some of the capabilities (the gap analysis is provided in section 3.1.3).

Table 7: Capabilities and their planned future state

Capability	Description and Reasoning	Future State Required
Service Delivery Control, History	**This capability enables control of citizen access to all services and tracking the history of services used/requested and their current delivery status.** This capability is one of the foundational elements of service delivery enabling one place for insights into service delivery for citizens receiving services, but also for government (e.g., service desk) that needs to see all interactions of citizen with government departments when handling their request. Also tracking information can be used to measure service delivery quality as the capability tracks actuals of service delivery that can be contrasted against committed or defined SLAs. This gives executives insights into investment areas for future service expansion/improvement.	▪ Details of service delivery status changes tracked ▪ Service start and status change dates, including completion captured to enable SLA compliance measurements and optimization ▪ Service delivery quality/status reports for executives at departments and government wide ▪ Having different SLAs for the same service delivered via different channels (in-person, web, over phone)
Unified service catalogue	**This capability allows unified management of catalogue of all services (not only e-services) provided by the government. Each service belongs to the institution providing it, defines SLAs for the service and channels over which the service is available.** Citizens benefit from this capability by being able to get full information on all services provided by government regardless of the department and regardless of the transaction type (channel). Unified service catalogue enables also tracking and measurement of service delivery	▪ Managed by all involved institutions – departments (initially), agencies, municipalities ▪ Any services managed within the catalogue, not only e-services ▪ All channels supported: ○ In-person ○ Over phone/fax ○ At home ○ (snail) Mail delivery ○ Courier delivery ○ E-mail ○ Portal ○ Mobile App ○ Chat bot

Capability	Description and Reasoning	Future State Required
	quality as described through the Service Delivery Control/History capability.	○ Social networks ○ API (G2G and G2B) ▪ Service types: ○ Informational – providing information as is or based on citizen request (priority 1) ○ Transactional – performing action requested by citizen (priority 1) ○ Data sets – sharing G2G or G2C data sets from government systems (priority 1) ○ Notifications – providing notifications to citizen on status changes, action to be taken (priority 2) ○ Subscription – providing services proactively based on citizen identifying interest in specific area, e.g., sending out property tax notices (priority 3)
Identity management and federation	**Capability providing both citizen and employee identity management, and profile management in unified way. Ensures citizens and employees do not need to use multiple credentials to access to various systems within the realm of providing citizen services. Enables management of citizen personal details (e.g., contact information) in single place.** One of the core capabilities that, if implemented well, can simplify access to government services and limit the perception of siloed government institutions.	Citizen identity and profile: ▪ Identity sources: NIDA, UK Verify, banks ▪ Single ID maintained within the capability for each user, business that gets dispersed over time to all institutions to introduce single ID for each user to enable G2G integration ▪ Business representation maintained only through validated ownership of business via integration with UK government legal entity registry – HMRC (via Government Gateway) ▪ Support for foreign nationals over time (EIDAS, …)

Capability	Description and Reasoning	Future State Required
		Employee identity and profile: ▪ Managed via centralized identity management solution with source data residing in Active Directory ▪ Partner identities can be federated in to have access to government systems as well in controlled manner ▪ Permissions managed via claims associated with employee identity Priorities: ▪ Residents ▪ Login via other trusted providers (banks) ▪ Resident right delegation ▪ Foreigner support ▪ Business representative support ▪ Business right delegation
Existing system integration and Exposing Backend System APIs	**Capability is one of the core enablers of 'only once' principle in citizen interactions because it supports management of exposing government APIs to other internal (G2G) and external (G2B) users. To enable that capability, it includes a unified system to system authentication and authorization approach and management of API versions, revisions, subscriptions of users.** For example, to validate if a citizen has previous social benefits when evaluating health service access, a Department of Communities' API could be queried without asking the citizen to bring in a certificate from Department of Communities. Certificates and licenses can be fully eliminated if all data is exposed G2G or even G2C.	▪ Priority audience – G2G ▪ Main scenarios – check single record, get list of code table entries, publish/subscribe to change event (not replication of millions of records every day) ▪ Integration standardized and enforced via central API hub ensuring single security approach and unified taxonomy/technology ▪ System identity management required as part of the capability implementation ▪ Developer documentation focus critical to facilitate service reuse

Capability	Description and Reasoning	Future State Required
Content management and publishing, knowledge management	**Capability enabling information about government events/structure etc. published. Also contains knowledge articles in knowledge base that can be queried by employees or exposed externally to citizens for self-service.** Given the drive for the citizens perception of a single government, this capability should be leveraging the same content types being exposed regardless of the department publishing information.	▪ Central content management solution populated by all departments involved ▪ Central knowledge base with option to have external and internal articles maintained by all departments and leveraged by service desk and various self-service solutions ▪ Communication strategy (tone of voice, taxonomies) to be defined by content management group
Inbox/outbox aka Secure Messaging	**Capability provides a fully digital document exchange between citizens and government in both directions (upload by citizen or sharing by government).** Potential savings implementing this capability due to the reduction in need for delivery of printed messages to citizens that have been onboarded. This capability can be further exposed to have single channel for document delivery where based on citizen access to platform it gets delivered either electronically or printed out and delivered via snail mail (hybrid).	▪ Digital only first, hybrid delivery lower priority ▪ All departments leverage the same service ▪ Single inbox/outbox for citizen ▪ Departments have workplace to access their inbox/outbox ▪ Departments can integrate their existing document/records management solutions via APIs exposed
Notifications	**Capability enables citizen to receive notifications (on status change, action to be taken) from government.** Having a single source of notifications for all government notification communication promotes perception of single integrated government, simplifies interaction.	▪ The same/style/brand for notifications from any government department ▪ Channels: e-mail, SMS, snail mail, mobile push notifications, chat bot messages ▪ Message merging support for FYI messages (e.g., delivered once per week/month as digest) vs. action messages (delivered immediately)
Service Desk	**Capability to handle any problem reports/complaints by citizens on using the solution or accessing services (especially unattended ones).**	▪ Centralized service desk used by service desk/customer service organisation

Capability	Description and Reasoning	Future State Required
		▪ Access to full customer service delivery history (audited) ▪ Generic service delivery for some of the services ▪ Access to internal knowledge base and tracking knowledge base use in supporting customer
Case Management	**Capability enables IT support for the government services that require a combination of automated and manual actions to take place based on predefined workflow.** Often implementation of workflow-based services also includes these aspects: ▪ Business rules management ▪ Integration into backend systems for automation of some of the workflows steps ▪ SLA management ▪ Support of multiple teams involved in overall process of handling a case	▪ Structured case management with controlled workflow ▪ Escalation support, reassignment ▪ Extensions to support integration (e.g., step of verifying citizen information in another government system via API call) ▪ Support for access to case management through unified employee identity management ▪ Insights into service delivery history of the requestor ▪ SLA tracking ▪ Audit support
Citizen Portal	**Capability provides the main interaction channel for citizens accessing information published by government – content and service catalogue – and the channel to initiate e-services.**	▪ Mobile first implementation approach supporting responsive design ▪ Unified portal to manage content, service catalogue, integrated functional modules and even specific e-services. ▪ Hub for common citizen facing functionality like profile management, identity, notifications, subscriptions ▪ Common UX library shared to other portal builders ▪ Multiple specialized portals requiring dedicated infrastructure/solution, e.g., health portal ▪ Support for Single Sign-on navigation to external sites

Capability	Description and Reasoning	Future State Required
		providing e-services, e.g., Health portal - Elements to simplify adding new services, e.g., eForms, payments integration
Citizen mobile apps	**Capability providing access for citizens to e-Services via smart phones.** Compared to the portal channel, this can provide a more functional experience, especially when linked to camera usage, GPS and other mobile specific sensors/capabilities.	- Central hub app that provides common functionality – identity, notifications, profile management, service catalogue - Integrated e-services into hub app for services reusing integrated extension mechanism - Common UX library shared to other mobile app builders - Multiple dedicated apps providing specialized functionality tailored for e-service provided
Open Data Publishing	**Capability to expose data sets shared by backend systems more broadly with the public, providing reports on top of open data for additional insights into the data sets shared.**	- Machine readable data sets - Reports using data sets shared and other public data sets to share information in rich way for interested parties to gain additional insights - Integration with overall service catalogue to have single source of government services, even for these services of publishing data sets
E-Participation	**e-Participation capability enables citizens to participate more actively in government decisions, influence them via digital media before decisions are made.**	- E-consultation for new regulations - Polls and Surveys - Controlled public discussions
Social Network Engagement	**Social network engagement capability enables citizen interaction with government over social networks – publishing information, replying to enquiries and managing more complex requests from citizens involving multiple departments to answer.**	- Social network monitoring - Unified tools for getting statistics from social network posts - Unified tools for posting/interacting with citizens

Capability	Description and Reasoning	Future State Required
		▪ Escalating information requests to process them via structured workflow
Maps	**Maps capability represents the management and publishing of map information to citizens. It includes possibility of rehosting map information in portals and mobiles as well.**	▪ Federated geo-information system allowing map and layer aggregation ▪ Components to rehost the map content in other solutions
Citizen Chatbot	**Capability enabling a new way of communicating with citizens using public messaging platforms – Facebook Messenger, Skype, Alexa etc.**	▪ Question and answer handling via chatbot ▪ Service catalogue enquiries handled via chatbot ▪ Text based interaction (via messengers like Facebook Messenger, Skype) ▪ Audio based interaction (via Alexa)
Developer Tools & Enabling Third Party Developers	**Capability contains a set of services and tools that are meant to simplify tasks of internal and external developers when building new systems and leveraging other existing services.** Example services that are developer focused and support providing additional capabilities when building services/systems: ▪ Usage tracking ▪ Feature flags ▪ API publishing and API subscription management Sustained IT service environment also needs tools for developers and maintainers so that configuration and documentation can be well maintained, accessible, information on usage of the services available to plan future enhancements.	▪ Usage tracking service ▪ IT services documentation management solution ▪ Configuration management (source code management) ▪ API documentation for internal and external developers ▪ Subscription management for API management ▪ Feature flags service for gradual service / functionality release
Payments and Invoices	**Some government services require payment. Therefore, this capability of providing a way for on-line payment is an important capability to truly enable a move to digital service delivery.**	Citizen/business representative: ▪ Viewing list of invoices to pay ▪ Viewing history of invoices/payments made ▪ Initiating payment

Capability	Description and Reasoning	Future State Required
	As an extension of service delivery payment processing capability includes invoice processing that can be used for invoices that are post-paid, e.g., invoices for property tax payment that is not really linked to service requested by the citizen.	▪ Processing payment on external payment gateway Government systems: ▪ Sending invoice to be paid to citizen ▪ Getting invoice payment status Government employees: ▪ Processing payment management complaints/issues
Records Management	**Records management is an important capability tracking all official government correspondence.** Given that some of the service request responses would be processed as documents (even if electronic), capability can be considered part of the service delivery, although more as supporting/integrated one, not primary.	▪ Registration of incoming communication (if tracked outside of other components, e.g., inbox/outbox) ▪ Registration of produced responses before they get delivered to citizens
Field Service	**Capability often extends the base capability of case management with support for managing teams of field workers (government employees or working on behalf of government) to provide service at the citizen or business location.** Capability often includes these sets of features: ▪ managing teams ▪ managing schedule ▪ managing assignment to cases ▪ handling rerouting (when worker or client is not available) ▪ support for navigation (planning routes on the map)	Not identified as priority for upcoming period.
Performance Management	**Capability enables government to have structured definition of strategy, programs, initiatives, targets and actuals to enable ongoing organisational**	Not identified as priority for upcoming period.

Capability	Description and Reasoning	Future State Required
	performance management, plan further corrective actions or investments. Specific to citizen service delivery, performance management KPIs can leverage information captured in service delivery tracking. But performance management systems go beyond just service delivery insights end enable track all other strategic initiatives and outcomes/goals they are achieving or not achieving.	
Event Ingestion and Advanced Analytics	**Capability enables government to leverage information from sensors and big data sources to provide enhanced services to citizens that otherwise would not be possible.** Example service using the capability could be a service to inform citizens about potential flood situation based on advanced analytics of various data sources, including historical data from water level and weather sensors.	Not identified as priority for upcoming period.

3.1.2. Common Capabilities

Many of the capabilities described in the previous subsection are already implemented (at least partially) as part of existing services in Northern Ireland or UK. To ensure a cost effective and sustainable environment for providing e-services, saving on duplicated effort and providing better usability of government solutions, it makes sense to have some of these capabilities invested in and provided centrally.

This subsection outlines the capabilities that should be developed as common capabilities to ensure more reuse is achieved and a more sustained service environment is created. This list of capabilities is a subset of all typical citizen service capabilities identified in the previous subsection and reflects the ones that are prioritized, and where a change of approach and/or extensions of functionality would need to be achieved by 2021.

The list of DSS owned common capabilities for service delivery is shown schematically in Figure 4. Each of the capabilities is assigned a number for reference purposes. Compared to the full capability list, some of the capabilities have been detailed to provide more context on the common nature of the capability required.

Note, the fact that these 20 capabilities are identified as being owned by DSS and being implemented as common does not mean that there cannot be separate solutions providing similar capabilities. In specific cases it still can be done as per an identified future state as defined in Table 7. For example, having a citizen portal as common capability does not prevent a specialized portal being created for a very specific service as long as it adheres to the overall principles and constraints of the service delivery architecture and uses as many common services as is reasonably possible.

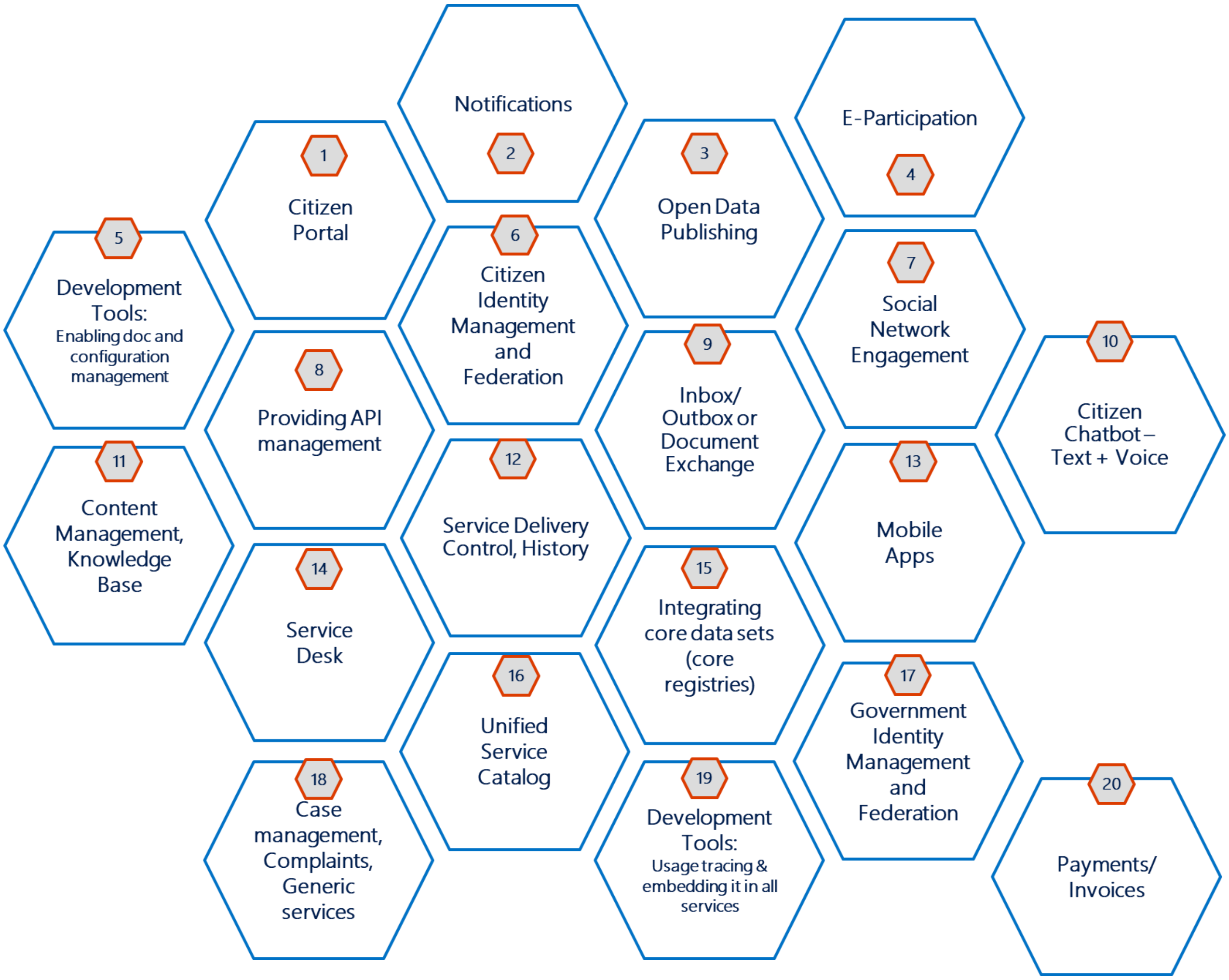

Notifications
2
E-Participation
4
1
Citizen Portal
3
Open Data Publishing
5
Development Tools: Enabling doc and configuration management
6
Citizen Identity Management and Federation
7
Social Network Engagement
9
Inbox/ Outbox or Document Exchange
8
Providing API management
10
Citizen Chatbot – Text + Voice
11
Content Management, Knowledge Base
12
Service Delivery Control, History
13
Mobile Apps
14
Service Desk
15
Integrating core data sets (core registries)
16
Unified Service Catalog
17
Government Identity Management and Federation
18
Case management, Complaints, Generic services
19
Development Tools: Usage tracing & embedding it in all services
20
Payments/ Invoices

Figure 4: List of future DSS owned common capabilities

The rationale behind these capabilities being DSS owned and elements of these that could be common elements are described in Table 8.

Table 8: DSS owned common capabilities

#	Common Capability	Common Elements	Reasoning
1	Citizen Portal	Portal platform and overall UX approach for other portals providing citizen facing data and services. Platform extensibility allowing new modules to be	Enabling common user experience is important element for citizen getting their services easy and without additional learning that might be introduced if many portals with different approaches exist.

#	Common Capability	Common Elements	Reasoning
		added/integrated if they are following extensibility guidelines.	NI Direct, MyNI already provided as centralized DSS owned services.
2	Notifications	Notifications service enabling any government institution to reach citizen or business representative via notification in a unified way.	Notification services require multiple integrations and dependency on paid services (e.g., sending SMS). Centralizing service not only unifies citizen experience but offers opportunity for optimal cost of the overall service. Gov.UK Notify already provided as centralized service that DSS can front to ensure personalized message delivery and notification tracking.
3	Open Data Publishing	Open data portal for publishing data sets, unified catalogue for all data sets to have common structure for data set description, unified standards. Enabled for multi-tenant use by multiple departments publishing their content.	Unified approach and single platform to publish open data drives standardization of underlying systems providing data to be published. Already a single open data portal exists for NI. Machine readable approach important for enhancing the solution and ensuring data is easier to publish in Gov.UK based open data solutions.
4	e-Participation	Common services for polls, surveys and legislation discussions. Enabled for multi-tenant use by multiple departments.	e-Participation elements like surveys, polls and participation in legislation process are non-department specific processes that can be achieved through single set of services.
5	Development Tools: Enabling doc and configuration management	Common document repository for technical documentation, source control for managing configuration and customizations of solutions, common build pipeline with support for dev/test environments.	Not having current system documentation and source a significant issue for system sustainability. Centralized management of these assets would also enable lock-in free system development approach.

#	Common Capability	Common Elements	Reasoning
6	Citizen identity management and federation	Identity hub providing federation with multiple identity providers. Rich profile management, including management of service subscriptions and delegations, business ownership.	To resolve data exchange issues G2G, single identity needs to be introduced without restricting login mechanism/approach. NIDA, Gov.UK Verify and Government Gateway already centralized components provided by DSS or national departments.
7	Social Network Management	Social network monitoring, statistics and engagements tooling accessible by multiple departments.	Reusing investment in the tooling across the government given generic nature of the functionality not linked to any specific department.
8	API Management	Central registry and gateway of all exposed department system and common component APIs (application programming interfaces) to enable G2G and G2C data and functionality sharing.	Standardization of approach, unified tracking of requests for usage statistics. Single team investing in platform capability.
9	Inbox/Outbox aka Secure Messaging	Central component with its APIS and portal/mobile pages enabling document exchange electronically between citizens and government.	Opportunity to save on paper letter delivery costs. Convenience for citizens maintaining history of all government interactions as part of their "profile". Centralized to enable single view of government for citizen.
10	Citizen Chatbot – Text and Voice	Chat bot supporting general greeting and evaluation dialogs as well as specific Q&A and service catalogue enquiry dialogs.	New way of citizen interaction expected by new generation of citizens. Centralized and common to drive recognition of single brand.
11	Content Management, Knowledge Base	Content and knowledge base management functionality accessible to various institutions. Approvals. Publishing content and knowledge base information to citizens via multiple channels.	Driving common brand and content structure across government to ensure single government brand. Saving the hosting costs by having centralized platform hosting all content.

#	Common Capability	Common Elements	Reasoning
12	Service Delivery History	Service to track all service delivery statuses. Reporting on top of service delivery history and service catalogue information.	Centralized to be able to provide insights into service delivery.
13	Mobile Apps	Main hub mobile app enabling management of profile, identity, notification and inbox tracking, browsing service catalogue. Support for multiple specialized mobile apps through unified UX guidelines for mobile apps.	Presence in native form on the mobile app, communication mechanism on new changes through regular updates of mobile app.
14	Service Desk	Common service desk application/solution across departments to ensure single phone line/web form (single channel) for raising issues with government.	Single government perception for citizen despite having multiple department specialists handling the requests.
15	Integrating Core Data Sets	Common adapters to access core data sets: properties, addresses, cars, citizens, permits/licenses to ensure consistency and kick start data exchange G2G.	Kick-starting data sharing will take investment of accessing existing data stores and exposing information. Requires central focus on this to expose all data sets using similar design approach/principles.
16	Unified Service Catalogue	Catalogue service exposing data to different channels and other components. Common administration screens available to various departments to manage their part of the catalogue.	Central component because root for many other centrally maintaining functionality, e.g., insights into service delivery. Also ensures consistency of service description across entire government.
17	Government Identity Management and Federation	Main identity management, identity and rights storage and federation engine.	Enabling single sign on for employees of government and partners using internal systems and providing citizen services.
18	Case Management	Common platform for building out new case management workflows easier.	Centralized to save on investment and ensure skills/training is limited.

#	Common Capability	Common Elements	Reasoning
19	Development Tools: Usage tracking	Usage tracking service used by multiple department systems to trace the activities happening, users/citizens accessing e-services.	Centralized to provide unified insights about all service delivery across the government, not just department by department or system by system.
20	Payments/Invoices	Payment service, payment screens in portal and mobile apps, payment administration for government employees.	Integration with payment gateway only once. Unified payments experience for all services.

3.1.3. Capability Assessment

The common capability definition provided in the previous subsection (see section 3.1.2) coupled with the assessment of current capabilities versus planned future capabilities to achieve strategic goals is summarized graphically in Figure 5.

It is important to stress that the assessment is not for any given service implementation, as its own implementation might have elements of the capabilities mentioned. Continued assessment and evolution of common capabilities is necessary, i.e., common capabilities should be assessed in their current implementation versus what is needed to drive primarily:

- new capabilities to drive citizen centric services supported in omni-channel way;
- sustained implementation and maintenance of the services and platforms implemented.

Figure 5 uses colour coding to define the gap of current capability versus the envisioned future state:

- White or NA – means that capability can be considered not implemented at the moment – either there are no IT support elements implemented or they are implemented in a siloed way in departments, but not as common capabilities identified in previous subsection;
- Very light blue or *1* – current implementation of capability relative to future needs provides some level of reuse, a change of the approach or significant additions are required, e.g., change of approach required, yet with reuse of existing knowledge and even base platforms;
- Light blue or *2* – relative to future state envisioned capability implementation has elements that need to be extended going forward, e.g., service that provides part of the required functionality and needs mandatory elements to be added – citizen identity capability providing user authentication for citizens via e-mail/password and requiring extensions/changes to support other identity provider federation and unified ID across entire landscape, support for business accounts;
- Blue or *3* – relative to future state require adjustments in their revisions to align to future state, e.g., use of the solution that covers quite a lot of functional areas, but might be lacking 1 or 2 non-critical areas to be added as part of overall development of the services going forward;
- Dark blue or *4* – rich existing capability that might need minor changes/additions to achieve future state, e.g., adding a standard based API in front of existing system, ensuring usage tracking is performed;

- Very dark blue or *Full* – capability fully matching or providing more than future state envisioned.

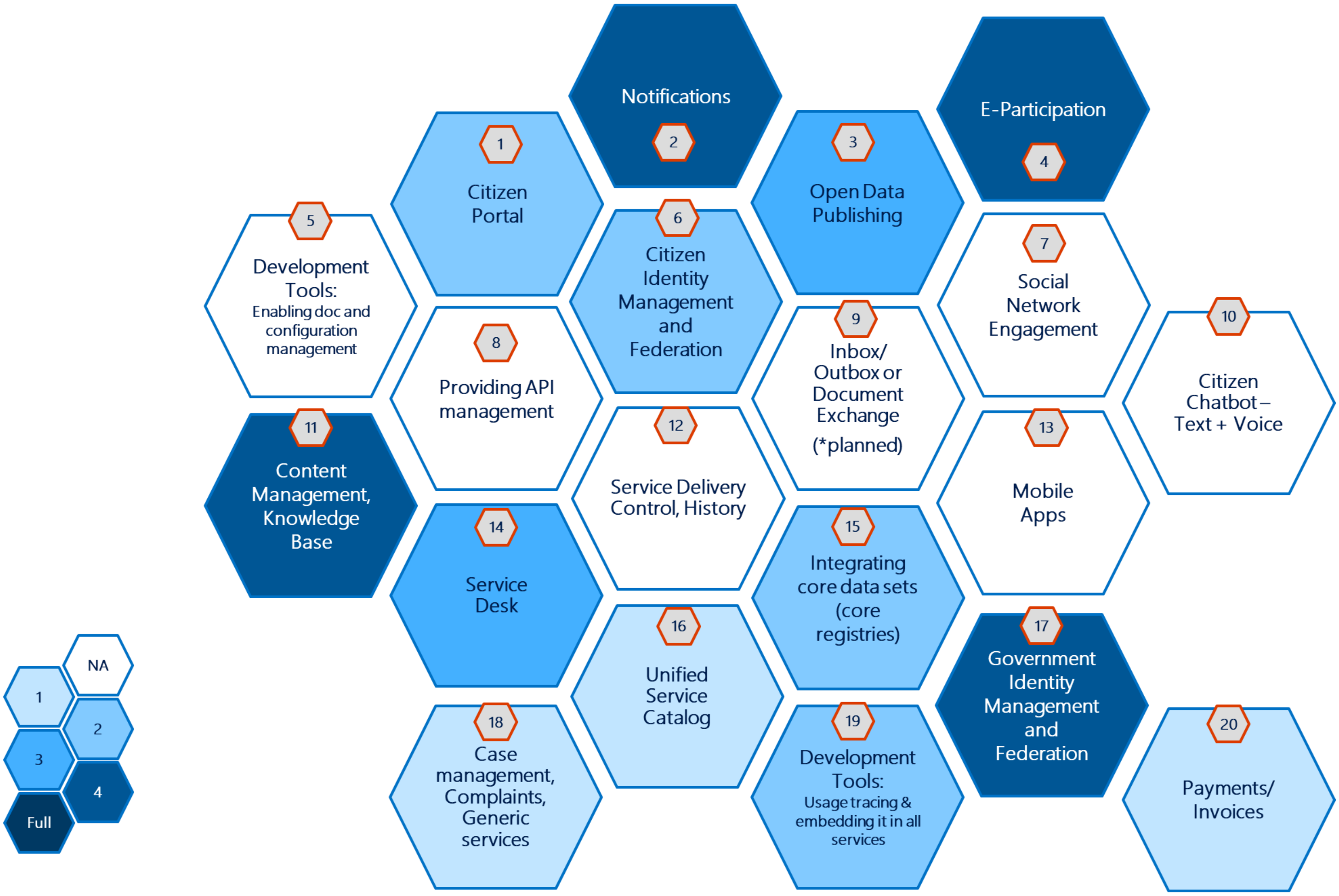

Notifications
2
E-Participation
4
1
Citizen Portal
3
Open Data Publishing
5
Development Tools: Enabling doc and configuration management
6
Citizen Identity Management and Federation
7
Social Network Engagement
8
Providing API management
9
Inbox/ Outbox or Document Exchange (*planned)
10
Citizen Chatbot – Text + Voice
11
Content Management, Knowledge Base
12
Service Delivery Control, History
13
Mobile Apps
14
Service Desk
15
Integrating core data sets (core registries)
16
Unified Service Catalog
17
Government Identity Management and Federation
18
Case management, Complaints, Generic services
19
Development Tools: Usage tracing & embedding it in all services
20
Payments/ Invoices
NA
1
2
3
4
Full

Figure 5: Gap assessment against future vision

This assessment shows that the main capabilities missing (are not there as common reusable ones) are the ones that would enable sustained development of systems and sharing of information in a unified way through well-defined and controlled APIs.

Also, omni-channel access to functionality is not enabled because at present there are multiple portals servicing content and e-services functionality, yet there is no citizen access to services via mobile apps, social networks or newer channels like citizen chatbot.

Capabilities like Citizen Identity management and Case management are positioned as reusable components but assessing them against the future vision or sustained development criteria, they need to be extended. The same with unified service catalogue that at present covers only e-services and does not provide more information that would be required for full a service catalogue covering all types of services delivered over multiple channels, supporting subscription services and data set services as well.

The capabilities that are most developed now comparing them to future state are:

- content management and knowledge base – multiple Drupal based systems used for content and service catalogue publishing now;

- Government Identity Management and Federation – Active Directory and ADFS based solution that already enables centralized employee and partner identity management, but would need standardization across the government systems and precise definition of information maintained in AD issued tokens;
- notifications leveraging Gov.UK Notify already for delivery of SMS, e-mails and snail mail notifications to citizens in a unified way; missing element is link to common NI identity to enable personalization of the delivery and tracking it;
- e-participation where software as a service solutions are used for survey management and also for feedback on upcoming legislation; this area requires standardization of the tools to be used in the future to ensure there are economies of scale instead of multiple tools procured for different departments.

3.2. Application Architecture View

Application architecture provides a services view of the overall solution, showing internal and external dependencies of these services. A logical architecture view of the solution is provided in this subsection.

3.2.1. Architecture Pattern

Before defining the services required to implement the common capabilities as identified in the capability definition section, it is important to define the architectural pattern of how services providing citizen capabilities should be built. This pattern applies not only to common capabilities and services providing common functionality, but also to all services providing citizen facing functionality.

To support omni-channel access to functionality exposed by various systems as e-services and to enable sustained development and evolution of this functionality over time, any service implemented should follow these principles:

- service functionality exposed to partners (G2G) or citizens and businesses (G2B/G2C) are exposed over REST based API;
- API(s) is published on API management common capability enabled layer to provide seamless versioning, enforce common security approach for sustained evolution of functionality over time;
- there can be multiple frontends leveraging the service API to provide end-user functionality, e.g., access to it via portal/mobile or access from another service or system;
- exchange of asynchronous messages (preferred over direct calls) is implemented via message queue-based solution leveraging versioned messages;
- UI exposed by government employees can be more tightly coupled to the service implementation to enable reuse for COTS products and drive more reuse of ready-made platforms (does not have to access functionality over APIs exposed API management);
- citizen and business access to service is secured using Citizen (and business) Identity Hub, government employee and system access to service functionality is secured using Government Employee Identity Management and Federation solution.

A schematically described pattern is shown in Figure 6. represents the typical service components in pink and external components using the service or used by the service in blue. The figure also identifies APIs and messages that can be versioned by showing V1 and V2 appropriately on interaction lines. Figure 6 also illustrates that there are components of the service that can be developed standalone (e.g., specific mobile app providing the service to citizens) and there are components that can be hosted on existing platforms (e.g., portal pages hosted on portal common) to achieve more seamless user experience and to ensure more reuse from implementation and also solution hosting perspective.

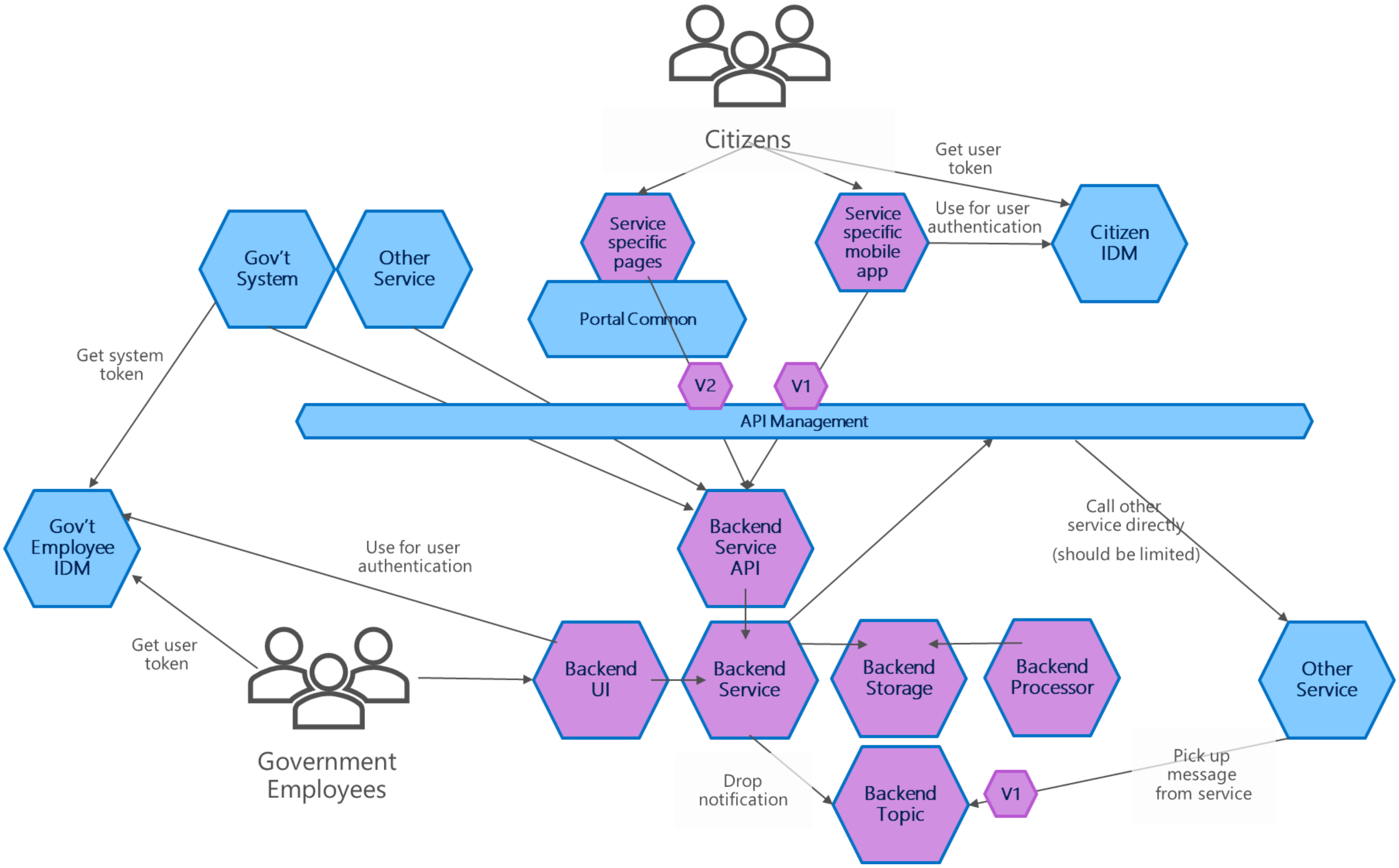


Figure 6: Service implementation pattern

Note that there are services (e.g., technical services like usage tracing) that might not have citizen UI specific components (only administrative ones exposed to employees).

3.2.2. Service Map

Overall service map and dependencies of services enabling common capabilities of citizen service delivery is displayed in Figure 7. Figure shows only main interactions of component groups, grouping components based on their responsibility area/type:

- identity and profile management;
- providing citizen interaction (channels);
- API management – providing "glue layer" for external access to functionality and ensuring decoupling/indirection;
- core service functionality exposed via APIs and providing internal employee user interaction;
- supporting all services for elements like audit and usage capturing;

- supporting DevSecOps teams managing configuration, making changes and running solution deployment and tests.

Note that although core services, profile management, supporting services are mostly shown as single logical elements, their actual implementation follows the previously identified architecture pattern where, for example, Inbox/outbox secure messaging service:

- has its backend APIs and management UI in core services layer,
- has its pages and screens in portal and mobile app platforms,
- relies on both identity management solutions to authenticate its users,
- exposes its APIs for citizens and external partner systems on API management layer,
- traces usage of the service via supporting components.

Elements shown with red border are platform elements that support building new types of certain services (e.g., new workflows in case management or new forms in forms engine, new UI modules in citizen services portal, new API registrations in API management). Being platform components as per architectural principles they support both multi-tenancy (to be used by teams in different departments) and extensibility by multiple development teams. Elements shown with blue border are ready-made multi-tenant components supporting multiple department teams, but not extensible by other developers.

Figure 7 also shows how other government and non-government systems can participate in the overall service delivery and reuse common platform, services and overall architectural approach:

- existing web and mobile solutions providing specialized services can leverage citizen identity and call existing common services or other government systems publishing data and functionality via API management layer;
- government systems reusing services can perform G2G calls to other systems exposing their data and services in a uniform way through API management;
- backend systems can publish their APIs to enable their e-services access the functionality or to enable other government systems accessing the data/functionality exposed;
- government systems can reuse important building block functionality from common capability services, things like profile management, notification sending, inbox/outbox for secure messaging, payment/invoice service, data integration and reporting platforms to host their data and reports (more on reusable services exposed via common services see in section 3.2.3).

Note that details of the priority items in the list of services identified in the figure below are provided in appendix 5.6. Each of the important capabilities are further detailed identifying the logical services comprising it. This deep dive information also illustrates the service implementation pattern on the example of specific services like Service Catalogue and Inbox/Outbox.

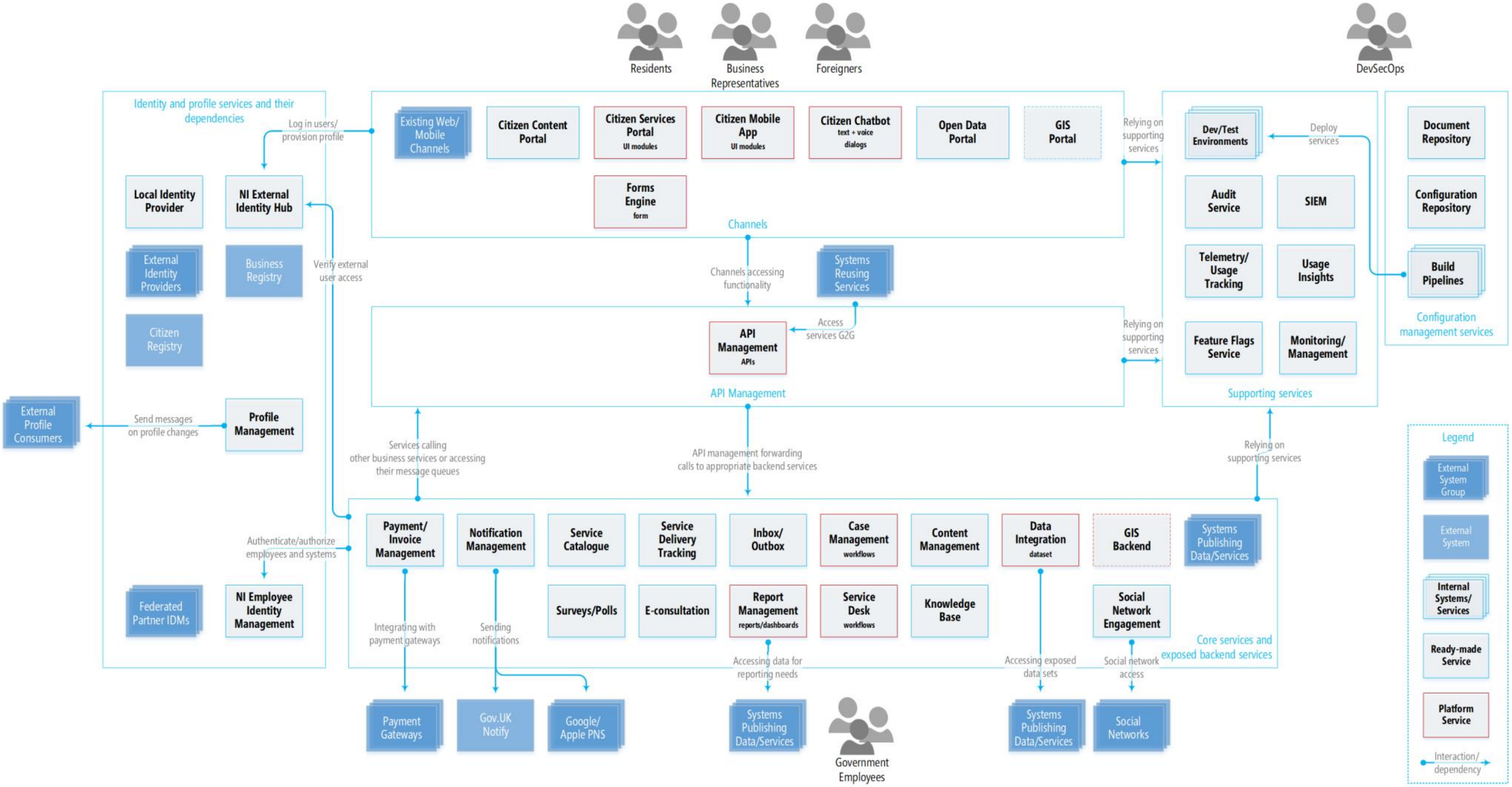


Figure 7: NI citizen service delivery common capability service map and dependencies

3.2.3. Reusable Services

Services defined in the service map that provide reusable capabilities and specifics of the reuse enabled is described in Table 9. Table 9 defines a reusable service catalogue for developers of other government systems that can be reused when building/maintaining their own citizen facing services or sharing data and functionality inside the government.

Table 9: Service reuse enabled

Service	Reuse Enabled	Specifics
NI external identity hub	Authenticating external citizen/resident/foreigner and business representative	Can be used to enable SSO with existing web sites/mobile apps. Can be used to secure APIs exposed to external customers.
NI employee identity management	Authenticating and authorizing internal government users and partners accessing UI of the internal systems. Authenticating and authorizing internal systems (other services) of other government departments accessing APIs to get data or functionality G2G.	
Profile management	Get profile information for citizen or business Get information on subscriptions to subscription-based services defined by department in service catalogue	Profile updates distributed in pub/sub way.
Notifications management	Send notifications to citizen or business using profile ID	Sending notifications over SMS/e-mail and snail mail initially. Adding functionality for mobile push notification delivery for small messages once mobile hub app implemented.
Inbox/outbox	Send documents/messages in secure way to citizen/business inbox Check delivery/read status Receive messages sent by citizens/business representatives	Both government employee UI as well as programmatic API enabled.
Service Delivery Tracking	Register service being delivered to citizen or business	

Service	Reuse Enabled	Specifics
	Update service status to enable visibility for citizen Get reports based on service delivery tracking information and service catalogue defining services and their transaction SLAs.	
Service Catalogue	Mange service catalogue, capturing information on all services provided, including those relying on traditional delivery (not e-services). Consume service catalogue information in own web sites/apps.	Management exposed as government employee UI. Access exposed via managed API.
Report Management	Define and publish internally reports accessing open data, data of other departments and own data. Define and publish externally (citizen access) reports accessing open data, data of other departments and own data.	
Payment/Invoice Management	Submit invoice to be paid by citizen/business representative Check invoice payment status Cancel invoice List invoices Process invoice/payment complaints	
Content management	Managing content using predefined content types, publishing content Re-publishing content in own web sites/mobile apps etc.	Administration through government employee UI Access via API
Knowledge base	Managing knowledge base articles, marking articles internal only or public Re-publishing knowledge base content in own web sites/mobile apps etc.	
API management	Exposing own standards-based REST APIs	As part of publishing defining products, policies that apply

Service	Reuse Enabled	Specifics
Forms engine	Designing e-forms, their versions Re-hosting e-forms in own portals/mobile apps	
Case management	Defining custom entities Defining custom human workflows to process citizen and business representative requests Defining government teams participating in workflow processing Managing business rules guiding more complex workflow processes Enabling custom automated workflow logic by calling out to existing APIs published Tracking case processing SLAs	
Service desk	Defining new service request types Defining custom human workflows for processing service requests Defining government teams participating in workflow processing Managing business rules guiding more complex workflow processes Enabling custom automated workflow logic by calling out to existing APIs published Tracking service request processing SLAs	
Telemetry/Usage Tracking and Usage Insights	Tracing technological events (errors, usage) Tracing custom business relevant usage events (e.g., user launching e-Service) Accessing usage reports	
Audit Service	Defining new audit event types Auditing important actions performed by service	

Service	Reuse Enabled	Specifics
	Accessing audit reports	
Data integration	Exposing own data sources through data integration as is (using open APIs) Exposing own data sources through transformation and cache	
Social network engagement	Defining social network monitoring criteria Getting social network statistics Interacting with citizens on social networks	
Surveys/Polls	Defining new surveys/polls Publishing surveys/polls Processing survey/poll results	
Feature Flags	Managing own feature rollout by defining feature flags and incorporating logic around them in channel components and services	
Configuration Management Services	Managing system documentation Managing system source code of customizations and configuration, deployment Managing build pipelines Reusing public cloud-based dev/test environments	
SIEM	Aggregating system events happening in the environments Performing analysis to identify suspicious patterns of activity	
Monitoring/ Management	Monitoring of all IT assets in the environment across various data centres hosting parts of the overall solution landscape. Alerts on top of the gathered information when certain unhealthy condition is met or soon to be met.	Monitoring requires single toolset (or set of integrated tools) to ensure single insight into overall environment. Management can be accomplished via multiple tools as

Service	Reuse Enabled	Specifics
	Reporting on top of previously captured IT related events. Managing system configuration.	management often is technology/solution specific.

3.3. Information View

An important element in enabling better citizen-centric services in government is information sharing among the departments. If done right, this eliminates requests for citizens to bring in certificates/permits issued by other government institutions when providing a service. Information sharing can go beyond sharing information internally by sharing open data to entire public and even enabling external developers building new services leveraging government data.

Sharing requires technical elements and standards to enable it uniformly and all these common enabling services have been defined in the previous subsection. Understanding data needs and data availability from government departments is key to planning data publishing over time and to prioritize data publishing initiatives.

This section provides an initial assessment of data elements that are needed, are available already or are planned over time to enable a data publishing initiative plan.

An initial assessment of data available from various departments and national agencies is provided in Figure 8. Note that it currently shares ideas of data that would be useful for other government departments providing services or public for statistics insights. Further work is required to verify actual government and public needs, data sets that are already exposed (but not in a standard way), data sets that can be exposed although not yet exposed.

Initial data asset assessment has shown that there are large amounts of data sets managed by government departments (e.g., ~240 managed by Department of Finance alone). This requires more analysis to define requirements and capabilities. This illustrates the important focus that needs to be allocated to information asset and their integration needs analysis as this is one of the big enablers for government data exchange to enable better citizen services. Proposed roadmap (see section 4.3) includes initiatives and organisational structure changes proposed to support this focus area.

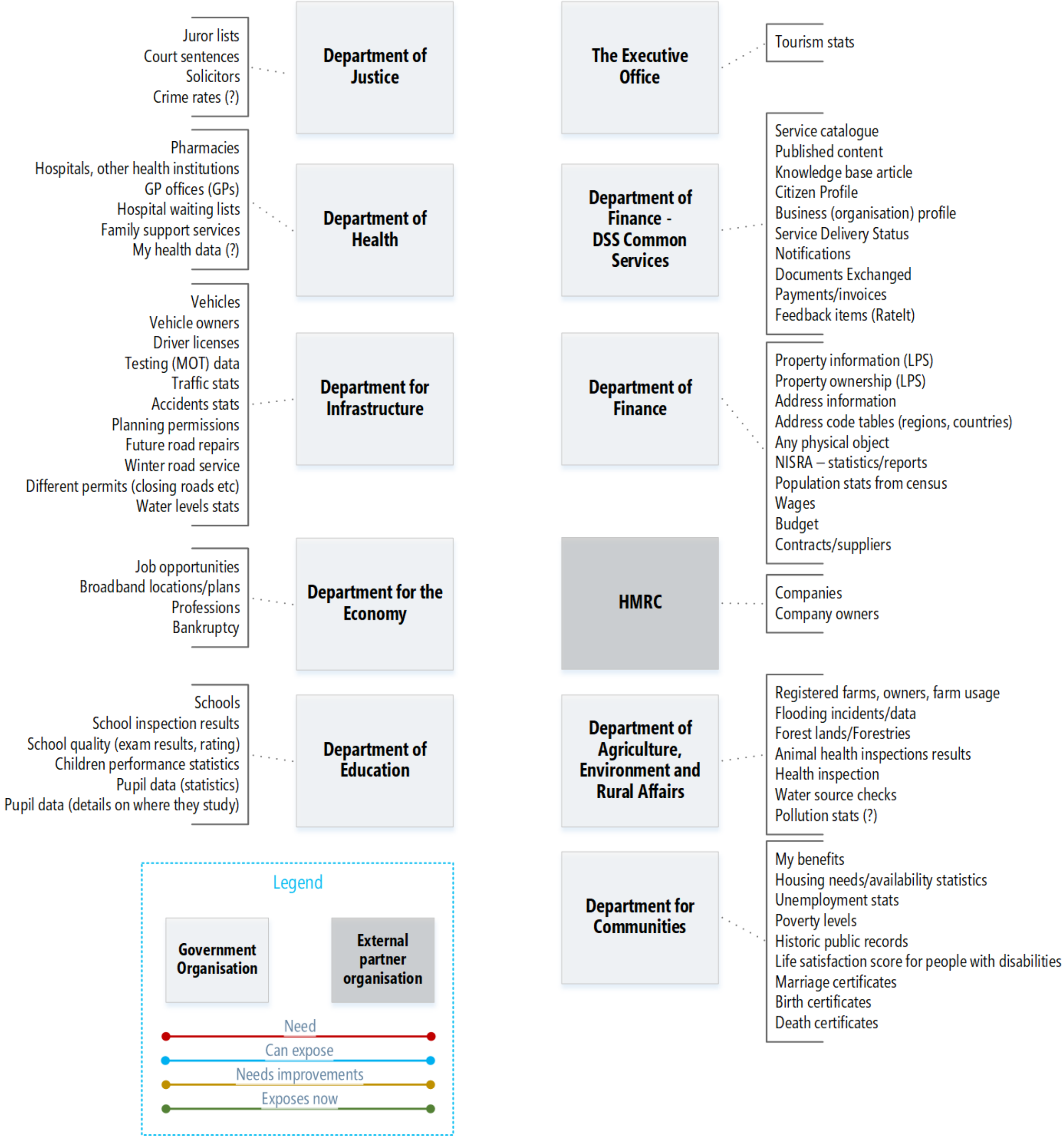


Figure 8: Initial information ownership and needs analysis

3.4. Development, Security & Operations Lifecycle View

Sustained service implementation and maintenance over time requires efficient development, security and operations tools and processes. The common tools to improve the development and maintenance are identified in section 3.2. This section provides more insights into processes and organizational structure required to ensure sustained development of services, especially common services.

3.4.1. Ownership

From a process ownership perspective, the service lifecycle is as defined in Figure 9. This figure shows that DSS leads strategy, design, transition, operation and improvement of common services, as well as supporting common strategy for all citizen service interaction. When it comes to department specific services, DSS enforces overall architecture constraints and principles, architecture pattern definition, yet actual service strategy, their implementation, transition and operations are owned by respective departments with support of DSS at various stages of the lifecycle.

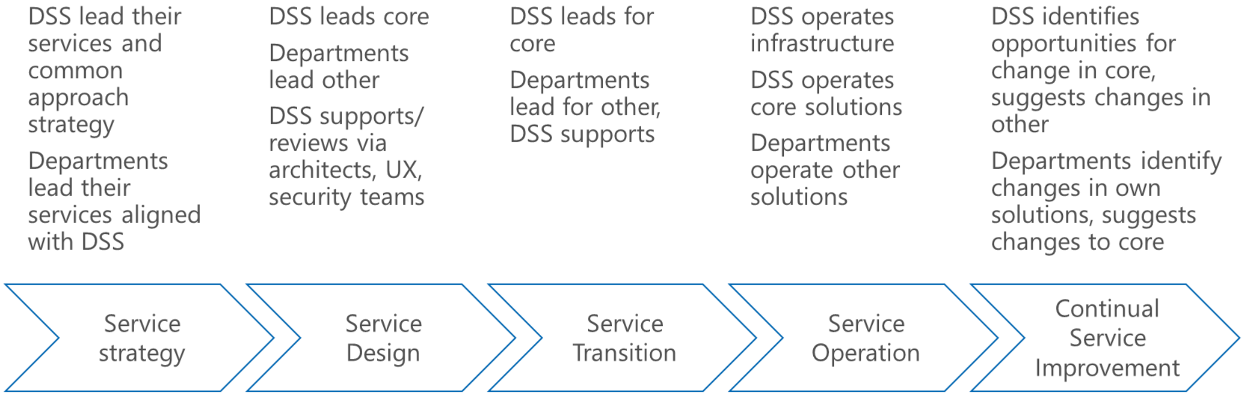

DSS lead their services and common approach strategy
Departments lead their services aligned with DSS
DSS leads core
Departments lead other
DSS supports/ reviews via architects, UX, security teams
DSS leads for core
Departments lead for other, DSS supports
DSS operates infrastructure
DSS operates core solutions
Departments operate other solutions
DSS identifies opportunities for change in core, suggests changes in other
Departments identify changes in own solutions, suggests changes to core
Service strategy
Service Design
Service Transition
Service Operation
Continual Service Improvement

Figure 9: Service lifecycle step ownership

3.4.2. Implementation Organizational Pattern

When considering the implementation of services according to the defined architecture, architectural constraints and aligned with common platforms that should be reused, it is important to:

- Ensure the entire team responsibilities are clearly defined;
- Limit dependencies among multiple teams involved in building the end-to-end citizen experience.

To achieve that while adhering to architectural pattern defined in section 3.2.1, the proposed implementation organization pattern for any service is to have multi-skilled teams building end-to-end services. These services would have citizen UI components (where needed) and backend components exposed via a shared API layer built by a single team. This enables the external procurement of such service implementations as deliverables which would then be fully verifiable. The only dependencies teams would optionally manage are dependencies on platform components such as portal and case management. The only hard dependencies are adhering to styles/approach and architectural patterns as well as publishing APIs on the API management layer. Note, that when developing an end-to end service, there is generally no dependency upon the API management layer as development will be possible by direct calls from client components into APIs being developed.

This implementation organizational pattern for citizen services is displayed schematically in Figure 10. Figure 10 shows multiple teams (represented by different colours) responsible for different services/platforms being implemented. Some of the services teams leverage reusable common platforms, whilst some are building very tailored specialized services.

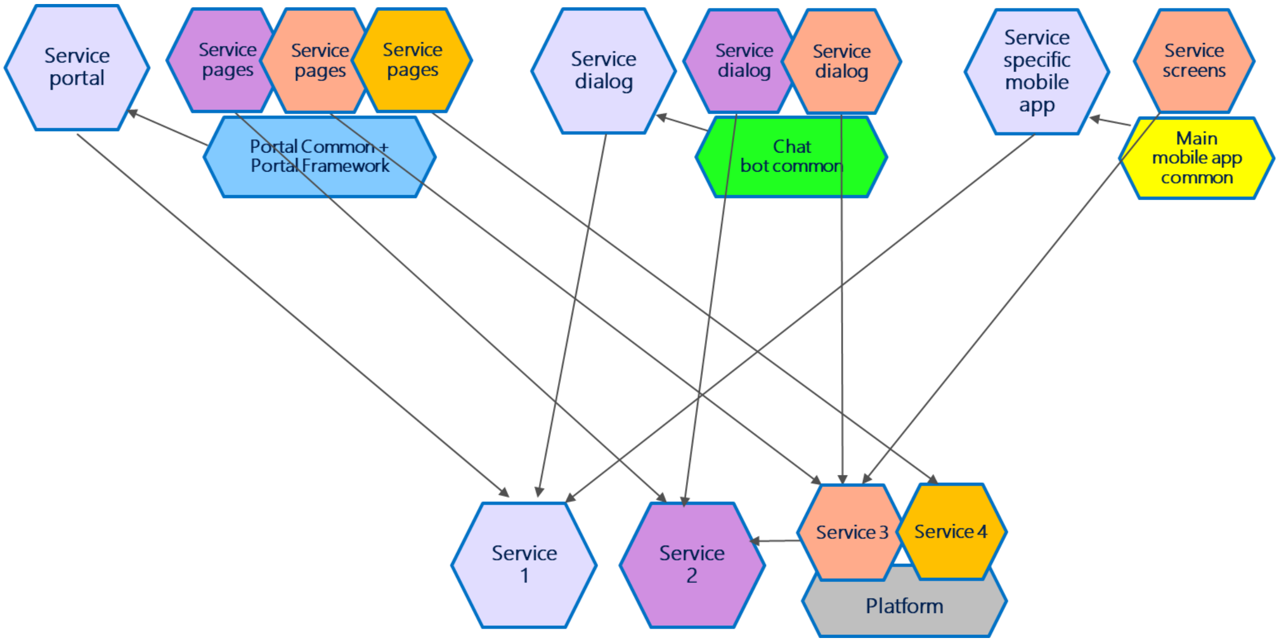


Figure 10: Implementation organizational pattern

3.4.3. Documentation and Configuration Management

To support sustained development and enhancement of services over time, maintaining documentation and configuration well, is critical.

As defined in the capability and logical architecture overview, there are development tools that are required to ensure centralized management of documentation and source code (configuration included). Beyond the centralized tools that should make management easier, standards for documenting IT services require updates to enforce use of the solutions.

Suggested changes in documentation and configuration management include:

- migration of government teams to use centralized documentation and configuration management;
- enabling contributions and reuse of code across the teams, including even public contributions to documentation or code;
- ensuring external procurement of services for development of IT solutions related to citizen service (and broadly – even internal services) require documentation and configuration to be manged as part of the centralized solution.

The minimal set of documentation required for a service includes:

- Business case and technical approach (document/section answering *why?* question for the service to be introduced);
- Context (personas and scenarios to be supported by the service – *what?*);
- Architectural design (identification of service components to be introduced, their internal and external dependencies, examples of control flow through these components to showcase the scenarios supported) and Component high level design (*how?*);
- Deployment guide (information on how to deploy the solution, what are the configuration parameters and deployment pre-requisites);

- Administration guide (information on operational tasks to follow when running the service in production).

Note the user guide is not included in the list of mandatory documentation because the suggested approach is to have visual cues, help and overall solution design to follow conventions that would enable solutions to be directly usable without special guide/help for users. In case of complex interactions suggestion is to rely on video materials showing how solution should be used to achieve specific scenarios/use cases.

More information on content of each of the documentation elements required is provided in appendix 5.4.

3.4.4. CI/CD

Continuous Integration, Continuous Delivery is the process to drive more automation, speedier adjustment to changes, earlier detection of integration issues and, if done right, less regression bugs. To speed up implementation of the solutions in government and to ensure changes to existing solutions do not introduce regression issues, CI/CD is an important practice to be adopted.

Depending on implementation technology leveraged for service implementation this also means the use of automated deployment into dev/test environments and (after necessary validation) automatic deployments of new versions in production as well.

3.4.5. Live Site Management

Live site management is the next level of the DevSecOps where lines between dev/test, pre-prod and prod environments start to blur and solutions are managed as ‘always-running’ services. Given the benefits it provides, it is worthwhile to consider some of the elements of Live site management even when implementing DevSecOps – namely feature flags-based release and detailed tracking of all technical and business events.

Live site management approach elements can be especially beneficial for platform services identified in application architecture view where a single service that is stable and does not get changed too much, hosts multiple “tenant” services developed, maintained and released by multiple teams.

Implementing platforms to be managed as Live site through a single infrastructure environment can be quite complex. To support this, services hosted on the platform can follow virtual “release rings” principle (see example of release rings in Windows in Figure 11) leveraging the Feature Flags service as defined in the previous section where features created would be made available to different tester groups (internal, beta) and only then to broad population. Release group management can be achieved through Profile Management service. For example, single Case Management platform instance can support multiple services at different “release stages” – 5 production services, 2 services in beta testing in pre-production and 1 in development/test.

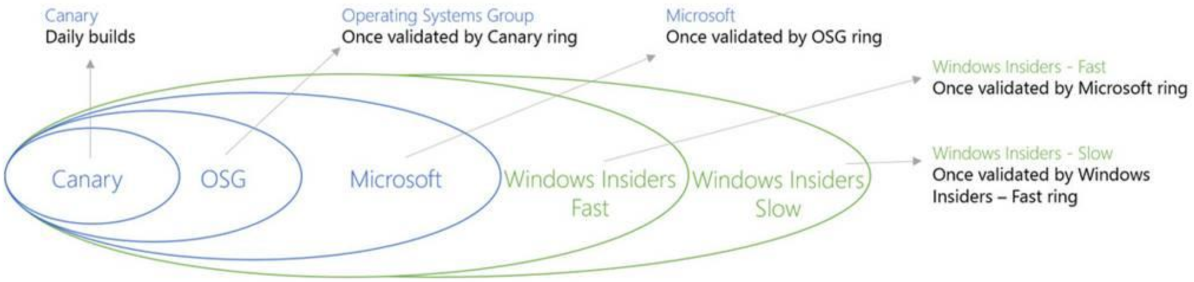


Figure 11: Example of management of dev/test/pre-production/production "environments" for Windows as a service

A Live site approach also introduces changes in solution team ownership. With Live sites the same multi-skill team developing and implementing the service is also responsible for uptime/maintenance of the service and further improvements.

Live site approach is running testing in production, therefore detailed usage and error reporting is a very important aspect that provides service owners with insights of what is working and what is not both from business requirements perspective and from technical perspective.

3.4.6. DevSecOps Pattern

The overall approach showing integrated technical capabilities and process flow to enable documentation and configuration management, CI/CD pipeline, service improvement through insights into service usage, monitoring of the environment and managing issues through unified DevSecOps teams is illustrated in Figure 12. This also references security specific products that should be part of the environment to ensure security related insights on top of gathered usage and IT environment event data. Figure 12 shows feature flags service to illustrate the suggested way on how feature releases would be planned for gradual release into production.

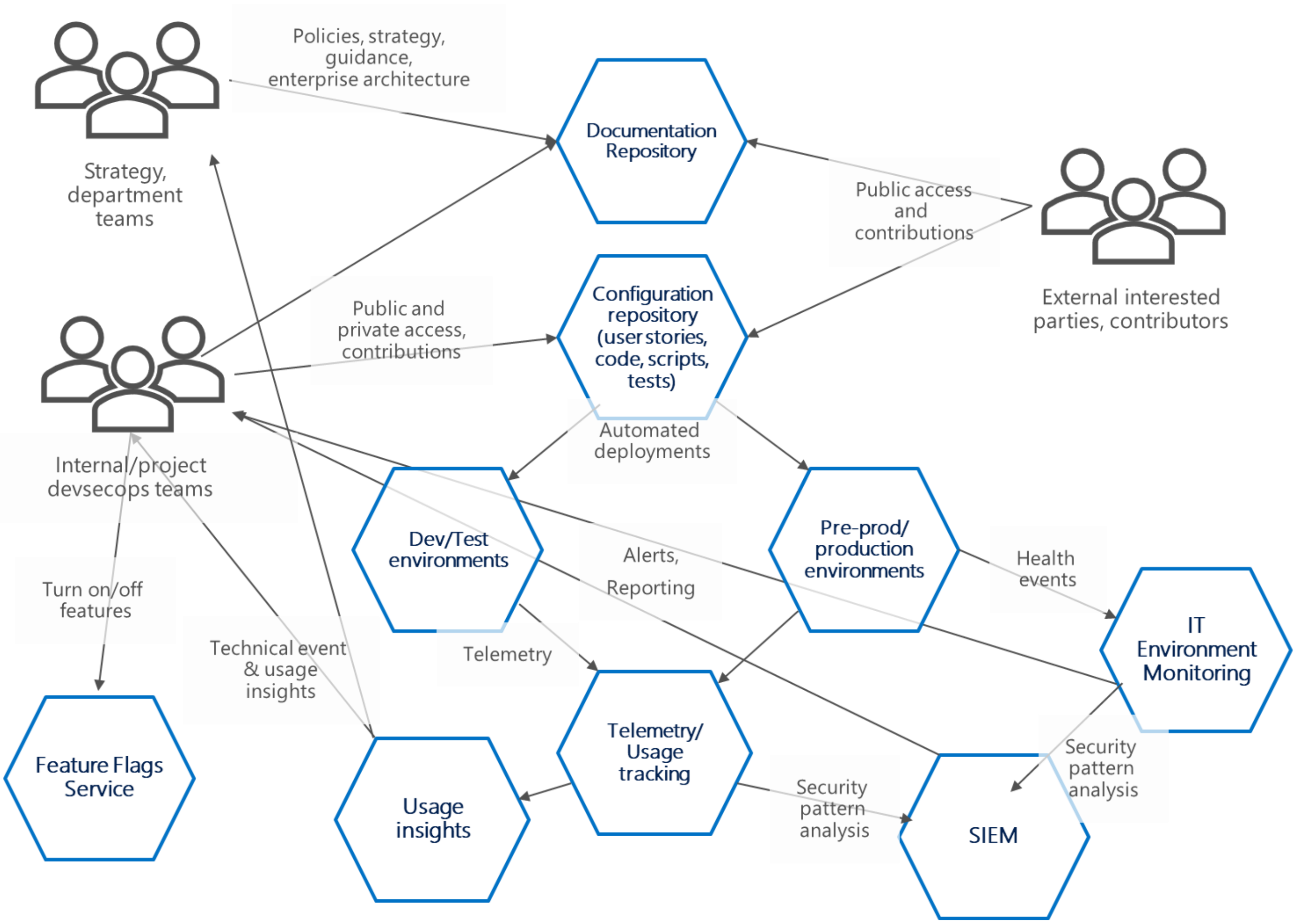

Policies, strategy, guidance, enterprise architecture
Strategy, department teams
Documentation Repository
Public access and contributions
External interested parties, contributors
Configuration repository (user stories, code, scripts, tests)
Public and private access, contributions
Internal/project devsecops teams
Automated deployments
Dev/Test environments
Alerts, Reporting
Pre-prod/ production environments
Health events
IT Environment Monitoring
Turn on/off features
Technical event & usage insights
Telemetry
Telemetry/ Usage tracking
Security pattern analysis
Security pattern analysis
Feature Flags Service
Usage insights
SIEM

Figure 12: DevSecOps Lifecycle overall view

3.5. Infrastructure View

This section describes the infrastructure approach that is required to enable modern environment for hosting citizen facing solutions. Note that although focus of this document and this section is on services provided to citizens, given use of internal systems in serving citizens many of the aspects documented in this section should be applicable to other systems hosted by the government.

3.5.1. Architecture Pattern

As one of the goals identified during the workshops for improving citizen services is ensuring faster time to market and sustained rate of improvements of e-services, it is important that the infrastructure approach supports more agile provisioning and changes in infrastructure environments. To achieve this, and focus effort more on developing/enhancing not running the infrastructure for the services, the suggested approach is to:

- focus on use of higher-level base services to host solutions (see next subsection 3.5.2 for details);
- leverage IT infrastructure agility and advanced offerings offered through public cloud providers;

- involve infrastructure planning into service planning and implementation process through integrated DevSecOps practices (see more in section 3.4)

The infrastructure pattern to support future citizen services platform and the services themselves is illustrated in Figure 13.

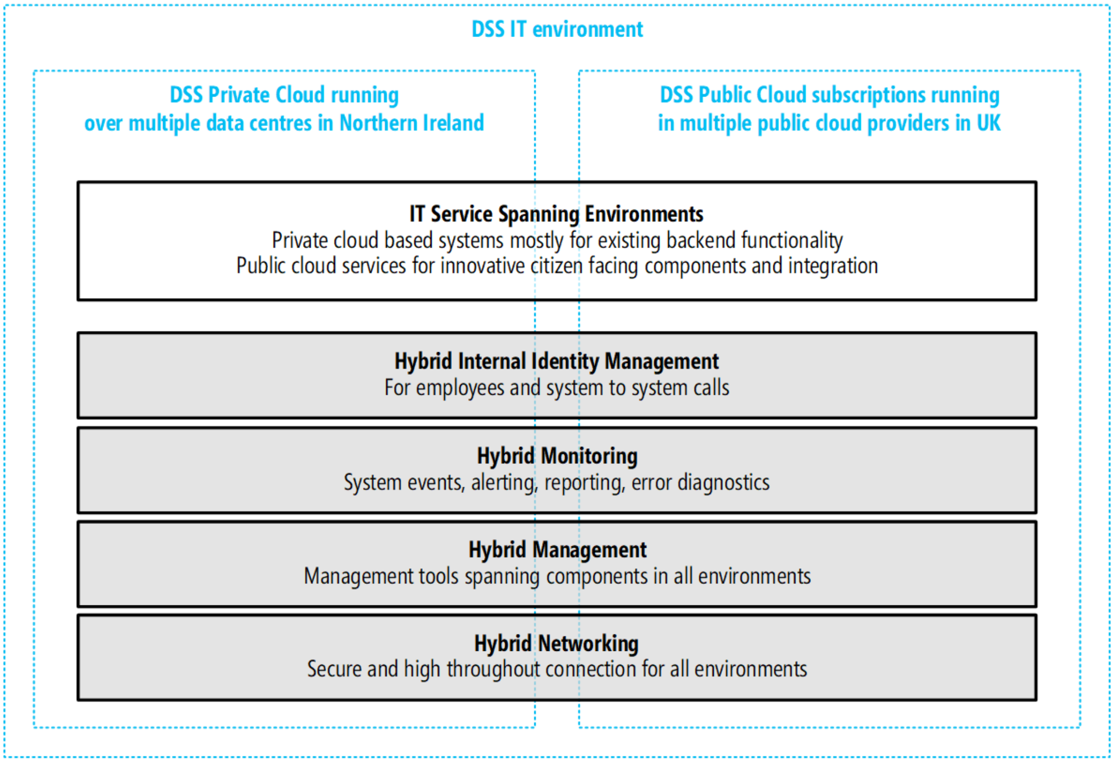

DSS IT environment
DSS Private Cloud running over multiple data centres in Northern Ireland
DSS Public Cloud subscriptions running in multiple public cloud providers in UK
IT Service Spanning Environments
Private cloud based systems mostly for existing backend functionality
Public cloud services for innovative citizen facing components and integration
Hybrid Internal Identity Management
For employees and system to system calls
Hybrid Monitoring
System events, alerting, reporting, error diagnostics
Hybrid Management
Management tools spanning components in all environments
Hybrid Networking
Secure and high throughout connection for all environments

Figure 13: Infrastructure pattern for services

The figure shows that end-to-end services in general case span multiple environments. For example, having a portal and other UI element interacting with citizens requiring public cloud enabled services and, having existing backend systems providing the backend data access in DSS private cloud environments.

The figure also shows that such environment requires support of multiple infrastructure elements:

- hybrid networking connecting various cloud environments in a secure way;
- hybrid identity sourced in Active Directory as per architectural constraints and supporting identity management in various cloud environments for internal users and for systems;
- hybrid monitoring to ensure all events from all environments are aggregated and available for further analysis and insights, also alerts;
- hybrid management to have tools that enable management of various platforms across all the environments.

Security in such distributed environment also requires additional focus. See more on security approach defined in section 3.6.

3.5.2. Hosting Model

At present most of the solutions run by departments are hosted by DSS in IaaS environments or procured as external managed service. Looking into the future and considering potential improvements into deployment consolidation, especially reuse of platforms, the hosting model should support additional middle ground options to raise the reuse level and speed of development for custom solutions, enable better hosting.

The models of hosting to support for solutions providing citizen services with evaluation criteria of when to pick one over another is provided in Table 10.

Table 10: Hosting models

Model	Description	When to use
IaaS	Model where solution builders have virtual machines allocated to them based on their specification. Solution builders then often deploy their own application stack and solutions on these virtual machines that need to be maintained with time together with application itself.	Suggested use only for legacy applications that do not support other hosting models. Can be used for very sensitive solutions that require maximum separation of solution from other solutions (if similar cannot be achieved in higher level platforms).
IaaS++	Model where solution builders get shared container deployment environment that provides advantages in deployment, amount of consolidation possible on the same hardware and maintenance.	Suggested for use in solutions requiring cloud independence (possibility to move from one cloud to another). Avoid using when advanced services are required. Do not use containers for hosting common IT services like RDBMS. Good to host stateless service components, e.g., web sites, APIs.
PaaS	Model where solution builders care only about their solution application code and configuration, not the infrastructure and application stack. Good for maintenance, but also for advanced features like declarative scalability, features like	Primary choice for all new custom developed solutions, e.g., APIs, Web sites, batch processing, case management/workflow solutions. Primary choice for application platform components like

Model	Description	When to use
	built in backups, DR, automated deployment and versioning. Extreme option of the PaaS is serverless platforms when instead of solution builders deploying full application and still defining sizing of the infrastructure to use, they are deploying application modules without knowledge of infrastructure to run them.	database management systems, noSQL data stores, queuing mechanisms, API management.
SaaS	Model to be used for services that can be implemented using configuration of ready-made platform (no customization via code allowed). For commodity functionality (e.g., collaboration) this reduces implementation risks and overall costs as commodity SaaS platforms are used by many customers, thus raising overall quality and decreasing the cost due to economy of scale.	Primary choice for services that provide commodity functionality, e.g., surveys, collaboration, and do not require Northern Ireland specific customisation that goes beyond what configuration offers. Should not be used for getting custom tailored services as benefits of lower price and reduced implementation risks disappear.

3.5.3. Environments

Given the speed of provisioning and de-provisioning the solutions in public cloud and discussed vision of targeting public cloud, management of dev and test environments in general case should be targeting automatic deployment in public cloud even for components that in production would run in hybrid mode or only private cloud. This approach also provides better support for DevSecOps processes described in section 3.4, where development teams can provision and de-provision multiple environments to enable true automation of CI/CD, automated test execution and deployment.

As described in the infrastructure pattern, the pre-production and production environment depending on the requirements of actual service spans multiple cloud environments. For services managed as live site as described in section 3.4.5 dev/test/pre-production and production environments can be the same main environment managed through feature flags for beta testing in production. This applies to services that over time are evolved with new functionality and should not be used for new services or large changes that change architecture of the base service.

For more information on the approach for DevSecOps for citizen services enabling solutions see section 3.4.

3.6. Security View

This section describes the aspects of a modern-day security practise and operations of a successful citizen services organization. It's providing DSS the very basics to build your on-going cyber security and security strategy and operations on top of.

3.6.1. Cyber Security vs Security

What's the difference between the two? IT security is seen as the traditional hygiene part of the full story – your physical perimeter security, layer 2 or 3 firewalls, malware filtering on various ingress points, patch management, technical or policy controls based on risk assessment and standardized responses to incidents. Whereas "cyber" is the new buzzword.

In general terms cyber security should be seen as a strategic approach to minimize the damage caused by an active threat actor, an attacker.

There can be no effective cyber security defence in place without the traditional security operations that are up to date and monitored appropriately.

3.6.2. Change in the landscape

In today's world, four out of five breaches happen because of stolen credentials. This typically does not occur through perimeter penetrations or elaborate network traffic eavesdropping schemes. With the notion of enabling end users to work anywhere with any device, the data is proliferated everywhere and the physical network boundary cannot control the majority of the threats.

The user identity has become the new security perimeter, as it is via the user identity that organization's systems and data is accessible anytime, anywhere. The success rate of the perpetrators of this perimeter is devastating. That success rate has called for a new approach to the security strategy and the architectural views supporting that.

DSS has adopted a cloud first strategy in providing citizen services. This same mind set should be extended towards the cyber defence strategy – utilizing the vast experience, technology solutions and agility to respond by in-particular public cloud providers. Using this in the right ways will provide DSS with additional capabilities which would be difficult to develop, manage and maintain themselves.

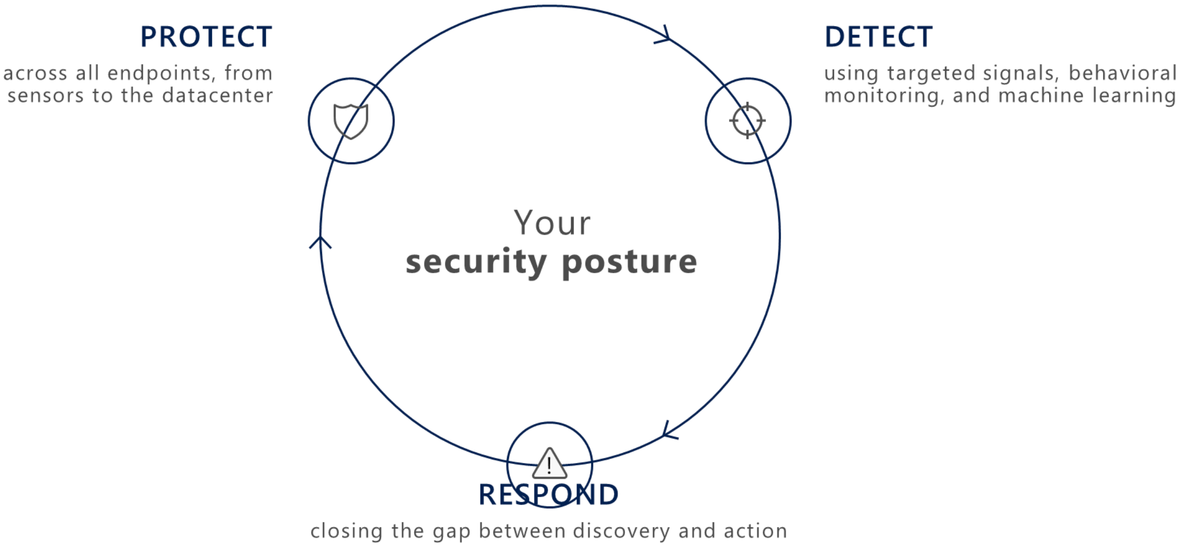
3.6.2.1. Assume Compromise

Instead of relying on a hard perimeter defence to thwart of the attackers, DSS should adopt the mind set of "assume the breach". This mind set change will help bring forth the necessity of certain capabilities like end user behaviour analytics or threat intelligence that are both based on machine learning technologies.

Assuming a compromise mind set will also help design systems that hold crucial data for citizen services – principles on how to store data, what types of data to store using the same controls, where to store citizens identities, how rich a profile should be in a single store. Assuming any one of the components will be breached will lead to well segregated information storages and will also require technological solutions that can support the use of such distribution.

3.6.3. Protect, Detect, Respond

From the security strategy perspective, the cycle of Protect, Detect, Respond should be the defining guideline in any architecture design. DSS should adopt security architecture patterns that are built around these principle functionalities:

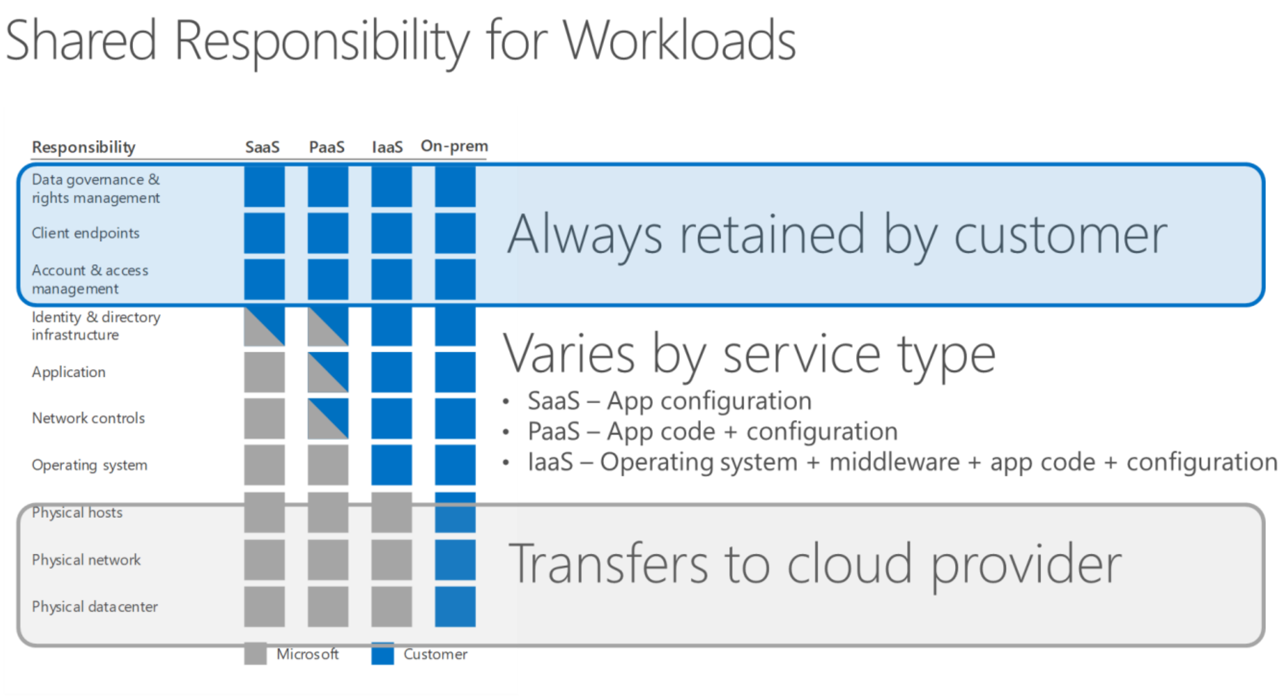

PROTECT
across all endpoints, from sensors to the datacenter
DETECT
using targeted signals, behavioral monitoring, and machine learning
Your
security posture
RESPOND
closing the gap between discovery and action

3.6.4. Security in a Cloud-enabled World

Cybersecurity threats make security more challenging—however the public cloud makes it easier for you to manage as the security load shifts to the service provider.

DSS security focus must shift from perimeter security to data, identity, and application layers.

The following diagram shows how the various layers and how the responsibilities are shared when providing services from a public cloud platform:



Shared Responsibility for Workloads

Responsibility	SaaS	PaaS	IaaS	On-prem
Data governance & rights management	🟦	🟦	🟦	🟦
Client endpoints	🟦	🟦	🟦	🟦
Account & access management	🟦	🟦	🟦	🟦
Identity & directory infrastructure	◪	◪	🟦	🟦
Application	⬜	◪	🟦	🟦
Network controls	⬜	◪	🟦	🟦
Operating system	⬜	⬜	🟦	🟦
Physical hosts	⬜	⬜	⬜	🟦
Physical network	⬜	⬜	⬜	🟦
Physical datacenter	⬜	⬜	⬜	🟦

⬜ Microsoft 🟦 Customer

Always retained by customer

Varies by service type

- SaaS – App configuration
- PaaS – App code + configuration
- IaaS – Operating system + middleware + app code + configuration

Transfers to cloud provider

3.6.4.1. Defend, Deter, Develop

The "Cyber Security A Strategic Framework for Action 2017-2021" aligns to the UK National Cyber Security Strategy and has adopted the key themes of Leadership, Defend, Deter and Develop.

From the national strategy:

- **DEFEND** We have the means to defend the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves;
- **DETER** The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so;
- **DEVELOP** We have an innovative, growing cyber security industry, underpinned by world-leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges.

Whilst the terminology used differs slightly from that used earlier in this section, the overall themes of the above stays the same: DSS needs the capabilities to DEFEND (Detect and Protect), DETER (Detect and Respond) and DEVELOP new capabilities together with industry leaders to meet these targets.

3.6.5. Security Architecture Recommendations

The following is a proposed set of next steps for Security Architecture in DSS;

- Add a role of Security Architect, that will help create an overall security strategy and help cover the gaps in the current security stance;
- Create the security strategy based on the commonalities of Protect/Detect/Respond and Defend/Deter/Develop;
- Evolve the strategic approach around the notions that "Identity is the security perimeter" and "Assume breach";
- Integrate the public cloud services provided actionable intelligence to DSS security operations.

3.7. Governance View – Enterprise Architecture

3.7.1. Enterprise Architecture Definition

The establishment of an Enterprise wide architecture function in DSS is a key priority and a required enabler for the future success of DSS to enable it to deliver on its strategic goals.

The following is a proposed definition for Enterprise Architecture in DSS;

- Enterprise architecture is the process of translating business vision and strategy into effective enterprise change by creating, communicating and improving the key requirements, principles and models that describe the enterprise's future state and enable its evolution;
- The scope of the enterprise architecture includes the people, processes, information and technology of the enterprise, and their relationships to one another and to the external environment;
- Enterprise architects compose holistic solutions that address the business challenges of the enterprise and support the governance needed to implement them.

3.7.2. EA Function Goals

The EA function in DSS will have the following goals;

- **Drive standardisation** of the provision of digital services through architecture practices and planning;
- **Reduce complexity** by highlight overlapping digital capabilities and increasing quality of business requirements;
- **Reduce costs** by identifying and programmatically removing solution and platform legacy components;
- **Increase agility** for solution delivery by defining and enforcing best practice design principles that enable increase speed of platform development, deployment and maintenance.

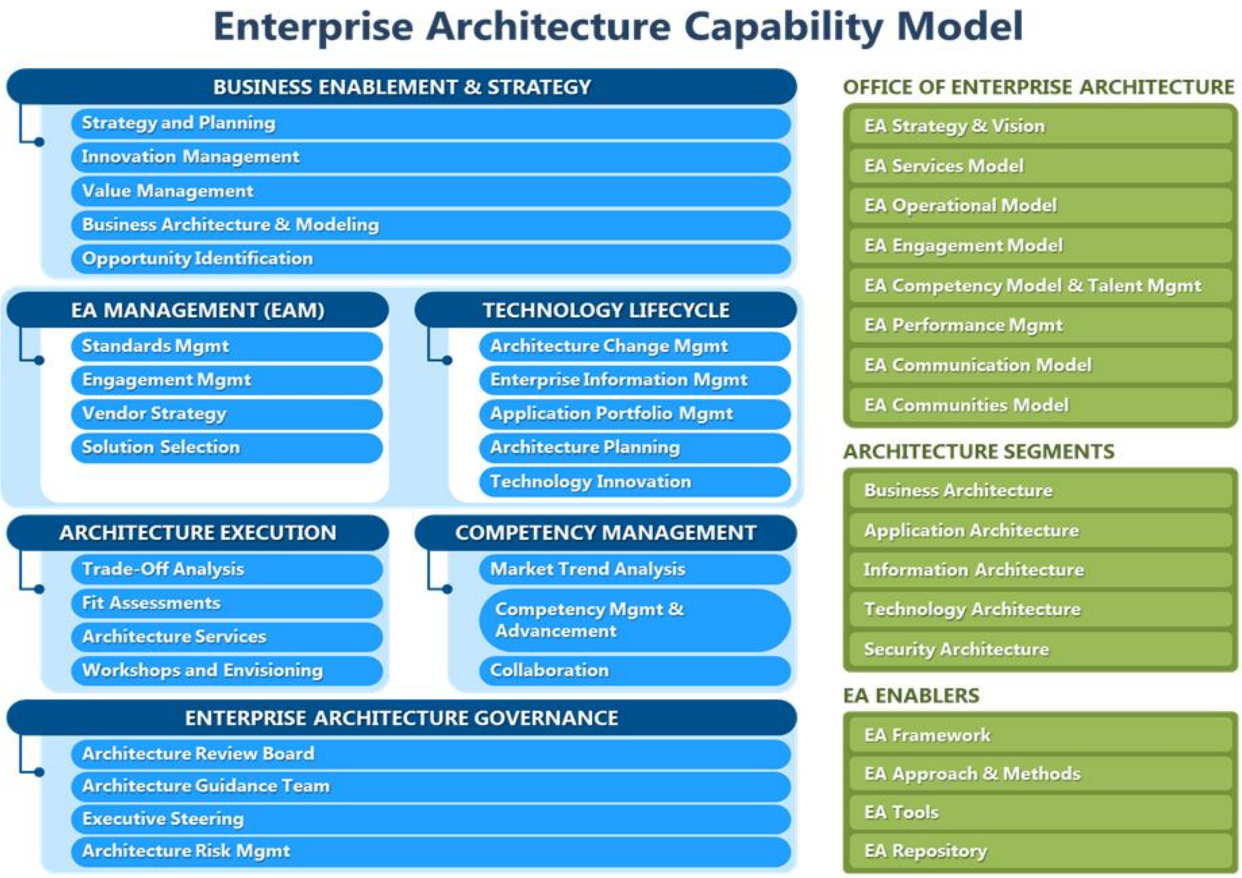
Additional expected benefits of an effective Enterprise Architecture function are as follows;

- Frees IT staff time to work mission-specific projects and innovations;
- Enables more innovation at the departmental level;
- Provides a stronger technology infrastructure at the central technology core;

- Reduces risk of exposure;
- Lowers total cost of service ownership;
- Reduce duplication of effort and services and increases reuse of existing systems and system components;
- Save time and costs in procurement (as a 'blueprint' can be provided to solution providers), contract management (roles and responsibilities are clearly defined), change management (impact analysis is easier).

3.7.3. Enterprise Architecture Capability Model

To deliver on the required goals and objectives of the EA function, there are a set of capabilities that the EA function will be required to perform. It is important to note that not all of these capabilities will be in place in the initial stage of formation of the EA team and require sustained development and investment in order to clearly define, prioritise and establish each of these capabilities.



Enterprise Architecture Capability Model

BUSINESS ENABLEMENT & STRATEGY
- Strategy and Planning
- Innovation Management
- Value Management
- Business Architecture & Modeling
- Opportunity Identification

EA MANAGEMENT (EAM)
- Standards Mgmt
- Engagement Mgmt
- Vendor Strategy
- Solution Selection

TECHNOLOGY LIFECYCLE
- Architecture Change Mgmt
- Enterprise Information Mgmt
- Application Portfolio Mgmt
- Architecture Planning
- Technology Innovation

ARCHITECTURE EXECUTION
- Trade-Off Analysis
- Fit Assessments
- Architecture Services
- Workshops and Envisioning

COMPETENCY MANAGEMENT
- Market Trend Analysis
- Competency Mgmt & Advancement
- Collaboration

ENTERPRISE ARCHITECTURE GOVERNANCE
- Architecture Review Board
- Architecture Guidance Team
- Executive Steering
- Architecture Risk Mgmt

OFFICE OF ENTERPRISE ARCHITECTURE
- EA Strategy & Vision
- EA Services Model
- EA Operational Model
- EA Engagement Model
- EA Competency Model & Talent Mgmt
- EA Performance Mgmt
- EA Communication Model
- EA Communities Model

ARCHITECTURE SEGMENTS
- Business Architecture
- Application Architecture
- Information Architecture
- Technology Architecture
- Security Architecture

EA ENABLERS
- EA Framework
- EA Approach & Methods
- EA Tools
- EA Repository

Each of these capabilities are described in the appendix 5.2.

3.7.4. Enterprise Architecture Maturity Model

The maturity level of an organisation's Enterprise Architecture programme can place constraints, or major positive benefits, on the ability to use technology implementations to deliver real business value.

Within the industry there are several different Maturity Models: which typically compare what might be perceived as "Industry Best Practice" against one organisation's current position, skills, approach and processes. One issue with these "standard" approaches, is that for an organisation that is newly developing their Enterprise Architecture practise, the level of inward inspection that is required in order to understand the current Maturity Level will distract from the actual practice of improving the Enterprise Architecture for the benefit of the organisation as a whole.

This additional Enterprise Architecture Maturity Model has been developed to be quick, easy to apply to DSS. It is designed to show at a high level where the Enterprise Architecture practice is at present, to give a picture of where they should be developing over the next year or two, and to allow Senior Management and broader stakeholders to see a progression from "Starting" through "Becoming useful", with a view of "Vitally Important" as soon as possible.

The EA Maturity Model uses four levels of Maturity.

1 – Basic	Reactive to requirements. Early establishment of an EA Function
2 – Repeatable	EA Processes are defined and being used in normal situations. IT Service Management is understanding the importance of the EA function. Discussions on business capabilities are happening.
3 – Managed	EA is driving technology decisions into the future. Common models in use across IT and the business.
4 – Optimised	Continuous, agile, value driven, approach to EA. EA working with senior IS and business leaders.

Within each of these Maturity Levels are several specific capability dimensions against which the current EA function has been assessed. These are, by design, a subset of the capability model outlined above to help inform a "good-enough" analysis and are the key pillars to enable an EA function to gain solid foundation. A more comprehensive analysis using the full capability dimensions outlined above should be planned for and performed by the EA leadership team at specific milestones in its development.

Stakeholder Involvement & Support	Who, within the IT and Business environments is the EA function interacting with
Architecture Governance / Compliance	How well aligned to the EA processes are the IT and Business environments
Management of Architecture team	Is the Architecture team itself well managed, supported and staffed
Architecture Scope	Is the EA focussed on just IT Services, or on the wider business environments
Architectural Standards	Is the EA function using common industry recognised standards

Architecture Planning Horizon	How far into the future does the EA influence stretch
Architecture Process	Have the processes been defined to allow the EA practise to function correctly within both the IT and Business environments
Architectural Quality	Are the Architectures produced of sufficient quality to allow the organisation to meet its defined business or IT goals
Business linkages	Is the EA function an integral part of the business planning cycle
Business Architecture	Does a proper Business Architecture exist and is it being used
Information Architecture	Does a proper Information Architecture exist and is it being used
Solutions / Application Architecture	Does a proper Application Architecture exist and is it being used
Technology Architecture	Does a proper Technology Architecture exist and is it being used
Impact	How wide is the impact of the EA function on the IT and Business environments

	Basic 1	Repeatable 2	Managed 3	Optimised 4
Stakeholder Involvement & Support	IT Management. Limited executive support (typically 1 stakeholder on the IT side)	Architecture Community. Broader executive support (typically a governance group, possibly some business executives)	Line of business support. More specifically, business resources involved in EA governance (e.g. portfolio management)	Corporate management support
Architecture Governance / Compliance	Ad-hoc approach to architecture development. Reactive to issues and not getting ahead of things. Governance structures being created (e.g. (setting up focus groups around specific topics).	Where Architectural processes and guidance are followed, they are seen to be of value. Established governance process exist but is not completely effective because of lack of executive support and governance may not match culture / needs	Process is well defined, communicated and regularly executed.	Value metrics drive EA process improvements
Management of Architecture team	Basic approach agreed. Stakeholders identified	Work in Progress. Plan established and agreed. Stakeholders on board.	Work progressing and well under way. Problems understood and handled by processes. Plan revised as required	Full achievement of capability
Architecture Scope	IT Services and other "biggest pain point" areas. Developing core principles and standards – bouncing ideas off respected IT domain experts.	IT environment, extending to first business areas. Covering individual major sections of IT (e.g. infrastructure or applications, but not both)	Across all IT areas. Within multiple business areas.	Integration across business areas
Architectural Standards	Understanding different industry and customer data and architecture models	Using a common model for all architectural artefacts	Using an industry standard model and approach (TOGAF, Zachman, MODAF, VRF) for architecture definitions	Helping to drive and extend the industry standard as a major practitioner
Rgulaltory / Industry Standards	Understanding of regulatory standards	Use of regulatory standards within Architectural models	Full compliance, integration and reporting of regulatory standards.	Influence & Drive Govt Standards.
Architecture Planning Horizon	Past / Present	Next year	Next 2 to 5 years	5 years and beyond
Architecture Process	Process and framework defined. Approach starting to be part of IT processes.	Architecture processes exist, begin followed, but not always consistently applied	Integrated, consistent process, consistently applied	Value driven process, measured and produces quality metrics
Architectural Quality	Process / framework / approach defined to measure quality	Process followed. Understanding of quality metrics, and how Architectures meet these.	Quality of the Architecture can be varied to meet Business Value	Value driven quality metrics
Business linkages	No explicit linkage to business issues or plans	Reactive to business needs. Some explicit linkage to business issues	Integrated with business planning. Architectural content linked to business needs	Strategic influence into business capability. Enterprise Architecture is seen as adding measurable value to the business
Business Architecture	Common IT / business language	Requirements driven	Principles driven	Common models
Information Architecture	Common Information Assurance language. Architecture artifacts and processes being created	Requirements driven. Process exists and is resurrected as needed to address technology deficiencies	Principles driven. Solutions delivery linked to architecture deliverables	Common models. Integrated planning of deliverables across Technology, Business, Applications.
Solutions / Application Architecture	Common Applications language	Requirements driven	Principles driven	Common models
Technology Architecture	Technology implementations tends to drive the Enterprise Architecture	Integrated planning. Technology acquisitions pass through Architectural "gates"	EA shapes technology requirements. Projects, solutions, applications, infrastructure are reviewed against the architecture standards	EA shaping technology trends and approaches for 5 years ahead
Impact	EA standards setting. EA Team identity being created	Integrated planning. Team credibility is growing. More requests for assistance	Architecture Team and deliverables have proven value	Architecture Team input influences the initial planning stages of business requirements and technology improvements

Legend:	Current State	Target (~2 Years)

The descriptions outlined in the model above are intended as indicative summary observations of the current state of the EA function and are generic descriptions by nature. The intent is to outline and highlight improvement areas that the team have identified to help inform a development and improvement plan for investment over the coming periods of time.

4. Roadmap

The roadmap section is based on analysis of gaps of common capabilities vs. the ones envisioned and based on understanding of processes and organization changes to be made. Initiatives have been proposed with a draft plan based on dependencies, impact of the initiative and its estimated size/complexity.

4.1. Initiatives

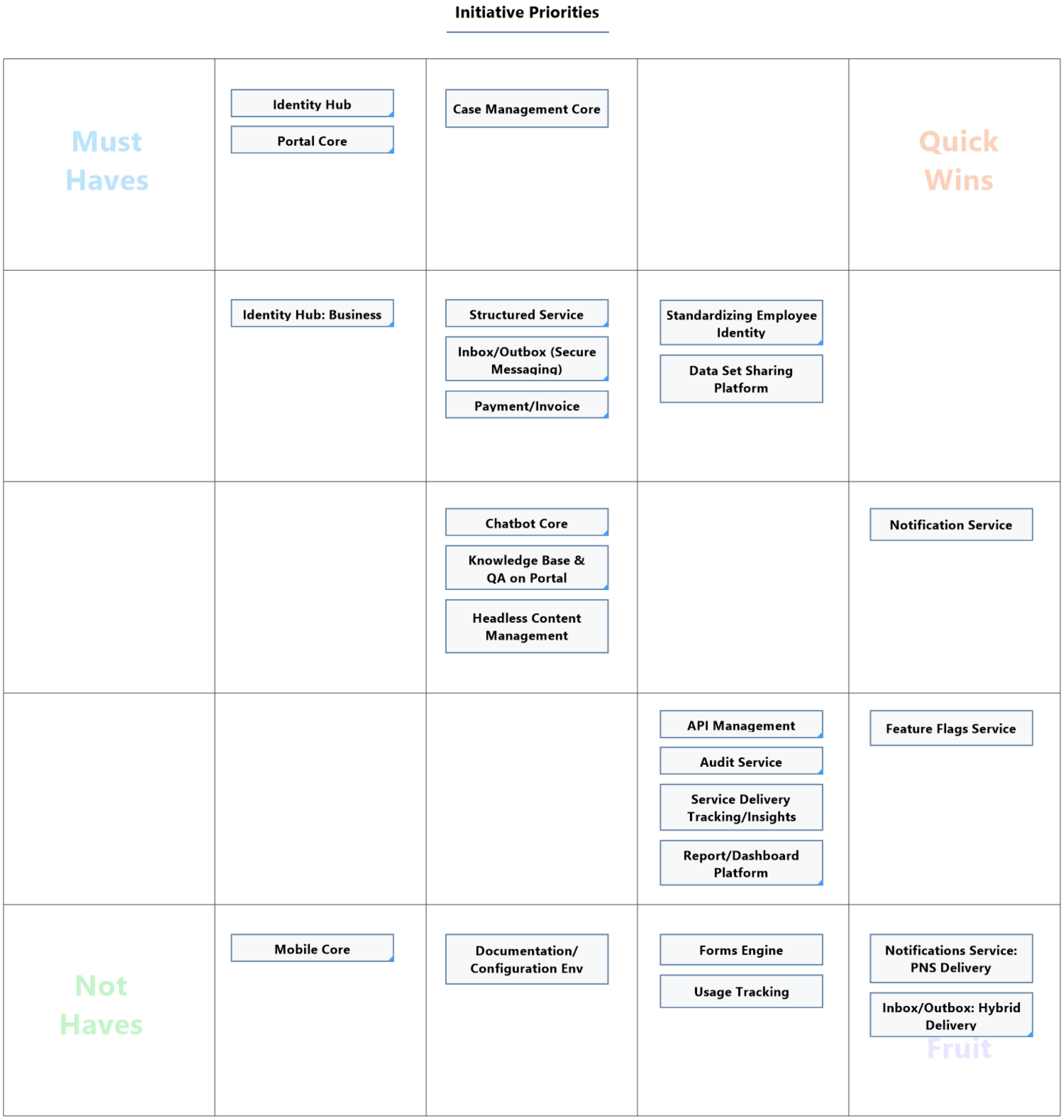
This subsection defines the suggested initiatives to close the gap identified between current situation with common services and platform and future state envisioned. There are three types of initiatives:

- **technical initiatives** are about enhancing technical capabilities by implementing new services or upgrading existing ones;
- **organisational initiatives** are about changing the teams or introducing new teams to achieve the required level of organizational support to achieve the outlined citizen service delivery goals;
- **process initiatives** are about changing existing processes or introducing new ones with the goal of achieving required level of involvement for governance purposes of citizen service IT investments.

4.1.1. Technical

Overview of the technical initiatives to implement and their relative value and resource complexity is summarized in Figure 14.

Note that prioritization results displayed in Figure 14 is based on isolated initiative value and size, not dependencies among the initiatives. Roadmap described in section 4.3 considers both initiative priorities identified in this section as well as technical dependencies, e.g. the fact that Documentation/Configuration Environment is a lower value, it is needed to implement higher level services like Data Set Sharing platform means that it from roadmap perspective needs to come first.



Must Haves	Identity Hub Portal Core	Case Management Core		Quick Wins
	Identity Hub: Business	Structured Service Inbox/Outbox (Secure Messaging) Payment/Invoice	Standardizing Employee Identity Data Set Sharing Platform	
		Chatbot Core Knowledge Base & QA on Portal Headless Content Management		Notification Service
			API Management Audit Service Service Delivery Tracking/Insights Report/Dashboard Platform	Feature Flags Service
Not Haves	Mobile Core	Documentation/ Configuration Env	Forms Engine Usage Tracking	Notifications Service: PNS Delivery Inbox/Outbox: Hybrid Delivery Fruit

Figure 14: Technical initiatives, their size and value

Detailed list of technical initiatives with their description, sourcing strategy and list of depending projects, dependencies and business reasoning is provided in Appendix 5.5.

4.1.2. Organizational Initiatives

The establishment and integration of an Enterprise Architecture function is the main organisational initiative in scope for analysis and development. As the EA function is developed in line with the recommendations below, it is expected that additional organisation and process initiatives will be identified such as the establishment and progression of capabilities such as Application Portfolio Management, Project Portfolio Management and Adoption and Change Management.

4.1.2.1. EA Maturity Development

Developing the maturity of Architecture principles and practices, through the establishment of the EA function is a critical initiative the needs to be a formal part of the DSS roadmap. This requires prioritisation, sustained planning and investment to deliver on the interim and target objectives for the function. For the purposes of discussion, interim objectives should be considered in a 6-12 month timeframe while the target objective was considered to by a 2-3 year investment plan.

For each of the capability areas assessed as part of the EA function, the following items have been highlighted as interim state and target state objectives

Capability Area	Interim Objectives	Target Objective
Stakeholder Involvement & Support **Current State:** 1 - Basic **Target State:** 3 - Managed	▪ IGIB Awareness & support of EA function ▪ DHoT moved from awareness to support and endorsement of Architecture blueprint and Roadmap	▪ Part of dept. business planning ▪ CEO & Departmental board engagement & support ▪ EA roadmaps linked to department 2-5 year plan
Architecture Governance / Compliance **Current State:** 1.5 Basic-Repeat **Target State:** 3 - Managed	▪ Architecture process checkpoints defined and aligned with current governance structures (TDG/SDA) ▪ Terms of reference and membership for SDA/TDG reviewed. ▪ Engage with GDS to compare/contrast and learn from their experience	▪ Contracts include EA defined mandatory requirements as part of contract assessment ▪ Effectiveness of governance functions is being measured / tracked and reported back to IGIB
Management of EA Team **Current State:** 1 - Basic **Target State:** 3 - Managed	▪ EA function is defined ▪ EA core team roles described, team size defined and established ▪ EA Process and EA execution defined ▪ EA teaming model defined and sized ▪ EA function development roadmap	▪ EA team with full compliment ▪ Certification paths completed ▪ Role progression are well defined. ▪ Well proven RACI model ▪ Participation in relevant EA forums and bodies
Architecture Scope **Current State:** 1 - Basic **Target State:** 3 - Managed	▪ More rigor around the same scope (greater visibility of and collaboration on projects within DSS) ▪ DSS Critical IT Services & Applications (where there is accountability)	▪ Scope of EA activities should encompass all ESS applications in EA portfolio & roadmap

Capability Area	Interim Objectives	Target Objective
Architectural Standards **Current State:** 1 - Beginning **Target State:** 3 - Managed	▪ List of key main processes & templates identified, described and "published" on Intranet ▪ EA Framework(s) evaluated, and direction decided (e.g. TOGAF) ▪ EA tooling investigated	▪ Methodology adopted and in use
Regulatory / Govt / Industry Standards **Current State:** 1 - Basic **Target State:** 2 - Repeatable	▪ Standards investigation and adopted into EA planning. e.g.; ○ GDS Standards Guidance assessed ○ UxM Standard ○ Cyber Security Standards ○ Accessibility Standards (EU Directive) ○ Cloud Security Principles	▪ Adherence to key agreed industry standards
Architectural Planning Horizon **Current State:** 1 - Basic **Target State:** 3 - Managed	▪ Key capabilities for following 12 months, planned/resourced and committed	▪ 2-5 year architecture development plan in place ▪ 6-month review process in place
Architectural Quality **Current State:** 1 - Beginning **Target State:** 2 - Repeatable	▪ The list of Architectural Quality attributes outlined above have been approved. ▪ Dry run Architecture quality review on specific project/solution and produce assessment	▪ Architecture Quality attributes are part of the contract / solution evaluation. ▪ Architecture quality is a mandated part of the Post Project Evaluation (PPE). ▪ Quality assessments are a peer-reviewed learning activity
Business linkages **Current State:** 2 - Repeatable **Target State:** 3 - Managed	▪ All projects in agreed PM tool (PV) ▪ PM process adopted across DSS ▪ Assess PM tool for use in EA Portfolio planning	▪ As per Stakeholder & Governance capabilities ▪ EA drives & inputs to portfolio optimisation (this process needs to be developed first) ▪ All target departments following defined PM process ▪ Adhered to Demand Management process (this process needs to be developed first)

Capability Area	Interim Objectives	Target Objective
Business Architecture **Current State:** 0 - Beginning **Target State:** 2 - Repeatable	▪ Understand what business process / business model documentation exists within current served departments. ▪ Understand Business Architecture modelling as it related to EA	▪ Requirements influenced by input from EA function and capabilities that exist
Information Architecture **Current State:** 0 - Beginning **Target State:** 2 - Repeatable	▪ Completion of Information View in section outlined above ▪ Evaluation of Information Asset register ▪ Define Privacy by Design EA guidelines and standards ▪ Understand IA current review & scope ▪ Information Architecture awareness and definition	▪ Information Architecture is a core discipline of the EA function maintaining
Solutions / Application Architecture **Current State:** 1 - Basic **Target State:** 3 - Managed	▪ Adoption of capability definition, language and terminology for application & solution architecture ▪ Completion of systems register ▪ Evaluate register to determine solution architecture patterns and capability gaps.	▪ Standards defined, adopted and monitored through established processes and governance
Technology Architecture **Current State:** 1 - Basic **Target State:** 3 - Managed	▪ Completion of systems register ▪ Evaluate register to determine additional infrastructure architecture patterns and Service map gaps. ▪ Adoption of IT Service map and Infrastructure Views	▪ Shaping Technology requirements regularly and in advance of upcoming platforms and solutions
Impact **Current State:** 0 - Beginning **Target State:** 2 - Repeatable	▪ EA Team awareness ▪ EA Standards / Guidelines outlined ▪ 2 quick wins for EA gained ▪ Status & progress communication	▪ Value measures defined

4.1.3. Process Initiatives

One of the initiatives outlined in the EA maturity development is to examine the remit and terms of reference of each of the Governance function groups in line with the existence of an Enterprise Architecture function.

4.1.3.1. EA Governance Development

As part of the Organisation analysis work, the existing oversight and governance structure was discussed. It is recognised that this is currently evolving, and this will need to be reviewed once the new governance structures are established. The primary relevant Governances teams identified as being responsible for oversight of the delivery of services are outlined in the table below with a review of how aligned the current remit is with the proposed remit of the Enterprise architecture function.

Group	Remit	EA Alignment
IGIB – Information Governance & Innovation Board	Strategy, Oversight, Signoff. Provide strategic governance for Information Technology, Information Assurance, Information Management. Owns and monitors the overarching NICS strategy.	**High** – Given the required business linkage, driving of standards and input to strategy development
SDA – Solution Design Authority	Standards, Technical Direction. Technical Approvals, Principles. Role to set standards, technical direction and approve technical design of new ICT services	Medium – Standards and principles required to be aligned at this point with process for approvals and exceptions.
TDG – Technical Design Group	Solution reviews, technical and application portfolio management.	Medium – Insight into Solution, Application & Technical specifications and requirements.
DHoT – Department Heads of Technology	Experience sharing, oversight, planning	Low – Provides insight into priorities, projects and general experience sharing.

At the current understanding, it is viewed that the EA function should report to and have a representation at IGIB in order to drive the effective alignment of business and technology priorities and investments as this is the area of strongest alignment. It is not recommended at this point to initiate a new governance structure given the EA function is only in early mobilisation phase. This should be reviewed as the function, goals and objectives evolve.

4.2. Benefit Dependency Map

A benefit dependency network (BDN) is a diagram having a specific structure that visualizes multiple cause-effect relationships organized into capabilities, changes and benefits. It is usually read from right to left to provide a one-page overview of how a business vision and outcomes can be achieved, and what is the supporting role of technology capabilities[2]. As such benefits dependency map allows to validate if and how technology capabilities help achieve overall goals set out by the government.

Note that benefits dependency map also defines organisational changes that need to be made and new business approaches that will be followed going forward (called business changes).

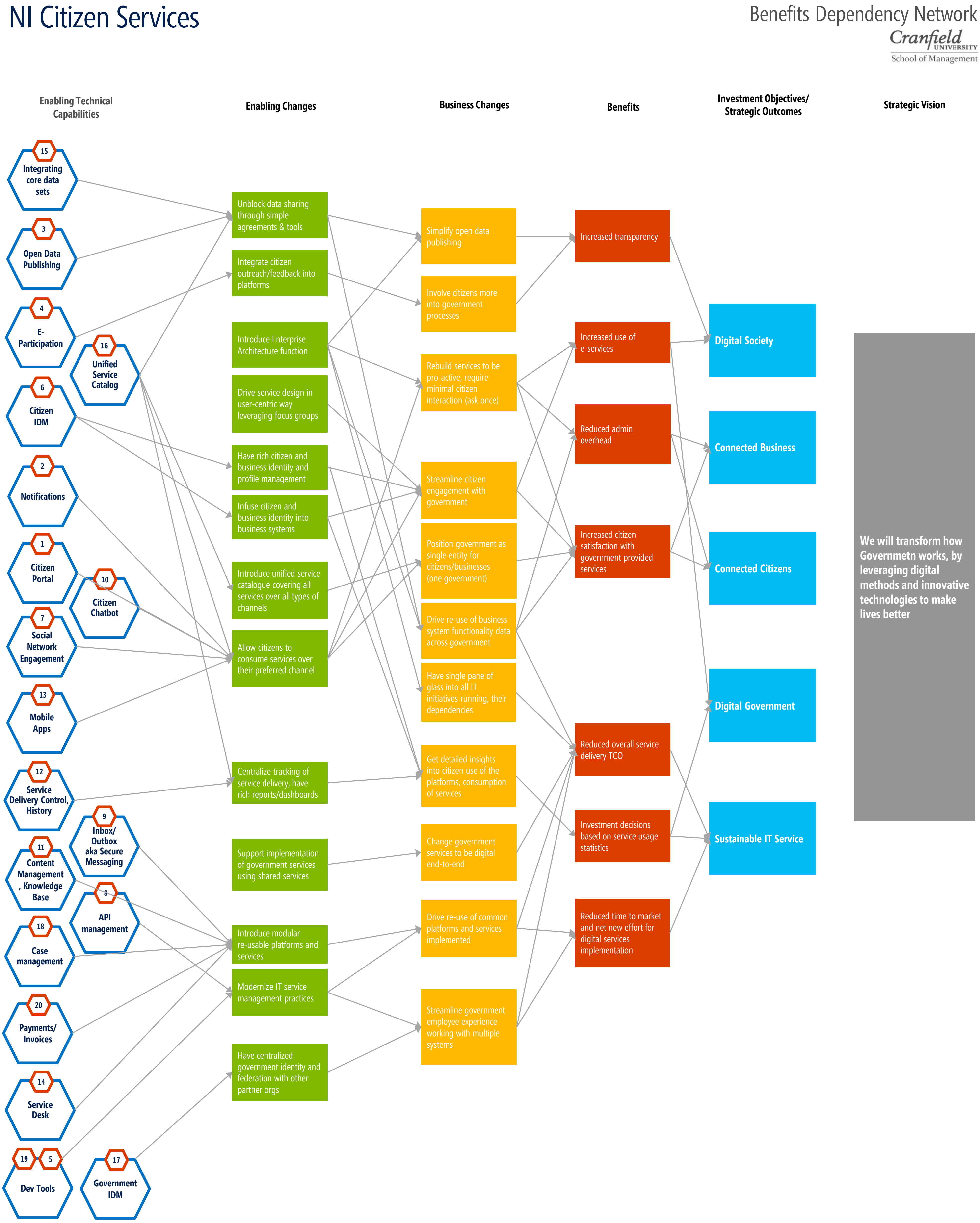
Not all enabling changes and business changes should have links to technology enablers if these are more process changes or team changes.

Examples providing more information on use of BDNs can be found in Harvard Business Review article on planning digital initiatives[3].

Figure 15 provides a BDN relating to the DSS engagement.

[2] See more in Benefits Management Best Practice Guidelines by John Ward, Peter Murray and Elizabeth Daniel, Cranfield School of Management, 2004

[3] See https://hbr.org/2016/06/a-tool-to-map-your-next-digital-initiative



NI Citizen Services

Benefits Dependency Network

Cranfield UNIVERSITY School of Management

Enabling Technical Capabilities

15 Integrating core data sets

3 Open Data Publishing

4 E-Participation

16 Unified Service Catalog

6 Citizen IDM

2 Notifications

1 Citizen Portal

10 Citizen Chatbot

7 Social Network Engagement

13 Mobile Apps

12 Service Delivery Control, History

9 Inbox/ Outbox aka Secure Messaging

11 Content Management , Knowledge Base

8 API management

18 Case management

20 Payments/ Invoices

14 Service Desk

19 5 Dev Tools

17 Government IDM

Enabling Changes

Unblock data sharing through simple agreements & tools

Integrate citizen outreach/feedback into platforms

Introduce Enterprise Architecture function

Drive service design in user-centric way leveraging focus groups

Have rich citizen and business identity and profile management

Infuse citizen and business identity into business systems

Introduce unified service catalogue covering all services over all types of channels

Allow citizens to consume services over their preferred channel

Centralize tracking of service delivery, have rich reports/dashboards

Support implementation of government services using shared services

Introduce modular re-usable platforms and services

Modernize IT service management practices

Have centralized government identity and federation with other partner orgs

Business Changes

Simplify open data publishing

Involve citizens more into government processes

Rebuild services to be pro-active, require minimal citizen interaction (ask once)

Streamline citizen engagement with government

Position government as single entity for citizens/businesses (one government)

Drive re-use of business system functionality data across government

Have single pane of glass into all IT initiatives running, their dependencies

Get detailed insights into citizen use of the platforms, consumption of services

Change government services to be digital end-to-end

Drive re-use of common platforms and services implemented

Streamline government employee experience working with multiple systems

Benefits

Increased transparency

Increased use of e-services

Reduced admin overhead

Increased citizen satisfaction with government provided services

Reduced overall service delivery TCO

Investment decisions based on service usage statistics

Reduced time to market and net new effort for digital services implementation

Investment Objectives/ Strategic Outcomes

Digital Society

Connected Business

Connected Citizens

Digital Government

Sustainable IT Service

Strategic Vision

We will transform how Governmetn works, by leveraging digital methods and innovative technologies to make lives better

Figure 15: Business dependency traceability network

4.3. Initial Plan

This subsection defines an initial implementation plan for both technical capability changes and for process and organizational initiatives.

4.3.1. Technical Initiatives

Overall roadmap representing all initiatives and based on dependencies as well as taking into account sizes of implementation and also priorities is displayed in Figure 16.

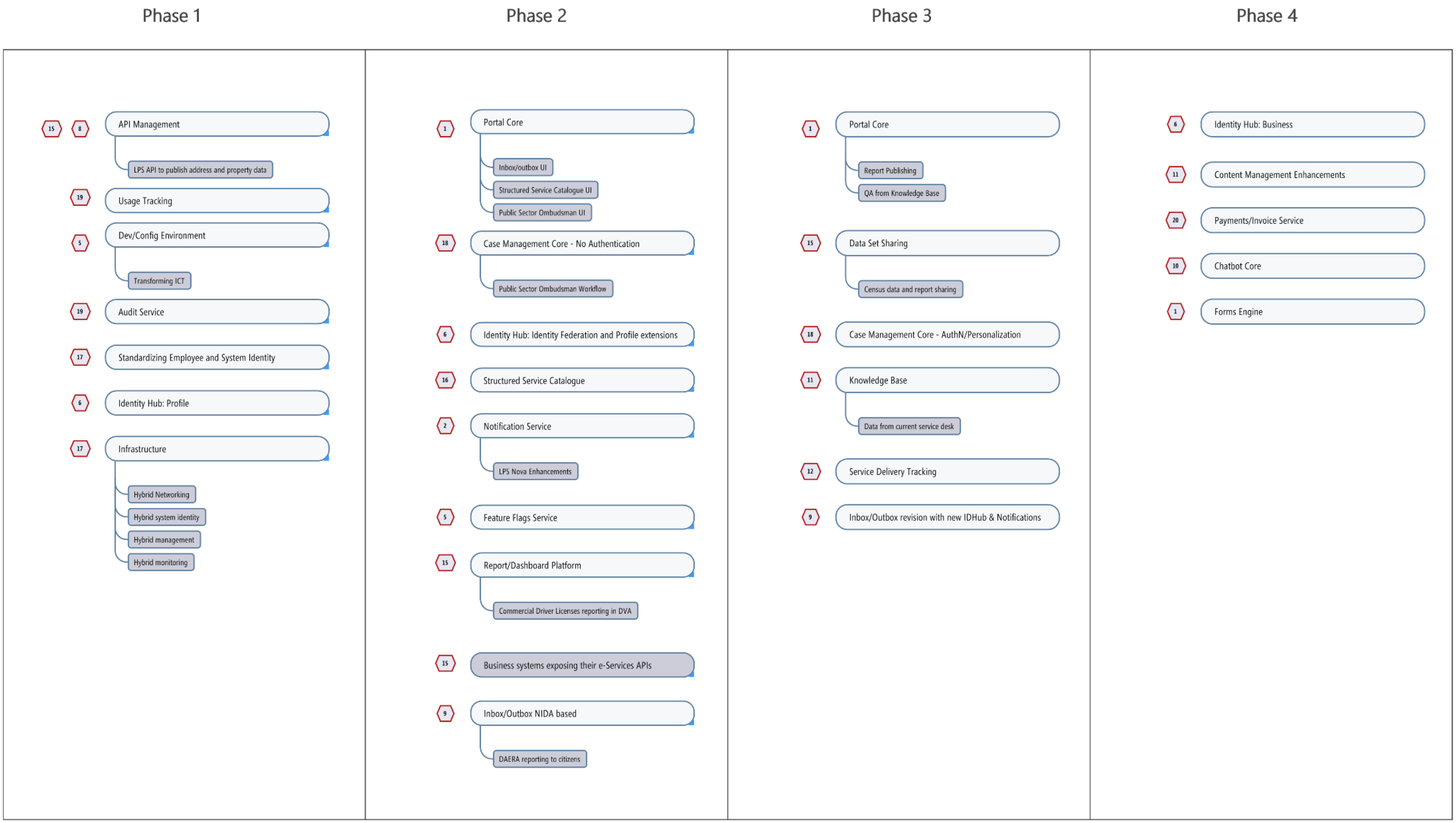

Phase 1
15
8
API Management
LPS API to publish address and property data
19
Usage Tracking
5
Dev/Config Environment
Transforming ICT
19
Audit Service
17
Standardizing Employee and System Identity
6
Identity Hub: Profile
17
Infrastructure
Hybrid Networking
Hybrid system identity
Hybrid management
Hybrid monitoring
Phase 2
1
Portal Core
Inbox/outbox UI
Structured Service Catalogue UI
Public Sector Ombudsman UI
18
Case Management Core - No Authentication
Public Sector Ombudsman Workflow
6
Identity Hub: Identity Federation and Profile extensions
16
Structured Service Catalogue
2
Notification Service
LPS Nova Enhancements
5
Feature Flags Service
15
Report/Dashboard Platform
Commercial Driver Licenses reporting in DVA
15
Business systems exposing their e-Services APIs
9
Inbox/Outbox NIDA based
DAERA reporting to citizens
Phase 3
1
Portal Core
Report Publishing
QA from Knowledge Base
15
Data Set Sharing
Census data and report sharing
18
Case Management Core - AuthN/Personalization
11
Knowledge Base
Data from current service desk
12
Service Delivery Tracking
9
Inbox/Outbox revision with new IDHub & Notifications
Phase 4
6
Identity Hub: Business
11
Content Management Enhancements
20
Payments/Invoice Service
10
Chatbot Core
1
Forms Engine

Figure 16: Overall roadmap based on dependencies and priorities in phases

Figure 16 shows all technical initiatives and their dependencies, balancing out the load over multiple phases without identifying specific timelines. Figure 17, Figure 18, Figure 19 and Figure 20 identify different paths through the overall dependency roadmap, planning the implementation of various services over multiple quarters. Note that all of these cannot be approached together without significant resource commitment. Therefore, further prioritization would need to be made or multiple teams involved if multiple programs of work would be required simultaneously.

Figure 17 shows roadmap of implementation of inbox/outbox aka secure messaging implementation that is split into two releases – one release that is based on current services, e.g., NIDA for authentication, another release that is leveraging external identity hub for more options for identity and profile management, it also leverages enhanced notifications service and it enables citizens to subscribe to subscription services that often would be provided using inbox/outbox.

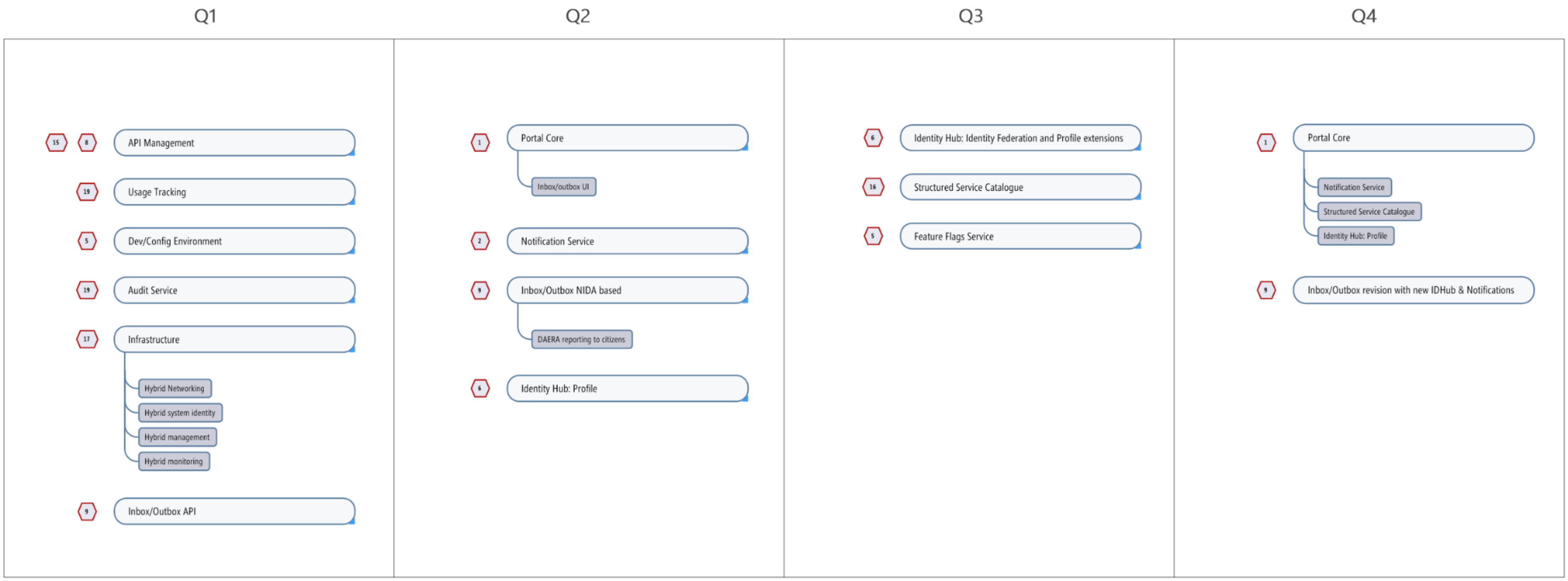


Figure 17: Inbox only roadmap enabling two releases

Figure 18 shows program of work associated with implementing a shared developer platform for case management and multiple specific services on top of it. Figure shows three deliveries happening over the period of 4 quarters – initial release supporting non-personalized cases, second release supporting user personalization, therefore tracking of case statuses via Service Delivery Tracking. The third release is where paid services are supported by the platform through improved payment service integration.

Note that figure shows multiple specific services that can be implemented as anchor projects on top of the platforms so that each platform improvement launch is associated with at least one specific department service leveraging the platform already. It then can be used as example for evaluating implementation of other services on top of the platform. This is a living document so DSS should continue to update the figure below.

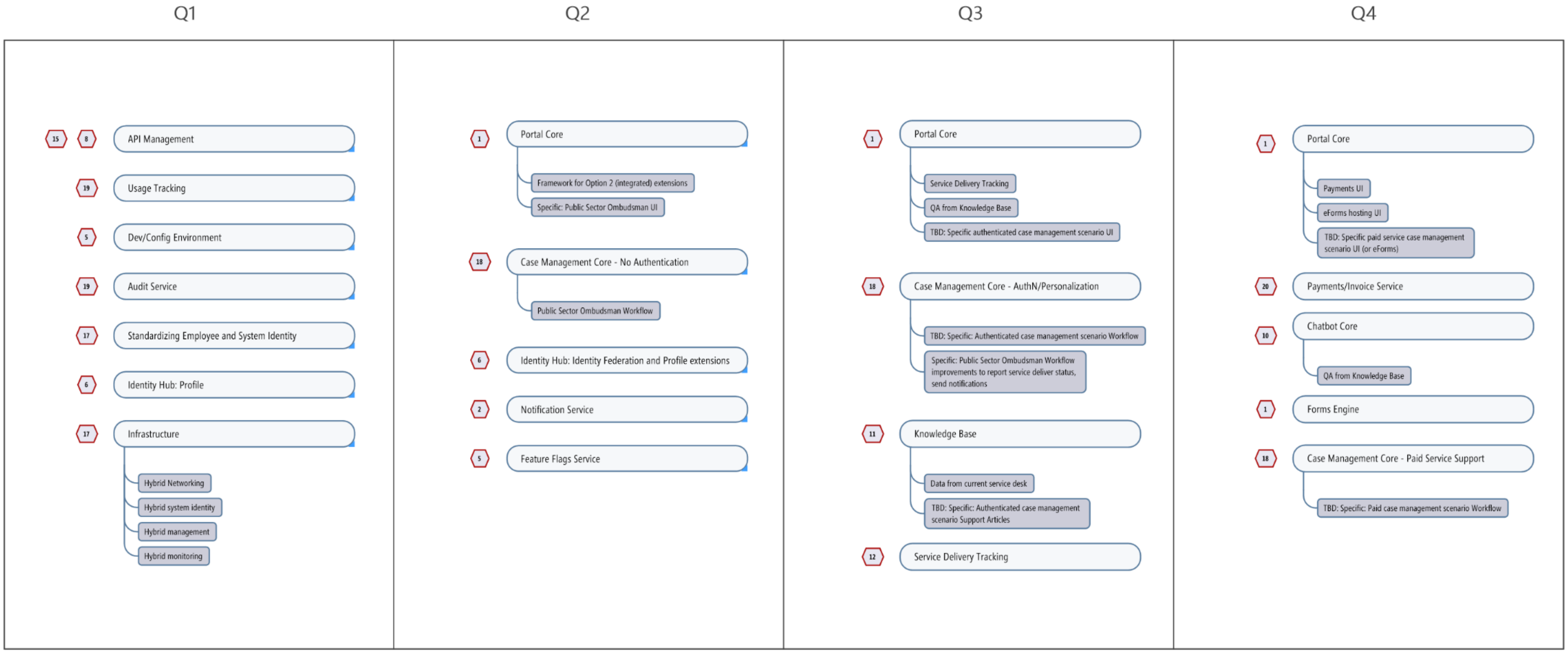

Q1
Q2
Q3
Q4
15
8
API Management
19
Usage Tracking
5
Dev/Config Environment
19
Audit Service
17
Standardizing Employee and System Identity
6
Identity Hub: Profile
17
Infrastructure
Hybrid Networking
Hybrid system identity
Hybrid management
Hybrid monitoring
1
Portal Core
Framework for Option 2 (integrated) extensions
Specific: Public Sector Ombudsman UI
18
Case Management Core - No Authentication
Public Sector Ombudsman Workflow
6
Identity Hub: Identity Federation and Profile extensions
2
Notification Service
5
Feature Flags Service
1
Portal Core
Service Delivery Tracking
QA from Knowledge Base
TBD: Specific authenticated case management scenario UI
18
Case Management Core - AuthN/Personalization
TBD: Specific: Authenticated case management scenario Workflow
Specific: Public Sector Ombudsman Workflow improvements to report service deliver status, send notifications
11
Knowledge Base
Data from current service desk
TBD: Specific: Authenticated case management scenario Support Articles
12
Service Delivery Tracking
1
Portal Core
Payments UI
eForms hosting UI
TBD: Specific paid service case management scenario UI (or eForms)
20
Payments/Invoice Service
10
Chatbot Core
QA from Knowledge Base
1
Forms Engine
18
Case Management Core - Paid Service Support
TBD: Specific: Paid case management scenario Workflow

Figure 18: Case management roadmap with multiple iterations

Figure 19 shows the program of work associated with improving data sharing. Three types of data sharing are supported through the capabilities built out as part of this program:

- Functionality and data sharing through REST based APIs that are managed through API management;
- Report creation and sharing that enables internal and external users access dynamic reports on top of internal and external data;
- Data set sharing enabling sharing larger data sets as full data sets, enables transformation of data before sharing and provides API access to these transformed and cached data sets.

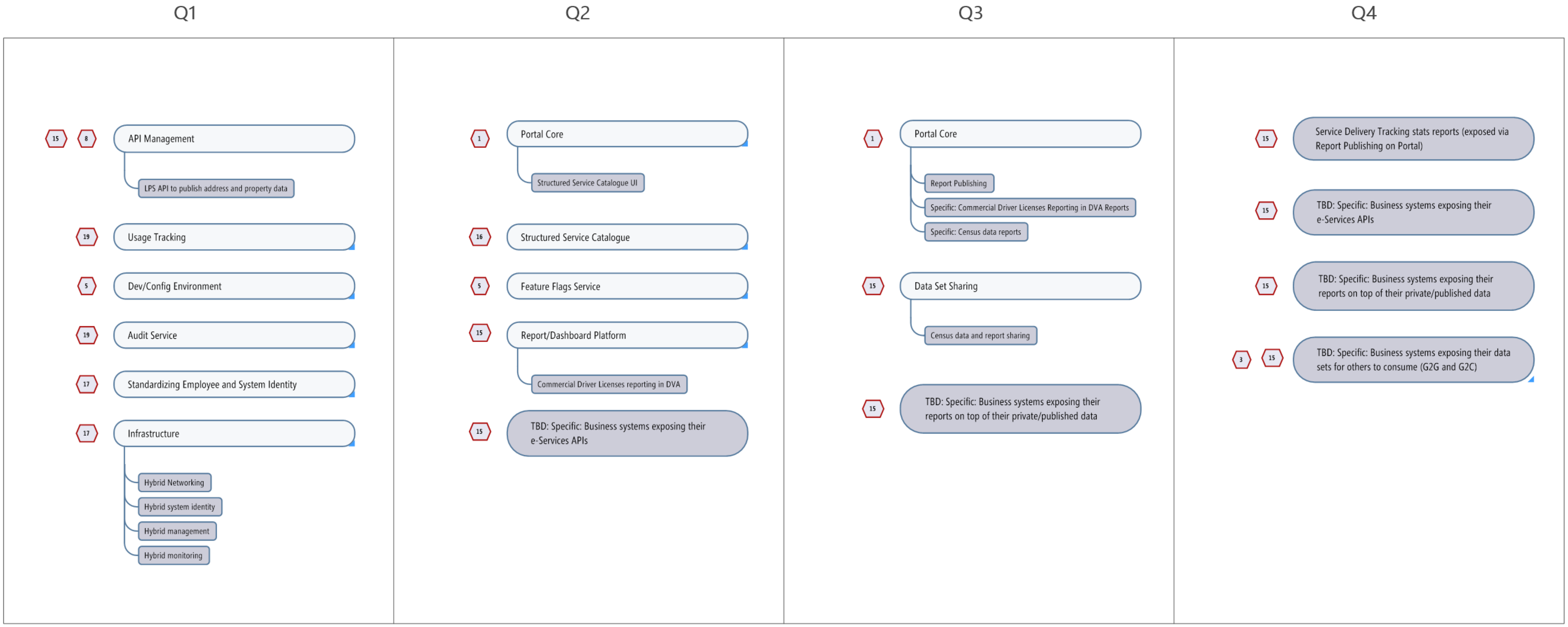

Q1
Q2
Q3
Q4
15
8
API Management
LPS API to publish address and property data
19
Usage Tracking
5
Dev/Config Environment
19
Audit Service
17
Standardizing Employee and System Identity
17
Infrastructure
Hybrid Networking
Hybrid system identity
Hybrid management
Hybrid monitoring
1
Portal Core
Structured Service Catalogue UI
16
Structured Service Catalogue
5
Feature Flags Service
15
Report/Dashboard Platform
Commercial Driver Licenses reporting in DVA
15
TBD: Specific: Business systems exposing their e-Services APIs
1
Portal Core
Report Publishing
Specific: Commercial Driver Licenses Reporting in DVA Reports
Specific: Census data reports
15
Data Set Sharing
Census data and report sharing
15
TBD: Specific: Business systems exposing their reports on top of their private/published data
15
Service Delivery Tracking stats reports (exposed via Report Publishing on Portal)
15
TBD: Specific: Business systems exposing their e-Services APIs
15
TBD: Specific: Business systems exposing their reports on top of their private/published data
3
15
TBD: Specific: Business systems exposing their data sets for others to consume (G2G and G2C)

Figure 19: Data sharing roadmap with multiple data sharing options included

Figure 20 shows the initiatives required to implement identity hub that enables authentication through broad set of providers and also that would manage detailed profile information not only for citizens (including service subscriptions, service delegations), but also for other types of profiles – non-residents, business representatives.

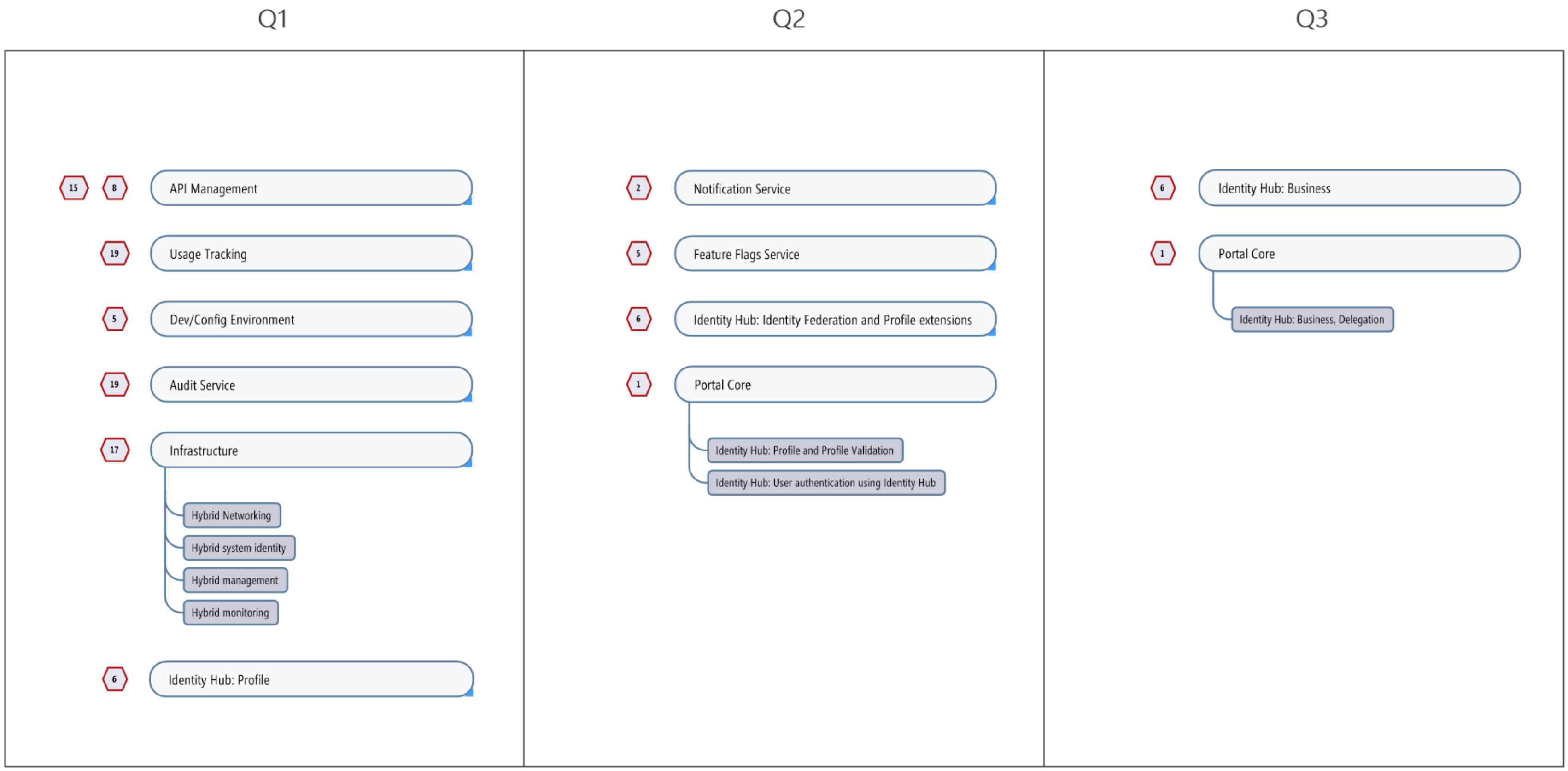


Figure 20: Enhanced identity hub service roadmap

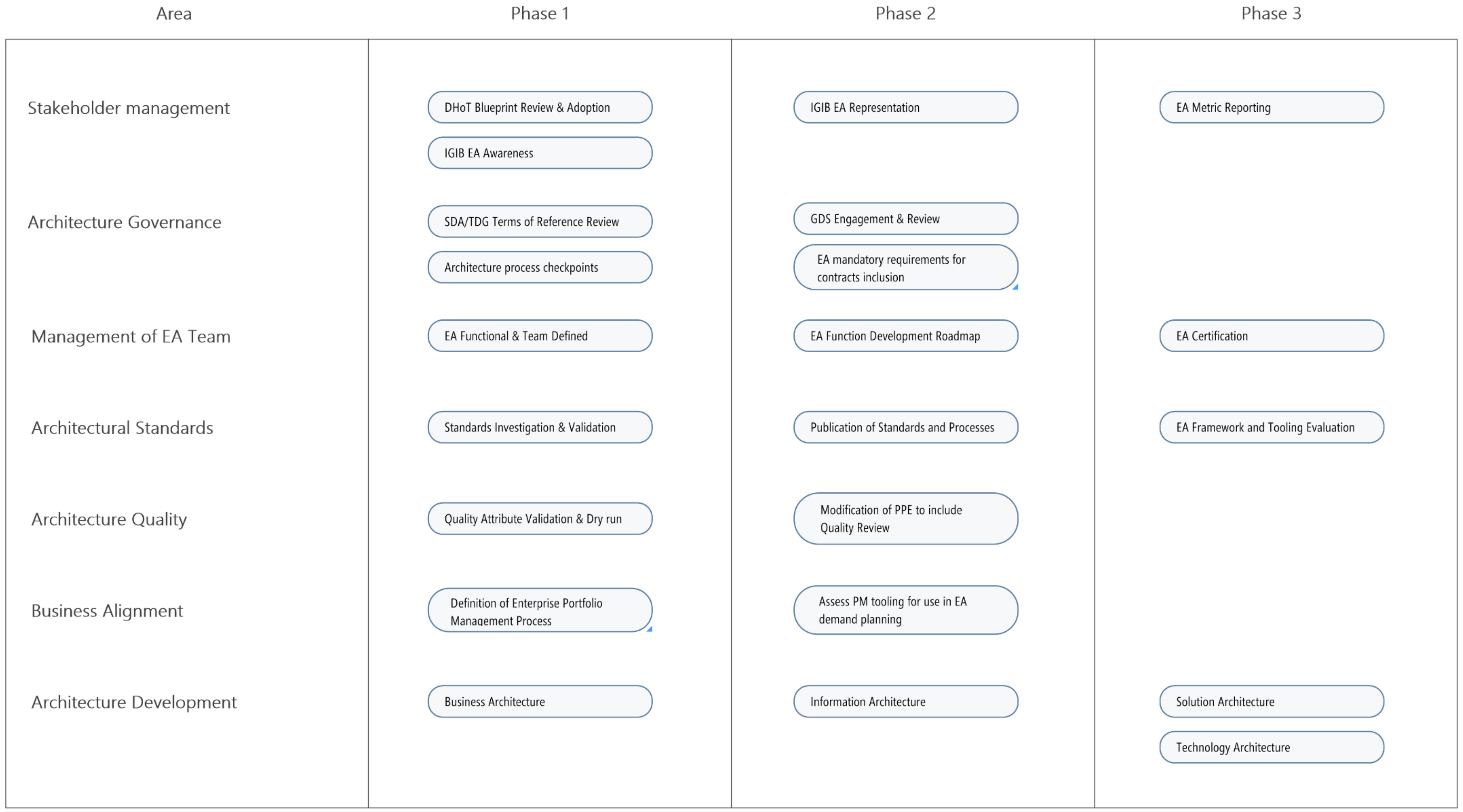
4.3.2. EA dependent Organisational Initiatives

Organisational and process change initiatives related to development and maturing enterprise architecture function are summarized in Figure 21.

The diagram outlines the roadmap to mature the capabilities of the EA function from current to identified target state, starting with foundational elements in Phase 1. The foundational elements of priority are focused primarily on EA Stakeholder Management, EA Function Definition & Business Alignment. These three core pillars are currently low maturity but are also critical to provide direction and focus on the future development roadmap. Focusing on these elements first will inform future plans, direction and investment.

The other three areas of foundational work; Standards, Quality & Governance seek to maximise on what is already in place. The intent should be to document and collaborate with a wider stakeholder audience to start the process of governance and standardisation.

Phase 2 & Phase 3 of these pillars then seeks to develop the maturity of these areas to move towards the target state.



Area	Phase 1	Phase 2	Phase 3
Stakeholder management	DHoT Blueprint Review & Adoption IGIB EA Awareness	IGIB EA Representation	EA Metric Reporting
Architecture Governance	SDA/TDG Terms of Reference Review Architecture process checkpoints	GDS Engagement & Review EA mandatory requirements for contracts inclusion	
Management of EA Team	EA Functional & Team Defined	EA Function Development Roadmap	EA Certification
Architectural Standards	Standards Investigation & Validation	Publication of Standards and Processes	EA Framework and Tooling Evaluation
Architecture Quality	Quality Attribute Validation & Dry run	Modification of PPE to include Quality Review	
Business Alignment	Definition of Enterprise Portfolio Management Process	Assess PM tooling for use in EA demand planning	
Architecture Development	Business Architecture	Information Architecture	Solution Architecture Technology Architecture

Figure 21: EA dependent organisational initiatives

5. Appendices

Appendices included provide additional details/explanation of the contents of the document.

5.1. Glossary of Key Terms

Table 11 details the key terms, acronyms and abbreviations used in this document.

Table 11: Key terms

Term	Description
ALM	Application Lifecycle Management
API	Application Programming Interface
CI/CD	Continuous integration, continuous delivery
COTS	Commercial of the Shelf
DAERA	Department of Agriculture, Environment and Rural Affairs
DFI	Department for Infrastructure
DHoT	Department Head of Technology
DSS	Digital Shared Services
DTS	Digital Transformation Service
EA	Enterprise Architecture
EAM	Enterprise Architecture Management
EIDAS	Electronic Identification, Authentication and trust Services
ERP	Enterprise Resource Planning
EU	European Union
FYI	For Your Information
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government

Term	Description
GDS	Government Digital Service
GP	General Practitioner
HMRC	Her Majesty's Revenue and Customs
IaaS	Infrastructure as a Service
ICT	Information Communication Technology
IDM	Identity Management
IGIB	Information Governance & Innovation Board
IT	Information Technology
JSON	JavaScript Object Notation
LPS	Land and Property Service
MOT	Vehicle Test
MS	Microsoft
MSFT	Microsoft
NCSC	National Cyber Security Centre
NGO	Non-governmental organisation
NI	Northern Ireland
NICS	Northern Ireland Civil Service
NISRA	Northern Ireland Statistics and Research Agency
OSG	Operating Systems Group (division of Microsoft)
PaaS	Platform as a Service
PII	Personal Identifiable Information
PNS	Push Notification Service

Term	Description
REST	Representational State Transfer
SaaS	Software as a Service
SDA	(Strategic) Solution Design Authority
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SME	Subject Matter Expert
SMS	Short Message Service
TDG	Technical Design Group
UI	User Interface
UX	User Experience
UXM	User Experience Model
VM	Virtual Machine

5.2. Inflight and Planned Projects

Capabilities	Service	Project/Scenario	Dept/Branch
API Management, Content Management, Notifications, Identity Management, Unified Service Catalogue, Open Data Publishing, Social Network Engagement, Integrating Core Datasets	**Internet**	Further development of the Drupal Platform	Digital Development
		SPORTNI - new website (s)	SPORTNI
Content Management, API Management, Notifications, Identity, Social Network Engagement, Chat Bot?		TollyMore National Outdoor Centre - new website	SPORTNI
Content Management, API Management, Notifications, Identity		Minister's Artwork	DoF - Minister's Office

Capabilities	Service	Project/Scenario	Dept/Branch
Content Management, API Management, Open Data Publishing		Register of Legal Aid Practitioners	DoJ
		HSC Applications / Widgets	SPORTNI - new website (s)
Content Management, API Management, Case Management, Notifications, Identity, Service History, Usage Tracing		NIPS Prison Visits online form	DOJ - NIPS
Content Management, API Management, Open Data Publishing		Pharmacy Plus Project	HSC
Content Management, API Management, Service Desk, Case Management, Notifications, Identity (Employee), Inbox/Outbox, Usage Tracing, Secure Document Store	**Application Development**	State Pathology Case Management System	DoJ SPD
API Management, Identity (Employee), Case Management, Notifications, Usage Tracing		IT Assist MADRAS Rewrite	DoF - IT Assist
Content Management, Citizen Portal, API Management, Service Desk, Case Management, Notifications, Identity (Citizen/Employee), Inbox/Outbox, Usage Tracing, Secure Document Store		Public Services Ombudsman's CMS rewrite	NI Ombudsman Office
Content Management, Citizen Portal, API Management, Service Desk, Case Management, Notifications, Identity (Citizen/Employee), Inbox/Outbox, Usage Tracing, Secure Document Store		NICS FOI Tracking System	DoF - ESS
Content Management, API Management, Open Data Publishing, Identity (employee), Integrating Core Data Sets		NICS Contractors Rota	DoF - CPD

Capabilities	Service	Project/Scenario	Dept/Branch
Content Management, API Management, Open Data Publishing, Identity (employee), Integrating Core Data Sets		DoH Upgrade of the NIAIC Incident Register	DoH
API Management, Case Management, Identity (employee), Integrating Core Data Sets, Usage Tracing, Mobile Apps		Pharmaceutical Inspection System	DoH
API Management, Case Management, Notifications, Identity (citizen/Employee), Inbox/Outbox, Secure Document Store, Integrating Core Data Sets		NICS HR Contractors Vetting System	DOF - NICS HR
Content Management, API Management, Service Desk, Case Management, Notifications, Identity (Employee), Inbox/Outbox, Usage Tracing, Secure Document Store		AFMD Accountability Grid System	DoF - PSD
Content Management, Citizen Portal, API Management, Open Data Publishing, Integrating Core Data Sets		Publication of Non-domestic Valuation List	DoF - LPS
API Management, Case Management, Notifications, Identity (Citizen/Employee), Inbox/Outbox, Secure Documents Storage, Integrating Core Data Sets		LPS Reval Online Valuation Review Form	DoF - LPS
API Management, Identity (Employee), Usage Tracing, Mobile Apps		NISRA Census Payroll System	DoF - NISRA
Community Info Branch and Hospital Info Branch/Extranet/Identity/Reports		Rewrite of DoH IAD CIB and HIB systems	DoH
Notifications, API Management, Identity Employee, Integrating Core Data Sets, Usage Tracing		Making Tax Digital For VAT	DoF - AccountNI
Content Management, Citizen Portal, API Management, Notifications, Integrating Core Data Sets, Social Network Engagement, Mobile apps		Careers Mobile App	DfE

Capabilities	Service	Project/Scenario	Dept/Branch
API Management, Identity (Citizen/Employee), Case Management, Inbox/Outbox, Secure Document Storage		Substance Misuse Database Rewrite	DoH
Content Management, Citizen Portal, API Management, Service Desk, Case Management, Notifications, Identity (Citizen/Employee), Inbox/Outbox, Usage Tracing, Secure Document Store		Police Ombudsman Case Management System	PONI
Document Store/Identity/Reporting/CMS/Register		Retail Energy Market Monitoring	UREGNI

5.3. EA Capability Model – Capability Definitions

Table 12: capability definitions

Capability	Sub-Capability	Description
Business Enablement & Strategy		Business Enablement is a grouping of related capabilities that advances an organization's business through enabling capabilities that drive business strategy, governance, organization and key business processes.
	Strategy and Planning	Capability that directly creates, drives, or influences a business-driven organizational strategy, direction, and decision making, enabled by business solutions
	Innovation Management	Discovery, enhancing, fostering or managing innovation in support of the advancement of business strategy and objectives
	Value Management	Modelling, tracking and managing business value definitions, metrics, and forecasts and their relationships to the business architecture
	Business Architecture & Modelling	Rationalizing the business strategy, capabilities, motivations, values, drivers and organization factors to better understand the business
	Opportunity Identification	Identifying, modelling, tracking and managing the business and IT opportunity lifecycle

Capability	Sub-Capability	Description
EA Management (EAM)		Capabilities that enable the definition, management, and governance of the enterprise's architectural IT assets and standards
	Standards Mgmt	Standards definition and exceptions reviews for applications, infrastructure, and services
	Engagement Mgmt	Enterprise-level quality assurance and oversight: standards compliance stage-gate architecture reviews
	Vendor Strategy	Identification, oversight and partnerships with the strategic vendors of the organization
Technology Lifecycle		The lifecycle management of information and related technology used by an organization
	Architecture Change Mgmt	Ensure solution alignment with target business value throughout organizational changes
	Enterprise Information Mgmt	Standardization of critical data for IT and business partner decision-making
	Application Portfolio Management	Documentation and analysis of applications, infrastructure, data, and links to business process
	Architecture Planning	Process for managing migration from current state to target architecture
	Technology Innovation	Assessment of emerging and new-to-organization technologies for architectural fit and business benefit
Architecture Execution		Capabilities for delivering and managing the execution of enterprise architecture services
	Trade-Off Analysis	Evaluation of alternatives against a given architecture problem that facilitates the decision-making process
	Fit Assessments	Assessment that applies at all levels in the architecting process to assess the level of compliance (i.e., fit) with the current Principles, Policies, and Standards the company has adopted. This allows for solution alignment with organizational mission and strategy.

Capability	Sub-Capability	Description
	Architecture Services	Program or project level activities that an Enterprise Architect engages on that could include: architecture modelling, architecture development, architecture decisions, architecture definition and delivery
	Solution Selection	Detailed specification and construction of solution architectures
	Workshops and Envisioning	Enable cross-organizational processes for the identification and exploration of opportunities and potential solutions
Competency Management		Advancement of an organization's abilities, knowledge, and communication to sustain or amplify the value to the business
	Market Trend Analysis	Identifying, analysing, and rationalizing of key market drivers, impacts and opportunities
	Competency Mgmt & Advancement	Classification, management and advancement of personnel skills and competencies mapped to career ladders
	Collaboration	Fostering an organization's architecture community with communication of key trends, knowledge sharing mechanisms and awareness of architectural information
Enterprise Architecture Governance		Cross organizational governance that spans IT and business units that have broad impact in the organization
	Architecture Review Board	Architecture compliance enforcement, consistency, reuse, and escalation support
	Architecture Guidance Team	Ratifies, maintains, discovers or manages the lifecycles of the principles, policies, standards, building blocks, frameworks and solution guidance
	Executive Steering	Participation in executive relations and communication
	Architecture Risk Mgmt.	Identification, creation, classification and remediation of risks identified through the activities of enterprise architecture and governance functions
Office of Enterprise Architecture		Management, sustainment, and delivery of the function of enterprise architecture

Capability	Sub-Capability	Description
	EA Strategy & Vision	Creation, development, and refinement of the EA's organizational 1 to 3-year plan, strategic initiatives, key organizational and architectural principles and organizational planning
	EA Services Model	The discrete offerings and activities that the Office of EA provides to the enterprise in a service centre manner
	EA Operational Model	The key artefacts, processes, KPI's, SLA's and OLA's that govern the execution of enterprise architecture
	EA Engagement Model	Interaction points, architecture contracts, roles and responsibilities regarding enterprise architecture
	EA Talent Mgmt	Identification of new, development of existing, and recruitment of the knowledge and skills required to enable the function of Enterprise Architecture
	EA Performance Mgmt	Management, monitoring and remediation of the effectiveness and efficiency of Enterprise Architecture for and to the organization to ensure value is delivered to the business
	EA Communication Model	The communication necessary for the adoption and maintenance of enterprise architecture services
	EA Communities Model	The management of the stakeholder groups involved in delivering and consuming EA services
Architecture Segments		Areas of concern for Enterprise Architecture to address as it solves the challenges in the enterprise
	Business Architecture	The business strategy, governance, organization, and key business process information, as well as the interaction between concepts.
	Application Architecture	A description of the major logical groupings of capabilities that manage the data objects necessary to process the data and support the business.
	Information Architecture	The structure of an organization's logical and physical data assets and data management resources beyond data or database implementation and design

Capability	Sub-Capability	Description
	Technology Architecture	The logical software and hardware capabilities that are required to support the deployment of business, information, and application services. This includes IT infrastructure, middleware, networks, communications, processing and standards.
	Security Architecture	Enterprise Architecture capabilities that address the security aspects of the business and technology architectures
EA Enablers		Enterprise Architecture delivery support, automation, effectiveness and sustainability
	EA Framework	Foundational structure, or set of structures, which can be used for developing a broad range of different architectures. It should describe a method for designing a target state of the enterprise in terms of a set of building blocks, and for showing how the building blocks fit together. It should contain a set of tools and provide a common vocabulary. It should also include a list of recommended standards and compliant products that can be used to implement the building blocks.
	EA Approach & Methods	Process for approaching the definition, development and execution of Enterprise Architecture in a structured and repeatable manner
	EA Tools	Automation of the EA Framework and Methods
	EA Repository	Logical or physical facility that captures architectural content to classify, retain, associate relationships, analyse it to effectively manage Enterprise Architecture assets

5.4. Mandatory Service Documentation

This appendix defines the minimal set of content that should be provided as part of any service implemented providing citizen services. Section is grouped into subsections – one per each of the documentation assets

5.4.1. Business Case and Technical Approach

Document/section of the service definition that provides information on the needs that solution is going to address and sketch of the technical approach allowing assessment of reuse (reuse of other existing services and potential reuse of the service being created), adherence to principles and constraints of the enterprise architecture.

Covers:

- Business requirements;
- Process(es) to be improved;
- Information assets/needed used (also might mean integration);
- Non-functional requirements;
- High level technical approach (logical architecture/sketch);
- Hosting plan.

Enables the evaluation of the initial investments required, allows for prioritization of initiative to implement the service planned.

5.4.2. Context

Document/section of the service definition that provide more details on the users of the solution (people and systems) and identifies full list (or representative amount of main services) that solution will support.

Covers:

- Personas (people and external systems or system groups);
- User stories (user story, value statement "so that", acceptance criteria).

This information enables assessment of full set of users to be involved, adoption and change management effort to be required as part of solution implementation, this also enables more precise estimation of technical implementation effort to be performed by internal teams or even external vendors.

5.4.3. Architectural Design

Document/section of service description identifies internal service components to be introduced, their internal and external dependencies, examples of control flow through these components to showcase the scenarios supported. It also contains high level design of the internal solution components.

Covers:

- System context (full list of external dependencies);
- Application architecture (internal and external components, their interdependencies);
- Component design (for each component) indicating reuse;
- Mapping to platforms/technologies used to implement the solution;
- Infrastructure view (whenever new infrastructure elements are introduced);
- Deployment view (information on how solution is designed for deployment and upgrades);
- Supportability view (information on monitoring/management/DR elements included in the solution);
- Security view (information on dedicated security controls/cross-cutting elements).

Documentation enables team supporting the solution and developers improving the solution to understand the main concepts of the solution, its architecture and design approach so that changes can be introduced with the least risk of introducing regression.

5.4.4. Deployment Guide

Document/section of service description provides guidance to DevSecOps on steps to follow to deploy solution, upgrade it to new version or deploy a bug fix. It also defines the pre-requisites and configuration parameters that exist for solution to be correctly deployed.

Document enables DevSecOps team to operate the solution as intended by implementers. Ideally the deployment guide should be short and reference automation that is implemented in the solution for its deployment/upgrade.

5.4.5. Administration Guide

Document/section of service description provides information on operational tasks to follow when running the service in production.

Covers:

- Configuration parameters that can be adjusted/reconfigured;
- Scale-up/scale-down approach and steps;
- Backup/restore for data and configuration of the solution;
- Management of application users/integrated systems (how to add/change user or external system accessing the solution);
- Monitoring approach and alerts/events for special attention based on health model of the solution;
- Identification of special events (peak loads expected for service etc.);
- Management tools to use to manage various aspects of the solution.

Document enables DevSecOps teams to efficiently manage the solutions they are hosting in production, ensure appropriate SLAs as per solution design and requirements.

5.5. Technical Initiatives

List of technical initiatives with identified initial sourcing strategy, assessed relative size and value, link to common capabilities getting enhanced and list of depending projects, as well as business value reasoning is provided in Table 13.

Table 13. Technical initiatives, their relative value, size and implementation reasoning

Initiative	Description	Initial sourcing strategy	Size	Value	Capabilities	List of depending projects/initiatives	Depends on	Why?
Implement documentation and configuration repository and devops pipeline	Documentation library wiki style to manage documentation in collaborative environment. Hosted GIT solution for all teams on-boarded Implement devops pipeline (build/deploy/test) and support on demand development/test environments.	Buy Public cloud	3	1	5	All new DSS run projects Projects of departments adopting the approach Transformation of ICT		Lack of information/ documentation on currently implemented services (especially when outsourced) Lack of reuse of services/code that otherwise would be possible (as per IP ownership clauses) Adopting latest development practices to achieve higher velocity, more visibility into project execution
Create usage tracking service	Usage tracking service with predefined approach for capturing different types of events Usage tracking reporting Support for standard tracking (web traffic, for example) and custom events for specific business relevant event tracking	Buy Public cloud	2	1	19	All new DSS run projects Projects of departments adopting the approach		Getting insights into value of services implemented through usage statistics Insights for executives Transparency (if shared to broader public)
Implement API management	Tools to publish and manage APIs, their versions and revisions Tools to define products and manage subscriptions Guidance for developers on what APIs should look like, security options that are allowed	Buy Hosting TBD	2	2	8	All new projects * Add projects that can share data, e.g., license validation		Sustained development/evolution of functionality over time via contracts managed through APIs Enabling only once access via data sharing G2G via API
Implement Audit service	Service to capture different audit records from various systems Audit non-repudiation (backup etc.) Audit reporting	Extend existing	2	2	12	All new services	Identity to track user related actions	GDPR requirement support Citizen insights into actions taken against their data
Implement Notification Service	Notification service as a shim on top of SMS provider, E-mail providers and GovUK Notify to push notifications, leverage template approach Has API to send/receive notifications, had admin/dev interface to manage notification types	Extending existing	1	3	2	Inbox/outbox (Secure Messaging) LPS Nova	Gov UK Notify SMS provider E-mail provider Identity/Profile dependency	Notifications linked to citizen profile enabling review through many channels
Implement Notification Service: Add PNS delivery	Notifications over PNS to deliver messages to mobile app (when it is implemented)	Extend existing	1	1	2	-	PNS provider Identity/Profile dependency Mobile Core	New notification channels not supported by Gov UK Notify, e.g., mobile app or notifications via web

Initiative	Description	Initial sourcing strategy	Size	Value	Capabilities	List of depending projects/initiatives	Depends on	Why?
Implement external identity hub	Federation hub - uses NIDA, GovUK Verify, Banks New profile system to support many credentials, different account types Exposes modern auth protocols - Oauth/OPenID Connect Admin screens to create/view profiles manually by admin Admin screens to register APIs and users of those APIs Subscription services support in profile	Buy+Build/Extend	4	5	6	MyNI LPS Nova Delegation - Child birth registration	NIDA Social networks GovUK Verify	Supporting multiple login providers, including social Having identity that spans countries Foundations for supporting multiple profile types (including organisational/business profiles) Rich profile enabling subscription services and service delegation
Implement business user support in identity hub	Adding business user support to identity hub so that users can log in as representatives of their companies, delegation as part of this to allow on behalf	Extend existing	4	4	6	OIDA Party Hub	Identity hub Service Catalogue Gov Gateway	Enabling eServices for businesses provided to their representatives or delegated people
Implement structured service catalogue	Supporting all types of service delivery (in-person, web, mobile, phone,…) Supporting service and service transactions Supporting reuse of service catalogue in different channels Subscription services support Portal part of service catalogue implemented as art of this	Extend existing	3	4	16	LPS Nova - subscription services	Portal core	SLA tracking for services Support for multiple channels of delivery Supporting not only e-services, but all service modes Support for service audiences (business, citizens, foreigners)
Implement inbox/outbox (secure messaging)	Electronic document exchange with government API for all action Portal pages of inbox outbox Admin pages of sending/receiving messages by government part of it	Reuse/ customize/buy	3	4	9	DAERA LPS Child birth registration Digital Toolkit	Citizen identity and profile Portal Core	End-to-end electronic communication with citizens and businesses Interaction history with government accessible to citizens
Implement hybrid delivery for secure messaging	Implement hybrid delivery support where for those not having "online account" the letters are printed out and delivered manually. No confirmed delivery.	Extend existing	1	1	9		Mass snail mail provider	Internal benefit of optimizing notifications with citizens - the same channel of sending documents regardless of notification channel
Implement headless content management	Expand content management to support product agnostic APIs to get the content in multiple channels. Expand content types to support elements for different channels, e.g., small description, large description, resized images.	Extend existing	3	3	11	MyNI Council systems Other mobile apps (e.g., Sport NI)		Support for multiple channels Publishing data on council web sites to reuse valuable content

Initiative	Description	Initial sourcing strategy	Size	Value	Capabilities	List of depending projects/initiatives	Depends on	Why?
Implement core personalized core portal experience	NIDirect portal extension or new portal Responsive UI to support mobile first Notifications, New identity Content management	Extend existing	4	5	1		Content Management Service Catalogue Inbox Identity Notifications service	Enabling extensivity via internal modules (to add new services tightly integrated) and external modules so that portal becomes extensible platform
Implement common core mobile app as hub	Catalogue, common citizen services, notifications hub from government Notifications and Inbox integration New identity and service catalogue Content management IOS and Android	Custom	4	1	13		Content Management Service Catalogue Inbox Identity Notifications service	Omni channel support Enabling extensivity via internal modules (to add new services tightly integrated)
Implement feature flags service	Enables gradual release. Needs a service implemented and feature flags data shared via API. Does not include adding feature support in all modules on other platforms.	Custom	1	2	5			Gradual feature release, testing in production with beta users (ring approach)
Standardizing the employee identity	Federation enablement for partner organizations. Already done now, but might require adjustments of approach for security claims management, registration of apps etc. Standardizing internal apps to use single identity approach.	Reuse current implementation	2	4	17	Internal need Replacement for HRConnect/AccountNI		More secure internal environment not requiring many credentials for employees
Implement service delivery tracking/history	Enabling business insights into service delivery Enabling SLA tracking across all services delivered in government that use tracking Service to track the delivery Reports on top of the data for owners of the service and overall platform owners	Extend	2	2	12	Unifying NIDirect/Contact centre status information	Service catalogue Identity Usage tracking/audit (for implementation)	SLA insights for executives Insights into what services get delivered Citizen interaction log for service desk/service centre
Implement knowledge base	QA support for external users Information on serving customers for service desk/call centre Linking in external video (YouTube) Integrating QA into public portal	Leverage existing platforms	3	3	11			Reduced service request count
Implementing report/dashboard management	Shared component to implement reports on top of various shared and cached data sources Support for creating reports/dashboards Support for publishing reports to employees Support for publishing reports on portal/mobile	Buy/reuse	2	2	15	DVA for Commercial driver licenses	Portal Core Mobile Core	Consistent dynamic dashboarding environment over any data Providing "ready-made stats reports" to citizens

Initiative	Description	Initial sourcing strategy	Size	Value	Capabilities	List of depending projects/initiatives	Depends on	Why?
Implementing core case management platform	Support for many developer teams Support for extensions of workflows Custom API in front of the platform (to verify citizen Ids calling)	Buy	3	5	18, 14	Public Sector Ombudsman	Service catalogue Portal Core Mobile Core Identity Notifications Inbox (?)	Many complex case management requirements across the departments
Improving G2G data sharing and open data delivery	Platform enhancements to work against unified service catalogue Data set caching service/environment/platform Standards based data publishing via APIs Reports using reporting platform	Buy/ configure	2	4	3	Census	Service catalogue Report/Dashboard management	Enabling only once access via data sharing G2G Enabling value on top of government data via open data
Implementing chat bot core	Chat bot base experience exposing data on various channels and enabling main chat relevant dialogs - greeting, evaluation, service catalogue, QA	Buy/build	3	3	10		Service Catalogue Knowledge Base	Accessibility (audio) Multi-channel (multi new channels of interaction)
Implementing forms engine for mobile/portal	Implementing forms engine to enable faster build-out of the forms for new e-services in more "declarative way" Update service catalogue to support new type of services	Buy/Reuse	2	1	1, 13		Portal Core Mobile Core Service Catalogue	More options for e-Service implementers to build UI for their services without dependency on technology of portal/mobile
Payment/invoices service	Service that enables government to provide invoices to pay (as a result of service or before starting delivery of e-service) Enables payment right away via integration with payment gateway Had administrative screens to follow up on potential issues - service desk to raise it, but screens to view payment details, status, processing.	Build on top of external gateway(s)	3	4	20		Mobile Core Portal Core External payment gateway Case management core - Service Desk Audit	Enabling paid services Enabling multiple providers of payments over time

5.6. Solution Architecture Details

This appendix includes detailed logical service architecture for the main services identified as high priority or the ones that are necessary pre-requisites for other services and platforms to implement. Each of the detailed service descriptions is provided in its own subsection.

5.6.1. Identity Management

Figure 22 shows the logical architecture of the identity management related services of the overall solution.

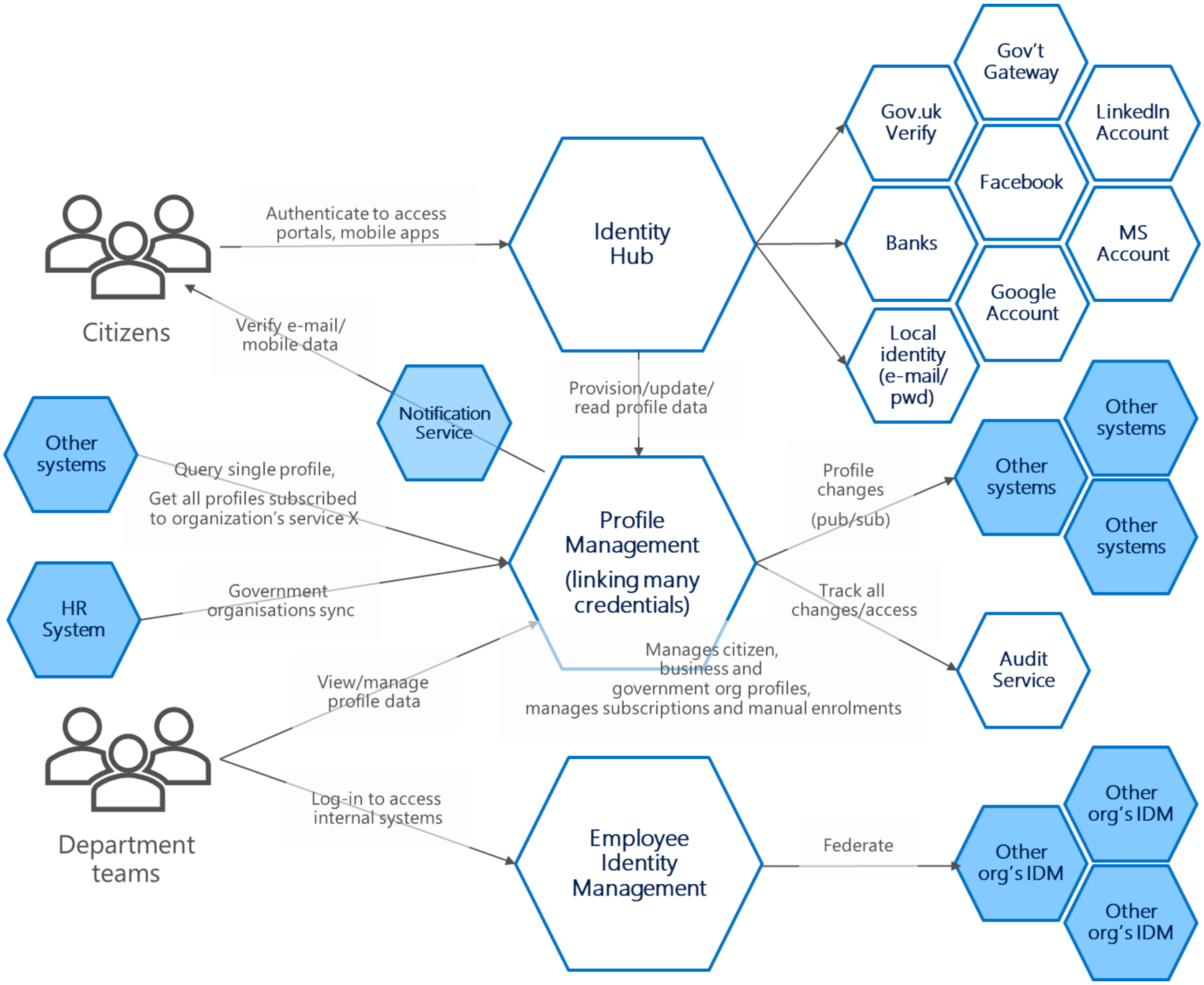

Gov't Gateway
Gov.uk Verify
LinkedIn Account
Facebook
Authenticate to access portals, mobile apps
Identity Hub
Banks
MS Account
Citizens
Google Account
Verify e-mail/ mobile data
Local identity (e-mail/ pwd)
Provision/update/ read profile data
Notification Service
Other systems
Other systems
Other systems
Query single profile,
Get all profiles subscribed to organization's service X
Profile changes
(pub/sub)
Other systems
Profile Management
(linking many credentials)
Other systems
HR System
Government organisations sync
Track all changes/access
Manages citizen, business and government org profiles, manages subscriptions and manual enrolments
Audit Service
View/manage profile data
Log-in to access internal systems
Department teams
Employee Identity Management
Federate
Other org's IDM
Other org's IDM
Other org's IDM

Figure 22: Logical architecture of the identity management services of the overall solution

As the main components it shows:

- Identity Hub – providing identity federation with different identity providers, including Local Identity (provided by NIDA at present);

- Profile Management service – holding information on the citizens, non-residents, business representatives and government organizations, holding their verified contact information, also holding information on user subscriptions to government services;
- Employee Identity Management – includes identity provider, identity federation service and profile and permissions store for government employees and partners providing citizen services on behalf of government.

Note that logical architecture identifies supporting services that are required to implement required future state functionality:

- notifications service to send out various profile related notifications, validate user e-mail and phone number;
- audit service to track sensitive changes or information access;
- various citizen and business representative identity providers responsible for providing claims about citizens;
- other systems that can either query profile or subscribe to profile change feed;
- HR system that provides government structure information into profile management to enable tracking of government "actors" using the same profile model as businesses are tracked within the profile.

5.6.2. API Management

Figure 23 provides logical architecture view of API management capability showing multiple internal services and identifying multiple external components/services that leverage API management or are used by API management.

Note that API management is "glue" component that is not externally visible (except to developers accessing API information when planning to call other systems) yet is very important to ensure sustainable service evolution over time. It enables redirection of APIs to new systems implementing them, enables versioning and API revisions. All that helps to decouple backend service API implementation from actual APIs exposed to users.

API management and Service Catalogue are linked where APIs defined on API management layer get defined in service catalogue as well to define what scopes are required for other systems to call APIs. Depending on needs, additional automation can be implemented to automatically manage the permissions of access to services on API management via permissions granted on Service Catalogue and stored against Government organisation profile. Note that ultimately permissions need to be controlled by services themselves as there are both functional and data access controls needed, yet API management would be able to check and enforce functional access permissions.

Systems using API management are:

- Government systems accessing functionality of other government departments or common components;
- Channel components accessing systems of government on behalf of users (citizens, business representatives or non-residents).

Core components of the API management capability are:

- API Management Portal/API used to manage the API definitions, products and subscriptions, configure various policies to be enforced;
- API Management Gateway – the one that receives all external calls and forwards them as per defined policies to relevant backend services;
- API Management Developer Portal used by developers to learn about approaches of using APIs, learning API definitions and even testing calls to backend APIs.

Usage tracking is an important dependency of API management that enables all incoming calls to be traced to enable both insights into service popularity, but also debugging any error situations/conditions.

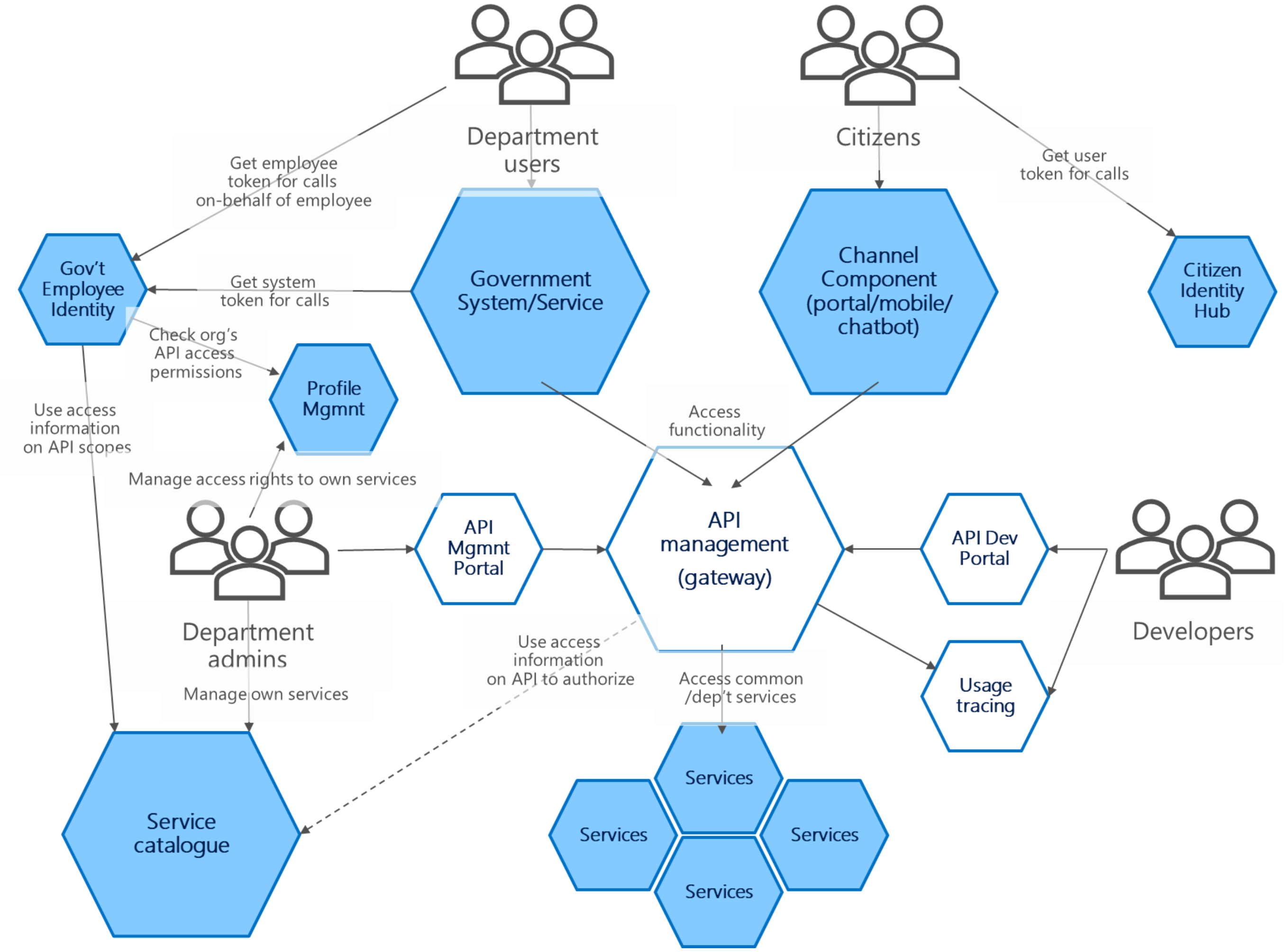

Department users
Citizens
Get employee token for calls on-behalf of employee
Get user token for calls
Gov't Employee Identity
Get system token for calls
Government System/Service
Channel Component (portal/mobile/ chatbot)
Citizen Identity Hub
Check org's API access permissions
Profile Mgmnt
Use access information on API scopes
Access functionality
Manage access rights to own services
API Mgmnt Portal
API management (gateway)
API Dev Portal
Developers
Department admins
Manage own services
Use access information on API to authorize
Access common /dep't services
Usage tracing
Service catalogue
Services
Services
Services
Services

Figure 23: Logical architecture of API management capability

5.6.3. Notification Service

Figure 24 shows the logical architecture of notifications service. It follows the service implementation pattern defined in section 3.2.1 where each service has:

- one or more citizen user interface components implemented on relevant platform;
- exposed APIs available to both citizens and government systems (leveraging appropriate identity solutions);
- backend components implementing the functionality that interact/integrate with other external services required;
- backend administrative UI that enables management of templates for notifications by government employees and that allows notifications to be sent out to groups of users manually.

Given citizen, business representative and even government organisation contact information is managed within profile management solution, this service depends on rich profile management to get the preferences of notification delivery and validated delivery addresses from profile management.

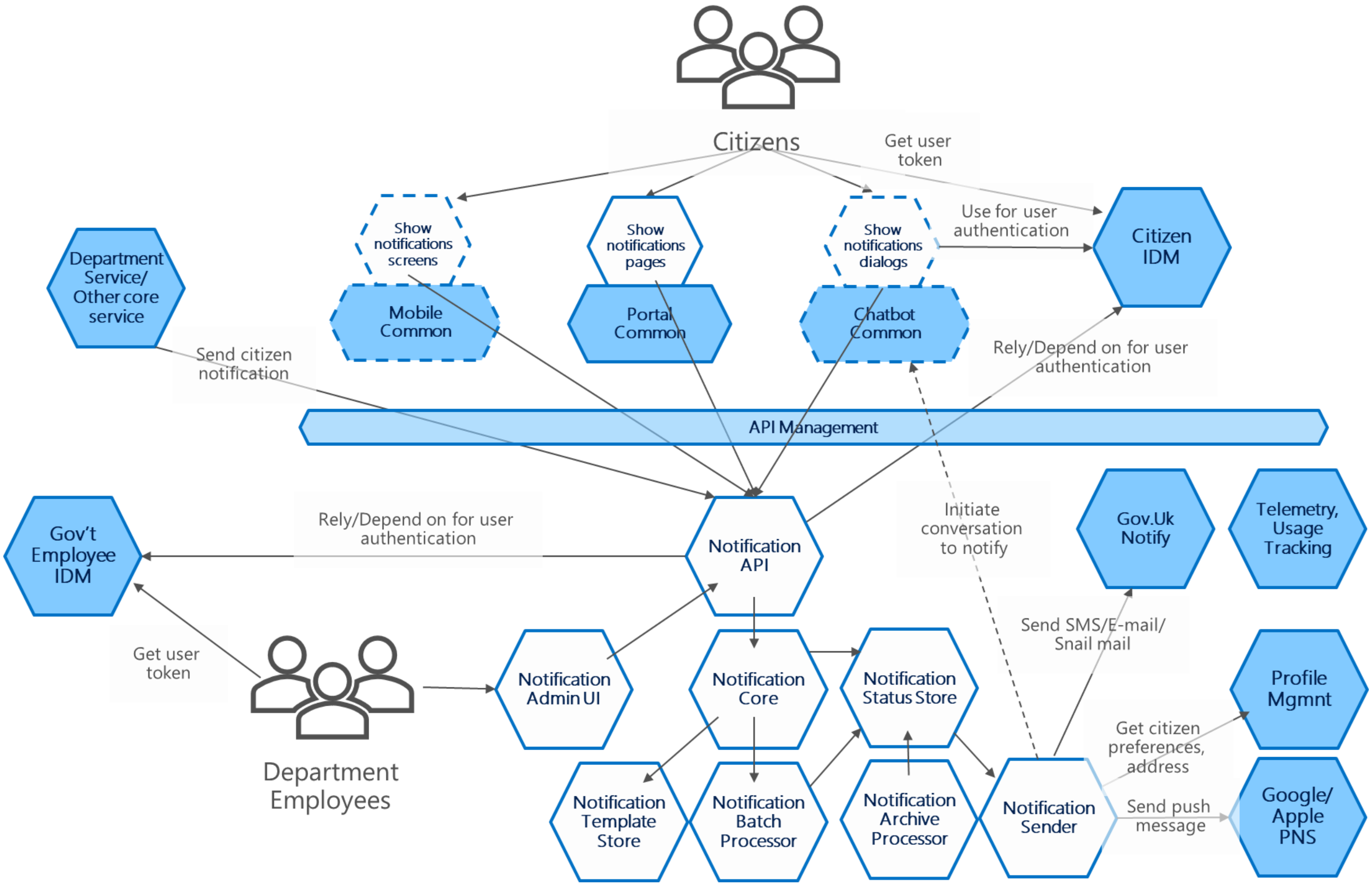

Citizens
Get user token
Show notifications screens
Show notifications pages
Show notifications dialogs
Use for user authentication
Citizen IDM
Department Service/ Other core service
Mobile Common
Portal Common
Chatbot Common
Send citizen notification
Rely/Depend on for user authentication
API Management
Gov't Employee IDM
Rely/Depend on for user authentication
Notification API
Initiate conversation to notify
Gov.Uk Notify
Telemetry, Usage Tracking
Get user token
Send SMS/E-mail/ Snail mail
Department Employees
Notification Admin UI
Notification Core
Notification Status Store
Profile Mgmnt
Get citizen preferences, address
Notification Template Store
Notification Batch Processor
Notification Archive Processor
Notification Sender
Send push message
Google/ Apple PNS

Figure 24: Logical architecture of notification service

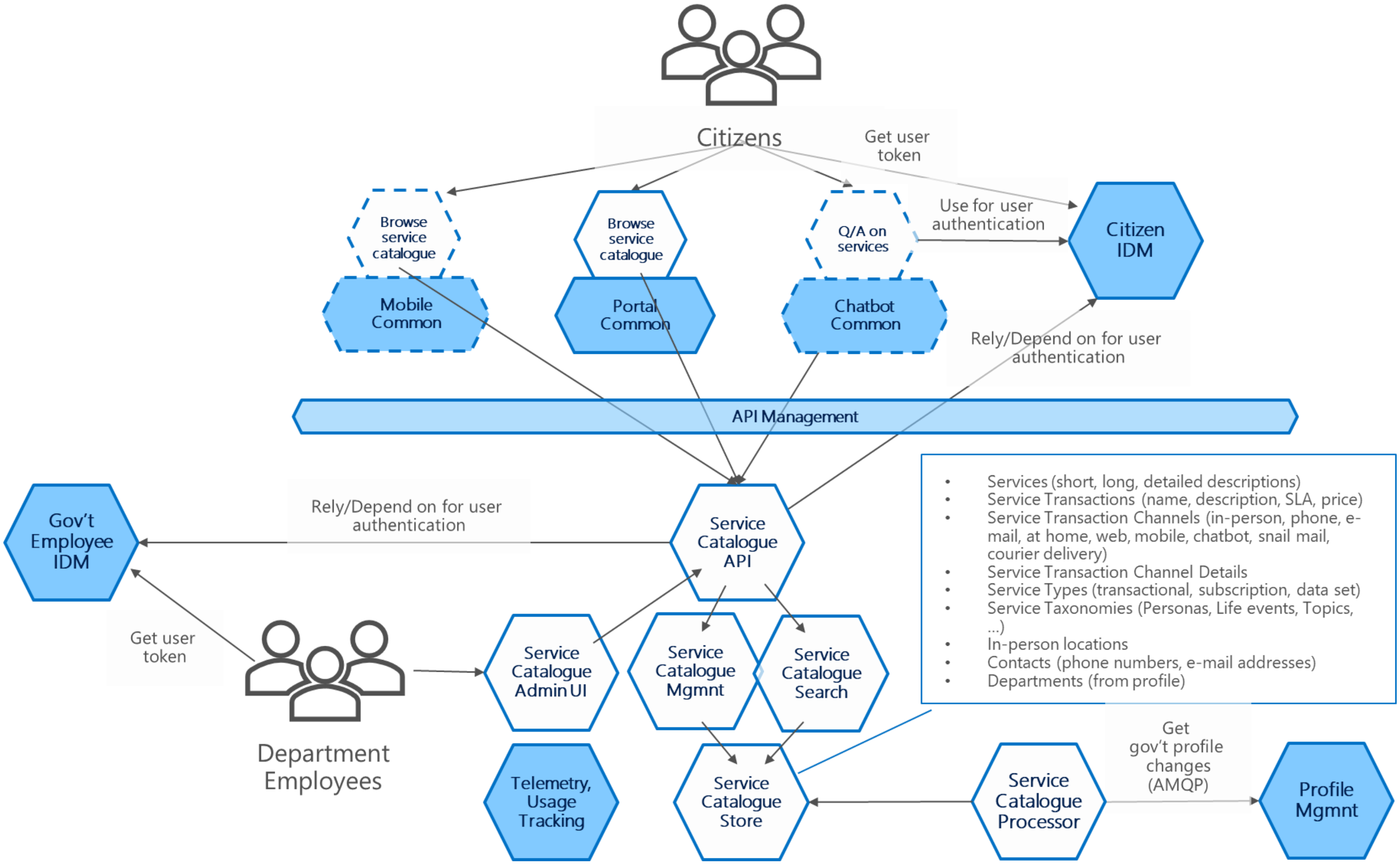
5.6.4. Service Catalogue

Service catalogue is one of the most central components of the citizen services enablement because it provides information not only for citizens to browse and find the required services, but also it is used to link service delivery information to, subscriptions and even API/service access security information (through the profile).

Logical architecture of the service catalogue capability components is shown in Figure 25. It shows that the service catalogue implementation also follows defined architecture pattern separating user experience components in multiple channels from the actual service implementation exposing citizen and government system functionality though APIs.

Administrators manage the service catalogue through administrative UI secured using government employee identity management solution. The main data types to maintain in a structured service catalogue are provided as examples in the comment included in the figure.

Beyond administrative functionality required to manage the catalogue, important functionality is catalogue search that be rich and should support refiners based on taxonomies, filtering based on audiences etc.



- Services (short, long, detailed descriptions)
- Service Transactions (name, description, SLA, price)
- Service Transaction Channels (in-person, phone, e-mail, at home, web, mobile, chatbot, snail mail, courier delivery)
- Service Transaction Channel Details
- Service Types (transactional, subscription, data set)
- Service Taxonomies (Personas, Life events, Topics, ...)
- In-person locations
- Contacts (phone numbers, e-mail addresses)
- Departments (from profile)

Figure 25: Logical architecture of Unified Service Catalogue capability

5.6.5. Inbox/Outbox

Figure 26 provides schematic view of services/components of the inbox/outbox capability also known as secure messaging that enables secure and fully digital exchange of messages and documents between citizens/business representatives and government departments/institutions.

Service implementation follows defined architecture pattern separating citizen UI components from backend components. Functionality to citizen channels and other government systems that need to interact with inbox/outbox is provided via APIs secured using appropriate identity management solution.

Inbox Admin UI is used by government institution employees to manage institution inbox (see received messages) and send messages/documents to citizens.

To notify citizens and government department employees about documents arriving in their inbox, solution depends on notification service that is being accessed via its APIs. Also, as each profile needs its inbox, solution subscribes to profile changes feed from profile management.

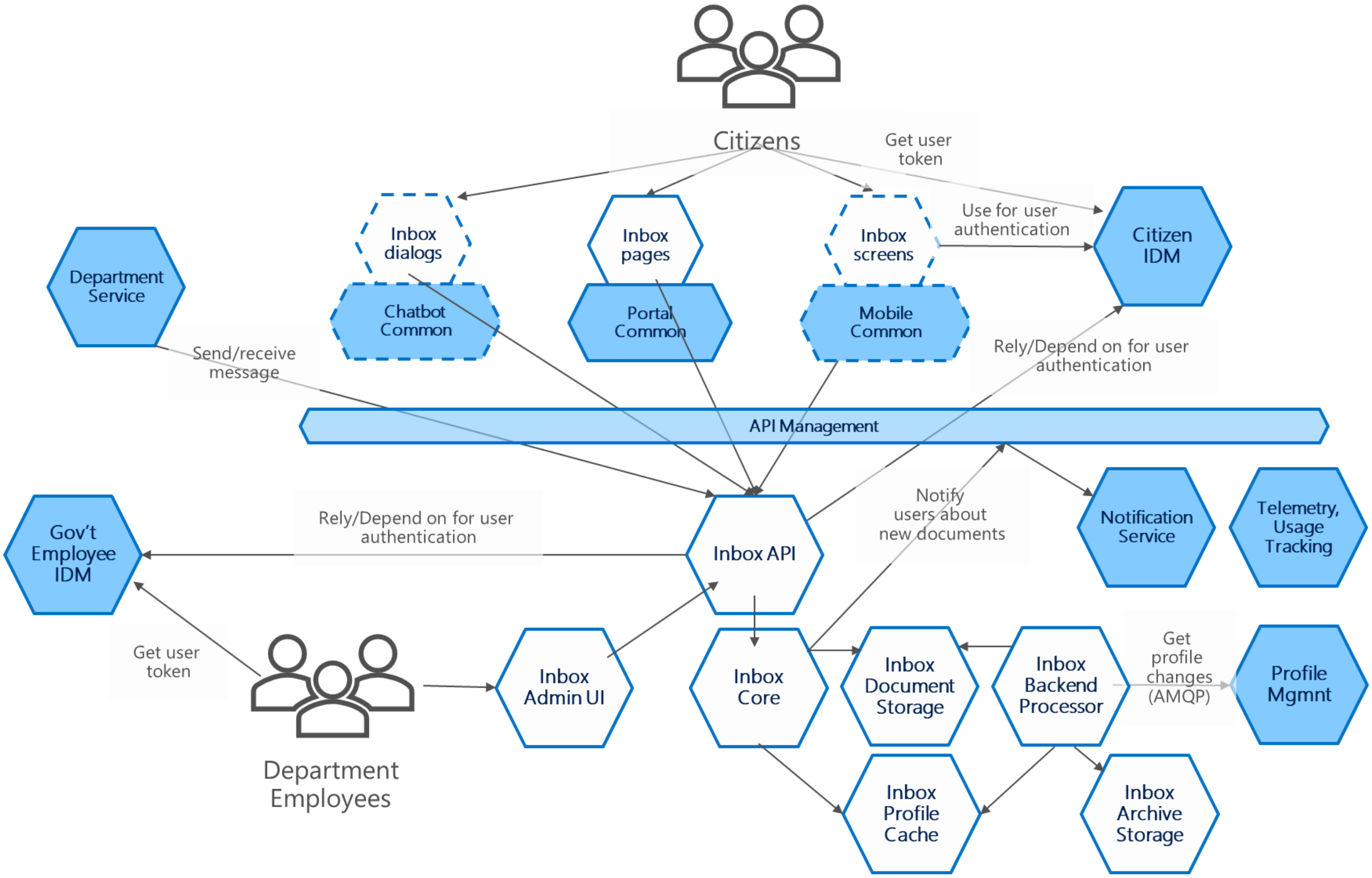


Figure 26: Logical architecture of inbox/outbox aka secure messaging capability

5.6.6. Citizen Portal

Figure 27 shows logical architecture of common citizen portal. Beyond showing the possible design for the citizen portal itself, this figure also illustrates the extensibility approach for other platforms as well.

The portal capability is made up of:

- common portal framework and tightly integrated modules (e.g., profile UI);

- specialized external portal that follows implementation guidance, but is implemented as separate solution hosted on the next-gen hosting environment (web apps cluster/service or container cluster) enabling more reuse from infrastructure perspective;
- specialized external portal that follows implementation guidance for portal, but is hosted using IaaS environment, limiting reuse to be only at virtual machine hosting environment.

Because most of the reuse and best user experience is achieved by tight module integration into UI, the preference should be building integrated UI modules instead of specialized portals where possible.

As for the tightly integrated modules, figure shows some of the UI elements of the other common services owned/provided by DSS – profile, authentication, inbox, notifications etc. At least these common component UI elements would need to be done in this tightly integrated mode for the benefit of user experience. Specialized portals are integrated via SSO and common UX guidance, but still the experience changes when navigating from common portal to any specialized one.

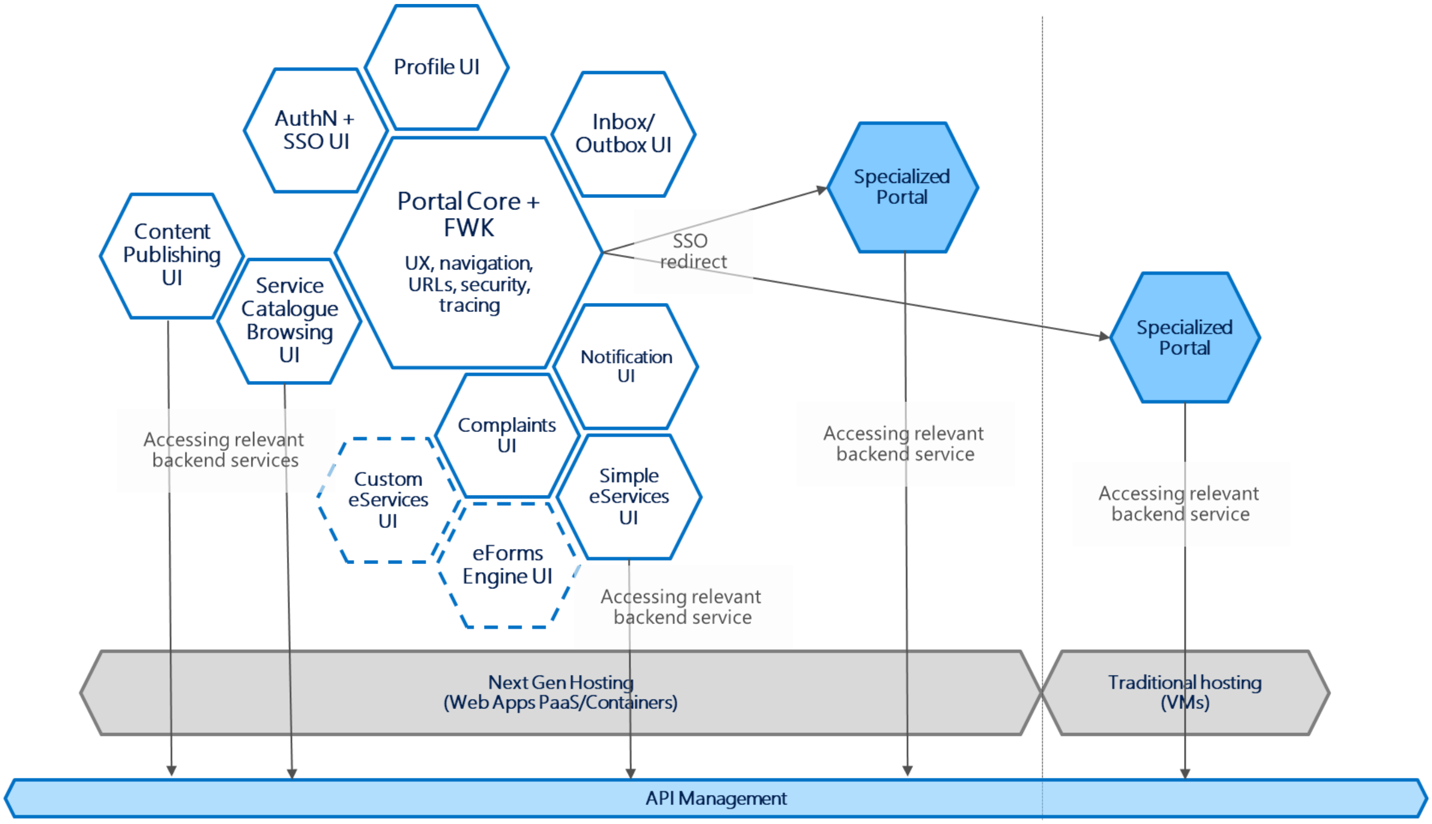

Profile UI
AuthN + SSO UI
Inbox/ Outbox UI
Portal Core + FWK
UX, navigation, URLs, security, tracing
Content Publishing UI
Service Catalogue Browsing UI
Notification UI
Complaints UI
Custom eServices UI
Simple eServices UI
eForms Engine UI
Specialized Portal
SSO redirect
Specialized Portal
Accessing relevant backend services
Accessing relevant backend service
Accessing relevant backend service
Accessing relevant backend service
Next Gen Hosting (Web Apps PaaS/Containers)
Traditional hosting (VMs)
API Management

Figure 27: Logical architecture of citizen portal capability, services providing portal experiences for citizens